

Windows 10 UWP용 VMware Horizon Client 사용

VMware Horizon Client for Windows 10 UWP 4.5

이 문서는 새 버전으로 교체되기 전까지 나열된 각 제품 버전 및 모든 이후 버전을 지원합니다. 이 문서에 대한 최신 버전을 확인하려면 <http://www.vmware.com/kr/support/pubs>를 참조하십시오.

KO-002509-00

vmware[®]

VMware 웹 사이트 (<http://www.vmware.com/kr/support/>) 에서 최신 기술 문서를 확인할 수 있습니다.
또한 VMware 웹 사이트에서 최신 제품 업데이트를 제공합니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

Copyright © 2016,2017 VMware, Inc. 판권 소유. 저작권 및 상표 정보.

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

목차

| | | |
|----------|--|----|
| 1 | Windows 10 UWP용 VMware Horizon Client 사용 | 5 |
| 2 | 설정 및 설치 | 7 |
| | 시스템 요구 사항 | 7 |
| | Windows Hello 인증 요구 사항 | 8 |
| | Horizon Client 용 연결 서버 준비 | 8 |
| | 지원되는 데스크톱 운영 체제 | 9 |
| | Windows 10 UWP용 Horizon Client 설치 또는 업그레이드 | 9 |
| | 최근 서버에 대한 정보를 Horizon Client 홈 창에 저장 | 9 |
| | 고급 TLS/SSL 옵션 구성 | 9 |
| | VMware Blast 옵션 구성 | 10 |
| | Horizon Client 도움말 표시 | 11 |
| 3 | 원격 데스크톱 및 애플리케이션 연결 관리 | 13 |
| | Horizon Client 의 인증서 검사 모드 설정 | 13 |
| | 디스플레이 프로토콜 선택 | 14 |
| | 원격 데스크톱 또는 애플리케이션에 연결 | 14 |
| | Horizon Client 에서 Windows Hello 사용 안 함 | 16 |
| | 원격 데스크톱 또는 애플리케이션을 시작 화면에 고정 | 16 |
| | 원격 데스크톱 또는 애플리케이션 연결 해제 | 16 |
| | 원격 데스크톱에서 로그오프 | 17 |
| 4 | 원격 데스크톱 또는 애플리케이션 사용 | 19 |
| | 기능 지원 표 | 19 |
| | 전체 화면 모드 사용 | 21 |
| | 원격 데스크톱 및 애플리케이션의 화면 해상도 조정 | 21 |
| | 로컬 확대/축소 기능 사용 | 21 |
| | 화면 잠금 방지 | 22 |
| | 사이드바 사용 | 22 |
| | 제스처 및 탐색 보조 기능 | 22 |
| | 멀티태스킹 | 23 |
| | Microsoft Display Dock과 함께 Horizon Client 사용 | 23 |
| | 텍스트와 이미지 복사 및 붙여넣기 | 23 |
| | 원격 애플리케이션에서 문서 저장 | 24 |
| | 국제화 | 24 |
| 5 | Horizon Client 문제 해결 | 25 |
| | Horizon Client 응답 중지 또는 원격 데스크톱 작동 중지 | 25 |
| | 원격 데스크톱 또는 애플리케이션 재설정 | 26 |
| | VMware Horizon Client 애플리케이션 제거 | 26 |
| | Workspace ONE 모드에서 서버에 연결 | 26 |

로그를 수집하여 기술 지원에 보내기 27

색인 29

Windows 10 UWP용 VMware Horizon Client 사용

1

Windows 10 UWP용 VMware Horizon Client 사용은 Windows 10 디바이스에서 데이터 센터의 원격 데스크톱이나 애플리케이션에 연결하기 위한 VMware Horizon[®] Client[™] 소프트웨어 설치 및 사용에 관한 정보를 제공합니다.

이 정보는 Windows 10 클라이언트 디바이스가 포함된 Horizon 배포를 설정해야 하는 관리자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터센터 운영에 익숙하고 경험 많은 시스템 관리자를 대상으로 작성되었습니다.

설정 및 설치

Windows 10 UWP 클라이언트용 Horizon 배포를 설정하려면 특정 연결 서버 설정을 사용해야 하고, Horizon Server 및 Windows 10 디바이스 클라이언트의 시스템 요구 사항을 충족해야 하며, VMware Horizon Client Windows 애플리케이션을 설치해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [“시스템 요구 사항,”](#) (7 페이지)
- [“Windows Hello 인증 요구 사항,”](#) (8 페이지)
- [“Horizon Client용 연결 서버 준비,”](#) (8 페이지)
- [“지원되는 데스크톱 운영 체제,”](#) (9 페이지)
- [“Windows 10 UWP용 Horizon Client 설치 또는 업그레이드,”](#) (9 페이지)
- [“최근 서버에 대한 정보를 Horizon Client 홈 창에 저장,”](#) (9 페이지)
- [“고급 TLS/SSL 옵션 구성,”](#) (9 페이지)
- [“VMware Blast 옵션 구성,”](#) (10 페이지)
- [“Horizon Client 도움말 표시,”](#) (11 페이지)

시스템 요구 사항

Horizon Client를 설치하는 디바이스 및 이에 사용되는 주변 기기는 특정 시스템 요구 사항을 만족해야 합니다.

운영 체제

- Windows 10 현재 분기(CB) 버전 1703(작성자 업데이트)
- Windows 10 현재 분기(CB) 버전 1607(1주년 업데이트)
- Windows 10 비즈니스용 현재 분기(CBB) 버전 1607(1주년 업데이트)
- Windows 10 장기 서비스 분기(LTSB) 버전 1607(1주년 업데이트)

Windows Hello 인증

[“Windows Hello 인증 요구 사항,”](#) (8 페이지)를 참조하십시오.

연결 서버, 보안 서버 및 Horizon Agent

View 6.x 이상 릴리스의 최신 유지 보수 릴리스

VMware는 디바이스에 VPN 연결이 필요하지 않도록 보안 서버 또는 Unified Access Gateway 장치 사용을 권장합니다.

원격 데스크톱 및 애플리케이션에 대한 디스플레이 프로토콜

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

Windows Hello 인증 요구 사항

Windows Hello를 사용하여 Horizon Client에서 인증을 받으려면 특정 요구 사항을 충족해야 합니다.

Windows 10 디바이스 모델

Windows Hello를 지원하는 모든 Windows 10 디바이스(예: Microsoft Surface Pro 4)

운영 체제 요구 사항**설정 > 계정 > 로그인 옵션**에서 Windows Hello를 설정합니다.**연결 서버 요구 사항**

- Horizon 6 버전 6.2 이후 릴리스
- 연결 서버에서 생체 인식을 사용 설정합니다. 자세한 정보는 View 관리 문서에서 "생체 인식 인증"을 참조하십시오.

Horizon Client 요구 사항

서버 로그인 대화 상자에서 **Windows Hello를 사용하도록 설정**을 눌러 Windows Hello를 사용하도록 설정합니다. 로그인 성공 후 Active Directory 자격 증명이 Windows 10 디바이스에 안전하게 저장됩니다. 처음 로그인하면 **Windows Hello를 사용하도록 설정**이 표시되지만 Windows Hello 인증 사용 설정 후에는 표시되지 않습니다.

Windows Hello 인증을 RSA SecurID 및 RADIUS 인증과 함께 2단계 인증의 일부로 사용할 수 있습니다.

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 있도록 하려면 다음과 같이 특정 풀 설정 및 보안 설정을 구성해야 합니다.

- Unified Access Gateway를 사용하려는 경우 Unified Access Gateway에서 작동하도록 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.
- 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.
- 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.
- Windows Hello 인증을 사용하려면 연결 서버에서 생체 인식 인증을 사용하도록 설정해야 합니다. 생체 인식 인증은 Horizon 6 버전 6.2 이상에서 지원됩니다. 자세한 내용은 View 관리 문서를 참조하십시오.

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 목록을 보려면 View 설치 문서의 "Horizon Agent에 대해 지원되는 운영 체제"를 참조하십시오.

Windows 10 UWP용 Horizon Client 설치 또는 업그레이드

VMware Horizon Client 애플리케이션은 Windows 10 UWP 애플리케이션이며 다른 Windows 10 UWP 애플리케이션과 같은 방식으로 설치할 수 있습니다.

필수 조건

- 클라이언트 디바이스가 Horizon Client 시스템 요구 사항을 충족하는지 확인합니다. "[시스템 요구 사항](#)," (7 페이지)의 내용을 참조하십시오.
- 아직 클라이언트 디바이스를 설정하지 않았다면 설정합니다. 디바이스에 대한 내용은 제조업체의 사용 설명서를 참조하십시오.

프로시저

- 1 디바이스에서 Microsoft Store 애플리케이션을 열고 Microsoft 계정으로 로그인합니다.
- 2 VMware Horizon Client 애플리케이션을 검색합니다.
- 3 **설치** 또는 **무료** 아이콘을 눌러 VMware Horizon Client 애플리케이션을 디바이스에 설치합니다.

최근 서버에 대한 정보를 Horizon Client 홈 창에 저장

서버에 처음으로 연결한 후 서버 바로 가기를 홈 창에 저장하도록 Horizon Client를 구성할 수 있습니다.

프로시저

- 1 Horizon Client 메뉴 표시줄의 왼쪽 상단에서 **옵션** 메뉴를 누릅니다.
서버에 연결된 경우 데스크톱 및 애플리케이션 선택 창 왼쪽 상단의 **옵션** 메뉴를 누를 수 있습니다. 원격 데스크톱이나 애플리케이션에 연결되어 있을 경우, 데스크톱이나 애플리케이션 창에서 **옵션** 버튼을 누르고 **설정**을 누를 수 있습니다.
- 2 **고급** 섹션을 확장하고 **최근 서버에 대한 정보 저장** 옵션을 **켜기**로 전환합니다.
이 옵션을 **끄기**로 설정하면 Horizon Client는 최근 서버를 홈 창에 저장하지 않습니다.

고급 TLS/SSL 옵션 구성

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

기본적으로 TLSv1.0, TLSv1.1 및 TLSv1.2가 사용됩니다. SSL v2.0 및 3.0은 지원되지 않습니다. 기본 암호 제어 문자열은 "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES"입니다.

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

연결 서버 인스턴스에서 수락하는 보안 프로토콜을 구성하는 방법은 View 보안 문서를 참조하십시오.

프로시저

- 1 Horizon Client 메뉴 표시줄의 왼쪽 맨 위에 있는 **옵션** 메뉴를 누르고 **SSL 옵션** 섹션을 확장합니다.
- 2 보안 프로토콜을 사용하도록 설정하거나 사용하지 않도록 설정하려면 보안 프로토콜 이름 아래의 **켜기** 또는 **끄기** 토글을 누릅니다.

TLSv1.0, TLSv1.1 및 TLSv1.2 프로토콜을 사용하거나 사용하지 않도록 설정할 수 있습니다. 세 가지 프로토콜 모두 기본적으로 사용하도록 설정되어 있습니다.

참고 TLSv1.0 및 TLSv1.2를 사용하려면 TLSv1.1을 사용하도록 설정해야 합니다. TLSv1.0 및 TLSv1.2를 사용하도록 설정한 경우에는 TLSv1.1을 사용하지 않도록 설정할 수 없습니다.

- 3 암호 제어 문자열을 변경하려면 기본 문자열을 바꾸고 **변경**을 누릅니다.
- 4 (선택 사항) 기본 암호 제어 문자열로 돌아가야 하는 경우에는 **기본값**을 누릅니다.

변경 사항은 다음에 서버에 연결할 때 적용됩니다.

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.

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 Horizon Client 메뉴 표시줄의 왼쪽 상단 모서리에 있는 **옵션** 메뉴를 누르고 **VMware Blast** 섹션을 확장합니다.

서버에 연결된 경우 데스크톱 및 애플리케이션 선택 창의 왼쪽 상단 모서리에 있는 **옵션** 메뉴를 누르고 **프로토콜** 섹션을 확장한 후 **VMware Blast**를 선택합니다. 서버에 로그인한 후에는 네트워크 상태 옵션을 변경할 수 없습니다.

2 디코딩 및 네트워크 상태 옵션을 구성합니다.

| 옵션 | 조치 |
|------------------------------------|--|
| H.264 디코딩 허용 | <p>연결 서버에 연결하기 전 또는 후에 Horizon Client에서 H.264 디코딩을 허용하도록 이 옵션을 구성합니다.</p> <p>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.</p> <p>JPG/PNG 디코딩을 사용하려면 이 옵션을 선택 취소합니다.</p> |
| 최상의 환경을 위해 네트워크 상태를 선택하십시오. | <p>연결 서버에 연결하기 전에만 이 옵션을 구성할 수 있습니다. 다음 네트워크 상태 옵션 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>연결 서버 및 보안 서버 인스턴스에 대한 Blast 보안 게이트웨이는 BEAT 네트워킹을 지원하지 않습니다.</p> |

Horizon Client 도움말 표시

Horizon Client 애플리케이션에서 도움말 시스템에 액세스하려면 메뉴 표시줄의 왼쪽 상단에서 **옵션** 메뉴를 누르고 정보 아이콘(!)을 누른 후 **온라인 도움말** 아래의 링크를 누릅니다. 서버에 연결하거나 원격 데스크톱 또는 애플리케이션에 로그인한 후 도움말 시스템을 표시할 수도 있습니다.

도움말 시스템은 제품 정보에 액세스할 수 있도록 웹 브라우저의 기능과 함께 몇 가지 추가 기능을 사용합니다. 따옴표, 와일드카드 및 부울 연산자가 포함된 쿼리를 사용하여 도움말을 검색할 수 있습니다.

원격 데스크톱 및 애플리케이션 연결 관리

3

Horizon Client를 사용하여 서버에 연결하고 원격 데스크톱 및 애플리케이션에 로그인할 수 있습니다. 관리자가 원격 데스크톱의 정책을 구성하는 방식에 따라 최종 사용자가 데스크톱에서 수행할 수 있는 작업의 수가 달라집니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “Horizon Client의 인증서 검사 모드 설정,” (13 페이지)
- “디스플레이 프로토콜 선택,” (14 페이지)
- “원격 데스크톱 또는 애플리케이션에 연결,” (14 페이지)
- “Horizon Client에서 Windows Hello 사용 안 함,” (16 페이지)
- “원격 데스크톱 또는 애플리케이션을 시작 화면에 고정,” (16 페이지)
- “원격 데스크톱 또는 애플리케이션 연결 해제,” (16 페이지)
- “원격 데스크톱에서 로그오프,” (17 페이지)

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.

관리자가 허용한 경우 인증서 검사 모드를 설정할 수 있습니다. Horizon Client 홈 창에서 메뉴 표시줄의 왼쪽 맨 위에 있는 **옵션** 메뉴를 누르고 **인증서 검사 모드** 섹션을 확장합니다. 다음 중에서 선택할 수 있습니다.

- **신뢰할 수 없는 서버에 연결하지 않습니다.** 인증서 검사에 실패할 경우 클라이언트가 서버에 연결할 수 없습니다. 검사 실패 내역이 오류 메시지에 나열됩니다.
- **서버 ID 인증서와 상관없이 연결을 시도합니다.** 이 설정은 인증서 검사가 수행되지 않음을 의미합니다.

Windows 10 UWP 애플리케이션에서 사용하는 인증서 메커니즘이 Windows 데스크톱 애플리케이션보다 제한되어 있으므로 **서버 ID 인증서와 상관없이 연결 시도**로 수준이 설정되어 있더라도 인증서 검사가 실패할 수 있습니다. 예를 들어, 인증서 검사가 다음 이유로 인해 실패할 수 있습니다.

- 루트 CA가 서명한 인증서가 해지되었습니다.
- 중간 CA가 서명한 인증서가 해지되었습니다.
- 인증서는 유효하지만 중간 CA가 해지되었습니다.
- 체인에 있는 인증서에 "중요"로 표시된 알 수 없는 확장자가 포함되어 있습니다.

디스플레이 프로토콜 선택

원격 데스크톱 또는 애플리케이션에 연결할 때 Horizon Client가 사용할 디스플레이 프로토콜을 선택할 수 있습니다.

프로시저

- 1 Horizon Client에서 Horizon Client 메뉴 표시줄 왼쪽 상단의 **옵션** 메뉴를 누릅니다.
서버에 연결된 경우 데스크톱 및 애플리케이션 선택 창 왼쪽 상단의 **옵션** 메뉴를 누를 수 있습니다.
- 2 **프로토콜** 섹션을 확장하고 사용할 디스플레이 프로토콜을 선택합니다.
VMware Blast에는 Horizon Agent 7.0 이상이 필요합니다.
- 3 (선택 사항) **VMware Blast**를 선택한 경우 **H.264 디코딩 허용** 옵션을 **켜기** 또는 **끄기**로 전환하여 H.264 인코딩을 사용하거나 사용하지 않도록 설정합니다.

이 옵션이 **켜기**로 설정되어 있으면 원격 데스크톱 또는 애플리케이션에 대한 Horizon Agent가 H.264 인코딩을 지원하는 경우 Horizon Client에서 H.264 인코딩을 허용합니다. 원격 데스크톱 또는 애플리케이션에 대한 Horizon Agent가 H.264 인코딩을 지원하지 않는 경우 Horizon Client는 JPEG/PNG 인코딩을 대신 사용합니다. 이 옵션이 **끄기**(기본 설정)로 설정된 경우 H.264 인코딩이 허용되지 않고 Horizon Client는 항상 JPEG/PNG 인코딩을 사용합니다.

다음에 원격 데스크톱 또는 애플리케이션에 연결할 때 Horizon Client는 사용자가 선택한 디스플레이 프로토콜을 사용합니다. 현재 연결된 세션에 대한 디스플레이 프로토콜을 변경할 수 없습니다.

선택한 디스플레이 프로토콜을 지원하지 않는 원격 데스크톱이나 애플리케이션에 연결할 경우 Horizon Client는 오류 메시지를 표시합니다.

원격 데스크톱 또는 애플리케이션에 연결

원격 데스크톱 또는 애플리케이션에 연결하려면 서버 이름과 사용자 계정의 자격 증명을 제공해야 합니다.

원격 애플리케이션을 사용하려면 연결 서버 6.0 이상에 연결해야 합니다.

참고 최종 사용자가 원격 데스크톱에 액세스할 수 있도록 하려면 우선 클라이언트 디바이스에서 원격 데스크톱으로 로그인할 수 있는지 테스트하십시오.

필수 조건

- Active Directory 사용자 이름/암호, RSA SecurID 사용자 이름/암호 또는 RADIUS 인증 사용자 이름/암호와 같은 로그인 자격 증명을 얻습니다.
- 로그인을 위한 NETBIOS 도메인 이름을 얻습니다. 예를 들어 mycompany.com보다는 mycompany를 사용할 수 있습니다.
- [“Horizon Client용 연결 서버 준비,”](#) (8 페이지)에 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.

회사에 디바이스에서 사용할 수 있는 원격 데스크톱에 라우팅 가능한 액세스를 제공할 내부 무선 네트워크가 있는 경우, 보안 서버 또는 VPN 연결을 설정하지 않아도 됩니다.

- 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.
- 연결 서버에서 제시한 SSL 인증서에 대한 인증서 검사 모드를 구성합니다. [“Horizon Client의 인증서 검사 모드 설정,”](#) (13 페이지)를 참조하십시오.
- Windows Hello를 사용하여 인증하려는 경우 Windows 10 디바이스에서 Windows Hello가 설정되어 있는지 확인하십시오. 전체 요구 사항을 보려면 [“Windows Hello 인증 요구 사항,”](#) (8 페이지)을 참조하십시오.

프로시저

- 1 VPN 연결이 필요한 경우 VPN을 켭니다.
- 2 **VMware Horizon Client** 애플리케이션을 누릅니다.
- 3 서버에 연결합니다.

| 옵션 | 설명 |
|-----------|---|
| 새 서버에 연결 | 서버 추가를 누르고 서버 이름을 입력한 후 연결 을 누릅니다. |
| 기존 서버에 연결 | 홈 창에서 서버 아이콘을 누릅니다. |

Horizon Client와 서버 간 연결에는 항상 SSL이 사용됩니다. SSL 연결의 기본 포트는 443입니다. 서버가 기본 포트를 사용하도록 구성되지 않은 경우에는 다음 예의 형식을 사용합니다.

view.company.com:1443.

- 4 RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명에 대한 메시지가 표시되는 경우 사용자 이름 및 암호를 입력하고 **로그인**을 누릅니다.

암호에 PIN 및 토큰에서 생성된 번호가 모두 포함될 수 있습니다.
- 5 사용자 이름과 암호를 물어보면 Active Directory 자격 증명을 입력합니다.
 - a 하나 이상의 데스크톱 또는 애플리케이션 풀에 대한 사용 권한이 있는 사용자의 사용자 이름 및 암호를 입력합니다.
 - b 도메인을 선택합니다.

- c (선택 사항) **Windows Hello를 사용하도록 설정** 버튼을 사용할 수 있는 경우 눌러서 Windows Hello 인증을 사용합니다.

Windows Hello를 사용하도록 설정 버튼은 서버에서 생체 인식 인증이 사용되도록 설정되어 있고 이전에 Windows Hello로 인증한 적이 없을 때만 표시됩니다.

- d **로그인**을 누릅니다.

Windows Hello가 사용되도록 설정되어 있고 처음으로 로그인하는 경우 Active Directory 자격 증명은 나중에 사용할 수 있도록 Windows 10 디바이스에서 안전하게 저장됩니다.

- 6 Windows Hello 인증이 요구될 경우 지문, 얼굴, 홍채 또는 PIN을 사용하여 인증합니다.

Windows Hello 인증을 사용하지 않으려면 **취소**를 클릭하여 사용자 이름 및 암호를 입력합니다.

- 7 연결할 데스크톱 또는 애플리케이션을 누릅니다.

원격 데스크톱 또는 애플리케이션이 시작됩니다.

Horizon Client 에서 Windows Hello 사용 안 함

이전에 Windows Hello 인증을 사용하여 로그인한 적이 있는 서버에 대해 Windows Hello를 사용하지 않도록 설정할 수 있습니다.

필수 조건

서버에 대한 바로 가기가 Horizon Client 홈 창에 표시되는지 확인합니다. 서버 바로 가기를 저장하도록 Horizon Client를 구성하려면 “[최근 서버에 대한 정보를 Horizon Client 홈 창에 저장](#),” (9 페이지)을 참조하십시오.

프로시저

- 1 Horizon Client 홈 창에서 서버 바로 가기를 길게 누릅니다.
- 2 컨텍스트 메뉴가 나타나면 **서버 로그아웃**을 누릅니다.

다음번에 서버에 연결할 때 사용자 이름 및 암호를 입력하면 서버 로그인 대화 상자에 **Windows Hello를 사용하도록 설정** 버튼이 나타납니다.

원격 데스크톱 또는 애플리케이션을 시작 화면에 고정

데스크톱 및 애플리케이션 선택 창에서 데스크톱 또는 애플리케이션을 마우스 오른쪽 버튼으로 클릭하거나 컨텍스트 메뉴에서 **시작 화면에 고정**을 선택하여 원격 데스크톱 또는 애플리케이션을 시작 화면에 고정할 수 있습니다.

서버에 로그인되지 않은 상태에서 시작 화면의 원격 데스크톱 또는 애플리케이션을 누르면 Horizon Client에서 원격 데스크톱 또는 애플리케이션을 시작하기 전에 서버에서 인증을 받으라는 메시지가 표시됩니다. 서버에 이미 로그인되어 있으면 원격 데스크톱 또는 애플리케이션이 시작되며 서버에서 인증을 받을 필요가 없습니다.

원격 데스크톱 또는 애플리케이션 연결 해제

애플리케이션이 원격 데스크톱에서 계속 열려 있도록 하려면 로그오프하지 않고 원격 데스크톱과의 연결을 끊으면 됩니다. 또한 원격 애플리케이션과의 연결을 끊으면 원격 애플리케이션이 계속 열려 있는 상태로 유지됩니다.

원격 데스크톱이나 애플리케이션에 로그인되어 있을 경우 데스크톱이나 애플리케이션 창에서 **연결 해제** 버튼을 누르고 **연결 해제**를 누르면 연결을 끊을 수 있습니다.

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

원격 데스크톱에서 로그오프

현재 원격 데스크톱에 연결 및 로그인되어 있는 경우, Windows **시작** 메뉴를 사용하여 로그오프할 수 있습니다.

데스크톱 또는 애플리케이션 창에서 **Ctrl+Alt+Del** 버튼을 누르고 **로그오프**를 눌러서 로그오프할 수도 있습니다.

원격 데스크톱에서 열려 있는 저장되지 않은 파일은 로그오프 진행 중에 닫힙니다. 로그오프하지 않고 원격 데스크톱에서 연결을 끊을 경우, 애플리케이션은 원격 데스크톱에서 계속 열려 있게 됩니다.

원격 데스크톱 또는 애플리케이션 사용

Horizon Client에는 다른 Windows 10 UWP 애플리케이션에 있는 공통 기능과 원격 데스크톱 및 애플리케이션에만 해당되는 기능이 포함됩니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “기능 지원 표,” (19 페이지)
- “전체 화면 모드 사용,” (21 페이지)
- “원격 데스크톱 및 애플리케이션의 화면 해상도 조정,” (21 페이지)
- “로컬 확대/축소 기능 사용,” (21 페이지)
- “화면 잠금 방지,” (22 페이지)
- “사이드바 사용,” (22 페이지)
- “제스처 및 탐색 보조 기능,” (22 페이지)
- “멀티태스킹,” (23 페이지)
- “Microsoft Display Dock과 함께 Horizon Client 사용,” (23 페이지)
- “텍스트와 이미지 복사 및 붙여넣기,” (23 페이지)
- “원격 애플리케이션에서 문서 저장,” (24 페이지)
- “국제화,” (24 페이지)

기능 지원 표

일부 기능은 특정 클라이언트 유형에서만 지원되고 다른 유형에서는 지원되지 않습니다. 예를 들어 USB 액세스는 Windows용 Horizon Client에서 지원되지만 Windows 10 UWP용 Horizon Client에서는 지원되지 않습니다.

표 4-1. Windows 10 UWP Horizon Client용 Windows 데스크톱에서 지원되는 기능

| 기능 | Windows 10 데스크톱 | Windows 8.x 데스크톱 | Windows 7 데스크톱 | Windows Vista 데스크톱 | Windows XP 데스크톱 | Windows Server 2008/2012 R2 및 Windows Server 2016 데스크톱 |
|-------------------|-----------------|------------------|----------------|--------------------|-----------------|--|
| USB 리디렉션 | | | | | | |
| 실시간 오디오-비디오(RTAV) | | | | | | |

표 4-1. Windows 10 UWP Horizon Client용 Windows 데스크톱에서 지원되는 기능 (계속)

| 기능 | Windows 10 데스크톱 | Windows 8.x 데스크톱 | Windows 7 데스크톱 | Windows Vista 데스크톱 | Windows XP 데스크톱 | Windows Server 2008/2012 R2 및 Windows Server 2016 데스크톱 |
|-------------------------|-----------------|------------------|----------------|--------------------|-----------------|--|
| 직렬 포트 리더렉션 | | | | | | |
| VMware Blast 디스플레이 프로토콜 | X | X | X | | | X |
| RDP 디스플레이 프로토콜 | | | | | | |
| PCoIP 디스플레이 프로토콜 | X | X | X | 제한됨 | 제한됨 | X |
| 개인 설정 관리 | | | | | | |
| Wyse MMR | | | | | | |
| Windows Media MMR | | | | | | |
| 위치 기반 인쇄 | X | X | X | 제한됨 | 제한됨 | X |
| 가상 인쇄 | | | | | | |
| 스마트 카드 | | | | | | |
| RSA SecurID 또는 RADIUS | X | X | X | 제한됨 | 제한됨 | X |
| 단일 로그인 | X | X | X | 제한됨 | 제한됨 | X |
| 다중 모니터 | | | | | | |

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. Windows Server 2016 데스크톱에는 Horizon Agent 7.0.2 이상이 필요합니다.

중요 View Agent 6.1 이상 및 Horizon Agent 7.0 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 및 Vista에 대한 확장된 지원 계약과 VMware와 이러한 게스트 운영 체제에 대한 확장된 지원 계약을 보유하고 있는 고객은 연결 서버 6.1이 포함된 View Agent 6.0.2 버전의 Windows XP 및 Vista 데스크톱을 배포할 수 있습니다.

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

RDS 호스트의 게시된 데스크톱에 대한 기능 지원

RDS 호스트는 Windows 원격 데스크톱 서비스와 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.

다음 표에는 지원되는 기능에 대한 행만 포함되어 있습니다. 특정 기능은 가상 시스템 RDS 호스트에서 지원되지만 물리적 시스템 RDS 호스트에서는 지원되지 않습니다.

표 4-2. View Agent 6.0.x 이상 또는 Horizon Agent 7.0 이상이 설치된 RDS 호스트에 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 |
| 단일 로그인 | 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 |
| PCoIP 디스플레이 프로토콜 | X | X | Horizon Agent 7.0.2 이상 |
| 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) |

각 게스트 운영 체제의 지원되는 버전 및 서비스 팩에 대한 자세한 내용은 View 5.x 또는 6.x 설치 설명서의 "View Agent에 대해 지원되는 운영 체제" 항목을 참조하십시오. Horizon 7 설치 설명서에서 "Horizon Agent에 대해 지원되는 운영 체제"를 참조하십시오.

전체 화면 모드 사용

Surface Pro 4 또는 Surface Book에서 원격 데스크톱과 애플리케이션을 전체 화면 모드 또는 창 모드로 표시할 수 있습니다. 기본적으로 전체 화면 모드가 사용되도록 설정되어 있습니다.

전체 화면 모드를 켜거나 끄려면 원격 데스크톱이나 애플리케이션에 로그인한 후 원격 데스크톱 또는 애플리케이션 창에서 **옵션** 버튼을 누르고 **전체 화면**을 누릅니다.

원격 데스크톱 및 애플리케이션의 화면 해상도 조정

화면 해상도가 높은 태블릿에서는 원격 데스크톱 또는 애플리케이션의 아이콘과 텍스트를 읽는 데 약간의 어려움이 있을 수 있습니다. 이 경우 화면 해상도를 낮춰서 가독성을 향상시킬 수 있습니다.

원격 데스크톱이나 애플리케이션에 로그인하기 전에 화면 해상도를 변경하려면 Horizon Client 메뉴 표시줄 왼쪽 상단의 **옵션** 메뉴를 누르고 **해상도 모드** 섹션을 확장한 후 해상도 옵션 중 하나를 선택합니다.

서버에 연결하거나 원격 데스크톱 또는 애플리케이션에 로그인한 후에도 화면 해상도를 변경할 수 있습니다.

로컬 확대/축소 기능 사용

로컬 확대/축소 기능을 사용하도록 설정하면 원격 데스크톱 또는 애플리케이션에서 두 손가락을 모으거나 펼쳐서 확대 및 축소할 수 있습니다.

Windows 8 및 Windows 10 가상 시스템 데스크톱, Windows Server 2012 R2, Windows Server 2016 RDS 데스크톱 및 애플리케이션의 경우 로컬 확대/축소 기능을 사용하도록 설정하지 않으면 두 손가락을 모으거나 펼쳐서 확대 및 축소할 수 없습니다.

프로시저

- 1 원격 데스크톱 또는 애플리케이션에 연결합니다.
- 2 데스크톱 또는 애플리케이션 창에서 **옵션** 버튼을 누른 후 **설정**을 누릅니다.
- 3 **고급** 섹션을 확장하고 **로컬 확대/축소** 옵션을 눌러 **켜기**로 전환합니다.

이 옵션을 **끄기**로 설정하면 원격 데스크톱이나 애플리케이션에서 로컬 확대/축소 기능을 사용할 수 없습니다. 이 옵션은 기본적으로 **켜기**로 설정되어 있습니다.

화면 잠금 방지

Windows 10 디바이스를 일정 시간 동안 사용하지 않으면 전원 절약을 위해 디스플레이가 어두워지고 화면 잠금이 활성화되거나 전원이 꺼집니다. 원격 데스크톱 또는 애플리케이션을 위해 화면 잠금을 방지하는 옵션을 설정할 수 있습니다.

참고 Windows 10 디바이스는 사용자가 보고 듣는 사용자 유휴 시간으로 간주합니다. 화면 잠금이 작동하기까지 필요한 유휴 시간은 디바이스의 사용자 설정에 따라 다릅니다.

프로시저

- 1 원격 데스크톱 또는 애플리케이션에 연결합니다.
- 2 데스크톱 또는 애플리케이션 창에서 **옵션** 버튼을 누른 후 **설정**을 누릅니다.
- 3 **고급** 섹션을 확장하고 **화면 항상 켜짐** 옵션을 **켜기**로 전환합니다.
 옵션을 **끄기**로 설정하면 화면 잠금이 작동할 수 있습니다.

사이드바 사용

원격 데스크톱이나 애플리케이션에 연결한 후 사이드바를 사용하여 다른 데스크톱과 애플리케이션을 열 수 있습니다.

표 4-3. 사이드바 작업

| 조치 | 설명 |
|----------------------|--|
| 사이드바 표시 | 원격 데스크톱 또는 애플리케이션 창에서 옵션 버튼을 누른 후 사이드바 를 누릅니다. |
| 사이드바 숨기기 | 원격 데스크톱 또는 애플리케이션 창 안쪽 아무 곳이나 누릅니다. |
| 원격 데스크톱 또는 애플리케이션 열기 | 사이드바에서 원격 데스크톱 또는 애플리케이션의 이름을 누릅니다. |
| 원격 데스크톱 또는 애플리케이션 검색 | 검색 상자에 원격 데스크톱 또는 애플리케이션의 이름을 입력합니다. 원격 데스크톱이나 애플리케이션을 열려면 검색 결과에서 해당 이름을 누릅니다. |

제스처 및 탐색 보조 기능

VMware는 기존 Windows 사용자 인터페이스 요소를 탐색하는 데 도움이 되는 사용자 상호 작용 보조 기능을 제공하고 있습니다.

클릭

다른 애플리케이션의 경우와 마찬가지로, 사용자 인터페이스 요소 클릭하려면 누르면 됩니다. 외부 마우스를 사용할 수도 있습니다.

오른쪽 클릭

오른쪽 클릭으로 사용할 수 있는 옵션은 다음과 같습니다.

- 외부 마우스를 사용하여 마우스 오른쪽 버튼을 클릭합니다.
- 터치패드의 경우 두 손가락으로 누릅니다.
- 터치 스크린의 경우 오른쪽 마우스 클릭 메뉴가 나타날 때까지 길게 누릅니다.

확대 및 축소

터치 스크린의 경우 두 손가락을 오므리거나 벌려서 확대/축소합니다.

터치 입력을 지원하는 운영 체제에서는 로컬 확대/축소 기능을 사용하도록 설정한 경우에만 터치 스크린 확대/축소가 작동합니다. “로컬 확대/축소 기능 사용,” (21 페이지)의 내용을 참조하십시오.

Windows 8, Windows 8.1, Windows 10, Windows Server 2012 및 Windows Server 2016은 터치 입력을 지원합니다.

스크롤 및 스크롤 막대

수직 스크롤에 대해 다음 옵션이 제공됩니다.

- 외부 마우스를 사용하여 스크롤합니다.
- 터치패드의 경우 엄지 손가락으로 길게 누른 다음 두 손가락으로 아래로 스크롤합니다.
- 터치 스크린의 경우 두 손가락으로 누른 다음 끌어서 스크롤하거나 한 손가락으로 스크롤 막대를 끕니다. 손가락 아래 텍스트가 손가락과 동일한 방향으로 이동합니다.

사운드, 음악 및 비디오

디바이스 사운드가 켜져 있는 경우 원격 데스크톱에서 오디오와 비디오를 재생할 수 있습니다.

Ctrl+Alt+Del

Windows 키 조합 Ctrl+Alt+Del은 원격 데스크톱 및 애플리케이션에서 지원되지 않으므로 원격 데스크톱 또는 애플리케이션 창에 있는 **Ctrl+Alt+Del** 버튼을 대신 누릅니다.

멀티태스킹

원격 데스크톱 또는 애플리케이션 연결을 끊지 않고 Horizon Client와 다른 애플리케이션 간에 전환할 수 있습니다.

Horizon Client 애플리케이션이 다른 애플리케이션과 함께 화면의 일부를 차지할 수 있도록 크기를 조정할 수 있습니다.

세션 시간이 초과되기 전에 세션을 얼마간 휴지 상태로 두면 이 세션을 유지할 것인지 묻는 메시지가 나타납니다. 세션을 유지하려면 화면의 아무 곳이나 누르거나 클릭하거나, 또는 키보드의 키를 누릅니다. 원격 데스크톱 또는 애플리케이션의 연결이 끊길 정도로 시간이 지났을 경우 Horizon Client가 데스크톱 및 애플리케이션 선택 창으로 돌아오고 다시 연결할지 묻는 메시지가 나타납니다.

Microsoft Display Dock과 함께 Horizon Client 사용

VMware Horizon Client 애플리케이션은 Continuum for Windows 10 Mobile과 연동됩니다. Microsoft Display Dock을 사용하여 Windows 10 스마트폰을 외부 디스플레이 및 마우스에 연결할 수 있습니다. 이 기능을 통해 Horizon Client를 마치 데스크톱 PC에서 사용하는 것처럼 사용할 수 있습니다.

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.

일반 텍스트만 복사한 후 붙여넣을 수 있습니다. 이미지 및 RTF(서식 있는 텍스트 형식)는 지원되지 않습니다.

Horizon 관리자는 복사 및 붙여넣기 작업이 클라이언트 시스템에서 원격 데스크톱이나 애플리케이션으로만 허용, 원격 데스크톱이나 애플리케이션에서 클라이언트 시스템으로만 허용, 둘 다 허용 또는 둘 다 허용되지 않도록 이 기능을 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.

클립보드는 복사 및 붙여넣기 작업에 64K의 데이터를 사용할 수 있습니다. 최대 클립보드 크기 이상을 복사하려고 하면 텍스트가 잘립니다.

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

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.

국제화

사용자 인터페이스와 설명서 모두 한국어, 영어, 일본어, 프랑스어, 독일어, 중국어 간체, 중국어 번체 및 스페인어로 제공됩니다. 또한 해당 언어의 문자를 입력할 수 있습니다.

Horizon Client 문제 해결

데스크톱을 재설정하거나 애플리케이션을 다시 설치하여 대부분의 Horizon Client 문제를 해결할 수 있습니다.

로그 수집을 활성화하고 문제 해결을 위해 로그 파일을 VMware로 전송할 수도 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- “Horizon Client 응답 중지 또는 원격 데스크톱 작동 중지,” (25 페이지)
- “원격 데스크톱 또는 애플리케이션 재설정,” (26 페이지)
- “VMware Horizon Client 애플리케이션 제거,” (26 페이지)
- “Workspace ONE 모드에서 서버에 연결,” (26 페이지)
- “로그를 수집하여 기술 지원에 보내기,” (27 페이지)

Horizon Client 응답 중지 또는 원격 데스크톱 작동 중지

창이 멈추면 먼저 원격 데스크톱 운영 체제를 재설정합니다.

문제점

Horizon Client가 작동하지 않거나 반복적으로 예기치 않게 종료되거나 원격 데스크톱이 멈춥니다.

원인

Horizon 서버가 올바르게 구성되어 있고 이를 보호하는 방화벽에 올바른 포트가 열려 있다고 가정할 경우, 나머지 문제는 대개 디바이스의 Horizon Client 또는 원격 데스크톱의 게스트 운영 체제와 관련된 것입니다.

해결 방법

- 원격 데스크톱의 운영 체제가 중지될 경우, 디바이스에서 Horizon Client를 사용하여 데스크톱을 재설정합니다.

이 옵션은 Horizon 관리자가 이 기능을 사용하도록 설정한 경우에만 사용할 수 있습니다.

- 디바이스의 애플리케이션을 제거했다가 다시 설치합니다.
- 서버 연결 시도 시 연결 오류가 발생하면 프록시 설정을 변경해야 할 수 있습니다.

원격 데스크톱 또는 애플리케이션 재설정

현재 원격 데스크톱 또는 애플리케이션에 연결되어 로그인된 경우 데스크톱 또는 애플리케이션 창의 **연결 끊기** 버튼을 누르고 **재설정**을 눌러 원격 데스크톱이나 애플리케이션을 재설정할 수 있습니다.

재설정 명령은 Horizon 관리자가 이를 허용하고 원격 데스크톱 또는 애플리케이션이 해당 작업을 수행할 수 있는 상태인 경우에만 사용할 수 있습니다.

데스크톱 운영 체제 또는 애플리케이션이 응답을 멈추면 원격 데스크톱 또는 애플리케이션을 다시 시작해야 할 수 있습니다.

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

원격 애플리케이션을 재설정하면 모든 원격 애플리케이션이 종료되고 모든 원격 애플리케이션 세션에서 로그오프됩니다. 원격 애플리케이션에서 저장되지 않은 변경 내용은 손실될 수 있습니다.

VMware Horizon Client 애플리케이션 제거

경우에 따라 Windows 10 UWP 디바이스에서 VMware Horizon Client 애플리케이션을 제거했다가 다시 설치하면 Horizon Client 관련 문제를 해결할 수 있습니다.

다른 Windows 10 UWP 애플리케이션과 마찬가지로 Horizon Client를 제거합니다.

프로시저

- 1 디바이스에서 VMware Horizon Client 애플리케이션을 찾습니다.
- 2 **VMware Horizon Client** 타일 또는 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **제거**를 누릅니다.

후속 작업

VMware Horizon Client 애플리케이션을 다시 설치합니다. "[Windows 10 UWP용 Horizon Client 설치 또는 업그레이드](#)," (9 페이지)의 내용을 참조하십시오.

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.

로그를 수집하여 기술 지원에 보내기

로깅을 사용하도록 설정하고 로그 번들을 수집하여 기술 지원에 보낼 수 있습니다.

일부 문제의 경우, 해결을 위해 로그를 수집하여 기술 지원에 보내야 할 수 있습니다. 원격 데스크톱 연결에 보안 터널 세션을 사용하는 경우 로깅은 Horizon Client의 성능에 영향을 줍니다. 로깅이 더 이상 필요하지 않다면 고급 로깅 기능을 해제해야 합니다.

필수 조건

VMware 기술 지원에 문의하여 수집하는 로그 파일을 어디로 보낼지 결정할 수 있습니다.

프로시저

- 1 Horizon Client에서 메뉴 표시줄 왼쪽 상단의 **옵션** 메뉴를 누릅니다.
서버에 연결된 경우 데스크톱 및 애플리케이션 선택 창 왼쪽 상단의 **옵션** 메뉴를 누를 수 있습니다. 원격 데스크톱이나 애플리케이션에 연결되어 있을 경우, 데스크톱이나 애플리케이션 창에서 **옵션** 버튼을 누르고 **설정**을 누를 수 있습니다.
- 2 **로깅** 섹션을 확장하고 **고급 로깅 설정** 옵션을 [켜기]로 설정합니다.
- 3 **지원 정보 수집**을 누르고 디바이스에서 로그 파일을 저장할 위치로 이동하여 디렉토리를 선택한 다음 **폴더 선택**을 누릅니다.
예를 들어 편의상 **데스크톱** 항목을 누르고 로컬 데스크톱에 있는 폴더에 로그를 저장할 수 있습니다.
Horizon Client는 사용자가 지정한 위치에 vmware-view-logs-타임 스탬프라는 폴더를 생성합니다.
- 4 (선택 사항) 기술 지원에 보내기 전에 로그 폴더의 .zip 파일을 생성하려면 마우스 오른쪽 버튼으로 폴더를 클릭하고 **보내기 > 압축(ZIP) 폴더**를 선택합니다.

후속 작업

VMware 기술 지원에 로그를 보냅니다.

색인

H

- Horizon Client
 - 데스크톱 연결 해제 16
 - 로그인 14
 - 문제 해결 25

S

- SSL 옵션 9

V

- VMware Blast 10

W

- Windows 10 UWP용 Horizon Client 5
- Windows Display Dock 23
- Windows Hello 인증 8, 16
- Windows Surface Pro 설정 7
- Workspace ONE 26

ㄱ

- 국제화 24
- 기능 지원 표 19

ㄷ

- 데스크톱 관리 13
- 데스크톱 재설정 26
- 도움말 시스템 11
- 디스플레이 프로토콜 14

ㄹ

- 로그오프 17
- 로그인
 - 데스크톱에 14
 - 서버에 14
- 로깅 27
- 로컬 확대/축소 21

ㅁ

- 멀티태스킹 23
- 문제 해결 25

ㅂ

- 보안 서버 8

ㅅ

- 사이드바 22

- 서버 정보 저장 9
- 설치 9
- 시스템 요구 사항 7
- 시작 화면에 고정 16

ㅇ

- 연결 서버 8
- 운영 체제 9
- 원격 데스크톱 및 애플리케이션 19
- 원격 데스크톱 연결 해제 16
- 원격 애플리케이션에서 문서 저장 24
- 이미지, 복사 23
- 인증서, 문제 무시 13

ㅈ

- 전체 화면 모드 21
- 제거 26
- 제스처 22

ㅊ

- 클라이언트 디바이스를 위한 요구 사항 8

ㅌ

- 텍스트, 복사 23
- 텍스트 및 이미지 복사 23
- 텍스트 및 이미지 붙여넣기 23

ㅎ

- 화면 잠금 22
- 화면 해상도 21

