Hongso Chae

Solutions Consultant

Active Directory 통합 관리 및 자동화 솔루션

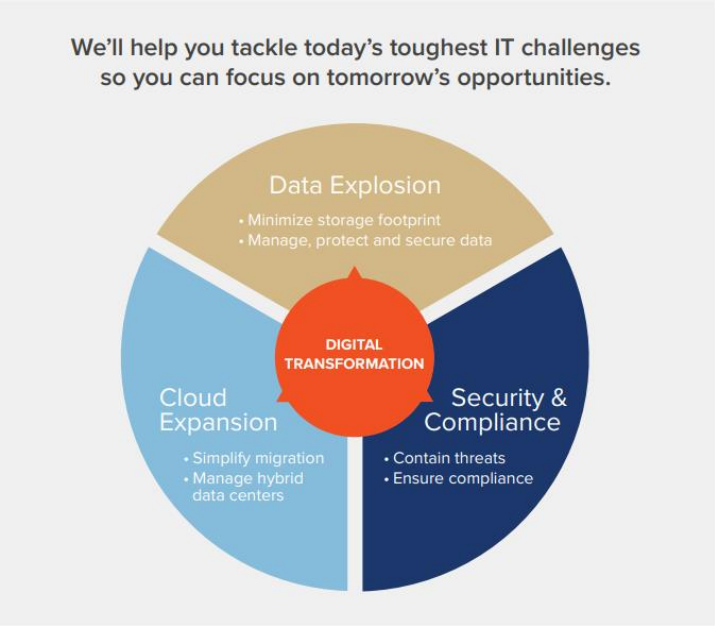
Active Roles 소개자료

Quest

회사 소개

Quest는 빠르게 변화하는 엔터프라이즈 IT 환경을 위한 소프트웨어 솔루션을 제공합니다.

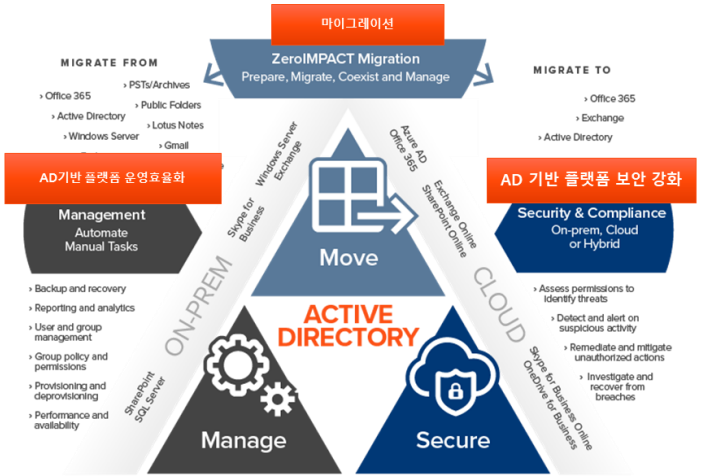
Quest는 데이터 폭발, 클라우드 확장, 하이브리드 데이터 센터, 보안 위협 및 규정 요구사항으로 인한 문제를 단순화할 수 있도록 지원하며 Fortune 500 대 기업의 95%와 Global 1000 대 기업의 90%를 포함하여 100 개국 130,000여 기업에 글로벌 서비스를 제공하고 있습니다.



Data Management	**Microsoft Platform**	Data Protection	**Unified Endpoint Management**	**IAM**

2년 연속 Microsoft 최우수 Global ISV

마이그레이션, 관리, 보안에 대한 통합 솔루션 제공



전체 Solution Overview

AD 보안

Active Directory 보안

권한 및 계정 감사

Change Auditor for AD

온라인 기반 즉시 복구

Recovery Manager for AD

Mac 정책관리

Privileged Access Suite

AD기반 환경의 필수요건인
AD보안(내/외부 위협 실시간
감시 및 감사)

Windows10 단말보안

단말 2FA 인증

Defender

GPO 관리

GPO Admin

패치 및 배포관리

System Management Appliance

Windows 10 환경에
최적화된 필수적인
GPO기반 단말 보안

컴플라이언스

컴플라이언스 대응

통합 패스워드 관리

Safeguard Password Manager

접근통제

Safeguard Session Manager

손쉽고 비용 효율적인
컴플라이언스 대응

통합 계정관리

AD기반의 시스템 계정관리와 통합 계정관리

AD계정 통합관리 및 HR 자동연동

Active Roles

통합 계정관리 및 거버넌스

Identity Manager(Gov)

통합 계정관리 및 거버넌스

운영 효율화

운영 효율화

AD 기반 셀프 패스워드 관리

Password Manager

이벤트 통합관리

InTrust Enterprise

자산관리

Asset Management Appliance

운영 편의성 향상을 통한
효율적 운영 및 운영 비용
최적화

Quest

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.

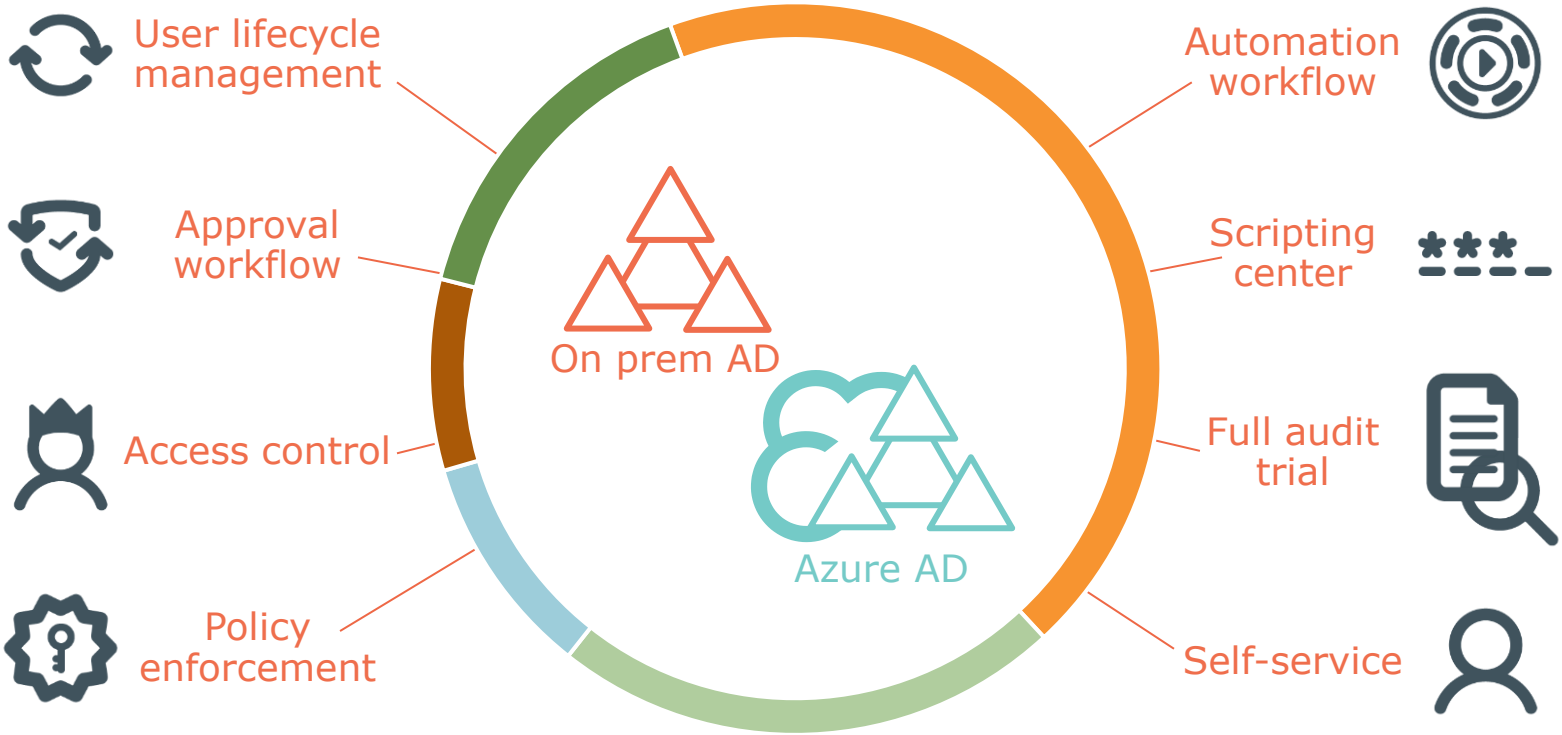
***Vendor Landscape: Active Directory Security and** Governance Solutions*
Forrester, January 5, 2016

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

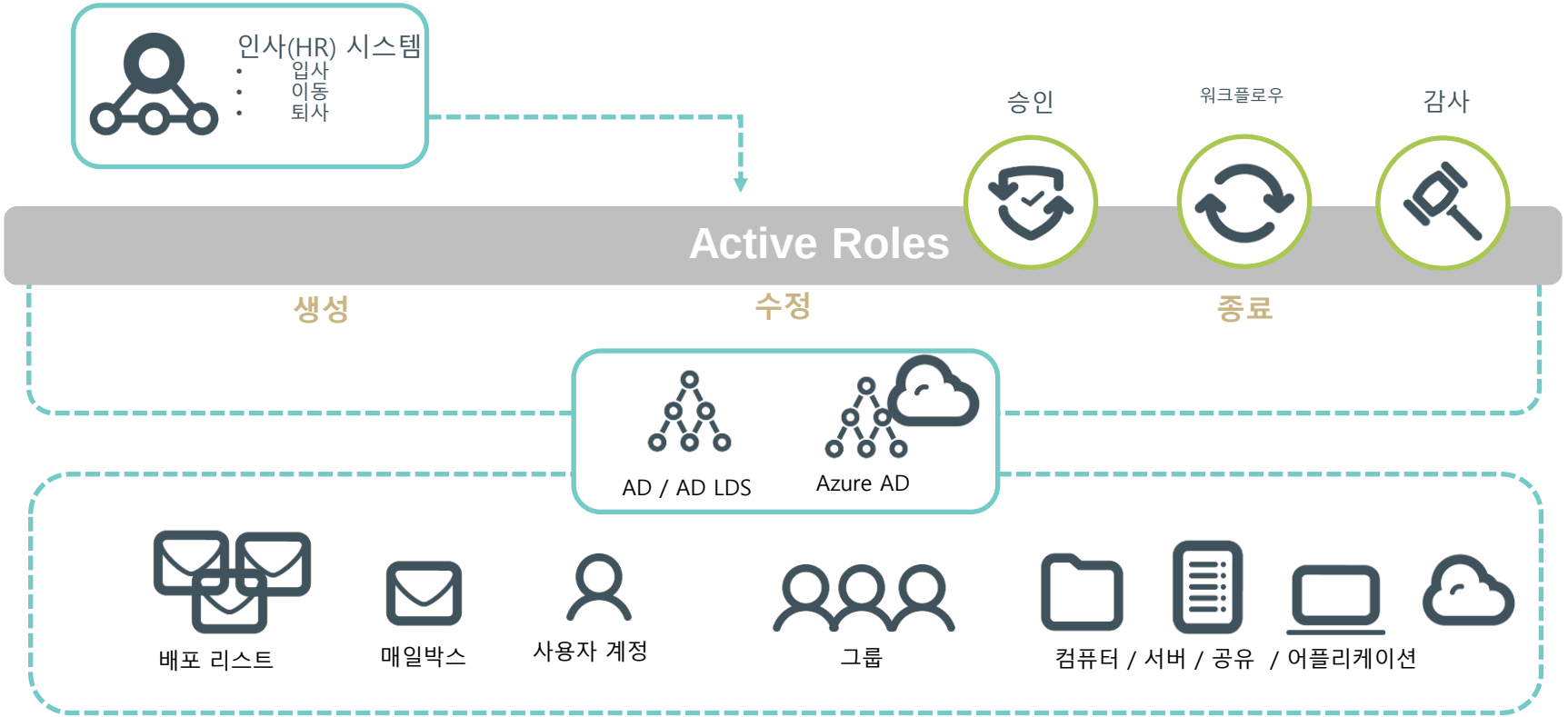
Quest

Active Roles



Virtual Firewall

자동화된 워크플로우 기반의 통합 AD계정관리

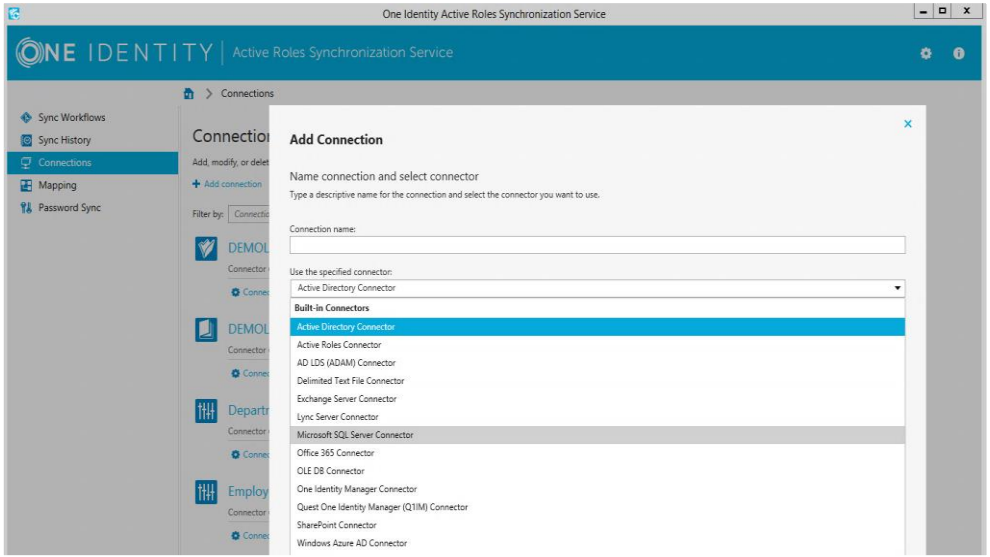


사용자 라이프사이클 관리

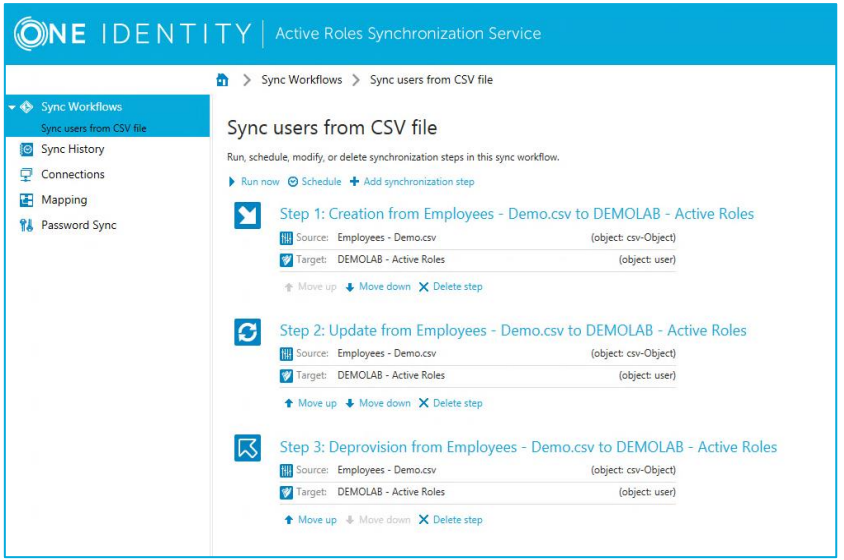
Quest

다양한 형태의 시스템과 계정 정보 동기화

다양한 형태의 시스템 연결 지원



동기화 설정을 통해서 자동으로 동기화 수행

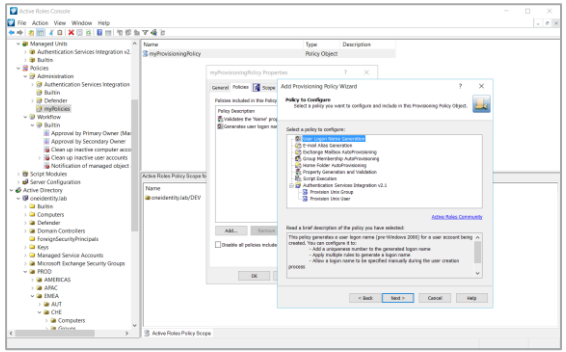


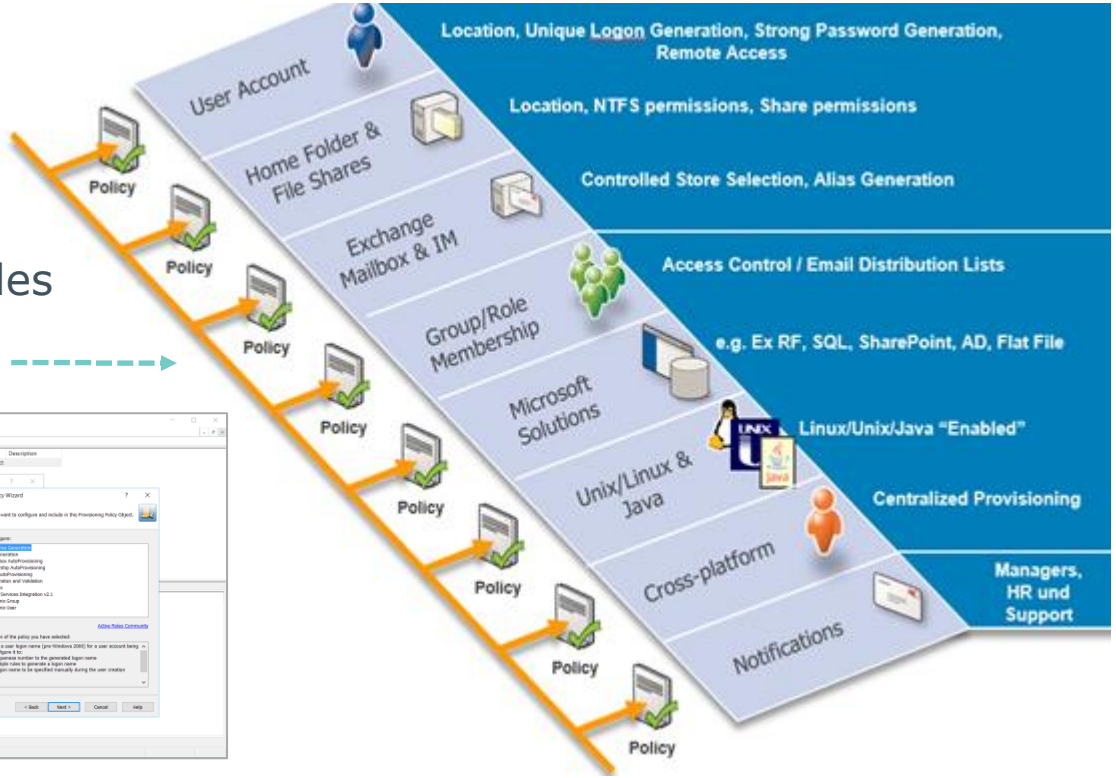
프로비저닝 – 자동화된 외부 계정 생성

인사(HR)시스템

- **입사**
- 이동
- 퇴사

Active Roles



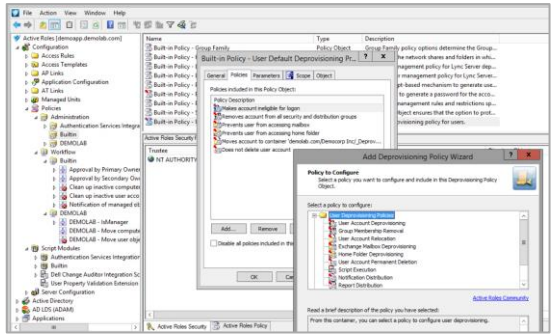


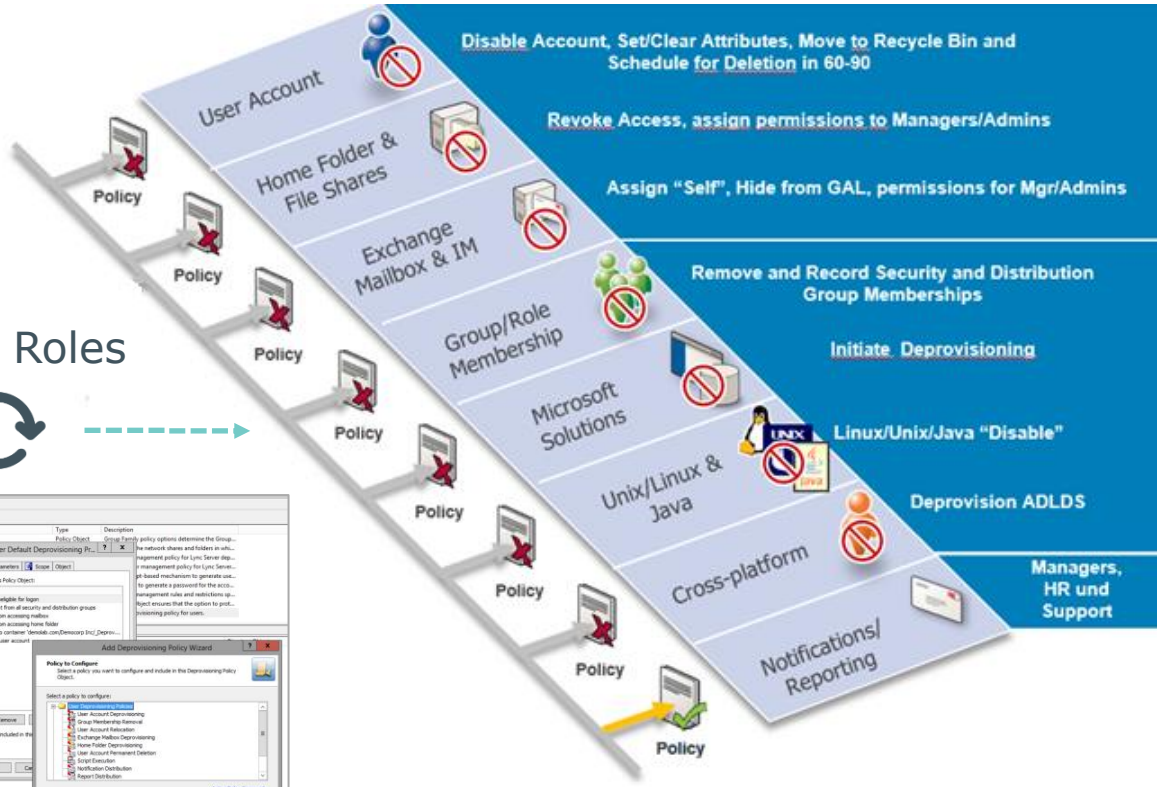
디프로비저닝 – 자동화된 외부 계정 삭제

인사(HR)시스템

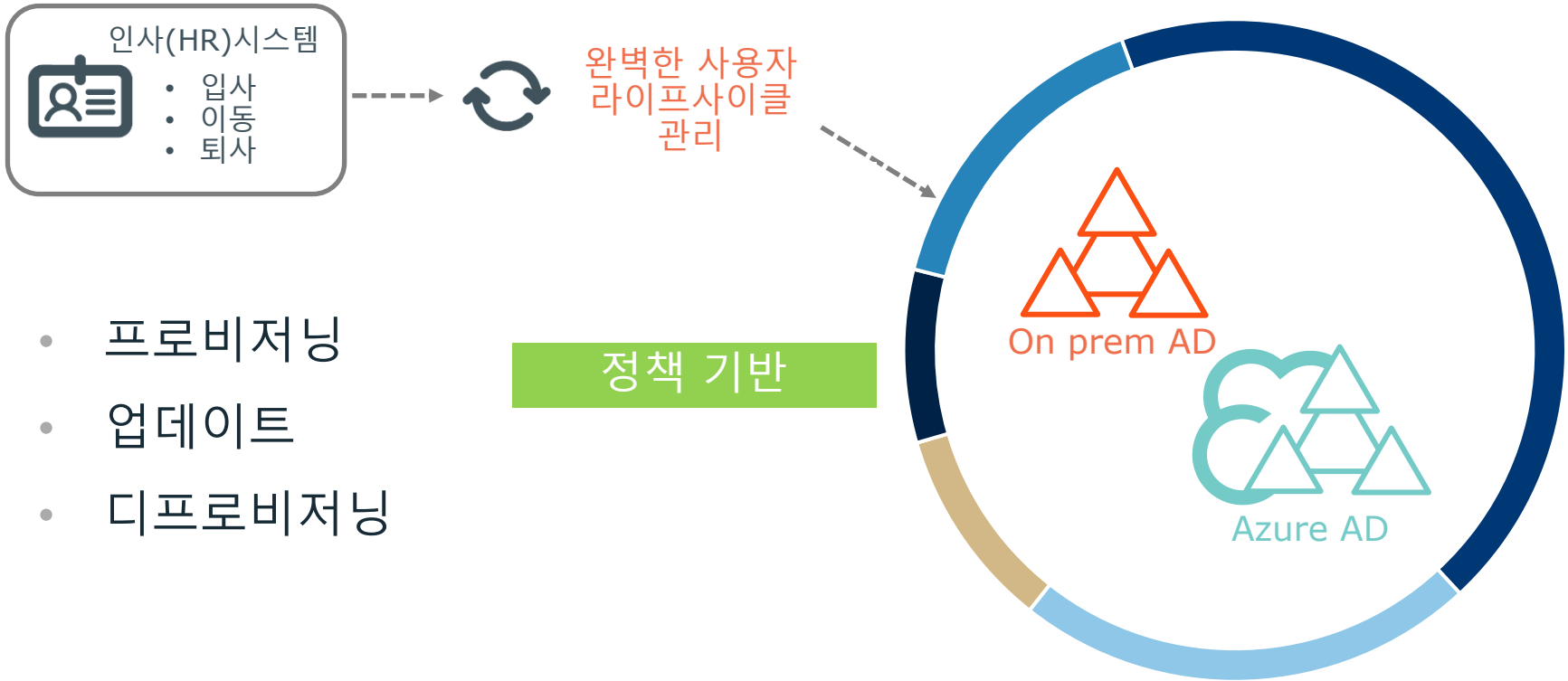
- 입사
- 이동
- **퇴사**

Active Roles





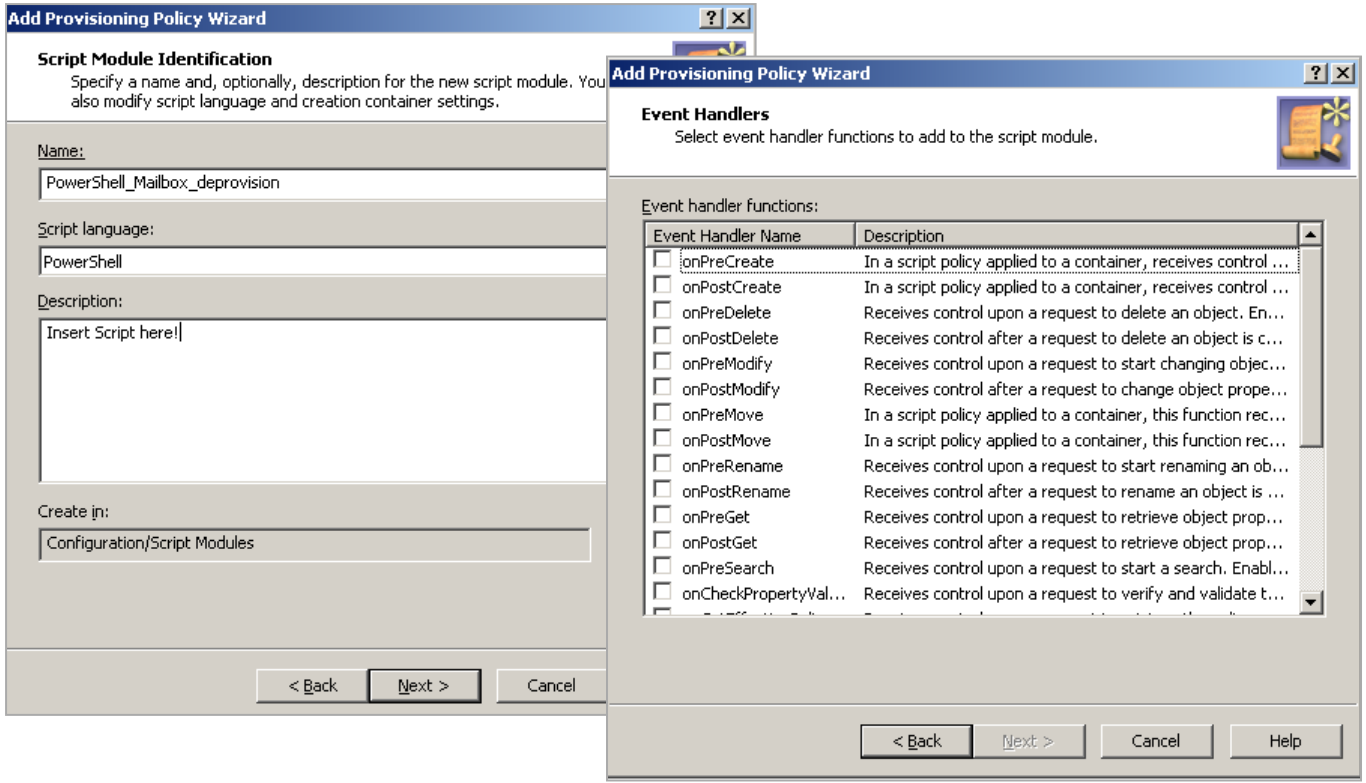
HR과 연동하여 정책 기반의 관리



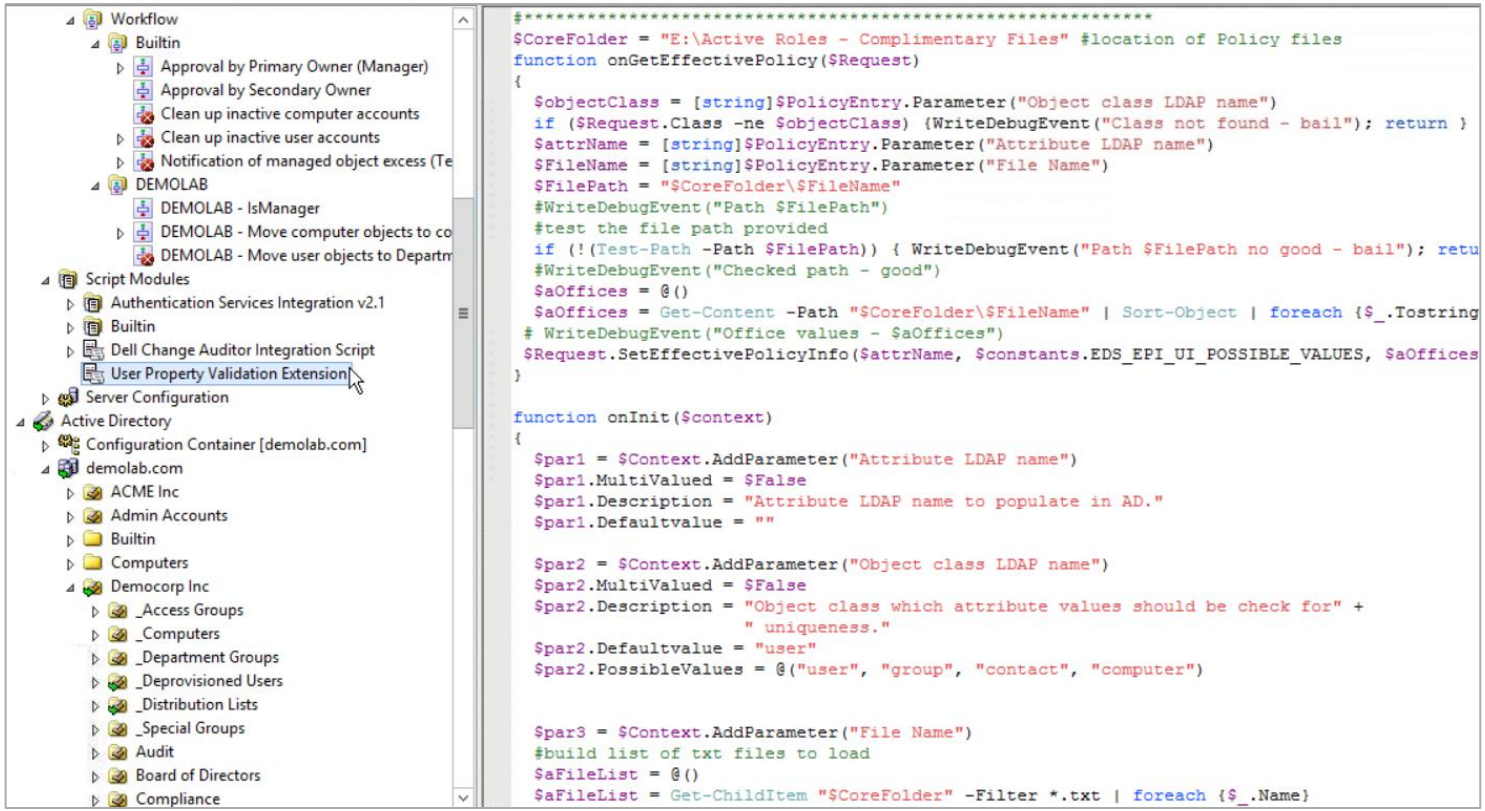
- 프로비저닝
- 업데이트
- 디프로비저닝

정책 기반

스크립트를 통한 정책 확장



스크립트 통합


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"); retu
#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}

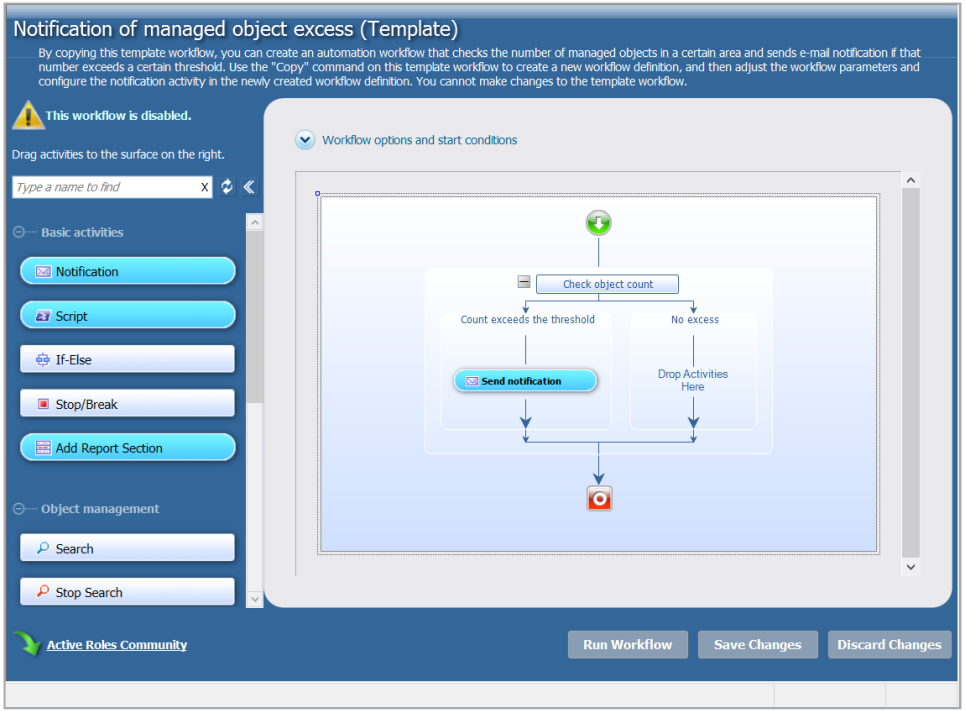
02

워크플로우와 자동화

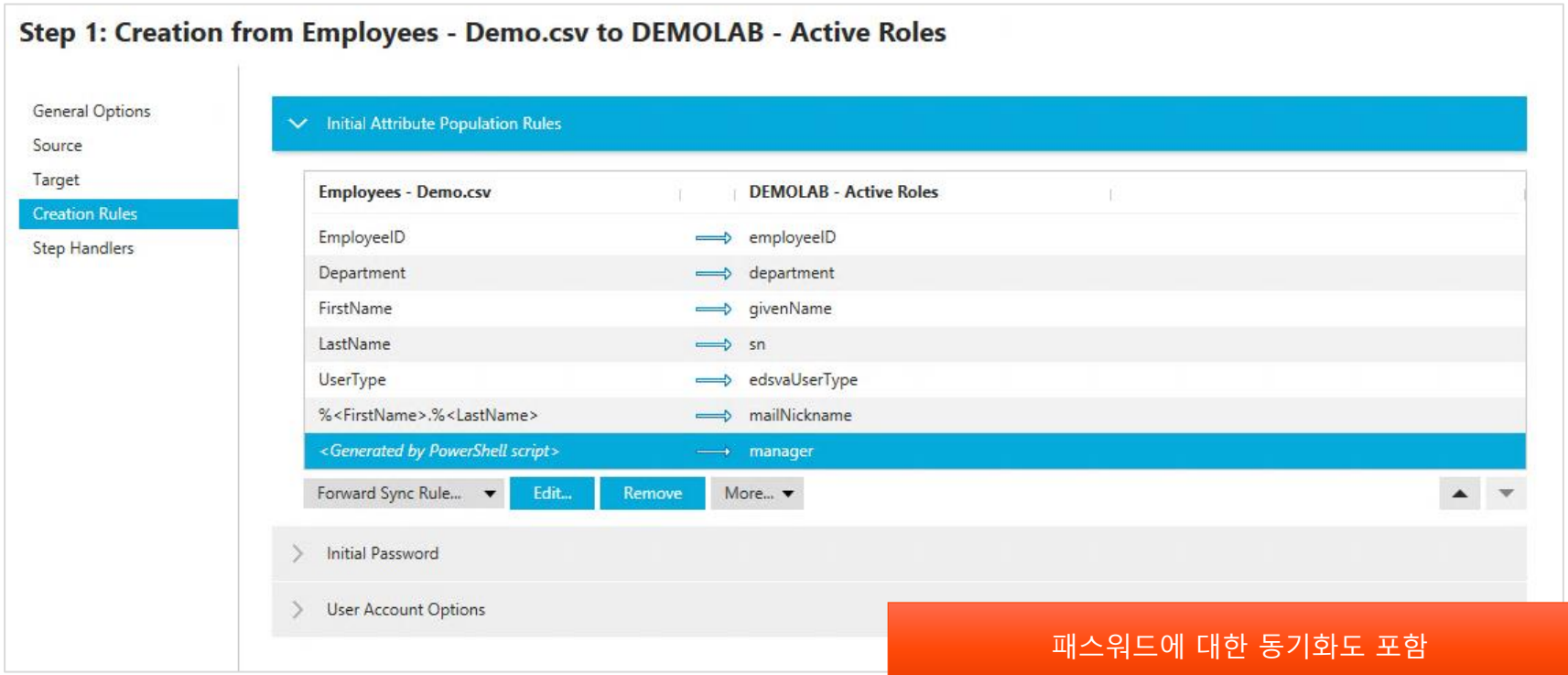
Quest

워크플로우 지원

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



타 시스템과의 자동 동기화 기반 연동



패스워드에 대한 동기화도 포함

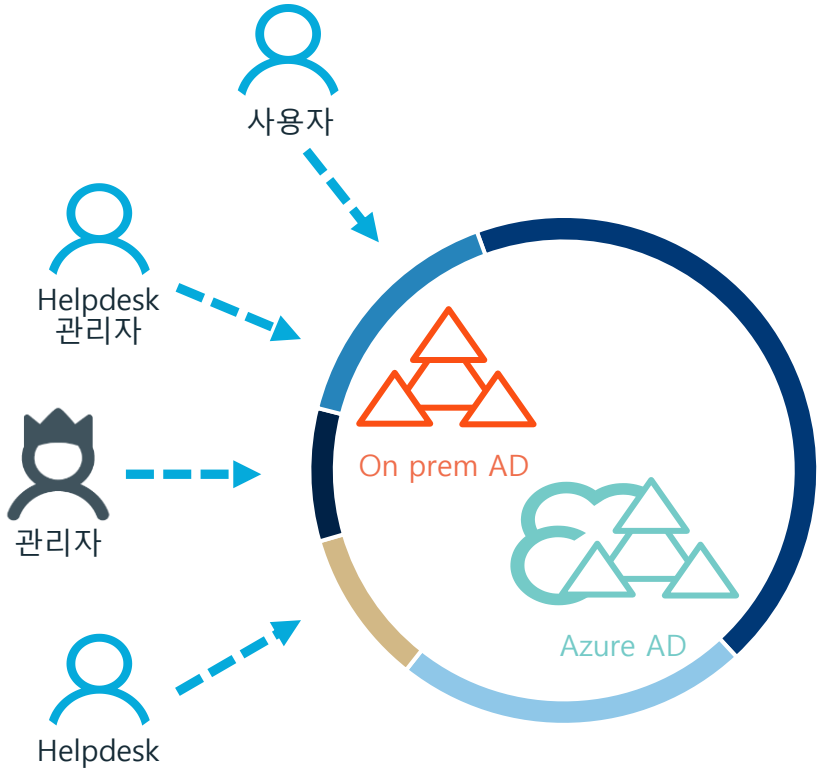
03

보안 및 예방관리

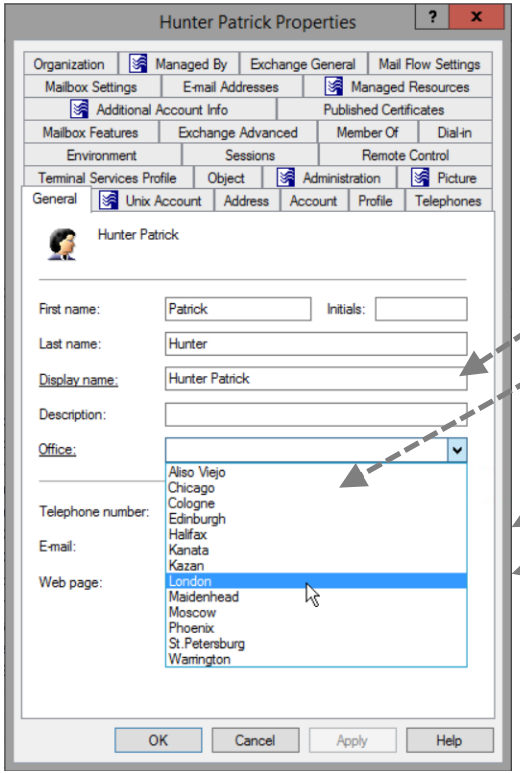
Quest

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



Display명은 Lastname Firstname으로 나타나야 한다.

사무실은 리스트에 나타난 것만 선택해야 한다.

전화 번호는 “+82 01# #### ####”형태가 되어야 한다.

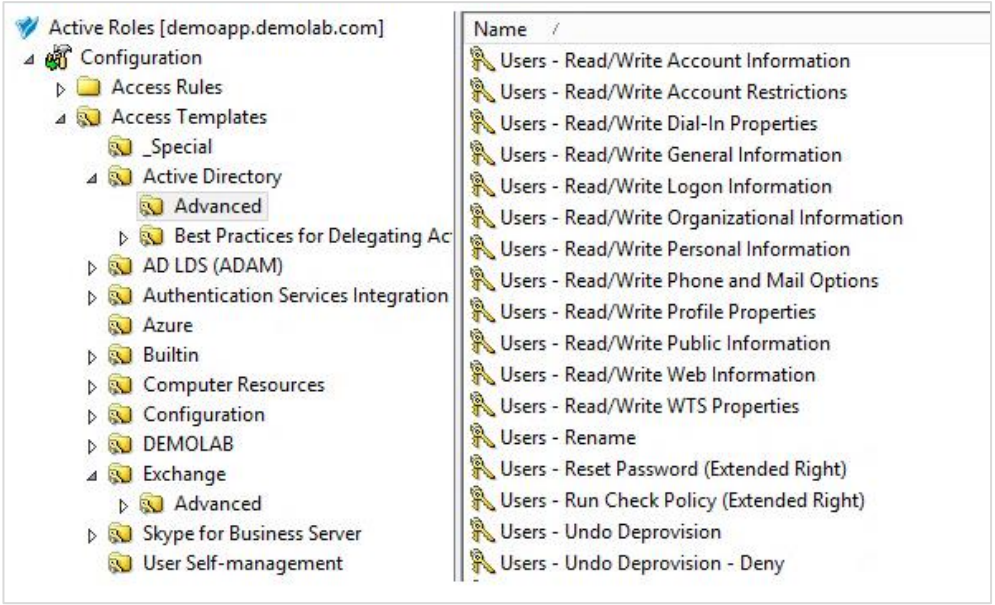
E-mail은 @quest.com으로 “Firstname.Lastname”형태로 구성되어야 한다.

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

Quest

관리자 권한 노출 위험성을 제거

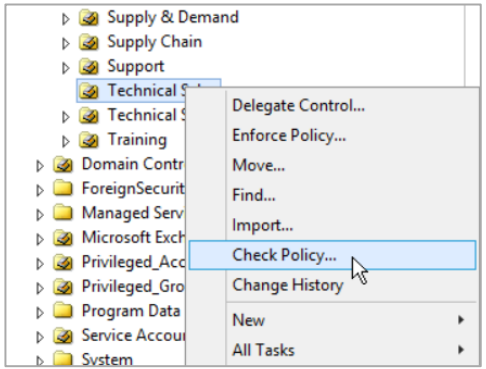
- Active Directory / Azure
- Exchange / Office 365
- SharePoint / Online
- Skype for Business



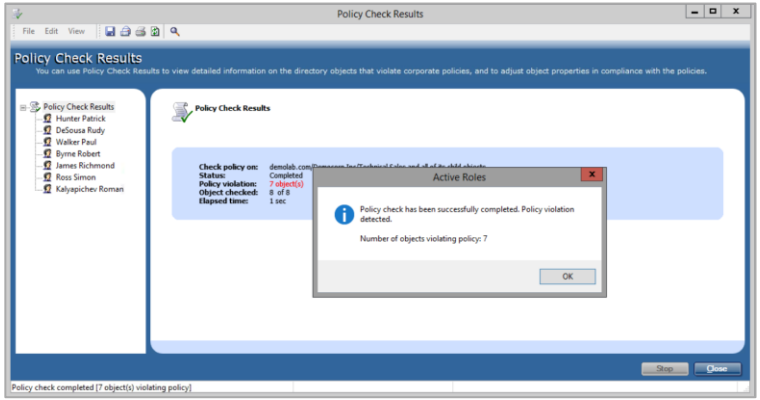
세분화된 권한을 적정한 담당자에게 할당하여 모든 권한을 갖는 관리자 계정으로 작업 하지 못하도록 관리

Quest

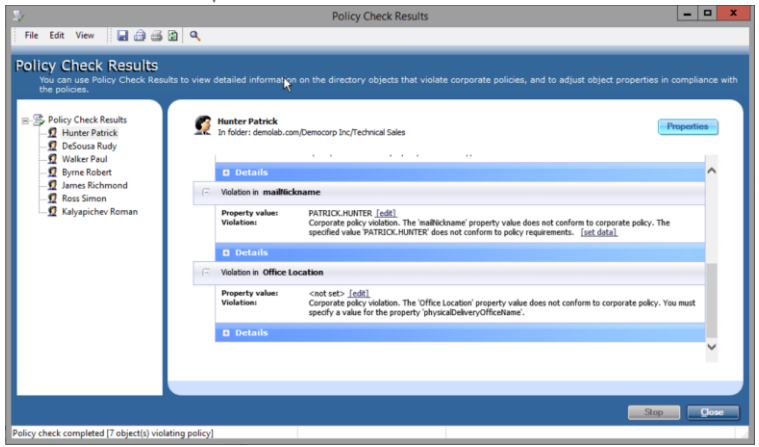
정책 검증



정책 위배 체크 수행

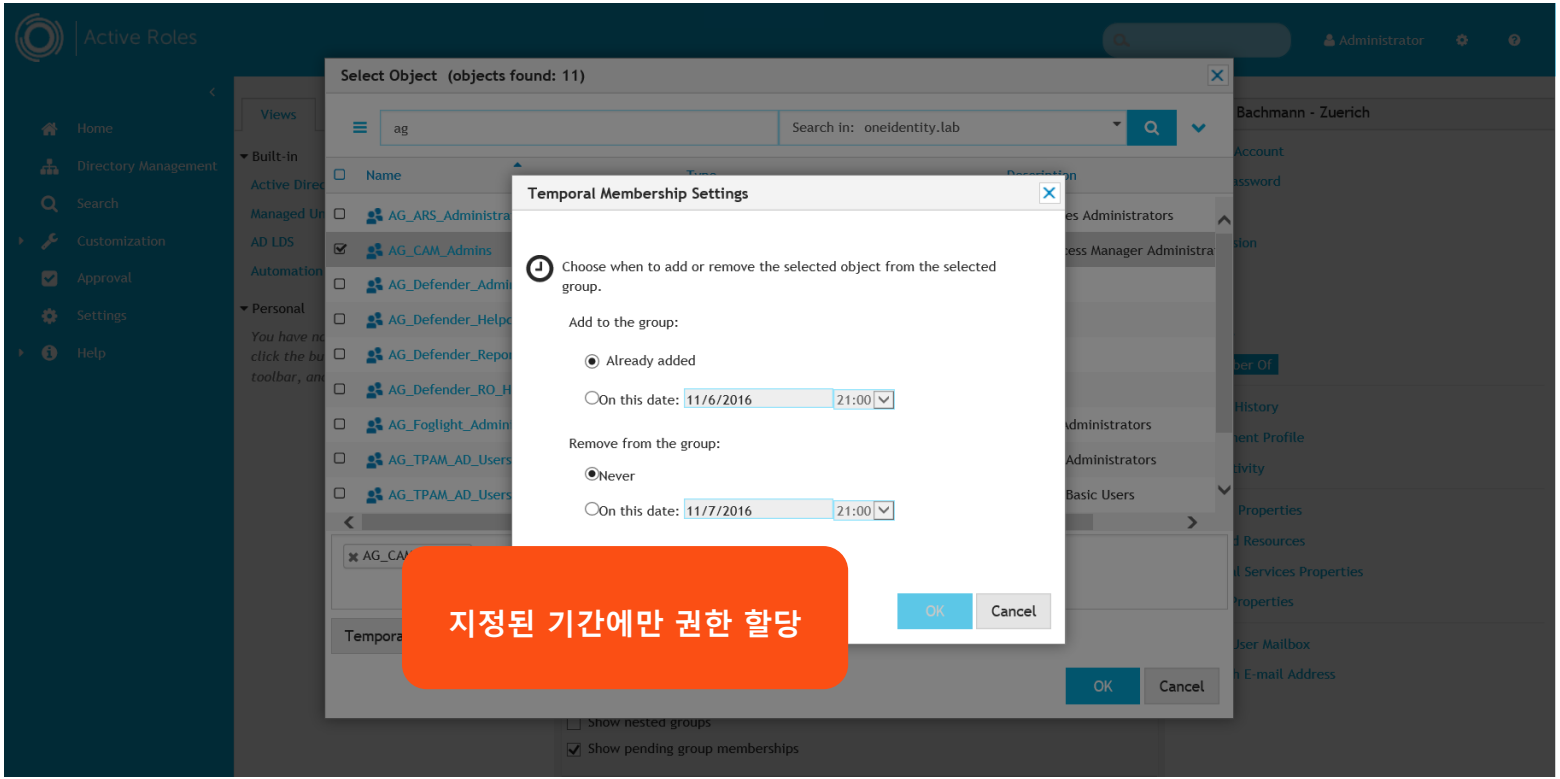


정책 위배 내역 제공



Quest

임시 사용자(그룹) 관리


Active Roles
Administrator
Select Object (objects found: 11)
ag
Search in: oneidentity.lab
Name
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
Show nested groups
Show pending group memberships

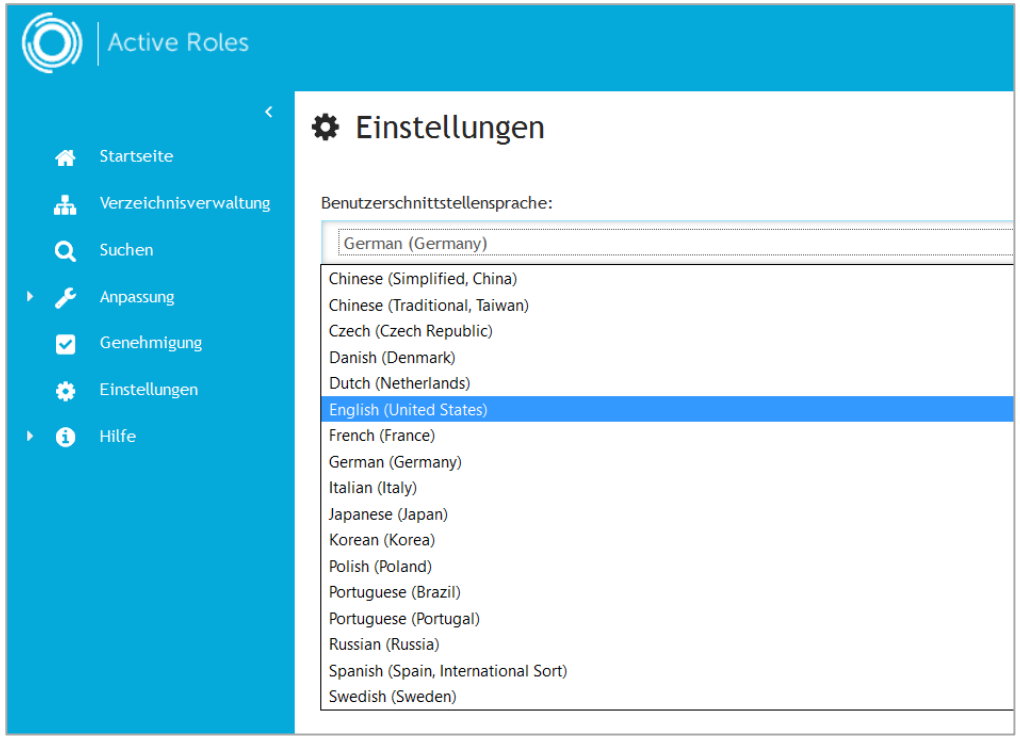
04

통합 관리

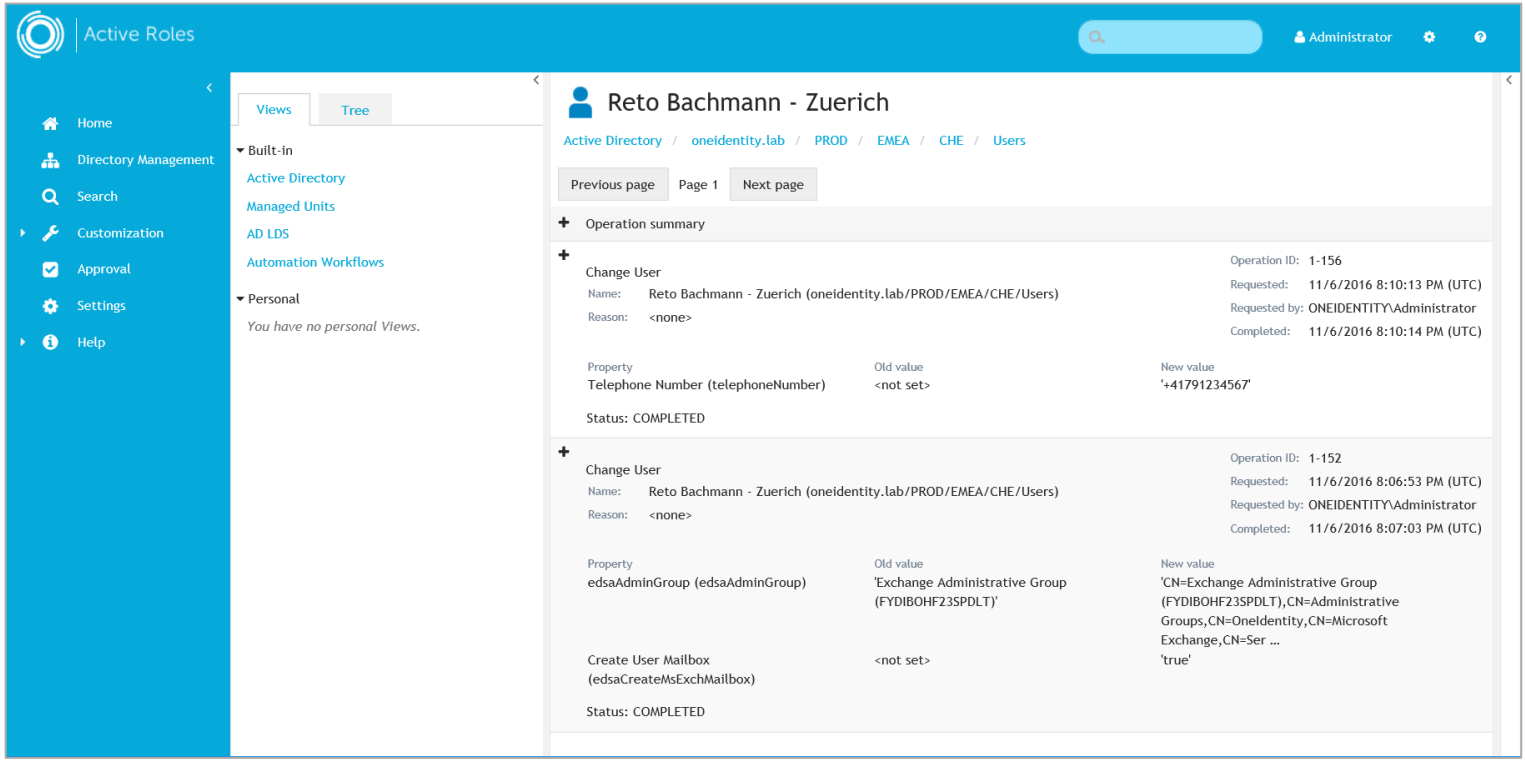
Quest

다양한 Browser와 언어지원(한국어 지원)

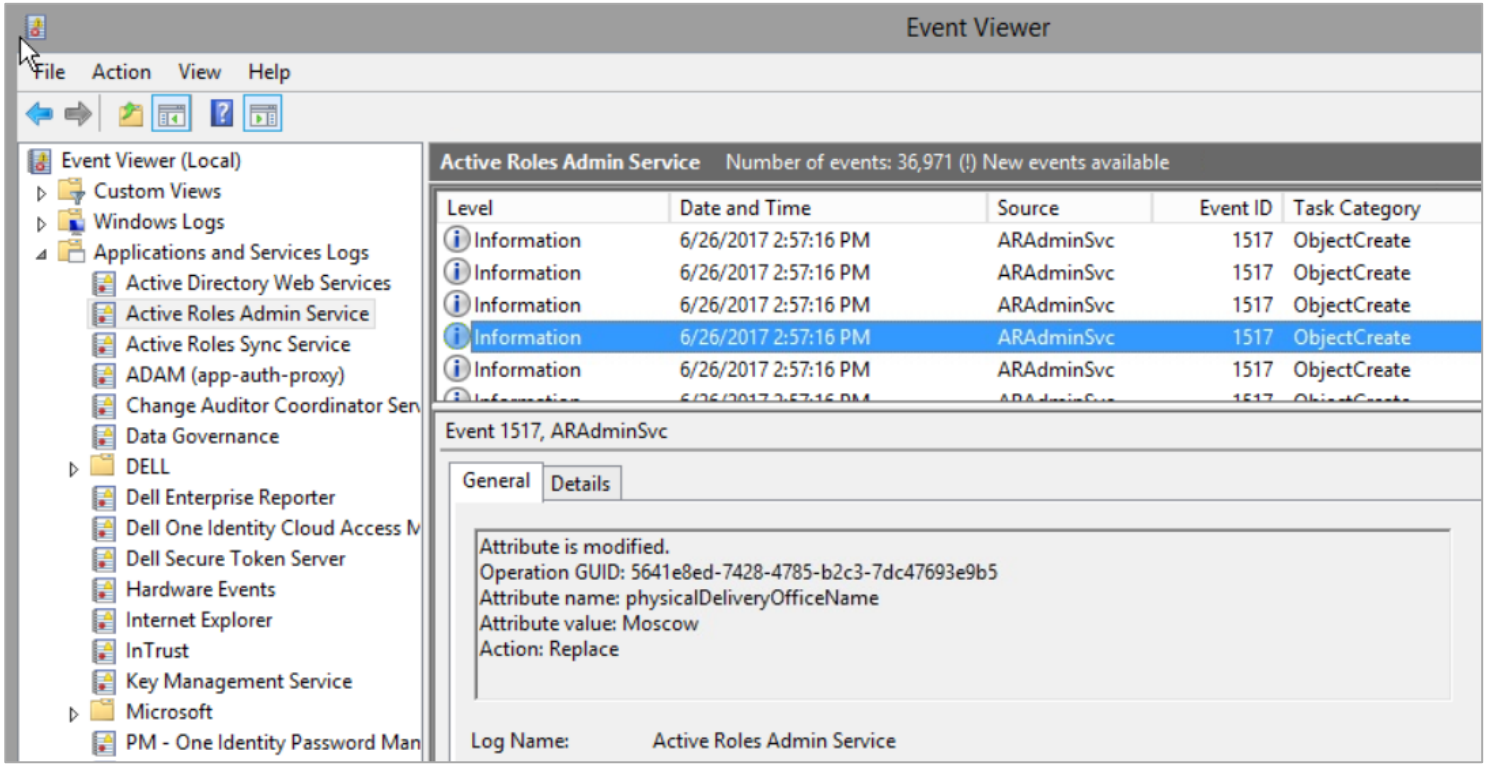
- Internet Explorer
- Edge
- Firefox
- Chrome



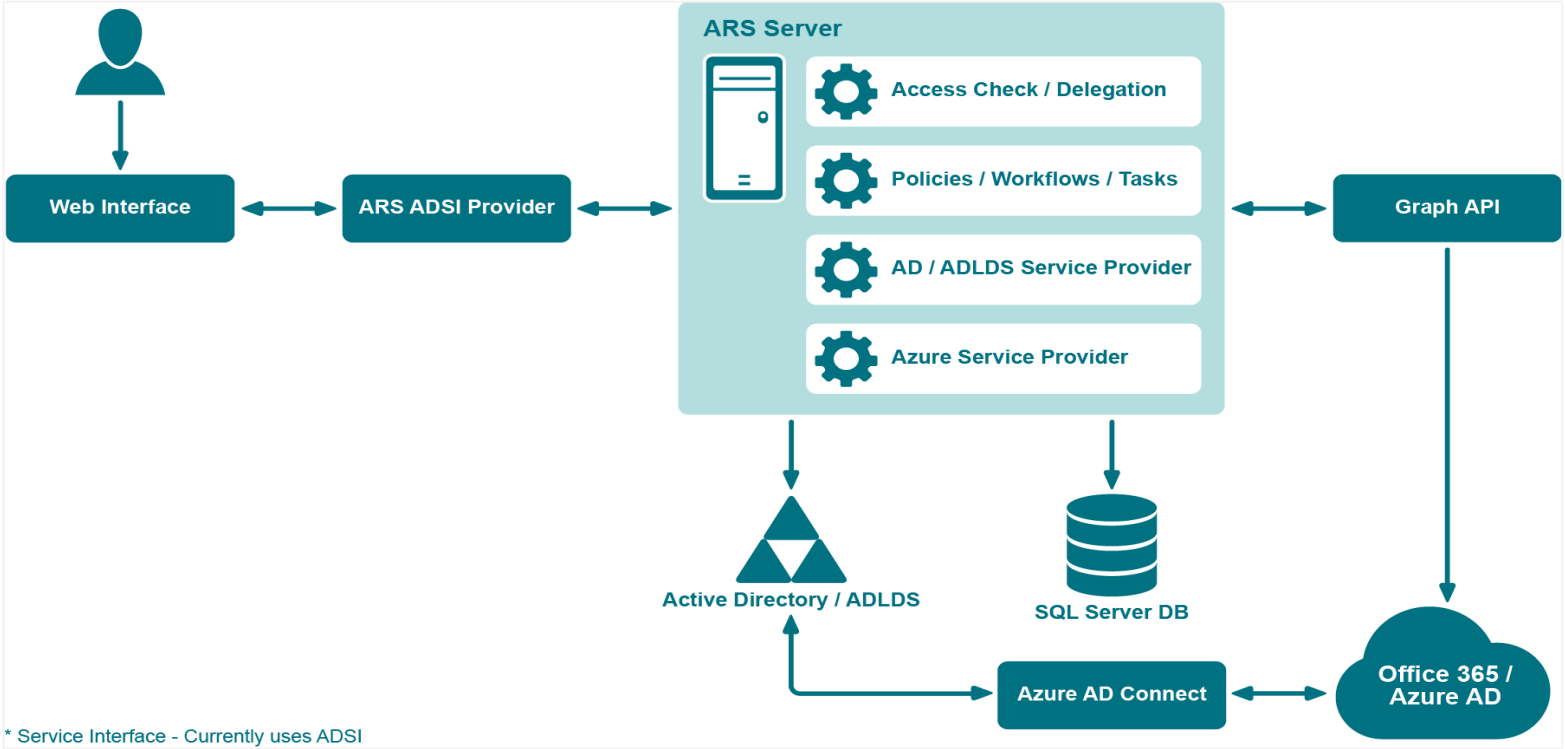
모든 변경 히스토리 내역 제공



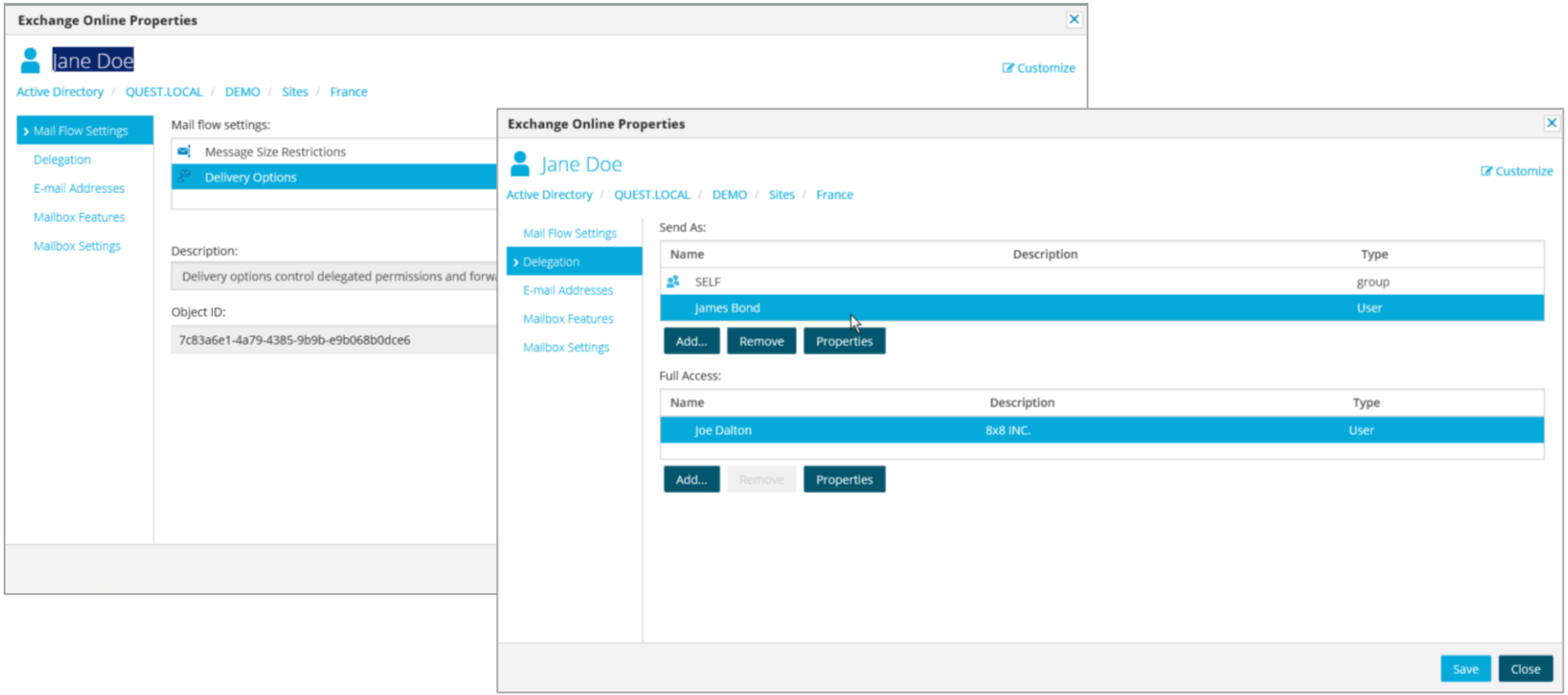
ARS의 작업 내역을 윈도우 이벤트로 제공



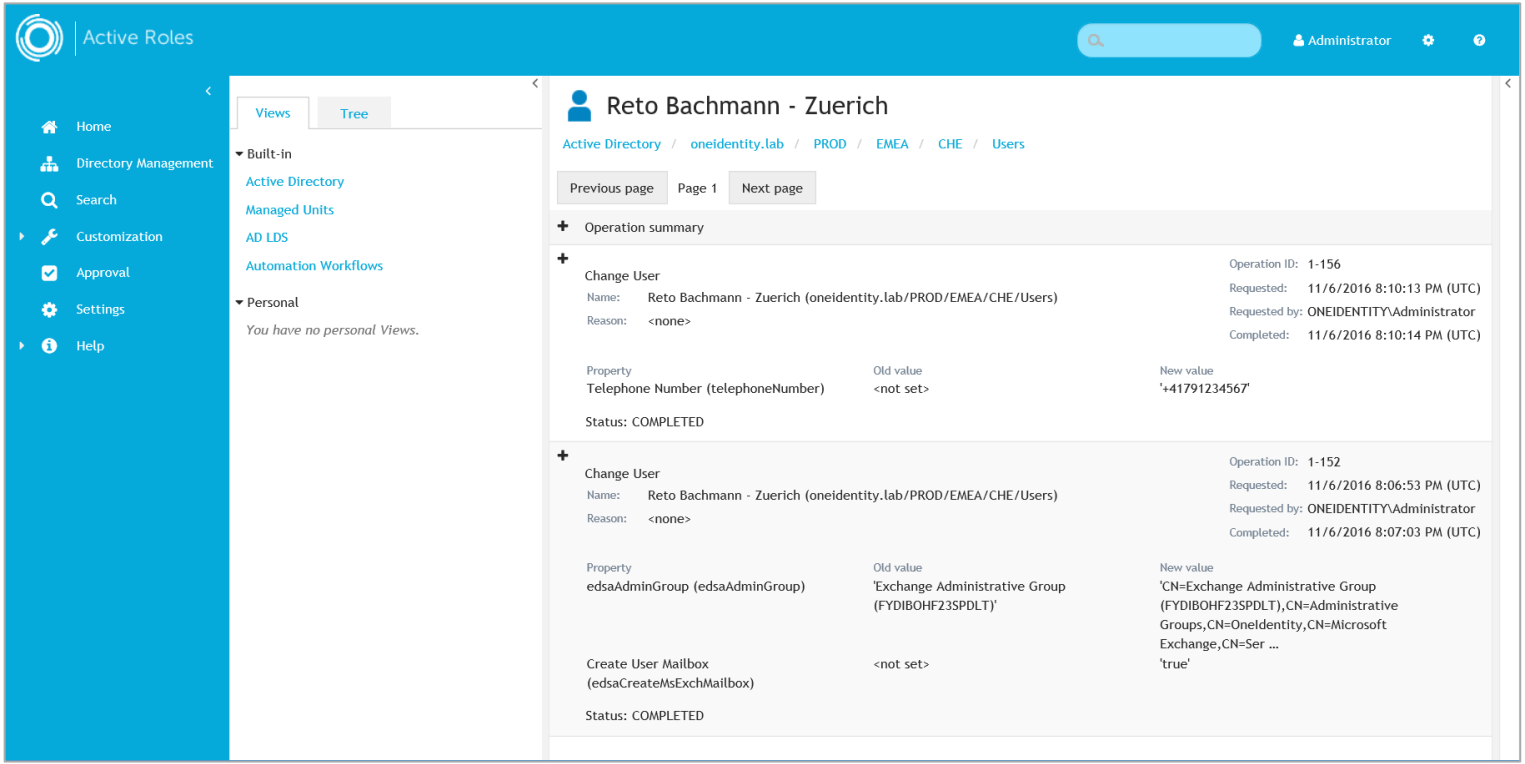
Hybrid환경에 대한 지원



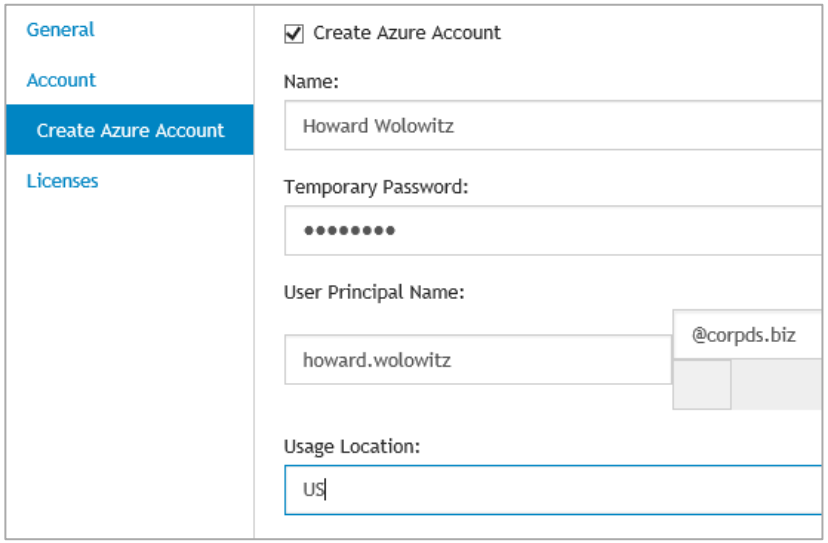
Exchange Online Mailbox 관리

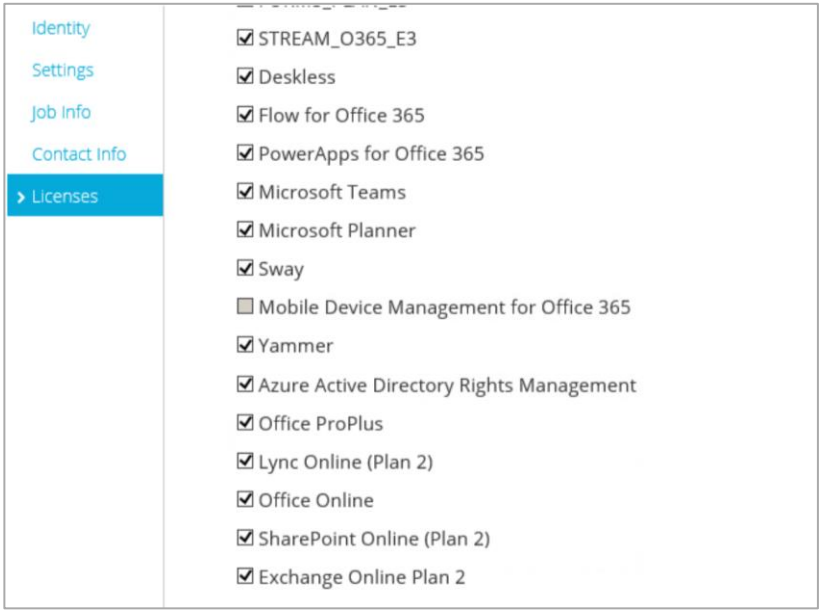


통합 리포트 및 변경 기록

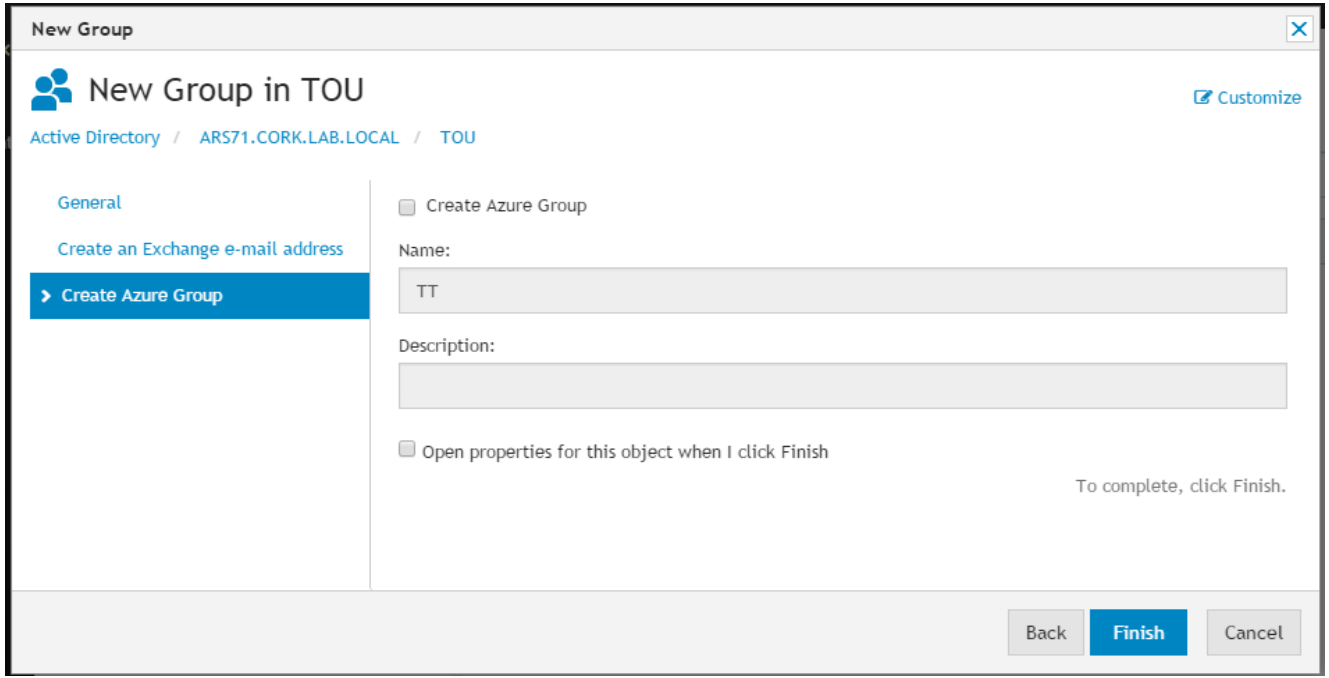

Active Roles
Administrator
Home
Directory Management
Search
Customization
Approval
Settings
Help
Views
Tree
Built-in
Active Directory
Managed Units
AD LDS
Automation Workflows
Personal
You have no personal Views.
Reto Bachmann - Zuerich
Active Directory / oneidentity.lab / PROD / EMEA / CHE / Users
Previous page
Page 1
Next page
Operation summary
Change User
Name: Reto Bachmann - Zuerich (oneidentity.lab/PROD/EMEA/CHE/Users)
Reason: <none>
Operation ID: 1-156
Requested: 11/6/2016 8:10:13 PM (UTC)
Requested by: ONEIDENTITY\Administrator
Completed: 11/6/2016 8:10:14 PM (UTC)
Property
Telephone Number (telephoneNumber)
Old value
<not set>
New value
'+41791234567'
Status: COMPLETED
Change User
Name: Reto Bachmann - Zuerich (oneidentity.lab/PROD/EMEA/CHE/Users)
Reason: <none>
Operation ID: 1-152
Requested: 11/6/2016 8:06:53 PM (UTC)
Requested by: ONEIDENTITY\Administrator
Completed: 11/6/2016 8:07:03 PM (UTC)
Property
edsaAdminGroup (edsaAdminGroup)
Old value
'Exchange Administrative Group (FYDIBOHF23SPDLT)'
New value
'CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=Oneldentity,CN=Microsoft Exchange,CN=Ser ...
Create User Mailbox (edsaCreateMsExchMailbox)
<not set>
'true'
Status: COMPLETED

신규 사용자 생성 : Azure AD / Office 365





신규 그룹 생성 : Azure AD / Office 365



감사합니다.

Quest