



Hongso Chae

Quest Software Korea | Solutions Consultant

Active Directory기반 환경 2FA 솔루션
: Quest Defender

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.

고객중심의 비즈니스로 전세계
100개국, 13만 고객사 보유

퀘스트소프트웨어를 판매하는
7,000개의 파트너

베스트 프랙티스를 자체 공유하는
400만 명의 커뮤니티 구성원

포춘 500대 기업 중 95%가
 퀘스트 제품 사용자

Microsoft 2018 Winner's Circle Member

Global Managed IP Co-Sell Partner





SIIA CODiE AWARDS 2018

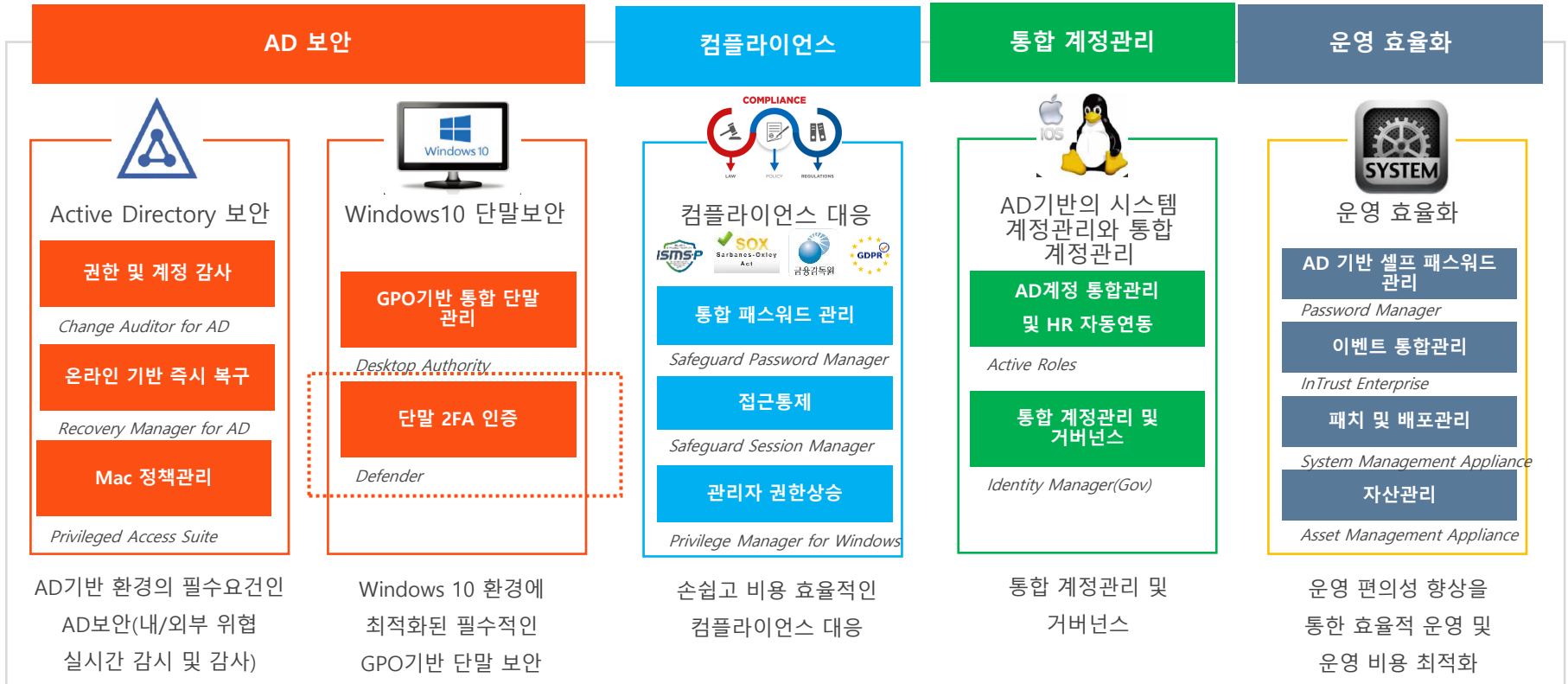


퀘스트소프트웨어의 솔루션



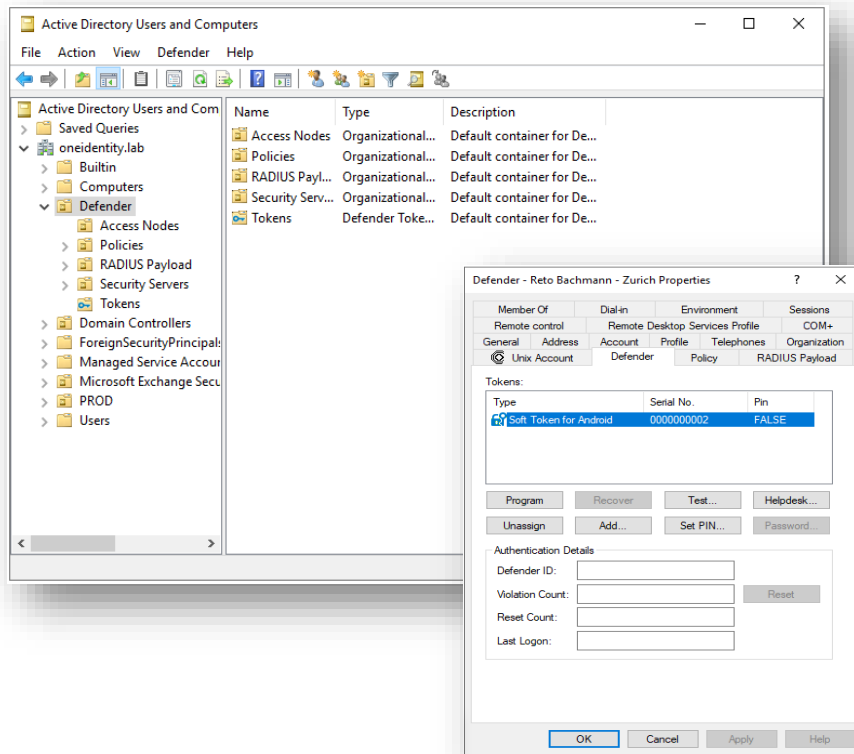
-  데이터베이스 관리
-  데이터보호
-  통합 엔드 포인트 관리
-  ID 및 액세스 관리
-  Microsoft 플랫폼 관리

Quest 보안 및 운영 Solution Overview



Active Directory와 완벽히 연동

- Active Directory 기본 관리 툴에서 관리
- 사용자별 토큰을 할당



웹 기반의 관리 포탈 제공

- 대시보드
- 시스템 설정
- 로그
- 토큰 배포
- 관리
- 리포트
- 헬프데스크

The image displays two overlapping browser windows. The top window shows the 'Defender - Dashboard' for an administrator. The dashboard includes a navigation menu with options like Dashboard, Configuration, Activity, Self-Service Settings, Helpdesk, and Management. The main content area features a 'Log Receiver Service' status indicator (Running), a 'Warnings from Defender Security Servers' section with a warning about an invalid LDAP connection, and a 'Authentication requests by DSS, last hour' chart showing 75 requests for 'ingmar.direct.cork.lab.local'. Below this is a line chart for 'Authentications per hour, last 24 hours'.

The bottom window shows the 'Defender' login page with fields for 'User name' (bachmann), 'Password', and 'Domain' (oneidentity). It includes a 'Remember me' checkbox and a 'Sign in' button.

특정 사용자의 문제를 손쉽게 분석 - Helpdesk

- 손쉽게 문제 해결

The top screenshot shows the 'User Details' tab for user 'Reto Bachmann - Z'. The user details table is as follows:

Full Name	Reto Bachmann - Z
User DN	CN=Reto Bachmann
SAM Account Name	BACHMANR
User Principal Name	BACHMANR@oneid
Defender ID	<Not Set> (Edit)
Last Successful Login (Windows)	3/24/2020 2:26:15
Last Failed Login (Windows)	2/3/2020 2:37:44 F
Last Successful Authentication (Defender)	Never
Violation Count	0
Reset Count	0

The bottom screenshot shows the 'Authentication Routes' tab with a table of routes:

Defender Security Server	Access Node	Defender Security Policy	Status	Comment
		No policy configured	Invalid	User not valid for this route

Soft토큰을 스마트폰에 등록(1/2)

- 사용자별로 손쉽게 토큰을 등록

Select a software token

Select the software token you want to register and use. After this token is registered to you, you can use it to authenticate and get access to the resources protected by Defender within your organization.

Contact your system administrator if the required software token is not listed here.

- Soft Token for Android
- Authy token
- E-mail token
- Google Authenticator
- Gridsure token
- SMS token

Step 1 of 3

Enter verification code

An e-mail message containing your verification link and code has been sent to Reto.Bachmann@oneidentity.lab.

To verify your identity, click the link in the e-mail message or enter the provided verification code in the text box below.

Verification code:

Back Next Finish Cancel

Defender

ONE IDENTITY

Register a hardware token

Request a software token

Mail

noReply@Defender@oneidentity.lab

Defender: verification code (Soft Token for Android)

Hello Reto Bachmann - Zurich,

You have received this message because you have requested a software token on the Defender Self-Service Portal.

You must verify your identity with Defender. Click the link below and follow the provided instructions: <http://localhost:85/Ticker/760202aabb701737c0f70da2f8ad69b6>

Alternatively, manually enter the following verification code on the Defender Self-Service Portal: **760202aabb701737c0f70da2f8ad69b6**

If you have not recently requested a software token, contact your system administrator.

Soft토큰을 스마트폰에 등록(2/2)


Select a softwar... ✓
Enter verificatio... ✓
Install and activ...

Install and activate token

A new software token has been registered to you. Download and install the software token and activate it using the provided activation code.

[Download Soft Token for Android](#)

Activation code:
**kazldgzr-fggnlkrz-cmyxmbd-hikronk-fattlavv-
lhmhlfav-pdyofomp-pckedox-chrwfrup-fjwvjdl-
kktodbwv-lannkhr**



If you are viewing this page on a device where this software token is already installed, you can click the link below to insert the activation code into the software token.

[Insert activation code in software token](#)


E-mail this information to:
 [Send](#)

Step 3 of 3 [Back](#) [Next](#) [Finish](#) [Cancel](#)

14:33 67%

Defender Soft Token

Scan a QR code or enter an activation code. The code is either provided by Defender administrator or obtained from the Self-Service Portal.



[Scan QR code](#)

[Enter activation code](#)

[Learn more about Defender](#)

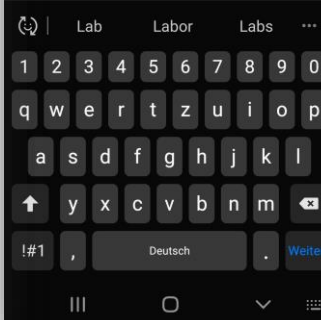
14:34 67%

New Token

Activate

One Identity Lab

kfwneikn-deoslepn-ggyvoexx-ehzxcawl-jg
mkjkrp-horyfjms-lkprdkvm-hkzpmimz-miur
akov-fosthivs-ealwdatu-nkzpckq




14:34 67%

Defender Soft Token

One Identity Lab

544032



리포팅

- 손쉽게 원하는 리포트 조회

The image displays two screenshots of the ONE IDENTITY Defender Reports interface. The top screenshot shows the 'Report scheduler' configuration page. The bottom screenshot shows the 'Schedule report' modal dialog.

Report scheduler configuration:

- Select a report:** Audit trail
- Report settings:**
 - Select a report type:** Audit report
 - Defender Security Server:** ZRHLABONE01
 - Reporting period:** Today
- Select date and time formats
- Buttons:** Schedule, Preview

Schedule report modal:

- Report description:** Token Assignment
- Recurrence:** Daily
- Start time:** 01:00 AM
- Generate this report:**
 - Every day
 - Every weekday
 - Every specified number of days
- Buttons:** Save, Cancel

Security tokens and their users table:

Token CN	Type	Serial #	User Principal Name
PDAN000000000002	Soft Token for Android	0000000002	Reto Bachmann - Zurich (BACHMANN@oneidentity.com)

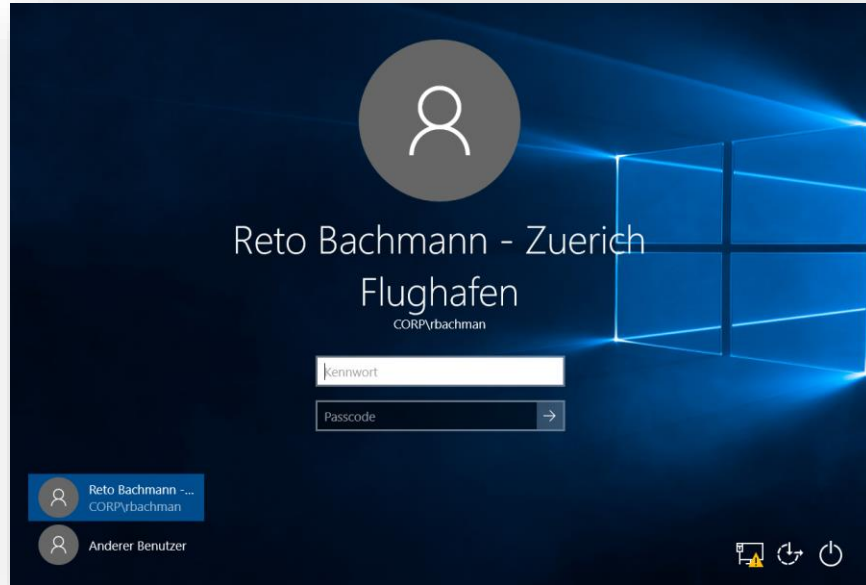
Defender지원 환경

- 별도의 추가 비용없이 다양한 어플리케이션에 사용 가능
(OWA, Citrix, Terminal Service, IIS ISAPI Filter, VPN Client, Windows Desktop 등)
- Aventail, Juniper, Symantec, MSFT IGA등에서 검증됨
- 윈도우 로그인 대체
 - 윈도우 패스워드 화면을 대체
 - 오프라인 로그인 모드 지원
 - 자동으로 패스워드 변경
 - 토큰사용자와 패스워드 사용자를 구분하는 정책 지원

적용 예시 - 윈도우 로그인

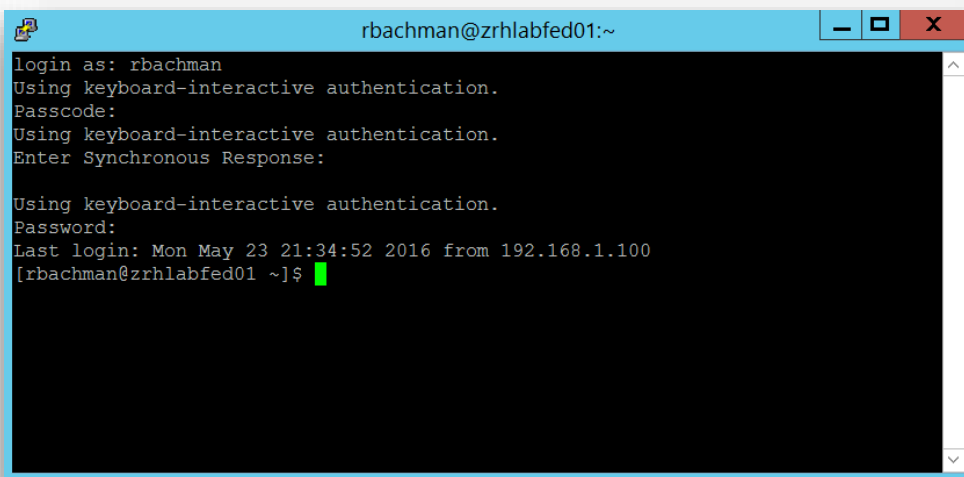


기존 패스워드에 추가 인증



기존 패스워드를 패스코드 방식으로 변경

적용 예시 – Unix / Linux



```
rbachman@zrhlabfed01:~  
login as: rbachman  
Using keyboard-interactive authentication.  
Passcode:  
Using keyboard-interactive authentication.  
Enter Synchronous Response:  
  
Using keyboard-interactive authentication.  
Password:  
Last login: Mon May 23 21:34:52 2016 from 192.168.1.100  
[rbachman@zrhlabfed01 ~]$
```

- SSH
- Gnome

Defender를 통한 2FA환경은

손쉽게 적은
비용으로 빠르게
구축 가능

AD기반에 최적화된
구성으로 높은
관리편의성

별도의 추가
비용없이 다양한
환경을 지원

감사합니다.



Quest[®]