Windows용 VMware Horizon Client 사용

수정 날짜: 2018년 1월 10일

VMware Horizon Client for Windows 4.5

vmware®

VMware 웹 사이트 (https://docs.vmware.com/kr/) 에서 최신 기술 문서를 확인할 수 있습니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

목차

Windows용 VMware Horizon Client 사용

이 Windows용 VMware Horizon Client 사용 설명서에서는 데이터센터에서 원격 데스크톱 또는 애플리케이션에 연결하기 위해 Microsoft Windows 클라이언트 시스템에서 VMware Horizon® Client™ 소프트웨어를 설치하고 사용하는 방법에 관한 정보를 제공합니다.

이 문서의 정보에는 Windows용 Horizon Client 설치 및 사용에 대한 시스템 요구 사항 및 지침이 포함되어 있습니다.

이 정보는 데스크톱 및 노트북과 같은 Microsoft Windows 클라이언트 시스템이 포함된 Horizon 배포를 설정해야 하는 관리자용입니다. 이 정보는 가상 시스템 기술과 데이터센터 운영에 익숙하고 경험 많은 시스템 관리자를 대상으로 작성되었습니다.

Windows 기반 클라이언트의 시스템 요구 사항 및 설정 1

Horizon Client 구성 요소가 실행되는 시스템은 특정 하드웨어 및 소프트웨어 요구 사항을 충족해야 합니다.

Windows 시스템의 Horizon Client는 연결 서버에 연결할 때 프록시 설정을 포함한 Microsoft Internet Explorer 인터넷 설정을 사용합니다. Internet Explorer 설정이 정확하고 Internet Explorer를 통해 연결 서버 URL에 액세스할 수 있어야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

Windows 클라이언트 시스템 요구 사항

지원되는 Microsoft Windows 운영 체제를 사용하는 PC 또는 노트북에 Windows용 Horizon Client를 설치할 수 있습니다.

Horizon Client를 설치할 PC 또는 노트북 그리고 여기에서 사용되는 주변 기기는 특정 시스템 요구 사항을 충족해야 합니다.

모델

모든 x86 또는 x86-64 Windows 디바이스

메모리

1GB RAM 이상

운영 체제

지원되는 운영 체제는 다음과 같습니다.

OS	버전	서비스 팩 또는 서비스 옵션	지원되는 버전
Windows 10	32 또는 64비트	현재 분기(CB) 버전 1703(작성자 업데이트) 현재 분기(CB) 버전 1607(1주년 업데이트) 비즈니스용 현재 분기(CBB) 버전 1607(1주년 업데이트) 장기 서비스 분기(LTSB) 버전 1607(1주년 업데이트) LTSB(Long-Term Servicing Branch) 버전 1507	Home, Pro, Enterprise 및 IoT Core
Windows 8 또는 8.1	32 또는 64비트	없음 또는 업데이트 2	Pro , Enterprise 및 Industry Embedded
Windows 7	32 또는 64비트	SP1	Home, Enterprise, Professional 및 Ultimate
Windows Server 2008 R2	64비트	최신 업데이트	Standard
Windows Server 2012 R2	64비트	최신 업데이트	Standard

Windows Server 2008 R2 및 Windows Server 2012 R2는 Horizon Client를 중첩 모드에서 실행하기 위해 지원됩니다. 자세한 내용은 중첩 모드에서 지원되는 기능의 내용을 참조하십시오.

연결 서버, 보안 서버 및 View Agent 또는 Horizon Agent

View 6.x 이상 릴리스의 최신 유지보수 릴리스

클라이언트 시스템이 회사 방화벽 외부에서 연결되는 경우 VMware는 클라이언트 시스템에 VPN 연결이 필요하지 않도록 보안 서버 또는 Unified Access Gateway 장치 사용을 권장합니다.

참고 또한 클라이언트는 Horizon 6 버전 6.2 이상 릴리스에서 사용할 수 있는 Unified Access Gateway 장치에 연결될 수 있습니다.

디스플레이 프로토콜

VMware Blast, PCoIP 및 RDP

PCoIP 및 VMware Blast를 위한 하드웨어 요구 사항

- 프로세서 속도가 800MHz 이상인 x86 기반 프로세서(SSE2 확장).
- 다양한 모니터 설정을 지원하기 위한 시스템 요구 사항 이상의 RAM 사용 가능. 일반적인 지침으로 다음 공식을 사용합니다.

```
20MB + (24 * (# monitors) * (monitor width) * (monitor height))
```

대체적으로 다음과 같이 계산할 수 있습니다.

```
1 monitor: 1600 x 1200: 64MB
2 monitors: 1600 x 1200: 128MB
3 monitors: 1600 x 1200: 256MB
```

RDP의 하드웨어 요구 사항

- 프로세서 속도가 800MHz 이상인 x86 기반 프로세서(SSE2 확장).
- 128MB RAM.

RDP 소프트웨어 요구 사항

- Windows 7의 경우 RDP 7.1 또는 8.0을 사용합니다. Windows 7에는 RDP 7이 포함되어 있습니다. Windows 7 SP1에는 RDP 7.1이 포함되어 있습니다.
- Windows 8의 경우 RDP 8.0을 사용하고 Windows 8.1의 경우 RDP 8.1을 사용합니다.
- Windows 10의 경우 RDP 10.0을 사용합니다.
- (View Agent 6.0.2 이하에서만 지원됨) Windows XP 데스크톱 가상 시스템의 경우 Microsoft 기술 자료(KB) 문서 323497 및 884020에 나열된 RDP 패치를 설치해야 합니다. RDP 패치를 설치하지 않는 경우 Windows Sockets 실패 오류 메시지가 클라이언트에 표시될 수 있습니다.
- 에이전트 설치 프로그램에서 인바운드 RDP 연결의 로컬 방화벽 규칙을 호스트 운영 체제의 현재 RDP 포트(일반적으로 3389)와 일치하도록 구성합니다. RDP 포트 번호를 변경할 경우에는 연결된 방화벽 규칙을 변경해야 합니다.

원격 데스크톱 클라이언트 버전은 Microsoft 다운로드 센터에서 다운로드할 수 있습니다.

비디오 및 그래픽 요구 사항

- Direct3D 11 비디오를 지원하는 그래픽 카드
- 최신 비디오 및 그래픽 카드 드라이버
- Windows 7 SP1의 경우 Windows 7 SP1 및 Windows Server 2008 R2 SP1용 플랫폼 업데이트를 설치합니다. 자세한 내용을 보려면 https://support.microsoft.com/ko-kr/kb/2670838로 이동하십시오.

실시간 오디오-비디오에 대한 시스템 요구 사항

실시간 오디오-비디오는 표준 웹캠, USB 오디오 및 아날로그 오디오 디바이스와 Skype, WebEx 및 Google Hangout과 같은 표준 회의 애플리케이션에서 작동합니다. 실시간 오디오-비디오를 지원하려면 Horizon 배포가 특정 소프트웨어 및 하드웨어 요구 사항을 충족해야 합니다.

원격 데스크톱

데스크톱에는 View Agent 5.2 이상이나 Horizon Agent 7.0 이상이 설치되어 있어야 합니다. View Agent 5.2 데스크톱의 경우 데스크톱에 해당 Remote Experience Agent도 설치되어 있어야 합니다. 예를 들어 View Agent 5.2가 설치된 경우 View 5.2 기능 팩 2에서 Remote Experience Agent도 설치해야 합니다. View Feature Pack 설치 및 관리 문서를 참조하십시오. View Agent 6.0 이상 또는 Horizon Agent 7.0 이상의 경우 기능 팩은 필요하지 않습니다. 게시된 데스크톱 및 애플리케이션에서 실시간 오디오-비디오를 사용하려면 Horizon Agent 7.0.2 이상을 설치해야 합니다.

Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

- Windows용 Horizon Client를 실행하는 모든 운영 체제에서 실시간 오디오-비디오가 지원됩니다. 자세한 내용은 Windows 클라이언트 시스템 요구 사항에 나와 있습니다.
- 웹캠 및 오디오 디바이스 드라이버가 설치되어 있어야 하며, 클라이언트 컴퓨터에서 웹캠 및 오디오 디바이스를 작동할 수 있어야 합니다. 실시간 오디오-비디오를 지원하기 위해 에이전트가 설치되어 있는 데스크톱 운영 체제에 디바이스 드라이버를 설치할 필요는 없습니다.

디스플레이 프로토콜

- PCoIP
- VMware Blast(Horizon Agent 7.0 이상 필요)

스캐너 리디렉션에 대한 시스템 요구 사항

로컬 클라이언트 시스템에 연결된 스캐너를 사용하여 원격 데스크톱 및 애플리케이션으로 정보를 스캔할 수 있습니다. 이 기능을 사용하려면 원격 데스크톱, 애플리케이션 및 클라이언트 컴퓨터가 특정 시스템 요구 사항을 충족해야 합니다.

원격 데스크톱

원격 데스크톱에는 스캐너 리디렉션 설정 옵션과 함께 View Agent 6.0.2 또는 Horizon Agent 7.0 이상이 상위 시스템 또는 템플릿 가상 시스템이나 RDS 호스트에 설치되어 있어야 합니다. Windows 데스크톱 및 Windows Server 게스트 운영 체제에서는 기본적으로 Horizon Agent 스캐너 리디렉션 설정 옵션이 선택되지 않습니다.

단일 사용자 가상 시스템 및 RDS 호스트에서 지원되는 게스트 운영 체제에 대한 정보와 원격 데스크톱 및 애플리케이션에서 스캐너 리디렉션을 구성하는 방법에 대한 정보는 Horizon 7에서 원격 데스크톱 기능 구성의 "스캐너 리디렉션 구성" 항목을 참조하십시오.

Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

- 스캐너 리디렉션은 Windows 7, Windows 8/8.1 및 Windows 10에서 지원됩니다.
- 스캐너 디바이스 드라이버가 설치되어 있어야 하며, 클라이언트 컴퓨터에서 스캐너를 작동할 수 있어야 합니다. 에이전트가 설치되어 있는 원격 데스크톱 운영 체제에는 스캐너 디바이스 드라이버를 설치하지 않아도 됩니다.

스캔 디바이스 표준

TWAIN 또는 WIA

디스플레이 프로토콜

- PCoIP
- VMware Blast(Horizon Agent 7.0 이상 필요)

RDP 데스크톱 세션에서는 스캐너 리디렉션이 지원되지 않습니다.

직렬 포트 리디렉션에 대한 시스템 요구 사항

이 기능을 사용하여 로컬로 연결된 직렬(COM) 포트(예: 내장형 RS232 포트 또는 USB-직렬 어댑터)를 원격 데스크톱으로 리디렉션할 수 있습니다. 직렬 포트 리디렉션을 지원하려면 Horizon 배포가 특정 소프트웨어 및 하드웨어 요구 사항을 충족해야 합니다.

원격 데스크톱

원격 데스크톱에는 직렬 포트 리디렉션 설정 옵션과 함께 View Agent 6.1.1 이상 또는 Horizon Agent 7.0 이상이 상위 가상 시스템 또는 템플릿 가상 시스템에 설치되어 있어야 합니다. 이 설치 옵션은 기본적으로 선택되어 있지 않습니다.

단일 세션 가상 시스템에서 다음 게스트 운영 체제가 지원됩니다.

- 32비트 또는 64비트 Windows 7

- 32비트 또는 64비트 Windows 8.x
- 32비트 또는 64비트 Windows 10
- Windows Server 2008 R2(데스크톱으로 구성)
- Windows Server 2012 R2(데스크톱으로 구성)
- Windows Server 2016(데스크톱으로 구성)

이 기능은 현재 Windows Server RDS 호스트에서는 지원되지 않습니다.

에이전트가 설치된 데스크톱 운영 체제에는 직렬 포트 디바이스 드라이버를 설치하지 않아도 됩니다.

참고 원격 데스크톱에서 직렬 포트 리디렉션 구성에 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성의 "직렬 포트 리디렉션 구성"을 참조하십시오.

Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

- 직렬 포트 리디렉션은 Windows 7, Windows 8.x 클라이언트 시스템 및 Windows 10에서 지원됩니다.
- 필요한 모든 직렬 포트 디바이스 드라이버가 설치되어 있어야 하며, 클라이언트 컴퓨터에서 직렬 포트를 작동할 수 있어야 합니다. 에이전트가 설치되어 있는 원격 데스크톱 운영 체제에는 디바이스 드라이버를 설치하지 않아도 됩니다.

디스플레이 프로토콜

- PCoIP
- VMware Blast(Horizon Agent 7.0 이상 필요)

RDP 데스크톱 세션에서는 VMware Horizon 직렬 포트 리디렉션이 지원되지 않습니다.

MMR(멀티미디어 리디렉션)에 대한 시스템 요구 사항

MMR(멀티미디어 리디렉션)을 사용하면 멀티미디어 스트림이 처리됩니다. 즉, 클라이언트 시스템에서 디코딩됩니다. 클라이언트 시스템은 미디어 컨텐츠를 재생하여 ESXi 호스트에 대한 부하를 줄여줍니다.

원격 데스크톱

- 단일 사용자 데스크톱에는 View Agent 6.0.2 이상이나 Horizon Agent 7.0 이상이 설치되어 있어야 합니다.
- 세션 기반 데스크톱에는 RDS 호스트에 View Agent 6.1.1 이상이나 Horizon Agent 7.0 이상이 설치되어 있어야 합니다.

	■ 원격 데스크톱 또는 애플리케이션에 대한 운영 체제 요구 사항 및 기타 소프트웨어 요구 사항과 구성 설정에 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성에서 Windows Media 멀티미디어 리디렉션에 대한 항목을 참조하십시오.
Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스	32비트 또는 64비트 Windows 7, Windows 8.x 또는 Windows 10.
지원되는 미디어 형식	Windows Media Player에서 지원되는 미디어 형식이 모두 지원됩니다. 예: M4V, MOV, MP4, WMP, MPEG-4 Part 2, WMV 7, 8 및 9, WMA, AVI, ACE, MP3, WAV. **참고** DRM 보호 컨텐츠는 Windows Media MMR을 통해 리디렉션되지 않습니다.

Flash 리디렉션에 대한 시스템 요구 사항

Flash 리디렉션을 사용 중이며 Internet Explorer 9, 10 또는 11을 사용할 경우 Flash 컨텐츠가 클라이언트 시스템으로 전송됩니다. 클라이언트 시스템은 미디어 컨텐츠를 재생하여 ESXi 호스트에 대한 부하를 줄여줍니다.

원격 데스크톱	■ 단일 사용자(VDI) 원격 데스크톱에 Flash 리디렉션 옵션을 포함한 Horizon Agent 7.0 이상이 설치되어 있어야 합니다. Flash 리디렉션 옵션은 기본적으로 선택되어 있지 않습니다. Horizon 7에서 가상 데스크톱 설정 문서에서 Horizon Agent 설치에 관한 항목을 참조하십시오. ■ 적절한 그룹 정책 설정이 구성되어 있어야 합니다. Horizon 7에서 가상 데스크톱 설정 문서에서 Flash 리디렉션 구성에 관한 항목을 참조하십시오. ■ Flash 리디렉션은 Windows 7, Windows 8, Windows 8.1 및 Windows 10 단일 사용자 원격 데스크톱에서 지원됩니다. ■ Internet Explorer 9, 10 또는 11이 해당 Flash ActiveX 플러그인과 함께 설치되어 있어야 합니다. ■ 설치 후 Internet Explorer에서 VMware View FlashMMR Server 추가 기능을 사용하도록 설정해야 합니다.
Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스	■ Flash 리디렉션은 Windows 7, Windows 8, Windows 8.1 및 Windows 10에서 지원됩니다.

- Flash ActiveX 플러그인이 설치 및 활성화되어 있어야 합니다.

원격 세션을 위한 디스플레이 프로토콜 VMware Blast, PCoIP

플래시 URL 리디렉션 사용에 대한 요구 사항

Adobe Media Server에서 클라이언트 끝점으로 플래시 컨텐츠를 직접 스트리밍하면 데이터센터 ESXi 호스트에 대한 부하를 줄이고, 데이터센터를 통해 추가 라우팅을 제거하고, 여러 클라이언트 끝점에 라이브 비디오 이벤트를 동시에 스트리밍하는 데 필요한 대역폭을 줄여줍니다.

플래시 URL 리디렉션 기능은 웹 페이지 관리자에 의해 웹 페이지 내에 포함된 JavaScript를 사용합니다. 가상 데스크톱 사용자가 웹 페이지 내에서 지정된 URL 링크를 클릭할 때마다 JavaScript는 가상 데스크톱 세션에서 클라이언트 끝점으로 ShockWave 파일(SWF)을 가로채서 리디렉션합니다. 그런 다음 끝점은 가상 데스크톱 세션 외부에서 로컬 VMware Flash Projector를 열고 로컬로 미디어 스트림을 재생합니다. 멀티캐스트 및 유니캐스트가 모두 지원됩니다.

이 기능은 올바른 버전의 에이전트 소프트웨어와 함께 사용할 때 제공됩니다. View 5.3의 경우 이 기능은 View Feature Pack의 일부인 Remote Experience Agent에 포함되어 있습니다. View 6.0 이상 릴리스의 경우 이 기능은 View Agent 또는 Horizon Agent에 포함되어 있습니다.

이 기능을 사용하려면 웹 페이지 및 클라이언트 디바이스를 설정해야 합니다. 클라이언트 시스템은 특정 소프트웨어 요구 사항을 충족해야 합니다.

- 클라이언트 시스템은 멀티캐스트 또는 유니캐스트 스트리밍을 시작하는 ShockWave 파일(SWF)을 호스팅하는 Adobe Web 서버에 IP를 연결해야 합니다. 필요할 경우, 해당 포트를 열 수 있도록 방화벽을 구성하여 클라이언트 디바이스가 이 서버에 액세스할 수 있게 허용합니다.
- 클라이언트 시스템에는 Internet Explorer(ActiveX 사용)용 Adobe Flash Player 10.1 이상이 있어야 합니다.

플래시 URL 리디렉션에 대한 원격 데스크톱 요구 사항의 목록 및 멀티캐스트 또는 유니캐스트 스트림을 제공하도록 웹 페이지를 구성하는 방법에 대한 지침은 Horizon 설명서를 참조하십시오.

Horizon Client 가 있는 Microsoft Lync에 대한 시스템 요구 사항

원격 데스크톱에서 Microsoft Lync 2013 클라이언트를 사용하여 Lync 인증 USB 오디오 및 비디오 디바이스로 비디오 채팅 호출 및 UC(Unified Communications) VoIP에 참여할 수 있습니다. 더 이상 전용 IP 휴대 전화가 필요하지 않습니다.

이 아키텍처를 사용하려면 원격 데스크톱에 Microsoft Lync 2013 클라이언트를 설치하고 클라이언트 끝점에 Microsoft Lync VDI 플러그인을 설치해야 합니다. 고객은 상태, 인스턴트 메시징, 웹 회의 및 Microsoft Office 기능에 Microsoft Lync 2013을 사용할 수 있습니다.

Lync VoIP 또는 비디오 채팅 호출이 실행될 때마다 Lync VDI 플러그인은 데이터 센터 서버에서 클라이언트 끝점으로 모든 미디어 처리를 오프로드하고 Lync 최적 오디오 및 비디오 코덱으로 모든 미디어를 인코딩합니다. 이 최적화된 아키텍처는 고도로 확장 가능하며 네트워크 대역폭 사용을 낮추고 고품질 실시간 VoIP 및 비디오 지원으로 지점간 미디어 전달을 제공합니다. 자세한 내용은 http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf에서 Horizon 6 및 Microsoft Lync 2013에 대한 백서를 참조하십시오.

참고 오디오 기록은 아직 지원되지 않습니다. 이 통합에는 PCoIP 디스플레이 프로토콜만 지원됩니다.

이 기능의 다음 요구 사항은 다음과 같습니다.

운영 체제

- 클라이언트 운영 체제: Windows 7 SP1, Windows 8.x 또는 Windows 10.
- 가상 시스템(에이전트) 운영 체제는 에이전트 버전에 따라 다릅니다.

버전	게스트 운영 체제
View Agent 6.2 이상 또는 Horizon Agent 7.0 이상	32비트 또는 64비트 Windows 7 SP1, Windows 8.x, Windows 10 또는 64비트 Windows Server 2008 R2 SP1 Microsoft RDS 호스트: Windows Server 2008 R2, Windows Server 2012 또는 Windows Server 2012 R2
View Agent 6.0 또는 6.1	32비트 또는 64비트 Windows 7 SP1, Windows 8.x 또는 64비트 Windows Server 2008 R2 SP1
View Agent 5.3	32비트 또는 64비트 Windows 7 SP1

클라이언트 시스템 소프트웨어

- Microsoft Lync VDI 플러그인의 32비트 버전

  중요 클라이언트 시스템에 Microsoft Office의 64비트 버전을 설치하면 안 됩니다. 필수 항목인 32비트 Microsoft Lync VDI 플러그인은 64비트 Microsoft Office 2013과 호환되지 않습니다.

- Microsoft Lync Server 2013 배포 중 생성된 보안 인증서를 신뢰할 수 있는 루트 인증 기관 디렉토리로 가져와야 합니다.

원격 데스크톱(에이전트) 소프트웨어

- View Agent 5.3 이상 또는 Horizon Agent 7.0 이상
- Microsoft Lync 2013 Client

  View 5.3 이상 에이전트에서는 Lync 2013 클라이언트 비트 수준이 가상 시스템 운영 체제의 비트 수준과 일치할 필요가 없습니다.

- Microsoft Lync Server 2013 배포 중 생성된 보안 인증서를 신뢰할 수 있는 루트 인증 기관 디렉토리로 가져와야 합니다.

필수 서버

- 연결 서버 5.3 이상을 실행 중인 서버

- Microsoft Lync Server 2013을 실행 중인 서버
- 가상 시스템을 호스팅하기 위한 vSphere 인프라

  vCenter Server 및 ESXi 호스트에서 vSphere 5.0 이상을 실행 중이어야 합니다.

하드웨어

- 이전에 나열된 각 필수 소프트웨어 구성 요소를 지원하는 하드웨어
- 클라이언트 끝점: 1.5GHz 이상 CPU 및 Microsoft Lync 2013 플러그인을 위한 최소 2GB의 RAM

참고 문제 해결 정보에 관해서는 VMware KB 2063769 및 VMware KB 2053732를 참조하십시오.

URL 컨텐츠 리디렉션 사용에 대한 요구 사항

URL 컨텐츠 리디렉션 기능을 사용하면 URL 컨텐츠가 클라이언트 시스템에서 원격 데스크톱이나 애플리케이션으로(클라이언트-에이전트 리디렉션) 또는 원격 데스크톱이나 애플리케이션에서 클라이언트 시스템으로(에이전트-클라이언트 리디렉션) 리디렉션될 수 있습니다.

예를 들어 클라이언트의 기본 Microsoft Word 애플리케이션에서 링크를 클릭하면 해당 링크가 원격 Internet Explorer 애플리케이션에서 열리고, 원격 Internet Explorer 애플리케이션에서 링크를 클릭하면 해당 링크가 클라이언트 시스템의 기본 브라우저에서 열립니다. HTTP, mailto 및 callto를 비롯한 프로토콜을 개수에 관계없이 리디렉션을 위해 구성할 수 있습니다.

URL을 입력하거나 클릭하고 URL을 리디렉션할 수 있는 지원되는 브라우저는 Internet Explorer 9, 10 및 11입니다.

참고 Microsoft Edge 브라우저를 포함하여 Windows 10 범용 애플리케이션 내부에서 클릭하는 링크의 경우 이 기능은 작동하지 않습니다.

클라이언트-에이전트 리디렉션을 사용하려면 Horizon Client를 설치할 때 URL 컨텐츠 리디렉션을 사용하도록 설정해야 합니다. URL 컨텐츠 리디렉션을 사용하도록 설정하려면 명령줄에서 Horizon Client를 설치해야 합니다. 자세한 정보는 명령줄에서 Horizon Client 설치의 내용을 참조하십시오.

에이전트-클라이언트 리디렉션을 사용하려면 Horizon 관리자가 Horizon Agent 설치 중에 URL 컨텐츠 리디렉션을 사용하도록 설정해야 합니다. 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 또는 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

또한 Horizon 관리자는 Horizon Client가 클라이언트 시스템에서 원격 데스크톱 또는 애플리케이션으로 URL 컨텐츠를 리디렉션하는 방법 또는 Horizon Agent가 원격 데스크톱 또는 애플리케이션에서 클라이언트 시스템으로 URL 컨텐츠를 리디렉션하는 방법을 지정하는 설정도 구성해야 합니다. 구성 정보는 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

Horizon Client 에서 비즈니스용 Skype를 사용하기 위한 요구 사항

가상 인프라에 부정적인 영향을 주지 않고 네트워크를 오버로드하지 않으면서 비즈니스용 Skype를 가상 데스크톱 내에서 실행할 수 있습니다. Skype 오디오 및 비디오 호출 동안 모든 미디어 처리는 가상 데스크톱 대신, Windows 클라이언트 시스템에서 진행됩니다.

이 기능을 사용하려면 Windows용 Horizon Client 설치 중에 클라이언트 시스템에 비즈니스용 Skype의 가상화 팩 기능을 설치해야 합니다. 자세한 정보는 2장Windows용 Horizon Client 설치의 내용을 참조하십시오.

또한 Horizon 관리자는 Horizon Agent 설치 중에 가상 데스크톱에 비즈니스용 Skype에 대한 VMware Virtualization Pack 기능을 설치해야 합니다. 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서를 참조하십시오.

전체 요구 사항은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

스마트 카드 인증 요구 사항

사용자 인증에 스마트 카드를 사용하는 클라이언트 시스템은 특정 요구 사항을 충족해야 합니다.

사용자 인증에 스마트 카드를 사용하는 각 클라이언트 시스템에는 다음 소프트웨어 및 하드웨어가 있어야 합니다.

- Horizon Client
- 호환 스마트 카드 판독기
- 제품 특정 애플리케이션 드라이버

또한 원격 데스크톱 또는 Microsoft RDS 호스트에 제품 특정 애플리케이션 드라이버를 설치해야 합니다.

Horizon은 PKCS#11 또는 Microsoft CryptoAPI 공급자를 사용하는 스마트 카드 및 스마트 카드 판독기를 지원합니다. 스마트 카드와 상호 작용하기 위한 도구를 제공하는 ActivIdentity ActivClient 소프트웨어 제품군을 선택적으로 설치할 수 있습니다.

스마트 카드를 사용하여 인증하는 사용자는 스마트 카드 또는 USB 스마트 카드 토큰이 있어야 하며 각 스마트 카드에는 사용자 인증서가 포함되어 있어야 합니다.

스마트 카드에 인증서를 설치하려면 등록 스테이션 역할을 하도록 컴퓨터를 설정해야 합니다. 이 컴퓨터는 사용자용 스마트 카드 인증서를 발행하는 기관이 있어야 하며 인증서를 발행하는 도메인의 구성원이어야 합니다.

중요 스마트 카드를 등록할 때 결과 인증서의 키 크기를 선택할 수 있습니다. 로컬 데스크톱에서 스마트 카드를 사용하려면 스마트 카드 등록 중에 1024비트 또는 2048비트 키 크기를 선택해야 합니다. 512비트 키를 가진 인증서는 지원되지 않습니다.

Microsoft TechNet 웹 사이트에는 Windows 시스템의 스마트 카드 인증 계획 및 구현에 대한 자세한 정보가 포함되어 있습니다.

Horizon Client 시스템의 이러한 요구 사항을 충족하는 것 외에도 다른 Horizon 구성 요소가 스마트 카드를 지원하기 위한 특정 구성 요구 사항을 충족해야 합니다.

- 스마트 카드 사용을 지원하도록 연결 서버를 구성하는 방법에 대한 자세한 내용은 View 관리 문서를 참조하십시오.

  신뢰할 수 있는 모든 사용자 인증서에 대해 적용할 수 있는 모든 CA(인증 기관) 인증서를 연결 서버 호스트나 보안 서버 호스트에 있는 서버 truststore 파일에 추가해야 합니다. 이러한 인증서에는 루트 인증서가 포함되며, 사용자의 스마트 카드 인증서가 중간 인증 기관에서 발급된 경우에는 중간 인증서도 포함되어야 합니다.

- 스마트 카드 인증을 구현하기 위해 Active Directory에서 수행해야 하는 작업에 대한 자세한 내용은 View 관리 문서를 참조하십시오.

Horizon Client 에서 사용자 이름 힌트 필드를 사용하도록 설정

일부 환경에서 스마트 카드 사용자는 단일 스마트 카드 인증서를 사용하여 여러 사용자 계정을 인증할 수 있습니다. 사용자는 스마트 카드 로그인 중에 **사용자 이름 힌트** 필드에 사용자 이름을 입력합니다.

Horizon Client 로그인 대화상자에 **사용자 이름 힌트** 필드가 나타나게 하려면 Horizon Administrator의 연결 서버 인스턴스에 대해 스마트 카드 사용자 이름 힌트 기능을 사용하도록 설정해야 합니다. 스마트 카드 사용자 이름 힌트 기능은 Horizon 7 버전 7.0.2 이상 서버 및 에이전트에서만 지원됩니다. 스마트 카드 사용자 이름 힌트 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 View 관리 문서를 참조하십시오.

작업 환경에서 보안 외부 액세스를 위해 보안 서버가 아닌 Unified Access Gateway 장치를 사용하는 경우 스마트 카드 사용자 이름 힌트 기능을 지원하도록 Unified Access Gateway 장치를 구성해야 합니다. 스마트 카드 사용자 이름 힌트 기능은 Unified Access Gateway 2.7.2 이상에서만 지원됩니다. Unified Access Gateway의 스마트 카드 사용자 이름 힌트 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성 문서를 참조하십시오.

참고 Horizon Client는 스마트 카드 사용자 이름 힌트 기능이 사용되도록 설정되어 있는 경우 단일 계정 스마트 카드 인증서를 계속 지원합니다.

디바이스 인증 요구 사항

클라이언트 디바이스에 대해 인증서 인증을 설정할 수 있습니다.

이 기능의 요구 사항은 다음과 같습니다.

- Unified Access Gateway 2.6 이상
- Horizon 7 버전 7.0 이상
- Unified Access Gateway가 수락할 클라이언트 디바이스에 설치되어 있는 인증서

지원되는 데스크톱 운영 체제

관리자는 게스트 운영 체제를 사용하여 가상 시스템을 생성하고 게스트 운영 체제에 에이전트 소프트웨어를 설치합니다. 최종 사용자는 클라이언트 디바이스에서 이러한 가상 시스템에 로그인할 수 있습니다.

지원되는 Windows 게스트 운영 체제 목록에 대해서는 View 설치 문서를 참조하십시오.

View Agent 6.1.1 이상 또는 Horizon Agent 7.0 이상이 설치되어 있는 경우 일부 Linux 게스트 운영 체제도 지원됩니다. 시스템 요구 사항, Horizon에서 사용하도록 Linux 가상 시스템 구성, 지원되는 기능 목록에 대한 자세한 내용은 Horizon 6 for Linux 데스크톱 설정 또는 Horizon 7 for Linux 데스크톱 설정 항목을 참조하십시오.

Horizon Client 용 연결 서버 준비

최종 사용자가 원격 데스크톱 및 애플리케이션에 연결할 수 있도록 하려면 관리자가 특정 작업을 수행해야 합니다.

최종 사용자가 연결 서버 또는 보안 서버에 연결하고 원격 데스크톱 또는 애플리케이션에 액세스할 수 있으려면 다음과 같이 특정 풀 설정 및 보안 설정을 구성해야 합니다.

- Unified Access Gateway를 사용하려는 경우 Unified Access Gateway에서 작동되도록 연결 서버를 구성합니다. Unified Access Gateway 배포 및 구성 문서를 참조하십시오. Unified Access Gateway 장치에서는 이전에 보안 서버에서만 담당했던 역할을 그대로 이행합니다.
- 보안 서버를 사용하는 경우 연결 서버 5.3.x 및 보안 서버 5.3.x 이상 릴리스의 최신 유지보수 릴리스를 사용하고 있는지 확인하십시오. 자세한 내용은 View 설치 문서를 참조하십시오.
- 클라이언트 디바이스에 보안 터널 연결을 사용하고, 보안 연결이 연결 서버 또는 보안 서버의 DNS 호스트 이름으로 구성될 경우, 클라이언트 디바이스에서 DNS 이름을 확인할 수 있는지 확인하십시오.

  보안 터널을 사용하도록 또는 사용하지 않도록 설정하려면 Horizon Administrator에서 **Horizon 연결 서버 설정 편집** 대화상자로 이동하여 **보안 터널을 사용하여 데스크톱에 연결** 확인란을 사용합니다.
- 데스크톱 또는 애플리케이션 풀이 생성되었으며 사용하려는 사용자 계정이 풀에 대한 액세스 권한을 갖고 있는지 확인하십시오. 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 또는 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

중요 고해상도 디스플레이가 있는 최종 사용자가 전체 화면 모드에서 원격 데스크톱을 볼 때 고해상도 모드 클라이언트 설정을 사용하려면 각각의 Windows 7 이상 원격 데스크톱에 충분한 VRAM을 할당해야 합니다. 필요한 vRAM의 양은 최종 사용자에 대해 구성된 모니터의 수와 디스플레이 해상도에 따라 달라집니다. 필요한 vRAM 양을 예상하려면 View 아키텍처 계획 문서를 참조하십시오.

- Horizon Client에 RSA SecurID 또는 RADIUS 인증과 같은 2단계 인증을 사용하려면 연결 서버에서 이 기능을 사용하도록 설정해야 합니다. 자세한 내용은 View 관리 문서의 2단계 인증에 대한 항목을 참조하십시오.
- Horizon Client에서 서버 URL 정보 및 **도메인** 드롭다운 메뉴를 비롯한 보안 정보를 숨기려면 Horizon Administrator에서 **클라이언트 사용자 인터페이스에서 서버 정보 숨기기** 및 **클라이언트 사용자 인터페이스에서 도메인 목록 숨기기** 설정을 사용하도록 설정합니다. 이러한 전역 설정은 Horizon 7 버전 7.1 이상에서 사용할 수 있습니다. 전역 설정 구성에 대한 자세한 내용은 View 관리 문서를 참조하십시오.

  도메인 드롭다운 메뉴가 숨겨져 있을 때 인증을 받으려면 **사용자 이름** 텍스트 상자에 *domain*₩*username* 또는 *user*name@*domain* 형식으로 사용자 이름을 입력하여 도메인 정보를 제공해야 합니다.

  중요 **클라이언트 사용자 인터페이스에서 서버 정보 숨기기** 및 **클라이언트 사용자 인터페이스에서 도메인 목록 숨기기** 설정을 사용하도록 설정하고 연결 서버 인터페이스에 대해 2단계 인증(RSA SecureID 또는 RADIUS)을 선택하는 경우 Windows 사용자 이름 일치를 적용하지 마십시오. Windows 사용자 이름 일치를 적용하면 사용자가 사용자 이름 텍스트 상자에 도메인 정보를 입력할 수 없게 되며 로그인이 항상 실패합니다. 자세한 내용은 View 관리 문서의 2단계 인증에 대한 항목을 참조하십시오.
- Horizon Client에서 게시된 애플리케이션에 대해 인증되지 않은 액세스 권한을 제공하려면 연결 서버에서 이 기능을 사용하도록 설정해야 합니다. 자세한 내용은 View 관리 문서에서 인증되지 않은 액세스에 대한 항목을 참조하십시오.

서버 로그인에 사용된 마지막 사용자 이름 지우기

클라이언트 사용자 인터페이스에서 도메인 목록 숨기기 전역 설정이 사용되는 연결 서버 인스턴스에 사용자가 로그인하는 경우 **도메인** 드롭다운 메뉴가 Horizon Client에서 숨겨지며 사용자는 Horizon Client **사용자 이름** 텍스트 상자에 도메인 정보를 제공합니다. 예를 들어 사용자는 *domain*₩*username* 또는 *username*@*domain* 형식으로 사용자 이름을 입력해야 합니다.

Windows 클라이언트 시스템에서 레지스트리 키는 마지막 사용자 이름을 저장했다가 다음번에 사용자가 서버에 로그인하는 경우 **사용자 이름** 텍스트 상자에 마지막 사용자 이름을 표시할지 여부를 결정합니다. 마지막 사용자 이름이 **사용자 이름** 텍스트 상자에 표시되지 않도록 하고 도메인 정보를 제공하지 않으려면 Windows 클라이언트 시스템에서 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩System₩dontdisplaylastusername 레지스트리 키의 값을 1로 설정해야 합니다.

Horizon Client에 **도메인** 드롭다운 메뉴 및 서버 URL 정보를 비롯한 보안 정보 숨기기에 관한 자세한 내용은 View 관리 문서에서 전역 설정에 관한 항목을 참조하십시오.

VMware Blast 옵션 구성

VMware Blast 디스플레이 프로토콜을 사용하는 원격 데스크톱 및 애플리케이션 세션에 대해 H.264 디코딩 및 네트워크 상태 옵션을 구성할 수 있습니다.

지원되는 최대 해상도는 클라이언트의 그래픽 처리 장치(GPU) 성능에 따라 달라집니다. JPEG/PNG에 대한 4K 해상도를 지원하는 GPU가 H.264에 대한 4K 해상도는 지원하지 못할 수 있습니다. H.264에 대한 해상도가 지원되지 않는 경우 Horizon Client에서는 JPEG/PNG를 대신 사용합니다.

서버에 로그인한 후에는 네트워크 상태 옵션을 변경할 수 없습니다. 서버에 로그인하기 전 또는 후에 H.264 디코딩을 구성할 수 있습니다.

필수 조건

이 기능에는 Horizon Agent 7.0 이상이 필요합니다.

프로시저

1 메뉴 표시줄에서 **옵션** 버튼을 클릭하고 **VMware Blast 구성**을 선택합니다.

서버에 로그인한 경우 **설정**(톱니) 아이콘을 클릭하고 **VMware Blast**를 선택할 수 있습니다. 서버에 로그인한 후에는 네트워크 상태 옵션을 변경할 수 없습니다.

2 디코딩 및 네트워크 상태 옵션을 구성합니다.

옵션	조치
H.264	연결 서버에 연결하기 전 또는 후에 Horizon Client에서 H.264 디코딩을 허용하도록 이 옵션을 구성합니다. 이 옵션이 선택된 경우(기본 설정) 에이전트에서 H.264 소프트웨어 또는 하드웨어 인코딩을 지원한다면 Horizon Client에서 H.264 디코딩을 사용합니다. 에이전트에서 H.264 소프트웨어 또는 하드웨어 인코딩을 지원하지 않을 경우 Horizon Client에서 JPG/PNG 디코딩을 사용합니다. JPG/PNG 디코딩을 사용하려면 이 옵션을 선택 취소합니다.
최상의 환경을 위해 네트워크 상태를 선택하십시오.	연결 서버에 연결하기 전에만 이 옵션을 구성할 수 있습니다. 다음 네트워크 상태 옵션 중 하나를 선택합니다. ■ **매우 좋음** – Horizon Client가 TCP 네트워킹만 사용합니다. 이 옵션은 LAN 환경에 이상적입니다. ■ **일반(기본값)** – Horizon Client가 혼합 모드에서 작동합니다. 혼합 모드에서 Horizon Client는 서버에 연결할 때 TCP 네트워킹을 사용하고, 에이전트 및 Blast 보안 게이트웨이(사용되도록 설정된 경우)가 BEAT(Blast Extreme Adaptive Transport) 연결을 지원하는 경우 BEAT를 사용합니다. 이 옵션은 기본 설정입니다. ■ **나쁨** – Horizon Client는 서버에서 BEAT 터널 서버가 사용되도록 설정된 경우에만 BEAT 네트워킹을 사용하고 그렇지 않으면 혼합 모드로 전환됩니다. **참고** Horizon 7 버전 7.1 이하에서 연결 서버 및 보안 서버 인스턴스는 BEAT 터널 서버를 지원하지 않습니다. Unified Access Gateway 2.9 이상에서는 BEAT 터널 서버를 지원합니다. 연결 서버 및 보안 서버 인스턴스에 대한 Blast 보안 게이트웨이는 BEAT 네트워킹을 지원하지 않습니다.

3 변경 사항을 저장하려면 **확인**을 클릭합니다.

H.264의 변경 사항은 다음에 사용자가 원격 데스크톱이나 애플리케이션에 연결하고 VMware Blast 디스플레이 프로토콜을 선택할 때 적용됩니다. 변경 사항은 기존 VMware Blast 세션에 영향을 주지 않습니다.

Internet Explorer 프록시 설정 사용

Horizon Client는 Internet Explorer에 구성된 프록시 설정을 자동으로 사용합니다.

프록시 설정 우회

Horizon Client는 Internet Explorer 프록시 우회 설정을 사용하여 연결 서버 호스트, 보안 서버 또는 Unified Access Gateway 장치와의 HTTPS 연결을 우회합니다.

보안 터널이 연결 서버 호스트, 보안 서버 또는 Unified Access Gateway 장치에서 사용되도록 설정되어 있는 경우 Horizon Client 구성 ADM 또는 ADMX 템플릿 파일에서 터널 프록시 바이패스 주소 목록 그룹 정책 설정을 사용하여 터널 연결을 우회할 주소 목록을 지정해야 합니다. 프록시 서버는 이러한 주소에 사용되지 않습니다. 세미콜론(;)을 사용하여 여러 항목을 구분합니다. 이 그룹 정책 설정은 다음 레지스트리 키를 생성합니다.

```
HKEY_LOCAL_MACHINE₩SOFTWARE₩Policies₩VMware, Inc.₩VMware VDM₩Client₩TunnelProxyBypass
```

직접 연결에 이 그룹 정책 설정을 사용할 수 없습니다. 그룹 정책 설정이 예상대로 적용되지 않는 경우 로컬 주소에 대한 프록시 우회를 시도하십시오. 자세한 내용은 https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/의 내용을 참조하십시오.

프록시 페일오버

Horizon Client는 Internet Explorer에서 **인터넷 옵션 > 연결 > LAN 설정**에 있는 **자동 구성** 아래의 **자동 구성 스크립트 사용** 설정으로 프록시 페일오버를 지원합니다. 이 설정을 사용하려면 여러 프록시 서버를 반환하는 자동 구성 스크립트를 생성해야 합니다.

VMware에서 수집하는 Horizon Client 데이터

고객 환경 향상 프로그램에 참여하는 회사의 경우, VMware는 특정 Horizon Client 필드에서 데이터를 수집합니다. 민감한 정보가 포함된 필드는 익명으로 처리됩니다.

VMware는 하드웨어 및 소프트웨어 호환성에 대한 우선 순위를 지정하기 위해 클라이언트의 데이터를 수집합니다. 회사의 관리자가 고객 환경 향상 프로그램에 참여하기로 결정하면 VMware는 고객 요구 사항에 대한 VMware의 대응 개선을 위해 배포에 대한 익명 데이터를 수집합니다. 조직을 식별할 수 있는 데이터는 수집하지 않습니다. Horizon Client 정보는 먼저 연결 서버로 전송된 다음 연결 서버 인스턴스, 데스크톱 풀 및 원격 데스크톱의 데이터와 함께 VMware로 전송됩니다.

연결 서버로 전송되는 동안 정보가 암호화되지만 클라이언트 시스템에서 해당 정보는 사용자별 디렉토리에 암호화되지 않은 것으로 기록됩니다. 이 로그에는 개인적으로 식별할 수 있는 정보가 없습니다.

연결 서버를 설치하는 관리자가 연결 서버 설치 마법사를 실행하는 동안 VMware 고객 환경 향상 프로그램에 참여할지를 선택하거나 관리자가 설치 후에 Horizon Administrator의 옵션을 설정할 수 있습니다.

표 1-1. 고객 환경 향상 프로그램을 위해 Horizon Client에서 수집하는 데이터

설명	이 필드는 익명으로 처리됩니까?	예시 값
Horizon Client 애플리케이션을 제작한 회사	아니요	VMware
제품 이름	아니요	VMware Horizon Client
클라이언트 제품 버전	아니요	(형식은 x.x.x-yyyyyy이며, 여기서 x.x.x는 클라이언트 버전 번호이고 yyyyyy는 빌드 번호입니다.)
클라이언트 바이너리 아키텍처	아니요	예를 들면 다음과 같습니다. ■ i386 ■ x86_64 ■ arm
클라이언트 빌드 이름	아니요	예를 들면 다음과 같습니다. ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
호스트 운영 체제	아니요	예를 들면 다음과 같습니다. ■ Windows 8.1 ■ Windows 7, 64비트 서비스 팩 1(빌드 7601) ■ iPhone OS 5.1.1(9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
호스트 운영 체제 커널	아니요	예를 들면 다음과 같습니다. ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ 알 수 없음(Windows 스토어용)
호스트 운영 체제 아키텍처	아니요	예를 들면 다음과 같습니다. ■ x86_64 ■ i386 ■ armv71 ■ ARM

표 1-1. 고객 환경 향상 프로그램을 위해 Horizon Client에서 수집하는 데이터 (계속)

설명	이 필드는 익명으로 처리됩니까?	예시 값
호스트 시스템 모델	아니요	예를 들면 다음과 같습니다. ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
호스트 시스템 CPU	아니요	예를 들면 다음과 같습니다. ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ 알 수 없음(iPad용)
호스트 시스템 프로세서의 코어 수	아니요	예: 4
호스트 시스템의 메모리 양(MB)	아니요	예를 들면 다음과 같습니다. ■ 4096 ■ 알 수 없음(Windows 스토어용)
연결된 USB 디바이스 수	아니요	2(USB 디바이스 리디렉션은 Linux, Windows 및 Mac 클라이언트에서만 지원됩니다.)
최대 동시 USB 디바이스 연결 수	아니요	2
USB 디바이스 공급업체 ID	아니요	예를 들면 다음과 같습니다. ■ Kingston ■ NEC ■ Nokia ■ Wacom
USB 디바이스 제품 ID	아니요	예를 들면 다음과 같습니다. ■ DataTraveler ■ Gamepad ■ 스토리지 드라이브 ■ 무선 마우스
USB 디바이스 제품군	아니요	예를 들면 다음과 같습니다. ■ 보안 ■ 휴먼 인터페이스 디바이스 ■ 이미징
USB 디바이스 사용 횟수	아니요	(디바이스가 공유된 횟수)

Windows용 Horizon Client 설치

2

VMware 웹 사이트 또는 연결 서버에서 제공하는 웹 액세스 페이지에서 Windows 기반 Horizon Client 설치 관리자를 구할 수 있습니다. Horizon Client를 설치한 후 최종 사용자를 위해 다양한 시작 옵션을 설정할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

Windows 클라이언트 운영 체제에서 FIPS 모드 사용

FIPS(Federal Information Processing Standard) 규격 암호화를 사용하여 Horizon Client를 설치하려는 경우 Horizon Client 설치 관리자를 실행하기 전에 먼저 클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정해야 합니다.

클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정한 경우 애플리케이션은 FIPS-140을 준수하고 FIPS 승인 작동 모드를 준수하는 암호화 알고리즘만 사용합니다. 로컬 보안 정책에서 또는 그룹 정책의 일부로 특정 보안 설정을 사용하도록 설정하거나 Windows 레지스트리 키를 편집하여 FIPS 모드를 사용하도록 설정할 수 있습니다.

중요 FIPS 규격 암호화를 사용해서 Horizon Client를 설치하는 방식은 Windows 7 SP1 이상 운영 체제가 있는 클라이언트 시스템에서만 지원됩니다.

Horizon 6 버전 6.2 이상에서 사용할 수 있는 FIPS 지원에 대한 자세한 내용은 View 설치 문서를 참조하십시오.

FIPS 구성 속성 설정

클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정하려면 클라이언트 컴퓨터에 대해 Windows 그룹 정책 설정 또는 Windows 레지스트리 설정을 사용할 수 있습니다.

- 그룹 정책 설정을 사용하려면 그룹 정책 편집기를 열고 Computer Configuration₩Windows Settings₩Security Settings₩Local Policies₩Security Options로 이동한 후 **시스템 암호화: 암호화, 해시 및 서명에 대해 FIPS 규격 알고리즘 사용** 설정을 사용하도록 설정합니다.
- Windows 레지스트리를 사용하려면 HKLM₩System₩CurrentControlSet₩Control₩Lsa₩FipsAlgorithmPolicy₩Enabled로 이동한 후 **사용**을 [1]로 설정합니다.

FIPS 모드에 대한 자세한 내용을 보려면 https://support.microsoft.com/en-us/kb/811833 사이트로 이동하십시오.

중요 Horizon Client 설치 관리자를 실행하기 전에 FIPS 모드를 사용하도록 설정하지 않으면 사용자 지정 설치 중에 FIPS 규격 암호화를 사용하는 설치 관리자 옵션이 나타나지 않습니다. FIPS 규격 암호화는 일반 설치 중에 사용하도록 설정되지 않습니다. FIPS 규격 암호화 옵션을 사용하지 않고 Horizon Client를 설치하고 나중에 이 옵션을 사용하기로 결정한 경우 클라이언트를 제거하고 클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정한 후 Horizon Client 설치 관리자를 다시 실행해야 합니다.

Windows용 Horizon Client 설치

최종 사용자는 클라이언트 시스템에서 원격 데스크톱 및 원격 애플리케이션에 연결하기 위해 Horizon Client를 엽니다. Windows 기반 설치 관리자 파일을 실행하여 모든 Horizon Client 구성 요소를 설치할 수 있습니다.

이 절차는 대화식 설치 마법사를 사용하여 Horizon Client를 설치하는 방법에 대해 설명합니다. 명령줄에서 Horizon Client를 설치하려면 명령줄에서 Horizon Client 설치를 참조하십시오. URL 컨텐츠 리디렉션 기능을 설치하려면 명령줄에서 설치 관리자를 실행해야 합니다.

참고 View Agent 6.0 이상 또는 Horizon Agent 7.0 이상을 실행하는 원격 데스크톱 가상 시스템에 Horizon Client를 설치할 수 있습니다. 최종 사용자가 Windows 씬 클라이언트 디바이스에서 원격 애플리케이션에 액세스하는 기업의 경우 이 설치 전략을 사용할 수 있습니다.

필수 조건

- 클라이언트 시스템에서 지원되는 운영 체제를 사용하는지 확인하십시오. Windows 클라이언트 시스템 요구 사항를 참조하십시오.
- Horizon Client 설치 관리자가 포함된 다운로드 페이지 URL이 있는지 확인합니다. 이 URL은 http://www.vmware.com/go/viewclients의 VMware 다운로드 페이지이거나 연결 서버 인스턴스의 URL일 수 있습니다.
- 클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.

- 도메인 컨트롤러에 최신 패치가 적용되었고 여유 디스크 공간이 있으며 서로 간에 통신이 가능한지 확인하십시오. 그렇지 않을 경우 Windows 8.1 시스템에서 설치 관리자를 실행하면 설치 관리자가 완료될 때까지 비정상적으로 오래 걸릴 수 있습니다. 이 문제는 시스템의 도메인 컨트롤러 또는 해당 계층 내 존재하는 다른 도메인 컨트롤러가 응답하지 않거나 연결할 수 없을 때 발생합니다.
- FIPS 규격 암호화를 사용하여 Horizon Client를 설치하려는 경우 Horizon Client 설치 관리자를 실행하기 전에 먼저 클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정합니다. Windows 클라이언트 운영 체제에서 FIPS 모드 사용를 참조하십시오.
- **USB 리디렉션** 구성 요소를 설치하려는 경우 다음을 수행합니다.
  - 클라이언트 디바이스 사용자가 원격 데스크톱에서 로컬로 연결된 USB 디바이스에 액세스할 수 있도록 허용할지 결정합니다. 액세스가 허용되지 않는 경우 **USB 리디렉션** 구성 요소를 설치하지 않거나 설치한 후 그룹 정책 설정을 사용하여 이를 사용하지 않도록 설정합니다. 그룹 정책을 사용하여 USB 리디렉션을 사용하지 않도록 설정하는 경우 나중에 클라이언트에 대해 USB 리디렉션을 사용하도록 설정할 때 Horizon Client를 다시 설치할 필요가 없습니다. 자세한 내용은 클라이언트 GPO에 대한 스크립팅 정의 설정의 내용을 참조하십시오.
  - 클라이언트 컴퓨터에서 Windows 자동 업데이트 기능이 해제되어 있는지 확인합니다.
- 최종 사용자가 현재 로그인한 사용자로서 Horizon Client와 원격 데스크톱에 로그인할 수 있도록 허용하는 기능을 사용할지 여부를 결정합니다. 사용자가 클라이언트 시스템에 로그인할 때 입력한 자격 증명 정보가 연결 서버 인스턴스 그리고 최종적으로 원격 데스크톱에 전달됩니다. 일부 클라이언트 운영 체제에서는 이 기능을 지원하지 않습니다.
- 최종 사용자에게 연결 서버 인스턴스의 FQDN(정규화된 도메인 이름)을 제공하도록 요청하지 않으려면 설치하는 동안 이를 제공할 수 있도록 FQDN을 확인합니다.

프로시저

1. 클라이언트 시스템에 관리자로 로그인합니다.
2. http://www.vmware.com/go/viewclients의 VMware 제품 페이지로 이동합니다.
3. 설치 관리자 파일(예: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe)을 다운로드합니다.

   xxxxxx는 빌드 번호이고 y.y.y는 버전 번호입니다.
4. 설치 관리자 파일을 두 번 클릭하여 설치를 시작합니다.

5 설치 유형을 선택하고 메시지에 따라 진행합니다.

옵션	조치
일반 설치	**동의 및 설치**를 클릭합니다. 설치 관리자는 USB 리디렉션 및 현재 사용자로 로그인 기능을 설치합니다.
사용자 지정 설치	**설치 사용자 지정**을 클릭하고 설치할 기능을 선택합니다. 기본 위치가 아닌 설치 위치를 지정하거나, IPv6 인터넷 프로토콜을 사용하거나, 기본 연결 서버 인스턴스를 구성하거나, 기본 로그인 동작을 구성하거나, FIPS 규격 암호화를 사용하도록 설정하거나, 64비트 시스템에 32비트 코어 원격 환경 구성 요소를 설치하거나, 비즈니스용 Skype의 가상화 팩 기능을 설치하려면 이 옵션을 선택해야 합니다. FIPS 규격 암호화 사용자 지정 설치 옵션은 클라이언트 운영 체제에서 FIPS 모드가 사용되도록 설정된 경우에만 설치 관리자에서 사용할 수 있습니다. 사용자 지정 기능을 선택할 때는 다음 지침을 따르십시오. ■ Horizon 환경의 모든 구성 요소가 IPv6 인터넷 프로토콜을 사용하지는 않을 경우 **IPv6** 옵션을 선택하지 마십시오. IPv6 환경에서는 특정 기능을 사용할 수 없습니다. 자세한 내용은 View 설치 문서를 참조하십시오. ■ 64비트 클라이언트 시스템에 제품용 64비트 플러그인이 없는 경우 **64비트 시스템의 32비트 코어 원격 환경** 기능을 선택합니다. 이 기능을 선택하는 경우 비즈니스용 Skype의 가상화 팩 기능을 설치할 수 없습니다.

특정 기능을 사용하려면 클라이언트 시스템을 다시 시작해야 합니다.

설치 관리자는 VMware Horizon Client(horizon_client_service) 및 VMware USB Arbitration Service(VMUSBArbService)를 포함하여 특정 Windows 서비스를 설치합니다.

후속 작업

Horizon Client를 시작하고 올바른 원격 데스크톱 또는 애플리케이션에 로그인할 수 있는지 확인합니다. 원격 데스크톱 또는 애플리케이션에 연결를 참조하십시오.

명령줄에서 Horizon Client 설치

명령줄에 설치 관리자 파일 이름, 설치 명령 및 설치 속성을 입력하여 Horizon Client를 설치할 수 있습니다.

명령줄에서 Horizon Client를 설치할 경우 자동 설치를 수행할 수 있습니다. 자동 설치를 사용하면 대규모 기업에서 Horizon Client를 효과적으로 배포할 수 있습니다.

Horizon Client 에 대한 설치 명령

명령줄에서 Horizon Client를 설치할 경우 특정 설치 명령을 지정할 수 있습니다.

다음 표에서는 Horizon Client 설치 명령에 대해 설명합니다.

표 2-1. Horizon Client 설치 명령

명령	설명
/? 또는 /help	Horizon Client 설치 명령 및 속성을 나열합니다.
/silent	Horizon Client를 자동으로 설치합니다. 마법사 프롬프트에 응답할 필요가 없습니다.

표 2-1. Horizon Client 설치 명령 (계속)

명령	설명
/install	Horizon Client를 대화식으로 설치합니다. 마법사 프롬프트에 응답해야 합니다.
/uninstall	Horizon Client를 제거합니다.
/repair	Horizon Client를 복구합니다.
/norestart	설치 프로세스 동안 모든 다시 시작 및 다시 시작 프롬프트를 표시하지 않습니다.
/x /extract	설치 관리자 패키지의 압축을 %TEMP% 디렉토리에 풉니다.

Horizon Client 에 대한 설치 속성

명령줄에서 Horizon Client를 설치할 경우 특정 설치 속성을 지정할 수 있습니다.

다음 표에서는 Horizon Client 설치 속성에 대해 설명합니다.

표 2-2. Horizon Client 설치 속성

속성	설명	기본값
INSTALLDIR	Horizon Client가 설치된 경로 및 폴더입니다. 예: INSTALLDIR=""D:₩abc₩my folder"" 해당 경로를 둘러싸고 있는 큰따옴표 쌍은 설치 관리자가 공백을 경로의 유효한 부분으로 해석하도록 합니다.	%ProgramFiles %₩VMware₩VMware Horizon View Client
VDM_IP_PROTOCOL_USAGE	Horizon Client 구성 요소가 통신에 사용하는 IP(네트워크 프로토콜) 버전을 지정합니다. 가능한 값은 IPv4 및 IPv6입니다.	IPv4
VDM_FIPS_ENABLED	FIPS 규격 암호화를 사용하여 Horizon Client를 설치할지 여부를 지정합니다. 값 1은 FIPS 규격 암호화를 사용하여 Horizon Client를 설치합니다. 값 0은 FIPS 규격 암호화를 사용하지 않고 Horizon Client를 설치합니다. **참고** 이 속성을 1로 설정하기 전에 먼저 Windows 클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정해야 합니다. Windows 클라이언트 운영 체제에서 FIPS 모드 사용를 참조하십시오.	0
VDM_SERVER	Horizon Client 사용자가 기본적으로 연결되는 연결 서버 인스턴스의 정규화된 도메인 이름(FQDN)입니다. 예: VDM_Server=cs1.companydomain.com 이 속성을 구성할 때 Horizon Client 사용자는 이 FQDN을 제공하지 않아도 됩니다.	없음

표 2-2. Horizon Client 설치 속성 (계속)

속성	설명	기본값
LOGINASCURRENTUSER_DISPLAY	Horizon Client 메뉴 표시줄의 **옵션** 메뉴에 **현재 사용자로 로그인**을 표시할지를 결정합니다. 올바른 값은 1(사용) 또는 0(사용 안 함)입니다.	1
LOGINASCURRENTUSER_DEFAULT	Horizon Client 메뉴 표시줄의 **옵션** 메뉴에 **현재 사용자로 로그인**이 기본적으로 선택되도록 할지를 결정합니다. 올바른 값은 1(사용) 및 0(사용 안 함)입니다. 현재 사용자로 로그인이 기본 로그인 동작인 경우, 클라이언트 시스템에 로그인할 때 사용자가 제공한 ID 및 자격 증명 정보가 연결 서버 인스턴스로 전달되고 최종적으로 원격 데스크톱으로 전달됩니다. 현재 사용자로 로그인이 기본 로그인 동작이 아닌 경우 사용자는 원격 데스크톱 또는 애플리케이션에 액세스하기 위해 ID 및 자격 증명 정보를 여러 번 제공해야 합니다.	0
ADDLOCAL	자동 설치로 설치할 기능을 지정합니다. 올바른 값은 다음과 같습니다. ■ ALL - URL 컨텐츠 리디렉션을 제외하고 사용 가능한 모든 기능을 설치합니다. ■ TSSO - 현재 사용자로 로그인 기능을 설치합니다. ■ USB - USB 리디렉션 기능을 설치합니다. 개별 기능을 지정하려면 기능 이름 목록을 쉼표로 구분하여 입력합니다. 이름 사이에 공백을 사용하지 마십시오. 예를 들어 USB 리디렉션 기능과 함께 Horizon Client를 설치하려고 하지만, 현재 사용자로 로그인 기능을 사용하지 않으려면 다음 명령을 입력하십시오. VMware-Horizon-Client-*y.y.y-xxxxxx*.exe /silent ADDLOCAL=USB	없음
INSTALL_32BITRMKS	64비트 클라이언트 시스템에서 32비트 코어 원격 환경 구성 요소를 설치할지 여부를 지정합니다. 1 값을 지정하면 32비트 코어 원격 환경 구성 요소가 설치됩니다. 0 값을 지정하면 64비트 코어 원격 환경 구성 요소가 설치됩니다. 64비트 클라이언트 시스템에 제품용 64비트 플러그인이 없는 경우 32비트 코어 원격 환경 구성 요소를 설치합니다. 이 속성은 32비트 클라이언트 시스템에서 유효하지 않습니다.	0

표 2-2. Horizon Client 설치 속성 (계속)

속성	설명	기본값
INSTALL_SFB	비즈니스용 Skype에 대한 VMware Virtulization Pack 기능을 설치할지 여부를 지정합니다. 1 값은 기능을 설치합니다. 0 값은 기능을 설치하지 않습니다. 이 기능은 32비트 코어 원격 환경 구성 요소(INSTALL_32BITRMKS=1)와 호환되지 않습니다.	0
URL_FILTERING_ENABLED	URL 컨텐츠 리디렉션 기능 설치 여부를 지정합니다. 1 값은 기능을 설치합니다. 0 값은 기능을 설치하지 않습니다. 대화식 설치에서 이 속성을 1로 설정하면 사용자 지정 설치 대화 상자에서 [추가 기능] 아래에 **URL 컨텐츠 리디렉션** 확인란이 표시되고 기본적으로 선택됩니다. 이 속성을 1로 설정하지 않으면 이 확인란이 표시되지 않습니다. **참고** ADDLOCAL=ALL 속성에는 [URL 컨텐츠 리디렉션] 기능이 포함되지 않습니다.	0

명령줄에서 Horizon Client 설치

설치 관리자 파일 이름을 입력하고 설치 명령 및 속성을 지정하여 명령줄에서 Horizon Client를 설치할 수 있습니다. 명령줄에서 Horizon Client를 자동으로 설치할 수 있습니다.

필수 조건

- 클라이언트 시스템에서 지원되는 운영 체제를 사용하는지 확인하십시오. Windows 클라이언트 시스템 요구 사항를 참조하십시오.
- 클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.
- 도메인 컨트롤러에 최신 패치가 적용되었고 여유 디스크 공간이 있으며 서로 간에 통신이 가능한지 확인하십시오. 그렇지 않을 경우 Windows 8.1 시스템에서 설치 관리자를 실행하면 설치 관리자가 완료될 때까지 비정상적으로 오래 걸릴 수 있습니다. 이 문제는 시스템의 도메인 컨트롤러 또는 해당 계층 내 존재하는 다른 도메인 컨트롤러가 응답하지 않거나 연결할 수 없을 때 발생합니다.
- FIPS 규격 암호화를 사용하여 Horizon Client를 설치하려는 경우 Horizon Client 설치 관리자를 실행하기 전에 먼저 클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정합니다. Windows 클라이언트 운영 체제에서 FIPS 모드 사용를 참조하십시오.
- 최종 사용자가 현재 로그인한 사용자로서 Horizon Client와 원격 데스크톱에 로그인할 수 있도록 허용하는 기능을 사용할지 여부를 결정합니다. 사용자가 클라이언트 시스템에 로그인할 때 입력한 자격 증명 정보가 연결 서버 인스턴스 그리고 최종적으로 원격 데스크톱에 전달됩니다. 일부 클라이언트 운영 체제에서는 이 기능을 지원하지 않습니다.
- Horizon Client 설치 명령을 숙지해야 합니다. Horizon Client에 대한 설치 명령를 참조하십시오.
- Horizon Client 설치 속성을 숙지해야 합니다. Horizon Client에 대한 설치 속성를 참조하십시오.

- 최종 사용자가 원격 데스크톱에서 로컬로 연결된 USB 디바이스에 액세스할 수 있는지 확인합니다. 액세스할 수 없으면 ADDLOCAL 설치 속성을 기능 목록으로 설정하고 USB 기능을 생략합니다. 자세한 내용은 Horizon Client에 대한 설치 속성의 내용을 참조하십시오.
- 최종 사용자에게 연결 서버 인스턴스의 FQDN(정규화된 도메인 이름)을 제공하도록 요청하지 않으려면 설치하는 동안 이를 제공할 수 있도록 FQDN을 확인합니다.

프로시저

1 클라이언트 시스템에 관리자로 로그인합니다.

2 http://www.vmware.com/go/viewclients의 VMware 제품 페이지로 이동합니다.

3 Horizon Client 설치 관리자 파일(예: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe)을 다운로드합니다.

xxxxxx는 빌드 번호이고 y.y.y는 버전 번호입니다.

4 Windows 클라이언트 컴퓨터에서 명령 프롬프트를 엽니다.

5 설치 관리자 파일 이름, 설치 명령 및 설치 속성을 한 줄에 입력합니다.

VMware-Horizon-Client-*y.y.y-xxxxxx*.exe [*commands*] [*properties*]

설치 관리자는 사용자가 지정한 설치 명령 및 속성에 따라 Horizon Client를 설치합니다. /silent 설치 명령을 지정하면 마법사 프롬프트가 나타나지 않습니다.

설치 관리자는 VMware Horizon Client(horizon_client_service) 및 VMware USB Arbitration Service(VMUSBArbService)를 포함하여 특정 Windows 서비스를 설치합니다.

예: 설치 명령

다음 명령은 Horizon Client를 대화식으로 설치하고 URL 컨텐츠 리디렉션 기능을 사용하도록 설정합니다.

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

다음 명령은 Horizon Client를 자동으로 설치하고, 설치 프로세스 동안 모든 다시 시작 및 다시 시작 프롬프트를 표시하지 않습니다.

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /norestart
```

후속 작업

Horizon Client를 설치할 때 URL 컨텐츠 리디렉션 기능을 사용하도록 설정한 경우 해당 기능이 설치되었는지 확인합니다. URL 컨텐츠 리디렉션 설치 확인를 참조하십시오.

Horizon Client를 시작하고 올바른 원격 데스크톱 또는 애플리케이션에 로그인할 수 있는지 확인합니다. 원격 데스크톱 또는 애플리케이션에 연결를 참조하십시오.

URL 컨텐츠 리디렉션 설치 확인

Horizon Client를 설치할 때 URL 컨텐츠 리디렉션 기능을 사용하도록 설정한 경우 해당 기능이 설치되었는지 확인하십시오.

필수 조건

Horizon Client를 설치할 때 URL_FILTERING_ENABLED=1 설치 속성을 지정합니다. 명령줄에서 Horizon Client 설치를 참조하십시오.

프로시저

1 클라이언트 시스템에 로그인합니다.

2 %PROGRAMFILES%₩VMware₩VMware Horizon View Client₩ 디렉토리로 이동한 후 vmware-url-protocol-launch-helper.exe 및 vmware-url-filtering-plugin.dll 파일이 해당 디렉토리에 설치되어 있는지 확인합니다.

3 클라이언트 시스템의 Internet Explorer에서 VMware Horizon View URL 필터링 플러그인 추가 기능이 설치되어 있는지와 사용되도록 설정되어 있는지 확인합니다.

온라인으로 Horizon Client 업그레이드

온라인 업그레이드 기능이 사용되도록 설정된 경우 온라인으로 Horizon Client를 업그레이드할 수 있습니다. 이 기능은 기본적으로 사용하지 않도록 설정됩니다.

그룹 정책 설정 Enable Horizon Client online update 및 URL for Horizon Client online update를 수정하여 이 기능을 사용하도록 설정할 수 있습니다. 자세한 내용은 클라이언트 GPO에 대한 일반 설정의 내용을 참조하십시오.

필수 조건

- Horizon Client를 업데이트하기 전에 작업을 저장합니다. 업데이트로 인해 시스템이 재부팅될 수 있습니다.
- 클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.

프로시저

1 관리자로 로그인합니다.

2 Horizon Client에서 두 화면 중 하나에 있는 **소프트웨어 업데이트**를 클릭합니다.

Horizon Client 화면	조치
연결 서버에 연결하기 전	**옵션 > 소프트웨어 업데이트**를 클릭합니다.
연결 서버에 연결한 후	**도움말 > 소프트웨어 업데이트**를 클릭합니다.

3 **업데이트 확인**을 클릭합니다.

4 **다운로드 및 설치**를 클릭합니다.

최종 사용자를 위한 Horizon Client 구성

3

최종 사용자를 위해 Horizon Client를 구성하는 작업에는 Horizon Client를 시작하도록 URI를 구성하고, 인증서 확인 모드를 구성하고, 고급 TLS/SSL 옵션을 설정하고, 그룹 정책 ADMX 템플릿 파일을 사용하여 사용자 지정 설정을 구성하는 작업이 포함될 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

일반 구성 설정

Horizon Client는 여러 구성 메커니즘을 제공하여 최종 사용자를 위한 로그인 및 데스크톱 선택 환경을 간소화하고 보안 정책을 적용합니다.

다음 표에는 하나 이상의 방법으로 설정 가능한 구성 설정 중 일부만 나열되어 있습니다.

표 3-1. 일반 구성 설정

설정	구성 메커니즘
연결 서버 주소	URI, 그룹 정책, 명령줄, Windows 레지스트리
Active Directory 사용자 이름	URI, 그룹 정책, 명령줄, Windows 레지스트리
도메인 이름	URI, 그룹 정책, 명령줄, Windows 레지스트리
데스크톱 디스플레이 이름	URI, 그룹 정책, 명령줄
창 크기	URI, 그룹 정책, 명령줄
디스플레이 프로토콜	URI, 명령줄

표 3-1. 일반 구성 설정 (계속)

설정	구성 메커니즘
인증서 검사 구성	그룹 정책, Windows 레지스트리
SSL 프로토콜 및 암호화 알고리즘 구성	그룹 정책, Windows 레지스트리

URI를 사용하여 Horizon Client 구성

URI(Uniform Resource Identifier)를 사용하면 Horizon Client를 시작하고 서버에 연결하며 특정 구성 옵션으로 특정 데스크톱 또는 애플리케이션을 열기 위해 최종 사용자가 클릭하는 링크가 포함된 웹 페이지나 이메일을 만들 수 있습니다.

최종 사용자를 위한 웹 또는 e-메일 링크를 생성하여 원격 데스크톱 또는 애플리케이션에 연결하는 프로세스를 간소화할 수 있습니다. 다음 정보의 일부 또는 전체를 제공하는 URI를 구성하여 이러한 링크를 생성해야 최종 사용자가 정보를 제공할 필요가 없어집니다.

- 연결 서버 주소
- 연결 서버의 포트 번호
- Active Directory 사용자 이름
- RADIUS 또는 RSA SecurID 사용자 이름(Active Directory 사용자 이름과 다른 경우)
- 도메인 이름
- 데스크톱 또는 애플리케이션 디스플레이 이름
- 창 크기
- 세션 재설정, 로그아웃, 시작 등의 작업
- 디스플레이 프로토콜
- USB 디바이스 리디렉션 옵션

URI를 구성하려면 Horizon Client 특정 경로 및 쿼리 부분으로 vmware-view URI 구성표를 사용합니다.

참고 클라이언트 소프트웨어가 클라이언트 컴퓨터에 이미 설치된 경우에만 URI를 사용하여 Horizon Client를 시작할 수 있습니다.

vmware-view URI 생성을 위한 구문

구문에는 vmware-view URI 구성표, 데스크톱 또는 애플리케이션을 지정하는 경로 부분 및 선택적으로 데스크톱 또는 애플리케이션 작업이나 구성 옵션을 지정하는 쿼리가 있습니다.

URI 사양

다음 구문을 사용하여 Horizon Client 시작에 필요한 URI를 만듭니다.

```
vmware-view://[authority-part][/path-part][?query-part]
```

필수 요소는 URI 구성표 vmware-view뿐입니다. 클라이언트 운영 체제 중 일부 버전에서는 구성표 이름의 대소문자를 구분합니다. 그러니, 반드시 vmware-view를 사용하십시오.

중요 모든 부분의 비ASCII 문자는 우선 UTF-8[STD63]에 따라 인코딩되어야 하며 해당 UTF-8 시퀀스의 각 8진수는 URI 문자로 표현되도록 퍼센트로 인코딩되어야 합니다.

ASCII 문자 인코딩에 대한 자세한 내용은 http://www.utf8-chartable.de/의 URL 인코딩 참조를 참고하십시오.

authority-part

서버 주소를 지정하고 선택적으로 사용자 이름, 기본값이 아닌 포트 번호 또는 두 가지 모두를 지정합니다. 서버 이름에는 밑줄(_)을 사용할 수 없습니다. 서버 이름은 DNS 구문에 따라야 합니다.

사용자 이름을 지정하려면 다음 구문을 사용하십시오.

```
user1@server-address
```

도메인을 포함하는 UPN 주소는 지정할 수 없습니다. 도메인을 지정하려면 URI에서 domainName 쿼리 부분을 사용할 수 있습니다.

포트 번호를 지정하려면 다음 구문을 사용하십시오.

```
server-address:port-number
```

path-part

데스크톱 또는 애플리케이션을 지정합니다. 데스크톱 디스플레이 이름 또는 애플리케이션 디스플레이 이름을 사용합니다. 이 이름은 데스크톱 또는 애플리케이션 풀이 생성될 때 Horizon Administrator에서 지정한 이름입니다. 디스플레이 이름에 공백이 있는 경우 %20 인코딩 메커니즘을 사용하여 공백을 나타냅니다.

query-part

사용할 구성 옵션이나 수행할 데스크톱 또는 애플리케이션 작업을 지정합니다. 쿼리는 대소문자를 구분하지 않습니다. 여러 쿼리를 사용하려면 쿼리 사이에 앰퍼샌드(&)를 사용합니다. 쿼리가 서로 충돌할 경우, 목록의 마지막 쿼리가 사용됩니다. 다음 구문을 사용하십시오.

```
query1=value1[&query2=value2...]
```

지원되는 쿼리

이 항목에는 이러한 Horizon Client 유형을 지원하는 쿼리가 나열됩니다. 데스크톱 클라이언트 및 모바일 클라이언트 등과 같은 여러 유형의 클라이언트에 대한 URI를 생성하는 경우 각 유형의 클라이언트 시스템에 대한 VMware Horizon Client 사용 설명서를 참조하십시오.

작업

표 3-2. 작업 쿼리와 함께 사용할 수 있는 값

값	설명
browse	지정된 서버에서 호스트된 사용 가능한 데스크톱 및 애플리케이션 목록을 표시합니다. 이 작업을 사용하면서 데스크톱 또는 애플리케이션을 지정할 필요는 없습니다.
start-session	지정된 데스크톱 또는 애플리케이션을 엽니다. 작업 쿼리가 제공되지 않고 데스크톱 또는 애플리케이션 이름이 제공되는 경우, start-session이 기본 작업입니다.
reset	지정된 데스크톱 또는 원격 애플리케이션을 종료하고 다시 시작합니다. 저장하지 않은 데이터는 손실됩니다. 원격 데스크톱 재설정은 PC에 있는 재설정 버튼을 누르는 것과 같습니다.
restart	지정된 데스크톱을 종료하고 다시 시작합니다. 원격 데스크톱을 다시 시작하는 것은 Windows 운영 체제 다시 시작 명령을 사용하는 것과 같습니다. 다시 시작되기 전에 저장하지 않은 데이터를 저장하라는 메시지가 일반적으로 운영 체제에 표시됩니다.
logoff	원격 데스크톱의 게스트 운영 체제에서 사용자를 로그아웃시킵니다. 애플리케이션을 지정하는 경우 작업을 무시하거나 최종 사용자에게 "잘못된 URI 작업"이라는 경고 메시지가 나타납니다.

args

원격 애플리케이션 실행에 추가할 명령줄 인수를 지정합니다. 구문 args=값을 사용합니다. 여기서 값은 문자열입니다. 다음 문자에는 % 인코딩을 사용하십시오.

- 콜론(:)에는 %3A를 사용합니다.
- 백슬래시(\)에는 %5C를 사용합니다.
- 공백( )에는 %20을 사용합니다.
- 큰따옴표 표시(")에는 %22를 사용합니다.

예를 들어 Notepad++ 애플리케이션에 대해 파일 이름 "My new file.txt"를 지정하려면 %22My%20new%20file.txt%22를 사용합니다.

appProtocol

원격 애플리케이션의 경우 올바른 값은 PCOIP 및 BLAST입니다. 예를 들어 PCoIP를 지정하려면 appProtocol=PCOIP 구문을 사용합니다.

connectUSBOnInsert

디바이스를 플러그인할 때 USB 디바이스를 포그라운드 가상 데스크톱에 연결합니다. 이 쿼리는 unattended 쿼리를 지정할 경우 암시적으로 설정됩니다. 이 쿼리를 사용하려면 action 쿼리를 start-session으로 설정하거나 아니면 action 쿼리가 없어야 합니다. 올바른 값은 true와 false입니다. 구문의 예는 connectUSBOnInsert=true입니다.

connectUSBOnStartup

클라이언트 시스템에 현재 연결되어 있는 모든 USB 디바이스를 데스크톱으로 리디렉션합니다. 이 쿼리는 unattended 쿼리를 지정할 경우 암시적으로 설정됩니다. 이 쿼리를 사용하려면 action 쿼리를 **start-session**으로 설정하거나 아니면 action 쿼리가 없어야 합니다. 올바른 값은 **true**와 **false**입니다. 구문의 예는 **connectUSBOnStartup=true**입니다.

desktopLayout

원격 데스크톱을 표시하는 창의 크기를 설정합니다. 이 쿼리를 사용하려면 action 쿼리를 **start-session**으로 설정하거나 아니면 action 쿼리가 없어야 합니다.

표 3-3. desktopLayout 쿼리의 올바른 값

값	설명
fullscreen	한 모니터에 전체 화면으로 표시합니다. 이 값은 기본값입니다.
multimonitor	모든 모니터에 전체 화면으로 표시합니다.
windowLarge	큰 창입니다.
windowSmall	작은 창입니다.
WxH	너비와 높이를 픽셀 단위로 지정하는 사용자 지정 해상도입니다. 구문의 예는 **desktopLayout=1280x800**입니다.

desktopProtocol

원격 데스크톱의 경우 올바른 값은 **RDP**, **PCOIP** 및 **BLAST**입니다. 예를 들어 PCoIP를 지정하려면 **desktopProtocol=PCOIP** 구문을 사용합니다.

domainName

원격 데스크톱 또는 애플리케이션에 연결 중인 사용자와 연결된 NETBIOS 도메인 이름입니다. 예를 들어 mycompany.com보다는 mycompany를 사용할 수 있습니다.

filePath

원격 애플리케이션에서 열려는 파일의 로컬 시스템 경로를 지정합니다. 드라이브 문자를 포함하는 전체 경로를 사용해야 합니다. 다음 문자에는 % 인코딩을 사용하십시오.

- 콜론(:)에는 **%3A**를 사용합니다.
- 백슬래시(\)에는 **%5C**를 사용합니다.
- 공백( )에는 **%20**을 사용합니다.

예를 들어 파일 경로 C:₩test file.txt를 나타내려면 **C%3A%5Ctest%20file.txt**를 사용하십시오.

tokenUserName

RSA 또는 RADIUS 사용자 이름을 지정합니다. RSA 또는 RADIUS 사용자 이름이 Active Directory 사용자 이름과 다른 경우에만 이 쿼리를 사용합니다. 이 쿼리를 지정하지 않고 RSA 또는 RADIUS 인증이 필요한 경우, Windows 사용자 이름을 사용합니다. 구문은 **tokenUserName=*name***입니다.

unattended	키오스크 모드에서 원격 데스크톱에 대해 서버 연결을 설정합니다. 이 쿼리를 사용하는 경우 클라이언트 디바이스의 MAC 주소에서 계정 이름을 생성했다면 사용자 정보를 지정하지 마십시오. 그러나 "custom-"으로 시작하는 이름과 같이 ADAM에서 사용자 지정 계정 이름을 생성한 경우 계정 정보를 지정해야 합니다.
useExisting	이 옵션이 true로 설정되어 있으면 Horizon Client 인스턴스를 하나만 실행할 수 있습니다. 사용자가 두 번째 서버에 연결하려고 할 경우에는 첫 번째 서버에서 로그아웃하여 데스크톱 및 애플리케이션 세션을 연결 해제해야 합니다. 이 옵션이 false로 설정되어 있으면 여러 Horizon Client 인스턴스를 실행할 수 있으며 사용자가 동시에 여러 서버에 연결할 수 있습니다. 기본값은 true입니다. 구문의 예는 useExisting=false입니다.
unauthenticatedAccessEnabled	이 옵션을 true로 설정하면 인증되지 않은 액세스 기능이 기본적으로 사용되도록 설정됩니다. **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 옵션이 사용자 인터페이스에 표시되며 선택됩니다. 이 옵션을 false로 설정하면 인증되지 않은 액세스 기능이 사용되지 않도록 설정됩니다. **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정이 숨겨지고 사용되지 않도록 설정됩니다. 이 옵션을 ""로 설정하면 인증되지 않은 액세스 기능이 사용되지 않도록 설정되고 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정이 사용자 인터페이스에서 숨겨지고 사용되지 않도록 설정됩니다. 구문 예는 unauthenticatedAccessEnabled=true입니다.
unauthenticatedAccessAccount	인증되지 않은 액세스 기능이 사용되도록 설정되면 사용할 계정을 설정합니다. 인증되지 않은 액세스가 사용되지 않도록 설정되면 이 쿼리는 무시됩니다. anonymous1 사용자 계정을 사용할 때의 구문 예는 unauthenticatedAccessAccount=anonymous1입니다.

vmware-view URI의 예

vmware-view URI 구성표를 사용하여 하이퍼텍스트 링크나 버튼을 만들고 e-메일 또는 웹 페이지에 이러한 링크를 포함할 수 있습니다. 예를 들어 최종 사용자가 이러한 링크를 클릭하여 특정 원격 데스크톱을 지정된 시작 옵션으로 열 수 있습니다.

URI 구문 예

각 URI 예에는 최종 사용자가 URI 링크를 클릭할 경우 나타나는 내용에 대한 설명이 이어집니다.

1
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session
```

Horizon Client가 시작되며 view.mycompany.com 서버에 연결됩니다. 로그인 상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인에 성공하고 나면 클라이언트는 디스플레이 이름이 **Primary Desktop**(기본 데스크톱)으로 표시되는 데스크톱에 연결되고 사용자는 게스트 운영 체제에 로그인됩니다.

참고 기본 디스플레이 프로토콜 및 창 크기가 사용됩니다. 기본 디스플레이 프로토콜은 PCoIP입니다. 기본 창 크기는 전체 화면입니다.

2
```
vmware-view://view.mycompany.com:7555/Primary%20Desktop
```

예를 들어 연결 서버의 비기본 포트 7555를 사용하는 것을 제외하면 이 URI는 이전 예와 동일한 효과를 가집니다. 기본 포트는 443입니다. 데스크톱 식별자가 제공되므로 start-session 작업이 URI에 포함되지 않아도 데스크톱이 열립니다.

3
```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP
```

Horizon Client가 시작되며 view.mycompany.com 서버에 연결됩니다. 로그인 상자에서 **사용자 이름** 텍스트 상자에 **fred**라는 이름이 채워집니다. 사용자는 도메인 이름 및 암호를 제공해야 합니다. 성공적으로 로그인되면 클라이언트는 디스플레이 이름이 **Finance Desktop**(재무 데스크톱)인 데스크톱에 연결되고 사용자는 게스트 운영 체제에 로그인됩니다. 연결에는 PCoIP 디스플레이 프로토콜이 사용됩니다.

4
```
vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST
```

Horizon Client가 시작되며 view.mycompany.com 서버에 연결됩니다. 로그인 상자에 사용자가 이름, 도메인 이름 및 암호를 입력해야 합니다. 로그인에 성공하면 클라이언트는 디스플레이 이름이 **Calculator(계산기)**인 애플리케이션에 연결됩니다. 이 연결은 VMware Blast 디스플레이 프로토콜을 사용합니다.

5
```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany
```

Horizon Client가 시작되며 view.mycompany.com 서버에 연결됩니다. 로그인 상자에서 **사용자 이름** 텍스트 상자에 **fred**라는 이름이 채워지고 **도메인** 텍스트 상자는 **mycompany**로 채워집니다. 사용자는 암호만 제공해야 합니다. 성공적으로 로그인되면 클라이언트는 디스플레이 이름이 **Finance Desktop**(재무 데스크톱)인 데스크톱에 연결되고 사용자는 게스트 운영 체제에 로그인됩니다.

6
```
vmware-view://view.mycompany.com/
```

Horizon Client가 시작되며 view.mycompany.com 서버에 연결하기 위한 로그인 메시지가 나타납니다.

7
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
```

Horizon Client가 시작되며 view.mycompany.com 서버에 연결됩니다. 로그인 상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인에 성공하면 Horizon Client에서 Primary Desktop(기본 데스크톱)에 대한 재설정 작업을 확인하라는 대화상자가 표시됩니다.

참고 Horizon 관리자가 데스크톱의 데스크톱 재설정 기능을 사용하도록 설정한 경우에만 이 작업을 사용할 수 있습니다.

8

```
vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
```

Horizon Client가 시작되며 view.mycompany.com 서버에 연결됩니다. 로그인 상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인에 성공하면 Horizon Client에서 Primary Desktop(기본 데스크톱)에 대한 다시 시작 작업을 확인하라는 대화상자가 표시됩니다.

참고 Horizon 관리자가 데스크톱의 데스크톱 다시 시작 기능을 사용하도록 설정한 경우에만 이 작업을 사용할 수 있습니다.

9

```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true
```

이 URI는 첫 번째 예와 동일한 효과를 가지며 클라이언트 시스템에 연결된 모든 USB 디바이스는 원격 데스크톱에 리디렉션됩니다.

10

```
vmware-view://
```

Horizon Client가 실행 중이 아니면 이 URI가 시작되고, Horizon Client가 실행 중이면 이를 포그라운드로 보냅니다.

11

```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

서버 10.10.10.10에서 My Notepad++를 시작하고 애플리케이션 실행 명령의 My new file.txt 인수를 전달합니다. 공백 및 큰따옴표는 퍼센트 이스케이프를 사용합니다. 파일 이름은 공백을 포함하므로 큰따옴표로 묶입니다.

다음 구문을 사용하여 Windows 명령줄 프롬프트에 이 명령을 입력할 수도 있습니다.

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "₩"my new.txt₩""
```

이 예제에서 큰따옴표는 \" 문자로 이스케이프됩니다.

12

```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

서버 10.10.10.10에서 Notepad++ 12를 시작하고 애플리케이션 실행 명령의 a.text b.txt 인수를 전달합니다. 인수가 큰따옴표로 묶여 있지 않기 때문에 파일 이름이 공백으로 구분되며, Notepad++에서 두 파일이 따로 열립니다.

참고 애플리케이션은 명령줄 인수를 사용하는 방식이 다를 수 있습니다. 예를 들어 워드패드에 인수 a.txt b.txt를 전달하면 워드패드에서 a.txt 파일 하나만 열립니다.

13
```
vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1
```

Horizon Client가 시작되고 **anonymous1** 사용자 계정을 사용하여 view.mycompany.com 서버에 연결됩니다. 로그인 자격 증명을 제공하라는 메시지가 표시되지 않고 메모장 애플리케이션이 시작됩니다.

HTML 코드 예

URI를 사용하여 e-메일 또는 웹 페이지에 포함할 하이퍼텍스트 링크 및 버튼을 만들 수 있습니다. 다음 예는 첫 번째 URI 예를 사용하여 **Test Link**라는 하이퍼텍스트 링크와 **TestButton**이라는 버튼을 코딩하는 방법을 보여줍니다.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

최종 사용자에 대한 인증서 검사 구성

관리자는 인증서 확인 모드를 구성할 수 있습니다(예: 항상 전체 확인이 수행되도록 구성).

인증서 검사는 연결 서버와 Horizon Client 간에 SSL 연결이 있을 때 수행됩니다. 관리자는 다음 전략 중 하나를 사용하도록 확인 모드를 구성할 수 있습니다.

- 최종 사용자가 확인 모드를 선택할 수 있습니다. 이 목록의 나머지 부분에서는 세 가지 확인 모드를 설명합니다.
- (확인 안 함) 인증서 검사를 수행하지 않습니다.
- (경고) 서버에서 자체 서명된 인증서를 제시할 경우 최종 사용자에게 경고합니다. 사용자는 이러한 유형의 연결을 허용할지 선택할 수 있습니다.
- (전체 보안) 전체 확인이 수행되고 전체 확인을 통과하지 못한 연결은 거부됩니다.

수행되는 확인 검사의 유형에 대한 자세한 내용은 Horizon Client의 인증서 검사 모드 설정를 참조하십시오.

Horizon Client 구성 ADMX 템플릿 파일(vdm_client.admx)을 사용하여 확인 모드를 설정합니다. 그룹 정책 설정을 제공하는 모든 ADMX 파일은 VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyy*.zip이라는 .zip 파일에 있습니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. http://www.vmware.com/go/downloadview의 VMware Horizon 다운로드 사이트에서 이 GPO 번들을 다운로드할 수 있습니다. 이 템플릿을 사용한 GPO 설정 제어에 대한 자세한 내용은 그룹 정책 템플릿을 사용하여 Windows용 VMware Horizon Client 구성을 참조하십시오.

참고 Horizon Client 구성 ADMX 템플릿 파일을 사용하면 암호화된 SSL 연결이 설정되기 전에 특정 암호화 알고리즘 및 프로토콜의 사용을 제한할 수도 있습니다. 이러한 설정에 대한 자세한 내용은 클라이언트 GPO에 대한 보안 설정을 참조하십시오.

인증서 확인 설정을 그룹 정책으로 구성하지 않을 경우, CertCheckMode 값 이름을 클라이언트 컴퓨터의 다음 레지스트리 키 중 하나에 추가하여 인증서 확인을 사용하도록 설정할 수도 있습니다.

- 32비트 Windows: HKEY_LOCAL_MACHINE₩Software₩VMware, Inc.₩VMware VDM₩Client₩Security
- 64비트 Windows: HKLM₩SOFTWARE₩Wow6432Node₩VMware, Inc.₩VMware VDM₩Client₩Security

다음 값을 레지스트리 키에 사용하십시오.

- 0은(는) Do not verify server identity certificates을(를) 구현합니다.
- 1은(는) Warn before connecting to untrusted servers을(를) 구현합니다.
- 2은(는) Never connect to untrusted servers을(를) 구현합니다.

레지스트리 키에 그룹 정책 설정 및 CertCheckMode 설정 모두를 구성할 경우 그룹 정책 설정이 레지스트리 키 값보다 우선합니다.

참고 향후 릴리스에서는 Windows 레지스트리를 사용하여 이 설정을 구성하지 못할 수 있습니다. GPO 설정을 사용해야 합니다.

Horizon Client 의 인증서 검사 모드 설정

관리자 및 최종 사용자는 임의 또는 일부 서버 인증서 검사가 실패할 경우 클라이언트 연결을 거부할지 여부를 구성할 수 있습니다.

인증서 검사는 연결 서버와 Horizon Client 간에 SSL 연결이 있을 때 수행됩니다. 인증서 검사에는 다음 확인 사항이 포함됩니다.

- 인증서가 해지되었습니까?
- 해당 인증서는 전송자 ID 확인 및 서버 통신 암호화 이외의 용도입니까? 즉, 올바른 유형의 인증서입니까?
- 인증서가 만료되었거나 나중에만 유효합니까? 즉, 컴퓨터 시계에 따라 인증서가 유효합니까?
- 인증서의 공통 이름이 이름을 보내는 서버의 호스트 이름과 일치합니까? 로드 밸런서가 Horizon Client에 입력된 호스트 이름과 일치하지 않는 인증서를 가진 서버에 Horizon Client를 리디렉션하는 경우 불일치가 발생할 수 있습니다. 또는 사용자가 클라이언트의 호스트 이름이 아닌 IP 주소를 입력할 경우 불일치가 발생할 수 있습니다.

- 알 수 없거나 신뢰할 수 없는 인증 기관(CA)에서 서명된 인증서입니까? 자체 서명된 인증서는 신뢰할 수 없는 CA 유형 중 하나입니다.

  이 검사를 통과하려면 신뢰할 수 있는 인증서 체인이 디바이스 로컬 인증서 저장소의 루트 위치에 있어야 합니다.

참고 자체 서명된 루트 인증서를 도메인의 모든 Windows 클라이언트 시스템에 배포하는 방법에 대한 자세한 내용은 View 설치 문서의 "신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가"를 참조하십시오.

관리자가 허용한 경우, Horizon Client를 사용하여 데스크톱에 로그인할 때 **SSL 구성**을 클릭하여 인증서 검사 모드를 설정할 수 있습니다. 다음 세 가지 선택 사항이 있습니다.

- **신뢰할 수 없는 서버에 연결하지 않습니다**. 인증서 검사에 실패할 경우 클라이언트가 서버에 연결할 수 없습니다. 검사 실패 내역이 오류 메시지에 나열됩니다.
- **신뢰할 수 없는 서버에 연결하기 전에 경고합니다**. 서버가 자체 서명 인증서를 사용하기 때문에 인증서 검사에 실패할 경우 **계속**을 클릭하여 경고를 무시할 수 있습니다. 자체 서명된 인증서의 경우 인증서 이름이 Horizon Client에서 입력한 서버 이름과 일치하지 않아도 됩니다.

  또한 인증서가 만료된 경우 경고를 받을 수 있습니다.
- **서버 ID 인증서가 확인되지 않습니다**. 이 설정은 인증서 검사가 수행되지 않음을 의미합니다.

인증서 검사 모드가 **경고**로 설정된 경우, 자체 서명된 인증서를 사용하는 연결 서버 인스턴스에 계속 연결할 수 있습니다.

관리자가 나중에 신뢰할 수 있는 인증 기관에서 보안 인증서를 설치할 경우, 연결할 때 모든 인증서 검사가 통과되도록 해당 특정 서버를 위해 이 신뢰할 수 있는 연결을 기억합니다. 나중에 해당 서버가 자체 서명된 인증서를 다시 제안할 경우 연결이 실패합니다. 특정 서버가 완전히 검사할 수 있는 인증서를 제안한 경우, 항상 해당 인증서를 제안해야 합니다.

중요 SSL Cipher Suite Order 그룹 정책 설정을 구성하는 것과 같이 이전에 회사의 클라이언트 시스템을 GPO를 통해 특정한 암호를 사용하도록 구성한 경우, ADMX 템플릿 파일에 포함된 Horizon Client 그룹 정책 보안 설정을 사용해야 합니다. 클라이언트 GPO에 대한 보안 설정의 내용을 참조하십시오. 또는 클라이언트의 SSLCipherList 레지스트리 설정을 사용할 수도 있습니다. Windows 레지스트리를 사용하여 Horizon Client 구성를 참조하십시오.

고급 TLS/SSL 옵션 구성

Horizon Client 및 원격 데스크톱의 Horizon Server 또는 Horizon Client 및 에이전트 사이에서 통신을 암호화하는 데 사용되는 보안 프로토콜과 암호화 알고리즘을 선택할 수 있습니다.

이러한 보안 옵션은 USB 채널을 암호화하는 데에도 사용됩니다.

기본 설정을 사용할 경우 암호 제품군은 128비트 또는 256비트 AES를 사용하며 익명 DH 알고리즘을 제거한 다음 암호화 알고리즘 키 길이 순서로 현재 암호 목록을 정렬합니다.

기본적으로 TLS v1.0, TLS v1.1 및 TLS v1.2를 사용하도록 설정되어 있습니다. SSL v2.0 및 v3.0은 지원되지 않습니다.

참고 TLS v1.0 및 RC4가 사용하지 않도록 설정된 경우 사용자가 Windows XP 데스크톱에 연결되었을 때 USB 리디렉션이 작동하지 않습니다. TLS v1.0 및 RC4를 사용 설정하여 이 기능을 사용할 경우 보안 위험을 인지하십시오.

클라이언트가 연결되는 서버에서 사용하도록 설정되어 있지 않은 Horizon Client에 대해 보안 프로토콜을 구성할 경우, TLS/SSL 오류가 발생하고 연결이 실패합니다.

중요 Horizon Client에서 사용하도록 설정한 하나 이상의 프로토콜을 원격 데스크톱에서도 사용하도록 설정해야 합니다. 그렇지 않으면 USB 디바이스를 원격 데스크톱에 리디렉션할 수 없습니다.

클라이언트 시스템에서 그룹 정책 설정 또는 Windows 레지스트리 설정을 사용하여 기본 암호 및 프로토콜을 변경할 수 있습니다. GPO 사용에 관한 자세한 내용은 클라이언트 GPO에 대한 보안 설정에서 "SSL 프로토콜 및 암호화 알고리즘 구성"이라는 설정을 참조하십시오. Windows 레지스트리에서 SSLCipherList 설정을 사용하는 방법은 Windows 레지스트리를 사용하여 Horizon Client 구성을 참조하십시오.

애플리케이션 다시 연결 동작 구성

서버와의 연결이 끊어져도 실행 중인 애플리케이션은 계속 열려 있을 수 있습니다. 서버에 다시 연결되었을 때 실행 중인 애플리케이션이 어떻게 동작할지 구성할 수 있습니다.

Horizon 관리자는 명령줄 또는 그룹 정책 설정을 통해 Horizon Client의 애플리케이션 다시 연결 동작 설정을 사용하지 않도록 설정할 수 있습니다. 그룹 정책 설정은 명령줄 설정보다 우선합니다. 자세한 내용은 Horizon Client 명령 사용의 -appSessionReconnectionBehavior 옵션 또는 클라이언트 GPO에 대한 스크립팅 정의 설정의 **연결이 끊어진 애플리케이션 세션 재개 동작** 그룹 정책 설정을 참조하십시오.

프로시저

1 Horizon Client의 데스크톱 및 애플리케이션 선택기 창에서 원격 애플리케이션을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택합니다.

2 [원격 애플리케이션] 창이 나타나면 애플리케이션 다시 연결 동작 설정을 선택합니다.

옵션	설명
열려 있는 애플리케이션에 다시 연결할지 묻기	서버에 다시 연결되면 Horizon Client가 하나 이상의 실행 중인 원격 애플리케이션이 있다고 알려줍니다. **애플리케이션에 다시 연결**을 클릭하여 애플리케이션 창을 다시 열거나 **지금 연결하지 않음**을 클릭하여 애플리케이션 창을 다시 열지 않을 수 있습니다.
열려 있는 애플리케이션에 자동으로 다시 연결	서버에 다시 연결할 경우 실행 중인 애플리케이션에 대한 애플리케이션 창이 자동으로 다시 열립니다.
묻지 않고 자동으로 다시 연결하지 않음	서버에 다시 연결할 경우 Horizon Client에서 실행 중인 애플리케이션을 다시 열라는 메시지가 표시되지 않고 실행 중인 애플리케이션 창이 다시 열리지 않습니다.

3 변경 사항을 저장하려면 **확인**을 클릭합니다.

설정은 다음에 서버에 연결할 때 적용됩니다.

그룹 정책 템플릿을 사용하여 Windows용 VMware Horizon Client 구성

VMware Horizon Client에는 VMware Horizon Client를 구성하는 데 사용할 수 있는 그룹 정책 ADMX 템플릿 파일이 포함되어 있습니다. 이 ADMX 템플릿 파일의 정책 설정을 Active Directory의 새 GPO 또는 기존 GPO에 추가하여 원격 데스크톱 연결을 최적화하고 보호할 수 있습니다.

템플릿 파일에는 컴퓨터 구성 및 사용자 구성 그룹 정책 모두가 포함됩니다.

- 컴퓨터 구성 정책은 호스트에서 클라이언트를 실행하는 사용자와 관계없이, Horizon Client에 적용되는 정책을 설정합니다.
- 사용자 구성 정책은 RDP 연결 설정뿐 아니라 Horizon Client를 실행하는 모든 사용자에게 적용되는 Horizon Client 정책을 설정합니다. 사용자 구성 정책은 동일한 컴퓨터 구성 정책보다 우선합니다.

Horizon은 데스크톱이 시작될 때 및 사용자가 로그인할 때 정책을 적용합니다.

Horizon Client 구성 ADMX 템플릿 파일(vdm_client.admx)과 그룹 정책 설정을 제공하는 모든 ADMX 파일은 VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyy*.zip 이라는 .zip 파일에서 사용할 수 있습니다. 여기서x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. http://www.vmware.com/go/downloadview의 VMware Horizon 다운로드 사이트에서 파일을 다운로드할 수 있습니다. 이러한 파일을 Active Directory 서버에 복사한 다음 그룹 정책 관리 편집기를 사용하여 관리 템플릿을 추가합니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

클라이언트 GPO에 대한 스크립팅 정의 설정

데스크톱 크기, 이름 및 도메인 이름 등, 명령줄에서 Horizon Client를 실행할 때 사용되는 동일한 설정에 대한 정책을 설정할 수 있습니다.

다음 표에서는 VMware Horizon Client 구성 ADMX 템플릿 파일의 스크립팅 정의 설정에 대해 설명합니다. 템플릿 파일은 각 스크립팅 정의 설정의 컴퓨터 구성 및 사용자 구성 버전을 제공합니다. 사용자 구성 설정은 동일한 컴퓨터 구성 설정보다 우선합니다. 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > 스크립팅 정의** 폴더에 있습니다.

표 3-4. VMware Horizon Client 구성 템플릿: 스크립팅 정의

설정	설명
Automatically connect if only one launch item is entitled	해당 사용자에게 권한이 주어진 유일한 데스크톱일 경우 자동 연결됩니다. 이 설정을 사용하면 데스크톱이 하나만 포함된 목록에서 데스크톱을 선택해야 하는 불필요한 수고를 피할 수 있습니다.
Connect all USB devices to the desktop on launch	클라이언트 시스템에서 사용할 수 있는 모든 USB 디바이스를 데스크톱을 시작할 때 데스크톱에 연결할지 여부를 지정합니다. **참고** 이 설정은 게시된 애플리케이션에 적용되지 않습니다.

표 3-4. VMware Horizon Client 구성 템플릿: 스크립팅 정의 (계속)

설정	설명
Connect all USB devices to the desktop when they are plugged in	클라이언트 시스템에 전원을 공급할 때 USB 디바이스를 데스크톱에 연결할지 여부를 지정합니다. **참고** 이 설정은 게시된 애플리케이션에 적용되지 않습니다.
DesktopLayout	원격 데스크톱에 로그인할 때 사용자에게 나타나는 Horizon Client 창의 레이아웃을 지정합니다. 레이아웃 선택 사항은 다음과 같습니다. ■ Full Screen ■ Multimonitor ■ Window - Large ■ Window - Small 이 설정은 또한 DesktopName to select setting이 설정된 경우에만 사용 가능합니다.
DesktopName to select	로그인 중 Horizon Client에서 사용하는 기본 데스크톱을 지정합니다.
Disable 3rd-party Terminal Services plugins	일반 RDP 플러그인으로 설치된 타사 터미널 서비스 플러그인을 Horizon Client에서 검사할지 여부를 지정합니다. 이 설정을 구성하지 않은 경우 Horizon Client는 기본적으로 타사 플러그인을 검사합니다. 이 설정은 USB 리디렉션과 같은 Horizon 특정 플러그인에 영향을 주지 않습니다.
Locked Guest Size	디스플레이가 모니터 한 대에서 사용되는 경우 원격 데스크톱의 화면 해상도를 지정합니다. 즉, 원격 데스크톱 디스플레이를 모든 모니터로 설정한 경우 이 설정은 작동하지 않습니다. 설정을 활성화하면 원격 데스크톱 자동 맞춤 기능이 비활성화됩니다. 최소 화면 크기는 640x480입니다. 최대 화면 크기는 4096x4096입니다. 이 설정은 PCoIP 연결에만 적용되며, RDP 연결에는 적용되지 않습니다. **중요** Horizon Administrator에서 설정된, 원격 데스크톱에 대해 지원되는 최대 해상도보다 해상도를 높게 설정하지 않는 것이 좋습니다. ■ 3D가 활성화되어 있는 경우 최대 2대의 모니터가 최대 해상도인 1920x1200으로 지원됩니다. ■ 3D가 활성화되어 있지 않는 경우 최대 4대의 모니터가 최대 해상도인 2560x1600으로 지원됩니다. 실제로는 원격 데스크톱의 운영 체제 버전, vRAM 용량 및 색 농도에 따른 해상도가 최대치보다 높게 설정되어 있을 경우 이 클라이언트 측 설정은 무시됩니다. 예를 들어, Horizon Administrator에서 데스크톱 해상도가 1920x1200으로 설정되어 있으면 원격 데스크톱의 기능에 따라 클라이언트에 표시되는 해상도는 1920x1200 이하일 수 있습니다.
Logon DomainName	로그인 중 Horizon Client에서 사용하는 NetBIOS 도메인을 지정합니다.
Logon Password	로그인 중 Horizon Client에서 사용하는 암호를 지정합니다. 암호는 Active Director에 의해 일반 텍스트로 저장됩니다. 보안을 강화하기 위해 이 설정을 지정하지 않는 것이 좋습니다. 사용자는 대화형으로 암호를 입력할 수 있습니다.
Logon UserName	로그인 중 Horizon Client에서 사용하는 암호를 지정합니다. 암호는 Active Director에 의해 일반 텍스트로 저장됩니다.
Server URL	로그인 중 Horizon Client에서 사용하는 URL(예: https://view1.example.com)을 지정합니다.

표 3-4. VMware Horizon Client 구성 템플릿: 스크립팅 정의 (계속)

설정	설명
Suppress error messages (when fully scripted only)	로그인 중 Horizon Client 오류 메시지가 숨겨지도록 할지 여부를 지정합니다. 이 설정은 로그인 프로세스가 완전히 스크립트로 작성된 경우에만(예를 들어, 정책을 통해 필요한 모든 로그인 정보가 자동으로 채워진 경우) 적용됩니다. 잘못된 로그인 정보 때문에 로그인이 실패한 경우 사용자에게 알리지 않고 Horizon Client 프로세스가 종료됩니다.
Disconnected application session resumption behavior	사용자가 서버에 다시 연결할 때 실행 중인 애플리케이션의 동작을 결정합니다. 선택 사항은 다음과 같습니다. ■ 열려 있는 애플리케이션에 다시 연결할지 묻기 ■ 열려 있는 애플리케이션에 자동으로 다시 연결 ■ 묻지 않고 자동으로 다시 연결하지 않음 이 설정이 사용되도록 설정되면 최종 사용자가 Horizon Client의 [설정] 페이지에서 애플리케이션 다시 연결 동작을 구성할 수 없습니다. 이 설정이 사용되도록 설정되면 최종 사용자가 Horizon Client에서 애플리케이션 다시 연결 동작을 구성할 수 있습니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Enable Unauthenticated Access to the server	Horizon Client를 사용 중인 경우 사용자가 애플리케이션에 액세스할 수 있도록 자격 증명을 입력해야 할지 여부를 결정합니다. 이 설정이 사용되도록 설정되면 Horizon Client에서 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정이 표시되고 사용하지 않도록 설정되며 선택됩니다. 인증되지 않은 액세스를 사용할 수 없는 경우 클라이언트는 다른 인증 방식으로 변경할 수 있습니다. 이 설정을 사용하지 않도록 설정하면 사용자는 애플리케이션에 로그인하고 액세스하려면 항상 자격 증명을 입력해야 합니다. Horizon Client에서 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정은 숨겨지고 선택 해제됩니다. 이 설정이 구성되어 있지 않으면(기본값) 사용자는 Horizon Client에서 인증되지 않은 액세스를 사용하도록 설정할 수 있습니다. **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정이 표시되고 사용되도록 설정되며 선택 해제됩니다.
Account to use for Unauthenticated Access	Enable Unauthenticated Access to the server 그룹 정책 설정이 사용되도록 설정되어 있거나 사용자가 Horizon Client에서 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인**을 선택하여 인증되지 않은 액세스를 사용하도록 설정하는 경우 Horizon Client에서 서버에 익명으로 로그인하는 데 사용할 인증되지 않은 액세스 사용자 계정을 지정합니다. 인증되지 않은 액세스가 서버에 대한 특정 연결에 사용되지 않는 경우 이 설정은 무시됩니다. 이 설정이 구성되지 않은 경우 사용자는 계정을 선택할 수 있습니다. 이 설정은 기본적으로 구성되어 있지 않습니다.

클라이언트 GPO에 대한 보안 설정

보안 설정에는 보안 인증서, 로그인 자격 증명 및 단일 로그온 기능에 대한 옵션이 포함됩니다.

다음 표에서는 Horizon Client 구성 ADMX 템플릿 파일의 보안 설정에 대해 설명합니다. 이 표는 설정에 컴퓨터 구성 및 사용자 구성 설정이 모두 포함되는지 또는 컴퓨터 구성 설정만 포함되는지를 보여줍니다. 두 가지 유형 모두를 포함하는 보안 설정의 경우, 사용자 구성 설정은 동등한 컴퓨터 구성 설정을 재정의합니다. 이러한 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > 보안 설정** 폴더에 있습니다.

표 3-5. Horizon Client 구성 템플릿: 보안 설정

설정	컴퓨터	사용자	설명
Allow command line credentials	X		사용자 자격 증명을 Horizon Client 명령줄 옵션으로 제공할 수 있는지 여부를 지정합니다. 이 설정이 사용되지 않도록 설정된 경우 사용자가 명령줄에서 Horizon Client를 실행할 때 smartCardPIN 및 password 옵션을 사용할 수 없습니다. 이 설정은 기본적으로 사용하도록 설정됩니다. 동등한 Windows 레지스트리 값은 AllowCmdLineCredentials입니다.
Servers Trusted For Delegation	X		사용자가 Horizon Client 메뉴 표시줄의 **옵션** 메뉴에서 **현재 사용자로 로그인**을 선택할 때 전달되는 사용자 ID 및 자격 증명 정보를 수락하는 연결 서버 인스턴스를 지정합니다. 연결 서버 인스턴스를 지정하지 않을 경우, 모든 연결 서버 인스턴스는 이 정보를 허용합니다. 연결 서버 인스턴스를 추가하려면 다음 형식 중 하나를 사용하십시오. ■ domain₩system$ ■ system$@domain.com ■ 연결 서버 서비스의 서비스 사용자 이름(SPN). 동등한 Windows 레지스트리 값은 BrokersTrustedForDelegation입니다.

표 3-5. Horizon Client 구성 템플릿: 보안 설정 (계속)

설정	컴퓨터	사용자	설명
Certificate verification mode	X		Horizon Client에서 수행되는 인증서 검사 수준을 구성합니다. 다음 모드 중 하나를 선택할 수 있습니다. ■ No Security. Horizon은 인증서 검사를 수행하지 않습니다. ■ Warn But Allow. 자체 서명 인증서가 Horizon에 의해 제공됩니다. 이런 경우 인증서 이름이 사용자가 Horizon Client의 사용자가 제공하는 연결 서버 이름과 일치하지 않아도 됩니다. 다른 인증서 오류 조건이 발생할 경우, Horizon에서 오류 대화 상자가 표시되고 사용자가 연결 서버에 연결할 수 없게 됩니다. Warn But Allow이 기본값입니다. ■ Full Security. 임의 유형의 인증서 오류가 발생할 경우 사용자는 연결 서버에 연결할 수 없습니다. Horizon은 사용자에게 인증서 오류를 표시합니다. 이 그룹 정책 설정이 구성되면 사용자는 Horizon Client에서 선택한 인증서 확인 모드를 볼 수 있지만 설정을 구성할 수는 없습니다. SSL 구성 대화 상자는 사용자에게 관리자가 설정을 차단했다고 알립니다. 이 설정이 구성되지 않았거나 사용하지 않도록 설정된 경우, Horizon Client 사용자는 인증서 확인 모드를 선택할 수 있습니다. 서버가 Horizon Client에서 제공한 인증서를 검사하도록 허용하려면 클라이언트에서 연결 서버 또는 보안 서버 호스트에 HTTPS로 연결해야 합니다. 연결 서버 또는 보안 서버 호스트에 HTTP로 연결하는 중간 디바이스로 SSL 부하를 분산시킨 경우에는 인증서 검사가 지원되지 않습니다. 이 설정을 그룹 정책으로 구성하지 않으려면 CertCheckMode 값 이름을 클라이언트 컴퓨터의 다음 레지스트리 키 중 하나에 추가하여 인증서 확인을 사용하도록 설정할 수도 있습니다. ■ 32비트 Windows: HKEY_LOCAL_MACHINE₩Software₩VMware, Inc.₩VMware VDM₩Client₩Security ■ 64비트 Windows: HKLM₩SOFTWARE₩Wow6432Node₩VMware, Inc.₩VMware VDM₩Client₩Security 다음 값을 레지스트리 키에 사용하십시오. ■ **0**은(는) No Security을(를) 구현합니다. ■ **1**은(는) Warn But Allow을(를) 구현합니다. ■ **2**은(는) Full Security을(를) 구현합니다. Windows 레지스트리 키에 그룹 정책 설정 및 CertCheckMode 설정 모두를 구성할 경우 그룹 정책 설정이 레지스트리 키 값보다 우선합니다. **참고** 향후 릴리스에서는 Windows 레지스트리를 사용하여 이 설정을 구성하지 못할 수 있습니다. GPO 설정을 사용해야 합니다.

표 3-5. Horizon Client 구성 템플릿: 보안 설정 (계속)

설정	컴퓨터	사용자	설명
Default value of the 'Log in as current user' checkbox	X	X	Horizon Client 메뉴 표시줄의 **옵션** 메뉴에서 **현재 사용자로 로그인**의 기본값을 지정합니다. 이 설정은 Horizon Client 설치 시 지정한 기본값을 재정의합니다. 사용자가 Horizon Client를 명령줄에서 실행하고 logInAsCurrentUser 옵션을 지정하면 해당 값이 이 설정을 재정의합니다. **옵션** 메뉴에서 **현재 사용자로 로그인**이 선택된 경우, 클라이언트 시스템에 로그인할 때 사용자가 제공한 ID 및 자격 증명 정보가 연결 서버 인스턴스로 전달되고 최종적으로 원격 데스크톱 또는 애플리케이션으로 전달됩니다. **현재 사용자로 로그인**이 선택 취소되면 사용자는 원격 데스크톱 또는 애플리케이션에 액세스하기 위해 ID 및 자격 증명 정보를 여러 번 제공해야 합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다. 동등한 Windows 레지스트리 값은 LogInAsCurrentUser입니다.
Display option to Log in as current user	X	X	Horizon Client 메뉴 표시줄의 **옵션** 메뉴에 **현재 사용자로 로그인**을 표시할지를 결정합니다. **현재 사용자로 로그인**이 표시되면 사용자는 해당 옵션을 선택하거나 선택 취소하고 기본값을 재정의할 수 있습니다. **현재 사용자로 로그인**이 숨겨지면 사용자는 Horizon Client **옵션** 메뉴에서 기본값을 재정의할 수 없습니다. Default value of the 'Log in as current user' checkbox 정책 설정을 사용하여 **현재 사용자로 로그인**의 기본값을 지정할 수 있습니다. 이 설정은 기본적으로 사용하도록 설정됩니다. 동등한 Windows 레지스트리 값은 LogInAsCurrentUser_Display입니다.
Enable jump list integration	X		이 설정은 Windows 7 이상 시스템의 작업 표시줄에 있는 Horizon Client 아이콘에 점프 목록이 나타나도록 할지 여부를 지정합니다. 점프 목록을 사용하여 사용자는 최근 연결 서버 인스턴스 및 원격 데스크톱에 연결할 수 있습니다. Horizon Client가 공유된 경우, 사용자가 최근 데스크톱의 이름을 보는 것을 원하지 않을 수 있습니다. 이 설정을 사용하지 않도록 설정하여 점프 목록을 사용하지 않도록 설정할 수 있습니다. 이 설정은 기본적으로 사용하도록 설정됩니다. 동등한 Windows 레지스트리 값은 EnableJumplist입니다.

표 3-5. Horizon Client 구성 템플릿: 보안 설정 (계속)

설정	컴퓨터	사용자	설명
Enable SSL encrypted framework channel	X	X	View 5.0 이하 데스크톱에 SSL이 사용되도록 설정할지 여부를 결정합니다. View 5.0 이전의 경우 포트 TCP 32111을 통해 데스크톱으로 전송되는 데이터는 암호화되지 않았습니다. ■ **사용**: SSL을 사용하도록 설정합니다. 하지만 원격 데스크톱에서 SSL이 지원되지 않는 경우에는 이전의 암호화되지 않은 연결로 대체될 수 있습니다. 예를 들어 View 5.0 이하 데스크톱의 경우 SSL이 지원되지 않습니다. **사용**이 기본 설정입니다. ■ **사용 안 함**: SSL을 사용하지 않도록 설정합니다. 이 설정은 권장되지 않지만 디버깅 작업이나 터널링되지 않은 채널에 유용할 수 있으며 WAN 가속기 제품에 의해 최적화될 수 있습니다. ■ **강제 적용**: SSL을 사용하도록 설정하며, SSL을 지원하지 않는 데스크톱에 대한 연결은 거부됩니다. 동등한 Windows 레지스트리 값은 EnableTicketSSLAuth입니다.
Configures SSL protocols and cryptographic algorithms	X	X	암호화된 SSL 연결이 설정되기 전에 특정 암호화 알고리즘 및 프로토콜의 사용을 제한하는 암호 목록을 구성합니다. 암호 목록은 콜론으로 구분된 하나 이상의 암호 문자열로 구성됩니다. **참고** 암호 문자열은 대/소문자를 구분합니다. 기본값은 **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**입니다. 즉 TLS v1, TLS v1.1 및 TLS v1.2가 사용되도록 설정되어 있습니다. (SSL v2.0 및 v3.0은 제거됩니다.) 암호 그룹은 128비트 또는 256비트 AES를 사용하며 익명 DH 알고리즘을 제거한 다음 암호화 알고리즘 키 길이 순서로 현재 암호 목록을 정렬합니다. 구성에 대한 참조 링크: http://www.openssl.org/docs/apps/ciphers.html 동등한 Windows 레지스트리 값은 SSLCipherList입니다.
Enable Single Sign-On for smart card authentication	X		스마트 카드 인증을 위해 단일 로그온이 사용되도록 설정할지 여부를 지정합니다. 단일 로그온을 사용하도록 설정하면 Horizon Client는 암호화된 스마트 카드 PIN을 임시 메모리에 저장한 후에 연결 서버에 제출합니다. 단일 로그온을 사용하지 않도록 설정하면 Horizon Client에 사용자 지정 PIN 대화 상자가 표시되지 않습니다. 동등한 Windows 레지스트리 값은 EnableSmartCardSSO입니다.
Ignore certificate revocation problems	X	X	해지된 서버 인증서와 연결된 오류를 무시할지를 결정합니다. 이러한 오류는 서버가 전송하는 인증서가 해지되었거나 클라이언트가 인증서 해지 상태를 확인할 수 없을 때 발생합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Unlock remote sessions when the client machine is unlocked	X	X	재귀 잠금 해제 기능을 사용하도록 설정할지를 결정합니다. 재귀 잠금 해제 기능은 클라이언트 시스템이 잠금 해제된 후에 모든 원격 세션의 잠금을 해제합니다. 이 기능은 사용자가 현재 사용자로 로그인 기능을 사용하여 서버에 로그인한 후에만 적용됩니다. 이 설정은 기본적으로 사용하도록 설정됩니다.

클라이언트 GPO에 대한 RDP 설정

Microsoft RDP 디스플레이 프로토콜 사용 시 오디오, 프린터, 포트 및 기타 디바이스 등의 리디렉션과 같은 옵션에 대한 그룹 정책을 설정할 수 있습니다.

다음 표에서는 Horizon Client 구성 ADMX 템플릿 파일의 RDP(원격 데스크톱 프로토콜) 설정에 대해 설명합니다. 모든 RDP 설정은 사용자 구성 설정입니다. 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > RDP 설정** 폴더에 있습니다.

표 3-6. Horizon Client 구성 관리 템플릿: RDP 설정

설정	설명
Audio redirection	원격 데스크톱에서 재생되는 오디오 정보를 리디렉션할지 여부를 지정합니다. 다음 설정 중 하나를 선택합니다. ■ **오디오 사용 안 함**: 오디오를 사용하지 않도록 설정합니다. ■ **VM에서 재생(VoIP USB 지원에 필요)**: 오디오가 원격 데스크톱 내에서 재생됩니다. 이 설정에는 클라이언트에 사운드를 제공할 공유 USB 오디오 디바이스가 필요합니다. ■ **클라이언트로 리디렉션**: 오디오가 클라이언트로 리디렉션됩니다. 이는 기본값 모드입니다. 이 설정은 RDP 오디오에만 적용됩니다. MMR을 통해 리디렉션된 오디오가 클라이언트에서 재생됩니다.
Enable audio capture redirection	기본 오디오 입력 디바이스를 클라이언트에서 원격 세션으로 리디렉션할지 여부를 지정합니다. 이 설정이 사용되도록 설정된 경우, 클라이언트의 오디오 리코딩 디바이스가 원격 데스크톱에 나타나며 오디오 입력을 기록할 수 있습니다. 기본 설정이 사용되지 않도록 설정됩니다.
Bitmap cache file size in 단위 for 숫자 bpp bitmaps	비트맵 캐시의 크기를 KB 또는 MB로 지정하여 특정 픽셀당 비트(bpp) 비트맵 색상 설정에 사용합니다. 이 설정의 개별 버전이 다음 단위 및 bpp 조합을 위해 제공됩니다. ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
In-memory bitmap cache size in KB for 8bpp bitmaps	8bpp 색상 설정에 사용할 RAM 비트맵 캐시의 크기를 킬로바이트로 지정합니다. ScaleBitmapCachesByBPP가 true(기본값)이면 이 캐시 크기에 픽셀당 바이트 수를 곱하여 실제 RAM 캐시 크기를 결정합니다. 이 설정이 사용되도록 지정되면 크기를 킬로바이트로 입력합니다.
Bitmap caching/cache persistence active	영구 비트맵 캐싱을 사용할지(활성) 여부를 지정합니다. 영구 비트맵 캐싱은 성능을 향상시킬 수 있지만 추가 디스크 공간이 필요합니다.
Color depth	원격 데스크톱의 색 농도를 지정합니다. 사용 가능한 설정 중 하나를 선택합니다. ■ 8비트 ■ 15비트 ■ 16비트 ■ 24비트 ■ 32비트 24비트 Windows XP 시스템의 경우 **컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 터미널 서비스**에서 최대 색 농도 제한 정책을 사용하도록 설정하고 24비트로 설정해야 합니다.

표 3-6. Horizon Client 구성 관리 템플릿: RDP 설정 (계속)

설정	설명
Cursor shadow	원격 데스크톱의 커서 아래에 섀도를 표시할지 여부를 지정합니다.
Desktop background	클라이언트가 원격 데스크톱에 연결할 때 데스크톱 배경을 표시할지 여부를 지정합니다.
Desktop composition	(Windows Vista 이상) 원격 데스크톱에서 데스크톱 구성이 사용되도록 설정할지 여부를 지정합니다. 데스크톱 구성이 사용되도록 설정된 경우, 개별 창은 더 이상 Microsoft Windows의 이전 버전에서처럼 화면 또는 기본 디스플레이 디바이스에 직접 드로잉하지 않습니다. 대신, 드로잉은 비디오 메모리의 오프스크린 표면으로 리디렉션되어 데스크톱 이미지로 렌더링되고 디스플레이에 표시됩니다.
Enable compression	RDP 데이터의 압축 여부를 지정합니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
Enable RDP Auto-Reconnect	RDP 프로토콜 연결 실패 후 RDP 클라이언트 구성 요소가 원격 데스크톱에 다시 연결을 시도할지 여부를 지정합니다. 이 설정은 Horizon Administrator에서 **보안 터널을 사용하여 데스크톱에 연결** 옵션이 사용되도록 설정된 경우 영향을 주지 않습니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Font smoothing	(Windows Vista 이상) 원격 데스크톱에서 앤티앨리어싱을 글꼴에 적용할지 여부를 지정합니다.
Menu and window animation	클라이언트가 원격 데스크톱에 연결할 때 메뉴 및 창에 대해 애니메이션이 사용되도록 설정할지 여부를 지정합니다.
Redirect clipboard	클라이언트가 원격 데스크톱에 연결할 때 로컬 클립보드 정보를 리디렉션할지 여부를 지정합니다.
Redirect drives	클라이언트가 원격 데스크톱에 연결할 때 로컬 디스크 드라이브를 리디렉션할지 여부를 지정합니다. 기본적으로 로컬 드라이브가 리디렉션됩니다. 이 설정을 사용하도록 설정하거나 구성되지 않은 상태로 두면 원격 데스크톱의 리디렉션된 드라이브의 데이터가 클라이언트 컴퓨터의 드라이브에 복사될 수 있습니다. 원격 데스크톱에서 사용자의 클라이언트 컴퓨터로 데이터를 전달할 경우 이 설정을 사용하지 않도록 설정하면 배포 시 보안상 위험이 발생할 수 있습니다. 또 다른 접근법은 Microsoft Windows 그룹 정책 설정인 Do not allow drive redirection을 사용하도록 설정하여 원격 데스크톱 가상 시스템에 폴더 리디렉션을 사용하지 않도록 설정하는 것입니다. Redirect drives 설정은 RDP에만 적용됩니다.
Redirect printers	클라이언트가 원격 데스크톱에 연결할 때 로컬 프린터를 리디렉션할지 여부를 지정합니다.
Redirect serial ports	클라이언트가 원격 데스크톱에 연결할 때 로컬 COM 포트를 리디렉션할지 여부를 지정합니다.
Redirect smart cards	클라이언트가 원격 데스크톱에 연결할 때 로컬 스마트 카드를 리디렉션할지 여부를 지정합니다. **참고** 이 설정은 RDP 및 PCoIP 연결 모두에 적용됩니다.
Redirect supported plug-and-play devices	클라이언트가 원격 데스크톱에 연결할 때 로컬 플러그 앤 플레이 및 POS(Point Of Sale) 디바이스를 리디렉션할지 여부를 지정합니다. 이 동작은 에이전트의 USB 리디렉션 구성 요소로 관리되는 리디렉션과 다릅니다.
Shadow bitmaps	비트맵을 표시할지 여부를 지정합니다. 이 설정은 전체 화면 모드에서 효과가 없습니다.
Show contents of window while dragging	사용자가 폴더를 새 위치로 끌어 놓을 때 폴더 내용이 나타날지 여부를 지정합니다.

표 3-6. Horizon Client 구성 관리 템플릿: RDP 설정 (계속)

설정	설명
Themes	클라이언트가 원격 데스크톱에 연결할 때 테마를 표시할지 여부를 지정합니다.
Windows key combination redirection	Windows 키 조합이 적용되는지 확인합니다. 이 설정을 사용하여 키 조합을 원격 가상 시스템으로 보내거나 키 조합을 로컬로 적용할 수 있습니다. 이 설정이 구성되지 않은 경우 키 조합이 로컬로 적용됩니다.
Enable Credential Security Service Provider	원격 데스크톱 연결에서 NLA(Network Level Authentication)를 사용할지 여부를 지정합니다. Windows Vista에서 원격 데스크톱 연결에는 기본적으로 NLA가 필요합니다. 게스트 운영 체제에 원격 데스크톱 연결을 위한 NLA가 필요한 경우, 이 설정을 사용하도록 설정해야 합니다. 그렇지 않으면 Horizon Client는 원격 데스크톱에 연결할 수 없습니다. 이 설정을 사용하도록 설정하는 것 외에도 다음 조건이 충족하는지 또한 확인해야 합니다. ■ 클라이언트 및 게스트 운영 체제 모두 NLA를 지원합니다. ■ 클라이언트 직접 연결은 연결 서버 인스턴스를 위해 사용되도록 설정됩니다. 터널링된 연결은 NLA와 함께 지원되지 않습니다.

클라이언트 GPO에 대한 일반 설정

설정에는 프록시 옵션, 표준 시간대 전달, 멀티미디어 가속 및 기타 디스플레이 설정이 포함됩니다.

일반 설정

다음 표에서는 Horizon Client 구성 ADMX 템플릿 파일의 일반 설정에 대해 설명합니다. 일반 설정은 컴퓨터 구성 및 사용자 구성 설정 모두를 포함합니다. 사용자 구성 설정은 동일한 컴퓨터 구성 설정보다 우선합니다. 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성** 폴더에 있습니다.

표 3-7. Horizon Client 구성 템플릿: 일반 설정

설정	컴퓨터	사용자	설명
Always on top		X	Horizon Client 창을 항상 맨 위 창으로 표시할지 여부를 지정합니다. 이 설정을 사용하도록 설정하면 Windows 작업 표시줄이 전체 화면의 Horizon Client 창을 가리지 않도록 합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Default value of the "Hide the selector after launching an item" check box	X	X	**항목을 시작하면 선택기 숨기기** 확인란이 기본적으로 선택되도록 할지 설정합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Disable time zone forwarding	X		원격 데스크톱 및 연결된 클라이언트 사이의 표준 시간대 동기화가 사용되지 않도록 설정할지 여부를 지정합니다.
Disable toast notifications	X	X	Horizon Client에서 알림을 사용하지 않도록 설정할지 여부를 결정합니다. 화면 모서리에 알림이 나타나지 않도록 하려면 이 설정을 사용합니다. **참고** 이 설정을 사용할 경우, 세션 시간 초과 기능이 활성화된 상태에서 5분 경고가 나타나지 않습니다.

표 3-7. Horizon Client 구성 템플릿: 일반 설정 (계속)

설정	컴퓨터	사용자	설명
Disallow passing through client information in a nested session	X		Horizon Client가 중첩 세션에서 클라이언트 정보를 통과하지 못하게 할지 여부를 지정합니다. 이 기능을 사용하도록 설정하면 Horizon Client가 Horizon 세션 내에서 실행될 경우 VM 디바이스 정보 대신 실제의 물리적 클라이언트 정보를 보냅니다. 이 설정은 클라이언트 정보인 디바이스 이름과 도메인, 클라이언트 유형, IP 주소 및 MAC 주소에 적용됩니다. 이 설정은 기본적으로 사용되지 않도록 설정됩니다. 즉, 중첩 세션의 클라이언트 정보 통과가 허용됩니다.
Don't check monitor alignment on spanning		X	기본적으로 클라이언트 데스크톱은 화면이 조합될 때 정확한 직사각형을 형성하지 않을 경우 다중 모니터를 스팬하지 않습니다. 이 설정을 사용하도록 설정하여 기본값을 재정의합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Enable multi-media acceleration		X	MMR(멀티미디어 리디렉션)이 클라이언트에서 사용되도록 설정할지 여부를 지정합니다. Horizon Client 비디오 디스플레이 하드웨어에 오버레이 지원이 없으면 MMR이 올바르게 작동하지 않습니다.
Enable relative mouse	X	X	(View 5.2 이상 릴리스만 해당) PCoIP 디스플레이 프로토콜 사용 시 상대 마우스를 사용하도록 설정합니다. 상대 마우스 모드를 사용하면 특정 그래픽 애플리케이션 및 게임의 마우스 동작이 향상됩니다. 원격 데스크톱에서 상대 마우스가 지원되지 않으면 이 설정이 사용되지 않습니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Enable the shade		X	Horizon Client 창의 상단에 있는 음영 메뉴 표시줄이 보일지 여부를 지정합니다. 이 설정은 기본적으로 사용하도록 설정됩니다. **참고** 음영 메뉴 표시줄은 키오스크 모드를 위해 기본적으로 사용되지 않도록 설정됩니다.
Enable Horizon Client online update	X		온라인 업그레이드 기능을 사용하도록 설정합니다. 이 설정은 기본적으로 사용되지 않도록 설정되어 있습니다.
Tunnel proxy bypass address list	X		터널 주소의 목록을 지정합니다. 프록시 서버는 이러한 주소에 사용되지 않습니다. 세미콜론(;)을 사용하여 여러 항목을 구분합니다.
URL for Horizon Client online help	X		Horizon Client가 도움말 페이지를 검색할 수 있는 대체 URL을 지정합니다. 이 설정은 인터넷 액세스 권한이 없기 때문에 원격으로 호스팅된 도움말 시스템을 검색할 수 없는 환경에서 사용하기 위한 것입니다.
Pin the shade		X	Horizon Client 창 상단의 음영에서 핀이 사용되도록 설정되고 메뉴 표시줄의 자동 숨김을 발생할지 않을지 여부를 지정합니다. 이 설정은 음영이 사용되지 않도록 설정된 경우 효과가 없습니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
Disable desktop disconnect messages	X	X	데스크톱 연결이 끊어졌을 때 표시되는 메시지를 사용하지 않도록 지정합니다. 이러한 메시지는 기본적으로 표시됩니다.

표 3-7. Horizon Client 구성 템플릿: 일반 설정 (계속)

설정	컴퓨터	사용자	설명
Disable sharing files and folders		X	Horizon Client에서 클라이언트 드라이브 리디렉션 기능을 사용할 수 있는지 지정합니다. 이 설정을 [사용]으로 설정하면 원격 애플리케이션에서 로컬 파일을 여는 기능을 포함하여 Horizon Client의 모든 클라이언트 드라이브 리디렉션 기능이 사용되지 않도록 설정됩니다. 또한 다음 요소가 Horizon Client 사용자 인터페이스에서 숨겨집니다. ■ [설정] 대화상자의 공유 패널 ■ 원격 데스크톱의 **옵션** 메뉴에 있는 **폴더 공유** 항목 ■ 시스템 트레이의 Horizon Client에 대한 **공유** 항목 ■ 서버 연결 후 원격 데스크톱이나 애플리케이션에 처음 연결할 때 나타나는 공유 대화상자 이 설정을 [사용 안 함]으로 설정하면 클라이언트 드라이브 리디렉션 기능이 모두 작동합니다. 이 설정을 구성하지 않으면 기본값은 [사용 안 함]입니다. 이 설정은 기본적으로 구성되어 있지 않습니다.
Always hide the remote floating language (IME) bar for Hosted Apps	X	X	애플리케이션 세션에 대해 부동 언어 표시줄을 해제합니다. 이 설정을 사용하도록 설정하면 로컬 IME 기능의 사용 여부와 상관 없이 부동 언어 표시줄이 원격 애플리케이션 세션에 표시되지 않습니다. 이 설정을 사용하지 않도록 설정하면 로컬 IME 기능이 사용되지 않도록 설정된 경우에만 부동 언어 표시줄이 표시됩니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Put icon cache in user's Local profile folder	X		Horizon Client가 아이콘 캐시 파일을 이전에 사용한 로밍 폴더 대신 사용자의 로컬 폴더에 배치할지 여부를 지정합니다. 이 설정을 [사용]으로 설정하면 Horizon Client가 사용자의 로컬 폴더에 아이콘 캐시 파일을 배치합니다. Horizon Client를 먼저 시작하면 로밍 폴더에서 로컬 폴더로 기존 캐시 파일이 이동되며 새 캐시 파일이 로컬 폴더에 배치됩니다. 이 정책을 사용하도록 설정하면 캐시 파일 동기화를 피하여 로밍 프로파일을 사용하는 경우 원격 애플리케이션의 응답 시간 개선에 도움이 될 수 있습니다. 이 설정을 구성하지 않으면 기본값은 [사용 안 함]입니다. 이 설정은 기본적으로 구성되어 있지 않습니다.
Disable opening local files in hosted applications		X	Horizon Client가 호스팅된 애플리케이션에서 지원하는 파일 확장명에 대한 로컬 처리기를 등록할지 여부를 지정합니다. 이 설정을 [사용]으로 설정하면 Horizon Client가 파일 확장명 처리기를 등록하지 않으며 사용자가 설정을 재정의할 수 없습니다. 이 설정을 [사용 안 함]으로 설정하면 Horizon Client가 항상 파일 확장명 처리기를 등록합니다. 기본적으로 파일 확장명 처리기가 등록되지만 사용자는 [설정] 대화 상자의 [공유] 창에서 **로컬 파일 시스템에서 원격 애플리케이션으로 로컬 파일을 여는 기능 설정** 설정을 사용하여 Horizon Client 사용자 인터페이스에서 이 기능을 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 로컬 폴더 및 드라이브에 대한 액세스 공유의 내용을 참조하십시오. 이 설정을 구성하지 않으면 기본값은 [사용 안 함]입니다. 이 설정은 기본적으로 구성되어 있지 않습니다.
Redirect smart card readers in Local Mode	X		Local Mode는 이 릴리스에서 지원되지 않습니다.

표 3-7. Horizon Client 구성 템플릿: 일반 설정 (계속)

설정	컴퓨터	사용자	설명
Delay the start of replications when starting Horizon Client with Local Mode	X		Local Mode는 이 릴리스에서 지원되지 않습니다.
Default Exit Behavior For Local Mode Desktops		X	Local Mode는 이 릴리스에서 지원되지 않습니다.

클라이언트 GPO에 대한 USB 설정

Windows용 Agent 및 Horizon Client 모두를 위한 USB 정책 설정을 정의할 수 있습니다. 연결 시 Horizon Client는 에이전트에서 USB 정책 설정을 다운로드하고 이 정책 설정을 Horizon Client USB 정책 설정과 함께 사용하여 호스트 시스템에서 리디렉션에 사용하도록 허용할 디바이스를 결정합니다.

다음 표에서는 Horizon Client 구성 ADMX 템플릿 파일의 복합 USB 분할을 위한 각 정책 설정에 대해 설명합니다. 이 설정은 컴퓨터 수준에서 적용됩니다. Horizon Client는 컴퓨터 수준의 GPO에서 설정을 우선적으로 읽고, 그 이외에는 HKLM₩Software₩Policies₩VMware, Inc.₩VMware VDM₩Client₩USB의 레지스트리에서 읽습니다. 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.

Horizon에서 복합 USB 디바이스 분할을 위한 정책을 적용하는 방법에 대한 설명은 Horizon 7에서 원격 데스크톱 기능 구성 문서에서 USB 리디렉션을 제어하기 위한 정책 사용에 관한 항목을 참조하십시오.

표 3-8. Horizon Client 구성 템플릿: USB 분할 설정

설정	속성
Allow Auto Device Splitting	복합 USB 디바이스의 자동 분할을 허용합니다. 기본값은 정의되어 있지 않으며 **false**와 같습니다.
Exclude Vid/Pid Device From Split	공급업체 및 제품 ID별로 지정된 복합 USB 디바이스를 분할에서 제외합니다. 설정 형식은 vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...입니다. ID 번호를 16진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다. 예: **vid-0781_pid-55**** 기본 값은 정의되어 있지 않습니다.
Split Vid/Pid Device	공급업체 및 제품 ID별로 지정된 복합 USB 디바이스의 구성 요소를 개별 디바이스로 처리합니다. 설정 형식은 다음과 같습니다. vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]) exintf 키워드를 사용하면 인터페이스 번호를 지정하여 구성 요소를 리디렉션에서 제외할 수 있습니다. ID 번호는 16진수로, 인터페이스 번호는 앞에 0이 표시되는 10진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다. 예: **vid-0781_pid-554c(exintf:01;exintf:02)** **참고** Horizon은 명시적으로 제외하지 않은 구성 요소를 자동으로 포함시키지 않습니다. Include Vid/Pid Device과 같은 필터 정책을 지정하여 해당 구성 요소를 포함시켜야 합니다. 기본 값은 정의되어 있지 않습니다.

다음 표에서는 Horizon Client 구성 ADMX 템플릿 파일의 USB 디바이스를 필터링하기 위한 각 정책 설정에 대해 설명합니다. 이 설정은 컴퓨터 수준에서 적용됩니다. Horizon Client는 컴퓨터 수준의 GPO에서 설정을 우선적으로 읽고, 그 이외에는 HKLM₩Software₩Policies₩VMware, Inc.₩VMware VDM₩Client₩USB의 레지스트리에서 읽습니다. Horizon에서 USB 디바이스 필터링을 위한 정책을 적용하는 방법에 대한 설명은 Horizon 7에서 원격 데스크톱 기능 구성 문서에서 USB 리디렉션의 필터 정책 설정 구성에 관한 항목을 참조하십시오.

표 3-9. Horizon Client 구성 템플릿: USB 필터링 설정

설정	속성
Allow Audio Input Devices	오디오 입력 디바이스가 리디렉션되도록 허용합니다. 기본값은 정의되어 있지 않으며 **true**와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Allow Audio Output Devices	오디오 출력 디바이스가 리디렉션되도록 허용합니다. 기본값은 정의되어 있지 않으며 **false**와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Allow HID-Bootable	부팅 시 사용할 수 있는 키보드 또는 마우스(HID 부팅 가능 디바이스라고도 부름) 이외의 입력 디바이스가 리디렉션되도록 허용합니다. 기본값은 정의되어 있지 않으며 **true**와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Allow Device Descriptor Failsafe Behavior	Horizon Client가 config/device 설명자를 가져오지 못할 경우에도 디바이스가 리디렉션되도록 허용합니다. config/desc에 실패한 경우에도 디바이스를 허용하려면 IncludeVidPid 또는 IncludePath와 같은 Include 필터에 포함시킵니다. 기본값은 정의되어 있지 않으며 **false**와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기 > Agent에서 구성할 수 없는 설정** 폴더에 있습니다.
Allow Other Input Devices	통합된 포인팅 디바이스가 있는 HID 부팅 가능 디바이스 또는 키보드 이외의 입력 디바이스가 리디렉션되도록 허용합니다. 기본값은 정의되어 있지 않으며 **true**와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Allow Keyboard and Mouse Devices	통합된 포인팅 디바이스(마우스, 트랙볼 또는 터치 패드)가 있는 키보드가 리디렉션되도록 허용합니다. 기본값은 정의되어 있지 않으며 **false**와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Allow Smart Cards	스마트 카드 디바이스가 리디렉션되도록 허용합니다. 기본값은 정의되어 있지 않으며 **false**와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.

표 3-9. Horizon Client 구성 템플릿: USB 필터링 설정 (계속)

설정	속성
Allow Video Devices	비디오 디바이스가 리디렉션되도록 허용합니다. 기본값은 정의되어 있지 않으며 true와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Disable Remote Configuration	USB 디바이스 필터링 수행 시 에이전트 설정을 사용하지 않도록 설정합니다. 기본값은 정의되어 있지 않으며 false와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기 > Agent에서 구성할 수 없는 설정** 폴더에 있습니다.
Exclude All Devices	모든 USB 디바이스가 리디렉션되지 않도록 제외합니다. true로 설정되면 기타 정책 설정을 사용하여 특정 디바이스 또는 디바이스 제품군을 리디렉션할 수 있습니다. false로 설정되면 기타 정책 설정을 사용하여 특정 디바이스 또는 디바이스 제품군이 리디렉션되지 않도록 방지할 수 있습니다. 에이전트에서 Exclude All Devices 값을 true로 설정하고 이 설정이 Horizon Client로 전달될 경우, 에이전트 설정이 Horizon Client 설정을 재정의합니다. 기본값은 정의되어 있지 않으며 false와 같습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Exclude Device Family	디바이스 제품군이 리디렉션되지 않도록 제외합니다. 설정 형식은 family_name_1[;family_name_2]...입니다. 예: bluetooth;smart-card 자동 디바이스 분할을 사용하도록 설정한 경우 Horizon은 복합 USB 디바이스 각 인터페이스의 디바이스 제품군을 검토하여 제외해야 할 인터페이스를 결정합니다. 자동 디바이스 분할을 사용하지 않도록 설정한 경우, Horizon은 전체 복합 USB 디바이스의 디바이스 제품군을 검토합니다. 기본 값은 정의되어 있지 않습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Exclude Vid/Pid Device	지정된 공급업체 및 제품 ID가 있는 디바이스가 리디렉션되지 않도록 제외합니다. 설정 형식은 vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...입니다. ID 번호를 16진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다. 예: vid-0781_pid-****;vid-0561_pid-554c 기본 값은 정의되어 있지 않습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Exclude Path	지정된 허브 또는 포트 경로의 디바이스가 리디렉션되지 않도록 제외합니다. 설정 형식은 bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2]...입니다. 버스 및 포트 번호를 16진수로 지정해야 합니다. 와일드카드 문자는 경로에 사용할 수 없습니다. 예: bus-1/2/3_port-02;bus-1/1/1/4_port-ff 기본 값은 정의되어 있지 않습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기 > Agent에서 구성할 수 없는 설정** 폴더에 있습니다.

표 3-9. Horizon Client 구성 템플릿: USB 필터링 설정 (계속)

설정	속성
Include Device Family	리디렉션될 수 있는 디바이스 제품군을 포함합니다. 설정 형식은 family_name_1[;family_name_2]...입니다. 예: **storage** 기본 값은 정의되어 있지 않습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.
Include Path	리디렉션될 수 있는 지정된 허브 또는 포트 경로의 디바이스를 포함합니다. 설정 형식은 bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2]...입니다. 버스 및 포트 번호를 16진수로 지정해야 합니다. 와일드카드 문자는 경로에 사용할 수 없습니다. 예: **bus-1/2_port-02;bus-1/7/1/4_port-0f** 기본 값은 정의되어 있지 않습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기 > Agent에서 구성할 수 없는 설정** 폴더에 있습니다.
Include Vid/Pid Device	지정된 공급업체 및 제품 ID가 있는 디바이스가 리디렉션되도록 포함합니다. 설정 형식은 vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...입니다. ID 번호를 16진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다. 예: **vid-0561_pid-554c** 기본 값은 정의되어 있지 않습니다. 이 설정은 그룹 정책 관리 편집기의 **VMware Horizon Client 구성 > USB 구성 보기** 폴더에 있습니다.

PCoIP 클라이언트 세션 변수 ADMX 템플릿 설정

PCoIP 클라이언트 세션 변수 ADMX 템플릿 파일(pcoip.client.admx)에는 PCoIP 디스플레이 프로토콜에 관련된 정책 설정이 포함됩니다. 관리자가 재정의할 수 있는 컴퓨터 기본값으로 설정을 구성하거나 재정의될 수 없는 값으로 사용자 설정을 구성할 수 있습니다. 재정의할 수 있는 설정은 그룹 정책 관리 편집기의 **PCoIP 클라이언트 세션 변수 > 재정의 가능한 관리자 기본값** 폴더에 있습니다. 재정의할 수 없는 설정은 그룹 정책 관리 편집기의 **PCoIP 클라이언트 세션 변수 > 재정의 불가능한 설정** 폴더에 있습니다.

ADMX 파일은 VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyy*.zip이라는 번들형 .zip 파일로 제공되며 https://my.vmware.com/web/vmware/downloads의 VMware 다운로드 사이트에서 다운로드할 수 있습니다. Desktop & End-User Computing에서 번들형 .zip 파일이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

표 3-10. PCoIP 클라이언트 세션 변수

설정	설명
Configure PCoIP client image cache size policy	PCoIP 클라이언트 이미지 캐시의 크기를 제어합니다. 클라이언트는 이미지 캐싱을 사용하여 이전에 전송된 디스플레이의 일부를 저장합니다. 이미지 캐싱은 재전송된 데이터 양을 감소시킵니다. 이 설정이 구성되지 않았거나 사용하지 않도록 설정된 경우, PCoIP는 기본 클라이언트 이미지 캐시 크기 250MB를 사용합니다. 이 설정을 사용할 경우, 클라이언트 이미지 캐시 크기를 최소 50MB에서 최대 300MB로 구성할 수 있습니다. 기본값은 250MB입니다.
Configure PCoIP event log verbosity	PCoIP 이벤트 로그의 자세한 표시 수준을 설정합니다. 값의 범위는 0(최대한 간단하게)~3(최대한 자세하게)입니다. 이 설정을 사용하도록 설정하면 자세한 표시 수준을 0에서 3까지 설정할 수 있습니다. 이 설정을 구성하지 않거나 사용하지 않도록 설정하면 이벤트 로그의 자세한 표시 수준이 2로 기본 설정됩니다. 활성 PCoIP 세션 도중 이 설정을 수정하면 새 설정이 즉시 적용됩니다.
Configure PCoIP session encryption algorithms	세션 협상 중 PCoIP 끝점에 의해 보급된 암호화 알고리즘을 제어합니다. 확인란 중 하나를 선택하면 연결된 암호화 알고리즘이 사용되지 않도록 설정됩니다. 적어도 한 개의 알고리즘을 사용하도록 설정해야 합니다. 이 설정은 에이전트 및 클라이언트 모두에 적용됩니다. 끝점은 사용하는 실제 세션 암호화 알고리즘을 협상합니다. FIPS140-2 승인 모드가 사용 설정된 경우 AES-128-GCM 암호화와 AES-256-GCM 암호화가 모두 사용 안 함으로 설정되었다면 **AES-128-GCM 암호화 사용 안 함** 값이 대체됩니다. Configure SSL Connections 설정이 사용되도록 설정되거나 구성되지 않은 경우, Salsa20-256round12 및 AES-128-GCM 알고리즘 모두 이 끝점에 의해 협상에 사용 가능합니다. 지원되는 암호화 알고리즘을 우선 순위에 따라 나열하면 SALSA20/12-256, AES-GCM-128 및 AES-GCM-256이며, 기본적으로 지원되는 모든 암호화 알고리즘을 이 끝점에서 협상에 사용할 수 있습니다.
Configure PCoIP virtual channels	PCoIP 세션에서 작동할 수 있는 가상 채널 및 작동할 수 없는 가상 채널을 지정합니다. 또한 이 설정은 PCoIP 호스트에서 클립보드 처리를 사용하지 않도록 설정할지 여부를 결정합니다. PCoIP 세션에서 사용되는 가상 채널은 가상 채널 인증 목록에 나타나야 합니다. 인증되지 않은 가상 채널 목록에 나타나는 가상 채널은 PCoIP 세션에서 사용될 수 없습니다. PCoIP 세션에서 사용하기 위해 최대 15개의 가상 채널을 지정할 수 있습니다. 여러 채널 이름을 세로 막대(|) 문자로 구분하십시오. 예를 들어, mksvchan 및 vdp_rdpvcbridge 가상 채널을 허용하는 가상 채널 인증 문자열은 **mksvchan|vdp_rdpvcbridge**입니다. 채널 이름이 세로 막대 또는 백슬래시(\) 문자를 포함할 경우, 그 앞에 백슬래시 문자를 삽입합니다. 예를 들어, 채널 이름 awk|ward\channel을 **awk\\|ward\\\channel**로 입력하십시오. 인증된 가상 채널 목록이 빈 경우, 모든 가상 채널이 허용되지 않습니다. 인증되지 않은 가상 채널 목록이 빈 경우, 모든 가상 채널이 허용됩니다. 가상 채널 설정은 에이전트 및 클라이언트 모두에 적용됩니다. 가상 채널을 사용하려면 에이전트 및 클라이언트 모두에서 가상 채널을 사용하도록 설정해야 합니다. 가상 채널 설정에는 PCoIP 호스트에서 원격 클립보드 처리를 사용하지 않도록 설정할 수 있는 개별 확인란이 있습니다. 이 값은 에이전트에만 적용됩니다. 기본적으로 클립보드 처리를 포함한 모든 가상 채널이 사용되도록 설정됩니다.

표 3-10. PCoIP 클라이언트 세션 변수 (계속)

설정	설명
Configure the Client PCoIP UDP port	소프트웨어 PCoIP 클라이언트에서 사용하는 UDP 클라이언트 포트를 지정합니다. UDP 포트 값은 사용할 기본 UDP 포트를 지정합니다. UDP 포트 범위 값은 기본 포트를 사용할 수 없을 경우 시도할 추가 포트의 수를 결정합니다. 범위는 기본 포트에서 기본 포트 및 포트 범위의 합계까지 스팬합니다. 예를 들어, 기본 포트가 50002이고 포트 범위가 64인 경우, 범위는 50002에서 50066까지 스팬합니다. 이 설정은 클라이언트에만 적용됩니다. 기본적으로 기본 포트는 50002이고 포트 범위는 64입니다.
Configure the maximum PCoIP session bandwidth	PCoIP 세션에서 초당 킬로비트로 최대 대역폭을 지정합니다. 대역폭은 모든 이미징, 오디오, 가상 채널, USB 및 컨트롤 PCoIP 트래픽을 포함합니다. 예상되는 동시 PCoIP 세션 수를 고려하여 이 값을 끝점이 연결되는 링크의 전체 용량으로 설정합니다. 예를 들어 4Mbit/s 인터넷 연결을 통해 연결하는 단일 사용자 VDI 구성(단일 PCoIP 세션)의 경우 이 값을 4Mbit로 설정하거나 다른 네트워크 트래픽에서 사용할 수 있는 양을 남겨 두기 위해 4Mbit보다 10% 적게 설정합니다. 여러 개의 동시 PCoIP 세션에서 링크를 공유하여 여러 VDI 사용자 또는 단일 RDS 구성을 형성할 것으로 예상되는 경우 그에 따라 설정을 조정할 수도 있습니다. 하지만 이 값을 낮게 설정하면 각 활성 세션의 최대 대역폭이 제한됩니다. 이 값을 설정하면 에이전트가 링크 용량보다 더 높은 비율로 전송하지 못하도록 하여 과도한 패킷 손실 및 열악한 사용자 환경으로 이어지는 것을 방지합니다. 이 값은 대칭형입니다. 클라이언트 및 에이전트가 클라이언트 및 에이전트 쪽에 설정된 두 값 중 더 낮은 값을 강제로 사용하도록 합니다. 예를 들어 클라이언트에서 4Mbit/s 최대 대역폭 설정이 구성되어도 에이전트가 더 낮은 비율을 사용하여 전송하도록 강제됩니다. 이 설정을 사용하지 않거나 끝점에 구성되지 않은 경우 끝점은 대역폭 제약을 부과하지 않습니다. 이 설정이 구성된 경우 설정은 끝점의 최대 대역폭 제약(초당 킬로비트)으로 사용됩니다. 이 설정이 구성되지 않은 경우 기본값은 초당 900000 킬로비트입니다. 이 설정은 에이전트 및 클라이언트에 적용됩니다. 두 개의 끝점에서 설정이 다른 경우, 더 낮은 값이 사용됩니다.
Configure the PCoIP transport header	PCoIP 전송 헤더를 구성하고 전송 세션 우선 순위를 설정합니다. PCoIP 전송 헤더는 모든 PCoIP UDP 패킷에 추가(전송 헤더가 사용하도록 설정되어 있고 양쪽 모두에서 지원하는 경우에만 해당)되는 32비트 헤더입니다. PCoIP 전송 헤더는 네트워크 디바이스가 네트워크 정체를 처리할 때 더 효율적으로 우선 수위를 지정하거나 QoS를 결정할 수 있도록 지원합니다. 기본적으로 전송 헤더를 사용하도록 설정되어 있습니다. 전송 세션 우선 순위는 PCoIP 전송 헤더에 보고되는 PCoIP 세션 우선 순위를 결정합니다. 네트워크 디바이스가 지정된 전송 세션 우선 순위에 따라 더 효율적으로 우선 순위를 지정하거나 QoS를 결정할 수 있도록 합니다. Configure the PCoIP transport header 설정을 사용하도록 설정한 경우 다음 전송 세션 우선 순위를 사용할 수 있습니다. ■ **높음** ■ **중간**(기본값) ■ **낮음** ■ **정의되지 않음** PCoIP 에이전트와 클라이언트가 전송 세션 우선 순위 값을 협상합니다. PCoIP 에이전트가 전송 세션 우선 순위 값을 지정하면 세션이 에이전트에서 지정한 세션 우선 순위를 사용합니다. 클라이언트에서만 전송 세션 우선 순위를 지정한 경우 세션이 클라이언트에서 지정한 세션 우선 순위를 사용합니다. 에이전트와 클라이언트 모두 전송 세션 우선 순위를 지정하지 않았거나 **정의되지 않은 우선 순위**가 지정된 경우 세션이 기본 값인 **중간** 우선 순위를 사용합니다.

표 3-10. PCoIP 클라이언트 세션 변수 (계속)

설정	설명
Enable/disable audio in the PCoIP session	오디오가 PCoIP 세션에서 사용되도록 설정되었는지 확인합니다. 양 끝점에 오디오가 사용되도록 설정되어 있어야 합니다. 이 설정이 사용되도록 설정된 경우, PCoIP 오디오가 허용됩니다. 이 설정이 사용되지 않도록 설정된 경우 PCoIP 오디오가 사용되지 않도록 설정됩니다. 이 설정이 구성되지 않은 경우, 오디오가 기본적으로 사용되도록 설정됩니다.
Configure the PCoIP session bandwidth floor	PCoIP 세션으로 예약된 대역폭을 위해 초당 킬로비트로 더 낮은 제한을 지정합니다. 이 설정은 끝점을 위해 예상된 최소 대역폭 전송률을 구성합니다. 이 설정을 사용하여 끝점을 위해 대역폭을 예약할 경우, 사용자는 대역폭을 사용할 수 있을 때까지 기다릴 필요가 없습니다(세션 응답을 향상시킴). 모든 끝점을 위해 예약된 총 대역폭을 초과 가입하지 않았는지 확인하십시오. 구성에서 모든 연결을 위한 대역폭 층의 합계는 네트워크 용량을 초과하지 않아야 합니다. 기본값은 0으로, 이는 최소 대역폭이 예약되어 있지 않음을 의미합니다. 이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우 예약된 최소 대역폭이 없습니다. 이 설정은 에이전트 및 클라이언트에 적용되지만 이 설정이 구성된 끝점에만 영향을 줍니다. 활성 PCoIP 세션 도중 이 설정을 수정하면 변경 사항이 즉시 적용됩니다.
Configure the PCoIP session MTU	PCoIP 세션의 UDP 패킷을 위해 MTU(최대 전송 단위) 크기를 지정합니다. MTU 크기는 IP 및 UDP 패킷 머리글을 포함합니다. TCP는 표준 MTU 발견 메커니즘을 사용하여 MTU를 설정하며 이 설정으로 영향을 받지 않습니다. 최대 MTU 크기는 1500바이트입니다. 최소 MTU 크기는 500바이트입니다. 기본값은 1300바이트입니다. 일반적으로 MTU 크기를 변경할 필요가 없습니다. 비정상적인 네트워크 설치로 인해 PCoIP 패킷 조각화가 발생할 경우 이 값을 변경하십시오. 이 설정은 에이전트 및 클라이언트에 적용됩니다. 두 개의 끝점에서 MTU 크기 설정이 다른 경우, 가장 작은 크기가 사용됩니다. 이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우 클라이언트는 에이전트와의 협상에서 기본값을 사용합니다.
Configure SSL connections to satisfy Security Tools	SSL 세션 협상 연결의 설정 방법을 지정합니다. 포트 스캐너와 같은 보안 도구를 충족하려면 이 설정을 사용하도록 지정하고 다음을 수행하십시오. 1 PCoIP에 사용할 서버 인증서에 서명한 인증 기관의 인증서를 신뢰할 수 있는 루트 인증서 저장소에 저장합니다. 2 인증서 저장소에서만 인증서를 로드하도록 에이전트를 구성합니다. 로컬 시스템의 개인 저장소가 사용되는 경우 단계 1에서 다른 저장소 위치를 사용하지 않았다면 CA 인증서 저장소 이름을 ROOT 값으로 변경하지 않은 채로 둡니다. 이 설정이 사용되지 않도록 지정되거나 구성되지 않으면 AES-128 암호 제품군을 사용할 수 없으며 끝점은 시스템 계정의 MY 저장소의 인증 기관 인증서와 ROOT 저장소의 인증 기관 인증서를 사용합니다.
Configure SSL protocols	암호화된 SSL 연결이 설정되기 전에 특정 프로토콜의 사용을 제한하는 OpenSSL 프로토콜을 구성합니다. 프로토콜 목록은 콜론으로 구분된 하나 이상의 OpenSSL 프로토콜 문자열로 구성됩니다. 모든 암호 문자열은 대/소문자를 구분하지 않습니다. 기본값은 TLS1.1:TLS1.2입니다. 즉, TLS v1.1 및 TLS v1.2가 사용되도록 설정되고 SSL v2.0, SSLv3.0 및 TLS v1.0은 사용되지 않도록 설정됨을 의미합니다. 이 설정이 클라이언트 및 에이전트 둘 다에서 지정되면 OpenSSL 프로토콜 협상 규칙이 준수됩니다.

표 3-10. PCoIP 클라이언트 세션 변수 (계속)

설정	설명
Configure PCoIP event log cleanup by time in days	PCoIP 이벤트 로그 정리 작업을 일수에 따라 구성할 수 있습니다. 이 설정이 구성되면 일수에 따라 로그 파일 정리가 제어됩니다. 예를 들어 n을 0이 아닌 값으로 설정하면 n일보다 오래된 로그 파일이 자동으로 삭제됩니다. 설정 값이 0이면 일수에 따라 파일 정리가 수행되지 않음을 나타냅니다. 이 정책이 사용되지 않도록 설정되거나 구성되지 않은 경우 일수에 따른 기본 이벤트 로그 정리 설정은 7입니다. 로그 파일 정리는 세션을 시작할 때 한 번 수행됩니다. 변경된 설정은 다음 세션까지 적용됩니다.
Configure PCoIP event log cleanup by size in MB	PCoIP 이벤트 로그 정리 작업을 크기(MB)에 따라 구성할 수 있습니다. 이 설정이 구성되면 크기(MB)에 따라 로그 파일 정리가 제어됩니다. 예를 들어 m을 0이 아닌 값으로 설정하면 mMB보다 큰 로그 파일이 자동으로 삭제됩니다. 설정 값이 0이면 크기에 따라 파일 정리가 수행되지 않음을 나타냅니다. 이 설정이 사용되지 않도록 지정되거나 구성되지 않은 경우 크기(MB)에 따른 기본 이벤트 로그 정리 설정은 100입니다.

명령줄에서 Horizon Client 실행

명령줄 또는 스크립트에서 Window용 Horizon Client를 실행할 수 있습니다. 최종 사용자가 데스크톱 애플리케이션에 액세스할 권한을 부여하는 키오스크 기반 애플리케이션을 실행할 경우 이 작업을 수행하고자 할 수 있습니다.

vmware-view.exe 명령을 사용하여 명령줄에서 Windows용 Horizon Client를 실행합니다. 명령에는 Horizon Client의 동작을 변경하도록 지정할 수 있는 옵션이 포함되어 있습니다.

Horizon Client 명령 사용

vmware-view 명령 구문이 Horizon Client 작업을 제어합니다.

Windows 명령 프롬프트에서 다음 vmware-view 명령 형식을 사용합니다.

```
vmware-view [command_line_option [argument]] ...
```

vmware-view 명령 실행 파일에 대한 기본 경로는 시스템에 따라 다릅니다.

- 32비트 시스템의 경우 경로는 C:₩Program Files₩VMware₩VMware Horizon View Client₩입니다.
- 64비트 시스템의 경우 경로는 C:₩Program Files (x86)₩VMware₩VMware Horizon View Client₩입니다.

편의를 위해 이 경로를 PATH 환경 변수에 이 경로를 추가하십시오.

다음 표에는 vmware-view 명령과 함께 사용할 수 있는 명령줄 옵션이 나와 있습니다.

표 3-11. Horizon Client 명령줄 옵션

옵션	설명
/?	명령 옵션 목록을 표시합니다.
-appName application_name	데스크톱 및 애플리케이션 선택 창에 표시될 애플리케이션의 이름을 지정합니다. 이 이름은 풀 생성 마법사에서 애플리케이션 풀에 대해 지정한 디스플레이 이름입니다.

표 3-11. Horizon Client 명령줄 옵션 (계속)

옵션	설명
-appProtocol protocol	사용할 원격 애플리케이션 디스플레이 프로토콜(사용 가능한 경우)을 지정합니다. 디스플레이 프로토콜은 Blast 또는 PCoIP일 수 있습니다.
-appSessionReconnectionBehavior 인수	애플리케이션 다시 연결 동작 설정을 지정합니다. ■ always: **열려 있는 애플리케이션에 자동으로 다시 연결** 구현 ■ never: **묻지 않고 자동으로 다시 연결하지 않음** 구현 ■ ask: **열려 있는 애플리케이션에 다시 연결할지 묻기** 구현 이 옵션을 사용하면 애플리케이션 다시 연결 설정이 Horizon Client의 [설정] 페이지에서 사용하지 않도록 설정됩니다.
-args 인수	원격 애플리케이션 실행에 추가할 명령줄 인수를 지정합니다. 예: vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "W"my new.txtW""
-connectUSBOnStartup	true로 설정되면 모든 USB 디바이스를 현재 호스트에 연결된 데스크톱으로 리디렉션합니다. -unattended 옵션을 지정할 경우 이 옵션이 암시적으로 설정됩니다. 기본값은 false입니다.
-connectUSBOnInsert	true로 설정하면 디바이스를 플러그인할 때 USB 디바이스를 포그라운드 데스크톱에 연결합니다. -unattended 옵션을 지정할 경우 이 옵션이 암시적으로 설정됩니다. 기본값은 false입니다.
-desktopLayout window_size	데스크톱의 창 표시 방법을 지정합니다. **fullscreen** 전체 화면을 표시합니다. **multimonitor** 다중 모니터를 표시합니다. **windowLarge** 큰 창입니다. **windowSmall** 작은 창입니다. **length X width** 사용자 지정 크기: 예: 800 X 600
-desktopName desktop_name	데스크톱 및 애플리케이션 선택 창에 표시될 데스크톱의 이름을 지정합니다. 이 이름은 풀 생성 마법사에서 풀에 대해 지정한 디스플레이 이름입니다. **중요** 키오스크 모드로 실행되는 클라이언트의 경우 이 옵션을 지정하지 마십시오. 이 옵션은 데스크톱이 키오스크 모드로 실행되는 경우 효과가 없습니다. 키오스크 모드에서는 권한이 부여된 데스크톱 목록의 첫 번째 데스크톱과 연결이 설정됩니다.
-desktopProtocol protocol	데스크톱 및 애플리케이션 선택 창에 표시될 디스플레이 프로토콜을 지정합니다. 디스플레이 프로토콜은 Blast, PCoIP 또는 RDP입니다.
-domainName domain_name	최종 사용자가 Horizon Client에 로그인하는 데 사용할 NETBIOS 도메인을 지정합니다. 예를 들면 mycompany.com보다는 mycompany를 사용합니다.
-file file_path	추가 명령 옵션 및 인수를 포함하는 구성 파일의 경로를 지정합니다. Horizon Client 구성 파일를 참조하십시오.
-h	도움말 옵션을 표시합니다.
-hideClientAfterLaunchSession	true로 설정되면 원격 세션을 시작한 후에 원격 데스크톱 및 애플리케이션 선택기 창과 **VMware Horizon Client 표시** 메뉴가 숨겨집니다. false로 설정되면 원격 세션을 시작한 후에 원격 데스크톱 및 애플리케이션 선택기 창과 **VMware Horizon Client 표시** 메뉴가 표시됩니다. 기본값은 true입니다.

표 3-11. Horizon Client 명령줄 옵션 (계속)

옵션	설명
-languageId Locale_ID	Horizon Client에서 여러 언어에 대한 지역화 지원을 제공합니다. 리소스 라이브러리를 사용할 수 있는 경우, 사용할 로컬 ID(LCID)를 지정하십시오. 미국 영어의 경우 0x409 값을 입력하십시오.

-listMonitors	연결된 모니터에 대한 인덱스 값과 디스플레이 레이아웃 정보를 나열합니다. 예:
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (-900, -410, 0, 1190)`
	-monitors 옵션에서 인덱스 값을 사용할 수 있습니다.

-logInAsCurrentUser	true로 설정하면 최종 사용자가 클라이언트 시스템에 로그인할 때 제공하는 자격 증명 정보를 사용하여 연결 서버 그리고 최종적으로 원격 데스크톱에 로그인합니다. 기본값은 false입니다.
-monitors "n[,n,n,n]"	다중 모니터 설정에서 사용할 모니터를 지정합니다. 여기서 n은 모니터의 인덱스 값입니다. -listMonitors 옵션을 사용하여 연결된 모니터의 인덱스 값을 결정합니다. 쉼표로 구분된 인덱스 값을 4개까지 지정할 수 있습니다. 예: **-monitors "1,2"** 이 옵션은 -desktopLayout을 multimonitor로 설정하지 않으면 적용되지 않습니다.
-nonInteractive	스크립트에서 Horizon Client를 시작할 때 오류 메시지 상자를 생략합니다. -unattended 옵션을 지정할 경우 이 옵션이 암시적으로 설정됩니다.
-noVMwareAddins	가상 인쇄와 같은 VMware 고유의 가상 채널을 로드하지 못하게 합니다.
-password password	최종 사용자가 Horizon Client에 로그인하는 데 사용할 암호를 지정합니다. 암호는 명령 콘솔이나 모든 스크립팅 도구를 통해 일반 텍스트로 처리됩니다. 암호를 자동으로 생성할 경우 키오스크 모드에서 클라이언트를 위해 이 옵션을 지정할 필요가 없습니다. 보안을 강화하기 위해 이 옵션을 지정하지 않는 것이 좋습니다. 사용자는 대화형으로 암호를 입력할 수 있습니다.
-printEnvironmentInfo	클라이언트 디바이스의 시스템 이름, IP 주소 및 MAC 주소를 표시합니다.
-serverURL connection_server	연결 서버 인스턴스의 URL, IP 주소 또는 FQDN을 지정합니다.
-shutdown	모든 데스크톱 및 애플리케이션과 관련 UI 구성 요소를 종료합니다.
-singleAutoConnect	사용자가 하나의 원격 데스크톱 또는 애플리케이션에 대한 권한만 있는 경우 서버에서 사용자 인증을 마치면 데스크톱 또는 애플리케이션이 자동으로 연결되고 사용자가 로그인되도록 지정합니다. 이 설정을 사용하면 하나의 항목만 포함된 목록에서 데스크톱이나 애플리케이션을 선택해야 하는 번거로움을 피할 수 있습니다.
-smartCardPIN PIN	최종 사용자가 로그인을 위해 스마트 카드를 삽입할 때 PIN을 지정합니다.
-usernameHint user_name	사용자 이름 힌트로 사용할 계정 이름을 지정합니다.
-standalone	역호환성 용도로 지원됩니다. 이 클라이언트에 대한 기본 동작입니다. -standalone을 지정할 필요가 없습니다. 동일하거나 다른 연결 서버 인스턴스에 연결할 수 있는 Horizon Client의 두 번째 인스턴스를 실행합니다. 동일한 서버 또는 다른 서버에 여러 데스크톱을 연결하는 경우, 보안 터널 사용은 지원되지 않습니다. **참고** 두 번째 데스크톱 연결에는 USB 디바이스, 스마트 카드, 프린터 및 다중 모니터와 같은 로컬 하드웨어에 대한 액세스 권한이 없을 수 있습니다.
-supportText file_name	텍스트 파일의 전체 경로를 지정합니다. 파일 내용이 [지원 정보] 대화상자에 표시됩니다.

표 3-11. Horizon Client 명령줄 옵션 (계속)

옵션	설명
-unattended	키오스크 모드의 클라이언트에 적합한 비대화식 모드에서 Horizon Client를 실행합니다. 또한 다음을 지정해야 합니다. ■ 클라이언트의 계정 이름(클라이언트 디바이스의 MAC 주소에서 계정 이름을 생성하지 않은 경우). 이름은 “custom-” 문자열 또는 ADAM에서 구성한 대체 접두사로 시작해야 합니다. ■ 클라이언트의 암호(클라이언트의 계정을 설정할 때 자동으로 암호를 생성하지 않은 경우). -unattended 옵션은 -nonInteractive, -connectUSBOnStartup, -connectUSBOnInsert 및 -desktopLayout multimonitor 옵션을 암시적으로 설정합니다.
-unauthenticatedAccessAccount	인증되지 않은 액세스를 사용하도록 설정된 경우 서버에 익명으로 로그인하는 데 사용할 인증되지 않은 액세스 사용자 계정을 지정합니다. 인증되지 않은 액세스가 사용되지 않도록 설정되면 이 옵션은 무시됩니다. 예: `vmware-view.exe -serverURL ag-broker.agwork.com -unauthenticatedAccessEnabled true -unauthenticatedAccessAccount anonymous1`
-unauthenticatedAccessEnabled	인증되지 않은 액세스 동작 지정: ■ true는 인증되지 않은 액세스를 사용하도록 설정합니다. 인증되지 않은 액세스를 사용할 수 없는 경우 클라이언트는 다른 인증 방식으로 변경할 수 있습니다. **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정은 Horizon Client에서 표시되고 사용되지 않도록 설정되며 선택됩니다. ■ false의 경우 애플리케이션에 로그인하고 액세스하기 위해서는 자격 증명을 입력해야 합니다. **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정은 Horizon Client에서 숨겨지고 선택 해제됩니다. 이 옵션을 지정하지 않으면 Horizon Client에서 인증되지 않은 액세스를 사용하도록 설정할 수 있습니다. **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정이 표시되고 사용되도록 설정되며 선택 해제됩니다.

표 3-11. Horizon Client 명령줄 옵션 (계속)

옵션	설명

-useExisting	단일 Horizon Client 세션에서 여러 원격 데스크톱 및 애플리케이션을 실행할 수 있습니다.
	이 옵션을 지정하면 Horizon Client는 동일한 사용자 이름, 도메인 및 서버 URL이 있는 세션이 이미 존재하는지 확인하고, 존재하는 경우 새 세션을 생성하는 대신 해당 세션을 다시 사용합니다.
	예를 들어 다음 명령에서 user-1은 계산기 애플리케이션을 실행하고 새 세션이 생성됩니다.
	`vmware-view.exe -userName user-1 -password secret -domainName domain -appName Calculator -serverURL view.mycompany.com -useExisting`
	다음 명령에서 user1은 동일한 사용자 이름, 도메인 및 서버 URL이 있는 그림판 애플리케이션을 실행하고 동일한 세션이 사용됩니다.
	`vmware-view.exe -userName user-1 -password secret -domainName domain -appName Paint -serverURL view.mycompany.com -useExisting`

-userName user_name	최종 사용자가 Horizon Client에 로그인하는 데 사용할 계정 이름을 지정합니다. 클라이언트 디바이스의 MAC 주소에서 계정 이름을 생성할 경우 키오스크 모드의 클라이언트를 위해 이 옵션을 지정할 필요가 없습니다.

-file, -languageId, -printEnvironmentInfo, -smartCardPIN 및 -unattended를 제외하고 Active Directory 그룹 정책을 사용하여 모든 옵션을 지정할 수 있습니다.

참고 그룹 정책 설정은 명령줄에서 지정하는 설정보다 우선적으로 적용됩니다.

Horizon Client 구성 파일

구성 파일에서 Horizon Client에 대한 명령줄 옵션을 읽을 수 있습니다.

구성 파일의 경로를 vmware-view 명령의 -filefile_path 옵션에 대한 인수로 지정할 수 있습니다. 파일은 유니코드(UTF-16) 또는 ASCII 텍스트 파일이어야 합니다.

예: 비대화식 애플리케이션을 위한 구성 파일의 예

다음 예는 비대화식 애플리케이션에 대한 구성 파일의 내용을 보여줍니다.

```
-serverURL https://view.yourcompany.com
-userName autouser
-password auto123
-domainName companydomain
-desktopName autodesktop
-nonInteractive
```

예: 키오스크 모드에서 클라이언트를 위한 구성 파일의 예

다음 예는 계정 이름이 MAC 주소 기반인 키오스크 모드의 클라이언트를 보여줍니다. 이 클라이언트에는 자동으로 생성된 암호가 있습니다.

```
-serverURL 145.124.24.100
-unattended
```

Windows 레지스트리를 사용하여 Horizon Client 구성

명령줄에서 이러한 설정을 지정하는 대신 Windows 레지스트리에서 Horizon Client를 위한 기본 설정을 정의할 수 있습니다. 그룹 정책 설정은 Windows 레지스트리 설정보다 우선하고, Windows 레지스트리 설정은 명령줄보다 우선합니다.

참고 향후 릴리스에서는 이 섹션에 설명된 Windows 레지스트리 설정이 지원되지 않을 수 있습니다. 이 경우 GPO 설정을 사용해야 합니다.

표 3-12에는 Horizon Client에 로그인하기 위한 레지스트리 설정이 나와 있습니다. 이러한 설정은 레지스트리의 HKEY_CURRENT_USER₩Software₩VMware, Inc.₩VMware VDM₩Client₩ 아래 위치합니다. 이 위치는 특정 사용자에 따라 다른 반면에 다음 표에 설명된 HKEY_LOCAL_MACHINE 설정은 컴퓨터 전역 설정이며 컴퓨터에 로그인할 권한을 가진 Windows 도메인 환경의 모든 로컬 사용자 및 모든 도메인 사용자에게 적용됩니다.

표 3-12. 자격 증명을 위한 Horizon Client 레지스트리 설정

레지스트리 설정	설명
암호	기본 암호를 지정합니다.
UserName	기본 사용자 이름을 지정합니다.

표 3-13에는 로그인 자격 증명이 없는 Horizon Client를 위한 레지스트리 설정이 나와 있습니다. 이러한 설정의 위치는 다음과 같이 시스템 유형에 따라 다릅니다.

- 32비트 Windows: HKEY_LOCAL_MACHINE₩Software₩VMware, Inc.₩VMware VDM₩Client₩
- 64비트 Windows: HKLM₩SOFTWARE₩Wow6432Node₩VMware, Inc.₩VMware VDM₩Client₩

표 3-13. Horizon Client 레지스트리 설정

레지스트리 설정	설명
DomainName	기본 NETBIOS 도메인 이름을 지정합니다. 예를 들면 mycompany.com보다는 mycompany를 사용합니다.
EnableShade	Horizon Client 창의 상단에 있는 메뉴 표시줄(음영)이 사용되도록 설정할지 여부를 지정합니다. 키오스크 모드의 클라이언트는 제외하고 메뉴 표시줄은 기본적으로 활성화되어 있습니다. **false** 값은 메뉴 표시줄을 비활성화합니다. **참고** 이 설정은 디스플레이 레이아웃을 **모든 모니터** 또는 **전체 화면**으로 설정한 경우에만 적용할 수 있습니다.

표 3-13. Horizon Client 레지스트리 설정 (계속)

레지스트리 설정	설명
ServerURL	URL, IP 주소 또는 FQDN을 사용하여 기본 연결 서버 인스턴스를 지정합니다.
EnableSoftKeypad	**true**로 설정되어 있으며 Horizon Client 창에 포커스가 있는 경우 마우스 또는 화면 키보드가 Horizon Client 창 외부에 있더라도 물리적 키보드, 화면 키보드, 마우스 및 필기 패드 이벤트가 원격 데스크톱 또는 원격 애플리케이션으로 전송됩니다. 기본값은 **false**입니다.

다음 표에는 추가 가능한 보안 설정이 나와 있습니다. 이러한 설정의 위치는 다음과 같이 시스템 유형에 따라 다릅니다.

- 32비트 Windows: HKEY_LOCAL_MACHINE₩Software₩VMware, Inc.₩VMware VDM₩Client₩Security
- 64비트 Windows: HKLM₩SOFTWARE₩Wow6432Node₩VMware, Inc.₩VMware VDM₩Client₩Security

표 3-14. 보안 설정

레지스트리 설정	설명 및 올바른 값
CertCheckMode	인증서 검사 모드를 지정합니다. ■ **0**은(는) Do not verify server identity certificates을(를) 구현합니다. ■ **1**은(는) Warn before connecting to untrusted servers을(를) 구현합니다. ■ **2**은(는) Never connect to untrusted servers을(를) 구현합니다.
SSLCipherList	암호화된 SSL 연결이 설정되기 전에 특정 암호화 알고리즘 및 프로토콜의 사용을 제한하는 암호 목록을 구성합니다. 암호 목록은 콜론으로 구분된 하나 이상의 암호 문자열로 구성됩니다. **참고** 모든 암호 문자열은 대소문자를 구분합니다. 기본값은 **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**입니다. 즉, TLSv.1, TLSv1.1 및 TLSv1.2가 사용되도록 설정됩니다. (SSL v2.0 및 v3.0은 제거됩니다.) 암호 그룹은 128비트 또는 256비트 AES를 사용하며 익명 DH 알고리즘을 제거한 다음 암호화 알고리즘 키 길이 순서로 현재 암호 목록을 정렬합니다. 구성에 대한 참조 링크: http://www.openssl.org/docs/apps/ciphers.html

원격 데스크톱 및 애플리케이션 연결 관리

4

Horizon Client를 사용하여 연결 서버 또는 보안 서버에 연결하고, 원격 데스크톱에서 로그인하거나 로그오프하고, 원격 애플리케이션을 사용합니다. 문제 해결을 위해 원격 데스크톱 및 애플리케이션을 재설정할 수도 있습니다.

관리자가 원격 데스크톱의 정책을 구성하는 방식에 따라 최종 사용자는 데스크톱에서 많은 작업을 수행할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- 원격 데스크톱 또는 애플리케이션에 연결
- 인증되지 않은 액세스를 사용하여 원격 애플리케이션에 연결
- 데스크톱 및 애플리케이션 선택기 사용에 관한 팁
- 로컬 폴더 및 드라이브에 대한 액세스 공유
- VMware Horizon Client 창 숨기기
- 데스크톱 또는 애플리케이션에 다시 연결
- 클라이언트 바탕 화면 또는 시작 메뉴에 데스크톱 또는 애플리케이션 바로 가기 생성
- 데스크톱 또는 애플리케이션 전환
- 로그오프 또는 연결 해제

원격 데스크톱 또는 애플리케이션에 연결

서버에 로그인한 후 사용 권한이 있는 원격 데스크톱 및 애플리케이션에 연결할 수 있습니다.

최종 사용자가 원격 데스크톱 및 애플리케이션에 액세스할 수 있도록 하기 전에 먼저 클라이언트 디바이스에서 원격 데스크톱 또는 애플리케이션에 연결할 수 있는지 테스트합니다. 서버를 지정하고 사용자 계정의 자격 증명을 제공해야 할 수 있습니다.

원격 애플리케이션을 사용하려면 연결 서버 6.0 이상에 연결해야 합니다.

Horizon Client가 원격 데스크톱에 설치되어 있어도 **현재 사용자로 로그인** 기능을 사용할 수 있습니다.

필수 조건

- 사용자 이름/암호, RSA SecurID 사용자 이름/암호, RADIUS 인증 사용자 이름/암호 또는 스마트 카드 PIN(개인 ID 번호)과 같은 로그인 자격 증명을 얻습니다.

- 로그인을 위한 NETBIOS 도메인 이름을 얻습니다. 예를 들어 mycompany.com보다는 mycompany를 사용할 수 있습니다.
- Horizon Client용 연결 서버 준비에 설명된 관리 작업을 수행하십시오.
- 회사 네트워크 외부에 있으면서 원격 데스크톱 또는 애플리케이션에 액세스하기 위해 보안 서버를 사용하지 않는 경우, 클라이언트 디바이스가 VPN 연결을 사용하도록 설정되어 있는지 확인하고 해당 연결을 켭니다.

  중요 대부분의 경우 VPN이 아닌 보안 서버를 사용합니다.

- 원격 데스크톱 또는 애플리케이션에 액세스하는 서버의 정규화된 도메인 이름(FQDN)이 있는지 확인합니다. 서버 이름에는 밑줄(_)을 사용할 수 없습니다. 포트가 443이 아닌 경우 포트 번호도 필요합니다.
- RDP 디스플레이 프로토콜을 사용하여 원격 데스크톱에 연결하려는 경우에는 AllowDirectRDP 에이전트 그룹 정책 설정을 사용하도록 설정했는지 확인합니다.
- 관리자가 허용한 경우 연결 서버에서 제시한 SSL 인증서에 대한 인증서 검사 모드를 구성합니다. 어떤 모드를 사용할지 결정하려면 Horizon Client의 인증서 검사 모드 설정를 참조하십시오.

프로시저

1. VPN 연결이 필요한 경우 VPN을 켭니다.
2. **VMware Horizon Client** 데스크톱 바로 가기를 두 번 클릭하거나 **시작 > 프로그램 > VMware Horizon Client**를 클릭합니다.
3. (선택 사항) 인증서 검사 모드를 설정하려면 메뉴 표시줄에서 **옵션** 버튼을 클릭하고 **SSL 구성**을 선택합니다.

   관리자가 허용한 경우에만 이 설정을 구성할 수 있습니다.
4. (선택 사항) 현재 로그인된 Windows 도메인 사용자로 로그인하려면 메뉴 표시줄에서 **옵션** 버튼을 클릭하고 **현재 사용자로 로그인**을 선택합니다.

   이 설정은 **현재 사용자로 로그인** 기능이 클라이언트 시스템에 설치되어 있는 경우 사용할 수 있습니다.
5. 추가된 서버가 없는 경우 **+ 서버 추가** 버튼을 두 번 클릭하거나 메뉴 표시줄에서 **+ 새 서버** 버튼을 클릭하고 연결 서버 또는 보안 서버의 이름을 입력하고 **연결**을 클릭합니다.

   Horizon Client와 연결 서버 간 연결에는 항상 SSL이 사용됩니다. SSL 연결의 기본 포트는 443입니다. 연결 서버가 기본 포트를 사용하도록 구성되지 않은 경우에는 다음 예의 형식을 사용합니다. `view.company.com:1443`.

   로그인 대화 상자가 나타나기 전에 확인 메시지가 표시될 수도 있습니다.

   참고 연결된 후에는 이 서버의 아이콘이 Horizon Client 홈 창에 저장됩니다. 이후에 Horizon Client를 사용하여 이 서버에 연결하려면 아이콘을 두 번 클릭하면 됩니다. 또는 이 단일 서버만 사용할 경우 서버의 아이콘을 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **이 서버에 자동 연결**을 선택합니다.

6 RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명을 묻는 메시지가 표시되면 사용자 이름과 암호를 입력하고 **계속**을 클릭합니다.

7 하나 이상의 데스크톱 또는 애플리케이션 풀을 사용할 권한이 있는 사용자의 자격 증명을 입력하고 도메인을 선택한 다음 **로그인**을 클릭합니다.

username@domain 형식을 사용하여 사용자 이름을 입력할 경우 이름은 @ 기호로 인해 UPN(사용자 주체 이름)으로 처리되므로 **도메인** 드롭다운 메뉴가 사용되지 않도록 설정됩니다.

도메인 드롭다운 메뉴가 숨겨져 있으면 사용자 이름을 *username@domain* 또는 *domain*₩*username*으로 입력해야 합니다.

8 (선택 사항) 원격 데스크톱의 디스플레이 설정을 구성하려면 데스크톱 아이콘을 마우스 오른쪽 버튼으로 클릭하거나 데스크톱 아이콘을 선택하고 창 위쪽에서 서버 이름 옆에 있는 **설정** 아이콘(톱니 모양)을 클릭합니다.

옵션	설명
디스플레이 프로토콜	관리자가 허용하는 경우 **연결 수단** 목록을 사용하여 디스플레이 프로토콜을 선택할 수 있습니다. VMware Blast에는 Horizon Agent 7.0 이상이 필요합니다.
디스플레이 레이아웃	**디스플레이** 목록을 사용하여 창 크기를 선택하거나 다중 모니터를 사용할 수 있습니다.

9 (선택 사항) 원격 데스크톱 또는 애플리케이션을 즐겨찾기로 표시하려면 데스크톱 또는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 클릭하고 나타나는 컨텍스트 메뉴에서 **즐겨찾기로 표시**를 선택합니다.

데스크톱 또는 애플리케이션 이름의 오른쪽 맨 위에 별 모양 아이콘이 나타납니다. 다음에 로그인할 때 **즐겨찾기 표시** 버튼을 클릭하여 이 애플리케이션 또는 데스크톱을 빠르게 찾을 수 있습니다.

10 원격 데스크톱 또는 애플리케이션에 연결하려면 아이콘을 두 번 클릭하거나 아이콘을 마우스 오른쪽 버튼으로 클릭한 후 컨텍스트 메뉴에서 **시작**을 선택합니다.

Microsoft RDS 호스트에서 호스팅되는 게시된 데스크톱에 연결하는 경우, 해당 데스크톱이 이미 다른 디스플레이 프로토콜을 사용하도록 설정되어 있으면 바로 연결되지 않습니다. 설정된 프로토콜을 사용할지, 아니면 선택한 프로토콜로 연결할 수 있도록 원격 운영 체제에서 로그오프할 것인지를 묻는 메시지가 나타납니다.

연결되면 원격 데스크톱 또는 애플리케이션 창이 나타납니다. 둘 이상의 데스크톱 또는 애플리케이션에 대한 권한이 있는 경우, 동시에 여러 항목에 연결할 수 있도록 데스크톱 및 애플리케이션 선택기 창도 계속 열려 있습니다.

공유 대화 상자에서 로컬 시스템의 파일에 대한 액세스를 허용하거나 거부할 수 있습니다. 자세한 내용은 로컬 폴더 및 드라이브에 대한 액세스 공유의 내용을 참조하십시오.

서버에 대한 인증이 실패하거나 클라이언트가 원격 데스크톱 또는 애플리케이션에 연결할 수 없는 경우 다음 작업을 수행하십시오.

- 연결 서버가 SSL을 사용하지 않도록 구성되어 있는지 확인합니다. 클라이언트 소프트웨어에는 SSL 연결이 필요합니다. Horizon Administrator의 전역 설정에서 **클라이언트 연결에 SSL 사용** 확인란이 선택 해제되어 있는지 검사합니다. 선택 해제되어 있다면 해당 확인란을 선택하여 SSL을 사용하거나, 클라이언트가 HTTPS 사용 로드 밸런서 또는 연결 서버에 HTTP로 연결하는 다른 중간 디바이스에 연결할 수 있도록 환경을 설정합니다.
- 연결 서버의 보안 인증서가 올바르게 작동하는지 확인합니다. 올바르게 작동하지 않는 경우, Horizon Administrator에서 데스크톱의 에이전트에 연결할 수 없다는 메시지가 표시될 수 있습니다. 이는 인증서 문제로 발생한 추가 연결 문제의 증상입니다.
- 연결 서버 인스턴스에 설정된 태그가 이 사용자의 연결을 허용하는지 확인합니다. View 관리 문서를 참조하십시오.
- 사용자에게 이 데스크톱 또는 애플리케이션에 액세스할 권한이 있는지 확인합니다. Horizon 7에서 가상 데스크톱 설정 또는 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.
- RDP 디스플레이 프로토콜을 사용하여 원격 데스크톱에 연결하는 경우 원격 운영 체제가 원격 데스크톱 연결을 허용하는지 확인합니다.

후속 작업

시작 설정을 구성합니다. 최종 사용자가 연결 서버 인스턴스의 호스트 이름을 제공할 필요가 없도록 하거나 다른 시작 설정을 구성하려는 경우에는 명령줄 옵션을 사용하여 데스크톱 바로 가기를 만드십시오. 명령줄에서 Horizon Client 실행를 참조하십시오.

인증되지 않은 액세스를 사용하여 원격 애플리케이션에 연결

관리자는 인증되지 않은 액세스 기능을 사용하여 인증되지 않은 액세스 사용자를 생성하고 이러한 사용자에게 연결 서버 인스턴스의 원격 애플리케이션에 대한 권한을 부여할 수 있습니다. 인증되지 않은 액세스 사용자는 서버에 익명으로 로그인하여 원격 애플리케이션에 연결할 수 있습니다.

기본적으로 사용자는 **옵션** 메뉴에서 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정을 선택하고 익명으로 로그인할 사용자 계정을 선택합니다. 관리자는 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 설정을 미리 선택하도록 그룹 정책 설정을 구성하여 특정한 인증되지 않은 액세스 사용자 계정을 갖는 사용자를 로그인할 수 있습니다.

필수 조건

- Horizon Client용 연결 서버 준비에 설명된 관리 작업을 수행하십시오.
- 연결 서버 인스턴스에서 인증되지 않은 액세스 사용자를 설정합니다. 자세한 내용은 View 관리 문서에서 “게시된 애플리케이션에 인증되지 않은 액세스 제공”을 참조하십시오.
- 회사 네트워크 외부에 있는 경우 클라이언트 디바이스가 VPN 연결을 사용하도록 설정되어 있는지 확인한 후 해당 연결을 설정하십시오.
- 원격 애플리케이션에 액세스하는 서버의 FQDN(정규화된 도메인 이름)이 있는지 확인합니다. 서버 이름에는 밑줄(_)을 사용할 수 없습니다. 포트가 443이 아닌 경우 포트 번호도 필요합니다.

- 관리자가 허용한 경우 연결 서버에서 제시한 SSL 인증서에 대한 인증서 검사 모드를 구성합니다. 어떤 모드를 사용할지 결정하려면 Horizon Client의 인증서 검사 모드 설정를 참조하십시오.
- (선택 사항) **인증되지 않은 액세스에 사용할 계정** 및 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인** 그룹 정책 설정을 구성하여 기본 인증되지 않은 액세스 동작을 변경합니다. 자세한 정보는 클라이언트 GPO에 대한 스크립팅 정의 설정의 내용을 참조하십시오.

프로시저

1 VPN 연결이 필요한 경우 VPN을 켭니다.

2 **VMware Horizon Client** 데스크톱 바로 가기를 두 번 클릭하거나 **시작 > 프로그램 > VMware Horizon Client**를 클릭합니다.

3 관리자가 이를 수행하도록 지시하는 경우 메뉴 표시줄에서 **옵션** 버튼을 클릭하고 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인**을 선택합니다.

클라이언트 시스템을 구성하는 방식에 따라 이 설정은 이미 선택되어 있을 수 있습니다.

4 (선택 사항) 인증서 검사 모드를 설정하려면 메뉴 표시줄에서 **옵션** 버튼을 클릭하고 **SSL 구성**을 선택합니다.

관리자가 허용한 경우에만 이 설정을 구성할 수 있습니다.

5 원격 애플리케이션에 대한 인증되지 않은 액세스 권한이 있는 서버에 연결합니다.

옵션	조치
새 서버에 연결	**+ 서버 추가** 버튼을 두 번 클릭하거나 메뉴 표시줄에서 **+ 새 서버** 버튼을 클릭하고 서버 이름을 입력한 후 **연결**을 클릭합니다.
기존 서버에 연결	Horizon Client 홈 창에서 서버 아이콘을 두 번 클릭합니다.

Horizon Client와 연결 서버 간 연결에는 항상 SSL이 사용됩니다. SSL 연결의 기본 포트는 443입니다. 연결 서버가 기본 포트를 사용하도록 구성되지 않은 경우에는 다음 예의 형식을 사용합니다. `view.company.com:1443`.

로그인 대화 상자가 나타나기 전에 확인 메시지가 표시될 수도 있습니다.

6 로그인 대화 상자가 나타나면 필요한 경우 **사용자 계정** 드롭다운 메뉴에서 사용자 계정을 선택합니다.

사용자 계정을 하나만 사용할 수 있는 경우 드롭다운 메뉴가 사용되지 않도록 설정되며 사용자 계정이 이미 선택되었을 것입니다.

7 (선택 사항) **항상 이 계정 사용** 확인란을 사용할 수 있는 경우 다음번에 서버에 연결할 때 로그인 대화 상자를 우회하려면 이를 선택합니다.

다음번에 서버에 연결하기 전에 이 설정을 선택 취소하려면 Horizon Client 홈 창에서 서버 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **저장되어 있는 인증되지 않은 액세스 계정 저장하지 않음**을 선택합니다.

8 **로그인**을 클릭하여 서버에 로그인합니다.

애플리케이션 선택 창이 나타납니다.

9 애플리케이션을 시작하려면 애플리케이션 아이콘을 두 번 클릭합니다.

데스크톱 및 애플리케이션 선택기 사용에 관한 팁

편의를 위해 Horizon Client 데스크톱 및 애플리케이션 선택기 화면의 아이콘 수를 줄이거나 재구성할 수 있습니다.

특정 서버에 인증 후 연결하면 사용 권한이 있는 모든 원격 데스크톱 및 애플리케이션에 대한 아이콘이 포함된 창이 나타납니다. 자주 사용하는 원격 데스크톱 및 애플리케이션을 빠르게 실행하려면 다음 제안 사항을 시도해 보십시오.

- 이름의 처음 몇 글자를 입력합니다. 예를 들어 Paint, PowerPoint 및 Publisher 아이콘이 있는 경우 pa를 입력하여 Paint 애플리케이션을 선택할 수 있습니다.

  입력한 문자와 일치하는 항목이 두 개 이상인 경우에는 F4 키를 눌러 일치하는 다음 항목으로 이동할 수 있습니다. 마지막 항목에 도달하면 F4 키를 눌러 일치하는 첫 번째 항목으로 돌아갈 수 있습니다.

- 아이콘을 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **즐겨찾기로 표시**를 선택하여 아이콘을 즐겨찾기로 표시합니다. 즐겨찾기를 선택한 후 **즐겨찾기 보기 표시** 버튼(별 모양 아이콘)을 클릭하여 즐겨찾기가 아닌 아이콘을 모두 제거합니다.

- 즐겨찾기 보기가 표시되어 있는 경우에는 아이콘을 선택하고 원하는 위치로 끌어서 아이콘 순서를 변경할 수 있습니다. 즐겨찾기 보기가 표시되어 있지 않은 경우에는 기본적으로 데스크톱 아이콘이 알파벳 순서로 먼저 나열된 다음 애플리케이션 아이콘이 알파벳 순서로 나열됩니다. 하지만 즐겨찾기 보기에서 아이콘을 끌어서 위치를 조정할 수 있습니다.

  아이콘의 순서는 서버와의 연결을 끊을 때 또는 애플리케이션이나 데스크톱을 실행할 때, 사용 중인 서버에 저장됩니다. 수동으로 서버 연결을 끊거나 항목을 실행하지 않는 경우에는 변경 내용이 저장되지 않습니다.

- 선택기 창을 사용하지 않고 자신의 로컬 데스크톱에서 원격 데스크톱 또는 애플리케이션에 액세스하려면 바로 가기를 만듭니다. 아이콘을 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **바로 가기 생성**을 선택합니다.

- 원격 데스크톱 또는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **시작 메뉴에 추가**를 선택하면 선택기 창을 열지 않고도 로컬 시작 메뉴에서 원격 데스크톱 또는 애플리케이션에 액세스할 수 있습니다.

참고 Windows 7 이상의 클라이언트 시스템을 사용 중인 경우에는 서버, 데스크톱 또는 애플리케이션에 연결한 후 Horizon Client를 열고 Windows 작업 표시줄에서 Horizon Client 아이콘을 마우스 오른쪽 버튼으로 클릭하여 최근 사용한 서버, 데스크톱 또는 애플리케이션을 선택할 수 있습니다. 목록에는 최대 10개의 항목이 나타납니다. 항목을 제거하려면 마우스 오른쪽 버튼으로 클릭하고 **이 목록에서 제거**를 선택합니다.

작업 표시줄에서 Horizon Client 아이콘을 마우스 오른쪽 버튼으로 클릭해도 이동 목록이 나타나지 않으면 작업 표시줄을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택한 다음 **시작 메뉴** 탭을 클릭합니다. 개인 정보 섹션에서 **최근에 사용한 항목을 저장하고 시작 메뉴 및 작업 표시줄에 표시** 확인란을 선택한 다음 **확인**을 클릭합니다.

로컬 폴더 및 드라이브에 대한 액세스 공유

Horizon Client에서 로컬 시스템에 있는 폴더 및 드라이브를 원격 데스크톱 및 애플리케이션과 공유하도록 구성할 수 있습니다. 드라이브는 매핑된 드라이브 및 USB 스토리지 디바이스를 포함할 수 있습니다. 이 기능을 클라이언트 드라이브 리디렉션이라 부릅니다.

Windows 운영 체제의 버전에 따라 Windows 원격 데스크톱에서 공유된 폴더 및 드라이브가 **내 PC** 폴더의 **장치 및 드라이브** 섹션이나 **컴퓨터** 폴더의 **기타** 섹션에 표시됩니다. 메모장과 같은 원격 애플리케이션에서 공유 폴더 또는 드라이브에 있는 파일을 탐색하고 열 수 있습니다. 공유하려고 선택한 폴더 및 드라이브가 파일 시스템에서 **MACHINE-NAME의 name** 이름 형식을 사용하는 네트워크 드라이브로 표시됩니다.

원격 데스크톱 또는 애플리케이션에 연결되어 있지 않아도 클라이언트 드라이브 리디렉션 설정을 구성할 수 있습니다. 설정은 모든 원격 데스크톱 및 애플리케이션에 적용됩니다. 즉, 로컬 클라이언트 폴더를 한 원격 데스크톱 또는 애플리케이션과만 공유하고 다른 원격 데스크톱 또는 애플리케이션과는 공유하지 않도록 설정을 구성할 수 없습니다.

로컬 파일 시스템에서 직접 원격 애플리케이션을 사용하여 로컬 파일을 여는 기능을 켤 수도 있습니다. 또한 로컬 파일을 마우스 오른쪽 버튼으로 클릭하면 **다음으로 열기** 메뉴에 사용 가능한 원격 애플리케이션이 표시됩니다. 파일을 두 번 클릭할 때 파일이 원격 애플리케이션에서 자동으로 열리도록 설정할 수도 있습니다. 이 기능을 사용하도록 설정하면 특정 파일 확장명을 갖는 로컬 파일 시스템의 모든 파일이 사용자가 로그인한 서버에 등록됩니다. 예를 들어 Microsoft Word가 서버에서 사용할 수 있는 원격 애플리케이션 중 하나이면 로컬 파일 시스템에서 .docx 파일을 마우스 오른쪽 버튼으로 클릭하고 원격 MS Word 애플리케이션에서 파일을 열 수 있습니다. 이 기능을 사용하려면 Horizon 6.2 서버 및 에이전트가 필요합니다.

관리자는 그룹 정책 설정을 사용하도록 설정하여 Horizon Client에서 클라이언트 드라이브 리디렉션 기능을 숨길 수 있습니다. 자세한 내용은 표 3-7에서 **파일 및 폴더 공유 사용 안 함**을 참조하십시오.

연결 서버 인스턴스에서 보안 터널이 사용되도록 설정된 상태에서 프록시 서버를 사용하도록 클라이언트 시스템의 브라우저를 구성하면 클라이언트 드라이브 리디렉션 성능이 저하될 수 있습니다. 최상의 클라이언트 드라이브 리디렉션 성능을 얻으려면 프록시 서버를 사용하지 않거나 LAN 설정을 자동으로 검색하도록 브라우저를 구성합니다.

필수 조건

원격 데스크톱 또는 애플리케이션과 폴더 및 드라이브를 공유하려면 클라이언트 드라이브 리디렉션 기능을 사용하도록 설정해야 합니다. 이 작업 동안 View Agent 6.1.1 이상 또는 Horizon Agent 7.0 이상이 설치되고 에이전트 **클라이언트 드라이브 리디렉션** 옵션이 사용되도록 설정됩니다. 또한 클라이언트 드라이브 리디렉션 동작을 제어하기 위한 설정 정책도 포함됩니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

프로시저

1 공유 패널이 표시된 설정 대화 상자를 엽니다.

옵션	설명
데스크톱 및 애플리케이션 선택 창에서	데스크톱 또는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택한 다음 나타난 창의 왼쪽 패널에서 **공유**를 선택합니다.
데스크톱 또는 애플리케이션에 연결하면 표시되는 공유 대화 상자에서	대화 상자에서 **설정 > 공유** 링크를 클릭합니다.
데스크톱 OS 내에서	메뉴 표시줄에서 **옵션 > 폴더 공유**를 선택합니다.

2 클라이언트 드라이브 리디렉션 설정을 구성합니다.

옵션	조치
특정 폴더 또는 드라이브를 원격 데스크톱 및 애플리케이션과 공유	**추가** 버튼을 클릭하고 공유할 폴더 또는 드라이브로 이동하여 선택한 다음 **확인**을 클릭합니다. **참고** 디바이스가 이미 USB 리디렉션 기능으로 원격 데스크톱이나 애플리케이션에 연결되어 있는 경우에는 USB 디바이스의 폴더를 공유할 수 없습니다. 또한 시작 시 또는 디바이스가 삽입될 때 USB 디바이스에 자동으로 연결되는 USB 리디렉션 기능은 켜지 마십시오. 이 기능을 켜면 다음에 Horizon Client를 시작하거나 USB 디바이스를 연결할 때 해당 디바이스가 클라이언트 드라이브 리디렉션 기능이 아닌 USB 리디렉션 기능을 사용하여 연결됩니다.
특정 폴더 또는 드라이브의 공유 중지	폴더 목록에서 폴더 또는 드라이브를 선택하고 **제거** 버튼을 클릭합니다.
로컬 사용자 디렉토리의 파일에 대한 원격 데스크톱 및 애플리케이션의 액세스 허용	**로컬 파일 user-name 공유** 확인란을 선택합니다.
USB 스토리지 디바이스를 원격 데스크톱 및 애플리케이션과 공유	**이동식 스토리지에 대한 액세스 허용** 확인란을 선택합니다. 클라이언트 드라이브 리디렉션 기능은 클라이언트 시스템에 삽입된 모든 USB 스토리지 디바이스와 모든 FireWire 및 Thunderbolt 연결 외부 드라이브를 자동으로 공유합니다. 따라서 공유할 특정 디바이스를 선택할 필요는 없습니다. **참고** USB 리디렉션 기능을 사용하여 원격 데스크톱 또는 애플리케이션에 이미 연결된 USB 스토리지 디바이스는 공유되지 않습니다. 이 확인란을 선택 해제하면 USB 리디렉션 기능을 사용하여 USB 스토리지 디바이스를 원격 데스크톱 및 애플리케이션에 연결할 수 있습니다.

옵션	조치
로컬 파일 시스템에서 원격 애플리케이션으로 로컬 파일을 여는 기능 설정	**호스팅된 애플리케이션에서 로컬 파일 열기** 확인란을 선택합니다. 이 옵션을 사용하는 경우 로컬 파일 시스템에서 파일을 마우스 오른쪽 버튼으로 클릭하고 원격 애플리케이션에서 파일을 열도록 선택합니다. 해당 파일 확장명을 갖는 모든 파일에 대해, 예를 들어 이 파일을 두 번 클릭하는 경우 기본적으로 원격 애플리케이션에서 열리도록 파일의 속성을 변경할 수도 있습니다. 파일을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택한 후 **변경**을 클릭하여 해당 형식의 파일을 열 원격 애플리케이션을 선택할 수 있습니다. 관리자가 이 기능을 사용하지 않도록 설정할 수 있습니다.
원격 데스크톱 또는 애플리케이션에 연결할 때 공유 대화 상자 표시 안 함	**데스크톱 또는 애플리케이션에 연결할 때 대화 상자 표시 안 함** 확인란을 선택합니다. 이 확인란이 선택 해제되어 있으면 서버에 연결한 후 데스크톱 또는 애플리케이션에 처음 연결할 때 공유 대화 상자가 나타납니다. 예를 들어, 서버에 로그인하여 데스크톱에 연결하면 공유 대화 상자가 표시됩니다. 그 후에 다른 데스크톱 또는 애플리케이션에 연결하면 대화 상자가 다시 표시되지 않습니다. 대화 상자를 다시 보려면 서버에서 연결을 해제한 다음 다시 로그인해야 합니다.

후속 작업

원격 데스크톱 또는 애플리케이션 내에서 공유 폴더를 볼 수 있는지 확인합니다.

- Windows 원격 데스크톱 내에서 파일 탐색기를 열고 **내 PC** 폴더의 **장치 및 드라이브** 폴더를 살펴보거나 Windows 탐색기를 열고 **컴퓨터** 폴더의 **기타** 섹션을 살펴봅니다.
- 해당되는 경우 원격 애플리케이션 내에서 **파일 > 열기** 또는 **파일 > 다른 이름으로 저장**을 선택하고 파일 시스템에서 **MACHINE-NAME의 folder-name** 이름 형식을 사용하는 네트워크 드라이브로 표시되는 폴더 또는 드라이브로 이동합니다.

VMware Horizon Client 창 숨기기

원격 데스크톱 또는 애플리케이션을 연 후 VMware Horizon Client 창을 숨길 수 있습니다.

또한 원격 데스크톱 또는 애플리케이션이 열린 후 항상 VMware Horizon Client 창을 숨기도록 환경설정을 설정할 수 있습니다.

참고 관리자는 그룹 정책 설정을 사용하여 원격 데스크톱 또는 애플리케이션을 연 후 창을 항상 숨길지 여부를 구성할 수 있습니다.

자세한 내용은 클라이언트 GPO에 대한 일반 설정의 내용을 참조하십시오.

프로시저

- 원격 데스크톱 또는 애플리케이션을 연 후 VMware Horizon Client 창을 숨기려면 VMware Horizon Client 창 모서리에 있는 **닫기** 버튼을 클릭합니다.
- 원격 데스크톱 또는 애플리케이션을 연 후 항상 VMware Horizon Client 창을 숨기도록 환경설정을 설정하려면 서버에 연결하기 전에 메뉴 표시줄에 있는 **옵션** 버튼을 클릭하고 **항목을 시작하면 선택기 숨기기**를 선택합니다.

- 숨겨진 VMware Horizon Client 창을 다시 표시하려면 시스템 트레이에서 VMware Horizon Client 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **VMware Horizon Client 표시**를 선택하거나 원격 데스크톱에 로그인했을 경우 메뉴 표시줄에서 **옵션** 버튼을 클릭하고 **다른 데스크톱으로 전환**을 선택합니다.

데스크톱 또는 애플리케이션에 다시 연결

보안을 위해 관리자는 특정 시간이 지난 후 사용자를 서버에서 로그오프하고 특정 시간(분) 동안 작업이 없으면 원격 애플리케이션을 잠그는 시간 제한을 설정합니다.

View 6.0 원격 애플리케이션 기능을 사용하면, 원격 애플리케이션을 특정 시간 동안 사용하지 않을 경우 애플리케이션이 자동으로 잠기기 30초 전에 경고 프롬프트가 나타납니다. 여기에 응답하지 않으면 애플리케이션이 잠깁니다. 기본적으로 시간 제한은 15분 동안 작업이 없을 때이지만 관리자가 이 시간을 변경할 수 있습니다.

예를 들어 하나 이상의 애플리케이션을 열어 두고 컴퓨터를 떠났다가 1시간 후에 돌아오면 애플리케이션 창이 더 이상 열려 있지 않을 수 있습니다. 대신, 애플리케이션 창을 (Suggested to use comma for clear meaning.) 다시 표시하려면 **확인** 버튼을 클릭하라는 대화 상자가 표시될 수 있습니다.

서버 시간 제한은 일반적으로 특정 시간 동안 아무런 작업도 수행되지 않는 경우에 대해 설정됩니다. 기본적으로 Horizon Client를 열고 특정 서버에 연결한 후 10시간이 지나면 다시 로그인해야 합니다. 이 시간 제한은 원격 애플리케이션이나 원격 데스크톱 중 어디에 연결했는지에 관계없이 적용됩니다.

이 시간 제한 설정을 구성하려면 Horizon Administrator에서 **전역 설정**으로 이동한 다음 일반 설정을 편집합니다.

클라이언트 바탕 화면 또는 시작 메뉴에 데스크톱 또는 애플리케이션 바로 가기 생성

원격 데스크톱 또는 애플리케이션의 바로 가기를 만들 수 있습니다. 바로 가기는 로컬에 설치된 애플리케이션의 바로 가기와 마찬가지로 클라이언트 바탕 화면에 나타납니다. 프로그램 목록에 나타나는 시작 메뉴 항목을 생성할 수도 있습니다.

프로시저

1 Horizon Client를 시작하고 서버에 로그인합니다.

2 데스크톱 및 애플리케이션 선택 창에서 애플리케이션이나 데스크톱을 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴가 나타나면 **바로 가기 생성** 또는 **시작 메뉴에 추가**를 선택합니다.

선택한 명령에 따라 클라이언트 바탕 화면이나 클라이언트 시스템의 시작 메뉴에 바로 가기 항목이 생성됩니다.

후속 작업

이 바로 가기는 이름을 바꾸거나 삭제할 수 있으며 로컬에 설치된 애플리케이션용 바로 가기에 대해 수행할 수 있는 것과 동일한 작업을 수행할 수 있습니다. 바로 가기를 사용할 때, 서버에 아직 로그인되지 않은 경우 원격 데스크톱이나 애플리케이션 창을 열기 전에 로그인하라는 메시지가 나타납니다.

데스크톱 또는 애플리케이션 전환

원격 데스크톱에 연결된 상태에서 다른 데스크톱으로 전환할 수 있습니다. 또한 원격 데스크톱에 연결된 상태에서 원격 응용 프로그램에 연결할 수도 있습니다.

프로시저

◆ 동일한 서버 또는 다른 서버에 있는 원격 데스크톱 또는 애플리케이션을 선택합니다.

옵션	조치
동일한 서버에 있는 다른 데스크톱 또는 애플리케이션 선택	다음 작업 중 하나를 수행합니다. ■ 현재 원격 데스크톱에 로그인한 상태라면 Horizon Client 메뉴 표시줄에서 **옵션 > 다른 데스크톱으로 전환**을 선택하고 실행할 데스크톱이나 애플리케이션을 선택합니다. ■ 현재 원격 애플리케이션에 로그인한 상태라면 시스템 트레이에서 **VMware Horizon Client** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **VMware Horizon Client 보기**를 선택하여 데스크톱 및 애플리케이션 선택기 창을 표시한 다음 다른 데스크톱 또는 애플리케이션 아이콘을 두 번 클릭합니다. ■ 데스크톱과 애플리케이션 선택기 창에서 다른 데스크톱 또는 애플리케이션 아이콘을 두 번 클릭합니다. 새 창에서 데스크톱 또는 애플리케이션이 열리며 열려 있는 여러 창 간에 전환할 수 있습니다.
다른 서버에 있는 다른 데스크톱 또는 응용 프로그램 선택	다음 작업 중 하나를 수행합니다. ■ 현재 데스크톱이나 애플리케이션을 열어 둔 상태로 유지하면서 다른 서버의 원격 데스크톱이나 애플리케이션을 연결하려면 Horizon Client의 새 인스턴스를 시작하여 다른 데스크톱이나 애플리케이션에 연결합니다. ■ 현재 데스크톱을 닫고 다른 서버의 데스크톱에 연결하려면 데스크톱 선택기 창으로 이동한 후 창의 왼쪽 맨 위에서 **연결 해제** 아이콘을 클릭하고 서버에서 로그오프할지 확인합니다. 현재 서버에서 연결이 끊기고 데스크톱 세션이 열립니다. 그런 다음 다른 서버에 연결할 수 있습니다.

로그오프 또는 연결 해제

일부 구성의 경우 로그오프하지 않은 채 원격 데스크톱과의 연결을 끊으면 데스크톱의 애플리케이션은 열려 있는 상태로 유지됩니다. 또한 서버와의 연결을 끊고 원격 응용 프로그램은 실행 중인 상태로 둘 수도 있습니다.

원격 데스크톱이 열려 있지 않더라도 원격 데스크톱 운영 체제에서 로그오프할 수 있습니다. 이 기능을 사용하면 데스크톱에 Ctrl+Alt+Del 명령을 전송하고 **로그오프**를 클릭하는 것과 동일한 결과가 나타납니다.

참고 Windows 키 조합인 Ctrl+Alt+Del은 원격 데스크톱에서 지원되지 않습니다. Ctrl+Alt+Del을 누르는 것과 동일한 명령을 실행하려면 메뉴 표시줄에서 **Ctrl+Alt+Delete 보내기** 버튼을 클릭합니다. 아니면 대부분의 경우 Ctrl+Alt+Insert를 눌러도 됩니다.

프로시저

- 로그오프하지 않은 상태로 원격 데스크톱과의 연결을 끊습니다.

옵션	조치
원격 데스크톱 창에서	다음 작업 중 하나를 수행합니다. ■ 데스크톱 창 모서리에 있는 **닫기** 버튼을 클릭합니다. ■ 데스크톱 창의 메뉴 표시줄에서 **옵션 > 연결 해제**를 선택합니다.
데스크톱 및 응용 프로그램 선택기 창에서	서버에서 여러 데스크톱 또는 응용 프로그램에 대한 권한이 있는 경우 데스크톱 및 응용 프로그램 선택기 창이 열립니다. 데스크톱 선택기 창의 왼쪽 상단에 있는 **이 서버와의 연결 해제** 아이콘을 클릭하고 경고 상자에서 **예**를 클릭합니다.

참고 관리자는 연결을 끊을 때 자동으로 로그오프하도록 데스크톱을 구성할 수 있습니다. 그러한 경우, 데스크톱에 열려 있는 모든 프로그램은 중지됩니다.

- 원격 데스크톱에서 로그오프하고 연결을 끊습니다.

옵션	조치
데스크톱 OS 내에서	Windows **시작** 메뉴를 사용하여 로그오프합니다.
메뉴 표시줄에서	**옵션 > 연결을 끊은 후 로그오프**를 선택합니다. 이 절차를 사용하면 원격 데스크톱에서 열려 있는 파일이 저장되지 않고 닫힙니다.

- 원격 응용 프로그램과의 연결을 끊습니다.

옵션	조치
서버는 제외하고 애플리케이션만 연결 해제	응용 프로그램 창의 모서리에 있는 **닫기** 버튼을 클릭하는 등의 일반적인 방법으로 응용 프로그램을 종료합니다.
서버와 애플리케이션 연결 해제	다음 작업 중 하나를 수행합니다. ■ 애플리케이션 선택기 창의 왼쪽 상단 모서리에 있는 **이 서버와의 연결 해제** 아이콘을 클릭하고 경고 상자에서 **예**를 클릭합니다. ■ 시스템 트레이에서 Horizon Client 아이콘을 마우스 오른쪽 버튼 클릭하고 **종료**를 선택합니다.
애플리케이션을 실행한 채로 애플리케이션 선택기 창 닫기	**닫기** 버튼을 클릭하면 애플리케이션 선택기 창만 닫힙니다.

- 열려 있는 원격 데스크톱이 없을 때 로그오프합니다.

  이 절차를 사용하면 원격 데스크톱에서 열려 있는 파일이 저장되지 않고 닫힙니다.

  a Horizon Client를 시작하고, 원격 데스크톱에 대한 액세스를 제공하는 서버에 연결한 다음, 인증 자격 증명을 제공합니다.

  b 데스크톱 아이콘을 오른쪽 클릭하고 **로그오프**를 선택합니다.

원격 데스크톱 또는 애플리케이션에서 작업

5

Horizon은 최종 사용자가 기대하는 친숙하고 개인화된 데스크톱 및 애플리케이션 환경을 제공합니다. 최종 사용자는 로컬 컴퓨터에 연결된 USB 및 다른 디바이스에 액세스하고 로컬 컴퓨터에서 감지할 수 있는 임의의 프린터에 문서를 전송하고 스마트 카드로 인증하며 다중 디스플레이 모니터를 사용할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

Windows 클라이언트용 기능 지원 표

일부 기능은 특정 유형의 Horizon Client에서만 지원되고 다른 유형에서는 지원되지 않습니다.

최종 사용자에게 제공할 디스플레이 프로토콜 및 기능을 계획하는 경우, 다음 정보를 사용하여 기능을 지원하는 클라이언트 운영 체제를 확인하십시오.

표 5-1. Windows 기반 Horizon Client 시스템에서 지원되는 원격 데스크톱 기능

기능	Windows XP 데스크톱(View Agent 6.0.2 이하)	Windows Vista 데스크톱(View Agent 6.0.2 이하)	Windows 7 데스크톱	Windows 8.x 데스크톱	Windows 10 데스크톱	Windows Server 2008/2012 R2 데스크톱 또는 Windows Server 2016 데스크톱
USB 리디렉션	제한됨	제한됨	X	X	X	X
클라이언트 드라이브 리디렉션			X	X	X	X
실시간 오디오-비디오(RTAV)	제한됨	제한됨	X	X	X	X
스캐너 리디렉션		제한됨	X	X	X	X
직렬 포트 리디렉션			X	X	X	X
VMware Blast 디스플레이 프로토콜			X	X	X	X
RDP 디스플레이 프로토콜	제한됨	제한됨	X	X	X	X
PCoIP 디스플레이 프로토콜	제한됨	제한됨	X	X	X	X
개인 설정 관리	제한됨	제한됨	X	X		
Wyse MMR	제한됨	제한됨				
Windows Media MMR			X	X	X	
위치 기반 인쇄	제한됨	제한됨	X	X	X	X
가상 인쇄	제한됨	제한됨	X	X	X	X
스마트 카드	제한됨	제한됨	X	X	X	X
RSA SecurID 또는 RADIUS	제한됨	제한됨	X	X	X	X
단일 로그온	제한됨	제한됨	X	X	X	X
다중 모니터	제한됨	제한됨	X	X	X	X

Windows 10 데스크톱에는 View Agent 6.2 이상 또는 Horizon Agent 7.0 이상이 필요합니다. Windows Server 2012 R2 데스크톱에는 View Agent 6.1 이상 또는 Horizon Agent 7.0 이상이 필요합니다.

중요 View Agent 6.1 이상 릴리스는 Windows XP 및 Windows Vista 데스크톱을 지원하지 않습니다. View Agent 6.0.2는 이러한 게스트 운영 체제를 지원하는 마지막 View 릴리스입니다. Microsoft와 Windows XP/Vista용 추가 지원 계약을 맺고, VMware와 이러한 게스트 운영 체제용 추가 지원 계약을 맺은 고객은 View 연결 서버 6.1을 사용하여 Windows XP 및 Vista 데스크톱의 View Agent 6.0.2 버전을 배포할 수 있습니다.

지원되는 각 클라이언트 운영 체제의 버전 또는 서비스 팩에 대한 자세한 내용은 Windows 클라이언트 시스템 요구 사항을 참조하십시오.

RDS 호스트의 게시된 데스크톱에 대한 기능 지원

RDS 호스트는 Windows 원격 데스크톱 서비스와 View Agent 또는 Horizon Agent가 설치되어 있는 서버 컴퓨터입니다. 여러 명의 사용자가 동시에 RDS 호스트에서 데스크톱 세션을 사용할 수 있습니다. RDS 호스트는 물리적 시스템 또는 가상 시스템일 수 있습니다.

참고 다음 표에는 지원되는 기능에 대한 행만 포함되어 있습니다. 텍스트가 View Agent 최소 버전을 지정하는 경우, "이상"이라는 단어는 Horizon Agent 7.0.x 이상을 포함함을 의미합니다.

표 5-2. View Agent 6.0.x 이상 또는 Horizon Agent 7.0.x 이상이 설치된 RDS 호스트에 대해 지원되는 기능

기능	Windows Server 2008 R2 RDS 호스트	Windows Server 2012 RDS 호스트	Windows Server 2016 RDS 호스트
RSA SecurID 또는 RADIUS	X	X	Horizon Agent 7.0.2 이상
스마트 카드	View Agent 6.1 이상	View Agent 6.1 이상	Horizon Agent 7.0.2 이상
단일 로그온	X	X	Horizon Agent 7.0.2 이상
RDP 디스플레이 프로토콜(데스크톱 클라이언트의 경우)	X	X	Horizon Agent 7.0.2 이상
PCoIP 디스플레이 프로토콜	X	X	Horizon Agent 7.0.2 이상
VMware Blast 디스플레이 프로토콜	Horizon Agent 7.0 이상	Horizon Agent 7.0 이상	Horizon Agent 7.0.2 이상
HTML Access	View Agent 6.0.2 이상(가상 시스템 전용)	View Agent 6.0.2 이상(가상 시스템 전용)	Horizon Agent 7.0.2 이상
Windows Media MMR	View Agent 6.1.1 이상	View Agent 6.1.1 이상	Horizon Agent 7.0.2 이상
USB 리디렉션(USB 스토리지 디바이스에만 해당)		View Agent 6.1 이상	Horizon Agent 7.0.2 이상
클라이언트 드라이브 리디렉션	View Agent 6.1.1 이상	View Agent 6.1.1 이상	Horizon Agent 7.0.2 이상
가상 인쇄(데스크톱 클라이언트에 해당)	View Agent 6.0.1 이상(가상 시스템 전용)	View Agent 6.0.1 이상(가상 시스템 전용)	Horizon Agent 7.0.2 이상(가상 시스템 전용)
스캐너 리디렉션	View Agent 6.0.2 이상	View Agent 6.0.2 이상	Horizon Agent 7.0.2 이상

표 5-2. View Agent 6.0.x 이상 또는 Horizon Agent 7.0.x 이상이 설치된 RDS 호스트에 대해 지원되는 기능 (계속)

기능	Windows Server 2008 R2 RDS 호스트	Windows Server 2012 RDS 호스트	Windows Server 2016 RDS 호스트
위치 기반 인쇄	View Agent 6.0.1 이상(가상 시스템 전용)	View Agent 6.0.1 이상(가상 시스템 전용)	Horizon Agent 7.0.2 이상(가상 시스템 전용)
여러 대의 모니터(데스크톱 클라이언트에 해당)	X	X	Horizon Agent 7.0.2 이상
Unity Touch(모바일 및 Chrome OS 클라이언트에 해당)	X	X	Horizon Agent 7.0.2 이상
실시간 오디오-비디오(RTAV)	Horizon Agent 7.0.2 이상	Horizon Agent 7.0.2 이상	Horizon Agent 7.0.3 이상

지원되는 각 게스트 운영 체제의 버전 또는 서비스 팩에 대한 자세한 내용은 View 설치 문서를 참조하십시오.

특정 기능에 대한 제한 사항

Windows 기반 클라이언트에서 지원되는 기능에는 다음과 같은 제한이 있습니다.

표 5-3. 특정 기능에 대한 요구 사항

기능	요구 사항
Windows Media MMR	View Agent 6.0.2 이상이 필요합니다. RDS 데스크톱에서 Windows Media MMR 기능을 사용하려면 View Agent 6.1.1 이상 또는 Horizon Agent 7.0 이상이 있어야 합니다. VMware Blast 디스플레이 프로토콜을 사용하는 경우 Horizon Agent 7.0 이상이 있어야 합니다.
직렬 포트 리디렉션	View Agent 6.1.1 이상이 필요합니다. Windows 10의 경우 View Agent 6.2 이상 또는 Horizon Agent 7.0 이상이 필요합니다. VMware Blast 디스플레이 프로토콜을 사용하는 경우 Horizon Agent 7.0 이상이 있어야 합니다.
Windows Server 2008 R2 데스크톱, RDS 데스크톱(가상 시스템 RDS 호스트에 있는 데스크톱) 및 원격 애플리케이션을 위한 가상 인쇄와 위치 기반 인쇄	Horizon 6.0.1(View 포함) 이상이 필요합니다. 이 기능을 위해 VMware Blast 디스플레이 프로토콜을 사용하는 경우 Horizon Agent 7.0 이상이 있어야 합니다.

표 5-3. 특정 기능에 대한 요구 사항 (계속)

기능	요구 사항
스캐너 리디렉션	View Agent 6.0.2 이상이 필요합니다. PCoIP 디스플레이 프로토콜이 필요합니다. Windows 10의 경우 View Agent 6.2 이상 또는 Horizon Agent 7.0 이상이 필요합니다. VMware Blast 디스플레이 프로토콜을 사용하는 경우 Horizon Agent 7.0 이상이 있어야 합니다.
클라이언트 드라이브 리디렉션	RDS 호스트에서 단일 사용자 가상 시스템 데스크톱 및 게시된 데스크톱을 사용하려면 View Agent 6.1.1 이상 또는 Horizon Agent 7.0 이상이 필요합니다. VMware Blast 디스플레이 프로토콜을 사용하는 경우 Horizon Agent 7.0 이상이 있어야 합니다.

참고 또한 Horizon Client를 사용하여 Windows 기반 원격 애플리케이션뿐만 아니라 원격 데스크톱에도 안전하게 액세스할 수 있습니다. Horizon Client에서 애플리케이션을 선택하면 로컬 클라이언트 디바이스에 있는 해당 애플리케이션의 창이 열리며 이 애플리케이션은 로컬에 설치된 것처럼 표시되고 작동합니다.

연결 서버 6.0 이상에 연결한 경우에만 원격 애플리케이션을 사용할 수 있습니다. 게시된 애플리케이션 및 게시된 데스크톱을 제공하는 RDS 호스트에 대해 지원되는 운영 체제에 대한 정보는 View 설치 문서를 참조하십시오.

이러한 기능 및 해당 제한 사항에 대한 설명은 View 아키텍처 계획 문서를 참조하십시오.

Linux 데스크톱에 대한 기능 지원

View Agent 6.1.1 이상 또는 Horizon Agent 7.0 이상이 설치되어 있는 경우 일부 Linux 게스트 운영 체제가 지원됩니다. 지원되는 Linux 운영 체제 목록과 지원되는 기능에 관한 정보는 Horizon 6 for Linux 데스크톱 설정 또는 Horizon 7에서 가상 데스크톱 설정을(를) 참조하십시오.

중첩 모드에서 지원되는 기능

중첩 모드는 최종 사용자가 제로 클라이언트에 로그인하면 Horizon Client가 자동으로 시작되고 사용자가 원격 데스크톱에 자동 로그인되는 제로 클라이언트 또는 씬 클라이언트를 위해 사용되기도 합니다. 이 원격 데스크톱의 경우 사용자가 호스팅된 애플리케이션을 실행합니다.

이 설정에서는 원격 데스크톱이 단일 사용자 가상 시스템 데스크톱이거나 RDS 호스트에서 제공하는 데스크톱입니다. 어떤 경우에든 호스팅된 애플리케이션을 제공하려면 원격 데스크톱에 Horizon Client 소프트웨어가 설치되어 있어야 합니다. 이 설정은 클라이언트가 다른 클라이언트가 설치된 데스크톱에 연결되므로 중첩 모드라고 합니다.

중첩 모드에서 Horizon Client를 실행할 때는 다음 운영 체제가 지원됩니다.

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7 Enterprise SP1
- Windows 10 Enterprise, 버전 1607

다음 기능은 사용자가 중첩 모드에서 Horizon Client를 사용할 때 지원됩니다.

- VMware Blast, PCoIP 및 RDP 디스플레이 프로토콜
- 위치 기반 인쇄
- 가상 인쇄
- 단일 로그온(스마트 카드 사용 안 함)
- 클립보드 리디렉션
- URL 컨텐츠 리디렉션
- 현재 사용자로 로그인

국제화

사용자 인터페이스와 문서는 한국어, 영어, 일본어, 프랑스어, 독일어, 중국어 간체, 중국어 번체 및 스페인어로 제공됩니다.

원격 애플리케이션에서 로컬 IME 사용

영어 이외의 키보드 및 로케일을 사용하는 경우 로컬 시스템에 설치된 IME(입력기)를 사용하여 영어 이외의 문자를 호스팅되는 원격 애플리케이션으로 보낼 수 있습니다.

또한 로컬 시스템의 알림 영역(시스템 트레이)에 있는 바로 가기 키와 아이콘을 사용하여 다른 IME로 전환할 수 있습니다. 원격 RDS 호스트에는 IME가 설치되어 있지 않아도 됩니다.

이 기능이 켜지면 로컬 IME가 사용됩니다. 원격 애플리케이션이 설치된 RDS 호스트에 IME가 설치되고 구성된 경우 해당 원격 IME는 무시됩니다.

기본적으로 이 기능은 꺼져 있습니다. 이 기능을 켜거나 끄기 위해 설정을 변경할 때마다 변경 내용을 적용하기 위해 서버에서 연결을 끊고 다시 로그인해야 합니다.

필수 조건

- 하나 이상의 IME가 클라이언트 시스템에 설치되어 있는지 확인합니다.
- 로컬 클라이언트 시스템의 입력 언어가 IME에서 사용되는 언어와 일치하는지 확인합니다.

  RDS 호스트의 입력 언어는 적용 가능하지 않습니다.
- 원격 데스크톱에 View Agent 6.0.2 또는 Horizon Agent 7.0 이상이 설치되어 있는지 확인합니다.

프로시저

1. Horizon Client의 데스크톱 및 애플리케이션 선택기 창에서 원격 애플리케이션을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택합니다.
2. 나타나는 원격 애플리케이션 창에서 **로컬 IME를 호스팅되는 애플리케이션으로 확장합니다.** 확인란을 선택하고 **확인**을 클릭합니다.

3 다음 옵션 중 하나를 사용하여 세션을 다시 시작합니다.

옵션	설명
서버에서 로그오프	서버에서 연결을 끊은 다음 서버에 다시 로그인하고 애플리케이션에 다시 연결합니다. 모든 원격 데스크톱과 마찬가지로 연결이 끊겼지만 닫히지 않은 애플리케이션을 재개할 수 있습니다.
애플리케이션 재설정	원격 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택한 다음 **재설정**을 클릭합니다. 원격 데스크톱이 열려 있는 경우 이 옵션을 사용해도 연결이 끊어지지 않습니다. 그러나 모든 원격 애플리케이션이 닫히므로 다시 시작해야 합니다.

설정은 세션을 다시 시작한 후에만 적용됩니다. 설정은 서버의 모든 호스팅되는 원격 애플리케이션에 적용됩니다.

4 로컬로 설치된 모든 애플리케이션과 마찬가지로 로컬 IME를 사용할 수 있습니다.

언어 지정 및 IME 아이콘이 로컬 클라이언트 시스템의 알림 영역(시스템 트레이)에 나타납니다. 바로 가기 키를 사용하여 다른 언어 또는 IME로 전환할 수 있습니다. 특정 작업을 수행하는 키 조합(예: 텍스트를 잘라내는 CTRL+X 및 다른 탭으로 이동하는 Alt+오른쪽 화살표)은 계속 올바르게 작동합니다.

참고 Windows 7 및 8.x 시스템에서 **텍스트 서비스 및 입력 언어** 대화상자(**제어판 > 국가 및 언어 > 키보드 및 언어 탭 > 키보드 변경 버튼 > 텍스트 서비스 및 입력 언어 > 고급 키 설정 탭**을 통해 사용 가능)를 사용하여 IME에 바로 가기 키를 지정할 수 있습니다.

화면 키보드에 대한 지원을 사용하도록 설정

마우스 또는 화면 키보드가 Horizon Client 창 외부에 있더라도 Horizon Client 창에 포커스가 있는 경우 물리적 키보드, 화면 키보드, 마우스 및 필기 패드 이벤트가 원격 데스크톱 또는 원격 애플리케이션으로 전송되도록 클라이언트 시스템을 구성할 수 있습니다.

이 기능은 Windows Surface Pro와 같은 x86 기반 Windows 태블릿을 사용하는 경우에 특히 유용합니다. 이 기능을 사용하려면 Windows 레지스트리 키 EnableSoftKeypad를 true로 설정해야 합니다. 이러한 키의 위치는 다음과 같이 시스템 유형에 따라 다릅니다.

- 32비트 Windows: HKEY_LOCAL_MACHINE₩Software₩VMware, Inc.₩VMware VDM₩Client₩
- 64비트 Windows: HKLM₩SOFTWARE₩Wow6432Node₩VMware, Inc.₩VMware VDM₩Client₩

원격 데스크톱 창 크기 조정

원격 데스크톱 창의 모서리를 끌어 창 크기를 조정하면 창 오른쪽 하단 구석의 도구 설명에 화면 해상도가 표시됩니다.

VMware Blast 또는 PCoIP 디스플레이 프로토콜을 사용 중인 경우 데스크톱 창의 크기를 변경하면 도구 설명이 다양한 화면 해상도를 표시하도록 변경됩니다. 이 정보는 특정 해상도로 원격 데스크톱 크기를 조정해야 하는 경우 유용합니다.

관리자가 게스트 크기를 잠갔거나 사용자가 RDP 디스플레이 프로토콜을 사용 중인 경우에는 원격 데스크톱 창의 해상도를 변경할 수 없습니다. 이러한 경우 해상도 도구 설명은 초기 해상도를 표시합니다.

모니터 및 화면 해상도

원격 데스크톱을 여러 모니터로 확장할 수 있습니다. 고해상도 모니터가 있다면 원격 데스크톱 또는 애플리케이션을 전체 해상도로 볼 수 있습니다.

[모든 모니터] 디스플레이 모드는 여러 대의 모니터에 원격 데스크톱 창을 표시합니다. 원격 데스크톱 창이 기본적으로 모든 모니터에 표시됩니다. 선택적 다중 모니터 기능을 사용하여 모니터의 일부에서만 원격 데스크톱 창을 표시할 수 있습니다.

[모든 모니터] 모드를 사용하고 있을 때 [최소화] 버튼을 클릭한 다음 다시 창을 최대화하면 창이 모든 [모니터 모드]로 돌아갑니다. 마찬가지로 [전체 화면] 모드를 사용하고 있을 때 창을 최소화한 다음 다시 최대화하면 창이 단일 모니터의 [전체 화면] 모드로 돌아갑니다.

Horizon Client가 모든 모니터를 사용하도록 지정한 경우 애플리케이션 창을 최대화하면 창이 해당 창을 포함하는 모니터의 전체 화면으로만 확장됩니다.

지원되는 다중 모니터 구성

Horizon Client는 다음 다중 모니터 구성을 지원합니다.

- 2대의 모니터를 사용할 경우, 모니터는 동일한 모드에 있지 않아도 됩니다. 예를 들어, 외부 모니터에 연결된 노트북을 사용할 경우, 외부 모니터는 세로 모드나 가로 모드여도 됩니다.
- 모니터 2대를 사용 중이고 전체 높이가 4096픽셀보다 작은 경우에만 모니터를 나란히 놓거나, 2x2로 쌓거나, 수직으로 쌓을 수 있습니다.
- 선택적 다중 모니터 기능을 사용하려면 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용해야 합니다. 자세한 내용은 다중 모니터 설정에서 특정 모니터 선택의 내용을 참조하십시오.
- 3D 렌더링 기능을 사용하려면 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용해야 합니다. 모니터를 2대까지 사용할 수 있으며 최대 해상도는 1920x1200입니다. 해상도가 4K(3840 X 2160)인 경우 모니터 1대만 지원됩니다.
- 인스턴트 클론 데스크톱 풀을 사용하는 경우 원격 데스크톱을 표시하기 위해 사용할 수 있는 최대 모니터 수는 2대이고 최대 해상도는 2560x1600입니다.

- VMware Blast 디스플레이 프로토콜이나 PCoIP 디스플레이 프로토콜을 사용하면 4K(3840 x 2160)의 원격 데스크톱 화면 해상도가 지원됩니다. 지원되는 4K 디스플레이 수는 데스크톱 가상 시스템의 하드웨어 버전 및 Windows 버전에 따라 다릅니다.

하드웨어 버전	Windows 버전	지원되는 4K 디스플레이 수
10(ESXi 5.5.x 호환)	7, 8, 8.x, 10	1
11(ESXi 6.0 호환)	7(3D 렌더링 기능 사용 안 함 및 Windows Aero 사용 안 함)	3
11	7(3D 렌더링 기능 사용)	1
11	8, 8.x, 10	1

  원격 데스크톱에는 View Agent 6.2 이상이나 Horizon Agent 7.0 이상이 설치되어 있어야 합니다. 최상의 성능을 위해 가상 시스템에 적어도 2GB의 RAM과 2개의 vCPU가 있어야 합니다. 이 기능을 사용하려면 네트워크 지연 시간이 낮고 패키지 손실률이 낮은 1000Mbps 대역폭과 같이 네트워크 상태가 양호해야 합니다.

  참고 원격 데스크톱 화면 해상도가 3840 x 2160(4K)으로 설정되면 화면의 항목이 더 작게 보일 수 있으며 원격 데스크톱의 화면 해상도 대화상자를 사용하여 텍스트 및 기타 항목을 더 크게 만들지 못할 수 있습니다. 이 시나리오에서는 클라이언트 시스템의 DPI를 적절하게 설정하고 DPI 동기화 기능을 사용하도록 설정하여 클라이언트 시스템의 DPI 설정을 원격 데스크톱으로 리디렉션할 수 있습니다.

- Microsoft RDP 7을 사용하는 경우 원격 데스크톱을 표시하기 위해 사용할 수 있는 최대 모니터 수는 16대입니다.
- Microsoft RDP 디스플레이 프로토콜을 사용하는 경우 Microsoft RDC(Remote Desktop Connection) 6.0 이상이 원격 데스크톱에 설치되어 있어야 합니다.

다중 모니터 설정에서 특정 모니터 선택

선택적 다중 모니터 기능을 사용하여 원격 데스크톱 창을 표시할 모니터를 선택할 수 있습니다. 예를 들어 모니터가 3대 있다면 원격 데스크톱 창이 3대 중 2대의 모니터에만 표시되도록 지정할 수 있습니다. 기본적으로 원격 데스크톱 창은 다중 모니터 설정에서 모든 모니터에 표시됩니다.

최대 4대의 인접 모니터를 선택할 수 있습니다. 모니터는 나란히 놓거나, 2x2로 쌓거나, 수직으로 쌓을 수 있습니다. 수직으로 쌓을 수 있는 최대 모니터 수는 2대입니다.

원격 애플리케이션에서는 이 기능이 지원되지 않습니다.

프로시저

1. Horizon Client를 시작하고 서버에 로그인합니다.
2. 데스크톱 및 애플리케이션 선택 창에서 원격 데스크톱을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택합니다.
3. **연결 수단** 드롭다운 메뉴에서 **PCoIP** 또는 **VMware Blast**를 선택합니다.

4 **디스플레이** 드롭다운 메뉴에서 **모든 모니터**를 선택합니다.

현재 클라이언트 시스템에 연결된 모니터의 축소 이미지가 [디스플레이] 설정에 표시됩니다. 디스플레이 토폴로지는 클라이언트 시스템의 디스플레이 설정을 따릅니다.

5 축소 이미지를 클릭하여 원격 데스크톱 창을 표시할 모니터를 선택하거나 선택을 취소합니다.

모니터를 선택하면 축소 이미지가 녹색으로 바뀝니다. 디스플레이 선택 규칙을 위반하면 경고 메시지가 나타납니다.

6 변경 사항을 저장하려면 **적용**을 클릭합니다.

7 **확인**을 클릭하여 대화상자를 닫습니다.

8 원격 데스크톱에 연결합니다.

원격 데스크톱에 연결하면 변경 사항이 즉시 적용됩니다. 변경 사항은 Horizon Client에서 나간 후 원격 데스크톱에 대한 Horizon Client 환경설정 파일에 저장됩니다.

다중 모니터 설정에서 단일 모니터 사용

여러 모니터가 있지만 하나의 모니터에서만 원격 데스크톱 창을 표시하고 싶은 경우 원격 데스크톱 창이 단일 모니터에서 열리도록 구성할 수 있습니다.

원격 애플리케이션에서는 이 환경설정이 지원되지 않습니다.

프로시저

1 Horizon Client를 시작하고 서버에 로그인합니다.

2 데스크톱 및 애플리케이션 선택 창에서 원격 데스크톱을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택합니다.

3 **연결 수단** 드롭다운 메뉴에서 **PCoIP** 또는 **VMware Blast**를 선택합니다.

4 **디스플레이** 메뉴에서 **창 – 크게**, **창 – 작게** 또는 **사용자 지정**을 선택합니다.

사용자 지정을 선택하면 특정 창 크기를 선택할 수 있습니다.

5 변경 사항을 저장하려면 **적용**을 클릭합니다.

적용을 클릭하면 변경 사항이 즉시 적용됩니다.

6 **확인**을 클릭하여 대화상자를 닫습니다.

기본적으로 원격 데스크톱 창은 기본 모니터에서 열립니다. 원격 데스크톱 창을 비기본 모니터로 끌어올 수 있습니다. 그러면 다음에 원격 데스크톱을 열 때 원격 데스크톱 창이 동일한 모니터에 표시됩니다. 창이 열린 후 모니터 중앙에 표시되며, 사용자가 창을 마우스로 끌어서 조정한 크기가 아닌 디스플레이 모드에 대해 선택한 창 크기가 사용됩니다.

디스플레이 크기 조정 사용

4K 모니터와 같은 고해상도 화면을 사용하거나 시력이 나쁜 사용자는 일반적으로 클라이언트 시스템에서 DPI(인치당 도트 수)를 100%보다 높게 설정하여 크기 조정을 사용하도록 설정합니다. 디스플레이 크기 조정 기능을 사용하면 원격 데스크톱 또는 애플리케이션이 클라이언트 시스템의 크기 조정 설정을 지원하기 때문에 원격 데스크톱 또는 애플리케이션이 너무 작은 크기가 아닌 정상적인 크기로 표시됩니다.

Horizon Client에서는 각 원격 데스크톱에 대해 별도로 디스플레이 크기 조정 설정을 저장합니다. 원격 애플리케이션의 경우 디스플레이 크기 조정 설정은 현재 로그인된 사용자에게 제공되는 모든 원격 애플리케이션에 적용됩니다. 디스플레이 크기 조정 설정은 클라이언트 시스템에서 DPI 설정이 100%인 경우에도 표시됩니다.

관리자는Horizon Client **Locked Guest Size** 그룹 정책 설정을 사용하도록 설정하여 디스플레이 크기 조정 설정을 숨길 수 있습니다. **Locked Guest Size** 그룹 정책 설정을 사용하도록 설정해도 DPI 동기화 기능을 사용하지 않도록 설정되지는 않습니다. DPI 동기화 기능을 사용하지 않도록 설정하려면 관리자가 **DPI 동기화** 그룹 정책 설정을 사용하지 않도록 설정해야 합니다. 자세한 내용은 DPI 동기화 사용의 내용을 참조하십시오.

다중 모니터 설정에서 디스플레이 크기 조정을 사용해도 Horizon Client에서 지원하는 모니터 수와 최대 해상도에는 영향을 미치지 않습니다. 디스플레이 크기 조정이 허용되며 적용된 경우, 크기 조정은 기본 모니터의 DPI 설정을 기반으로 이루어집니다.

이 절차는 원격 데스크톱 또는 애플리케이션에 연결하기 전에 [디스플레이 크기 조정] 기능을 사용하도록 설정하는 방법을 설명합니다. **옵션 > 디스플레이 크기 조정 허용**을 선택하여 원격 데스크톱에 연결한 후에 디스플레이 크기 조정 기능을 사용하도록 설정할 수 있습니다.

프로시저

1. Horizon Client를 시작하고 서버에 연결합니다.
2. 데스크톱 및 애플리케이션 선택 창에서 원격 데스크톱 또는 애플리케이션을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택합니다.
3. **디스플레이 크기 조정 허용** 확인란을 선택합니다.
4. 변경 사항을 저장하려면 **적용**을 클릭합니다.
5. **확인**을 클릭하여 대화상자를 닫습니다.

DPI 동기화 사용

DPI 동기화 기능을 사용하면 원격 데스크톱의 DPI 설정이 새로운 원격 세션에서도 클라이언트 시스템의 DPI 설정과 일치하게 할 수 있습니다. 세션을 시작할 때 Horizon Agent에서는 원격 데스크톱의 DPI 값을 클라이언트 시스템의 DPI 값과 일치하도록 설정합니다.

DPI 동기화 기능으로는 활성 원격 세션의 DPI 설정을 변경할 수 없습니다. 기존 원격 세션에 다시 연결하면 디스플레이 크기 조정 기능을 통해 원격 데스크톱이나 애플리케이션의 크기가 적절하게 조정됩니다.

DPI 동기화 기능은 기본적으로 사용하도록 설정되어 있습니다. 관리자는 Horizon Agent **DPI 동기화** 그룹 정책 설정을 사용하지 않도록 설정하여 DPI 동기화 기능을 사용하지 않도록 설정할 수 있습니다. 구성 변경을 적용하려면 로그아웃했다가 다시 로그인해야 합니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

DPI 동기화 기능과 디스플레이 크기 조정 기능을 모두 사용하도록 설정한 경우에는 한 번에 한 가지 기능만 적용됩니다. 디스플레이 크기 조정은 DPI 동기화가 아직 적용되지 않은 경우에만(즉, 원격 데스크톱의 DPI 설정이 클라이언트 시스템의 DPI 설정과 일치하기 전) 이루어지며, DPI 설정이 일치되고 나면 디스플레이 크기 조정은 더 이상 작동하지 않습니다.

단일 세션 가상 시스템 데스크톱의 경우 DPI 동기화 기능이 다음 게스트 운영 체제에서 지원됩니다.

- 32비트 또는 64비트 Windows 7
- 32비트 또는 64비트 Windows 8.x
- 32비트 또는 64비트 Windows 10
- Windows Server 2008 R2(데스크톱으로 구성)
- Windows Server 2012 R2(데스크톱으로 구성)
- Windows Server 2016(데스크톱으로 구성)

게시된 데스크톱 및 게시된 애플리케이션의 경우 DPI 동기화 기능이 다음 RDS 호스트에서 지원됩니다.

- Windows Server 2012 R2
- Windows Server 2016

DPI 동기화 기능에는 Horizon Agent 7.0.2 이상 및 Horizon Client 4.2 이상이 필요합니다.

참고 Horizon Client 4.2와 Horizon Agent 7.0 또는 7.0.1이나 Horizon Client 4.0 또는 4.1과 Horizon Agent 7.0.2 이상을 사용하는 경우에는 DPI 동기화 기능을 사용할 수 없습니다. 이러한 시나리오에서는 디스플레이 크기 조정 기능만 사용할 수 있습니다.

다음은 DPI 동기화 기능의 사용에 대한 팁입니다.

- 클라이언트 시스템에서 DPI 설정을 변경하는 경우에는 로그아웃했다가 다시 로그인하여 Horizon Client에 클라이언트 시스템의 새 DPI 설정을 인식시켜야 합니다. 이 요구 사항은 클라이언트 시스템에서 Windows 10을 실행하는 경우에도 적용됩니다.
- DPI 설정이 100% 이상인 클라이언트 시스템에서 원격 세션을 시작한 다음 DPI 설정이 100% 이상의 다른 값으로 설정된 다른 클라이언트 시스템에서 같은 세션을 사용하는 경우, 두 번째 클라이언트 시스템에서 DPI 동기화가 작동하도록 하려면 두 번째 클라이언트 시스템에서 세션을 로그아웃했다가 다시 로그인해야 합니다.
- Windows 10과 Windows 8.x 시스템은 여러 모니터에서 여러 DPI 설정을 지원하지만, DPI 동기화 기능에서는 클라이언트 시스템의 기본 모니터에 설정된 DPI 값만 사용합니다. 또한 원격 데스크톱에 있는 모든 모니터는 클라이언트 시스템의 기본 모니터와 동일한 DPI 설정을 사용합니다. Horizon Client는 여러 모니터에서의 여러 다른 DPI 설정을 지원하지 않습니다.

- 관리자가 Horizon Agent의 **DPI 동기화** 그룹 정책 설정 값을 변경하는 경우에는 새 설정을 적용하려면 로그아웃했다가 다시 로그인해야 합니다.
- 여러 모니터에서 여러 DPI 설정을 지원하는 노트북을 외부 모니터에 연결하고 외부 모니터를 기본 모니터로 설정한 경우, 외부 모니터를 분리하거나 다시 연결할 때마다 Windows에서 기본 모니터와 기본 모니터 DPI 설정을 자동으로 변경합니다. 이런 경우에는 클라이언트 시스템에서 로그아웃했다가 다시 로그인하여 Horizon Client에 기본 모니터 변경을 인식시키고, 원격 데스크톱이나 애플리케이션에서 로그아웃했다가 다시 로그인하여 클라이언트 시스템과 원격 데스크톱 또는 애플리케이션의 DPI 설정이 일치하게 만들어야 합니다.
- Windows 10 클라이언트 시스템의 경우 바탕화면을 마우스 오른쪽 버튼으로 클릭하고, **디스플레이 설정 > 고급 디스플레이 설정 > 텍스트 및 기타 항목의 고급 크기 조정**을 선택하고, **사용자 지정 배율 수준을 설정할 수 있습니다** 링크를 클릭한 다음 로그아웃했다가 다시 로그인하여 새 DPI 설정이 적용되도록 합니다.

데스크톱 창이 열려 있는 동안 디스플레이 모드 변경

원격 데스크톱 연결을 해제하지 않아도 [모든 모니터] 모드에서 [전체 화면] 모드로 변경하는 등의 디스플레이 모드 변경이 가능합니다.

원격 애플리케이션에서는 이 기능이 지원되지 않습니다.

필수 조건

VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용하고 있는지 확인합니다.

프로시저

1 클라이언트 시스템의 알림 영역(시스템 트레이)에서 **Horizon Client** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 해당 옵션을 선택하여 설정 창을 엽니다.

   참고 애플리케이션 및 데스크톱 선택 창에서 설정 창을 열 수도 있습니다.

2 원격 데스크톱을 선택한 후 디스플레이 옵션을 선택합니다.

USB 디바이스 연결

원격 데스크톱에서 USB 플래시 드라이브, 카메라 및 프린터와 같은 로컬로 연결된 USB 디바이스를 사용할 수 있습니다. 이 기능을 USB 리디렉션이라 부릅니다.

이 기능을 사용하면 로컬 클라이언트 시스템에 연결된 대부분의 USB 디바이스를 Horizon Client의 메뉴에서 사용할 수 있습니다. 디바이스를 연결 및 연결 해제하는 메뉴를 사용합니다.

참고 View Agent 6.1 이상 또는 Horizon Agent 7.0 이상에서는 RDS 호스트의 게시된 데스크톱 및 애플리케이션에서 사용하기 위해 로컬로 연결된 USB 썸 플래시 드라이브 및 하드 디스크를 리디렉션할 수도 있습니다. 보안 스토리지 드라이브, USB CD-ROM 등의 다른 유형의 스토리지 디바이스를 포함한 다른 유형의 USB 디바이스는 게시된 데스크톱 및 애플리케이션에서 지원되지 않습니다. Horizon Agent 7.0.2 이상에서는 게시된 데스크톱 및 애플리케이션이 TOPAZ 서명 패드, Olympus Dictation 풋패달 및 Wacom 서명 패드를 비롯한 더 많은 일반 USB 디바이스를 지원할 수 있습니다. 보안 스토리지 드라이브 및 USB CD-ROM 드라이브를 비롯한 다른 유형의 USB 디바이스는 게시된 데스크톱 및 애플리케이션에서 지원되지 않습니다.

원격 데스크톱에서 USB 디바이스를 사용하는 경우 다음과 같은 제약이 있습니다.

- Horizon Client의 메뉴에서 USB 디바이스에 액세스하고 원격 데스크톱에서 디바이스를 사용하는 경우에는 로컬 컴퓨터의 디바이스에 액세스할 수 없습니다.
- 메뉴에는 나타나지 않지만 원격 데스크톱에서 사용할 수 있는 USB 디바이스에는 키보드 및 포인팅 디바이스와 같은 휴먼 인터페이스 디바이스가 포함됩니다. 원격 데스크톱 및 로컬 컴퓨터는 이러한 디바이스를 동시에 사용합니다. 이러한 디바이스와의 상호 작용은 네트워크 지연으로 인해 느려질 수 있습니다.
- 대용량 USB 디스크 드라이브는 데스크톱에 나타나는 데 수 분이 소요될 수 있습니다.
- 일부 USB 디바이스에는 특정 드라이버가 필요합니다. 필요한 드라이버가 원격 데스크톱에 설치되어 있지 않은 경우 USB 디바이스를 원격 데스크톱에 연결하면 드라이버를 설치하라는 메시지가 나타날 수 있습니다.
- Android 기반 Samsung 스마트폰, 태블릿 등 MTP 드라이버를 사용하는 USB 디바이스를 연결하려는 경우, USB 디바이스가 자동으로 원격 데스크톱에 연결되도록 Horizon Client를 구성합니다. 메뉴 항목을 사용하여 USB 디바이스를 수동으로 리디렉션하려고 할 경우, 연결을 해제했다가 다시 연결하기 전에는 해당 디바이스가 리디렉션되지 않습니다.
- **USB 디바이스 연결** 메뉴를 사용하여 스캐너에 연결하지 마십시오. 스캐너 디바이스를 사용하려면 스캐너 리디렉션 기능을 사용하십시오. 이 기능이 View Agent 6.0.2 이상 또는 Horizon Agent 7.0 이상에서 사용되는 경우 Horizon Client에서도 사용할 수 있습니다. 스캐너 사용을 참조하십시오.
- 웹캠은 **USB 디바이스 연결** 메뉴를 사용하는 USB 리디렉션에서 지원되지 않습니다. 웹캠 또는 오디오 입력 디바이스를 사용하려면 실시간 오디오-비디오 기능을 사용해야 합니다. 이 기능은 View 5.2 기능 팩 2 이상 릴리스가 있는 경우 사용할 수 있습니다. 웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용을 참조하십시오.
- USB 오디오 디바이스의 리디렉션 가능 여부는 네트워크의 상태에 따라 달라질 수 있으며 안정적이지 않습니다. 일부 디바이스의 경우, 유휴 상태에서도 높은 데이터 처리량을 요구합니다. View 5.2 기능 팩 2 이상 릴리스에 포함된 실시간 오디오-비디오 기능이 설치되어 있는 경우, 오디오 입력 및 출력 디바이스가 해당 기능을 통해 잘 작동하며 해당 디바이스에 대해 USB 리디렉션을 사용하지 않아도 됩니다.

USB 디바이스를 원격 데스크톱에 수동 또는 자동으로 연결할 수 있습니다.

참고 USB 이더넷 디바이스 및 터치 스크린 디바이스와 같은 USB 디바이스를 원격 데스크톱으로 리디렉션하지 마십시오. USB 이더넷 디바이스를 리디렉션할 경우, 클라이언트 시스템의 네트워크 연결이 끊깁니다. 터치 스크린 디바이스를 리디렉션할 경우, 원격 데스크톱에서는 터치 입력은 수신하지만 키보드 입력은 수신하지 않습니다. USB 디바이스에 자동 연결하도록 가상 데스크톱을 설정한 경우, 특정 디바이스를 제외하도록 정책을 구성할 수 있습니다.

중요 이 절차는 VMware Horizon Client 메뉴 항목을 사용하여 USB 디바이스를 원격 데스크톱에 자동 연결하도록 구성하는 방법에 대한 설명입니다. Horizon Client 명령줄 인터페이스를 사용하거나 그룹 정책을 만들어 자동 연결을 구성할 수도 있습니다.

명령줄 인터페이스에 대한 자세한 내용은 명령줄에서 Horizon Client 실행의 내용을 참조하십시오. 그룹 정책을 만드는 데 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

필수 조건

- 원격 데스크톱에서 USB 디바이스를 사용하려면 Horizon 관리자가 원격 데스크톱에서 USB 기능을 사용하도록 설정해야 합니다.

  이 작업에는 에이전트의 **USB 리디렉션** 구성 요소 설치가 포함되며 USB 리디렉션에 관련된 정책의 설정이 포함될 수 있습니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

- Horizon Client가 설치되어 있으면 **USB 리디렉션** 구성 요소가 설치되어 있는 것입니다. 설치에 이 구성 요소를 포함하지 않은 경우 클라이언트를 제거한 후 설치 관리자를 다시 실행하여 **USB 리디렉션** 구성 요소를 포함하십시오.

프로시저

- USB 디바이스를 원격 데스크톱에 수동으로 연결합니다.
  a USB 디바이스를 로컬 클라이언트 시스템에 연결합니다.
  b VMware Horizon Client 메뉴 표시줄에서 **USB 디바이스 연결**을 클릭합니다.
  c USB 디바이스를 선택합니다.

  이 디바이스는 수동으로 로컬 시스템에서 원격 데스크톱으로 리디렉션됩니다.

- USB 디바이스를 원격 호스팅되는 애플리케이션에 연결합니다.
  a 데스크톱 및 애플리케이션 선택기 창에서 원격 애플리케이션을 엽니다.

  애플리케이션의 이름은 관리자가 해당 애플리케이션에 대해 구성한 이름입니다.

  b 데스크톱 및 애플리케이션 선택기 창에서 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택합니다.
  c 왼쪽 창에서 **USB 디바이스**를 선택합니다.
  d 오른쪽 창에서 USB 디바이스를 선택하고 **연결**을 클릭합니다.

e 애플리케이션을 선택하고 **확인**을 클릭합니다.

참고 목록의 애플리케이션 이름은 애플리케이션 자체에서 가져오며 관리자가 데스크톱 및 애플리케이션 선택기 창에 표시되도록 구성한 애플리케이션 이름과 일치하지 않을 수 있습니다.

이제 USB 디바이스를 원격 애플리케이션과 함께 사용할 수 있습니다. 애플리케이션을 닫은 후 USB 디바이스가 즉시 릴리스되지 않습니다.

f 애플리케이션 사용을 완료한 경우 로컬 시스템에서 액세스할 수 있도록 USB 디바이스를 릴리스하려면 데스크톱 및 애플리케이션 선택기 창에서 설정 창을 다시 연 후 **USB 디바이스**를 선택하고 **연결 끊기**를 선택합니다.

- USB 디바이스를 로컬 시스템에 연결할 때 원격 데스크톱에 자동으로 연결되도록 Horizon Client를 구성합니다.

  Android 기반 Samsung 스마트폰 및 태블릿과 같이 MTP 드라이버를 사용하는 디바이스에 연결하려면 자동 연결 기능을 사용합니다.

  a USB 디바이스를 연결하기 전에 Horizon Client를 시작하고 원격 데스크톱에 연결하십시오.

  b VMware Horizon Client 메뉴 표시줄에서 **USB 디바이스 연결 > 삽입 시 USB 디바이스 자동 연결**을 선택합니다.

  c USB 디바이스를 연결합니다.

  Horizon Client를 시작한 후 로컬 시스템에 연결하는 USB 디바이스는 원격 데스크톱으로 리디렉션됩니다.

- Horizon Client 시작 시 USB 디바이스를 원격 데스크톱에 자동 연결하도록 Horizon Client를 구성합니다.

  a VMware Horizon Client 메뉴 표시줄에서 **USB 디바이스 연결 > 시동 시 USB 디바이스 자동 연결**을 선택합니다.

  b USB 디바이스에 연결하고 Horizon Client를 다시 시작합니다.

  Horizon Client를 시작하면 로컬 시스템에 연결된 USB 디바이스는 원격 데스크톱으로 리디렉션됩니다.

데스크톱에 USB 디바이스가 나타납니다. USB 디바이스가 데스크톱에 나타나는 데 최대 20초까지 걸릴 수 있습니다. 처음 디바이스를 데스크톱에 연결할 때 드라이버를 설치하라는 메시지가 나타날 수 있습니다.

USB 디바이스가 몇 분이 지나도 데스크톱에 나타나지 않을 경우, 디바이스의 연결을 끊었다가 클라이언트 컴퓨터에 디바이스를 다시 연결합니다.

후속 작업

USB 리디렉션에 문제가 있는 경우, Horizon 7에서 원격 데스크톱 기능 구성 문서에서 USB 리디렉션 문제 해결에 대한 항목을 참조하십시오.

USB 디바이스를 다시 시작할 때 재연결하도록 클라이언트 구성

원격 데스크톱에 USB 디바이스를 자동으로 연결하도록 Horizon Client를 구성하지 않은 경우, 가끔 다시 시작하는 특정 디바이스에 다시 연결하도록 Horizon Client를 구성할 수 있습니다. 그렇지 않으면 업그레이드 중 디바이스가 다시 시작할 때 디바이스는 원격 데스크톱이 아니라 로컬 시스템에 연결됩니다.

운영 체제 업그레이드 중 자동으로 다시 시작되는 스마트 폰이나 태블릿과 같은 USB 디바이스를 연결하려는 경우, 해당 특정 디바이스를 원격 데스크톱에 다시 연결하도록 Horizon Client를 설정할 수 있습니다. 이 작업을 수행하려면 클라이언트에서 구성 파일을 편집합니다.

Horizon Client에서 **삽입 시 자동 연결** 옵션을 사용할 경우, 클라이언트 시스템에 연결하는 모든 디바이스는 원격 데스크톱에 리디렉션됩니다. 일부 디바이스만 연결되도록 하려면 다음 절차를 사용하여 특정 USB 디바이스만 자동으로 연결되도록 Horizon Client를 구성합니다.

필수 조건

디바이스의 공급업체 ID(VID) 및 제품 ID(PID)의 16진수 형식을 결정합니다. 지침을 보려면 http://kb.vmware.com/kb/1011600에서 VMware 기술 자료 문서를 참조하십시오.

프로시저

1 텍스트 편집기를 사용하여 클라이언트에서 config.ini 파일을 엽니다.

OS 버전	파일 경로
Windows 7, 8.x 또는 Windows 10	C:₩ProgramData₩VMware₩VMware USB Arbitration Service₩config.ini
Windows XP	C:₩Documents and Settings₩All Users₩Application Data₩VMware₩VMware USB Arbitration Service₩config.ini

2 특정 디바이스에 slow-reconnect 속성을 설정합니다.

```
usb.quirks.device0 = "vid:pid slow-reconnect"
```

여기서, vid:pid는 디바이스의 공급업체 ID 및 제품 ID를 16진수로 표시한 것입니다. 예를 들어, 다음 줄은 이 속성을 두 개의 USB 디바이스에 설정합니다.

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

0에서부터 순서대로 usb.quirks.device*N* 디바이스 속성을 지정합니다. 예를 들어, usb.quirks.device0 줄에 usb.quirks.device1이 아니라 usb.quirks.device2 줄이 이어지면 첫 번째 줄만 읽습니다.

스마트폰 및 태블릿과 같은 디바이스가 펌웨어나 운영 체제 업그레이드를 진행 중이면 디바이스가 다시 시작하여 이를 관리하는 원격 데스크톱에 연결되기 때문에 업그레이드에 성공합니다.

웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용

실시간 오디오-비디오 기능을 통해 원격 데스크톱에서 로컬 컴퓨터의 웹캠 또는 마이크를 사용할 수 있습니다. 실시간 오디오-비디오는 표준 회의 애플리케이션 및 브라우저 기반 비디오 애플리케이션과 호환되며 표준 웹캠, 오디오 USB 디바이스 및 아날로그 오디오 입력을 지원합니다.

실시간 오디오-비디오 기능 설정과 원격 데스크톱의 프레임 속도 및 이미지 해상도 구성에 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오. 클라이언트 시스템에서 이러한 설정 구성에 대한 자세한 내용은 http://kb.vmware.com/kb/2053644의 VMware 기술 자료 문서, Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients(Horizon View 클라이언트의 실시간 오디오-비디오에 대한 프레임 속도 및 해상도 설정)을 참조하십시오.

실시간 오디오-비디오 기능의 올바른 설치와 작동을 확인하는 테스트 애플리케이션을 다운로드하려면 http://labs.vmware.com/flings/real-time-audio-video-test-application 페이지로 이동합니다. 이 테스트 애플리케이션은 VMware 플링(fling)으로 제공되므로 기술 지원이 따로 없습니다.

웹캠을 사용할 수 있는 경우

Horizon 관리자가 실시간 오디오-비디오 기능을 구성하고, 사용자가 VMware Blast 디스플레이 프로토콜이나 PCoIP 디스플레이 프로토콜을 사용하는 경우, 기본 제공되거나 로컬 컴퓨터에 연결된 웹캠을 데스크톱에서 사용할 수 있습니다. Skype, Webex 또는 Google Hangouts 등의 회의 애플리케이션에서 이 웹캠을 사용할 수 있습니다.

원격 데스크톱에 Skype, Webex 또는 Google Hangouts와 같은 애플리케이션을 설치하는 동안 애플리케이션의 메뉴에서 입력 및 출력 디바이스를 선택할 수 있습니다. 가상 시스템 데스크톱의 경우에는 VMware 가상 마이크 및 VMware 가상 웹캠을 선택할 수 있습니다. 게시된 데스크톱의 경우에는 원격 오디오 디바이스와 VMware 가상 웹캠을 선택할 수 있습니다.

그러나 많은 애플리케이션의 경우에 이 기능은 저절로 작동되며 입력 디바이스를 선택하지 않아도 됩니다.

현재 웹캠을 로컬 컴퓨터에서 사용 중일 경우, 원격 데스크톱에서 동시에 사용할 수 없습니다. 또한, 원격 데스크톱에서 웹캠을 사용 중이면 로컬 컴퓨터에서 동시에 웹캠을 사용할 수 없습니다.

중요 USB 웹캠을 사용 중일 경우, Horizon Client의 **USB 디바이스 연결** 메뉴를 사용하여 연결하지 마십시오. 그렇게 연결하기 위해 USB 리디렉션을 통해 디바이스를 라우팅하면 비디오 채팅에 대한 성능을 사용할 수 없게 됩니다.

로컬 컴퓨터에 연결된 웹캠이 하나 이상 있는 경우, 원격 데스크톱에서 사용할 기본 웹캠을 구성할 수 있습니다.

Windows 클라이언트 시스템에서 기본 웹캠 또는 마이크 선택

실시간 오디오-비디오 기능의 경우, 클라이언트 시스템에 여러 개의 웹캠이나 마이크가 있으면 원격 데스크톱이나 애플리케이션에서는 그중 하나만 사용됩니다. 기본 웹캠이나 마이크를 지정하려는 경우에는 Horizon Client에서 실시간 오디오-비디오 기능을 구성할 수 있습니다.

사용 가능할 경우 원격 데스크톱 또는 애플리케이션에서 기본 웹캠 또는 마이크가 사용되며 그렇지 않을 경우 다른 웹캠이나 마이크가 사용됩니다.

실시간 오디오-비디오 기능을 사용하면 비디오 디바이스, 오디오 입력 디바이스 및 오디오 출력 디바이스는 USB 리디렉션을 사용하지 않아도 작동하며, 필요한 네트워크 대역폭 양이 대폭 감소합니다. 아날로그 오디오 입력 디바이스도 지원됩니다.

참고 USB 웹캠이나 마이크를 사용하는 경우, Horizon Client의 **USB 디바이스 연결** 메뉴를 사용하여 연결하지 마십시오. 연결하려면 디바이스가 실시간 오디오-비디오 기능을 사용할 수 없도록 USB 리디렉션을 통해 디바이스를 라우팅합니다.

필수 조건

- 클라이언트 시스템에 USB 웹캠이나 USB 마이크 또는 다른 유형의 마이크가 설치되어 있고 작동하는지 확인합니다.
- 원격 데스크톱 또는 애플리케이션에 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용하고 있는지 확인합니다.
- 서버에 연결합니다.

프로시저

1 [설정] 대화상자를 열고 왼쪽 창에서 **실시간 오디오-비디오**를 선택합니다.

[설정] 대화상자는 데스크톱 및 애플리케이션 화면의 오른쪽 상단에서 **설정**(톱니) 아이콘을 클릭하거나 데스크톱 또는 애플리케이션 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택하면 열 수 있습니다.

2 **기본 웹캠** 드롭다운 메뉴에서 기본 웹캠을 선택하고 **기본 마이크** 드롭다운 메뉴에서 기본 마이크를 선택합니다.

드롭다운 메뉴에는 클라이언트 시스템에서 사용할 수 있는 웹캠과 마이크가 표시됩니다.

3 **확인** 또는 **적용**을 클릭하여 변경 사항을 저장합니다.

다음번에 원격 데스크톱 또는 애플리케이션을 시작하면 선택한 기본 웹캠과 마이크가 원격 데스크톱이나 애플리케이션으로 리디렉션됩니다.

텍스트와 이미지 복사 및 붙여넣기

기본적으로 클라이언트 시스템에서 원격 데스크톱 또는 애플리케이션으로 텍스트를 복사하여 붙여 넣을 수 있습니다. Horizon 관리자가 해당 기능을 사용하도록 설정한 경우, 원격 데스크톱 또는 애플리케이션에서 클라이언트 시스템으로 또는 두 개의 원격 데스크톱 또는 애플리케이션 간에 텍스트를 복사하여 붙여넣을 수 있습니다.

지원되는 파일 형식에는 텍스트, 이미지 및 RTF(서식 있는 텍스트)가 포함됩니다. 몇 가지 제한 사항이 적용됩니다.

VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용할 경우, Horizon 관리자는 이 기능을 클라이언트 시스템에서 원격 데스크톱 또는 애플리케이션으로만 또는 원격 데스크톱 또는 애플리케이션에서 클라이언트 시스템으로만 복사 및 붙여넣기가 가능하도록 설정하거나, 두 작업이 모두 가능하도록 또는 모두 불가능하도록 설정할 수 있습니다.

Horizon 관리자는 Horizon Agent와 관련된 그룹 정책 설정을 구성하여 복사 및 붙여넣기 기능을 구성합니다. Horizon Server 및 Agent 버전에 따라 관리자는 그룹 정책을 사용하여 복사 및 붙여넣기 작업 동안 클립보드 형식을 제한하거나 스마트 정책을 사용하여 원격 데스크톱의 복사 및 붙여넣기 동작을 제어할 수도 있습니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

Horizon 7 버전 7.0 이하와 Horizon Client 4.0 이하에서 클립보드는 복사 및 붙여넣기 작업에 1MB의 데이터를 사용할 수 있습니다. Horizon 7 버전 7.0.1 이상과 Horizon Client 4.1 이상에서는 서버와 클라이언트 둘 다에 대해 클립보드 메모리 크기를 구성할 수 있습니다. PCoIP 또는 VMware Blast 세션이 설정되어 있을 때 서버에서 클립보드 메모리 크기를 클라이언트로 보냅니다. 유효 클립보드 메모리 크기는 서버와 클라이언트의 클립보드 메모리 크기 값 중에서 작은 쪽입니다.

서식이 지정된 텍스트를 복사하는 경우 일부 데이터는 텍스트이고 일부 데이터는 서식 정보입니다. 대용량의 서식이 지정된 텍스트 또는 텍스트 및 이미지를 복사하는 경우, 텍스트와 이미지를 붙여넣으려고 하면 서식 또는 이미지를 제외한 일반 텍스트의 일부 또는 전부가 보일 수 있습니다. 세 가지 유형의 데이터가 별도로 저장되는 경우가 있기 때문입니다. 예를 들면, 복사하는 문서의 유형에 따라 이미지가 이미지 또는 RTF 데이터로 저장될 수도 있습니다.

텍스트 및 RTF 데이터가 모두 최대 클립보드 크기 미만을 사용하는 경우 서식이 지정된 텍스트를 붙여넣습니다. 종종 텍스트 및 서식에서 최대 클립보드 크기 이상을 사용하는 경우 RTF 데이터를 폐기하고 일반 텍스트를 붙여넣기 위해 RTF 데이터를 잘라낼 수 없습니다.

서식이 지정된 모든 텍스트와 이미지를 한 번 작업으로 모두 선택하여 붙여넣을 수 없는 경우 각 작업에서 적은 용량으로 복사 및 붙여넣어야 합니다.

클라이언트 컴퓨터의 원격 데스크톱 및 파일 시스템 간에는 파일을 복사하고 붙여넣을 수 없습니다.

클라이언트 클립보드 메모리 크기 구성

Horizon 7 버전 7.0.1 이상과 Horizon Client 4.1 이상에서는 서버와 클라이언트 둘 다에 대해 클립보드 메모리 크기를 구성할 수 있습니다.

PCoIP 또는 VMware Blast 세션이 설정되어 있을 때 서버에서 클립보드 메모리 크기를 클라이언트로 보냅니다. 유효 클립보드 메모리 크기는 서버와 클라이언트의 클립보드 메모리 크기 값 중에서 작은 쪽입니다.

클립보드 메모리 크기를 설정하려면 Windows 레지스트리 값 HKLM₩Software₩VMware, Inc.₩VMware VDP₩Plugins₩MKSVchan₩ClientClipboardSize를 수정합니다. 값 유형은 REG_DWORD입니다. 값은 KB 단위로 지정됩니다. 0을 지정하거나 값을 지정하지 않을 경우, 기본 클라이언트 클립보드 메모리 크기는 8,192KB(8MB)입니다.

클립보드 메모리 크기가 크면 네트워크에 따라 성능이 저하될 수 있습니다. VMware에서는 클립보드 메모리 크기를 16MB보다 크지 않은 값으로 설정할 것을 권장합니다.

원격 애플리케이션 사용

원격 애플리케이션은 클라이언트 PC 또는 노트북에 설치된 애플리케이션과 형태 및 느낌이 같습니다.

- 애플리케이션을 통해 원격 애플리케이션을 최소화 및 최대화할 수 있습니다. 원격 애플리케이션을 최소화하면 클라이언트 시스템의 작업 표시줄에 나타납니다. 작업 표시줄의 아이콘을 클릭하여 원격 애플리케이션을 최소화 및 최대화할 수도 있습니다.
- 원격 애플리케이션은 해당 애플리케이션 내에서 또는 작업 표시줄의 아이콘을 마우스 오른쪽 버튼으로 클릭하여 종료할 수 있습니다.
- Alt+Tab을 눌러서 열린 원격 애플리케이션 사이에서 전환할 수 있습니다.
- 원격 애플리케이션이 Windows 시스템 트레이 항목을 생성하면 해당 항목이 Windows 클라이언트 컴퓨터의 시스템 트레이에도 나타납니다. 기본적으로, 시스템 트레이 아이콘은 알림을 표시할 때만 나타나지만 이 동작은 원래 설치된 애플리케이션과 마찬가지로 사용자 지정할 수 있습니다.

  참고 제어판을 열어서 알림 영역 아이콘을 사용자 지정할 경우, 원격 애플리케이션 아이콘의 이름은 VMware Horizon Client - 애플리케이션 이름으로 나열됩니다.

원격 애플리케이션에서 문서 저장

Microsoft Word, WordPad 등의 일부 원격 애플리케이션을 사용하여 문서를 생성하고 저장할 수 있습니다. 이들 문서가 저장되는 위치는 회사의 네트워크 환경에 따라 달라집니다. 예를 들어 문서는 로컬 컴퓨터에 마운트된 홈 공유에 저장될 수 있습니다.

관리자는 ADMX 템플릿 파일을 사용하여 문서 저장 위치를 지정하는 그룹 정책을 설정할 수 있습니다. 이 정책을 **원격 데스크톱 서비스 사용자 홈 디렉토리 설정**이라고 합니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

원격 데스크톱 또는 애플리케이션에서 인쇄

원격 데스크톱에서 가상 프린터 또는 클라이언트 컴퓨터에 연결된 USB 프린터로 인쇄할 수 있습니다. 가상 인쇄 및 USB 인쇄는 충돌 없이 함께 작동됩니다.

다음과 같은 유형의 원격 데스크톱과 애플리케이션에서 가상 인쇄 기능을 사용할 수 있습니다.

- Windows Server 운영 체제를 실행하는 원격 데스크톱
- 가상 시스템 RDS 호스트의 세션 기반 데스크톱
- 원격 호스팅되는 애플리케이션

원격 데스크톱에서 가상 프린터 기능에 대한 인쇄 환경설정 지정

가상 인쇄 기능을 사용하면 최종 사용자가 추가 인쇄 드라이버를 원격 데스크톱에 설치할 필요 없이 원격 데스크톱에서 로컬 또는 네트워크 프린터를 사용할 수 있습니다. 이 기능을 통해 사용할 수 있는 각 프린터의 경우 데이터 압축, 인쇄 품질, 양면 인쇄, 색상 등의 환경을 설정할 수 있습니다.

프린터가 로컬 컴퓨터에 추가되고 나면 Horizon Client는 원격 데스크톱에서 사용할 수 있는 프린터 목록에 해당 프린터를 추가합니다. 추가 구성은 필요하지 않습니다. 관리자 권한을 가진 사용자는 가상 프린터 구성 요소와의 충돌 없이 원격 데스크톱에 프린터 드라이버를 계속 설치할 수 있습니다.

중요 이 기능은 다음 유형의 프린터에서 사용할 수 없습니다.

- 원격 데스크톱의 가상 USB 포트에 연결하기 위해 USB 리디렉션 기능을 사용 중인 USB 프린터

  가상 인쇄 기능을 함께 사용하기 위해 원격 데스크톱에서 USB 프린터 연결을 끊어야 합니다.
- 파일로 인쇄하기 위한 Windows 기능

  인쇄 대화 상자에서 **파일로 인쇄** 확인란을 선택할 수 없습니다. 파일을 생성하는 프린터 드라이버를 사용할 수 있습니다. 예를 들어 PDF 작성 프로그램을 사용하여 PDF 파일로 인쇄할 수 있습니다.

이 절차는 Windows 7 또는 Windows 8.x(데스크톱) 운영 체제가 설치된 원격 데스크톱용으로 작성되었습니다. 이 절차는 Windows Server 2008 및 Windows Server 2012에 대한 절차와 유사하지만 정확하게 동일한 것은 아닙니다.

필수 조건

에이전트의 가상 인쇄 구성 요소가 원격 데스크톱에 설치되어 있는지 확인합니다. 원격 데스크톱 파일 시스템에서 C:₩Program Files₩Common Files₩ThinPrint 폴더가 있는지 확인합니다.

가상 인쇄를 사용하려면 Horizon 관리자가 원격 데스크톱에 대해 가상 인쇄 기능을 사용하도록 설정해야 합니다. 이 작업에는 에이전트 설치 관리자의 **가상 인쇄** 설정 옵션을 사용하도록 설정하고 가상 인쇄 동작 관련 정책을 설정하는 작업이 포함됩니다. 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 또는 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

프로시저

1. Windows 7 또는 Windows 8.x 원격 데스크톱에서 **시작 > 디바이스 및 프린터**를 클릭합니다.
2. 디바이스 및 프린터 창에서 마우스 오른쪽 버튼으로 기본 프린터를 클릭하고, 컨텍스트 메뉴에서 **프린터 속성**을 선택한 후 프린터를 선택합니다.

   View Agent 6.2 이상 또는 Horizon Agent 7.0 이상이 설치된 경우 가상 프린터가 RDS 호스트의 단일 사용자 가상 시스템 데스크톱에서는 <printer_name>으로, 게시된 데스크톱에서는 <printer_name>(s<session_ID>)으로 표시됩니다. View Agent 6.1 이전 버전이 원격 데스크톱에 설치되어 있는 경우 가상 프린터가 <printer_name>#:<number>로 표시됩니다.
3. 프린터 속성 창에서 **디바이스 설치** 탭을 클릭하고 사용할 설정을 지정합니다.
4. **일반** 탭에서 **환경설정**을 클릭하고 사용할 설정을 지정합니다.
5. 인쇄 환경설정 대화 상자에서 다른 탭을 선택하고 사용할 설정을 지정합니다.

   페이지 조정 고급 설정의 경우, VMware는 기본 설정을 유지할 것을 권장합니다.
6. **확인**을 클릭합니다.

7 사용자 지정 용지 양식을 사용하려면 클라이언트에서 양식을 정의합니다.

a **제어판 > 하드웨어 및 소리 > 디바이스 및 프린터**로 이동합니다.

b 프린터를 선택하고 화면 상단에서 **인쇄 서버 속성**을 클릭합니다.

c **양식** 탭에서 설정을 지정하고 **양식 저장**을 클릭합니다.

이제 이 양식을 원격 데스크톱에서 사용할 수 있습니다.

USB 프린터 사용

Horizon 환경에서 가상 프린터 및 리디렉션된 USB 프린터가 충돌 없이 함께 작동할 수 있습니다.

USB 프린터는 로컬 클라이언트 시스템에서 USB 포트에 연결된 프린터입니다. USB 프린터로 인쇄 작업을 보내려면 USB 리디렉션 기능을 사용하거나 가상 인쇄 기능을 사용할 수 있습니다. USB 인쇄는 네트워크 상태에 따라 가상 인쇄보다 더 빠를 수도 있습니다.

- 필요한 드라이버가 원격 데스크톱에도 설치되어 있으면 USB 리디렉션 기능을 사용하여 USB 프린터를 원격 데스크톱의 가상 USB 포트에 연결할 수 있습니다.

  이 리디렉션 기능을 사용할 경우 프린터는 더 이상 클라이언트의 실제 USB 포트에 로컬로 연결되지 않으며, 이런 이유로 USB 프린터가 로컬 클라이언트 시스템의 로컬 프린터 목록에 나타나지 않습니다. 또한 이는 원격 데스크톱에서 USB 프린터로 인쇄할 수 있지만 로컬 클라이언트 시스템에서는 인쇄할 수 없다는 뜻입니다.

  원격 데스크톱에서는 리디렉션된 USB 프린터가 <printer_name>으로 나타납니다.

  USB 프린터 연결 방법에 대한 자세한 내용은 USB 디바이스 연결에 나와 있습니다.

- 일부 클라이언트에서는 가상 인쇄 기능을 사용하여 USB 프린터로 인쇄 작업을 보낼 수도 있습니다. 가상 인쇄 기능을 사용할 경우 원격 데스크톱 및 로컬 클라이언트에서 USB 프린터로 인쇄할 수 있으며 원격 데스크톱에 프린터 드라이버를 설치할 필요가 없습니다.

Adobe Flash 디스플레이 제어

Horizon 관리자는 컴퓨팅 리소스를 확보하는 수준에서 Adobe Flash 컨텐츠를 원격 데스크톱에 표시되도록 설정할 수 있습니다. 일부의 경우 이 설정으로 인해 재생 품질이 저하될 수 있습니다. 마우스 포인터를 Adobe Flash 컨텐츠로 이동하면 Horizon 관리자가 지정하는 Adobe Flash 설정을 재정의할 수 있습니다.

Adobe Flash 디스플레이 제어는 Windows의 Internet Explorer 세션과 Adobe Flash 버전 9 및 10에서만 사용할 수 있습니다. Adobe Flash 디스플레이 품질을 제어하려면 Adobe Flash를 전체 화면 모드로 실행하지 말아야 합니다.

프로시저

1 필요에 따라, 원격 데스크톱 내의 Internet Explorer에서 해당 Adobe Flash 컨텐츠를 검색하여 시작합니다.

  Horizon 관리자가 Adobe Flash 설정을 구성한 방법에 따라 프레임 수가 줄어들거나 재생 품질이 저하될 수 있습니다.

2 재생 중에 마우스 포인터를 Adobe Flash 컨텐츠 내부로 가져갑니다.

커서가 Adobe Flash 컨텐츠 내에 머무는 동안에는 디스플레이 품질이 개선됩니다.

3 품질 개선 상태를 유지하려면 Adobe Flash 컨텐츠 내부를 두 번 클릭합니다.

Horizon Client 외부에서 열리는 URL 링크 클릭

관리자는 원격 데스크톱 또는 애플리케이션 내부에서 클릭하는 URL 링크가 클라이언트 시스템의 기본 브라우저에서 열리도록 구성할 수 있습니다. 이 링크는 웹 페이지, 전화 번호, e-메일 주소이거나 다른 유형의 링크일 수 있습니다. 이 기능을 URL 컨텐츠 리디렉션이라고 합니다.

관리자는 사용자가 원격 데스크톱이나 애플리케이션에서 열기 위해 클라이언트 시스템의 브라우저나 애플리케이션 내에서 클릭하는 URL 링크를 구성할 수도 있습니다. 이 시나리오에서 Horizon Client가 아직 열려 있지 않으면 Horizon Client가 시작되고 로그인 메시지가 표시됩니다.

관리자는 보안을 위해 URL 컨텐츠 리디렉션 기능을 설정할 수도 있습니다. 예를 들어, 회사 네트워크 내부에서 네트워크 외부의 URL을 가리키는 링크를 클릭할 경우, 링크를 원격 애플리케이션에서 더 안전하게 열 수 있습니다. 관리자는 어떤 애플리케이션이 링크를 열지 구성할 수 있습니다.

Horizon Client를 처음 시작하고 URL 컨텐츠 리디렉션 기능이 구성된 서버에 연결하면 리디렉션을 위한 링크를 클릭할 때 VMware Horizon URL 필터 애플리케이션을 열라는 메시지가 Horizon Client에 표시됩니다. **열기**를 클릭하여 URL 컨텐츠 리디렉션을 허용합니다.

URL 컨텐츠 리디렉션 기능이 구성된 방식에 따라 Horizon Client에서 기본 웹 브라우저를 VMware Horizon URL 필터로 변경할지 묻는 경고 메시지를 표시할 수 있습니다. 이 메시지가 표시되면 **"VMware Horizon URL 필터" 사용** 버튼을 클릭하여 VMware Horizon URL 필터가 기본 브라우저가 되도록 허용합니다. **"VMware Horizon URL 필터" 사용**을 클릭한 후에 기본 브라우저를 변경하지 않으면 이 메시지가 한 번만 표시됩니다.

사용자가 URL을 클릭하면 Horizon Client에서 애플리케이션을 선택하도록 요구하는 경고 메시지를 표시할 수도 있습니다. 이 메시지가 표시되면 **애플리케이션 선택**을 클릭하여 클라이언트 시스템에서 애플리케이션을 검색하거나 **App Store 검색**을 클릭하여 새 애플리케이션을 검색한 후 설치합니다. **취소**를 클릭하면 URL이 열리지 않습니다.

각 회사에서는 자체 URL 리디렉션 정책을 구성합니다. 회사 내에서 URL 컨텐츠 리디렉션 기능이 작동하는 방식에 대해 질문이 있는 경우 시스템 관리자에게 문의하십시오.

CAD 및 3D 애플리케이션의 상대 마우스 기능 사용

View 5.2 이상 데스크톱에서 CAD 또는 3D 애플리케이션을 사용할 때 Blast Extreme 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용할 경우, 상대 마우스 기능을 사용하도록 설정하면 마우스 성능이 향상됩니다.

대개 3D 렌더링이 필요하지 않은 애플리케이션을 사용할 경우, Horizon Client는 절대 좌표를 사용하여 마우스 포인터 이동에 대한 정보를 전송합니다. 절대 좌표를 사용하면 클라이언트는 특히 회사 네트워크 밖에 있을 때 마우스 이동을 로컬로 렌더링하여 성능을 높여줍니다.

AutoCAD와 같은 그래픽 위주의 애플리케이션을 사용해야 하는 작업이나 3D 비디오 게임 재생을 위해 절대 좌표가 아닌 상대 좌표를 사용하는 상대 마우스 기능을 사용하도록 설정하여 마우스 성능을 개선할 수 있습니다. 이 기능을 사용하려면 Horizon Client 메뉴 표시줄에서 **옵션 > 상대 마우스 사용**을 선택합니다.

참고 전체 화면 모드가 아닌 창 모드에서 Horizon Client를 사용하고 상대 마우스 기능을 사용하도록 설정한 경우, Horizon Client 메뉴 옵션으로 마우스 포인터를 이동하거나 Horizon Client 창 외부로 포인터를 이동하지 못할 수 있습니다. 이 상황을 해결하려면 Ctrl+Alt를 누릅니다.

상대 마우스 기능을 사용하도록 설정하면 WAN에서 회사 네트워크 외부에 있는 경우 성능이 더 저하될 수 있습니다.

중요 이 기능을 사용하려면 View 5.2 이상 데스크톱이 필요하며 데스크톱 풀에 대해 3D 렌더링 기능을 사용하도록 설정해야 합니다. 3D 렌더링에 사용 가능한 옵션 및 풀 설정에 대한 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 또는 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

스캐너 사용

로컬 클라이언트 시스템에 연결된 스캐너를 사용하여 원격 데스크톱 및 애플리케이션으로 정보를 스캔할 수 있습니다. 이 기능은 USB 리디렉션을 사용할 경우 얻을 수 있는 대역폭에 비해 상당히 적은 대역폭을 사용하여 스캔 데이터를 리디렉션합니다.

스캐너 리디렉션은 TWAIN 및 WIA(Windows Image Acquisition) 형식과 호환 가능한 표준 스캔 디바이스를 지원합니다. 클라이언트 시스템에 스캐너 디바이스 드라이버를 설치해야 하지만 에이전트가 설치된 원격 데스크톱 운영 체제에는 스캐너 디바이스 드라이버를 설치하지 않아도 됩니다.

Horizon 관리자가 스캐너 리디렉션 기능을 구성한 경우, Blast Extreme 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용하면 원격 데스크톱 또는 애플리케이션에서 로컬 시스템에 연결된 스캐너를 사용할 수 있습니다.

중요 스캐너를 사용 중인 경우 Horizon Client의 **USB 디바이스 연결** 메뉴에서 스캐너를 연결하지 마십시오. 이 메뉴에서 연결하면 USB 리디렉션을 통해 디바이스가 라우팅되고 성능을 사용할 수 없게 됩니다.

스캔 데이터가 원격 데스크톱 또는 애플리케이션으로 리디렉션되는 경우 로컬 컴퓨터에서 스캐너에 액세스할 수 없습니다. 이와 반대로 스캐너가 로컬 컴퓨터에서 사용 중인 경우 원격 데스크톱 또는 애플리케이션에서 스캐너에 액세스할 수 없습니다.

스캐너 리디렉션 기능 사용에 관한 팁

- 기본이 아닌 스캐너를 선택하거나 구성 설정을 변경하려면 원격 데스크톱의 시스템 트레이 또는 알림 영역의 스캐너 아이콘( )을 클릭합니다. RDS 애플리케이션에서 시스템 트레이 아이콘은 로컬 클라이언트 컴퓨터로 리디렉션됩니다.

이 아이콘을 클릭할 때 나타나는 메뉴는 사용하지 않아도 됩니다. 스캐너 리디렉션은 추가 구성 없이 작동합니다. 두 개 이상의 디바이스가 클라이언트 컴퓨터에 연결된 경우 아이콘 메뉴를 사용하여 사용할 디바이스 변경과 같은 옵션을 구성할 수 있습니다.

참고 표시되는 메뉴에 스캐너가 없으면 호환되지 않는 스캐너가 클라이언트 컴퓨터에 연결되어 있는 것입니다. 스캐너 아이콘이 표시되지 않으면 스캐너 리디렉션 기능이 사용하지 않도록 설정되었거나 원격 데스크톱에 설치되지 않은 것입니다. 스캐너 리디렉션 기능은 Mac 또는 Linux 클라이언트 시스템에서 지원되지 않으므로 해당 시스템에는 이 아이콘이 나타나지 않습니다.

- 메뉴에서 **환경설정** 옵션을 클릭하여 이미지 압축 제어, 스캐너 리디렉션 메뉴에서 웹캠 숨기기 및 기본 스캐너 선택 방법 결정 등의 옵션을 선택합니다.

  VMware에서 권장하는 대로 실시간 오디오-비디오 기능을 사용하여 웹캠을 리디렉션하려는 경우 웹캠을 숨기는 옵션을 선택할 수 있습니다. 직접 사진을 찍어서 스캔하려면 웹캠과 함께 스캐너 리디렉션을 사용하면 됩니다.

  참고 특정 스캐너를 사용하도록 스캐너 리디렉션을 구성하는 경우 해당 스캐너를 사용할 수 없으면 스캐너 리디렉션이 작동하지 않습니다.

- 대부분의 TWAIN 스캐너는 기본적으로 스캐너 설정 대화상자를 표시하지만 일부 스캐너는 표시하지 않습니다. 설정 옵션을 표시하지 않는 스캐너의 경우 스캐너 아이콘 메뉴의 **환경설정** 옵션을 사용하여 **항상 스캐너 설정 대화상자 표시** 옵션을 선택할 수 있습니다.
- 너무 큰 이미지를 스캔하거나 너무 높은 해상도로 스캔하는 경우 기능이 작동하지 않을 수 있습니다. 이런 경우에 스캔 진행률 표시기가 멈추거나 스캐너 애플리케이션이 예상치 않게 종료될 수도 있습니다. 원격 데스크톱을 최소화하는 경우 해상도가 너무 높게 설정되어 있다는 오류 메시지가 클라이언트 시스템에 표시될 수 있습니다. 이 문제를 해결하려면 해상도를 낮추거나 더 작은 크기로 이미지를 잘라낸 다음 다시 스캔하십시오.

직렬 포트 리디렉션 사용

이 기능을 사용하여 로컬로 연결된 직렬(COM) 포트(예: 내장형 RS232 포트 또는 USB-직렬 어댑터)를 리디렉션할 수 있습니다. 프린터, 바코드 판독기 및 기타 직렬 디바이스와 같은 디바이스를 이러한 포트에 연결한 후 원격 데스크톱에서 사용할 수 있습니다.

Horizon 관리자가 직렬 포트 리디렉션 기능을 구성한 경우, VMware Blast Extreme 또는 PCoIP 디스플레이 프로토콜을 사용하면 추가 구성 없이 원격 데스크톱에서 직렬 포트 리디렉션이 작동합니다. 예를 들어 로컬 클라이언트 시스템의 COM1이 원격 데스크톱의 COM1로 리디렉션됩니다. COM 포트를 아직 사용하고 있지 않으면 COM2가 COM2로 리디렉션됩니다. 원격 데스크톱에 COM 포트가 이미 있는 경우에는 충돌을 피하기 위해 해당 COM 포트가 매핑됩니다. 예를 들어 COM1 및 COM2가 원격 데스크톱에 이미 있으면 클라이언트의 COM1은 기본적으로 COM3에 매핑됩니다.

클라이언트 시스템에 필수 디바이스 드라이버를 설치해야 하지만 에이전트가 설치된 원격 데스크톱 운영 체제에는 디바이스 드라이버를 설치하지 않아도 됩니다. 예를 들어 로컬 클라이언트 시스템에서 특정 디바이스 드라이버가 작동되어야 하는 USB-직렬 어댑터를 사용하는 경우에는 클라이언트 시스템에서만 해당 드라이버를 설치하면 됩니다.

중요 USB-직렬 어댑터에 연결하는 디바이스를 사용하는 경우에는 Horizon Client의 **USB 디바이스 연결** 메뉴에서 디바이스를 연결하지 마십시오. 이 메뉴에서 연결하면 USB 리디렉션을 통해 디바이스가 라우팅되고 직렬 포트 리디렉션 기능은 사용되지 않습니다.

직렬 포트 리디렉션 기능 사용에 관한 팁

- 매핑된 COM 포트를 연결하고, 연결을 끊고, 사용자 지정하려면 원격 데스크톱의 시스템 트레이 또는 알림 영역의 직렬 포트 아이콘( )을 클릭합니다.

  직렬 포트 아이콘을 클릭하면 **VMware Horizon용 직렬 COM 리디렉션** 컨텍스트 메뉴가 나타납니다.

  참고 컨텍스트 메뉴의 항목이 회색으로 표시되면 관리자가 구성을 잠금 것입니다. 이 아이콘은 필요한 에이전트 버전 및 Windows용 Horizon Client를 사용하고 있는 경우에만 표시되며 Blast Extreme 또는 PCoIP를 통해 연결해야 합니다. Mac, Linux 또는 모바일 클라이언트에서 원격 데스크톱에 연결하는 경우에는 이 아이콘이 나타나지 않습니다.

- 컨텍스트 메뉴에서 포트 항목은 **COM1이(가) COM3에 매핑됨** 등의 형식을 사용하여 표시됩니다. 이 예제에서 COM1에 해당하는 첫 번째 포트는 물리적 포트이거나 로컬 클라이언트 시스템에서 사용되는 USB-직렬 어댑터입니다. 이 예제에서 COM3에 해당하는 두 번째 포트는 가상 데스크톱에서 사용되는 포트입니다.
- COM 포트를 마우스 오른쪽 버튼으로 클릭하고 **포트 속성** 명령을 선택합니다.

  COM 속성 대화상자에서 원격 데스크톱 세션이 시작될 때 자동으로 연결되도록 포트를 구성하거나 일부 모뎀 및 기타 디바이스에 필요한 DSR을 무시할 수 있습니다(즉, data-set-ready 신호 무시).

  또한 원격 데스크톱에 사용되는 포트 번호를 변경할 수도 있습니다. 예를 들어 클라이언트의 COM1 포트가 원격 데스크톱의 COM3에 매핑되지만 사용하는 애플리케이션에 COM1이 필요한 경우에는 포트 번호를 COM1로 변경할 수 있습니다. COM1이 원격 데스크톱에 이미 있으면 **COM1(중복됨)**이 표시될 수 있습니다. 이 중복된 포트도 계속 사용할 수 있습니다. 원격 데스크톱은 ESXi 호스트 및 클라이언트 시스템의 포트를 통해 직렬 데이터를 수신할 수 있습니다.
- 매핑된 COM 포트에 액세스해야 하는 애플리케이션을 시작하기 전에 해당 포트에 연결되는지 확인하십시오. 예를 들어 COM 포트를 마우스 오른쪽 버튼으로 클릭하고 **연결**을 선택하여 원격 데스크톱에서 해당 포트를 사용합니다. 애플리케이션을 시작할 경우, 애플리케이션은 직렬 포트를 엽니다.

  리디렉션된 COM 포트가 열려 있고 원격 데스크톱에서 사용되고 있으면 로컬 컴퓨터에서 해당 포트에 액세스할 수 없습니다. 반대로, COM 포트가 로컬 컴퓨터에서 사용되고 있으면 원격 데스크톱에서 해당 포트에 액세스할 수 없습니다.

- 원격 데스크톱에서 Windows 장치 관리자의 **포트 설정** 탭을 사용하여 특정 COM 포트에 대한 기본 전송 속도를 설정할 수 있습니다. 클라이언트 시스템에서 Windows 장치 관리자의 동일한 설정을 사용해야 합니다. 이 탭의 설정은 애플리케이션이 포트 설정을 지정하지 않는 경우에만 사용됩니다.
- COM 포트 연결을 끊으려면 애플리케이션에서 포트를 닫거나 애플리케이션을 닫아야 합니다. 그런 후 **연결 해제** 명령을 선택하여 연결을 끊고 물리적 COM 포트를 클라이언트 시스템에서 사용할 수 있게 설정할 수 있습니다.
- 자동으로 연결할 직렬 포트를 구성할 경우 직렬 포트가 열리는 애플리케이션을 실행한 다음 데스크톱 세션 연결을 끊었다가 다시 연결하면 자동 연결 기능이 작동하지 않습니다. 직렬 포트의 시스템 트레이 아이콘 메뉴 옵션으로도 연결할 수 없습니다. 대부분의 경우 애플리케이션이 직렬 포트를 더 이상 사용할 수 없습니다. 이것은 정상적인 현상입니다. 애플리케이션을 종료하고 데스크톱 세션 연결을 해제한 다음 다시 연결하여 문제를 해결해야 합니다.

키보드 바로 가기

메뉴 명령과 공통 작업에 키보드 바로 가기를 사용할 수 있습니다.

Horizon Client 에서 모든 애플리케이션에서와 같은 방식으로 작동하는 바로 가기

표 5-4. 공통 키보드 바로 가기

조치	키 또는 키 조합
대화상자에서 강조 표시된 버튼을 클릭합니다.	Enter 키를 누릅니다.
컨텍스트 메뉴를 불러옵니다.	Shift+F10을 누릅니다.
대화상자에서 **취소** 버튼을 클릭합니다.	ESC를 누릅니다.
서버 섹션 창이나 데스크톱 및 애플리케이션 선택 창에서 항목 간을 이동합니다.	화살표 방향으로 이동하려면 화살표 키를 사용합니다. 오른쪽으로 이동하려면 Tab 키를 누릅니다. 왼쪽으로 이동하려면 Shift+Tab을 누릅니다.
서버 섹션 창이나 데스크톱 및 애플리케이션 선택 창에서 항목을 삭제합니다.	Delete를 누릅니다.
Windows 8.x에서 시작 화면과 데스크톱 화면 사이를 이동합니다.	Windows 키를 누릅니다.

Horizon Client 창(서버 선택 목록) 바로 가기

표 5-5. 연결할 서버를 지정하는 창에 따른 키 조합

메뉴 명령 또는 조치	키 조합
브라우저 창에서 도움말 시스템 열기	Alt+O+H, Ctrl+H
새 서버 명령	Alt+N
지원 정보 창 표시	Alt+O+S
Horizon Client 정보 창 표시	Alt+O+V

표 5-5. 연결할 서버를 지정하는 창에 따른 키 조합 (계속)

메뉴 명령 또는 조치	키 조합
SSL 구성 명령	Alt+O+O
항목을 시작한 후 선택기 숨기기 명령	Alt+O+I

원격 데스크톱 및 애플리케이션 선택기 바로 가기

표 5-6. 데스크톱 및 애플리케이션 선택 창에서 사용할 키 및 키 조합

메뉴 명령 또는 조치	키 조합
브라우저 창에서 도움말 시스템 열기	Alt+O+H, Ctrl+H
옵션 메뉴 표시	Alt+O
지원 정보 창 표시	Alt+O+S
Horizon Client 정보 창 표시	Alt+O+V
원격 데스크톱에서 로그오프	Shift+F10+O
서버에서 연결 해제 및 로그오프	Alt+D
즐겨찾기 표시와 **모두 표시** 사이에서 전환	Alt+F
즐겨찾기를 표시하는 동안 애플리케이션 또는 데스크톱 이름의 첫 글자 몇 개를 입력하고 검색어와 일치하는 다음 항목으로 이동	F4
즐겨찾기를 표시하는 동안 검색어와 일치하는 이전 항목으로 이동	Shift+F4
즐겨찾기로 표시 또는 즐겨찾기 지정 해제	Shift+F10+F
설정 메뉴 표시	Alt+S 또는 Shift+F10+S
선택한 항목 실행	Enter 또는 Shift+F10+L
원격 데스크톱 또는 애플리케이션 바로 가기를 클라이언트 시스템 시작 메뉴(Windows 7 이전) 또는 시작 화면(Windows 8.x)에 고정	Shift+F10+A
선택한 원격 데스크톱의 설정 표시 컨텍스트 메뉴 표시	Shift+F10+D
PCoIP 디스플레이 프로토콜을 사용하여 선택한 원격 데스크톱에 연결	Shift+F10+P
RDP 디스플레이 프로토콜을 사용하여 선택한 원격 데스크톱에 연결	Shift+F10+M
선택한 항목의 데스크톱 바로 가기 생성	Shift+F10+C
선택한 항목을 시작 메뉴 또는 시작 화면에 추가	Shift+F10+A
선택한 데스크톱 재설정(관리자가 재설정을 허용할 경우)	Shift+F10+R
데스크톱 및 애플리케이션 목록 새로고침	F5

데스크톱 창(PCoIP 또는 VMware Blast Extreme 세션) 바로 가기

원격 데스크톱 운영 체제에 들어가서 키를 누르기 전에 Ctrl+Alt를 먼저 누르거나 Horizon Client 메뉴 표시줄을 클릭하면 이러한 바로 가기가 실행됩니다.

표 5-7. PCoIP 및 VMware Blast 세션에 대한 키 조합

메뉴 명령 또는 조치	키 조합
마우스 커서를 원격 데스크톱 운영 체제 내에 있지 않도록 해제	Ctrl+Alt
옵션 메뉴 표시	Alt+O
지원 정보 창 표시	Alt+O+M
Horizon Client 정보 창 표시	Alt+O+V
폴더 공유 설정 대화 상자 호출	Alt+O+F
디스플레이 크기 조정 사용 토글	Alt+O+N
다른 데스크톱으로 전환 명령	Alt+O+S
이 데스크톱에 자동 연결 명령	Alt+O+A
상대 마우스 활성화 명령	Alt+O+E
Ctrl+Alt+Del 보내기 명령	Alt+O+C
연결 해제 명령	Alt+O+D
연결 해제 및 로그오프 명령	Alt+O+L
USB 디바이스 연결 명령	Alt+U

Horizon Client 문제 해결

6

데스크톱을 다시 시작 또는 재설정하거나 VMware Horizon Client 애플리케이션을 다시 설치하여 Horizon Client와 관련된 대부분의 문제를 해결할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

키보드 입력 문제

원격 데스크톱 또는 애플리케이션에서 입력할 때 키 입력이 전혀 작동하지 않는 경우 로컬 클라이언트 시스템의 보안 소프트웨어 문제일 수 있습니다.

문제점

원격 데스크톱 또는 애플리케이션에 연결되었을 때 입력해도 문자가 표시되지 않습니다. 키 하나가 계속 반복되는 증상이 나타날 수도 있습니다.

원인

Norton 360 Total Security와 같은 일부 보안 소프트웨어에는 keylogger 프로그램을 감지하고 키 입력 로그를 차단하는 기능이 포함되어 있습니다. 이 보안 기능은 원래 암호 및 신용 카드 번호 도용과 같이 원치 않는 스파이웨어로부터 시스템을 보호하는 것이 목적입니다. 하지만 이 보안 소프트웨어 때문에 Horizon Client에서 키 입력을 원격 데스크톱이나 애플리케이션으로 보내지 못할 수 있습니다.

해결 방법

- 클라이언트 시스템에서 바이러스 백신 또는 보안 소프트웨어의 keylogger 감지 기능을 끄십시오.

Workspace ONE 모드에서 서버에 연결

Horizon Client를 통해 직접 서버에 연결할 수 없거나 데스크톱 및 애플리케이션 사용 권한이 Horizon Client에 표시되지 않는 경우 Workspace ONE 모드를 서버에서 사용하도록 설정할 수 있습니다.

문제점

- Horizon Client를 통해 직접 서버에 연결을 시도하는 경우 Horizon Client에서 Workspace ONE 포털로 리디렉션됩니다.
- URI 또는 바로 가기를 통해 데스크톱 또는 애플리케이션을 열거나 파일 연결을 통해 로컬 파일을 열 경우 요청이 인증을 위해 사용자를 Workspace ONE 포털로 리디렉션합니다.
- Workspace ONE을 통해 데스크톱 또는 애플리케이션을 열고 Horizon Client가 시작된 후 Horizon Client에서 사용 권한이 있는 다른 원격 데스크톱 또는 애플리케이션을 확인하거나 열 수 없습니다.

원인

Horizon 7 버전 7.2부터 관리자는 연결 서버 인스턴스에서 Workspace ONE 모드를 사용하도록 설정할 수 있습니다. 이 동작은 Workspace ONE 모드가 연결 서버 인스턴스에서 사용되도록 설정된 경우에 나타나는 정상적인 것입니다.

해결 방법

Workspace ONE을 사용하여 Workspace ONE 사용 서버에 연결하고 원격 데스크톱 및 애플리케이션에 액세스합니다.

Horizon Client 가 예기치 않게 종료될 경우 해야 할 일

사용자가 닫지 않아도 Horizon Client가 종료될 수 있습니다.

문제점

Horizon Client가 예기치 않게 종료될 수 있습니다. 연결 서버 구성에 따라 View 연결 서버에 대한 보안 연결이 없습니다와 같은 메시지가 나타날 수 있습니다. 일부의 경우 아무런 메시지도 표시되지 않습니다.

원인

이 문제는 연결 서버와의 연결이 끊어졌을 때 발생합니다.

해결 방법

- Horizon Client를 다시 시작합니다. 연결 서버가 다시 실행되는 즉시 올바로 연결할 수 있습니다. 연결 문제가 계속 발생할 경우 Horizon 관리자에게 문의하십시오.

원격 데스크톱 다시 시작

데스크톱 운영 체제가 응답을 멈추면 원격 데스크톱을 다시 시작해야 합니다. 원격 데스크톱을 다시 시작하는 것은 Windows 운영 체제 다시 시작 명령을 사용하는 것과 같습니다. 다시 시작되기 전에 저장하지 않은 데이터를 저장하라는 메시지가 일반적으로 데스크톱 운영 체제에 표시됩니다.

Horizon 관리자가 데스크톱의 데스크톱 다시 시작 기능을 사용하도록 설정한 경우에만 원격 데스크톱을 다시 시작할 수 있습니다.

데스크톱 다시 시작 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 또는 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

프로시저

- **데스크톱 다시 시작** 명령을 사용하십시오.

옵션	조치
데스크톱 OS 내에서	메뉴 표시줄에서 **옵션 > 데스크톱 다시 시작**을 선택합니다.
데스크톱 선택 창에서	데스크톱 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **데스크톱 다시 시작**을 선택합니다.

  다시 시작 작업을 확인하라는 메시지가 Horizon Client에 표시됩니다.

원격 데스크톱의 운영 체제가 재부팅되고 Horizon Client 연결이 끊어진 후 데스크톱에서 로그오프됩니다.

후속 작업

원격 데스크톱에 재연결을 시도하기 전에 시스템 시동을 위해 적절한 시간 동안 기다려 주십시오.

원격 데스크톱을 다시 시작해도 문제가 해결되지 않으면 원격 데스크톱을 재설정해야 할 수 있습니다. 원격 데스크톱 또는 원격 애플리케이션 재설정을 참조하십시오.

원격 데스크톱 또는 원격 애플리케이션 재설정

데스크톱 운영 체제가 응답하지 않고 원격 데스크톱을 다시 시작해도 문제가 해결되지 않으면 원격 데스크톱을 재설정해야 할 수 있습니다. 원격 애플리케이션을 재설정하면 열려 있는 모든 애플리케이션이 종료됩니다.

원격 데스크톱 재설정은 물리적 PC의 재설정 버튼을 눌러 PC를 강제로 다시 시작하는 것과 동일합니다. 원격 데스크톱에서 열려 있는 모든 파일은 저장되지 않고 닫힙니다.

원격 애플리케이션 재설정은 저장되지 않은 데이터를 저장하지 않고 모든 애플리케이션을 종료하는 것과 동일합니다. 다른 RDS 서버 팜의 애플리케이션을 비롯하여 열려 있는 모든 원격 애플리케이션이 닫힙니다.

Horizon 관리자가 데스크톱의 데스크톱 재설정 기능을 사용하도록 설정한 경우에만 원격 데스크톱을 재설정할 수 있습니다.

데스크톱 재설정 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 또는 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

프로시저

1 원격 데스크톱을 재설정하려면 **데스크톱 재설정** 명령을 사용하십시오.

옵션	조치
데스크톱 OS 내에서	메뉴 표시줄에서 **옵션 > 데스크톱 재설정**을 선택합니다.
데스크톱 및 애플리케이션 선택 창에서	데스크톱 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **데스크톱 재설정**을 선택합니다.

2 원격 애플리케이션을 재설정하려면 데스크톱 및 애플리케이션 선택 창에서 **재설정** 버튼을 사용합니다.

   a 메뉴 표시줄에서 **설정** 버튼(톱니 아이콘)을 클릭합니다.

   b 왼쪽 창에서 **애플리케이션**을 선택하고, 오른쪽 창에서 **재설정** 버튼을 클릭한 후 **확인**을 클릭합니다.

원격 데스크톱을 재설정하면 원격 데스크톱의 운영 체제가 재부팅되고 Horizon Client 연결이 끊어진 후 데스크톱에서 로그오프됩니다. 원격 애플리케이션을 재설정하면 애플리케이션이 종료됩니다.

후속 작업

원격 데스크톱 또는 애플리케이션에 재연결을 시도하기 전에 시스템 시동을 위해 적절한 시간 동안 기다려 주십시오.

Windows용 Horizon Client 복구

경우에 따라 Horizon Client 애플리케이션을 복구하면 Horizon Client 관련 문제를 해결할 수 있습니다.

필수 조건

클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.

프로시저

- Horizon Client를 대화형으로 복구하려면 Horizon Client 설치 관리자를 두 번 클릭하거나 명령줄에서 /repair 설치 명령을 사용하여 Horizon Client 설치 관리자를 실행하고 **복구**를 클릭합니다.
- Horizon Client를 자동으로 복구하려면 명령줄에서 /silent 및 /repair 설치 명령을 사용하여 Horizon Client 설치 관리자를 실행합니다.

  예: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe /silent /repair

Windows용 Horizon Client 제거

Horizon Client를 복구해도 문제가 해결되지 않으면 Horizon Client를 제거했다가 다시 설치해야 할 수 있습니다.

다음 절차에서는 Horizon Client 설치 관리자가 있는 경우 Horizon Client를 제거하는 방법을 보여 줍니다. Horizon Client 설치 관리자가 없는 경우 Windows 시스템에서 다른 애플리케이션을 제거하는 경우와 같은 방식으로 Horizon Client를 제거할 수 있습니다. 예를 들어 Windows 운영 체제의 [프로그램 추가/제거] 기능을 사용하여 Horizon Client를 제거할 수 있습니다.

필수 조건

클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.

프로시저

- Horizon Client를 대화형으로 제거하려면 Horizon Client 설치 관리자를 두 번 클릭하거나 명령줄에서 /uninstall 설치 명령을 사용하여 Horizon Client 설치 관리자를 실행하고 **제거**를 클릭합니다.
- Horizon Client를 자동으로 제거하려면 명령줄에서 /silent 및 /uninstall 설치 명령을 사용하여 Horizon Client 설치 관리자를 실행합니다.

  예: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe /silent /uninstall

후속 작업

Horizon Client를 다시 설치합니다. 2장Windows용 Horizon Client 설치를 참조하십시오.