



Key Features of MIM & Azure AD Connect

2017 NYC Forum

Chris Lloyd & Jim Troyer

Common MIM Use Cases

User Provisioning



Automated

Driven by authoritative sources

Standardized

de-provisioning

Group Management



Self-service

Reduction of service tickets

Approval driven

Fixes Hybrid Exchange group problems

Self-Service Password Reset



Self-service

Reduction of service tickets

Desktop integration

Azure MFA

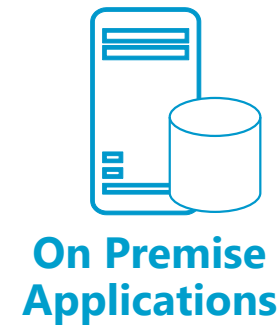
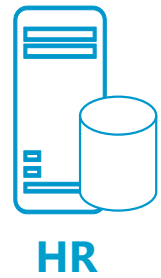
What's New In MIM 2016 SP1?



- Sync engine unchanged
- Upgrade from FIM has same feel as installing hotfixes in FIM
- Some technologies supported
 - Cross browser support
 - Windows Server 2016
 - Microsoft SQL 2016
 - SCSM 2012, 2012R2, 2016
 - .NET 4.0 required!
 - Azure MFA



Synchronize Enterprise Identities



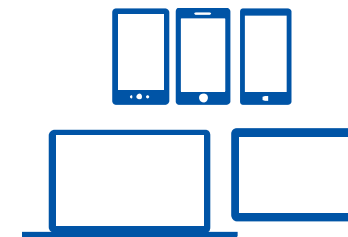
Password reset

Delegated group management

Self-Service Password Reset Options



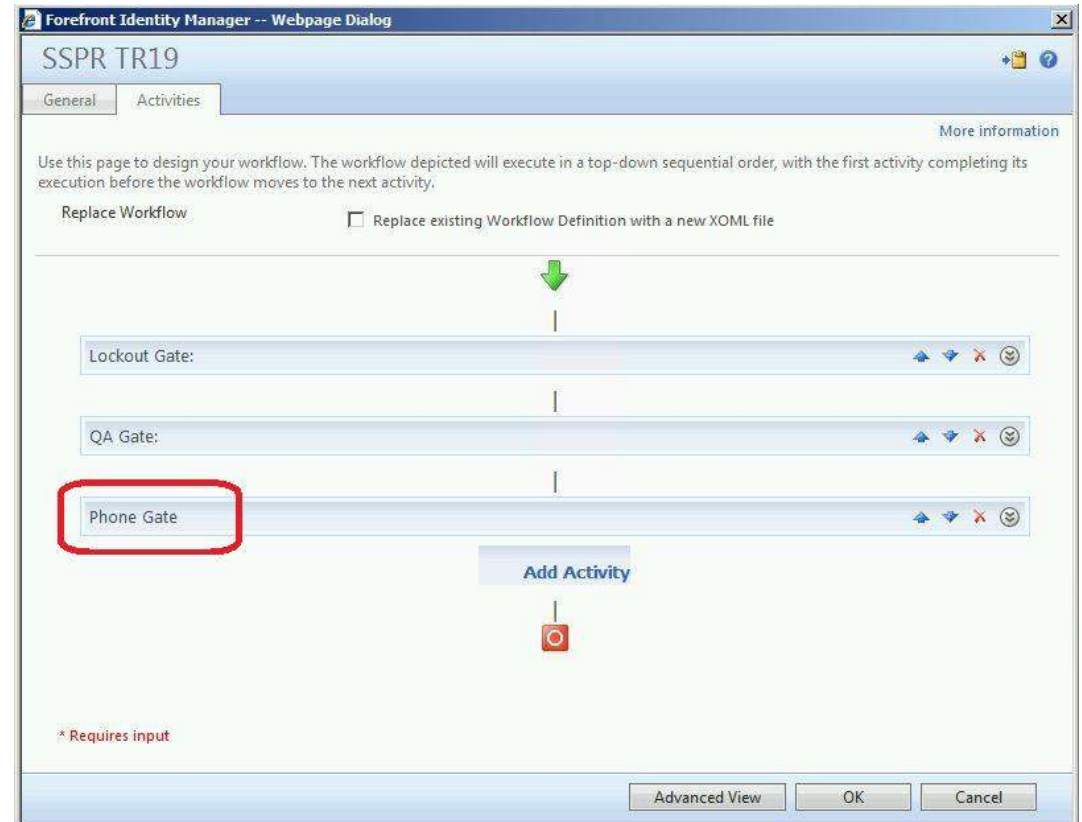
Registration and reset is performed in the cloud and password is written back to Active Directory. Multiple authentication gates are available. Account can also be unlocked rather than password reset.



Registration is performed through web portal. Reset can be performed via the web portal or credential provider. Multiple authentication gates are available. Account can also be unlocked rather than password reset.

Leveraging Azure MFA

- New phone gate added
- Account unlock
- Azure MFA service
 - Phone call
 - SMS one time code

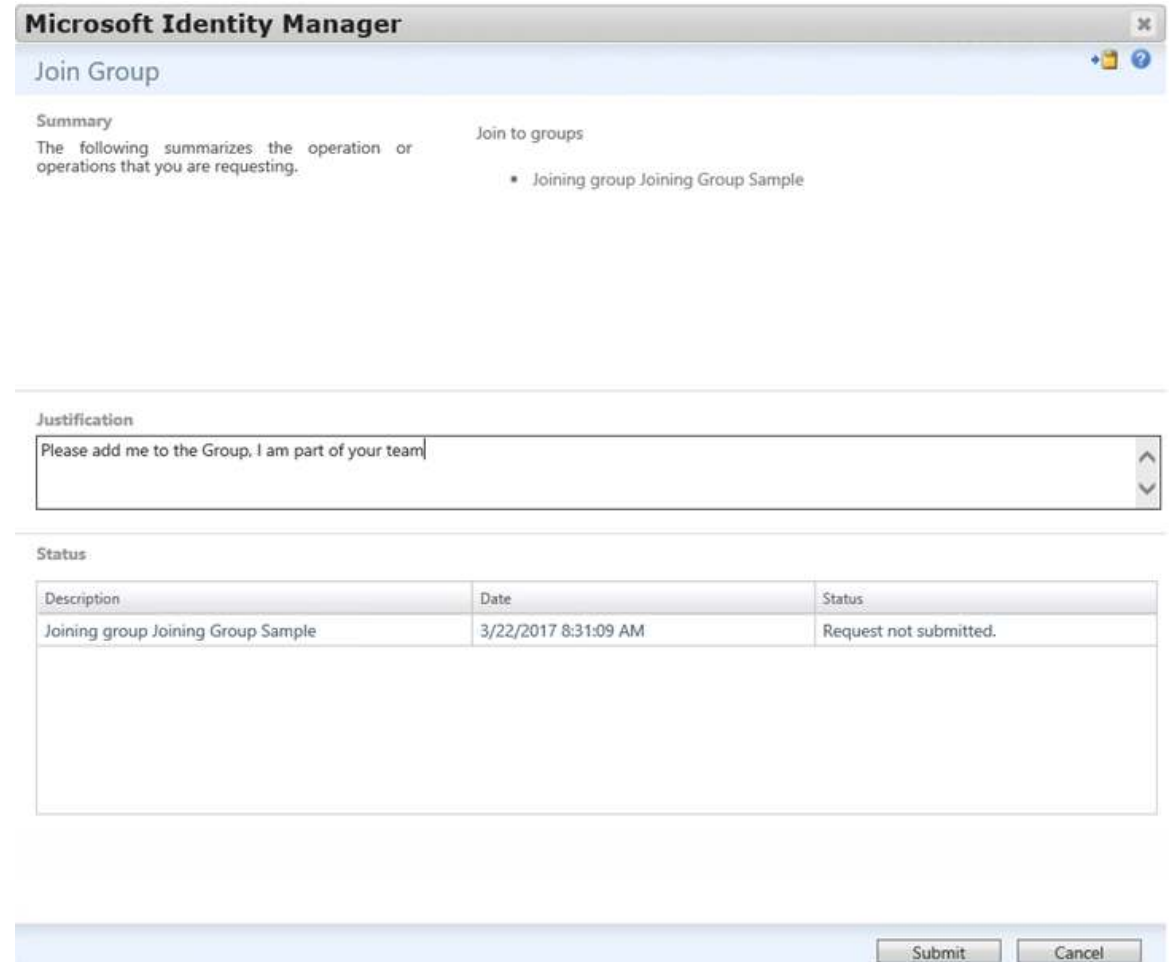


Approval Justification

Justification and responses for group membership joins.

XPATH for email templates

- [//Request/Justification]
- [//WorkflowData/Reason]



The screenshot shows the 'Join Group' window in Microsoft Identity Manager. It includes a 'Summary' section with a list of requested groups, a 'Justification' text box containing the text 'Please add me to the Group, I am part of your team', and a 'Status' table.

Description	Date	Status
Joining group Joining Group Sample	3/22/2017 8:31:09 AM	Request not submitted.

Buttons for 'Submit' and 'Cancel' are visible at the bottom right of the window.

Custom Group Objects

Previously locked down to Group object type.

Required Attributes

- ExplicitMember, ComputedMember and Membership Locked

Justification supported on join

Create Binding

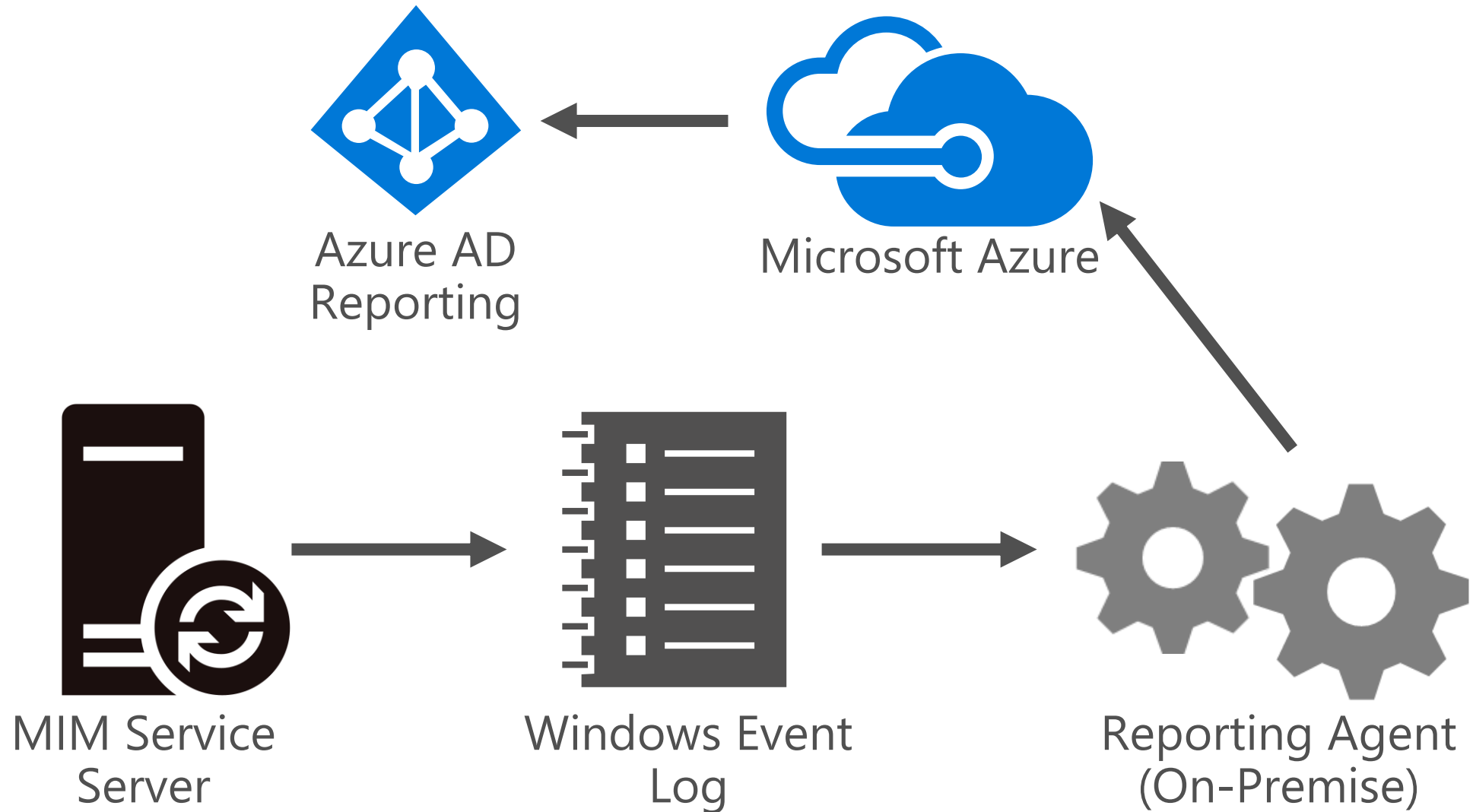
General | Attribute Override | Localization | Validation | Summary

Resource Type
* Custom Groups
The resource type that the attribute will be bound to.

Attribute Type
* Manually-managed Membership
The attribute type that will be bound to the selected resource type.

Required
Specifies that the attribute is required.

Azure Reporting



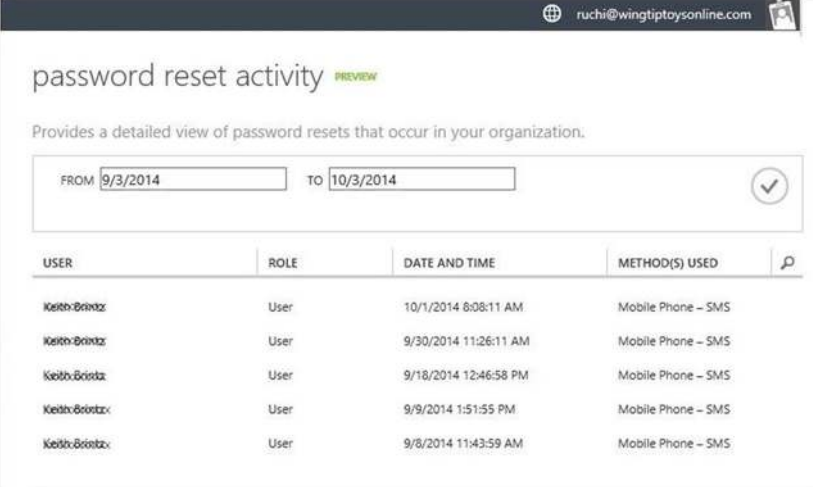
Reporting

MIM Reporting

- Group Membership Change
- Set Membership Change
- Group History
- Set History
- User History
- Request History
- Management Policy Rule History

MIM Hybrid Reporting

- Self Service Password Registration
- Self Service Password Reset
- Self Service Group Management



password reset activity PREVIEW

Provides a detailed view of password resets that occur in your organization.

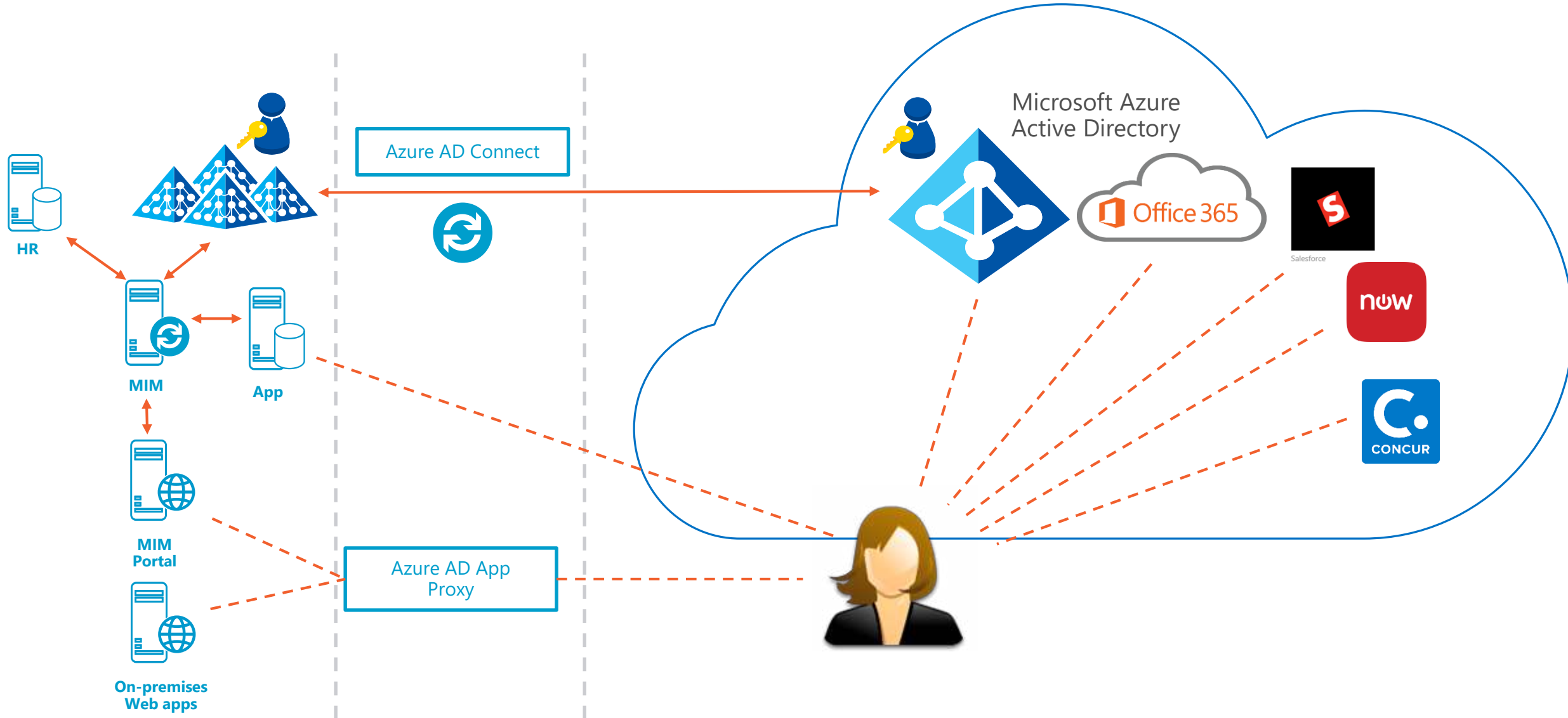
FROM 9/3/2014 TO 10/3/2014

USER	ROLE	DATE AND TIME	METHOD(S) USED	
Keith.Brinza	User	10/1/2014 8:08:11 AM	Mobile Phone - SMS	
Keith.Brinza	User	9/30/2014 11:26:11 AM	Mobile Phone - SMS	
Keith.Brinza	User	9/18/2014 12:46:58 PM	Mobile Phone - SMS	
Keith.Brinza	User	9/9/2014 1:51:55 PM	Mobile Phone - SMS	
Keith.Brinza	User	9/8/2014 11:43:59 AM	Mobile Phone - SMS	

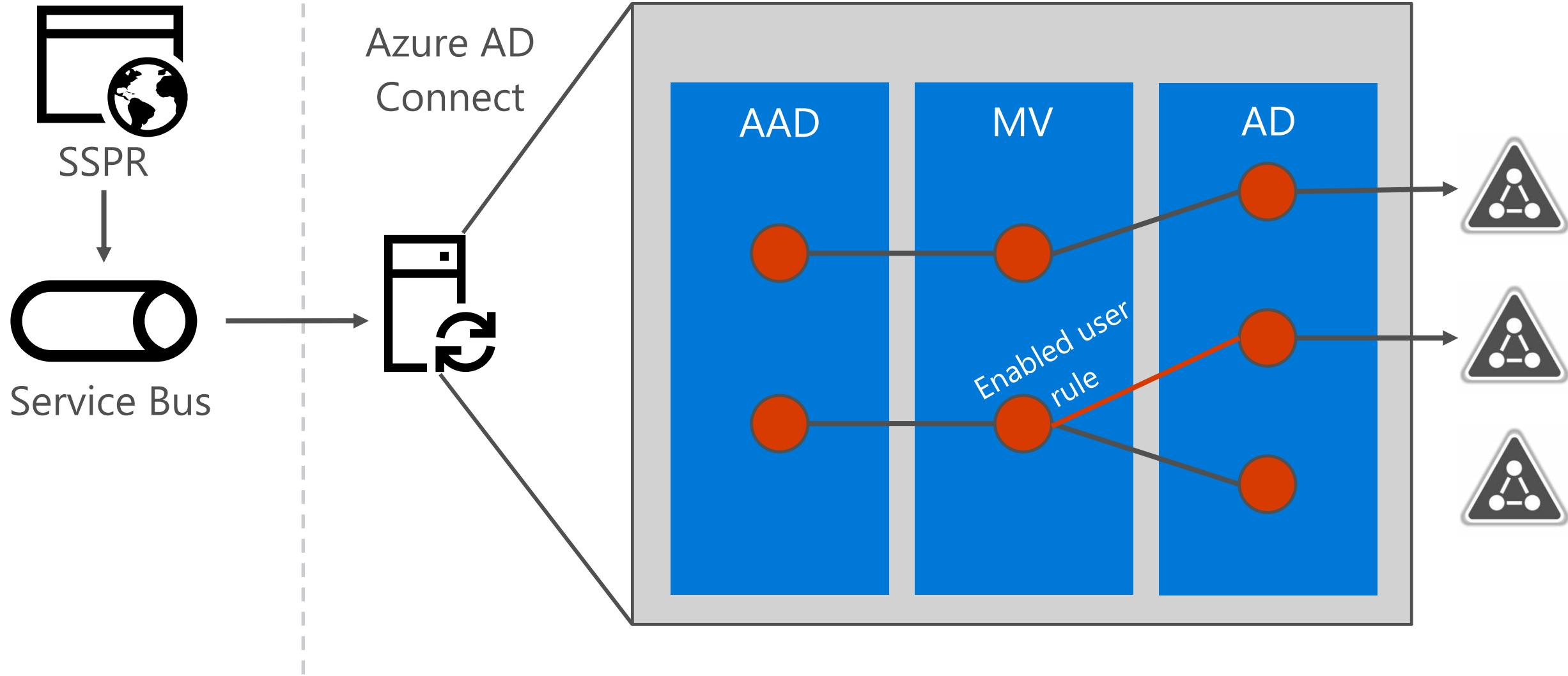


MIM Demo

MIM & Azure AD Premium

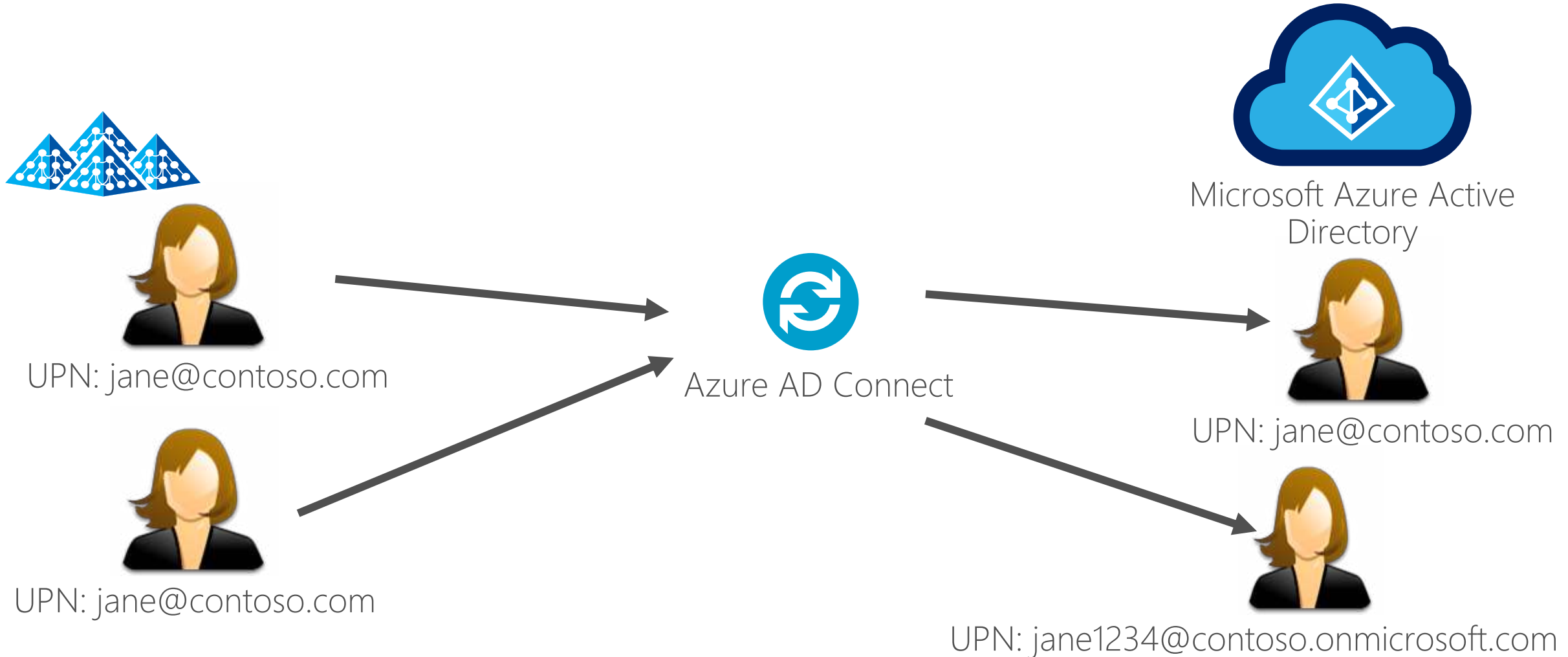


Password Write-Back

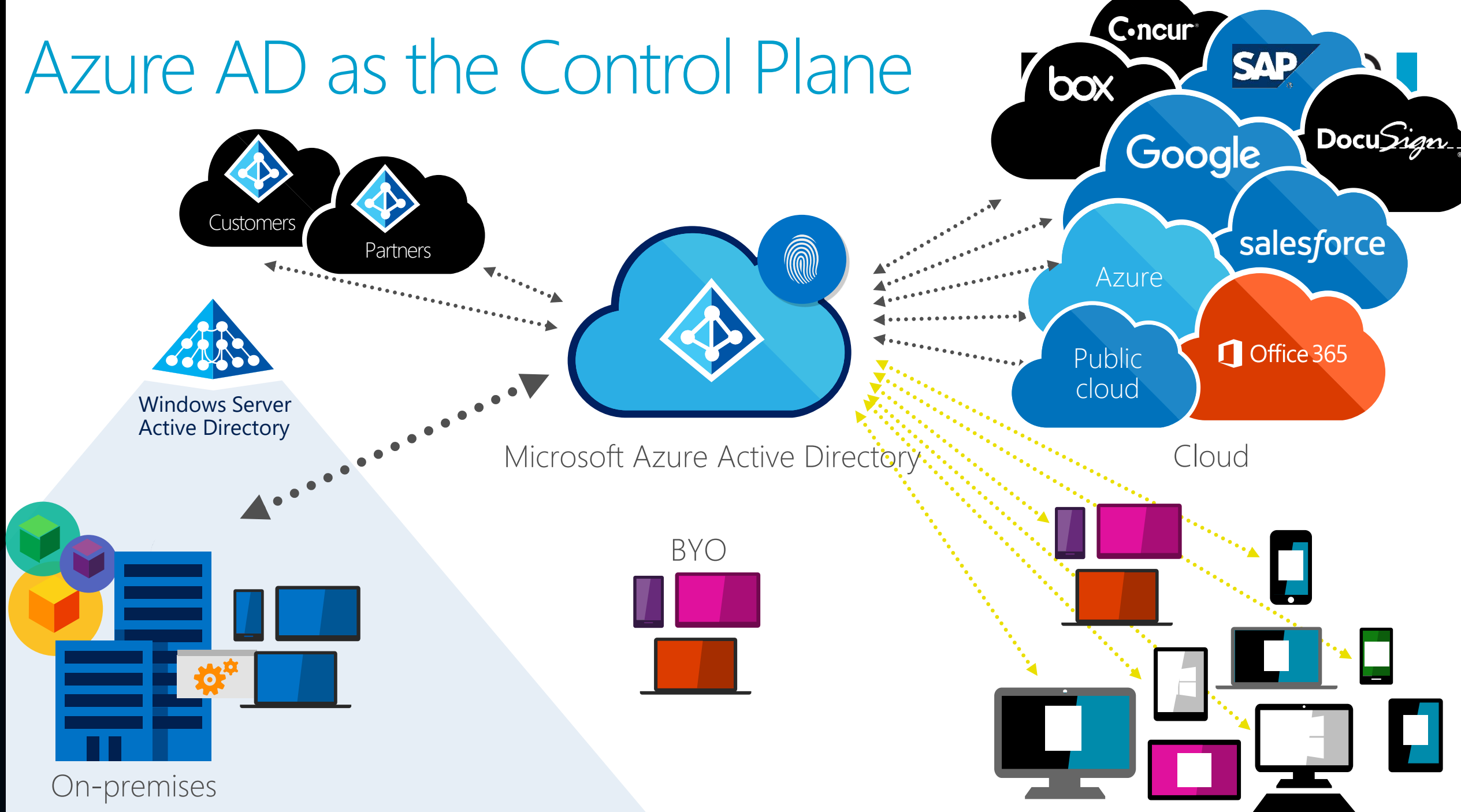


Duplicate Attribute Resiliency

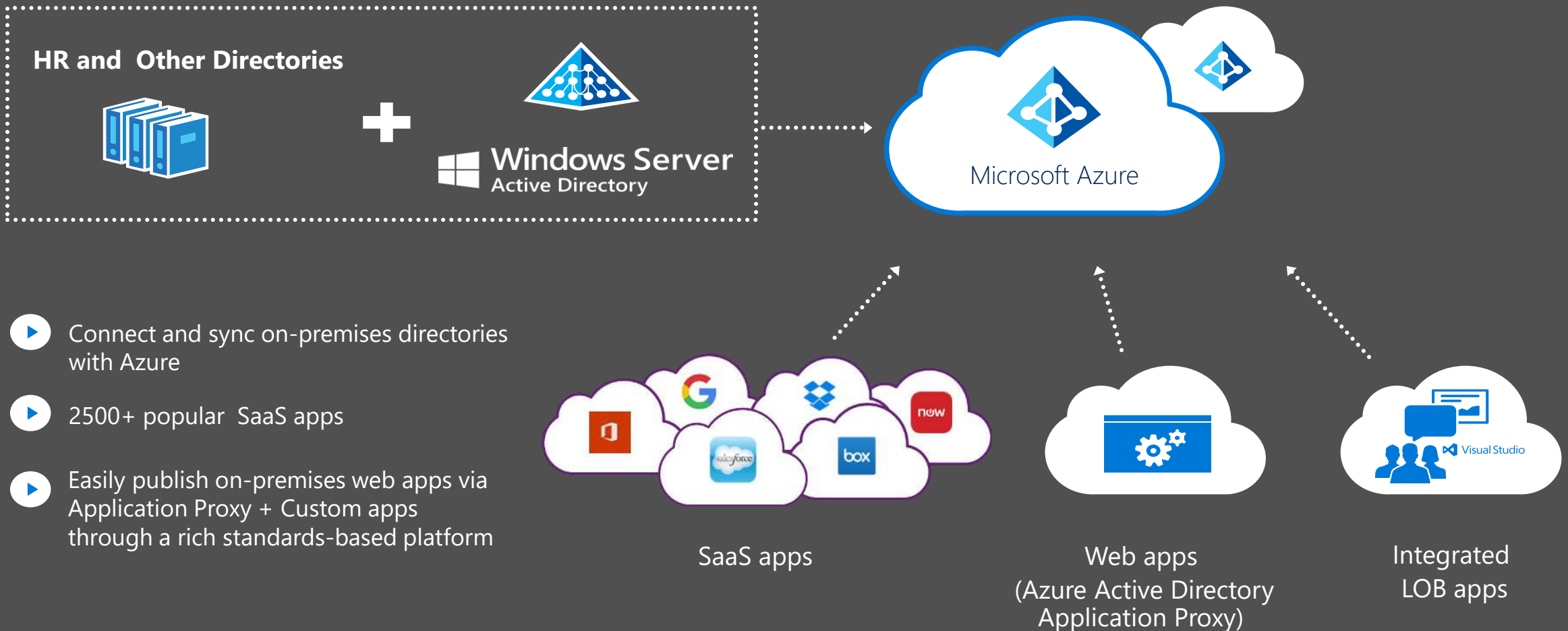
Reducing friction with userPrincipalName and proxyAddresses



Azure AD as the Control Plane



Cloud & On-Premises Applications



Manage Application Access with User Attributes

1. Create a security group
2. Configure the rule on the group
3. Assign the group to applications
4. Verify that the right users have access

NEW

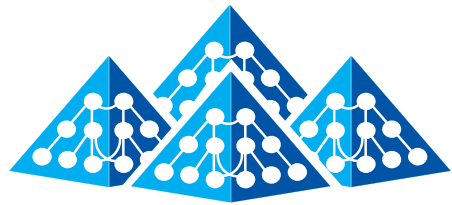
SALESFORCE

RULE
All users where...

USER NAME	USER NAME
Administrator	Administrator@oxford.com
Admin	Admin@oxford.com
Agent	Agent@oxford.com
...	...

Full Name	Alias	Username
...

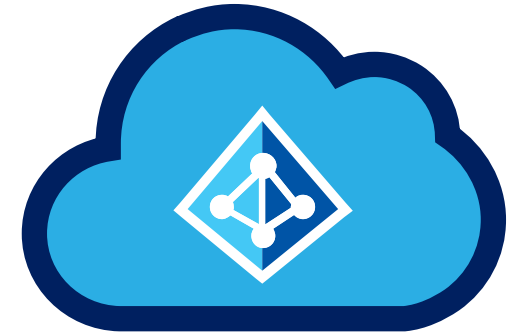
Extending Azure AD Schema



UPN: jane@contoso.com
givenName: Jane
sn: Smith
division: East Region



Azure AD Connect



Microsoft Azure Active Directory

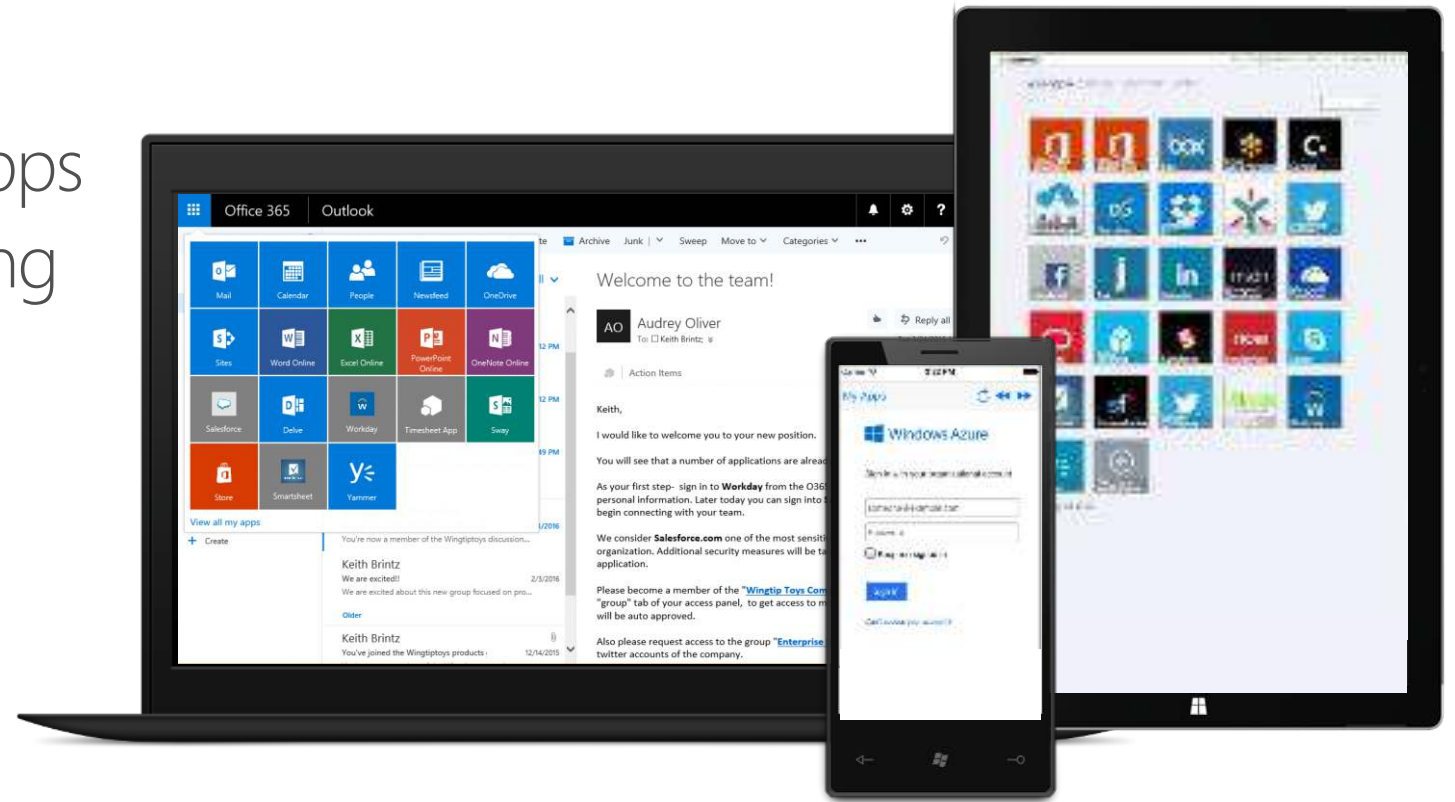


UPN: jane@contoso.com
givenName: Jane
sn: Smith
Extension_98k23h298kds3894kjdf93_division: East Region

Consistent Experience Across Applications

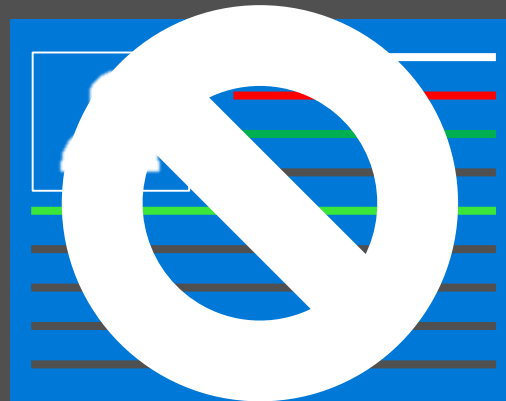
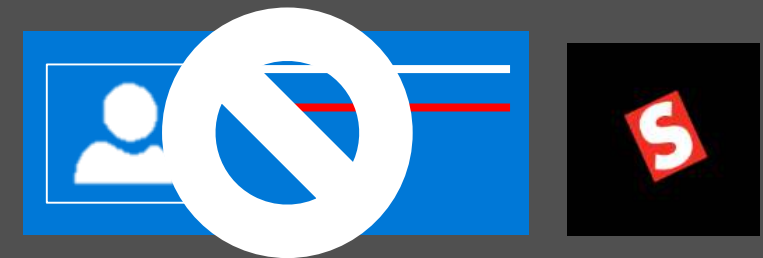


- Company branded, personalized application Access Panel:
<http://myapps.microsoft.com>
+ iOS and Android Mobile Apps
- Integrated O365 app launching (waffle)
- Manage your account and groups
- Self-service password reset
- Application access requests



Outbound Provisioning

- Automatically add, update, and disable user accounts in applications
- Configure attribute mappings per application
- Provisioning and usage reports





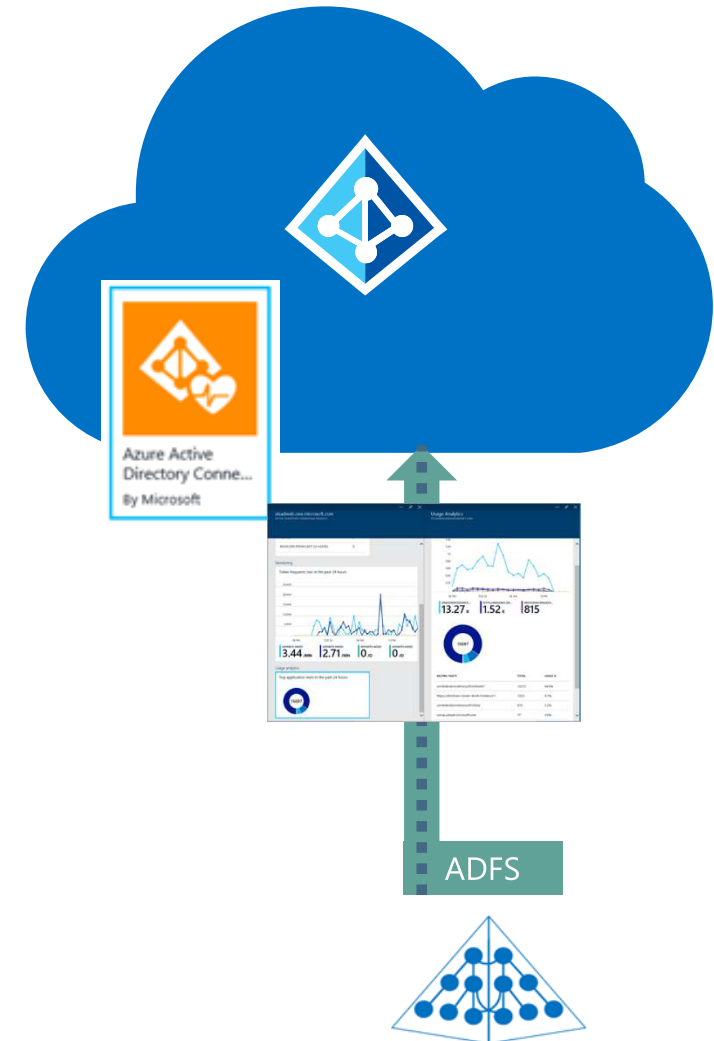
Azure AD & Salesforce

Demo

Azure AD Connect Health

Azure AD Connect and Connect Health

- Simplifies connecting and synchronizing on-premises directories with Azure AD
- Integrates with ADFS to provide federation when needed (domain-joined SSO, smart card or 3rd party MFA, etc.)
- Monitors health, performance, and usage of Azure AD Connect environment to ensure users have reliable access to on-premises and cloud resources from any device





Questions?