

SSO를 사용하여 NTLM을 올바르게 설정하려면 어떻게 해야 합니까(투명하게 전송된 자격 증명)?

목차

질문:

증상:NTLM 인증이 사용될 때 브라우저에 자격 증명을 묻는 메시지가 표시됩니다.

환경:Cisco WSA(Web Security Appliance), 모든 버전의 AsyncOS

클라이언트가 자격 증명을 자동으로 전송할지(SSO - Single Sign On) 또는 최종 사용자에게 자격 증명을 수동으로 입력하도록 프롬프트를 표시할지 여부에 영향을 줄 수 있습니다. SSO와 함께 NTLM을 구현할 때 다음 항목을 확인합니다.

WSA 인증 구성:

NTLM Basic만이 아니라 NTLMSSP를 사용하도록 WSA가 설정되어 있는지 확인합니다.

이 설정은 GUI의 **Web Security Manager > Identities** 페이지 아래에서 찾을 수 있습니다. 적절한 ID를 편집한 다음 Define Members by Authentication(인증별 구성원 정의) > **Authentication Schemes(인증 체계) 설정**을 선택합니다.

다음 옵션 중 하나를 선택합니다.

NTLMSSP는 클라이언트가 자격 증명을 웹 프록시에 안전하고 투명하게 보낼 수 있도록 합니다.

NTLM Basic에서는 자격 증명을 입력하라는 메시지가 표시되면 클라이언트가 일반 텍스트로 사용자 이름과 암호를 보낼 수 있습니다.

Use Basic(기본 사용) 또는 NTLMSSP(NTLMSSP 사용) 옵션을 선택한 경우 클라이언트가 가장 적합한 방법을 선택합니다(권장). 클라이언트가 NTLMSSP를 지원하는 경우 이 방법을 사용하며 다른 모든 브라우저에서는 Basic을 사용합니다.이를 통해 호환성을 극대화할 수 있습니다.

클라이언트 트러스트:

클라이언트가 WSA를 신뢰하지 않으면 해당 클라이언트의 자격 증명을 투명하게 전송하지 않습니다.다음은 클라이언트가 WSA를 신뢰하지 않는 환경의 문제를 해결하는 데 도움이 되는 지침입니다.

클라이언트가 인증 리디렉션 URL을 신뢰하지 않습니다(투명 구축만 해당).

투명 구축에서 WSA는 인증을 수행하려면 클라이언트를 자신에게 리디렉션해야 합니다. 클라이언트가 이 리디렉션 위치를 신뢰할 수 있거나 신뢰할 수 없습니다.

기본적으로 WSA는 P1의 FQDN(또는 프록시 데이터에 사용되는 경우 M1 인터페이스)으로 리디렉션됩니다. 이 FQDN은 FQDN이므로 Internet Explorer는 이 FQDN이 네트워크 외부의 리소스인 것으로 간주하므로 이를 신뢰하지 않습니다.

Internet Explorer가 WSA를 신뢰하도록 하는 두 가지 방법이 있습니다.