

Using the Identity Panel Suite

Course code A801

Using the Identity Panel Suite

Course Number: A801

Module 1: The Identity Panel Suite

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Module Overview.....	1
Lesson 1: Overview of the Identity Panel Suite.....	2
Identity Panel Suite - Overview.....	3
Introducing Identity Panel	4
Identity Panel.....	4
Uplift for MIM	5
Identity Panel Continuous History.....	5
Introducing HyperSync Panel	6
What is HyperSync Panel?.....	6
Synchronization.....	6
Hyperverses.....	7
HyperSync Panel and MIM	7
Introducing Service Panel.....	8
What is Service Panel?	8
User Management.....	9
Service Desk and Administrators.....	9
Security.....	9
Dependence on Identity Panel.....	10
Introducing Access Panel	11
What is Access Panel?.....	11
Entitlement Management	11
Just in Time	12
Other Features.....	12
Access Review	12
Dependency on Identity Panel.....	13
Introducing Test Panel.....	14
What is Test Panel?	14
Synchronization Engines	15
Test Structure	15
Dependency on Identity Panel.....	15
Lesson 2: Identity Panel Basics.....	16
Getting Data in	17
Providers	17

Silos..... 17

Schedules and scans..... 18

Viewing Data 19

 Dashboards..... 19

 History..... 20

 Reporting..... 21

 Time Traveler 22

Lab 1: Tour of Identity Panel 24

Module Overview

Module Overview



- Overview of the Identity Panel Suite
- Identity Panel Basics
- Lab 1:

www.oxfordcomputertraining.com

www.softwareidm.com

In this module we will look at the applications in the Identity Panel suite and take a look at Identity Panel which underpins all of them.

Lesson 1: Overview of the Identity Panel Suite

Lesson 1: Overview of the Identity Panel Suite

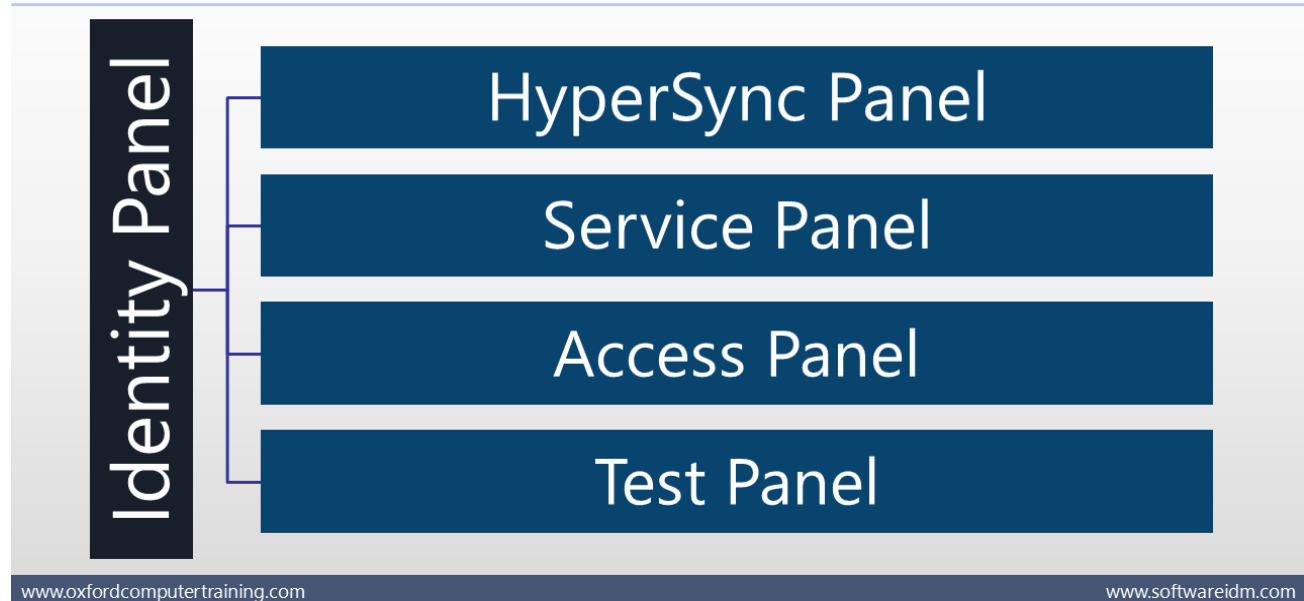


- Identity Panel Suite - overview
- Introducing Identity Panel
- Introducing HyperSync Panel
- Introducing Service Panel
- Introducing Access Panel
- Introducing Test Panel

In this lesson, we look at the various applications in the Identity Panel suite.

Identity Panel Suite - Overview

Identity Panel Suite – Overview



The Identity Panel suite is comprised of the following applications:

- Identity Panel - a vendor neutral identity management umbrella for companies managing identities, identity lifecycle systems, and identity platforms. It is the core component required by the other 4 applications.
- HyperSync Panel - a fully customizable synchronization engine to propagate identity information across systems.
- Service Panel - a customizable portal for fulfilling self-service identity management requests, and approvals.
- Access Panel - a governance application that can provide Roles Based Access Control (RBAC), Attribute Based Access Control (ABAC), Access reviews (AKA Attestation, certification, or recertification), and Just in Time (JIT) access management/Privileged Access Management (PAM).
- Test Panel - provides automated testing for identity lifecycle and provisioning systems.

Introducing Identity Panel

Introducing Identity Panel



- Identity Panel is a flexible tool for monitoring and analyzing operations and data from disparate identity repositories:
 - Directories such as: Active Directory (AD) and Azure AD
 - Sources of truth such as: Workday and SQL Server-based HR systems
 - Other services such as: AD FS, Office 365
- It can present a joined-up view of each identity, its lifecycle, its relationship to other identities, and also of operational activity
- It has comprehensive reporting capabilities and a powerful workflow engine
- It can monitor and analyze (and to some extent control) synchronization systems such as MIM, Azure AD Connect, and Azure AD Connect CloudSync (and include data to which they have access)
- Uplift for MIM- to support and enhance MIM
- Identity Panel stores a continuous history of the data it collects when it regularly scans systems for changes
- Identity Panel is the core product in SoftwareIDM's Identity Panel Suite

www.oxfordcomputertraining.com

www.softwareidm.com

Identity Panel

Identity Panel is a flexible tool which can monitor and analyze identity data and operations from multiple repositories across an enterprise and present a joined-up view of each identity (across all systems), of its lifecycle, and of its relationship to other objects - and also operational activity.

Its comprehensive reporting capabilities allows you to analyze identity data, point up discrepancies, identify unused accounts, and help maintain the consistency and security of your enterprise.

Its powerful workflow engine, allows you to trigger an action based on a change to identity data such as, running a PowerShell command, sending a notification email, or disabling a user.

It can connect up to a wide variety of disparate systems including:

- Directories such as Active Directory (AD), AD LDS, and Azure AD
- Sources of truth such as formal HR systems, like Workday - and indeed just about any HR system, contractor system, student system etc. (many of these are based on SQL Server, which Identity Panel can readily access)
- Other services such as AD FS (in which, notably, claims are of interest), Office 365 (from which it can collect information about Office365 licensing, mailbox statistics, last logons etc.)

It can also monitor and analyze synchronization engines such as Microsoft Identity Manager (MIM), Azure AD Connect, and Azure AD Connect CloudSync - and indeed, can control MIM which does not

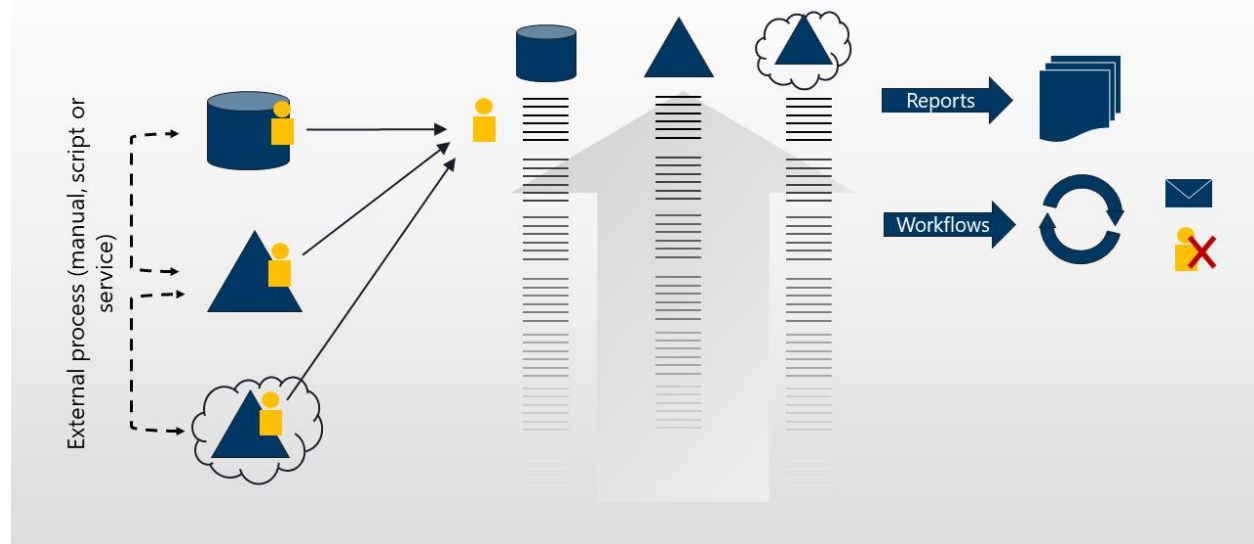
have its own scheduler or dashboard. Since these, and especially MIM, are typically connected to many other systems, Identity Panel can have access to, and can present, data from sources to which it is not directly connected.

Uplift for MIM

Uplift is an Identity Panel feature that supports and enhances MIM. Uplift allows all MA configuration to be brought into Identity Panel, and then provides a codeless approach to configuration which does not impact performance or flexibility. It is called Uplift because it undergirds synchronization logic, allowing a simpler functional syntax rather than traditional imperative logic. Uplift features are covered in a later module.

Identity Panel Continuous History

Identity Panel stores a continuous history of the data it collects – and it does so, by regularly scanning systems for changes. Clearly, for this to work reliably, a correctly configured schedule of activity is vital, and this is readily achieved with Identity Panel's built-in scheduler.



Note: Identity Panel is the core product in SoftwareIDM's Identity Panel suite - it is a dependency for all the other tools (panels) in the suite. So, for example, HyperSync Panel cannot function alone - Identity Panel needs to be in place.

Note: In the past, there was another product called Sync Panel - this is now part of Identity Panel.

Introducing HyperSync Panel

Introducing HyperSync Panel



- Synchronizes identity data between repositories
 - Provisions target systems with objects (such as users and groups)
 - Generates unique values and other expressions
 - Flows attributes
 - Deprovisions objects
- Provides support for:
 - Stateful synchronization - e.g. changes based on attribute changes
 - Event-based activity - e.g. changes based on today's date
- Can build and maintain a "Hyperverse" metadirectory
 - Based on a custom schema, and populated with authoritative data
 - Provides a unified view
 - Simplifies rule definitions where there are multiple sources and/or targets
- Requires Identity Panel for connectivity and data
- HyperSync Panel can co-exist with, or replace, Microsoft identity Manager (MIM)

www.oxfordcomputertraining.com

www.softwareidm.com

What is HyperSync Panel?

HyperSync Panel is SoftwareIDM's synchronization engine for provisioning objects such as users and groups (including the generation of unique values), deprovisioning them, and for flowing attributes (or expressions based on attributes) between them, keeping them up-to-date as changes arise.

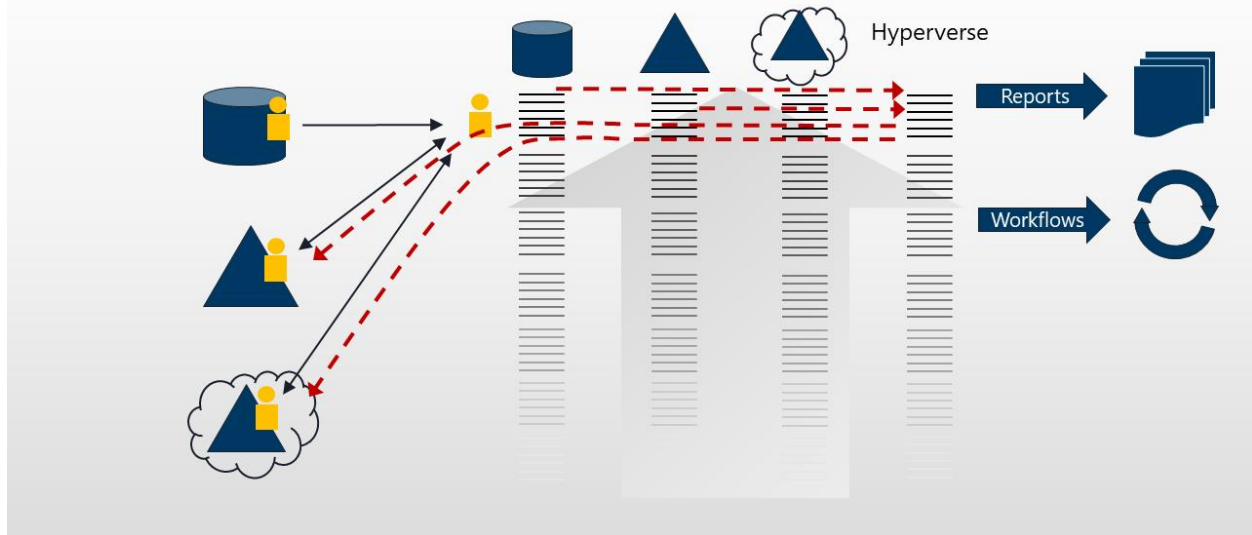
Synchronization

HyperSync Panel provides support for stateful synchronization and event-based synchronization - so that it can meet business requirements by responding to changes to the object itself, or trigger activity based on an external factor such as a date transition.

- **Stateful synchronization example:** when the user's department changes in the HR source system, HyperSync Panel can ensure that that is reflected in a target system such as Azure AD, both in terms of the department attribute itself, and any consequences such as a group membership.
- **Event-based synchronization example:** for a contractor who has an end date in the HR system, HyperSync Panel can be configured to disable the corresponding AD user account when the end date is reached.

Hyperverser

HyperSync Panel can maintain a "Hyperverser" - a metadirectory based on a schema that you define, and populated with authoritative data (objects and attributes) according to rules you define. This is useful both for providing a unified view of the authoritative data (based on multiple sources of data), and avoiding the need to repeatedly define the attribute flows that generate new attributes where there are multiple targets for those attributes. Such new attributes can involve complex expressions, including the generation of unique values (e.g. for account names).



HyperSync Panel and MIM

HyperSync Panel can co-exist with MIM, or completely replace it - HyperSync Panel includes all the functionality of the MIM Synchronization Service, and lots more besides. The Hyperverser is broadly equivalent to the MIM Metaverse.

Note: Identity Panel is a dependency for HyperSync Panel - Identity Panel provides the connectivity and data utilized by HyperSync Panel.

Introducing Service Panel

Introducing Service Panel



- Service Panel is a web-based portal for managing identity data, fully customizable, with all the features you would expect, including "Code Red"
- For all users it is a self-service application through which they can:
 - Access a "white pages" directory
 - Edit their own identity data
 - Raise and track requests
- For managers, these capabilities are extended to their reports
- Service Desk and administrators can implement, monitor and troubleshoot provisioning and other identity processes
- Service Panel can be integrated with systems like ServiceNow, extending the reach of those systems to all Identity Panel endpoints
- Security is controlled at every level, so that only appropriate objects and attributes are available to any actor
- Service Panel requires Identity Panel

www.oxfordcomputertraining.com

www.softwareidm.com

What is Service Panel?

Service Panel is a web-based portal for managing identity data and making requests, with all the features you would expect such as:

- Fully customizable look and feel, such as the logo, name, colors, and layout
- Integrated authentication (e.g. Azure AD or AD)
- Forms can be built from data across multiple systems
- Useful form inputs such as auto-complete, drop-down, value constraints, uniqueness checking etc.
- The ability to modify multiple systems from a single request
- Change request and approval processes
- "Code Red" feature

Note: "Code Red" is an action taken on instant dismissal of an employee. The organization needs to ensure that the employee no longer has access to corporate systems. "Code Red" provides you with a single "button" to disable the employee's accounts in connected systems such as AD and Azure AD, and revoke any of the employee's active sessions in Office 365 (for example).

User Management

Service Panel provides a self-service portal for all authenticated users, where users can:

- View and edit their own identity data
- Raise requests such as join a distribution list, or application access
- Track their requests with "traffic light" visuals

This capability is extended for managers so that they can view and edit the identity data of the people they manage.

It also provides a "white pages" directory (you define which attributes are visible) so that users can easily search for information (across multiple systems).

Service Desk and Administrators

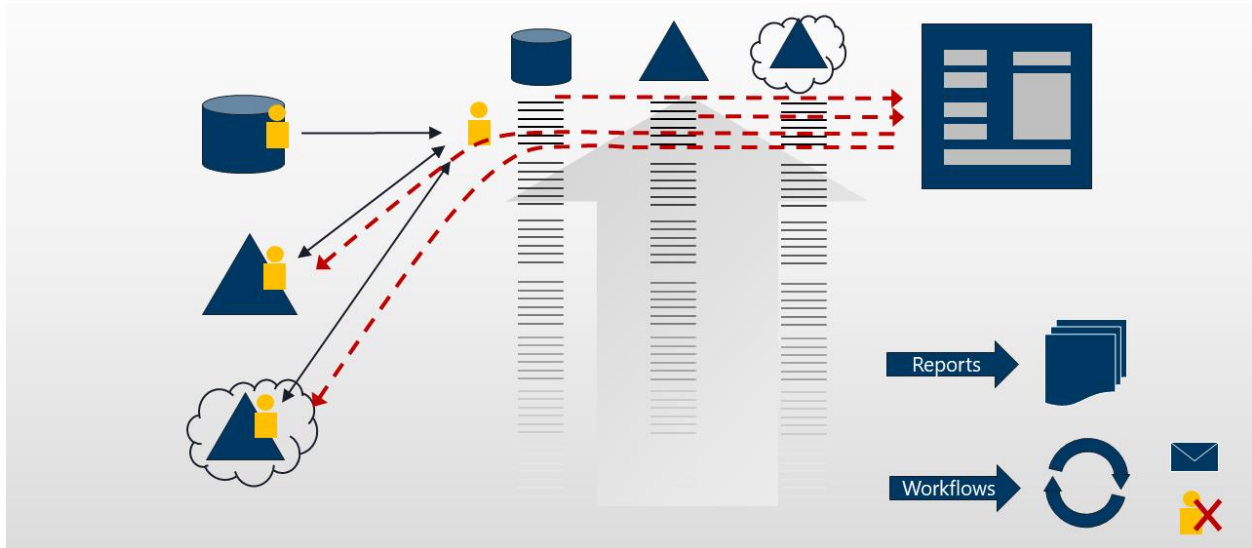
Service Desk and administrators can implement, monitor and troubleshoot provisioning and other identity processes. In Service Panel a single workflow can have one or several steps such as approvals, and changes can be written to one or more connected systems. Each step can be tracked, with success and/or failure notifications.

For example, if a user requests a mailbox in the Service Panel portal, their manager can approve it and the change will be written out to O365. The initiator (user) is able to see when the request has been approved and when it is ready for use, and Service Desk is also able to track its progress, and if the request fails, to be notified as such, and to see which steps have failed.

Service Panel includes its own workflow engine for approvals and actions, but also offers integration with your choice of workflows from ServiceNow, Microsoft Flow, and Azure Logic Apps workflows. This integration with systems like ServiceNow, extends their reach to all the Identity Panel endpoints (systems to which Identity Panel connects either directly or through a synchronization service like MIM).

Security

Security is implemented at every level, and readily configured. Security settings allow attribute and object visibility to be limited based on role membership and identity ownership - so only appropriate objects and attributes are visible/editable by any actor (for example self, manager, or Service Desk).



Dependence on Identity Panel

Service Panel is a web application, with settings and configuration controlled through Identity Panel. Service Panel is a separate application with a distinct host-name, but is not a standalone product, it requires Identity Panel for connectivity, data etc.

Introducing Access Panel

Introducing Access Panel



- An identity and resource governance solution providing ABAC, JIT access/PAM, RBAC, Access Reviews
- Entitlement
 - Entitlement management - manage group memberships, and other types of entitlements (e.g. single-value attributes)
 - Entitlement control – can be based on a role (RBAC), or attribute (ABAC), or an exception
- JIT candidates are able to activate access using a variety of policies and processes (time windows, approvals, extensions, justification forms, multiple response, escalation, expiration)
- It also provides support for native criteria (e.g. Azure dynamic groups), separation of duties (SoD), and criteria-based candidacy
- Offers a comprehensive range of access review features
 - Performed against security principals, applications, entitlements or role assignments
 - Rolling, recurring, ad-hoc, or triggered by a change (e.g. attribute, or risk level)
- Access Panel requires Identity Panel for connectivity, data, workflows etc.

What is Access Panel?

Access Panel is an identity and resource governance solution which provides:

- ABAC (Attribute Based Access Control)
- Just-in-Time access/PAM (Privileged Access Management)
- Traditional RBAC (Role Based Access Control)
- Access Reviews - attestation/certification support requests, recurring review, risk modeling, and access expiry

Entitlement Management

Types of Entitlement

Access Panel is not limited to managing traditional membership-based entitlements like groups, but also has flexibility to handle entitlements such as:

- Reference attributes
- Multi-value attributes
- Single-value attributes
- Rule-based objects

Methods for Managing Entitlements

An entitlement can be granted based on membership of a role (traditional Role Based Access Control), or on the values of particular attributes entitlements (Attribute Based Access Control). Exceptions to such rules can also be made.

Just in Time

Access Panel provides Just in Time support with candidates able to elevate their access, using policies and processes such as:

- Activation time windows
- Approval policies (owner/manager)
- Policy based on group risk and application association
- Policies based on actor (self, manager, owner)
- Multi-response request policies with escalation and reminder rules
- Enforced and optional entitlement expiration policies
- Activation extension policies with extension notifications
- Custom justification and approval forms
- Support for email, SMS, and workflow/Service Desk system integrated approval flows

Other Features

Access Panel also provides support for native criteria which cannot be directly changed by Access Panel (e.g. Azure dynamic groups), separation of duties (SoD), and criteria-based candidacy.

Access Review

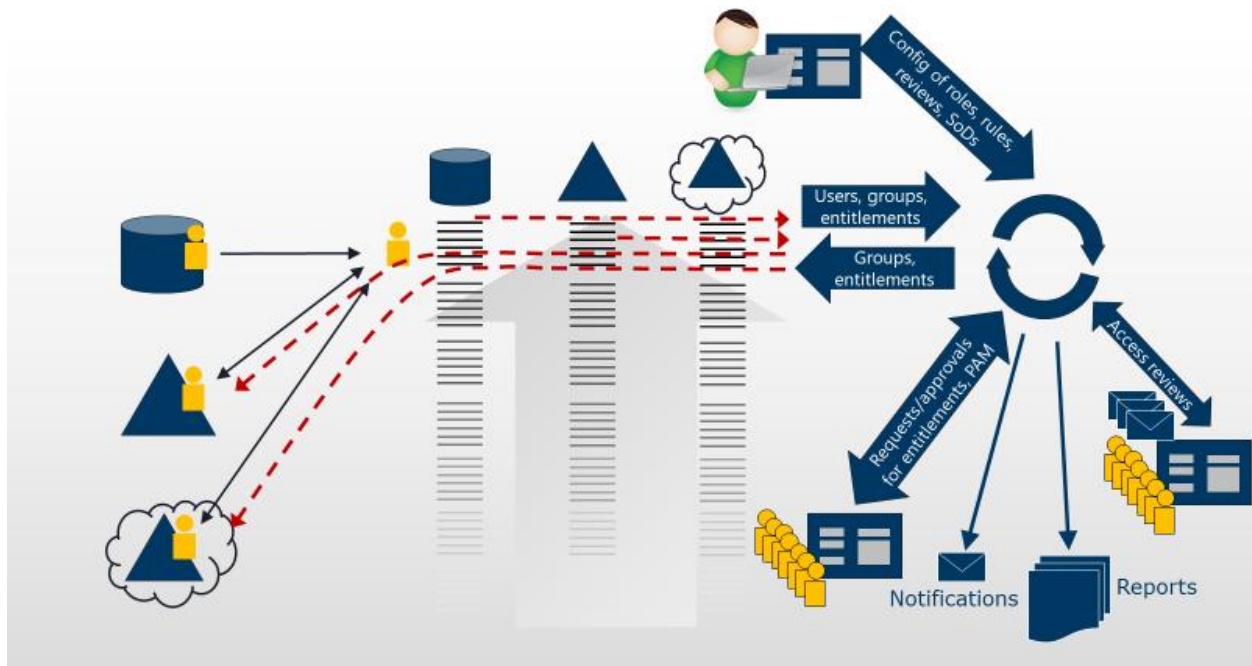
Access Reviews are also known as attestation, certification, or re-certification. In Access Panel these can take place across a wide range of object classes and filtering modes.

Access Reviews may be performed against security principals (e.g. users, groups), applications, entitlements, or role assignments. This allows organizations to review permissions directly, review the rules that drive permissions, and separately review policy exceptions and violations.

Certifications can relate to multiple modes such as entitlements (permission/membership assignments), resource ownership, or role assignments.

Access reviews may be rolling, recurring, or ad-hoc, or based on a trigger such as an attribute change, an application assignment, or a change to the risk level.

There is communication support for multiple delivery channels including email, SMS, Service Desk/Ticketing system, and workplace messaging channels such as Teams or Slack.



Dependency on Identity Panel

Access Panel is dependent on Identity Panel. It leverages Identity Panel's connectivity to offer access management across Active Directory, Azure/Office 365, database driven line-of-business applications, ServiceNow, and other platforms to which Identity Panel is connected.

Introducing Test Panel

Introducing Test Panel



- Provides two types of automated testing relating to identity management implementation (which are often overlooked):
 - Ensuring that the configuration meets the predefined business requirements
 - Regression testing after system modification
- Test Panel thus ensures that business requirements are met with accuracy and consistency, and cuts down time spent on QA and debugging
- Usually we are effectively testing a synchronization engine, such as MIM, Azure AD Connect, or HyperSync Panel
- Test structure
 - Test cases are grouped into test suites
 - Test cases are composed of fixtures, a schedule, and set of assertions to check the results
 - Usually each test case will have a corresponding reset test case
- Fixtures can be configured to emulate system changes (e.g. HR provisioning)
- Test Panel is dependent on Identity Panel

www.oxfordcomputertraining.com

www.softwareidm.com

What is Test Panel?

Test panel provides automated testing for your identity management implementation.

For example, we might expect that part of your identity management solution would be to ensure that whenever a user is entered into the HR system they are provisioned into AD and/or Azure AD with appropriate attributes and properties. So, an obvious test is to create a user in the HR system and verify the result.

There are two important types of test, both of which can be difficult and time consuming, and hence are commonly overlooked:

- Ensuring that the configuration meets the predefined business requirements
- Regression testing after system modification (applying a suite of known tests to establish that nothing has been broken)

Test Panel automates these processes, allowing tests to be run repeatedly, ensuring that business requirements are met with accuracy and consistency - and significantly cutting down time spent on QA and debugging.

Synchronization Engines

Any identity management solution will have a mechanism in place for performing actions, such as the provisioning described in the above example. Usually this will be a synchronization engine, such as MIM (for which Test panel was originally conceived), Azure AD Connect, or HyperSync Panel - so it is primarily this mechanism that is effectively being tested, and a test cycle will mostly involve testing the requirement, fixing any errors in the synchronization engine configuration, and retesting.

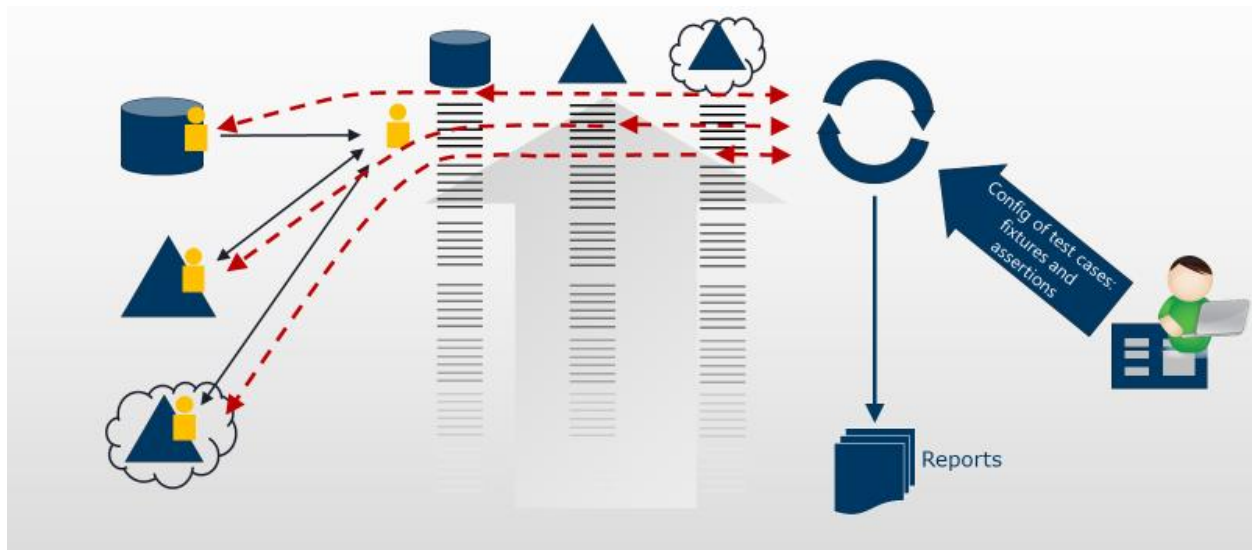
Test Structure

Test cases are grouped into test suites and break-down into:

- Fixtures that modify the data presented to the sync engine (e.g. putting a “mock” change into a Workday feed, such as creating a new user)
- A schedule to run the synchronization process
- A set of assertions to check the results (making sure an account is created in Azure AD, checking the UPN etc.)

Usually each test case will have a corresponding reset test case (to put things back as they were) so that a test can be run again and again as necessary (regression testing).

Test Panel has the ability to emulate other systems. This allows you to test your integration with other systems, without actually having access to those systems, and then promote those changes into production automatically.



Dependency on Identity Panel

Test Panel is dependent on Identity Panel, leveraging Identity Panel’s connectivity (and indeed it does not have an interface of its own).

Lesson 2: Identity Panel Basics

Lesson 2: Identity Panel Basics



- Getting Data in
 - Providers
 - Silos
 - Schedules and scans
- Viewing Data
 - Dashboards
 - History
 - Reports
 - Time Traveler

Identity Panel can import data from a variety of sources and this data can be accessed in a number of ways. In this lesson, we take a look at some of the basics in Identity Panel.

Getting Data in

Getting Data in



- **Providers** are used to connect to source systems, a number of different types are available:
 - Directories Connection, Azure Connection, LDAP Connection
 - Data Connection for Workday, SQL Connection
 - MS Sync Connection (for synchronization engines like MIM or Azure AD Connect)
- **Silos** are sets of identity data
 - Most Providers will produce one silo, e.g. Active Directory or an HR system based on SQL Server
 - Others will produce many silos, for example Azure AD Connect (MS Sync Connection) would produce one silo for each system Azure AD Connect is connected to plus itself (the "Metaverse") – the same applies to MIM
- **Schedules and scans**
 - Identity Panel scans connected systems, reading all information or just changes since the last scan - scans can be invoked manually or via a schedule
 - A schedule can include steps to scan multiple systems, or to perform other tasks such as running a PowerShell script, sending a report or truncating a log
 - The scheduler may not capture every single change

www.oxfordcomputertraining.com

www.softwareidm.com

Providers

Identity Panel can connect to various source systems in order to collect identity data. The mechanism used is the Provider. In Identity Panel, there are various Providers available, including:

- Azure connection
- Directories connection (used for on-premises Active Directory)
- LDAP Connection
- Data Connection for Workday
- SQL Connection
- MS Sync Connection - for connecting to synchronization engines like MIM or Azure AD Connect

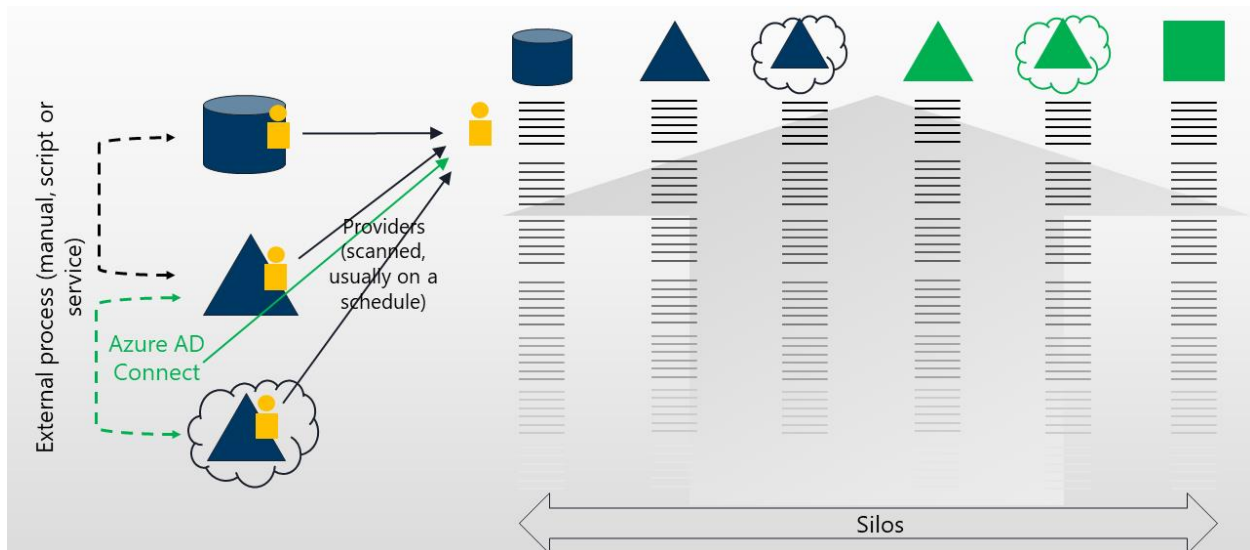
So, we might configure a Directories Connection to get data from our local Active Directory, and a SQL Connection to get data from our on-premises HR system, and so on.

Silos

Silos are sets of identity data, held in Identity Panel's database, usually having been imported (scanned) from a connected system.

Most Providers will produce one silo, for example our local Active Directory, our Azure AD tenant, or and on-premises HR system in SQL server. Other Providers may produce many silos, for example

if we configure an MS Sync Connection to get data from Azure AD Connect, this will produce one silo for each system that Azure AD Connect itself connects to, plus one for itself (the "Metaverse"):



The same applies to MIM (MIM and Azure AD Connect are basically the same technology).

Schedules and scans

Identity Panel scans connected systems, either as a result of manual intervention or on a timed schedule. Full scans re-read (and import) all the relevant data whereas delta scans only read (and import) the changes since the last scan. Clearly, delta scans are quicker to perform.

Any number of schedules can be set up to recur on a regular basis. A schedule will include a number of steps. A typical step will scan a system, but it could also perform another action such as running a PowerShell script (for example to restart a service), sending a report to an individual or a group, or truncating a log (for example, a password log).

While it may seem desirable, when configuring Identity Panel, to try keep a continuous history of identity data in the connected systems, it may not be possible that the schedules can be arranged such that the systems are scanned often enough to capture every single change. However, it should be possible to capture a meaningful history of significant changes.

Note: It is important to understand that what you see depends on when, and how often, the scheduler performs scans.

First, the apparent time of a change will depend on when a scan took place.

Second - this was mentioned above but is worth re-iterating - it is possible that not all changes have been captured. If the scheduler does not run frequently enough, or if it is not - for whatever reason - run for a period of time, the continuous history may be broken. For example, a number of changes could be made to an attribute, and only the last state recorded.

Viewing Data

Viewing Data



- Exactly what you see depends on your role and how Identity Panel has been configured
- The **dashboard** tab displays status windows, charts, tables of health statistics etc. – you can create multiple dashboards and customize them for different user roles
- The **history** tab presents a history of recent Identity Panel operations including scans and schedules – it will display failed as well as successful operations, you can filter and search the history, and further details are available through hyperlinks and mouseovers
- The **reporting** tab allows tabular reports to be generated and displayed in the browser or downloaded as a file – you can build your own reports; the point-in-time report feature allows reports to be constructed as if they were being viewed at a particular time in the past
- The **Time Traveler**
 - Allows you to see objects as they are now and in the past
 - You can explore changes to objects across silos
 - Generally access it through a particular object of interest (perhaps you searched for it, or maybe it came up as a link in a report)
 - The apparent time of a change will depend on when a scan took place, and it is possible that not all changes have been captured (depends when it was scanned)

www.oxfordcomputertraining.com

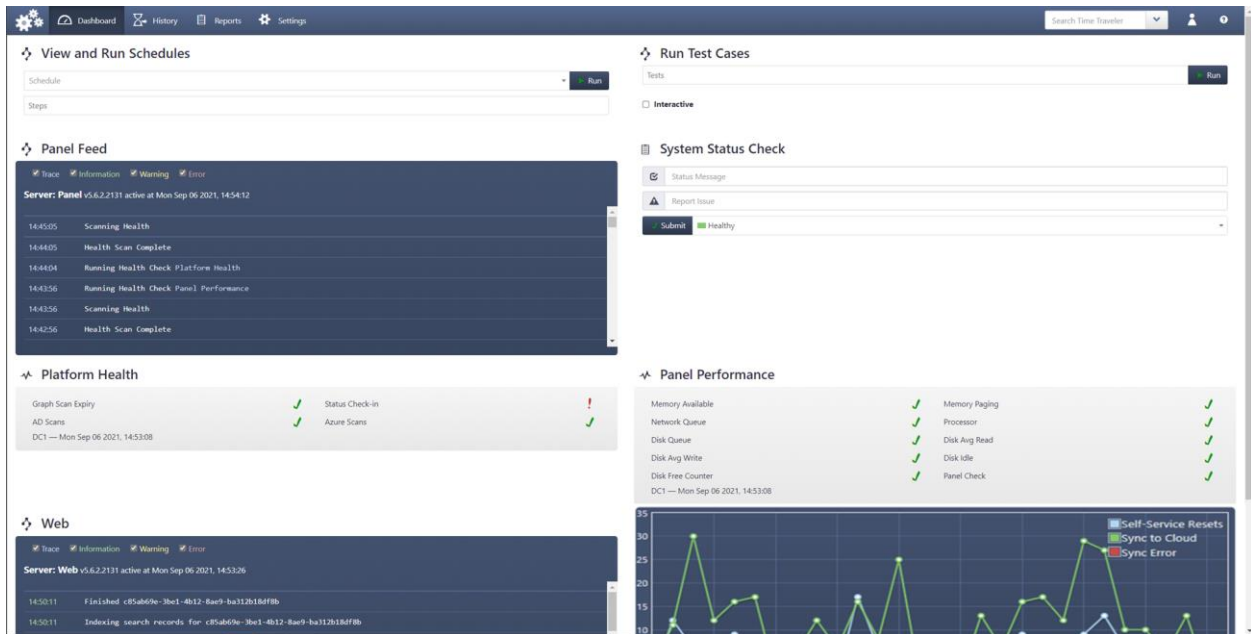
www.softwareidm.com

Exactly what you see depends on your role and how Identity Panel has been configured. You may not see all of these features - and what you do see may be limited in its scope compared to what we show here.

Dashboards

Identity Panel has various modules which can be included in a dashboard, such as:

- Charts and tables for displaying information (e.g. statistics and run history)
- Health visuals (e.g. service status, or last scan date)
- A Scheduler for running tasks manually (e.g. run a delta Azure scan, or run a maintenance task)

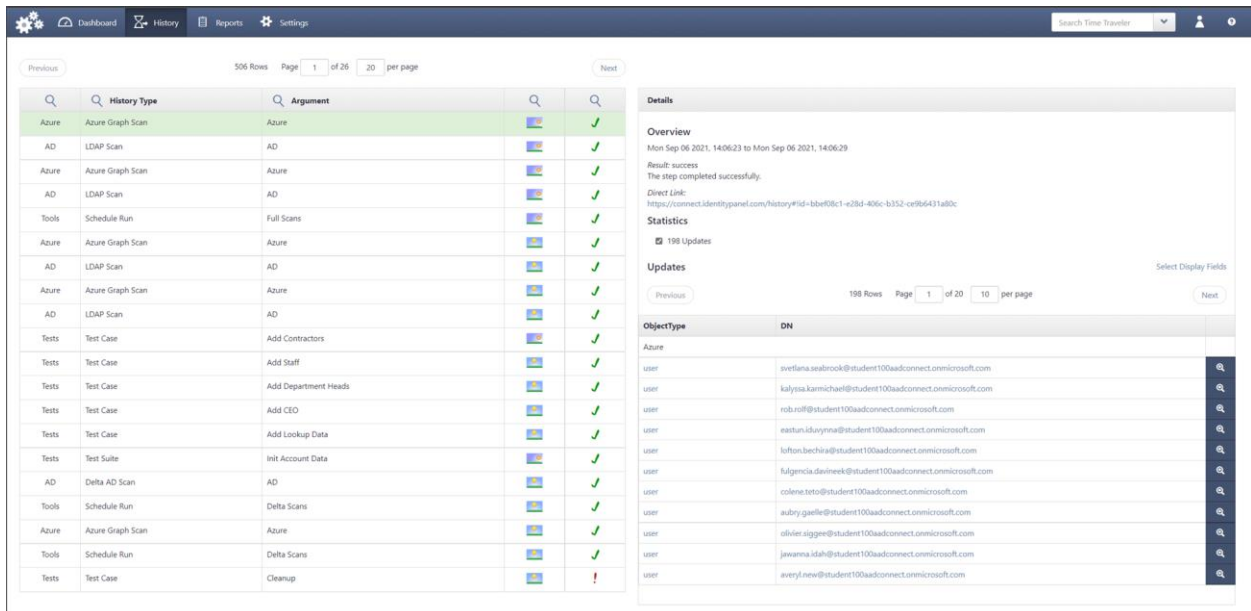


An administrator can create multiple dashboards and customize them for different user roles. Your dashboard is what you see when you first load Identity Panel.

History

The History tab presents a history of recent Identity Panel operations - such as when Identity Panel scanned various system for their latest data.

You can filter and search the history and further details are available through hyperlinks and mouseovers.



It will display failed as well as successful operations:

The screenshot displays the 'History' module in the Identity Panel Suite. The main table shows a list of operations with columns for 'History Type' and 'Argument'. The 'Add Staff' operation is highlighted in green, indicating a failure. The 'Details' panel on the right provides an overview of the failed operation, including the 'Step' table and 'Failed Fixtures' table.

Step	Result	Run By	Duration
Add Staff	!	DC1	N/A
AD Full Scan	✓	DC1	N/A
Azure Graph Scan	✓	DC1	N/A
Finalize Add Staff	✓	DC1	N/A

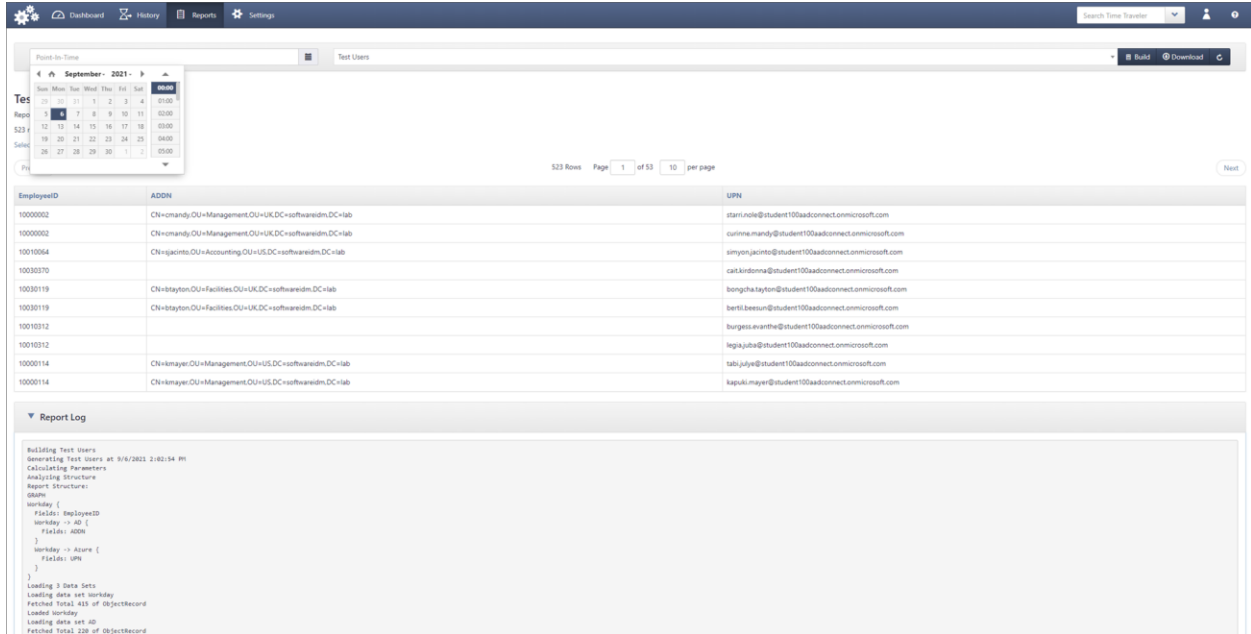
Name	Result	Type	Time Stamp
Add Staff	Fixture Failed	Load Fixture	Mon Sep 06 2021, 12:25:17
Add Azure for AD	Error	Graph Create User	Mon Sep 06 2021, 12:26:22

The history module auto-refreshes itself every 30 seconds.

Reporting

The reporting tab allows tabular reports to be generated and displayed in the browser or downloaded as files. As well as standard reports, administrators can create reports based on available identity and health data, and make them available (what is actually available to you depends on your role).

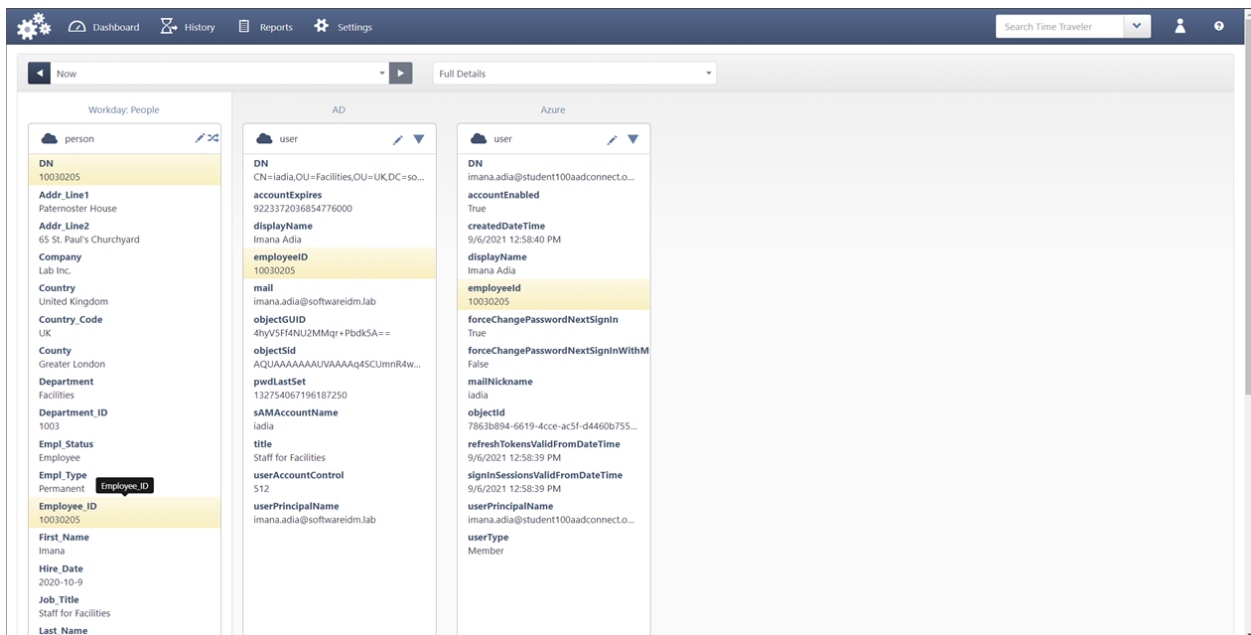
Reports may be downloaded as Excel, Attribute Value Pair, Tab Delimited, or JSON files.



The point-in-time report feature allows reports to be constructed as if they were being viewed at a particular time in the past.

Time Traveler

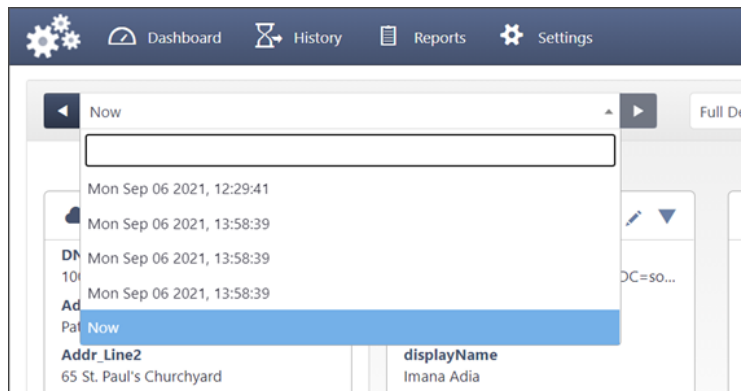
The Time Traveler is the interface used to explore changes in users (and other objects like groups, mailboxes etc.) There is no tab for this - you generally access it through a particular object of interest (perhaps you searched for it, or maybe it came up as a link in a report). For example, here we can see Imana Adia in the Time Traveler:



The identity is represented in HR (Workday: People), in Active Directory (AD), and also in Azure Active Directory (Azure). In this example, Identity Panel has been configured to perform a logical join of the identity data across silos (using EmployeeId in this case) - giving us a unified view of the identity. In the picture, we have moused over the Employee_Id in Workday and the interface has highlighted the identical data in other silos. This is helpful in visualizing the data, but has nothing to do with the joining method.

Note: Other silos might exist, in which the user is not represented at all, or is represented but a suitable joining attribute isn't available. Such silos will not be shown (Silos will only be shown in respect of logically joined objects).

"Now" is a special timestamp indicating the current state of the object across all silos. In the below diagram the right arrow is greyed out as we can't go any further forward in time than "Now", but we could select a previous point in time (when changes were detected by a previous scan).



Lab 1: Tour of Identity Panel

Lab 1: A tour of Identity Panel



- Exercise 1: Orientation

Logon Information - replace XX with your assigned student number e.g. 01

Virtual machine	IDPLabXX.WestEurope.cloudapp.azure.com
Domain username	softwareIDM\Labadmin
Azure username	labadmin@IDPLabXX.onmicrosoft.com
Password	\$IDMTrainingLogin

Estimated time: 30 minutes

Using the Identity Panel Suite

Course Number: A801

Lab 1: A tour of Identity Panel

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Lab 1: Scenario Familiarization	1
Scenario	1
Exercise 1: Orientation	1

Lab 1: Scenario Familiarization

Introduction

Your lab environment consists of an Azure tenant, and an Identity Panel instance in the cloud. Your Global Administrator account in Azure AD (LabAdmin) is also used to administer Identity Panel (which is using Azure AD authentication).

You also have a VM which hosts the on-premises services which are need to communicate with Identity Panel (and for some utilities). The VM is a domain controller, and so hosts Active Directory too.

Software IDM's Identity Panel is already installed and is populated with data from AD, Azure AD and also in a simulated Workday feed.

Scenario

In this lab, you will familiarize yourself with the environment and Identity Panel. You will:

- Find your way around the training environment
- Gain an understanding of the identity data available
- Gain an understanding of how this data is captured and represented in Identity Panel

Exercise 1: Orientation

Task 1: Connect to your VM and sign in (if necessary)

1. Run **RDP** (type RDP from the Start menu)
2. Connect to **IDPLabXX.WestEurope.cloudapp.azure.com** (where **XX** is your assigned student number – e.g. 01)
3. Sign in as **LabAdmin** with the password **\$IDMTrainingLogin**

Task 2: Examine Active Directory

4. From your VM (signed in as **labadmin**)
5. Open **Active Directory Users and Computers** (ADUC)
6. Find the two OUs called **US** and **UK**, and examine them – you should find:
 - a. A number of sub-OUs (one for each department)
 - b. A number of users in each one
7. Find a department head
 - a. Right-click the **UK** OU and click **Find...**
 - b. Switch to the **Advanced** tab

- c. Click **Field**, select **user** and then click **Job Title**
- d. For the value enter **Vice** and click **Find Now** and then **Yes** (to add your criteria)

Note: We are looking for an OU that a department head, with the Job Title of “Vice President of ...”.

8. **Double-click** one of the users you just found
9. Switch to the **Organization** tab and confirm that they are indeed a Vice President of an OU and that they are also a manager with direct reports.

Note: If, by chance, there aren't any reports, cancel the dialog and go back to step 8 (choosing a different Vice President).

10. Switch to the **Account** tab and examine their user logon names (sAMAccountName and userPrincipalName), e.g. softwareidm\fbaggins and frodo.baggins@softwareidm.lab
11. Cancel the dialogs and examine the corresponding OUs, one under the UK OU, and one under the US OU, and verify that the user accounts are those direct reports

Note: AD does not have a “manager of” field for a user – this data is calculated “on the fly”. Later on we will see how Identity Panel displays this data.

Task 3: Connect to Azure AD (if necessary)

12. Run the **Edge** browser in the VM (actually you would equally do this from your own local machine)
13. Navigate to **portal.azure.com**
14. Sign in as **labadmin@IDPLabXX.onmicrosoft.com** (where **XX** is your assigned student number – e.g. 01) with the password **\$IDMTrainingLogin**
15. Click the **Azure Active Directory** service

Task 4: Examine Azure Active Directory

16. Select **Users**
17. Search for the same head of department you just accessed in ADUC (e.g. Frodo)
18. Notice several things:
 - a. His account is enabled
 - b. He is not synced (Azure AD Connect is not in use)

Note: Although some of his attributes match up with on-premises AD (for example his Name/displayName and – though you may not have noticed – his Employee ID/employeeID), his User principal name does not match his on-premises UPN (we will consider this matter further in a later lab).

19. Use the breadcrumb (top left) to go back to **Home > Identity Panel Training Lab XX** and select **Groups**
20. You should be able to see a group for each department – select the one that corresponds to the OU you were just using, e.g. **AZ-SG-10003-Facilities**

Note: The Source is “Cloud” – meaning that this is not synchronized from AD

21. Examine the membership and the owner (should be the department head)

Task 5: Connect to Identity Panel (if necessary)

22. In your browser, open another tab and navigate to **connect.identitypanel.com**
23. Select **Log In** and sign in as **labadmin@IDPLabXX.onmicrosoft.com** (where **XX** is your assigned student number – e.g. 01) with the password **\$IDMTrainingLogin**
24. You are presented with the Identity Panel dashboard

Note: The dashboard is configurable, it has amongst other things information about system health and the ability to run schedules and other tasks.

Task 6: Explore the Dashboard

25. The dashboard has a number of modules – what you see depends on the configuration of Identity Panel, including your role(s) – review the **Platform Health** module

Note: It is likely that you have a some red exclamation marks, because the environment will probably have been sitting idle for a while, and it has not been configured to run regular scans automatically. You would do this in production, but for a classroom it makes sense to keep things manual so that you are in control and can see what is going on. Let’s assume (or pretend) that your Azure Scan health probe is a red exclamation mark indicating that it has not been scanned recently.

26. In the **View and Run Schedules** module, from the **Schedule** dropdown, select **Full Scans**

Note: Each schedule consists of one or more steps, and in production, you would expect that all steps would be run in order to a schedule. When you manually select a schedule like this, the steps dropdown is populated with all the steps in that schedule. You can select any step(s) you like from the dropdown, or you choose to run the entire schedule (by simply not selecting any steps).

It is possible to select multiple steps, and multiple steps from different schedules.

27. Click **Steps** and select **2: Azure Graph Scan**
28. Click **Run**

Note: You will see a new dropdown appear under the steps dropdown – this will only be there while your chosen steps are running, and it allows you to monitor progress.

29. Click the ► to expand the dropdown (if you were not quick enough, just click **Run** again)

Note: You will have noticed that it remembers your steps and you can immediately repeat a run, or add to it etc. You should take care to clear any existing steps that you don't want to run.

30. Refresh the page, and verify that the **Azure Scans** health probe goes to a green tick (this does not happen right away - health modules update automatically every minute – so just keep trying)

Task 6: Explore History

31. Select the **History** tab

Note: This shows the recent history, with the most recent item at the top – so your most recent run should be at the top, represented by a Schedule run item, and then all the steps (just the one in our case). Of course, nothing interesting is happening.

32. Select the **Schedule Run**, and note that it is a summary which tells you which steps were run (just one), when it was run, and whether it was successful (amongst other things)
33. Select the **Azure Graph Scan** and note that it gives similar information – but there is nothing to report
34. Click the **magnifying glass icon** above the **column of green ticks**
35. From the **Statistics dropdown**, select **Update** and click **OK**
36. Select the most recent **LDAP Scan of AD**

Note: Again, what you see depends on what has been happening in this particular environment, but probably you are seeing a load of updates that were scanned in from Active Directory (if you don't see any, try another LDAP Scan entry). At this stage we are just showing you how it lists all the objects affected – presenting them as hyperlinks to the objects concerned.

37. Follow the hyperlink for a user object – e.g.
CN=ggrayhame,OU=Management,OU=UK,DC=softwareidm,DC=lab

Task 6: Explore Time Traveler

Note: The hyperlink has presented the object in question, in the Time Traveler – showing the state of the object at the point in time when that LDAP scan (or whatever) took place in one silo, but also other silos showing corresponding objects from other systems etc.

Any attributes in green are attributes that were detected as having been added since the last scan.

The Time Traveler is usually accessed through a hyperlink or a search – there is no tab called “Time Traveler”.

38. Mouseover the **EmployeeID** and note the gold highlights – this attribute appears in all silos because it has generally been used as an identifying attribute
39. Use the ◀ and ▶ or the dropdown to travel to the very beginning (when the AD object was first scanned) and to the end (which is the state “Now”)
40. In **Search Time Traveler** (top right), enter **Frodo** and press **ENTER**

Note: You are presented with a number of silos, returned, all of which contain at least one object that contains the word Frodo in at least one of its attributes.

41. Expand **AD: 1 results** (▶)
42. Click the hyperlink for the user object (e.g. CN=fbaggins,OU=Facilities...)

Note: The user is presented in the Time Traveler as before – but this time to the “Now” state. Of course, as before, you can navigate through time.

Task 6: Explore Reports

Note: What reports you have available depends on those in the initial system configuration, plus any that have been imported, or new ones which you may have created.

43. Select the **Reports** tab
44. From the **Select Report** dropdown, select **AD – Users With/Without Manager**
45. Click **Build** to see a list of users, their managers, and some details of both

Note: You can select a parameter as either With (users with their managers), or Without (a list of users who do not have managers). Also you can produce the reports for a point in time – of which more later.

Using the Identity Panel Suite

Course Number: A801

Module 2: Identity Panel Suite and MIM

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Module Overview.....	1
Identity Panel Suite’s relationship to MIM	1
Lesson 1: Synchronization Engines.....	2
The Need for Synchronization Engines	3
Multiple Repositories for Identity Data	3
Synchronization Engines	3
Microsoft Synchronization Engines	5
Other Microsoft Synchronization	7
HyperSync Panel.....	8
Replacing MIM.....	8
MIM Coexistence	9
Uplift for MIM	10
Lesson 2: Other MIM Modules.....	12
The MIM Portal and Service Panel	13
The Need for an Identity Portal.....	13
The MIM Portal	14
Service Panel	14
BHOLD and Access Panel	15
Identity Management solutions	15
The Need for Governance	15
BHOLD	16
Access Panel	16
MIM and Test Panel.....	17
The Need for Testing	17
Lab 2: Identity Panel Suite (and MIM)	18

Module Overview

Module Overview



- Synchronization Engines
- Other MIM Modules
 - The MIM Portal and Service Panel
 - BHOLD and Access Panel
 - MIM and Test Panel
- Lab 2

Identity Panel Suite's relationship to MIM

Identity Panel has a long history with Microsoft Identity Manager (MIM), and its predecessors – it was initially very much an add-on to MIM. So, it is perhaps not surprising that the question is often asked: Does Identity Panel need MIM? The answer is “no” – because Identity Panel Suite has gone on to be far more than a MIM add-on.

As MIM nears end of life, another question that is often asked is: Can Identity Panel Suite replace MIM? The short answer is “yes”, and in this module we will look in some detail at this topic. We will look at the importance of keeping identity objects in various systems up to date, and the part played in this by synchronization engines such as MIM, Azure AD Connect and HyperSync panel. We will also look at the other major components of MIM – the portal and BHOLD – and how Service Panel and Access Panel align with these.

Lesson 1: Synchronization Engines

Lesson 1: Synchronization Engines



- The need for synchronization engines
- Microsoft synchronization engines
- HyperSync Panel
 - Replacing MIM
 - MIM coexistence

In this lesson we examine why organizations have a need for synchronization engines.

The Need for Synchronization Engines

The Need for Synchronization Engines



- Manually managing the same (or similar) information in many repositories is administratively onerous, leads to delays and inconsistencies, and is ultimately not good for security
- Semi-manual activities like file transfers and scripts can help, but still lack rigor
- A good synchronization engine:
 - Synchronizes objects and their attributes automatically
 - Runs often enough to provide timely data
 - Connects to just about any system likely to be encountered
 - Allows flexible transformation of attributes
 - Has customizable internal logic for mediating between multiple sources of truth
 - Is resilient with regards to temporary loss of external system availability
 - Provides health and diagnostic data
 - Has a comprehensive reporting capability, can trigger workflows, and possibly other functionality (such as password sync)

Multiple Repositories for Identity Data

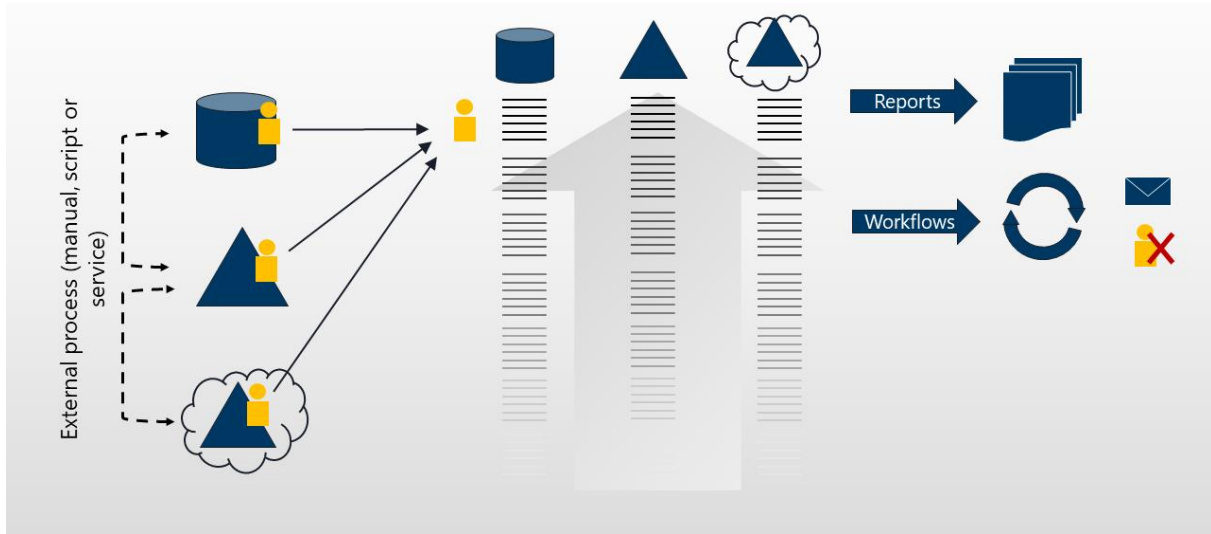
Most organizations will have many repositories for identity data, as we have already discussed – including AD, Azure AD, an HR system etc.

Essentially, the same, or similar, data is needed in all these systems. Maintaining this manually is administratively onerous, and leads to delays in making the data available where it is needed. Manual errors lead to inconsistent data – and this data is often the basis for decisions about group memberships and roles – in other words it also leads to poor security.

Many organizations will have somewhat improved this situation by using regular file transfers, or writing scripts which can be run from time-to-time – but this still lacks the rigor provided by a formal synchronization engine.

Synchronization Engines

A synchronization engine can obviate these issues, providing a robust mechanism.



A good synchronization engine will include the following features:

- Maintains object synchronization automatically - provisioning and deprovisioning objects as needed, and propagating changes to their attributes as they arise
- Runs often enough to provide timely data, for example to support authentication and authorization decisions, and simply to provide current data for other purposes, such as white pages
- Connects to just about any system likely to be encountered – certainly, this will include directories, databases, and web APIs, as well as being able to process drop files like CSV or AVP
- Allows flexible transformation of attributes, for example converting dates, or combining several attributes into another attribute (like displayname)
- Is highly customizable, and includes logic for mediating between multiple sources of truth such as multiple HR systems (for example resulting from mergers and acquisitions), student databases, contractor systems etc.
- Automatically recovers from temporary loss of connectivity, or an external system failure
- Provides information about its own health, and diagnostic capabilities when issues arise
- Has comprehensive reporting functionality
- Includes the capability to trigger workflows based on events (e.g. an attribute change or a date event)
- May include other desirable functionality, such as password sync

Microsoft Synchronization Engines

Microsoft Synchronization Engines



- MIM Sync – note that we are not including the MIM Portal here
 - Generic on-premises workhorse - widely used, and very reliable
 - Lacks workflow and reporting capability, and has limited health data available
 - Requires considerable effort to implement, including some coding
- Azure AD Connect “Classic”
 - Based on MIM, but re-engineered to remove the need for coding
 - Specifically intended for synchronizing AD with Azure AD (and more recently, Workday)
 - Additionally has authentication support (e.g. Password Hash Sync and Pass-Through Authentication)
 - Largely wizard-driven, but also very customizable
 - Very widely used, very reliable – but not generic
- Azure AD Connect CloudSync
- Other Microsoft synchronization processes
 - Other synchronization processes may be present about which Identity Panel has no direct information
 - It is important to understand what processes may be affecting the Silos we can see – for example a delay in such a process may lead to inconsistent data in the Silos
 - E.g. Workday synchronization, and internal Azure synchronizations

Identity Panel has Providers for these

www.oxfordcomputertraining.com

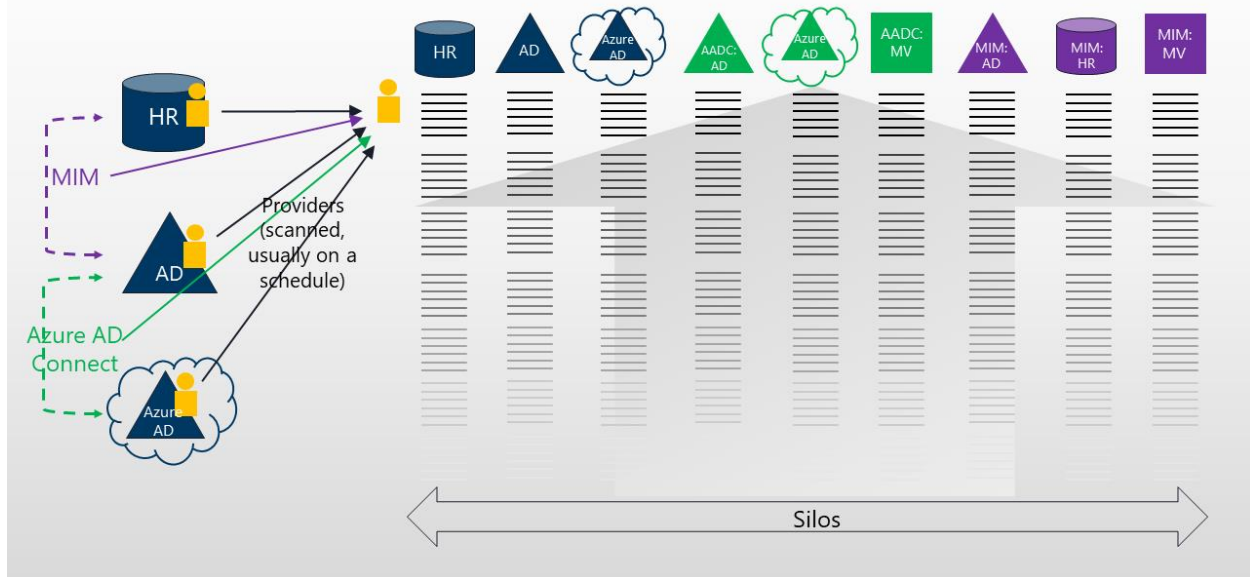
www.softwareidm.com

Microsoft provide two on-premises synchronization engines for which Identity Panel has Providers. Where these Providers are implemented, you will see additional silos as previously discussed. Both of these include a metadirectory (a directory of directories), which Microsoft calls a Metaverse (MV). MIM and Azure AD Connect each give rise to an additional silo for their MV.

In the following diagram, you can see how it is possible, in Identity Panel, to see information from a single system presented in multiple silos:

- Identity Panel has a direct connection to AD, which is represented as a silo (in blue in the diagram)
- Identity Panel has a direct connection to Azure AD Connect, and so it has silos not only for the Azure AD Connect MV, but also for the systems that Azure AD Connect is connected to, so we see another AD silo, and an Azure AD silo (in green in the diagram)
- Identity Panel has a direct connection to MIM, and so it has silos not only for the MIM MV, but also for the systems that MIM is connected to, so in our example we see another AD silo and an HR silo (in purple in the diagram)

Microsoft Synchronization Engines



Microsoft Identity Manager

MIM comes in two primary parts. We are talking here about the synchronization engine – but note that there is a MIM Portal, not relevant to our discussion here, but for which Identity Panel does have a provider, and also a replacement in the form of Service Panel.

MIM is a generic on-premises workhorse – meaning that it can connect to just about any system. It is widely used, and has proved to be very robust and reliable. It does lack a few desirable features, such as workflow and reporting capability, and it has limited health and diagnostic data available.

Implementing MIM is a significant undertaking, requiring a formal project, with (at least) test and production environments. Notably, it requires some coding in Visual Basic or Visual C#.

Azure AD Connect “Classic”

Azure AD Connect is based on MIM, but re-engineered to remove the need for coding – instead all configuration can be done through the GUI. Being based on MIM, it is technically a generic system, but it is specifically intended for synchronizing AD with Azure AD, and it is not supported to use it in a generic fashion.

It is very widely used and very reliable. A certain amount of reporting, and quite good health monitoring is provided through Azure AD.

Implementation is extremely easy, being largely wizard driven, although it allows a great deal of further customization.

Note: Azure AD Connect goes beyond the scope of a simple synchronization engine, by providing authentication support including Password Hash Sync, Pass-Through Authentication (Azure AD authentication is delegated to on-premises AD), and support for federation, e.g. AD FS.

Other Microsoft Synchronization

Identity Panel has a full “understanding” of MIM and Azure AD Connect – and can present silos from these, and information about their health. However, there are other synchronization processes that can affect the systems we can see in Identity Panel - but about which Identity Panel has no direct information.

The relevance of bringing these up is that we must understand what processes may be in place and how they affect the systems that Identity Panel touches. Notably, a delay – or (worse) a broken synchronization process – could result in inconsistent data appearing in Identity Panel silos.

Azure AD Connect CloudSync

There is a cloud version of Azure AD Connect called “Azure AD Connect CloudSync”. As yet, this does not have the same functionality as the classic version (though it does deal with a particular scenario not covered by the classic version – that of separate disconnected AD domains).

Identity Panel has a provider for this too.

Workday Sync

Microsoft provide two mechanisms for importing Workday users and synchronizing them to either Azure AD, or to AD. In the latter case this is logically part of Azure AD Connect (which of course goes on to synchronize AD to Azure AD as usual). But the synchronization from Workday to AD is not technically part of the same synchronization mechanism.

So, although we might see a silo for Workday (because, as already discussed, Identity Panel has a Workday provider), we would never see any evidence (within Identity Panel) of either of these two processes.

Azure synchronization

A great deal of synchronization goes on in Azure under the covers – for example between Azure AD and Office 365 – but this does not take the form of a visible synchronization engine. The relevance here, is that a delay could result in inconsistent data appearing the Azure AD and Office 365 silos.

HyperSync Panel

HyperSync Panel



- As already covered
 - A full feature synchronization engine, which is part of the Identity Panel suite
 - Does rather more than MIM sync does, and does so without code
 - Utilizes Identity Panel capabilities such as data, connectivity (including writing back), report and workflow engines and other features
 - Includes event-based as well as stateful rules (MIM is entirely state-based)
 - Can build and maintain a “Hyperverser” metadirectory
- HyperSync Panel can coexist with, or replace, Microsoft identity Manager (MIM)
 - MIM has a limited life, and HyperSync Panel is a perfect replacement
 - Organizations who use MIM widely, may find it difficult to migrate in one go – HyperSync Panel can readily coexist; new workloads can be configured in HyperSync Panel, and existing MIM workloads gradually transferred
 - Uplift for MIM – brings in the custom connectors developed for MIM - allows for a codeless approach that does not impact on performance and provides improved flexibility and version control
- Optionally leads to one additional silo: the Hyperverser

www.oxfordcomputertraining.com

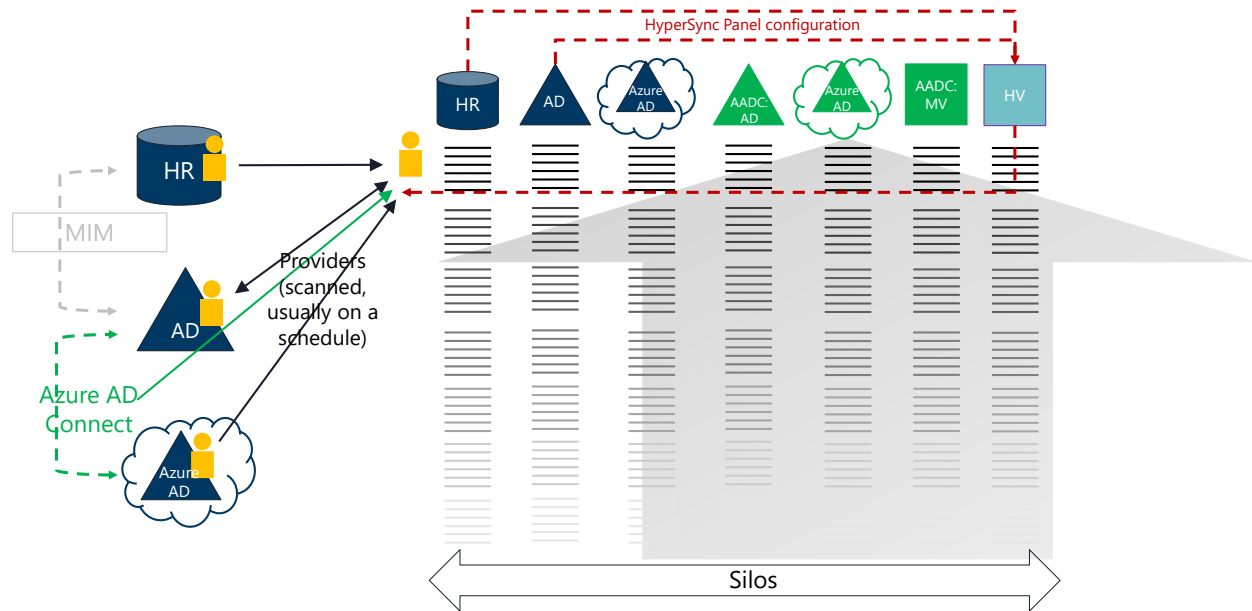
www.softwareidm.com

In the previous module we introduced HyperSync Panel, but as a reminder, here are some key features:

- It is a full feature synchronization engine, which is part of the Identity Panel Suite and provides everything you would expect from a good synchronization engine.
- It does rather more than MIM sync does, and is implemented without the need for code
- HyperSync Panel is dependent on Identity Panel for data and connectivity (including writing back), and so benefits from other Identity Panel features such as its reporting, workflow engine, support for unique values etc.
- MIM is entirely state-based, it goes through a regular cycle responding to changes in the data. HyperSync Panel has stateful rules (just like MIM), but it also has event-based rules which can respond to things such as date transitions, and can invoke any process action available in Identity Panel (sending an email, delicensing a user etc.).
- Optionally, you can configure a “Hyperverser” metadirectory (like MIM’s “metaverse”) – generally useful in all but the simplest implementations

Replacing MIM

Microsoft has announced that support for MIM will stop at some point, and so organizations have to consider what to replace it with. It does not look like Microsoft will replace MIM with an entirely similar replacement engine, preferring to make all its investments in the cloud. HyperSync Panel therefore represents a perfect replacement, being a cloud-based synchronization engine with full support for legacy on-premises environments.



In this scenario, MIM has been replaced by HyperSync Panel, which is now synchronizing HR with AD. It is assumed that Azure AD Connect is in place (synchronizing AD with Azure AD).

Since HyperSync Panel has no direct connectivity to source systems, and relies on Identity Panel, no additional silos are visible, except the Hyperverse (if configured).

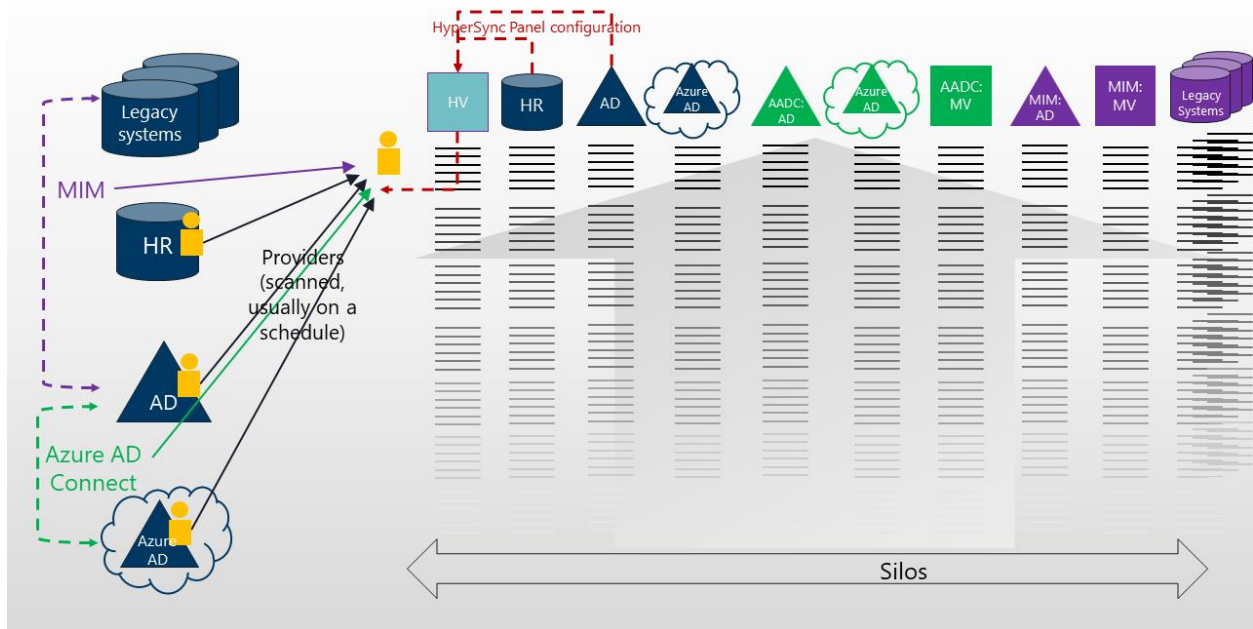
MIM Coexistence

Some organizations have invested heavily in MIM, and may find it difficult to migrate from MIM in one go. HyperSync Panel can readily coexist with MIM; new workloads can be configured in HyperSync Panel (rather than further embedding MIM), and existing MIM workloads can be migrated to HyperSync Panel in an orderly manner as time allows and circumstances dictate. And as icing on the cake, with Uplift for MIM, HyperSync Panel can utilize custom (ECMA2) connectors that have been developed for MIM.

In the following scenario, MIM is still in place, synchronizing AD with various legacy systems. HyperSync Panel has taken over the primary task of synchronizing HR with AD. This has the advantage that any new requirements arising from changes in the HR system (perhaps result from a merger or acquisition, or a migration of HR to the cloud) can be accommodated without further MIM development.

Again, it is assumed that Azure AD Connect is in place, and the Hyperverse has been configured.

Coexistence



Uplift for MIM

As previously mentioned, Uplift is an Identity Panel feature that supports and enhances MIM. With Uplift, custom (ECMA2) connectors that have been developed for MIM, can be brought into Identity Panel. It provides a codeless approach to configuration which does not impact performance or flexibility.

Architecturally, it is a helper library for writing provisioning and extension DLLs for MIM. Rule logic is expressed in an XML file, and a DLL consumes the XML at runtime to perform the required actions. This is open source software under the MS-RL license (Microsoft Reciprocal License).

It offers many additional features, for example:

- You can use the Identity Panel expression language (which is richer than the equivalent in MIM)
- Notably you can use the functionality that Identity Panel makes available to handle unique value requirements
- It also provides utilities to aid in attribute flow and provisioning, writing log entries, sending notification emails, and looking up values in SQL and XML files.
- Version control for the Synchronization Service configuration
- Environment variable management
- Intellisense, and a graphical Rules Editor
- Promotion tools, for migrating configuration from dev to test to QA to production (for example)
- Identity Panel becomes aware of flows and can display much richer data as a result (reads portal rules too, though will not allow editing)

Note: If you transition to using Uplift for configuring MIM, migration to HyperSync Panel is facilitated when that becomes necessary.

Lesson 2: Other MIM Modules

Lesson 2: Other MIM Modules



- The MIM Portal and Service Panel
- BHOLD and Access Panel
- MIM and Test Panel

In this lesson we examine the other MIM modules and how they relate to the Identity Panel Suite.

The MIM Portal and Service Panel

The MIM Portal and Service Panel



- Many organizations will have needs which go beyond simple synchronization
- Not all authoritative identity data is to be found in the HR system (or equivalent)
- An Identity Portal that can access the authoritative data gathered from multiple systems can provide solutions for many requirements including: white pages, user self-service, management of object attributes and properties (including groups), management of useful lookups
- All such access must be subject to security requirements, of course
- The MIM Portal effectively acts on the MIM metaverse, and hence on the data in target systems, and can be configured to provide the above functionality, plus self-service password reset (SSPR)
- Migration from the MIM Portal to Azure AD currently leaves some significant gaps
- Service Panel takes the above requirements in its stride (including SSPR and Password Sync) and also integrates with ServiceNow
- Service Panel is thus:
 - A flexible and capable UI for Azure AD identity data, and for all identity data from multiple sources
 - A replacement for MIM, but it can also work alongside it, facilitating orderly migration when the time is right

www.oxfordcomputertraining.com

www.softwareidm.com

The Need for an Identity Portal

Many organizations will have needs which go beyond simple synchronization, including the ability for users, managers, help desk and administrators to access – and in some cases act upon – identity data.

Much authoritative identity data is to be found in the HR system (or equivalent), but by no means all of it – and in any case an HR system is geared to HR, not to these other groups of users. An Identity Portal that can access the authoritative data gathered from multiple systems can provide solutions for many requirements including:

- White pages
- User self-service (for attributes such as home address and telephone numbers, next of kin details etc.)
- User self-service for groups (requesting membership or managing their own groups)
- The ability to manage some user attributes and properties (attributes such as phone numbers and alternative email addresses, licensing, emergency disabling of accounts etc.)
- Group management (of AD security groups, for example)
- Management of useful lookups, such as departments, cost centers etc.

All such access must be subject to security requirements, of course.

The MIM Portal

The MIM Portal gets its data from the MIM metaverse – in other words it has access to the aggregated identity data about any objects held in the synchronization engine. Any changes it makes feed back to the metaverse, and thence to the target systems according to the configuration.

It can be configured to provide all the above functionality, plus self-service password reset (SSPR) for Active Directory (AD). SSPR can be readily migrated to Azure AD, where it benefits from integrated MFA, as well as all the investments Microsoft is making in keeping passwords secure. Azure AD also provides excellent group management (including self-service) for Azure AD groups. It does not provide direct management for AD (local) groups, although it does provide support for "writing back" to AD groups (synchronizing Azure AD groups to AD).

All this means that migration from the MIM Portal to Azure AD currently leaves some significant gaps, notably the above-mentioned management of AD groups, but also there is a lack of customizable forms for such solutions as white pages, user self-service and user management by managers and help desk.

Service Panel

Service Panel takes the above requirements in its stride (including SSPR and Password Sync), while offering additional capabilities, such as integration with ServiceNow (extending that product to all the systems touched by Identity Panel).

Note: SSPR is included with Service Panel, whereas in Azure, users require a minimum of a P1 license for SSPR.

Service Panel is thus a flexible and capable UI for Azure AD identity data, and for all identity data from multiple sources. With regards to the MIM Portal it can be a replacement, but can also work alongside the MIM Portal, allowing an orderly migration when the time is right.

BHOLD and Access Panel

BHOLD and Access Panel



- An Identity Management solution with MIM or Identity Panel at its heart brings other opportunities, like an Identity Portal (see the last topic) or a governance application
- An Identity Management solution can bring rigor and consistency to authentication processes, but also to authorization processes (managing group memberships, role objects, key user attributes, for example)
- Identity Governance is about the controls we put in place to ensure appropriate authorizations
- This is usually done through mechanisms such as approvals of user requests for access, just in time privileged access, periodic reviews of who has access to what, and so on
- All this needs to happen in many or all of the connected systems, and ideally can be tied back to a central enterprise role schema
- BHOLD was an acquisition by Microsoft, added to MIM bundle, but now effectively deprecated
- Access Panel provides almost all the above functionality, and it continues to be developed
- It can provide that functionality for MIM, but it can also be part of a replacement for MIM, providing rich governance functionality alongside HyperSync Panel

Identity Management solutions

Having an Identity Management solution with MIM or Identity Panel at its heart brings other opportunities, because once you have brought together all the authoritative data into a canonical representation of each identity in the metaverse or Hyperverses, it becomes possible to manipulate that data in useful ways. An Identity Portal (from the last topic) is one such possibility, and a governance application is another.

An Identity Management solution can bring rigor and consistency to authentication processes by managing account names and passwords, but also to authorization processes by managing group memberships, other objects, and/or attributes involved in authentication decisions (key user attributes and role objects, for example).

The Need for Governance

Identity Governance is about the controls we put in place to ensure users have the authorizations they should have, and do not have those they should not have. This is usually done through mechanisms such as:

- Approvals of user requests for access (for membership of a group, for example) by the owner of an application, or the manager of a department (for example)
- The ability to provide just in time privileged access, with policies covering candidature (who can request such privileged access), approval, escalation of approval, notification, justification forms, time windows and extensions

- Periodic reviews of who has access to what, for example: group memberships, licenses, roles, or even native criteria (for example the query-based criteria used in Azure AD groups)

All this needs to happen in many or all of the connected systems, and ideally can be tied back to a central enterprise role schema – meaning that by giving a user an enterprise role, they get a corresponding set of permissions across many systems, and by getting a number of roles they get all the access they need. This is an ideal rarely achieved, and there are typically many exceptions – but it is a target to aim for.

BHOLD

BHOLD was an acquisition by Microsoft that was added to the MIM bundle. It provided some of the above capabilities, but sadly was never developed into what it might have been. It is now effectively deprecated by Microsoft.

Access Panel

Access Panel provides almost all the above functionality, and it continues to be developed. It leverages Identity Panels capabilities (connections to various systems, workflows, notifications, reporting, and – of course – the very fact that it holds the required data).

It can provide that functionality for MIM, but it can also be part of a replacement for MIM, providing rich governance functionality alongside HyperSync Panel. In short although not a perfect feature for feature match to BHOLD, it is an effective replacement for BHOLD (whether or not MIM is still in use).

MIM and Test Panel

MIM and Test Panel



- Any system upon which an enterprise depends should be fully tested – especially if security decisions are being taken based on data provided by that system, which is the case for an Identity Management solution
- Automating such testing, so that tests are being repeatedly and consistently applied during the development of the system, and again when modifications are made to that system, brings significant savings in time, as well being a more rigorous and reliable approach
- Test Panel does exactly this (MIM does not have such a facility)
- Test Panel can act as a testing harness for a MIM-based solution, or a HyperSync Panel-based solution
- Importantly, if HyperSync Panel is being used alongside MIM during migration, Test Panel can provide ongoing checking that the replacement solution is still meeting the solution requirements

The Need for Testing

Any system upon which an enterprise depends should be fully tested – especially if security decisions are being taken based on data provided by that system, which is the case for an Identity Management solution.

Automating such testing, so that tests are being repeatedly and consistently applied during the development of the system, and again when modifications are made to that system, brings significant savings in time, as well being a more rigorous and reliable approach.

Test Panel does exactly this. MIM, on the other hand, provides no such facility – so there is no question here of replacing part of MIM. Nevertheless, Test Panel is the final part of the story of “The Identity Panel Suite and MIM”.

Test Panel can act as a testing harness for a MIM-based solution, or a HyperSync Panel-based solution. Importantly, if HyperSync Panel is being used alongside MIM during migration, Test Panel can provide ongoing checking that the replacement solution is still meeting the solution requirements.

Lab 2: Identity Panel Suite (and MIM)

Lab 2: Identity Panel Suite (and MIM)



- Exercise 1: Service Panel
- Exercise 2: HyperSync Panel
- Exercise 3: Access Panel

Logon Information - replace XX with your assigned student number e.g. 01

Virtual machine	IDPLabXX.WestEurope.cloudapp.azure.com
Domain username	softwareIDM\Labadmin
Azure username	labadmin@IDPLabXX.onmicrosoft.com
Password	\$IDMTrainingLogin

Estimated time: 60 minutes

Using the Identity Panel Suite

Course Number: A801

Lab 2: The Identity Panel Suite (and MIM)

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Lab 2: Identity Panel Suite (and MIM)	1
Scenario.....	1
Exercise 1: Service Panel.....	1
Exercise 2: HyperSync Panel	3
Exercise 3: Access Panel.....	5

Lab 2: Identity Panel Suite (and MIM)

Scenario

- In Lab 1 we took a brief tour of Identity Panel – the core application in the Identity Panel Suite
- In this lab we take a quick look at some of the features of the other applications in the Identity Panel Suite
- Those familiar with MIM will be able to map these features onto Microsoft Identity Panel (MIM) features, and hence gain an understanding of how Identity Panel Suite can replace MIM

Exercise 1: Service Panel

- Service Panel allows us to view and edit the identity data that has been scanned from various systems by Identity Panel.
- For those interested, this is very similar to the ability to view and edit users and groups in the MIM Portal.

Task 1: Examine Service Panel as an Admin

1. Navigate to **connect.servicepanel.app**
2. If prompted, sign in as **labadmin@IDPLabXX.onmicrosoft.com** (where **XX** is your assigned student number – e.g. 01) with the password **\$IDMTrainingLogin**
3. Click **DETAIL** and note the additional attributes that are displayed
4. Click **Service Panel** to get back to the previous view

Note: What you are seeing is a self-service portal – and everything is configurable. In the classroom environment we have provided a number of forms. At the top left is what is known as a Business Card view of your own data. When you clicked **DETAIL**, it took you to the Detail View (and then you came back again). Since you are an Admin, you see a lot of forms that not everyone would have access to (like Create Employee and Create Management Data).

5. In the **Search People** form click **SEARCH** to see a list of users (you could have searched for a particular person)
6. Enter **Took** in the Search text and click **Search** (magnifying glass)
7. Click **Peregrin Took** and note that you can edit certain attributes (pencil icon)
8. Change the mobile phone number (click the pencil icon, enter a justification, enter a mobile number, click **NEXT**), then click **BACK TO HOME**
9. Edit Peregrin's mobile phone number again and change it to a different number

Note: Later on, we will examine how you can see the current and previous value for Peregrin's mobile phone number.

Task 2: Create an Employee

10. Click **CREATE EMPLOYEE** and enter the details as follows:
 - a. First Name: **Duncan**
 - b. Last Name: **Idaho**
 - c. Location: **201: London Office (UK)**
 - d. Office Phone: **GB 1234567890**
 - e. Mobile: **GB 1234567899**
11. Click **Next** and continue:
 - a. Manager: **Frodo Baggins**
 - b. Job Title: **Order clerk**
 - c. Department: **1003: Facilities**
12. Click **SUBMIT**
13. Click **BACK TO HOME**

Note: As yet, this person has not been created in any external system, and therefore cannot be scanned back in – and so will not yet be found via a search.

14. In **Azure AD**, navigate to **All users** and verify that there is no account for Duncan Idaho
15. On your **VM**, navigate to **ADUC** and verify that there is no account for Duncan Idaho.
16. In **Identity Panel** (connect.identitypanel.com), from the **Dashboard**, under **View and Run Schedules**, select **Provision Sync** and click **Run**
17. A **Provision Sync** panel appears – click the ► to expand it and you will see the steps involved

Note: There are some important things to understand about the process of synchronization – and since you are now waiting for that to happen, it is the perfect time to mention them!

First, you can monitor the progress of the schedule from the View and Run Schedules module, or from History. In this case you can see several steps.

It can take many synchronizations for a new user (for example) to be propagated fully everywhere you need it. This is because some steps depend on values generated in subsequent steps. For this reason, a typical schedule may involve several synchronization steps. Also, sometimes you want to scan a system to read back generated attributes, before continuing to synchronize.

The actual processing time for a single new user (like the one you have just done) is very quick. However, steps are placed in a queue, with the queue being regularly checked (every 15 seconds in our lab environment). So a number of these 15 second periods can pass if there are several steps, and so it may take a minute or so to complete the schedule.

It should be clear that if there are many changes, the time to schedule them will not increase in proportion. It will still only take a minute or so if there are 10 new users, or even 100.

18. When the steps have completed (and the **Provision Sync** panel has disappeared), check that Duncan exists in Azure AD, and also in the UK/Facilities OU in AD
19. Back in Identity Panel in **Search Time Traveler** enter **Duncan** and press ENTER

20. Click the ► next to **Azure** and click the link for Duncan

Note: You see Duncan in Time Traveler, with silos for Azure, AD, Workday, Hyperverse (more later) and Service Panel (more later). We have added the user to Workday (actually we have only simulated this), unique values have been generated, and the user has been provisioned to our two directories.

Task 3: Use Service Panel as a user (non-admin)

21. In an InPrivate browser session, navigate to **Service Panel** (connect.servicepanel.app), click Log in, and sign in as **frodo.baggins@idplabXX.onmicrosoft.com** with password **\$IDMTrainingLogin** (if you are prompted to change your password, just change it to **\$IDMTrainingLogin1**)
22. You are taken to your dashboard – notice that (because you are you are not an Admin):
 - a. You have fewer Service Panel forms on your dashboard
 - b. You can only modify your mobile phone attributes
 - c. If you search for Peregrin Took you will find that you cannot modify any attributes
23. Close the InPrivate browsing window as we don't need this any more

Exercise 2: HyperSync Panel

- Most organizations like to keep their identity data aligned between various systems, such as HR, AD and Azure AD.
- As discussed in the module, there are two Microsoft synchronization engines of note: MIM and Azure AD Connect – but we are not using these here.
- So, the scenario here is that we have a need to synchronize HR, AD and Azure AD, and we are going to briefly look at how HyperSync Panel has been configured to achieve this. This is a huge topic and there is a separate course covering this, so we are only going to touch on these issues here.
- For those interested, this is a potential replacement for the MIM synchronization engine.

Task 1: Understand how the Hyperverse is populated

24. Select the **Settings** tab and then click **HyperSync Panel** (on the left)
25. Under **Hyperverse schemas**, expand **person** (►) - the Hyperverse has only been defined for a person, and with the attributes you can see
26. Select **Attribute Flow** (at the top) – the columns here are Name, Flow Target Silo, Object Type and a Scope Filters, so you can see that:
 - a. Many of them flow attributes to the Hyperverse
 - b. The names give a good indication of what is being flowed (so many of them are from HR, which is Workday)
 - c. Scope Filters are used to restrict the flow to certain subsets of objects
27. Expand **HR-Import Job Details** (►), and expand the **department** mapping (►)

Note: Each of these mappings flows something to the Flow Target Silo (the Hyperverse in this case). The department mapping maps the Workday Department attribute to the Hyperverse department attribute (or put another way, flows the department value from Workday to the Hyperverse).

28. Expand the **isCorporate** mapping (▶)

Note: Here you can see an expression used in a mapping. We are looking for the word “corporate” in the Location_Type attribute, which will generate a True or False which is flowed to the isCorporate attribute in the Hyperverse.

29. Scroll up and click **View Flow Rule Editor** (the hyperlink under **Mappings**) – which gives you a graphical way of viewing and editing the mappings – you can see the department mapping, and if you scroll down to the isCorporate mapping, and click the question mark, you can again see the expression
30. Close the Rule Help dialog

Note: Once the schema and the flows exist, the Hyperverse object will be created (if it does not already exist) and kept up to date during subsequent synchronization.

We have looked at some flows from HR to the Hyperverse, but in general Hyperverse flow can be from many sources.

If you make any changes, please do not save them! Simply refresh the page.

Task 2: Understand how an AD account is provisioned

31. Select **Stateful Sync** (at the top)
32. In this case the columns are Name (which should indicate what it does), Root Context Silo (usually where the data will come from), Object Type (in the Root Context Silo), and Scope Filters
33. Expand **Provision AD User** – there is a lot going on here:
- Scope Filters control which Hyperverse objects this will apply to
 - Condition Rule is a further constraint, in this case used to validate that the Hyperverse object is ready, and that the relevant object does not already exist in AD
 - Acton Queue Data are values that will be used to generate initial attributes during provisioning (such as a DN, sAMAccountname and employeeId) – these are generated in a manner much like Attribute Flow Rule mappings – in fact there is a Flow Rule Editor
 - Process actions – in this case just a Sync Action which (if you go on expanding) specifies an AD user with its initial required attributes (DN, sAMAccountName, userAccountControl and UnicodePwd), and further initial attribute flows (employeeID, displayName and userPrincipalName)
34. Select **Attribute Flow** (at the top) to see that there are also regular attribute flows to AD (which will happen on subsequent syncs, too) such as AD - Export Corporate and AD - Disable Inactive

Note: There are many other things we could look at here, but hopefully this has given you the gist of how HyperSync Panel is configured.

Task 3: Understand how an Azure AD account is provisioned

Note: Many organizations will be running Azure AD Connect and so will not need this, but in our lab environment we have a rule to emulate the action of Azure AD Connect (for a user).

35. Select **Stateful Sync** (at the top) and expand **Lab AADC - AD to Azure**
 - a. Condition - this only happens if there is a user in the AD silo that is not in the Azure Silo
 - b. Action Queue Data - it generates initial attribute values you would expect for an Azure account
 - c. As you continue down, as before, you should be able to see that an Azure AD user is being created
 - d. As an interesting addition, if you scroll back up and expand **upn** (under Action Queue Data), you can see an expression that replaces the AD UPN suffix with the name of the Azure domain – and does so using two variables
 - e. Scroll up and select **Environment Settings** (on the left) and note that the variables refer to `@softwareIDM.lab` and `@idplabXX.onmicrosoft.com` (the former being the local domain, and the latter being the internet domain in use)

Exercise 3: Access Panel

- Entitlements come in various shapes and sizes, using group memberships, roles, attributes, entitlement objects and so on. Groups are perhaps the most common amongst these – and in our environment they provide a good example for us to use.
- For suitably licensed users, Azure AD provides dynamic (query-based) groups – and of course it provides assigned (purely manual) groups. AD does not provide dynamic security groups. Access Panel allows for scenarios not covered by either of these directories.
- In this lab we will use Access Panel to manage a group, which will be criteria -based (like a dynamic group), but will allow exceptions. This is just one of many scenarios that Access panel enables.
- For those interested, Access Panel is an alternative to MIM portal functionality for managing groups, and also for B HOLD management of permissions.

Task 1: Examine the group

36. In **Azure AD**, locate the **AZ-SG-1003-Facilities** group, and ascertain that it has a number of direct (that is, assigned) members – and that Duncan Idaho is not one of them
37. In **Identity Panel** locate the **AZ-SG-1003-Facilities** group in **Time Traveler**, focusing on the **Azure Silo**
38. Click the **Count** for the **members** attribute and then click **Search** – satisfy yourself that Duncan is not a member of the group (there may be more than one page of results – you can change the number per page, from 10 to 20 for example)
39. Navigate to **connect.accesspanel.app** signing in as **labadmin@IDPLabXX.onmicrosoft.com** if necessary (with the password **\$IDMTrainingLogin**)
40. Select **Resources** on the left

41. Enter the **Search Term** as **Facilities** and click **SEARCH**
42. Click the link for **AZ-SG-1003-Facilities** and you are presented with an overview of the group
43. Select the **MANAGE** tab (at the top) and scroll down to see the Criteria Rule that drives the membership of this group – on the face of it this will include everyone in the Facilities department
44. Scroll up and select **ENTITLEMENTS (MEMBERS)** and establish that Duncan does not appear (even though he is in the Facilities department)
45. In Identity Panel, from the dashboard, run a **Full Sync - twice** (the first sync imports the new user to Access Panel, and the second sync evaluates his entitlements)

Note: Access Panel requires a full synchronization to process changes. We haven't run a full sync before, which is why Duncan does not yet appear.

46. When the process finishes check that he is now a member of the group in **Azure AD, Time Traveler** and **Access Panel**

Task 2: Make exceptions to the membership

47. Click the **dustbin icon** next to one of the other users
48. Click **Find Principals** (near the bottom of the page), find **Alan Turing** and click **ADD+**
49. Click **SUBMIT**
50. In Identity Panel, from the dashboard, run a **Full Sync**
51. When the process finishes satisfy yourself that the changes have been reflected in **Azure AD, Time Traveler** and **Access Panel** – in Access Panel these exceptions are called out as Explicit or Exclusive

Using the Identity Panel Suite

Course Number: A801

Module 3: Time Traveler

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Module Overview.....	1
Lesson 1: Time Traveler Basics	2
Accessing the Time Traveler	3
Search.....	3
History	5
Other hyperlinks.....	5
Time Traveler Presentation	7
What silos are presented?	7
Focus Silo.....	7
Attribute Value Highlights.....	8
Timestamps	12
The Date/Time Dropdown.....	12
What Timestamps are Generated, and when?	13
"Dates from All Silos" checkbox	13
Reference and Multi-value Attributes.....	15
Introduction	15
Timestamps for Reference and Multi-value Attributes.....	15
Attribute History	17
Introduction	17
Simple, single attributes.....	17
Multi-value and Reference Attributes	18
Select Display Fields.....	19
Advanced search.....	20
Lesson 2: Other Time Traveler Features	21
Advanced Time Traveler Search	22
Search Time Traveler	22
The Advanced Search Dialog.....	22
Customized Time Traveler Views.....	24
Shutter views	24
Attribute Names	25
Securely sharing a URL	28
Lab 3: Time Traveler	29

Module Overview

Module Overview



- Lesson 1: Time Traveler Basics
- Lesson 2: Other Time Traveler Features
- Lab 3

www.oxfordcomputertraining.com

www.softwareidm.com

In this module, we will look at the Time Traveler, the key interface for examining identities in their various silos over time.

Lesson 1: Time Traveler Basics

Lesson 1: Time Traveler Basics



- Accessing the Time Traveler
- Time Traveler Presentation
- Timestamps
- Reference and Multi-value Attributes
- Attribute History

www.oxfordcomputertraining.com

www.softwareidm.com

The Time Traveler is the interface used to explore changes to objects over time. You briefly looked at it in Module 1. Now it is time to delve into the details.

Accessing the Time Traveler

Accessing the Time Traveler



- Time Traveler shows you all the data about a particular identity at a given point in time, across all the relevant silos – you can access it in a number of ways
- Search facility
 - Always present at the top right in Identity Panel
 - By default searches across all attributes and all silos in the current view, on a whole word basis
 - Can use the * (multiple characters) or ? (single character) wild cards, and search within a particular silo
 - Returns a list of silos with the number of results in each silo or "No Search Results" - you can expand a silo and select from the list of object hyperlinks (silo becomes focus, uses the last timestamp)
- History
 - Whether you see History, and how much you see, depends on your role
 - Includes statistics and errors, which are presented as hyperlinks, many of which will bring up the relevant object in the Time Traveler, at the date and time of the operation (scan or scheduled run)
- Other hyperlink references
 - You can click any reference attribute value in the Time Traveler or a report
 - Brings up the identity in the Time Traveler, at the same date and time, with focus on the object's silo

www.oxfordcomputertraining.com

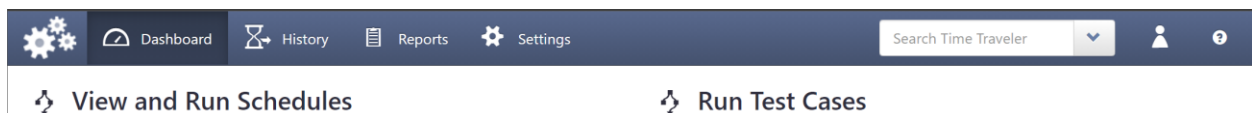
www.softwareidm.com

The Time Traveler shows you data about a particular identity (user, contact, group etc.) at a given point in time, across all the relevant silos. The way that you get to the Time Traveler is generally:

- From a search
- From an object hyperlink in the History
- From an object hyperlink in the Time Traveler (such as a reference to a manager or group member)
- From a link in a report

Search

You can use the search facility, which is always present at the top right in Identity Panel.



If you simply search for a word, Identity Panel will search across all attributes and across all silos available in the current view (this could be all silos and attributes, or a subset, depending on how your administrator has configured the system, and the choices you make). It matches whole words – so you could search for Ford and you would find anybody whose first name or last name is Ford, or any attribute that contains the search word (like Company = The Ford Motor Company).

Note: If you find that this kind of search returns too many results, you can use a more advanced type of search – see next lesson.

You can use the * (multiple characters) or ? (single character) wild cards and you can search identities within a particular silo.

The screenshot shows the Time Traveler search interface. At the top, there is a navigation bar with icons for Dashboard, History, Reports, and Settings, along with a search bar and user profile. Below this, a 'Search Results' section displays 'Results for: vice president'. A dropdown menu shows 'AD: 14 results'. Below the dropdown, there are 'Previous' and 'Next' buttons, and pagination information: '14 Rows Page 1 of 2 10 per page'. A table lists search results with columns for 'ObjectType' and 'DN'. Each row has a magnifying glass icon on the right side.

ObjectType	DN
user	CN=ntraver,OU=Facilities,OU=US,DC=softwareidm,DC=lab
user	CN=sdiethild,OU=Management,OU=US,DC=softwareidm,DC=lab
user	CN=sburan,OU=Sales,OU=US,DC=softwareidm,DC=lab
user	CN=cfabienne,OU=Legal,OU=UK,DC=softwareidm,DC=lab

The search results are presented as a list of silos with the number of results in each silo or "No Search Results". You can expand a silo to list the objects found in that silo – these are hyperlinks which can take you to the Time Traveler, with your newly found object in the selected silo as the focus.

Note: The Focus silo is simply the one on the left. More about this soon!

The screenshot shows the detailed view of a user in the Time Traveler interface. The top navigation bar is the same as in the previous screenshot. Below it, there is a 'Now' section with a 'Full Details' dropdown. The main content area is divided into three silos: AD, Azure, and Workday: People. Each silo displays a list of attributes for the selected user.

Silo	Object Type	Attributes
AD	user	DN: CN=sdiethild,OU=Management,OU=U... accountExpires: 9223372036854776000 displayName: Samvell Diethild employeeID: 10000002 mail: samvell.diethild@softwareidm.lab objectGUID: Roz35TQG602+V9gZCWfu/g== objectSid
Azure	user	DN: samvell.diethild@student100aadconne... accountEnabled: True createdDateTime: 9/7/2021 1:06:56 PM displayName: Samvell Diethild employeeid: 10000002 forceChangePasswordNextSignIn: True forceChangePasswordNextSignInWithM...
Workday: People	person	DN: 10000002 Addr_Line1: 100 S Michigan Ave Addr_Line2: Company: Lab Inc. Country: United States of America Country_Code: US County: Cook

History

Depending on your role, you may have access to the History (or perhaps to a short version of the History on your Dashboard). An entry in the History might be an operation such as a scan of AD or Azure AD, and typically there will be associated statistics and errors, which are presented as hyperlinks, allowing you to drill down and look in detail at an object of interest (user, group etc.) in the Time Traveler.

The focus will be on the silo concerned (the one containing the object concerned), usually at the date and time of the operation that gave rise to it.





The screenshot displays the 'History' section of the Identity Panel Suite. The main table lists 188 rows of history entries. The selected entry is 'AD LDAP Scan AD'. The details panel on the right provides an overview of the operation, including the result (success), a direct link, and statistics (15 updates). Below the details, a table lists object types and their DNs.

Object Type	DN
AD	
user	CN=ntraver,OU=Facilities,OU=US,DC=softwareidm,DC=lab
user	CN=sdieithild,OU=Management,OU=US,DC=softwareidm,DC=lab
user	CN=stabilenne,OU=Legal,OU=UK,DC=softwareidm,DC=lab
user	CN=Isonnie,OU=Operations,OU=UK,DC=softwareidm,DC=lab
user	CN=jgothfraidh,OU=Human Resources,OU=UK,DC=softwareidm,DC=lab
user	CN=rvalin,OU=Accounting,OU=US,DC=softwareidm,DC=lab
user	CN=pkirkley,OU=Public Relations,OU=US,DC=softwareidm,DC=lab
user	CN=nregal,OU=Organization Development,OU=US,DC=softwareidm,DC=lab








Other hyperlinks

You can click any reference attribute value in the Time Traveler or a report, and bring up the identity in the Time Traveler, usually at the same date and time, with focus on the object's silo.

For example, in the following Time Traveler picture, you could follow either of the "member Of" hyperlink references, and be presented with that group - also in the Time Traveler:

 Dashboard
 History
 Reports
 Settings

◀ Now
▶
 Dates from All Silos

Workday: People	AD	Azure
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;">  person  </div> <div style="font-size: 0.9em;"> <p>DN 10000416</p> <p>Addr_Line1 100 S Michigan Ave</p> <p>Addr_Line2</p> <p>Company Lab Inc.</p> <p>Country United States of America</p> <p>Country_Code US</p> <p>County Cook</p> <p>Department Management</p> <p>Department_ID 1000</p> <p>Empl_Status Contractor</p> <p>Empl_Type Temporary</p> <p>Employee_ID 10000416</p> <p>End_Date 2023-9-2</p> <p>First_Name Macon</p> <p>Hire_Date 2018-7-22</p> </div> </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;">  user  ▼ </div> <div style="font-size: 0.9em;"> <p>DN CN=mdontrel,OU=Management,OU=...</p> <p>accountExpires 9223372036854776000</p> <p>displayName Macon Dontrel</p> <p>employeeID 10000416</p> <p>mail macon.dontrel@softwareidm.lab</p> <p>objectGUID TgRy57wLUUSroLY7wpuFww==</p> <p>member Of CN=All US staff SG,OU=Management,...</p> <p style="margin-left: 20px;">CN=Management SG,OU=Manageme...</p> <p>Count: 2 </p> <p>objectSid AQUAAAAAAAAUVAQAq4SCUmnR4w...</p> <p>pwdLastSet 132754939540705740</p> <p>sAMAccountName mdontrel</p> <p>title Contractor for Management</p> <p>userAccountControl 512</p> <p>userPrincipalName macon.dontrel@softwareidm.lab</p> </div> </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;">  user  ▼ </div> <div style="font-size: 0.9em;"> <p>DN macon.dontrel@student100aadconnec...</p> <p>accountEnabled True</p> <p>createdDateTime 9/7/2021 1:12:34 PM</p> <p>displayName Macon Dontrel</p> <p>employeeid 10000416</p> <p>forceChangePasswordNextSignIn True</p> <p>forceChangePasswordNextSignInWithM False</p> <p>mailNickname mdontrel</p> <p>objectId 98b68995-9c95-483c-8894-88941844...</p> <p>refreshTokensValidFromDateTime 9/7/2021 1:12:34 PM</p> <p>signInSessionsValidFromDateTime 9/7/2021 1:12:34 PM</p> <p>userPrincipalName macon.dontrel@student100aadconnec...</p> <p>userType Member</p> </div> </div>

Time Traveler Presentation

Time Traveler Presentation



- Time Traveler presents silos in which it finds objects that are “joined” to the identity in question (at a point in time)
- The silo on the left is the “focus silo” (highlighted, and typically the focus of investigations)
 - HR the focus- e.g. reviewing how attributes in HR relate to attributes in target systems
 - You can rearrange the other silos by clicking the names, or by dragging silos, and you can collapse silos
- Attribute value highlights
 - If you mouse over an attribute, it is highlighted in **yellow** – any *matching values* are also highlighted – it is very important to understand that this is not because of any actual connection
 - Contrast attribute highlights with the **Contrails** feature that can be enabled to show sync engine (e.g. MIM or HyperSync Panel) relationships between attributes
 - Newly populated attributes are shown in **green** – e.g. after an initial import
 - Modified attributes are shown in **blue** – e.g. modified telephone number or department

What silos are presented?

As discussed there are several ways to access the Time Traveler – but basically you will have clicked an object hyperlink. The Time Traveler presents that object, and objects in other silos that it considers are joined to that object. Depending on how you accessed the Time Traveler, you may be seeing the related objects as they are “Now”, or as they were at some previous point in time (at a different “Timestamp” – see next topic).

Identity Panel has its own mechanism for finding objects it considers to be “joined” – this can be configured. Though we do not cover join configuration, we can say that typically it will be matching up objects according to unique attributes available in the various silos. Silos only appear if there is a joined object to show.

Focus Silo

The silo on the left we refer to as the “focus silo” - both in the sense of it being highlighted, and in the sense that it is typically the focus of your investigations.

For example, you might be looking at attributes in the HR system and how they relate to attributes in target systems (like Active Directory, SAP, or Office 365). If so, it would make sense to have the HR silo in focus - and to arrange the rest of the silos in order of their interest to you.

- You can rearrange the other silos by dragging them. As you drag a silo to a new location, others move around it.
- You can also click the name of a silo and it will be made the focus.
- You can also collapse silos if they are not of interest.

Attribute Value Highlights

Yellow (or Gold): matching attribute values

If you mouse over an attribute, it is highlighted in yellow/gold. Any other matching values are also highlighted. It is very important to understand that this is not because Identity Panel knows they are connected in some way (for example by an attribute flow rule in MIM or HyperSync Panel) - it is simply Identity Panel recognizing that the values are the same.

The screenshot displays the Identity Panel Suite interface with three silos: Workday: People, AD, and Azure. The interface shows attribute values for a user across these silos, with matching values highlighted in yellow/gold.

Silo	Attribute	Value
Workday: People	DN	10030002
AD	employeeID	10030002
Azure	employeeid	10030002

Other attributes shown in the AD silo include: DN (CN=fbaggins,OU=Facilities,OU=UK,DC...), accountExpires (9223372036854776000), displayName (Frodo Baggins), mail (frodo.baggins@softwareidm.lab), objectGUID (Q7Vg/Qu0jEmH/O3OjOtlVQ==), managerOf (CN=sthorly,OU=Facilities,OU=US,DC=...), memberOf (CN=Facilities SG,OU=Facilities,OU=UK,...), objectSid (AQUAAAAAAAAUAAAAq4SCUmnR4w...), pwdLastSet (132756977294394850), sAMAccountName (fbaggins), and title.

Contrails

This should be contrasted with Contrails, which is a feature you can enable, which highlights a relationship between attributes, resulting from synchronization configuration in HyperSync Panel, MIM or Azure AD Connect.

In the following example HyperSync Panel is our sync engine, and we have turned on Contrails (☒), and selected First_Name. What we see is interestingly complicated, because First_Name is used to generate a number of attributes, both directly and indirectly:

- A Hyperverses metadirectory has been defined
- There are mappings to attributes in the Hyperverses, using attributes from our source of truth (Workday HR) – these contrails are green
- You can select a question mark icon to see the details for a mapping – we have highlighted the mapping for displayName, and we can see that a mapping is defined in an Attribute Flow Rule which uses an expression to concatenate First_Name and Last_Name
- There are mappings to attributes in AD and Azure AD, using attributes from other silos (blue ones are precedent – precedence is complicated feature, but in essence the blue ones take priority, but a grey one could flow a value if a precedent mapping would flow a null)

The screenshot displays the Identity Panel Suite interface with several silos and their attributes:

- Workday: People:** Attributes include DN, Addr_Line1, Addr_Line2, City, Company, Country, Country_Code, Department, Department_ID, Empl_Status, Empl_Type, Employee_ID, First_Name, Hire_Date, Job_Title, Last_Name, Location_Desc, Location_ID, Location_Type, Mobile_Phone, and Manager_ID.
- Hyperverses:** Attributes include DN, accountName, adDN, azureid, azureUPN, city, company, country, countryCode, county, department, deptId, displayName, employeeid, employeeStatus, employeeType, givenName, hireDate, isActive, isCorporate, isDormant, and locationDesc.
- AD:** Attributes include DN, accountExpires, company, department, displayName, employeeID, givenName, I, mail, objectGUID, manager, objectSid, physicalDeliveryOfficeName, postalCode, pwnLastSet, sAMAccountName, sn, streetAddress, title, and userAccountControl.
- Azure:** Attributes include DN, accountEnabled, createdDateTime, displayName, employeeid, forceChangePasswordNextSignIn, forceChangePasswordNextSignInWithMFA, givenName, jobTitle, mailNickname, objectId, members OF, refreshTokensValidFromDateTime, securityIdentifier, signInSessionsValidFromDateTime, surname, and title.

Contrails (lines) connect attributes between silos. Green lines represent mappings from Workday HR to Hyperverses. Blue lines represent mappings from Hyperverses to AD and Azure AD. A 'Rule Details' window is open for the 'displayName' attribute in the AD silo, showing the following information:

```

Rule Type: Attribute Flow
Rule: HR - Import Names, Expression: '$(Trim(workday: People.First_Name)) (Trim(workday: People.Last_Name))'
    
```

To be clear, a Hyperverse is not a requirement – it would have been possible in this case to generate rules that flow attributes from HR to AD, and others from HR to Azure AD. But we can see here the advantages of a Hyperverse:

- It can give us a central, authoritative view of an identity
- It can save on transformations: displayName (for example) only needs to be defined once

Contraails shows how attributes are intended flow as a result of synchronization activity. While the yellow/gold highlight is simply identifying similar values.

Green highlights: new

Newly populated attributes are shown in green, so just after an initial creation, the object in a silo will be almost entirely green.

The screenshot displays the Identity Panel Suite interface with three columns of user attributes. The 'person' column shows attributes like DN, Addr_Line1, and Department. The 'AD' column shows attributes like DN, accountExpires, and displayname. The 'Azure' column shows attributes like DN, accountEnabled, and displayName. The 'Azure' column attributes are highlighted in green, indicating they are newly populated.

person	AD	Azure
DN 10000002	DN CN=sdiethild,OU=Management,OU=U...	DN samvell.diethild@student100aadconne...
Addr_Line1 100 S Michigan Ave	accountExpires 9223372036854776000	accountEnabled True
Addr_Line2 Lab Inc.	displayName Samvell Diethild	displayName Samvell Diethild
Company Lab Inc.	employeeID 10000002	employeeid 10000002
Country United States of America	mail samvell.diethild@softwareidm.lab	forceChangePasswordNextSignIn True
Country_Code US	objectGUID Roz35TQG602+V9gZCWfu/g==	forceChangePasswordNextSignInWithM False
Country Cook	objectSid AQUAAAAAAAAUAAAAq45CUmnR4w...	mailNickname sdiethild
Department Management	pwdLastSet 132754936164926740	objectid ed120827-7ad0-410a-b6a5-55f6100c2...
Department_ID 1000	sAMAccountName sdiethild	refreshTokensValidFromDateTime 9/7/2021 1:06:56 PM
Empl_Status Employee	title Vice President of Management	signInSessionsValidFromDateTime 9/7/2021 1:06:56 PM
Empl_Type Permanent	userAccountControl 512	userPrincipalName samvell.diethild@student100aadconne...
Employee_ID 10000002	userPrincipalName samvell.diethild@softwareidm.lab	userType Member
First_Name Samvell		
Hire_Date 2020-7-11		
Job_Title Vice President of Management		
Last_Name Diethild		
Location_Desc		

Blue highlights: modified

Modified attributes are shown in blue, for example when a telephone number changes or a department changes.

The screenshot displays the Identity Panel Suite interface with three panels showing user details for 'user'.

AD Panel:

- DN:** CN=sdiethild,OU=Management,OU=U...
- accountExpires:** 9223372036854776000
- department:** Management
- displayName:** Samvell Diethild
- employeeID:** 10000002
- mail:** samvell.diethild@softwareidm.lab
- objectGUID:** Roz35TQG602+V9gZCWfu/g==
- manager:** CN=sjery,OU=Management,OU=US,D... +
- objectSid:** AQUAAAAAAAAUVA...AAq45CUmnR4w...
- pwdLastSet:** [Redacted]
- sAMAccountName:** sdiethild
- title:** Vice President of Management
- userAccountControl:** 512
- userPrincipalName:** samvell.diethild@softwareidm.lab

Azure Panel:

- DN:** samvell.diethild@student100aadconne...
- accountEnabled:** True
- createdDateTime:** 9/7/2021 1:06:56 PM
- department:** Management
- displayName:** Samvell Diethild
- employeeID:** 10000002
- forceChangePasswordNextSignIn:** True
- forceChangePasswordNextSignInWithM:** False
- mailNickname:** sdiethild
- objectId:** ed120827-7ad0-410a-b6a5-55f6100c2...
- refreshTokensValidFromDateTime:** 9/7/2021 1:06:56 PM
- signInSessionsValidFromDateTime:** 9/7/2021 1:06:56 PM
- userPrincipalName:** samvell.diethild@student100aadconne...
- userType:** Member

Workday: People Panel:

- DN:** 10000002
- Addr_Line1:** 100 S Michigan Ave
- Addr_Line2:** [Redacted]
- Company:** Lab Inc.
- Country:** United States of America
- Country_Code:** US
- County:** Cook
- Department:** Management
- Department_ID:** 1000
- Empl_Status:** Employee
- Empl_Type:** Permanent
- Employee_ID:** 10000002
- First_Name:** Samvell
- Hire_Date:** 2020-7-11
- Job_Title:** Vice President of Management
- Last_Name:** Diethild
- Location_Desc:** [Redacted]

Timestamps

Timestamps



- When you view an identity in the Time Traveler, you do so for a particular point in time, selected from a dropdown of available timestamps
- The final timestamp is a special one called "Now" – current state of the identity across silos
- Focus Silo – on the left, and by default we see timestamps generated for this silo
- Timestamps are generated when:
 - Identity Panel detects a change while scanning a system
 - As a result of Identity Panel actions e.g. HyperSync Panel
 - MIM is a special case: Identity Panel can control MIM Sync, and hence detect all changes
- In simple cases we might see a series of changes to an object – but we will only see all the changes from a system if timely scans have taken place
- "Dates from All Silos"
 - Incorporates the timestamps from changes to related objects in other silos
 - Inception - you can only see timestamps from the point in time when the object first existed in the focus silo – for this reason, it often makes sense to keep your source of truth as the focus silo, since this will typically have the earliest timestamp

www.oxfordcomputertraining.com

www.softwareidm.com

The Date/Time Dropdown

When you view an identity in the Time Traveler, you do so for a particular point in time. The Time Traveler includes a dropdown with a list of available timestamps (time and date), and you can choose to view the identity at any of these points in time. Essentially, these are the timestamps when a scan identified that something happened to the object in question.

The final timestamp is a special one called "Now" and simply shows the current state of the object across silos (as far as Identity Panel "knows").

You can navigate through time with respect to the object in the focus silo, by clicking the right and left arrows associated with the dropdown, or by selecting a timestamp from the dropdown itself.

The screenshot shows the Time Traveler interface. At the top, there is a dropdown menu for timestamps, currently showing 'Now'. Below the dropdown, there are two columns of details for a user object. The left column shows address and company information, and the right column shows user-specific details like DN, accountEnabled, and employeeID.

Field	Value
DN	frodo.baggins@student100aadconnec...
accountEnabled	True
createdDateTime	9/8/2021 10:05:15 PM
displayName	Frodo Baggins
employeeid	10030002
mail	frodo.baaains@softwareidm.lab
displayName	Frodo Baggins
employeeID	10030002
mail	frodo.baaains@softwareidm.lab
displayname	Frodo Baggins
employeeid	10030002
mail	frodo.baaains@softwareidm.lab

Timestamps and the focus Silo

By default, the list of timestamps we see is a list of timestamps generated in relation to the object in question, in the focus silo. Other silos will likely have other timestamps relating to changes to associated objects in those silos. Generally, we don't see all the timestamps from every related object in every silo. We might say that the list of timestamps is "focus silo centric".

What Timestamps are Generated, and when?

Timestamps are generated when Identity Panel scans a connected system and detects a change.

However, there are circumstances in which Identity Panel generates timestamps because it "knows" something happened. For example, if Test Panel makes changes to a system, or if HyperSync Panel synchronizes objects, we can expect that it records timestamps.

Also, MIM is a special case of a connected system. Identity Panel is able to completely control the MIM synchronization process, and when it does it has access to every change that goes through MIM. Thus, Identity Panel can detect and record a complete history of the MIM silos (even though that MIM history will probably not be a complete history of the systems it connects to). This is not true for Azure AD Connect which runs on its own (usually 30 minute) synchronization cycle.

Depending on what system is being scanned, exactly when changes take place in systems, and when scans take place, you may get results that are – on the face of things – unexpected.

In the simplest cases we might expect to see just a series of changes to an object. So, if we consider the lifecycle of a typical user identity in our lab environment, we might expect to see timestamps for the user object in the HR silo, as follows:

- Initial creation of the user from the HR system
- A change to a job title (for example) will generate one or more timestamps, depending on the exact timing of scans and synchronizations
- Another change to another HR attribute
- A change to the status in the HR system – marked as being on sabbatical (for example)
- And so on...

This will only happen if a scan takes place between each change. A number of changes could take place (in more than one editing session), before a scan is run. Identity Panel will see a single set of changes with a single timestamp. To be quite clear, if an attribute is changed from A to B, then B to C, without a scan in between, Identity Panel will see this as a single change from A to C with a single timestamp. Further, if an attribute is changed from A to B, then B to C, then C back to A, without a scan in between, Identity Panel will not detect a change at all.

"Dates from All Silos" checkbox

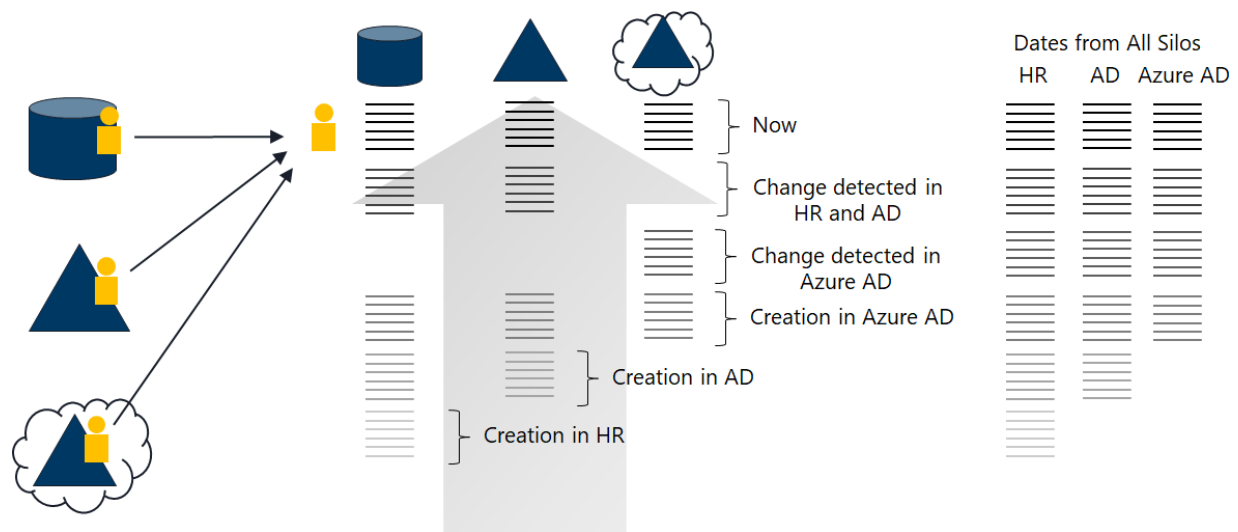
As discussed, by default, the list of timestamps is restricted to those generated in respect of the focus silo – it can be useful to include timestamps recorded against other silos – selecting the "Dates from All Silos" checkbox. This will usually lead to more timestamps (of course), and hence more steps as you move through time. Usefully it can thus provide a more complete picture of changes –

perhaps allowing you to see changes as they propagate from system to system, which is not always possible using just the timestamps for the focus silo.

However, timestamps can still only be presented if the object in the focus silo existed at that time. Put another way, you can only see timestamps from the point of inception of the object in the focus silo (from the point in time in time when the object first existed in the focus silo), for this reason it often makes sense to have your source of truth as the focus silo, since this will typically have the earliest timestamp. Note though, that when it comes to viewing contrails, you may be less concerned about timestamps, and hence you might choose a different silo as your focus - the one associated with the rules in which you are interested.

In the diagram we see that creation in HR has been recorded, then creation in AD (which in this case also generated an HR timestamp – we don't need to know why), then creation in Azure AD (again we see other timestamps). Then, however, a change is detected in Azure (perhaps the generation of GUID in that system) – with no corresponding change in HR or AD. And so on – creating “holes” in the diagram (where no timestamp was warranted).

We can see that the default list of timestamps for HR is smaller than if we select “Dates from all silos”.



Reference and Multi-value Attributes

Reference and Multi-value Attributes



- Many attributes are simple strings
 - A few of these are multi-value e.g. proxy addresses
 - Some attributes are reference attributes e.g. manager or group member
- Reference and multi-valued attributes are handled differently
 - Timestamps not created unless another attribute is modified too
 - Multi-value additions in **green**, deletions in **red** (you don't see many of these)
 - To see a continuous history, you must use the attribute history feature (see next topic)
- References are displayed as hyperlinks – you can drill down
- For every reference attribute, Identity Panel generates a “pseudo” reverse reference attribute and adds “Of” to the attribute name displayed
 - The user attribute **Manager** gives rise to the user attribute **Manager Of**
 - The group attribute **Member** gives rise to the user (or group) attribute **Member Of**

Introduction

Many of the attributes we deal with will be simple strings of characters. A few of these are multi-value, for example proxyAddresses. Some attributes are reference attributes - for example manager (a single-value reference attribute), or group member (a multi-value reference attribute which can have more than one member). These attributes are handled a little differently in the Time Traveler.

Timestamps for Reference and Multi-value Attributes

Timestamps are not created when changes occur to these, unless by chance another “normal” attribute change is captured by a scan at the same time. In these circumstances, additions to reference or multi-value attributes are shown in green, while deletions are shown in red. To be clear, you won't often see these!

To see a continuous history, you need to use the attribute history feature (see next topic). The “Now” timestamp always give you the current view of all attributes (as far as Time Traveler knows).

Note: References are displayed as hyperlinks, which can be used to quickly drill down to those referenced objects.

The screenshot displays the Identity Panel Suite interface. On the left, a user profile for 'user' is shown with various attributes including DN, accountExpires, displayName, employeeID, mail, objectGUID, member Of, manager, objectSid, pwdLastSet, sAMAccountName, and telephoneNumber. The 'member Of' attribute is highlighted in green, and the 'telephoneNumber' attribute is highlighted in light green. On the right, a 'Workday: People' view is shown with a list of users. Below this, a 'Manager_ID Of' attribute is highlighted in yellow, showing a list of Manager_ID values (10030365, 10030352, 10030320, 10030312, 10030116, 10030114, 10030083, 10030082, 10030073, 10030070) and a count of 13. Below the list, the 'Manager_ID' attribute is shown with a count of 1, and the 'State' attribute is shown with a count of 1. The 'State' attribute is highlighted in light green, and the 'Status' attribute is shown with a value of 'Active'. The 'None' attribute is shown with a count of 1. The 'None' attribute is highlighted in light green. The 'None' attribute is shown with a count of 1. The 'None' attribute is highlighted in light green.

Reverse reference attributes

For every reference attribute, like member (groups) or manager (user), Identity Panel generates the reverse reference attribute and adds "Of" to the attribute name displayed. Thus, you will see that a user might have pseudo reference attributes for "manager Of" (multi-value) and "member Of" (also multi-value) - even though neither of these attributes really exists in the systems concerned. Of course a group can also have a memberOf pseudo attribute.

In AD Users and Computers, a similar trick is performed: when you examine the properties of a user and you can see which groups they are a member of.

Attribute History

Attribute History



- The history of an individual attribute in any visible silo is readily available
- For simple, single-value attributes like display name or job title, it is simply a matter of clicking the attribute of interest, in the silo of interest
- Reference attribute values (attributes that point to other objects, like manager or member) are presented as hyperlinks to the referenced objects – for this reason alone they have to be handled differently: you click the Count value, this applies to:
 - All types of reference attributes, including single-value reference attributes like manager
 - Other multi-value attributes (of course these values are not hyperlinks)
 - "Reverse" or "Of" references generated by Identity Panel, such as "Manager Of" and "Member Of"
- In the search results you can select which fields to display
- Advanced Search
 - Simply clicking Search gets you to the whole history, or you can enter a search value, time windows for add and remove, and (for reference attributes) an optional attribute to search (versus all attributes)
 - You can use the wild cards * and ?

Introduction

So far we have looked at objects as a whole, but the history of an individual attribute in any visible silo is readily available too. Multi-value and reference attributes are handled a little differently from simple, single attributes.

Simple, single attributes

For simple, single-value attributes like display name or job title, you can simply click the attribute of interest, in the silo of interest. Many of these attributes will be strings, but this applies equally to numbers, booleans, and binaries. For example, on clicking department in the HR silo, we might get this:

The screenshot shows the 'Attribute History for pwdLastSet' dialog box. The table within the dialog is as follows:

Change	Timestamp	Value	Run History
Update	Thu Sep 09 2021, 12:38:58	132756611303151840	Source
Update	Thu Sep 09 2021, 12:35:24	0	Source
Add	Wed Sep 08 2021, 23:05:14	132756123148319780	Source

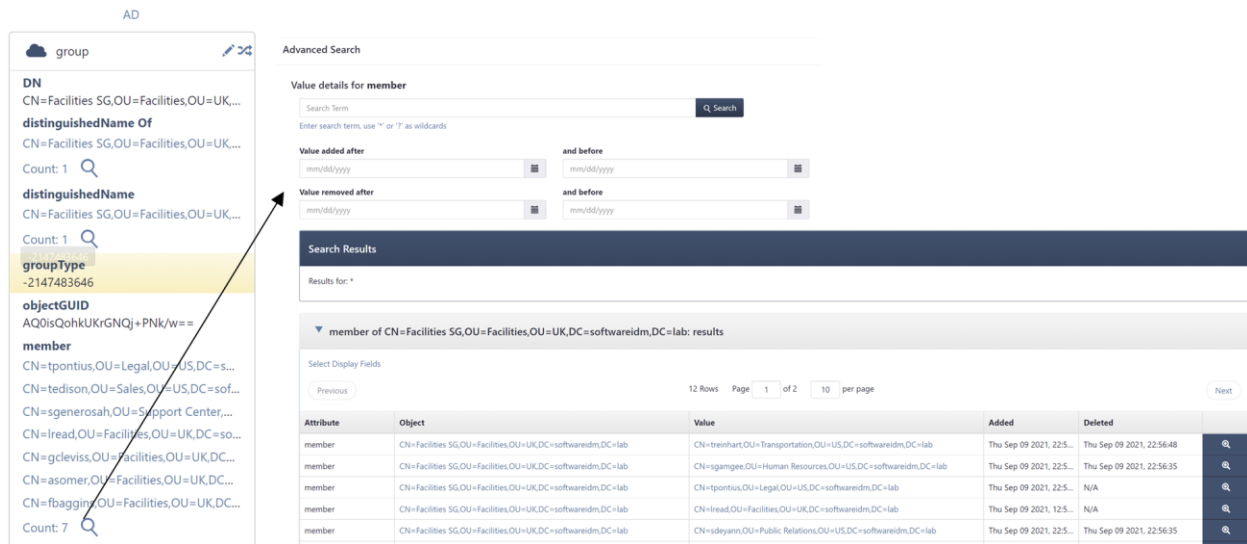
The background shows the user's profile details for 'frodo.baggins@softwareidm.lab', including attributes like DN, accountExpires, displayName, employeeID, mail, objectGUID, objectSid, sAMAccountName, title, userAccountControl, userPrincipalName, forceChangePasswordNextSignIn, forceChangePasswordNextSignInWithM, mailNickname, objectId, refreshTokensValidFromDateTime, signInSessionsValidFromDateTime, userPrincipalName, userType, Country_Code, County, Department, Department_ID, Empl_Status, Empl_Type, Employee_ID, First_Name, and Hire_Date.

At some point this attribute first took a value, in this case when the object was created. Later, presumably, an administrator reset the password with the “User must change password at next logon” selected (what this does is set pwdLastSet to 0). Next, we assume, the user did indeed change their password. Of course, timestamps had to be created (effectively scans had to take place) between each action for these to be recorded.

Multi-value and Reference Attributes

We have already seen that multi-value and reference attribute values are presented as hyperlinks that link to the referenced objects. For this reason alone, they have to be handled a little differently. There is a Count value underneath the attribute value (even if it is a single value reference attribute like manager), and you click this to access the attribute history.

For example, the member attribute of a group will show a list of members, each is a hyperlink that will take you to the member (usually a user). The Count tells you how many members there were at the selected date/time. The magnifying glass icon next to the Count indicates that you can drill down to the history. Clicking the Count brings up an Advanced Search dialog, and if you click Search without modifying any search parameters, you get to the history:

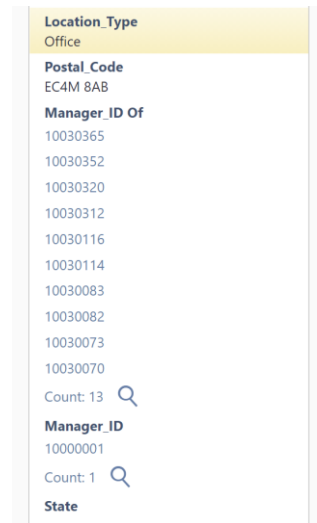


This applies to:

- All types of reference attributes, including single-value reference attributes like manager
- Other multi-value attributes (of course in this case, the values are not hyperlinks) - for example, department in the LDS silo is multi-value (even though it only ever has a single value)
- "Reverse" or "Of" references generated by Identity Panel, such as **manager_ID Of** and **member Of**

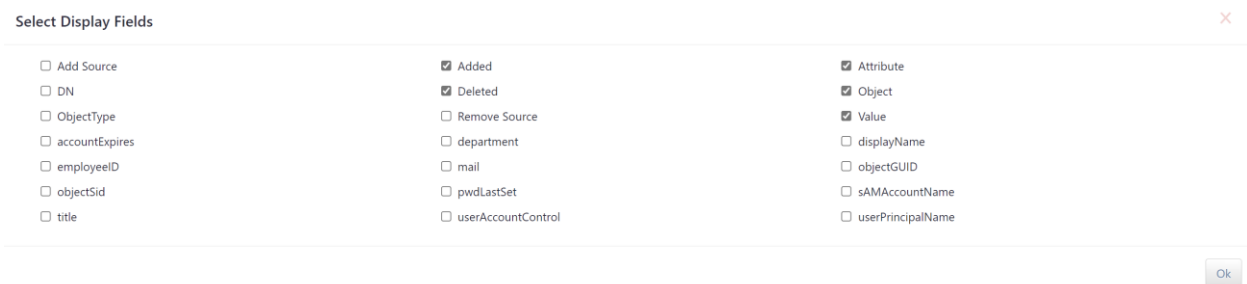
In the screenshot (right), you can see the **manager_ID** attribute, and the generated **manager_ID Of** attribute, for a user in the Workday silo.

As with the member attribute you can get a history of the manager_ID Of attribute – and you can also get at attribute history in the same way.



Select Display Fields

You can also select which fields to display by clicking **Select Display Fields**:



Note that when viewing the history for the member attribute, it is likely you will want to include **Added** and **Deleted**.

Advanced search

For attributes other than simple, single-value attributes, clicking them brings up an Advanced Search dialog. Simply clicking Search gets you to the whole history, but you can modify the search. For example, here we have clicked the member attribute:

Advanced Search

Value details for **member**

vice* Q Search

Enter search term, use '*' or '?' as wildcards

Value added after mm/dd/yyyy 📅

Value removed after mm/dd/yyyy 📅

Hide Removed Reference Values

Q Search

and before mm/dd/yyyy 📅

September 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat	
29	30	31	1	2	3	4	00:00
5	6	7	8	9	10	11	01:00
12	13	14	15	16	17	18	02:00
19	20	21	22	23	24	25	03:00
26	27	28	29	30	1	2	04:00
							05:00

We are about to see members of the group concerned. You can narrow the search:

- You can use wildcards (for example: the intention here is to get all vice presidents)
- You can specify a range of dates/times for adds and deletes (or removes) - so anyone who became a member in a time window, or stopped being a member (you can leave a date unspecified to make the time window open at one end)
- You can check the box to “Hide Removed Reference Values”

Note: Search criteria are ANDed. So you can search for a reference added within a time window, or a reference removed within a time window, or a reference both added and removed within time windows, but you can't search for all changes within the time window (both adds and removes) because the search criteria are ANDed. Also note that any date selected defaults to 00:00 (midnight just before the day starts).

Lesson 2: Other Time Traveler Features

Lesson 2: Other Time Traveler Features



- Advanced Time Traveler Search
- Customized Time Traveler Views
- Securely sharing a URL

www.oxfordcomputertraining.com

www.softwareidm.com

In this lesson, we will discuss some of the other Time Traveler features.

Advanced Time Traveler Search

Advanced Time Traveler Search



- You use “Search Time Traveler” to find objects, which you then view in the Time Traveler
 - If you simply enter a value, Identity Panel searches for that value in all attributes in all objects
 - Search works on a whole word basis, but you can use the wildcards * and ?
 - Often many results are returned and you will need to narrow down the search
- Advanced search limits the search to a single silo - first you choose which Silo from the dropdown, after which you are presented with the Advanced Search dialog, which lets you:
 - Enter a Search Term to search across all attributes and objects as before, but only in the chosen Silo
 - Choose a particular attribute to be searched, with a choice of operators
 - Contains (word search, can use wildcards, words are ORed, better matches at the top), example: “Development Research” will find “Research and Development”, and “Research”, and “Development”
 - Phrase (word search in order of words), example: “Development Research” will not find “Research and Development”, but “Research Development” will find “Research and Development”
 - Specify a particular object type (the dropdown is populated according to the chosen silo)
 - Specify a date ranges for creation
 - Specify a date range for (any) modification
 - Specify that deleted objects should be included

www.oxfordcomputertraining.com

www.softwareidm.com

Search Time Traveler

You use the Search Time Traveler feature to find objects, which you then view in the Time Traveler. If you simply enter a value and press ENTER, Identity Panel searches for that value in all attributes in all objects. Search works on a whole word basis, but you can use the * and ? wildcards. If you are smart about it, or lucky, you can maybe find the exact object you want, or at least a small list of candidates, but often you will need to narrow down the search.

The Advanced Search Dialog

To invoke the Advanced Search you must first choose a silo from the dropdown (and indeed your search is then limited to that Silo). The Advanced Search dialog lets you:

- Search the entire Silo
- Enter a Search Term (a value), and search across all attributes and objects as before, but in the chosen Silo
- Choose a particular attribute to be searched, with a choice of operators:
 - Contains
 - Searches at word boundaries
 - You can use wildcards
 - If you enter multiple words, a list is returned of all objects with any of the words, with closer matches (i.e. more words matching) at the top of the list

- Example: “Development Research” will find “Research and Development”, and “Research”, and “Development”
- Phrase
 - Searches at word boundaries
 - Searches for a sequence of words in a particular order
 - Example: “Development Research” will not find “Research and Development”, but “Research Development” will find “Research and Development”
- Specify a particular object type
 - The dropdown is populated according to the chosen silo
 - The default is all objects (if you don’t specify one)
- Specify a date range for creation
- Specify a date range for (any) modification
- Specify that deleted objects should be included

Advanced Search ✕

Search Silo

AD ▼

Start by choosing which silo of data to search within.

Attribute (Opt.) ▼ Contains x ▼

Search Term Q Search

Enter search term, use "*" or "?" as wildcards

Object Type

Object Type ▼

Created after and before

mm/dd/yyyy mm/dd/yyyy

Modified after and before

mm/dd/yyyy mm/dd/yyyy

Include Deleted Records

Q Search

Ok

Customized Time Traveler Views

Customized Time Traveler Views



- When you access the Time Traveler, depending on how things are configured, you may see a specially filtered Shutter View:
 - The names and presentation of attributes and silos may have been changed to aid clarity
 - The number of attributes and silos may have been restricted, either for security reasons, or simply to reduce the clutter
- A Shutter View is a custom view that can display a limited subset of your data in the Time Traveler
 - Depending on your role you may have many shutter views or it can be locked down to a single view
- An administrator can turn off time-traveling for a role – in other words, you might only be able to see the most recent state of objects
- Shutter views control which silos and attributes you see, and how they are displayed – “MIM Lab: AD” might become “Active Directory”, 131075078247942570 might become 2016-05-12 06:23
- When a shutter view has been selected, Search is limited by the shutter view
- Depending on your role, you will – in any case – only be able to access certain attributes
- An administrator can rename attributes – and this will apply across all views
- It is possible that attribute names, and other labels in the Identity Panel, are localized

www.oxfordcomputertraining.com

www.softwareidm.com

When you access the Time Traveler, depending on how things are configured you may see a specially filtered view – a “Shutter View”:

- The names and presentation of attributes and silos may have been changed to aid clarity
- The number of attributes and silos may have been restricted either for security reasons, or simply to reduce the clutter

Shutter views

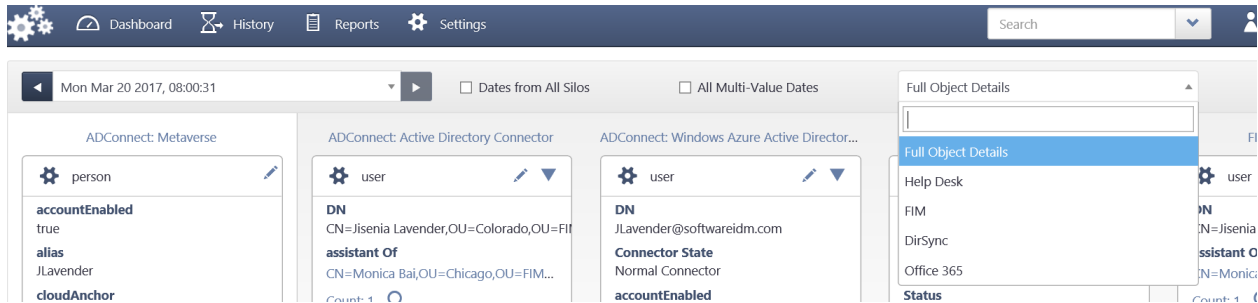
A shutter view is a sort of elaborate filter - it is a custom view that can display a limited subset of your data in the Time Traveler, and transform attribute values.

An administrator can use shutter views to create simplified windows into your data, to aid clarity or simply so that you won't be bombarded by a sea of attributes!

Which views do you get?

Depending on your role you will have different Shutter Views (or filtered views) available:

- You may have a list of Shutter Views in a dropdown (see the picture below)
- If no particular Shutter View has been configured for you, you get a default view called “Full Details” (you may not actually see that name until you select it from the dropdown)



- You may be restricted to one view which you cannot change

Characteristics of Shutter Views

Time Travel

An administrator can turn off time-traveling for a role – in other words, you might only be able to see the most recent state of objects (“Now”).

Silos and Attributes

Shutter views control which silos you see, which attributes you see, and how they are displayed (the format). So in addition to simply restricting data, it is possible that:

- In one view a silo is called “MIM Lab: AD” and in another the same silo is called “Active Directory”
- In one view an attribute is displayed as 131075078247942570 (an Active Directory “file time” format) and in another the same attribute might be displayed as 2016-05-12 06:23

Search

When a shutter view has been selected, Search is limited by the Shutter View. So search takes place across the silos available to the view, and the attributes available in each silo.

Roles and Security

Depending on your role, you will only be able to access certain attributes – this applies whatever shutter view you select.

Attribute Names

An administrator can rename attributes – and this will apply across all views. For example:

- The Active Directory attribute called “sn” might be displayed as “Surname”
- The Office 365/Azure AD attribute called “Ext #5” might be displayed as “Employee ID”

The only reason this might matter to you is if you are already familiar with the original attribute name in a given system – which could be confusing.

The following shows the default “Full Details” in a particular case:

The screenshot displays three user profiles in a side-by-side comparison view. At the top, there is a navigation bar with a 'Now' dropdown, a 'Dates from All Silos' checkbox, and a 'Full Details' button. The profiles are categorized as follows:

- Workday: People:**
 - person** (ID: 10030002)
 - Addr_Line1:** Paternoster House
 - Addr_Line2:** 65 St. Paul's Churchyard
 - Company:** Lab Inc.
 - Country:** United Kingdom
 - Country_Code:** UK
 - County:** Greater London
 - Department:** Facilities
 - Department_ID:** 1003
 - Empl_Status:** Employee
 - Empl_Type:** Permanent
 - Employee_ID:** 10030002
 - First_Name:** Frodo
 - Hire_Date:** 2011-5-5
 - Job_Title:** Vice President of Facilities
- AD:**
 - user** (ID: 10030002)
 - DN:** CN=fbaggins,OU=Facilities,OU=UK,DC=...
 - accountExpires:** 9223372036854776000
 - displayName:** Frodo Baggins
 - employeeID:** 10030002
 - mail:** frodo.baggins@softwareidm.lab
 - objectGUID:** Q7Vg/Qu0jEmH/O3OjOtlVQ==
 - manager Of:** CN=sthorry,OU=Facilities,OU=US,DC=... (Count: 1)
 - member Of:** CN=Facilities SG,OU=Facilities,OU=UK,... (Count: 1)
 - objectSid:** AQUAAAAAAAAUAAAAq4SCUmnR4w...
 - pwdLastSet:** 132756977294394850
 - sAMAccountName:** fbaggins
 - title:** Vice President of Facilities
 - userAccountControl:** 512
- Azure:**
 - user** (ID: 10030002)
 - DN:** frodo.baggins@student100aadconnec...
 - accountEnabled:** True
 - country:** United Kingdom
 - createdDateTime:** 9/8/2021 10:05:15 PM
 - department:** Facilities
 - displayName:** Frodo Baggins
 - employeeid:** 10030002
 - forceChangePasswordNextSignIn:** True
 - forceChangePasswordNextSignInWithM:** False
 - givenName:** Frodo
 - jobTitle:** Vice President of Facilities
 - mailNickname:** fbaggins
 - objectId:** cbe9f892-6a5b-41e4-b0d2-de4384dcf...
 - postalCode:** EC4M 8AB
 - refreshTokensValidFromDateTime:** 9/8/2021 10:05:15 PM

This one shows a modified view in which the AD silo has been renamed, and some attributes (notably userAccountControl and pwdLastSet) have been formatted for readability:

The screenshot displays the Identity Panel Suite interface with a navigation bar at the top showing 'Now', a search filter 'Dates from All Silos', and a user selection 'AD'. The main content is divided into three columns representing different data sources:

- Workday: People:** Shows a 'person' object with attributes like DN (10030002), Addr_Line1 (Paternoster House), Addr_Line2 (65 St. Paul's Churchyard), Company (Lab Inc.), Country (United Kingdom), Country_Code (UK), County (Greater London), Department (Facilities), Department_ID (1003), Empl_Status (Employee), Empl_Type (Permanent), Employee_ID (10030002), First_Name (Frodo), Hire_Date (2011-5-5), and Job_Title (Vice President of Facilities).
- Active Directory:** Shows a 'user' object with attributes like DN (CN=fbaggins,OU=Facilities,OU=UK,DC=...), accountExpires (9999-12-31T23:59:59.9999999), displayName (Frodo Baggins), employeeID (10030002), mail (frodo.baggins@softwareidm.lab), objectGUID (Q7Vg/Qu0jEmH/O3OjOtlVQ==), managerOf (CN=sthorly,OU=Facilities,OU=US,DC=...), memberOf (CN=Facilities SG,OU=Facilities,OU=UK,...), objectSid (S-1-5-21-1384285355-149148009-164...), pwdLastSet (2021-09-09T21:48:49.439485+00:00), sAMAccountName (fbaggins), title (Vice President of Facilities), userAccountControl (NORMAL_ACCOUNT), and userPrincipalName.
- Azure:** Shows a 'user' object with attributes like DN (frodo.baggins@student100aadconnec...), accountEnabled (True), country (United Kingdom), createdDateTime (9/8/2021 10:05:15 PM), department (Facilities), displayName (Frodo Baggins), employeeid (10030002), forceChangePasswordNextSignIn (True), forceChangePasswordNextSignInWithM (False), givenName (Frodo), jobTitle (Vice President of Facilities), mailNickname (fbaggins), objectId (cbe9f892-6a5b-41e4-b0d2-de4384dcf...), postalCode (EC4M 8AB), and refreshTokensValidFromDateTime (9/8/2021 10:05:15 PM).

Localization

It is possible that attribute names, and other labels in the Identity Panel, are localized – translated into another human language like Portuguese or German. This will depend on Identity Panel having been configured for the language concerned, and the browser having been switched to the language, too.

To switch to a different language of choice, assuming that the language you would like has already been configured in Identity Panel, you need to make sure that the language has been added to Windows via the Control Panel, configure your browser to use the language, and restart your browser.

If you encounter the wrong language, your first stop is to check the browser settings. Your second stop is to tell your administrator.

Securely sharing a URL

Securely Sharing a URL



- When you have found a particular presentation of data – be it a filtered history, or a Time Traveler view, you can simply copy the URL and send it to someone else
- They will only be able to access data according their role and the security settings for that role
- For example, if you are viewing an identity with all the attributes, across all relevant silos, for a particular date/time, you can copy the URL, and someone else can get to that exact same view, at the same time - to the extent that their role (and the associated security) allows it
- Example URLs:
 - <https://panelweb/object/83fc4c0b-3420-e711-810f-002248017a5e#!timestamp=2017-04-13T11%3A22%3A33.49Z>
 - <https://panelweb/object/83fc4c0b-3420-e711-810f-002248017a5e#!timestamp=now>

www.oxfordcomputertraining.com

www.softwareidm.com

When you have found a particular presentation of data – be it a filtered history, or a Time Traveler view – you can simply copy the URL and send it to someone else

They will only be able to access the data according their role and the security settings for that role, so you do not need to worry about someone seeing something they shouldn't.

For example, if you are viewing an identity, all the attributes, across all relevant silos, for a particular date/time, you can copy the URL, and someone else can get to that exact same view, at the same time - to extent that their role (and the associated security) allows it.

Example URLs:

<https://panelweb/object/83fc4c0b-3420-e711-810f-002248017a5e#!timestamp=2017-04-13T11%3A22%3A33.49Z>

<https://panelweb/object/83fc4c0b-3420-e711-810f-002248017a5e#!timestamp=now>

Lab 3: Time Traveler

Lab 3: Time Traveler



- Exercise 1: Time Traveler
- Exercise 2: Reference Attributes
- Exercise 3: Other Time Traveler Features

Logon Information - replace XX with your assigned student number e.g. 01

Virtual machine	IDPLabXX.WestEurope.cloudapp.azure.com
Domain username	softwareIDM\Labadmin
Azure username	labadmin@IDPLabXX.onmicrosoft.com
Password	\$IDMTrainingLogin

Estimated time: 60 minutes

Using the Identity Panel Suite

Course Number: A801

Lab 3: Time Traveler

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Lab 3: Time Traveler	1
Scenario.....	1
Exercise 1: Time Traveler.....	1
Exercise 2: Reference Attributes	7
Exercise 3: Other Time Traveler Features.....	8

Lab 3: Time Traveler

Scenario

In this Lab you will familiarize yourself with Time Traveler. You will:

- Examine the Time Traveler
- Examine reference attributes
- Examine other Time Traveler features

Exercise 1: Time Traveler

The main tasks for this exercise are as follows:

- Explore the Time Traveler interface
- Time traveling and the Focus Silo
- Examine the effect of the "Dates from All Silos" checkbox

Task 1: Explore the Time Traveler interface

Note: A general way of accessing the Time Traveler is by Search. The search tool is always available (top right) and it can be used to search across all silos, or within a particular silo using a number of advanced search features (which will be covered later).

1. In Identity Panel (connect.identitypanel.com) if necessary sign in as **labadmin@IDPLabXX.onmicrosoft.com** (where **XX** is your assigned student number – e.g. 01) with the password **\$IDMTrainingLogin**
2. Search for **Took** in Time Traveler and follow the hyperlink for **Peregrin Took** in the **Azure** silo

Note: The search is a global search across all attributes and all silos (by default). As there is only one person called Took (and it's not used in any other attribute) you get at most one result per directory silo. If you were to search for something like "facilities" you would get several results because several people have a department attribute value of facilities and there is an Azure group called facilities.

3. Mouse over **employeeID**

Note: As already mentioned, when you mouse over attributes they are highlighted in gold and any attributes showing the same data in other silos are also highlighted in gold. This highlight depends on the values that Identity Panel sees and **not** on any relationship between the fields.

Attributes highlighted in blue are the attributes that are changing at the point in time. New attribute values are shown in green and attribute values to be deleted (rarely seen except when looking at multi-value attributes such as `memberOf` or `Member`) are shown in red.

4. Notice that **mobilePhone** is highlighted in blue (because the attribute value changed)
5. Click **mobilePhone**

Note: This gives you an immediate history of changes to this attribute value for this user – we edited Peregrin Took’s phone number twice using Service Panel, and here we can see the current value (in blue), and the previous new value (in green) and you can also get to the schedule run that recorded a value change.

In our lab environment, the mobile phone number changes were implemented in Service panel by workflows. In Identity Panel History, workflow events are recorded as a single summary entry which is generated once an hour, or when Panel Service restarts. We will restart Panel Service to ensure that the workflow summary is available in the History now.

6. Close the **Attribute History for mobilePhone** window
7. On your VM in **Services.msc** restart **SoftwareIDM.PanelService**
8. After a minute or so, in Identity Panel click **mobilePhone** and follow either of the Run History **Source** hyperlinks - you can see the Workflow summary record which includes the workflow which gave rise to this value
9. Close the **Attribute History For mobilePhone** window and click the **Back** button to return to Time Traveler

Note: So, you can actually go straight to the history entry associated with the value change, or come back to the Time Traveler and go to a different one - and having perhaps found something interesting, further explore the particular run history step that gave rise to it (like looking at the other objects that were changed at the same time).

Note: Reference and multi-value attributes behave a little differently and we will cover them later.

10. Click ▼ at the top right of one of the silos *on the right* - this collapses the silo which is useful when you have many silos
11. Click ► to expand it again

Note: Most of the time, viewing your data in Time Traveler and clicking the attributes to examine their changes, provides enough information for you to understand what has happened to an object. Occasionally, you may find that you need to examine an object in more depth travelling through time so that you can see the entire state of all the corresponding objects at any given time - we will do this in the next task.

Task 2: Time traveling and the Focus Silo

Note: In the Time Traveler what you see is a representation of an object and its attributes in each silo in which it is present, at a particular point in time. There are a few key points that are important to grasp early on. The aim of Time Traveler is that you can look at the set of corresponding objects in all the silos at a given point in time - but this can only happen if Identity Panel was able to scan at that point. Usually it scans the connected systems on a schedule you define, so if you were to make a series of changes to an attribute value in a source system without an Identity Panel scan taking place, Identity Panel (and Time Traveler) would only see the aggregated result of all those attribute value changes.

12. In Time Traveler, search for **Duncan** and follow the link for the **Azure** silo

Note: We used the Service Panel form to create a (simulated) user in Workday. HyperSync Panel created (projected) an object in the Hyperverses, and then provisioned AD and Azure AD - it also created an object in Service Panel (this acts as an anchor for Service Panel).

13. Click the **date/time** dropdown and notice that there are a few timestamps (in addition to the Now state)

Note: These are the dates and times where Identity Panel has recorded a changed to the Duncan object but specifically for the Azure silo - because Azure is the silo that is on the far left - it is the one in focus so the timestamps reflect changes to the Duncan object in that silo. What we see to the right of this, is the state of the corresponding objects in the other silos at these dates and times. You are not seeing every date/time where something happens to any Duncan object in any silo - we will cover this shortly.

14. From the **date/time** dropdown select the **oldest date** (the top one in the list) - and the attributes in the Azure silo are highlighted in green

Note: All the attributes in the Azure silo are highlighted in green, reflecting the fact that every single one of them has just been added - the object has just been created at that point in time

15. Notice that at the bottom of the Azure silo, you see that:
 - a. The status of the object is Added (the entire object has been added) - there is a hyperlink to go to the history step where this happened (if you click this, click the back button to get back)
 - b. There are a number of changes reported, corresponding to the number of timestamps (in addition to the Now timestamp) in the dropdown - each silo will have a number of timestamps corresponding to the number of changes Identity Panel has scanned in or "seen" for the "Duncan" object in that silo.
16. Also notice that even though you have selected the oldest timestamp corresponding objects exist in other Silos

Note: Remember that in the classroom we have an environment where broadly speaking, we create new employees using Service Panel forms. When a new employee is created, Service Panel creates the identity in our simulated Workday (HR system), attribute flow projects the object into the

Hyperverser, and then HyperSync Panel sync rules can, depending on various attribute values, can provision it into AD and Azure.

17. Make **Workday: People** the focus silo - either by clicking **Workday: People** or by dragging the whole silo across to the left
18. Select the *oldest timestamp* from the dropdown

Note: This is the moment in time when the "Duncan" object is created in the Workday silo (and he does not yet exist in the others).

19. **Step forward** one timestamp at a time and note the changes that happen:
 - a. A corresponding object is projected in to the Hyperverser
 - b. A corresponding object is provisioned into AD (using the HyperSync Panel Stateful Sync rule called "Provision AD User", which we saw in Lab 2)
 - c. A corresponding object is provisioned into the Service Panel placeholder Silo (this is just there to facilitate Service Panel features)
 - d. A corresponding object is provisioned into Azure (using the HyperSync Panel Stateful Sync rule called "Lab AADC – AD to Azure", which we saw in Lab 2)
20. Finally **step forward** to **Now** (and you see the current state for all silos, including AD having been updated with additional attributes)

Note: The silo you choose to have in focus will depend on what you are looking for. For example, if you are interested in seeing changes to the AD object, you may well decide to have that silo in focus.

Note: Remember a timestamp is only recorded when one (or many) changes to an object have occurred in a particular silo.

Task 3: Dates from All Silos

21. Make **Azure** the focus silo – remember we only have a few timestamps (and the special "Now" timestamp)
22. Select the **Dates from All Silos** checkbox
23. Click the **date/time** dropdown and notice that there are many more timestamps

Note: By selecting this checkbox we are including the timestamps of changes from all the silos (where the corresponding Duncan object exists), meaning that as you step forward in time you see all the changes for Duncan across **all** silos, not just changes to Duncan in the Azure silo – BUT the timestamps displayed are constrained by the silo in focus - dates prior to the object's existence or after the object's deletion in the "focus" silo are omitted - more on this later.

24. Select the *oldest timestamp* – when the object was created in Azure
25. **Step forward** through the timestamps and see how changes flow through all the silos
26. Make **Workday: People** the focus silo and notice that there are even more timestamps now

27. Scroll up the list of timestamps, and select the **oldest timestamp** – this is the point when Service Panel created the object in Workday
28. If you like, **step through time** and see how the object (and its attributes) has been projected and provisioned into the various Silos

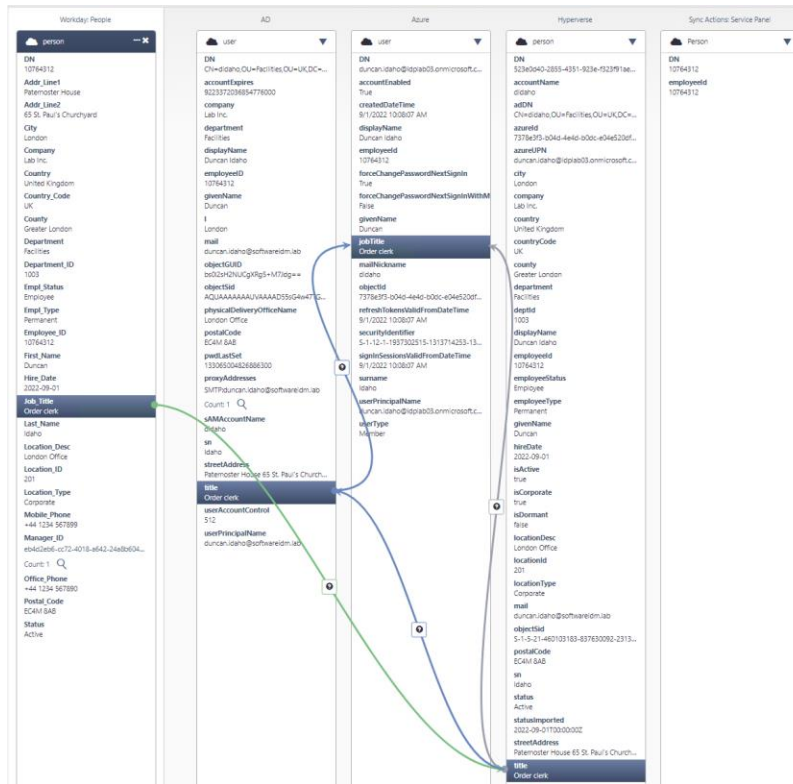
Note: This level of forensic examination is extreme, and is done so that you can understand exactly what is captured - very often you can quickly grasp what has happened to an object with minimal date/time travel.

Task 4: Using Contrails

Note: It is helpful not only to see the corresponding values of attributes in different silos, but to visualize the attribute mappings that populate the attributes. For this we have “Contrails”. You can turn on contrails, and then click an attribute to see the Attribute Flow Rule mappings associated with it. This only works for the focus silo (the one on the left).

29. In Identity Panel still in the Time Traveler for Duncan, with Workday as the focus silo, at the top of the **Workday** silo, click the “Show Contrails” icon (🔗), then click **Department**:

30. Click the question marks in turn (green for import to Hyperserve, blue for others), to see which Attribute Flow Rules define these mappings (you saw these in a previous lab)
31. Select **Job Title** (in the Workday silo):



Note: This time you see a lower precedence flow (gray).

You can look at other contrails, but they can become very complex where expressions are involved. For example, an expression may reference an attribute (e.g. “If this attribute exists, then flow that attribute ...”), even though it is never actually used to generate data. This can lead to a lot of Contrails!

Task 5: Accessing the Time Traveler from History

Note: Often you will find yourself troubleshooting runs and finding an object of interest - Time Traveler lets you examine all the changes that have happened to this object.

32. In Identity Panel go to the **History** tab

Note: Currently we are seeing the most recent runs, and there may not be anything interesting happening - you may just see a smart column of green ticks. There is a filter that allows us to pick out runs with statistics or errors.

33. Filter for an Azure Graph Scan that has some statistics:
 - a. Click the **filter** button (**magnifying glass** icon above the column of green ticks)
 - b. In the **Filter Result** dialog select the **Statistics** dropdown, select **Any** and click **Ok**
 - c. Click the **magnifying glass** icon in the **History Type** column
 - d. In the **Filter History Type** dialog, from the dropdown, select **Azure Graph Scan** and click **Ok**

34. In the details pane you should be able to see an update for Peregrin Took- click the hyperlink for **user** (Peregrin.Took@idplabXX.onmicrosoft.com) and you are again taken to the Time Traveler at that point in time

Exercise 2: Reference Attributes

The main tasks for this exercise are as follows:

- Examine the group Members attribute
- Examine the user Members Of attribute
- Examine the user Manager and Manager Of attributes
- Learn how to perform attribute advanced searches

Task 1: Examining Group Members (multi-value reference attribute)

35. Click the **dropdown** next to Search Time Traveler
36. In the Advanced Search:
 - a. Select **Azure** as the Search Silo
 - b. Select **group** as the Object Type
 - c. Enter **Facilities** as the Search Term
 - d. Click **Search**
37. Follow the **group** hyperlink that has been returned
38. Go to the **Now** state and click the **Count:** hyperlink under the **members** list
39. In the **Advanced Search** dialog, click **Search** – a new browser tab opens
40. Click **Select Display Fields** and see that you can choose which fields to include – select **department** and click **Ok**
41. Change the number per page to **20** so that you can see all the members

Note: You can see that while most of the members are from the facilities department, there is one who is not – and also one who has been deleted. Hopefully you can see that this is entirely consistent with the exercise you did earlier in Access Panel.

Task 2: Examining User Member Of (reverse reference attribute)

42. Find the hyperlink for **Duncan Idaho**, and click it – you now see him in the Time Traveler
43. Make sure that the **Azure** silo is the focus and examine the **members Of** attribute

Note: This is not a real attribute – it has been generated by Identity Panel so that you can readily see a user's group membership.

As a matter of interest, there is no Timestamp for the Azure user object associated with the member Of – it will have been generated when the group gained the user as a member. If you want to see when it happened, you can do so through the Count hyperlink.

44. Click the **Count:** hyperlink under **members Of** and click **Search** – a new tab opens showing you the history (if the timestamp matches a timestamp for the user, that is a coincidence)

Task 3: Examining User Manager (single value ref attribute) and Manager Of

45. Close an excess tabs and dialogs so that you have **Duncan** in **Time Traveler**
46. In the **AD** silo you can see that his manager is Frodo Baggins – click the link to **Frodo**

Note: You can see that Frodo is the manager of several people (including Duncan, of course). Manager Of is not a real attribute, it is generated by Identity Panel for your benefit.

47. In the **AD** silo click the **Count:** hyperlink under **manager Of** and click **Search** and a new tab opens showing you the history – if you look at the Added column you can see that Duncan was added as a report later than all the others (when you created him)

Task 4: Attribute Advanced Search

48. Navigate to the **Facilities** group in **Time Traveler** (there are several ways you can do this)
49. Follow the **Count:** link under the **members** attribute
50. In the **Value added after** dropdown, select *today's date* and click **Search**

Note: You can use the added/removed before/after fields to narrow down a search for forensic purposes. You can also hide removed reference values (which simply removes clutter).

Beware of creating irrational searches! If you specify removed before today and added after today, the conditions are ANDed and you won't see any results.

Also note that Search Terms are whole words (Duncan, not Dunc) – though you can use wildcards (like "dunc*" for Duncan, or "cl?rk" for clerk or clark).

Exercise 3: Other Time Traveler Features

Scenario

The main tasks for this exercise are as follows:

- Securely sharing Time Traveler information via the URL
- Examine Shutter Views

Task 1: Securely sharing Time Traveler information via the URL

51. Use the **Advanced Search** to find all **AD users** whose **title** contains the word **vice**
52. **Copy the URL**, open another browser tab and **paste the URL** - you are taken to the same search results
53. Follow the hyperlink for **Frodo Baggins** and go back a couple of steps in time

54. **Copy the URL** and in your other browser tab **paste in the URL** - note that the URL includes the timestamp and takes you to the same timestamp

Note: When you share a URL, people can only access the URL if they have the relevant permissions. Security is covered in a later module.

Task 2: Using a shutter view

55. Notice what attributes are displayed in the AD silo, particularly:
- userAccountControl is 512
 - objectSID is represented as AQUAAAA...etc.
 - pwdLastSet is a number (a FileTime format)
56. Select **AD** from the shutter view dropdown (just to the right of Dates from All Silos checkbox)
57. The attributes are now displayed in a more readable form

Note: A shutter view can modify what you see (hopefully to make it easier to understand), but also it can restrict what you see. Shutter views can also be used to rename silos and attributes. An administrator can configure multiple shutter views and assign them to users – so what you see depends on who you are.

58. In **Service Panel** (connect.servicepanel.app) search for **Duncan** and select him
59. Scroll down and click **Emergency Disable**
60. Enter a **Justification**, select the **Confirm Account Disable?** checkbox and click **DISABLE**
61. Navigate to **Duncan** in the **Time Traveler** and select the **AD** shutter view
62. In the AD silo, userAccountControl should reflect that his account has been disabled
63. Check in AD and Azure AD that his account has been disabled/blocked

Using the Identity Panel Suite

Course Number: A801

***Module 4: Dashboards, Scheduler, Operations
History and Reports***

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Module Overview.....	1
Lesson 1: Dashboards.....	2
What are Dashboards?	3
Introducing dashboards.....	3
Dashboard modules	3
Dashboard Modules.....	4
History Charts Display	4
History Display.....	5
Monitor Health Check Results	5
View and Run Schedules	6
Other Modules	6
Lesson 2: Schedules.....	10
The Scheduler	11
What is the Scheduler?.....	11
Schedule Queue	13
Lesson 3: Operations History	15
History Records and Simple Filtering.....	16
Filtering by Results and Statistics	18
Filter Results dialog (History Result)	18
Examining the Result Panel	20
The Results Panel.....	20
Overview.....	20
Statistics.....	22
Lesson 4: Reporting.....	25
Reports	26
What are Reports?	26
Report Output.....	26
Which Reports can you Run?	27
Running Reports.....	28
Access to reports	28
Report Caching.....	28
Providing Parameters	29
Point-in-time	30

Drilling Down..... 31

Lab 4: Dashboards, Operations history and reporting..... 32

Module Overview

Module Overview



- Dashboards
- Scheduler
- Operations History
- Reports
- Lab 4

Lesson 1: Dashboards

Lesson 1: Dashboards



- What are dashboards?
- Dashboard modules

www.oxfordcomputertraining.com

www.softwareidm.com

In this lesson, we will examine dashboards.

What are Dashboards?

What are Dashboards?



- A dashboard typically shows summary data in various modules (like charts and tables)
- Identity Panel allows you to create multiple dashboards and assign them to roles
 - If a user has multiple roles their dashboard is a concatenation of all modules from their dashboards
- Modules have customizable settings based on module type
 - Most modules can be half or full page width
- Same module types can be repeated multiple times with different configurations
 - e.g. History charting used once to show recent sync errors, and again to show password reset history

Introducing dashboards

When you open Identity Panel, you are first presented with a dashboard, which typically shows summary data, displayed in the form of charts, tables and other modules – but what you actually see depends on your role and how Identity Panel has been configured.

Identity Panel allows an administrator to create multiple dashboards and assign them to roles – so what you see depends on your role or roles. If a user is a member of multiple roles, their resulting dashboard will be a concatenation of all modules from all their dashboards.

Dashboard modules

Dashboard modules have customizable settings based on the module type. Most module types can also be customized to display in half the page width or full-width.

Often a dashboard will use a module type multiple times with different configurations. For example, one History Chart module might be used once to show recent sync errors, and another might show password reset history.

Dashboard Modules

Dashboard Modules



- History Charts Display
 - Highly customizable charting module which aggregates history counters like sync operations, workflow and health check operations, password resets, etc.
 - Each datapoint on a chart is hover-able (name, count and dates) and clickable (pre-filtered history of aggregated history records)
 - Charts do not auto-refresh (you must refresh the page)
- History Display
 - Filtered sub-set of history (ten most recent entries)
 - Auto-refreshes every 30 seconds
- Monitor Health Check Results
 - Most recent health check results
 - Auto-refreshes once per minute
- View and Run Schedules
 - status of pending and executing schedule steps, plus ad-hoc execution
- Other: Report Dashboard Module, View Output from Panel Service, Excel Provider Dashboard, Run Test Panel, Status Check-in



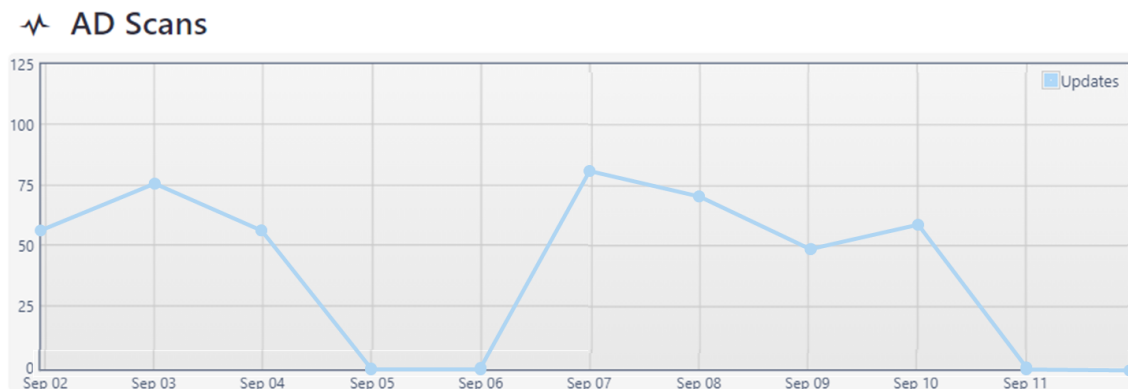
www.oxfordcomputertraining.com

www.softwareidm.com

The following dashboard modules are available:

History Charts Display

This module is a highly customizable charting module which aggregates history counters. Examples of chartable events include scans, sync operations (like adds, updates, deletes, and errors), attribute changes, workflow operations and health check operations.



Each data-point on a chart is hover-able and clickable. Hovering over a point displays the name of the data series, the exact count, and the time span the count aggregates. Clicking a data-point will











open the History panel in a new tab, pre-filtered to the exact run history records that were aggregated to produce the chart data-point.

The chart module does not auto-refresh its results. To update the chart, you must refresh the browser page.

History Display

This shows a filtered sub-set of history results – it supports essentially the same filtering settings as the history interface (covered later).

Run History

	History Type	Argument		
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓
AD	Delta AD Scan	AD		✓

The history module always displays the most recent ten entries matching the provided filters. The history module auto-refreshes itself every 30 seconds.

Monitor Health Check Results

The health check module displays the most recent health check results. It auto-refreshes itself once per minute.

A health check module is comprised of a number of health probes such as SQL Disk Space, (see below). Health probes either return a value, or a green tick (which generally means “healthy”), or a red cross (which generally means something is wrong).

Panel Performance

Memory Available	✓	Memory Paging	✓
Network Queue	✓	Processor	✓
Disk Queue	✓	Disk Avg Read	✓
Disk Avg Write	✓	Disk Idle	✓
Disk Free Counter	✓	Panel Check	✓

DC1 — Wed Oct 13 2021, 18:25:08

SQL Health MIM Lab

SQL DB Size (FIMSync)	128.2 MB	SQL DB Size (FIMService)	275.8 MB
SQL Log Size (FIMSync)	14.9 MB	SQL Log Size (FIMService)	1.5 GB
SQL Disk Space (FIMSync)	✓	SQL Disk Space (FIMService)	✓
FIMSync DB available	✓	FIMServer DB available	✓
FIMSync DB backed up recently	!	FIMServer DB backed up recently	!

sidm99 — Wed Sep 06 2017, 6:42:49 PM

View and Run Schedules

This displays status of pending and executing schedule steps and allows steps to be executed ad-hoc:

View and Run Schedules

Regular cycle Run

Steps

Step	Status	Service
AD Delta Import on MIM Lab	Paused	×
AD Delta Sync on MIM Lab	Paused	×
LDS Export on MIM Lab	Paused	×

We will go into some detail on this in the next topic.

Other Modules

There are some other, more specialized modules.

View Output from Panel Service

This is not likely to make sense for a non-administrator, but for completeness, this can show the more recent activity from some of Identity Panel Services, either from one of the servers running the on-premises Identity Panel services, or from the web agent. It refreshes itself approximately every 10 seconds:

Panel Service

Trace Information Warning Error

Server: sidm99

7:06:09 AM	Scanning Health
7:05:09 AM	Health Scan Complete
7:05:09 AM	Running Health Check SQL Health MIM Lab
7:05:09 AM	Scanning Health
7:04:09 AM	Health Scan Complete
7:04:09 AM	Scanning Health

Web

Trace Information Warning Error

Server: Web v5.6.3.2135 active at Mon Oct 18 2021, 16:54:25

16:50:09	Finished c85ab69e-3be1-4b12-8ae9-ba312b18df8b
16:50:09	Indexing search records for c85ab69e-3be1-4b12-8ae9-ba312b18df8b
16:45:09	Finished c85ab69e-3be1-4b12-8ae9-ba312b18df8b
16:45:09	Indexing search records for c85ab69e-3be1-4b12-8ae9-ba312b18df8b
16:40:09	Finished c85ab69e-3be1-4b12-8ae9-ba312b18df8b
16:40:09	Indexing search records for c85ab69e-3be1-4b12-8ae9-ba312b18df8b

Report Dashboard Module

A module to view and refresh a report. You can run a report easily enough from the Reports tab, but this can be configured to display a particular report, right on the dashboard.

Locations

Select Display Fields

Previous 4 Rows Page 1 of 1 10 per page Next

Location_ID	Location_Desc	Addr_Line1	Addr_Line2	City	County	Country	Country_Code	Postal_Code	State	State_Code	Location_Type
100		100 S Michigan Ave		Chicago	Cook	United States of America	US	60606	Illinois	IL	Corporate
101		550 Colorado Ave		Denver	Denver	United States of America	US	80101	Colorado	CO	Frontline
102		213 W Wesley St Ste 200		Wheaton	Du Page	United States of America	US	60187	Illinois	IL	Frontline
201		Paternoster House	65 St. Paul's Churchyard	London	Greater London	United Kingdom	UK	EC4M 8AB			Corporate

Run Test Panel

We actually have one of these on the lab Environment dashboard – even though Test Panel is not something we cover explicitly in this course!



It allows us to run and monitor Test Cases in much the same way as we can run and monitor Schedules. In the lab environment we use this to load users for test purposes (and clean them up afterwards). In general, we could create suites of tests for our identity management systems, and run the tests from the dashboard.

Excel Provider Dashboard

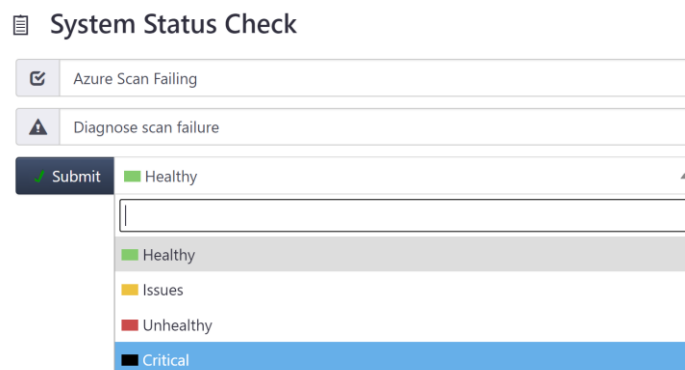
Identity Panel can process bulk updates based on spreadsheet input. So, for example, we might want to bulk disable a bunch of accounts, the names of which are held in a spreadsheet.

You can create a provider for the spreadsheet, you can build a test case (a fixture) to perform the necessary actions on that spreadsheet (this can then appear as one of the tests in the Run Test Panel module, above), and you can then add an Excel Provider Dashboard module to allow the upload or download of the spreadsheet.

Someone on a service desk can then have a dashboard that allows them to upload the spreadsheet and perform the action. They can also download the spreadsheet (to check the entries, or to use it as a template for a new one).

Status Check-in

This module allows manual registration of status about systems. You can use this in various ways, but typically you provide a note, and (if relevant) an action that should be taken, along with a categorization):



The results can be viewed by reporting on Note Record objects:

Check-in Report

Days

Number of days to show data for

Report generated Sun Sep 12 2021, 19:01:48

3 rows

Select Display Fields

Previous

3 Rows Page 1 of 1 10 per page

Next

Health	User	Message	Issue	Time Stamp
Critical	labadmin@student100aadconnect.onmicrosoft.com	Azure Scan Failing	Diagnose scan failure	2021-09-12 18:01
Issues	labadmin@student100aadconnect.onmicrosoft.com	Heath check failing for scan	Diagnose scan issues	2021-09-12 17:42
Healthy	labadmin@student100aadconnect.onmicrosoft.com	Status checked everything looks fine		2021-09-12 17:41

Lesson 2: Schedules

Lesson 2: Schedules



- The Scheduler
- Schedule queue

www.oxfordcomputertraining.com

www.softwareidm.com

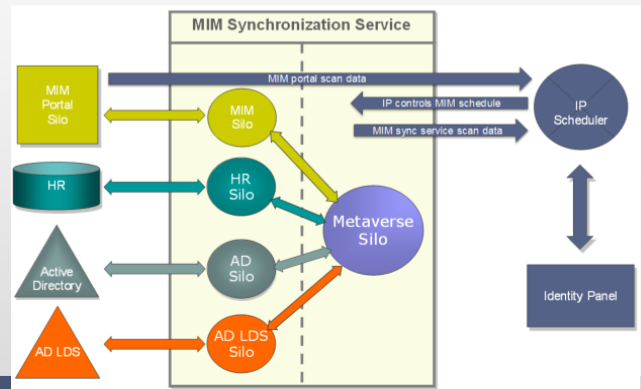
In this lesson, we will examine the scheduler and schedule queues.

The Scheduler

The Scheduler



- The Identity Panel scheduler can run a regular sequence of operational steps, such as scans of various systems (along with any necessary tests and checks) and reports
- An administrator will set up one or more schedules consisting of such a sequence of steps
 - Which steps are available depends on which modules are installed and enabled
 - For the most part, they will run automatically as configured
- Sometimes it is desirable to kick off a schedule manually, and your dashboard can include a module for running schedules, as well as for monitoring and clearing schedules
- Identity Panel can also schedule MIM, gathering historical data as it does – a typical schedule will include a lot of such MIM steps, and can also scan the MIM Portal



www.oxfordcomputertraining.com

www.softwareidm.com

What is the Scheduler?

The purpose of the Identity Panel scheduler is to run a regular sequence of operational steps, such as scans of various systems (along with any necessary tests and checks) and reports.

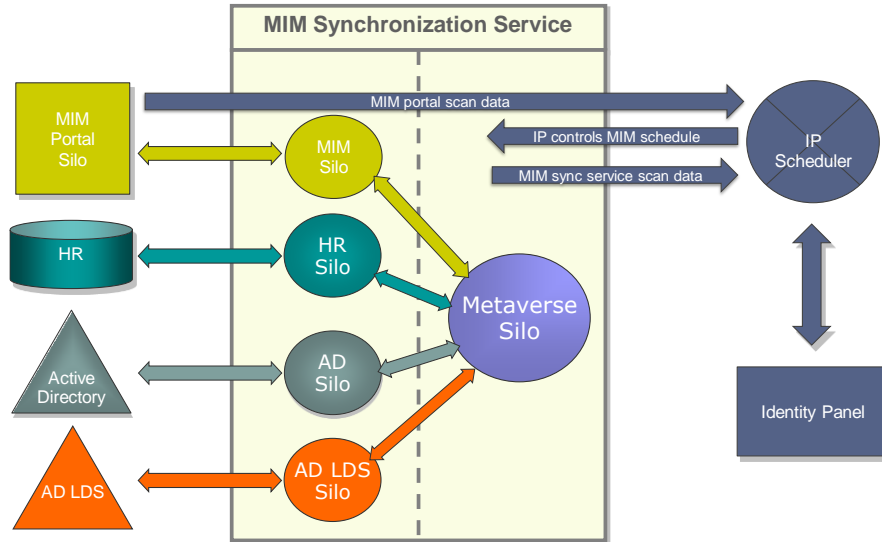
Automatic or Manual?

An administrator will set up one or more schedules consisting of such a sequence of steps, and for the most part, they will run automatically as configured. The steps that are available to build a schedule depends on which Identity Panel Suite modules are installed and enabled.

Sometimes it is desirable to kick off a schedule manually, and for this purpose your dashboard can include a module for running schedules on demand, as well as for monitoring and clearing schedules.

MIM and HyperSync

We have discussed the various sync engines available. It should be unsurprising to learn that running a HyperSync schedule is part of the job of the scheduler. More surprising is that the MIM sync engine does not have its own scheduler – and that Identity Panel is an excellent choice for performing this task. Not only can it run the MIM sync schedule, but it can scan at a detailed level as it does so, thus gathering complete historical MIM data.



Each system will need some or all of import, synchronization and export steps, and so a typical schedule will include a lot of such MIM steps, plus scans of other systems (like AD, ADFS, and the MIM Portal).

Schedule Queue

Schedule Queue



- The schedule queue is available on the dashboard (while steps are pending, running, or paused)
- When you run a schedule manually from the dashboard, the queue will appear
- You can expand it to see the progress through the steps, though you may have to be quite quick, as there is not much going on in our lab set-up, and the whole cycle may only take a few seconds (except if it is paused, of course)
- You can pause the queue manually – or it could be paused by a Condition Rule configured in the schedule; once paused (whether manually or as a result of a Condition Rule), and to some extent even when not paused, you can review the queue, and manage the queue as follows:
 - Terminate the entire queue
 - Terminate individual steps
 - Execute the next step
 - Execute the remaining steps (select the "To End" checkbox)

www.oxfordcomputertraining.com

www.softwareidm.com

The schedule queue appears on the dashboard (if configured), but only while there are steps pending, running or paused.

When you run a schedule manually from the dashboard, the queue will appear. You can expand it to see the progress through the steps, though you may have to be quite quick in our lab environment, as there is not much going on in our lab set-up, and the whole cycle may only take a few seconds (except if it is paused, of course).

You can pause the queue manually – or it could be paused by a Condition Rule configured in the schedule. Once paused (whether manually or not), and to some extent even when not paused, you can review the queue:

View and Run Schedules

Regular cycle Run

Steps

Regular cycle ▶ To End ✖

Step	Status	Service
AD Delta Import on MIM Lab	Paused	✖
AD Delta Sync on MIM Lab	Paused	✖
LDS Export on MIM Lab	Paused	✖
LDS Delta Import on MIM Lab	Paused	✖
LDS Delta Sync on MIM Lab	Paused	✖
MIM Lab Portal Scan	Paused	✖

You can manage the queue as follows:

- Kill the entire queue
- Kill individual steps
- Execute the next step
- Execute the remaining steps (select the "To End" checkbox)

Lesson 3: Operations History

Lesson 3: Operations History



- History records and simple filtering
- Filtering by results and statistics
- Examining the result panel

www.oxfordcomputertraining.com

www.softwareidm.com

In this lesson, we will examine the Operations History and how to filter it.

History Records and Simple Filtering

History Records and Simple Filtering



- On the History tab you get a list of records recorded by Identity Panel (it auto-refreshes every 30 seconds)
- Many of these will reflect the schedules that have run automatically - and there will typically be a repeating pattern - but it records manual actions too
- What is actually recorded will vary depending on the schedule step that gave rise to it
- The history may run to a huge number of records, so you can simply filter by Provider (like AD, Workday, History Type (LDAP Scan, Azure Graph Scan), Argument (like Delta Sync, Full Sync), From and To Date Range, or Result (see next topic)
- You simply click a magnifying glass and select a value, or enter a date; click it again to clear it (filters are ANDed)
- Not all the steps that you include in your schedules will result in an explicit record in the history (for example sending an email) - but the success or otherwise of that step will be recorded in a Schedule Run step (the same is true for skipped steps)
- You can very quickly see all the records relating to a schedule run by clicking the Filter Steps hyperlink in the Schedule Run overview

www.oxfordcomputertraining.com

www.softwareidm.com

On the History tab you get a list of records logged by Identity Panel (it auto-refreshes every 30 seconds). Generally speaking, most of these will reflect the schedules that have run automatically - and there will typically be a repeating pattern - but it records manual actions too. What is actually recorded will vary depending on the schedule step that gave rise to it.

The history may run to a huge number of records, and so filtering is a very important tool for finding data of interest. At its simplest, you can filter by:

- **Provider:** like AD, Workday, Azure AD, Tools, Tests, Workflow etc.
- **History Type:** like LDAP Scan, Azure Graph Scan, Schedule Run, Process Workflows, Test Suite etc.
- **Argument:** like Delta Sync, Full Sync, Provider Settings Changed etc.
- **Date Range:** From and To dates of run
- **Result:** (See next topic)

You simply click a magnifying glass and select a value, or enter a date. Click it again to clear it. You can have several filters – they are additive (they are ANDed together).

Not all the steps that you include in your schedules will result in an explicit record in the history (for example sending an email) - but the success or otherwise of that step will be recorded in a Schedule Run step. The same is true for skipped steps.

In the following screen-grab you can see the details for a particular, regular schedule run. On the left you see an entry for the run as a whole – this is highlighted, and so on the right (in the Results Panel) you are seeing the detail that goes with that.

In this case we can see that many steps were skipped, and actually only 5 steps were completed. On the left we see these 5 completed steps as additional entries (above the initial entry). We could select one of these steps (on the left, or in the Results Panel on the right, as it happens) if we wanted to see the detail for that step alone.

The screenshot displays the Identity Panel Suite interface. On the left, a table lists history entries. The entry for 'Tools - Schedule Run - Regular cycle' is highlighted. On the right, the 'Details' panel for this entry is shown, including an overview of the run and a table of individual steps.

History Type	Argument	Time	Result
MIM Lab	MIM Portal	Delta Sync	☀️
MIM Lab	MIM Portal	Delta Import	☀️
MIM Lab	MIM Portal	Export	☀️
MIM Lab	HR	Full Import	☀️
MIM Lab	HR	Export	☀️
Tools	Schedule Run	Regular cycle	🌙

Step	Result	Run By
HR Export on MIM Lab	☑️	sidm99
HR Full Import on MIM Lab	☑️	sidm99
HR Delta Sync on MIM Lab	🚫	
MIM Portal Export on MIM Lab	☑️	sidm99
MIM Portal Delta Import on MIM Lab	☑️	sidm99
MIM Portal Delta Sync on MIM Lab	☑️	sidm99
AD Export on MIM Lab	🚫	sidm99
AD Delta Import on MIM Lab	🚫	
AD Delta Sync on MIM Lab	🚫	
LDS Export on MIM Lab	🚫	
LDS Delta Import on MIM Lab	🚫	
LDS Delta Sync on MIM Lab	🚫	
MIM Lab Portal Scan	🚫	

History Type	Argument	Time	Result
MIM Portal	Delta Sync	☀️	☑️
MIM Portal	Delta Import	☀️	☑️
HR	Full Import	☀️	☑️
MIM Portal	Export	☀️	☑️
HR	Export	☀️	☑️

Note: History entry time (depicted with a sun or moon graphic), is in local time (based on your PC time zone).

Filtering by Results and Statistics

Filtering by Results and Statistics



- The rightmost column of the history shows a green tick or a red exclamation mark - clicking the magnifying glass brings up a dialog with two dropdowns, which both allow multiple selections
- History Result
 - This allows you to filter according to the result of the history record: success (case-sensitive), Steps Failed, Steps incomplete – and error messages
 - The drop-down is populated with error messages depending on what has been recorded in history (completed-export-errors, stopped-extension-dll-file-not-found etc. – MIM messages)
- Statistics
 - It allows you to filter for the presence (1 or more) of the numeric counters from a History Record (ORed together)
 - You may see counters like Add, Update, Rename, Import failure etc.
 - Schedule counters include: Queued Step, Started Step, Completed Step, Failed Step, Cancelled Step, Skipped Step (you can quickly find these by typing in a few letters, like "ste")
- Hints:
 - A useful option (at least in the classroom) is "Any", which quickly excludes all "empty" runs
 - If you want to find all cases of Skipped Step or Cancelled step - do not filter by History Type because that is likely to exclude what you are looking for
 - Don't mix filters on history result AND statistics at the same time – you may not get the results you expect!

Filter Results dialog (History Result)

The rightmost column of the history shows a green tick or a red exclamation mark. Clicking the associated magnifying glass brings up a dialog with two dropdowns. Both allow multiple selections:

Tools	History Type	Argument		
Tools	Schedule Run	Full Scans		✓
Workf...	Process Workflows	Health Check Failed		✓
Tools	Process Workflows	Lab AADC - Flow Attributes		✓
Tools	HyperSync Panel	Full		✓
Tools	WebAgent.exe	--sync --full c85ab69e-3be1-4b12-8a...		✓
Tools	Schedule Run	Full Sync		✓
Tools	HyperSync Panel	Full		✓
Tools	WebAgent.exe	--sync --full c85ab69e-3be1-4b12-8a...		✓
Tools	Schedule Run	Full Sync		✓
Tools	Schedule Run	Full Scans		✓
Tools	WebAgent.exe	--sync --full c85ab69e-3be1-4b12-8a...		!
Tools	Schedule Run	Full Sync		✓

History Result

This allows you to filter according to the result of the history record – options here will include Error and Success (case-sensitive). You can leave this blank to include all.

The dropdown is populated with error messages depending on what has been recorded in history. For example, if MIM is involved you might see completed-export-errors, stopped-extension-dll-file-not-found - messages that would be familiar to MIM admins.

Statistics

This dropdown is also populated with error messages depending on what has been recorded in history, for example:

- Add
- Update
- Rename
- Import failure
- Filtered Connector
- ... and so on

Schedule counters include:

- Queued Step
- Started Step
- Completed Step
- Failed Step
- Cancelled Step
- Skipped Step

You can quickly find these by typing in a few letters (like "ste").

Note: A useful option (at least in the classroom) is "Any". This quickly excludes all the runs where nothing happened.

Note: If you want to find all cases of Skipped Step or Cancelled step - do not filter by History Type because that is likely to exclude what you are looking for.

Note: It is not a good idea to filter by History type AND Statistics. It won't break anything, but you might not get the results you expect, and it tends to be meaningless anyway!

Examining the Result Panel

Examining the Results Panel



- There are two sections to the results panel – overview and statistics
- What you see depends on the record's History Type
- At its simplest the overview section has dates, the result, and a hyperlink
- Others will have statistics too, and a schedule run has much more going on in its Overview - a summary of steps and the result of each one
 - You can hover over the symbol for a step for more details (skipped, failed, cancelled etc.)
 - Only those that actually ran have hyperlinks - because only those have a record to go to
- The statistics you see depends on the History Type:
 - An Azure graph scan can include users, groups and devices that have been added or updated
 - MIM Portal Scan will have Creates and Updates (for example) of portal objects, including users and groups - but also including sets, MPRs, requests and approvals
 - For a Schedule Run the detail will include the number of steps queued, how many of them completed, failed, cancelled etc.
- Statistic display options - checkboxes can be used to hide and show statistics, you can select "Display Fields" and preview details, and drill down to the object in the Time Traveler (at that timestamp)
- For an MIM Management Agent run like an AD export, or a HR Full Import, or a MIM Sync, you get all the statistics you might see in the MIM Synchronization Service Manager

www.oxfordcomputertraining.com

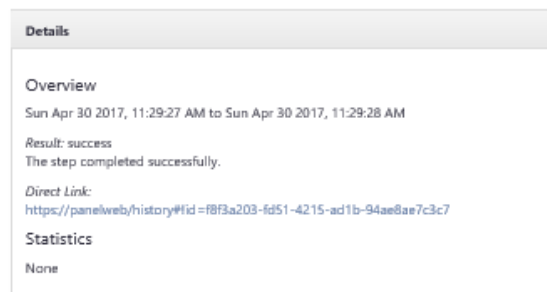
www.softwareidm.com

The Results Panel

What you see in the Results Panel depends on the record's History Type. All have an Overview - and some of them have statistics (if there are no statistics there is a label saying "None").

Overview

The simplest overview section simply has a start and end date, the result (hopefully "success"), and a hyperlink (which could in any case be copied from the browser's address bar):



An Azure Graph Scan - to take another example - has a similar Overview section, but will typically have statistics too.

Details

Overview
 Wed Sep 08 2021, 23:13:33 to Wed Sep 08 2021, 23:13:44
Result: success
 The step completed successfully.
Direct Link:
<https://connect.identitypanel.com/history#id=0d7109d2-3608-403d-a312-6eb147471b81>

Statistics
 4 Updates

Updates Select Display Fields

4 Rows
Page

of 1
per page

ObjectType	DN
Azure	
user	ammon.hadaseh@student100aadconnect.onmicrosoft.com
user	bryant.tawfiq@student100aadconnect.onmicrosoft.com
user	prosper.dace@student100aadconnect.onmicrosoft.com
user	churhill.landon@student100aadconnect.onmicrosoft.com

A schedule run has more going on in its Overview - a summary of steps and the result of each one. Here is an example:

Details

Overview
 Sat Apr 29 2017, 2:43:48 PM to Sat Apr 29 2017, 2:45:15 PM
Result: Steps Incomplete
Direct Link:
<https://panelweb/history#id=a5e1b623-daae-4430-8761-103845c56922>
Schedule: Regular cycle
History:
 Filter: Steps
 Steps:

Step	Result	Run By
HR Export on MIM Lab	✓	sidm99
HR Full Import on MIM Lab	✓	sidm99
HR Delta Sync on MIM Lab	⚡	
MIM Portal Export on MIM Lab	✓	sidm99
MIM Portal Delta Import on MIM Lab	✓	sidm99
MIM Portal Delta Sync on MIM Lab	✓	sidm99
AD Export on MIM Lab	!	sidm99
AD Delta Import on MIM Lab	⚡	
AD Delta Sync on MIM Lab	⚡	
LDS Export on MIM Lab	⚡	
LDS Delta Import on MIM Lab	⚡	
LDS Delta Sync on MIM Lab	⚡	
MIM Lab Portal Scan	⚡	

The result for each step can be success (green tick) an error (red exclamation mark), or the other symbol you see here, which indicates another status (e.g. Skipped, Cancelled, Pending). To see what is going on you can hover over each symbol, in which case you would learn (in this case) that:

- The HR Delta Sync was skipped (according to skip rule on the previous step HR Full Import, which says if nothing was imported from HR, there is no need to synchronize it)
- The AD Export failed (actually because of a badly configured rule)
- The remaining steps were cancelled (manually after the schedule was paused)

Only those that actually ran have hyperlinks - because only those have a History Record to view.

Statistics

The statistics you see depend - of course - on the History Type. Here are a few representative examples.

Azure Graph Scan

This is a scan of Azure AD (technically it uses the Microsoft Graph API). Typically, we are going to find users, groups and/or devices that are new (Adds), or have changes (Updates), or maybe Deletes. In the following you can see 2 new groups and lots of updates to users:

Details

Overview
 Wed Sep 15 2021, 15:07:14 to Wed Sep 15 2021, 15:07:21
 Result: success
 The step completed successfully.
 Direct Link:
<https://connect.identitypanel.com/history#iid=620ceba2-70df-460f-a558-40cdd0b0477e>

Statistics

2 Adds 23 Updates

Adds

Previous 2 Rows Page 1 of 1 10 per page

ObjectType	DN
Azure	
group	Test group 2
group	Test Group 1

Updates

Previous 23 Rows Page 1 of 3 10 per page

ObjectType	DN
Azure	
user	smitty.fae@student100aadconnect.onmicrosoft.com
user	achantae.nick@student100aadconnect.onmicrosoft.com
user	kristin.jewellen@student100aadconnect.onmicrosoft.com
user	schura.skelly@student100aadconnect.onmicrosoft.com

Object Details (Right Panel):

```

ObjectType: user
DN: smitty.fae@student100aadconnect.onmicrosoft.com
DN: smitty.fae@student100aadconnect.onmicrosoft.com
accountEnabled: True
createdDateTime: 9/8/2021 10:07:15 PM
department: Management
displayName: Smitty Fae
employeeId: 10000089
forceChangePasswordNextSignIn: True
forceChangePasswordNextSignInWithMfa: False
givenName:
jobTitle:
mailNickname: sfae
objectId: 87878d22-8c9f-4c9f-b565-91e9fe5213a6
refreshTokensValidFromDateTime: 9/8/2021 10:07:15 PM
signInSessionsValidFromDateTime: 9/8/2021 10:07:15 PM
surname:
userPrincipalName: smitty.fae@student100aadconnect.onmicrosoft.com
userType: Member
    
```

You can de-select statistics checkboxes to hide detail.

Display Options

Some of the little checkboxes (under Statistics) can be used to hide and show the various lists of statistics, so that you can focus on what interests you (this may not be very valuable in this case, but generally you may have many more of these). Some of the little checkboxes have no effect.

You can **Select Display Fields** – this is can very useful for certain types of object that have many fields.

Drilling Down

In some cases, as you can see in this example, you can mouseover a magnifying glass to preview details of an object – but you can also drill down using a hyperlink. This will take you to the object concerned in the Time Traveler (at the Timestamp concerned).

MIM Portal Scan

A more specialized example is the MIM Portal Scan, which will have Creates and Updates (for example) of portal objects, including users and groups - but also includes sets, MPRs, and requests and approvals.

Details

Overview
Thu Apr 27 2017, 11:23:49 AM to Thu Apr 27 2017, 11:23:50 AM
Result: success
The step completed successfully.
Direct Link:
<https://panelweb/history#fid=457e6634-fcfd-4b39-990f-ade31cd47055>

Statistics

6 Adds 24 Updates 18 Portal Request Creates
 2 Portal Approval Needed 2 Portal Approves

Adds Select Display Fields

Previous 6 Rows Page 1 of 1 10 per page Next

Object Type	Display Name	
MIM Lab: Portal		
Person	Roman Miklus	
Person	Peter Connelly	
Person	Robert Lyon	
Person	Susanna Stubberod	
Person	Steven Thorpe	
Person	Fred Viidul	

Updates Select Display Fields

Previous 24 Rows Page 1 of 3 10 per page Next

Object Type	Display Name	
MIM Lab: Portal		
Set	All Requests	
Set	User Administrators	

Schedule Run

For a Schedule Run the detail will include the number of steps queued, how many of them completed, failed, cancelled etc. Actually, only the completed steps are shown in a list, but you have them all in the overview anyway:

Statistics

1 Run Schedule
 13 Queued Steps
 5 Completed Steps
 1 Failed Step
 1 Skipped Step
 6 Cancelled Steps

Completed Steps Select Display Fields

 5 Rows Page of 1 per page

History Type	Argument	Time	Result	
History Details				
HR	Export		✓	
MIM Portal	Export		✓	
MIM Portal	Delta Import		✓	
HR	Full Import		✓	
MIM Portal	Delta Sync		✓	

A MIM Management Agent run

For an MA run like an AD export, or a HR Full Import, or a MIM Sync, you get all the statistics you might see in the MIM Synchronization Service Manager, such as: Export Failures, Export Errors, Export Adds, Export Updates, Import Flows, Provision Adds, Adds, Updates and so on. You can show and hide all these with the checkboxes. Here is an example for HR Delta Synchronization (51 Projections have been hidden):

Statistics

51 Projections
 100 Provision Adds

Provision Adds Select Display Fields

 100 Rows Page of 10 per page

Object Type	DN	
AD		
user	CN=JohnS,OU=LABS,DC=uklab,DC=identitypanel,DC=com	
user	CN=JennyG,OU=LABS,DC=uklab,DC=identitypanel,DC=com	
user	CN=LeonorM,OU=LABS,DC=uklab,DC=identitypanel,DC=com	
user	CN=AndreaD,OU=LABS,DC=uklab,DC=identitypanel,DC=com	
user	CN=PaulK,OU=LABS,DC=uklab,DC=identitypanel,DC=com	
MIM Portal		
Person	39739ed1-efe1-471c-9870-efe8fe78f849	
Person	44e5a0e4-7277-4691-82b4-0d1b2b2070bb	
Person	a8e9f718-6ddd-4c7b-98cf-4093143b50ed	

Note: You can select display fields – this is can very useful for the MIM portal run because the DNs aren’t intuitive.

Lesson 4: Reporting

Lesson 4: Reporting



- Reports
- Running reports
- Providing parameters
- Point-in-time
- Drilling down

In this lesson, we will look at how to access reports, run reports and filter them.

Reports

Reports



- In Identity Panel an administrator can write sophisticated reports based on the data held in Identity Panel (password resets, identity attributes in particular silos, group memberships etc.)
- There are no default reports as such, but SoftwareIDM make sample reports available
- The lab environment has been pre-populated with reports such as:
 - AD – Manager Account Expiration and Flags
 - AD – Password Last Set
 - AD - Users With/Without Manager
 - Azure – Expired Active Users
 - Azure Filter users
- Reports can be downloaded in a number of formats: Excel, HTML, Delimited, XML, JSON
- Security - what you can do depends on your role; an admin can limit access to:
 - The Reports feature
 - To specific reports
 - To the underlying data (down to attribute level)
- Note that reports can be downloaded and then emailed (to anyone), circumventing security

www.oxfordcomputertraining.com

www.softwareidm.com

What are Reports?

In Identity Panel an administrator can write sophisticated reports based on the data held in Identity Panel – for example: password resets, identity attributes in particular silos, group memberships, what 0365 licenses users have and so on.

There are no default reports as such, but SoftwareIDM do make sample reports available on their support site – these can be used as-is, or repurposed. So, while there may be some commonality between the reports available in different implementations, don't expect them to all be the same.

The lab environment has been pre-populated with a number of typical reports, such as:

- AD - Manager Account Expiration and Flags
- AD – Password Last Set
- Users With/Without Manager
- Azure – Expired Active Users
- Azure – Filter Users

Report Output

By default, reports are produced in your browser window. Reports can be downloaded in a number of formats: Excel, HTML, Delimited, XML, JSON. Excel and HTML can be useful if you want to email them to someone else.

Which Reports can you Run?

This depends on your role. An administrator will be able to see all reports, and see all the output from those reports. Other users will typically not see everything:

- They may not even have access to the Reports feature at all, in which case they will not be able to run a report by any means
- They may have access to the Reports feature, but only to a limited set of reports
- May have access to a report but not to some or all of the underlying data (since security can act at the attribute level)

Note: Reports can be downloaded and then emailed (to anyone) – obviously this circumvents the above security measures!

Running Reports

Running Reports



- Reports can be run directly from the reports tab by selecting a report from the dropdown, then clicking the Build button
- You can copy a report URL, and paste it into another browser (subject to the security discussed in the previous topic)
- A URL link could be included in an email sent as part of a schedule – or a schedule can include the actual report, or part of it
- Some reports can take a while to process – for this reason they are cached for a configurable period of time (you can see the time in the Report Log) – refresh the report to be sure of picking up the most recent data
 - Reports can be based on reports (visible in the Report Log)– you may need to refresh the base report
- For some reports you can provide additional parameters (like a date, period of time, or attribute)
 - they can be optional or required

www.oxfordcomputertraining.com

www.softwareidm.com

Access to reports

Reports can be run directly from the reports tab by selecting a report from the dropdown, then clicking the Build button.

You can copy a report URL, and paste it into another browser – or another user can paste it into their browser. The report will be produced again, subject to the security discussed in the previous topic.

Such a URL link could be included in an email sent as part of a schedule – or a schedule can include the actual report (as though downloaded and sent), or part of it.

Report Caching

Some reports can take a while to process, so repeatedly building the same report can be tedious. In order to avoid you being held up when repeatedly producing the same report, Identity Panel caches a report for a period of time (which is configurable). If you need a completely fresh run of the report – for example because you know the data just changed – then click the refresh button (to the right of the Build and Download buttons).

Reports Based on Other Reports

Reports can be based on other reports. If so, then in order to refresh the derivative report, you must actually go and refresh the base report. In the following example the report we care about is

AD Users With/Without Manager – but it relies on the base report Z-System AD Users (the “Z” is just a trick to send it to the bottom of the drop-down).

AD - Users With/Without Manager

Report filtering users by whether or not they have a manager assigned. Uses Z-System AD Users base report. To refresh report, rebuild Z-System AD Users, then rebuild this report.

Mode: With

Whether to run report in with, or without manager mode

Report generated Tue Oct 19 2021 13:24:23

35 rows

Select Display Fields

35 rows Page 1 of 4 10 per page

DN	displayName	manager	manager mail	manager accountExpires	manager userAccountControl	mail	mailNickname	sAMAccountName	targetAddress	userPrincipalName	accountExpires	lastLogonTimestamp
CN=aholdyer,OU=Public Relations,OU=UKDC=softwareidm,DC=lab	Alle Holdyer	CN=ptrook,OU=Public Relations,OU=UKDC=softwareidm,DC=lab	ptrook@softwareidm.lab	0 - Never	NORMAL_ACCOUNT	alle.holdyer@softwareidm.lab		aholdyer		alle.holdyer@softwareidm.lab	2023-06-21 00:00:00	0 - Never
CN=anick,OU=Public Relations,OU=UKDC=softwareidm,DC=lab	Acharnee Nick	CN=ptrook,OU=Public Relations,OU=UKDC=softwareidm,DC=lab	ptrook@softwareidm.lab	0 - Never	NORMAL_ACCOUNT	acharneanick@softwareidm.lab		anick		acharneanick@softwareidm.lab	0 - Never	0 - Never

You would have to refresh the base report to be sure you are seeing the latest data in AD Users With/Without Manager. If you scroll to the end of the report, and expand the report log, you can see that the time of generation of the base report, is earlier than the time of generation of the report on which it depends.

```

▼ Report Log
Building AD - Users With/Without Manager
Generating AD - Users With/Without Manager at 10/19/2021 12:24:22 PM
Calculating Parameters
Analyzing Structure
Report Structure:
GRAPH
AD {
  Fields: DN, displayName, manager, manager mail, manager accountExpires, manager userAccountControl, mail, mailNickname, sAMAccountName, targetAddress
}
Loading 1 Data Sets
Loading dependency report AD
Generating Z-System AD Users at 10/19/2021 12:12:55 PM
Calculating Parameters
Analyzing Structure
Report Structure:
GRAPH
Users {
    
```

Providing Parameters

For some reports, you can provide additional parameters. For example, you might have a report for “AD Recent Changes” which presents two parameters, Days (which defaults to 7, meaning the last 7 days), and which attribute(s) you are interested in.

Sometimes, parameters are optional (like changing the number of days in our example), but they can also be required (like attribute choice in our example). Where an attribute is required, it may not be obvious until you try to build the report without it, in which case the attribute is highlighted in red, with a red exclamation mark.

Point-in-time

Point-In-Time



- All reports can be run for a particular point-in-time – as though it were run on the date you have chosen
- For example, we could run an “AD Recent Changes” report to get the changes to “Job Title” in the last 7 days, or we could choose a date in the past and get another list of users whose “Job Title” changed in the 7 days prior to that time
- An obvious use of this is for system audits and forensic purposes – another is side by side comparisons
- To be clear, where a report produces data depending on “today” – like password changes in the last 7 days – “today” has to be interpreted as the “Point-In Time”

www.oxfordcomputertraining.com

www.softwareidm.com

All reports can be run for a particular Point-in-Time. In other words, you can choose to run the report as though it were run on the date you have chosen. For example, we could run an “AD Recent Changes” report for “now” – giving us changes to some attribute(s) during the last 7 days, or we could choose a date in the past and get another list of changes in the 7 days leading up to the chosen Point in Time. Of course, users may have been added, deleted, and modified in the meantime.

An obvious use of this is for system audits and forensic purposes. Another use is that you could export “before” and “after” reports, and compare them (in Excel or some other application).

To be clear, where a report produces data depending on “today” – like password changes in the last 7 days – “today” has to be interpreted as the “point-in time”. In other words, you can get password changes in the 7 days prior to your chosen point-in-time.

Drilling Down

Drilling Down



- Reports can be written so that they include simple data, or (where appropriate) hyperlinks to other objects in the Time Traveler
- Depending on how the report has been written, this may take you to the “current” state of the object, or the state of the object at the time concerned

www.oxfordcomputertraining.com

www.softwareidm.com

Reports can be written so that they include simple data, or (where appropriate) hyperlinks to other objects. These can be used to jump directly to the objects concerned, in the Time Traveler.

Depending on how the report has been written, this may take you to the “current” state of the object, or the state of the object at the time concerned. This is relevant where you have chosen a Point-in-Time, or where your report includes a historical record (for example you might list schedules with errors and want to drill down to the objects of interest *at the time of the error*).

Lab 4: Dashboards, Operations history and reporting

Lab 4: Dashboards, Operations history and reporting



- Exercise 1: Some additional dashboard features
- Exercise 2: Working with Operations History
- Exercise 3: Running reports

Logon Information - replace XX with your assigned student number e.g. 01

Virtual machine	IDPLabXX.WestEurope.cloudapp.azure.com
Domain username	softwareIDM\Labadmin
Azure username	labadmin@IDPLabXX.onmicrosoft.com
Password	\$IDMTrainingLogin

Estimated time: 30 minutes

Using the Identity Panel Suite

Course Number: A801

Lab 4: Dashboards, Operations history and reporting

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SoftwareIDM.

© 2022 SoftwareIDM. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Lab 4: Dashboards, Operations History, and Reports	1
Exercise 1: Some additional dashboard features.....	1
Exercise 2: Working with Operations History	2
Exercise 3: Running reports	3

Lab 4: Dashboards, Operations History, and Reports

Exercise 1: Some additional dashboard features

Scenario

You have already used some of the dashboard features – here you will use a few more.

Task 1: System Status Check

1. In **Identity Panel**, on the **Dashboard**, in the **System Status Check** module, submit a new entry as follows:
 - a. Status message: **Azure and AD Scans not working**
 - b. Report issue: **Diagnose Scan Failure**
 - c. Select **Unhealthy** and click **Submit**
2. **Submit** another entry of your own
3. Select the **Reports** tab
4. Select the **Identity Panel – Check-in** report and click **Build**
5. Your 2 entries are probably the only ones!

Task 2: Add a chart

6. Select the **Settings** tab and then select **Dashboards** on the left

Note: There is only one dashboard – and you should be able to correlate the 7 defined modules with what you have been looking at on the dashboard.

7. Expand the **Admin** dashboard (▶)
8. From the **Select Type** dropdown, select **History Charts Display** and click **+ New**
9. Click **Name**, enter **AD Updates** and expand it (▶)
10. From the **Provider** dropdown select **AD**
11. Set the **Time Range** as follows:
 - a. Interval **1**
 - b. Unit **Days**
 - c. From **10**
 - d. Unit **Days**
12. Under **Series** click **+ New** and enter **AD updates** as the **label**
13. Choose a **color** and from the **Counters** dropdown select **Update** (start typing “upd...”)
14. Scroll to the very top of the page and click **Save** and enter the commit message **New dashboard module**

15. Select the **Dashboard** tab and verify that you see the new module – what you see depends on what you have been doing!
16. In your **Virtual Machine**, in **Active Directory Users and Computers**, reset the password for a number of users (choose ones we have not been using)

Note: Of course, any change to an attribute that is being scanned will do, but as a rule it is likely that the HR system is authoritative for most attributes of interest. So we are choosing to do a password reset because AD is authoritative for it. We will pick up pwdLastSet when we scan.

17. Back in **Identity Panel** run a **Delta Scan** of **AD**
18. From the **Dashboard**, verify that you can see the most recent changes in the **AD updates** chart – and click *the data point concerned*

Note: You now see the history record(s) concerned. Essentially it has been filtered (see next task).

19. Follow the link for one of the users, and you will be able to see the new Timestamp for **pwdLastSet**, and that it has been modified (blue)
20. Select the **AD** shutter view to see a formatted date

Exercise 2: Working with Operations History

Scenario

You have already used the History feature – here we go into a little more detail

Task 1: Further filtering

21. Switch to the **History** tab, and click the left-most **magnifying glass** icon

Note: This is the Provider dropdown – it is pre-populated with the list of a Providers, and you simply choose one of them if that helps.

This and the next two magnifying glasses allow you to select from choices you see in the columns beneath them.

22. Select **AD** and click **Ok**

Note: You can clear a filter by clicking the Magnifying Glass with a cross icon.

23. Clear all the filters
24. Click the **magnifying glass** icon for **filter date** noting that the icons reflect the time of day or night with the approximate position of the sun or moon
25. For the **From** date choose *yesterday around 2 hours ago* and click **OK** – you should expect to see a smaller number of rows
26. Clear all the filters
27. Click the **magnifying glass** icon for Filter Result (the right most one)

Note: You can make further choices from History Result (basically success or some kind of error, which is populated based on the history), and Statistics (a useful one here is “Any”).

Sometimes, when you click a link elsewhere, you will be brought to an already filtered History (as in the previous task).

28. Close the dialog

Exercise 3: Running reports

Scenario

The main tasks for this exercise are as follows:

- Run a report
- Sharing reports
- Drilling down in reports

Task 1: Running a Report

29. Switch to the **Reports** tab
30. From the **Select Report** dropdown, select **AD - Password Last Set** and click **Build**
31. Sort on **pwdLastSet** (you will need to click this twice to get the most recent at the top)

Note: You may find that the ones you just reset do not show up at the top. If so this will be because the report takes its data from the base report called Z-System AD Users, and that needs to be rebuilt. This will happen anyway eventually (and may indeed have happened) – but if we want to be sure of up to date results, we will have to build that report first.

Usually the description under the report title will indicate which base report is in use (if any). In any case you can see this information, and when any base report was last built, by scrolling to the bottom and expanding the Report Log (in this case

you will see “Generating Z-System AD Users etc.”)

32. From the **Select Report** dropdown, select **Z-System AD Users** and click the **Clear cache and refresh report** button (to the right of the Build and Download buttons)
33. Verify that the report generated timestamp is current
34. From the **Select Report** dropdown, select **AD - Password Last Set** and click **Build**
35. Sort on **pwdLastSet** (you will need to click this twice to get the most recent at the top)
36. Verify that you can see your recent changes at the top
37. The report is generated with several pages of users – change it to **200** per page and now all the users in AD are displayed on a single page
38. Click **Point-In-Time** and select **yesterday**
39. Click **Build** and sort on **pwdLastSet**

40. Verify that the new resets are not part of this report – we are seeing what the report would have looked like yesterday

Task 2: Sharing Reports

41. **Copy the browser URL** and **paste** it into a different tab (or even a different browser) – you may have to sign in again, of course

Note: You can share reports that you have generated by sharing the URL – access to the URL is subject to Identity Panel's security.

42. From the Reports page click **Download** (top right)
43. In the **Download File Name** enter **YesterdaypwdLastSetReport** ensure the download format is **Delimited** and click **Ok**
44. If your browser prompts, click **Save**
45. Navigate to the **Downloads** folder and open **YesterdaypwdLastSetReport.txt**

Note: Reports can be downloaded in a number of formats including Excel, HTML, and XML which can be viewed by users who don't have access to Identity Panel.

Task 3: Drilling down in reports

46. From the **Select Report** dropdown, select **AD – UserAccountControl Flags**, ensure you **clear the Point-In-Time date**, select **ACCOUNTDISABLE** as the **Flag**, and click **Build**
47. Verify that you can see the user that you Emergency Terminated in an earlier lab
48. Follow the link for the **user** you terminated and you are taken to the Time Traveler (you may want to change the Shutter View)




About Oxford Computer Training

We are the worldwide specialists for training in Microsoft identity and mobility technologies. Oxford Computer Training is part of Oxford Computer Group.

oxfordcomputertraining.com

 Follow us on Twitter: [@OCGTraining](https://twitter.com/OCGTraining)

 Find us on LinkedIn: [oxford-computer-training](https://www.linkedin.com/company/oxford-computer-training)

 Like us on Facebook: [@OCGTraining](https://www.facebook.com/OCGTraining)