Identity Management and Reporting Made Easy

→ Simon Veale

Steven Griffiths

Peter Sidebotham

Kocho

BECOME GREATER

Agenda

→ SoftwareIDM's Identity Panel Suite can turbo-charge all of your Identity and Access Management needs.

- → Introduction
- → Just how bad is my identity data?
- → An approach to an IdM solution implementation
- → Adding access governance

The team

→ Simon Veale

→ Steven Griffiths

→ Peter Sidebotham

Introduction

Which of the following applies to you?

→ We use Microsoft Identity Manager - Synchronization Service only

→ We use Microsoft Identity Manager - Synchronization Service and Portal

→ We use a different Identity and Access Management solution

→ We don’t have any automated Identity and Access Management

Introduction

The Identity Panel Suite consists of five components. We’re not planning to cover all of them in depth in this session.

What’s the focus of this session?

HyperSync

Service Panel

Q&A (feel free to ask about any components)

What’s not?

Identity Panel (except Scanning & Reporting)

Access Panel

Test Panel

Introduction

→ Those with Microsoft Identity Manager

→ Those just starting their IdAM journey

→ Those looking to “modernise” the user experience

→ Those looking to grow their Identity and Access Management solution

Introduction

Microsoft Entra

Protect access to any app or resource

Safeguard your organization by protecting access to every app and every resource for every user.

Secure and verify every identity

Effectively secure every identity including employees, customers, partners, apps, devices, and workloads across every environment.

Provide only the access necessary

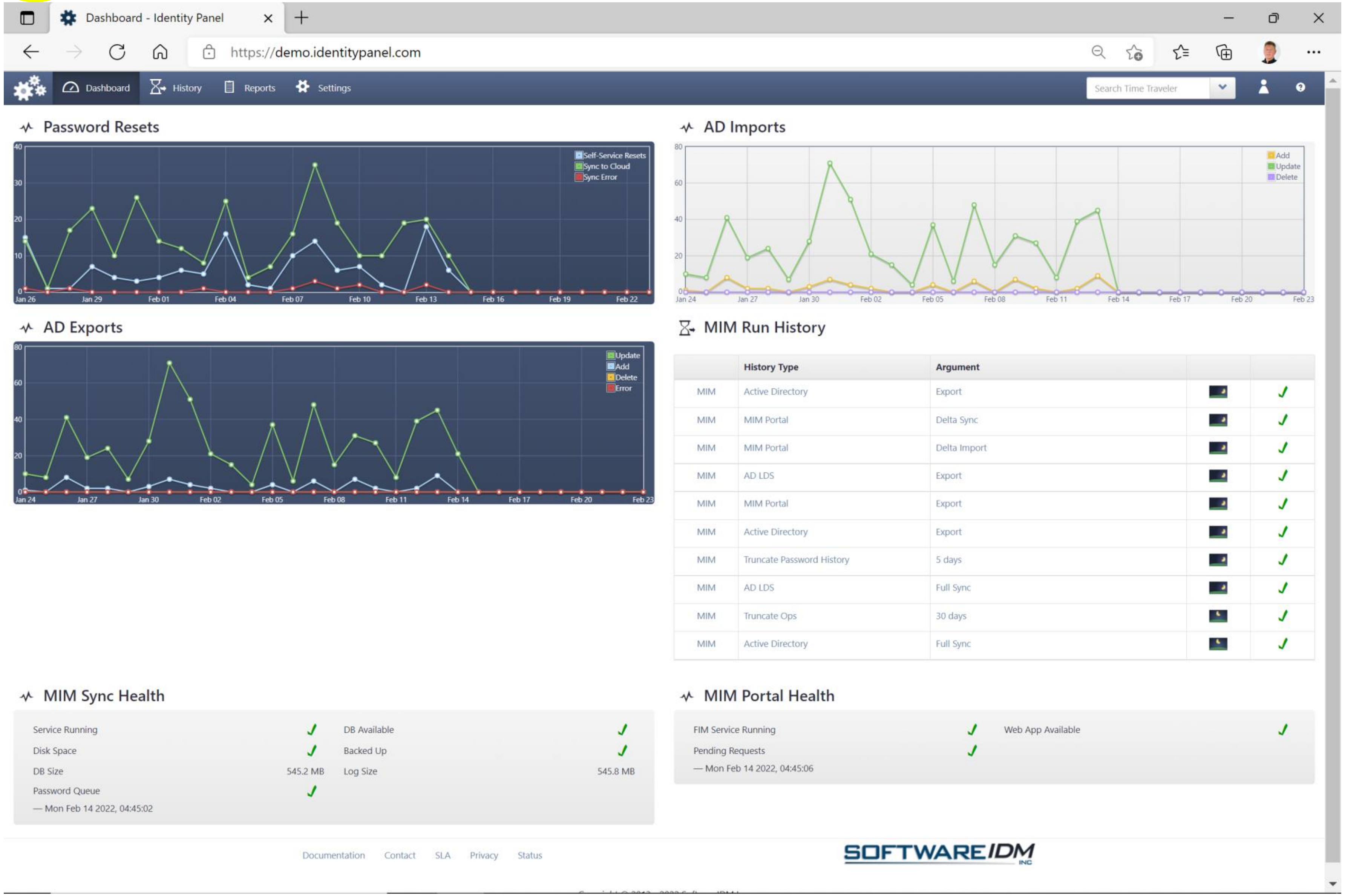
Discover and right-size permissions, manage access lifecycles, and ensure least privilege access for any identity.

Those with MIM

Identity Panel

- → Dashboard
- → Time Traveller
- → Reports
- → Schedules
- → RBAC

Identity Panel - dashboard



MIM Run History

	History Type	Argument		
MIM	Active Directory	Export		✓
MIM	MIM Portal	Delta Sync		✓
MIM	MIM Portal	Delta Import		✓
MIM	AD LDS	Export		✓
MIM	MIM Portal	Export		✓
MIM	Active Directory	Export		✓
MIM	Truncate Password History	5 days		✓
MIM	AD LDS	Full Sync		✓
MIM	Truncate Ops	30 days		✓
MIM	Active Directory	Full Sync		✓

MIM Sync Health

Service Running	✓	DB Available	✓
Disk Space	✓	Backed Up	✓
DB Size	545.2 MB	Log Size	545.8 MB
Password Queue	✓		

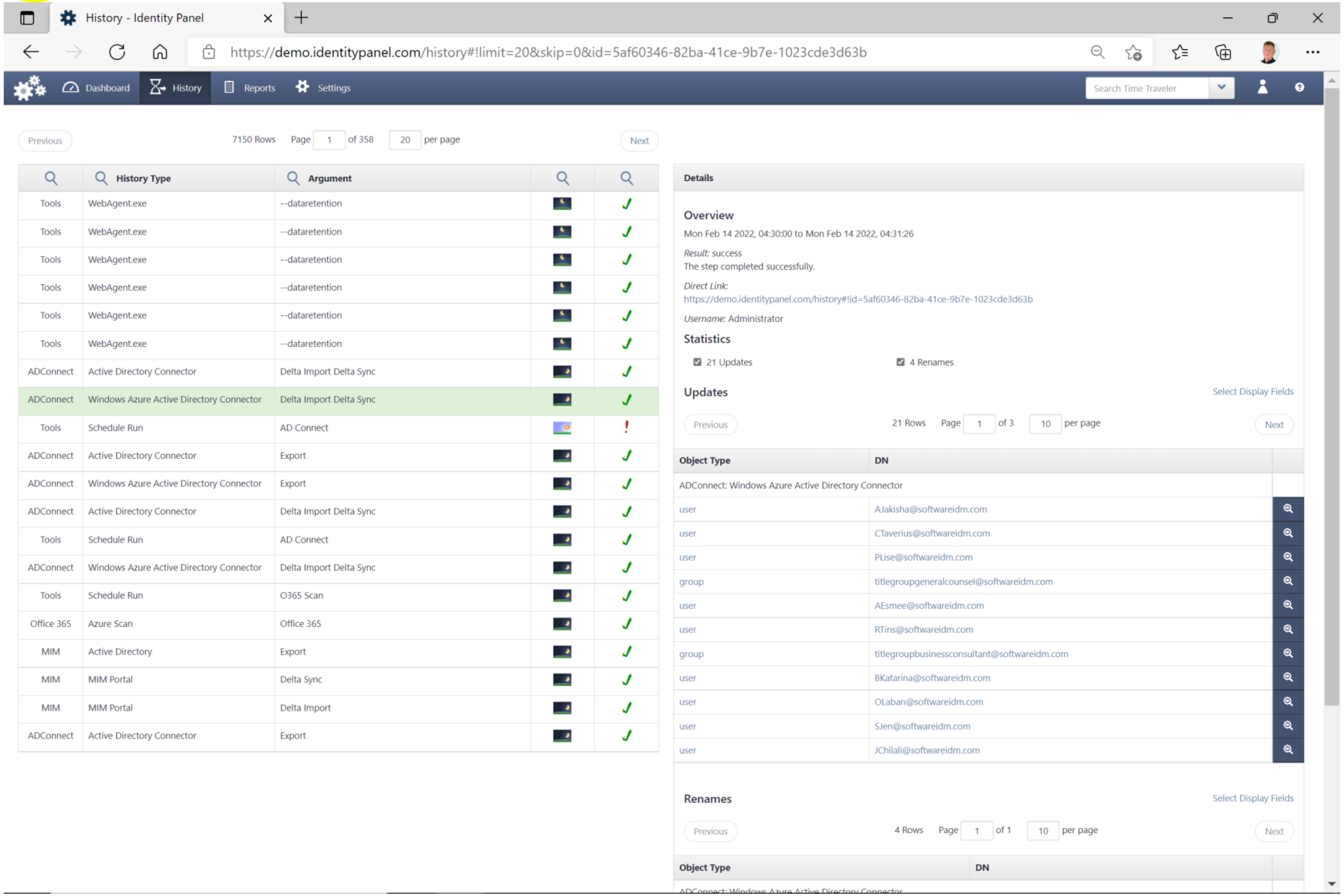
— Mon Feb 14 2022, 04:45:02

MIM Portal Health

FIM Service Running	✓	Web App Available	✓
Pending Requests	✓		

— Mon Feb 14 2022, 04:45:06

Identity Panel - history


History - Identity Panel
https://demo.identitypanel.com/history#!limit=20&skip=0&id=5af60346-82ba-41ce-9b7e-1023cde3d63b
Dashboard
History
Reports
Settings
Search Time Traveler
Previous
Next

7150 Rows Page 1 of 358 20 per page

	History Type	Argument		
Tools	WebAgent.exe	--dataretention		✓
Tools	WebAgent.exe	--dataretention		✓
Tools	WebAgent.exe	--dataretention		✓
Tools	WebAgent.exe	--dataretention		✓
Tools	WebAgent.exe	--dataretention		✓
Tools	WebAgent.exe	--dataretention		✓
ADConnect	Active Directory Connector	Delta Import Delta Sync		✓
ADConnect	Windows Azure Active Directory Connector	Delta Import Delta Sync		✓
Tools	Schedule Run	AD Connect		!
ADConnect	Active Directory Connector	Export		✓
ADConnect	Windows Azure Active Directory Connector	Export		✓
ADConnect	Active Directory Connector	Delta Import Delta Sync		✓
Tools	Schedule Run	AD Connect		✓
ADConnect	Windows Azure Active Directory Connector	Delta Import Delta Sync		✓
Tools	Schedule Run	O365 Scan		✓
Office 365	Azure Scan	Office 365		✓
MIM	Active Directory	Export		✓
MIM	MIM Portal	Delta Sync		✓
MIM	MIM Portal	Delta Import		✓
ADConnect	Active Directory Connector	Export		✓

Details

Overview

Mon Feb 14 2022, 04:30:00 to Mon Feb 14 2022, 04:31:26

Result: success
The step completed successfully.

Direct Link:
https://demo.identitypanel.com/history#!id=5af60346-82ba-41ce-9b7e-1023cde3d63b

Username: Administrator

Statistics

☑ 21 Updates ☑ 4 Renames

Updates Select Display Fields

Previous 21 Rows Page 1 of 3 10 per page Next

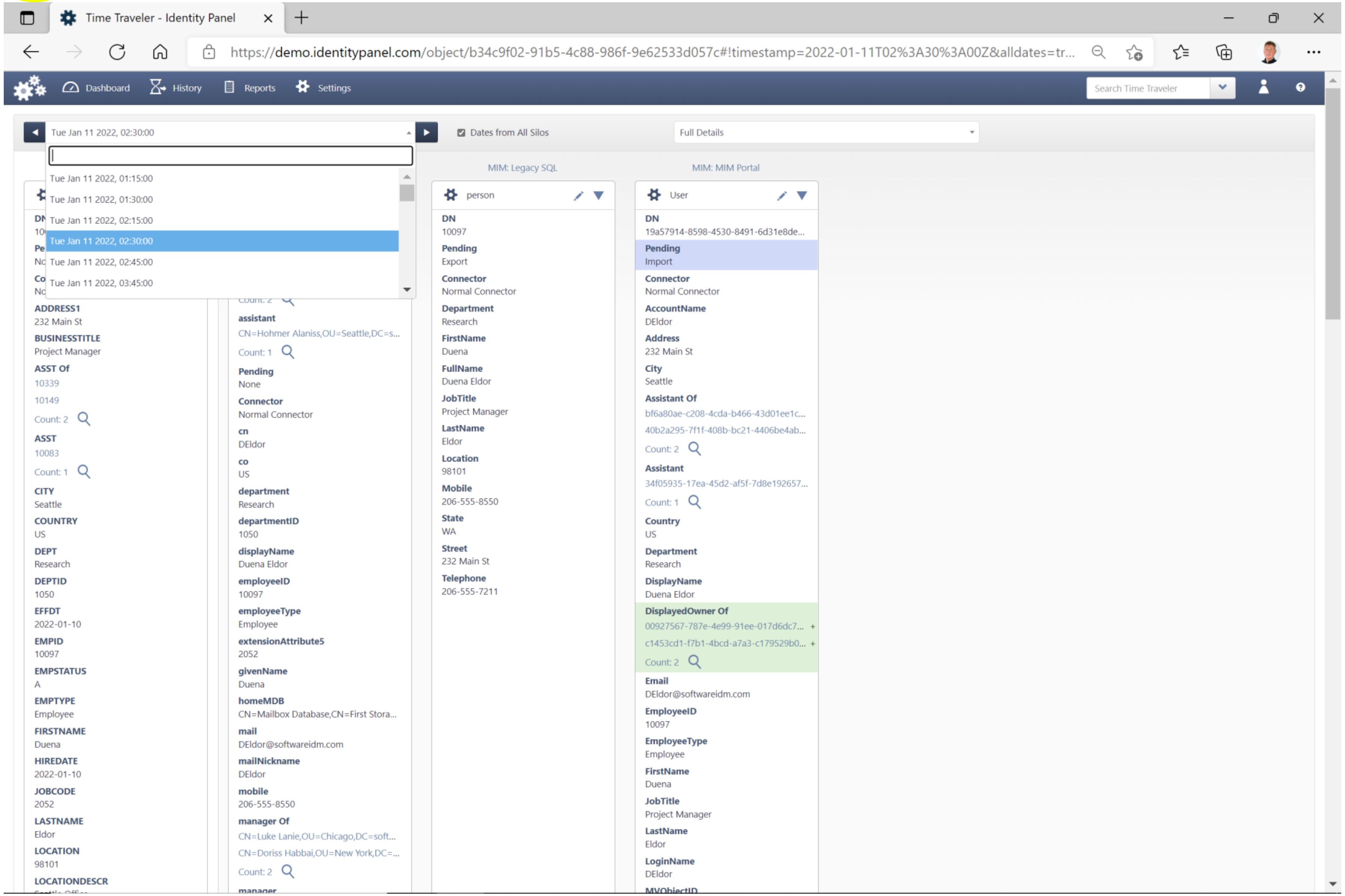
Object Type	DN
ADConnect: Windows Azure Active Directory Connector	
user	AJakisha@softwareidm.com
user	CTaverius@softwareidm.com
user	PLise@softwareidm.com
group	titlegroupgeneralcounsel@softwareidm.com
user	AEsmee@softwareidm.com
user	RTins@softwareidm.com
group	titlegroupbusinessconsultant@softwareidm.com
user	BKatarina@softwareidm.com
user	OLaban@softwareidm.com
user	SJen@softwareidm.com
user	JChilali@softwareidm.com

Renames Select Display Fields

Previous 4 Rows Page 1 of 1 10 per page Next

Object Type	DN
ADConnect: Windows Azure Active Directory Connector	

Identity Panel - time traveller


Time Traveler - Identity Panel
https://demo.identitypanel.com/object/b34c9f02-91b5-4c88-986f-9e62533d057c#!timestamp=2022-01-11T02%3A30%3A00Z&alldates=tr...
Dashboard
History
Reports
Settings
Search Time Traveler

Tue Jan 11 2022, 02:30:00

☑ Dates from All Silos

Full Details

- Tue Jan 11 2022, 01:15:00
- Tue Jan 11 2022, 01:30:00
- Tue Jan 11 2022, 02:15:00
- Tue Jan 11 2022, 02:30:00
- Tue Jan 11 2022, 02:45:00
- Tue Jan 11 2022, 03:45:00

DN
10
Pe
No
Co
No
ADDRESS1
232 Main St
BUSINESSTITLE
Project Manager
ASST Of
10339
10149
Count: 2
ASST
10083
Count: 1
CITY
Seattle
COUNTRY
US
DEPT
Research
DEPTID
1050
EFFDT
2022-01-10
EMPID
10097
EMPSTATUS
A
EMPTYPE
Employee
FIRSTNAME
Duena
HIREDATE
2022-01-10
JOBCODE
2052
LASTNAME
Eldor
LOCATION
98101
LOCATIONDESCR

Count: 2
assistant
CN=Hohmer Alaniss,OU=Seattle,DC=s...
Count: 1
Pending
None
Connector
Normal Connector
cn
DEldor
co
US
department
Research
departmentID
1050
displayName
Duena Eldor
employeeID
10097
employeeType
Employee
extensionAttribute5
2052
givenName
Duena
homeMDB
CN=Mailbox Database,CN=First Stora...
mail
DEldor@softwareidm.com
mailNickname
DEldor
mobile
206-555-8550
manager Of
CN=Luke Lanie,OU=Chicago,DC=soft...
CN=Doriss Habbai,OU=New York,DC=...
Count: 2
manager

MIM: Legacy SQL

person

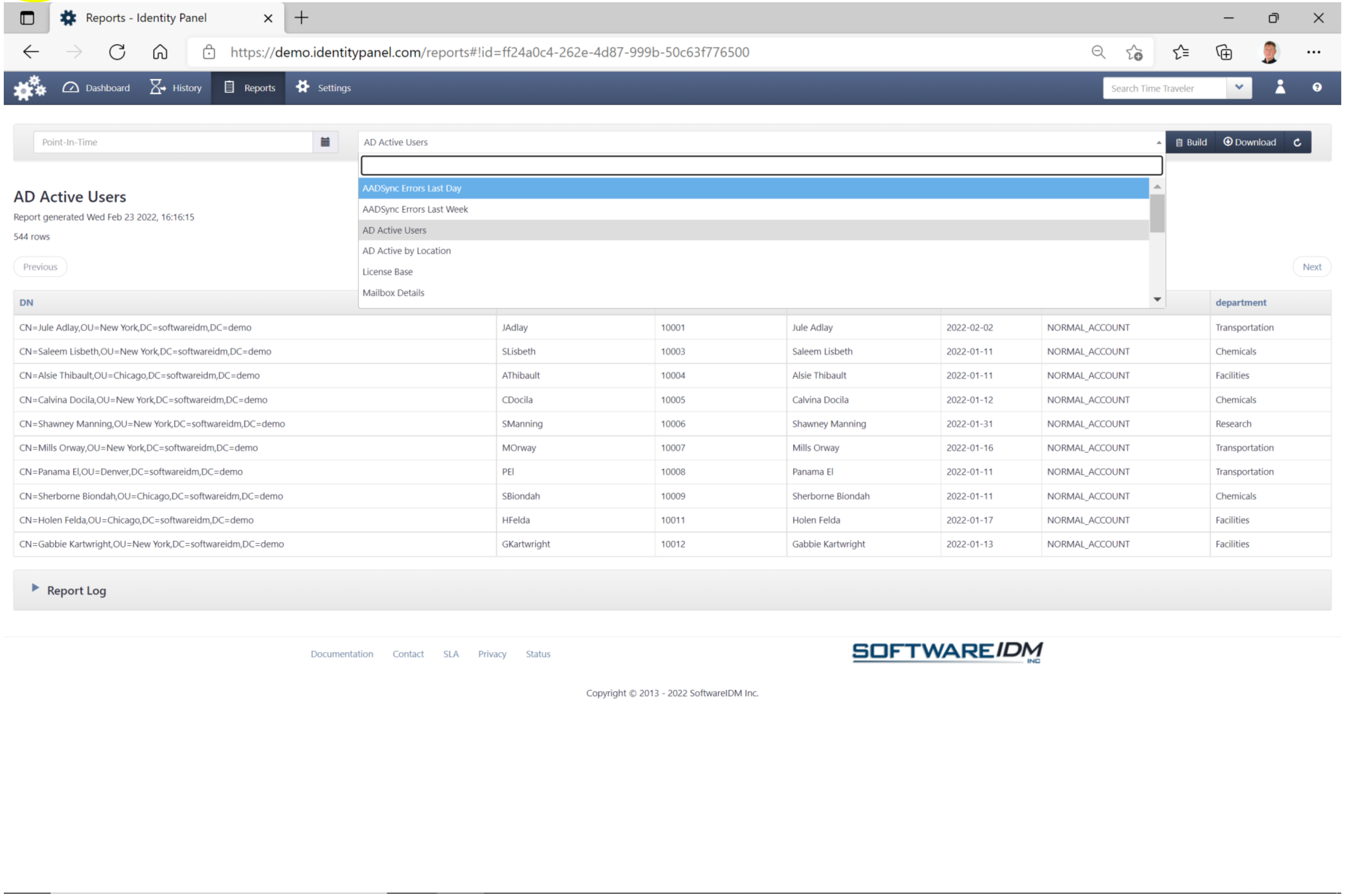
DN
10097
Pending
Export
Connector
Normal Connector
Department
Research
FirstName
Duena
FullName
Duena Eldor
JobTitle
Project Manager
LastName
Eldor
Location
98101
Mobile
206-555-8550
State
WA
Street
232 Main St
Telephone
206-555-7211

MIM: MIM Portal

User

DN
19a57914-8598-4530-8491-6d31e8de...
Pending
Import
Connector
Normal Connector
AccountName
DEldor
Address
232 Main St
City
Seattle
Assistant Of
bf6a80ae-c208-4cda-b466-43d01ee1c...
40b2a295-7f1f-408b-bc21-4406be4ab...
Count: 2
Assistant
34f05935-17ea-45d2-af5f-7d8e192657...
Count: 1
Country
US
Department
Research
DisplayName
Duena Eldor
DisplayedOwner Of
00927567-787e-4e99-91ee-017d6dc7... +
c1453cd1-f7b1-4bcd-a7a3-c179529b0... +
Count: 2
Email
DEldor@softwareidm.com
EmployeeID
10097
EmployeeType
Employee
FirstName
Duena
JobTitle
Project Manager
LastName
Eldor
LoginName
DEldor
MVObjectID

Identity Panel - reports



AD Active Users

Report generated Wed Feb 23 2022, 16:16:15

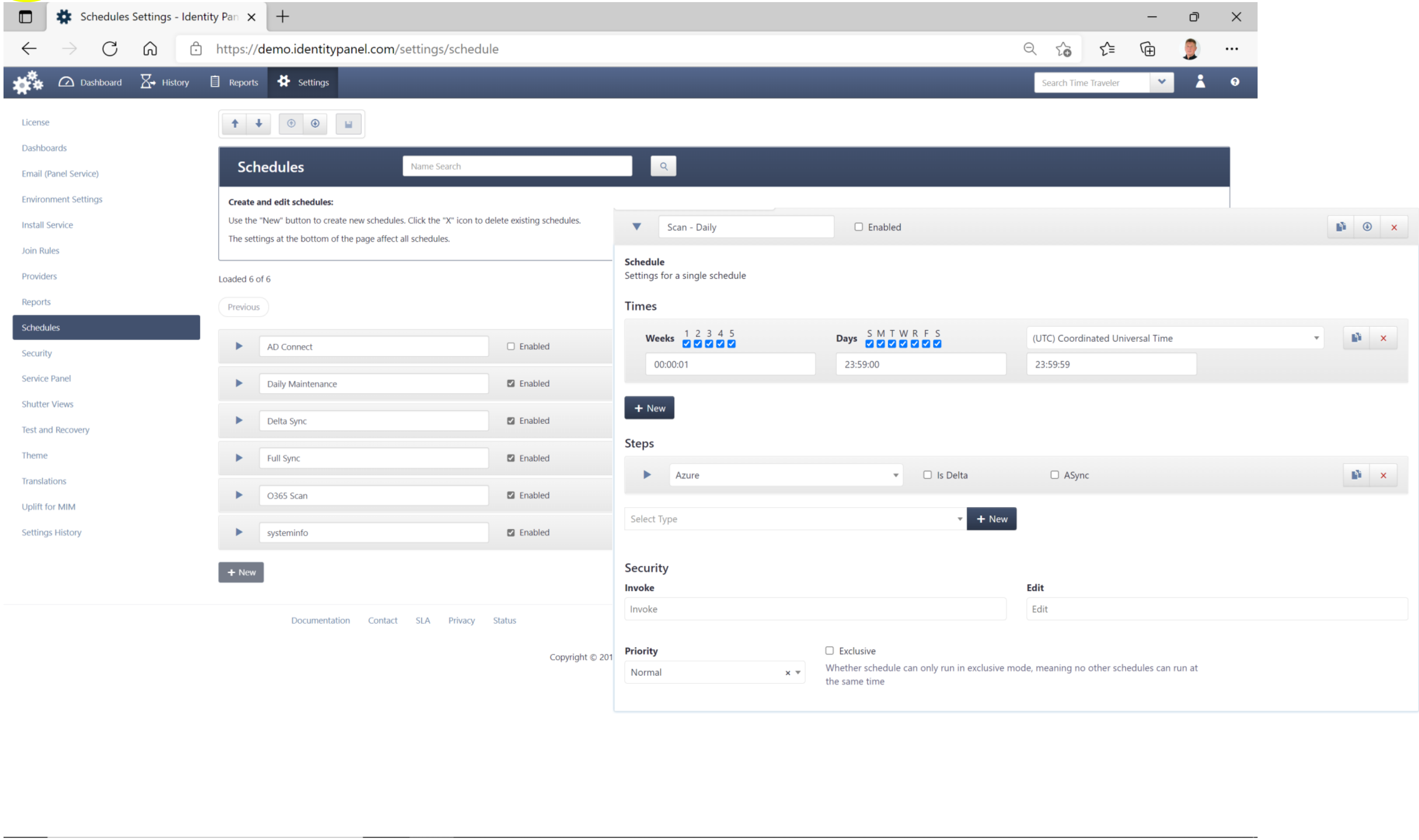
544 rows

DN						department
CN=Jule Adlay,OU=New York,DC=softwareidm,DC=demo	JAdlay	10001	Jule Adlay	2022-02-02	NORMAL_ACCOUNT	Transportation
CN=Saleem Lisbeth,OU=New York,DC=softwareidm,DC=demo	SLisbeth	10003	Saleem Lisbeth	2022-01-11	NORMAL_ACCOUNT	Chemicals
CN=Alsie Thibault,OU=Chicago,DC=softwareidm,DC=demo	AThibault	10004	Alsie Thibault	2022-01-11	NORMAL_ACCOUNT	Facilities
CN=Calvina Docila,OU=New York,DC=softwareidm,DC=demo	CDocila	10005	Calvina Docila	2022-01-12	NORMAL_ACCOUNT	Chemicals
CN=Shawney Manning,OU=New York,DC=softwareidm,DC=demo	SManning	10006	Shawney Manning	2022-01-31	NORMAL_ACCOUNT	Research
CN=Mills Orway,OU=New York,DC=softwareidm,DC=demo	MOrway	10007	Mills Orway	2022-01-16	NORMAL_ACCOUNT	Transportation
CN=Panama El,OU=Denver,DC=softwareidm,DC=demo	PEl	10008	Panama El	2022-01-11	NORMAL_ACCOUNT	Transportation
CN=Sherborne Biondah,OU=Chicago,DC=softwareidm,DC=demo	SBiondah	10009	Sherborne Biondah	2022-01-11	NORMAL_ACCOUNT	Chemicals
CN=Holen Felda,OU=Chicago,DC=softwareidm,DC=demo	HFelda	10011	Holen Felda	2022-01-17	NORMAL_ACCOUNT	Facilities
CN=Gabbie Kartwright,OU=New York,DC=softwareidm,DC=demo	GKartwright	10012	Gabbie Kartwright	2022-01-13	NORMAL_ACCOUNT	Facilities

▶ Report Log

Copyright © 2013 - 2022 SoftwareIDM Inc.

Identity Panel - schedules



Schedules Settings - Identity Pan

https://demo.identitypanel.com/settings/schedule

Schedules

Name Search

Create and edit schedules:

Use the "New" button to create new schedules. Click the "X" icon to delete existing schedules.

The settings at the bottom of the page affect all schedules.

Loaded 6 of 6

Previous

▶ AD Connect □ Enabled

▶ Daily Maintenance ☑ Enabled

▶ Delta Sync ☑ Enabled

▶ Full Sync ☑ Enabled

▶ O365 Scan ☑ Enabled

▶ systeminfo ☑ Enabled

+ New

Copyright © 201

▼ Scan - Daily □ Enabled

Schedule

Settings for a single schedule

Times

Weeks 1 2 3 4 5 ☑ ☑ ☑ ☑ ☑ **Days** S M T W R F S ☑ ☑ ☑ ☑ ☑ ☑ ☑ (UTC) Coordinated Universal Time

00:00:01 23:59:00 23:59:59

+ New

Steps

▶ Azure □ Is Delta □ ASync

Select Type + New

Security

Invoke

Invoke

Edit

Edit

Priority

Normal

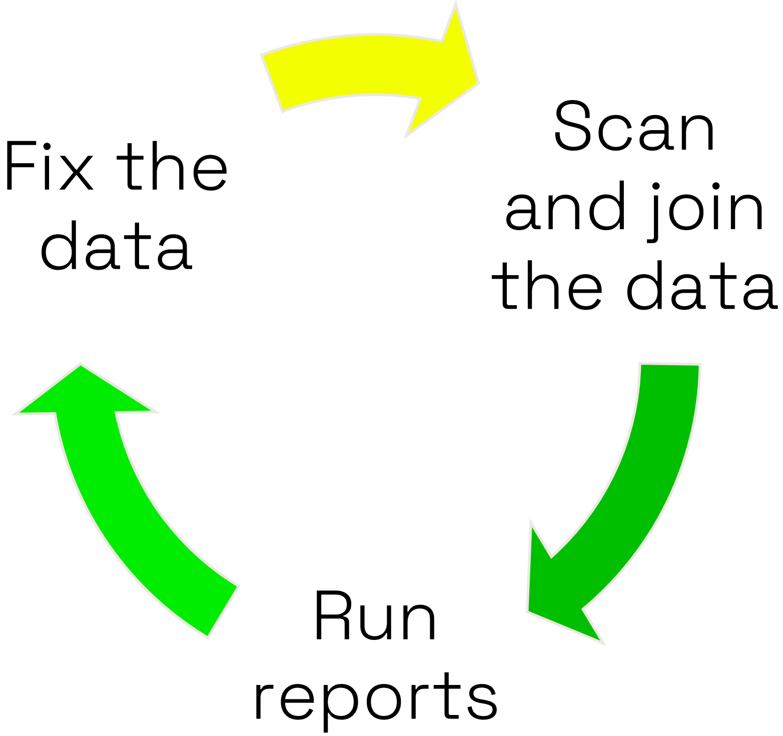
□ Exclusive

Whether schedule can only run in exclusive mode, meaning no other schedules can run at the same time

Those just starting

Identity Panel

- → What state is my data in?
  - → Potential joins
  - → Orphaned accounts
  - → Active accounts that shouldn't be
  - → Dormant accounts
  - → Mismatched attributes



Those looking to modernise (automation)

HyperSync Panel

- Runs in the cloud
- Removes entirely the need for on-premises servers (or VMs) for MIM
- Many times faster than MIM
- State-based or event-driven
- Can trigger actions based on time
- Has Thresholds to prevent large-scale unexpected changes
- Shares a common configuration interface and script language with all the other Identity Panel Suite components
- Everything is web-based
- Is very intuitive in its operation for those who know MIM
- Has all of the benefits provided by Identity Panel

Those looking to modernise (user experience)

Service Panel

- → More modern look and feel
- → More customisable
- → More flexible in its presentation of data
- → More flexible in accepting changes
- → Uses the same roles as other Identity Panel components
- → Shares a common configuration interface and language with all the other Identity Panel Suite components
- → Has all of the benefits provided by Identity Panel

Those looking to grow

Access Panel

- ABAC (attribute-based access control).
- JIT (Just In Time) access / PAM (Privileged Access Management).
- RBAC (traditional role-based access control).
- Attestation / recertification.
- Access reviews.

Identity Panel

How good is your Identity data?

- Client X
  - We use a script
  - We're not sure what it does – the author left years ago
  - It has to run 5 times before a user is fully provisioned (= 5 days)
  - It has some things in it we know we don't need, but we don't dare remove them
- Client Y
  - We have an IdM system but only one person understands it and he's changed jobs
  - It works perfectly – they said
  - At go-live, a huge report of pending changes. All investigated and all valid. Client too afraid to implement for existing users
- Client Z
  - We have an old system and upgrading and renewing licenses is too expensive
  - At go-live, a huge report of pending changes. All investigated and all valid

Reports

- Configure in Identity Panel
- Download in different formats, Excel, HTML, Delimited, XML, JSON
- Automatic production and dissemination based on a schedule
- Reports can be inputs to other reports
- Reports can be inputs to workflows
- Recipients only see what they have permission to see

Time Traveller

- Answer questions like…
  - What did my identity data look like at a point in time?
  - How and when did my identity data get like this?
  - How is my identity data flowing between different systems? E.g. Workday to AD.

Reporting demo

HyperSync Panel

HyperSync Panel

→ Similar in concept to MIM

→ Extensible schema

→ Stateful Sync rules + event-driven

→ Attribute Flow rules

→ Throttling and thresholds

→ Scope Filters

→ Logging

→ Preview synchronisation

→ SaaS application

→ Removes entirely the need for on-premises servers (or VMs) for MIM

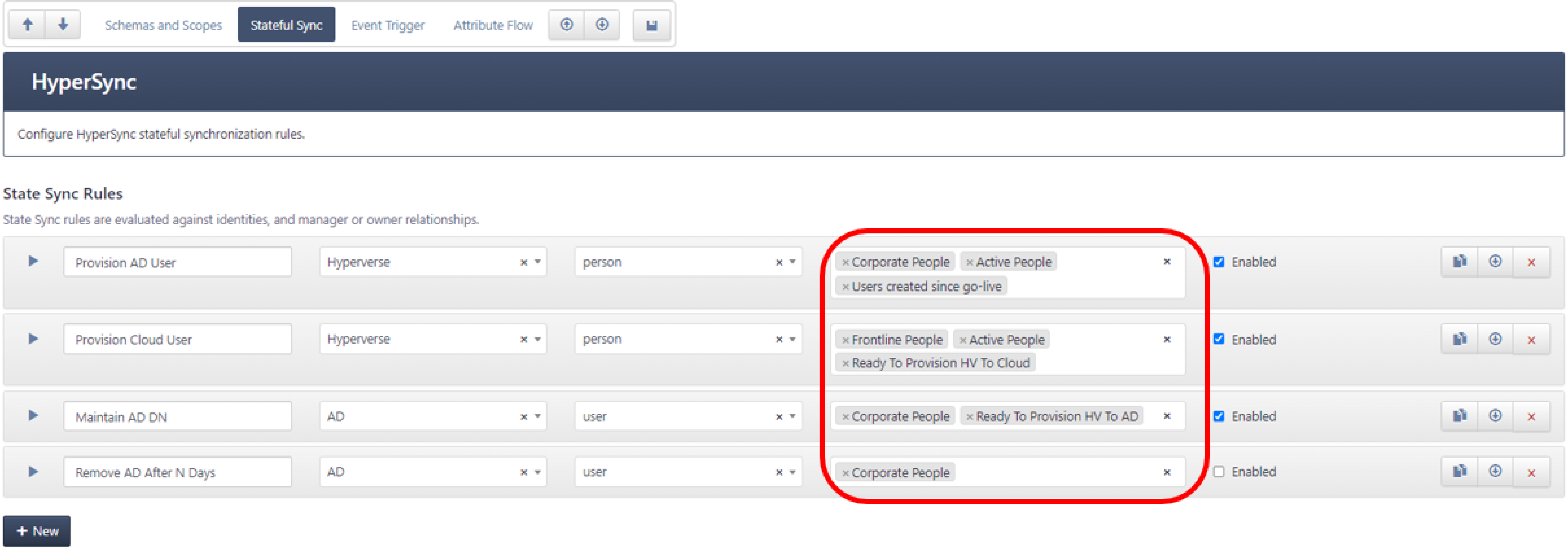
→ Up to 100x faster than MIM in executing rules-based logic

→ Shares a common configuration interface and script language

Scope Filters

- Rules for identifying classes of identities to apply sync logic
- These have also proved very useful for:
    - Supporting roll-out by location, country
    - Specifically excluding individuals
- Beware of referencing objects that are not in scope, e.g. manager

Scope filters



HyperSync

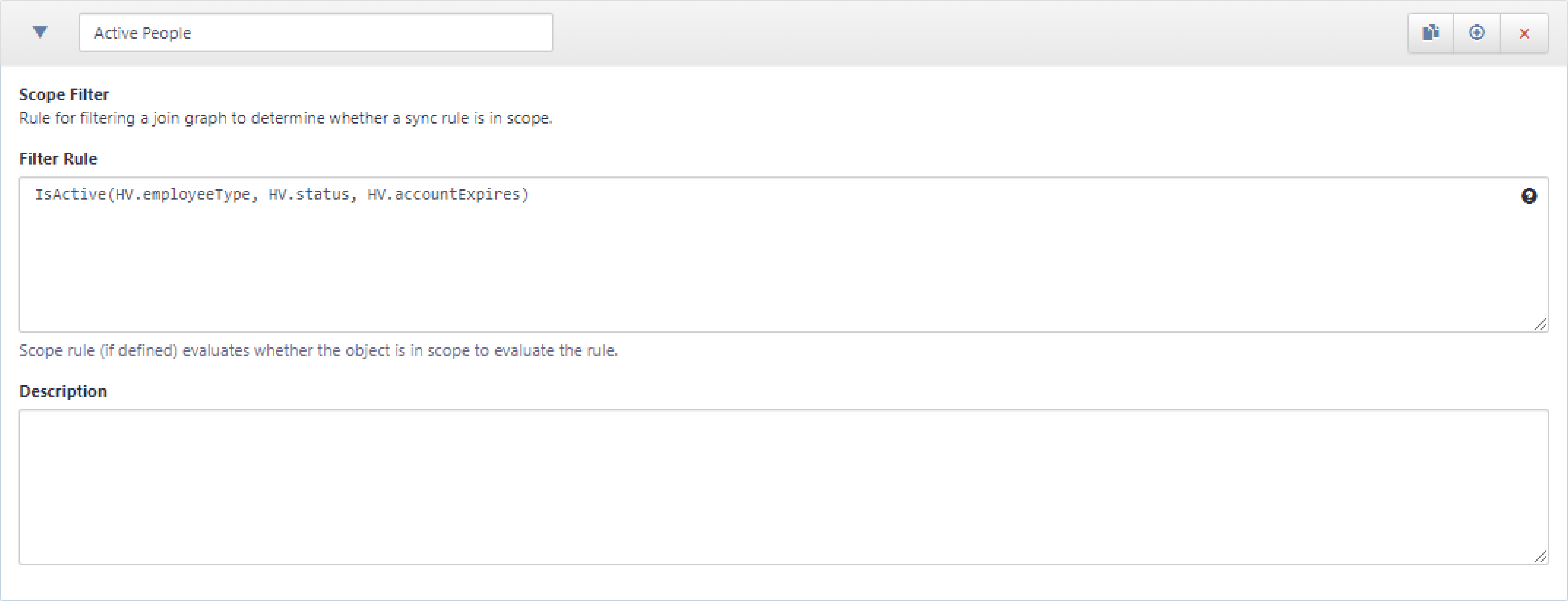
Configure HyperSync stateful synchronization rules.

State Sync Rules

State Sync rules are evaluated against identities, and manager or owner relationships.

Provision AD User	Hyperverse	person	× Corporate People × Active People × Users created since go-live	☑ Enabled
Provision Cloud User	Hyperverse	person	× Frontline People × Active People × Ready To Provision HV To Cloud	☑ Enabled
Maintain AD DN	AD	user	× Corporate People × Ready To Provision HV To AD	☑ Enabled
Remove AD After N Days	AD	user	× Corporate People	□ Enabled

Scoping Filter example



Active People

Scope Filter

Rule for filtering a join graph to determine whether a sync rule is in scope.

Filter Rule

```
IsActive(HV.employeeType, HV.status, HV.accountExpires)
```

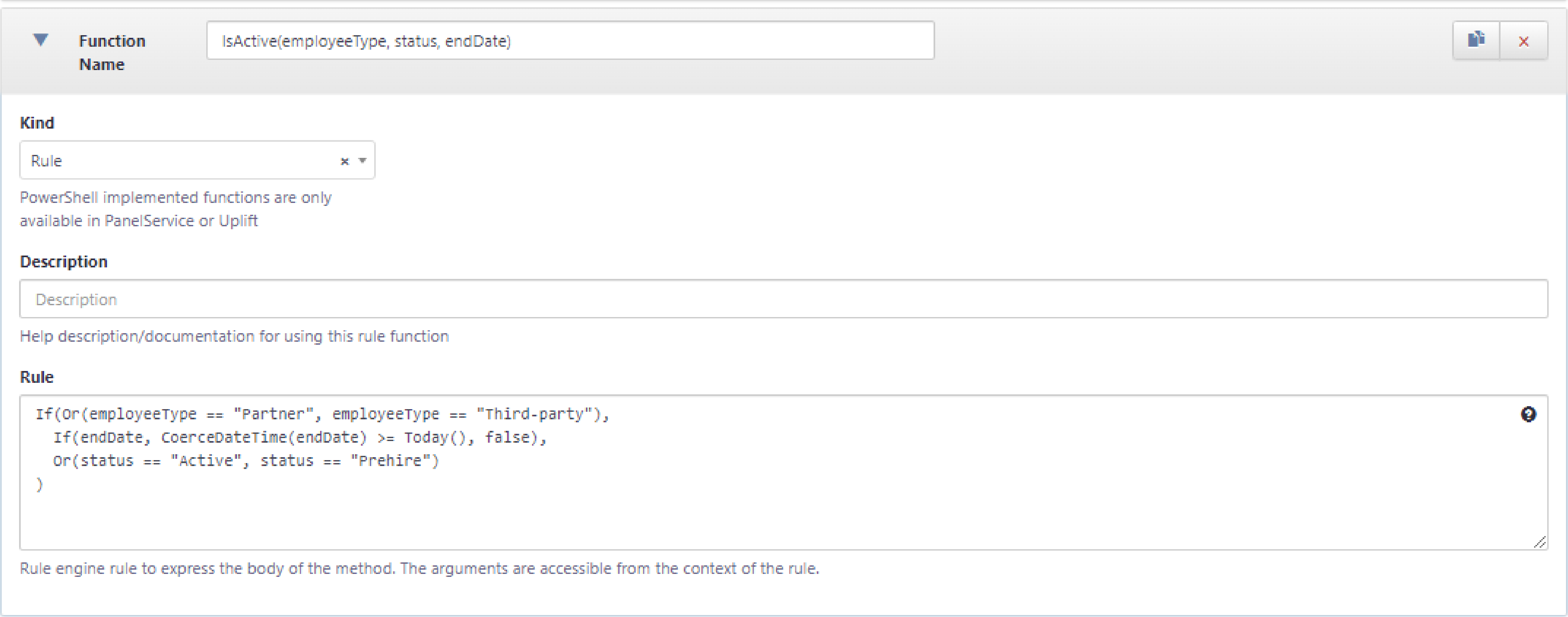
Scope rule (if defined) evaluates whether the object is in scope to evaluate the rule.

Description

Functions

- Encapsulate more complicated rule engine logic
- Logic that is used in multiple places, sync rules, reports

Function example



Function Name IsActive(employeeType, status, endDate)

Kind

Rule

PowerShell implemented functions are only available in PanelService or Uplift

Description

Description

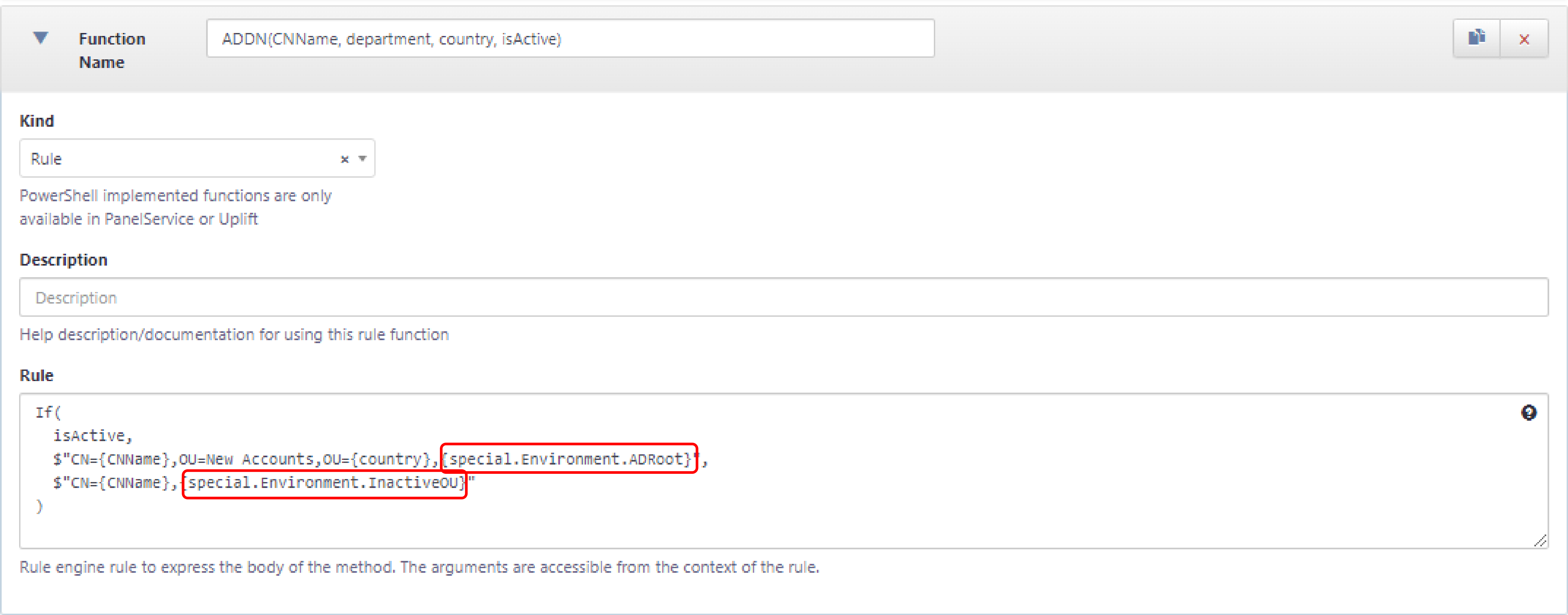
Help description/documentation for using this rule function

Rule

```
If(Or(employeeType == "Partner", employeeType == "Third-party"),
  If(endDate, CoerceDateTime(endDate) >= Today(), false),
  Or(status == "Active", status == "Prehire")
)
```

Rule engine rule to express the body of the method. The arguments are accessible from the context of the rule.

Function example



Function Name ADDN(CNName, department, country, isActive)

Kind

Rule

PowerShell implemented functions are only available in PanelService or Uplift

Description

Description

Help description/documentation for using this rule function

Rule

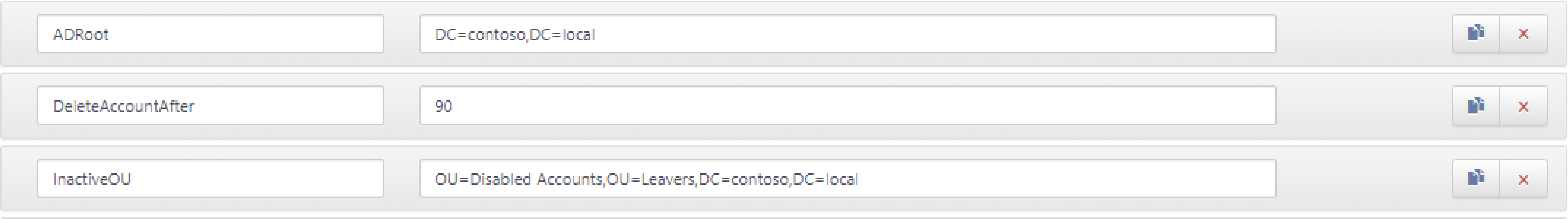
```
If(
  isActive,
  $"CN={CNName},OU=New Accounts,OU={country},{special.Environment.ADRoot}",
  $"CN={CNName},{special.Environment.InactiveOU}"
)
```

Rule engine rule to express the body of the method. The arguments are accessible from the context of the rule.

Environment Variables

- → Variables to substitute into rule values
- → New environment variables will be copied between environments, e.g. development to production
- → Values of existing environment variables will not be changed when copying between environments

Environment Variables examples



ADRoot	DC=contoso,DC=local
DeleteAccountAfter	90
InactiveOU	OU=Disabled Accounts,OU=Leavers,DC=contoso,DC=local

Joiner demo

Mover demo

Leaver demo

Service Panel

Service Panel typical scenarios

Who	What
→ Administrator	→ Emergency suspension
→ HR	→ Request an admin account
→ Auditor	→ Re-enable dormant account
→ Manager	→ Update personal contact details
→ Individual	→ Manage contractor accounts

Service Panel

- More modern look and feel
- More customisable. E.g. multiple forms for different user types, and different operations, where MIM restricts to one “form” per object type.
- More flexible in its presentation of data (not restricted to single screen, single column), collapsible form sections. More flexible in accepting changes, with options for separate forms, multi-page forms, and the ability to save partially completed forms.
- Uses the same roles as other Identity Panel components.
- Shares a common configuration interface and script language with all the other Identity Panel Suite components.
- Has all of the benefits provided by Identity Panel

Service Panel demo

Access Panel

Access Panel demo

Kocho

BECOME GREATER

Thank you

→ Any questions?