CTA 시스템에 로그 파일을 업로드하기 위한 Blue Coat ProxySG 구성

최종 업데이트: 2016년 4월 18일

목차

표기 규칙

이 설명서는 다음과 같은 표기 규칙을 사용합니다.

표기 규칙	표시
굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은** 글꼴로 표시합니다.
기울임꼴 글꼴	문서 제목, 새로운 용어 또는 강조된 용어 및 사용자가 값을 제공해야 하는 인수는 *기울임꼴* 글꼴로 표시됩니다.
[ ]	대괄호로 묶인 요소는 선택적 요소입니다.
{x | y | z }	필수 대체 키워드는 중괄호로 묶어 세로 선으로 구분합니다.
[x | y | z]	선택적 대체 키워드는 대괄호로 묶어 세로 선으로 구분합니다.
문자열	따옴표 없는 문자의 집합입니다. 문자열 주변에 따옴표를 사용하지 마십시오. 그렇지 않으면 따옴표도 문자열에 포함됩니다.
courier 글꼴	시스템에서 표시되는 터미널 세션 및 정보는 courier 글꼴로 표시합니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 우물 정자(#)는 코멘트 행을 나타냅니다.

참고: *독자가 참고해야 하는 내용*임을 의미합니다. 참고에는 유용한 제안이나 해당 설명서에서 다루지 않는 자료에 대한 참조 정보가 포함됩니다.

주의: ***독자가 주의해야 하는 항목*임을 의미합니다. 이 경우, 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 합니다.**

경고: 중요한 안전상의 지침

위험을 의미합니다. 부상이 발생할 수 있는 상황입니다. 장비를 작동하기 전에 전기 관련 재해에 유의하고 사고 예방을 위해 표준 절차를 숙지하십시오. 각 경고의 끝에는 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾을 수 있도록 명령문 번호가 제공됩니다.

이 지침을 반드시 숙지하십시오.

규정: 추가 정보 제공 및 규정/고객 요구 사항 준수를 위해 제공됩니다.

소개

이 문서에서는 Blue Coat ProxySG에서 Cisco CTA(Cognitive Threat Analytics) 시스템에 로그 파일을 업로드하도록 구성하는 방법에 대해 설명합니다. 로그 파일이 시스템에 업로드되면 CTA에서 데이터를 분석하고 CTA 포털에 그 결과를 보고합니다.

사전 요구 사항

요구 사항

Cisco ScanCenter는 Cisco Cloud Web Security의 관리 포털입니다. 먼저 Cisco ScanCenter에서 Blue Coat ProxySG를 위한 디바이스 계정을 생성해야 합니다.

- Cisco ScanCenter에 로그인합니다.
- **Threats(위협)** 탭을 클릭합니다.
- 페이지의 오른쪽 위에 있는 전역 설정 메뉴 아이콘을 클릭합니다.
- **Device Accounts(디바이스 계정)**를 클릭합니다.
- **Automatic(자동)** 업로드 방법을 선택합니다.

자세한 내용은 Cisco ScanCenter 관리 설명서의 "프록시 디바이스 업로드" 섹션을 참조하십시오.

디바이스 계정이 생성되었으면 Cisco ScanCenter의 Add Device Account(디바이스 계정 추가) 페이지에 있는 다음 정보를 복사하여 프록시 컨피그레이션에 붙여넣습니다.

- HTTPS 호스트: `etr.cloudsec.sco.cisco.com`
- HTTPS 경로
- 프록시 디바이스를 위해 생성된 디바이스 사용자 이름. 대/소문자를 구분하며 프록시 디바이스마다 다릅니다.
- 디바이스 비밀번호. 대/소문자를 구분합니다.

Blue Coat ProxySG에 액세스하려면 다음 항목이 필요합니다.

- Blue Coat ProxySG의 호스트 이름 또는 IP 주소
- Blue Coat ProxySG에 대한 로그인 자격 증명
    - 기본 사용자 이름은 admin입니다.
    - 기본 비밀번호는 없으며 반드시 구성해야 합니다.
- Java™ 플러그인이 있는 웹 브라우저, Blue Coat는 Google Chrome, Opera 또는 Safari를 지원하지 않습니다.

주의: 이 문서의 내용은 랩 환경의 디바이스를 토대로 생성된 것입니다. 네트워크가 실행 중인 경우 모든 컨피그레이션 명령의 잠재적 영향을 미리 숙지하시기 바랍니다.

사용된 구성 요소

이 문서의 내용은 다음 하드웨어에서 테스트한 것입니다.

- Blue Coat ProxySG 600

이 문서의 내용은 다음 소프트웨어 버전에서 테스트한 것입니다.

- SGOS 6.5.7.5
- SGOS 6.5.6.1

참고: 다른 버전은 CTA에 업로드할 때 제대로 작동하지 *않을* 가능성이 있어 현재 지원되지 *않습니다*.

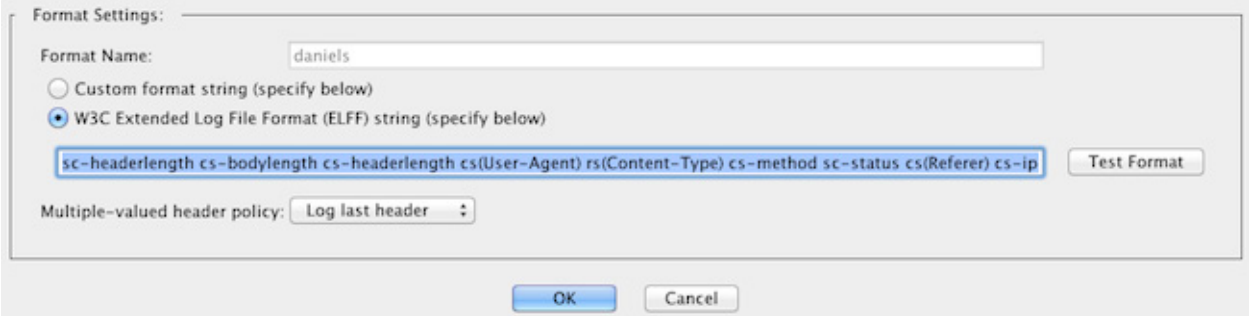
구성

프록시 구성

1. 웹 브라우저에서 Blue Coat ProxySG로 이동합니다.
    a. https://sg_600.*hostname*:8082/ 또는
    b. https://*a.b.c.d*:8082/ 여기서 *a.b.c.d*는 프록시의 IP 주소입니다.
2. 필요하다면 비보안 HTTPS 인증서를 수락하고 진행합니다.
3. admin으로 로그인합니다.
4. 필요하다면 Java™ 보안 경고에 동의하고 진행합니다.

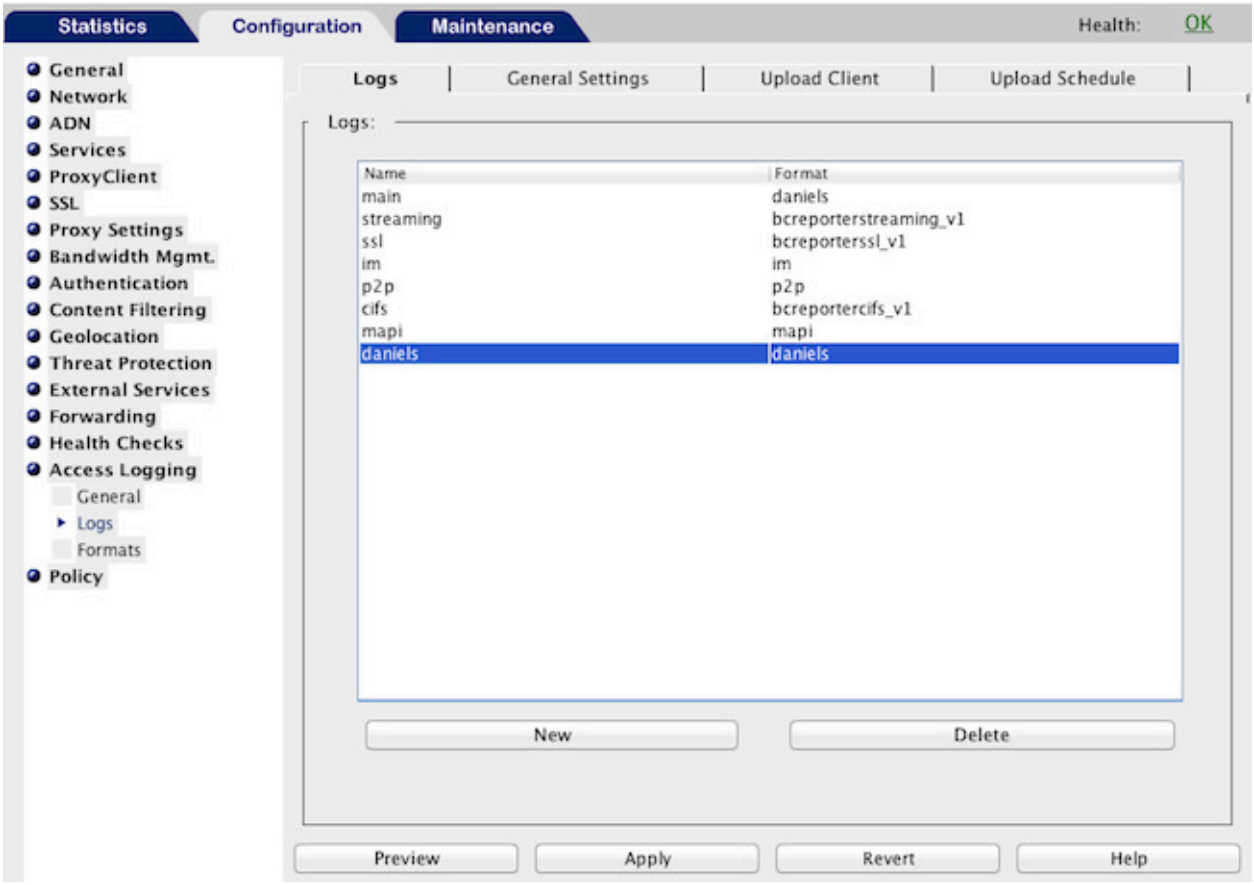
5. **Configuration(컨피그레이션)** > **Access Logging(액세스 로깅)** > **General(일반)**로 이동합니다.
6. **Enable Access Logging(액세스 로깅 활성화)** 확인란을 선택하고 **Apply(적용)** 버튼을 클릭합니다.

7. **Configuration(컨피그레이션)** > **Access Logging(액세스 로깅)** > **Formats(형식)**로 이동합니다.
8. 새 형식 항목을 생성하려면 **New(새로 만들기)** 버튼을 클릭합니다.
9. **Format Name(형식 이름)** 필드에 고유한 이름을 입력합니다. 여기서는 daniels를 사용합니다.



10. **W3C Extended Log File Format (ELFF) string(W3C ELFF 문자열)** 라디오 버튼을 클릭하고 필드에 다음 문자열을 붙여넣습니다.
```
timestamp time-taken c-ip cs-username s-ip s-port c-port cs-uri cs-bytes sc-bytes sc-bodylength sc-headerlength cs-bodylength cs-headerlength cs(User-Agent) rs(Content-Type) cs-method sc-status cs(Referer) cs-ip r-ip r-port rs(Location) s-action
```
11. **OK(확인)** 버튼을 클릭합니다.
12. **Apply(적용)** 버튼을 클릭합니다.

13. **Configuration(컨피그레이션)** > **Access Logging(액세스 로깅)** > **Logs(로그)**으로 이동합니다.
14. 새 로그 항목을 생성하려면 **New(새로 만들기)** 버튼을 클릭합니다.
15. Log Name(로그 이름) 및 Log Format(로그 형식) 모두 9단계에서 생성한 형식 이름을 선택합니다. 여기서는 `daniels`를 사용합니다.



16. **OK(확인)** 버튼을 클릭합니다.
17. **Apply(적용)** 버튼을 클릭합니다.
18. 팝업 경고 메시지가 나타날 수 있는데, 무시해도 좋습니다. 이전 형식의 로그 항목이 현재 형식의 항목과 동일한 로그 파일에 존재할 수 있음을 알리는 메시지입니다.

19. **Upload Client(클라이언트 업로드)** 탭을 클릭합니다.
20. **Log(로그)** 풀다운에서 15단계의 로그를 선택합니다.
21. **Client type(클라이언트 유형)** 풀다운에서 **HTTP Client(HTTP 클라이언트)**를 선택합니다.
22. **Client type(클라이언트 유형)** 옆의 **Settings(설정)** 버튼을 클릭하면 새 창이 나타납니다.

23. **Host(호스트)** 필드에 Cisco ScanCenter에서 제공된 호스트를 입력합니다. 예를 들면 다음과 같습니다.
    `etr.cloudsec.sco.cisco.com`
24. **Port(포트)** 필드에 `443`을 입력합니다.
25. **Path(경로)** 필드에 Cisco ScanCenter에서 제공된 경로를 입력합니다. 예를 들면 다음과 같습니다.
    `/upload/`*`username`*

26. **Username(사용자 이름)** 필드에 Cisco ScanCenter에서 해당 디바이스에 대해 생성된 사용자 이름을 입력합니다. 디바이스 사용자 이름은 대/소문자를 구분하며 프록시 디바이스마다 다릅니다.
27. 여기서는 **Filename(파일 이름)** 필드를 바꾸지 않습니다.
28. **Use secure connections(SSL)(보안 연결(SSL) 사용)** 확인란을 선택합니다.
29. **Change Primary Password(기본 비밀번호 변경)** 버튼을 클릭하면 새 창이 나타납니다.

30. 비밀번호 필드에 Cisco ScanCenter에서 해당 디바이스에 대해 생성된 비밀번호를 입력합니다. 디바이스 비밀번호는 대/소문자를 구분합니다.
31. **OK(확인)** 버튼을 클릭합니다.

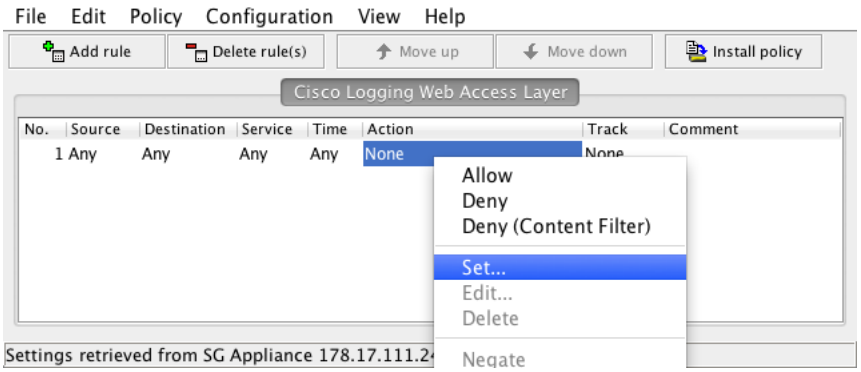
32. **Upload Schedule(일정 업로드)** 탭을 클릭합니다.
33. **Log(로그)** 풀다운에서는 9단계에서 생성한 형식 이름을 선택합니다.
34. **Upload the log file(로그 파일 업로드)** 섹션에서 로그 파일 업로드 간격을 선택합니다. **Every(간격)** 0시간 55분으로 지정합니다.

프록시로 보호하는 사용자 수	권장 업로드 기간
2,000명 미만	55분
알 수 없음 또는 2,000명 ~ 4,000명	30분
4,000명 ~ 6,000명	20분
6,000명 이상	10분

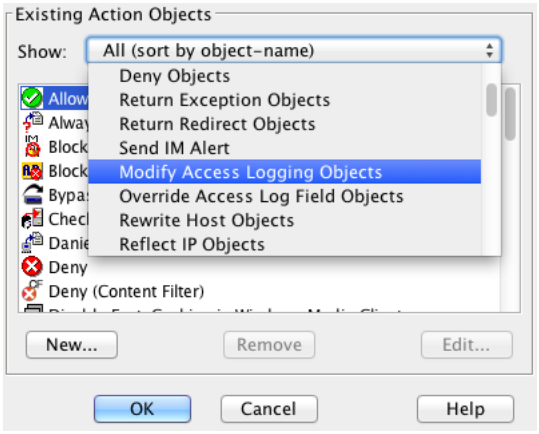
35. **Apply(적용)** 버튼을 클릭합니다.

36. **Configuration(컨피그레이션)** > **Policy(정책)** > **Visual Policy Manager(비주얼 정책 관리자)**로 이동합니다.
37. **Launch(실행)** 버튼을 클릭합니다. 새 창이 나타납니다.

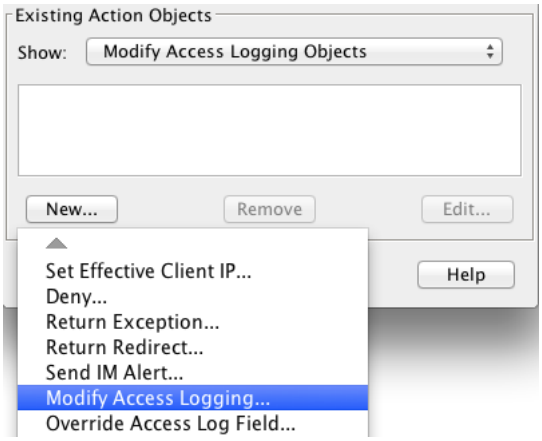
38. **Policy(정책)** > **Add Web Access Layer(웹 액세스 레이어 추가)**로 이동합니다.
39. 레이어 이름을 Cisco Logging Web Access Layer로 지정하고 **OK(확인)**를 클릭합니다.
40. 커서를 **Action(작업)** 열로 이동하고 마우스 오른쪽 버튼을 클릭한 다음 **Set(설정)**를 선택합니다.



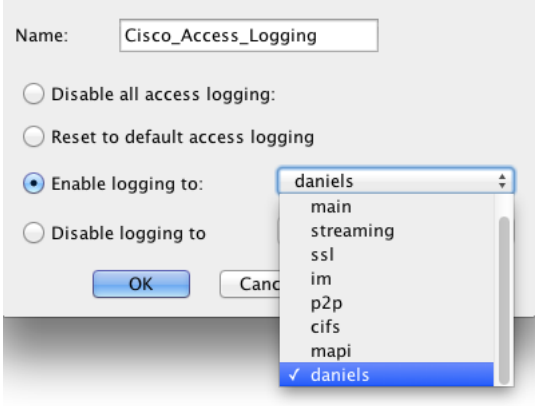
41. **Show(표시)** 풀다운에서 **Modify Access Logging Objects(액세스 로깅 개체 수정)**를 선택합니다.



42. **New(새로 만들기)** 버튼을 클릭하고 **Modify Access Logging(액세스 로깅 수정)**을 선택합니다.



43. 이름을 입력합니다. 여기서는 `Cisco_Access_Logging`을 사용합니다.
44. **Enable logging to(로깅 활성화)** 라디오 버튼을 클릭하고 풀다운에서 15단계의 로그를 선택합니다. 여기서는 `daniels`를 사용합니다.

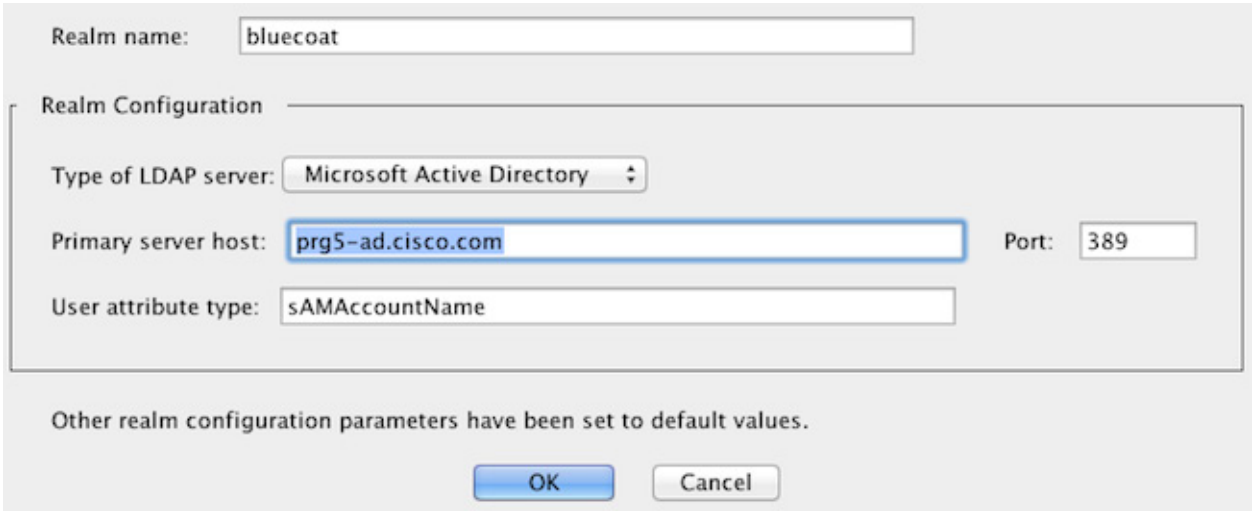


45. **OK(확인)** 버튼을 클릭합니다.
46. **OK(확인)** 버튼을 다시 클릭합니다.
47. **Install Policy(정책 설치)** 버튼을 클릭합니다.
48. "policy installation was successful(정책 설치 성공)" 메시지가 표시되면 Visual Policy Manager(비주얼 정책 관리자) 창을 닫습니다.

사용자 인증

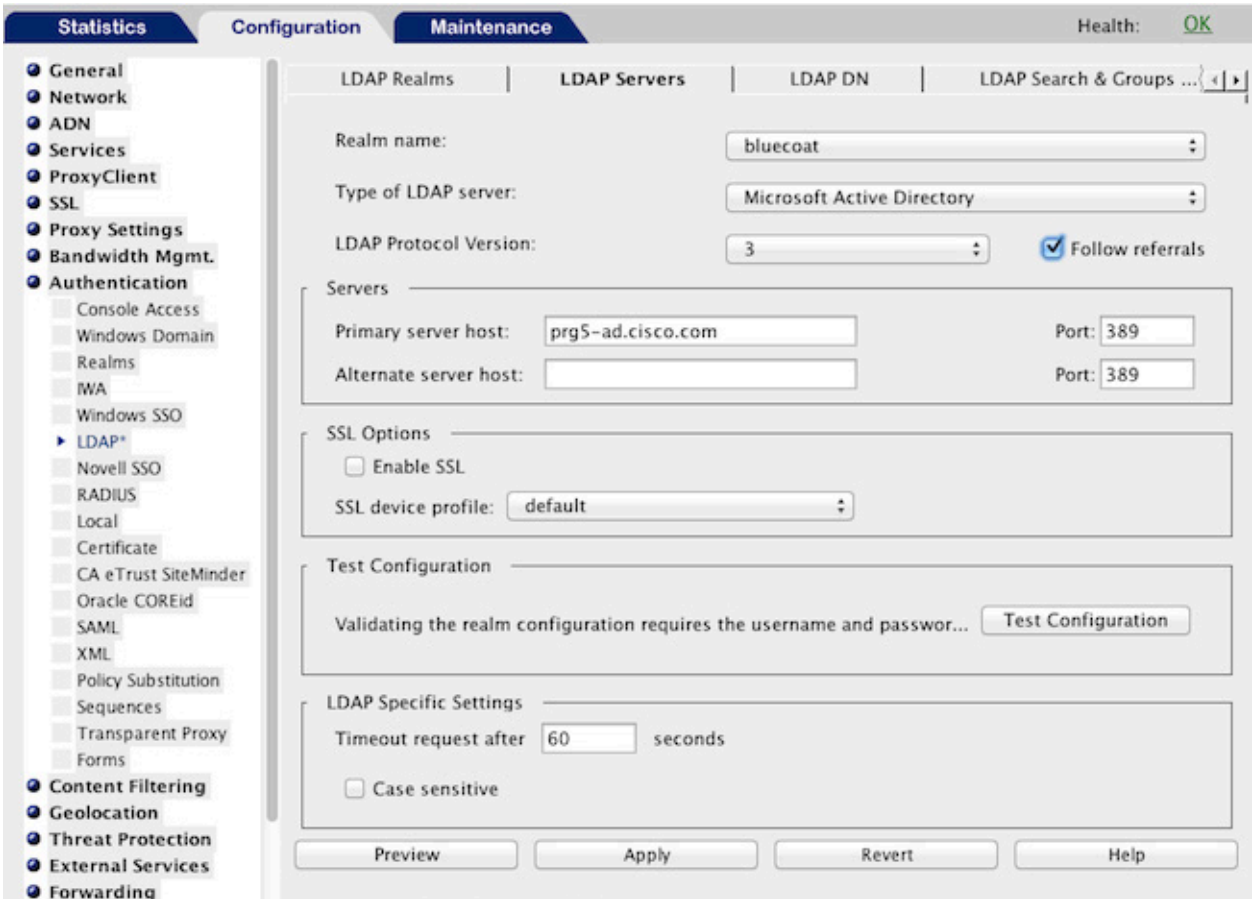
액세스 로그에 대한 사용자 세부 정보를 얻으려면 사용자를 인증해야 합니다. 다음 단계에 따라 LDAP 인증을 설정합니다.

1. **Configuration(컨피그레이션)** > **Authentication(인증)** > **LDAP**으로 이동합니다.
2. LDAP 영역을 생성하기 위해 **LDAP Realms(LDAP 영역)** 탭에서 **New(새로 만들기)** 버튼을 클릭합니다.
3. 영역의 이름 및 영역 컨피그레이션 매개변수를 입력합니다. 예를 들면 다음과 같습니다.



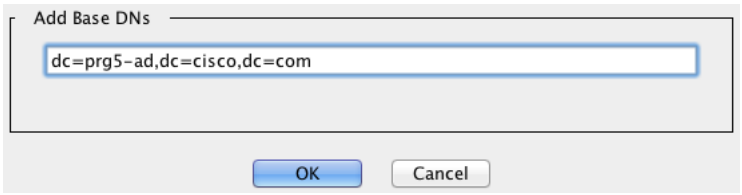
4. **OK(확인)** 버튼을 클릭합니다.

5. **LDAP Servers(LDAP 서버)** 탭을 클릭합니다.
6. **Realm name(영역 이름)** 풀다운에서는 이전에 생성한 LDAP 영역을 선택합니다.
7. **Follow referrals(추천 적용)** 확인란을 선택합니다.
8. **Type of LDAP server(LDAP 서버 유형)**를 선택하고 **기본 서버 호스트**를 입력합니다. 예를 들면 다음과 같습니다.



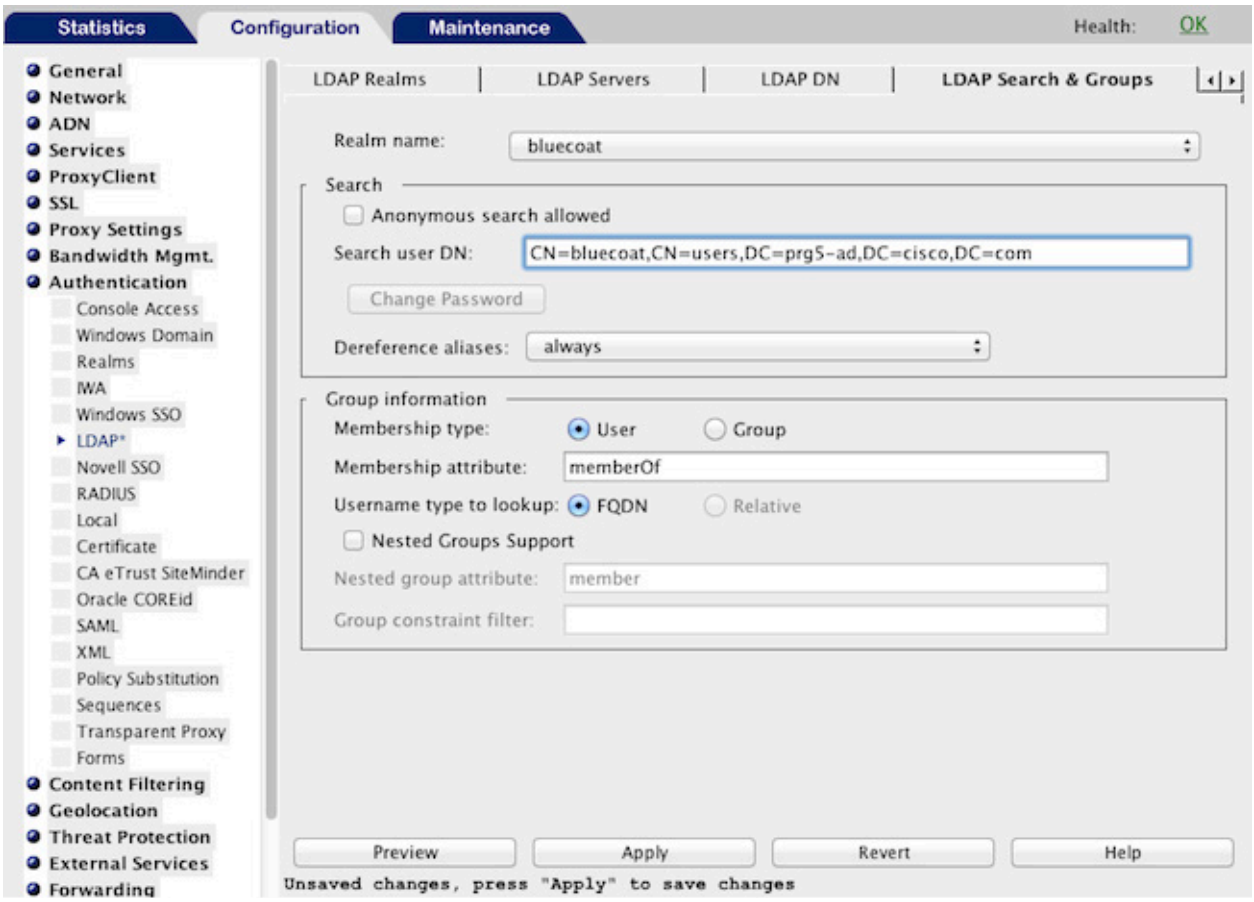
9. **Apply(적용)** 버튼을 클릭합니다.

10. **LDAP DN** 탭을 클릭합니다.
11. **New(새로 만들기)** 버튼을 클릭합니다.
12. **Add Base DNs(기본 DN 추가)** 필드에 DN 문자열을 입력합니다. 예를 들면 다음과 같습니다.



13. **OK(확인)** 버튼을 클릭합니다.

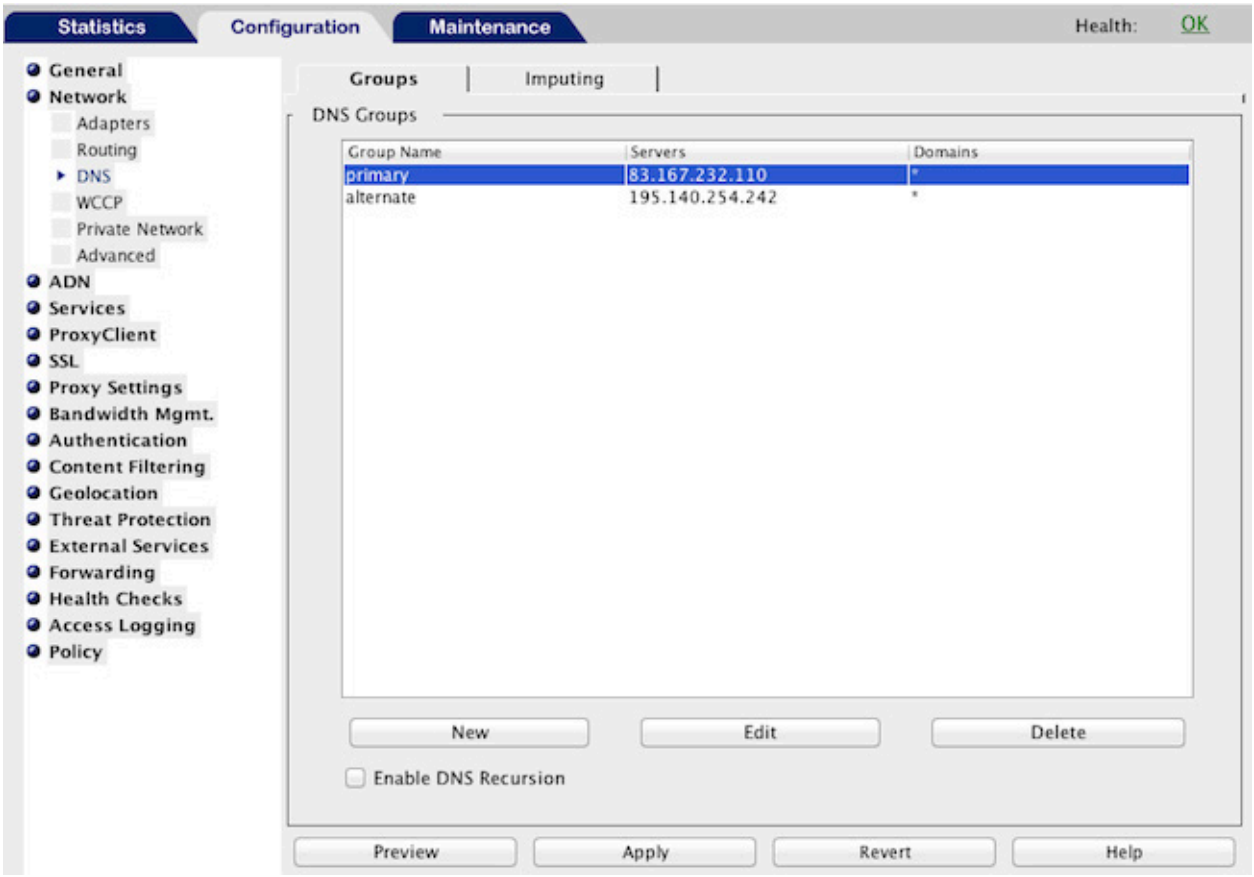
14. **LDAP Search & Groups(LDAP 검색 및 그룹)** 탭을 클릭합니다.
15. **Realm name(영역 이름)** 풀다운에서는 이전에 생성한 LDAP 영역을 선택합니다.
16. **Search user DN(사용자 DN 검색)** 정보를 입력합니다. 예를 들면 다음과 같습니다.

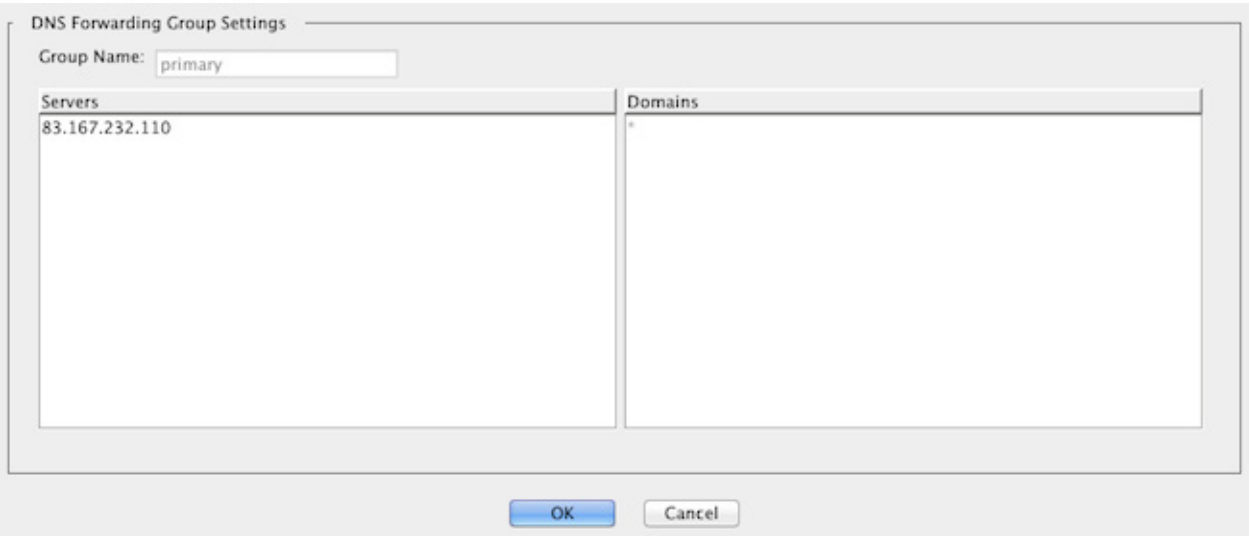


17. **Change Password(비밀번호 변경)** 버튼을 클릭합니다.
18. 비밀번호 필드에 비밀번호를 입력하고 **OK(확인)** 버튼을 클릭합니다.
19. **Apply(적용)** 버튼을 클릭합니다.

DNS 구성

다음 컨피그레이션 섹션은 선택 사항입니다. 이 항목을 변경하기 전에 IT 팀에 문의하십시오. Microsoft Active Directory를 사용하는 경우 DNS 서버 목록에 그 주소를 추가해야 하는 경우도 있습니다. 예를 들면 다음과 같습니다.





다음 단계

Cisco ScanCenter에 로그인하고 DEVICE ACCOUNTS(디바이스 계정) 페이지에서 업로드가 성공적인지 확인합니다. Blue Coat ProxySG가 보호하는 디바이스에서 웹을 탐색할 때 파일에 로깅된 텔레메트리 데이터가 분석을 위해 CTA 시스템에 업로드되며 Threats(위협) 탭과 CTA 포털에 표시됩니다. 자세한 내용은 Cisco ScanCenter 관리 설명서 릴리스 5.2의 32장, "프록시 디바이스 업로드" 섹션을 참조하십시오.

트러블슈팅

1. Blue Coat ProxySG에 로그인합니다.
2. **Configuration(컨피그레이션)** > **Access Logging(액세스 로깅)** > **Logs(로그)** > **Upload client(클라이언트 업로드)**로 이동합니다.
3. **Test upload(업로드 테스트)** 버튼을 클릭합니다.
4. **Statistics(통계)** > **Advanced(고급)** > **Event Log(이벤트 로그)**로 이동하여 로그 파일을 봅니다.
5. **Show event log tail with refresh time(새로고침 시간과 함께 이벤트 로그 테일 표시)**을 클릭합니다.

문서 가져오기 및 서비스 요청 제출

설명서 다운로드, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출, 추가 정보 수집에 대한 자세한 내용은 *Cisco 제품 설명서 업데이트*(http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html)를 참조하십시오.

새로 개정된 Cisco 기술 문서를 모두 보여주는 *What's New in Cisco Product Documentation(Cisco 제품 설명서의 새로운 사항)*을 RSS 피드로 구독하면 콘텐츠가 데스크톱으로 곧바로 전달되어 리더 애플리케이션으로 읽어볼 수 있습니다. RSS 피드는 무료로 제공되는 서비스입니다.