

# iOS용 VMware Horizon Client 설치 및 설정 가이드

VMware Horizon Client for iOS 2103

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

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

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

Copyright © 2021 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

# 목차

## iOS용 VMware Horizon Client 설치 및 설정 가이드 6

### 1 설정 및 설치 7

#### 시스템 요구 사항 7

##### iOS 클라이언트에 대한 시스템 요구 사항 8

##### 실시간 오디오-비디오에 대한 시스템 요구 사항 9

##### 스마트 카드 인증 요구 사항 9

##### Touch ID 인증 요구 사항 10

##### Face ID 인증 요구 사항 11

##### OPSWAT 통합 요구 사항 12

##### 지원되는 데스크톱 운영 체제 12

#### Horizon Client용 연결 서버 준비 13

#### Horizon Client 설치 15

##### iOS 디바이스에 Horizon Client 설치 또는 업그레이드 15

##### Horizon Client를 iOS 디바이스에 제공하도록 Workspace ONE UEM 구성 15

#### Embedded RSA SecurID 소프트웨어 토큰 사용 19

#### 가상 스마트 카드 생성 20

#### 가상 스마트 카드 관리 21

#### 스마트 카드 미들웨어와 가상 스마트 카드 연결 21

#### OPSWAT를 사용하여 디바이스 ID 공유 구성 23

#### 고급 TLS 옵션 구성 23

#### VMware Blast 옵션 구성 24

#### Horizon Client 기본 보기 구성 25

#### Horizon Client 데이터 공유 구성 25

##### VMware에서 수집하는 Horizon Client 데이터 26

### 2 URI를 사용하여 Horizon Client 구성 28

#### vmware-view URI 생성을 위한 구문 28

#### vmware-view URI의 예 31

### 3 원격 데스크톱 및 게시된 애플리케이션 연결 관리 35

#### Horizon Client에서 인증서 검사 모드 설정 36

#### 원격 데스크톱 또는 게시된 애플리케이션에 연결 36

#### 클라이언트 드라이브 리디렉션을 사용하여 로컬 스토리지 액세스 공유 39

#### 저장된 서버 관리 40

#### 즐겨 찾는 원격 데스크톱 또는 게시된 애플리케이션 선택 41

- 원격 데스크톱 또는 게시된 애플리케이션에서 연결 해제 42
- 원격 데스크톱에서 로그오프 42
- 서버에서 연결 해제 43
- 원격 데스크톱 및 게시된 애플리케이션 바로 가기 관리 43
- Horizon Client에서 3D Touch 사용 43
- Horizon Client에서 Spotlight 검색 사용 44
- Horizon Client에서 Split View 및 Slide Over 사용 45
- Horizon Client에서 iPad 분리식 키보드 사용 45
- 바로 가기 및 URL 끌어오기 45
- Horizon Client 위젯 사용 46

#### 4 Microsoft Windows 데스크톱 또는 게시된 애플리케이션 사용 47

- iOS 클라이언트용 기능 지원 48
- 원격 데스크톱에서 Unity Touch 사이드바 사용 49
- 게시된 애플리케이션에서 Unity Touch 사이드바 사용 50
- 모바일 디바이스에서 Horizon Client 도구 사용 51
- 제스처 54
- 터치 리디렉션을 통해 기본 운영 체제 제스처 사용 55
- 화면 해상도 및 외부 디스플레이 사용 55
- DPI 동기화 사용 57
- 외부 키보드 및 기타 입력 디바이스 58
  - Horizon Client에서 Swiftpoint GT 마우스 사용 60
- 실시간 오디오-비디오 기능 사용 60
  - 실시간 오디오-비디오 기능의 카메라 설정 구성 61
- 좌우를 바꾼 마우스 버튼을 지원하도록 Horizon Client 구성 62
- 텍스트와 이미지 복사 및 붙여넣기 62
  - 로깅 복사 및 붙여넣기 작업 63
- 텍스트 및 이미지 끌어오기 64
- 원격 데스크톱 또는 게시된 애플리케이션에서 인쇄 64
- 게시된 애플리케이션에서 문서 저장 65
- 여러 클라이언트 디바이스에서 게시된 애플리케이션의 다중 세션 사용 65
- 멀티태스킹 66
- 셀룰러 데이터 경고 메시지 표시하지 않음 66
- 화면 활성화 유지 67
- PCoIP 클라이언트 측 이미지 캐시 67

#### 5 문제 해결 68

- 원격 데스크톱 다시 시작 68
- 원격 데스크톱 또는 게시된 애플리케이션 재설정 69
- 로깅 정보를 수집 및 VMware에 전송 70

Horizon Client 로그 수집 활성화	70
수동으로 Horizon Client 로그 파일 검색 및 전송	71
Horizon Client 로그 수집 비활성화	71
VMware에 Horizon Client 충돌 데이터 보고	72
Horizon Client 응답 중지 또는 원격 데스크톱 작동 중지	72
프록시 사용 시 연결 문제	73
Workspace ONE 모드에서 서버에 연결	73

# iOS용 VMware Horizon Client 설치 및 설정 가이드

이 가이드에서는 iOS 디바이스에서 VMware Horizon<sup>®</sup> Client<sup>™</sup> 소프트웨어를 설치, 구성 및 사용하는 방법에 대한 정보를 제공합니다.

이 정보는 iOS 클라이언트 디바이스가 포함된 VMware Horizon 배포를 설정해야 하는 관리자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영을 잘 아는 숙련된 시스템 관리자를 대상으로 작성되었습니다.

최종 사용자인 경우 "iOS용 VMware Horizon Client 사용자 가이드" 문서를 참조하거나 Horizon Client 온라인 도움말을 참조하십시오.

# 설정 및 설치

# 1

iOS 클라이언트를 위해 VMware Horizon 배포를 설정하려면 특정 연결 서버 구성 설정을 사용해야 하고, VMware Horizon Server 및 iOS 클라이언트의 시스템 요구 사항을 충족해야 하며, Horizon Client용 애플리케이션을 설치해야 합니다.

본 장은 다음 항목을 포함합니다.

- 시스템 요구 사항
- Horizon Client용 연결 서버 준비
- Horizon Client 설치
- Embedded RSA SecurID 소프트웨어 토큰 사용
- 가상 스마트 카드 생성
- 가상 스마트 카드 관리
- 스마트 카드 미들웨어와 가상 스마트 카드 연결
- OPSWAT를 사용하여 디바이스 ID 공유 구성
- 고급 TLS 옵션 구성
- VMware Blast 옵션 구성
- Horizon Client 기본 보기 구성
- Horizon Client 데이터 공유 구성

## 시스템 요구 사항

Horizon Client가 실행되는 iOS 디바이스는 특정 하드웨어 및 소프트웨어 요구 사항을 충족해야 합니다.

## iOS 클라이언트에 대한 시스템 요구 사항

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

### 운영 체제

- iOS 12.x
- iOS 13.x
- iOS 14.x
- iPadOS 13.x
- iPadOS 14.x

### (선택 사항) 외부 키보드

iPad 키보드 도크 및 Apple 무선 키보드(Bluetooth).

### 스마트 카드 인증

[스마트 카드 인증 요구 사항](#)의 내용을 참조하십시오.

### Touch ID 인증

[Touch ID 인증 요구 사항](#)의 내용을 참조하십시오.

### Face ID 인증

[Face ID 인증 요구 사항](#)의 내용을 참조하십시오.

### 연결 서버 및 Horizon Agent

Horizon 7 버전 7.5 이상 릴리스의 최신 유지 보수 릴리스.

클라이언트 디바이스가 회사 방화벽 외부에서 연결되는 경우 클라이언트 디바이스에 VPN 연결이 필요하지 않도록 Unified Access Gateway 장치를 사용합니다. 디바이스에서 사용할 수 있는 원격 데스크톱에 라우팅 가능한 액세스를 제공하기 위한 내부 무선 네트워크가 회사에 있는 경우, Unified Access Gateway 또는 VPN 연결을 설정하지 않아도 됩니다.

### 디스플레이 프로토콜

- PCoIP
- VMware Blast

### 네트워크 프로토콜

- IPv4
- IPv6

IPv6 환경에서의 Horizon 사용에 대한 자세한 내용은 "Horizon 설치" 문서를 참조하십시오.

## 실시간 오디오-비디오에 대한 시스템 요구 사항

실시간 오디오-비디오는 표준 오디오 및 비디오 디바이스에서 Skype, WebEx 및 Google Hangout과 같은 표준 회의 애플리케이션과 함께 사용할 수 있습니다. 실시간 오디오-비디오를 지원하려면 Horizon 환경이 특정 소프트웨어 및 하드웨어 요구 사항을 충족해야 합니다.

### 원격 데스크톱 및 게시된 애플리케이션

Horizon Agent 7.5 이상.

### 클라이언트 액세스 디바이스

iOS용 Horizon Client를 실행하는 모든 iOS 디바이스에서 실시간 오디오-비디오가 지원됩니다. 자세한 내용은 [iOS 클라이언트에 대한 시스템 요구 사항](#)의 내용을 참조하십시오.

## 스마트 카드 인증 요구 사항

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

### 파생된 자격 증명 기능 사용

파생된 자격 증명 기능을 사용하려면 Horizon Administrator는 게시된 데스크톱을 호스팅하는 RDS 호스트 또는 가상 데스크톱에 스마트 카드 미들웨어를 설치해야 합니다. 동일한 가상 데스크톱 또는 RDS 호스트에 PIV 카드에 대해 설치된 다른 미들웨어가 없어야 합니다. VMware에서는 Charismathics CSSI/CSTC 5.2.2 및 ActivClient 7.1을 테스트했습니다. Windows Inbox Smart Card Minidriver는 지원되지 않습니다.

클라이언트 디바이스에서 Purebred 애플리케이션을 사용하여 파생된 자격 증명을 생성하고, 클라이언트 디바이스에 자격 증명을 프로비저닝하고, 가상 스마트 카드를 생성하고, 가상 스마트 카드를 원격 데스크톱에 설치된 스마트 카드 미들웨어와 연결해야 합니다. 자세한 내용은 [가상 스마트 카드 생성 및 스마트 카드 미들웨어와 가상 스마트 카드 연결](#) 항목을 참조하십시오.

## Horizon Client에서 사용자 이름 힌트 텍스트 상자를 사용하도록 설정

일부 환경에서 스마트 카드 사용자는 단일 스마트 카드 인증서를 사용하여 여러 사용자 계정을 인증할 수 있습니다. 사용자는 스마트 카드를 사용하여 로그인할 때 **사용자 이름 힌트** 텍스트 상자에 사용자 이름을 입력합니다.

**사용자 이름 힌트** 텍스트 상자가 Horizon Client 로그인 대화상자에 나타나게 하려면 연결 서버에서 스마트 카드 사용자 이름 힌트 기능을 사용하도록 설정합니다. 스마트 카드 사용자 이름 힌트 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.

작업 환경에서 보안 외부 액세스를 위해 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 "VMware Unified Access Gateway 배포 및 구성" 문서를 참조하십시오.

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

## 추가 스마트 카드 인증 요구 사항

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

### 연결 서버 및 보안 서버 호스트

관리자는 신뢰할 수 있는 모든 사용자 인증서에 대해 적용할 수 있는 모든 CA(인증 기관) 인증서 체인을 연결 서버 호스트나 보안 서버 호스트에 있는 서버 truststore 파일에 추가해야 하고, 보안 서버가 사용될 경우에는 보안 서버 호스트에 있는 서버 truststore 파일에 추가해야 합니다. 이러한 인증서 체인은 루트 인증서를 포함하며, 중간 인증 기관이 사용자의 스마트 카드 인증서를 발급하는 경우 중간 인증서도 포함해야 합니다.

스마트 카드 사용을 지원하도록 연결 서버를 구성하는 방법에 대한 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.

### Unified Access Gateway 장치

Unified Access Gateway 장치의 스마트 카드 인증 구성에 대한 자세한 내용은 "VMware Unified Access Gateway 배포 및 구성" 문서를 참조하십시오.

### Active Directory

스마트 카드 인증을 구현하기 위해 관리자가 Active Directory에서 수행해야 하는 작업에 대한 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.

## Touch ID 인증 요구 사항

Horizon Client에서 사용자 인증을 위해 Touch ID를 사용하려면 특정 요구 사항을 충족해야 합니다.

### iPad 및 iPhone 모델

iPad Air 2 및 iPhone 6와 같이 Touch ID를 지원하는 iPad 또는 iPhone 모델

### 운영 체제 요구 사항

- iOS 8 이상
- Touch ID 및 암호 설정에서 하나 이상의 지문을 추가합니다.

### 연결 서버 요구 사항

- Horizon 7 버전 7.5 이상.
- 연결 서버에서 생체 인식을 사용 설정합니다. 자세한 정보는 "Horizon 관리" 문서에서 "생체 인식 인증"을 참조하십시오.

- 연결 서버 인스턴스는 Horizon Client에 유효한 루트 서명 인증서를 제공해야 합니다.

### Horizon Client 요구 사항

- 인증서 검사 모드를 **신뢰할 수 없는 서버에 연결하지 않음** 또는 **신뢰할 수 없는 서버에 연결하기 전에 경고**로 설정해야 합니다. 인증서 검사 모드 설정에 대한 자세한 정보는 [Horizon Client에서 인증서 검사 모드 설정](#)의 내용을 참조하십시오.
- 서버 로그인 창의 **암호** 텍스트 상자에서 Touch ID(지문) 아이콘을 눌러 Touch ID를 사용하도록 설정합니다. 로그인 성공 후 Active Directory 자격 증명이 iOS 디바이스의 키체인에 안전하게 저장됩니다.

Touch ID를 스마트 카드 인증과 함께 사용하고 RSA SecurID 및 RADIUS 인증과 함께 2 요소 인증의 일부로 사용할 수 있습니다. Touch ID를 스마트 카드 인증과 함께 사용할 경우 PIN 입력 후 Horizon Client에서 서버에 연결하고 Touch ID 로그인 창이 나타나지 않습니다.

### Face ID 인증 요구 사항

Horizon Client에서 사용자 인증을 위해 Face ID를 사용하려면 특정 요구 사항을 충족해야 합니다.

#### iPad 및 iPhone 모델

Face ID를 지원하는 iPad 또는 iPhone 모델(예: iPhone X)

#### 운영 체제 요구 사항

- iOS 11 이상
- [Face ID 및 암호] 설정에서 Face ID 스캔을 추가합니다.

#### 연결 서버 요구 사항

- Horizon 7 버전 7.5 이상.
- 연결 서버에서 생체 인식을 사용 설정합니다. 자세한 정보는 "Horizon 관리" 문서에서 "생체 인식 인증"을 참조하십시오.
- 연결 서버 인스턴스는 Horizon Client에 유효한 루트 서명 인증서를 제공해야 합니다.

### Horizon Client 요구 사항

- 인증서 검사 모드를 **신뢰할 수 없는 서버에 연결하지 않음** 또는 **신뢰할 수 없는 서버에 연결하기 전에 경고**로 설정해야 합니다. 인증서 검사 모드 설정에 대한 자세한 정보는 [Horizon Client에서 인증서 검사 모드 설정](#)의 내용을 참조하십시오.
- 서버 로그인 창의 **암호** 텍스트 상자에서 Face ID(얼굴) 아이콘을 눌러 Face ID를 사용하도록 설정합니다. 로그인 성공 후 Active Directory 자격 증명이 iOS 디바이스의 키체인에 안전하게 저장됩니다.

Face ID를 스마트 카드 인증과 함께 사용하고 RSA SecurID 및 RADIUS 인증과 함께 2 요소 인증의 일부로 사용할 수 있습니다. Face ID를 스마트 카드 인증과 함께 사용할 경우 PIN 입력 후 Horizon Client에서 서버에 연결하고 Face ID 로그인 창이 나타나지 않습니다.

## OPSWAT 통합 요구 사항

일부 회사에서는 관리자가 타사 OPSWAT MetaAccess 애플리케이션과 Unified Access Gateway를 통합할 수 있습니다. 일반적으로 회사의 BYOD(Bring-Your-Own-Device) 환경에서 비관리형 디바이스에서 사용되는 이러한 통합을 통해 조직에서는 Horizon Client 디바이스에 대한 디바이스 수락 정책을 정의할 수 있습니다.

예를 들어 관리자는 클라이언트 디바이스가 암호로 보호되도록 하거나 최소 운영 체제 버전이 있어야 하는 디바이스 수락 정책을 정의할 수 있습니다. 디바이스 허용 정책을 준수하는 클라이언트 디바이스는 Unified Access Gateway를 통해 원격 데스크톱 및 게시된 애플리케이션에 액세스할 수 있습니다. Unified Access Gateway는 디바이스 허용 정책을 준수하지 않는 클라이언트 디바이스에서 원격 리소스에 대한 액세스를 거부합니다.

OPSWAT 통합을 사용하려면 다음 요구 사항을 충족해야 합니다.

- 관리자는 Unified Access Gateway에서 끝점 규정 준수 검사 기능을 구성해야 합니다. Unified Access Gateway 3.8 이상이 필요합니다. 자세한 내용은 "VMware Unified Access Gateway 배포 및 구성" 문서를 참조하십시오.
- 클라이언트 디바이스에 OPSWAT 모바일 애플리케이션을 설치해야 합니다. App Store에서 OPSWAT 모바일 애플리케이션을 다운로드할 수 있습니다.

Horizon Client는 클라이언트 디바이스에 고유한 디바이스 ID를 생성합니다. Horizon Client를 시작하고 OPSWAT 모바일 애플리케이션이 설치되면 Horizon Client는 디바이스 ID를 OPSWAT 모바일 애플리케이션과 공유할지 묻는 메시지를 표시합니다. 디바이스 ID를 공유하려면 **공유**를 누릅니다. **다시 묻지 않음**을 누르면 Horizon Client에서는 디바이스 ID를 공유하지 않으며 공유할지 묻는 메시지도 다시 표시하지 않습니다. 이 대화상자를 닫으려면 **취소**를 누릅니다.

**공유**를 누르면 OPSWAT는 클라이언트 디바이스의 보안 상태를 확인하고 규정 준수 보고서를 MetaAccess 서버로 전송합니다. 클라이언트 디바이스가 이미 OPSWAT에 등록된 경우에는 성공적으로 등록됩니다. 디바이스가 OPSWAT에 등록되지 않은 경우 오류 메시지가 표시되고 디바이스가 등록되지 않습니다. Horizon Client로 돌아가려면 **돌아가기**를 누릅니다.

Horizon Client에서 설정을 사용하거나 사용하지 않도록 지정하여 디바이스 ID 공유를 구성할 수 있습니다. 자세한 내용은 [OPSWAT를 사용하여 디바이스 ID 공유 구성](#)의 내용을 참조하십시오.

## 지원되는 데스크톱 운영 체제

Horizon 관리자는 게스트 운영 체제가 있는 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 "Horizon 설치" 문서를 참조하십시오.

일부 Linux 게스트 운영 체제도 지원됩니다. 시스템 요구 사항, Linux 가상 시스템 구성 및 지원되는 기능 목록에 대한 자세한 내용은 "Horizon에서 Linux 데스크톱 설정" 문서를 참조하십시오.

## Horizon Client용 연결 서버 준비

최종 사용자가 서버에 연결하고 원격 데스크톱 또는 게시된 애플리케이션에 액세스할 수 있으려면 Horizon 관리자가 다음과 같이 특정 연결 서버 설정을 구성해야 합니다.

### Unified Access Gateway 및 보안 서버

VMware Horizon 배포에 Unified Access Gateway 장치가 포함된 경우 Unified Access Gateway를 사용하도록 연결 서버를 구성합니다. "VMware Unified Access Gateway 배포 및 구성" 문서를 참조하십시오. Unified Access Gateway 장치는 보안 서버와 동일한 역할을 수행합니다.

VMware Horizon 배포에 보안 서버가 포함된 경우 연결 서버 7.5 및 보안 서버 7.5 이상 릴리스의 최신 유지보수 릴리스를 사용하고 있는지 확인하십시오. 자세한 내용은 사용하는 Horizon 버전에 대한 설치 문서를 참조하십시오.

---

**참고** 보안 서버는 VMware Horizon 2006 이상에서 지원되지 않습니다.

---

### 보안 터널 연결

클라이언트 디바이스에 보안 터널 연결을 사용하고, 보안 연결이 연결 서버 인스턴스 또는 보안 서버의 DNS 호스트 이름으로 구성될 경우, 클라이언트 디바이스에서 DNS 이름을 확인할 수 있는지 확인하십시오.

### 데스크톱 및 애플리케이션 풀

데스크톱 및 애플리케이션 풀을 구성할 때 다음 검사 목록을 사용합니다.

- 데스크톱 또는 애플리케이션 풀이 생성되었으며 사용하려는 사용자 계정이 풀에 대한 액세스 권한을 갖고 있는지 확인하십시오. 자세한 내용은 "Horizon에서 가상 데스크톱 설정" 및 "Horizon에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.
- 데스크톱 또는 애플리케이션 풀이 VMware Blast 디스플레이 프로토콜이나 PCoIP 디스플레이 프로토콜을 사용하도록 설정되어 있는지 확인합니다. 자세한 내용은 "Horizon에서 가상 데스크톱 설정" 및 "Horizon에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.

### 사용자 인증

사용자 인증을 설정할 때는 다음 검사 목록을 사용합니다.

- Horizon Client에서 Touch ID 또는 Face ID 인증을 사용하려면 연결 서버에서 생체 인식 인증을 사용하도록 설정해야 합니다. 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.
- 최종 사용자가 연결 서버 인스턴스에 연결할 때마다 자격 증명을 입력할 필요가 없도록 Horizon Client에 암호를 저장할 수 있게 하려면 연결 서버에서 이 기능에 대한 Horizon LDAP를 구성합니다.

사용자가 암호를 저장할 수 있으려면 Horizon LDAP가 이를 허용하도록 구성되어 있고, Horizon Client 인증서 확인 모드가 **신뢰할 수 없는 서버에 연결하기 전에 경고** 또는 **신뢰할 수 없는 서버에 연결하지 않음**으로 설정되어 있고, Horizon Client에서 연결 서버가 제공하는 서버 인증서를 완전히 확인할 수 있어야 합니다. 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.

- Horizon Client에서 RSA SecurID 또는 RADIUS 인증과 같은 2 요소 인증을 사용하려면 연결 서버 인스턴스에서 2 요소 인증 기능을 사용하도록 설정해야 합니다. Horizon 7 버전 7.11부터는 RADIUS 인증 로그인 페이지에서 레이블을 사용자 지정할 수 있습니다. Horizon 7 버전 7.12부터 원격 세션이 시간 초과된 후에 실행되도록 2 요소 인증을 구성할 수 있습니다. 자세한 내용은 "Horizon 관리" 문서의 2 요소 인증에 대한 항목을 참조하십시오.
- Horizon Client에서 서버 URL을 숨기려면 **클라이언트 사용자 인터페이스에서 서버 정보 숨기기** 전역 설정을 사용하도록 설정합니다. 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.
- Horizon Client에서 **도메인** 드롭다운 메뉴를 숨기려면 **클라이언트 사용자 인터페이스에서 도메인 목록 숨기기** 전역 설정을 사용하도록 설정합니다. Horizon 7 버전 7.8부터 이 설정이 기본적으로 사용하도록 설정됩니다. 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.
- Horizon Client로 도메인 목록을 전송하려면 Horizon Console에서 **도메인 목록 보내기** 전역 설정을 사용하도록 설정합니다. 이 설정은 Horizon 7 버전 7.8 이상에서 사용할 수 있으며 기본적으로 사용하지 않도록 설정됩니다. 이전 Horizon 7 버전은 도메인 목록을 보냅니다. 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.

다음 표에서는 **도메인 목록 보내기** 및 **클라이언트 사용자 인터페이스에서 도메인 목록 숨기기** 전역 설정에 따라 사용자가 서버에 로그인하는 방법이 어떻게 결정되는지를 보여 줍니다.

도메인 목록 보내기 설정	클라이언트 사용자 인터페이스에서 도메인 목록 숨기기 설정	사용자가 로그인하는 방법
사용 안 함(기본값)	사용	<p><b>도메인</b> 드롭다운 메뉴는 숨겨져 있습니다. 사용자는 <b>사용자 이름</b> 텍스트 상자에 다음 값 중 하나를 입력해야 합니다.</p> <ul style="list-style-type: none"> <li>■ 사용자 이름(다중 도메인의 경우 허용되지 않음)</li> <li>■ <b>도메인\사용자 이름</b></li> <li>■ <b>username@domain.com</b></li> </ul>
사용 안 함(기본값)	사용 안 함	<p>클라이언트에서 기본 도메인이 구성된 경우 기본 도메인이 <b>도메인</b> 드롭다운 메뉴에 표시됩니다. 클라이언트가 기본 도메인을 알 수 없는 경우 <b>도메인</b> 드롭다운 메뉴에 <b>*DefaultDomain*</b>이 나타납니다. 사용자는 <b>사용자 이름</b> 텍스트 상자에 다음 값 중 하나를 입력해야 합니다.</p> <ul style="list-style-type: none"> <li>■ 사용자 이름(다중 도메인의 경우 허용되지 않음)</li> <li>■ <b>도메인\사용자 이름</b></li> <li>■ <b>username@domain.com</b></li> </ul>

도메인 목록 보내기 설정	클라이언트 사용자 인터페이스에서 도메인 목록 숨기기 설정	사용자가 로그인하는 방법
사용	사용	<p><b>도메인</b> 드롭다운 메뉴는 숨겨져 있습니다. 사용자는 <b>사용자 이름</b> 텍스트 상자에 다음 값 중 하나를 입력해야 합니다.</p> <ul style="list-style-type: none"> <li>■ 사용자 이름(다중 도메인의 경우 허용되지 않음)</li> <li>■ <b>도메인\사용자 이름</b></li> <li>■ <b>username@domain.com</b></li> </ul>
사용	사용 안 함	<p><b>사용자 이름</b> 텍스트 상자에 사용자 이름을 입력하고 <b>도메인</b> 드롭다운 메뉴에서 도메인을 선택할 수 있습니다. 또는 <b>사용자 이름</b> 텍스트 상자에 다음 값 중 하나를 입력할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>도메인\사용자 이름</b></li> <li>■ <b>username@domain.com</b></li> </ul>

## Horizon Client 설치

다른 iOS 애플리케이션을 설치하는 것과 같은 방식으로 Horizon Client를 설치할 수 있습니다. 최종 사용자에게 Horizon Client를 제공하도록 VMware Workspace ONE UEM을 구성할 수도 있습니다.

### iOS 디바이스에 Horizon Client 설치 또는 업그레이드

Horizon Client는 VMware 다운로드 페이지 또는 App Store에서 설치할 수 있습니다.

사전 요구 사항

- 아직 iOS 디바이스를 설정하지 않았다면 설정하십시오. 자세한 내용은 Apple에서 제공하는 사용자 가이드를 참조하십시오.
- Horizon Client 설치 관리자가 포함된 다운로드 페이지 URL이 있는지 확인합니다. 이 URL은 <http://www.vmware.com/go/viewclients>의 VMware 다운로드 페이지이거나 연결 서버 인스턴스의 URL일 수 있습니다.

절차

- 1 iOS 디바이스, Mac 또는 PC에서 설치 관리자 파일을 다운로드하기 위한 URL을 찾아보거나 App Store에서 Horizon Client 애플리케이션을 검색합니다.
- 2 애플리케이션을 다운로드합니다.
- 3 Mac 또는 PC에 애플리케이션을 다운로드한 경우, iOS 디바이스를 컴퓨터에 연결하고 iTunes의 화면 지침을 따릅니다.
- 4 설치가 성공했는지 확인하려면 iOS 디바이스에 **Horizon** 애플리케이션 아이콘이 나타나는지 확인하십시오.

### Horizon Client를 iOS 디바이스에 제공하도록 Workspace ONE UEM 구성

iOS 디바이스 사용자에게 Horizon Client를 제공하도록 Workspace ONE UEM을 구성할 수 있습니다.

원하는 경우 연결 서버 인스턴스의 기본 목록을 지정할 수 있습니다. 지정하는 연결 서버 인스턴스는 Horizon Client에서 바로 가기로 표시됩니다.

#### 사전 요구 사항

- Workspace ONE UEM을 설치 및 배포합니다. <https://my.workspaceone.com/products/Workspace-ONE-UEM>의 내용을 참조하십시오.
- Workspace ONE UEM Console에 익숙해지십시오. 자세한 내용은 <https://docs.vmware.com/kr/VMware-Workspace-ONE-UEM/index.html>에서 Workspace ONE UEM 제품 설명서를 참조하십시오.

#### 절차

- 1 Workspace ONE UEM Console에 관리자 권한으로 로그인합니다.
- 2 **계정 > 사용자 > 목록 보기**를 선택하고 **사용자 추가**를 클릭한 다음 모바일 디바이스에서 Horizon Client를 실행할 사용자의 계정을 추가합니다.
- 3 **계정 > 사용자 > 사용자 그룹**을 선택하고 **추가**를 클릭한 다음 생성한 사용자 계정에 대한 사용자 그룹을 생성합니다.
- 4 Horizon Client 애플리케이션을 업로드하고 추가합니다.
  - a **애플리케이션 및 책 > 애플리케이션 > 목록 보기**를 선택하고 **공용** 탭에서 **애플리케이션 추가**를 클릭합니다.
  - b App Store에서 Apple iOS용 VMware Horizon Client를 검색한 다음 선택합니다.
  - c **정보** 탭에서 애플리케이션 이름을 입력하고 지원되는 iOS 디바이스 모델을 지정합니다.
  - d **할당** 탭에서 Horizon Client 애플리케이션을 이미 생성한 사용자 그룹에 할당합니다.

e (선택 사항) 하나 이상의 기본 서버를 구성합니다.

다음 옵션 중 하나만 구성할 수 있습니다. 두 옵션을 동시에 구성하는 것은 지원되지 않습니다.

**참고** 이 기능은 iOS 7 이상이 설치된 디바이스에서만 지원됩니다. iOS 6 디바이스에는 기본 연결 서버 목록을 푸시(push)할 수 없습니다.

옵션	설명
<p><b>서버, 사용자 이름 및 도메인 정보 구성</b></p>	<p>배포 탭에서 푸시 모드를 선택하고 <b>애플리케이션 구성 보내기</b> 확인란을 선택한 후 <b>구성 키</b> 텍스트 상자에 <b>broker_list</b>를 입력하고 <b>값 유형</b> 드롭다운 메뉴에서 <b>문자열</b>을 선택한 후 <b>구성 값</b> 텍스트 상자에 기본 서버 목록을 JSON 형식으로 입력합니다.</p> <p><b>서버</b> 속성을 사용하여 서버의 IP 주소 또는 호스트 이름을 지정하고 <b>사용자 이름</b> 및 <b>도메인</b> 속성은 서버에 사용 권한이 부여된 사용자의 이름과 도메인을 지정하며 <b>설명</b> 속성은 서버의 설명을 지정합니다.</p> <p>다음 예에서는 4개의 기본 서버를 지정합니다.</p> <pre data-bbox="678 766 1420 997"> {"settings":{   "server-list":[     {"server":"123.456.1.1","description":"View server 1"},     {"server":"123.456.1.2","description":"View server 2"},     {"server":"123.456.1.3","description":"View server 3"},     {"server":"viewserver4.mydomain.com","description":"View server 4","username":"vmware","domain":"view"}   ]}}                     </pre>
<p><b>서버 정보만 구성</b></p>	<p>배포 탭에서 푸시 모드를 선택하고 <b>애플리케이션 구성 보내기</b> 확인란을 선택한 후 <b>구성 키</b> 텍스트 상자에 <b>servers</b>를 입력하고 <b>값 유형</b> 드롭다운 메뉴에서 <b>문자열</b>을 선택한 후 <b>구성 값</b> 텍스트 상자에 서버의 IP 주소 또는 호스트 이름을 입력합니다. 대소문자를 구분하여 <b>servers</b>를 입력해야 합니다.</p> <p>서버 목록을 지정하려면 여러 IP 주소 또는 호스트 이름을 쉼표로 구분하여 <b>구성 값</b> 텍스트 상자에 입력합니다.</p> <p>다음 예에서는 3개의 기본 서버를 지정합니다.</p> <pre data-bbox="678 1291 1420 1333"> 123.456.1.1, viewserver4.mydomain.com, 123.456.1.2                     </pre>

지정하는 서버는 VMware Horizon Client에서 바로 가기로 표시됩니다.

- f (선택 사항) 카메라 설정을 구성하려면 **구성 키** 텍스트 상자에 **설정**을 입력하고, **값 유형** 드롭다운 메뉴에서 **문자열**을 선택하고, **구성 값** 텍스트 상자에 카메라 설정을 JSON 형식으로 입력합니다.

**camera\_position** 속성을 사용하여 카메라 위치를 지정하고 **video\_quality** 속성을 사용하여 비디오 품질을 지정합니다. 올바른 **camera\_position** 속성은 **전면** 및 **후면**입니다. 올바른 **video\_quality** 속성은 **기본**, **높음**, **중간** 및 **낮음**입니다.

예:

```

{"camera": {
  "camera_position": "rear",
  "video_quality": "medium"
}}
```

- g Horizon Client 애플리케이션을 게시합니다.

**5** 각 iOS 디바이스에 Workspace ONE UEM Agent를 설치하고 설정합니다.

iTunes에서 Workspace ONE UEM Agent를 다운로드할 수 있습니다.

**6** Workspace ONE UEM Console을 사용하여 모바일 디바이스에 Horizon Client 애플리케이션을 설치합니다.

**배포** 탭의 유효 날짜 이전에 Horizon Client 애플리케이션을 설치할 수 없습니다.

**결과**

Workspace ONE UEM에서 Horizon Client 애플리케이션과 연결된 사용자 그룹의 iOS 디바이스에 Horizon Client를 전달합니다.

사용자가 Horizon Client를 시작하면 Horizon Client는 디바이스의 Workspace ONE UEM Agent와 통신합니다. 연결 서버 인스턴스의 기본 목록을 구성한 경우 Workspace ONE UEM이 서버 정보를 디바이스의 Workspace ONE UEM Agent로 푸시하면 이러한 서버에 대한 바로 가기가 Horizon Client에 표시됩니다.

나중에 Workspace ONE UEM Console을 사용하여 서버 목록에 대해 연결 서버 인스턴스를 수정, 삭제 또는 추가하고 해당 변경 내용을 iOS 디바이스로 푸시할 수 있습니다. Workspace ONE UEM에서 iOS 디바이스로 새 서버 목록을 푸시할 경우 Horizon Client는 다음 규칙을 사용합니다.

- 새 서버 목록에 디바이스의 서버 목록에 존재하지 않는 서버가 포함될 경우 Horizon Client는 디바이스의 서버 목록 맨 처음에 서버를 추가합니다.
- 새 서버 목록에 디바이스의 서버 목록에 이미 있는 서버가 포함될 경우 디바이스의 서버 목록에서의 해당 위치는 변경되지 않습니다.
- 새 서버 목록에 디바이스의 서버 목록에 있는 서버가 포함되지 않을 경우 Horizon Client에서는 디바이스의 서버 목록에서 해당 서버를 삭제합니다.

## Embedded RSA SecurID 소프트웨어 토큰 사용

RSA SecurID 소프트웨어 토큰을 생성하여 최종 사용자에게 배포하면 사용자는 PIN과 토큰 코드가 아닌 PIN만 입력하여 인증할 수 있습니다.

### 시스템 요구 사항

CT-KIP(Cryptographic Token Key Initialization Protocol)라고도 하는 동적 시드 프로비저닝 또는 CTF(Compressed Token Format)를 사용하여 사용하기 간편한 RSA 인증 시스템을 설정할 수 있습니다. 이 시스템에서는 최종 사용자에게 보낼 URL을 생성합니다. 토큰을 설치하기 위해 최종 사용자는 이 URL을 클라이언트 디바이스의 Horizon Client에 직접 붙여 넣습니다. 최종 사용자가 Horizon Client를 통해 연결 서버 인스턴스에 연결하면 이 URL을 붙여 넣을 수 있는 대화 상자가 나타납니다.

소프트웨어 토큰이 설치되면 최종 사용자는 PIN을 입력하여 인증합니다. 외부 RSA 토큰의 경우, 최종 사용자는 하드웨어 또는 소프트웨어 인증 토큰이 생성한 토큰 코드와 PIN을 입력해야 합니다.

RSA를 사용할 수 있는 연결 서버 인스턴스에 Horizon Client가 연결되어 있는 경우 최종 사용자가 URL을 복사하고 Horizon Client에 붙여 넣을 수 있도록 다음 URL 접두사가 지원됩니다.

- viewclient-securid://
- com.rsa.securid.iphone://
- com.rsa.securid://

URL을 눌러 토큰을 설치하는 최종 사용자의 경우, viewclient-securid:// 접두사만 지원됩니다.

동적 시드 프로비저닝이나 파일 기반(CTF) 프로비저닝 사용에 대한 자세한 내용은 "iPhone 디바이스용 RSA SecurID 소프트웨어 토큰" 웹 페이지(<http://www.rsa.com/node.aspx?id=3652>) 또는 "Android용 RSA SecurID 소프트웨어 토큰" 웹 페이지(<http://www.rsa.com/node.aspx?id=3832>)를 참조하십시오.

### 최종 사용자 지침

최종 사용자에게 보낼 CTFString URL 또는 CT-KIP URL을 생성할 때 암호나 활성화 코드를 포함하거나 포함하지 않은 채 URL을 생성할 수 있습니다. 다음 정보가 포함된 이메일을 통해 이 URL을 최종 사용자에게 보냅니다.

- 소프트웨어 토큰 설치 대화 상자로 이동 방법
  - 연결 서버 인스턴스에 연결할 때 RSA SecurID 자격 증명을 묻는 Horizon Client 대화 상자에서 **외부 토큰**을 누르도록 최종 사용자에게 안내합니다.
- CTFString URL 또는 CT-KIP URL(일반 텍스트 형식)
  - URL이 서식 지정되어 있으면 최종 사용자가 Horizon Client에서 URL을 사용하려고 하면 오류 메시지가 표시됩니다.
- 활성화 코드(생성한 CT-KIP URL에 활성화 코드가 포함되어 있지 않은 경우)
  - 최종 사용자는 대화 상자의 텍스트 상자에 이 활성화 코드를 입력해야 합니다.

- CT-KIP URL에 활성화 코드가 포함된 경우, 소프트웨어 토큰 설치 대화 상자의 **암호 또는 활성화 코드** 텍스트 상자에 값을 입력할 필요가 없음을 최종 사용자에게 안내합니다.

## 가상 스마트 카드 생성

파생된 자격 증명 기능을 사용하려면 서버에 로그인하고 원격 데스크톱에 연결할 때 사용할 가상 스마트 카드를 생성해야 합니다. 하나의 가상 스마트 카드가 여러 개의 인증서를 보유할 수 있습니다.

### 사전 요구 사항

- 클라이언트 디바이스, 원격 데스크톱, RDS 호스트, 연결 서버 호스트 및 기타 Horizon 구성 요소가 스마트 카드 인증 요구 사항을 충족하는지 확인합니다. [스마트 카드 인증 요구 사항](#)의 내용을 참조하십시오.
- Purebred 애플리케이션을 사용하여 파생된 자격 증명을 생성하고 클라이언트 디바이스에서 자격 증명을 프로비저닝합니다.
- 디바이스에 암호가 있는지 확인합니다. 가상 스마트 카드를 생성하려면 암호가 필요합니다.

### 절차

- 1 Horizon Client 창 하단의 **설정**을 누릅니다.
- 2 **파생된 자격 증명**을 누르고 **새 가상 스마트 카드 생성**을 누릅니다.
- 3 디바이스 인증을 수행합니다.
  - Touch ID 또는 Face ID가 사용되도록 설정된 경우 Touch ID 또는 Face ID로 인증을 받습니다.
  - Touch ID 및 Face ID가 둘 다 사용되지 않도록 설정된 경우 암호로 인증을 받습니다.
- 4 가상 스마트 카드의 PIN을 입력하고 확인합니다.
- 5 **계속**을 누르고 Purebred 키체인에서 파생된 자격 증명을 가져옵니다.
  - a **PIV 인증 인증서**를 누릅니다.
  - b **Purebred 키체인** 위치를 선택합니다.
  - c 가져올 인증서를 선택합니다.
- 6 (선택 사항) PIV 인증 인증서를 가져온 후 디지털 서명 인증서 또는 암호화 인증서를 가져오려면 **디지털 서명 인증서** 또는 **암호화 인증서**를 누르고 지침을 따르십시오.
- 7 가상 스마트 카드를 생성하려면 **완료**를 누릅니다.

파생된 자격 증명이 **설정** 창에 나타납니다. **파생된 자격 증명 사용** 설정을 [켜기]로 전환합니다.
- 8 다른 Horizon 환경에 대해 다른 가상 스마트 카드를 생성하려면 **새 가상 스마트 카드 생성**을 누르고 이러한 단계를 반복합니다.

다음에 수행할 작업

[스마트 카드 미들웨어와 가상 스마트 카드 연결](#))에서 이 항목의 HTML 버전을 사용하십시오.

## 가상 스마트 카드 관리

Horizon Client에서 가상 스마트 카드의 PIN을 재설정할 수 있습니다. 가상 스마트 카드를 삭제할 수도 있습니다. 가상 스마트 카드를 사용하여 원격 데스크톱에 로그인한 후, 원격 데스크톱의 Charismathics 보안 토큰 구성자를 사용하여 인증서 및 키를 보고, 가상 스마트 카드에 대한 사용자 PIN을 관리하고 변경할 수 있습니다.

사전 요구 사항

[가상 스마트 카드 생성](#).

절차

- ◆ 가상 스마트 카드의 PIN을 재설정하려면 다음 단계를 수행합니다.
  - a Horizon Client 창 하단의 **설정**을 누릅니다.
  - b **파생된 자격 증명**을 누릅니다.
  - c 가상 스마트 카드를 누릅니다.
  - d **PIN 재설정**을 누릅니다.
  - e 현재 PIN을 입력하고 새 PIN을 입력 및 확인한 후 **완료**를 누릅니다.
- ◆ 가상 스마트 카드를 제거하려면 다음 단계를 수행합니다.
  - a Horizon Client 창 하단의 **설정**을 누릅니다.
  - b **파생된 자격 증명**을 누릅니다.
  - c 가상 스마트 카드를 터치하고 왼쪽으로 살짝 민 후 **삭제**를 누릅니다.

## 스마트 카드 미들웨어와 가상 스마트 카드 연결

파생된 자격 증명 기능을 사용하려면 가상 스마트 카드를 원격 데스크톱에 설치된 스마트 카드 미들웨어와 연결하는 Active Directory의 GPO(그룹 정책 개체)를 생성해야 합니다. 그런 다음 원격 데스크톱을 포함하는 OU(조직 구성 단위)에 GPO를 적용합니다.

사전 요구 사항

- 파생된 자격 증명을 사용하기 위한 시스템 요구 사항이 충족되었는지 확인합니다. [스마트 카드 인증 요구 사항](#)의 내용을 참조하십시오.
- [가상 스마트 카드 생성](#))에서 이 항목의 HTML 버전을 사용하십시오.
- Active Directory 서버를 호스팅하는 시스템에 관리자 도메인 사용자로 로그인할 수 있는지 확인합니다.
- Active Directory 서버에서 MMC와 그룹 정책 관리 편집기 스냅인을 사용할 수 있는지 확인합니다.

절차

- 1 Active Directory 서버에서 그룹 정책 관리 콘솔(`gpmmc.msc`)을 엽니다.
- 2 **그룹 정책 개체**를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기**를 선택합니다.
- 3 **이름** 텍스트 상자에 그룹 정책 개체의 이름(예: 파생된 자격 증명)을 입력하고 **확인**을 클릭합니다.
- 4 생성한 그룹 정책 개체를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 선택합니다.
- 5 **컴퓨터 구성 > 기본 설정 > Windows 설정**을 확장합니다.
- 6 **레지스트리**를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 수집 항목**을 선택합니다.
- 7 수집 항목 이름을 수집에서 의미 있는 이름으로 변경합니다(예: 미들웨어 이름 Charismathics).
- 8 원격 데스크톱에 설치된 스마트 카드 미들웨어를 가상 스마트 카드와 연결하는 레지스트리 항목을 생성하려면 생성한 수집 항목을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 레지스트리 항목**을 선택합니다.

가상 스마트 카드를 Charismathics 미들웨어와 연결하려면 다음 값을 사용합니다.

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\VMware Remote Smart Card]
- "ATR"=hex:3b,1c,96,56,4d,57,61,72,65,43,61,72,64,23,31
- "Crypto Provider"="Charismathics Smart Security Interface CSP"

가상 스마트 카드를 ActivClient 미들웨어와 연결하려면 다음 값을 사용합니다.

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\VMware Remote Smart Card]
- "80000001"="C:\\Program Files\\HID Global\\ActivClient\\ac.scapi.scmd.dll"
- "ATR"=hex:3b,1c,96,56,4d,57,61,72,65,43,61,72,64,23,31
- "ATRMASK"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff
- "Crypto Provider"="Microsoft Base Smart Card Crypto Provider"
- "Smart Card Key Storage Provider"="Microsoft Smart Card Key Storage Provider"

- 9 그룹 정책 관리 편집기를 열고 원격 데스크톱이 포함된 OU에 새 GPO를 연결합니다.  
가상 데스크톱의 경우 가상 데스크톱을 포함하는 OU에 GPO를 연결합니다. 게시된 데스크톱의 경우 RDS 호스트를 포함하는 OU에 GPO를 연결합니다.
- 10 원격 데스크톱에서 레지스트리 설정을 확인하려면 원격 데스크톱을 다시 시작하거나 원격 데스크톱을 열고 `cmd gpupdate /force(을)`를 실행합니다.

다음에 수행할 작업

서버에 로그인하고 원격 데스크톱에 연결합니다. 프로세스는 물리적 스마트 카드를 사용할 때와 같습니다.

**참고** 가상 스마트 카드를 사용하여 인증을 받을 때 잘못된 PIN을 6회 이상 입력하면 가상 스마트 카드가 제거되므로 새 가상 스마트 카드를 생성해야 합니다.

## OPSWAT를 사용하여 디바이스 ID 공유 구성

클라이언트 디바이스에 OPSWAT 모바일 애플리케이션이 설치된 경우 Horizon Client를 시작할 때 클라이언트 디바이스 ID를 공유할지 묻는 메시지가 표시됩니다. Horizon Client에서 설정을 구성하여 디바이스 ID 공유를 사용하거나 사용하지 않도록 설정할 수도 있습니다.

사전 요구 사항

OPSWAT 통합을 구성합니다. [OPSWAT 통합 요구 사항](#)의 내용을 참조하십시오.

절차

- 1 Horizon Client 창의 아래쪽에 있는 **설정**을 누르고 **OPSWAT와 디바이스 ID 공유**를 누릅니다.
- 2 **OPSWAT와 디바이스 ID 공유** 옵션을 눌러 켜기 또는 끄기로 전환합니다.

이 설정을 끄기로 전환하면 해당 설정이 사용되지 않도록 설정되고 다음번에 Horizon Client를 시작할 때 Horizon Client에서는 디바이스 ID를 공유할지 묻는 메시지가 표시됩니다.

이 설정을 켜기로 전환하면 다음 옵션 중 하나를 선택해야 합니다.

옵션	설명
공유하기	Horizon Client는 디바이스 ID를 OPSWAT와 공유합니다. OPSWAT는 클라이언트 디바이스의 보안 상태를 확인하고 규정 준수 보고서를 MetaAccess 서버로 전송합니다. 클라이언트 디바이스가 이미 OPSWAT에 등록된 경우에는 성공적으로 등록됩니다. 디바이스가 OPSWAT에 등록되지 않은 경우 오류 메시지가 표시되고 디바이스가 등록되지 않습니다. Horizon Client로 돌아가려면 <b>돌아가기</b> 를 누릅니다.
다시 묻지 않음	Horizon Client에서는 디바이스 ID를 OPSWAT와 공유하지 않으며 디바이스 ID를 다시 공유할지 묻는 메시지가 표시되지 않습니다.
취소	다음번에 Horizon Client를 시작할 때 Horizon Client에서는 디바이스 ID를 공유할지 묻는 메시지가 표시됩니다.

## 고급 TLS 옵션 구성

Horizon Client 및 서버, Horizon Client 및 Horizon Agent 사이에서 통신을 암호화하는 데 Horizon이 사용하는 보안 프로토콜과 암호화 알고리즘을 선택할 수 있습니다.

기본적으로 TLS v1.1 및 TLS v1.2가 사용되도록 설정되어 있습니다. SSL v2.0, SSL v3.0 및 TLS v1.0은 지원되지 않습니다. 기본 암호 제어 문자열은 "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES"입니다.

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

연결 서버가 수락할 수 있는 보안 프로토콜을 구성하는 방법에 대한 내용은 "Horizon 보안" 문서를 참조하십시오.

#### 절차

- 1 Horizon Client 창 하단의 **설정**을 누릅니다.
- 2 **고급 SSL 옵션**을 누릅니다.
- 3 **기본 설정으로 재설정** 옵션이 꺼짐으로 설정되어 있는지 확인합니다.
- 4 보안 프로토콜을 사용하도록 설정하거나 사용하지 않도록 설정하려면 보안 프로토콜 이름 옆의 **켜기** 또는 **끄기** 토글을 누릅니다.
- 5 암호 제어 문자열을 변경하려면 기본 문자열을 바꿉니다.
- 6 (선택 사항) 기본 설정으로 되돌리려면 창의 오른쪽 상단 모서리에 있는 **재설정**을 누릅니다.

#### 결과

변경 사항은 다음에 서버에 연결할 때 적용됩니다.

## VMware Blast 옵션 구성

VMware Blast 디스플레이 프로토콜을 사용하는 원격 데스크톱 및 게시된 애플리케이션 세션에 맞게 VMware Blast 옵션을 구성할 수 있습니다.

서버에 연결하기 전 또는 후에 H.264 디코딩을 구성할 수 있습니다. H.264는 비디오 압축을 위한 업계 표준으로, 디지털 비디오를 저장하거나 전송할 때 적은 용량이 사용되는 형식으로 변환하는 프로세스입니다.

서버에 연결한 후에 VMware Blast가 기본 설정 프로토콜인 경우에만 **VMware Blast** 설정이 표시됩니다.

#### 사전 요구 사항

설치된 Horizon Agent 버전에 따라, Horizon 관리자는 에이전트 측 그룹 정책 설정을 사용하여 H.264를 포함하는 VMware Blast 기능을 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서의 "VMware Blast 정책 설정"을 참조하십시오.

#### 절차

- 1 Horizon Client를 시작합니다.
- 2 Horizon Client 창 하단의 **설정**을 누르고 **VMware Blast**를 누릅니다.

서버에 로그인하면 VMware Blast가 기본 설정 프로토콜인 경우에만 **VMware Blast** 설정이 표시됩니다.

**3** Horizon Client에서 H.264 디코딩을 허용하려면 **H.264** 옵션을 눌러 켜기로 전환합니다.

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. 이 옵션을 선택 취소하는 경우 Horizon Client는 JPG/PNG 디코딩을 사용합니다.

**결과**

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

## Horizon Client 기본 보기 구성

Horizon Client를 시작할 때 최근에 사용한 원격 데스크톱 및 게시된 애플리케이션 바로 가거나 서버 바로 가기가 표시될지 여부를 구성할 수 있습니다.

**절차**

- 1 Horizon Client 창 하단의 **설정**을 누릅니다.
- 2 **기본 보기**를 누릅니다.
- 3 기본 보기를 선택하려면 옵션을 누릅니다.

옵션	설명
최근 항목	Horizon Client 시작 시 <b>최근</b> 창이 표시됩니다. <b>최근</b> 창에는 최근 사용한 원격 데스크톱 및 게시된 애플리케이션에 대한 바로 가기가 있습니다. 기본 설정입니다.
서버	Horizon Client 시작 시 <b>서버</b> 창이 표시됩니다. <b>서버</b> 창에는 Horizon Client에 추가한 서버에 대한 바로 가기가 있습니다.

**결과**

선택한 기본 보기가 즉시 적용됩니다.

## Horizon Client 데이터 공유 구성

Horizon 관리자가 VMware CEIP(고객 환경 향상 프로그램)에 참여하기로 한 경우 VMware는 연결 서버를 통해 클라이언트 시스템에서 익명 데이터를 수집하고 수신합니다. 이 클라이언트 데이터를 연결 서버와 공유할지 여부를 구성할 수 있습니다.

CEIP에 가입하도록 Horizon을 구성하는 방법에 대한 자세한 내용은 "Horizon 관리" 문서를 참조하십시오.

데이터 공유는 기본적으로 Horizon Client에서 사용하도록 설정됩니다. 서버에 연결하기 전에 데이터 공유 설정을 구성해야 합니다. 이 설정은 모든 서버에 적용됩니다. 서버에 연결한 후에는 Horizon Client 데이터 공유 설정을 변경할 수 없습니다.

절차

- 1 Horizon Client 창 하단의 **설정**을 누르고 **데이터 공유 허용**을 누릅니다.
- 2 **데이터 공유 허용** 설정을 눌러서 켜기 또는 끄기로 전환합니다.

## VMware에서 수집하는 Horizon Client 데이터

Horizon Administrator가 고객 환경 향상 프로그램에 참여하기로 결정하고 클라이언트 시스템에서 데이터 공유가 사용되도록 설정되면 VMware는 클라이언트 시스템에 대한 데이터를 수집합니다.

VMware는 하드웨어 및 소프트웨어 호환성에 대한 우선 순위를 지정하기 위해 클라이언트 시스템의 데이터를 수집합니다. Horizon 관리자가 고객 환경 향상 프로그램에 참여하기로 결정하면 VMware는 고객 요구 사항에 보다 잘 대응하기 위해 배포에 대한 익명 데이터를 수집합니다. VMware는 조직을 식별할 수 있는 데이터를 수집하지 않습니다. Horizon Client 정보는 먼저 연결 서버 인스턴스로 전송되고 연결 서버, 데스크톱 풀 및 원격 데스크톱에 대한 데이터와 함께 VMware로 전송됩니다.

정보는 연결 서버 인스턴스로 전송되는 과정에서 암호화됩니다. 클라이언트 시스템의 정보는 사용자별 디렉토리에 암호화되지 않은 상태로 기록됩니다. 이 로그에는 개인적으로 식별할 수 있는 정보가 없습니다.

Horizon 관리자는 연결 서버를 설치할 때 또는 설치 후에 Horizon Console에서 옵션을 설정하여 VMware 고객 환경 향상 프로그램에 참여할지 선택할 수 있습니다.

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

설명	이 필드는 익명으로 처리됩니까?
Horizon Client 애플리케이션을 제작한 회사	아니요
제품 이름	아니요
클라이언트 제품 버전	아니요
클라이언트 바이너리 아키텍처	아니요
클라이언트 빌드 이름	아니요
호스트 운영 체제	아니요
호스트 운영 체제 커널	아니요
호스트 운영 체제 아키텍처	아니요
호스트 시스템 모델	아니요
호스트 시스템 CPU	아니요
호스트 시스템 프로세서의 코어 수	아니요
호스트 시스템의 메모리 양(MB)	아니요
연결된 USB 디바이스 수	아니요
최대 동시 USB 디바이스 연결 수	아니요
USB 디바이스 공급업체 ID	아니요
USB 디바이스 제품 ID	아니요

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

설명	이 필드는 익명으로 처리됩니까?
USB 디바이스 제품군	아니요
USB 디바이스 사용 횟수	아니요

# URI를 사용하여 Horizon Client 구성

# 2

URI(Uniform Resource Identifier)를 사용하여 최종 사용자가 Horizon Client를 시작하거나, 서버에 연결하거나, 원격 데스크톱 또는 게시된 애플리케이션을 열기 위해 클릭할 수 있는 웹 페이지 또는 이메일 링크를 생성할 수 있습니다.

다음 정보의 일부 또는 전체를 제공하는 URI를 구성하여 이러한 링크를 생성해야 최종 사용자가 정보를 제공할 필요가 없어집니다.

- 서버 주소
- 서버의 포트 번호
- Active Directory 사용자 이름
- RADIUS 또는 RSA SecurID 사용자 이름(Active Directory 사용자 이름과 다른 경우)
- 도메인 이름
- 원격 데스크톱 또는 게시된 애플리케이션 표시 이름
- 세션 재설정, 로그아웃, 시작 등의 작업

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

URI를 사용하여 Horizon Client를 시작하려면 Horizon Client가 클라이언트 컴퓨터에 이미 설치되어 있어야 합니다.

본 장은 다음 항목을 포함합니다.

- [vmware-view URI 생성을 위한 구문](#)
- [vmware-view URI의 예](#)

## vmware-view URI 생성을 위한 구문

URI 구문에는 `vmware-view` URI 구성표, 원격 데스크톱 또는 게시된 애플리케이션을 지정하는 경로 부분 및 선택적으로 원격 데스크톱 또는 게시된 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-view`뿐입니다. 일부 클라이언트 운영 체제의 일부 버전에서는 구성표 이름의 대/소문자를 구분하므로 `vmware-view`를 입력합니다.

**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 모두. 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

원격 데스크톱 또는 게시된 애플리케이션의 디스플레이 이름입니다. 디스플레이 이름은 데스크톱 풀 또는 애플리케이션 풀이 생성될 때 Horizon Console에서 지정됩니다. 디스플레이 이름에 공백이 있는 경우 **%20** 인코딩 메커니즘을 사용하여 공백을 나타냅니다.

또는 데스크톱이나 애플리케이션 풀 ID를 포함하는 경로 문자열에 해당하는 데스크톱 또는 애플리케이션 ID를 지정할 수 있습니다. 데스크톱 또는 애플리케이션 ID를 찾으려면 연결 서버 호스트에서 ADSI Edit를 열고 `DC=vdi,dc=vmware,dc=int`로 이동한 후 `OU=Applications` 노드를 선택합니다. 모든 데스크톱 및 애플리케이션 풀이 나열됩니다. `distinguishedName` 특성은 ID 값을 지정합니다. ID 값을 URI에 지정하기 전에 인코딩해야 합니다(예: `cn%3Dwin7-32%2C%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

**참고** 둘 이상의 원격 데스크톱 또는 게시된 애플리케이션의 디스플레이 이름은 동일하지만 데스크톱 및 애플리케이션 ID는 고유합니다. 특정 원격 데스크톱 또는 게시된 애플리케이션을 지정하려면 디스플레이 이름 대신 데스크톱 또는 애플리케이션 ID를 사용합니다.

### query-part

사용할 구성 옵션 또는 수행할 원격 데스크톱 또는 게시된 애플리케이션 작업. 쿼리는 대소문자를 구분하지 않습니다. 여러 쿼리를 사용하려면 쿼리 사이에 앰퍼샌드(&)를 사용합니다. 쿼리가 충돌하는 경우 Horizon Client는 목록의 마지막 쿼리를 사용합니다. 다음 구문을 사용하십시오.

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

## 지원되는 쿼리

다음 쿼리는 이 유형의 Horizon Client에 지원됩니다. 여러 유형의 클라이언트(예: 데스크톱 클라이언트 및 모바일 클라이언트)에 대한 URI를 생성하는 경우 각 유형의 클라이언트 시스템에 대한 설치 및 설정 가이드에서 지원되는 쿼리 목록을 참조하십시오.

### 작업

표 2-1. 작업 쿼리와 함께 사용할 수 있는 값

값	설명
browse	지정된 서버에서 호스트된 사용 가능한 원격 데스크톱 및 게시된 애플리케이션 목록을 표시합니다. 이 작업을 사용하면 원격 데스크톱 또는 게시된 애플리케이션을 지정할 필요는 없습니다. <b>browse</b> 작업을 사용하여 원격 데스크톱이나 게시된 애플리케이션을 지정할 경우, 사용 가능한 항목 목록에서 원격 데스크톱 또는 게시된 애플리케이션이 강조 표시됩니다.
start-session	지정된 원격 데스크톱 또는 게시된 애플리케이션을 엽니다. 작업 쿼리가 제공되지 않고 원격 데스크톱 또는 게시된 애플리케이션 이름이 제공되는 경우, <b>start-session</b> 이 기본 작업입니다.
reset	지정된 원격 데스크톱 또는 게시된 애플리케이션을 종료하고 다시 시작합니다. 저장하지 않은 데이터는 손실됩니다. 원격 데스크톱 재설정은 PC에 있는 재설정 버튼을 누르는 것과 같습니다.
restart	지정된 원격 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.
logout	원격 데스크톱의 게스트 운영 체제에서 사용자를 로그아웃시킵니다. 게시된 애플리케이션을 지정하는 경우 작업을 무시하거나 최종 사용자에게 "잘못된 URI 작업"이라는 경고 메시지가 나타납니다.

### args

게시된 애플리케이션이 시작될 때 추가할 명령줄 인수를 지정합니다. 구분 **args=** 값을 사용합니다. 여기서 값은 문자열입니다. 다음 문자에는 % 인코딩을 사용하십시오.

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

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

### appProtocol

게시된 애플리케이션의 경우 올바른 값은 **PCoIP** 및 **BLAST**입니다. 예를 들어 PCoIP를 지정하려면 **appProtocol=PCoIP** 구문을 사용합니다.

### defaultLaunchView

Horizon Client가 시작될 때의 기본 보기를 설정합니다. 올바른 값은 **recent**와 **servers**입니다.

### desktopProtocol

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

### domainName

원격 데스크톱 또는 게시된 애플리케이션에 연결 중인 사용자와 연결된 NETBIOS 도메인 이름을 지정합니다. 예를 들어 **mycompany.com**보다는 **mycompany**를 사용할 수 있습니다.

### 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, Horizon Client에서 Windows 사용자 이름을 사용합니다. 구문은 **tokenUserName=name**입니다.

## vmware-view URI의 예

vmware-view URI 구성표를 사용하면 하이퍼텍스트 링크나 버튼을 만들고 이메일 또는 웹 페이지에 이러한 링크를 포함할 수 있습니다. 예를 들어 최종 사용자는 URI 링크를 클릭하여 지정된 시작 옵션으로 원격 데스크톱을 시작할 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 대화상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인이 성공적으로 수행되면 클라이언트는 디스플레이 이름이 **Primary Desktop**(기본 데스크톱)인 원격 데스크톱에 연결되고 사용자는 게스트 운영 체제에 로그인됩니다.

**참고** 이 예에서는 기본 디스플레이 프로토콜 및 창 크기가 사용됩니다. 기본 디스플레이 프로토콜은 PCoIP이며 기본 창 크기는 전체 화면입니다.

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client가 시작되며 **view.mycompany.com** 서버에 연결됩니다. 로그인 대화상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인에 성공하면 클라이언트는 데스크톱 ID `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int`(인코딩된 값 `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`)인 원격 데스크톱에 연결됩니다.

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

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

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

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

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

Horizon Client가 시작되며 **view.mycompany.com** 서버에 연결됩니다. 로그인 대화상자에 사용자가 이름, 도메인 이름 및 암호를 입력해야 합니다. 로그인이 성공적으로 수행되면 클라이언트는 디스플레이 이름이 **Calculator**(계산기)인 게시된 애플리케이션에 연결 합니다. 이 연결은 VMware Blast 디스플레이 프로토콜을 사용합니다.

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

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

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

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

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

Horizon Client가 시작되며 `view.mycompany.com` 서버에 연결됩니다. 로그인 대화상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인이 성공적으로 수행되면 Horizon Client에서 **Primary Desktop**(기본 데스크톱)에 대한 재설정 작업을 확인하라는 대화상자가 표시됩니다.

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

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

Horizon Client가 시작되며 `view.mycompany.com` 서버에 연결됩니다. 로그인 대화상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인이 성공적으로 수행되면 Horizon Client에서 **Primary Desktop**(기본 데스크톱)에 대한 다시 시작 작업을 확인하라는 대화상자가 표시됩니다.

**참고** Horizon 관리자가 데스크톱에 대해 다시 시작 기능을 사용하도록 설정한 경우에만 이 작업을 사용할 수 있습니다.

10 `vmware-view://`

Horizon Client가 이미 실행되고 있으면 포그라운드로 전환됩니다. Horizon Client가 실행되고 있지 않으면 시작됩니다.

11 `vmware-view:///defaultlaunchview=recent`

Horizon Client가 시작되고 **최근** 창이 표시됩니다.

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

서버 10.10.10.10에서 My Notepad++를 시작하고 게시된 애플리케이션 시작 명령에 인수 `My new file.txt`를 전달합니다. 파일 이름은 공백을 포함하므로 큰따옴표로 묶입니다.

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

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

**참고** 명령줄 인수를 사용하는 방식은 게시된 애플리케이션마다 다를 수 있습니다. 예를 들어 워드패드에 인수 `a.txt b.txt`를 전달하면 워드패드에서 `a.txt` 파일 하나만 열립니다.

## 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>
```

# 원격 데스크톱 및 게시된 애플리케이션 연결 관리

# 3

최종 사용자는 Horizon Client를 사용하여 서버에 연결하고, 연결할 서버 목록을 편집하고, 원격 데스크톱에 로그인하거나 로그오프하고, 게시된 애플리케이션을 사용할 수 있습니다. 문제 해결을 위해 최종 사용자는 원격 데스크톱 및 게시된 애플리케이션을 재설정할 수도 있습니다.

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

본 장은 다음 항목을 포함합니다.

- Horizon Client에서 인증서 검사 모드 설정
- 원격 데스크톱 또는 게시된 애플리케이션에 연결
- 클라이언트 드라이브 리디렉션을 사용하여 로컬 스토리지 액세스 공유
- 저장된 서버 관리
- 즐겨 찾는 원격 데스크톱 또는 게시된 애플리케이션 선택
- 원격 데스크톱 또는 게시된 애플리케이션에서 연결 해제
- 원격 데스크톱에서 로그오프
- 서버에서 연결 해제
- 원격 데스크톱 및 게시된 애플리케이션 바로 가기 관리
- Horizon Client에서 3D Touch 사용
- Horizon Client에서 Spotlight 검색 사용
- Horizon Client에서 Split View 및 Slide Over 사용
- Horizon Client에서 iPad 분리식 키보드 사용
- 바로 가기 및 URL 끌어오기
- Horizon Client 위젯 사용

## Horizon Client에서 인증서 검사 모드 설정

Horizon Client와 서버 간의 연결에 대해 서버 인증서 검사가 수행됩니다. 인증서는 디지털 양식의 확인 방법으로, 여권 또는 운전 면허증과 비슷합니다.

서버 인증서 검사는 다음 확인 작업을 포함합니다.

- 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.

iOS 디바이스에 설치할 수 있는 자체 서명된 루트 인증서를 배포하는 방법에 대한 자세한 내용은 Apple 웹 사이트에서 해당 지침을 참조하십시오. 예를 들어, iPad의 경우 [http://www.apple.com/ipad/business/docs/iPad\\_Certificates.pdf](http://www.apple.com/ipad/business/docs/iPad_Certificates.pdf)의 내용을 참조하십시오.

인증서 검사 모드를 설정하려면 Horizon Client를 시작하고 Horizon Client 창 하단에서 **설정**을 누르고 **인증서 확인 모드**를 누릅니다. 다음 옵션 중 하나를 선택할 수 있습니다.

- **신뢰할 수 없는 서버에 연결하지 않습니다.** 이 설정은 인증서 검사 중 하나라도 실패하는 경우 서버에 연결할 수 없음을 의미합니다. 검사 실패 내역이 오류 메시지에 나열됩니다.
- **신뢰할 수 없는 서버에 연결하기 전에 경고합니다.** 이 설정은 **계속**을 클릭하면 서버가 자체 서명된 인증서를 사용하기 때문에 인증서 검사에 실패할 경우에 발생하는 경고를 무시할 수 있음을 의미합니다. 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.

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.

## 원격 데스크톱 또는 게시된 애플리케이션에 연결

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

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

사전 요구 사항

- **Active Directory** 사용자 이름/암호, **RSA SecurID** 사용자 이름/암호, **RADIUS** 인증 자격 증명 또는 스마트 카드 PIN(개인 ID 번호)과 같이 로그인하기 위한 자격 증명을 얻습니다.
- 로그인을 위한 **NETBIOS** 도메인 이름을 얻습니다. 예를 들어 **mycompany.com** 대신 **mycompany**를 사용할 수 있습니다.
- **Horizon Client용 연결 서버 준비**에 설명된 관리 작업을 수행하십시오.
- 회사 네트워크 외부에 있으며 원격 데스크톱 및 게시된 애플리케이션에 액세스하기 위해 **VPN** 연결이 필요한 경우 클라이언트 디바이스가 **VPN** 연결을 사용하도록 설정되어 있는지 확인하고 해당 연결을 켜십시오.
- 원격 데스크톱 또는 게시된 애플리케이션에 액세스하는 서버의 정규화된 도메인 이름(FQDN)이 있는지 확인합니다. 서버 이름에는 밑줄(\_)을 사용할 수 없습니다. 포트가 **443**이 아닌 경우 포트 번호도 필요합니다.
- 내장형 **RSA SecurID** 소프트웨어를 사용하려면 올바른 **CT-KIP URL** 및 활성 코드가 있어야 합니다. **Embedded RSA SecurID 소프트웨어 토큰 사용**의 내용을 참조하십시오.
- 서버에서 제공한 인증서에 대한 인증서 검사 모드를 구성합니다. **Horizon Client에서 인증서 검사 모드 설정**의 내용을 참조하십시오.
- **Touch ID**를 사용하여 인증하려는 경우 iOS 디바이스의 [**Touch ID 및 인증번호**] 설정에서 하나 이상의 지문을 추가하십시오. **Touch ID** 인증에 대한 전체 요구 사항을 보려면 **Touch ID 인증 요구 사항**의 내용을 참조하십시오.
- **Face ID** 인증을 사용하려는 경우 클라이언트 디바이스에서 [**Face ID**] 옵션이 사용 설정되어 있고 **Face ID** 스캔이 등록되어 있는지 확인하십시오. **Face ID** 인증에 대한 전체 요구 사항을 보려면 **Face ID 인증 요구 사항**의 내용을 참조하십시오.

절차

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

옵션	조치
새 서버에 연결	서버 이름과 설명(선택 사항)을 입력하고 <b>연결</b> 을 누릅니다. 서버가 이미 추가된 경우, 대신 창의 오른쪽 상단 모서리에 있는 <b>새로 만들기</b> 를 누릅니다.
기존 서버에 연결	<b>서버</b> 창에서 서버 바로 가기를 누릅니다.

Horizon Client와 서버 간 연결에는 항상 TLS가 사용됩니다. TLS 연결의 기본 포트는 443입니다. 서버가 기본 포트를 사용하도록 구성되지 않은 경우에는 형식 *servername:port*를 사용합니다(예: **view.company.com:1443**).

- 4 스마트 카드가 필수 또는 선택 사항일 경우, 사용할 스마트 카드 인증서를 선택하고 PIN을 입력합니다. 스마트 카드에 하나의 인증서만 있는 경우 해당 인증서가 이미 선택되어 있습니다. 여러 인증서가 있는 경우 인증서를 스크롤할 수 있습니다.
- 5 RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명에 대해 묻는 메시지가 표시되면 자격 증명을 입력하고, 포함된 RSA SecurID 토큰을 사용하려면 포함된 토큰을 설치합니다.

옵션	조치
기존 토큰 사용	스마트폰에서 하드웨어 인증 토큰이나 소프트웨어 인증 토큰을 사용하는 경우 사용자 이름과 암호를 입력합니다. 암호에 PIN 및 토큰에서 생성된 번호가 모두 포함될 수 있습니다.
소프트웨어 토큰 설치	<ol style="list-style-type: none"> <li>a 외부 토큰을 누릅니다.</li> <li>b 소프트웨어 토큰 설치 대화상자에서, 시스템 관리자가 이메일로 보낸 CT-KIP URL 또는 CTFString URL을 붙여넣습니다. URL에 활성 코드가 포함된 경우 <b>암호 또는 활성 코드</b> 텍스트 상자에 아무 값도 입력할 필요가 없습니다.</li> </ol>

- 6 RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명에 대해 묻는 메시지가 다시 표시되면 토큰에서 다음에 생성된 번호를 입력합니다.

PIN을 입력하거나 이전에 입력한 동일한 생성 번호를 입력하지 마십시오. 필요한 경우 새 번호가 생성될 때까지 기다리십시오.

이 단계는 첫 번째 인증번호를 잘못 입력했거나 RSA 서버의 구성 설정이 변경된 경우에만 필요합니다.

- 7 (선택 사항) Touch ID를 사용하여 인증하려는 경우 **암호** 텍스트 상자 오른쪽에서 Touch ID(지문) 아이콘을 누릅니다.

Touch ID가 사용되지 않도록 설정되면 아이콘이 회색이 됩니다. Touch ID가 사용되도록 설정되면 아이콘이 녹색으로 바뀝니다. Touch ID 인증은 서버에서 생체 인식이 사용 설정되어 있고 이전에 Touch ID로 인증한 적이 없을 때만 사용할 수 있습니다.

- 8 (선택 사항) Face ID를 사용하여 인증하려는 경우 **암호** 텍스트 상자 오른쪽에서 Face ID(얼굴) 아이콘을 누릅니다.

Face ID가 사용되지 않도록 설정되면 아이콘이 회색이 됩니다. Face ID가 사용되도록 설정되면 아이콘이 녹색으로 바뀝니다. Face ID 인증은 서버에서 생체 인식이 사용 설정되어 있고 이전에 Face ID로 인증한 적이 없을 때만 사용할 수 있습니다.

- 9 사용자 이름과 암호를 묻는 메시지가 나타나면 **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.

**도메인** 드롭다운 메뉴가 숨겨져 있으면 사용자 이름을 **username@domain** 또는 **domain\username**으로 입력합니다.
  - c (선택 사항) 시스템 관리자가 이 기능을 사용하도록 설정했고 서버 인증서를 완전히 확인할 수 있는 경우, **이 암호 기억** 옵션을 눌러 켜짐으로 전환합니다.
  - d **로그인**을 누릅니다.

Touch ID 또는 Face ID가 사용 설정되어 있고 처음으로 로그인하는 경우 **Active Directory** 자격 증명은 나중에 사용할 수 있도록 iOS 디바이스의 키체인에 안전하게 저장됩니다.

- 10 Touch ID 인증을 하라는 메시지가 표시되면 손가락을 **홈** 버튼에 올려 놓습니다.
- 11 Face ID 인증을 하라는 메시지가 표시되면 디바이스의 화면을 주시합니다.

처음으로 Horizon Client에서 Face ID를 사용하여 인증하려고 하면 iOS에 Horizon Client에서 Face ID를 사용할 수 있도록 허용하라는 메시지가 표시됩니다. Face ID 인증을 사용하지 않으려면, **허용 안 함**을 눌러 대신 사용자 이름 및 암호를 입력합니다.

- 12 (선택 사항) 사용할 디스플레이 프로토콜을 선택하려면 Horizon Client 창 하단에서 **설정**을 누르고 **기본 설정 프로토콜**을 누릅니다.

**VMware Blast**는 더 나은 배터리 수명을 제공하며 고급 3D 및 모바일 디바이스 사용자를 위한 최적의 프로토콜입니다.

- 13 원격 데스크톱 또는 게시된 애플리케이션을 눌러서 연결합니다.

게시된 데스크톱에 연결하는 경우 해당 데스크톱이 이미 **Microsoft RDP** 디스플레이 프로토콜을 사용하도록 설정되어 있으면 바로 연결되지 않습니다. **PCoIP** 디스플레이 프로토콜 또는 **VMware Blast** 디스플레이 프로토콜로 연결할 수 있도록 원격 운영 체제에서 로그오프할 것인지를 묻는 메시지가 나타납니다.

## 결과

처음으로 원격 데스크톱 또는 게시된 애플리케이션에 연결하면 Horizon Client는 원격 데스크톱 또는 게시된 애플리케이션에 대한 바로 가기를 **최근** 창에 저장합니다. 다음에 원격 데스크톱 또는 게시된 애플리케이션에 연결할 때는 서버 바로 가기를 누르는 대신 이 바로 가기를 누르면 됩니다.

## 클라이언트 드라이브 리디렉션을 사용하여 로컬 스토리지 액세스 공유

Horizon Client에서 로컬 스토리지를 원격 데스크톱이나 게시된 애플리케이션과 공유하도록 구성할 수 있습니다. 이 기능을 클라이언트 드라이브 리디렉션이라 부릅니다.

Windows 원격 데스크톱 또는 게시된 애플리케이션에서 로컬 스토리지는 **Documents (Z:)** 네트워크 폴더에 표시됩니다. 이 네트워크 폴더의 파일을 원격 데스크톱에 복사할 수 있고, 원격 데스크톱의 파일을 이 네트워크 폴더에 복사할 수 있습니다. 원격 데스크톱에서 이 네트워크 폴더의 파일 및 폴더를 편집하고, 삭제하고, 이름을 바꿀 수도 있습니다.

#### 사전 요구 사항

- 클라이언트 드라이브 리디렉션 기능을 사용 설정합니다. 이 작업을 수행하면 에이전트 **클라이언트 드라이브 리디렉션** 옵션이 사용하도록 설정됩니다. 또한 클라이언트 드라이브 리디렉션 동작을 제어하기 위한 설정 정책이나 레지스트리 설정도 포함됩니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.
- iOS 디바이스에 iOS 11 이상이 설치되어 있는지 확인합니다.

#### 절차

- 1 Horizon Client 창 하단에서 **설정**을 눌러서 [설정] 창을 열고 **파일 공유**를 누릅니다.
- 2 클라이언트 드라이브 리디렉션을 사용하도록 설정하려면 [설정] 창에서 **파일 공유**를 누르고 해당 옵션을 켭니다.
- 3 원격 데스크톱 또는 게시된 애플리케이션에 연결합니다.

#### 다음에 수행할 작업

원격 데스크톱 또는 게시된 애플리케이션의 변경 사항을 확인합니다.

- Windows 원격 데스크톱에서 **Documents (Z:)**라는 네트워크 폴더를 엽니다.
- 게시된 애플리케이션에서 **파일 > 열기** 또는 **파일 > 다른 이름으로 저장**을 선택하고(해당될 경우) 네트워크 폴더 **Documents (Z:)**로 이동합니다.

## 저장된 서버 관리

서버에 연결하면 Horizon Client가 **서버** 창에 해당 서버의 바로 가기를 저장합니다. Horizon Client는 이름을 잘못 입력하거나 잘못된 IP 주소를 입력하더라도 서버 바로 가기를 저장합니다. 서버 바로 가기를 편집하고 제거할 수 있습니다.

#### 절차

- 1 창 하단에 있는 **서버**(클라우드 아이콘)를 눌러 저장된 서버를 표시합니다.

2 컨텍스트 메뉴가 나타날 때까지 서버 바로 가기를 길게 터치합니다.

옵션	조치
사용자 이름, 도메인, 서버 이름 또는 설명 변경	a 컨텍스트 메뉴에서 <b>서버 편집</b> 을 누릅니다. b <b>서버 편집</b> 창에서 내용을 변경합니다. c <b>업데이트</b> 를 눌러서 변경 사항을 저장합니다.
서버 바로 가기 제거	컨텍스트 메뉴에서 <b>서버 삭제</b> 를 누릅니다. 서버 바로 가기를 제거하는 경우 서버와 연결된 원격 데스크톱 및 게시된 애플리케이션 바로 가기도 삭제됩니다.
저장된 암호 잊기	컨텍스트 메뉴에서 <b>암호를 잊음</b> 을 누릅니다. 이 옵션은 이전에 저장된 암호가 있을 경우에만 사용할 수 있습니다.
Touch ID 비활성화	<b>로그아웃</b> 을 누릅니다. 이 옵션은 이전에 Touch ID를 사용 설정한 경우에만 사용할 수 있습니다.
Face ID 사용 안 함	<b>로그아웃</b> 을 누릅니다. 이 옵션은 이전에 Face ID를 사용 설정한 경우에만 사용할 수 있습니다.

## 즐거 찾는 원격 데스크톱 또는 게시된 애플리케이션 선택

즐거 찾는 원격 데스크톱 및 게시된 애플리케이션을 선택할 수 있습니다. 즐겨찾기 항목에 대한 바로 가기는 별 모양으로 식별되며 **즐거찾기** 탭에 표시됩니다. 서버에서 로그오프한 후에도 즐겨찾기 항목은 저장됩니다.

사전 요구 사항

서버에 연결하는 데 필요한 자격 증명(예: 사용자 이름/암호 또는 RSA SecurID/암호)을 획득합니다.

절차

- 1 서버에 연결하려면 창 하단에 있는 **서버**(클라우드 아이콘)를 누르고 서버 아이콘을 누릅니다.
- 2 메시지가 표시되면 RSA 사용자 이름/암호나 Active Directory 사용자 이름/암호 또는 둘 다를 제공합니다.
- 3 즐겨 찾는 원격 데스크톱 또는 게시된 애플리케이션을 선택하거나 선택을 취소하려면 다음 단계를 수행합니다.

옵션	조치
즐거찾기 선택	컨텍스트 메뉴가 나타날 때까지 원격 데스크톱 또는 게시된 애플리케이션 바로 가기를 길게 터치하고 <b>즐거찾기로 표시</b> 를 누릅니다. 바로 가기의 오른쪽 상단에 모서리에 별이 표시되고 바로 가기가 <b>즐거찾기</b> 창에 나타납니다.
즐거찾기 선택 취소	컨텍스트 메뉴가 나타날 때까지 원격 데스크톱 또는 게시된 애플리케이션 바로 가기를 길게 터치하고 <b>즐거찾기 표시 해제</b> 를 누릅니다. 바로 가기의 오른쪽 상단 모서리에 더 이상 별이 표시되지 않으며 바로 가기가 <b>즐거찾기</b> 창에서 사라집니다.

- 4 (선택 사항) 즐겨 찾는 원격 데스크톱 또는 게시된 애플리케이션만 표시하려면 창 하단의 **즐겨찾기**(별 모양 아이콘)를 누릅니다.

창 하단에 있는 **모두**(클라우드 아이콘)를 눌러서 모든 사용 가능한 원격 데스크톱 및 게시된 애플리케이션을 표시합니다.

## 원격 데스크톱 또는 게시된 애플리케이션에서 연결 해제

원격 데스크톱에 로그인되어 있을 때 애플리케이션이 원격 데스크톱에서 계속 열려 있도록 하기 위해 로그 오프하지 않고 연결을 해제할 수 있습니다. 또한 게시된 애플리케이션과의 연결을 해제하면 게시된 애플리케이션이 계속 열려 있는 상태로 유지됩니다.

원격 데스크톱 또는 게시된 애플리케이션의 연결을 해제하려면 **Horizon Client** 도구 원형 메뉴 아이콘 누르고 **연결 해제** 아이콘을 누릅니다. **Horizon Client** 도구 원형 메뉴 아이콘은 원격 데스크톱 또는 게시된 애플리케이션에 연결하면 창 가운데에 나타납니다. 자세한 내용은 [모바일 디바이스에서 Horizon Client 도구 사용](#)의 내용을 참조하십시오.

---

**참고** Horizon administrator는 연결을 끊을 때 로그오프하도록 원격 데스크톱을 구성할 수 있습니다. 그러한 경우, 원격 데스크톱에 열려 있는 모든 애플리케이션은 닫힙니다.

---

## 원격 데스크톱에서 로그오프

원격 데스크톱이 Horizon Client에서 열리지 않은 경우에도 원격 데스크톱에서 로그오프할 수 있습니다. 원격 데스크톱이 Horizon Client에서 열린 경우 **Windows 시작** 메뉴를 사용하여 로그오프할 수 있습니다.

### 사전 요구 사항

Active Directory 사용자 이름/암호, RSA SecurID 사용자 이름/암호 또는 RADIUS 인증 사용자 이름/암호와 같이 로그인하기 위한 자격 증명을 획득합니다.

### 절차

- 1 Horizon Client 창 하단에 있는 **서버**(클라우드 아이콘)를 누르고 서버 바로 가기를 누릅니다.
- 2 메시지가 표시되면 **RSA** 사용자 이름/암호나 **Active Directory** 사용자 이름/암호 또는 둘 다를 제공합니다.
- 3 컨텍스트 메뉴가 나타날 때까지 원격 데스크톱 바로 가기를 길게 터치합니다.
- 4 컨텍스트 메뉴에서 **로그오프**를 누릅니다.

### 결과

로그오프한 후에 원격 데스크톱의 연결이 끊어집니다. 원격 데스크톱에서 열려 있는 저장되지 않은 파일은 로그아웃 진행 중에 닫힙니다.

### 다음에 수행할 작업

서버에서 연결을 해제합니다. [서버에서 연결 해제](#)의 내용을 참조하십시오.

## 서버에서 연결 해제

원격 데스크톱이나 게시된 애플리케이션의 사용이 완료되면 서버에서 연결을 끊을 수 있습니다.

서버에서 연결을 끊으려면 Horizon Client 창의 왼쪽 위 모서리에서 **로그아웃** 버튼을 누릅니다.

## 원격 데스크톱 및 게시된 애플리케이션 바로 가기 관리

원격 데스크톱 또는 게시된 애플리케이션에 연결한 후 Horizon Client는 항목에 대한 바로 가기를 저장합니다. 이러한 바로 가기를 다시 정렬하거나 제거할 수 있습니다.

원격 데스크톱 및 게시된 애플리케이션 바로 가기가 많이 있으면 여러 페이지에 걸쳐 표시될 수 있습니다. 페이지를 밀어 넘기면서 더 많은 바로 가기를 볼 수 있습니다. 필요에 따라, Horizon Client에서는 모든 바로 가기를 포함하기 위해 페이지를 만듭니다.

절차

- ◆ **최근** 창에서 원격 데스크톱 또는 게시된 애플리케이션 바로 가기를 제거하려면 다음 단계를 수행합니다.
  - a 바로 가기를 길게 터치합니다.
  - b **X** 버튼을 누릅니다.
- ◆ 원격 데스크톱 또는 게시된 애플리케이션 바로 가기를 이동하려면 바로 가기를 길게 터치한 상태에서 새 위치로 끈 다음 **완료**를 누릅니다.
  - 존재하는 페이지로만 바로 가기를 끌어올 수 있습니다.

## Horizon Client에서 3D Touch 사용

3D Touch 지원 iPhone 6s 또는 iPhone 6s Plus가 있는 경우 Peek와 Pop 제스처를 사용하여 Horizon Client와 상호 작용할 수 있습니다.

## Horizon 애플리케이션에서 Peek 및 Pop 사용

iOS 디바이스 홈 화면에서 **Horizon** 애플리케이션을 꼭 누르면 빠른 동작 메뉴를 볼 수 있습니다. 빠른 동작 메뉴에서 **최근 서버에 연결**을 누르면 가장 최근에 사용한 서버로 연결할 수 있습니다. 최근 사용 서버가 없으면 **최근 서버에 연결** 항목을 눌러 새 서버를 추가할 수 있습니다.

원격 데스크톱이나 게시된 애플리케이션에 연결하고 나면 Horizon Client에서 빠른 동작 메뉴에 해당 원격 데스크톱이나 게시된 애플리케이션 바로 가기를 추가합니다. 예를 들어 Win7이라는 이름의 원격 데스크톱에 연결할 경우 Horizon Client에서 **Win7에 연결**을 추가합니다. 바로 가기를 눌러 원격 데스크톱 또는 게시된 애플리케이션에 연결할 수 있습니다.

**Horizon** 아이콘 빠른 동작 메뉴는 바로 가기를 3개까지 포함할 수 있습니다.

## Horizon Client 안에서 Peek와 Pop 사용

데스크톱 및 애플리케이션 선택 창에서 원격 데스크톱이나 게시된 애플리케이션을 꺾 눌러서 빠른 동작 메뉴를 표시할 수 있습니다. 빠른 동작 메뉴의 항목을 누르면 원격 데스크톱이나 게시된 애플리케이션에 따라 연결, 로그오프, 즐겨찾기로 표시 등의 작업을 수행할 수 있습니다. 원격 데스크톱 또는 게시된 애플리케이션을 미리 보고 연결할 수도 있습니다.

빠른 동작 메뉴는 **서버**, **최근**, **즐겨찾기** 창에서도 사용할 수 있습니다. 예를 들어 **서버** 창에서 저장된 서버를 꺾 눌러서 빠른 동작 메뉴의 항목을 누르면 수정, 제거, 서버 연결을 할 수 있습니다. **최근** 창에서 원격 데스크톱이나 게시된 애플리케이션 바로 가기를 꺾 누르고 빠른 동작 메뉴의 항목을 누르면 바로 가기를 삭제하거나 원격 데스크톱 또는 게시된 애플리케이션으로 연결할 수 있습니다. 저장된 서버 또는 원격 데스크톱이나 게시된 애플리케이션을 미리 보고 연결할 수도 있습니다.

## Horizon Client 도구에 대해 Peek 사용

기본적으로 Horizon Client 도구 원형 메뉴 아이콘은 원격 데스크톱 또는 게시된 애플리케이션에 연결하면 창 가운데에 나타납니다. 원형 메뉴 아이콘을 누르면 메뉴가 확대되어 각 도구의 아이콘이 표시되며, 원하는 항목을 눌러 선택할 수 있습니다. 원형 메뉴 아이콘과 도구 아이콘 그림은 [모바일 디바이스에서 Horizon Client 도구 사용](#)에서 참조하십시오.

Horizon Client 도구에 대해 Peek를 사용 설정하면 Horizon Client 도구 원형 메뉴 아이콘이 표시되지 않습니다. 각 도구에 대한 아이콘을 표시하려면 창의 아무 곳이나 깊게 누릅니다.

Horizon Client 도구에 대해 Peek를 사용 설정하려면 Horizon Client 창 하단에서 **설정**을 누르고 **터치**를 누른 다음 **메뉴 엮보기** 설정을 켜기로 전환합니다. 원격 데스크톱이나 게시된 애플리케이션에 연결되어 있는 경우에는 Horizon Client 도구 원형 메뉴에서 **설정**(톱니) 아이콘을 눌러 설정에 액세스할 수 있습니다.

## Horizon Client에서 Spotlight 검색 사용

iOS 9 이상 디바이스에서는 Spotlight 검색을 사용하여 원격 데스크톱 및 게시된 애플리케이션을 검색하고 연결할 수 있습니다.

Horizon Client에서 서버에 로그인하면 서버의 원격 데스크톱과 게시된 애플리케이션이 Spotlight 인덱스로 추가됩니다. 최근에 로그인한 서버의 원격 데스크톱과 게시된 애플리케이션만 인덱싱됩니다.

Spotlight 검색을 사용하여 특정 원격 데스크톱이나 게시된 애플리케이션을 찾으려면 Spotlight 검색 필드에 이름이나 이름 일부를 입력합니다. 예를 들어 이름이 Win 2012 RDS 데스크톱인 원격 데스크톱을 찾으려면 **Win** 또는 **RDS**를 입력하면 됩니다.

Spotlight 검색을 사용하여 자주 사용하는 원격 데스크톱과 게시된 애플리케이션을 찾으려면 Spotlight 검색 필드에 **즐겨찾기**를 입력합니다. 원격 데스크톱이나 게시된 애플리케이션을 검색하려면 Spotlight 검색 필드에 **vmware** 또는 **horizon**를 입력합니다.

검색 결과는 최대 10개 항목을 포함합니다.

원격 데스크톱이나 게시된 애플리케이션에 연결하려면 검색 결과에서 해당 이름을 누릅니다. 현재 서버에 연결되지 않았다면 Horizon Client 로그인 창이 표시되어 로그인할 수 있게 됩니다.

## Horizon Client에서 Split View 및 Slide Over 사용

Split View와 Slide Over를 지원하고 iOS 9 이상이 실행되는 모든 iPad 모델에서 Horizon Client와 함께 이러한 기능을 사용할 수 있습니다.

Split View와 Slide Over를 사용하면 Horizon Client 및 다른 애플리케이션을 동시에 열 수 있습니다. Horizon Client를 기본 또는 보조 애플리케이션으로 실행할 수 있습니다.

디바이스를 회전하거나 기본 애플리케이션과 보조 애플리케이션을 구분하는 수직선을 밀면 Horizon Client에서 창 크기에 맞춥니다. 원격 데스크톱에 연결되어 있고 해상도 설정이 자동 - 맞춤으로 설정되어 있으면 원격 데스크톱은 창 크기에 맞게 조정됩니다. 해상도 설정 방법에 대한 내용은 [디스플레이 해상도 설정 변경](#)을 참조하십시오.

Horizon Client에서는 Picture in Picture를 지원하지 않습니다.

## Horizon Client에서 iPad 분리식 키보드 사용

서버에 연결할 때와 원격 데스크톱에서 작업할 때 Horizon Client에서 분할 모드로 iPad 화면 키보드를 사용할 수 있습니다. 이 기능은 분리식 키보드 기능을 지원하는 모든 iPad 모델에서 지원됩니다.

화면 키보드를 분할하려면 텍스트 필드 내부를 누르고 화면 키보드의 오른쪽 아래 모서리에서 **키보드** 키를 길게 터치한 다음 **분할**을 누릅니다. 분리식 키보드를 병합하려면 **병합**을 누릅니다.

화면 키보드가 분할 모드일 때는 화면 키보드의 두 부분 사이에 있는 공간이 투명합니다.

---

**참고** 화면 키보드가 분할 모드일 때는 보조 키 막대를 사용할 수 없습니다. 보조 키 막대를 사용하려면 키보드를 병합해야 합니다.

---

## 바로 가기 및 URL 끌어오기

서버, 원격 데스크톱 및 게시된 애플리케이션 바로 가기 및 URL(Uniform Resource Identifier)을 끌어올 수 있습니다.

이 기능을 사용하려면 iOS 11 이상이 실행되는 iPad가 필요합니다.

Horizon Client **서버** 창에서 다른 애플리케이션(예: Notes)으로 서버 바로 가기를 끌어올 수 있습니다. 서버 바로 가기는 다른 애플리케이션에서 URI(예: `vmware-view://server address`)로 나타납니다. 다른 애플리케이션에서 **서버** 창으로 서버 주소 또는 URI를 끌어올 수 있습니다. 또한 이 기능을 사용하여 **서버** 창에서 서버 바로 가기의 순서를 변경할 수도 있습니다.

서버에 연결한 후 Horizon Client 데스크톱 및 애플리케이션 선택 창 또는 **즐거찾기** 창에서 다른 애플리케이션(예: Notes)으로 원격 데스크톱 또는 게시된 애플리케이션 바로 가기를 끌어올 수 있습니다. 바로 가기는 다른 애플리케이션에서 URI(예: `vmware-view://server-name/item-name`)로 나타납니다. 다른 애플리케이션에서 데스크톱 및 애플리케이션 선택 창, **즐거찾기** 창 또는 **최근** 창으로 원격 데스크톱 또는 게시된 애플리케이션 URI를 끌어올 수 있습니다.

URI 구문에 대한 내용은 [vmware-view URI 생성을 위한 구문](#)을 참조하십시오.

## Horizon Client 위젯 사용

iOS 10 이상 디바이스가 있는 경우 iOS 디바이스의 [검색] 화면에 Horizon Client 위젯을 추가할 수 있습니다.

Horizon Client 위젯을 [검색] 화면에 추가하려면 [검색] 화면에서 **편집**을 클릭하고 위젯 목록에서 Horizon Client 옆에 있는 녹색 더하기(+) 버튼을 누른 후 **완료**를 클릭합니다.

원격 데스크톱 또는 게시된 애플리케이션에 연결해본 적이 없으면 Horizon Client 위젯에는 아직 시작한 데스크톱/애플리케이션이 없습니다. 라는 메시지가 표시됩니다. 원격 데스크톱 또는 게시된 애플리케이션에 연결한 후에 최근에 사용한 원격 데스크톱 또는 게시된 애플리케이션에 대한 바로 가기가 위젯에 나타납니다. 이 바로 가기를 눌러 [검색] 화면에서 원격 데스크톱 또는 게시된 애플리케이션을 열 수 있습니다.

3D Touch 지원 디바이스가 있는 경우 Horizon Client 위젯은 iOS 디바이스 홈 화면에서 **Horizon** 애플리케이션을 누르면 빠른 동작 메뉴에 나타납니다.

# Microsoft Windows 데스크톱 또는 게시된 애플리케이션 사용

# 4

iOS용 Horizon Client에는 iOS 디바이스에서 탐색하는 데 도움이 되는 추가 기능이 포함되어 있습니다. 사용자는 원격 데스크톱 및 게시된 애플리케이션이 있는 외부 디바이스를 사용하고, iOS 디바이스의 텍스트 및 이미지를 원격 데스크톱 및 게시된 애플리케이션으로 복사하고, 게시된 애플리케이션에서 문서를 저장할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- iOS 클라이언트용 기능 지원
- 원격 데스크톱에서 Unity Touch 사이드바 사용
- 게시된 애플리케이션에서 Unity Touch 사이드바 사용
- 모바일 디바이스에서 Horizon Client 도구 사용
- 제스처
- 터치 리디렉션을 통해 기본 운영 체제 제스처 사용
- 화면 해상도 및 외부 디스플레이 사용
- DPI 동기화 사용
- 외부 키보드 및 기타 입력 디바이스
- 실시간 오디오-비디오 기능 사용
- 좌우를 바꾼 마우스 버튼을 지원하도록 Horizon Client 구성
- 텍스트와 이미지 복사 및 붙여넣기
- 텍스트 및 이미지 끌어오기
- 원격 데스크톱 또는 게시된 애플리케이션에서 인쇄
- 게시된 애플리케이션에서 문서 저장
- 여러 클라이언트 디바이스에서 게시된 애플리케이션의 다중 세션 사용
- 멀티태스킹
- 셀룰러 데이터 경고 메시지 표시하지 않음

- 화면 활성 유지
- PCoIP 클라이언트 측 이미지 캐시

## iOS 클라이언트용 기능 지원

특정 게스트 운영 체제 및 원격 데스크톱 기능에는 특정 Horizon Agent 버전이 필요합니다. 이 정보는 최종 사용자가 사용할 수 있도록 할 기능을 계획할 때 사용합니다.

### 지원되는 Windows 가상 데스크톱

Windows 가상 데스크톱은 단일 세션 가상 시스템입니다.

이 버전의 Horizon Client는 Horizon Agent 7.5 이상이 설치된 Windows 가상 데스크톱에서 작동합니다. 지원되는 게스트 운영 체제에는 Windows 7, Windows 8.x, Windows 10, Windows Server 2012 R2, Windows server 2016 및 Windows Server 2019가 포함되며 다음과 같은 제한이 있습니다.

- Windows Server 2019 가상 데스크톱에는 Horizon Agent 7.7 이상이 필요합니다.
- Windows 7 및 Windows 8.x 가상 데스크톱은 Horizon Agent 2006 이상에서 지원되지 않습니다.

### RDS 호스트의 지원되는 게시된 데스크톱

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

이 Horizon Client 버전은 Horizon Agent 7.5 이상이 설치된 RDS 호스트에서 작동합니다. 지원되는 게스트 운영 체제에는 Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 및 Windows Server 2019가 포함되며 다음과 같은 제한이 있습니다.

- Windows Server 2019 RDS 호스트에는 Horizon Agent 7.7 이상이 필요합니다.
- Windows Server 2012 RDS 호스트는 Horizon Agent 2006 이상에서 지원되지 않습니다.

### 특정 기능에 대한 요구 사항 및 제한 사항

일부 원격 데스크톱 기능에는 특정 요구 사항 또는 제한 사항이 있습니다.

- VMware Integrated Printing 기능을 사용하려면 Horizon Agent 2006 이상이어야 합니다.
- VMware Integrated Printing 기능은 Windows 10, Windows Server 2016 및 Windows Server 2019 원격 데스크톱에서만 지원됩니다. Windows 7, Windows 8.x 및 Windows Server 2012 R2 원격 데스크톱에서는 이 기능을 사용할 수 없습니다.

### 지원되는 Linux 데스크톱

지원되는 Linux 게스트 운영 체제 목록 및 지원되는 기능에 대한 자세한 내용은 "Horizon에서 Linux 데스크톱 설정" 문서를 참조하십시오.

## 원격 데스크톱에서 Unity Touch 사이드바 사용

Unity Touch 사이드바에서 원격 데스크톱의 애플리케이션 또는 파일로 빠르게 이동할 수 있습니다. 이 사이드바를 통해 파일 및 애플리케이션을 열고, 실행 중인 애플리케이션 간에 전환하고, 원격 데스크톱에서 창과 애플리케이션을 최소화하거나 최대화하거나 복원하거나 닫을 수 있습니다.

Unity Touch 기능은 Horizon 관리자가 사용하도록 설정한 경우에만 사용할 수 있습니다. 사용자에게 부동 데스크톱이 있는 경우, Windows 로밍 사용자 프로파일이 원격 데스크톱에 구성된 경우에만 사용자의 즐겨찾는 애플리케이션 및 파일을 저장할 수 있습니다. 또한 Horizon 관리자는 사이드바가 처음 나타날 때 최종 사용자에게 나타나는 기본 **즐거찾는 애플리케이션** 목록을 만들 수 있습니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서의 "Unity Touch 구성"을 참조하십시오.

Unity Touch 기능을 사용하도록 설정한 경우, 원격 데스크톱에 처음 연결할 때 창 왼쪽에 사이드바가 나타납니다.

Unity Touch 사이드바가 닫히면 창 왼쪽에 탭이 나타납니다. 이 탭을 오른쪽으로 밀어서 사이드바를 열 수 있습니다. 탭을 위 또는 아래로 밀 수도 있습니다.

Unity Touch 사이드바를 통해 원격 데스크톱에서 여러 작업을 수행할 수 있습니다.

표 4-1. 원격 데스크톱에 대한 Unity Touch 사이드바 작업

조치	절차
사이드바 표시	탭을 오른쪽으로 밀니다. 사이드바가 열려 있는 상태에서는 원격 데스크톱 창 또는 Horizon Client 도구 원형 메뉴에서 작업을 수행할 수 없습니다.
사이드바 숨기기	사이드바를 닫으려면 탭을 왼쪽으로 밀니다. 사이드바가 열려 있는 상태에서는 원격 데스크톱 창 또는 Horizon Client 도구 원형 메뉴에서 작업을 수행할 수 없습니다. Horizon Client 도구 원형 메뉴를 포함한 원격 데스크톱 창을 터치하여 사이드바를 숨길 수 있습니다.
애플리케이션으로 이동	<b>모든 프로그램</b> 을 누르고 Windows 시작 메뉴에서 원하는 애플리케이션으로 이동합니다.
파일로 이동	<b>내 파일</b> 을 눌러 User 폴더에 액세스하고 파일로 이동합니다. <b>내 파일</b> 에는 내 그림, 내 문서 및 다운로드 등의 폴더가 있습니다. <b>내 파일</b> 에는 사용자 프로필(%USERPROFILE% 디렉토리)의 폴더가 포함됩니다. %USERPROFILE% 디렉토리에서 시스템 폴더의 위치를 변경하는 경우, 위치가 변경된 로컬 폴더이든 네트워크 공유 폴더이든 상관 없이 <b>내 파일</b> 메뉴에도 위치가 변경된 폴더의 콘텐츠가 표시될 수 있습니다.
애플리케이션 또는 파일 검색	<ul style="list-style-type: none"> <li>■ <b>검색</b> 상자를 누르고 애플리케이션 또는 파일의 이름을 입력합니다.</li> <li>■ 목소리 받아쓰기를 사용하려면 키보드의 마이크를 누릅니다.</li> <li>■ 애플리케이션 또는 파일을 실행하려면 검색 결과에서 애플리케이션 또는 파일의 이름을 누릅니다.</li> <li>■ 사이드바의 홈 보기로 되돌아가려면 <b>X</b>를 눌러 <b>검색</b> 상자를 닫습니다.</li> </ul>
애플리케이션 또는 파일 열기	사이드바에서 파일 또는 애플리케이션의 이름을 누릅니다. 애플리케이션이 시작되고 사이드바가 닫힙니다.
실행 중인 애플리케이션 또는 열린 창 간 전환	<b>실행 중인 애플리케이션</b> 에서 애플리케이션 이름을 누릅니다. 한 개의 애플리케이션에 대해 두 개 이상의 파일이 열려 있는 경우, 애플리케이션 옆에 있는 펼침 단추(>)를 눌러 목록을 확장합니다.

표 4-1. 원격 데스크톱에 대한 Unity Touch 사이드바 작업 (계속)

조치	절차
실행 중인 애플리케이션 또는 창 최소화	<ol style="list-style-type: none"> <li>1 실행 중인 애플리케이션에서 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다.</li> <li>2 나타나는 <b>자세히</b> 버튼을 누릅니다.</li> <li>3 <b>최소화</b>를 누릅니다.</li> </ol>
실행 중인 애플리케이션 또는 창 최대화	<ol style="list-style-type: none"> <li>1 실행 중인 애플리케이션에서 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다.</li> <li>2 나타나는 <b>자세히</b> 버튼을 누릅니다.</li> <li>3 <b>최대화</b>를 누릅니다.</li> </ol>
실행 중인 애플리케이션 또는 창 닫기	<p>실행 중인 애플리케이션에서 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다. 나타나는 <b>닫기</b> 버튼을 누릅니다.</p>
실행 중인 애플리케이션이나 창을 이전의 크기 및 위치로 복원	<ol style="list-style-type: none"> <li>1 실행 중인 애플리케이션에서 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다.</li> <li>2 나타나는 <b>자세히</b> 버튼을 누릅니다.</li> <li>3 <b>복원</b>을 누릅니다.</li> </ol>
즐거찾는 애플리케이션 또는 파일 목록 만들기	<ol style="list-style-type: none"> <li>1 애플리케이션 또는 파일을 검색하거나 <b>즐거찾는 애플리케이션</b> 또는 <b>즐거찾는 문서</b> 목록에서 <b>관리</b>를 누릅니다.  관리 표시줄이 나타나지 않을 경우, <b>즐거찾는 애플리케이션</b> 또는 <b>즐거찾는 파일</b> 옆에 있는 펼침 단추(&gt;)를 누릅니다.</li> <li>2 검색 결과나 사용 가능한 애플리케이션 또는 파일 목록에서 즐겨찾기 이름 옆에 있는 확인란을 누릅니다.  마지막으로 추가한 즐겨찾기가 즐겨찾기 목록의 맨 위에 표시됩니다.  예를 들어, 모든 모바일 디바이스에 즐겨찾기가 저장되면 스마트폰이나 태블릿 중 무엇을 사용하든지 동일한 목록이 표시됩니다.</li> </ol>
애플리케이션이나 파일을 즐겨찾기 목록에서 제거	<ol style="list-style-type: none"> <li>1 애플리케이션 또는 파일을 검색하거나 <b>즐거찾는 애플리케이션</b> 또는 <b>즐거찾는 문서</b> 목록에서 <b>관리</b>를 누릅니다.  관리 표시줄이 나타나지 않을 경우, <b>즐거찾는 애플리케이션</b> 또는 <b>즐거찾는 문서</b> 옆에 있는 펼침 단추(&gt;)를 누릅니다.</li> <li>2 즐겨찾기 목록에서 애플리케이션 또는 파일의 이름 옆에 있는 확인란을 누르면 제거됩니다.</li> </ol>
즐거찾기 목록의 애플리케이션이나 파일 다시 정렬	<ol style="list-style-type: none"> <li>1 <b>즐거찾는 애플리케이션</b> 또는 <b>즐거찾는 문서</b> 목록에서 <b>관리</b>를 누릅니다.  관리 표시줄이 나타나지 않을 경우, <b>즐거찾는 애플리케이션</b> 또는 <b>즐거찾는 문서</b> 옆에 있는 펼침 단추(&gt;)를 누릅니다.</li> <li>2 즐겨찾기 목록에서 애플리케이션이나 파일의 이름 왼쪽에 있는 핸들을 길게 터치하고 목록 내에서 위나 아래로 끌어 옮깁니다.</li> </ol>

## 게시된 애플리케이션에서 Unity Touch 사이드바 사용

Unity Touch 사이드바에서 게시된 애플리케이션으로 빠르게 이동할 수 있습니다. 이 사이드바를 통해 게시된 애플리케이션을 시작하고, 실행 중인 게시된 애플리케이션 간에 전환하고, 게시된 애플리케이션을 최소화하거나 최대화하거나 복원하거나 닫을 수 있습니다. 원격 데스크톱으로 전환할 수도 있습니다.

Unity Touch 기능은 Horizon 관리자가 사용하도록 설정한 경우에만 사용할 수 있습니다.

Unity Touch 기능을 사용하도록 설정한 경우, 게시된 애플리케이션에 처음 연결할 때 창 왼쪽에 Unity Touch 사이드바가 나타납니다. Unity Touch 사이드바가 닫히면 창 왼쪽에 탭이 나타납니다. 이 탭을 오른쪽으로 밀어서 사이드바를 다시 열 수 있습니다. 탭을 위 또는 아래로 밀 수도 있습니다.

Unity Touch 사이드바를 통해 게시된 애플리케이션에서 여러 작업을 수행할 수 있습니다.

표 4-2. 게시된 애플리케이션에 대한 Unity Touch 사이드바 작업

조치	절차
사이드바 표시	사이드바를 열려면 탭을 오른쪽으로 밀니다. 사이드바가 열려 있으면 게시된 애플리케이션 창에서 작업을 수행할 수 없습니다.
사이드바 숨기기	사이드바를 닫으려면 탭을 왼쪽으로 밀니다. 사이드바가 열려 있으면 게시된 애플리케이션 창에서 작업을 수행할 수 없습니다. Horizon Client 도구 원형 메뉴를 포함한 게시된 애플리케이션 창을 터치하여 사이드바를 숨길 수 있습니다.
실행 중인 게시된 애플리케이션 간 전환	<b>현재 연결</b> 아래의 애플리케이션을 누릅니다. <b>참고</b> 데이터 손실을 방지하려면 다중 세션 모드에 있는 게시된 애플리케이션에서 전환하기 전에 데이터를 저장합니다.
게시된 애플리케이션 열기	사이드바의 <b>사용 가능한 애플리케이션</b> 아래에서 게시된 애플리케이션 이름을 누릅니다. 게시된 애플리케이션이 시작되고 사이드바가 닫힙니다.
실행 중인 게시된 애플리케이션 닫기	1 <b>현재 연결</b> 에서 게시된 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다. 2 나타나는 <b>닫기</b> 버튼을 누릅니다.
실행 중인 게시된 애플리케이션 최소화	1 <b>현재 연결</b> 에서 게시된 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다. 2 나타나는 <b>자세히</b> 버튼을 누릅니다. 3 <b>최소화</b> 를 누릅니다.
실행 중인 게시된 애플리케이션 최대화	1 <b>현재 연결</b> 에서 게시된 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다. 2 나타나는 <b>자세히</b> 버튼을 누릅니다. 3 <b>최대화</b> 를 누릅니다.
실행 중인 게시된 애플리케이션 복원	1 <b>현재 연결</b> 에서 게시된 애플리케이션 이름을 터치하고 오른쪽에서 왼쪽으로 밀니다. 2 나타나는 <b>자세히</b> 버튼을 누릅니다. 3 <b>복원</b> 을 누릅니다.
원격 데스크톱으로 전환	<b>데스크톱</b> 아래에서 원격 데스크톱 이름을 누릅니다.

## 모바일 디바이스에서 Horizon Client 도구 사용

모바일 디바이스의 Horizon Client 도구에는 화면 키보드, 가상 터치패드, 구성 설정, 화살표 키 및 기능 키에 대한 가상 키패드 표시용 버튼이 포함됩니다.

Horizon Client 도구 원형 메뉴 아이콘은 원격 데스크톱 또는 게시된 애플리케이션에 연결하면 창 가운데에 나타납니다. 원형 메뉴를 누르면 확대되어 각 도구의 아이콘이 표시되며, 원하는 항목을 눌러 선택할 수 있습니다. 도구 아이콘 밖을 누르면 아이콘이 다시 원형 메뉴 아이콘으로 축소됩니다.

원형 메뉴에는 여러 도구가 있습니다.

표 4-3. 원형 메뉴 아이콘

아이콘	설명
	Horizon Client 도구 원형 메뉴
	연결 끊기
	화면 키보드(표시/숨기기 전환)
	설정
	탐색 키
	가상 터치패드
	제스처 도움말

## 화면 키보드

화면 키보드는 표준 화면 키보드보다 더 많은 키를 가지고 있습니다. 예를 들어 **Control** 키와 **Fn** 키도 사용할 수 있습니다. 화면 키보드를 표시하려면 세 손가락으로 동시에 화면을 누르거나 **키보드** 아이콘을 누릅니다.

메모나 새 연락처 등 텍스트 필드를 누를 때마다 화면 키보드가 표시되는 기능을 사용할 수도 있습니다. 텍스트 필드가 아닌 영역을 누를 경우, 키보드가 사라집니다.

**중요** 세 손가락 누르기를 사용하려면 확대/축소를 위한 iOS의 접근성 기능이 꺼져 있어야 합니다. 확대/축소 접근성 기능이 켜져 있을 경우 세 개 손가락으로 두 번 누르면 확대/축소되고 세 개 손가락으로 한 번 누르면 아무 동작도 수행되지 않습니다.

외부 키보드를 사용하는 경우에도, 기능 키, **Ctrl**, **Alt**, **Win** 및 화살표 키가 포함된 한 줄 화면 키보드가 계속 나타날 수 있습니다. 일부 키가 없는 외부 키보드도 있습니다.

## 문자열 보내기

화면 키보드에서 **Ctrl** 키의 왼쪽에 있는 펜 아이콘을 눌러 로컬 입력 버퍼를 표시합니다. 이 텍스트 상자에 입력한 텍스트는 **보내기**를 누를 때까지 애플리케이션에 전송되지 않습니다. 예를 들어 메모장과 같은 애플리케이션을 열고 펜 아이콘을 누르면 입력한 텍스트는 **보내기**를 누를 때까지 메모장 애플리케이션에 나타나지 않습니다.

네트워크 연결이 양호하지 않을 경우 이 기능을 사용하십시오. 즉, 문자를 입력할 때 애플리케이션에 문자가 즉시 나타나지 않을 경우 이 기능을 사용하십시오. 이 기능으로, 최대 1,000개 문자를 신속하게 입력한 다음 **보내기**나 **Return**을 눌러 1,000개 문자를 애플리케이션에서 한 번에 모두 표시할 수 있습니다.

## 탐색 키

Horizon Client 도구 또는 화면 키보드에서 **Ctrl/Page** 아이콘을 눌러 탐색 키를 표시합니다. 이러한 키에는 Page Up, Page Down, 화살표 키, 기능 키 및 Alt, Del, Shift, Ctrl, Win 및 Esc와 같이 Windows 환경에서 자주 사용하는 키가 포함됩니다. 연속적인 키 입력의 경우 화살표 키를 누르고 있으면 됩니다. Ctrl/Page 아이콘에 대한 그림은 이 항목의 처음에 있는 표를 참조하십시오.

Ctrl+Shift와 같이 Shift 키가 포함된 키 조합을 사용해야 하는 경우 이 키패드의 Shift 키를 사용합니다. Ctrl+Alt+Shift 등의 키 조합을 누르려면 먼저 화면 상의 Ctrl 키를 누릅니다. Ctrl 키가 파란색으로 변하면 화면 상의 Alt 키를 누릅니다. Alt 키가 파란색으로 변하면 화면 상의 Shift 키를 누릅니다. Ctrl+Alt+Del 키 조합에 대해 화면 상에 하나의 키가 제공됩니다.

## 화면 터치패드 및 전체 화면 터치패드

가상 터치패드는 노트북 컴퓨터의 터치패드와 유사한 일반 크기로 표시하거나, 디바이스 화면 전체를 사용하여 표시할 수 있습니다.

기본적으로 터치패드 아이콘을 누르면 화면의 아무 곳이나 터치하여 마우스 포인터를 이동할 수 있습니다. 화면이 전체 화면 터치패드가 됩니다.

- 손가락으로 터치패드 주위를 이동하면 원격 데스크톱 또는 게시된 애플리케이션 주위를 이동하는 마우스 포인터가 나타납니다.
- 일반 크기 및 전체 화면 가상 터치패드를 사용하여 한 번 클릭 및 두 번 클릭을 수행할 수 있습니다.
- 일반 터치패드에는 왼쪽 클릭 및 오른쪽 클릭 버튼도 있습니다.
- 왼쪽 클릭 버튼을 누른 채 끌어 놓기를 시뮬레이션하려면 한 손가락으로 두 번 누른 다음 끌어 옵니다. 이 기능을 사용하려면 Horizon Client 도구를 사용하여 옵션 대화 상자를 표시하고 **터치패드 누르기 및 끌기** 옵션을 클릭하여 켜기로 전환합니다.
- 두 개 손가락으로 누른 다음 끌어 수직 방향으로 스크롤할 수 있습니다.

일반 크기의 가상 터치패드를 디바이스 측면으로 끌어 놓으면 디바이스를 잡고 있는 상태에서 엄지 손가락으로 터치패드를 작동할 수 있습니다.

가상 터치패드를 오른쪽 클릭과 왼쪽 클릭 버튼을 포함한 노트북 터치패드처럼 사용할 수 있습니다. Horizon Client 도구 원형 메뉴 아이콘을 눌러서 확장하고 **설정(톱니)** 아이콘을 누른 다음 **터치**를 누르고 **전체 화면 터치패드 모드** 설정을 끕니다.

터치패드 사용 시 포인터 이동 속도를 조정하려면 Horizon Client 도구 원형 메뉴 아이콘을 눌러서 확장하고 **설정(톱니)** 아이콘을 누른 다음 **터치**를 누르고 **터치패드 민감도** 옵션의 슬라이더를 끌어 조정합니다.

**전체 화면 터치패드 모드** 및 **터치패드 민감도** 설정을 Horizon Client [설정] 창에서 설정할 수도 있습니다. Horizon Client 창 하단에서 **설정**을 누르고 **터치**를 눌러 터치패드 설정을 표시합니다.

원격 데스크톱 또는 계시된 애플리케이션에 로그인된 상태에서 터치패드 설정을 변경하면 다음번에 같은 iOS 디바이스에서 원격 데스크톱 또는 계시된 애플리케이션에 연결하면 터치패드 설정이 그대로 유지됩니다.

## 제스처

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

### 클릭

다른 애플리케이션의 경우와 마찬가지로 사용자 인터페이스 요소를 눌러 클릭합니다.

원격 데스크톱에서 1초 동안 길게 누르면 정밀한 배치를 위해 마우스 포인터와 함께 돋보기가 나타납니다. 이 기능은 특히 창 크기를 조정하는 경우 유용합니다.

---

**참고** 원격 데스크톱을 왼손 사용자용으로 구성한 경우 [좌우를 바꾼 마우스 버튼을 지원하도록 Horizon Client 구성](#)의 내용을 참조하십시오.

---

### 오른쪽 클릭

오른쪽 클릭으로 사용할 수 있는 옵션은 다음과 같습니다.

- Horizon Client 도구를 사용하여 일반 크기의 가상 터치패드를 표시하고 터치패드의 오른쪽 클릭 버튼을 사용합니다.
- 터치 스크린을 두 손가락으로 거의 동시에 누릅니다. 첫 번째 손가락을 누른 위치에 오른쪽 클릭이 작동됩니다.

### 스크롤 및 스크롤 막대

수직 스크롤에 대해 다음 옵션이 제공됩니다.

- 터치 스크린을 하나 또는 두 개의 손가락으로 누른 다음 끌어서 스크롤합니다. 손가락 아래 텍스트가 손가락과 동일한 방향으로 이동합니다.

---

**중요** 한 손가락으로 스크롤하는 동작은 화면을 확대한 상태이거나 화면 키보드가 표시되어 있거나 전체 화면 터치패드를 사용하는 경우에는 작동하지 않습니다.

---

- Horizon Client 도구를 사용하여 터치패드를 표시하고, 두 손가락으로 터치패드를 누른 다음 끌어서 스크롤합니다.
- 화면 터치패드를 사용하여 마우스 포인터를 이동하고 스크롤 막대를 클릭합니다.

### 확대 및 축소

다른 애플리케이션에서와 마찬가지로 터치 스크린에서 두 손가락을 서로 벌리거나 오므려서 확대/축소합니다.

## 창 크기 조정

전체 화면 터치패드를 사용하여 창 크기를 조정하는 경우 창의 모서리 또는 측면에서 손가락을 누른 채로 끌어서 크기를 조정하거나 한 손가락으로 두 번 누른 다음 드래그합니다.

일반 크기의 가상 터치패드를 사용하는 경우 왼쪽 클릭 버튼을 누른 채 창의 모서리 또는 측면 끌어 놓기 동작을 수행하려면 한 손가락으로 두 번 누른 다음 끌어옵니다.

둘 중 어떤 가상 터치패드도 사용하지 않는 경우 창의 모서리나 측면에 돋보기가 나타날 때까지 길게 누릅니다. 크기 조정 화살표가 나타날 때까지 손가락을 움직입니다. 손가락을 화면에서 뺍니다. 돋보기가 크기 조정 원으로 바뀝니다. 이 크기 조정 원을 누르고 끌어서 창 크기를 조정합니다.

## 사운드, 음악 및 비디오

디바이스 사운드가 켜져 있는 경우 원격 데스크톱에서 오디오를 재생할 수 있습니다.

## 터치 리디렉션을 통해 기본 운영 체제 제스처 사용

터치 리디렉션 기능을 사용할 경우 원격 데스크톱이나 게시된 애플리케이션에서 터치 기반 모바일 디바이스의 기본 운영 체제 제스처를 사용할 수 있습니다. 예를 들어 Windows 8.1 원격 데스크톱에서 항목을 길게 터치한 다음 놓아서 항목의 컨텍스트 메뉴를 표시할 수 있습니다.

터치 리디렉션을 사용하도록 설정한 경우 Horizon Client 로컬 제스처(예: 두 번 클릭 및 손가락 모으기)는 더 이상 지원되지 않습니다. Unity Touch 사이드바를 표시하려면 Unity Touch 탭 버튼을 끌어야 합니다.

터치 리디렉션은 대부분의 원격 데스크톱에 연결할 때 기본적으로 사용하도록 설정됩니다.

터치 리디렉션을 사용하지 않도록 설정하려면 Horizon Client 창 하단에서 **설정**을 누르고 **터치**를 누른 다음 **Windows 기본 터치 제스처** 설정을 끄기로 전환합니다. 원격 데스크톱이나 게시된 애플리케이션에 연결되어 있는 경우에는 Horizon Client 도구 원형 메뉴에서 **설정(톱니)** 아이콘을 누릅니다.

## 화면 해상도 및 외부 디스플레이 사용

외부 디스플레이에서 Horizon Client를 사용하고 화면 해상도를 변경할 수 있습니다.

클라이언트 디바이스를 외부 디스플레이나 프로젝터에 연결하는 경우 Horizon Client는 특정 최대 디스플레이 해상도를 지원합니다. 클라이언트 디바이스에서 사용하는 화면 해상도를 변경하여 높은 화면 해상도의 스크롤을 허용할 수도 있습니다.

## 원격 데스크톱의 화면 해상도 확대

기본적으로 디스플레이 해상도는 전체 원격 데스크톱이 클라이언트 디바이스 안쪽에 알맞게 표시되고 원격 데스크톱 아이콘과 작업 표시줄 아이콘이 특정 크기가 되도록 설정됩니다. 더 큰 해상도를 사용하는 경우 원격 데스크톱이 여전히 클라이언트 디바이스 크기에 맞지만, 원격 데스크톱 및 작업 표시줄 아이콘은 더 작아집니다.

손가락으로 확대 동작을 하여 원격 데스크톱을 디바이스 화면보다 크게 확대할 수 있습니다. 그리고 누른 다음, 끌어서 원격 데스크톱의 가장자리에 접근할 수 있습니다.

## 디스플레이 해상도 설정 변경

원격 데스크톱이나 게시된 애플리케이션에서 해상도를 변경하려면 Horizon Client 도구 원형 메뉴 아이콘을 눌러서 확장하고 **설정**(톱니) 아이콘을 누른 다음 **해상도**를 누릅니다. Horizon Client [설정] 창에서 해상도를 변경할 수도 있습니다. Horizon Client 창 하단의 **설정**을 누르고 **해상도**를 누릅니다.

**참고** 3/4 크기 조정 및 크기 조정 없음을 포함한 특정 옵션은 디바이스가 확대 모드일 때 iPhone 6에서 사용할 수 없습니다. 이러한 옵션을 표시하려면 확대/축소 모드를 종료해야 합니다.

## 고해상도 모드 사용

고해상도 모드 기능을 사용하여 원격 데스크톱 및 게시된 애플리케이션에서 최상의 디스플레이 품질을 얻을 수 있습니다.

Horizon Client 설정 창에서 고해상도 모드를 사용하도록 설정하려면 Horizon Client 창 하단에서 **설정**을 누르고 **해상도**를 누른 후 **고해상도 모드**를 눌러 커짐으로 전환합니다. 원격 데스크톱 또는 게시된 애플리케이션에서 [고해상도 모드]를 사용하도록 설정하려면 Horizon Client 도구 원형 메뉴 아이콘을 눌러 확장하고 **설정**(톱니) 아이콘을 누른 후 **해상도**를 누르고 **고해상도 모드** 설정을 눌러 켵니다.

고해상도 모드 기능에는 다음 요구 사항 및 제한 사항이 적용됩니다.

- 기존 세션에 대해서는 고해상도 모드 기능을 사용할 수 없습니다. 로그아웃한 후 새 세션으로 로그인해야 기능이 적용됩니다.
- 고해상도 모드 기능을 사용하려면 iPad Pro 또는 Retina 디스플레이가 포함된 iPad 또는 iPad mini가 있어야 합니다.
- 고해상도 모드 기능에서는 대역폭이 많이 사용될 수 있습니다. 대역폭을 최적화하려면 **고해상도 모드** 설정을 [끔]으로 설정합니다.

**고해상도 모드**는 기본적으로 사용하도록 설정되어 있습니다.

## 외부 모니터 및 프로젝터 사용

**해상도** 설정을 사용하여 외부 모니터 및 프로젝터를 위한 높은 해상도를 설정할 수 있습니다.

프로젝터나 연결된 모니터에서 원격 데스크톱을 표시하는 동안 디바이스에 키보드와 확장 화면 터치패드를 표시하려면 **프레젠테이션 모드**를 사용하도록 설정하십시오. 확장된 터치패드와 키보드는 디바이스를 외부 모니터에 꽂으면 나타납니다. 외부 디스플레이에서 제공하는 최대 해상도를 디바이스가 감지합니다.

**프레젠테이션 모드** 설정을 끄면 Unity Touch 사이드바를 포함하여 전체 디바이스 디스플레이를 프로젝터 또는 연결된 모니터에 미러링할 수 있습니다. 원격 데스크톱에 연결되어 있고 **프레젠테이션 모드** 설정이 사용되는 경우 **완료**를 클릭하면 미러 모드로 전환됩니다.

**프레젠테이션 중에 화면 활성 상태 유지** 설정을 사용하여 프레젠테이션 모드에서 일정 시간 동안 작업하지 않을 때 디스플레이가 꺼지지 않도록 할 수 있습니다.

원격 데스크톱이나 게시된 애플리케이션에서 Horizon Client 도구 원형 메뉴 아이콘을 눌러서 확장하고 **설정**(톱니) 아이콘을 눌러 이러한 설정을 구성할 수 있습니다. Horizon Client 창 하단에서 **설정**(톱니) 아이콘을 눌러 이러한 설정을 구성할 수도 있습니다.

## 외부 디스플레이에서 민감한 정보 숨기기

외부 모니터나 프로젝터에서 Horizon Client를 사용할 때 사용자 데이터 보안을 위해 암호 및 인증번호와 같은 민감한 정보가 숨겨집니다.

## DPI 동기화 사용

DPI 동기화 기능은 원격 데스크톱 또는 게시된 애플리케이션의 DPI 설정이 클라이언트 시스템의 DPI 설정과 일치하는지 확인합니다.

디스플레이 크기 조정 기능과 마찬가지로 DPI 동기화 기능을 통해 높은 DPI 디스플레이에서 텍스트 및 아이콘의 가독성을 높일 수 있습니다. 글꼴 및 이미지의 크기가 커지고 흐리게 나타낼 수 있는 디스플레이 크기 조정 기능과 달리, DPI 동기화 기능을 사용하면 선명도를 유지하면서 글꼴과 이미지의 크기를 늘릴 수 있습니다. 이러한 이유로 DPI 동기화 기능은 일반적으로 최적의 사용자 환경을 위해 선호됩니다.

DPI 동기화를 사용하지 않도록 설정하면 디스플레이 크기 조정이 사용됩니다. 디스플레이 크기 조정 기능을 통해 원격 데스크톱 또는 게시된 애플리케이션 크기를 적절히 조정할 수 있습니다.

**DPI 동기화** 에이전트 그룹 정책 설정은 DPI 동기화 기능의 사용 여부를 결정합니다. 이 기능은 기본적으로 사용하도록 설정됩니다.

## DPI 동기화 동작

기본 DPI 동기화 동작은 에이전트 시스템에 설치된 Horizon Agent 버전에 따라 다릅니다.

Horizon Agent 2012부터는 클라이언트의 모니터당 DPI 설정이 에이전트와 동기화되고, 기본적으로 원격 세션 중에 변경 사항이 즉시 적용됩니다. 이 기능은 모니터당 DPI 동기화 에이전트 그룹 정책 설정에 의해 제어됩니다. 모니터당 DPI 동기화 기능은 가상 데스크톱 및 물리적 데스크톱에서 기본적으로 지원됩니다. 게시된 데스크톱에서는 지원되지 않습니다.

이전 Horizon Agent 버전에서 클라이언트는 시스템 DPI 설정에 대한 동기화만 지원합니다. 초기 연결 중에 DPI 동기화가 수행되고, 다시 연결될 경우 필요하면 디스플레이 크기 조정이 수행됩니다. DPI 동기화가 작동하고 클라이언트 시스템의 DPI 설정이 원격 데스크톱의 DPI 설정과 일치하면 사용자 인터페이스에서 디스플레이 크기 조정 허용 옵션을 선택하더라도 디스플레이 크기 조정이 적용될 수 없습니다. Windows에서는 사용자가 현재 사용자 세션에 대한 시스템 수준 DPI 설정을 변경하는 것을 허용하지 않으므로 원격 세션에 로그인하고 시작하는 경우에만 DPI 동기화가 수행됩니다. 원격 세션 중에 DPI 설정을 변경하는 경우 원격 데스크톱의 DPI 설정이 클라이언트 시스템의 새 DPI 설정과 일치하도록 로그아웃했다가 다시 로그인해야 합니다.

에이전트 DPI 설정은 Windows 레지스트리 `Computer\HKEY_CURRENT_USER\Control Panel\Desktop:LogPixels`에 있습니다.

---

**참고** 시스템 DPI 설정이 기본 모니터의 DPI 설정과 동일하지 않을 수 있습니다. 예를 들어 기본 모니터를 닫았으며 시스템이 기본 모니터와는 다른 DPI 설정을 갖는 외부 디스플레이로 전환되는 경우 시스템 DPI 설정은 이전에 닫은 기본 모니터의 DPI 설정과 여전히 동일합니다.

---

이 버전의 클라이언트는 Horizon Agent 버전 7.8 ~ 2006에서 제공되는 연결당 DPI 동기화 에이전트 그룹 정책 설정을 지원하지 않습니다.

DPI 동기화 그룹 정책 설정에 대한 자세한 내용은 Horizon Agent 버전에 대한 "Horizon에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

## 가상 데스크톱에 대해 지원되는 게스트 운영 체제

가상 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 2012 R2(데스크톱으로 구성)
- Windows Server 2016(데스크톱으로 구성)
- Windows Server 2019(데스크톱으로 구성)

---

**참고** 데스크톱으로 구성된 Windows Server 시스템에서 모니터당 DPI 동기화 기능은 지원되지 않습니다.

---

## 게시된 데스크톱 및 게시된 애플리케이션에 대해 지원되는 RDS 호스트

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

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

---

**참고** RDS 호스트의 경우 모니터당 DPI 동기화 기능이 지원되지 않습니다. 이 제한은 VM 호스팅된 애플리케이션 기능을 사용하여 데스크톱 풀에서 실행되는 게시된 애플리케이션에는 적용되지 않습니다

---

## 외부 키보드 및 기타 입력 디바이스

원격 데스크톱 및 게시된 애플리케이션에서 iPad 키보드 도크 및 Apple 무선 키보드(Bluetooth) 외부 키보드를 사용할 수 있습니다. iPad Pro에서 Apple Pencil을 포인터 디바이스로 사용할 수 있습니다. 이 기능을 지원하는 모든 iOS 디바이스에서 Swiftpoint GT 마우스를 사용할 수 있습니다. iPadOS 13.4부터 iPad에서 외부 마우스를 사용할 수 있습니다.

## 외부 키보드를 Horizon Client에서 사용하도록 설정

Horizon Client는 iPad 키보드 도크 외부 키보드를 자동으로 감지합니다.

원격 데스크톱이나 게시된 애플리케이션에서 Apple 무선 키보드(Bluetooth)를 사용하려면 해당 키보드를 iPad와 연결합니다. iPad가 무선 키보드를 감지하도록 하려면 세 손가락으로 동시에 화면을 누르거나 Horizon Client 도구의 **키보드** 버튼을 누릅니다. iPad가 Apple 무선 키보드(Bluetooth) 키보드를 감지하도록 하려는 경우 분리식 키보드 모드에서 화면 키보드를 사용하지 마십시오.

iPad가 Apple 무선 키보드(Bluetooth)를 감지한 후에는 Horizon Client 도구 또는 세 손가락 누르기를 사용하여 화면 키보드를 표시할 수 없습니다. 이러한 기능을 사용하려면 Eject 키를 눌러 외부 키보드를 비활성화합니다.

---

**참고** Apple 무선 키보드(Bluetooth)를 사용하면 원격 데스크톱에서 일본어 전자 물결표를 올바르게 입력하지 못합니다.

---

## iPad에서 마우스 사용

iPadOS 13.4 이상에서는 외부 마우스를 원격 데스크톱 및 게시된 애플리케이션에서 사용할 수 있습니다. 블루투스 및 USB 마우스 모두 지원됩니다.

Apple Magic Mouse 및 Apple Magic Trackpad의 경우 2세대 이상 디바이스만 사용하십시오. 1세대 디바이스는 부분적으로만 지원됩니다.

왼손잡이 사용자의 경우 다음 권장 사항을 따르십시오.

- 원격 데스크톱에서 왼손잡이 모드를 사용하도록 설정한 경우에는 Horizon Client에서 **왼손 사용자 모드** 옵션을 항상 사용하도록 설정합니다. [좌우를 바꾼 마우스 버튼을 지원하도록 Horizon Client 구성](#)의 내용을 참조하십시오.
- 물리적 마우스에서 왼손 사용자 모드를 사용하려면 iPad 설정에서 왼손 모드를 구성합니다. 원격 데스크톱에서 왼손 사용자 모드가 사용하도록 설정되어 있는지 여부에 관계없이 iPad 설정을 사용해야 합니다.

## 국제 키보드 사용

한국어, 영어, 일본어, 프랑스어, 독일어, 중국어 간체, 중국어 번체 및 스페인어 문자를 입력할 수 있습니다.

한국어 및 일본어 IME(입력기)를 사용하는 원격 데스크톱의 경우 iOS 디바이스에서 영어 키보드를 사용합니다. 한국어 또는 일본어 키보드를 사용하는 경우 원격 데스크톱 Windows IME 영어/한국어 또는 영어/일본어 모드가 iOS 키보드 로케일과 동기화되지 않습니다.

## iPad에서 Apple Pencil 사용

iPad를 사용하면 원격 데스크톱 및 게시된 애플리케이션에서 Apple Pencil을 사용할 수 있습니다. 전체 기능을 사용하려면 원격 데스크톱 또는 게시된 애플리케이션에 연결할 때 VMware Blast 디스플레이 프로토콜을 사용합니다. PCoIP 디스플레이 프로토콜을 사용할 경우 Apple Pencil은 손가락 터치와 동일한 방식으로 동작합니다.

## Horizon Client에서 작동하도록 Swiftpoint GT 마우스 설정

원격 데스크톱 및 게시된 애플리케이션에서 작동하도록 Swiftpoint GT 마우스를 설정해야 합니다. [Horizon Client에서 Swiftpoint GT 마우스 사용](#)의 내용을 참조하십시오.

## Horizon Client에서 Swiftpoint GT 마우스 사용

Swiftpoint GT 마우스가 있는 경우 Horizon Client에서 원격 데스크톱 및 게시된 애플리케이션과 함께 작동하도록 설정할 수 있습니다.

사전 요구 사항

- Swiftpoint GT 마우스를 켭니다.
- 클라이언트 디바이스에서 Bluetooth를 켭니다.

절차

- 1 Horizon Client 창 하단의 **설정**을 누릅니다.
- 2 [설정] 창에서 **마우스**를 누릅니다.
- 3 **Swiftpoint GT 마우스**를 누르고 옵션을 켜기로 전환합니다.

Horizon Client에 Swiftpoint GT 마우스가 표시되고 이 마우스에 연결하는 옵션이 표시됩니다.

Bluetooth가 켜져 있지 않으면 Horizon Client는 마우스와 클라이언트 디바이스를 연결하기 전에 iOS 설정으로 이동한 후 Bluetooth를 켜라는 메시지를 표시합니다.

- 4 (선택 사항) Horizon Client에서 Swiftpoint GT 마우스를 사용하는 방법에 대한 자세한 내용을 보려면 <http://www.swiftpoint.com/vmware> 링크를 클릭합니다.

결과

마우스를 디바이스와 연결하고 나면 마우스 동작이 Horizon Client로 여는 원격 데스크톱과 게시된 애플리케이션으로 리디렉션됩니다.

## 실시간 오디오-비디오 기능 사용

실시간 오디오-비디오 기능을 통해 원격 데스크톱 또는 게시된 애플리케이션에서 클라이언트 디바이스의 기본 제공 카메라 및 마이크를 사용할 수 있습니다. 실시간 오디오-비디오는 표준 디바이스에서 Skype, WebEx 및 Google Hangout과 같은 표준 회의 애플리케이션과 함께 사용할 수 있습니다.

실시간 오디오-비디오 기능은 클라이언트 디바이스에 Horizon Client를 설치하면 기본적으로 사용 설정됩니다.

원격 데스크톱 및 게시된 애플리케이션에 대한 실시간 오디오-비디오 기능 설정에 대한 내용은 "Horizon Client에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

카메라 또는 마이크를 처음 사용하면 Horizon Client에서 카메라 또는 마이크 액세스 권한을 요청합니다. 마이크 또는 카메라 사용 권한을 부여해야 원격 데스크톱 또는 게시된 애플리케이션에서 사용할 수 있습니다. iOS 설정 애플리케이션에서 Horizon Client에 대한 마이크 개인 정보 보호 설정을 변경하여 마이크 액세스 권한을 사용하거나 사용하지 않도록 설정할 수 있습니다. iOS 설정 애플리케이션에서 Horizon Client에 대한 카메라 개인 정보 보호 설정을 변경하여 카메라 액세스 권한을 사용하거나 사용하지 않도록 설정할 수 있습니다. 마이크 및 카메라에 대한 액세스를 거부하면 Horizon Client는 실시간 오디오-비디오 기능을 사용하지 않도록 설정합니다.

Horizon Client가 백그라운드 모드인 경우(예: 다른 애플리케이션으로 전환한 경우) Horizon Client는 마이크 및 카메라에 대한 제어 권한을 포기합니다.

**참고** Horizon Client는 사용자가 클라이언트 디바이스를 회전할 때 프레젠테이션 모드에서 원격 데스크톱 방향을 조정하지 않으므로, 사용자가 클라이언트 디바이스를 회전할 때 실시간 오디오-비디오 기능이 카메라 방향을 조정하지 않습니다.

클라이언트 디바이스에 전면 및 후면 카메라가 둘 다 있는 경우 원격 데스크톱 또는 게시된 애플리케이션에 사용할 카메라를 선택할 수 있습니다. 사용할 비디오 해상도를 선택할 수도 있습니다. Horizon Client에서 이러한 카메라 설정을 구성하는 방법에 대한 자세한 내용은 [실시간 오디오-비디오 기능의 카메라 설정 구성](#)을 참조하십시오.

## 실시간 오디오-비디오 기능의 카메라 설정 구성

실시간 오디오-비디오 기능을 통해 원격 데스크톱 또는 게시된 애플리케이션에서 클라이언트 디바이스의 기본 제공 카메라를 사용할 수 있습니다. 클라이언트 디바이스에 전면 및 후면 카메라가 둘 다 있는 경우 원격 데스크톱 또는 게시된 애플리케이션에 사용할 카메라를 선택할 수 있습니다. 사용할 비디오 해상도를 선택할 수도 있습니다.

### 사전 요구 사항

비디오 해상도를 변경하려면 원격 데스크톱 또는 게시된 애플리케이션에 연결되어 있지 않아야 합니다.

### 절차

**1** Horizon Client에서 **설정**을 열고 **카메라**를 누릅니다.

- 원격 데스크톱이나 게시된 애플리케이션에 연결되지 않은 경우에는 Horizon Client 창 하단에서 **설정**을 누릅니다.
- 원격 데스크톱이나 게시된 애플리케이션에 연결되어 있는 경우에는 Horizon Client 도구 윗형 메뉴에서 **설정(톱니)** 아이콘을 누릅니다.

**2** 실시간 오디오-비디오 기능을 사용할 카메라를 선택하려면 **전면** 또는 **후면**을 누릅니다.

**3** 비디오 해상도를 설정하려면 비디오 해상도 설정 중 하나를 선택합니다.

원격 데스크톱 또는 게시된 애플리케이션에 연결되어 있으면 비디오 해상도를 변경할 수 없습니다.

기본 설정을 선택하면 비디오 해상도는 원격 데스크톱에 대한 **해상도 - 기본 이미지 해상도 너비(픽셀 단위)** 및 **해상도 - 기본 이미지 해상도 높이(픽셀 단위)**를 기준으로 지정됩니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서의 "실시간 오디오-비디오 그룹 정책 설정"을 참조하십시오. **높음, 중간** 또는 **낮음**을 선택하는 경우 원격 데스크톱의 비디오 해상도가 재정의됩니다.

## 좌우를 바꾼 마우스 버튼을 지원하도록 Horizon Client 구성

원격 데스크톱에서 주 및 보조 마우스 버튼이 전환되면 좌우를 바꾼 마우스 버튼을 지원하도록 Horizon Client를 구성할 수 있습니다.

주 마우스 버튼이 오른쪽 버튼이 되도록 원격 데스크톱 내에서 마우스 속성을 설정할 경우(예: 왼손잡이 사용자), Horizon Client의 **왼손 사용자 모드** 옵션을 켜야 합니다. 마우스 버튼의 좌우를 바꿀 때 이 옵션을 켜지 않을 경우, 한 번 누르면 보조 마우스 버튼의 클릭과 같은 역할을 하게 됩니다. 예를 들어, 한 번 누르면 텍스트를 선택하거나 커서를 삽입하는 것이 아니라 컨텍스트 메뉴가 표시될 수 있습니다.

### 절차

- ◆ 이미 원격 데스크톱에 연결된 경우 다음 단계를 수행하십시오.
  - a Horizon Client 도구 원형 메뉴 아이콘을 눌러서 확장하고 **설정(톱니)** 아이콘을 눌러서 [설정] 창을 엽니다.
  - b [설정] 창의 **터치**를 누릅니다.
  - c 옵션을 켜려면 **왼손 사용자 모드**를 누릅니다.
  - d **완료**를 눌러서 [설정] 창을 닫습니다.
- ◆ 원격 데스크톱에 연결되지 않은 경우 다음 단계를 수행하십시오.
  - a Horizon Client 창 하단의 **설정**을 누릅니다.
  - b [설정] 창의 **터치**를 누릅니다.
  - c 옵션을 켜려면 **왼손 사용자 모드**를 누릅니다.

### 결과

이제 한 번 누르면 주 마우스 버튼으로 클릭하는 것과 같은 역할을 하게 됩니다.

## 텍스트와 이미지 복사 및 붙여넣기

기본적으로 iOS 디바이스에서 원격 데스크톱 또는 게시된 애플리케이션으로 복사하여 붙여넣을 수 있습니다. 원격 데스크톱 또는 게시된 애플리케이션에서 iOS 디바이스로 또는 두 개의 원격 데스크톱 또는 게시된 애플리케이션 간에 복사하여 붙여넣을 수도 있습니다. 단, Horizon 관리자가 이러한 기능을 사용하도록 설정해야 합니다. 지원되는 파일 형식에는 일반 텍스트, 이미지 및 RTF(서식 있는 텍스트)가 포함됩니다.

iOS 디바이스의 클립보드에 복사한 데이터는 원격 데스크톱에 로그인할 때 원격 데스크톱의 클립보드에 복사됩니다. 원격 데스크톱에 로그인하면 원격 데스크톱의 클립보드에 복사한 데이터가 iOS 디바이스의 클립보드에 복사됩니다.

복사하여 붙여넣기 기능에는 다음과 같은 제한 사항이 있습니다.

- RTF 데이터에 이미지가 포함되어 있으면 Horizon Client가 원격 데스크톱의 클립보드에 있는 RTF 데이터를 iOS 디바이스의 클립보드에 있는 데이터와 동기화할 때 이미지가 손실됩니다.
- 텍스트 및 RTF 데이터의 합계가 최대 클립보드 크기 미만을 사용하는 경우 서식이 지정된 텍스트를 붙여넣습니다. 종종 RTF 데이터를 자를 수 없는 경우도 있습니다. 텍스트 및 서식에서 최대 클립보드 크기 이상을 사용하는 경우 RTF 데이터가 폐기되고 일반 텍스트가 붙여넣어집니다. 서식이 지정된 모든 텍스트를 한 번의 작업으로 모두 선택하여 붙여넣을 수 없는 경우 각 작업에서 더 적은 양을 복사 및 붙여넣어야 합니다.
- 클립보드 크기를 초과하지 않더라도 특정 이미지를 복사하여 붙여넣지 못할 수도 있습니다. 이 문제는 Horizon Client에서 이미지를 PNG 형식으로 변환하고 PNG 이미지가 클립보드 크기를 초과하는 경우에 발생합니다. Horizon Client는 복사하여 붙여넣기 작업 중에 모든 이미지를 PNG 형식으로 변환합니다.

Horizon 관리자는 복사 및 붙여넣기 작업이 iOS 디바이스에서 원격 데스크톱이나 게시된 애플리케이션으로만 허용, 원격 데스크톱이나 게시된 애플리케이션에서 iOS 디바이스로만 허용, 둘 다 허용 또는 둘 다 허용되지 않도록 이 기능을 구성할 수 있습니다.

Horizon 관리자는 Horizon Agent와 관련된 그룹 정책을 설정하여 클립보드 크기 변경을 비롯한 복사하여 붙여넣기 동작을 구성할 수 있습니다. 기본 클립보드 크기는 1MB입니다. 클립보드는 최대 16MB의 데이터를 수용할 수 있습니다. Horizon Server 및 Agent 버전에 따라, Horizon 관리자는 그룹 정책을 사용하여 복사 및 붙여넣기 작업 동안의 클립보드 형식을 제한하거나 스마트 정책을 사용할 수도 있습니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

## 로깅 복사 및 붙여넣기 작업

클립보드 감사 기능을 사용하도록 설정하면 Horizon Agent는 복사 및 붙여넣기 기능에 대한 정보를 에이전트 시스템의 이벤트 로그에 기록합니다. 클립보드 감사 기능은 기본적으로 사용되지 않도록 설정됩니다.

클립보드 감사 기능을 사용하도록 설정하려면 **클립보드 감사 구성** 그룹 정책 설정을 구성해야 합니다.

필요에 따라 **클라이언트가 감사를 지원하지 않을 때 클라이언트 측으로의 클립보드 리디렉션을 차단할지 여부** 그룹 정책 설정을 구성하여 클립보드 감사 기능을 지원하지 않는 클라이언트로의 클립보드 리디렉션을 차단할지 여부를 지정할 수 있습니다.

클립보드 리디렉션에 대한 그룹 정책 설정에 대한 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

이 기능을 사용하려면 에이전트 시스템에 Horizon Agent 7.7 이상이 필요합니다.

복사 및 붙여넣기 작업에 대한 정보가 기록되는 이벤트 로그를 VMware Horizon RX 감사라고 합니다. 예 이전트 시스템에서 이벤트 로그를 보려면 Windows 이벤트 뷰어를 사용합니다. 중앙 위치에서 이벤트 로그를 보려면 VMware Log Insight 또는 Windows 이벤트 수집기를 구성합니다. Log Insight에 대한 내용은 <https://docs.vmware.com/kr/vRealize-Log-Insight/index.html>을 참조하십시오. Windows 이벤트 수집기에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

## 텍스트 및 이미지 끌어오기

iOS 11 이상을 실행하는 iPad가 있는 경우 클라이언트 디바이스의 텍스트 및 이미지를 원격 데스크톱의 게시된 애플리케이션 또는 열려 있는 애플리케이션으로 끌어올 수 있습니다. 예를 들어, iPad에서 Safari의 텍스트를 원격 데스크톱의 워드패드 애플리케이션에 끌어서 놓을 수 있습니다. 일반 텍스트 및 RTF(서식 있는 텍스트 형식) 텍스트가 모두 지원됩니다.

Horizon 관리자는 Horizon Agent와 관련된 그룹 정책을 설정하여 클립보드 크기 변경을 비롯한 끌어서 놓기 동작을 구성할 수 있습니다. 기본 클립보드 크기는 1MB입니다. 클립보드는 최대 16MB의 데이터를 수용할 수 있습니다. Horizon Server 및 Agent 버전에 따라, 관리자는 그룹 정책을 사용하여 끌어서 놓기 작업 동안의 클립보드 형식을 제한하거나 스마트 정책을 사용할 수도 있습니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

이 기능의 제한 사항은 다음과 같습니다.

- 여러 이미지는 동시에 끌어올 수 없습니다.
- 텍스트와 이미지는 동시에 끌어올 수 없습니다.
- 클립보드 크기를 초과하지 않더라도 특정 이미지는 끌어오지 못할 수도 있습니다. 이 문제는 Horizon Client에서 이미지를 PNG 형식으로 변환하고 PNG 이미지가 클립보드 크기를 초과하는 경우에 발생합니다. Horizon Client는 끌어서 놓기 작업 중에 모든 이미지를 PNG 형식으로 변환합니다.
- 원격 데스크톱 또는 게시된 애플리케이션에서 클라이언트 디바이스로 텍스트 및 이미지를 끌어올 수 없습니다.

## 원격 데스크톱 또는 게시된 애플리케이션에서 인쇄

VMware Integrated Printing 기능을 사용하여 원격 데스크톱 또는 게시된 애플리케이션에서 AirPrint 지원 프린터로 인쇄할 수 있습니다.

이 기능을 사용하려면 VMware Integrated Printing 옵션을 사용하도록 설정한 가상 시스템이나 RDS 호스트에 Horizon Agent를 설치해야 합니다. 자세한 내용은 "Horizon에서 가상 데스크톱 설정" 또는 "Horizon에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.

원격 데스크톱 또는 게시된 애플리케이션에서 인쇄하는 과정은 두 단계로 진행됩니다. 예를 들어, Windows 애플리케이션에서 **파일 > 인쇄**를 선택하고 모바일 디바이스에 속하는 가상 프린터를 선택한 후 **인쇄**를 누릅니다. 그러면 디바이스의 [인쇄] 대화상자가 나타납니다. 디바이스의 [인쇄] 대화상자에서 **인쇄**를 다시 클릭합니다. 필요에 따라 사본 수, 용지 크기 등과 같은 로컬 인쇄 옵션을 선택할 수 있습니다.

Horizon 관리자는 **비데스크톱 클라이언트에 대해 프린터 리디렉션 사용 안 함** 그룹 정책 설정을 사용하여 VMware Integrated Printing 기능을 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

## 게시된 애플리케이션에서 문서 저장

Microsoft Word, 워드패드 등의 일부 게시된 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.

Horizon 관리자는 **원격 데스크톱 서비스 사용자 홈 디렉토리 설정**이라는 RDS 프로파일 그룹 정책 설정을 사용하여 문서 저장 위치를 지정할 수 있습니다. 자세한 내용은 "Horizon에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

## 여러 클라이언트 디바이스에서 게시된 애플리케이션의 다중 세션 사용

게시된 애플리케이션에 대해 다중 세션 모드를 사용하도록 설정하면 여러 다른 클라이언트 디바이스에서 서버에 로그인할 때 동일한 게시된 애플리케이션의 여러 세션을 사용할 수 있습니다.

예를 들어, 클라이언트 A에서 게시된 애플리케이션을 다중 세션 모드로 연 다음, 클라이언트 B에서 동일한 게시된 애플리케이션을 열면, 게시된 애플리케이션이 클라이언트 A에서 열린 상태로 남아 있고 게시된 애플리케이션의 새 세션이 클라이언트 B에서 열립니다. 비교해보면 다중 세션 모드가 사용되지 않도록 설정된 경우(단일 세션 모드) 클라이언트 A에서 게시된 애플리케이션 세션의 연결이 끊어졌다가 클라이언트 B에서 다시 연결됩니다.

다중 세션 모드 기능에는 다음과 같은 제한 사항이 있습니다.

- 다중 세션 모드는 비즈니스용 Skype 등과 같이 다중 인스턴스를 지원하지 않는 애플리케이션에는 작동하지 않습니다.
- 다중 세션 모드에서 게시된 애플리케이션을 사용하는 동안 애플리케이션 세션 연결이 해제되면 자동으로 로그오프되고 저장되지 않은 모든 데이터는 손실됩니다.

### 사전 요구 사항

Horizon 관리자는 애플리케이션 폴에 대해 다중 세션 모드를 사용하도록 설정해야 합니다. Horizon 관리자가 허용하지 않으면 사용자는 게시된 애플리케이션에 대한 다중 세션 모드를 수정할 수 없습니다.

"Horizon에서 게시된 데스크톱 및 애플리케이션 설정"의 내용을 참조하십시오. 이 기능에는 Horizon 7 버전 7.7 이상이 필요합니다.

### 절차

- 1 서버에 연결합니다.

**2** Horizon Client 창 하단의 **설정**을 누르고 **다중 실행**을 누릅니다.

다중 세션 모드에서 사용할 수 있는 게시된 애플리케이션이 없는 경우 **다중 실행** 설정이 표시되지 않습니다.

**3** 게시된 애플리케이션을 다중 세션 모드에서 사용하려면 게시된 애플리케이션 이름 옆에 있는 토글을 눌러 [설정]으로 전환합니다.

Horizon 관리자가 게시된 애플리케이션에 대해 다중 세션 모드를 적용하면 이 설정을 변경할 수 없습니다.

## 멀티태스킹

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

Horizon Client는 다른 애플리케이션으로 전환할 때 데이터 전송을 일시 중단합니다. Horizon Client로 다시 전환하면 데이터 전송이 재개됩니다.

기본적으로 Horizon Client는 iOS 9.0 이상 디바이스에서 최대 3분 동안 백그라운드로 실행됩니다. 3분 후에 Horizon Client를 재개하고 사용자 자격 증명을 입력하지 않고도 이전 원격 데스크톱 또는 게시된 애플리케이션 세션을 계속 사용할 수 있습니다. 서버 세션 시간 초과 또는 유효 세션 시간 초과에 해당되는 경우에만 자격 증명을 다시 입력하면 됩니다.

## 셀룰러 데이터 경고 메시지 표시하지 않음

Horizon Client에서 셀룰러 데이터 연결을 사용 중인 것을 감지하면 네트워크 사용량 대화 상자가 나타나서 원격 데스크톱 또는 게시된 애플리케이션 연결이 데이터 요금제의 상당 부분을 사용할 수 있다고 알려줍니다.

네트워크 사용량 대화 상자는 서버에 연결하고 원격 데스크톱 또는 게시된 애플리케이션에 연결을 시도한 후, 최근 원격 데스크톱 또는 게시된 애플리케이션 바로 가기를 누른 후 및 게시된 애플리케이션에 연결하고 Unity Touch 사이드바에서 다른 게시된 애플리케이션 또는 원격 데스크톱을 시작하려고 시도한 후에 나타납니다. 네트워크 사용량 대화 상자는 Horizon Client를 시작할 때만 나타납니다.

네트워크 사용량 대화상자가 나타난 후 이 대화상자가 표시되지 않도록 설정할 수 있습니다. 또한 네트워크 사용량 대화 상자를 항상 표시하지 않도록 옵션을 설정할 수도 있습니다.

### 절차

- ◆ Horizon Client에서 네트워크 사용량 대화상자가 나타난 후 이를 표시하지 않으려면 네트워크 사용량 대화상자에서 **다시 알리지 않음**을 누릅니다.
- ◆ 네트워크 사용 대화 상자를 항상 표시하지 않도록 옵션을 설정하려면 Horizon Client 창 하단에서 **설정**을 누르고 **셀룰러 데이터 경고** 옵션을 끄기로 전환합니다.

## 화면 활성화 유지

기본적으로 Horizon Client는 iOS **자동 잠금** 옵션에 설정된 간격이 만료되면 백그라운드 상태가 됩니다. **자동 잠금** 간격과 관계없이 Horizon Client를 포그라운드 상태로 유지하도록 Horizon Client 설정을 구성할 수 있습니다.

프레젠테이션 모드를 사용하는 경우 이 기능을 사용하도록 설정할 필요가 없습니다. 프레젠테이션 모드에서는 화면이 항상 활성화 상태를 유지합니다.

### 절차

- 1 원격 데스크톱 또는 게시된 애플리케이션에 연결합니다.
- 2 Horizon Client 도구 원형 메뉴에서 **설정**(톱니) 아이콘을 누릅니다.
- 3 **화면 활성화 유지**를 누릅니다.
- 4 **화면 활성화 유지** 옵션을 눌러 전환합니다.
- 5 **완료**를 눌러서 [설정] 창을 닫습니다.

## PCoIP 클라이언트 측 이미지 캐시

PCoIP 클라이언트 측 이미지 캐시에는 클라이언트의 이미지 내용이 저장되어 데이터 재전송을 방지합니다. 이 기능으로 대역폭 사용량이 감소합니다.

PCoIP 이미지 캐시는 공간적 및 일시적 중복성을 캡처합니다. 예를 들어 PDF 문서를 아래쪽으로 스크롤하면 창 아래쪽에 새 내용이 나타나고 창 위쪽의 기존 내용은 사라집니다. 나머지 콘텐츠는 일정하게 유지되며 위로 이동됩니다. PCoIP 이미지 캐시는 공간적 및 일시적 중복성을 감지할 수 있습니다.

스크롤할 때 클라이언트로 보내는 표시 정보는 주로 일련의 캐시 색인이므로 이미지 캐시를 사용하면 대역폭이 크게 절감됩니다. 이러한 효율적인 스크롤은 LAN과 WAN 모두에서 유용합니다.

- 대역폭의 제한을 상대적으로 덜 받는 LAN에서는 클라이언트 측 이미지 캐싱을 사용하면 대역폭이 크게 절감됩니다.
- WAN에서는 사용 가능한 대역폭 제한 이내로 유지해야 하기 때문에 클라이언트 측 캐싱을 사용하지 않으면 스크롤 성능이 저하됩니다. WAN에서 클라이언트 측 캐싱을 사용하면 대역폭이 절감되며 부드럽고 응답성이 뛰어난 스크롤 환경이 보장됩니다.

클라이언트 측 캐싱을 사용할 경우 클라이언트는 이전에 전송한 디스플레이 일부를 저장합니다. 캐시 크기는 사용 가능한 RAM의 절반입니다. RAM의 용량이 50MB 미만일 경우 캐시 크기는 50MB입니다.

# 문제 해결

# 5

원격 데스크톱 또는 게시된 애플리케이션을 다시 시작 또는 재설정하거나, Horizon Client를 다시 설치하여 대부분의 Horizon Client 문제를 해결할 수 있습니다.

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

본 장은 다음 항목을 포함합니다.

- 원격 데스크톱 다시 시작
- 원격 데스크톱 또는 게시된 애플리케이션 재설정
- 로깅 정보를 수집 및 VMware에 전송
- VMware에 Horizon Client 충돌 데이터 보고
- Horizon Client 응답 중지 또는 원격 데스크톱 작동 중지
- 프록시 사용 시 연결 문제
- Workspace ONE 모드에서 서버에 연결

## 원격 데스크톱 다시 시작

원격 데스크톱 운영 체제가 더 이상 응답하지 않을 경우 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 원격 데스크톱 운영 체제에 표시됩니다.

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

데스크톱 다시 시작 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 "Horizon에서 가상 데스크톱 설정" 또는 "Horizon에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.

### 절차

- 1 서버에 연결하려면 창 하단에 있는 **서버**(클라우드 아이콘)를 누르고 서버 아이콘을 누릅니다.
- 2 메시지가 표시되면 RSA 사용자 이름/암호나 Active Directory 사용자 이름/암호 또는 둘 다를 제공합니다.

- 3 컨텍스트 메뉴가 나타날 때까지 원격 데스크톱 바로 가기를 길게 터치합니다.
- 4 컨텍스트 메뉴에서 **다시 시작**을 누릅니다.

#### 결과

원격 데스크톱의 운영 체제가 다시 시작되고 클라이언트 연결이 끊어진 후 원격 데스크톱에서 로그오프됩니다.

#### 다음에 수행할 작업

원격 데스크톱에 재연결을 시도하기 전에 시스템 다시 시작을 위해 적당한 시간 동안 기다려 주십시오.

원격 데스크톱을 다시 시작해도 문제가 해결되지 않으면 원격 데스크톱을 재설정해야 할 수 있습니다. [원격 데스크톱 또는 게시된 애플리케이션 재설정](#)의 내용을 참조하십시오.

## 원격 데스크톱 또는 게시된 애플리케이션 재설정

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

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

게시된 애플리케이션을 재설정하면 저장되지 않은 데이터를 저장하지 않고 애플리케이션이 종료됩니다. 다른 RDS 서버 팜의 애플리케이션을 비롯하여 열려 있는 모든 게시된 애플리케이션이 닫힙니다.

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

원격 데스크톱 재설정 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 "[Horizon에서 가상 데스크톱 설정](#)" 또는 "[Horizon에서 게시된 데스크톱 및 애플리케이션 설정](#)" 문서를 참조하십시오.

#### 사전 요구 사항

Active Directory 사용자 이름/암호, RSA SecurID 사용자 이름/암호 또는 RADIUS 인증 사용자 이름/암호와 같은 로그인 자격 증명을 얻습니다.

#### 절차

- 1 창 하단에 있는 **서버**(클라우드 아이콘)를 누르고 서버 아이콘을 눌러 서버에 연결합니다.
- 2 메시지가 표시되면 RSA 사용자 이름/암호나 Active Directory 사용자 이름/암호 또는 둘 다를 제공합니다.
- 3 컨텍스트 메뉴가 나타날 때까지 원격 데스크톱 또는 게시된 애플리케이션 바로 가기를 길게 터치합니다.
- 4 컨텍스트 메뉴에서 **재설정**을 누릅니다.

## 결과

원격 데스크톱을 재설정하면 원격 데스크톱의 운영 체제가 다시 부팅되고 Horizon Client 연결이 끊어진 후 원격 데스크톱에서 로그오프됩니다. 게시된 애플리케이션을 재설정하면 모든 게시된 애플리케이션이 종료됩니다.

## 다음에 수행할 작업

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

## 로깅 정보를 수집 및 VMware에 전송

로그 정보를 수집하고 문제 해결을 위해 로그 파일을 VMware에 전송하도록 Horizon Client를 구성할 수 있습니다.

로그 수집이 활성화된 상태에서 Horizon Client가 예기치 않게 종료될 경우, Horizon Client를 다시 시작할 때 로그 파일을 VMware로 전송하라는 메시지가 표시됩니다.

로그 파일을 VMware로 전송할 경우 Horizon Client는 해당 클라이언트 디바이스에 구성된 이메일 계정에서 메시지를 전송하고 마지막 5개 로그 파일이 포함된 GZ 파일을 첨부합니다. 파일 이름에는 타임 스탬프가 포함됩니다(예: `Horizon_View_Client_logs_timestamp.log.gz`).

언제라도 로그 파일을 수동으로 검색 및 전송할 수 있습니다.

## Horizon Client 로그 수집 활성화

로그 수집을 사용하는 경우 Horizon Client는 VMware에서 Horizon Client 문제를 해결하는 데 유용한 정보가 포함된 로그 파일을 만듭니다.

로그 수집은 Horizon Client의 성능에 영향을 주므로 문제가 발생한 경우에만 로그 수집을 사용합니다.

### 사전 요구 사항

이메일 계정이 해당 디바이스에 구성되어 있는지 확인하십시오. Horizon Client에서는 이 이메일 계정을 사용하여 로그 파일을 보냅니다.

### 절차

- 1 이미 원격 데스크톱 또는 게시된 애플리케이션에 연결된 경우 다음 단계를 수행하십시오.
  - a Horizon Client 도구 원형 메뉴 아이콘을 눌러서 확장하고 **설정**(톱니) 아이콘을 눌러서 [설정] 창을 엽니다.
  - b [설정] 창의 **로그 수집**을 누릅니다.
  - c **로깅** 옵션을 눌러서 켜기로 전환합니다.
  - d **완료**를 눌러서 [설정] 창을 닫습니다.

- 2 원격 데스크톱 또는 게시된 애플리케이션에 연결되지 않은 경우 다음 단계를 수행하십시오.
  - a Horizon Client 창 하단에서 **설정**을 눌러서 [설정] 창을 엽니다.
  - b [설정] 창의 **로그 수집**을 누릅니다.
  - c **로깅** 옵션을 눌러서 켜기로 전환합니다.

#### 결과

로그 수집을 활성화하면 Horizon Client에서는 몇 가지 로그 파일을 생성합니다. Horizon Client가 예기치 않게 종료되었거나 종료 후 다시 시작될 때 이러한 로그 파일이 병합되어 하나의 GZ 파일로 압축됩니다. 로그를 보내도록 선택한 경우에는 Horizon Client에서 GZ 파일을 이메일 메시지에 첨부합니다.

실행 중인 원격 데스크톱에서 설정으로 전환하고, 로그 수집을 활성화한 후 다시 원격 데스크톱으로 전환하면 원격 데스크톱에 다시 연결해야 전체 로그 파일을 수집할 수 있습니다.

## 수동으로 Horizon Client 로그 파일 검색 및 전송

클라이언트 디바이스에서 Horizon Client 로그 수집이 사용하도록 설정되어 있는 경우 언제든지 로그 파일을 수동으로 검색하고 보낼 수 있습니다.

이 절차에서는 Horizon Client를 통해 로그 파일을 검색하고 보내는 방법을 설명합니다. 클라이언트 디바이스가 PC 또는 Mac에 연결된 경우 iTunes를 사용하여 로그 파일을 검색할 수도 있습니다.

#### 사전 요구 사항

- 이메일 계정이 해당 클라이언트 디바이스에 구성되어 있는지 확인하십시오. Horizon Client는 이 이메일 계정에서 로그 파일을 보냅니다.
- Horizon Client 로그 수집을 활성화합니다. [Horizon Client 로그 수집 활성화](#)의 내용을 참조하십시오.

#### 절차

- 1 Horizon Client에서 창 맨 위에 있는 이메일 아이콘을 누릅니다.
- 2 **받는 사람:** 줄에 이메일 수신자 주소를 입력하고 **전송**을 클릭하여 메시지를 보냅니다.  
클라이언트 디바이스에 구성된 이메일 계정이 **보낸 사람:** 줄에 표시됩니다.  
기존 GZ 로그 파일이 메시지에 첨부됩니다. Horizon Client는 GZ 로그 파일을 최대 5개까지 저장합니다. GZ 로그 파일 수가 5개를 초과할 경우 가장 오래된 파일이 삭제됩니다.

## Horizon Client 로그 수집 비활성화

로그 수집은 Horizon Client의 성능에 영향을 주므로 문제를 해결하는 경우 이외에는 로그 수집을 사용하지 않도록 설정하십시오.

## 절차

- 1 이미 원격 데스크톱 또는 게시된 애플리케이션에 연결된 경우 다음 단계를 수행하십시오.
  - a Horizon Client 도구 원형 메뉴 아이콘을 눌러서 확장하고 **설정(톱니)** 아이콘을 눌러서 [설정] 창을 엽니다.
  - b [설정] 창의 **로그 수집**을 누릅니다.
  - c **로깅** 옵션을 눌러서 켜기로 전환합니다.
  - d **완료**를 눌러서 [설정] 창을 닫습니다.
- 2 원격 데스크톱 또는 게시된 애플리케이션에 연결되지 않은 경우 다음 단계를 수행하십시오.
  - a Horizon Client 창 하단에서 **설정**을 눌러서 [설정] 창을 엽니다.
  - b [설정] 창의 **로그 수집**을 누릅니다.
  - c **로깅** 옵션을 눌러서 켜기로 전환합니다.

## VMware에 Horizon Client 충돌 데이터 보고

VMware에 충돌 데이터를 보고하도록 Horizon Client를 구성할 수 있습니다.

### 절차

- 1 Horizon Client 창 하단의 **설정**을 누릅니다.
- 2 **충돌 보고**를 누릅니다.
- 3 **충돌 보고** 옵션을 눌러서 켜기 또는 끄기로 전환합니다.

이 설정은 기본적으로 사용하도록 설정됩니다.

### 결과

Horizon Client가 응답을 중지하는 경우 다음번에 Horizon Client가 시작될 때 충돌 로그 파일이 서버에 업로드됩니다.

## Horizon Client 응답 중지 또는 원격 데스크톱 작동 중지

Horizon Client가 응답 중지하거나 원격 데스크톱 작동이 중지됩니다.

### 문제

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

### 원인

서버가 올바르게 구성되고 올바른 방화벽 포트가 열려 있는 경우 문제의 원인은 일반적으로 Horizon Client 디바이스의 또는 원격 데스크톱 운영 체제와 관련이 있습니다.

### 해결책

- ◆ 원격 데스크톱 운영 체제가 멈출 경우 클라이언트 디바이스에서 Horizon Client를 사용하여 데스크톱을 재설정합니다.

Horizon 관리자가 데스크톱 재설정 기능을 사용하도록 설정한 경우에만 이 옵션을 사용할 수 있습니다.

- ◆ 클라이언트 디바이스에서 Horizon Client 애플리케이션을 제거했다가 다시 설치합니다.
- ◆ 원격 데스크톱 재설정 및 Horizon Client 재설치가 도움이 되지 않을 경우, Apple의 클라이언트 디바이스 사용 설명서에 설명된 대로 클라이언트 디바이스를 재설정할 수 있습니다.
- ◆ 서버 연결 시도 시 연결 오류가 발생하면 프록시 설정을 변경해야 할 수 있습니다.

## 프록시 사용 시 연결 문제

LAN에 연결되어 있는 동안 프록시를 사용하여 서버에 연결할 경우 가끔 오류가 발생합니다.

### 문제

원격 데스크톱에서 서버로 보안 연결을 사용하도록 Horizon 환경이 설정되어 있고 클라이언트 디바이스가 HTTP 프록시를 사용하도록 구성된 경우, 연결하지 못할 수 있습니다.

### 원인

Windows Internet Explorer와 달리, 클라이언트 장치에는 로컬 주소의 프록시를 우회하는 인터넷 옵션이 없습니다. 외부 주소를 찾아보는 데 HTTP 프록시를 사용하고, 내부 주소를 사용하여 서버에 연결할 경우, 연결을 설정하지 못했습니다라는 오류 메시지가 나타날 수 있습니다.

### 해결책

- ◆ 클라이언트 디바이스가 더 이상 프록시를 사용하지 않도록 프록시 설정을 제거하십시오.

## Workspace ONE 모드에서 서버에 연결

Horizon Client를 통해 직접 서버에 연결할 수 없으며, 원격 데스크톱 및 게시된 애플리케이션 사용 권한이 Horizon Client에 표시되지 않습니다.

### 문제

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

## 원인

Horizon 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.

## 해결책

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