USA & APAC Office
Seattle
Swivel Secure, Inc.
1001 4th Ave #3200
Seattle, WA 98154

+1 949 480 3626 (Pacific Time)
Toll Free: 866.963.AUTH (2884)
usa@swivelsecure.com

UK & Ireland Offices
North
Equinox 1
Audby Lane
Wetherby, Leeds
LS22 7RD

HQ: +44 (0)1134 860 123
Support: +44 (0)1134 860 111
hq@swivelsecure.com

South
Pinewood
Chineham Business Park
Chineham, Basingstoke
RG24 8AL

EMEA Offices
Portugal
Estrada de Alfragide,
N.º 67, Alfrapark – Lote H, Piso 0,
2614-519 Amadora

+351 215 851 487
portugal@swivelsecure.com

Spain
Av. Juan Carlos I, nº 13 – 2ª
planta (Torre Garena)
Alcalá de Henares
28806 Madrid

+34 911 571 103
espana@swivelsecure.com

KOREA

www.swivelsecure.co.kr
02-3461-8124 array-sales@arraynetwork.co.kr

AuthControl Sentry®

지능형 멀티팩터 인증 솔루션

AuthControl Sentry 는 PINsafe® 특허 기술을 핵심으로 리스크 기반 동적 제어 를 제공하는 지능형 멀티팩터 인증 솔루션입니다.

swivelsecure

www.swivelsecure.com

swivelsecure

AuthControl Sentry® 지능형 멀티팩터 인증솔루션

AuthControl Sentry®는 52개 이상의 국가에서 금융, 공공, 의료, 교육 및 제조를 포함한 전 산업 분야에서 운영중입니다. AuthControl Sentry는 진정한 지능형 멀티팩터 인증 솔루션으로 애플리케이션과 데이터에 대한 무단 액세스를 방지합니다.

AuthControl Sentry®는 다양한 아키텍처 요구사항을 지원합니다. 유연하며 광범위한 인증 팩터를 통해 폭넓은 기능을 제공합니다.

AuthControl Sentry는 모바일 애플리케이션 또는 지문 인식과 같은 생체 인식까지 같은 다양한 인증 팩터를 지원하는 업계 선도적인 인증 솔루션입니다.

Capture the QR code to see the full diagram of AuthControl Sentry®, the complete multi-factor authentication stakeholder solution.

특장점

- 특허 기반의 PINsafe® 기술 – 8페이지 참조
- 온프레미스 및 클라우드 아키텍처 지원
- 단일 테넌시(Tenancy) 및 단일 계층형 클라우드 솔루션으로 최적화된 맞춤형 구성 및 제어 기능 제공
- 리스크 기반 인증 및 싱글사인온을 기본 기능으로 제공
- 수백 개의 애플리케이션과 원활한 연동
- 광범위한 인증 방법을 통해 최대 10가지 인증 팩터 적용 가능

Office 365 , eCommerce , ERP 액세스 등 모든 종류의 애플리케이션 액세스 인증에 적용이 가능합니다.

- ✓ Employees
- ✓ Customers
- ✓ Suppliers

Architecture

온프레미스 및 클라우드 아키텍처 지원

AuthControl Sentry®에는 제한이 없습니다. 클라우드에서 호스팅하든 온프레미스에서 호스팅하든, 액세스를 요청하는 사용자가 고객인지, 직원인지, 공급자인지 관계없이 액세스에 대한 인증이 가능하도록 설계되었습니다.

온프레미스 아키텍처

로콜 설치형 AD 에이전트를 제공하기 때문에 AD를 인터넷을 통해 공유하지 않고도 사용자 계정 동기화와 내부 시스템에 액세스가 가능합니다.

클라우드 아키텍처

고정 IP: 각 AuthControl 고객은 전용 고정 IP를 할당 받습니다.리소스, 응용 프로그램, 프로그래밍 인터페이스, 포털, 데이터베이스등 어떤 종류의 자원도 타 고객과 공유하지 않습니다.

전용 환경 제공 : AuthControl Cloud는 전용 가상 시스템을 제공합니다. 공유 멀티 테넌트(Multi-tenant) 옵션이 없으므로 전체 관리 및 제어가 가능합니다. 이는 솔루션을 유연하게 구성하여 고객의 요구 사항을 정확하게 충족할 수 있음을 의미합니다.

전용 방화벽 제공 : 고객별로 전용 방화벽을 제공하기 때문에 맞춤형 보안 및 액세스 제어가 가능합니다.

swivelsecure

Features

싱글사인온을 기본으로 제공

AuthControl Sentry®용 SSO(Single Sign-On) 기능은 사용자가 단일 인증 프로세스를 통해 모든 애플리케이션에 액세스가 가능하도록 해줍니다. 따라서 보안에 영향을주지않고 효율적인 작업이 가능합니다.

지속적인 보안

Swivel Secure는 사용자에게 단일 액세스 포인트를 제공하는 통합 포털을 제공합니다. 이 단일 액세스 포인트를 사용하면 사용자의 권한 관리, 감사 목적의 사용자 행동을 추적이 가능하여 보안을 강화와 책임소재의 명확화가 가능합니다.

비용 절감 효과

SSO를 활용하면 암호와 관련하여 IT 헬프데스크에 대한 호출의 필요성이 줄어들어 상당한 비용 절감 효과를가 있습니다.한번의 로그인으로 모든 애플리케이션에 액세스할 수 있기 때문에 생산성 향상에도 기여합니다.

직관적인 UI

SSO는 사용자가 리스크 기반 정책 엔진을 통해 한번의 인증으로 모든 애플리케이션에 액세스할 수 있어 높은 효율성을 제공합니다.
사용자가 VPN, 온프레미스 또는 클라우드를 통해 애플리케이션에 액세스하더라도 통합 포털 내에서 직관적인 SSO 인증이 가능하도록 자동으로 안내해 줍니다.

Features

리스크 기반 인증 : 기본 기능으로 제공

RBA(Risk-based AuthControl Sentry®)는 애플리케이션 액세스에 적합한 수준의 인증을 자동으로 요청합니다. RBA는 정책 엔진에 설정된 매개 변수를 기반으로 사용자, 해당 장치 및 사용하는 애플리케이션에 따라 승인에 필요한 적절한 수준의 인증을 요구하는 기능입니다.

다이내믹 & 지능적

사용자 환경에 따라 인증강도가 달라

- 사용자가 액세스 하려고 목적지 애플리케이션은?
- 사용자는 속한 Group은?
- 사용자가 액세스를 시도하는장소는?
- 사용자가 사용하고 있는 디바이스는?

정책 엔진

Points system에 기반한 어댑티브 인증정책 엔진을 사용하며, 관리자가 애플리케이션별, 사용자별 매개 변수를 설정할 수 있습니다.

- 사용자가 속한 그룹
- 액세스 대상 애플리케이션
- IP 주소
- 마지막 인증 시점
- X.509 Cert
- 사용하는 디바이스
- 사용자의 지리적 위치 (GeoIP)
- 지리적 이동성 : 최종 로그인한 지점에서부터 현재 로그인 장소간의 거리. 시간당 이동 가능 시간을 계산 함

리스크 기반 인증 : 사례-1

구매 담당 부서의 직원이 매니저와 함께 공급업체를 방문하기 위해 동남아로 날아갔습니다.
그녀는 방금 식당에서 식사를 마쳤는데, 다음날 회의를 위해 몇 가지 구성품의 재고 조사를 잊어버렸다는 것을 깨달았습니다. 그녀는 회사에서 발급한 모바일기를 사용하여 ERP 시스템에 빨리 로그인해야겠다고 생각했습니다.

ERP system	
필요한 점수 : 120 points	
LAN	0
Known IP	0
Managed Device	50
IP Range (Asia)	-100
필요한 인증 방식	
Username&Password	10
Mobile App	60
Fingerprint	20

결과 – 인증 실패
비록 그녀가 ERP에 접근하기 위해 회사에서 제공한 장치를 사용하고 있지만, 그녀가 있는 위치 때문에 IP 범위에 -100 포인트가 설정됩니다. 또한 그녀가 멀티팩터 인증을 사용하려고 하지만, 설정된 정책에 따르면 요구되는 포인트에 크게 못 미치게되어 ERP에 대한 접근이 허용되지 않습니다.

리스크 기반 인증 : 사례-2

판매관리자가 사무실에서 근무하고 있으며 회의 후 CRM 시스템에 접속하려고 합니다. 그는 회사에서 발행한 노트북을 사용하고 있으며 사내에 위치한 어플리케이션에 접속하고 있습니다.

CRM system	
필요한 점수 : 120 points	
LAN	50
Known IP	50
Managed Device	50
IP Range (US)	50
필요한 인증 방식	
Username&Password	10
Mobile App	60
Fingerprint	20

결과 – 인증 성공
판매관리자는 CRM에 접근하기 위해 필요한 점수를 충분히 초과합니다. 일단, 인증을 받으면 SSO(Single Sign-On)를 이용해 다른 애플리케이션에도 액세스할 수 습니다.
그는 동남아에 출장중인 구매 담당자로부터 전화를 받고 ERP 시스템에 접속해서 주어진 부품 번호의 수량을 제공할 수 도 있습니다.

최고의 유연성과 제어능력

정책 엔진을 통해 새로운 규칙을 만들고 기존 규칙을 결합할 수 있습니다. 또한 복잡성하고 다양한 시나리오를 지원하는 메커니즘을 제공할 수 있습니다.

Features

사용자 포털

사용자 포털은 관리자에게 다양한 설정 환경을 제공하고, 사용자는 사용자 포털을 통해 자신과 관련된 작업을 스스로 수행할 수 있습니다.

관리자는 사용자가 사용자 포털을 통해 PIN 변경, 재설정 또는 모바일 앱 프로비저닝과 같은 정기적인 요구 사항을 스스로 실행할 수 있도록 권한을 부여할 수 있습니다.

모바일 앱 제공

사용자는 PIN을 변경하고 재설정할 수 있을 뿐만 아니라 모바일 앱도 쉽게 프로비저닝할 수 있습니다. 모바일 앱을 프로비저닝하는 단계를 상세히 설명하는 이메일과 설정을 위한 QR 코드가 전송됩니다. 모바일 앱의 설치가 끝나면, 사용자는 일회성 코드(OTC) 또는 PUSH 알림과 같은 방법으로 모든 애플리케이션에 대한 인증이 가능합니다.

셀프 서비스

셀프 서비스 사용자 포털은 헬프데스크를 통한 지원 요청이 줄어들어 관련 비용을 크게 절감할 수 있습니다.

효율성 향상

사용자는 Swivel Secure의 사용자 포털을 통해 다음과 같은 기본 요구 사항을 스스로 수행할 수 있습니다.

- PIN 변경
- PIN 초기화
- 모바일 앱 프로비저닝
- 하드웨어 토큰 재동기화

보안 규정에 따라 정책 설정이 가능하도록 제한을 가할 수 있습니다.

Technology

PINsafe® 특허 기술

PINsafe®는 특허 기술로서 이미지 기반 PINpad®, PICpad 및 TURing의 배경 기술입니다. 이들은 AuthControl Sentry® 인증 방식의 일부분으로서 애플리케이션, 네트워크 및 데이터에 대한 무단 액세스를 방지할 수 있는 멀티팩터 인증 솔루션입니다.

PINsafe®의 작동 방식

각 사용자에게 PIN이 발급됩니다. 하지만 그 PIN이 직접 입력되지는 않습니다.

사용자에게 10자리 보안 문자열(임의 문자 또는 숫자로 구성)이 전송됩니다. 보안 문자열은 그래픽(TURing, PINPad® 또는 PICPad)으로 표시되거나 이메일 또는 SMS 통해 전송할 수 있습니다.

PIN은 제공되는 문자열에 대한 위치 표시자로 사용되어 일회용 코드가 추출됩니다.

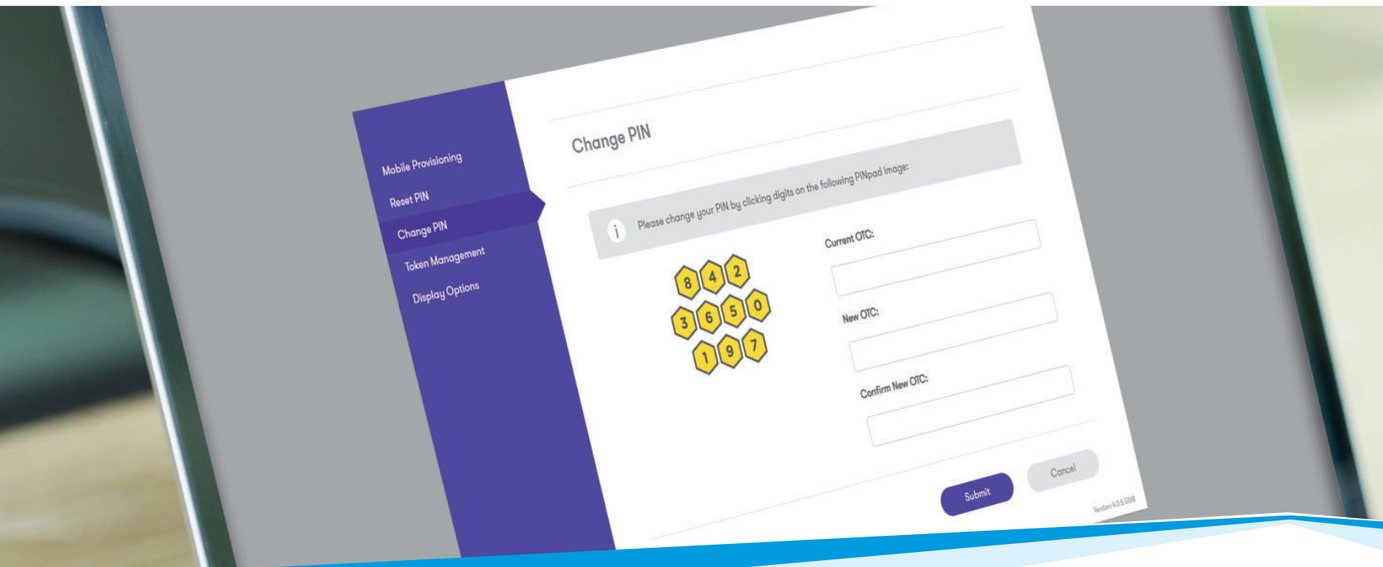
실제 사용 예

아래의 예는 PIN이 1370이고, 보안 문자열이 5721694380이므로 로그인 코드는 5240인 경우입니다.

보안 문자열은 아래와 같이 다양한 장치 및 애플리케이션들과 연동되어 활용됩니다.

- Windows 로그인
- Array Networks, Citrix, F5, Pulse등과 같은 원격 액세스 로그인
- OWA, Apache 및 Microsoft IIS를 통한 웹 액세스

Your PIN	1		3				7			0
Encrypted Security No.	5	7	2	1	6	9	4	3	8	0
Your one time code	5		2				4			0



PINsafe®는 사용자가 PIN을 직접 입력해야 하는 것을 방지하므로, 중간자 공격에 대응이 가능합니다.

Factors

다양한 인증 팩터들

Swivel Secure는 조직 전반의 다양한 분야에서 유연성있게 활용될 수있도록 광범위한 종류의 인증 팩터들을 제공합니다.

모바일 앱(AuthControl Mobile®)의 OTC, 기존 하드웨어 토큰 또는 지문 방식과 같은 다양한 인증 팩터들을 사용하여 비즈니스 보안 요구사항에 맞는 최적의 보안 및 설정 기능을 제공합니다.

AuthControl Mobile®: OTC

인증이 필요할 때마다 앱에 표시된 OTC를 사용하면 됩니다. 99개의 코드를 미리 제공할 수 있기 때문에 이 방식의 OTC 기능은 오프라인에서 사용할 수 있을 만큼 요긴합니다. 일단 코드를 입력하면, 당신이 원하는 어플리케이션에 대한 접근을 허가받을 것이다.

Image 팩터 : PINpad®

10자리 코드가 사용자의 웹 브라우저에 숫자 그리드 형태로 표시됩니다. 사용자는 자신의 PIN을 나타내는 이미지를 클릭하기만 하면 됩니다. 클릭한 각 이미지는 PIN과는 다른 OTC 코드를 AuthControl Sentry®로 전송하여 인증하게 됩니다.

Image 팩터 : PICpad

PIC패드(PICpad)는 직원과 고객 모두의 언어 다양성을 고려한 인증 팩터입니다.

PICpad는 PINPad®와 동일한 원칙을 사용하여 숫자 대신 기호를 표시하여 다국적 환경에서 일관성 있는 의미를 제공합니다.

AuthControl Mobile®: PUSH

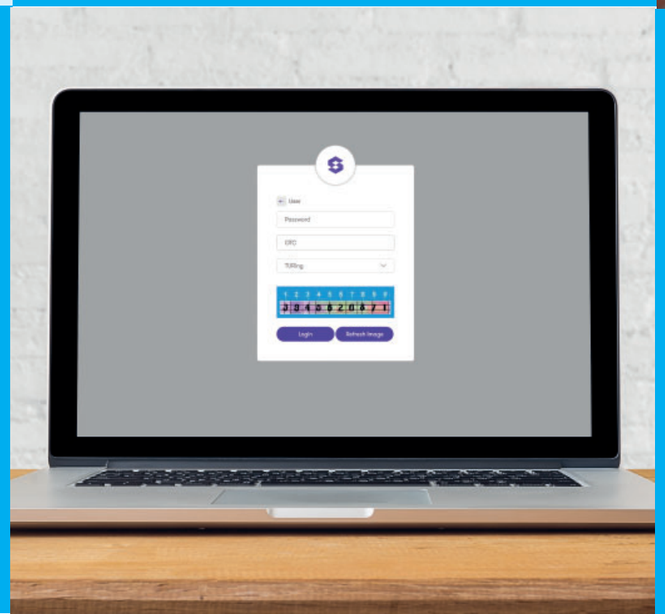
PUSH기능은 모바일 앱의 버튼을 누르기만 하면 모바일로 직접 전송되는 알림으로 인증을 확인할 수 있습니다.

최소한의 설정만으로도 Swivel One Touch® 기능을 신속하게 구축이 가능합니다.

Image 팩터 : TURing

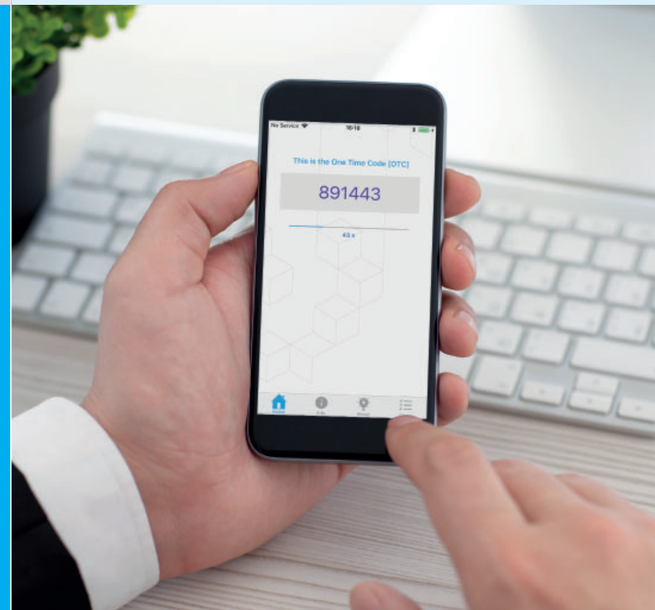
10자리 코드가 사용자의 웹 브라우저에 직사각형 이미지의 형태로 표시됩니다. 사용자는 PIN을 위치 인식자로 사용하여 이미지로부터 OTC를 얻게 됩니다.

예: PIN이 1370이면 표시된 이미지에서 첫 번째, 세 번째, 일곱 번째, 열 번째 문자를 가져오면 됩니다. 참 쉽죠?



AuthControl Mobile®: OATH

OATH 소프트 토큰은 0부터 60까지의 Time-based 토큰으로 기존 하드웨어 토큰과 유사합니다. OATH 호환 소프트 토큰은 인증에 사용될 6자리 코드를 제공합니다.



Mobile: SMS

SMS를 통한 OTC 전송에서 중간 가로채기로부터 보호하기 위해, PINsafe®를 활용합니다. SMS에는 두 개의 알파뉴메릭으로 이루어진 보안 문자열을 포함하고 있으며, 사용자의 PIN과 결합하여 OTC가 생성됩니다.
즉, 중간에 SMS 가로채기를 하여도 PIN을 모르면 OTC를 추출할 수 없습니다.

Biometrics: fingerprint

지문 인식은 Windows 10 생체 인식 프레임워크와 NITGEN 지문 액세스 컨트롤러를 사용하여 AuthControl Credential® 공급자에게 제공됩니다. 사용자는 NITGEN 지문 컨트롤러 또는 노트북에 내장된 지문 판독기를 사용하여 인증할 수 있다.

AuthControl Voice

AuthControl Voice는 사용자에게 전화를 걸어 음성으로 일회성 코드(OTC) 또는 PUSH 알림(YES 또는 NO)을 제공합니다. 사용자는 음성으로 제공된 OTC를 입력창에 입력하게 됩니다.

Hardware token

하드웨어 토큰 방식은 하드웨어 토큰의 버튼을 누를 때마다 새로운 코드를 제공하여 무단 액세스를 방지합니다.

swivelsecure

타 시스템 연동

AuthControl Sentry®는 RADIUS, ADFS, SAML 및 독자적인 API – AgentXML을 통해 수백 개의 애플리케이션 및 어플라이언스 소프트웨어와 연동이 됩니다.

AuthControl Sentry®는 Salesforce에 액세스하거나, 모바일 앱으로 인증하거나, 이미지 인증자를 사용하여 Windows Credential Provider에 로그인해야 하는 경우등 광범위한 애플리케이션과 장치를 지원합니다.

라이센스 정책

유연한 라이센스 및 가격 모델을 제공합니다. 라이센싱은 등록사용자수에 따라 결정됩니다.

User Licensing

모든 조직에 적합한 유연한 라이센스 계획 및 가격 책정 모델.

- AuthControl Sentry® 라이센스는 사용자 수에 따라 결정됨
- 각 라이센스에는 모든 인증 팩터가 포함되어 있음
- MFA, SSO 및 RBA가 AuthControl Sentry®에 모두 포함되어 있음
- 1, 3, 5 또는 7년 사용 계약 또는 영구 계약으로 사용 가능

On-Premise

온프레미스 또는 프라이빗 클라우드에서 호스팅되는 솔루션에는 영구 라이센스를 사용할 수 있습니다. 가격은 사용자당 책정되며 최소 10명의 사용자로부터 시작하며, 사용자 볼륨에 따라 단위 가격이 낮아지는 구조이기 때문에 필요한 라이선스를 한 번에 구입하는 경우가 비용효율적입니다.

Cloud

사용료 방식 라이센스는 클라우드 에 적용하기 적합합니다. 조직이 수요 변화에 따라 사용자 수를 유연하게 조정할 수 있습니다. 선불비용이 없으며 해지에 따른 페널티도 없습니다. OPEX방식의 서비스 운영과 다양한 사용자를 대상으로 하는 서비스 사업자에게 이상적인 방식입니다.

Licensing options

온프레미스 및 클라우드 라이센싱 옵션 비교

Type of License	On-Premise	Cloud
Risk-based Authentication	✓	✓
Integrations (SAML/ADFS/RADIUS)	✓	✓
On-Premise & Cloud Applications	✓	✓
All Authentication Factors	✓	✓
AD Agent & AD Sync	✓	✓
Unified Portal with Single sign-on	✓	✓
Reporting	✓	✓
Appliance (Physical/Virtual)	✓	✗
Amazon AWS Image	✗	✓
24x7x365	Optional	✓

서비스 및 기술지원

표준 및 프리미엄수준의 서비스를 제공합니다. 업그레이드, 구축, 마이그레이션 및 복잡한 연동을 위한 프로페셔널 서비스를 이용할 수도 있습니다.

Entry Level Maintenance Agreement

지원시간 : 1일 8시간, 주 5일. 소프트웨어 업그레이드, 업데이트 및 버그수정

Standard Maintenance Agreement

지원시간 : 영업일 기준 24시간

Premium Maintenance Agreement

지원 시간 : 24 x 7 지원

전문가의 지원이 즉시 필요한 조직에 이상적.

전문 기술 서비스

Swivel Secure는 멀티팩터 인증 솔루션을 설치하고 시스템 연동 및 하드웨어간의 호환성 보장을 위한 추가적인 또는 맞춤형 기술 지원이 필요한 조직을 위해 광범위한 프로페셔널 서비스를 제공합니다.

전담 엔지니어 배당

고객사 전담 엔지니어를 통해 사전 예방적 가이드와 정기점검등 모든 기술적 지원을 제공합니다.

Swivel Secure appliance 업그레이드

Swivel Secure는 업그레이드 중에 발생할 수 있는 몇 가지 문제를 인식하고 서비스와 비즈니스의 중단을 최소화하기 위해 개발된 업그레이드 서비스를 제공합니다.

복잡한 네트워크 인프라와 통합

전문 엔지니어 팀이 귀사의 기술 설계자 및 서비스 팀과 긴밀하게 협력합니다.

- 기존 네트워크 아키텍처에맞게 조정
- 조직의 아키텍처 및 변경 관리 요구 사항 충족

새로운 RADIUS 또는 SAML 연동

소프트웨어 개발팀에서 다음 작업을 수행할 수 있음:

- 새로운 통합 요구에 대한 분석 및 개발
- 새로운 플러그인 지원
- 기능 요청에 따라 지속적인 소프트웨어 개선