



Hongso Chae  
Solutions Consultant

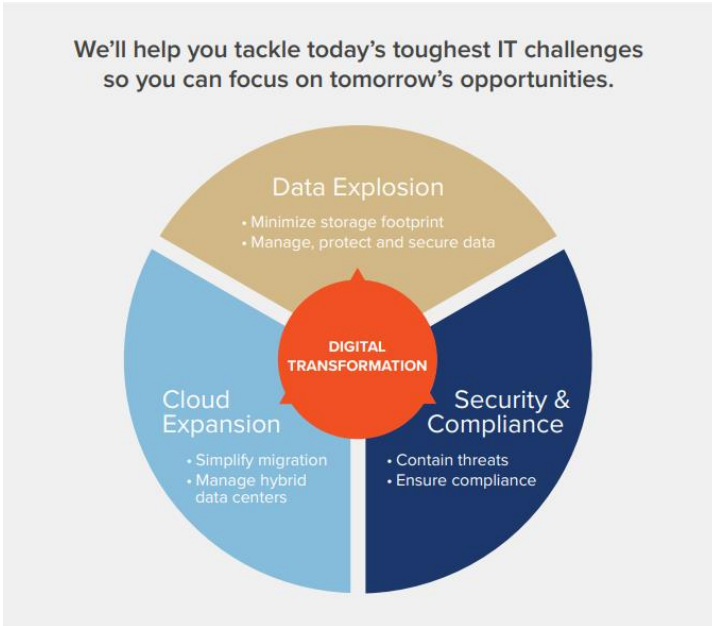
Active Directory 통합 관리 및 자동화 솔루션  
Active Roles 소개자료

Quest

# 회사 소개

Quest는 빠르게 변화하는 엔터프라이즈 IT 환경을 위한 소프트웨어 솔루션을 제공합니다.

Quest는 데이터 폭발, 클라우드 확장, 하이브리드 데이터 센터, 보안 위협 및 규정 요구사항으로 인한 문제를 단순화할 수 있도록 지원하며 Fortune 500 대 기업의 95%와 Global 1000 대 기업의 90%를 포함하여 100 개국 130,000여 기업에 글로벌 서비스를 제공하고 있습니다.



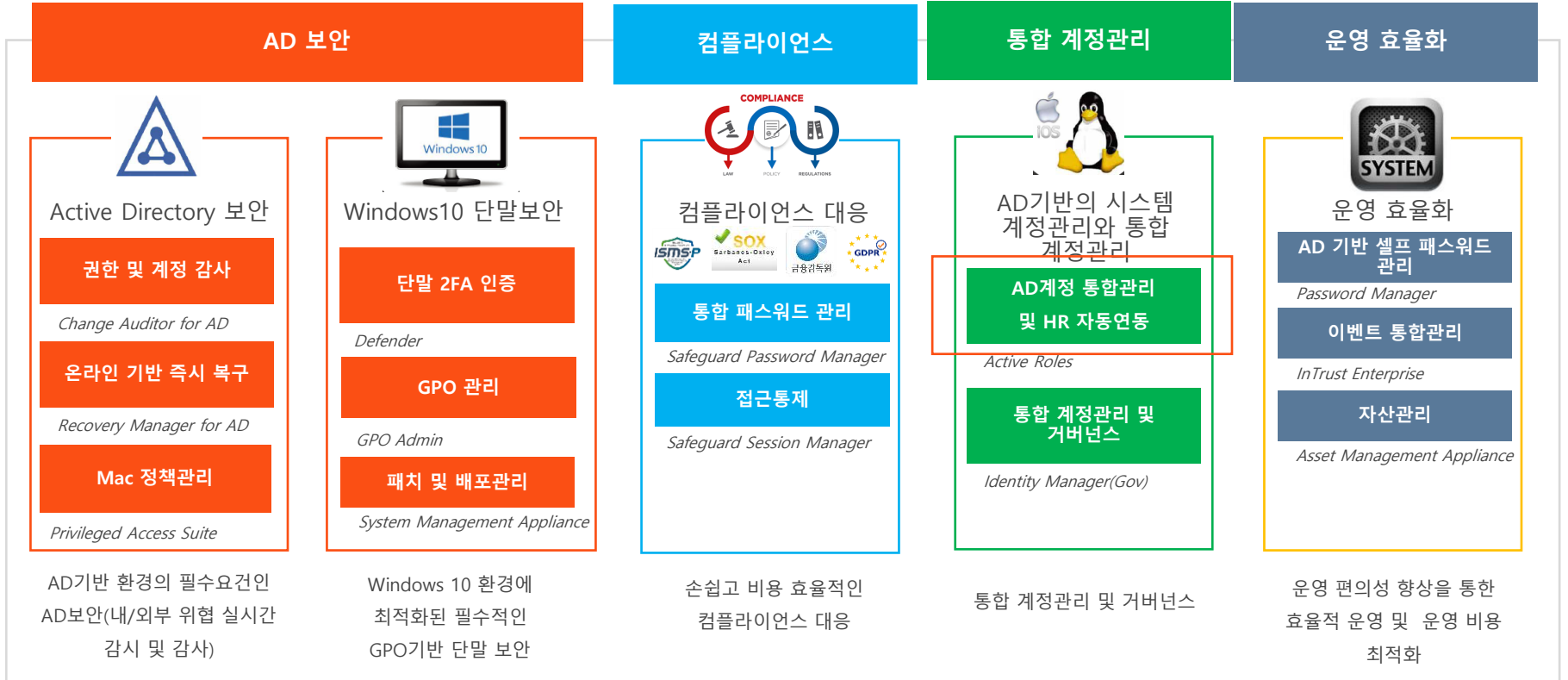
## 2년 연속 Microsoft 최우수 Global ISV



## 마이그레이션, 관리, 보안에 대한 통합 솔루션 제공



# 전체 Solution Overview



# Active Roles(ARS)는?

- AD관리 및 보안 영역의 마켓 리더
- Hybrid AD환경을 지원하는 최초의 관리 및 보안 툴
- 6천만개의 AD계정을 관리 및 보호
- 전세계 2,500개의 기업에서 사용 중
- 250명부터 80만개의 계정에 적용

[One Identity] provides AD monitoring and group management as part of its IAM portfolio. Active Roles provides a proxy-based architecture that provides views of AD permissions and can provision and delegate access to AD.

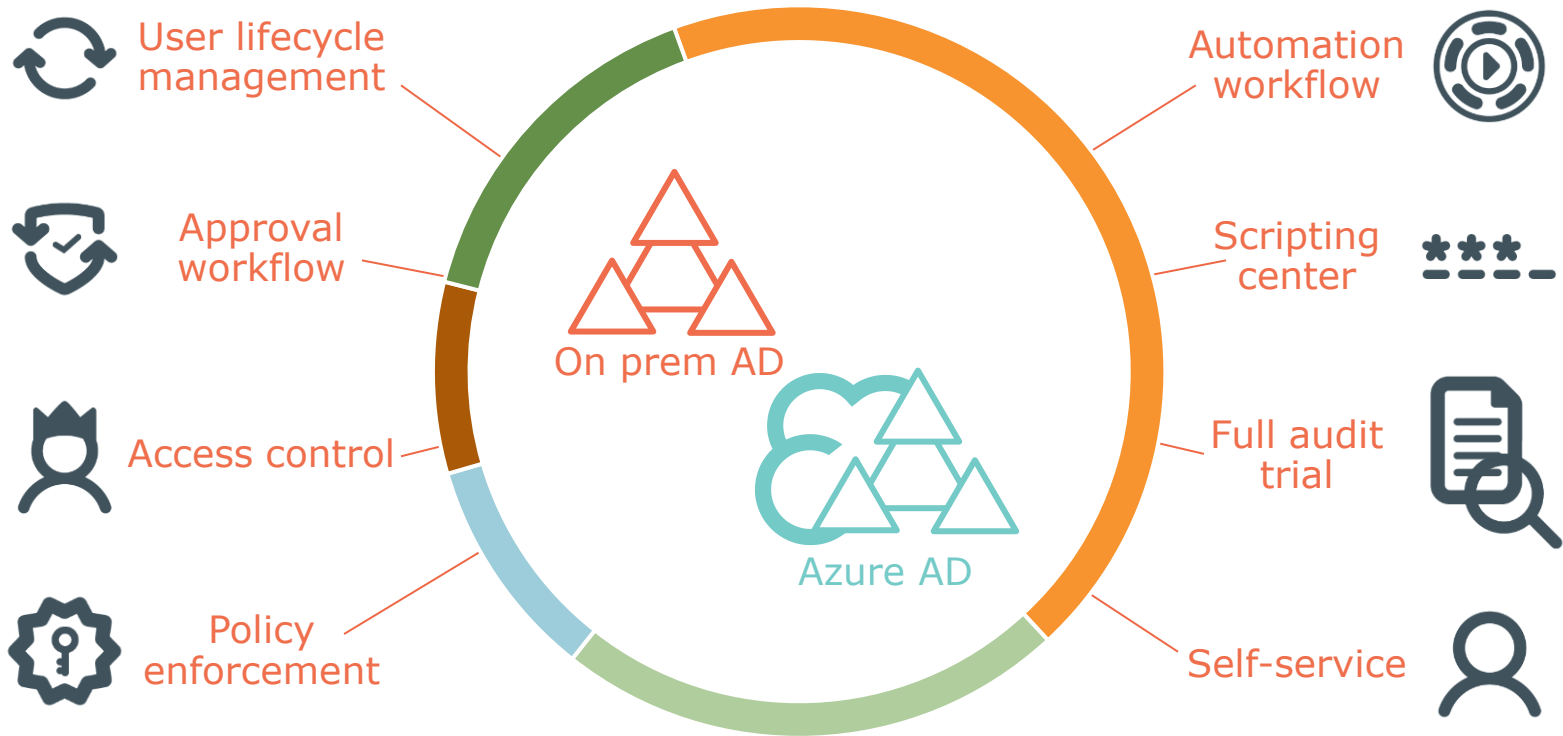
*Vendor Landscape: Active Directory Security and Governance Solutions*  
Forrester, January 5, 2016

Active Roles is the Swiss Army Knife of Active Directory. I can do so much with it, which makes my life so much easier

*Ryan Gevaza*  
Systems Analyst  
Moore Public Schools

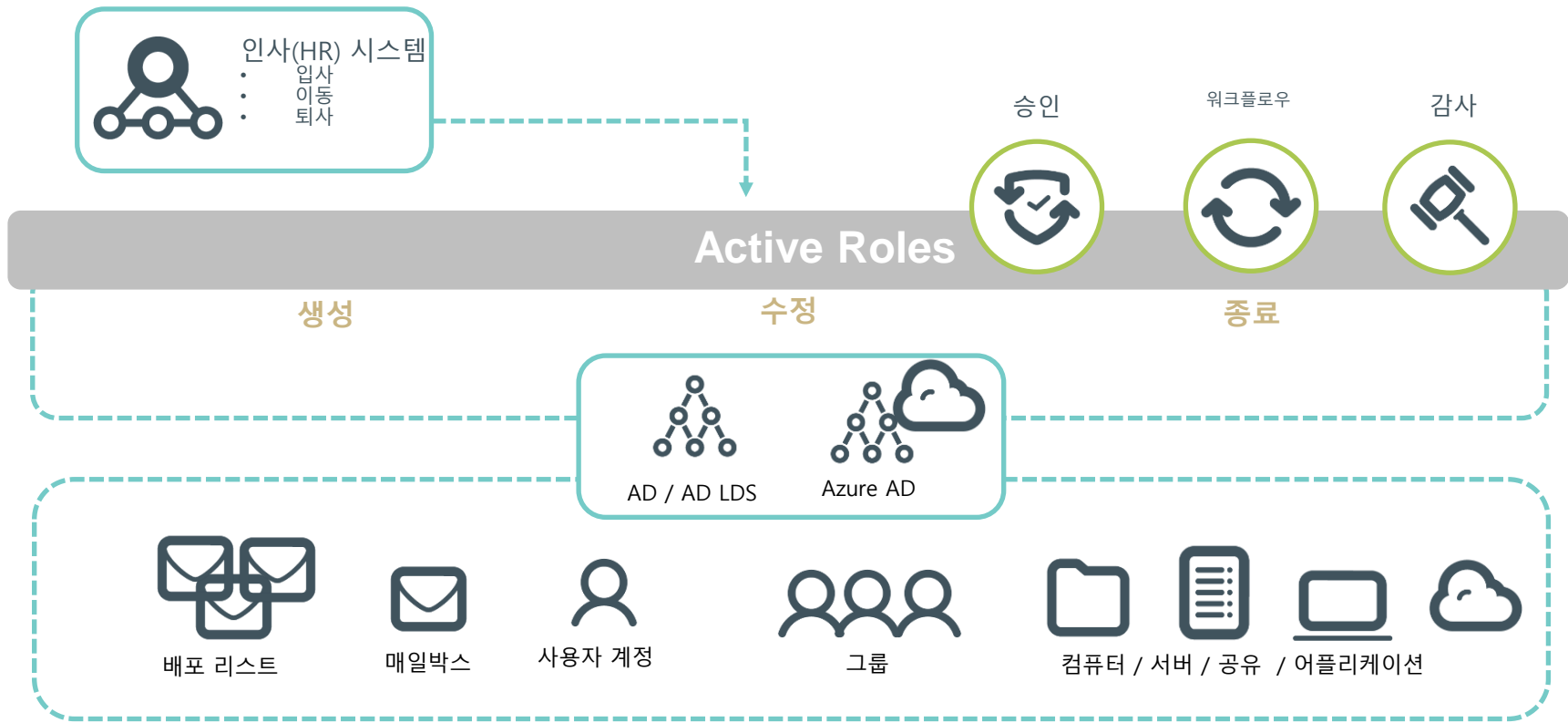


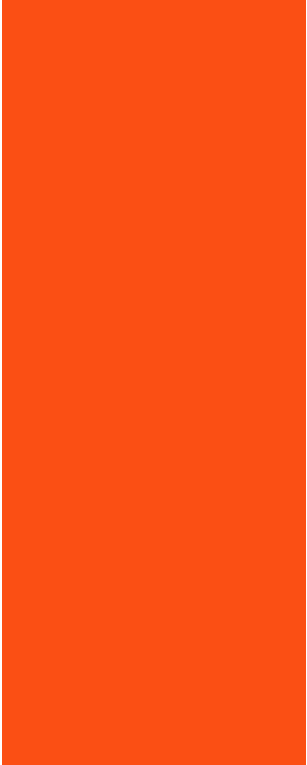
# Active Roles



# Virtual Firewall

# 자동화된 워크플로우 기반의 통합 AD계정관리

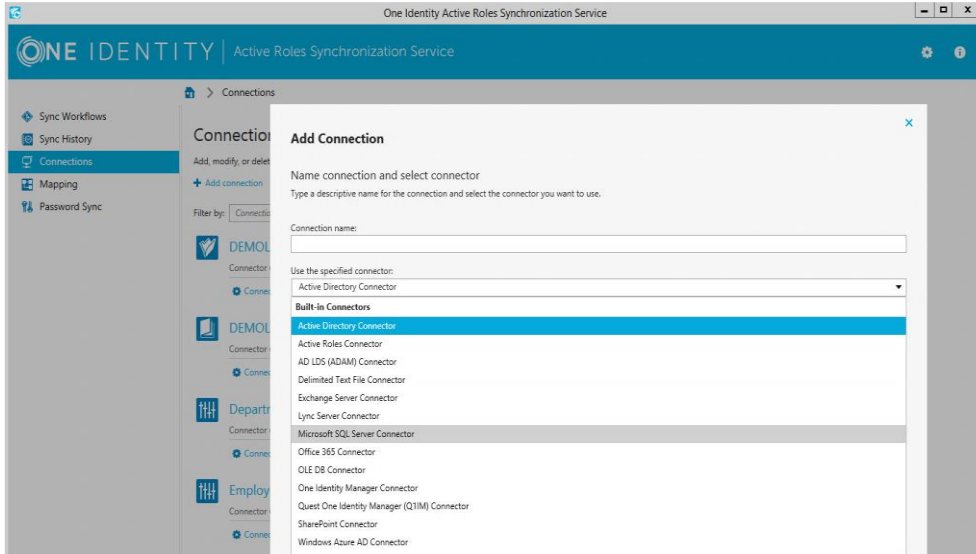




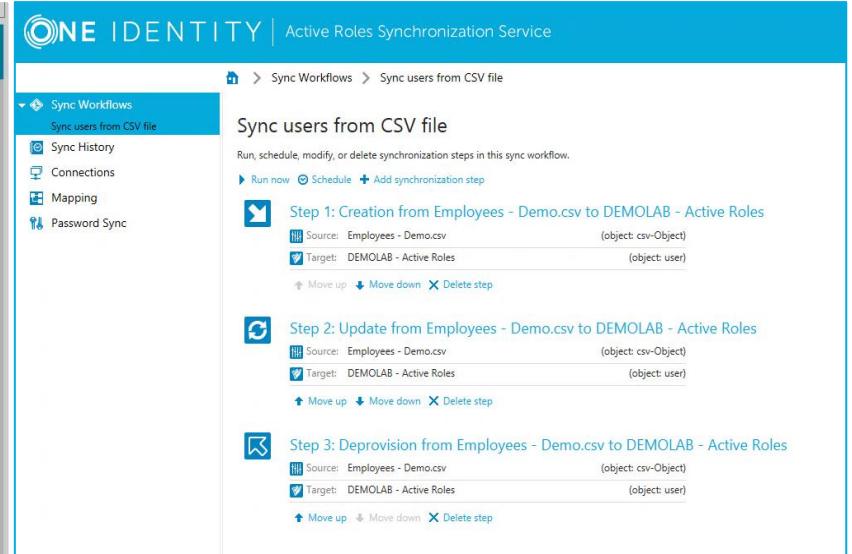
# 사용자 라이프사이클 관리

# 다양한 형태의 시스템과 계정 정보 동기화

다양한 형태의 시스템 연결 지원



동기화 설정을 통해서 자동으로 동기화 수행



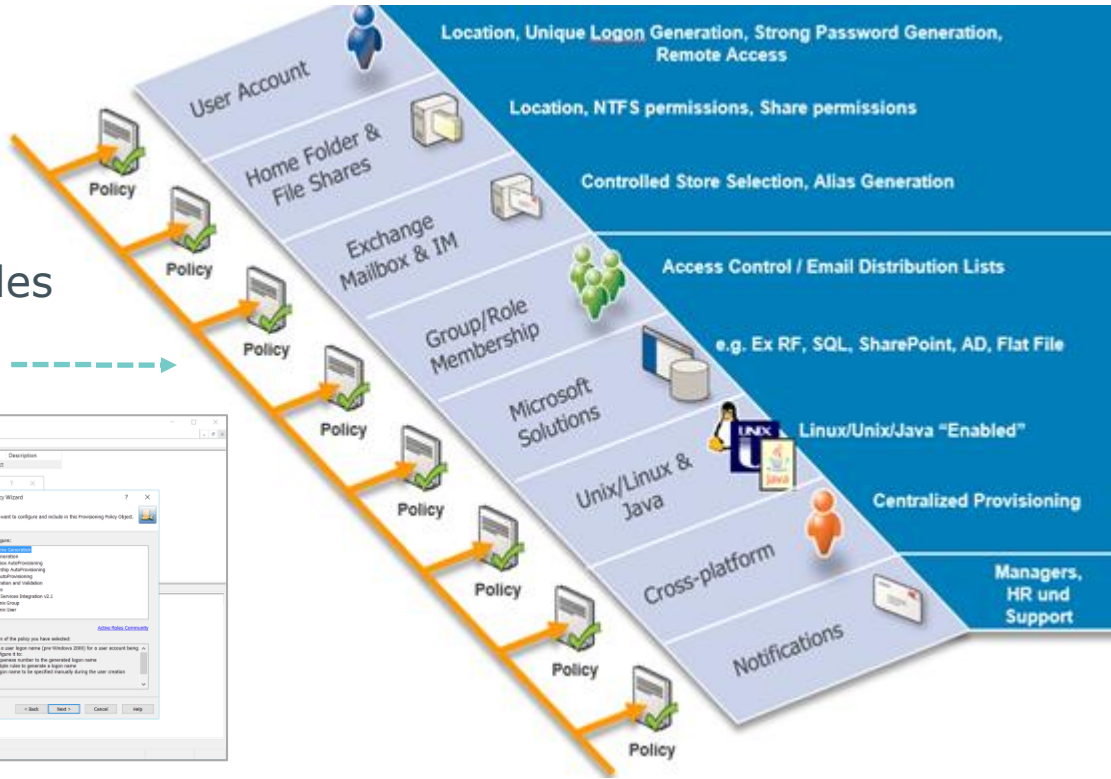
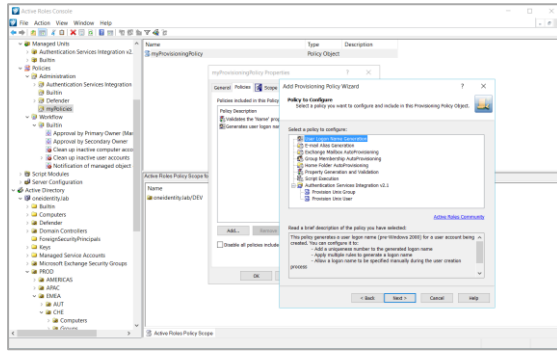


# 프로비저닝 - 자동화된 외부 계정 생성

인사(HR)시스템

- 입사
- 이동
- 퇴사

Active Roles

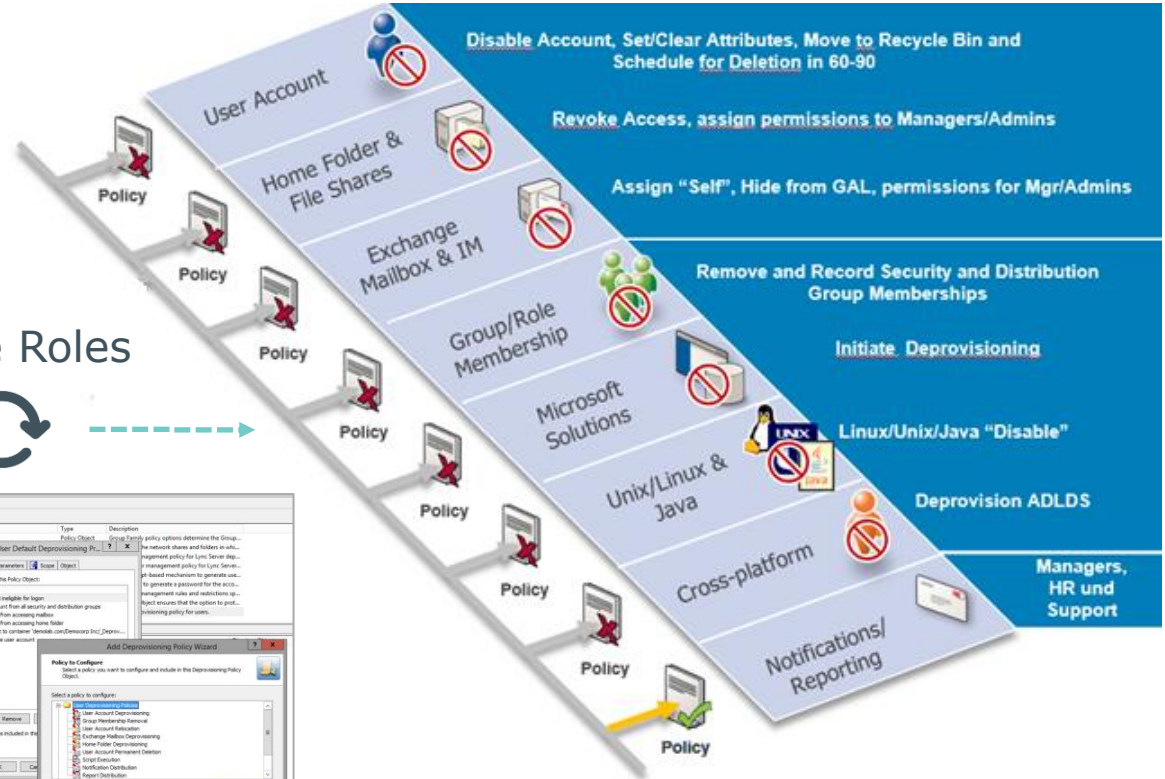
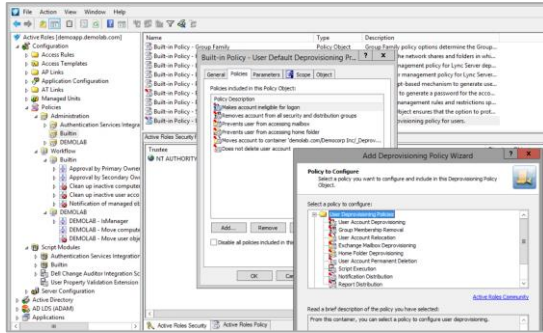


# 디프로비저닝 - 자동화된 외부 계정 삭제

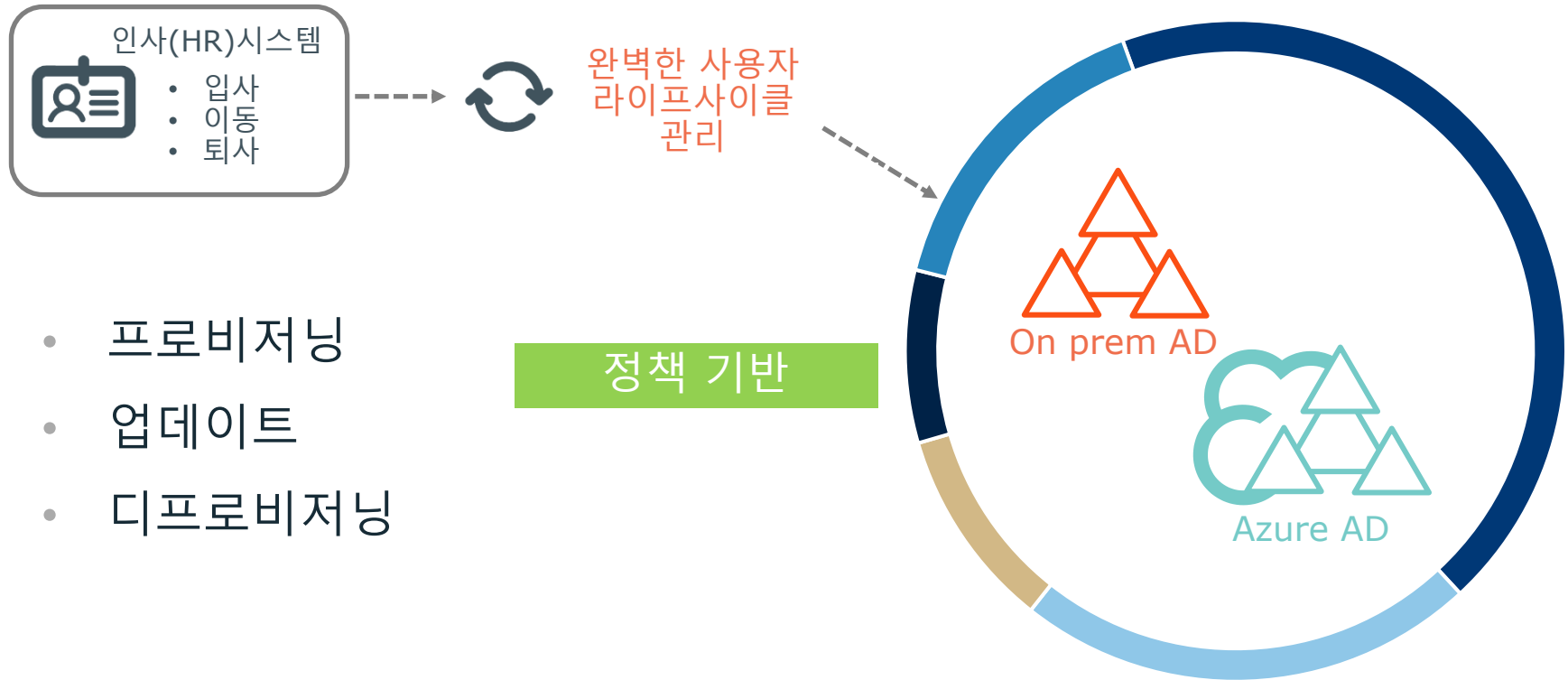
인사(HR)시스템

- 입사
- 이동
- 퇴사

Active Roles



# HR과 연동하여 정책 기반의 관리



# 스크립트를 통한 정책 확장

The image shows two overlapping windows from the 'Add Provisioning Policy Wizard'.

**Left Window: Script Module Identification**  
Specify a name and, optionally, description for the new script module. You also modify script language and creation container settings.

Name: PowerShell\_Mailbox\_deprovision

Script language: PowerShell

Description: Insert Script here!

Create in: Configuration/Script Modules

Buttons: < Back, Next >, Cancel

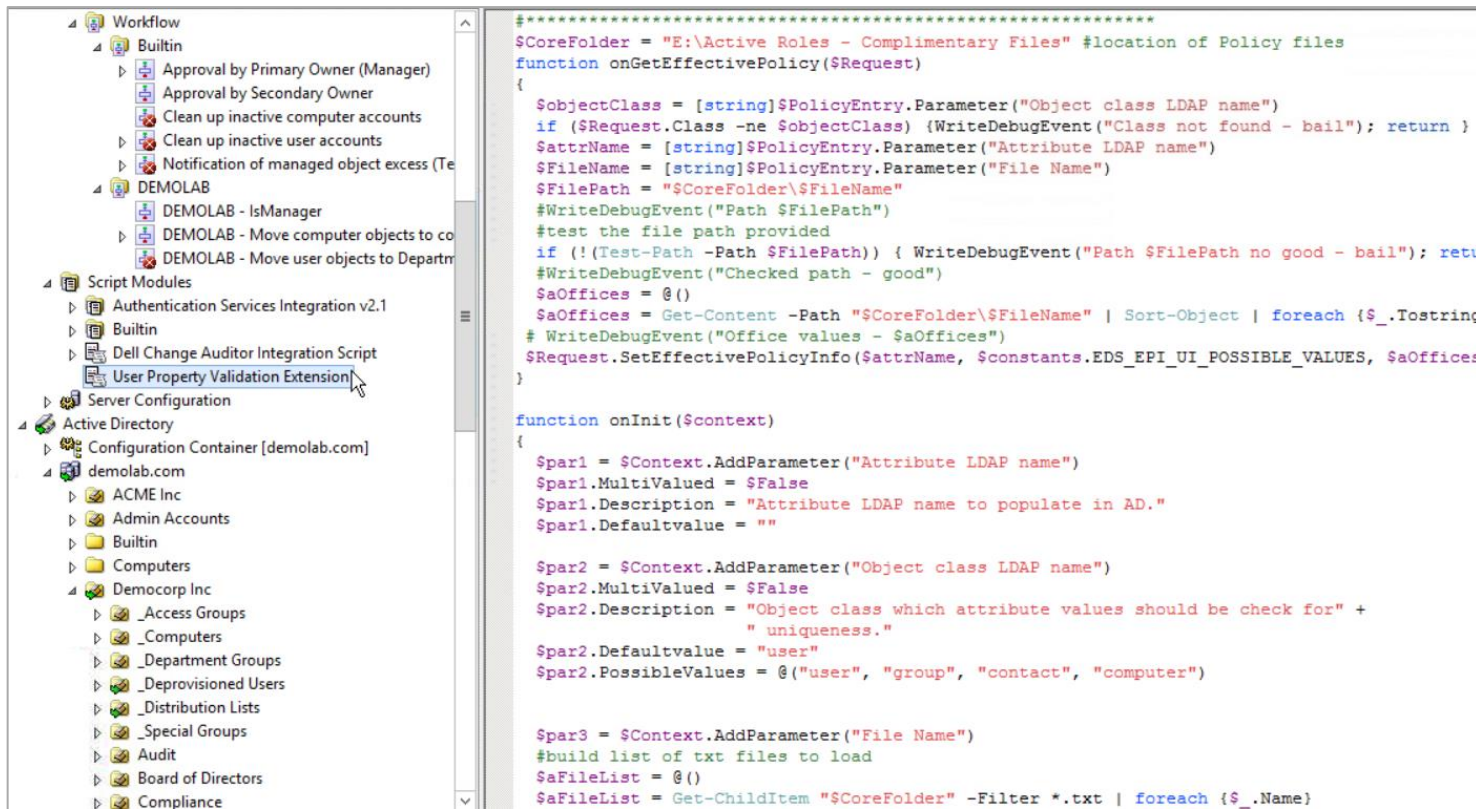
**Right Window: Event Handlers**  
Select event handler functions to add to the script module.

Event handler functions:

Event Handler Name	Description
<input type="checkbox"/> onPreCreate	In a script policy applied to a container, receives control ...
<input type="checkbox"/> onPostCreate	In a script policy applied to a container, receives control ...
<input type="checkbox"/> onPreDelete	Receives control upon a request to delete an object. En...
<input type="checkbox"/> onPostDelete	Receives control after a request to delete an object is c...
<input type="checkbox"/> onPreModify	Receives control upon a request to start changing objec...
<input type="checkbox"/> onPostModify	Receives control after a request to change object prope...
<input type="checkbox"/> onPreMove	In a script policy applied to a container, this function rec...
<input type="checkbox"/> onPostMove	In a script policy applied to a container, this function rec...
<input type="checkbox"/> onPreRename	Receives control upon a request to start renaming an ob...
<input type="checkbox"/> onPostRename	Receives control after a request to rename an object is ...
<input type="checkbox"/> onPreGet	Receives control upon a request to retrieve object prop...
<input type="checkbox"/> onPostGet	Receives control after a request to retrieve object prop...
<input type="checkbox"/> onPreSearch	Receives control upon a request to start a search. Enabl...
<input type="checkbox"/> onCheckPropertyVal...	Receives control upon a request to verify and validate t...

Buttons: < Back, Next >, Cancel, Help

# 스크립트 통합



The image shows a PowerShell script editor interface. On the left is a tree view of a workflow, and on the right is the script code.

**Workflow Tree (Left):**

- Workflow
  - Builtin
    - Approval by Primary Owner (Manager)
    - Approval by Secondary Owner
    - Clean up inactive computer accounts
    - Clean up inactive user accounts
    - Notification of managed object excess (Te...
  - DEMOLAB
    - DEMOLAB - IsManager
    - DEMOLAB - Move computer objects to co...
    - DEMOLAB - Move user objects to Departm...
  - Script Modules
    - Authentication Services Integration v2.1
    - Builtin
    - Dell Change Auditor Integration Script
    - User Property Validation Extension
  - Server Configuration
  - Active Directory
    - Configuration Container [demolab.com]
  - demolab.com
    - ACME Inc
    - Admin Accounts
    - Builtin
    - Computers
    - Democorp Inc
      - \_Access Groups
      - \_Computers
      - \_Department Groups
      - \_Deprovisioned Users
      - \_Distribution Lists
      - \_Special Groups
      - Audit
      - Board of Directors
      - Compliance

```
*****  
$CoreFolder = "E:\Active Roles - Complimentary Files" #location of Policy files  
function onGetEffectivePolicy($Request)  
{  
    $ObjectClass = [string]$PolicyEntry.Parameter("Object class LDAP name")  
    if ($Request.Class -ne $ObjectClass) {WriteDebugEvent("Class not found - bail"); return }  
    $AttrName = [string]$PolicyEntry.Parameter("Attribute LDAP name")  
    $FileName = [string]$PolicyEntry.Parameter("File Name")  
    $FilePath = "$CoreFolder\$FileName"  
    #WriteDebugEvent("Path $FilePath")  
    #test the file path provided  
    if (!(Test-Path -Path $FilePath)) { WriteDebugEvent("Path $FilePath no good - bail"); return }  
    #WriteDebugEvent("Checked path - good")  
    $aOffices = @()  
    $aOffices = Get-Content -Path "$CoreFolder\$FileName" | Sort-Object | foreach {$_.Tostring}  
    # WriteDebugEvent("Office values - $aOffices")  
    $Request.SetEffectivePolicyInfo($AttrName, $constants.EDS_EPI_UI_POSSIBLE_VALUES, $aOffices)  
}  
  
function onInit($context)  
{  
    $par1 = $Context.AddParameter("Attribute LDAP name")  
    $par1.MultiValued = $False  
    $par1.Description = "Attribute LDAP name to populate in AD."  
    $par1.Defaultvalue = ""  
  
    $par2 = $Context.AddParameter("Object class LDAP name")  
    $par2.MultiValued = $False  
    $par2.Description = "Object class which attribute values should be check for" +  
        " uniqueness."  
    $par2.Defaultvalue = "user"  
    $par2.PossibleValues = @("user", "group", "contact", "computer")  
  
    $par3 = $Context.AddParameter("File Name")  
    #build list of txt files to load  
    $aFileList = @()  
    $aFileList = Get-ChildItem "$CoreFolder" -Filter *.txt | foreach {$_.Name}
```

02

# 워크플로우와 자동화

# 워크플로우 지원

- 작업에 대한 요청을 승인처리
- GUI기반의 워크플로우 엔진 제공을 통한 손쉬운 워크플로우 생성
- 워크플로우 기반의 관리를 통해서 프로세스의 자동화

Notification of managed object excess (Template)

By copying this template workflow, you can create an automation workflow that checks the number of managed objects in a certain area and sends e-mail notification if that number exceeds a certain threshold. Use the "Copy" command on this template workflow to create a new workflow definition, and then adjust the workflow parameters and configure the notification activity in the newly created workflow definition. You cannot make changes to the template workflow.

**⚠ This workflow is disabled.**

Drag activities to the surface on the right.

Type a name to find

Basic activities

- Notification
- Script
- If-Else
- Stop/Break
- Add Report Section

Object management

- Search
- Stop Search

Workflow options and start conditions

```
graph TD; Start(( )) --> Check[Check object count]; Check -- "Count exceeds the threshold" --> Send[Send notification]; Check -- "No excess" --> Drop[Drop Activities Here]; Send --> End(( )); Drop --> End;
```

Active Roles Community

Run Workflow Save Changes Discard Changes

# 타 시스템과의 자동 동기화 기반 연동

## Step 1: Creation from Employees - Demo.csv to DEMOLAB - Active Roles

General Options

Source

Target

Creation Rules

Step Handlers

### Initial Attribute Population Rules

#### Employees - Demo.csv

#### DEMOLAB - Active Roles

EmployeeID	⇒	employeeID
Department	⇒	department
FirstName	⇒	givenName
LastName	⇒	sn
UserType	⇒	edsvaUserType
%<FirstName>.%<LastName>	⇒	mailNickname
<Generated by PowerShell script>	⇒	manager

Forward Sync Rule...

Edit...

Remove

More...

> Initial Password

> User Account Options

패스워드에 대한 동기화도 포함

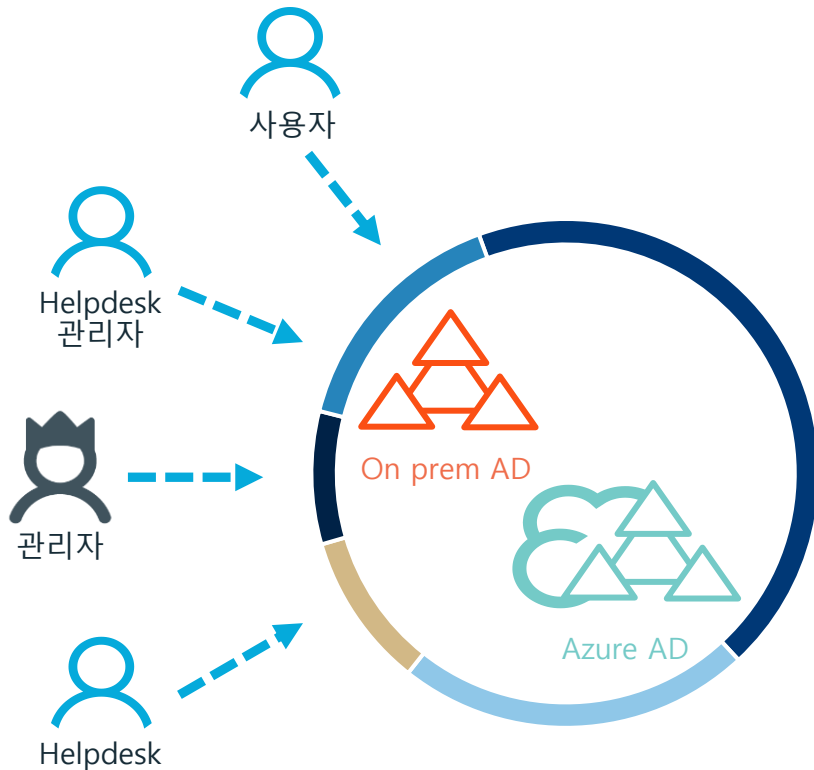


03

## 보안 및 예방관리

# Active Directory의 가상 방화벽을 제고

- 최소 권한 관리자
- 관리자 계정 노출 위험을 제거
- 보안 위협을 사전에 예방하는 관리 가능
- 모든 작업에 대한 Access를 체크



# 정책 시행

Hunter Patrick Properties

Organization Managed By Exchange General Mail Flow Settings

Mailbox Settings E-mail Addresses Managed Resources

Additional Account Info Published Certificates

Mailbox Features Exchange Advanced Member Of Dial-in

Environment Sessions Remote Control

Terminal Services Profile Object Administration Picture

General Unix Account Address Account Profile Telephones

Hunter Patrick

First name: Patrick Initials:

Last name: Hunter

Display name: Hunter Patrick

Description:

Office:

Aliso Viejo  
Chicago  
Cologne  
Edinburgh  
Halifax  
Kanata  
Kazan  
London  
Maidenhead  
Moscow  
Phoenix  
St. Petersburg  
Warrington

Telephone number:

E-mail:

Web page:

OK Cancel Apply Help

Display명은 Lastname Firstname으로 나타나야 한다.

사무실은 리스트에 나타난 것만 선택해야 한다.

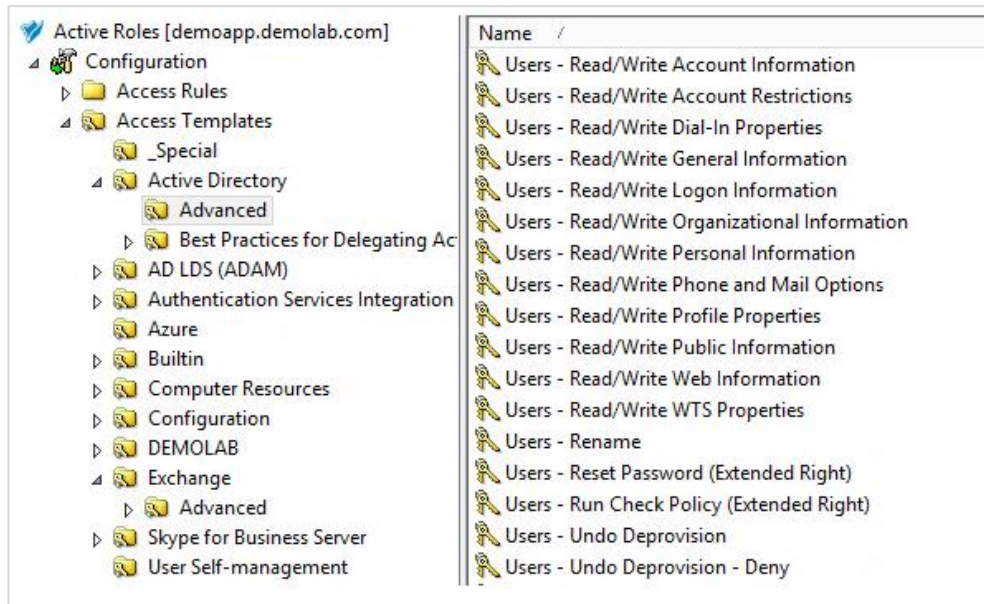
전화 번호는 "+82 01# #### #####"형태가 되어야 한다.

E-mail은 @quest.com으로 "Firstname.Lastname"형태로 구성되어야 한다.

정책을 사전에 정의하여 사용자로 인한 문제 및 정책 위배 문제를 사전에 제거

# 관리자 권한 노출 위험성을 제거

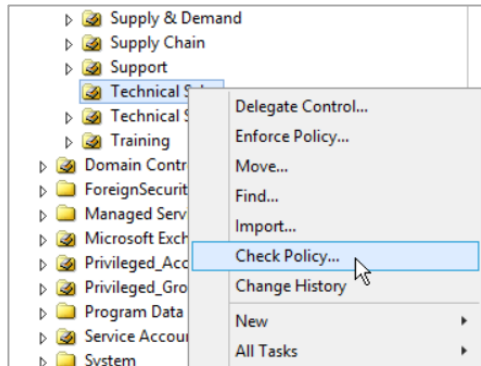
- Active Directory / Azure
- Exchange / Office 365
- SharePoint / Online
- Skype for Business



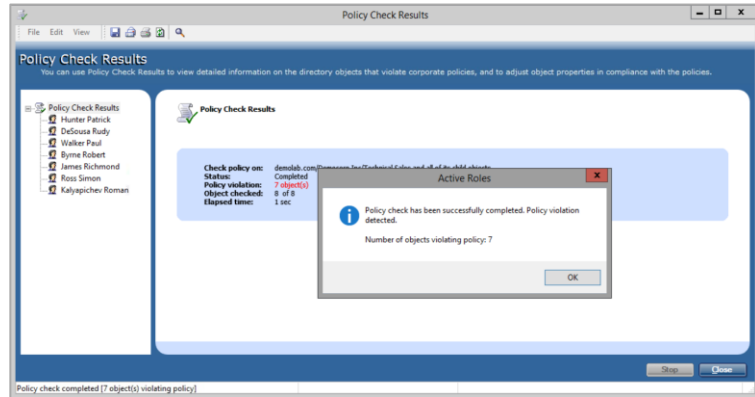
Name
Users - Read/Write Account Information
Users - Read/Write Account Restrictions
Users - Read/Write Dial-In Properties
Users - Read/Write General Information
Users - Read/Write Logon Information
Users - Read/Write Organizational Information
Users - Read/Write Personal Information
Users - Read/Write Phone and Mail Options
Users - Read/Write Profile Properties
Users - Read/Write Public Information
Users - Read/Write Web Information
Users - Read/Write WTS Properties
Users - Rename
Users - Reset Password (Extended Right)
Users - Run Check Policy (Extended Right)
Users - Undo Deprovision
Users - Undo Deprovision - Deny

세분화된 권한을 적절한 담당자에게 할당하여 모든 권한을 갖는 관리자 계정으로 작업 하지 못하도록 관리

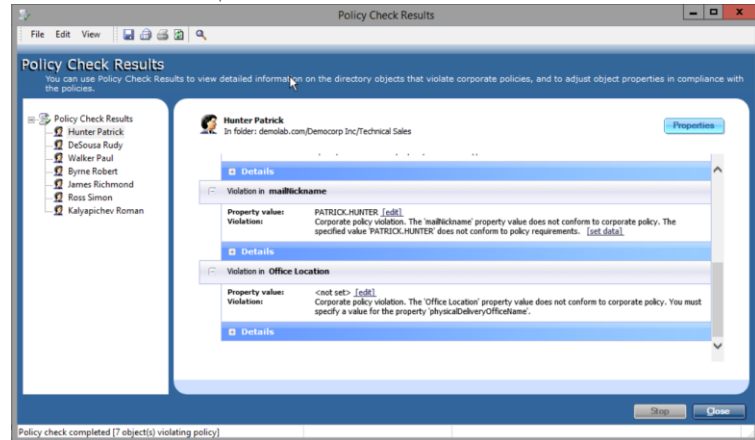
# 정책 검증



정책 위반 체크 수행



정책 위반 내역 제공



# 임시 사용자(그룹) 관리

The screenshot displays the Active Roles management console. A 'Select Object' dialog box is open, showing a list of objects with 'AG\_CAM\_Admins' selected. Overlaid on this is a 'Temporal Membership Settings' dialog box. The settings dialog has a warning icon and the text: 'Choose when to add or remove the selected object from the selected group.' It contains two sections: 'Add to the group:' with options for 'Already added', 'On this date: 11/6/2016 21:00', and 'Remove from the group:' with options for 'Never' and 'On this date: 11/7/2016 21:00'. An orange callout box at the bottom of the settings dialog contains the text '지정된 기간에만 권한 할당' (Grant rights only for the specified period). The background shows the 'Active Roles' sidebar and a list of roles.

Temporal Membership Settings

Choose when to add or remove the selected object from the selected group.

Add to the group:

- Already added
- On this date: 11/6/2016 21:00

Remove from the group:

- Never
- On this date: 11/7/2016 21:00

OK Cancel

지정된 기간에만 권한 할당

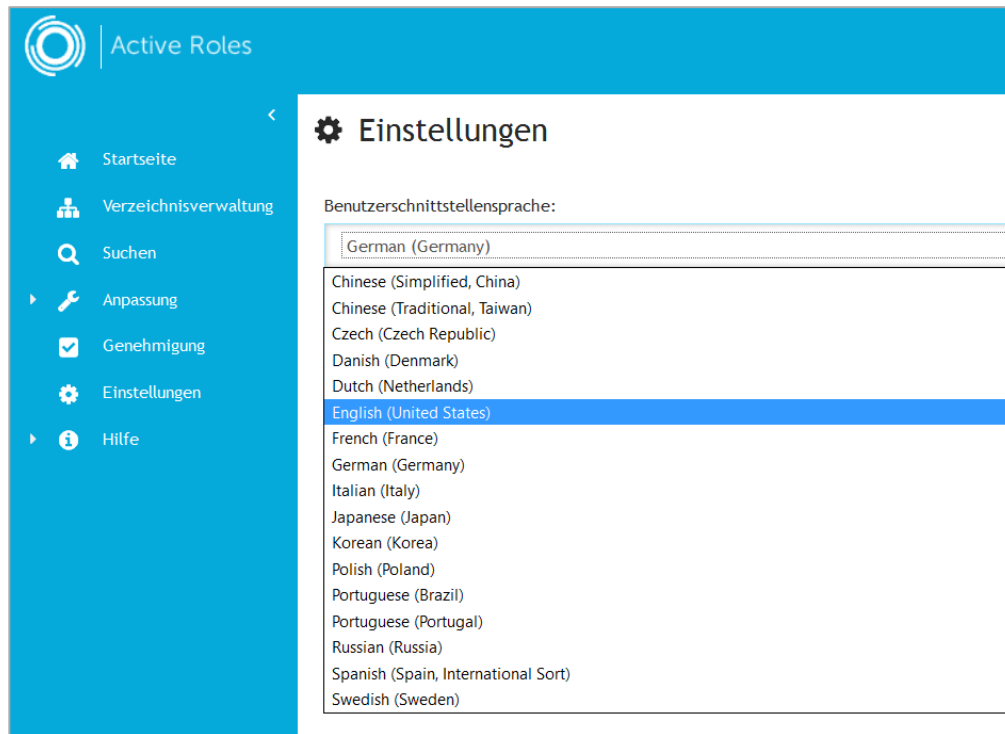
OK Cancel

04

# 통합 관리

# 다양한 Browser와 언어지원(한국어 지원)

- Internet Explorer
- Edge
- Firefox
- Chrome





# 모든 변경 히스토리 내역 제공

The screenshot displays the Active Roles user profile page for Reto Bachmann - Zuerich. The interface includes a navigation sidebar on the left with options like Home, Directory Management, Search, Customization, Approval, Settings, and Help. The main content area shows the user's profile and a list of change operations.

**Active Roles** | Administrator

**Views** | **Tree**

**Built-in**

- Active Directory
- Managed Units
- AD LDS
- Automation Workflows

**Personal**

You have no personal Views.

### Reto Bachmann - Zuerich

Active Directory / oneidentity.lab / PROD / EMEA / CHE / Users

Previous page | Page 1 | Next page

**Operation summary**

**Change User** | Operation ID: 1-156

Name: Reto Bachmann - Zuerich (oneidentity.lab/PROD/EMEA/CHE/Users) | Requested: 11/6/2016 8:10:13 PM (UTC)

Reason: <none> | Requested by: ONEIDENTITY\Administrator

Completed: 11/6/2016 8:10:14 PM (UTC)

Property	Old value	New value
Telephone Number (telephoneNumber)	<not set>	'+41791234567'

Status: COMPLETED

**Change User** | Operation ID: 1-152

Name: Reto Bachmann - Zuerich (oneidentity.lab/PROD/EMEA/CHE/Users) | Requested: 11/6/2016 8:06:53 PM (UTC)

Reason: <none> | Requested by: ONEIDENTITY\Administrator

Completed: 11/6/2016 8:07:03 PM (UTC)

Property	Old value	New value
edsaAdminGroup (edsaAdminGroup)	'Exchange Administrative Group (FYDIBOHF23SPDLT)'	'CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=OneIdentity,CN=Microsoft Exchange,CN=Ser ...'
Create User Mailbox (edsaCreateMsExchMailbox)	<not set>	'true'

Status: COMPLETED

# ARS의 작업 내역을 윈도우 이벤트로 제공

The screenshot displays the Windows Event Viewer application. The left-hand pane shows the tree view with 'Active Roles Admin Service' selected under 'Applications and Services Logs'. The main pane shows a list of events for this service, with one event selected and its details expanded.

**Active Roles Admin Service** Number of events: 36,971 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	6/26/2017 2:57:16 PM	ARAdminSvc	1517	ObjectCreate
Information	6/26/2017 2:57:16 PM	ARAdminSvc	1517	ObjectCreate
Information	6/26/2017 2:57:16 PM	ARAdminSvc	1517	ObjectCreate
Information	6/26/2017 2:57:16 PM	ARAdminSvc	1517	ObjectCreate
Information	6/26/2017 2:57:16 PM	ARAdminSvc	1517	ObjectCreate

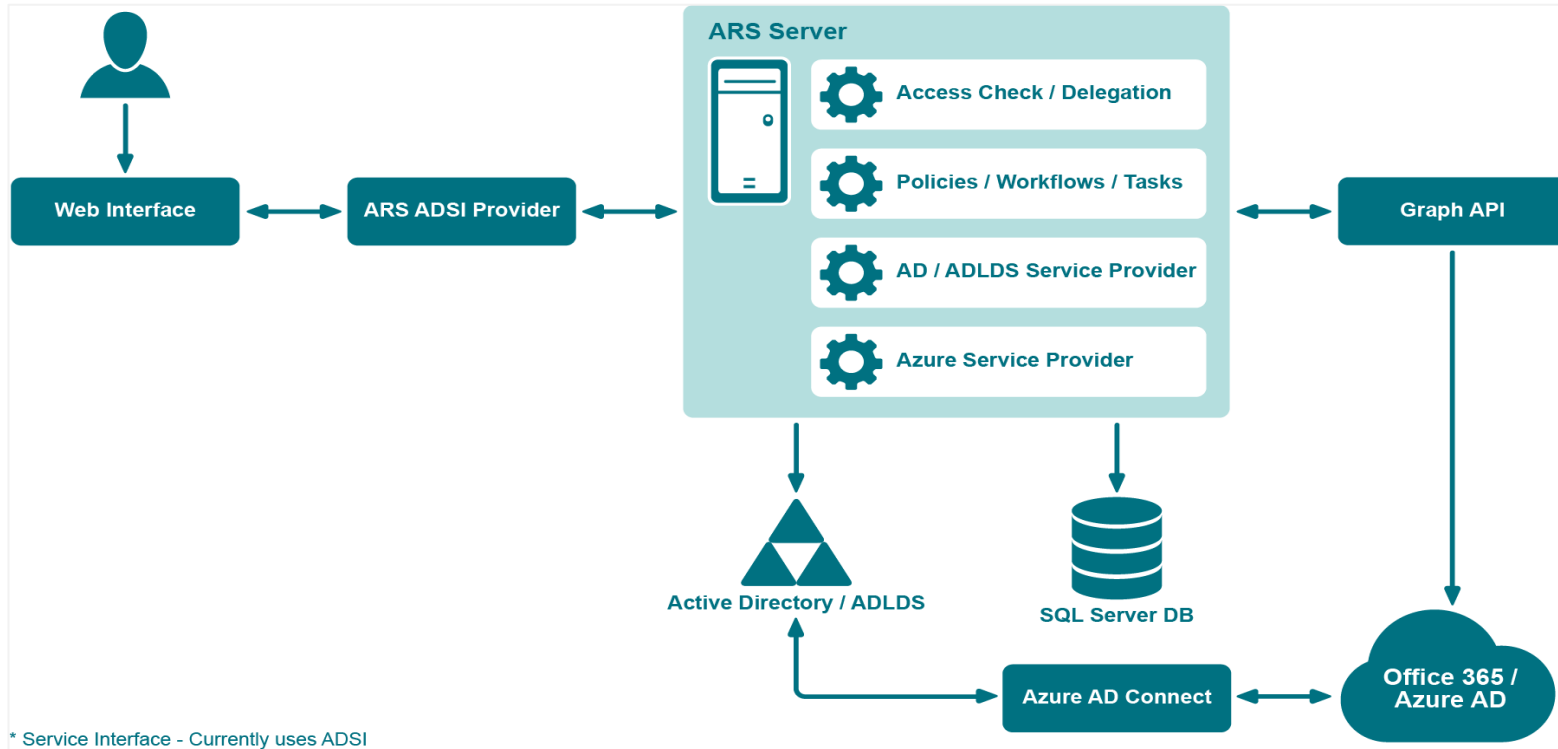
**Event 1517, ARAdminSvc**

General Details

Attribute is modified.  
Operation GUID: 5641e8ed-7428-4785-b2c3-7dc47693e9b5  
Attribute name: physicalDeliveryOfficeName  
Attribute value: Moscow  
Action: Replace

Log Name: Active Roles Admin Service

# Hybrid환경에 대한 지원



\* Service Interface - Currently uses ADSI

# Exchange Online Mailbox 관리

The screenshot displays the Exchange Online Mailbox management interface for Jane Doe. The main window is titled "Exchange Online Properties" and shows the "Delegation" settings. The left sidebar lists various settings, with "Delegation" selected. The main content area shows a table of delegation entries. The "Send As" section is expanded, showing a table with columns for Name, Description, and Type. The "Full Access" section is also visible, showing a table with columns for Name, Description, and Type. The "Properties" button for the "James Bond" entry is highlighted.

Exchange Online Properties

Jane Doe

Active Directory / QUEST.LOCAL / DEMO / Sites / France

Mail flow settings:

- Message Size Restrictions
- Delivery Options

Description:

Delivery options control delegated permissions and forwarding.

Object ID:

7c83a6e1-4a79-4385-9b9b-e9b068b0dce6

Exchange Online Properties

Jane Doe

Active Directory / QUEST.LOCAL / DEMO / Sites / France

Mail Flow Settings

- Delegation
- E-mail Addresses
- Mailbox Features
- Mailbox Settings

Send As:

Name	Description	Type
SELF		group
James Bond		User

Add... Remove Properties

Full Access:

Name	Description	Type
Joe Dalton	Bx8 INC.	User

Add... Remove Properties

Save Close

# 통합 리포트 및 변경 기록

The screenshot displays the Active Roles console interface. The left sidebar contains navigation options: Home, Directory Management, Search, Customization, Approval, Settings, and Help. The main content area shows the user profile for Reto Bachmann - Zuerich, with a breadcrumb trail: Active Directory / oneidentity.lab / PROD / EMEA / CHE / Users. Below the profile, there are two sections for change logs, each with a 'Change User' header and a plus sign icon. The first section shows a change to the Telephone Number property, and the second section shows changes to the edsaAdminGroup and Create User Mailbox properties. Each entry includes the operation ID, requested time, requested by, and completed time.

Views | Tree

Home  
Directory Management  
Search  
Customization  
Approval  
Settings  
Help

Active Roles

Administrator

Active Directory / oneidentity.lab / PROD / EMEA / CHE / Users

Previous page | Page 1 | Next page

**Change User** (Operation ID: 1-156)  
Name: Reto Bachmann - Zuerich (oneidentity.lab/PROD/EMEA/CHE/Users)  
Reason: <none>  
Requested: 11/6/2016 8:10:13 PM (UTC)  
Requested by: ONEIDENTITY\Administrator  
Completed: 11/6/2016 8:10:14 PM (UTC)

Property	Old value	New value
Telephone Number (telephoneNumber)	<not set>	'+41791234567'

Status: COMPLETED

**Change User** (Operation ID: 1-152)  
Name: Reto Bachmann - Zuerich (oneidentity.lab/PROD/EMEA/CHE/Users)  
Reason: <none>  
Requested: 11/6/2016 8:06:53 PM (UTC)  
Requested by: ONEIDENTITY\Administrator  
Completed: 11/6/2016 8:07:03 PM (UTC)

Property	Old value	New value
edsaAdminGroup (edsaAdminGroup)	'Exchange Administrative Group (FYDIBOHF23SPDLT)'	'CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=Oneidentity,CN=Microsoft Exchange,CN=Ser ...'
Create User Mailbox (edsaCreateMsExchMailbox)	<not set>	'true'

Status: COMPLETED

# 신규 사용자 생성 : Azure AD / Office 365

General	<input checked="" type="checkbox"/> Create Azure Account
Account	Name: Howard Wolowitz
Create Azure Account	Temporary Password: ●●●●●●
Licenses	User Principal Name: howard.wolowitz @corpds.biz
	Usage Location: US

Identity	<input checked="" type="checkbox"/> STREAM_O365_E3
Settings	<input checked="" type="checkbox"/> Deskless
Job Info	<input checked="" type="checkbox"/> Flow for Office 365
Contact Info	<input checked="" type="checkbox"/> PowerApps for Office 365
> Licenses	<input checked="" type="checkbox"/> Microsoft Teams
	<input checked="" type="checkbox"/> Microsoft Planner
	<input checked="" type="checkbox"/> Sway
	<input type="checkbox"/> Mobile Device Management for Office 365
	<input checked="" type="checkbox"/> Yammer
	<input checked="" type="checkbox"/> Azure Active Directory Rights Management
	<input checked="" type="checkbox"/> Office ProPlus
	<input checked="" type="checkbox"/> Lync Online (Plan 2)
	<input checked="" type="checkbox"/> Office Online
	<input checked="" type="checkbox"/> SharePoint Online (Plan 2)
	<input checked="" type="checkbox"/> Exchange Online Plan 2

# 신규 그룹 생성 : Azure AD / Office 365

New Group

New Group in TOU [Customize](#)

Active Directory / ARS71.CORK.LAB.LOCAL / TOU

General

[Create an Exchange e-mail address](#)

**> Create Azure Group**

Create Azure Group

Name:  
TT

Description:

Open properties for this object when I click Finish

To complete, click Finish.

Back **Finish** Cancel

감사합니다.

Quest