Cisco ISE와 WSA 통합 가이드

Revised: December 8, 2015,

Cisco ISE와 WSA 통합

Cisco ISE와 WSA 통합 개요

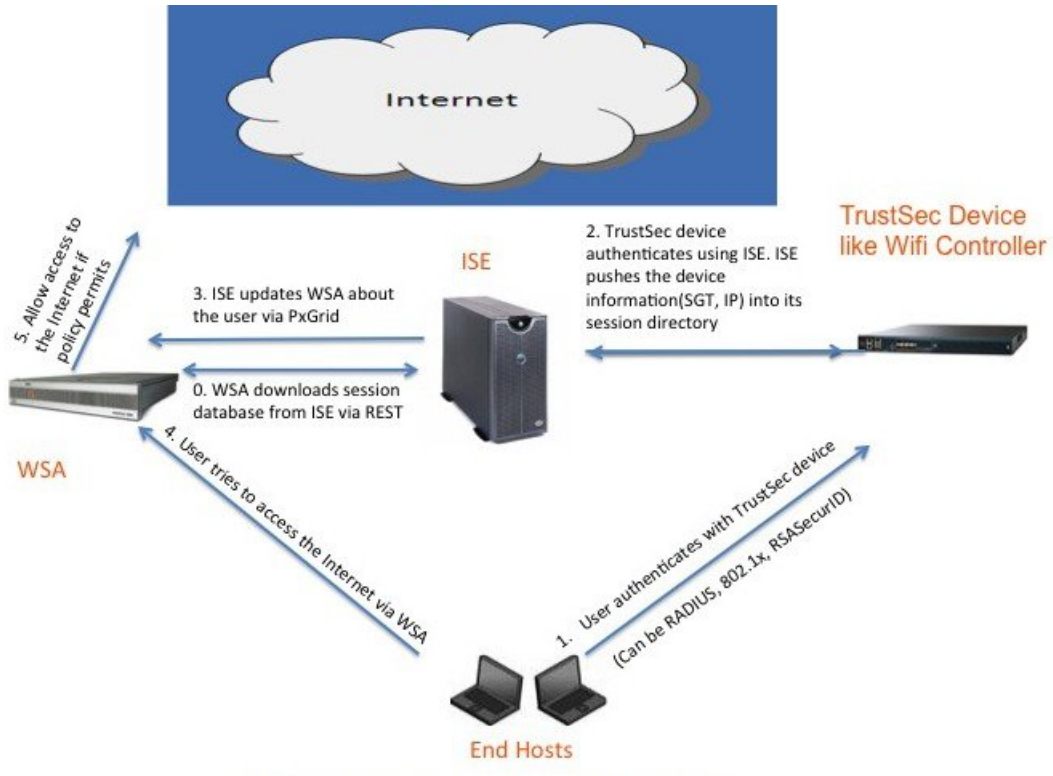
Cisco ISE(Identity Services Engine) 및 WSA(Web Security Appliance)를 통합하면 WSA 사용 시 ISE에서 제공되는 다양한 기능을 활용하여 엔드포인트를 식별하고 적절한 액세스 정책을 적용할 수 있으며 그중에서도 가장 중요한 것은 SGT(TrustSec Secure Group Tagging) 기능일 것입니다. TrustSec SGT 기능을 사용하면 사용자를 서로 다른 ID 그룹으로 분류할 수 있습니다. 예를 들어, 보안 그룹 SGT10에 속한 사용자는 특정한 소셜 네트워킹 사이트에만 액세스할 수 있습니다. WSA에서 액세스 정책은 ISE가 사용자 세션을 할당하는 SGT 태그를 사용하여 생성됩니다.

802.1X 같은 인증 방법은 WSA에서 지원되지 않습니다. ISE로 WSA를 통합하면 더욱 안전한 802.1X 인증 방법을 사용하여 ISE를 통해 WSA 사용자를 인증할 수 있습니다. Cisco pxGrid 기능을 사용하면 Cisco ISE에서 WSA로 컨텍스트 기반 정보를 공유하여 사용자를 인증하고 적절한 정책을 적용할 수 있습니다.

ISE-WSA 구축

Cisco ISE와 WSA를 통합하면 인해 사용자의 IP 주소를 기준으로 사용자를 식별할 수 있으며, Cisco WSA는 Cisco ISE에서 IP-사용자 매핑을 가져옵니다. 레이턴시 및 성능에 미치는 영향을 줄이려면 구축 시 Cisco ISE와 WSA 간의 최소 간격을 유지하는 것이 좋습니다.

아래 그림에는 Cisco ISE-WSA 통합 워크플로가 설명되어 있습니다.



지원되는 ISE 및 WSA 버전

- Cisco ISE, 릴리스 1.3
- Cisco WSA, 릴리스 8.7.0 이상

Cisco ISE와 WSA 통합 워크플로

Cisco ISE를 WSA와 통합하기 위해 수행해야 할 단계:

절차

단계 **1**	WSA 클라이언트의 SGT 생성
단계 **2**	WSA 설정
단계 **3**	WSA에서 ISE 기능 구성
단계 **4**	WSA 클라이언트의 ID 프로파일 생성
단계 **5**	WSA 클라이언트의 액세스 정책 생성

WSA 클라이언트의 SGT 생성

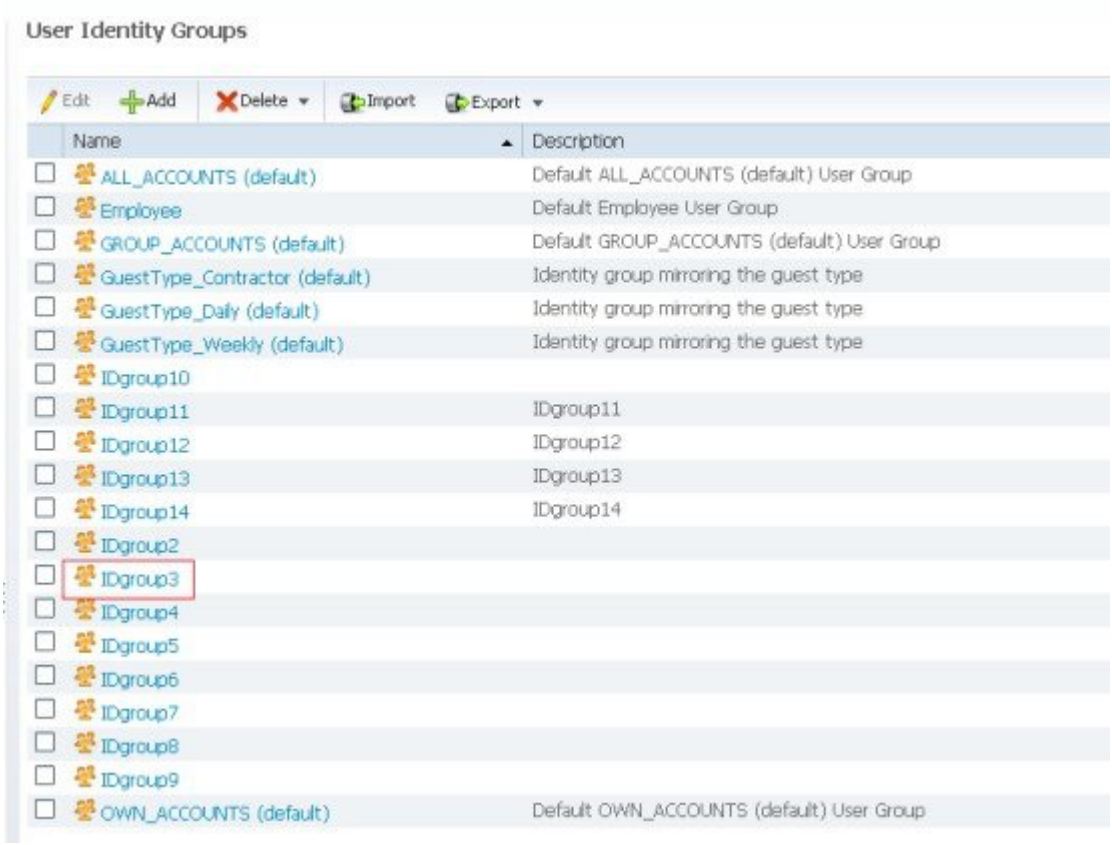
통합을 시작하려면 사용자에 대한 새로운 ID 그룹(예: IDGroup3)을 생성하고 이 ID 그룹을 SGT(예: SGTGroup3)에 연결해야 합니다. 마지막으로, 이전에 생성한 ID 그룹에 속하는 사용자를 위해 IEE 802.1X 인증을 사용하는 정책 집합을 생성해야 합니다.

시작하기 전에

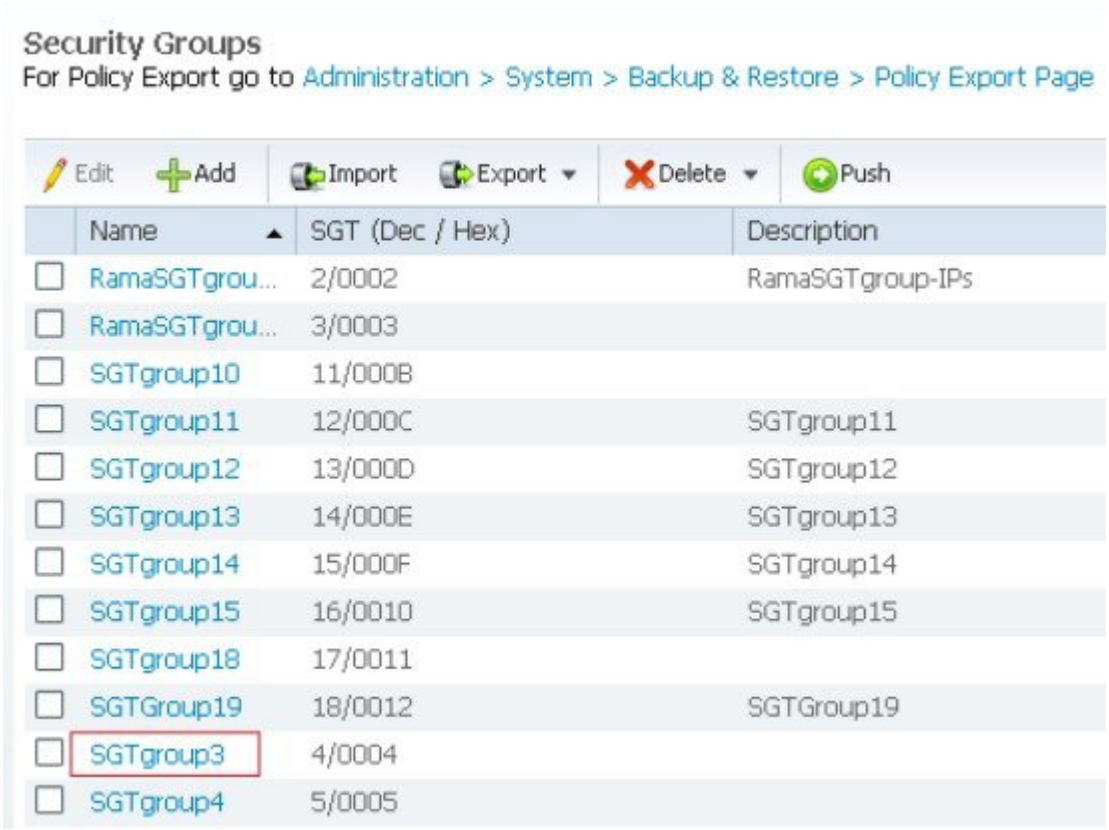
- ISE 서버에서 모든 기존 WSA 클라이언트를 삭제합니다(**Administration** > **pxGrid Services** > **Clients**).
- WSA의 요청을 처리하려면 WSA 클라이언트 IP 주소가 ISE에 입력되어 있어야 합니다.
- pxGrid 서비스가 활성화되어 있는지 확인합니다. Connected to pxGrid 메시지가 pxGrid 서비스 페이지에 표시되어 있는지 확인합니다. (**Administration** > **pxGrid Services**)
- CA 서명 인증서를 생성했는지 확인합니다.
- ISE 서버에서 인증서를 변경할 때마다 ISE 서버를 다시 시작해야 합니다.
- **Administration** > **Certificates** > **Trusted Certificates** > **Import**를 선택하여 pxGrid 인증서, ISE 서버 관리자 인증서, WSA 인증서 및 키를 가져온 다음 ISE와 WSA 간의 양방향 통신을 활성화합니다.
- Personas 섹션에서 **Administration** > **System** > **Deployment** > **General Settings** 페이지를 선택하고 pxGrid 확인란을 선택하여 ISE와 WSA 간의 통신을 활성화합니다.
- **Administration** > **pxGrid Services**를 선택하고 **Enable Auto-Registration** 옵션을 선택합니다. Auto-Registration 옵션이 비활성화되어 있다면 WSA pxGrid 클라이언트가 ISE의 pxGrid 서버에 연결하려고 시도할 경우, ISE 서버 관리자는 수동으로 WSA 클라이언트 등록을 허용해야 합니다.
- **Administration** > **Certificates** > **Trusted Certificates** > **Edit** 페이지를 선택하여 WSA 인증서를 편집합니다. **Usage** 섹션에서 **Trusted For** 옵션 아래의 모든 확인란을 선택합니다.
- **Administration** > **System** > **Settings** > **Protocols** > **ERS Settings** 페이지를 선택하고 **ERS Setting for Primary Administration Node** 섹션에서 **Enable ERS for Read/Write** 옵션을 활성화하여 REST 서버와 WSA의 통신을 활성화합니다.

절차

단계 **1** **Administration** > **Identity Management** > **Groups** > **Add**를 선택하여 WSA 사용자 ID 그룹을 생성합니다.

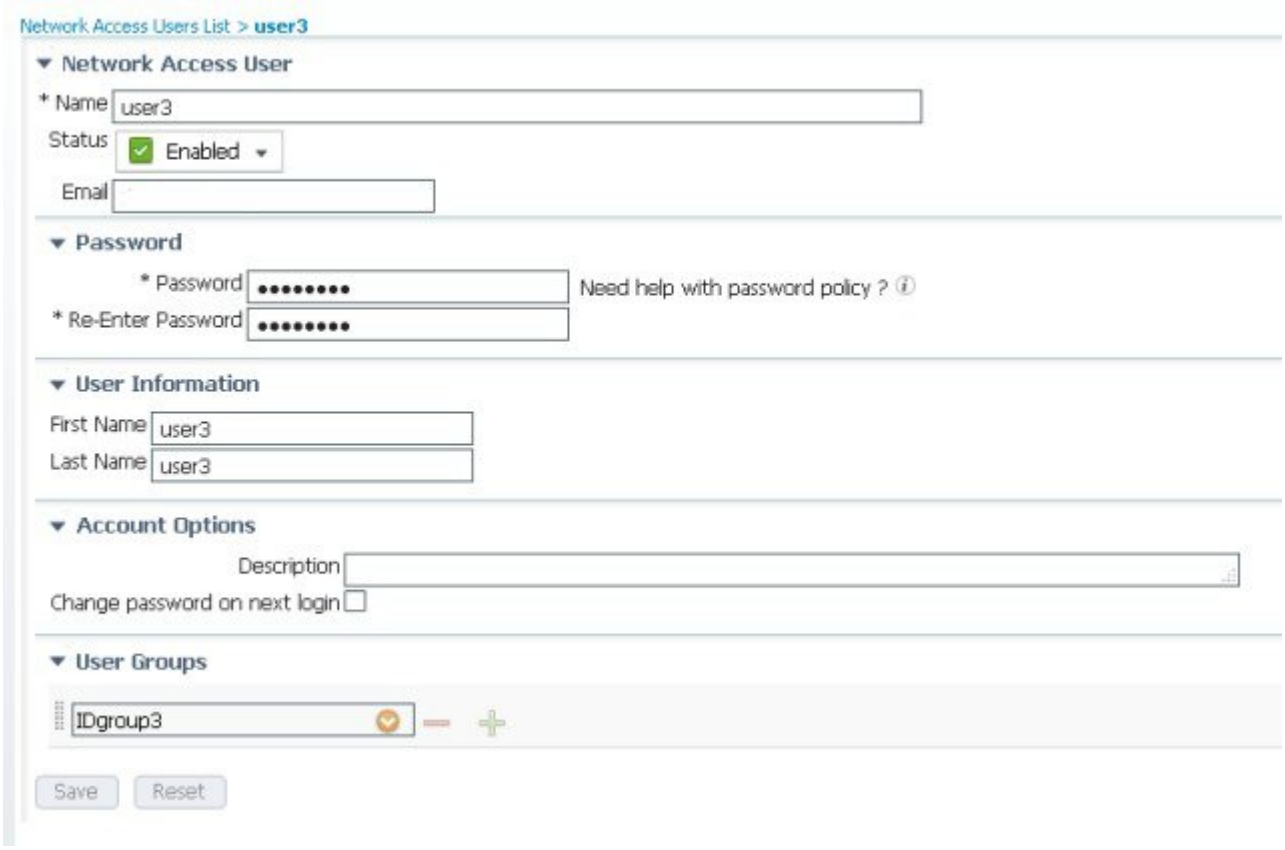


단계 **2** **Policy > Policy Elements > Results > TrustSec > Security Groups > Add**를 선택하여 Security Groups 페이지에서 필수 WSA 관련 SGT를 정의합니다.



단계 **3** **Administration** > **Identity Management** > **Identities** > **Users**를 선택합니다.

단계 **4** **Add**를 클릭하여 네트워크 액세스 사용자를 생성합니다.


Network Access Users List > user3
Network Access User
* Name user3
Status Enabled
Email
Password
* Password ••••••••
Need help with password policy ?
* Re-Enter Password ••••••••
User Information
First Name user3
Last Name user3
Account Options
Description
Change password on next login
User Groups
IDgroup3
Save
Reset

Network Access Users

Edit | Add | Change Status | Import | Export | Delete | Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Gro...
Enabled	linh					Employee
Enabled	user1		user1	user1		Employee
Enabled	user10		user10	user10		IDgroup10
Enabled	user100		user100	user100		IDgroup10
Enabled	user101		user101	user101		Employee
Enabled	user102		user	102		Employee
Enabled	user103		user	103		Employee
Enabled	user11		user11	user11		IDgroup11
Enabled	user111		user111	user111		IDgroup11
Enabled	user12		user12	user12		IDgroup12
Enabled	user122		user122	user122		IDgroup12
Enabled	user13		user13	user13		IDgroup13
Enabled	user133		user133	user133		IDgroup13
Enabled	user14		user14	user14		IDgroup14
Enabled	user144		user144	user144		IDgroup14
Enabled	user15		user15	user15		GuestType_Contr...
Enabled	user155		user155	user155		GuestType_Contr...
Enabled	user18		user18	user18		Employee
Enabled	user19		user19	user19		Employee
Enabled	user2		user2	user2		IDgroup2
Enabled	user22		user22	user22		IDgroup2
Enabled	user3		user3	user3		IDgroup3
Enabled	user33		user33	user33		IDgroup3
Enabled	user4		user4	user4		IDgroup4
Enabled	user44		user44	user44		IDgroup4

사용자가 서로 다른 ID 그룹에 할당됩니다.

단계 **5** **Policy** > **Policy Sets** > **WirelessWGA** > **Authorization Policy**를 선택하여 해당 ID 및 SGT 그룹에 적용 가능한 규칙을 생성합니다.

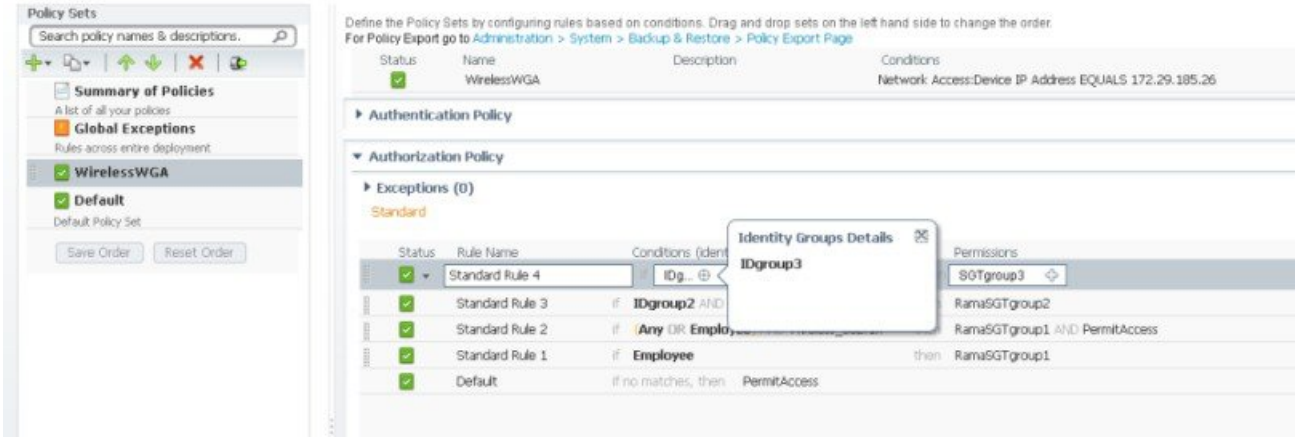
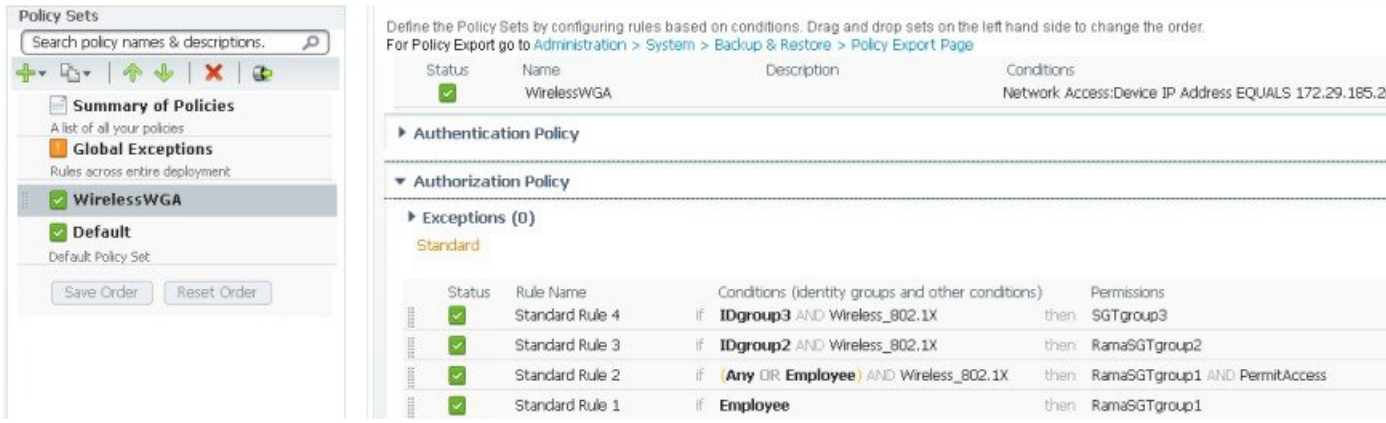


그림 ***1:***



다음에 할 작업

ISE-WSA 통합을 위해서는 WSA를 구성해야 합니다.

WSA 설정

시작하기 전에

- WSA 어플라이언스를 네트워크 및 디바이스에 연결합니다.
- System Setup Wizard 워크시트를 완료합니다.
- 가상 어플라이언스에서 System Setup Wizard를 실행하려는 경우, loadlicense 명령을 사용하여 가상 어플라이언스 라이센스를 로드하십시오. 전체 내용을 보려면 http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html에서 Cisco Content Security Virtual Appliance Installation Guide를 참조하십시오.

절차

단계 **1**	브라우저를 열고 WSA의 IP 주소를 입력합니다. System Setup Wizard를 처음 실행하는 경우, 기본 IP 주소인 https://192.168.42.42:8443 또는 http://192.168.42.42:8080을 사용하십시오. 여기서 192.168.42.42는 기본 IP 주소, 8080은 HTTP의 기본 관리자 포트 설정, 8443은 HTTPS의 기본 관리자 포트입니다. 어플라이언스가 이미 구성된 경우, M1 포트의 IP 주소를 사용합니다.
단계 **2**	어플라이언스 로그인 화면이 나타나면 사용자 이름 및 비밀번호를 입력합니다. 기본적으로, 어플라이언스는 다음과 같은 사용자 이름 및 비밀번호와 함께 제공됩니다. • Username: admin • Password: ironport
단계 **3**	**System Administration** > **System Setup Wizard**를 선택하여 **Start**, **Network**, **Security**, **Review**라는 네 가지 탭이 포함된 시작 페이지를 엽니다.
단계 **4**	어플라이언스가 이미 구성된 경우, 컨피그레이션을 재설정하려고 한다는 경고 메시지가 표시됩니다. **System Setup Wizard**를 계속 진행하려면 **Reset Configuration** 버튼을 클릭합니다. 어플라이언스가 재설정되고 브라우저가 어플라이언스 홈 화면으로 새로 고침됩니다.
단계 **5**	**Start** 탭에서 최종 사용자 라이센스 계약의 약관을 읽고 동의합니다.
단계 **6**	**Begin Setup**을 클릭하여 계속 진행합니다.
단계 **7**	**Network** 탭에서 필요에 따라 제공된 참조 테이블을 사용하는 모든 설정을 구성합니다.
단계 **8**	**Security** 탭에서 모든 설정을 구성합니다.
단계 **9**	**Review** 탭에서 컨피그레이션 정보를 검토합니다. 옵션을 변경해야 할 경우 해당 섹션의 **Edit** 버튼을 클릭합니다.
단계 **10**	**Install This Configuration**을 클릭합니다. 컨피그레이션이 설치되면 **Next Steps** 페이지가 표시되어야 합니다. 그러나 설정 과정 동안 구성한 IP, 호스트 이름 또는 DNS 설정에 따라 이 단계에서 어플라이언스의 연결이 끊어질 수 있습니다. 브라우저에 "Page not found" 메시지가 표시될 경우, URL을 변경하여 새 주소 설정을 반영하고 페이지를 다시 로드합니다. 그런 다음, 수행하려는 모든 후속 설정 작업을 계속 진행합니다.

WSA에서 ISE 기능 구성

시작하기 전에

- ISE 서버 호스트 이름 또는 IP 주소를 가져옵니다.
- 외부에서 생성된 인증서/키 조합을 사용 중인 경우, WSA 클라이언트 인증 인증서 및 키 파일을 가져옵니다.
- WSA 데이터 초기화를 위한 ISE 관리자 인증서를 가져옵니다.
- WSA 데이터 서브스크립션을 위한 ISE pxGrid 인증서를 가져옵니다.

절차

단계 **1** **Network > Identity Services Engine**을 선택하여 Identity Services Engine configuration 페이지를 엽니다.

단계 **2** **Edit Settings**를 클릭하여 WSA 클라이언트, ISE 관리자, pxGrid 인증서를 추가하거나 업데이트합니다.

단계 **3** **Enable ISE Service** 확인란이 선택되어 있는지 확인하여 ISE 서비스를 활성화합니다.

단계 **4** 해당 호스트 이름 또는 IPv4 주소를 사용하여 ISE 서버를 식별합니다.

단계 **5** WSA-ISE 서버 상호 인증을 위한 클라이언트 인증서를 제공하는 데 사용할 방법을 선택합니다.

- Use Uploaded Certificate and Key — 필요에 따라 파일을 업로드하고 선택합니다.
- Use Generated Certificate and Key — 필요한 경우 새 인증서 및 키를 생성합니다.
  - **Generate New Certificate and Key**를 클릭합니다.
  - **Generate Certificate and Key** 대화 상자에서 인증서 서명에 표시할 정보를 입력합니다.
  - **Generate**를 클릭합니다.
  - **Download Certificate Signing Request**(DCSR) 링크를 클릭하여 이를 CA(Certificate Authority)에 제출합니다. CA에서 서명된 인증서를 받은 후에는 **Browse**를 클릭하고 서명된 인증서 위치로 이동합니다. 파일 업로드를 클릭합니다.
  - CA 루트가 기존에 없는 경우 ISE 서버의 **Administration** > **Certificates** > **Trused Certificates** 아래에 CA 루트를 추가합니다.
- 또는, 사용자가 CA 서명 WSA 클라이언트 인증서를 사용하지 않으려는 경우:
  - **Download Certificate**를 클릭하고 인증서를 로컬 폴더에 다운로드합니다.
  - 이 인증서를 ISE 서버의 **Administration** > **Certificates** > **Trused Certificates**에 업로드합니다.

단계 **6** 로컬로 저장된 WSA 클라이언트 인증서 및 키를 사용하려는 경우, 해당 인증서가 **Administration**> **Certificates** > **Trusted Certificates** 경로에 있는지 확인하십시오. 또는, ISE 서버 Admin UI의 **Administration**> **Certificates** > **Trusted Certificates** > **Import** 경로로 인증서를 가져옵니다.

단계 **7** ISE 사용자 프로파일 데이터의 벌크 다운로드에 사용할 ISE 관리자 인증서를 WSA에 제공합니다. 인증서 파일을 찾아 선택한 다음, Upload Files를 클릭합니다. 추가 정보를 보려면 Uploading a Root Certificate and Key(22~25페이지)를 참조하십시오.

단계 **8** WSA-ISE 데이터 서브스크립션(ISE 서버에 대한 지속적인 쿼리)을 위한 ISE pxGrid 인증서를 제공합니다. 인증서 파일을 찾아 선택한 다음, Upload Files를 클릭합니다. 추가 정보를 보려면 Uploading a Root Certificate and Key(22~25페이지)를 참조하십시오.

단계 **9** (선택 사항) **Start Test**를 클릭합니다. 테스트:

- 해당 IP 주소에 대한 ISE 호스트 이름을 확인합니다.
- WSA 클라이언트 인증서를 확인합니다.
- ISE pxGrid 인증서를 확인합니다.

- ISE 관리자 인증서를 확인합니다.
- ISE pxGrid에 대한 연결을 확인하고 SGT를 검색합니다.
- REST 서버에 대한 연결을 확인합니다.

단계 **10** **Submit**을 클릭한 다음 **Commit Changes**를 클릭합니다.

WSA 식별 프로파일 설정

Web Security Manager > **Identification Profiles** > **Add Identification Profile**을 선택하여 ISE를 통해 인증해야 하는 WSA 클라이언트의 ID 프로파일을 생성합니다. Identification Profiles 페이지에는 다음 섹션이 포함됩니다.

섹션	설명
Client/User Identification Profiles	식별 프로파일을 활성화합니다. • Name — 식별 프로파일의 이름을 입력합니다. • Description — 설명을 입력합니다. • Insert Above — 정책이 수신 요청과 일치해야 하는 순서를 입력합니다(위에서 아래로).
사용자 식별	Transparently identify users with ISE — ISE에서 가져오는 사용자 이름 및 관련 SGT입니다.
Fallback to Authentication Realm or Guest Privileges	사용자 인증이 ISE에서 제공되지 않는 경우: • Support Guest Privileges — WSA를 통해 사용자를 프록시화하고 게스트로 인증할 수 있습니다. • Require Authentication — WSA를 통해 사용자를 프록시화하고 NTLM(Windows NT Lan Manager), LDAP(Lightweight Directory Access Protocol), Kerberos 또는 TUI(Transparent User Identification) 같은 프로토콜을 사용하여 인증할 수 있습니다. • Block Transactions — ISE에서 식별할 수 없는 사용자에 대한 □인터넷액세스를 허용하지 않습니다.

Fallback to Authentication Realm 또는 Guest Privileges의 옵션은 선택한 사항에 따라 달라집니다.

Fallback to Authentication Realm or Guest Privileges 옵션	설명
게스트 권한 지원	변경 내용 없음

Fallback to Authentication Realm or Guest Privileges 옵션	설명
인증 필요	영역 또는 시퀀스 선택: • authLDAP • ntlmrealm • 모든 영역 인증 서로게이트: • IP Address — 웹 프록시는 특정 IP 주소의 인증된 사용자를 추적합니다. TUI의 경우, 이 옵션을 선택합니다. • Persistent Cookie — 웹 프록시는 애플리케이션당 각 사용자에 대한 영구적 쿠키를 생성하여 특정 애플리케이션의 인증된 사용자를 추적합니다. 애플리케이션을 종료해도 쿠키는 제거되지 않습니다. • Session Cookie — 웹 프록시는 애플리케이션당 각 도메인의 사용자에 대한 세션 쿠키를 생성하여 특정 애플리케이션의 인증된 사용자를 추적합니다. (그러나 사용자가 동일한 애플리케이션에서 같은 도메인에 대해 다른 자격 증명을 제공할 경우, 쿠키를 덮어씁니다.) 애플리케이션을 종료하면 쿠키도 제거됩니다.
Block Transactions	변경 내용 없음

WSA 클라이언트의 ID 프로파일 생성

WSA 클라이언트의 식별 프로파일을 생성하고 서브넷 10.4.100.0/24의 사용자에게 게스트 권한을 할당해야 합니다.

절차

단계 **1** **Web Security Manager** > **Identification Profiles** > **Add Identification Profile**을 선택합니다.

단계 **2** **Enable Identification Profile** 섹션에서 필수 세부 정보를 입력합니다.

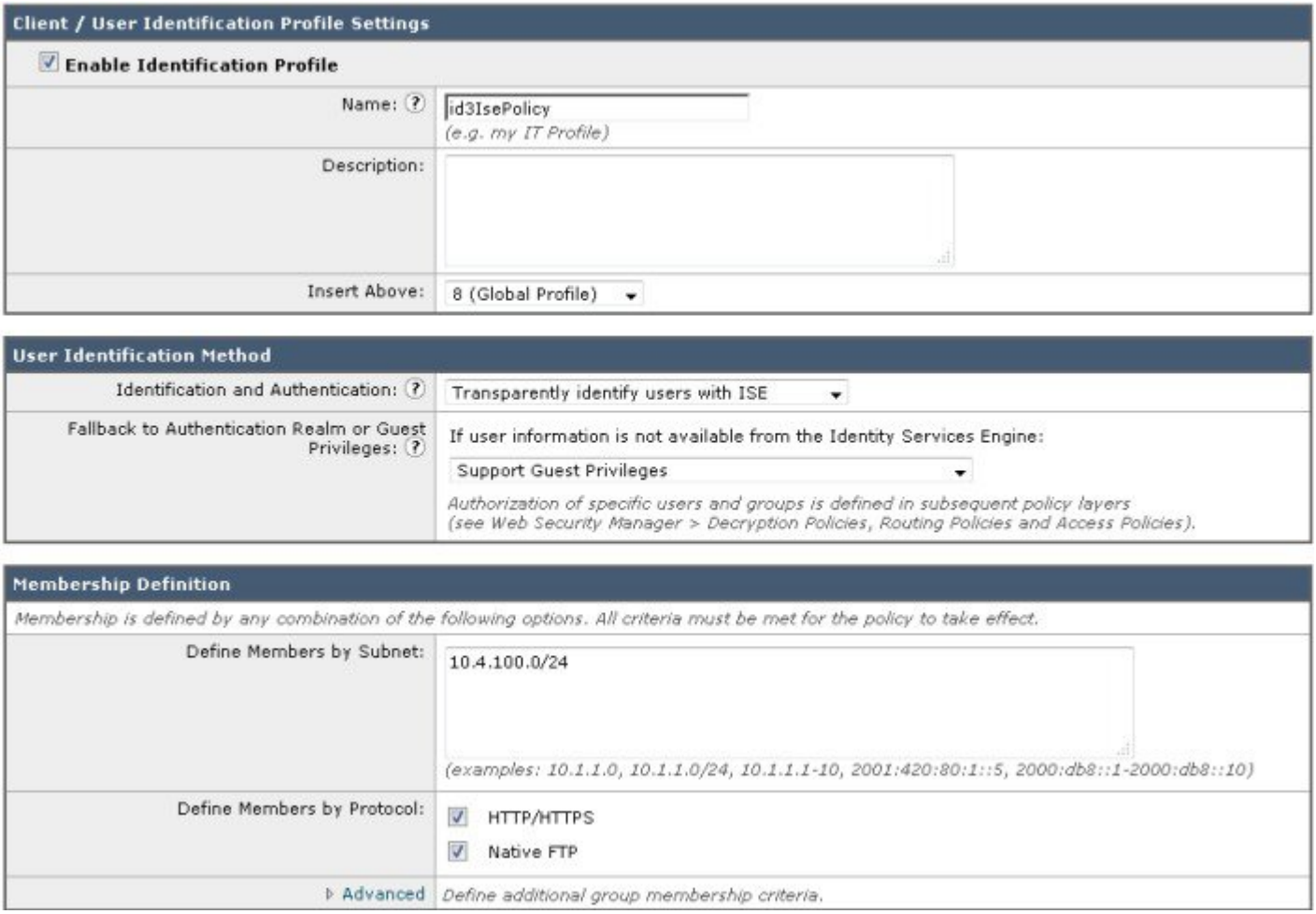
단계 **3** **User Identification Method** 섹션에서 **Transparently Identify Users with ISE** 및 **Support Guest Privileges**를 선택합니다.

단계 **4** **Membership Definition** 섹션에서 서브넷 주소(예: 10.4.100.0/24)를 입력합니다.

단계 **5** **Define Members by Protocol** 섹션에서 필수 옵션(예: **HTTP/HTTPS** 및 **Native FTP** 옵션)을 선택합니다.

단계 **6**

단계 **7** **Submit**을 클릭합니다.



사용자 또는 엔드포인트를 완전히 차단하도록 선택할 수도 있습니다.

WSA 클라이언트의 액세스 정책 생성

서브넷 10.4.100.0/24의 사용자에 대한 식별 프로파일을 생성했습니다. ISE에서 검색한 SGT를 확인해야 액세스 정책을 필수 SGT에 연결할 수 있습니다.

참고 또는, CLI 명령 isedata를 사용하여 검색한 ISE SGT를 확인할 수도 있습니다.

절차

단계 **1** **Web Security Manager** > **Access Policies** > **Add Policy**를 선택합니다.

단계 **2** **Policy Settings** 섹션에서 필수 세부 정보를 입력합니다.

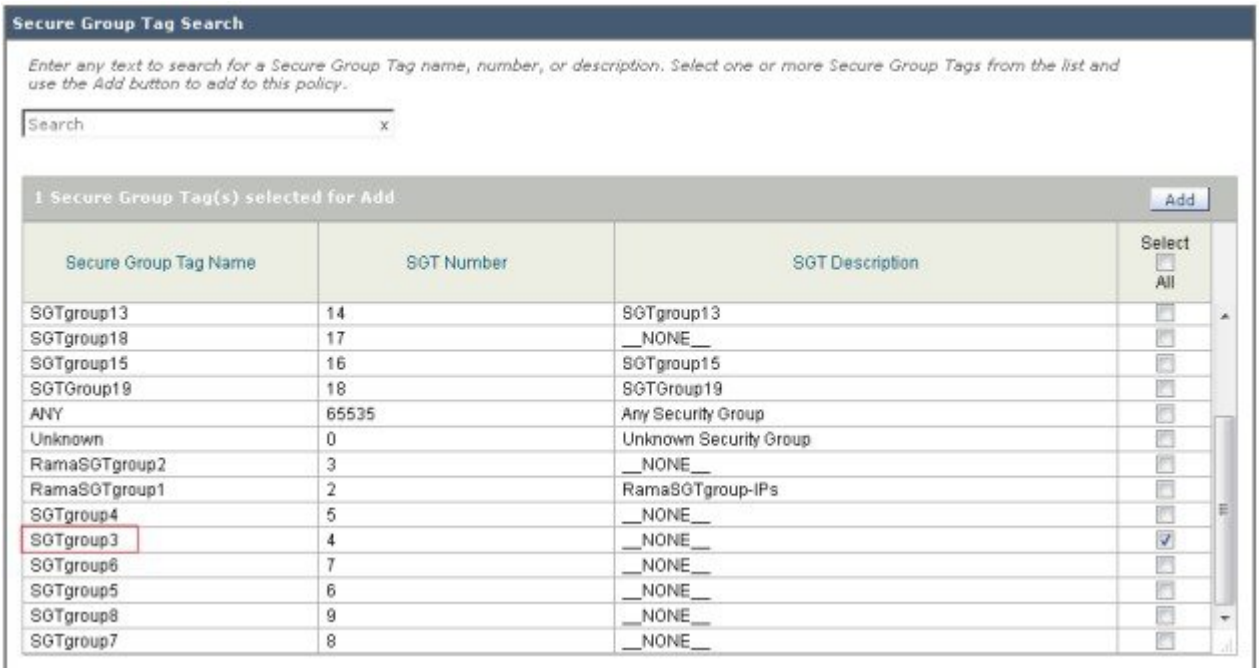
단계 **3** **Policy Member Definition** 섹션의 **Identification Profiles and Users** 드롭다운 목록에서 **Select One or More Identification Profiles**를 선택합니다.

단계 **4** **Select Identification Profile** 드롭다운 목록에서 이전에 생성한 정책을 선택합니다.

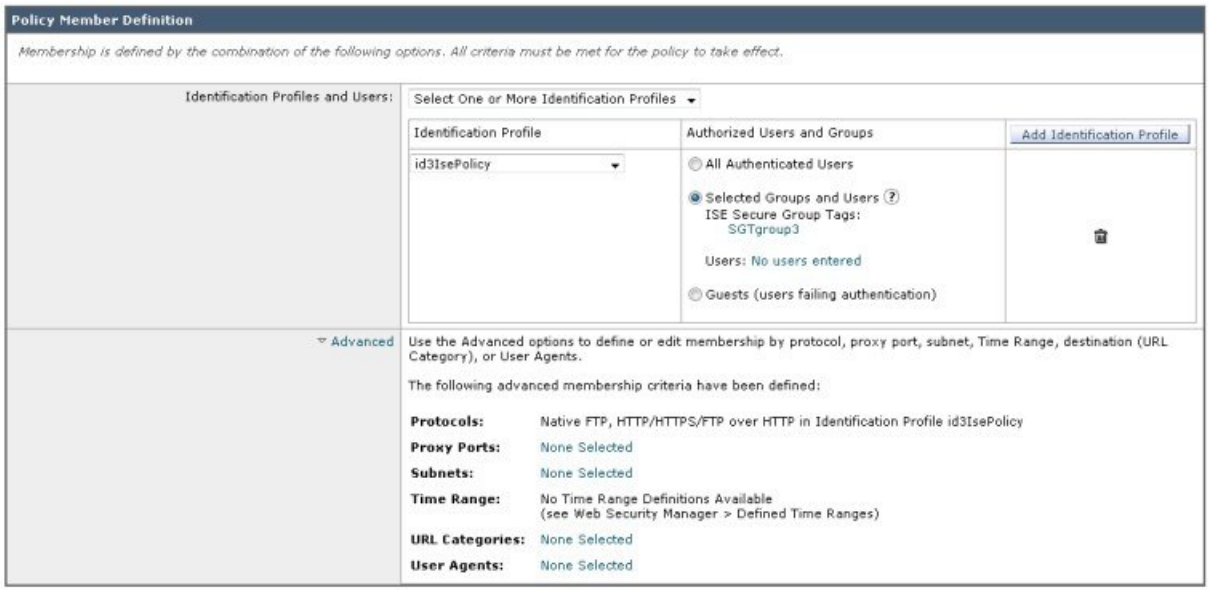
단계 **5** **Authorized Users and Groups** 열에서 **Selected Groups and Users**를 선택합니다.

단계 **6** **No Tags Entered** 링크를 클릭하여 ISE 서버에서 SGT를 가져옵니다. (해당 목록은 **ISE Policy**> **Results** > **Trustsec** > **Security Groups** 페이지와 동일합니다.)

단계 **7** 필수 SGT(예: SGTgroup3)를 선택하고 **Add**를 클릭하여 선택한 SGT를 **Authorized Secure Group Tags** 섹션에 추가합니다.



단계 **8** **Done**을 클릭하여 선택한 SGT를 액세스 정책에 추가합니다.



WSA 프로파일은 생성한 SGT에 연결됩니다.

WSA 보고를 사용하여 사용자 상태 보기

사용자에 대한 ID 프로파일 및 액세스 정책을 생성한 후에는 사용자가 네트워크에 로그온했을 때의 상태를 확인할 수 있습니다. **Reporting** > **Web Tracking** 페이지로 이동한 다음 필수 필드를 입력하고 **Search**를 클릭하여 **Results** 섹션을 봅니다. 예를 들어, User3가 ISE에 의해 인증된 경우 보고서에는 클라이언트 IP 주소와 함께 "Identified by ISE"라는 텍스트가 표시됩니다. 게스트 사용자 및 차단된 IP 주소의 경우, 클라이언트 IP 주소만 표시됩니다. 전체 내용을 보려면 WSA 사용자 가이드에서 Web Tracking 페이지를 참조하십시오.

로그 파일을 사용하여 ISE-WSA 통합 트러블슈팅

WSA는 시스템 및 트래픽 관리와 관련된 작업을 로그 파일에 기록합니다. ISE-WSA 통합과 관련된 로그는 W3C 로그, 액세스 로그, ISE 로그, 프록시 로그입니다. 이러한 로그를 사용하여 통합 관련 문제를 모니터링하고 문제를 해결할 수 있습니다.

로그 파일	기능	**WSA GUI** 경로	**SSH** 명령
W3CLogs	웹 프록시 클라이언트 기록을 W3C 호환 형식으로 기록합니다.	**System Administration** > **Log Subscriptions**	GUI 컨피그레이션에 따라 —System Administration > Log Subscriptions / logconfig
액세스 로그	웹 프록시 클라이언트 기록을 기록합니다.	**System Administration**> **Log Subscriptions** > **accesslogs**	ssh admin@WSA tail ise_service_log

로그 파일	기능	**WSA GUI** 경로	**SSH** 명령
ISE 로그	ISE 서버와의 통신 성공 또는 실패 같은 ISE 사용과 관련된 메시지를 기록합니다.	**System Administration** > **Log Subscriptions** > **ise_service_log**	ssh admin@WSA tail ise_service_log
프록시 로그	웹 프록시와 관련된 오류를 기록합니다. 이는 모든 웹 프록시 관련 로그 중에서 가장 기본적인 기록입니다. 웹 프록시와 관련하여 더욱 구체적인 문제를 해결하려면, 해당 웹 프록시 모듈에 대한 로그 서브스크립션을 생성합니다.	**System Administration** > **Log Subscriptions** > **proxylogs**	ssh admin@WSA tail proxylogs

액세스 로그 파일 - 예

트러블슈팅에 사용할 수 있는 액세스 로그 파일의 몇 가지 예는 아래와 같습니다.

예 **1: SGT**가 없는 **ISE** 캐시의 사용자에게 적용된 정책에 액세스합니다.

```
1424330486.386 320 10.19.75.75 TCP_MISS/200 68632 GET http://www.bing.com/ "user1" DIRECT/www.bing.com text/html
DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup
<IW_srch,6.1,1,"-",-,-,-,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_srch,-,"-","-","Bing","Search
Engine","-","-",1715.80,0,-,"-","-",1,"-",-,-,"-","-"> - SSO_ISE
```

예 **2:** 일치하는 **SGT**가 있는 **ISE** 캐시의 사용자에게 적용된 정책에 액세스합니다.

```
1424331112.566 0 10.19.75.75 TCP_DENIED/403 0 GET http://www.bing.com/ "user1" NONE/- -
BLOCK_WEBCAT_12-BYODPolicy-DefaultGroup-NONE-NONE-NONE-NONE
<IW_srch,6.1,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,IW_srch,-,"-","-","Unknown","Unknown","-","-",0.00,0,-,"-","-",-,"-",-,-,"-","-">
 - SSO_ISE
```

예 **3:** 게스트로 대체되는 정책에 액세스합니다.

```
1424330523.414 155 172.29.177.25 TCP_MISS/200 68647 GET http://www.bing.com/ "(Unauthenticated)172.29.177.25"
 DIRECT/www.bing.com text/html DEFAULT_CASE_12-DefaultGroup-Default
Group-NONE-NONE-NONE-DefaultGroup
<IW_srch,6.1,1,"-",-,-,-,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_srch,-,"-","-","Bing","Search
Engine","-","-",3543.07,0,-,"-","-",1,"-",-,-,"-","-
"> - GUEST
```

예 **4:** 트랜잭션 차단으로 대체되는 정책에 액세스합니다.

```
1424331683.561 0 172.29.177.25 TCP_DENIED/403 0 GET http://www.bing.com/ - NONE/- -
OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,-,-,"-","-","-","-","-","-",0.00,0,-,"-","-",-,"-",-,-,"-","-">
 - NONE
```

ISE 로그 파일 - 예

트러블슈팅에 사용할 수 있는 ISE 로그 파일의 예는 아래와 같습니다.

```
Thu Mar 12 20:41:29 2015 Info: Begin Logfile
Thu Mar 12 20:41:30 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_service.ini
Thu Mar 12 20:41:30 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Thu Mar 12 20:41:30 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Thu Mar 12 20:41:30 2015 Info: ISEService: Running
Thu Mar 12 20:41:30 2015 Info: ISEDynamicConfigThread: Started Server..
Thu Mar 12 20:41:30 2015 Info: ISEService: Sending ready signal...
Thu Mar 12 20:41:31 2015 Info: ISEBulkDownloader: Downloaded 12 SGTs in 0.162157773972 seconds
Thu Mar 12 20:41:32 2015 Info: ISEBulkDownloader: Downloaded 0 sessions in 0.316617965698 seconds
```

ISE-WSA 통합 트러블슈팅 - ISE 서버 연결

이 섹션에서는 ISE를 WSA와 통합할 때 발생할 수 있는 문제에 대해 설명합니다.

- 네트워크 문제: 구성된 ISE 서버 포트에 연결 문제가 발생할 수 있습니다. 예를 들어, 포트 5222에 방화벽 문제가 발생할 수 있습니다. 텔넷 및 tcpdump 명령을 사용하여 네트워크 문제를 디버그할 수 있습니다.
- 인증서 문제:

인증서	다음과 같은 경우 문제가 발생할 수 있습니다.
CA 서명	• 관리자 또는 pxGrid 인증서 루트 CA가 WSA에 없을 경우 • WSA 클라이언트 인증서에 서명한 루트 CA가 ISE 트러스트된 인증서 저장소에 없을 경우
자체 서명	• WSA 클라이언트 인증서가 ISE 트러스트된 인증서 저장소에 없을 경우 • ISE 관리자 또는 pxGrid 인증서가 WSA에 없을 경우
모두	• 유효했던 인증서가 업로드 도중 현재 날짜로 만료된 경우

- ID 매핑 쿼리 문제: 다음과 같은 문제가 발생할 수 있습니다.
  - 포트 443에서 SSL 핸드셰이크가 성공했음에도 불구하고, ISE 서버에서 SGT가 다운로드될 경우. ISE 서버에서 문제를 디버그해야 합니다.
  - WSA가 ISE에서 인증한 사용자에 대한 액세스를 거부할 경우. isedata 캐시 및 isedata 통계 명령을 사용합니다.

- 패킷 캡처: 어플라이언스가 연결된 네트워크를 통해 전송/수신된 TCP/IP 및 기타 패킷을 캡처하고 표시할 수 있습니다. WSA 사용자 가이드에서 Packet Capture 페이지를 참조하십시오.
- 정책 추적: WSA 사용자 가이드 Tracing Client Requests 페이지를 참조하십시오.

ISE-WSA 통합과 관련된 SMA 개요

Cisco SMA(Security Management Appliance)는 웹 보안을 관리하고 트러블슈팅을 수행할 뿐만 아니라, 수개월 또는 수년간 데이터 스토리지를 위한 공간을 유지하는 통합 관리 플랫폼입니다. 이는 네트워크에 구축된 WSA를 관리 및 보고하는 데 사용되는 중앙 집중식 시스템입니다. 예를 들어, 구축 환경에 WSA가 5개 있을 경우 SMA에는 모든 WSA가 통합된 하나의 보고서만 표시됩니다. 보고서를 SMA에 할당한 후에는 WSA에서 보고서를 볼 수 없습니다. SMA에서 지원되는 기능은 관련 WSA에서 해당 기능을 지원할 때만 제공됩니다.

SMA에는 WSA의 ISE 구성 여부에 대한 정보가 포함됩니다. ISE가 구성된 경우, SMA에는 SGT와 관련된 정보가 포함됩니다. SGT를 활용하여 SMA에서 WSA에 정책을 생성할 수 있습니다. SMA는 약 5분마다 ISE와 관련된 정보를 주기적으로 업데이트합니다. 표준 컨피그레이션을 생성한 후 이를 구축 환경 내에 있는 모든 WSA에 게시할 수 있습니다. SMA의 GUI(그래픽 사용자 인터페이스)는 WSA와 유사하지만 몇 가지 기능을 위한 고유 인터페이스가 있습니다.

SMA에서 **Web** > **Utilities** > **Web Appliance Status**를 선택한 다음 ISE가 활성화된 경우 찾아야 하는 필수 WSA를 클릭합니다.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands