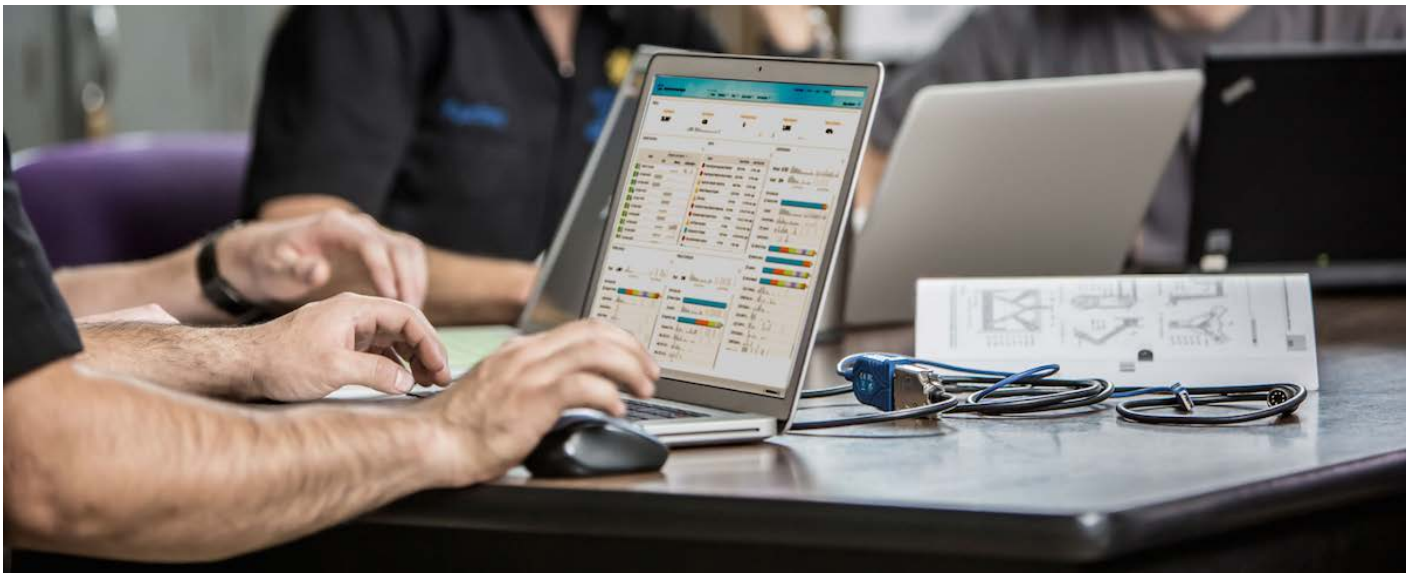


Cisco Meraki EMM과 Cisco Identity Service Engine의 통합

보안 액세스 방법 가이드 시리즈

작성자: **Imran Bashir**

날짜: **2015년 3월**

목차

MDM(Mobile Device Management)

개요

Cisco Meraki Enterprise Mobility Management(EMM) 소프트웨어는 모바일 운영자, 서비스 제공업체, 기업의 환경 전반에 구축된 모바일 디바이스를 보호, 모니터링, 관리하고 지원합니다. 일반적인 Cisco Meraki EMM 구성은 클라우드 기반 정책 서버 및 모바일 디바이스 클라이언트로 이루어집니다. 그러나 오로지 네트워크에서만 (ACL, TrustSec SGT 등에 따라) 엔드포인트에 대한 세분화된 액세스를 제공할 수 있는 경우가 많습니다. 클라우드 기반 Cisco Meraki EMM 정책 서버가 정책 결정 지점의 역할을 한다면 Cisco ISE(Identity Services Engine)는 추가적인 네트워크 기반 정책 시행 지점이 될 것입니다. 완전한 솔루션이 되기 위해서는 ISE에서 Cisco Meraki 클라우드 EMM 서버로부터 데이터를 받아야 합니다.

다음은 이 솔루션의 주요 활용 사례입니다.

디바이스 등록 – 등록되지 않은 엔드포인트가 온프레미스 방식으로 네트워크에 액세스하면 Cisco Meraki EMM 클라우드의 등록 페이지로 리디렉션되어 사용자 역할, 디바이스 유형 등에 따라 등록됩니다. 또한 Meraki는 디바이스에 기업 애플리케이션, 이를테면 AnyConnect(VPN), Jabber(협업) 등을 프로비저닝할 수 있는데, 그러면 디바이스가 오프프레미스 상태일 때 사용자가 (정책에 따라) 기업 리소스에 안전하게 액세스하는 것이 가능합니다.

리미디에이션 – 규정 준수 상태에 따라 규정 위반 엔드포인트는 제한적 액세스만 가능해집니다.

정기적인 규정 준수 확인 – 정기적으로 Cisco Meraki EMM 클라우드 서버에 규정 준수를 확인합니다.

Cisco Meraki EMM 클라우드를 통해 ISE **관리자가 디바이스에 대한 원격 작업** 수행(예: 관리 대상 디바이스의 원격 지우기)

엔드유저가 ISE My Devices Portal을 사용하여 개인 디바이스 관리(예: 전체 지우기, 전사적 지우기, PIN 잠금)

Cisco Systems © 2015

샘플 네트워크 토폴로지

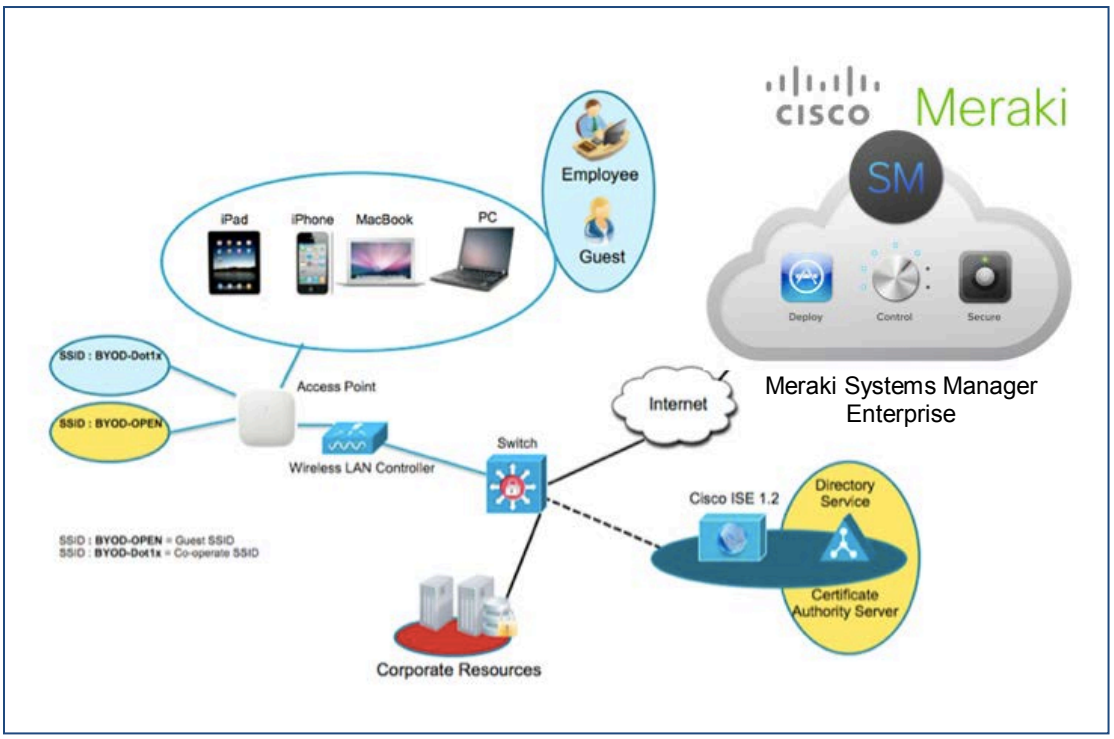


그림 1. ISE+EMM 통합 토폴로지

Cisco Meraki EMM 클라우드 통합의 활용 사례 개요

1. 사용자가 디바이스를 SSID에 연결합니다.
2. 사용자 디바이스가 등록되지 않은 경우 사용자는 BYOD 온보딩 플로우(부록 참조)를 거칩니다.
3. ISE에서 Cisco Meraki EMM 클라우드에 API 호출을 수행합니다.
4. 이 API 호출에서 해당 사용자의 디바이스 및 디바이스의 포스처 상태가 목록으로 반환됩니다. 엔드포인트 디바이스의 MAC 주소를 입력 매개변수로 전달할 수 있습니다.
5. 사용자의 디바이스가 이 목록에 없을 경우 디바이스가 Cisco Meraki EMM 클라우드에 등록되지 않았음을 의미합니다. ISE는 ISE에 리디렉션하기 위해 NAD에 권한 부여 메시지를 보냅니다. 그러면 사용자는 Cisco Meraki EMM 클라우드(홈 페이지 또는 랜딩 페이지)에 리디렉션됩니다.
6. ISE는 Cisco Meraki EMM 클라우드를 사용하여 이 디바이스를 프로비저닝해야 함을 인식하고 사용자에게 알맞은 페이지를 표시하여 등록을 진행하게 합니다.
7. 사용자는 Cisco Meraki EMM 클라우드 정책 엔진으로 이동하여 등록을 완료합니다. Cisco Meraki EMM 클라우드 서버에 의해, 또는 사용자가 브라우저를 새로 고치는 방식으로 자동 리디렉션을 통해 다시 ISE가 제어 권한을 갖습니다.
8. ISE는 Cisco Meraki EMM 클라우드에 다시 쿼리하여 포스처 상태를 파악합니다.
9. 사용자 디바이스가 Cisco Meraki EMM 클라우드에 구성된 포스처(규정 준수) 정책에 부합하지 않을 경우 디바이스의 규정 위반 사실, 그 이유, 네트워크 리소스 액세스를 위한 규정 준수의 필요성을 알립니다.
10. 사용자의 디바이스가 규정 준수 상태가 되면 Cisco Meraki EMM 클라우드가 내부 테이블에서 디바이스 상태를 업데이트합니다.

11. 이 단계에서 사용자가 브라우저를 새로 고칠 수 있으며, 그러면 다시 ISE가 제어 권한을 갖게 됩니다.
12. 또한 ISE는 정기적으로 Cisco Meraki EMM 클라우드에 폴링하여 규정 준수 정보를 얻고 적절하게 COA를 실행합니다.

구성 요소

표 1. 이 문서에서 사용된 구성 요소 Tab

구성 요소	하드웨어	테스트한 기능	Cisco IOS® Software Release
Cisco Identity Services Engine(ISE)	모두: 1121/3315, 3355, 3395, VMware, 3415, 3495	통합 AAA, 정책 서버, 서비스(게스트, 프로파일러, 포스처)	ISE 1.3
EMM 서버	EMM	클라우드 서비스	
WLC(Wireless LAN Controller)	5500-series 2500-series WLSM-2 가상 컨트롤러	프로파일링 및 COA(Change of Authorization)	Unified Wireless 7.2
Cisco Meraki Cloud Wireless LAN		Cisco Meraki EMM 클라우드를 통한 클라우드 관리형 무선 기존 WLC를 대체하는 용도로 테스트	해당 없음
테스트 디바이스: 예) Apple iOS, Google Android.	Apple & Google	해당 없음	Apple iOS 5.0 이상 Google Android 2.3 이상

참고: 이 문서의 데모에서는 Cisco Meraki EMM 클라우드 구성만 다룹니다. Cisco의 방법 가이드를 참조하여 ISE 및 WLC/Meraki를 권장 상태로 구성하는 것이 좋습니다.
방법 가이드: http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf
추가 가이드: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html
https://docs.meraki.com/display/kb/Wireless+LAN

MDM 통합 구성 단계 사용

Cisco ISE와 MDM의 통합 구성

그림 2는 MDM 통합 구성의 주요 단계를 보여줍니다.

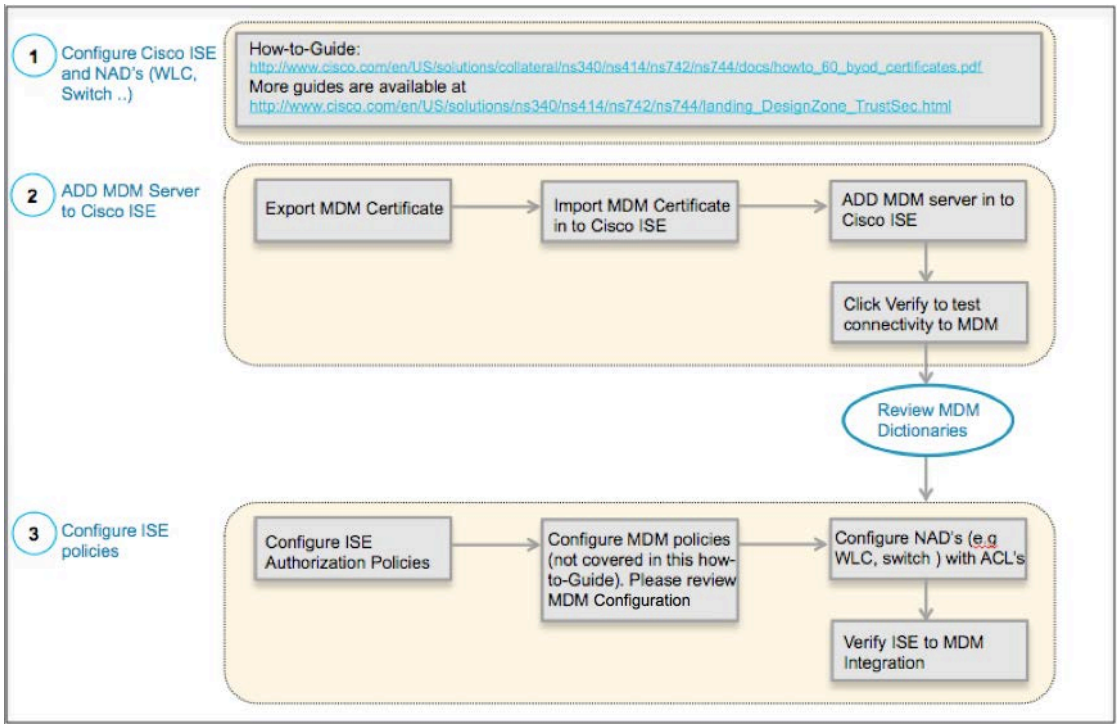


그림 2. MDM 구성 플로우

ISE에 외부 MDM 서버 추가

Cisco Meraki의 EMM 서버는 클라우드 서비스로 사용할 수 있습니다. 클라우드에서 설치, 기본 설정, 규정 준수 확인이 구성된 다음 ISE에 추가될 수 있습니다.

MDM 서버 인증서 내보내기

1단계 EMM 서버 인증서를 내보내 로컬 시스템에 저장합니다.

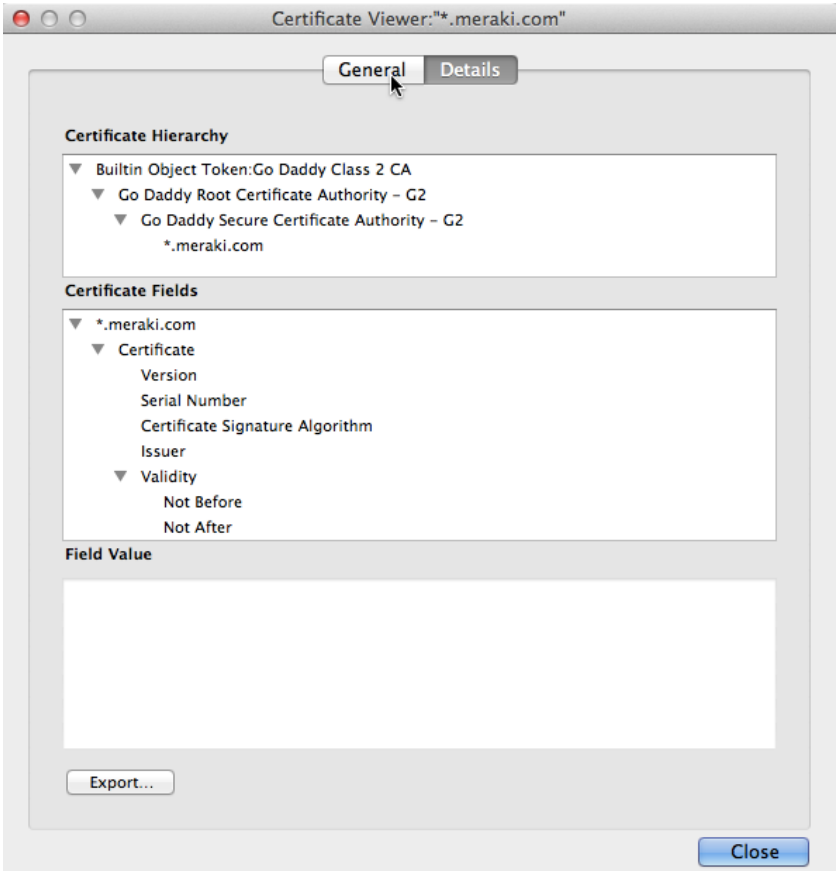


그림 3. MDM 인증서 내보내기

2단계 ISE에 인증서를 가져옵니다.

Administration -> Certificates -> Trusted Certificates -> Import로 이동합니다.

Certificate File에서 Browse를 클릭하고 Meraki Certificate를 선택합니다.

선택 사항: 친숙한 이름을 추가하고 Submit을 클릭합니다.

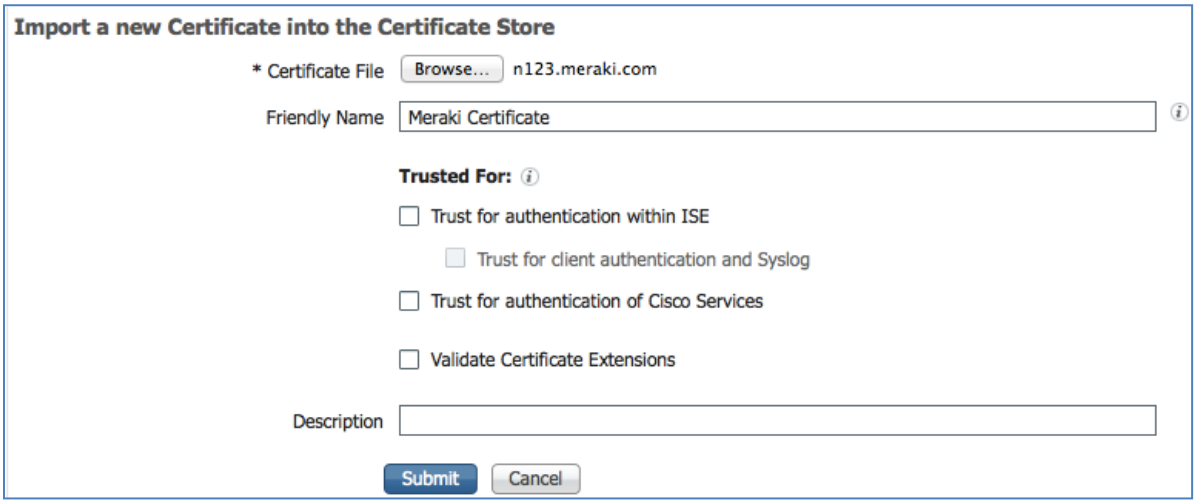


그림 4. Cisco ISE에 MDM 인증서 가져오기

3단계 인증서가 인증서 저장소에 있는지 확인합니다.

Trusted Certificates에서

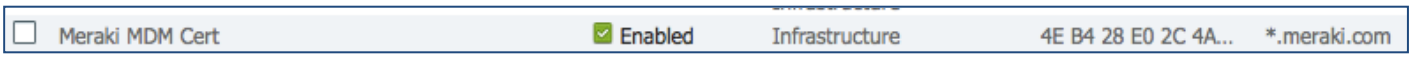


그림 5. Cisco ISE에서 MDM 인증서 확인

4단계 MDM 서버를 추가합니다. **Administration -> MDM**

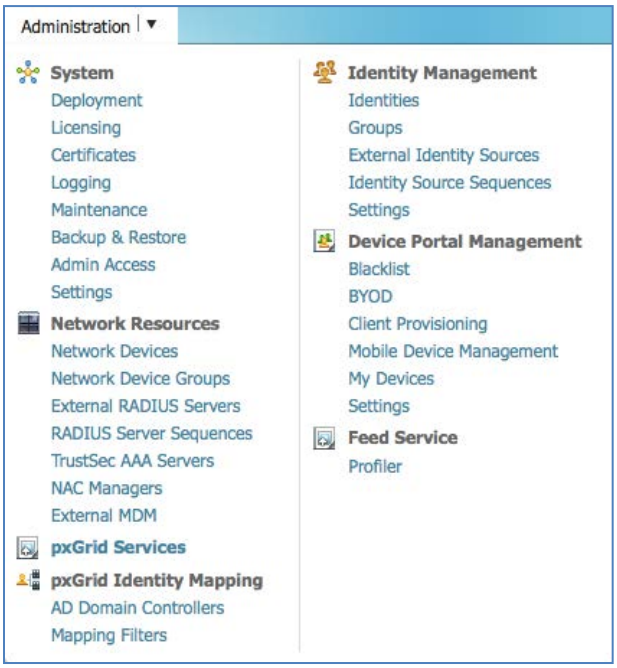


그림 6. Cisco ISE에서 MDM 서버 추가

5단계 ADD를 클릭하고 MDM 서버 세부 정보를 입력합니다.

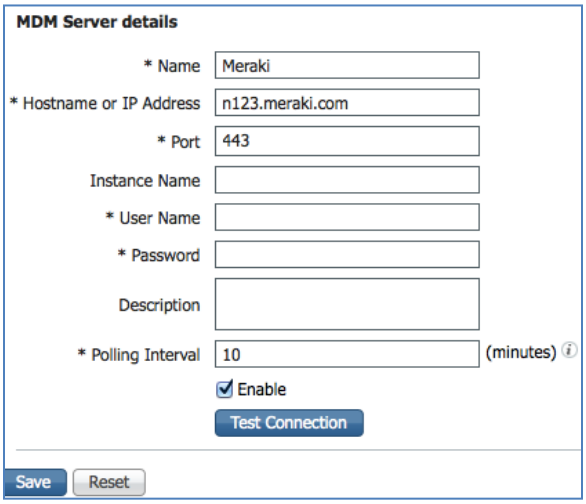


그림 7. Cisco ISE에서 MDM 서버 추가

6단계 **Test Connection**을 클릭합니다. ISE에서 연결이 작동 중임을 확인합니다.

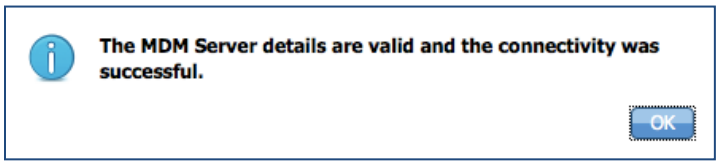


그림 8. Cisco ISE에서 MDM 서버 추가

7단계 이 팝업 창에서 OK를 클릭하고 확인란을 선택합니다. 

8단계 Submit 버튼을 클릭합니다. 서버가 추가됩니다. 

다음 성공 메시지가 관리자에게 표시됩니다.

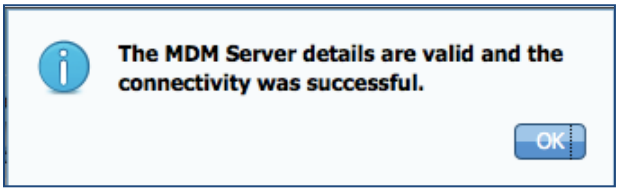


그림 9. Cisco ISE에서 MDM 서버 추가

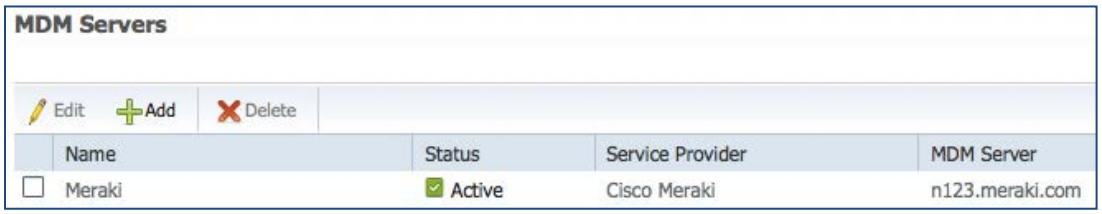


그림 10. 서버 추가 성공

MDM 딕셔너리 검토

MDM 서버가 추가되었으면 지원되는 딕셔너리가 ISE에 나타납니다. 이는 나중에 ISE 권한 부여 정책에서 사용할 수 있습니다.

1단계 **Policy -> Policy Elements -> Dictionaries -> System -> MDM -> Dictionary Attribute**로 이동합니다.

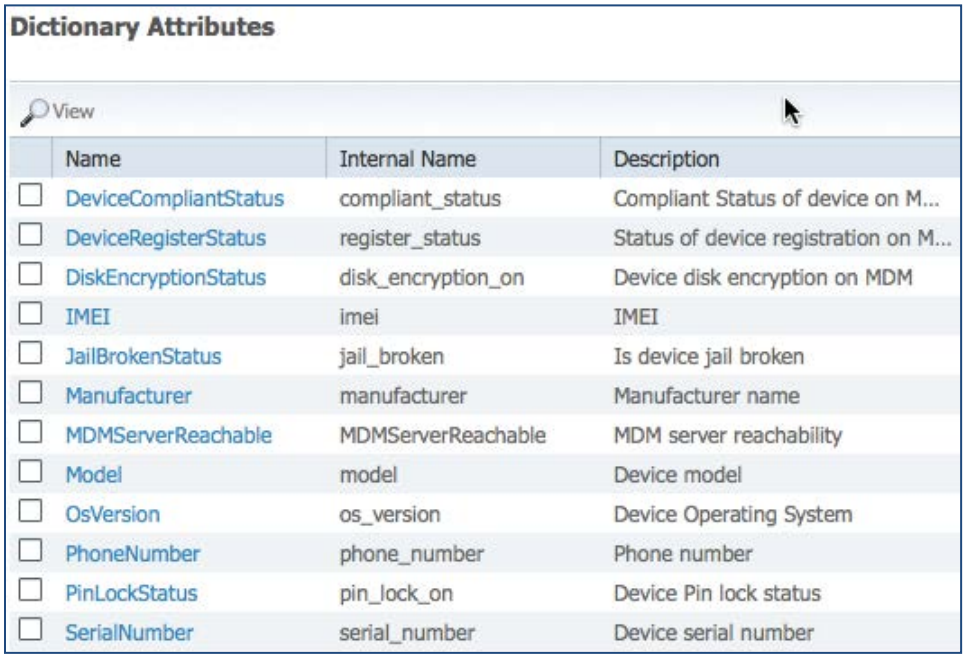


그림 11. Cisco ISE에서 MDM 딕셔너리 검토

ISE 권한 부여 정책 구성

MDM 서버가 ISE에 추가되었으면 MDM 서버를 위해 추가된 새 딕셔너리를 활용하도록 ISE에서 권한 부여 정책을 구성할 수 있습니다.

참고: 이 문서의 데모에서는 **MDM:DeviceRegisterStatus EQUALS UnRegistered** 및 **MDM:DeviceCompliantStatus EQUALS NonCompliant** 딕셔너리 속성을 사용합니다. 추가 속성도 구성하고 테스트하십시오.

2단계 WLC에서 "**NSP-ACL**"이라는 이름의 ACL을 생성합니다. 이는 나중에 정책에서 BYOD 신청자 프로비저닝, 인증서 프로비저닝, MDM 쿼런틴을 위해 선택된 클라이언트를 리디렉션하는 데 사용합니다.

- Cisco Identity Services Engine IP 주소 = 10.35.50.165
- 내부 기업 네트워크 = 192.168.0.0, 172.16.0.0(리디렉션)
- MDM 서버 서브넷 = 204.8.168.0

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

그림 12. BYOD 플로우에 클라이언트를 리디렉션하기 위한 액세스 제어 목록

NSP-ACL 설명

1. 서버에서 클라이언트로 가는 모든 "아웃바운드" 트래픽을 허용합니다.
2. 문제 해결을 위해 클라이언트에서 서버로 가는 "인바운드" ICMP 트래픽을 허용합니다. 이는 선택 사항입니다.
3. 등록되지 않고 규정에 부합하지 않은 디바이스가 MDM 에이전트를 다운로드하고 규정 준수 확인을 진행할 수 있도록 MDM 서버에 대한 액세스를 허용합니다.
4. 웹 포털 및 신청자/인증서 프로비저닝 플로우를 위해 클라이언트에서 서버와 ISE로 가는 모든 "인바운드" 트래픽을 허용합니다.
5. 이름 확인을 위해 클라이언트에서 서버로 가는 "인바운드" DNS 트래픽을 허용합니다.
6. IP 주소를 위해 클라이언트에서 서버로 가는 "인바운드" DHCP 트래픽을 허용합니다.
7. (회사 정책에 따라) ISE로 리디렉션하기 위해 클라이언트에서 서버와 기업 리소스로 가는 모든 "인바운드" 트래픽을 거부합니다.
8. (회사 정책에 따라) ISE로 리디렉션하기 위해 클라이언트에서 서버와 기업 리소스로 가는 모든 "인바운드" 트래픽을 거부합니다.

9. (회사 정책에 따라) ISE로 리디렉션하기 위해 클라이언트에서 서버와 기업 리소스로 가는 모든 "인바운드" 트래픽을 거부합니다.
10. (회사 정책에 따라) ISE로 리디렉션하기 위해 클라이언트에서 서버와 기업 리소스로 가는 모든 "인바운드" 트래픽을 거부합니다.
11. (회사 정책에 따라) ISE로 리디렉션하기 위해 클라이언트에서 서버와 기업 리소스로 가는 모든 "인바운드" 트래픽을 거부합니다.
12. (회사 정책에 따라) ISE로 리디렉션하기 위해 클라이언트에서 서버와 기업 리소스로 가는 모든 "인바운드" 트래픽을 거부합니다.
13. 나머지 트래픽을 모두 허용합니다(선택 사항).

3단계 MDM 정책에 부합하지 않은 디바이스를 위해 "MDM_Quarantine"이라는 권한 부여 프로필을 만듭니다. 이러한 경우 규정에 부합하지 않은 모든 디바이스가 ISE에 리디렉션되고 다음 메시지가 표시됩니다.

4단계 Policy → **Policy Elements → Results, Click Authorization → Authorization Profiles → ADD**를 클릭합니다.

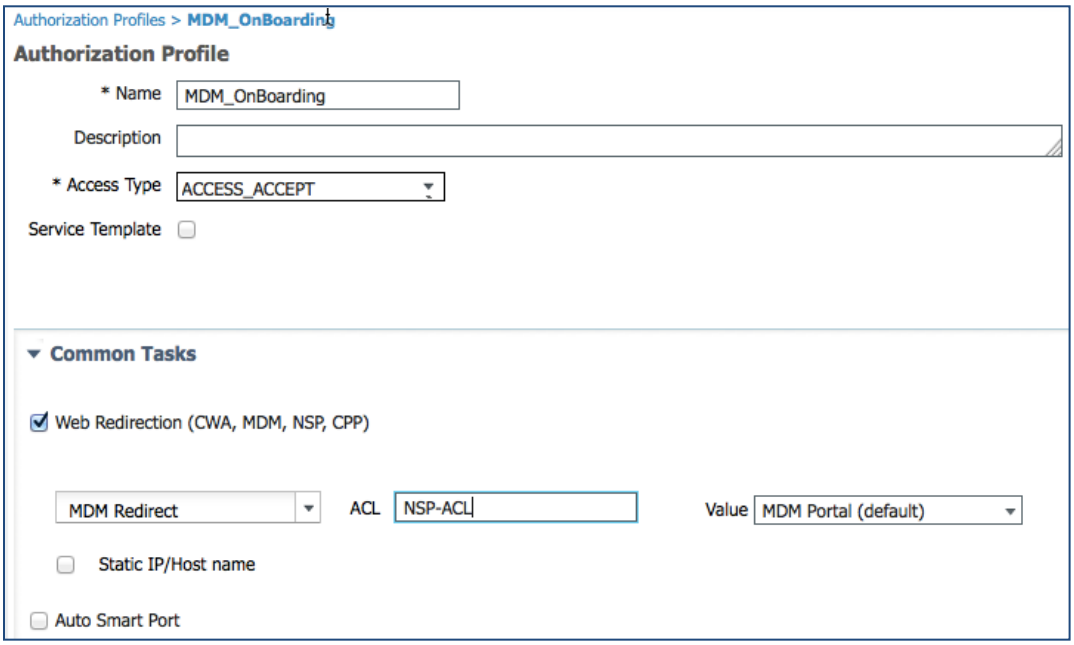


그림 13. 권한 부여 정책 구성

그림 14. NSP-ACL

참고: WLC에서 NSP-ACL를 정의해야 합니다.

5단계 권한 부여 정책을 만듭니다. Policy → **Authorization** → **Authorization Profiles**를 클릭합니다. **Insert New Rule Below**를 클릭합니다.

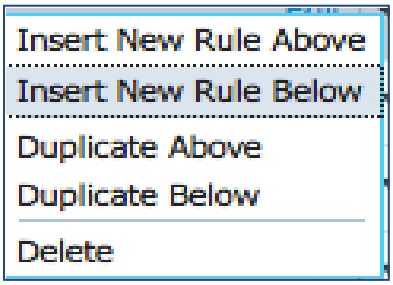


그림 15. 새 규칙 삽입

다음 권한 부여 정책을 추가하십시오.

MDM_OnBoarding = 이 권한 부여 정책은 아직 Cisco Meraki EMM 클라우드에 등록되지 않은 디바이스를 위해 추가됩니다. 디바이스가 이 규칙에 부합하면 ISE EMM 랜딩 페이지로 전달됩니다. 여기서는 사용자에게 Cisco Meraki EMM 클라우드에 디바이스를 등록하는 것에 대한 정보를 제공합니다. 엔드유저에게 Cisco Meraki 네트워크 ID를 제공해야 합니다(Meraki Dashboard의 MDM > Add devices 페이지에 있음).

그림 13: ISE에서 Meraki 네트워크 ID를 위한 EMM 포털 구성

그림 16. ISE에서 Meraki 네트워크 ID를 위한 EMM 포털 구성

MDM_OnBoarded = 디바이스가 ISE와 MDM에 등록되었고 ISE 및 MDM 정책에 부합한다면 네트워크 액세스 권한이 부여됩니다.

Default = 디바이스가 위 정책에 부합하지 않을 경우, 이를테면 MDM에 등록되지 않았거나 MDM에 부합하지 않을 경우 Default Deny Rule을 적용합니다.

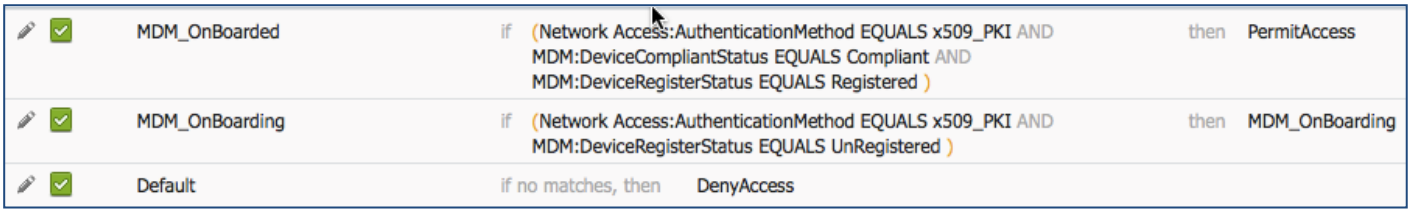
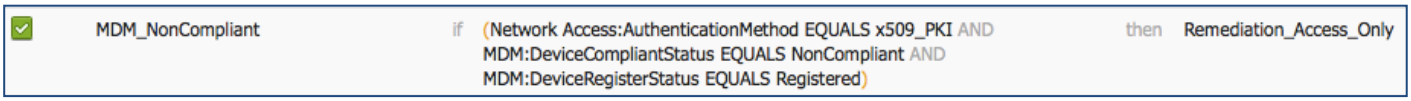


그림 17. 권한 부여 정책 구성 보기

다 끝났습니다!

참고: MDM에 등록되었지만 규정에 부합하지 않은 디바이스에게 제한적 액세스(예: 리미디에이션 액세스만)를 허용하는 규칙을 추가할 수도 있습니다.



신청자 프로필과 함께 인증서를 프로비저닝하는 것에 대한 자세한 내용은 방법 가이드 **BYOD Using Certificates for Differentiated Access**를 참조하십시오.

참고: Cisco ISE 등에 대해 더 세부적으로 MDM 정책을 정의할 수도 있습니다.

데모

i-device, Android, Windows 및 MAC OSx 온보딩의 엔드유저 경험을 살펴보려면 다음 웹 사이트를 방문하십시오.

http://wwwin.cisco.com/tech/snsbu/prod-sols/ise/#sectionName=4

부록 A: Meraki EMM 구성

여기서는 기업 정책을 위한 Cisco Meraki EMM 클라우드의 구성을 조명합니다. 활용 사례 및 기업 정책에 적합한 구성에 대해서는 Cisco Meraki 설명서를 참조하십시오. 여기서는 설정 및 실행에 필요한 간단한 구성만 다룹니다.

주요 내용은 다음과 같습니다.

- Cisco Meraki EMM 클라우드에서 가져와 ISE 서버에 구성해야 하는 ISE 설정 확인
- 엔드포인트에 푸시하도록 애플리케이션 구성

1단계 Cisco Meraki 관리 웹 인터페이스에 액세스합니다.

a. **Admin** PC에서 표준 웹 브라우저를 실행합니다. 주소 표시줄에 Cisco Meraki URL을 입력합니다.

https://dashboard.meraki.com

참고: 여기에 제시된 URL은 샘플입니다.

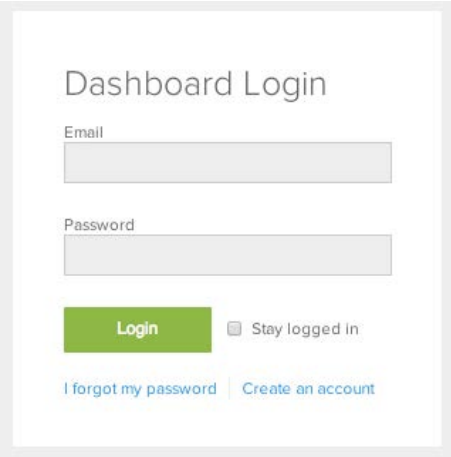


그림 18. 로그인 패널

b. 사용자 이름과 비밀번호로 로그인합니다. 로그인했으면 시스템 관리자 네트워크로 이동합니다.

2단계 ISE 설정

a. **Organization > MDM page**로 이동합니다. 여기서 "ISE 설정의" URL, 사용자 이름, 비밀번호를 확인합니다. 이 설정이 ISE 서버에서 구성되어야 합니다(이전 단원의 #4단계 참조).

그림 19. ISE 설정

3단계 Cisco Meraki Server의 보안 정책

a. Configure > Policies 페이지로 이동합니다. 여기서는 보안 정책(예: 화면 잠금, 디스크 암호화, 실행 중인 블랙리스트 애플리케이션 등)을 생성하고 구성할 수 있습니다.

b. **Configure > General → ISE settings**로 이동합니다. 어떤 정책을 ISE에 보고할지 지정할 수 있습니다.

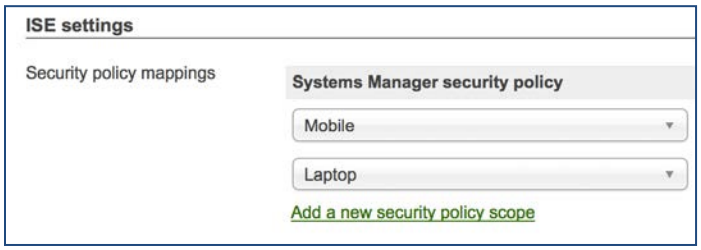


그림 20. ISE 설정

Meraki에서 애플리케이션 구성

여기서는 Cisco AnyConnect와 같은 기업 애플리케이션을 위해 Cisco Meraki EMM 클라우드를 구성합니다. 그런 다음 AnyConnect 애플리케이션과 함께 푸시할 VPN 프로필도 구성합니다. 그러면 디바이스가 오프프레미스 상태에서 (VPN을 통해) 안전하게 기업 데이터 및 애플리케이션에 액세스할 수 있습니다. Meraki 구성 인터페이스에 로그인한 다음 애플리케이션을 구성합니다.

a. **MDM > Apps** 페이지로 이동합니다.

b. 화면 오른쪽의 **Add New** 아이콘을 클릭합니다.

c. **iOS** 앱을 선택합니다.

d. 검색에 **AnyConnect**를 입력합니다.

e. **ADD**를 클릭하고 변경 내용을 저장합니다.

그림 21. Cisco AnyConnect

4단계 VPN 프로필을 구성합니다.

5단계 **MDM > Settings > VPN** 페이지로 이동합니다.

6단계 Configure a VPN network를 클릭합니다.

7단계 이름테면 **VPN Server address**를 입력합니다. 다음은 vpn.cisco.com으로 연결하는 구성입니다.

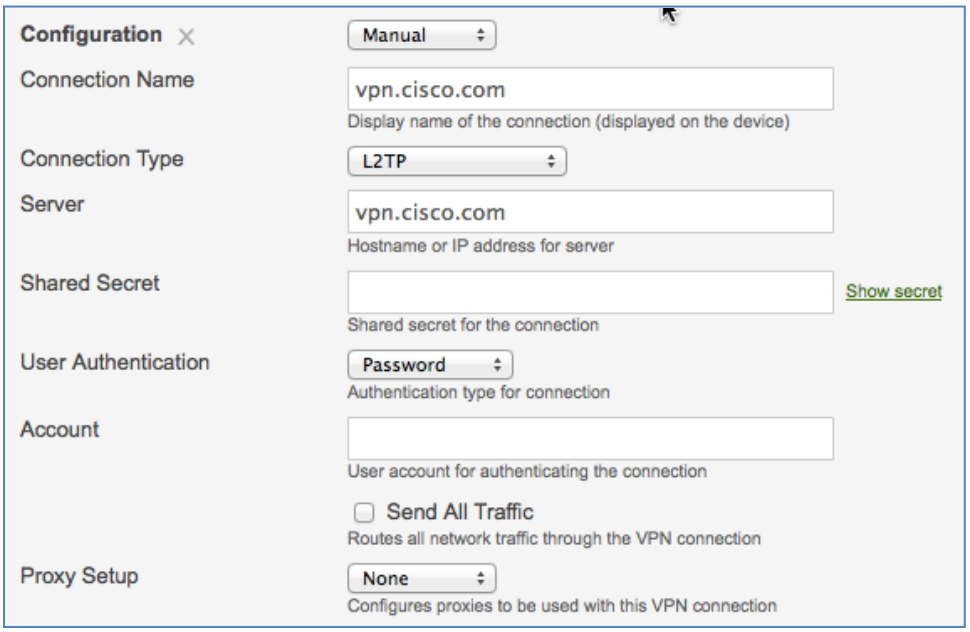


그림 22. 구성의 예

부록 B: Cisco ASA 샘플 구성

다음은 ASA 서버의 샘플 구성입니다. 여기서는 Meraki MDM 프로비저닝 디바이스 애플리케이션인 **Cisco AnyConnect**가 다시 연결하여 VPN 연결을 설정할 수 있습니다.

이 설정에 사용한 ASA 버전 = ASA Version 9.3(1)
하드웨어: ASA5515, 8192MB RAM, CPU Clarkdale 3059MHz, 1CPU(4코어)

외부 인터페이스, DNS 및 ISE 정책 서비스 노드의 IP 구성은 바뀝니다. 실제 네트워크의 ASA 및 ISE IP 주소로 대체하십시오.

외부 인터페이스의 IP 주소 = 1.1.1.100
기본 게이트웨이의 IP 주소 = 1.1.1.1
ISE PSN 노드의 IP 주소 = 2.2.2.2
DNS 서버의 IP 주소 = 10.10.10.10

```
ASA Version 9.3(1)
!
terminal width 511
hostname VPN
domain-name test.ocm
names
ip local pool user-dhcp-pool 10.42.36.10-10.42.36.254 mask 255.255.254.0
!
interface GigabitEthernet0/0
 speed 1000
 duplex full
 nameif outside
 security-level 0
 ip address 1.1.1.100 255.255.255.248 standby 1.1.1.101
!
interface GigabitEthernet0/1
 speed 1000
 duplex full
 nameif inside
 security-level 100
 ip address 10.42.20.148 255.255.255.248 standby 10.42.20.149
!
!
boot system disk0:/asa931-smp-k8.bin
ftp mode passive
clock timezone PST8PDT -8
clock summer-time PDT recurring10.10.10.10
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 10.10.10.10
domain-name test.ocm
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network ocsp.quovadisglobal.com
 fqdn ocsp.quovadisglobal.com
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list pre-posture remark exclude DNS server
access-list pre-posture extended deny ip any host 10.10.10.10
access-list pre-posture extended permit tcp any host 2.2.2.2 eq www
```

```
access-list pre-posture remark exclude ISE PSN Servers
access-list pre-posture extended deny ip any host 2.2.2.2
access-list pre-posture remark Permit ALL Traffic
access-list pre-posture extended permit ip any any
access-list pre-posture extended permit ip any object ocsp.quovadisglobal.com log
access-list test extended permit icmp any any
access-list 101 extended permit icmp any any
access-list test101 extended permit ip any4 any4
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
asdm image disk0:/asdm-731-101.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route outside 0.0.0.0 0.0.0.0 1.1.1.1 1
route inside 10.19.151.208 255.255.255.240 1.1.1.103 1
route inside 0.0.0.0 0.0.0.0 1.1.1.103 tunneled
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
aaa-server RADIUS-SERVERS protocol radius
 accounting-mode simultaneous
 interim-accounting-update
 max-failed-attempts 5
 merge-dacl before-avpair
 dynamic-authorization
aaa-server RADIUS-SERVERS (inside) host 2.2.2.2
 timeout 21
 key *****
 authentication-port 1812
 accounting-port 1813
 radius
-common-pw *****
 acl-netmask-convert auto-detect
acl-netmask-convert auto-detect
aaa-server OTP protocol radius
aaa-server OTP (inside) host 10.35.48.251
 key *****
aaa-server OTP_ETE protocol radius
aaa-server OTP_ETE (inside) host 10.35.50.200
 key *****
 radius-common-pw *****
user-identity default-domain LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console MGMT-RBAC LOCAL
http server enable 8443
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
service resetoutside
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev2 ipsec-proposal ESP
 protocol esp encryption aes-gcm-256 aes-gcm-192
 protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES256
```

```
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal SAMPG-IKE
 protocol esp encryption aes-256 aes-192 3des
 protocol esp integrity sha-256 sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map REMOTE-ACCESS 10 set pfs group5
crypto dynamic-map REMOTE-ACCESS 10 set ikev1 transform-set ESP-AES-256-SHA
crypto dynamic-map REMOTE-ACCESS 10 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-
AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-
MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES
DES
crypto map RA-IPSEC-VPN 10 ipsec-isakmp dynamic REMOTE-ACCESS
crypto map RA-IPSEC-VPN interface outside
crypto map inside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map inside_map interface inside
crypto ca trustpoint ciscoca
 enrollment terminal
 subject-name CN=vpn.test.ocm
 keypair sslvpnkeypair
 crl configure
subject-name CN=10.35.91.252,CN=vpn
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 fqdn vpn.test.ocm
 subject-name CN=vpn.test.ocm,OU=ISE,O=Cisco,C=US
 crl configure
crypto ca trustpoint ASDM_TrustPoint1
 enrollment terminal
 fqdn vpn.test.ocm
 subject-name CN=vpn.test.ocm,OU=ISE,O=Cisco,C=US
 keypair sslvpnkeypair
 crl configure
crypto ca trustpoint ASDM_Launcher_Access_TrustPoint_23
 enrollment self
 subject-name CN=10.35.91.252,CN=vpn
 crl configure
crypto ca trustpoint ASDM_Launcher_Access_TrustPoint_24
 enrollment self
 subject-name CN=10.35.91.252,CN=vpn
 crl configure
crl configure
crypto ca trustpool policy
crypto ca certificate chain ciscoca

crypto ikev2 policy 1
 encryption aes-256 aes-192 aes 3des
 integrity sha256 sha md5
 group 14 5 2 1
 prf sha256 sha
 lifetime seconds 86400
crypto ikev2 remote-access trustpoint ciscoca
crypto ikev1 enable outside
crypto ikev1 enable inside
crypto ikev1 policy 1
 authentication pre-share
```

```
 encryption aes-256
 hash sha
 group 5
 lifetime 86400
crypto ikev1 policy 2
 authentication pre-share
 encryption aes-192
 hash sha
 group 5
 lifetime 86400
crypto ikev1 policy 3
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
```

```
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
no ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 30
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
!
tls-proxy maximum-session 200
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 171.68.38.65 source inside prefer
ntp server 10.81.254.202 source inside
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ciscoca outside
ssl trust-point ASDM_Launcher_Access_TrustPoint_28 inside
ssl trust-point ASDM_Launcher_Access_TrustPoint_28 inside vpnlb-ip

group-policy DfltGrpPolicy attributes
 dns-server value 10.10.10.10
 vpn-idle-timeout 1440
 vpn-session-timeout 28800
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client
 ipsec-udp enable
 default-domain value test.ocm
 webvpn
  anyconnect ssl rekey time 300
  anyconnect ssl rekey method ssl
  anyconnect profiles value vpnlisting type user
group-policy CISCOVPN internal
group-policy CISCOVPN attributes
 dns-server value 10.10.10.10
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 2
 vpn-idle-timeout 1440
```

```
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2 ssl-client
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain value test.ocm
 backup-servers keep-client-config
 webvpn
  anyconnect ssl rekey method ssl
  anyconnect modules value dart,iseposture
  anyconnect profiles value vpnlisting type user
dynamic-access-policy-record DfltAccessPolicy
username sampg password n4q2SM5y13X3ysFc encrypted privilege 15
username admin password ezv7202P8kRjcMXI encrypted privilege 15
tunnel-group npf-sjvpn type remote-access
tunnel-group npf-sjvpn general-attributes
 address-pool user-dhcp-pool
 authentication-server-group RADIUS-SERVERS
 accounting-server-group RADIUS-SERVERS
 default-group-policy CISCOVPN
tunnel-group npf-sjvpn webvpn-attributes
 group-alias SAMPG-IPSEC-VPN disable
group-alias SAMPG-SSL-VPN enable
tunnel-group npf-sjvpn ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
!
service-policy global_policy interface outside
prompt hostname priority state
no call-home reporting anonymous
Cryptochecksum:f75d25311e04e6a83e7e2b0b4d5ce1b1
: end
```

부록 C: 참조

Cisco TrustSec System:

http://www.cisco.com/go/trustsec

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

디바이스 구성 설명서:

Cisco Identity Services Engine 사용 설명서:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Cisco IOS Software, Cisco IOS XE Software, Cisco NX-OS Software 릴리스에 대한 자세한 내용은 다음 URL을 참조하십시오.

Cisco Catalyst 2900 Series 스위치:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

Cisco Catalyst 3000 Series 스위치:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

Cisco Catalyst 3000-X Series 스위치:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

Cisco Catalyst 4500 Series 스위치:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

Cisco Catalyst 6500 Series 스위치:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

Cisco ASR 1000 Series 라우터:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

Cisco Wireless LAN Controller:
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html