Cisco ISE 포트 참조

Cisco ISE 모든 페르소나 노드 포트

표 *1:* 모든 노드에서 사용하는 포트

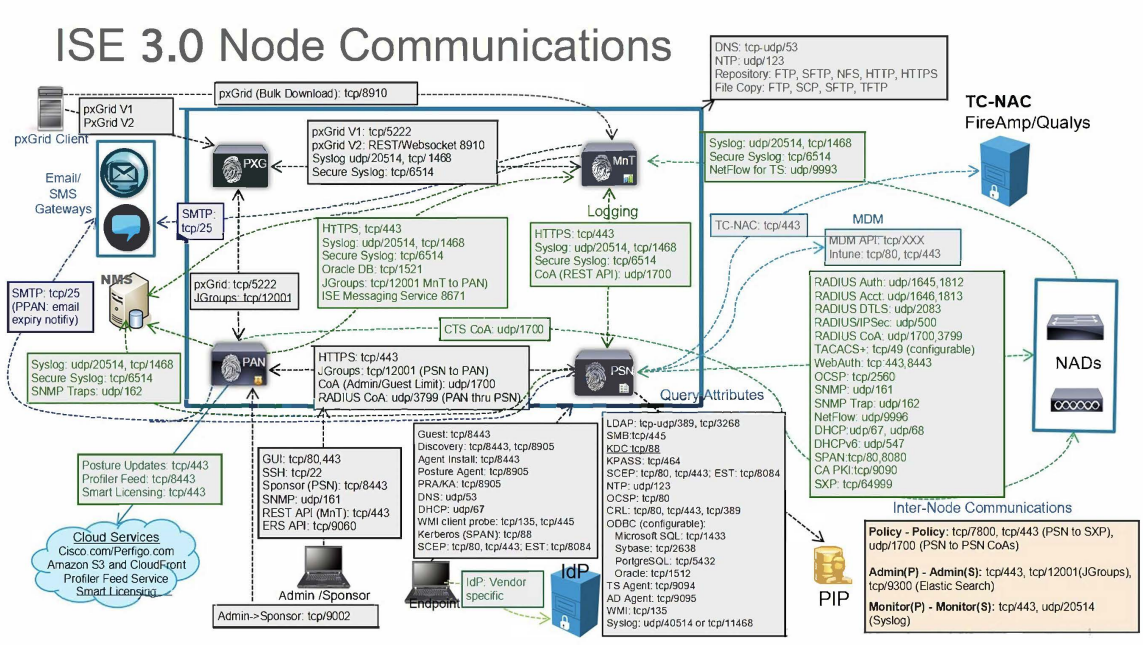
Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스**(**기가비트 이더넷 **1~5,** 결합 **1** 및 **2)**의 포트
복제 및 동기화	• HTTPS(SOAP): TCP/443 • 데이터 동기화/복제 (JGroups): TCP/12001(글로벌) • ISE 메시징 서비스: SSL: TCP/8671 • 프로파일러 엔드포인트 소유권 동기화/복제: TCP/6379	—

Cisco ISE 인프라

이 부록에서는 Cisco ISE에서 외부 애플리케이션 및 디바이스와의 인트라네트워크 통신에 사용하는 TCP 및 User Datagram Protocol UDP 포트를 나열합니다. 이 부록에 나열된 Cisco ISE 포트는 해당 방화벽에서 열린 상태여야 합니다.

Cisco ISE 네트워크에서 서비스를 구성할 때 다음 사항을 기억하십시오.

- 포트는 구축에서 활성화된 서비스에 따라 활성화됩니다. Cisco ISE는 ISE에서 실행 중인 서비스가 여는 포트 외의 다른 모든 포트에 대한 액세스를 거부합니다.
- Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다.
- RADIUS는 모든 NIC(Network Interface Card)에서 수신합니다.
- Cisco ISE 서버 인터페이스는 VLAN 태깅을 지원하지 않습니다. 하드웨어 어플라이언스에 설치하는 경우, Cisco ISE 노드에 연결하는 데 사용하는 스위치 포트에서 VLAN 트렁킹를 비활성화하고 이러한 포트를 액세스 레이어 포트로 구성해야 합니다.
- 임시 포트 범위는 10000 ~ 65500입니다. 이는 Cisco ISE 릴리스 2.1 이상에서도 동일하게 유지됩니다.
- 클라우드의 VMware는 사이트 대 사이트 VPN 네트워크 구성에서 지원됩니다. 따라서 NAT 또는 포트 필터링 없이 네트워크 액세스 디바이스 및 클라이언트에서 Cisco ISE 로의 IP 주소 또는 포트 연결성을 설정해야 합니다.
- 모든 NIC는 IP 주소로 구성할 수 있습니다.



참고 ISE에서 TCP 연결 유지 시간은 60분입니다. ISE 노드간에 TCP 시간 초과 값이 있으면 방화벽에서 적절하게 조정합니다.

Cisco ISE 관리 노드 포트

다음 표에는 관리 노드에서 사용하는 포트가 나와 있습니다.

표 *2:* 관리 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스**(**기가비트 이더넷 **1~5,** 결합 **1** 및 **2)**의 포트
관리	• HTTP: TCP/80, HTTPS: TCP/443(TCP/80이 TCP/443으로 리디렉션, 구성 불가) • SSH 서버: TCP/22 • 외부 RESTful 서비스(ERS) REST API: TCP/9060 • 관리자 GUI에서의 게스트 계정 관리: TCP/9002 • ElasticSearch(상황 가시성, 기본 관리자 노드의 데이터를 보조 관리자 노드로 복제): TCP/9300 참고 포트 80 및 443은 관리 웹 애플리케이션을 지원하며 기본적으로 활성화되어 있습니다. Cisco ISE에 대한 HTTPS 및 SSH 액세스는 기가비트 이더넷 0으로 제한됩니다. TCP/9300는 수신 트래픽용 기본 및 보조 관리 노드 모두에서 열려 있어야 합니다.	—

Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스**(**기가비트 이더넷 **1~5,** 결합 **1** 및 **2)**의 포트
모니터링	• SNMP 쿼리: UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다. • ICMP	
로깅(아웃바운드)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. • SNMP 트랩: UDP/162	
외부 ID 소스 및 리소스(아웃바운드)	• 관리자 사용자 인터페이스 및 엔드포인트 인증 • LDAP: TCP/389, 3268, UDP/389 • SMB: TCP/445 • KDC: TCP/88 • KPASS: TCP/464 • WMI: TCP/135 • ODBC: 참고 ODBC 포트는 타사 데이터베이스 서버에서 구성할 수 있습니다. • Microsoft SQL: TCP/1433 • Sybase: TCP/2638 • PortgreSQL: TCP/5432 • Oracle: TCP/1521 • NTP: UDP/123 • DNS: UDP/53, TCP/53 참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스(기가비트 이더넷 1~5, 결합 1 및 2)의 포트
Email(이메일)	게스트 계정 및 사용자 암호 만료 이메일 알림: SMTP: TCP/25	
스마트 라이선싱	TCP/443을 통한 Cisco 클라우드 연결	

Cisco ISE 모니터링 노드 포트

다음 표에는 모니터링 노드에서 사용하는 포트가 나와 있습니다.

표 *3:* 모니터링 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스(기가비트 이더넷 1~5, 결합 1 및 2)의 포트
관리	• HTTP: TCP/80, HTTPS: TCP/443 • SSH 서버: TCP/22	—
모니터링	SNMP(Simple Network Management Protocol): UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다. • ICMP	
로깅	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. • SMTP: 알림 이메일용 TCP/25 • SNMP 트랩: UDP/162	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스(기가비트 이더넷 1~5, 결합 1 및 2)의 포트

외부 ID 소스 및 리소스(아웃바운드)	• 관리자 사용자 인터페이스 및 엔드포인트 인증
	  • LDAP: TCP/389, 3268, UDP/389
	  • SMB: TCP/445
	  • KDC: TCP/88, UDP/88
	  • KPASS: TCP/464
	• WMI: TCP/135
	• ODBC:
	  참고 ODBC 포트는 타사 데이터베이스 서버에서 구성할 수 있습니다.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521, 15723, 16820
	• NTP: UDP/123
	• DNS: UDP/53, TCP/53
	참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.	

pxGrid용 일괄 다운로드	SSL: TCP/8910	

Cisco ISE 정책 서비스 노드 포트

보안 강화를 위해 Cisco ISE는 HSTS(HTTP Strict Transport Security)를 지원합니다. Cisco ISE는 HTTPS 응답을 보내 HTTPS를 이용해야 ISE에만 액세스할 수 있음을 브라우저에 알립니다. 사용자가 HTTPS가 아닌 HTTP를 이용해 ISE에 액세스하려고 하면, 브라우저는 HTTPS 연결로 변경한 다음 네트워크 트래픽 생성을 시작합니다. 이 기능을 사용하면 서버가 리디렉션하기 전에 브라우저가 암호화되지 않은 HTTP를 사용하여 Cisco ISE에 요청을 전송하는 일을 방지할 수 있습니다.

다음 표에는 정책 서비스 노드에서 사용하는 포트가 나와 있습니다.

표 *4:* 정책 서비스 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스 또는 결합 **1** 및 **2**의 포트
관리	• HTTP: TCP/80, HTTPS: TCP/443 • SSH 서버: TCP/22 • OCSP: TCP/2560	Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다.
클러스터링(노드 그룹)	노드 그룹/JGroups: TCP/7800	—
SCEP	TCP/9090	—
IPSec/ISAKMP	UDP/500	—
디바이스 관리	TACACS+: TCP/49 참고 이 포트는 릴리스 2.1 이상에서 구성할 수 있습니다.	
SXP	• PSN(SXP 노드)에서 NAD: TCP/64999 • PSN에서 SXP(노드 간 통신): TCP/443	
TC-NAC	TCP/443	
모니터링	SNMP(Simple Network Management Protocol): UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다.	
로깅(아웃바운드)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. • SNMP 트랩: UDP/162	
세션	• RADIUS 인증: UDP/1645, 1812 • RADIUS 계정 관리: UDP/1646, 1813 • RADIUS DTLS 인증/계정 관리: UDP/2083. • RADIUS CoA(Change of Authorization) Send: UDP/1700 • RADIUS CoA(Change of Authorization) Listen/Relay: UDP/1700, 3799 참고 UDP 포트 3799는 구성 불가합니다.	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스 또는 결합 1 및 2의 포트

외부 ID 소스 및 리소스(아웃바운드)	• 관리자 사용자 인터페이스 및 엔드포인트 인증
	  • LDAP: TCP/389, 3268
	  • SMB: TCP/445
	  • KDC: TCP/88
	  • KPASS: TCP/464
	• WMI: TCP/135
	• ODBC:
	  참고 ODBC 포트는 타사 데이터베이스 서버에서 구성할 수 있습니다.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521
	• NTP: UDP/123
	• DNS: UDP/53, TCP/53
	참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.	

패시브 ID(인바운드)	• TS Agent: tcp/9094 • AD Agent: tcp/9095 • Syslog: UDP/40514, TCP/11468	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스 또는 결합 1 및 2의 포트
웹 포털서비스 - 게스트/웹 인증 - 게스트 스폰서 포털 - 내 디바이스 포털 - 클라이언트 프로비저닝 - 인증서 프로비저닝 - 차단 목록 포털	HTTPS(Cisco ISE 서비스를 위해 인터페이스가 활성화되어야 함) • 차단 목록 포털: TCP/8000-8999(기본 포트는 TCP/8444.) • 게스트 포털 및 클라이언트 프로비저닝: TCP/8000-8999(기본 포트는 TCP/8443) • 인증서 프로비저닝 포털: TCP/8000~8999(기본 포트는 TCP/8443입니다.) • 내 디바이스 포털: TCP/8000-8999(기본 포트는 TCP/8443) • 스폰서 포털: TCP/8000-8999(기본 포트는 TCP/8443) • 게스트 및 스폰서 포털의 SMTP 게스트 알림: TCP/25	
포스처 - 검색 - 프로비저닝 - 평가/하트비트	• 검색(클라이언트): TCP/80(HTTP), TCP/8905(HTTPS) 참고 기본적으로 TCP/80은 TCP/8443으로 리디렉션됩니다. 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 Cisco ISE는 TCP 포트 8905에서 포스처 및 클라이언트 프로비저닝용 관리자 인증서를 제공합니다. Cisco ISE는 TCP 포트 8443(또는 포털 사용을 위해 구성한 포트)에서 포털 인증서를 제공합니다. • 검색(정책 서비스 노드): TCP/8443, 8905(HTTPS) AnyConnect를 지원하는 Cisco ISE, 릴리스 2.2 이상 또는 릴리스 4.4 이상에서 이 포트를 구성할 수 있습니다. • 평가 - 포스처 협상 및 에이전트 보고서: TCP/8905(HTTPS)	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스 또는 결합 1 및 2의 포트
BYOD(Bring Your Own Device)/NSP(Network Service Protocol) - 리디렉션 - 프로비저닝 - SCEP	• 프로비저닝 - URL 리디렉션: 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 • EST 인증이 포함된 Android 장치의 경우: TCP/8084. 포트 8084은 Android 장치용 Redirect ACL에 추가해야 합니다. • 프로비저닝 - Active-X 및 Java Applet 설치(마법사 설치 시작 포함): 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 • 프로비저닝 - Cisco ISE에서 마법사 설치(Windows, Mac OS): TCP/8443 • 프로비저닝 - Google Play에서 마법사 설치(Android): TCP/443 • 프로비저닝 - 신청자 프로비저닝 프로세스: TCP/8905 • SCEP 프록시-CA: TCP/80 또는 TCP/443(SCEP RA URL 컨피그레이션 기반)	
MDM(Mobile Device Management) API 통합	• URL 리디렉션: 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 • API: 벤더별 • 에이전트 설치 및 디바이스 등록: 벤더별	
프로파일링	• NetFlow: UDP/9996 참고 이 포트는 구성 가능합니다. • DHCP: UDP/67 참고 이 포트는 구성 가능합니다. • DHCP SPAN Probe: UDP/68 • HTTP: TCP/80, 8080 • DNS: UDP/53(lookup) 참고 이 포트는 라우트 테이블에 따라 달라집니다. • SNMP 쿼리: UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다. • SNMP 트랩: UDP/162 참고 이 포트는 구성 가능합니다.	

Cisco ISE pxGrid Service 포트

다음 표에는 pxGrid 서비스 노드에서 사용하는 포트가 나와 있습니다.

표 ***5: pxGrid*** 서비스 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스**(**기가비트 이더넷 **1~5,** 결합 **1** 및 **2)**의 포트
관리	• SSL: TCP/5222(노드 간 통신) • SSL: TCP/7400(노드 그룹 통신)	—
pxGrid 가입자	TCP/8910	

OCSP 및 CRL 서비스 포트

OCSP(Online Certificate Status Protocol) 서비스 및 CRL(Certificate Revocation List)에서는 OCSP/CRL을 호스팅하는 서비스 또는 CA 서버에 따라 포트가 달라집니다. 다만 Cisco ISE 서비스 및 포트에 대한 참조에서는 Cisco ISE 관리 노드, 정책 서비스 노드모니터링 노드에서 각각 사용하는 기본 포트가 나열됩니다.

OCSP의 경우 사용 가능한 기본 포트는 TCP 80/TCP 443입니다. Cisco ISE 관리 포털에서는 OCSP 서비스에 대해 http 기반 URL을 기대하므로 TCP 80이 기본값입니다. 비기본 포트를 사용할 수도 있습니다.

CRL에서는 기본 프로토콜에 HTTP, HTTPS, LDAP가 포함되며 기본 포트는 각각 80, 443, 389입니다. 실제 포트는 CRL 서버에 따라 달라집니다.

Cisco ISE 프로세스

다음 표에는 Cisco ISE 프로세스 및 프로세스 서비스 영향이 나와 있습니다.

프로세스 이름	Description(설명)	서비스 영향
데이터베이스 리스너	Oracle 엔터프라이즈 데이터베이스 리스너	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
데이터베이스 서버	Oracle 엔터프라이즈 데이터베이스 서버입니다. 구성 및 운영 데이터를 모두 저장합니다.	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.

Application Server(애플리케이션 서버)	ISE용 메인 Tomcat 서버	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
프로파일러 데이터베이스	ISE 프로파일링 서비스용 Redis 데이터베이스	ISE 프로파일링 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
AD 커넥터	Active Directory Runtime	Active Directory 인증을 수행하려면 ISE에 대해 Running(실행 중) 상태여야 합니다.
MnT 세션 데이터베이스	MnT 서비스용 Oracle TimesTen 데이터베이스	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
MnT 로그 수집기	MnT 서비스용 로그 수집기	MnT 운영 데이터에 대해 Running(실행 중) 상태여야 합니다.
MnT 로그 프로세서	MnT 서비스용 로그 프로세서	MnT 운영 데이터에 대해 Running(실행 중) 상태여야 합니다.
Certificate Authority 서비스	ISE 내부 CA 서비스	ISE 내부 CA가 활성화되었다면 Running(실행 중) 상태여야 합니다.

필수 인터넷 URL

다음 표에는 특정 URL을 사용하는 기능이 나와 있습니다. IP 트래픽이 Cisco ISE 및 이러한 리소스 간에 이동할 수 있도록 네트워크 방화벽 또는 프록시 서버 중 하나를 구성해야 합니다. 나열된 URL에 대해 이 액세스를 제공할 수 없는 경우에는 관련된 기능이 손상되거나 작동하지 않습니다.

표 *6:* 필수 *URL* 액세스

기능	URL
포스처 업데이트	https://www.cisco.com/ https://iseservice.cisco.com
프로파일링 피드 서비스	https://ise.cisco.com
스마트 라이선싱	https://tools.cisco.com
대화형 도움말	https://cdn.walkme.com https://playerserver.walkme.com https://ec.walkme.com https://rapi.walkme.com https://papi.walkme.com https://s3.amazonaws.com https://s3.walkmeusercontent.com