

Tidal Enterprise Orchestrator: 강화된 Windows 설정 유효성 검사

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[증상](#)

[상태](#)

[해결](#)

[Windows 정책 설정 확인](#)

[관련 정보](#)

소개

Microsoft® Windows에 대해 권장되는 강화 정책을 사용하면 보안 강화 구성으로 인해 Business Objects InfoView 웹 인터페이스가 차단될 수 있습니다. 보안 오류 대화 상자는 신뢰할 수 있는 웹 사이트 목록에 사이트를 추가하도록 사용자에게 알립니다.

[사전 요구 사항](#)

[요구 사항](#)

이 문서에 대한 특정 요건이 없습니다.

[사용되는 구성 요소](#)

Windows 2003, Windows 2008

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

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

[증상](#)

Windows 시스템을 강화하여 정책 설정을 적용하면 TEO Windows 스크립트 및 Windows 명령 작업이 작동하지 않을 수 있습니다. 사용자가 올바른 설정을 확인하는 것이 좋습니다.

[상태](#)

해결 방법 찾기

[해결](#)

[Windows 정책 설정 확인](#)

Windows 정책 설정을 확인하려면 다음 단계를 완료하십시오.

1. Start(시작) > Administrative Tools(관리 툴) > Local Security Policy(로컬 보안 정책)를 클릭합니다.
2. Security Settings(보안 설정)에서 Local Policies(로컬 정책)를 확장합니다. 그런 다음 보안 옵션을 클릭합니다.
3. Security Options(보안 옵션) 창에서 Network access(네트워크 액세스)를 마우스 오른쪽 버튼으로 클릭하고 Properties(속성)를 선택합니다. 네트워크 인증을 위한 .NET 패스포트의 자격 증명 저장을 허용하지 않도록 네트워크 액세스를 설정합니다. 대화 상자가 표시됩니다.
4. Disabled(비활성화됨) 옵션을 클릭합니다. 그런 다음 확인을 클릭합니다. 정책 설정이 검증됩니다.

[관련 정보](#)

- [기술 지원 및 문서 - Cisco Systems](#)