AppDynamics에서 단일 로그인 구성 및 문제 해결

목차

소개

이 문서에서는 AppDynamics에서 SSO(단일 로그인)를 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Single Sign-On을 구성하려면 사용자에게 어카운트 소유자(기본값) 역할 또는 관리, 에이전트, 마법사 시작 권한이 있는 사용자 지정 역할이 있어야 합니다.
- IdAccount에 대한 관리자 액세스
- AppDynamics의 메타데이터 또는 구성 세부 정보(예: 엔터티 ID, ACS URL).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AppDynamics 컨트롤러

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SSO(Single Sign-On)는 사용자가 한 번에 로그인하고 각 애플리케이션에 대해 다시 인증할 필요 없이 여러 애플리케이션, 시스템 또는 서비스에 액세스할 수 있는 인증 메커니즘입니다.

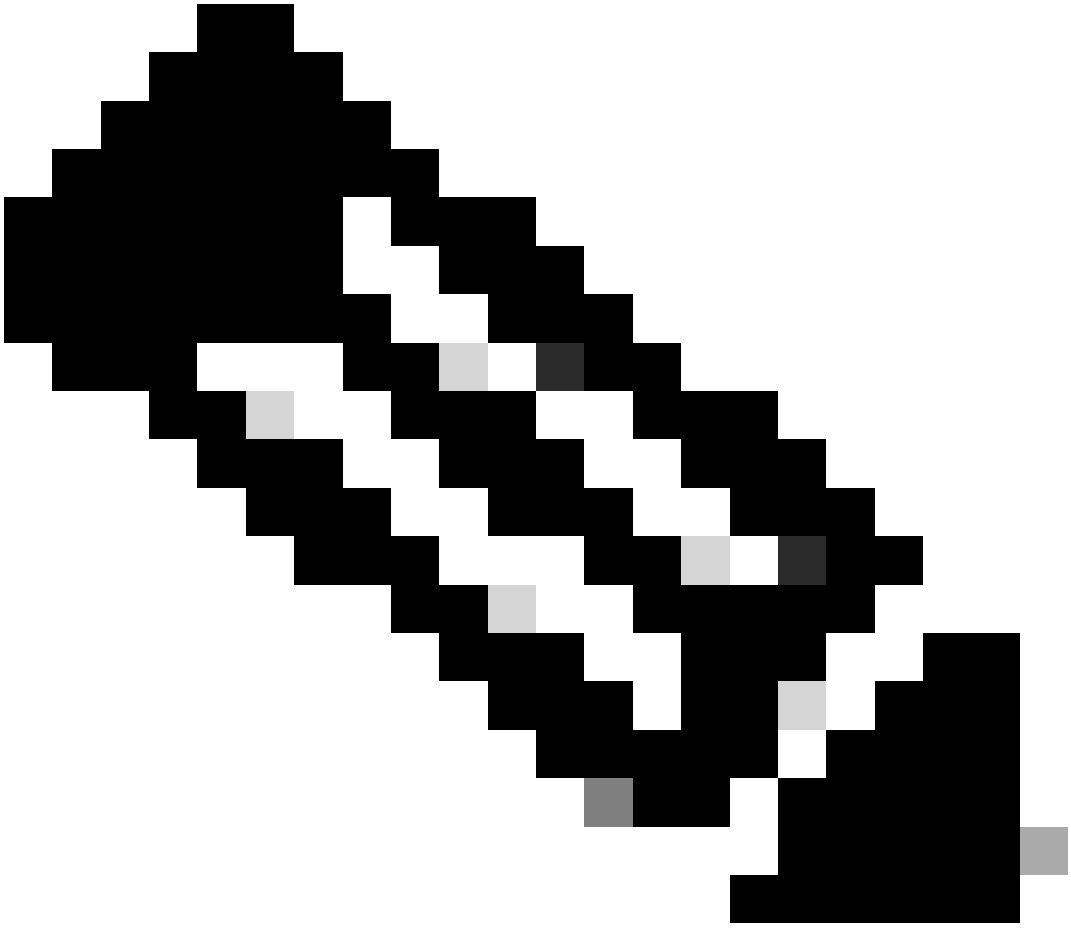
SAML(Security Assertion Markup Language)은 SSO를 구현하는 데 사용되는 기술 중 하나입니다. IdP(Identity Provider)와 SP(Service Provider) 간에 인증 및 권한 부여 데이터를 안전하게 교환하여 SSO를 활성화하는 프레임워크와 프로토콜을 제공합니다.

SAML 어설션

- XML 기반 메시지는 IdP와 SP 간에 교환됩니다.
- 세 가지 어설션 유형을 제공합니다.
  - 인증 확인: 사용자가 인증되었음을 확인합니다.
  - 특성 어설션: 사용자 이름 또는 역할과 같은 사용자 특성을 공유합니다.
  - 권한 부여 결정 어설션: 사용자에게 권한이 부여된 작업을 나타냅니다.

SAML의 주요 역할

- IdP(ID 공급자)
  - 사용자의 ID를 확인합니다.
  - 사용자의 식별 정보를 포함하는 SAML Assertion을 생성합니다.
- 서비스 공급자(SP)
  - 사용자가 액세스하려는 애플리케이션 또는 시스템입니다.
  - IdP에 의존하여 사용자를 인증합니다.
  - 사용자에게 해당 리소스 또는 애플리케이션에 대한 액세스 권한을 부여하기 위해 SAML 어설션을 수락합니다.
- 사용자(주체)
  - 요청을 시작하거나 서비스 공급자에서 리소스에 액세스하려고 시도하는 실제 사용자.
  - IdP(인증) 및 SP와 상호 작용합니다.



참고: AppDynamics는 IdP에서 시작한 SSO와 SP에서 시작한 SSO를 모두 지원합니다.

SP에서 시작한 플로우:

- 사용자는 응용 프로그램(예: AppDynamics)의 URL을 입력하거나 링크를 클릭하여 서비스 공급자로 이동합니다.
- SP가 기존 세션을 확인합니다. 세션이 존재하지 않으면 SP는 사용자가 인증되지 않았음을 인식하고 SSO 프로세스를 시작합니다.
- SP는 SAML 인증 요청을 생성하고 인증을 위해 사용자를 IdP로 리디렉션합니다.
    - 이 요청에는 다음이 포함됩니다.
        - 엔터티 ID: 서비스 공급자 고유 식별자입니다.
        - ACS(Assertion Consumer Service) URL: 여기서 IdP는 인증 후 SAML Assertion을 전송합니다.
        - SP 및 보안 세부 정보(예: 서명된 요청, 암호화 요구 사항)에 대한 메타데이터
- 사용자가 IdP 로그인 페이지로 리디렉션됩니다.
- IdP는 사용자 이름/비밀번호 또는 다단계 인증을 통해 사용자를 인증합니다.
- 인증에 성공하면 IdP는 SAML Assertion(보안 토큰)을 생성합니다.

- SAML Assertion은 HTTP POST Binding(대부분의 경우) 또는 HTTP Redirect Binding을 사용하여 사용자 브라우저를 통해 SP로 다시 전송됩니다.
- SP가 SAML Assertion을 검증하여 다음을 확인합니다.
    - 신뢰할 수 있는 IdP에서 발급되었습니다.
    - 이 주소는 SP 엔티티 ID를 통해 SP로 전달됩니다.
    - 만료되거나 훼손되지 않았습니다(IdP 공개 키를 사용하여 검증됨).

- SAML Assertion이 유효한 경우 SP는 사용자에 대한 세션을 생성합니다.
- 사용자에게 애플리케이션 또는 리소스에 대한 액세스 권한이 부여됩니다.

IdP에서 시작된 흐름:

- 사용자는 포털에서 IdP 로그로 이동하여 자격 증명을 입력합니다.
- IdP는 사용자를 인증합니다(예: 사용자 이름/비밀번호 조합, 다단계 인증).
- 인증 후 IdP는 사용자가 액세스할 수 있는 사용 가능한 애플리케이션 또는 서비스(SP) 목록을 제공합니다.
- 사용자가 원하는 SP(예: AppDynamics)를 선택합니다.
- IdP가 선택한 SP에 대한 SAML Assertion을 생성합니다.

- IdP는 사용자를 SP Assertion Consumer Service(ACS) URL로 리디렉션하고 HTTP POST 바인딩 또는 HTTP 리디렉션 바인딩을 사용하여 SAML Assertion을 함께 전송합니다.
- SP가 SAML Assertion을 수신하여 다음과 같이 검증합니다.
    - 신뢰할 수 있는 IdP가 어설션을 발행하는지 확인합니다.
    - 어설션 무결성 및 만료를 확인합니다.
    - 사용자 ID 및 기타 특성을 확인합니다.

- SAML Assertion이 유효한 경우 SP는 사용자에 대한 세션을 생성합니다.
- 사용자에게 애플리케이션 또는 리소스에 대한 액세스 권한이 부여됩니다.

구성

AppDynamics Controller는 Cisco Customer Identity 또는 외부 SAML IdP(ID 제공자)를 사용하여 사용자를 인증하고 권한을 부여할 수 있습니다.

지원되는 ID 공급자

AppDynamicscertificates for these identity providers(IdP):

- 옥타
- 오넬로진
- Ping ID
- Azure AD
- IBM 클라우드 ID
- AD FS(Active Directory Federation Service)

HTTP POST 바인딩을 지원하는 다른 IdP도 AppDynamics SAML 인증과 호환됩니다.

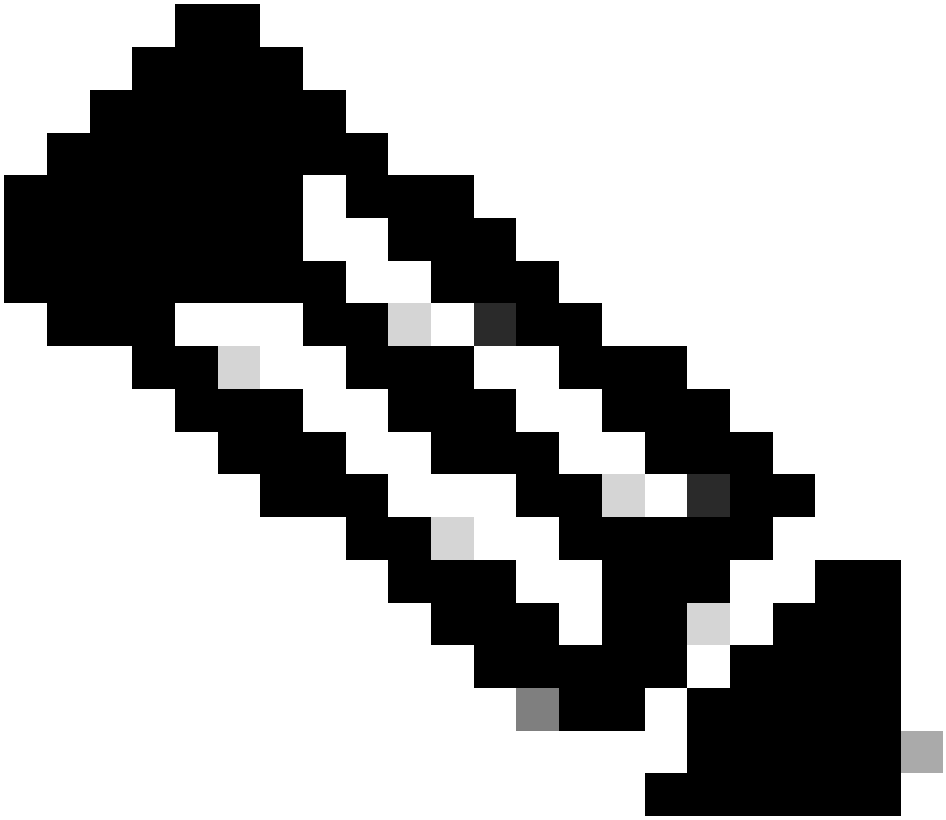
AppDynamics에서 SAML을 구성하는 단계

1단계. AppDynamics 컨트롤러 세부 정보 수집

- 엔터티 ID(SP 엔터티 ID): AppDynamics의 고유 식별자입니다(예: https://<controller-host>:<port>/controller).
  - 구문: https://<controller_domain>/컨트롤러
  - 예: https://<your_controller_domain>/컨트롤러

- 회신 URL(Assertion Consumer Service, ACS URL): IdP가 인증 후 SAML 응답을 보내는 서비스 공급자(예: AppDynamics)의 엔드포인트입니다.
  - 구문: https://<controller_domain>/controller/saml-auth?accountName=<account_name>
  - 예: https://your_controller_domain/controller/saml-auth?accountName=youraccountname

---



참고: 온프레미스 컨트롤러의 경우 accountName이 다른 멀티테넌트 컨트롤러가 없는 경우 기본 계정 이름은 customer1입니다.

- 단일 로그아웃 URL(선택 사항): SAML 로그아웃 요청을 처리할 SP의 엔드포인트(예: https://<controller_domain>/controller).

2단계. IdP에서 새 응용 프로그램을 만들고 메타데이터 다운로드

- 애플리케이션 생성 영역 찾기: 대개 IdP 관리 콘솔 또는 대시보드 내에 있으며, 애플리케이션, 웹 및 모바일 앱, 엔터프라이즈 애플리케이션 또는 당사자 등의 레이블이 표시되어 있습니다.
- 사용자 정의 또는 일반 SAML 응용 프로그램 추가: 사용자 정의 SAML 응용 프로그램 또는 일반 SAML 서비스 공급자 통합을 구성할 수 있는 옵션을 선택합니다.
- 애플리케이션 세부사항 제공: 애플리케이션에 이름을 지정하고 식별 아이콘을 업로드할 수 있습니다(선택 사항).
- 특성 매핑(사용자 이름, displayName, 전자 메일 또는 역할)을 추가하여 사용자 정보를 AppDynamics에 전달합니다.
- IdP 메타데이터 파일을 다운로드하거나 다음 세부 사항을 기록해 둡니다.
    - IdP 로그인 URL
    - 로그아웃 URL
    - 속성 이름
    - 인증서

3단계. AppDynamics 컨트롤러에서 SAML 인증 구성

- Controller UIas an Account Owner 역할 또는 Administration, Agents, Getting Started Wizard 권한이 있는 역할에 로그인합니다.
- 사용자 이름(오른쪽 상단) > 관리 > 인증 공급자 > SAML 선택을 클릭합니다.

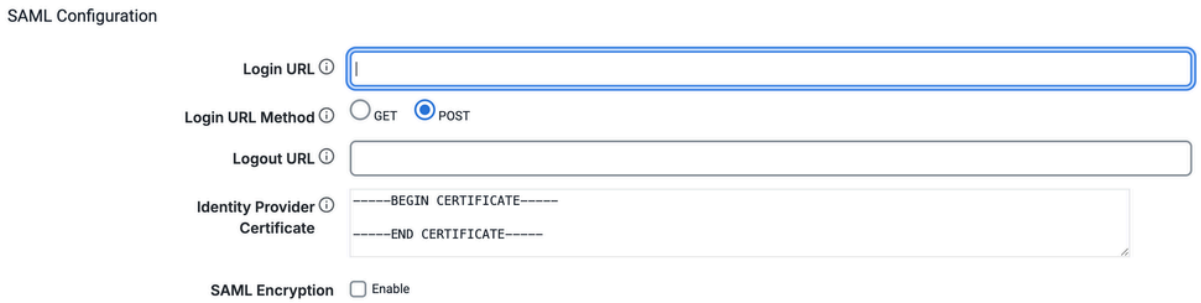
- SAML Configuration(SAML 컨피그레이션) 섹션에서 다음 세부 정보를 추가합니다.

    - 로그인 URL: AppDynamics Controller가 SP(서비스 공급자)에서 시작한 로그인 요청을 라우팅하는 IdP 로그인 URL입니다.

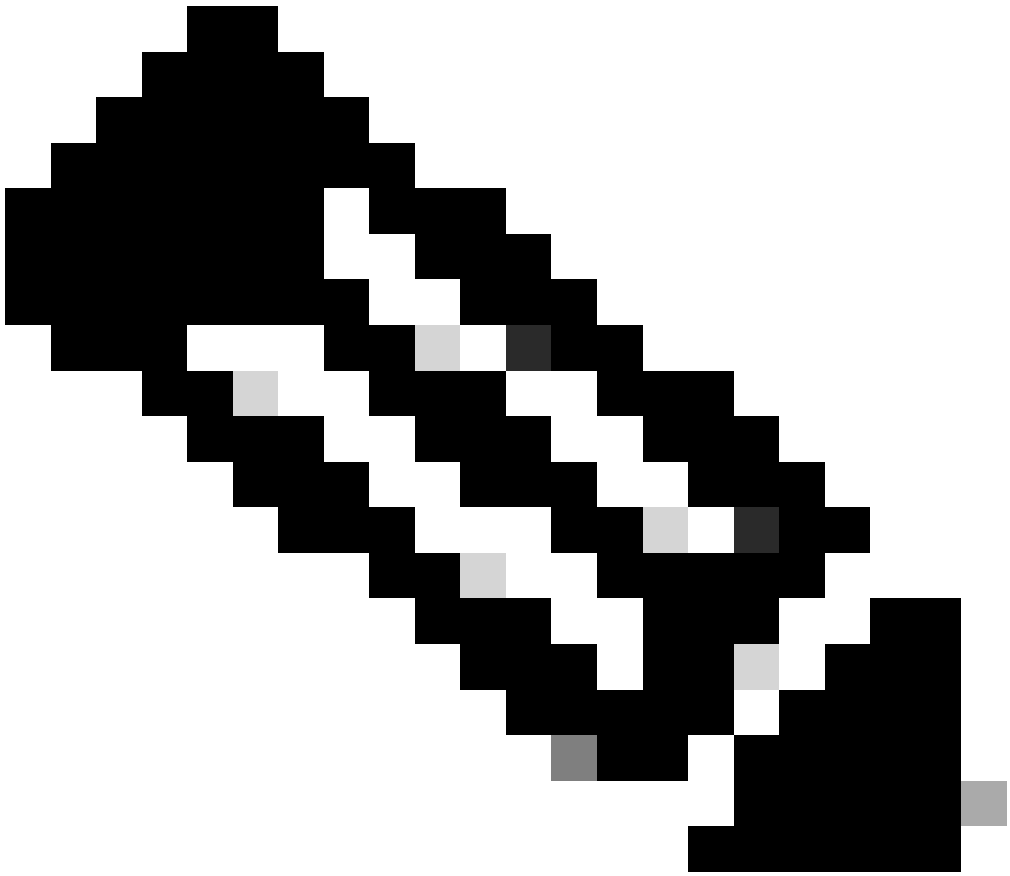
    - 로그아웃 URL(선택 사항): 사용자가 로그아웃한 후 AppDynamics Controller에서 사용자를 리디렉션하는 URL입니다. 로그아웃 URL을 지정하지 않으면 사용자가 로그아웃할 때 AppDynamics 로그인 화면이 표시됩니다.

    - 인증서: IdP의 X.509 인증서 BEGIN CERTIFICATE와 END CERTIFICATE 구분 기호 사이에 인증서를 붙여넣습니다. 소스 인증서 자체에서 BEGIN CERTIFICATE 및 END CERTIFICATE 구분 기호를 복제하지 마십시오.

    - SAML 암호화(선택 사항): SAML 응답을 IdP에서 서비스 공급자로 암호화하여 SAML 인증의 보안을 강화할 수 있습니다. AppDynamics에서 SAML 응답을 암호화하려면 SAML 어설션을 암호화하도록 IdP(ID 공급자)를 구성한 다음 특정 인증서 및 개인 키를 사용하여 암호 해독하도록 AppDynamics 컨트롤러를 구성해야 합니다.



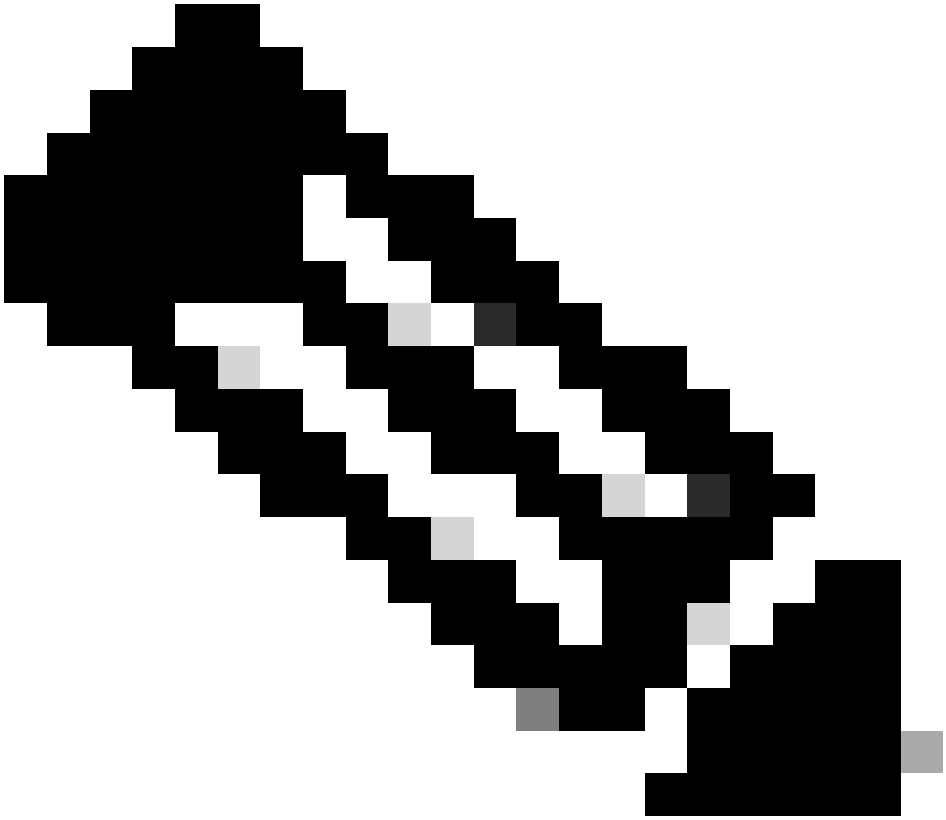
- SAML Attribute Mappings 섹션에서 SAML 특성을 매핑합니다(예: AppDynamics의 해당 필드에 대한 사용자 이름, DisplayName, 전자 메일



참고: AppDynamics는 SAML 사용자의 사용자 이름, 전자 메일 및 표시 이름을 표시합니다. 기본적으로 SAML 응답의 NameID 특성을 사용하여 사용자 이름을 생성합니다. 이 특성은 displayName으로도 사용됩니다. 이 동작은 SAML 응답에 사용자 이름, 이메일 및 displayname 특성을 포함하여 사용자 정의할 수 있습니다. AppDynamics에서 IdP 설정을 구성하는 동안 사용자는 이러한 특성 이름을 지정할 수 있습니다. 로그인하는 동안 AppDynamics는 특성 매핑이 구성되었는지 확인합니다. 매핑이 구성되어 있고 일치하는 특성이 SAML 응답에 있는 경우 AppDynamics는 해

당 특성 값을 사용하여 사용자 이름, 전자 메일 및 displayname을 설정합니다.

- SAML Group Mappings 섹션에서 이러한 세부 정보를 추가합니다.
  - SAML 그룹 속성 이름: 그룹 정보를 포함하는 SAML 속성의 이름을 입력합니다. 일반적으로 그룹, 그룹 또는 롤, 롤 또는 그룹 멤버십입니다.
  - 그룹 속성 값: 그룹 속성에 적합한 값 형식을 선택합니다. IdP에서 그룹 정보를 구성하는 방법에 따라 여러 중첩 그룹 값 또는 단일 값이 일반적인 옵션에 포함됩니다.

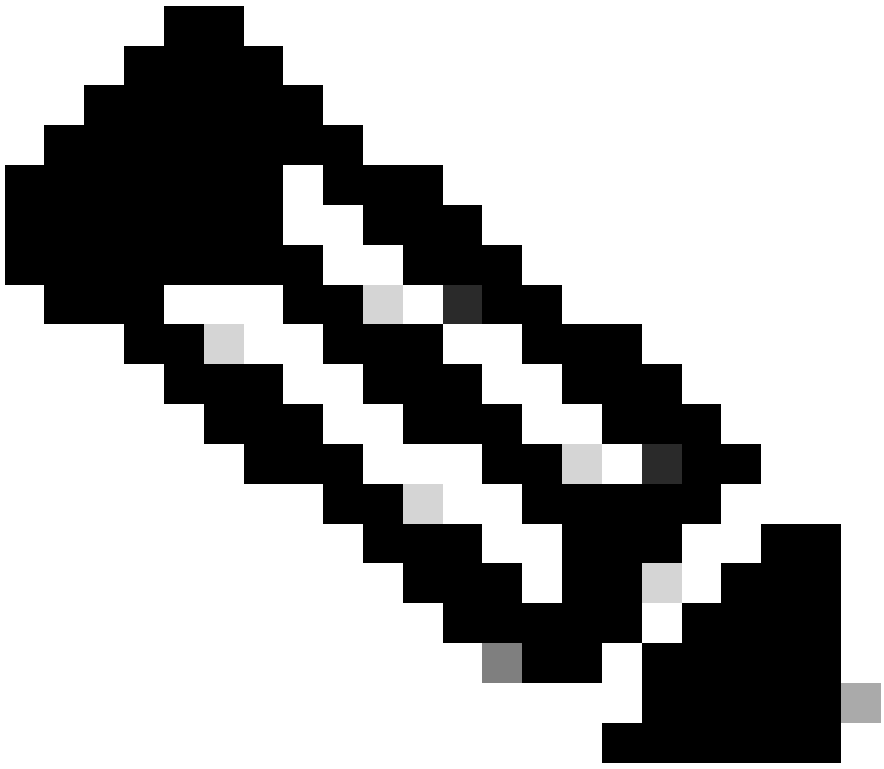


참고: 그룹 정보가 LDAP(Lightweight Directory Access Protocol) 형식인 경우 Value is in LDAP Format(값이 LDAP 형식임)을 선택합니다.

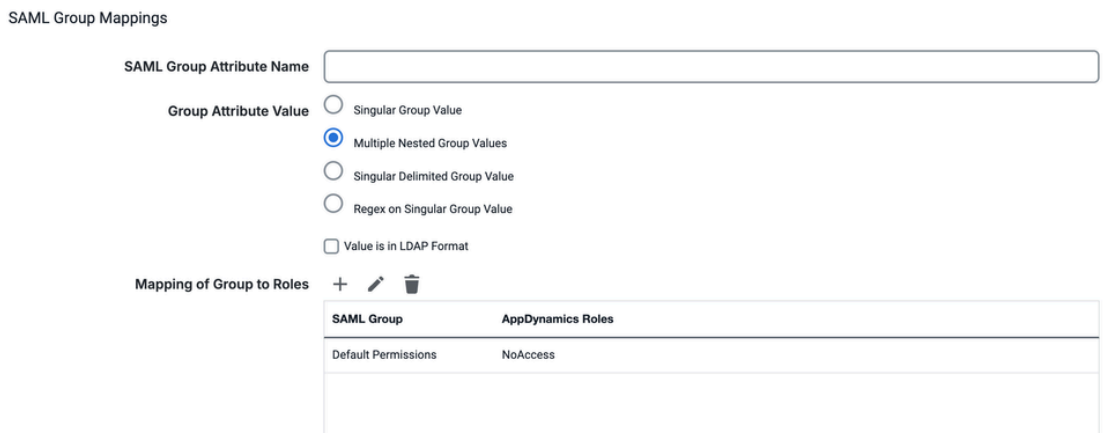
  - 역할에 그룹 매핑: + 버튼을 눌러 새 매핑을 추가합니다.
    - SAML 그룹: AppDynamics 역할에 매핑할 SAML 그룹(IdP에 정의됨)의 이름을 입력합니다.
    - 역할: SAML 그룹에 속한 사용자에게 할당할 사용 가능한 목록에서 해당

AppDynamics 역할을 선택합니다.

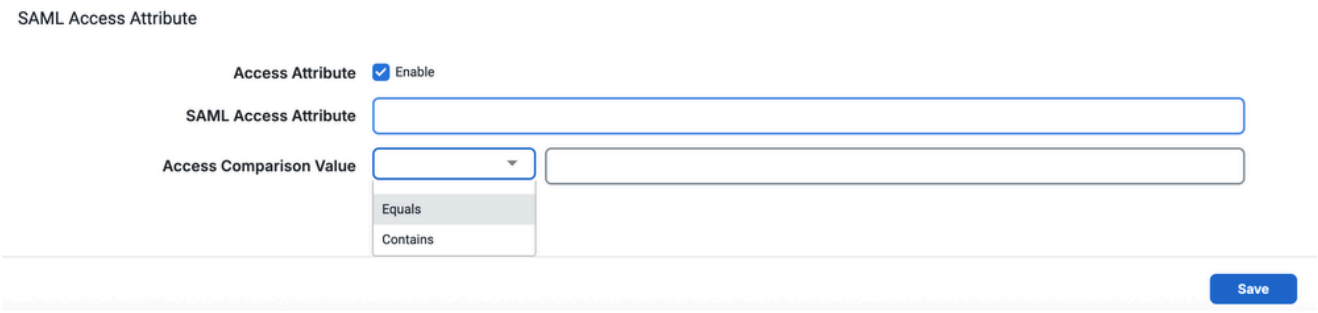
- 기본 사용 권한: SAML 그룹 매핑이 구성되지 않았거나 사용자 SAML 어설션에 그룹 정보가 포함되어 있지 않으면 AppDynamics는 기본 사용 권한으로 돌아갑니다.



참고: 최소 권한이 있는 역할을 기본 권한에 할당하는 것이 좋습니다.



- SAML Access Attribute(SAML 액세스 특성) 섹션에서 다음 세부 정보를 추가합니다(선택 사항).
  - SAML 액세스 특성: SAML 응답의 특성 이름을 입력합니다. 액세스 검증에 사용됩니다.
  - 액세스 비교 값: 다음 두 가지 옵션을 사용할 수 있습니다.
    1. 같음: SAML 응답의 특성 값이 컨피그레이션에 지정된 값과 정확히 일치하는 경우에만 액세스가 부여됩니다.
    2. 포함 내용: SAML 응답의 특성 값이 컨피그레이션에 지정된 값을 포함할 경우 액세스가 부여됩니다.
  - 사용 시 작동 방식:
    1. AppDynamics는 SAML 응답에서 SAML Access Attribute 필드에 지정된 특성을 검색합니다.
    2. 선택한 방법(같음 또는 포함)을 기준으로 특성의 값을 사용자 정의 액세스 비교 값과 비교합니다.
    3. 비교에 성공하면 사용자에게 액세스 권한이 부여됩니다.
    4. 비교가 실패하면 로그인 시도가 거부됩니다.
- Save(저장)를 클릭하여 Configuration(컨피그레이션)을 저장합니다.



다음을 확인합니다.

- 브라우저를 열고 AppDynamics Controller로 이동합니다. 서드파티 IdP 서비스에 대한 Log in(로그인) 대화 상자가 나타납니다.
- Log in with Single Sign-On을 클릭합니다. 시스템에서 IdP로 리디렉션합니다.
- 자격 증명을 입력하고 제출합니다.
- 인증에 성공하면 IdP가 AppDynamics 컨트롤러로 사용자를 리디렉션합니다.

일반적인 문제 및 해결 방법

400 잘못된 요청

- 문제점: AppDynamics 컨트롤러에 로그인하려고 할 때 사용자에게 400개의 잘못된 요청 오류가 발생했습니다.
- 샘플 오류:

```
HTTP status 400 - Bad Request
Message: Error while processing SAML Authentication Response - see server log for details
Description: The request sent by the client was syntactically incorrect.
```

- 일반적인 근본 원인:
    - 유효하지 않은 SAML 인증서
    - SAML 응답이 최대 길이보다 큽니다.
    - 잘못된 엔터티 ID 또는 ACS URL
- 해결책:
    - 유효하지 않은 SAML 인증서
        - IdP(ID 공급자)에서 제공한 인증서가 유효하고 최신 버전인지 확인합니다.
        - IdP 인증서의 만료 날짜를 확인합니다. 만료된 경우 IdP에서 새 인증서를 가져옵니다.
        - 인증서가 IdP 측에서 업데이트된 경우 새 인증서가 업로드되고 AppDynamics에서 구성되었는지 확인합니다.
        - AppDynamics에서 인증서를 업데이트하는 단계:
            - Administration, Agents, Getting Started Wizard 권한이 있는 역할 또는 계정 소유자 역할로 컨트롤러 UI에 로그인합니다.
            - 사용자 이름(오른쪽 상단) > 관리 > 인증 공급자 > SAML 선택을 클릭합니다.
            - SAML Configuration(SAML 컨피그레이션) 섹션에서 certificate(인증서) 필드를 찾고 기존 인증서를 IdP에서 제공한 새 인증서로 교체합니다.
            - Save(저장)를 클릭하여 SAML 컨피그레이션을 업데이트합니다.

    - SAML 응답이 최대 길이보다 큽니다.
        - 이 문제는 컨트롤러 버전 23.11 이상에서 GlassFish에서 Jetty Server로 컨트롤러를 이동할 때 발생합니다. Jetty Server에는 -Dorg.eclipse.jetty.server라는 속성이 있습니다. 에 있는 Request.maxFormContentSize/appserver/jetty/start.d/start.ini 파일입니다. SAML 응답 크기가 이 속성에 설정된 값을 초과하면 컨트롤러가 페이로드를 거부하고 400 Bad Request를 반환합니다 오류.
        - 대규모 SAML 응답의 원인:
            - 과도한 특성: SAML 어설션에 너무 많은 특성이 포함되어 있습니다.
            - 서명 또는 암호화된 SAML 응답: 서명 또는 암호화는 응답 크기를 늘립니다.
            - 추가 사용자 또는 그룹 데이터: IdP(Identity Provider)에 추가 사용자 또는 그룹 데이터가 있습니다.

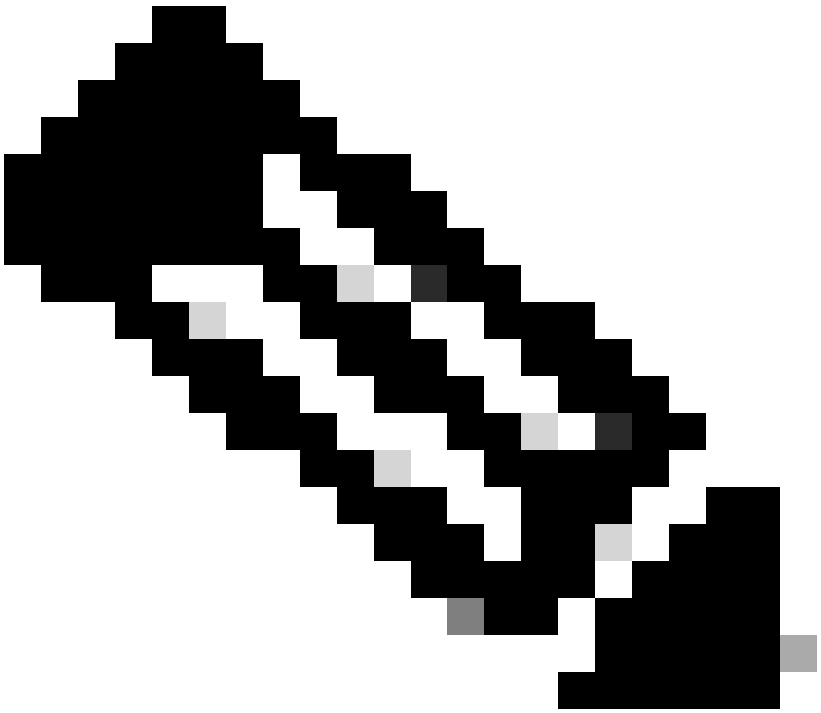
        - 이 문제를 해결하는 방법에는 두 가지가 있습니다. 이러한 솔루션 중 하나 또는 둘 다를 구현하면 문제를 해결하고 페이로드가 거부되지 않도록 할 수 있습니다.
            1. maxFormContentSize 값 증가
                - 온프레미스 컨트롤러의 경우: 에서 -Dorg.eclipse.jetty.server.Request.maxFormContentSize 속성을 업데이트합니다./appserver/jetty/start.d/start.ini 파일을 더 큰 값으로 지정하고 컨트롤러를 다시 시작합니다.
                - SaaS 컨트롤러의 경우: 지원 팀에서 이 문제를 해결하도록 지원 티켓을 제출합니다.

            2. SAML 응답 최적화

                IdP(Identity Provider)와 함께 다음 사항을 조정하여 SAML 응답의 크기를 줄

입니다.

        - 불필요한 특성 제외: IdP 컨피그레이션을 통해 SAML 어설션에서 사용되지 않거나 중복된 특성을 제거합니다.
        - 암호화 비활성화(허용되는 경우): 암호화는 SAML 응답 크기를 늘립니다. HTTPS를 통해 연결이 이미 보호되어 있는 경우, 암호화 기능을 비활성화하여 크기를 줄이는 것이 좋습니다.
    - 잘못된 엔터티 ID 또는 ACS URL
        - Idp에서:
            - 엔티티 ID가 https://your_controller_domain/controller인지 확인합니다. 엔티티 ID가 다른 경우 업데이트합니다.
            - ACS URL이 https://your_controller_domain/controller/saml-auth?accountName=youraccountname인지 확인합니다. ACS URL이 다른 경우 적절하게 업데이트합니다.



참고: accountName은 AppDynamics 계정 이름과 일치해야 합니다. (예: customer1)

- 사용자 권한 누락
    - 문제점: 컨트롤러에 로그인했지만 필요한 역할과 권한을 받지 못했습니다.
    - 컨피그레이션 및 SAML 응답 예:
        - SAML 사용자의 Group 속성에서 name은 값이 AppD_Admin 및 AppD_Power_User인 Groups입니다.

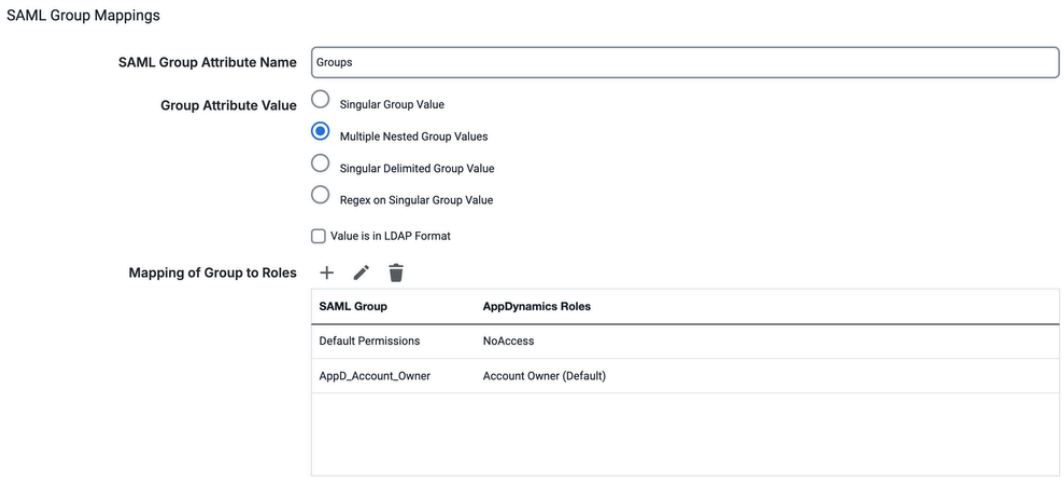
AppD_Admin

AppD_Power_User

- AppDynamics의 SAML 그룹 매핑 섹션에서 이러한 매핑이 구성됩니다.
  - SAML 그룹 특성 이름: 그룹
  - 그룹 특성 값: 여러 중첩된 그룹 값
  - 그룹 역할에 매핑:

SAML 그룹	AppDynamics 역할
AppD_계정_소유자	계정 소유자(기본값)
기본 권한	액세스 권한 없음

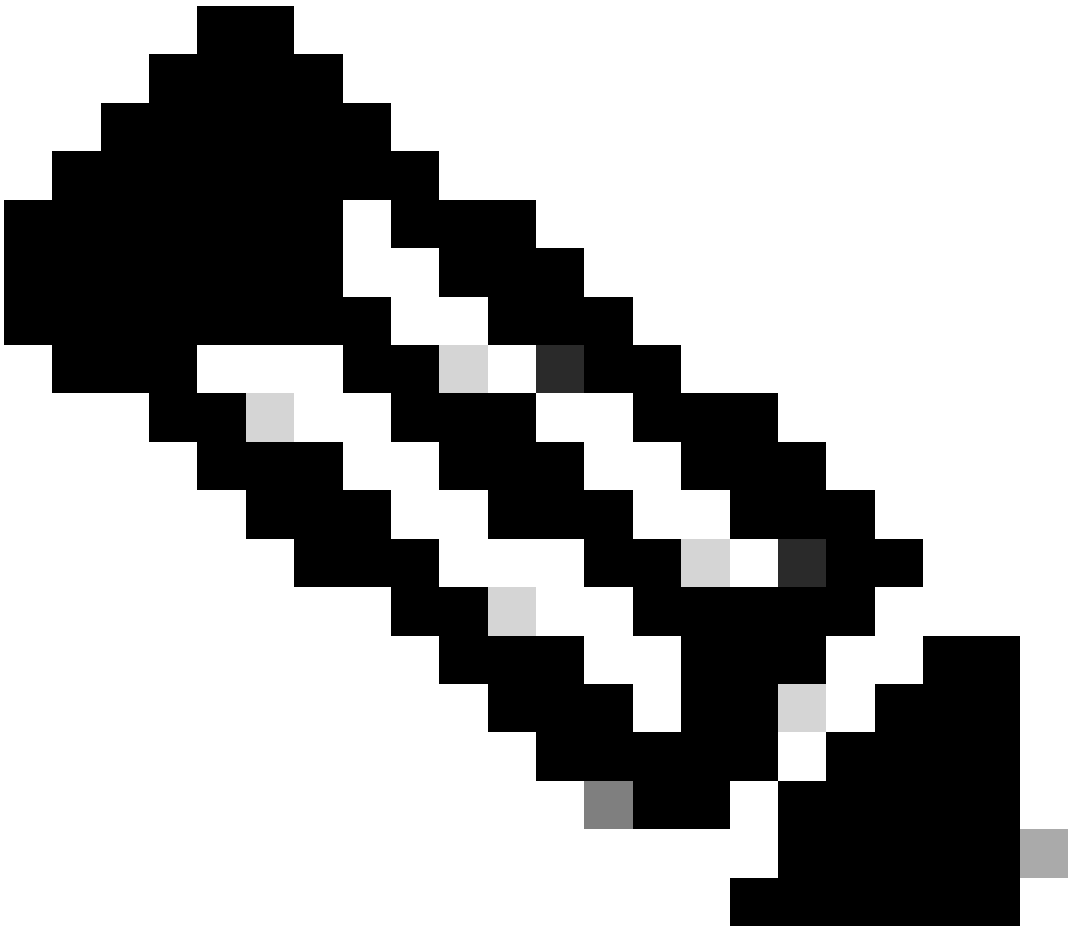
No Access는 권한이 없는 사용자 지정 역할입니다.



- 일반적인 문제 및 솔루션
  - SAML 응답에 그룹 특성이 없습니다.
    - IdP의 SAML 응답에 필수 그룹 특성이 없거나 SAML 응답의 그룹에 대한 특

성 이름이 Roles로 설정되어 있는 반면 AppDynamics에서는 Groups로 구성되어 있습니다.
    - 그룹 특성이 제공되지 않으면 사용자에게 AppDynamics의 기본 권한과 연결된 역할이 자동으로 할당됩니다.
    - 이 문제를 해결하려면 SAML 응답에 올바른 그룹 특성을 포함하도록 IdP가 구성되어 있고 그룹의 특성 이름이 AppDynamics의 구성과 일치하는지 확인하십시오.

- SAML 응답에 제공된 사용자 그룹에 대해 AppDynamics에 구성된 해당 SAML 그룹 매핑이 없습니다.
    - SAML 응답에서 Groups 특성은 값 AppD_Admin 및 AppD_Power_User를 포함합니다. 그러나 AppDynamics에서는 AppD_Account_Owner 그룹에 대해서만 그룹 매핑이 존재합니다.
    - AppD_Admin 또는 AppD_Power_User에 해당하는 매핑이 없으므로 사용자에게 어떤 역할이나 권한도 할당되지 않습니다.
    - 이 문제를 해결하려면 적절한 역할 및 권한 할당을 위해 AppDynamics에서 누락된 그룹 매핑(예: AppD_Admin 및 AppD_Power_User)을 추가합니다.



참고: AppDynamics에 구성된 SAML 그룹 특성 이름이 SAML 응답의 그룹 특성과 동일하지 않은 경우에만 기본 권한이 SAML 사용자에게 적용됩니다.

- SAML 사용자의 이메일 및/또는 이름 누락 또는 부정확함
  - 문제: 이는 일반적으로 AppDynamics의 특성 구성이 SAML 응답에서 오는 특성과 일치하지 않을 때 발생합니다.
  - SAML 응답 예: SAML 응답의 속성은 다음과 같습니다. User.email, User.fullName 및 그룹

```
example@domain.com
```

```
FirstName LastName
```

```
AppD_Admin
```

```
AppD_Power_User
```

- AppDynamics의 SAML 특성 매핑 예
  - 사용자 이름 특성: 사용자 이름
  - 표시 이름 특성: User.firstName 또는 공백
  - 이메일 특성: User.userPrincipal 또는 공백

  - 근본 원인: AppDynamics에 구성된 표시 이름 및 전자 메일 특성이 SAML 응답에 제공된 특성과 일치하지 않습니다.
    - 그 결과
      - 이메일이 공백으로 설정되어 있습니다.
      - 표시 이름은 기본적으로 사용자 이름으로 설정됩니다.
  - 해결책: AppDynamics에 구성된 표시 이름 및 전자 메일 특성이 SAML 응답의 해당 특성과 일치하는지 확인합니다.
    - 예를 들면 다음과 같습니다.
      - Display Name 특성을 User.fullName으로 업데이트합니다.
      - Email 특성을 User.email로 업데이트합니다.

- HTTP 404 오류

- 문제점: 사용자가 컨트롤러에 로그인할 수 없으며 404 not found 오류가 발생합니다.
- 샘플 오류: 컨트롤러 로그(온프레미스 컨트롤러에만 해당)에서 다음 오류가 표시됩니다.

```
[#|2025-01-10T21:16:35.222+0000|SEVERE|glassfish 4.1|com.singularity.ee.controller.auth.saml.SAMLA
com.appdynamics.platform.services.auth.exception.SamlException: Requested url validation failed
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.validateRequest
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.getSamlAuthenti
```

- 근본 원인: 이 오류는 일반적으로 컨트롤러 데이터베이스에 구성된 컨트롤러 URL이 로그인에 사용된 컨트롤러 URL 또는 IdP에 구성된 URL과 일치하지 않을 때 발생합니다
- 해결책:
  - 온프레미스 컨트롤러의 경우:
    - 이 명령을 실행하여 컨트롤러 URL을 업데이트합니다(권장).

```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{
```

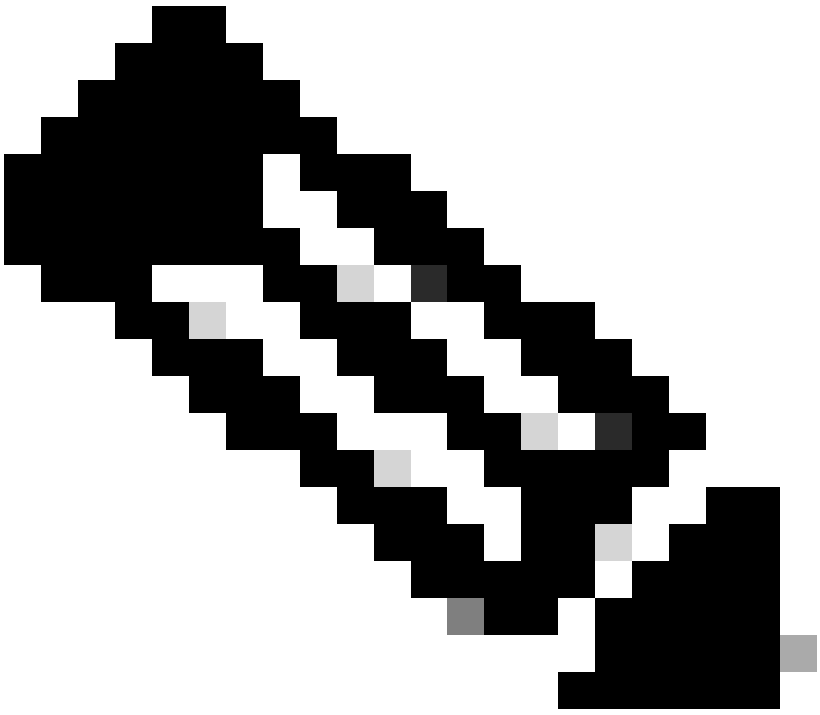
```
/controller" }' http://

 /controller/rest/accounts/

  /update-controller-url
```

- 또는 컨트롤러 데이터베이스에서 이러한 명령을 실행하여 컨트롤러 URL을 업데이트할 수 있습니다.

```
UPDATE controller.account SET controller_url ='

' WHERE id=

 ;
UPDATE mds_auth.account SET controller_url='

 ' WHERE name='

  ';
```

- <ACCOUNT_ID>를 가져오려면 이 명령을 실행합니다.

```
Select id from controller.account where name = '

      ';
```



참고: 동일한 문제가 여전히 관찰될 경우 curl -X POST -u root@system https://<controller_domain>/controller/api/controllermds/syncAll을 실행합니다.

- 바꾸기:
  - 컨트롤러에 액세스하기 위해 사용 중인 실제 컨트롤러 URL이 있는 <NEW_CONTROLLER_URL>.
  - <controller_domain>을(를) 컨트롤러 도메인과 연결합니다.
  - <youraccountname>을(를) 계정 이름과 함께 사용합니다.

- SaaS 컨트롤러의 경우: 지원 팀에서 이 문제를 해결하도록 지원 티켓을 제출합니다.

추가 지원 필요

질문이 있거나 문제가 있는 경우 다음 세부 정보가 포함된 지원 티켓을 생성하십시오.

- Error Details or Screenshot(오류 세부사항 또는 스크린샷): 특정 오류 메시지 또는 문제의 스크린샷을 제공합니다.

- SAML 응답: SAML-Trace 및 HAR 파일 수집
- Controller Server.log(온프레미스 전용): 해당되는 경우 <controller-install-dir>/logs/server.log의 컨트롤러 서버 로그를 제공합니다.

관련 정보

AppDynamics 설명서

SaaS 구축용 SAML

SaaS 구축을 위한 SAML 응답 암호화

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.