

# View 보안

VMware Horizon 7 7.2



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware 코리아**  
서울시 강남구  
영동대로 517  
아셈타워 13층  
(우) 06164  
전화: +82 2 3016 6500  
팩스: +82 2 3016 6501  
[www.vmware.com/kr](http://www.vmware.com/kr)

Copyright © 2009–2017 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

# 목차

View 보안 5

## 1 Horizon 7 계정, 리소스 및 로그 파일 6

Horizon 7 계정 6

Horizon 7 리소스 7

Horizon 7 로그 파일 8

## 2 View 보안 설정 9

View Administrator의 보안 관련 전역 설정 9

View Administrator의 보안 관련 서버 설정 11

View LDAP의 보안 관련 설정 12

## 3 포트 및 서비스 14

View TCP 및 UDP 포트 14

View에서의 HTTP 리디렉션 17

View 연결 서버 호스트의 서비스 18

보안 서버의 서비스 18

## 4 View 연결 서버 인스턴스 또는 보안 서버의 보안 프로토콜 및 암호 제품군 구성 20

보안 프로토콜과 암호 제품군의 기본 전역 정책 20

전역 수락 및 제안 정책 구성 21

View LDAP에 정의된 전역 수락 및 제안 정책 21

전역 수락 및 제안 정책 변경 22

개별 View Server의 수락 정책 구성 23

View 데스크톱에서 제안 정책 구성 24

이전 프로토콜 및 암호가 View에서 사용되지 않도록 설정됨 24

## 5 Blast 보안 게이트웨이의 보안 프로토콜 및 암호 제품군 구성 27

BSG(Blast 보안 게이트웨이)의 보안 프로토콜 및 암호 제품군 구성 27

## 6 보안 Horizon 7 환경에 USB 디바이스 배포 29

모든 유형의 디바이스에 대한 USB 리디렉션 사용 안 함 29

특정 디바이스에 대해 USB 리디렉션을 사용하지 않도록 설정 30

## 7 연결 서버 및 보안 서버의 HTTP 보호 조치 33

Internet Engineering Task Force 표준 33

World Wide Web Consortium 표준 34

크로스 원본 리소스 공유 34

컨텐츠 보안 정책	36
다른 보호 조치	37
MIME 유형 보안 위협 줄이기	37
사이트 간 스크립팅 공격 완화	37
컨텐츠 유형 검사	37
사용자 에이전트 화이트리스트	38
HTTP 보호 조치 구성	38

# View 보안

"View 보안"에서는 VMware Horizon 7의 보안 기능에 대한 간단한 참조 정보를 제공합니다.

- 필수 시스템 및 데이터베이스 로그인 계정.
- 보안과 관련이 있는 구성 옵션 및 설정.
- 보안 관련 구성 파일 및 암호, 그리고 보안 작업을 위해 권장되는 액세스 제어 등 보호해야 할 리소스.
- 로그 파일 위치 및 용도.
- View가 올바르게 작동하기 위해 열어 두거나 사용하도록 설정해야 하는 외부 인터페이스, 포트 및 서비스입니다.

## 대상

이 정보는 IT 의사 결정권자, 설계자 및 관리자를 비롯하여 View의 보안 구성 요소를 숙지해야 하는 사용자를 대상으로 합니다.

# Horizon 7 계정, 리소스 및 로그 파일

# 1

특정 구성 요소에 대해 서로 다른 계정을 사용하면 개인에게 필요한 것보다 많은 액세스 및 권한이 부여되는 것을 방지할 수 있습니다. 구성 파일과 중요한 데이터가 있는 위치를 알면 다양한 호스트 시스템에서 보안을 설정하는 데 도움이 됩니다.

**참고** Horizon 7.0부터 View Agent가 Horizon Agent로 변경되었습니다.

본 장은 다음 항목을 포함합니다.

- [Horizon 7 계정](#)
- [Horizon 7 리소스](#)
- [Horizon 7 로그 파일](#)

## Horizon 7 계정

Horizon 7 구성 요소를 관리하려면 시스템 계정과 데이터베이스 계정을 설정해야 합니다.

표 1-1. Horizon 7 시스템 계정

Horizon 구성 요소	필수 계정
Horizon Client	원격 데스크톱과 애플리케이션에 액세스할 수 있는 사용자를 위해 Active Directory에 사용자 계정을 구성합니다. 사용자 계정은 원격 데스크톱 사용자 그룹의 구성원이어야 하지만 이 계정에는 Horizon 관리자 권한이 필요하지 않습니다.
vCenter Server	Horizon 7를 지원하는 데 필요한 작업을 vCenter Server에서 수행할 권한이 있는 사용자 계정을 Active Directory에 구성합니다. 필요한 권한에 대한 자세한 내용은 "View 설치" 문서를 참조하십시오.

Horizon 구성 요소	필수 계정
View Composer	View Composer에서 사용할 Active Directory에 사용자 계정을 생성하십시오. 연결된 클론 데스크톱을 Active Directory 도메인에 연결하려면 View Composer에서 이 계정을 사용해야 합니다. 사용자 계정은 Horizon 관리 계정과 달라야 합니다. 특정 Active Directory 컨테이너에서 컴퓨터 개체를 생성 또는 제거하는 데 필요한 최소 권한을 계정에 부여하십시오. 예를 들어, 계정에는 도메인 관리자 권한이 필요하지 않습니다. 필요한 권한에 대한 자세한 내용은 "View 설치" 문서를 참조하십시오.
연결 서버	Horizon 7를 설치할 때 특정 도메인 사용자, 로컬 관리자 그룹 또는 특정 도메인 사용자 그룹을 Horizon Administrator로 지정할 수 있습니다. Horizon Administrator로 구성된 전용 도메인 사용자 그룹을 생성하는 것이 좋습니다. 기본값은 현재 로그인된 도메인 사용자입니다. Horizon Administrator에서는 <b>View 구성 &gt; 관리자</b> 를 사용하여 Horizon Administrator 목록을 변경할 수 있습니다. 필요한 권한에 대한 자세한 내용은 "View 관리" 문서를 참조하십시오.

표 1-2. Horizon 데이터베이스 계정

Horizon 구성 요소	필수 계정
View Composer 데이터베이스	SQL Server 또는 Oracle 데이터베이스는 View Composer 데이터를 저장합니다. View Composer 사용자 계정과 연결할 수 있는 데이터베이스의 관리 계정을 생성합니다. View Composer 데이터베이스 설정에 대한 자세한 내용은 "View 설치" 문서를 참조하십시오.
Horizon 연결 서버에서 사용하는 이벤트 데이터베이스	SQL Server 또는 Oracle 데이터베이스는 Horizon 이벤트 데이터를 저장합니다. Horizon Administrator가 이벤트 데이터에 액세스하는 데 사용할 수 있는 데이터베이스의 관리 계정을 생성합니다. View Composer 데이터베이스 설정에 대한 자세한 내용은 "View 설치" 문서를 참조하십시오.

보안 취약점의 위험을 감소시키려면 다음 작업을 수행하십시오.

- 조직에서 사용하는 다른 데이터베이스 서버와는 별도의 서버에 Horizon 7 데이터베이스를 구성합니다.
- 단일 사용자 계정이 여러 데이터베이스에 액세스하지 못하도록 하십시오.
- View Composer 및 이벤트 데이터베이스 액세스를 위한 별도의 계정을 구성하십시오.

## Horizon 7 리소스

Horizon 7에는 보호해야 하는 몇 가지 구성 파일과 유사한 리소스가 포함되어 있습니다.

표 1-3. Horizon 연결 서버 및 보안 서버 리소스

리소스	위치	보호
LDAP 설정	적용할 수 없습니다.	LDAP 데이터는 역할 기반 액세스 제어의 일부로 자동 보호됩니다.
LDAP 백업 파일	%ProgramData%\VMware\WDM\backups	액세스 제어로 보호됩니다.
locked.properties (보안 게이트웨이 구성 파일)	install_directory\VMware\Wmware View\Server\Wsslgateway\Wconf	이 파일은 Horizon 관리자 이외의 모든 사용자 액세스로부터 보호해야 합니다.

리소스	위치	보호
absg.properties(Blast 보안 게이트웨이 구성 파일)	install_directory\VMware\VMware View\Server\Wappblastgateway	이 파일은 Horizon 관리자 이외의 모든 사용자 액세스로부터 보호해야 합니다.
로그 파일	Horizon 7 로그 파일의 내용을 참조하십시오.	액세스 제어로 보호됩니다.
web.xml (Tomcat 구성 파일)	install_directory\VMware View\Server\Wbroker\Web apps\WROOT\Web-INF	액세스 제어로 보호됩니다.

## Horizon 7 로그 파일

Horizon 7에서는 해당 구성 요소의 설치 및 작업을 기록하는 로그 파일을 생성합니다.

**참고** Horizon 7 로그 파일은 VMware 지원에서 사용하기 위한 것입니다. VMware에서는 이벤트 데이터베이스를 구성하고 사용하여 Horizon 7을 모니터링할 것을 권장합니다. 자세한 내용은 “View 설치” 및 “View 통합” 설명서를 참조하십시오.

표 1-4. Horizon 7 로그 파일

Horizon 구성 요소	파일 경로 및 기타 정보
모든 구성 요소(설치 로그)	%TEMP%\Wvminst.log_date _ timestamp %TEMP%\Wvmmsi.log_date _ timestamp
Horizon Agent	<Drive Letter>:\ProgramData\VMware\WDM\logs <Drive Letter>:\ProgramData\VMware\WDM\logs에 저장된 Horizon 7 로그 파일에 액세스하려면 상승된 관리자 권한으로 프로그램에서 로그를 열어야 합니다. 그러려면 프로그램 파일을 마우스 오른쪽 버튼으로 클릭하고 <b>관리자 권한으로 실행</b> 을 선택합니다. UDD(사용자 데이터 디스크)가 구성되어 있으면 <Drive Letter>는 UDD에 해당하는 드라이브 문자입니다. PCoIP 로그는 이름이 pcoip_agent*.log와 pcoip_server*.log입니다.
게시된 애플리케이션	SQL Server 또는 Oracle 데이터베이스 서버에 구성된 View 이벤트 데이터베이스. Windows 애플리케이션 이벤트 로그. 기본적으로 사용하지 않도록 설정됩니다.
View Composer	연결된 클론 데스크톱의 %system_drive%\Windows\Temp\VMware-viewcomposer-ga-new.log. View Composer 로그에는 QuickPrep 및 Sysprep 스크립트의 실행 정보가 포함됩니다. 이 로그에는 스크립트 실행 시작 시간과 종료 시간 및 모든 출력 또는 오류 메시지가 기록됩니다.
연결 서버 또는 보안 서버	<Drive Letter>:\ProgramData\VMware\WDM\logs. 로그 디렉토리는 View 일반 구성 ADMX 템플릿 파일(vdm_common.admx)의 로그 구성 설정에서 구성 가능합니다. PCoIP 보안 게이트웨이 로그는 PCoIP Secure Gateway 하위 디렉토리에 있는 SecurityGateway_*.log라는 파일에 기록됩니다. Blast 보안 게이트웨이 로그는 Blast Secure Gateway 하위 디렉토리에 있는 absg*.log라는 파일에 기록됩니다.
Horizon 서비스	SQL Server 또는 Oracle 데이터베이스 서버에 구성된 Horizon 이벤트 데이터베이스. Windows 시스템 이벤트 로그.



## View 보안 설정

View에는 구성의 보안을 조정하는 데 사용할 수 있는 여러 설정이 포함되어 있습니다. 필요 시 View Administrator를 사용하거나 ADSI Edit 유틸리티를 사용하여 설정에 액세스할 수 있습니다.

---

**참고** Horizon Client 및 Horizon Agent의 보안 설정에 대한 자세한 내용은 "Horizon Client 및 Agent 보안" 문서를 참조하십시오.

---

본 장은 다음 항목을 포함합니다.

- [View Administrator의 보안 관련 전역 설정](#)
- [View Administrator의 보안 관련 서버 설정](#)
- [View LDAP의 보안 관련 설정](#)

### View Administrator의 보안 관련 전역 설정

클라이언트 세션 및 연결에 대한 보안 관련 전역 설정은 View Administrator의 **View 구성 > 전역 설정**에서 액세스할 수 있습니다.

표 2-1. 보안 관련 전역 설정

설정	설명
<b>데이터 복구 암호 변경</b>	<p>암호는 암호화된 백업에서 View LDAP 구성을 복원할 때 필요합니다.</p> <p>View 연결 서버 버전 5.1 이상을 설치할 때 데이터 복구 암호를 입력하십시오. 설치 후에 View Administrator에서 이 암호를 변경할 수 있습니다.</p> <p>View 연결 서버를 백업할 때 View LDAP 구성이 암호화된 LDIF 데이터로 내보내집니다. vdmimport 유틸리티를 사용해 암호화된 백업을 복원하려면 데이터 복구 암호를 입력해야 합니다. 암호는 1 ~ 128자 사이여야 합니다. 조직의 모범 사례에 따라 보안 암호를 생성하십시오.</p>
<b>메시지 보안 모드</b>	<p>JMS 메시지가 View 구성 요소 간에 전송될 때 사용되는 보안 메커니즘을 결정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>사용 안 함</b>으로 설정된 경우, 메시지 보안 모드를 사용하지 않습니다.</li> <li>■ <b>사용</b>으로 설정된 경우 JMS 메시지의 레거시 메시지 서명 및 확인이 수행됩니다. View 구성 요소는 서명되지 않은 메시지를 거부합니다. 이 모드는 SSL 및 일반 JMS 연결의 혼합을 지원하지 않습니다.</li> <li>■ <b>항상</b>으로 설정된 경우 모든 메시지를 암호화하기 위해 모든 JMS 연결에 대해 SSL이 사용됩니다. View 구성 요소가 메시지를 전송하고 메시지를 수신하는 대상인 JMS 항목을 제한하기 위해 액세스 제어도 사용하도록 설정됩니다.</li> <li>■ <b>혼합</b>으로 설정된 경우, 메시지 보안 모드를 사용하도록 설정되지만 View Manager 3.0 이전의 View 구성 요소에는 적용되지 않습니다.</li> </ul> <p>신규 설치의 경우 기본 설정은 <b>항상</b>입니다. 이전 버전에서 업그레이드하는 경우 이전 버전에서 사용된 설정이 유지됩니다.</p> <p><b>중요</b> 모든 View 연결 서버 인스턴스, 보안 서버 및 View 데스크톱을 이 릴리스로 업그레이드한 후 메시지 보안 모드를 <b>항상</b>으로 설정하는 것이 좋습니다. <b>항상</b> 설정은 많은 중요한 보안 향상 기능과 MQ(메시지 대기열) 업데이트를 제공합니다.</p>
<b>항상된 보안 상태(읽기 전용)</b>	<p><b>메시지 보안 모드</b>가 <b>사용</b>에서 <b>항상</b>으로 변경될 때 나타나는 읽기 전용 필드입니다. 단계적으로 변경되기 때문에 이 필드에는 단계에 따른 진행률이 표시됩니다.</p> <ul style="list-style-type: none"> <li>■ <b>Message Bus 다시 시작을 기다리는 중</b>은 첫 번째 단계입니다. 이 상태는 포드의 모든 연결 서버 호스트에서 VMware Horizon View Message Bus 구성 요소 서비스를 수동으로 다시 시작하거나 포드의 모든 연결 서버 인스턴스를 수동으로 다시 시작할 때까지 표시됩니다.</li> <li>■ <b>항상 보류 중</b>은 다음 상태입니다. 모든 View Message Bus 구성 요소 서비스가 다시 시작된 후 시스템이 모든 데스크톱 및 보안 서버에 대한 메시지 보안 모드를 <b>항상</b>으로 변경하기 시작합니다.</li> <li>■ <b>항상</b>은 최종 상태로, 모든 구성 요소가 이제 <b>항상</b> 메시지 보안 모드를 사용하고 있음을 나타냅니다.</li> </ul>
<b>네트워크 중단 후 보안 터널 연결 재인증</b>	<p>Horizon Client가 보안 터널 연결을 사용하여 View 데스크톱과 애플리케이션에 연결하는 경우 네트워크 중단이 발생했을 때 사용자 자격 증명을 재인증해야 하는지 여부를 결정합니다.</p> <p>이 설정은 보안을 강화합니다. 예를 들어, 도난당한 노트북이 다른 네트워크로 이동된 경우 네트워크 연결이 일시적으로 중단되었기 때문에 사용자가 View 데스크톱과 애플리케이션에 자동으로 액세스할 수 없습니다.</p> <p>이 설정은 기본적으로 사용하지 않도록 설정됩니다.</p>
<b>강제로 사용자 연결 끊기</b>	<p>사용자가 View에 로그인한 후 지정된 시간(분)이 경과하면 모든 데스크톱과 애플리케이션의 연결을 끊습니다. 이때 데스크톱과 애플리케이션은 사용자가 언제 열었는지에 관계없이 모두 한꺼번에 연결이 끊어집니다.</p> <p>기본값은 600분입니다.</p>

설정	설명
<b>애플리케이션을 지원하는 클라이언트의 경우</b> <b>사용자가 키보드와 마우스 사용을 중지하면 해당 애플리케이션의 연결을 끊고 SSO 자격 증명 삭제</b>	<p>클라이언트 디바이스에서 키보드나 마우스 활동이 없을 때 애플리케이션 세션을 보호합니다. ...<b>분 후</b>로 설정한 경우 View에서는 지정된 시간(분) 동안 아무런 사용자 작업이 없으면 모든 애플리케이션의 연결을 끊고 SSO 자격 증명을 삭제합니다. 데스크톱 세션의 연결이 끊어집니다. 따라서 사용자는 연결이 끊어진 애플리케이션에 로그인하여 다시 연결하거나, 새로운 데스크톱 또는 애플리케이션을 실행해야 합니다.</p> <p><b>안 함</b>으로 설정하면 View에서는 사용자 작업이 없어도 애플리케이션 연결을 끊거나 SSO 자격 증명을 삭제하지 않습니다.</p> <p>기본값은 <b>안 함</b>입니다.</p>
<b>기타 클라이언트</b> <b>SSO 자격 증명 삭제</b>	<p>특정 시간이 경과한 후 SSO 자격 증명을 삭제합니다. 이 설정은 애플리케이션 원격 작업을 지원하지 않는 클라이언트에 사용됩니다. ...<b>분 후</b>로 설정한 경우 사용자가 클라이언트 디바이스에서 작업 중이더라도 View에 로그인한 후 지정된 시간(분)이 경과하면 다시 로그인하여 데스크톱에 연결해야 합니다.</p> <p>기본값은 <b>15분 후</b>입니다.</p>
<b>보안 서버 연결에 IPSec 사용</b>	<p>IPSec(Internet Protocol Security)를 사용해 보안 서버와 View 연결 서버 인스턴스를 연결할지 결정하십시오. 이 설정은 FIPS 모드에서 보안 서버를 설치하기 전에 사용되도록 설정해서는 안 됩니다. 그렇지 않으면 페어링이 실패합니다.</p> <p>기본적으로 보안 서버 연결용 IPSec가 활성화되어 있습니다.</p>
<b>View Administrator 세션 시간 초과</b>	<p>세션 시간이 초과될 때까지 유효 View Administrator 세션이 지속되는 시간을 결정하십시오.</p> <p><b>중요</b> View Administrator 세션 시간 초과(단위: 분)를 높게 설정하면 View Administrator를 무단으로 사용할 위험이 높아집니다. 따라서 유효 세션이 오랫동안 지속되도록 허용할 경우 주의해야 합니다.</p> <p>기본적으로 View Administrator 세션 시간 초과는 30분입니다. 세션 시간 초과를 1 ~ 4,320 분으로 설정할 수 있습니다.</p>

이러한 설정 및 각 설정이 보안에 미치는 영향에 대한 자세한 내용은 "View 관리" 설명서를 참조하십시오.

**참고** 모든 Horizon Client와 View Administrator를 View에 연결하려면 SSL이 필요합니다. View 배포 시 로드 밸런서나 기타 클라이언트, 중간 서버를 사용할 경우 SSL의 부하를 이러한 서버로 분산시킨 다음 개별 View 연결 서버 인스턴스 및 보안 서버에서 비 SSL 연결을 구성할 수 있습니다. "View 관리" 설명서에서 "SSL 연결 부하를 중간 서버로 분산"을 참조하십시오.

## View Administrator의 보안 관련 서버 설정

보안 관련 서버 설정은 View Administrator의 **View 구성 > 서버**에서 액세스할 수 있습니다.

표 2-2. 보안 관련 서버 설정

설정	설명
<b>시스템에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용</b>	<p>사용자가 PCoIP 디스플레이 프로토콜을 사용하여 View 데스크톱과 애플리케이션에 연결할 때 Horizon Client가 View 연결 서버나 보안 서버 호스트에 추가적인 보안 연결을 생성하는지 여부를 결정합니다.</p> <p>이 설정을 사용하지 않도록 설정하면 View 연결 서버 또는 보안 서버 호스트를 거치지 않고 클라이언트와 View 데스크톱 또는 RDS 호스트 사이에 데스크톱 또는 애플리케이션 세션이 바로 구축됩니다.</p> <p>이 설정은 기본적으로 사용하지 않도록 설정됩니다.</p>
<b>보안 터널을 사용하여 시스템에 연결</b>	<p>사용자가 View 데스크톱이나 애플리케이션에 연결할 때 Horizon Client가 View 연결 서버 또는 보안 서버 호스트에 추가적인 HTTPS 연결을 생성하는지 여부를 결정합니다.</p> <p>이 설정을 사용하지 않도록 설정하면 View 연결 서버 또는 보안 서버 호스트를 거치지 않고 클라이언트와 View 데스크톱 또는 RDS 호스트 사이에 데스크톱 또는 애플리케이션 세션이 바로 구축됩니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
<b>시스템에 Blast 연결용 Blast 보안 게이트웨이 사용</b>	<p>웹 브라우저 또는 Blast Extreme 디스플레이 프로토콜을 사용하여 데스크톱에 액세스하는 클라이언트에서 Blast 보안 게이트웨이를 사용하여 View 연결 서버에 대한 보안 터널을 설정하는지 여부를 결정합니다.</p> <p>사용하도록 설정되지 않은 경우, Blast Extreme 세션과 웹 브라우저를 사용하는 클라이언트는 View 연결 서버를 우회하여 View 데스크톱에 직접 연결합니다.</p> <p>이 설정은 기본적으로 사용하지 않도록 설정됩니다.</p>

이러한 설정 및 각 설정이 보안에 미치는 영향에 대한 자세한 내용은 “View 관리” 설명서를 참조하십시오.

## View LDAP의 보안 관련 설정

보안 관련 설정은 View LDAP의 개체 경로

cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int에 있습니다. ADSI Edit 유틸리티를 사용하여 View 연결 서버 인스턴스에서 이 설정의 값을 변경할 수 있습니다. 변경 사항은 그룹 내의 모든 다른 View 연결 서버 인스턴스에 자동으로 전파됩니다.

표 2-3. View LDAP의 보안 관련 설정

이름-값 쌍	설명
<b>cs-allowunencryptedstartsession</b>	<p>특성은 <code>pae-NameValuePair</code>입니다.</p> <p>이 특성은 원격 사용자 세션을 시작할 때 View 연결 서버 인스턴스와 데스크톱 사이에 보안 채널이 필요한지 여부를 제어합니다.</p> <p>데스크톱 컴퓨터에 View Agent 5.1 이상이나 Horizon Agent 7.0 이상이 설치되어 있는 경우, 이 특성은 아무런 영향을 주지 않으며 보안 채널이 항상 필요합니다. 데스크톱 컴퓨터에 View 5.1보다 이전 버전의 View Agent가 설치되어 있는 경우, 데스크톱 컴퓨터가 속해 있는 도메인과 View 연결 서버 인스턴스의 도메인 사이에 양방향 신뢰 관계가 구축되어 있지 않으면 보안 채널을 설정할 수 없습니다. 이 경우에는 보안 채널 없이 원격 사용자 세션을 시작할 수 있는지 여부를 결정하는 데 이 특성이 중요한 역할을 합니다.</p> <p>어떤 경우든 사용자 자격 증명과 인증 티켓은 정적 키로 보호됩니다. 보안 채널은 동적 키를 사용하여 기밀성을 한층 더 강화합니다.</p> <p><b>0</b>으로 설정한 경우 보안 채널을 설정할 수 없으면 원격 사용자 세션이 시작되지 않습니다. 이 설정은 모든 데스크톱이 신뢰할 수 있는 도메인에 속해 있거나 모든 데스크톱에 View Agent 5.1 이상이 설치되어 있는 경우에 적합합니다.</p> <p><b>1</b>로 설정하면 보안 채널을 설정할 수 없어도 원격 사용자 세션을 시작할 수 있습니다. 이 설정은 일부 데스크톱이 신뢰할 수 있는 도메인에 속해 있지 않고 이전 버전의 View Agent가 설치되어 있는 경우에 적합합니다.</p> <p>기본 설정:</p> <p><b>1.</b></p>

## 포트 및 서비스

View 구성 요소가 서로 통신할 수 있도록 특정 UDP 및 TCP 포트가 열려 있어야 합니다. 각 유형의 View Server에서 실행되는 Windows 서비스를 알면 서버에 속하지 않은 서비스를 식별하는 데 도움이 됩니다.

본 장은 다음 항목을 포함합니다.

- View TCP 및 UDP 포트
- View 연결 서버 호스트의 서비스
- 보안 서버의 서비스

### View TCP 및 UDP 포트

View에서는 구성 요소 간 네트워크 액세스에 TCP 및 UDP 포트를 사용합니다.

설치 도중 View가 기본적으로 사용되는 포트를 열도록 Windows 방화벽 규칙을 선택적으로 구성할 수 있습니다. 설치 후에 기본 포트를 변경하려면 업데이트된 포트에 대한 액세스를 허용하도록 Windows 방화벽 규칙을 수동으로 재구성해야 합니다. "View 설치" 문서의 "View 서비스의 기본 포트 교체"를 참조하십시오.

표 3-1. View에서 사용되는 TCP 및 UDP 포트

소스	포트	대상	포트	프로토콜	설명
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	55000	Horizon Agent	4172	UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	4172	Horizon Client	*	UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다. <b>참고</b> 대상 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
보안 서버	500	View 연결 서버	500	UDP	IPsec 협상 트래픽입니다.
보안 서버	*	View 연결 서버	4001	TCP	JMS 트래픽입니다.
보안 서버	*	View 연결 서버	4002	TCP	JMS SSL 트래픽입니다.
보안 서버	*	View 연결 서버	8009	TCP	IPsec을 사용하지 않을 경우 AJP13으로 전달된 웹 트래픽입니다.

소스	포트	대상	포트	프로토콜	설명
보안 서버	*	View 연결 서버	*	ESP	NAT 없이 IPsec을 사용할 경우 AJP13으로 전달된 웹 트래픽입니다.
보안 서버	4500	View 연결 서버	4500	UDP	NAT 디바이스를 통해 IPsec를 사용할 경우 AJP13으로 전달된 웹 트래픽입니다.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	*	Horizon Agent	3389	TCP	터널 연결을 사용할 경우 Microsoft RDP에서 View 데스크톱으로 가는 트래픽입니다.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	*	Horizon Agent	9427	TCP	터널 연결을 사용할 경우 Windows Media MMR 리디렉션 및 클라이언트 드라이브 리디렉션입니다.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	*	Horizon Agent	32111	TCP	터널 연결을 사용할 경우 USB 리디렉션 및 시간대 동기화입니다.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	*	Horizon Agent	4172	TCP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP입니다.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	*	Horizon Agent	22443	TCP	Blast 보안 게이트웨이를 사용할 경우 VMware Blast Extreme입니다.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	*	Horizon Agent	22443	TCP	Blast 보안 게이트웨이를 사용할 경우 HTML Access입니다.
Horizon Agent	4172	Horizon Client	*	UDP	PCoIP 보안 게이트웨이를 사용하지 않을 경우 PCoIP입니다. <b>참고</b> 대상 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
Horizon Agent	4172	View 연결 서버, 보안 서버 또는 Unified Access Gateway 장치	55000	UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다.
Horizon Agent	4172	Unified Access Gateway 장치	*	UDP	PCoIP입니다. View 데스크톱 및 애플리케이션이 UDP 포트 4172에서 Unified Access Gateway 장치로 PCoIP 데이터를 다시 보냅니다. 대상 UDP 포트가 수신된 UDP 패킷의 소스 포트여서 이것이 응답 데이터일 때는 보통 이에 대한 명시적 방화벽 규칙을 추가할 필요가 없습니다.

소스	포트	대상	포트	프로토콜	설명
Horizon Client	*	View 연결 서버 또는 보안 서버 또는 Unified Access Gateway 장치	80	TCP	기본적으로 SSL(HTTPS 액세스)은 클라이언트 연결에 사용하도록 설정되어 있지만 특정한 경우에는 포트 80(HTTP 액세스)을 사용할 수 있습니다. <a href="#">View에서의 HTTP 리디렉션</a> 을 참조하십시오.
Horizon Client	*	View 연결 서버, 보안 서버 또는 Unified Access Gateway 장치	443	TCP	View 로그인에 사용되는 HTTPS입니다. (터널 연결을 사용하는 경우 이 포트는 터널링에도 사용됩니다.)
Horizon Client	*	View 연결 서버 또는 보안 서버 또는 Unified Access Gateway 장치	4172	TCP 및 UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP입니다.
Horizon Client	*	Horizon Agent	3389	TCP	터널 연결 대신 직접 연결을 사용할 경우 View 테스트 톱에 대한 Microsoft RDP 트래픽입니다.
Horizon Client	*	Horizon Agent	9427	TCP	터널 연결 대신 직접 연결이 사용될 경우 Windows Media MMR 리디렉션과 클라이언트 드라이브 리디렉션입니다.
Horizon Client	*	Horizon Agent	32111	TCP	터널 연결 대신 직접 연결을 사용할 경우 USB 리디렉션 및 시간대 동기화입니다.
Horizon Client	*	Horizon Agent	4172	TCP 및 UDP	PCoIP 보안 게이트웨이가 사용되지 않을 경우 PCoIP입니다.  <b>참고</b> 소스 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
Horizon Client	*	Horizon Agent	22443	TCP 및 UDP	VMware Blast
Horizon Client	*	View 연결 서버, 보안 서버 또는 Unified Access Gateway 장치	4172	TCP 및 UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다.  <b>참고</b> 소스 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
웹 브라우저	*	보안 서버 또는 Unified Access Gateway 장치	8443	TCP	HTML Access입니다.
View 연결 서버	*	View 연결 서버	48080	TCP	View 연결 서버 구성 요소 간의 내부 통신용입니다.
View 연결 서버	*	vCenter Server 또는 View Composer	80	TCP	vCenter Server 또는 View Composer 액세스를 위해 SSL을 사용하지 않도록 설정된 경우 SOAP 메시지입니다.
View 연결 서버	*	vCenter Server	443	TCP	vCenter Server에 액세스할 때 SSL을 사용하도록 설정된 경우의 SOAP 메시지입니다.



소스	포트	대상	포트	프로토콜	설명
View 연결 서버	*	View Composer	18443	TCP	View Composer에 액세스할 때 SSL을 사용하도록 설정된 경우의 SOAP 메시지입니다.
View 연결 서버	*	View 연결 서버	4100	TCP	JMS inter-router 트래픽입니다.
View 연결 서버	*	View 연결 서버	4101	TCP	JMS SSL inter-router 트래픽입니다.
View 연결 서버	*	View 연결 서버	8472	TCP	Cloud Pod 아키텍처의 팟 간 통신용입니다.
View 연결 서버	*	View 연결 서버	22389	TCP	Cloud Pod 아키텍처의 전역 LDAP 복제용입니다.
View 연결 서버	*	View 연결 서버	22636	TCP	Cloud Pod 아키텍처의 보안 전역 LDAP 복제용입니다.
Unified Access Gateway 장치	*	View 연결 서버 또는 로드 밸런서	443	TCP	HTTP 액세스. Unified Access Gateway 장치가 TCP 포트 443에서 연결하여 View 연결 서버 인스턴스나 여러 View 연결 서버 인스턴스 앞의 로드 밸런서와 통신합니다.
View Composer 서비스	*	ESXi 호스트	902	TCP	View Composer에서 View Composer 내부 디스크 그리고, 지정된 경우, 영구 디스크와 시스템 임시 디스크를 포함하여 연결된 클론 디스크를 사용자 지정할 때 사용됩니다.

**참고** 클라이언트가 PCoIP에 사용하는 UDP 포트 번호는 변경될 수 있습니다. 포트 50002가 사용 중이면 클라이언트가 50003을 고르고, 포트 50003이 사용 중이면 50004를 고르는 방식입니다. 포에 별표(\*)가 나열된 경우 ANY 값으로 방화벽을 구성해야 합니다.

**참고** Microsoft Windows Server에서는 Horizon 7 환경의 모든 연결 서버 간에 동적 포트 범위가 열려 있어야 합니다. 이러한 포트는 Microsoft Windows에서 RPC(원격 프로시저 호출) 및 Active Directory 복제의 정상적인 작업을 위해 필요합니다. 동적 포트 범위에 대한 자세한 내용은 Microsoft Windows Server 설명서를 참조하십시오.

## View에서의 HTTP 리디렉션

HTTP를 통해 연결을 시도하면 View Administrator에 대한 연결 시도를 제외하고 자동으로 HTTPS로 리디렉션됩니다. 최신 Horizon Client는 HTTPS를 기본으로 사용하므로 HTTP 리디렉션이 필요하지 않지만 Horizon Client 다운로드 등 사용자가 웹 브라우저에 연결할 경우에는 HTTP 리디렉션이 유용합니다.

HTTP 리디렉션의 문제는 비보안 프로토콜이라는 점입니다. 사용자가 주소 표시줄에 **https://**를 입력하는 습관을 들이지 않은 경우 예상한 페이지가 올바르게 표시되더라도 공격자가 웹 브라우저를 손상하거나, 맬웨어를 설치하거나, 자격 증명을 훔칠 수 있습니다.

**참고** 외부 연결을 위한 HTTP 리디렉션은 TCP 포트 80에 대한 인바운드 트래픽을 허용하도록 외부 방화벽을 구성한 경우에만 발생할 수 있습니다.

HTTP를 통해 View Administrator에 연결하려는 시도는 리디렉션되지 않습니다. 그 대신 HTTPS를 사용해야 함을 알리는 오류 메시지가 표시됩니다.

시도하는 모든 HTTP 연결이 리디렉션되지 않도록 하려면 “View 설치” 설명서에서 “연결 서버에 대한 클라이언트 연결에 HTTP 리디렉션 사용 안 함”을 참조하십시오.

SSL 클라이언트 연결 부하를 중간 디바이스에 분산한 경우 View 연결 서버 인스턴스 또는 보안 서버의 포트 80에 연결할 수도 있습니다. “View 관리” 설명서에서 “SSL 연결 부하를 중간 서버로 분산”을 참조하십시오.

SSL 포트 번호를 변경한 경우에 HTTP 리디렉션을 허용하려면 “View 설치” 설명서에서 “연결 서버에 대한 HTTP 리디렉션 포트 번호 변경”을 참조하십시오.

## View 연결 서버 호스트의 서비스

View의 작업은 View 연결 서버 호스트에서 실행할 여러 서비스에 따라 달라집니다.

표 3-2. View 연결 서버 호스트 서비스

서비스 이름	시작 유형	설명
VMware Horizon View Blast 보안 게이트웨이	자동	보안 HTML Access 및 Blast Extreme 서비스를 제공합니다. 이 서비스는 클라이언트가 Blast Secure Gateway를 통해 View 연결 서버에 연결할 경우 실행 중이어야 합니다.
VMware Horizon View 연결 서버	자동	연결 브로커 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다. 이 서비스를 시작 또는 중지할 경우 Framework, Message Bus, Security Gateway 및 Web 서비스 또한 시작 또는 중지합니다. 이 서비스는 VMwareVDMDS 또는 VMware Horizon View Script Host 서비스를 시작 또는 중지하지 않습니다.
VMware Horizon View Framework 구성 요소	수동	이벤트 로깅, 보안 및 COM+ 프레임워크 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMware Horizon View Message Bus 구성 요소	수동	View 구성 요소 간 메시징 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMware Horizon View PCoIP 보안 게이트웨이	수동	PCoIP Secure Gateway 서비스를 제공합니다. 이 서비스는 클라이언트가 PCoIP Secure Gateway를 통해 View 연결 서버에 연결할 경우 실행 중이어야 합니다.
VMware Horizon View Script Host	사용 안 함	가상 시스템을 삭제할 때 실행된 타사 스크립트의 지원을 제공합니다. 이 서비스가 기본적으로 사용되지 않도록 설정됩니다. 스크립트를 실행할 경우 이 서비스를 사용하도록 설정해야 합니다.
VMware Horizon View Security Gateway 구성 요소	수동	공용 게이트웨이 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMware Horizon View 웹 구성 요소	수동	웹 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMwareVDMDS	자동	LDAP 디렉터리 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다. View를 업그레이드하는 동안 이 서비스는 기존 데이터가 올바르게 마이그레이션되도록 합니다.

## 보안 서버의 서비스

View의 작업은 보안 서버에서 실행되는 몇 가지 서비스에 따라 달라집니다.

표 3-3. 보안 서버 서비스

서비스 이름	시작 유형	설명
VMware Horizon View Blast 보안 게이트웨이	자동	보안 HTML Access 및 Blast Extreme 서비스를 제공합니다. 클라이언트가 Blast 보안 게이트웨이를 통해 이 보안 서버에 연결하는 경우에는 이 서비스가 반드시 실행되어야 합니다.
VMware Horizon View 보안 서버	자동	보안 서버 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다. 이 서비스를 시작 또는 중지할 경우 Framework 및 Security Gateway 서비스 또한 시작 또는 중지합니다.
VMware Horizon View Framework 구성 요소	수동	이벤트 로깅, 보안 및 COM+ 프레임워크 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMware Horizon View PCoIP 보안 게이트웨이	수동	PCoIP Secure Gateway 서비스를 제공합니다. 클라이언트가 PCoIP 보안 게이트웨이를 통해 이 보안 서버에 연결하는 경우에는 이 서비스가 반드시 실행되어야 합니다.
VMware Horizon View Security Gateway 구성 요소	수동	공용 게이트웨이 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.

# View 연결 서버 인스턴스 또는 보안 서버의 보안 프로토콜 및 암호 제품군 구성

## 4

View 연결 서버에서 허용하는 보안 프로토콜 및 암호 제품군을 구성할 수 있습니다. 복제된 그룹의 모든 View 연결 서버 인스턴스에 적용되는 전역 수락 정책을 정의하거나, 개별 View 연결 서버 인스턴스 및 보안 서버의 수락 정책을 정의할 수 있습니다.

View 연결 서버 인스턴스가 vCenter Server와 View Composer에 연결할 시점을 제안하도록 보안 프로토콜 및 암호 제품군을 구성할 수도 있습니다. 복제된 그룹의 모든 View 연결 서버에 적용되는 전역 제안 정책을 정의할 수 있습니다. 개별 인스턴스를 정의해 전역 제안 정책을 취소할 수 없습니다.

---

**참고** View 연결 서버의 보안 설정은 BSG(Blast 보안 게이트웨이)에 적용되지 않습니다. BSG의 보안을 별도로 구성해야 합니다. [장 5 Blast 보안 게이트웨이의 보안 프로토콜 및 암호 제품군 구성](#)의 내용을 참조하십시오.

---

Oracle의 무제한 강도 관할 정책(Unlimited Strength Jurisdiction Policy) 파일이 표준으로 포함되어므로 기본적으로 256비트 키가 허용됩니다.

본 장은 다음 항목을 포함합니다.

- [보안 프로토콜과 암호 제품군의 기본 전역 정책](#)
- [전역 수락 및 제안 정책 구성](#)
- [개별 View Server의 수락 정책 구성](#)
- [View 데스크톱에서 제안 정책 구성](#)
- [이전 프로토콜 및 암호가 View에서 사용되지 않도록 설정됨](#)

## 보안 프로토콜과 암호 제품군의 기본 전역 정책

전역 수락 및 제안 정책은 기본적으로 특정 보안 프로토콜과 암호 제품군을 사용하도록 설정합니다.

표 4-1. 기본 전역 정책

기본 보안 프로토콜	기본 암호 제품군
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
■ TLS 1.0	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	■ TLS_RSA_WITH_AES_128_CBC_SHA
	■ TLS_RSA_WITH_AES_256_CBC_SHA

모든 연결 클라이언트가 TLS 1.1 및/또는 TLS 1.2를 지원하는 경우 수락 정책에서 TLS 1.0을 삭제해도 됩니다.

## 전역 수락 및 제안 정책 구성

전역 수락 및 제안 정책은 View LDAP 특성에 정의됩니다. 이러한 정책은 복제된 그룹의 모든 View 연결 서버 인스턴스 및 보안 서버에 적용됩니다. 전역 정책을 변경하려면 View 연결 서버 인스턴스에서 View LDAP를 편집하십시오.

각 정책은 다음 View LDAP 위치에서 단일값 특성입니다.

cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int

## View LDAP에 정의된 전역 수락 및 제안 정책

전역 수락 및 제안 정책을 정의하는 View LDAP 특성을 편집할 수 있습니다.

### 전역 수락 정책

다음 특성은 보안 프로토콜을 열거합니다. 최신 프로토콜이 제일 앞에 오도록 목록을 정렬해야 합니다.

```
pae-ServerSSLSecureProtocols = WL IST:TLSv1.2,TLSv1.1,TLSv1
```

다음 특성은 암호 제품군을 열거합니다. 이 예는 축약된 목록을 보여 줍니다.

```
pae-ServerSSLCipherSuites = WL IST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

다음 특성은 암호 제품군의 우선 순위를 제어합니다. 일반적으로 서버에서 지정하는 암호 제품군 순서는 중요하지 않으며 클라이언트에서 지정하는 순서가 사용됩니다. 서버에서 지정하는 암호 제품군 순서를 사용하려면 다음 특성을 설정합니다.

```
pae-ServerSSLHonorClientOrder = 0
```

## 전역 제안 정책

다음 특성은 보안 프로토콜을 열거합니다. 최신 프로토콜이 제일 앞에 오도록 목록을 정렬해야 합니다.

```
pae-ClientSSLSecureProtocols = WLIST:TLSv1.2,TLSv1.1,TLSv1
```

다음 특성은 암호 제품군을 열거합니다. 이 목록은 선호도 순으로 정렬해야 합니다. 가장 선호하는 암호 제품군을 제일 앞에 놓고 두 번째로 선호하는 제품군은 그 다음에 놓는 등 선호도 순으로 정렬하십시오. 이 예는 축약된 목록을 보여 줍니다.

```
pae-ClientSSLCipherSuites = WLIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

## 전역 수락 및 제안 정책 변경

보안 프로토콜 및 암호 제품군의 전역 수락 및 제안 정책을 변경하려면 ADSI 편집 유틸리티를 사용해 View LDAP 특성을 편집합니다.

### 사전 요구 사항

- 수락 및 제안 정책을 정의하는 View LDAP 특성을 숙지하십시오. [View LDAP에 정의된 전역 수락 및 제안 정책](#)의 내용을 참조하십시오.
- 사용하고 있는 Windows Server 운영 체제 버전에서 ADSI 편집 유틸리티를 사용하는 방법은 Microsoft TechNet 웹 사이트를 참조하십시오.

### 절차

- 1 View 연결 서버 컴퓨터에서 ADSI 편집 유틸리티를 시작합니다.
- 2 콘솔 트리에서 **연결**을 선택합니다.
- 3 **고유 이름 또는 명명 컨텍스트를 선택하거나 입력합니다** 텍스트 상자에 고유 이름 DC=vdi, DC=vmware, DC=int를 입력합니다.
- 4 **도메인 또는 서버를 선택하거나 입력합니다** 텍스트 상자에서 **localhost:389** 또는 View 연결 서버 컴퓨터의 정규화된 도메인 이름(FQDN)과 포트 389를 차례로 선택하거나 입력합니다.  
예: localhost:389 또는 mycomputer.mydomain.com:389
- 5 ADSI 편집 트리를 확장하고 **OU=Properties**를 확장한 다음 오른쪽 창에서 **OU=Global**과 **OU=Common**을 차례로 선택합니다.
- 6 **CN=Common, OU=Global, OU=Properties** 개체에서 변경할 각 특성을 선택하고 새 보안 프로토콜 또는 암호 제품군 목록을 입력합니다.
- 7 pae-ServerSSLSecureProtocols를 수정한 경우에는 각 연결 서버 인스턴스와 보안 서버에서 Windows 서비스 VMware Horizon View 보안 게이트웨이 구성 요소를 다시 시작합니다.  
pae-ClientSSLSecureProtocols를 수정한 후에는 서비스를 다시 시작할 필요가 없습니다.

## 개별 View Server의 수락 정책 구성

개별 View 연결 서버 인스턴스 또는 보안 서버의 로컬 수락 정책을 지정하려면 `locked.properties` 파일에 속성을 추가해야 합니다. View server에 `locked.properties` 파일이 없으면 만들어야 합니다.

구성할 각 보안 프로토콜에 대해 `secureProtocols.n` 항목을 추가합니다. `secureProtocols.n=security protocol` 구문을 사용합니다.

구성할 각 암호 제품군에 대해 `enabledCipherSuite.n` 항목을 추가합니다. `enabledCipherSuite.n=cipher suite` 구문을 사용합니다.

변수  $n$ 은 각 항목 유형에 순차적으로(1, 2, 3) 추가하는 정수입니다.

암호 제품군의 우선 순위를 제어하는 `honorClientOrder` 항목을 추가합니다. 일반적으로 서버에서 지정하는 암호 제품군 순서는 중요하지 않으며 클라이언트에서 지정하는 순서가 사용됩니다. 서버에서 지정하는 암호 제품군 순서를 사용하려면 다음 구문을 사용합니다.

```
honorClientOrder=false
```

`locked.properties` 파일의 항목에서 구문이 올바르고 암호 제품군 및 보안 프로토콜 이름의 철자가 올바른지 확인합니다. 파일에 오류가 있을 경우 클라이언트와 서버 간의 협상이 실패할 수 있습니다.

### 절차

- 1 View 연결 서버 또는 보안 서버 컴퓨터의 SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집하십시오.  
예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\`
- 2 연결된 보안 프로토콜과 암호 제품군을 포함한 `secureProtocols.n` 및 `enabledCipherSuite.n` 항목을 추가합니다.
- 3 `locked.properties` 파일을 저장합니다.
- 4 변경 사항을 적용하려면 VMware Horizon View 연결 서버 서비스 또는 VMware Horizon View 보안 서버 서비스를 다시 시작합니다.

## 예제: 개별 서버의 기본 수락 정책

다음 예는 `locked.properties` 파일에서 기본 정책을 지정하는 데 필요한 항목을 보여 줍니다.

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2
secureProtocols.2=TLSv1.1
secureProtocols.3=TLSv1

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
```

```

enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA

# Use the ordering of cipher suites given above:

honorClientOrder=false

```

## View 데스크톱에서 제안 정책 구성

Windows를 실행하는 View 데스크톱에서 제안 정책을 구성함으로써 View 연결 서버에 대한 Message Bus 연결의 보안을 관리할 수 있습니다.

View 연결 서버가 연결 실패 방지를 위해 동일 정책을 수용하도록 구성되어 있는지 확인하십시오.

### 절차

- 1 View 데스크톱에서 Windows 레지스트리 편집기를 시작합니다.
- 2 HKEY\_LOCAL\_MACHINE\Software\VMware, Inc.\VMware VDMWAgentWConfiguration 레지스트리 키로 이동합니다.
- 3 새 문자열(REG\_SZ) 값인 ClientSSLSecureProtocols를 추가합니다.
- 4 **\LIST:protocol\_1,protocol\_2,...** 형식으로 암호 제품군 목록에 대한 값을 설정합니다.

최신 프로토콜 순으로 프로토콜을 나열합니다. 예:

```
WL IST:TLSv1.2,TLSv1.1,TLSv1
```

- 5 새 문자열(REG\_SZ) 값인 ClientSSLCipherSuites를 추가합니다.
- 6 **\LIST:cipher\_suite\_1,cipher\_suite\_2,...** 형식으로 암호 제품군 목록에 대한 값을 설정합니다.

이 목록은 가장 선호하는 암호 제품군부터 선호도 순으로 정렬해야 합니다. 예:

```
WL IST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

## 이전 프로토콜 및 암호가 View에서 사용되지 않도록 설정됨

더 이상 안전하지 않은 것으로 간주되는 일부 이전 프로토콜 및 암호는 기본적으로 View에서 사용되지 않도록 설정되어 있습니다. 필요할 경우 수동으로 사용하도록 설정할 수 있습니다.

### DHE 암호 제품군

자세한 내용은 <http://kb.vmware.com/kb/2121183>의 내용을 참조하십시오. DSA 인증서와 호환되는 암호 제품군은 Diffie-Hellman 사용 후 삭제 키를 사용하며 Horizon 6 버전 6.2부터는 기본적으로 더 이상 사용되지 않도록 설정되어 있습니다.



연결 서버 인스턴스, 보안 서버 및 View 데스크톱의 경우 본 가이드의 설명에 따라 View LDAP 데이터베이스, `locked.properties` 파일 또는 레지스트리를 편집함으로써 이러한 암호 제품군을 사용하도록 설정할 수 있습니다. [전역 수락 및 제안 정책 변경](#), [개별 View Server의 수락 정책 구성](#) 및 [View 데스크톱에서 제안 정책 구성](#)의 내용을 참조하십시오. 다음 제품군 중 하나 이상을 포함하는 암호 제품군 목록을 아래의 순서대로 정의할 수 있습니다.

- TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256(TLS 1.2만 해당, FIPS 제외)
- TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384(TLS 1.2만 해당, FIPS 제외)
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256(TLS 1.2만 해당)
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256(TLS 1.2만 해당)
- TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA

View Composer 및 VADC(View Agent Direct-Connection) 시스템의 경우 “View 설치” 문서의 “View Composer 및 Horizon Agent 시스템용 SSL/TLS에서 취약한 암호 사용 안 함” 절차를 따를 때 암호 목록에 다음을 추가하면 DHE 암호 제품군을 사용하도록 설정할 수 있습니다.

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

**참고** ECDSA 인증서에 대한 지원을 사용하도록 설정할 수 없습니다. 이러한 인증서는 지원된 적이 없습니다.

## SSLv3

Horizon 7에서 SSL 버전 3.0이 제거되었습니다.

자세한 내용은 <http://tools.ietf.org/html/rfc7568>의 내용을 참조하십시오.

## RC4

자세한 내용은 <http://tools.ietf.org/html/rfc7465>의 내용을 참조하십시오.

연결 서버 인스턴스, 보안 서버 및 View 데스크톱의 경우 `C:\Program Files\VMware\VMware View\WServer\jre\lib\security\java.security` 구성 파일을 편집하여 연결 서버, 보안 서버 또는 Horizon Agent 시스템에서 RC4를 사용하도록 설정할 수 있습니다. 파일 끝에는 `jdk.tls.legacyAlgorithms`라는 다중 행 항목이 있습니다. RC4\_128 및 그 뒤의 쉼표를 이 항목에서 제거하고 경우에 따라 연결 서버, 보안 서버 또는 Horizon Agent 시스템을 재시작합니다.

View Composer 및 VADC(View Agent Direct-Connection) 시스템의 경우 “View 설치” 문서의 “View Composer 및 Horizon Agent 시스템용 SSL/TLS에서 취약한 암호 사용 안 함” 절차를 따를 때 암호 목록에 다음을 추가하면 RC4를 사용하도록 설정할 수 있습니다.

```
TLS_RSA_WITH_RC4_128_SHA
```

## TLS 1.0

Horizon 7에서 TLS 1.0은 기본적으로 사용하지 않도록 설정됩니다.

자세한 내용은 [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-1.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf) 및 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>를 참조하십시오. TLS 1.0을 사용하도록 설정하는 방법에 대한 지침은 "View 업그레이드" 문서에 있는 "연결 서버의 vCenter 연결에서 TLSv1 사용" 및 "View Composer에서 vCenter의 TLSv1 및 ESXi 연결 사용" 섹션을 참조하십시오.

# Blast 보안 게이트웨이의 보안 프로토콜 및 암호 제품군 구성

## 5

View 연결 서버의 보안 설정은 BSG(Blast 보안 게이트웨이)에 적용되지 않습니다. BSG의 보안을 별도로 구성해야 합니다.

본 장은 다음 항목을 포함합니다.

- BSG(Blast 보안 게이트웨이)의 보안 프로토콜 및 암호 제품군 구성

## BSG(Blast 보안 게이트웨이)의 보안 프로토콜 및 암호 제품군 구성

`absg.properties` 파일을 편집하면 BSG의 클라이언트 측 수신기에서 수락되는 보안 프로토콜 및 암호 제품군을 구성할 수 있습니다.

허용되는 프로토콜은 낮은 것에서 높은 것 순으로 TLS1.0, TLS1.1 및 TLS1.2입니다. SSLv3 이하와 같이 오래된 프로토콜은 허용되지 않습니다. 두 개의 속성 `localHttpsProtocolLow` 및 `localHttpsProtocolHigh`는 BSG 수신기에서 수락하는 프로토콜의 범위를 결정합니다. 예를 들어 `localHttpsProtocolLow=tls1.0` 및 `localHttpsProtocolHigh=tls1.2`를 설정하면 수신기에서 TLS1.0, TLS1.1 및 TLS1.2를 수락합니다. 기본 설정은 `localHttpsProtocolLow=tls1.1` 및 `localHttpsProtocolHigh=tls1.2`입니다. BSG의 `absg.log` 파일을 검사하면 특정 BSG 인스턴스에 대해 적용되는 값을 확인할 수 있습니다.

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>의 CIPHER LIST FORMAT 섹션 아래에 정의된 형식을 사용하여 암호 목록을 지정해야 합니다. 다음과 같은 암호 목록이 기본값입니다.

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

### 절차

- 1 연결 서버 인스턴스에서 `install_directory\VMware\VMware View\Server\Wappblastgateway\Wabsg.properties` 파일을 편집합니다.

기본적으로 설치 디렉토리는 `%ProgramFiles%`입니다.

- 2    프로토콜 범위를 지정하려면 속성 `localHttpsProtocolLow` 및 `localHttpsProtocolHigh`를 편집합니다.

예를 들면 다음과 같습니다.

```
localHttpsProtocolLow=tls1.0  
localHttpsProtocolHigh=tls1.2
```

프로토콜을 하나만 사용하도록 설정하려면 `localHttpsProtocolLow` 및 `localHttpsProtocolHigh` 모두에 같은 프로토콜을 지정합니다.

- 3    암호 제품군 목록을 지정하려면 `localHttpsCipherSpec` 속성을 편집합니다.

예를 들면 다음과 같습니다.

```
localHttpsCipherSpec=ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!  
aNULL:!eNULL
```

- 4    Windows 서비스 VMware HorizonView Blast 보안 게이트웨이를 다시 시작합니다.

# 보안 Horizon 7 환경에 USB 디바이스 배포

## 6

USB 디바이스는 BadUSB라고 하는 보안 위협에 취약할 수 있습니다. 이 보안 위협에서는 일부 USB 디바이스의 펌웨어가 빼앗겨 악성 소프트웨어로 교체될 수 있습니다. 예를 들어 디바이스가 네트워크 트래픽을 리디렉션하거나 키보드를 에뮬레이션하고 키 입력을 캡처하게 만들 수 있습니다. 이 보안 취약점에 대해 Horizon 7 배포를 보호하도록 USB 리디렉션 기능을 구성할 수 있습니다.

USB 리디렉션을 사용하지 않도록 설정하여 USB 디바이스가 사용자의 Horizon 7 데스크톱 및 애플리케이션으로 리디렉션되는 것을 방지할 수 있습니다. 또는 특정 USB 디바이스의 리디렉션을 사용하지 않도록 설정하여 사용자가 데스크톱 및 애플리케이션의 특정 디바이스에 대한 액세스 권한만 갖도록 허용할 수 있습니다.

이러한 단계의 수행 여부는 조직의 보안 요구 사항에 따라 결정됩니다. 이러한 단계는 필수가 아닙니다. USB 리디렉션을 설치하고 Horizon 7 배포의 모든 USB 디바이스에 대해 기능을 사용하도록 설정한 상태로 유지할 수 있습니다. 최소한 조직이 이 보안 취약점에 대한 노출을 제한해야 하는 범위를 심각하게 고려합니다.

본 장은 다음 항목을 포함합니다.

- 모든 유형의 디바이스에 대한 USB 리디렉션 사용 안 함
- 특정 디바이스에 대해 USB 리디렉션을 사용하지 않도록 설정

## 모든 유형의 디바이스에 대한 USB 리디렉션 사용 안 함

일부 보안 수준이 높은 환경에서는 사용자가 클라이언트 디바이스에 연결했을 수 있는 모든 USB 디바이스를 원격 데스크톱 및 애플리케이션으로 리디렉션할 수 없습니다. 모든 데스크톱 풀, 특정 데스크톱 풀 또는 데스크톱 풀 내의 특정 사용자에 대해 USB 리디렉션 기능을 사용하지 않도록 설정할 수 있습니다.

각자의 상황에 맞게 다음의 전략 중에 선택하여 사용하십시오.

- Horizon Agent를 데스크톱 이미지 또는 RDS 호스트에 설치할 때 **USB 리디렉션** 설정 옵션의 선택을 취소합니다. (이 옵션은 기본적으로 선택 취소되어 있습니다.) 이 접근 방식은 데스크톱 이미지 또는 RDS 호스트에서 배포된 모든 원격 데스크톱 및 애플리케이션의 USB 디바이스에 대한 액세스를 방지합니다.
- Horizon Administrator에서 특정 풀에 대한 액세스를 거부하거나 허용하도록 **USB 액세스** 정책을 편집합니다. 이 접근 방식을 사용하면 데스크톱 이미지를 변경할 필요가 없으며 특정 데스크톱 및 애플리케이션 풀의 USB 디바이스에 대한 액세스를 제어할 수 있습니다.

RDS 데스크톱 및 애플리케이션 풀에 대해 전역 **USB 액세스** 정책만 사용할 수 있습니다. 개별 RDS 데스크톱 또는 애플리케이션 풀에 대해서는 이 정책을 설정할 수 없습니다.

- View Administrator에서 데스크톱 또는 애플리케이션 풀 수준에서 정책을 설정한 후 **사용자 재정의**의 설정을 선택하고 사용자를 선택하여 풀의 특정 사용자에게 대한 정책을 재정의할 수 있습니다.
- Horizon Agent 측 또는 클라이언트 측 중 상황에 맞게 Exclude All Devices 정책을 **true**로 설정합니다.
- 스마트 정책을 사용하여 **USB 리디렉션** Horizon 정책 설정을 사용하지 않도록 설정하는 정책을 만듭니다. 이 접근 방식을 사용하면 특정 조건이 충족된 경우에 특정 원격 데스크톱에서 USB 리디렉션을 사용하지 않도록 설정할 수 있습니다. 예를 들어, 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결하면 USB 리디렉션을 사용하지 않도록 설정하는 정책을 구성할 수 있습니다.

Exclude All Devices 정책을 **true**로 설정하면 Horizon Client는 모든 USB 디바이스가 리디렉션되지 않도록 차단합니다. 기타 정책 설정을 사용하여 특정 디바이스 또는 디바이스 제품군을 리디렉션할 수 있습니다. 정책을 **false**로 설정하면 Horizon Client는 다른 정책 설정에 의해 차단된 USB 디바이스를 제외한 모든 USB 디바이스의 리디렉션을 허용합니다. Horizon Agent와 Horizon Client 모두에 정책을 설정할 수 있습니다. 다음 표에서는 Horizon Agent와 Exclude All Devices 모두에 Horizon Client 정책을 설정할 경우 클라이언트 컴퓨터에서 정책이 어떻게 적용되는지를 보여 줍니다. 차단되어 있지만 않으면 기본적으로 모든 USB 디바이스는 리디렉션할 수 있습니다.

표 6-1. 모든 디바이스 제외 정책 결합 효과

Horizon Agent의 모든 디바이스 제외 정책	Horizon Client의 모든 디바이스 제외 정책	결합된 효율적 모든 디바이스 제외 정책
<b>false</b> 또는 정의되지 않음(모든 USB 디바이스 포함)	<b>false</b> 또는 정의되지 않음(모든 USB 디바이스 포함)	모든 USB 디바이스 포함
<b>false</b> (모든 USB 디바이스 포함)	<b>true</b> (모든 USB 디바이스 제외)	모든 USB 디바이스 제외
<b>true</b> (모든 USB 디바이스 제외)	임의 또는 정의되지 않음	모든 USB 디바이스 제외

Disable Remote Configuration Download 정책을 **true**로 설정한 경우, Horizon Agent의 Exclude All Devices 값이 Horizon Client에 전달되지 않지만 Horizon Agent와 Horizon Client는 Exclude All Devices의 로컬 값을 적용합니다.

이러한 정책은 Horizon Agent 구성 ADMX 템플릿 파일(vdm\_agent.admx)에 포함되어 있습니다. 자세한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성"의 "Horizon Agent 구성 ADMX 템플릿의 USB 설정"을 참조하십시오.

## 특정 디바이스에 대해 USB 리디렉션을 사용하지 않도록 설정

일부 사용자는 원격 데스크톱 또는 애플리케이션에서 작업을 수행할 수 있도록 로컬로 연결된 특정 USB 디바이스를 리디렉션해야 할 수 있습니다. 예를 들어 의사는 Dictaphone USB 디바이스를 사용하여 환자의 의료 정보를 기록해야 할 수 있습니다. 이러한 경우 모든 USB 디바이스에 대한 액세스를 사용하지 않도록 설정할 수 없습니다. 그룹 정책 설정을 사용하여 특정 디바이스에 대한 USB 리디렉션을 사용하거나 사용하지 않도록 설정할 수 있습니다.

특정 디바이스에 대한 USB 리디렉션을 사용하도록 설정하기 전에 엔터프라이즈 내 클라이언트 시스템에 연결된 물리적 디바이스를 신뢰해야 합니다. 공급망을 신뢰할 수 있는지 확인합니다. 가능하면 USB 디바이스에 대한 관리망을 기록합니다.

또한 알 수 없는 소스의 디바이스를 연결하지 않도록 직원을 교육합니다. 가능하면 환경의 디바이스를 서명된 펌웨어 업데이트만 수락하고 FIPS 140-2 Level 3 인증을 획득했으며 다른 종류의 펌웨어 업데이트 가능 펌웨어를 지원하지 않는 디바이스로 제한합니다. 이러한 유형의 USB 디바이스는 소스를 찾기 어려우며 디바이스 요구 사항에 따라 소스를 찾는 것이 불가능할 수 있습니다. 이러한 옵션은 유용하지 않을 수 있지만 고려할만한 가치가 있습니다.

각 USB 디바이스에는 컴퓨터에 대해 식별하는 고유한 벤더 및 제품 ID가 있습니다. Horizon Agent 구성 그룹 정책 설정을 구성하여 알려진 디바이스 유형에 대한 포함 정책을 설정할 수 있습니다. 이러한 접근 방식을 통해 알 수 없는 디바이스가 사용자 환경에 침투하도록 허용하는 위험을 없앨 수 있습니다.

예를 들어 알려진 디바이스 벤더 및 제품 ID, vid/pid=0123/abcd를 제외한 모든 디바이스가 원격 데스크톱 또는 애플리케이션으로 리디렉션되는 것을 방지할 수 있습니다.

```
ExcludeAllDevices    Enabled

IncludeVidPid        o:vid-0123_pid-abcd
```

**참고** 이 구성 예는 보호를 제공하지만 잘못된 디바이스가 vid/pid를 보고할 수 있으므로 여전히 공격이 발생할 수 있습니다.

기본적으로 Horizon 7는 특정 디바이스 제품군이 원격 데스크톱 또는 애플리케이션으로 리디렉션되는 것을 차단합니다. 예를 들어 HID(휴먼 인터페이스 디바이스) 및 키보드는 게스트에 나타나지 않도록 차단됩니다. 일부 릴리스된 BadUSB 코드는 USB 키보드 디바이스를 대상으로 합니다.

특정 디바이스 제품군이 원격 데스크톱 또는 애플리케이션으로 리디렉션되는 것을 방지할 수 있습니다. 예를 들어 모든 비디오, 오디오 및 대용량 스토리지 디바이스를 차단할 수 있습니다.

```
ExcludeDeviceFamily  o:video;audio;storage
```

반대로 모든 디바이스가 리디렉션되는 것을 방지하지만 특정 디바이스 제품군이 사용되는 것을 허용함으로써 화이트리스트를 생성할 수 있습니다. 예를 들어 스토리지 디바이스를 제외한 모든 디바이스를 차단할 수 있습니다.

```
ExcludeAllDevices    Enabled

IncludeDeviceFamily  o:storage
```

원격 사용자가 데스크톱 또는 애플리케이션에 로그인하여 감염시키는 경우 다른 위험이 발생할 수 있습니다. 회사 방화벽 외부에서 비롯되는 모든 Horizon 7 연결에 대한 USB 액세스를 방지할 수 있습니다. USB 디바이스는 외부적으로 사용되지 않고 내부적으로 사용될 수 있습니다.

포트 32111은 시간대 동기화에도 사용되므로 TCP 포트 32111을 차단하여 USB 디바이스에 대한 외부 액세스를 사용 중지하면 시간대 동기화가 작동하지 않습니다. 제로 클라이언트의 경우 USB 트래픽이 UDP 포트 4172를 통해 가상 채널 내에 포함됩니다. 포트 4172가 디스플레이 프로토콜과 USB 리디렉션에 사용되므로 포트 4172를 차단할 수 없습니다. 필요한 경우 제로 클라이언트에서 USB 리디렉션을 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 제로 클라이언트 제품 설명서를 참조하거나 제로 클라이언트 벤더에 문의하십시오.

특정 디바이스 제품군이나 특정 디바이스를 차단하도록 정책을 설정하면 BadUSB 악성 소프트웨어로 감염되는 위험을 줄일 수 있습니다. 이러한 정책은 모든 위험을 줄이지는 않지만 전체 보안 전략의 유효한 부분이 될 수 있습니다.

이러한 정책은 Horizon Agent 구성 ADMX 템플릿 파일(vdm\_agent.admx)에 포함되어 있습니다. 자세한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성"의 내용을 참조하십시오.



# 연결 서버 및 보안 서버의 HTTP 보호 조치

# 7

Horizon 7에서는 HTTP 프로토콜을 이용한 통신을 보호하기 위해 몇 가지 조치를 사용합니다.

본 장은 다음 항목을 포함합니다.

- [Internet Engineering Task Force 표준](#)
- [World Wide Web Consortium 표준](#)
- [다른 보호 조치](#)
- [HTTP 보호 조치 구성](#)

## Internet Engineering Task Force 표준

연결 서버와 보안 서버는 특정 Internet Engineering Task Force(IETF) 표준을 준수합니다.

- 보안 재협상이라고 하는 RFC 5746 Transport Layer Security(TLS) - Renegotiation Indication Extension은 기본적으로 사용하도록 설정됩니다.

---

**참고** 클라이언트 주도 재협상은 연결 서버와 보안 서버에서 기본적으로 사용하지 않도록 설정됩니다. 사용하도록 설정하려면 [HKLM\SOFTWARE\VMware, Inc.\VMware VDM\plugins\Wssnm\WTunnelService\Params]JvmOptions 레지스트리 값을 편집하고 문자열에서 `-Djdk.tls.rejectClientInitiatedRenegotiation=true`를 제거합니다.

---

- 전송 보안이라고도 하는 RFC 6797 HTTP Strict Transport Security(HSTS)는 기본적으로 사용하도록 설정됩니다. 이 설정은 사용하지 않도록 설정할 수 없습니다.
- 반클릭재킹이라고도 하는 RFC 7034 HTTP Header Field X-Frame-Options는 기본적으로 사용하도록 설정됩니다. locked.properties 파일에 x-frame-options=OFF 항목을 추가하면 이 옵션을 사용하지 않도록 설정할 수 있습니다. locked.properties 파일에 속성을 추가하는 방법은 [HTTP 보호 조치 구성](#) 항목을 참조하십시오.

---

**참고** Horizon 7 버전 7.2 이하 릴리스에서는 이 옵션을 변경해도 HTML Access에 대한 연결에 영향을 미치지 않습니다.

---

- 사이트 간 요청 위조를 방지하는 RFC 6454 원본 검사가 기본적으로 사용됩니다. locked.properties에 checkOrigin=false 항목을 추가하면 이 옵션을 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 [크로스 원본 리소스 공유](#)의 내용을 참조하십시오.

---

**참고** 이전 릴리스에서는 기본적으로 이 보호를 사용하지 않도록 설정되었습니다.

---

## World Wide Web Consortium 표준

연결 서버 및 보안 서버는 특정 W3C(World Wide Web Consortium) 표준을 준수합니다.

- 클라이언트 측 크로스 원본 요청을 제한하는 CORS(크로스 원본 리소스 공유)는 기본적으로 사용되도록 설정됩니다. `locked.properties`에 `enableCORS=false` 항목을 추가하면 이 옵션을 사용하지 않도록 설정할 수 있습니다.
- 광범위한 콘텐츠 주입 취약점을 완화하는 CSP(콘텐츠 보안 정책)는 기본적으로 사용되도록 설정됩니다. `locked.properties`에 `enableCSP=false` 항목을 추가하면 이 옵션을 사용하지 않도록 설정할 수 있습니다.

### 크로스 원본 리소스 공유

CORS(크로스 원본 리소스 공유) 기능은 요청 시 클라이언트에 정책 정보를 제공하고 요청이 정책을 준수하는지를 확인하여 클라이언트 측 크로스 원본 요청을 조절합니다. 이 기능은 기본적으로 사용하도록 설정됩니다.

정책에는 수락될 수 있는 HTTP 메서드 집합, 요청을 시작할 수 있는 위치 및 유효한 콘텐츠 유형이 포함됩니다. 이러한 항목은 요청 URL에 따라 다르며 `locked.properties`에 항목을 추가하여 필요에 따라 다시 구성할 수 있습니다.

속성 이름 뒤에 있는 생략 부호는 속성이 목록을 수락할 수 있음을 나타냅니다.

표 7-1. CORS 속성

속성	값 유형	마스터 기본값	기타 기본값
<code>enableCORS</code>	<code>true</code> <code>false</code>	<code>true</code>	<code>n/a</code>
<code>acceptContentType...</code>	<code>http-content-type</code>	<code>application/x-www-form-urlencoded,application/xml,text/xml</code>	<ul style="list-style-type: none"> <li>■ <code>admin=application/x-amf</code></li> <li>■ <code>helpdesk=application/json,application/text,application/x-www-form-urlencoded</code></li> <li>■ <code>view-vlsi-rest=application/json</code></li> </ul>
<code>acceptHeader...</code>	<code>http-header-name</code>	<code>*</code>	<code>n/a</code>
<code>exposeHeader...</code>	<code>http-header-name</code>	<code>*</code>	<code>n/a</code>
<code>filterHeaders</code>	<code>true</code> <code>false</code>	<code>true</code>	<code>n/a</code>
<code>checkOrigin</code>	<code>true</code> <code>false</code>	<code>true</code>	<code>n/a</code>

속성	값 유형	마스터 기본값	기타 기본값
allowCredentials	true false	false	admin=true broker=true helpdesk=true misc=true portal=true saml=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET,HEAD,POST	misc=GET,HEAD saml=GET,HEAD
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension...	chrome-extension-hash	OFF	n/a

Locked.properties 파일의 CORS 속성 예:

```
enableCORS = true
allowPreflight = true
checkOrigin = true
checkOrigin-misc = false
allowMethod.1 = GET
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

## 원본 검사

원본 검사는 기본적으로 사용되도록 설정됩니다. 사용되도록 설정되면 원본이 없거나, 원본이 외부 URL에 지정된 주소, balancedHost 주소, portalHost 주소, chromeExtension 해시 null 또는 localhost 인 경우에만 요청이 수락됩니다. 원본이 이러한 항목 중 하나가 아니면 "예기치 않은 원본" 오류가 로깅되고 상태 404가 반환됩니다.

여러 개의 연결 서버 또는 보안 서버가 로드 밸런싱된 경우 locked.properties에 balancedHost 항목을 추가하여 로드 밸런서 주소를 지정해야 합니다. 이 주소에서는 포트 443이 가정됩니다.

클라이언트를 Unified Access Gateway 또는 다른 게이트웨이를 통해 연결해야 할 경우 locked.properties에 portalHost 항목을 추가하여 모든 게이트웨이 주소를 지정해야 합니다. 이러한 주소에서도 포트 443이 가정됩니다. 외부 URL에 지정된 것과 다른 이름을 사용하여 연결 서버나 보안 서버에 대한 액세스 권한을 제공하려는 경우에도 같은 작업을 수행합니다.

Chrome 확장 클라이언트는 초기 원본을 고유한 ID로 설정합니다. 연결이 성공하려면 locked.properties에 chromeExtension 항목을 추가하여 확장을 등록합니다.

## 컨텐츠 보안 정책

CSP(컨텐츠 보안 정책) 기능은 규격 브라우저에 정책 지시문을 제공하여 XSS(사이트 간 스크립팅) 같은 다양한 클래스의 컨텐츠 주입 취약성을 완화합니다. 이 기능은 기본적으로 사용하도록 설정됩니다. locked.properties에 항목을 추가하여 정책 지시문을 재구성할 수 있습니다.

표 7-2. CSP 속성

속성	값 유형	마스터 기본값	기타 기본값
enableCSP	true false	true	n/a
content-security-policy	directives-list	default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data::style-src 'self' 'unsafe-inline';font-src 'self' data:	portal=child-src 'self' blob::default-src 'self';connect-src 'self' wss::font-src 'self' data::img-src 'self' data: blob::media-src 'self' blob::object-src 'self' blob::script-src 'self' 'unsafe-inline' 'unsafe-eval' data::style-src 'self' 'unsafe-inline';frame-ancestors 'self'
x-frame-options	OFF specification	deny	portal=sameorigin
x-content-type-options	OFF specification	nosniff	n/a
x-xss-protection	OFF specification	1; mode=block	n/a

CSP 속성을 locked.properties 파일에 추가할 수 있습니다. CSP 속성 예:

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' data:
content-security-policy-portal = default-src 'self';frame-ancestors 'self'
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

## 다른 보호 조치

Horizon 7에서는 Internet Engineering Task Force 및 W3 표준 외에도 다른 조치를 사용해서 HTTP 프로토콜을 이용한 통신을 보호할 수 있습니다.

### MIME 유형 보안 위험 줄이기

기본적으로 Horizon 7은 HTTP 응답에서 `x-content-type-options: nosniff` 헤더를 전송하여 MIME 유형 혼란을 바탕으로 한 공격을 방지합니다.

`locked.properties` 파일에 다음 항목을 추가하면 이 기능을 사용하지 않도록 설정할 수 있습니다.

```
x-content-type-options=OFF
```

### 사이트 간 스크립팅 공격 완화

기본적으로 Horizon 7은 XSS(사이트 간 스크립팅) 필터 기능을 사용하여 HTTP 응답에서 `x-xss-protection=1; mode=block` 헤더 전송에 의한 사이트 간 스크립팅 공격을 완화합니다.

`locked.properties` 파일에 다음 항목을 추가하면 이 기능을 사용하지 않도록 설정할 수 있습니다.

```
x-xss-protection=OFF
```

### 콘텐츠 유형 검사

Horizon 7에서는 기본적으로 다음의 선언된 콘텐츠 유형에 대한 요청만 수락합니다.

- `application/x-www-form-urlencoded`
- `application/xml`
- `text/xml`

**참고** 이전 릴리스에서는 기본적으로 이 보호를 사용하지 않도록 설정되었습니다.

View가 수락하는 콘텐츠 유형을 제한하려면 `locked.properties` 파일에 다음 항목을 추가합니다.

```
acceptContentType.1=content-type
```

예 :

```
acceptContentType.1=x-www-form-urlencoded
```

다른 콘텐츠 유형을 수락하려면 `acceptContentType.2=content-type` 등의 항목을 추가합니다.

선언된 모든 콘텐츠 유형에 대한 요청을 수락하려면 `acceptContentType=*`를 지정합니다.

**참고** Horizon 7 버전 7.2 이하 릴리스에서는 이 목록을 변경해도 Horizon Administrator에 대한 연결에 영향을 미치지 않습니다.

## 사용자 에이전트 화이트리스트

Horizon 7과 상호 작용할 수 있는 사용자 에이전트를 제한하려면 화이트리스트를 설정합니다. 기본적으로 모든 사용자 에이전트가 수락됩니다.

**참고** 엄격히 말해 보안 기능은 아닙니다. 사용자 에이전트 감지는 연결하는 클라이언트 또는 브라우저에서 제공하는 사용자 에이전트 요청 헤더에 의존합니다. 이러한 헤더는 스푸핑될 수 있습니다. 일부 브라우저에서는 사용자가 요청 헤더를 수정할 수 있도록 허용합니다.

사용자 에이전트는 해당 이름 및 최소 버전으로 지정됩니다. 예:

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

즉, Google Chrome 버전 14 이상 및 Safari 버전 5.1 이상에서만 HTML Access를 사용하여 연결하도록 허용됩니다. 모든 브라우저는 다른 서비스에 연결할 수 있습니다.

인식된 다음 사용자 에이전트 이름을 입력할 수 있습니다.

- Android
- Chrome
- Edge
- IE
- Firefox
- Opera
- Safari

**참고** 이러한 모든 사용자 에이전트가 Horizon 7에서 지원되는 것은 아닙니다. 예는 다음과 같습니다.

## HTTP 보호 조치 구성

HTTP 보호 조치를 구성하려면 연결 서버 또는 보안 서버 인스턴스의 SSL 게이트웨이 구성 폴더에서 locked.properties 파일을 생성하거나 편집해야 합니다.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`

- Locked.properties에서 속성을 구성하려면 다음 구문을 사용합니다.

```
myProperty = newValue
```

- 속성 이름은 항상 대/소문자를 구분하며 값은 대/소문자를 구분할 수도 있습니다. = 기호 주위의 공백은 선택 사항입니다.

- CORS 및 CSP 속성의 경우 마스터 값뿐 아니라 서비스 특정 값을 설정할 수 있습니다. 예를 들어 관리 서비스는 Horizon Administrator 요청을 처리하며, 속성 이름 뒤에 -admin을 추가하여 다른 서비스에 영향을 미치지 않으면서 이 서비스에 대해 속성을 설정할 수 있습니다.

```
myProperty-admin = newValueForAdmin
```

- 마스터 값과 서비스 특정 값을 둘 다 지정하면 서비스 특정 값이 명명된 서비스에 적용되고 마스터 값이 다른 모든 서비스에 적용됩니다. 이 방식의 유일한 예외는 특수 값 "OFF"입니다. 속성에 대한 마스터 값을 "OFF"로 설정하면 이 속성에 대한 모든 서비스 특정 값이 무시됩니다.

예:

```
myProperty = OFF
myProperty-admin = newValueForAdmin ; ignored
```

- 일부 속성은 값 목록을 수락할 수 있습니다.

단일 값을 설정하려면 다음 속성을 입력하십시오.

```
myProperty = newValue
myProperty-admin = newValueForAdmin
```

목록 값을 허용하는 속성에 대해 여러 값을 설정하려면 각 값을 별도 줄에 지정할 수 있습니다.

```
myProperty.1 = newValue1
myProperty.2 = newValue2
myProperty-admin.1 = newValueForAdmin1
myProperty-admin.2 = newValueForAdmin2
```

- 서비스 특정 구성을 만들 때 사용할 올바른 서비스 이름을 확인하려면 디버그 로그에서 다음 시퀀스가 포함된 줄을 찾아보십시오.

```
(ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
```

이 예에서 서비스 이름은 admin입니다. 다음과 같은 일반적인 서비스 이름을 사용할 수 있습니다.

- Horizon Administrator의 경우 admin
- 연결 서버의 경우 broker
- 로컬 파일 처리의 경우 docroot
- 기술 지원의 경우 helpdesk
- HTML Access의 경우 portal
- SAML 통신(VIDM)의 경우 saml
- 보안 터널의 경우 tunnel
- View API의 경우 view-vlsi
- 기타의 경우 misc