

# Horizon 7에서 원격 데스크톱 톱 기능 구성

VMware Horizon 7 7.2



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

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

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

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

# 목차

## 1 Horizon 7에서 원격 데스크톱 기능 구성 7

## 2 원격 데스크톱 기능 구성 8

### Unity Touch 구성 8

#### Unity Touch 시스템 요구 사항 9

#### Unity Touch에 표시된 즐겨찾기 애플리케이션 구성 9

### 멀티캐스트 또는 유니캐스트 스트리밍을 위한 플래시 URL 리디렉션 구성 12

#### 플래시 URL 리디렉션 시스템 요구 사항 13

#### 플래시 URL 리디렉션 기능이 설치되어 있는지 확인 14

#### 멀티캐스트 또는 유니캐스트 스트림을 제공하는 웹 페이지 설정 15

#### 플래시 URL 리디렉션용 클라이언트 디바이스 설정 15

#### 플래시 URL 리디렉션 사용 안 함 또는 사용 16

### Flash 리디렉션 구성 17

#### Flash 리디렉션에 대한 시스템 요구 사항 18

#### Flash 리디렉션 설치 및 구성 19

#### Windows 레지스트리 설정을 사용하여 Flash 리디렉션 구성 21

### 실시간 오디오-비디오 구성 23

#### 실시간 오디오-비디오 구성 옵션 23

#### 실시간 오디오-비디오에 대한 시스템 요구 사항 24

#### USB 리디렉션 대신 실시간 오디오-비디오가 사용되는지 확인 25

#### 기본 웹캠 및 마이크 선택 26

#### 실시간 오디오-비디오 그룹 정책 설정 구성 34

#### 실시간 오디오-비디오 대역폭 37

### 스캐너 리디렉션 구성 38

#### 스캐너 리디렉션에 대한 시스템 요구 사항 38

#### 스캐너 리디렉션의 사용자 작업 39

#### 스캐너 리디렉션 그룹 정책 설정 구성 40

### 직렬 포트 리디렉션 구성 44

#### 직렬 포트 리디렉션에 대한 시스템 요구 사항 44

#### 직렬 포트 리디렉션의 사용자 작업 45

#### 직렬 포트 리디렉션 구성 지침 46

#### 직렬 포트 리디렉션 그룹 정책 설정 구성 47

#### USB-직렬 어댑터 구성 50

### Windows Media MMR(멀티미디어 리디렉션)에 대한 액세스 관리 51

#### Horizon 7에서 멀티미디어 리디렉션 사용 52

#### Windows Media MMR에 대한 시스템 요구 사항 52

#### 네트워크 지연 시간을 기반으로 Windows Media MMR을 사용할지 여부 결정 53

#### 클라이언트 드라이브 리디렉션에 대한 액세스 관리 54

그룹 정책을 사용하여 클라이언트 드라이브 리디렉션 사용 안 함	55
레지스트리 설정을 사용하여 클라이언트 드라이브 리디렉션 구성	55
비즈니스용 Skype 구성	57

### 3 URL 콘텐츠 리디렉션 구성 60

URL 콘텐츠 리디렉션 이해	60
URL 콘텐츠 리디렉션 요구 사항	61
Cloud Pod 아키텍처 환경에서 URL 콘텐츠 리디렉션 사용	61
URL 콘텐츠 리디렉션 기능이 있는 Horizon Agent 설치	62
에이전트에서 클라이언트로의 리디렉션 구성	62
GPO에 URL 콘텐츠 리디렉션 ADMX 템플릿 추가	62
URL 콘텐츠 리디렉션 그룹 정책 설정	63
URL 콘텐츠 리디렉션 규칙 생성을 위한 구문	65
에이전트에서 클라이언트로의 리디렉션 그룹 정책 예	66
클라이언트에서 에이전트로의 리디렉션 구성	67
URL 콘텐츠 리디렉션 기능이 있는 Windows용 Horizon Client 설치	67
vdmutil 명령줄 유틸리티 사용	68
로컬 URL 콘텐츠 리디렉션 설정 생성	69
전역 URL 콘텐츠 리디렉션 설정 생성	71
사용자 또는 그룹에 URL 콘텐츠 리디렉션 설정 할당	73
URL 콘텐츠 리디렉션 설정 테스트	74
URL 콘텐츠 리디렉션 설정 관리	75
그룹 정책 설정을 사용하여 클라이언트에서 에이전트로의 리디렉션 구성	76
URL 콘텐츠 리디렉션 제한	77
지원되지 않는 URL 콘텐츠 리디렉션 기능	77

### 4 원격 데스크톱 및 애플리케이션에서 USB 디바이스 사용 79

USB 디바이스 유형의 제한 사항	80
USB 리디렉션 설정 개요	81
네트워크 트래픽 및 USB 리디렉션	82
USB 디바이스에 대한 자동 연결	83
보안 Horizon 7 환경에 USB 디바이스 배포	84
모든 유형의 디바이스에 대한 USB 리디렉션 사용 안 함	84
특정 디바이스에 대해 USB 리디렉션을 사용하지 않도록 설정	85
로그 파일을 사용하여 문제 해결 및 USB 디바이스 ID 확인	87
USB 리디렉션 제어를 위한 정책 사용	87
복합 USB 디바이스를 위한 디바이스 분할 정책 설정 구성	88
USB 디바이스를 위한 필터 정책 설정 구성	91
USB 디바이스 제품군	95
Horizon Agent 구성 ADMX 템플릿에서의 USB 설정	95
USB 리디렉션 문제 해결	98

## 5 데스크톱 풀 및 애플리케이션 풀의 정책 구성 101

- Horizon Administrator에서 정책 설정 101
  - 전역 정책 설정 구성 102
  - 데스크톱 풀 정책 구성 102
  - 사용자를 위한 정책 구성 103
  - Horizon 7 정책 103
- 스마트 정책 사용 104
  - 스마트 정책 요구 사항 104
  - User Environment Manager 설치 104
  - User Environment Manager 구성 105
  - Horizon 스마트 정책 설정 105
  - 대역폭 프로파일 참조 106
  - Horizon 스마트 정책 정의에 조건 추가 107
  - User Environment Manager에 Horizon 스마트 정책 생성 109
- Active Directory 그룹 정책 사용 110
  - 원격 데스크톱의 OU 생성 110
  - 원격 데스크톱에 대해 루프백 처리를 사용하도록 설정 111
- Horizon 7 그룹 정책 관리 템플릿 파일 사용 111
- Horizon 7 ADMX 템플릿 파일 111
- Active Directory에 ADMX 템플릿 파일 추가 113
- Horizon Agent 구성 ADMX 템플릿 설정 114
  - 원격 데스크톱에 전송한 클라이언트 시스템 정보 121
  - Horizon 데스크톱에서 명령 실행 125
- PCoIP 정책 설정 125
  - PCoIP 일반 설정 126
  - PCoIP 클립보드 설정 134
  - PCoIP 대역폭 설정 137
  - PCoIP 키보드 설정 139
  - PCoIP 무손실 빌드 기능 140
- VMware Blast 정책 설정 141
  - VMware Blast에 대해 무손실 압축 사용 144
- 원격 데스크톱 서비스 그룹 정책 사용 145
  - RDS 디바이스 단위 CAL 스토리지 구성 145
  - Active Directory에 원격 데스크톱 서비스 ADMX 파일 추가 146
  - RDS 애플리케이션 호환성 설정 147
  - RDS 연결 설정 148
  - RDS 디바이스 및 리소스 리디렉션 설정 152
  - RDS 라이선싱 설정 156
  - RDS 프린터 리디렉션 설정 158
  - RDS 프로파일 설정 160
  - RDS 연결 서버 설정 163

RDS 원격 세션 환경 설정	167
RDS 보안 설정	173
RDS 세션 시간 제한	177
RDS 임시 폴더 설정	180
위치 기반 인쇄 설정	181
위치 기반 인쇄 그룹 정책 DLL 파일 등록	183
위치 기반 인쇄 그룹 정책 구성	183
위치 기반 인쇄 그룹 정책 설정 구문	184
Active Directory 그룹 정책 예제	186
Horizon 7 시스템을 위한 OU 생성	186
Horizon 7 그룹 정책에 대한 GPO 생성	187
GPO에 Horizon 7 ADMX 템플릿 파일 추가	188
원격 데스크톱에 대해 루프백 처리를 사용하도록 설정	189

## **6** Active Directory 그룹 정책 예제 191

Horizon 7 시스템을 위한 OU 생성	191
Horizon 7 그룹 정책에 대한 GPO 생성	192
GPO에 Horizon 7 ADMX 템플릿 파일 추가	193
원격 데스크톱에 대해 루프백 처리를 사용하도록 설정	194

# Horizon 7에서 원격 데스크톱 기능 구성

# 1

“Horizon 7에서 원격 데스크톱 기능 구성”에서는 가상 시스템 데스크톱 또는 RDS 호스트에서 Horizon Agent와 함께 설치되는 원격 데스크톱 기능을 구성하는 방법을 설명합니다. 정책을 구성하여 데스크톱 풀과 애플리케이션 풀, 시스템 및 사용자의 동작을 제어할 수도 있습니다.

## 대상

이 정보는 가상 시스템 데스크톱 또는 RDS 호스트에서 원격 데스크톱 기능 또는 정책을 구성하려는 모든 사용자를 위해 작성되었습니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영을 잘 아는 Windows 시스템 관리자를 대상으로 작성되었습니다.

## 원격 데스크톱 기능 구성

Horizon Agent와 함께 설치되는 특정 원격 데스크톱 기능은 코어 Horizon 7 릴리스뿐 아니라 기능 팩 업데이트 릴리스에서도 업데이트할 수 있습니다. 이러한 기능을 구성하여 최종 사용자의 원격 데스크톱 환경을 개선할 수 있습니다.

이러한 기능에는 HTML Access, Unity Touch, 플래시 URL 리디렉션, 실시간 오디오-비디오, Windows Media MMR(멀티미디어 리디렉션), USB 리디렉션, 스캐너 리디렉션 및 직렬 포트 리디렉션 등이 있습니다.

HTML Access에 대한 자세한 내용은 VMware Horizon Client 설명서 웹 페이지에 있는 "HTML Access 사용" 문서를 참조하십시오.

USB 리디렉션에 대한 자세한 내용은 [장 4 원격 데스크톱 및 애플리케이션에서 USB 디바이스 사용](#)을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [Unity Touch 구성](#)
- [멀티캐스트 또는 유니캐스트 스트리밍을 위한 플래시 URL 리디렉션 구성](#)
- [Flash 리디렉션 구성](#)
- [실시간 오디오-비디오 구성](#)
- [스캐너 리디렉션 구성](#)
- [직렬 포트 리디렉션 구성](#)
- [Windows Media MMR\(멀티미디어 리디렉션\)에 대한 액세스 관리](#)
- [클라이언트 드라이브 리디렉션에 대한 액세스 관리](#)
- [비즈니스용 Skype 구성](#)

### Unity Touch 구성

태블릿 및 스마트폰 사용자는 Unity Touch를 통해 Windows 애플리케이션 및 파일을 간편하게 찾아 보고 검색하고 열어보며, 즐겨찾기 애플리케이션 및 파일을 선택하고, 시작 메뉴 또는 작업 표시줄 없이도 실행되는 애플리케이션 간에 쉽게 전환할 수 있습니다. Unity Touch 사이드바에 나타나는 즐겨찾는 애플리케이션 기본 목록을 구성할 수 있습니다.

Unity Touch를 설치하면 **Unity Touch 활성화** 그룹 정책 설정을 구성하여 Unity Touch 기능을 활성화하거나 비활성화할 수 있습니다.



iOS 및 Android 디바이스용 VMware Horizon Client 설명서에서는 Unity Touch에서 제공하는 최종 사용자 기능에 대한 정보를 제공합니다.

## Unity Touch 시스템 요구 사항

Unity Touch를 지원하려면 Horizon Client를 설치한 Horizon Client 소프트웨어 및 모바일 디바이스가 특정 버전 요구 사항을 충족해야 합니다.

### Horizon 7 데스크톱

Unity Touch를 지원하려면 최종 사용자가 액세스하는 가상 시스템에 다음 소프트웨어가 설치되어 있어야 합니다.

- View Agent 6.0 이상을 설치하면 Unity Touch 기능이 설치됩니다. "Horizon 7에서 가상 데스크톱 설정" 문서에서 "가상 시스템에 View Agent 설치"를 참조하십시오.
- 운영 체제: Windows 7(32비트 또는 64비트), Windows 8(32비트 또는 64비트), Windows 8.1(32비트 또는 64비트), Windows Server 2008 R2, Windows Server 2012 R2 또는 Windows 10(32비트 또는 64비트)

### Horizon Client 소프트웨어

Unity Touch가 지원되는 Horizon Client 버전:

- iOS용 Horizon Client 2.0 이상
- Android용 Horizon Client 2.0 이상

### 모바일 디바이스 운영 시스템

Unity Touch가 지원되는 모바일 디바이스 운영 체제:

- iOS 5.0 이상
- Android 3(Honeycomb), Android 4(Ice Cream Sandwich), Android 4.1 및 4.2(Jelly Bean).

## Unity Touch에 표시된 즐겨찾기 애플리케이션 구성

태블릿 및 스마트폰 사용자는 Unity Touch 기능을 통해 Unity Touch 사이드바에서 Horizon 7 데스크톱 애플리케이션 또는 파일로 빠르게 이동할 수 있습니다. 편의를 위해 최종 사용자가 사이드바에 나타나는 즐겨찾기 애플리케이션을 지정할 수 있지만 관리자가 즐겨찾기 애플리케이션 기본 목록을 구성할 수 있습니다.

부동 할당 데스크톱 풀을 사용하는 경우, Active Directory에서 로밍 사용자 프로파일을 활성화하지 않으면 데스크톱에서 연결을 해제하는 경우 최종 사용자가 지정한 즐겨찾는 애플리케이션 및 즐겨찾는 파일이 사라집니다.

최종 사용자가 Unity Touch를 사용하도록 설정된 데스크톱에 처음 연결하면 즐겨찾기 애플리케이션 목록의 기본 목록이 그대로 남습니다. 그러나 사용자가 별도의 즐겨찾기 애플리케이션 목록을 구성하면 기본 목록은 무시됩니다. 사용자의 즐겨찾는 애플리케이션 목록은 사용자의 로밍 프로파일에 남아 있고 사용자가 부동 또는 전용 풀의 다른 시스템에 연결하면 사용할 수 있습니다.

즐거찾기 애플리케이션의 기본 목록을 생성한 상태에서 해당 애플리케이션 중 하나 이상이 Horizon 7 데스크톱 운영 체제에 설치되어 있지 않거나 해당 애플리케이션에 대한 경로가 [시작] 메뉴에 없는 경우, 해당 애플리케이션은 즐겨찾기 목록에 나타나지 않습니다. 이 동작을 사용하면 즐겨찾기 애플리케이션의 마스터 기본 목록 하나를 설정하여 서로 다른 애플리케이션 모음이 설치된 여러 가상 시스템 이미지에 적용할 있습니다.

예를 들어, Microsoft Office 및 Microsoft Visio가 한 가상 시스템에 설치되어 있고 Windows Powershell 및 VMware vSphere Client가 또 다른 가상 시스템에 설치되어 있는 경우 4개의 애플리케이션을 모두 포함하는 하나의 목록을 생성할 수 있습니다. 설치된 애플리케이션만 각 데스크톱에 기본 즐겨찾기 애플리케이션으로 나타납니다.

다양한 방법을 사용하여 즐겨찾기 애플리케이션에 대한 기본 목록을 지정할 수 있습니다.

- 데스크톱 풀에 있는 가상 시스템의 Windows 레지스트리에 값 추가
- Horizon Agent 설치 관리자에서 관리 설치 패키지 생성 및 가상 시스템에 패키지 배포
- 가상 시스템의 명령줄에서 Horizon Agent 설치 관리자 실행

---

**참고** Unity Touch는 애플리케이션 바로 가기가 **시작** 메뉴의 [프로그램] 폴더에 있다고 가정합니다. [프로그램] 폴더 외부에 바로 가기가 있을 경우 바로 가기 경로에 접두사 **Programs**를 붙입니다. 예를 들어, Windows Update.Ink는 ProgramData\Microsoft\Windows\Start Menu 폴더에 있다고 가정합니다. 이 바로 가기를 기본 즐겨찾기 애플리케이션으로 게시하려면 바로 가기 경로에 접두사 **Programs**를 붙입니다. 예: "Programs/Windows Update.Ink".

---

#### 사전 요구 사항

- 가상 시스템에 Horizon Agent가 설치되어 있는지 확인합니다.
- 가상 시스템에 대한 관리 권한이 있는지 확인합니다. 이 절차에서는 레지스트리 설정을 편집해야 할 수 있습니다.
- 부동 할당 데스크톱 풀이 있는 경우 Active Directory를 사용하여 로밍 사용자 프로파일을 설정합니다. Microsoft에서 제공한 지침을 따르십시오.

부동 할당 데스크톱 풀 사용자는 로그인할 때마다 즐겨찾는 애플리케이션 및 즐겨찾는 파일 목록을 볼 수 있습니다.

## 절차

- ◆ (선택 사항) Windows 레지스트리에 값을 추가하여 즐겨찾기 애플리케이션의 기본 목록을 생성합니다.

- regedit를 열고 HKLM\Software\VMware, Inc.\VMware Unity 레지스트리 설정으로 이동합니다.  
64비트 가상 시스템에서는 HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity 디렉토리로 이동합니다.
- FavAppList라는 문자열 값을 생성합니다.
- 기본 즐겨찾기 애플리케이션을 지정합니다.

다음 형식을 사용하여 **시작** 메뉴에서 사용되는 애플리케이션에 대한 바로 가기 경로를 지정합니다.

```
path-to-app-1|path-to-app-2|path-to-app-3|...
```

예 :

```
Programs/Accessories/Accessibility/Speech Recognition.Ink|Programs/VMware/VMware vSphere Client.Ink|
Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.Ink
```

- ◆ (선택 사항) Horizon Agent 설치 관리자에서 관리 설치 패키지를 생성하여 즐겨찾기 애플리케이션의 기본 목록을 생성합니다.

- 명령줄에서 다음 형식을 사용하여 관리 설치 패키지를 생성합니다.

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR="" 관리자 설치 패키지를 저장하는 네트워크
공유"" UNITY_DEFAULT_APPS="" 레지스트리에서 설정해야 하는 기본 즐겨찾기 애플리케이션의 목록""
```

예 :

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR="" VMware-installer-share\VMwareViewFeaturePack
W"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.Ink|Programs/Accessories/
System Tools/Character Map.Ink|Programs/Accessories/Windows PowerShell/Windows PowerShell.Ink|Programs/
Internet Explorer (64-bit).Ink|Programs/Google Chrome/Google Chrome.Ink|Programs/iTunes/iTunes.Ink|
Programs/Microsoft Office/Microsoft SharePoint Workspace 2010.Ink|Programs/PuTTY/PuTTY.Ink|Programs/
Skype/Skype.Ink|Programs/WebEx/Productivity Tools/WebEx Settings.Ink|""
```

- 조직에서 사용되는 표준 MSI(Microsoft Windows Installer) 배포 방법을 사용하여 네트워크 공유에서 데스크톱 가상 시스템에 관리 설치 패키지를 배포합니다.

- ◆ (선택 사항) 가상 시스템의 명령줄에서 직접 Horizon Agent 설치 관리자를 실행하여 즐겨찾기 애플리케이션의 기본 목록을 생성합니다.

다음 형식을 사용합니다.

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS="" 레지스트리에서 설정해야 하는 기본 즐겨찾기 애플리케이션의 목록""
```

**참고** 이 명령으로 Horizon Agent 설치와 즐겨찾기 애플리케이션의 기본 목록 지정을 동시에 실행할 수 있습니다. 이 명령을 실행하기 전에 Horizon Agent를 설치하지 않아도 됩니다.

## 다음에 수행할 작업

Windows 레지스트리를 편집하거나 명령줄에서 Horizon Agent를 설치하여 가상 시스템에서 이 작업을 직접 수행한 경우, 새로 구성된 가상 시스템을 배포해야 합니다. 스냅샷을 생성하거나 템플릿을 만들고 데스크톱 풀을 생성하거나 기존 풀을 재구성할 수 있습니다. 또는 Active Directory 그룹 정책을 생성하여 새 구성을 배포할 수 있습니다.

## 멀티캐스트 또는 유니캐스트 스트리밍을 위한 플래시 URL 리디렉션 구성

이제 고객은 Adobe Media Server 및 멀티캐스트 또는 유니캐스트를 사용하여 가상 데스크톱 인프라(VDI) 환경에서 라이브 비디오 이벤트를 전달할 수 있습니다. VDI 환경에서 멀티캐스트 또는 유니캐스트 라이브 비디오 스트림을 전달하려면 원격 데스크톱을 우회하여 미디어 소스에서 끝점으로 미디어 스트림을 직접 전송해야 합니다. 플래시 URL 리디렉션 기능은 ShockWave Flash(SWF) 파일을 가로채서 원격 데스크톱에서 클라이언트 끝점으로 리디렉션하여 이 기능을 지원합니다.

그러면 클라이언트의 로컬 플래시 미디어 플레이어를 사용하여 플래시 콘텐츠가 표시됩니다.

Adobe Media Server에서 클라이언트 끝점으로 플래시 콘텐츠를 직접 스트리밍하면 데이터 센터 ESXi 호스트에 대한 부하를 줄이고, 데이터 센터를 통해 추가 라우팅을 제거하고, 여러 클라이언트 끝에 플래시 콘텐츠를 동시에 스트리밍하는 데 필요한 대역폭을 줄여줍니다.

플래시 URL 리디렉션 기능은 웹 페이지 관리자에 의해 HTML 웹 페이지 내에 포함된 JavaScript를 사용합니다. 원격 데스크톱 사용자가 웹 페이지 내에서 지정된 URL 링크를 클릭할 때마다 JavaScript는 SWF 파일을 가로채서 원격 데스크톱 세션에서 클라이언트 끝점으로 리디렉션합니다. 그러면 끝점은 원격 데스크톱 세션 외부에서 로컬 Flash Projector를 열고 로컬로 미디어 스트림을 재생합니다.

플래시 URL 리디렉션을 구성하려면 HTML 웹 페이지 및 클라이언트 디바이스를 설정해야 합니다.

## 절차

### 1 플래시 URL 리디렉션 시스템 요구 사항

플래시 URL 리디렉션을 지원하려면 Horizon 7 배포가 특정 소프트웨어 및 하드웨어 요구 사항을 충족해야 합니다.

### 2 플래시 URL 리디렉션 기능이 설치되어 있는지 확인

이 기능을 사용하려면 먼저 가상 데스크톱에 플래시 URL 리디렉션 기능이 설치되어 실행 중인지 확인해야 합니다.

### 3 멀티캐스트 또는 유니캐스트 스트림을 제공하는 웹 페이지 설정

플래시 URL 리디렉션이 실행되도록 허용하려면, 멀티캐스트 또는 유니캐스트 스트림에 대한 링크를 제공하는 MIME HTML(MHTML) 웹 페이지에 JavaScript 명령을 포함시켜야 합니다. 사용자는 원격 데스크톱의 브라우저에 이러한 웹 페이지를 표시하여 비디오 스트림에 액세스합니다.

### 4 플래시 URL 리디렉션용 클라이언트 디바이스 설정

플래시 URL 리디렉션 기능은 원격 데스크톱에서 클라이언트 디바이스로 SWF 파일을 리디렉션합니다. 이러한 클라이언트 디바이스가 멀티캐스트 또는 유니캐스트 스트림에서 플래시 비디오를 재생하도록 허용하려면 클라이언트 디바이스에 해당 Adobe Flash Player가 설치되어 있는지 확인해야 합니다. 또한 미디어 소스에 대해 IP도 연결되어 있어야 합니다.

### 5 플래시 URL 리디렉션 사용 안 함 또는 사용

플래시 URL 리디렉션 기능은 `VDM_FLASH_URL_REDIRECTION=1` 속성을 사용하여 Horizon Agent를 자동 설치할 경우 사용하도록 설정됩니다. 해당 가상 시스템에서 Windows 레지스트리 키의 값을 설정하면 선택한 원격 데스크톱에서 플래시 URL 리디렉션 기능을 사용하지 않도록 설정하거나 다시 사용하도록 설정할 수 있습니다.

## 플래시 URL 리디렉션 시스템 요구 사항

플래시 URL 리디렉션을 지원하려면 Horizon 7 배포가 특정 소프트웨어 및 하드웨어 요구 사항을 충족해야 합니다.

### Horizon 7 데스크톱

- View Agent 6.0 이상을 자동 설치하는 동안 명령줄에 `VDM_FLASH_URL_REDIRECTION` 속성을 입력하면 플래시 URL 리디렉션을 설치할 수 있습니다. "Horizon 7에서 가상 데스크톱 설정" 문서에서 "Horizon Agent의 자동 설치 속성"을 참조하십시오.
- 데스크톱은 Windows 7 64비트 또는 32비트 운영 체제를 실행해야 합니다.
- 지원되는 데스크톱 브라우저에는 Internet Explorer 8, 9 및 10, Chrome 29.x, Firefox 20.x가 있습니다.

### 플래시 미디어 플레이어 및 ShockWave Flash(SWF)

Strobe Media Playback과 같이 적절한 플래시 미디어 플레이어를 웹 사이트에 통합해야 합니다. 웹 페이지에서 `multicastplayer.swf` 또는 `StrobeMediaPlayback.swf`를 사용하여 멀티캐스트 콘텐츠를 스트리밍할 수 있습니다. 라이브 유니캐스트 콘텐츠를 스트리밍하려면 `StrobeMediaPlayback.swf`를 사용해야 합니다. RTMP 스트리밍 및 HTTP 동적 스트리밍과 같이 지원되는 다른 기능에 대해 `StrobeMediaPlayback.swf`를 사용할 수도 있습니다.

### Horizon Client 소프트웨어

다음 Horizon Client 릴리스는 멀티캐스트 및 유니캐스트를 지원합니다.

- Linux 또는 최신 릴리스용 Horizon Client 2.2
- Windows용 Horizon Client 2.2 이상 릴리스

다음 Horizon Client 릴리스는 멀티캐스트만 지원합니다(유니캐스트는 지원하지 않음).

- Linux용 Horizon Client 2.0 또는 2.1
- Windows용 Horizon Client 5.4

### Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

- 플래시 URL 리디렉션은 x86 썬 클라이언트 디바이스에서 Linux용 Horizon Client를 실행하는 모든 운영 체제에서 지원됩니다. 이 기능은 ARM 프로세서에서 지원되지 않습니다.
- 플래시 URL 리디렉션은 Windows용 Horizon Client가 실행되는 모든 운영 체제에서 지원됩니다. 자세한 내용은 "Windows용 VMware Horizon Client 사용" 문서를 참조하십시오.
- Windows 클라이언트 디바이스에서는 Internet Explorer에 대해 Adobe Flash Player 10.1 이상을 설치해야 합니다.
- Linux 썬 클라이언트 디바이스의 경우, libexpat.so.0 및 libflashplayer.so 파일을 설치해야 합니다. [플래시 URL 리디렉션용 클라이언트 디바이스 설정](#)을 참조하십시오.

---

**참고** 플래시 URL 리디렉션을 사용하면 멀티캐스트 또는 유니캐스트 스트림이 조직의 방화벽 외부에 있을 수 있는 클라이언트 디바이스에 리디렉션됩니다. 클라이언트가 멀티캐스트 또는 유니캐스트 스트림을 시작하는 ShockWave Flash(SWF) 파일을 호스팅하는 Adobe Web 서버에 액세스할 수 있어야 합니다. 필요할 경우, 해당 포트를 열 수 있도록 방화벽을 구성하여 클라이언트 디바이스가 이 서버에 액세스할 수 있게 허용합니다.

---

## 플래시 URL 리디렉션 기능이 설치되어 있는지 확인

이 기능을 사용하려면 먼저 가상 데스크톱에 플래시 URL 리디렉션 기능이 설치되어 실행 중인지 확인해야 합니다.

멀티캐스트 또는 유니캐스트 리디렉션을 지원하고자 하는 모든 데스크톱에 플래시 URL 리디렉션 기능이 설치되어 있어야 합니다. Horizon Agent 설치 지침에 대해서는 "Horizon 7에서 가상 데스크톱 설정" 문서에서 "Horizon Agent의 자동 설치 속성"을 참조하십시오.

### 절차

- 1 PCoIP를 사용하는 원격 데스크톱 세션을 시작합니다.
- 2 작업 관리자를 엽니다.
- 3 데스크톱에서 ViewMPServer.exe 프로세스가 실행 중인지 확인하십시오.

## 멀티캐스트 또는 유니캐스트 스트림을 제공하는 웹 페이지 설정

플래시 URL 리디렉션이 실행되도록 허용하려면, 멀티캐스트 또는 유니캐스트 스트림에 대한 링크를 제공하는 MIME HTML(MHTML) 웹 페이지에 JavaScript 명령을 포함시켜야 합니다. 사용자는 원격 데스크톱의 브라우저에 이러한 웹 페이지를 표시하여 비디오 스트림에 액세스합니다.

또한 플래시 URL 리디렉션에 문제가 발생할 경우 최종 사용자에게 표시되는 영어 오류 메시지를 사용자 지정할 수 있습니다. 현지화된 오류 메시지를 최종 사용자에게 표시하려면 이 옵션 단계를 수행합니다. MHTML 웹 페이지에 현지화된 텍스트 문자열과 함께 `var vmwareScriptErrorMessage` 구성을 포함해야 합니다.

### 사전 요구 사항

MHTML 웹 페이지에 `swfobject.js` 라이브러리를 가져왔는지 확인하십시오.

### 절차

- 1 MHTML 웹 페이지에 `viewmp.js` JavaScript 명령을 포함시킵니다.

예: `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

- 2 (선택 사항) 최종 사용자에게 전송되는 플래시 URL 리디렉션 오류 메시지를 사용자 지정합니다.

예: `"var vmwareScriptErrorMessage=localized error message"`

- 3 `viewmp.js` JavaScript 명령을 포함시키고 선택적으로 플래시 URL 리디렉션 오류 메시지를 사용자 지정한 후 ShockWave Flash(SWF) 파일을 MHTML 웹 페이지로 가져옵니다.

사용자가 원격 데스크톱에 웹 페이지를 표시하면 `viewmp.js` JavaScript 명령이 원격 데스크톱에서 플래시 URL 리디렉션 메커니즘을 호출한 다음 이 메커니즘을 통해 데스크톱에서 호스팅 클라이언트 디바이스로 SWF 파일을 리디렉션합니다.

## 플래시 URL 리디렉션용 클라이언트 디바이스 설정

플래시 URL 리디렉션 기능은 원격 데스크톱에서 클라이언트 디바이스로 SWF 파일을 리디렉션합니다. 이러한 클라이언트 디바이스가 멀티캐스트 또는 유니캐스트 스트림에서 플래시 비디오를 재생하도록 허용하려면 클라이언트 디바이스에 해당 Adobe Flash Player가 설치되어 있는지 확인해야 합니다. 또한 미디어 소스에 대해 IP도 연결되어 있어야 합니다.

**참고** 플래시 URL 리디렉션을 사용하면 멀티캐스트 또는 유니캐스트 스트림이 조직의 방화벽 외부에 있을 수 있는 클라이언트 디바이스에 리디렉션됩니다. 클라이언트가 멀티캐스트 또는 유니캐스트 스트림을 시작하는 SWF 파일을 호스팅하는 Adobe Web 서버에 액세스할 수 있어야 합니다. 필요할 경우, 해당 포트를 열 수 있도록 방화벽을 구성하여 클라이언트 디바이스가 이 서버에 액세스할 수 있게 허용합니다.

## 절차

- ◆ 클라이언트 디바이스에 Adobe Flash Player를 설치합니다.

운영 체제	조치
<b>Windows</b>	Internet Explorer에 Adobe Flash Player 10.1 이상을 설치합니다.
<b>Linux</b>	<p>a libexpat.so.0 파일을 설치하거나 이 파일이 이미 설치되어 있는지 확인합니다.</p> <p>파일이 /usr/lib 또는 /usr/local/lib 디렉토리에 설치되어 있는지 확인합니다.</p> <p>b libflashplayer.so 파일을 설치하거나 이 파일이 이미 설치되어 있는지 확인합니다.</p> <p>Linux 운영 체제의 경우 적합한 플래시 플러그인 디렉토리에 해당 파일이 설치되어 있어야 합니다.</p> <p>c wget 프로그램을 설치하거나 이 프로그램 파일이 이미 설치되어 있는지 확인합니다.</p>

## 플래시 URL 리디렉션 사용 안 함 또는 사용

플래시 URL 리디렉션 기능은 VDM\_FLASH\_URL\_REDIRECTION=1 속성을 사용하여 Horizon Agent를 자동 설치할 경우 사용하도록 설정됩니다. 해당 가상 시스템에서 Windows 레지스트리 키의 값을 설정하면 선택한 원격 데스크톱에서 플래시 URL 리디렉션 기능을 사용하지 않도록 설정하거나 다시 사용하도록 설정할 수 있습니다.

## 절차

- 1 가상 시스템에서 Windows 레지스트리 편집기를 시작합니다.
- 2 플래시 URL 리디렉션을 제어하는 Windows 레지스트리 키로 이동합니다.

옵션	설명
<b>Windows 7 64비트</b>	HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware ViewMPWEnabled = <i>value</i>
<b>Windows 7 32비트</b>	HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware ViewMPWEnabled = <i>value</i>

- 3 플래시 URL 리디렉션을 사용하거나 사용하지 않도록 값을 설정합니다.

옵션	값
사용 안 함	0
사용	1

기본적으로 값은 1로 설정되어 있습니다.



## Flash 리더렉션 구성

Flash 리더렉션 기능을 사용하면 Flash 콘텐츠를 클라이언트 시스템으로 보내서 Flash Player ActiveX 버전을 사용하는 Flash 컨테이너 창에서 재생할 수 있습니다.

**참고** Horizon 7.0에서 Flash 리더렉션은 기술 미리보기 기능입니다. Horizon 7.0.1에서는 완전히 지원됩니다.

이 기능의 이름은 Flash URL 리더렉션이라는 기능과 비슷하지만, 다음 표와 같은 중요한 차이가 있습니다.

표 2-1. Flash 리더렉션 기능과 Flash URL 리더렉션의 비교

차이점	Flash 리더렉션	플래시 URL 리더렉션
지원 수준	기술 지원이 제공되지 않는 Horizon 7.0의 기술 미리보기 기능입니다. Horizon 7.0.1에서는 완전히 지원됩니다.	완전히 지원됨
이 기능을 지원하는 Horizon Client 유형	Windows 클라이언트만	Windows 클라이언트와 Linux 클라이언트
디스플레이 프로토콜	Horizon 7.0에서는 PCoIP만 해당합니다. Horizon 7.0.1에서는 PCoIP 및 VMware Blast입니다.	PCoIP
브라우저	에이전트의 경우 Internet Explorer 9, 10 또는 11(원격 데스크톱)	Horizon Client 및 Horizon Agent에서 현재 지원되는 모든 브라우저
구성 메커니즘	에이전트 측 GPO를 사용하여 Flash 리더렉션을 사용하거나 사용하지 않을 웹 사이트 화이트리스트 또는 블랙리스트 지정	웹 페이지에서 필요한 JavaScript를 포함하도록 소스 코드 수정

## 기능 제한 사항

Flash 리더렉션 기능에는 다음과 같은 제한이 있습니다.

- Flash Player 창 안의 URL 링크를 클릭하면 원격 데스크톱(에이전트 측)이 아닌 클라이언트에서 브라우저가 열립니다.
- Flash 리더렉션을 사용할 때 일부 브라우저 버전에서 일부 웹 사이트가 작동하지 않습니다. 예를 들어, Internet Explorer 11을 사용하는 경우에는 vimeo.com 웹 사이트가 작동하지 않습니다.
- Horizon 7.0에서는 Flash 및 Java 스크립팅이 정상적으로 작동하지 않을 수 있습니다.
- Flash 콘텐츠를 재생하는 동안 Horizon Client 창이 정지할 수 있지만, Windows 레지스트리 키를 설정하면 이 문제를 해결할 수 있습니다.

32비트 클라이언트에서 HKLM\Software\VMware, Inc.\VMware VDMWClient\Enabled3DRenderer 값을 "FALSE"로 설정하고, 64비트 클라이언트에서 HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDMWClient\Enabled3DRenderer를 "FALSE"로 설정합니다.

- YouTube 웹 사이트의 경우 재생 문제를 방지하기 위해 기본적으로 외부 인터페이스가 사용되지 않도록 설정됩니다. 따라서 자동 재생, [다음] 및 [이전] 버튼, Theater 모드 기능이 작동하지 않습니다. YouTube 웹 사이트의 최신 업데이트에서 Flash 미디어를 사용하도록 설정하려면 **호환성 보기 설정**에서 youtube.com을 삭제하고 비디오의 URL에 수동으로 &nohtml5=1을 추가해야 합니다. 예: https://www.youtube.com/watch?v=NwmRD25HWGE&nohtml5=1.
- 원격 데스크톱에서 appMode=1을 Windows 레지스트리 키로 설정하지 않는 한 YouTube 사이트에서 추천 비디오를 클릭할 수 없습니다.
- 클라이언트에 오디오 디바이스가 없으면 YouTube Flash 미디어를 재생할 때 오류가 발생합니다.
- redbox.com의 경우 Flash 리더렉션이 작동하지 않습니다.
- Flash 컨텍스트 메뉴(오른쪽 클릭으로 활성화)는 사용되지 않도록 설정됩니다.
- Horizon Client 버전 4.1이 PCoIP를 통해 Horizon 7.0 데스크톱에 연결되면 Flash 리더렉션이 실패합니다. Flash 콘텐츠가 데스크톱의 기본 플레이어에 의해 재생되거나 흰색 화면이 표시됩니다.

## Flash 리더렉션에 대한 시스템 요구 사항

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

### 원격 데스크톱

- 단일 사용자(VDI) 원격 데스크톱에 Flash 리더렉션 옵션을 포함한 Horizon Agent 7.0 이상이 설치되어 있어야 합니다. Flash 리더렉션 옵션은 기본적으로 선택되어 있지 않습니다.  
“Horizon 7에서 가상 데스크톱 설정” 문서에서 “Horizon Agent 사용자 지정 설치 옵션”을 참조하십시오.
- 적절한 그룹 정책 설정이 구성되어 있어야 합니다. [Flash 리더렉션 설치 및 구성](#)를 참조하십시오.
- Flash 리더렉션은 Windows 7, Windows 8, Windows 8.1 및 Windows 10 단일 사용자 원격 데스크톱에서 지원됩니다.
- Internet Explorer 9, 10 또는 11이 해당 Flash ActiveX 플러그인과 함께 설치되어 있어야 합니다.
- 설치 후 Internet Explorer에서 VMware View FlashMMR Server 추가 기능을 사용하도록 설정해야 합니다.

### Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

- Horizon Client 4.0 이상이 설치되어 있어야 합니다. Flash 리더렉션 옵션은 기본적으로 사용하도록 설정되어 있습니다.  
“Windows용 VMware Horizon Client 사용” 문서에서 Horizon Client 설치에 관한 항목을 참조하십시오.
- Flash 리더렉션은 Windows 7, Windows 8, Windows 8.1 및 Windows 10에서 지원됩니다.

- Flash ActiveX 플러그인이 설치 및 활성화되어 있어야 합니다.

**원격 세션을 위한 디스플레이 프로토콜** VMware Blast, PCoIP

## Flash 리디렉션 설치 및 구성

원격 데스크톱에서 로컬 클라이언트 시스템의 Flash Player 창으로 Flash 콘텐츠를 리디렉션하려면 원격 데스크톱 및 클라이언트 시스템에 Flash 리디렉션 기능과 Internet Explorer를 설치하고 이 기능을 사용할 웹 사이트를 지정해야 합니다.

클라이언트 시스템에 이 기능을 설치하려면 Horizon Client 4.0 이상 설치 관리자를 사용해야 합니다. 원격 데스크톱에 이 기능을 설치하려면 Horizon Agent 7.0 이상 설치 관리자를 사용하고 기본적으로 선택되어 있지 않은 올바른 설치 옵션을 선택해야 합니다. 이 기능을 사용하도록 설정하고 이 기능을 사용할 웹 사이트를 지정하려면 그룹 정책을 사용합니다.

**참고** 또는 원격 데스크톱에서 Windows 레지스트리 설정을 사용하여 Flash 리디렉션에 사용할 웹 사이트의 화이트리스트를 구성할 수 있습니다. [Windows 레지스트리 설정을 사용하여 Flash 리디렉션 구성](#)를 참조하십시오.

### 사전 요구 사항

- Active Directory 서버를 호스팅하는 시스템에 관리자 도메인 사용자로 로그인할 수 있는지 확인합니다.
- Active Directory 서버에서 MMC와 그룹 정책 개체 편집기 스냅인을 사용할 수 있는지 확인합니다.
- Horizon Agent 구성 ADMX 템플릿(vdm\_agent.admx 파일)이 원격 데스크톱의 OU에 추가되었는지 확인합니다.
- Flash 콘텐츠를 리디렉션할 수 있거나 없는 웹 사이트 목록을 컴파일합니다. 목록에 지정된 URL만 Flash 콘텐츠를 리디렉션할 수 있도록 하는 화이트리스트를 컴파일합니다. 목록에 지정된 URL이 Flash 콘텐츠를 리디렉션할 수 없도록 하는 블랙리스트를 컴파일합니다.
- Flash ActiveX가 설치되고 제대로 작동되는지 확인합니다. 설치를 확인하려면 Internet Explorer를 실행하고 <https://helpx.adobe.com/flash-player.html>로 이동합니다.

### 절차

- 1 Windows 7, Windows 8, Windows 8.1 또는 Windows 10 클라이언트 시스템에서 필요한 버전의 Horizon Client 및 Flash Player ActiveX 버전을 설치합니다.
  - Horizon Client 4.0 이상을 설치합니다. "Windows용 VMware Horizon Client 사용" 문서에서 Horizon Client 설치에 관한 항목을 참조하십시오.
  - 필요한 경우 NPAPI 버전이 아닌 ActiveX 버전의 Flash Player를 설치합니다. Flash Player는 Internet Explorer 10 및 11에 기본적으로 설치됩니다. Internet Explorer 9의 경우는 <https://get.adobe.com/flashplayer/> 사이트에서 Flash Player를 다운로드 및 설치해야 할 수도 있습니다.

- 2 Windows 7, Windows 8, Windows 8.1 또는 Windows 10 원격 데스크톱에서 필요한 버전의 Horizon Agent 및 Internet Explorer와 Flash Player를 설치합니다.
  - Horizon Agent 7.0 이상을 설치하고 Flash 리디렉션(시험용) 옵션을 선택해야 합니다. 이 옵션은 기본적으로 선택되지 않습니다.
  - Internet Explorer 9, 10 또는 11을 설치합니다.
  - 필요한 경우 NPAPI 버전이 아닌 ActiveX 버전의 Flash Player를 설치합니다. Flash Player는 Internet Explorer 10 및 11에 기본적으로 설치됩니다. Internet Explorer 9의 경우는 <https://get.adobe.com/flashplayer/> 사이트에서 Flash Player를 다운로드 및 설치해야 할 수도 있습니다.
- 3 원격 데스크톱에 있는 Internet Explorer의 메뉴 표시줄에서 **도구 > 추가 기능 관리**를 선택하고 **VMware View FlashMMR Server**가 나열되어 있으며 사용하도록 설정되어 있는지 확인합니다.
- 4 Active Directory 서버에서 그룹 정책 관리 편집기를 열고 **컴퓨터 구성**에서 Flash 리디렉션 정책 설정을 편집합니다.

이 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > 클래식 관리 템플릿 > VMware Horizon Agent 구성 > VMware FlashMMR** 폴더에 있습니다.

설정	설명
<b>Flash 멀티미디어 리디렉션 사용</b>	Flash 리디렉션(FlashMMR)이 원격 데스크톱(에이전트 측)에서 사용하도록 설정되어 있는지 지정합니다. 이 기능을 사용하도록 설정하면 Flash 멀티미디어 데이터를 지정된 URL에서 TCP 채널을 통해 클라이언트로 전달하며, 클라이언트 시스템에서 로컬 Flash Player를 호출합니다. 이 기능을 사용하면 에이전트 측의 CPU 및 네트워크 대역폭에 대한 수요가 크게 줄어듭니다.
<b>FlashMMR을 사용할 최소 직사각형 크기</b>	Flash 콘텐츠를 재생하는 직사각형의 최소 너비와 높이를 픽셀 단위로 지정합니다. 예를 들어, <b>400,300</b> 이면 너비 400픽셀, 높이 300픽셀이 지정됩니다. Flash 리디렉션은 Flash 콘텐츠가 이 정책에 지정된 값 이상인 경우에만 사용됩니다. 이 GPO가 구성되지 않은 경우에는 기본값인 <b>320,200</b> 을 사용합니다.

- 5 그룹 정책 관리 편집기에서 **사용자 구성**에 있는 Flash 리디렉션 정책 설정을 편집합니다.
 

이 설정은 **사용자 구성 > 정책 > 관리 템플릿 > 클래식 관리 템플릿 > VMware Horizon Agent 구성 > VMware FlashMMR** 폴더에 있습니다.

  - a (Horizon 7.0.3 이상) Flash 리디렉션에 사용할 호스트 URL 목록을 정의하기 위한 **FlashMMR URL 목록 사용 정의** 설정을 열고 **사용** 라디오 버튼을 선택합니다.
  - b [URL 사용] 드롭다운 목록에서 화이트리스트 또는 블랙리스트 중에서 사용하도록 설정할 목록을 선택합니다.
    - 화이트리스트를 사용하도록 설정하려면 **화이트리스트 사용**을 선택합니다.
    - 블랙리스트를 사용하도록 설정하려면 **블랙리스트 사용**을 선택합니다.

기본적으로 화이트리스트가 사용되도록 설정됩니다.

- c Flash 리더렉션을 사용하거나 사용하지 않을 호스트 URL 목록을 추가하기 위한 **FlashMMR을 사용/사용하지 않도록 설정하는 URL 목록 호스팅** 설정을 열고 **사용** 라디오 버튼을 선택합니다.
- d **표시** 버튼을 클릭합니다.
- e [이름] 옆에 전체 조건으로 컴파일한 전체 URL을 입력하고 [값] 옆은 비워 둡니다.

**http://** 또는 **https://**를 반드시 포함하십시오. 정규식을 사용할 수 있습니다. 예를 들어, **https://\*.google.com** 및 **http://www.cnn.com**을 지정할 수 있습니다.

(Horizon 7.0) [값] 옆은 비워 둡니다.

(Horizon 7.0.1 이상) [값] 옆에서 **requireIECompatibility=true** 또는 **appMode=0** 중 하나 또는 둘 다를 지정할 수 있습니다(쉼표로 두 문자열 구분).

웹 사이트에서는 기본적으로 HTML5를 지원하며 이러한 웹 사이트에서는 Flash 리더렉션이 작동하지 않습니다. 이러한 사이트가 작동하려면 **requireIECompatibility=true**를 설정해야 합니다. YouTube 웹 사이트에는 이 매개 변수가 필요하지 않습니다.

기본적으로 Flash 리더렉션이 실행될 때 외부 인터페이스 지원이 사용되도록 설정됩니다. 이로 인해 성능이 저하될 수 있습니다. 특정 경우에 **appMode=0**을 설정하면 성능이 향상되고 사용자 환경이 개선될 수 있습니다.

- 6 에이전트 시스템에서 명령 프롬프트를 열고 다음 디렉토리로 변경합니다.

```
%Program Files%\Common Files\VMware\Remote Experience
```

- 7 다음 명령을 실행하여 Internet Explorer에 화이트리스트 또는 블랙리스트를 추가합니다.

```
cscript mergeflashmmrwhitelist.vbs
```

- 8 Internet Explorer를 다시 시작하십시오.

**requireIECompatibility=true** 매개 변수가 설정된 사이트가 Internet Explorer의 호환성 보기에 추가됩니다. 메뉴 표시줄에서 **도구 > 호환성 보기 설정**을 선택하면 이 설정을 확인할 수 있습니다.

Horizon 7.0에서만 사이트가 Internet Explorer의 신뢰할 수 있는 사이트 목록에도 추가됩니다. Internet Explorer 메뉴 표시줄에서 **도구 > 인터넷 옵션**을 선택하고 **보안** 탭에서 **사이트** 버튼을 클릭하면 신뢰할 수 있는 사이트를 확인할 수 있습니다.

## Windows 레지스트리 설정을 사용하여 Flash 리더렉션 구성

Active Directory 서버에 관리자 권한이 없는 도메인 사용자인 경우에는 대신 원격 데스크톱의 Windows 레지스트리 키에 적절한 값을 설정하여 Flash 리더렉션을 구성할 수 있습니다.

GPO 설정 대신 이 절차를 사용하여 Flash 리더렉션을 구성할 수 있습니다.

## 사전 요구 사항

- 목록에 지정된 URL만 Flash 콘텐츠를 리디렉션할 수 있도록 하는 웹 사이트의 화이트리스트를 컴파일합니다. 웹 사이트의 블랙리스트를 컴파일할 수 있지만 블랙리스트를 사용하도록 설정하기 위해 Windows 레지스트리 설정을 사용할 수는 없습니다. 블랙리스트는 목록에 지정된 URL만 Flash 콘텐츠를 리디렉션할 수 없도록 합니다. 블랙리스트를 사용하도록 설정하려면 Flash 리디렉션에 대한 GPO 설정을 사용해야 합니다.
- 원격 데스크톱에 Horizon Agent 7.0 이상이 Flash Player와 Internet Explorer 9, 10 또는 11과 함께 설치되어 있는지 확인합니다. [Flash 리디렉션 설치 및 구성](#)의 내용을 참조하십시오.
- Horizon Client 4.0 이상과 Flash Player ActiveX 버전을 사용하고 있는지 확인합니다.

## 절차

- 1 Horizon Client를 사용하여 원격 데스크톱에 액세스합니다(에이전트 시스템).
- 2 에이전트 시스템에서 Windows 레지스트리 편집기(regedit.exe)를 열고 다음 폴더로 이동한 다음 **FlashRedirection**을 1로 설정합니다.

```
HKLM\Software\VMware, Inc.\VMware FlashMMR
```

**참고** 이 설정으로 Flash 리디렉션 기능을 사용할 수 있지만, HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR에서 이 설정이 사용되도록 설정되어 있지 않으면(0으로 설정) Flash 리디렉션이 도메인 전체에서 사용 안 함으로 설정되며, 도메인 관리자가 Flash 리디렉션을 사용하도록 설정해야 합니다.

- 3 다음 폴더로 이동합니다.

```
HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR
```

이 폴더가 아직 없으면 만드십시오.

- 4 VMware FlashMMR 폴더에서 **UrlWhiteList**라는 하위 키를 만듭니다.
- 5 **UrlWhiteList** 키를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 문자열 값**을 선택한 후 이름에 Flash 리디렉션을 사용할 웹 사이트의 URL을 입력합니다.  
정규식을 사용할 수 있습니다. 예를 들어, **https://\*.google.com**을 지정할 수 있습니다. **데이터** 값은 비워 두어야 합니다.
- 6 (선택 사항) (Horizon 7.0.1 및 7.0.2만 해당) 새 레지스트리 값의 [데이터] 필드에 데이터 **requireIECompatibility=true, appMode=0** 또는 두 항목을 모두 추가합니다(쉼표로 두 문자열 구분).

웹 사이트에서는 기본적으로 HTML5를 지원하며 이러한 웹 사이트에서는 Flash 리디렉션이 작동하지 않습니다. 이러한 사이트가 작동하려면 **requireIECompatibility=true**를 설정해야 합니다. YouTube 웹 사이트에는 이 매개 변수가 필요하지 않습니다.

기본적으로 Flash 리디렉션이 실행될 때 외부 인터페이스 지원이 사용되도록 설정됩니다. 이로 인해 성능이 저하될 수 있습니다. Horizon 7.0.1 이상의 경우 상황에 따라 **appMode=0**을 설정하면 성능을 개선할 수 있고 **appMode=1**을 설정하면 사용자 환경을 개선할 수 있습니다.

- 7 이전 단계를 반복하여 URL을 더 추가하고, 마치면 레지스트리 편집기를 닫습니다.
- 8 에이전트 시스템에서 명령 프롬프트를 열고 다음 디렉토리로 변경합니다.

```
%Program Files%Common FilesVMwareRemote Experience
```

- 9 다음 명령을 실행하여 Internet Explorer에 화이트 리스트를 추가합니다.

```
cscript mergeflashmmrwhitelist.vbs
```

- 10 Internet Explorer를 다시 시작하십시오.

**requireIECompatibility=true** 매개 변수가 설정된 사이트가 Internet Explorer의 호환성 보기에 추가됩니다. 메뉴 표시줄에서 **도구 > 호환성 보기 설정**을 선택하면 이 설정을 확인할 수 있습니다.

Horizon 7.0에서만 사이트가 Internet Explorer의 신뢰할 수 있는 사이트 목록에도 추가됩니다. Internet Explorer 메뉴 표시줄에서 **도구 > 인터넷 옵션**을 선택하고 **보안** 탭에서 **사이트** 버튼을 클릭하면 신뢰할 수 있는 사이트를 확인할 수 있습니다.

## 실시간 오디오-비디오 구성

실시간 오디오-비디오를 통해 Horizon 7 사용자는 원격 데스크톱에서 Skype, Webex, Google Hangouts 및 기타 온라인 회의 애플리케이션을 실행할 수 있습니다. 실시간 오디오-비디오를 사용하면 클라이언트 시스템에 로컬로 연결된 웹캠 및 오디오 디바이스가 원격 데스크톱으로 리디렉션됩니다. 이 기능은 USB 리디렉션을 사용할 경우 얻을 수 있는 대역폭에 비해 상당히 적은 대역폭을 사용하여 비디오 및 오디오 데이터를 데스크톱으로 리디렉션합니다.

실시간 오디오-비디오는 표준 회의 애플리케이션 및 브라우저 기반 비디오 애플리케이션과 호환되며 표준 웹캠, 오디오 USB 디바이스 및 아날로그 오디오 입력을 지원합니다.

이 기능은 데스크톱 운영 체제에서 VMware 가상 웹캠 및 VMware 가상 마이크를 설치합니다. VMware 가상 웹캠은 브라우저 기반 비디오 애플리케이션 및 기타 타사 회의 소프트웨어와의 호환성이 향상된 커널 모드 웹캠 드라이버를 사용합니다.

회의 또는 비디오 애플리케이션이 실행되면 이러한 VMware 가상 디바이스를 표시 및 사용하여 클라이언트에서 로컬로 연결된 디바이스로부터 오디오-비디오 리디렉션을 처리합니다. VMware 가상 웹캠 및 마이크는 데스크톱 운영 체제의 디바이스 관리자에 나타납니다.

리디렉션을 사용하도록 설정하려면 Horizon Client 시스템에 오디오 및 웹캠 디바이스용 드라이버를 설치해야 합니다.

## 실시간 오디오-비디오 구성 옵션

실시간 오디오-비디오가 포함된 Horizon Agent를 설치하면 해당 기능이 Horizon 7 데스크톱에서 별도의 구성 없이 작동됩니다. 표준 디바이스 및 애플리케이션에 대해 웹캠 프레임 속도 및 이미지 해상도에 대한 기본값이 권장됩니다.



이러한 기본값을 변경하여 특정 애플리케이션, 웹캠 또는 환경에 적용할 그룹 정책 설정을 구성할 수 있습니다. 기능을 함께 사용하거나 사용하지 않도록 설정하는 정책을 설정할 수도 있습니다. ADMX 템플릿 파일을 통해 Active Directory 또는 개별 데스크톱에 실시간 오디오-비디오 그룹 정책 설정을 설치할 수 있습니다. [실시간 오디오-비디오 그룹 정책 설정 구성](#)를 참조하십시오.

사용자가 내장되어 있거나 클라이언트 컴퓨터에 연결된 여러 웹캠 및 오디오 입력 디바이스를 가지고 있는 경우, 데스크톱으로 리디렉션될 기본 웹캠 및 오디오 입력 디바이스를 구성할 수 있습니다. [기본 웹캠 및 마이크 선택](#)를 참조하십시오.

---

**참고** 기본 오디오 디바이스는 선택할 수 있지만 기타 오디오 구성 옵션은 사용할 수 없습니다.

---

웹캠 이미지 및 오디오 입력이 원격 데스크톱으로 리디렉션되면 로컬 컴퓨터에서 웹캠 및 오디오 디바이스에 액세스할 수 없습니다. 반대로, 로컬 컴퓨터에서 이러한 디바이스를 사용 중이면 원격 데스크톱에서 해당 디바이스에 액세스할 수 없습니다.

지원되는 애플리케이션에 대한 자세한 내용은 <http://kb.vmware.com/kb/2053754>의 VMware 기술 자료 문서, "Guidelines for Using Real-Time Audio-Video with 3rd-Party Applications on Horizon View Desktops" (Horizon View 데스크톱에서 타사 애플리케이션을 통한 실시간 오디오-비디오 사용 지침)를 참조하십시오.

## 실시간 오디오-비디오에 대한 시스템 요구 사항

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

### 원격 데스크톱

View Agent 6.0 이상 또는 Horizon Agent 7.0 이상을 설치하면 실시간 오디오-비디오 기능이 설치됩니다. 게시된 데스크톱 및 애플리케이션에서 이 기능을 사용하려면 Horizon Agent 7.0.2 이상을 설치해야 합니다. Horizon Agent 설치에 대한 자세한 내용은 설치 문서를 참조하십시오.

### Horizon Client 소프트웨어

Windows용 Horizon Client 2.2 이상 릴리스

Linux용 Horizon Client 2.2 이상 릴리스. Linux용 Horizon Client 3.1 이하 버전의 경우 이 기능은 타사 공급업체에서 제공하는 Linux용 Horizon Client 버전에서만 사용할 수 있습니다. Linux용 Horizon Client 3.2 이상 버전의 경우 이 기능은 VMware에서 제공하는 클라이언트 버전에서도 사용할 수 있습니다.

Mac용 Horizon Client 2.3 이상 릴리스

iOS용 Horizon Client 4.0 이상 릴리스

Android용 Horizon Client 4.0 이상 릴리스

### Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

- Windows용 Horizon Client를 실행하는 모든 운영 체제
- x86 디바이스에서 Linux용 Horizon Client를 실행하는 모든 운영 체제. 이 기능은 ARM 프로세서에서 지원되지 않습니다.



- Mac OS X Mountain Lion(10.8) 이상. 모든 이전 버전의 Mac OS X 운영 체제에서는 이 기능을 사용할 수 없습니다.
- iOS용 Horizon Client를 실행하는 모든 운영 체제
- Android용 Horizon Client를 실행하는 모든 운영 체제
- 지원되는 클라이언트 운영 체제에 대한 자세한 내용은 해당 시스템 또는 디바이스에 대한 "VMware Horizon Client사용" 문서를 참조하십시오.
- 웹캠 및 오디오 디바이스 드라이버가 설치되어 있어야 하며, 클라이언트 컴퓨터에서 웹캠 및 오디오 디바이스를 작동할 수 있어야 합니다. 실시간 오디오-비디오를 지원하기 위해 에이전트가 설치되어 있는 데스크톱 운영 체제에 디바이스 드라이버를 설치할 필요는 없습니다.

#### 디스플레이 프로토콜

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

## USB 리디렉션 대신 실시간 오디오-비디오가 사용되는지 확인

실시간 오디오-비디오는 회의 애플리케이션에서 사용하도록 웹캠 및 오디오 입력 리디렉션을 지원합니다. Horizon Agent로 설치할 수 있는 USB 리디렉션 기능은 웹캠 리디렉션을 지원하지 않습니다. USB 리디렉션을 통해 오디오 입력 디바이스를 리디렉션하는 경우, 오디오 스트림이 실시간 오디오-비디오 세션 동안 비디오와 제대로 동기화되지 않으며 네트워크 대역폭에 대한 요구량 감소 이점이 사라집니다. 웹캠 및 오디오 입력 디바이스가 USB 리디렉션이 아닌 실시간 오디오-비디오를 통해 데스크톱으로 리디렉션되는지 확인하기 위해 조치를 취할 수 있습니다.

데스크톱에 USB 리디렉션을 구성한 경우, 최종 사용자는 Windows 클라이언트 메뉴 모음에서 **USB 디바이스 연결** 옵션을 선택하거나 Mac 클라이언트에서 **데스크톱 > USB** 메뉴를 선택하여 로컬로 연결되어 있는 USB 디바이스를 연결하고 표시할 수 있습니다. Linux 클라이언트는 기본적으로 오디오 및 비디오 디바이스의 USB 리디렉션을 차단하며 최종 사용자에게 USB 디바이스 옵션을 제공하지 않습니다.

최종 사용자가 **USB 디바이스 연결** 또는 **데스크톱 > USB** 목록에서 USB 디바이스를 선택하면 비디오 또는 오디오 회의에 해당 디바이스를 사용할 수 없게 됩니다. 예를 들어, 사용자가 Skype 호출을 하는 경우 비디오 이미지가 나타나지 않거나 오디오 스트림 성능이 저하될 수 있습니다. 회의 세션이 진행되는 동안 최종 사용자가 디바이스를 선택하는 경우, 웹캠 또는 오디오 리디렉션이 손상됩니다.

최종 사용자에게 이러한 디바이스를 숨기고 잠재적인 손상을 방지하기 위해 VMware Horizon Client에서 웹캠 및 오디오 입력 디바이스를 표시하지 않도록 USB 리디렉션 그룹 정책 설정을 구성할 수 있습니다.

특히, Horizon Agent에 대한 USB 리디렉션 필터링 규칙을 생성하고 audio-in 및 video 디바이스 제품군 이름을 사용하지 않도록 지정할 수 있습니다. USB 리디렉션에 대한 그룹 정책 설정 및 필터링 규칙 지정에 대한 자세한 내용은 [USB 리디렉션 제어를 위한 정책 사용](#)의 내용을 참조하십시오.

**경고** USB 디바이스 제품군을 사용하지 않도록 USB 리디렉션 필터링 규칙을 설정하지 않는 경우에는 VMware Horizon Client 메뉴 모음의 **USB 디바이스 연결** 또는 **데스크톱 > USB** 목록에서 웹캠 또는 오디오 디바이스를 선택할 수 없다는 점을 최종 사용자에게 직접 알립니다.

## 기본 웹캠 및 마이크 선택

클라이언트 컴퓨터에 하나 이상의 웹캠 및 마이크가 있는 경우, 실시간 오디오-비디오가 데스크톱으로 리디렉션할 기본 웹캠 및 기본 마이크를 구성할 수 있습니다. 이러한 디바이스를 내장하거나 로컬 클라이언트 컴퓨터에 연결할 수 있습니다.

Windows용 Horizon Client 4.2 이상이 설치된 Windows 클라이언트 컴퓨터의 경우에는 Horizon Client 설정 대화상자에서 실시간 오디오-비디오 설정을 구성하여 기본 웹캠이나 마이크를 선택할 수 있습니다. Horizon Client 버전이 더 낮은 경우에는 레지스트리 설정을 수정하여 기본 웹캠을 선택하고 Windows 운영 체제의 사운드 컨트롤을 사용하여 기본 마이크를 선택합니다.

Mac 클라이언트 컴퓨터에서 Mac 기본 시스템을 사용하여 기본 웹캠 또는 마이크를 지정할 수 있습니다.

Linux 클라이언트 컴퓨터에서 구성 파일을 편집하여 기본 웹캠을 지정할 수 있습니다. 기본 마이크를 선택하려면 클라이언트 컴퓨터의 Linux 운영 체제에서 사운드 컨트롤을 구성합니다.

사용 가능한 경우 실시간 오디오-비디오가 기본 웹캠을 리디렉션합니다. 그렇지 않은 경우, 실시간 오디오-비디오는 시스템 목록에서 제공하는 첫 번째 웹캠을 사용합니다.

## Windows 클라이언트 시스템에서 기본 웹캠 또는 마이크 선택

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

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

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

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

이 절차는 Windows용 Horizon Client 4.2 이상에만 적용됩니다. 클라이언트 버전이 더 낮은 경우에는 레지스트리 설정을 수정하여 기본 웹캠을 선택하고 Windows 운영 체제의 사운드 컨트롤을 사용하여 기본 마이크를 선택해야 합니다. 자세한 내용은 Horizon Client 버전의 "Windows용 VMware Horizon Client 사용" 문서를 참조하십시오.

## 사전 요구 사항

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

## 절차

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

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

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

드롭다운 메뉴에는 클라이언트 시스템에서 사용할 수 있는 웹캠과 마이크가 표시됩니다.

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

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

## Mac 클라이언트 시스템에서 기본 마이크 선택

클라이언트 시스템에 여러 마이크가 있을 경우, 하나의 마이크만 원격 데스크톱에서 사용됩니다. 클라이언트 시스템의 시스템 기본 설정을 사용하여 원격 데스크톱의 기본 마이크를 지정할 수 있습니다.

실시간 오디오-비디오 기능을 통해, 오디오 입력 디바이스 및 오디오 출력 디바이스는 USB 리디렉션을 사용하지 않고 함께 작동하며, 필요한 네트워크 대역폭 양이 대폭 감소했습니다. 아날로그 오디오 입력 디바이스도 지원됩니다.

이 절차에서는 클라이언트 시스템의 사용자 인터페이스에서 마이크를 선택하는 방법을 설명합니다. 관리자는 Mac 기본 시스템을 사용하여 기본 마이크를 구성할 수도 있습니다. [Mac 클라이언트 시스템에서 기본 웹캠 또는 마이크 구성](#)의 내용을 참조하십시오.

---

**중요** USB 마이크를 사용 중인 경우 Horizon Client의 **연결 > USB** 메뉴에서 마이크를 연결하지 마십시오. 그렇게 연결하기 위해 USB 리디렉션을 통해 디바이스를 라우팅하면 디바이스에서 실시간 오디오-비디오 기능을 사용할 수 없습니다.

---

## 사전 요구 사항

- 클라이언트 시스템에 USB 마이크 또는 다른 유형의 마이크가 설치되어 있고 작동이 가능한지 확인하십시오.
- 원격 데스크톱에 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용하고 있는지 확인하십시오.

## 절차

- 1 클라이언트 시스템에서 **Apple 메뉴 > 시스템 환경설정**을 선택하고 **사운드**를 클릭합니다.
- 2 사운드 기본 설정의 입력 창을 엽니다.
- 3 사용할 마이크를 선택합니다.

이후에 원격 데스크톱과 연결하여 호출을 시작하면 클라이언트 시스템에서 선택했던 기본 마이크가 데스크톱에서 사용됩니다.

## Mac 클라이언트에서 실시간 오디오-비디오 구성

Mac 기본 시스템을 사용하여 명령줄에서 실시간 오디오-비디오 설정을 구성할 수 있습니다. 기본 시스템에서는 터미널(/Applications/Utilities/Terminal.app)을 사용하여 Mac 사용자 기본값을 읽고 쓰고 삭제할 수 있습니다.

Mac 기본 시스템은 도메인에 속합니다. 일반적으로 도메인은 각 애플리케이션에 해당합니다. 실시간 오디오-비디오 기능의 도메인은 com.vmware.rtav입니다.

### 실시간 오디오-비디오를 구성하는 구문

다음 명령을 사용하여 실시간 오디오-비디오를 구성할 수 있습니다.

### 표 2-2. 실시간 오디오-비디오를 구성하는 명령 구문

명령	설명
<code>defaults write com.vmware.rtav srcWCamId " 웹캠 사용자 ID "</code>	원격 데스크톱에서 사용할 기본 웹캠을 설정합니다. 이 값이 설정되지 않으면 웹캠은 시스템 목록에서 자동으로 선택됩니다. 클라이언트 시스템에 연결되어 있거나 내장되어 있는 웹캠 중에서 지정할 수 있습니다.
<code>defaults write com.vmware.rtav srcAudioInId " 오디오 디바이스 사용자 ID "</code>	원격 데스크톱에서 사용할 기본 마이크(오디오 입력 디바이스)를 설정합니다. 이 값이 설정되지 않으면 클라이언트 시스템에 설정된 기본 녹음 디바이스가 원격 데스크톱에서 사용됩니다. 클라이언트 시스템에 연결되어 있거나 내장되어 있는 마이크 중에서 지정할 수 있습니다.
<code>defaults write com.vmware.rtav srcWCamFrameWidth 픽셀</code>	이미지 너비를 설정합니다. 기본값은 하드코딩된 값인 320픽셀입니다. 이미지 너비를 다른 픽셀 값으로 변경할 수 있습니다.
<code>defaults write com.vmware.rtav srcWCamFrameHeight 픽셀</code>	이미지 높이를 설정합니다. 기본값은 하드코딩된 값인 240픽셀입니다. 이미지 높이를 다른 픽셀 값으로 변경할 수 있습니다.
<code>defaults write com.vmware.rtav srcWCamFrameRate fps</code>	프레임 속도를 설정합니다. 기본값은 15fps입니다. 프레임 속도를 다른 값으로 변경할 수 있습니다.
<code>defaults write com.vmware.rtav LogLevel " 수준 "</code>	실시간 오디오-비디오 로그 파일(~/Library/Logs/VMware/vmware-RTAV-pid.log)의 로깅 수준을 설정합니다. 로깅 수준을 trace 또는 debug로 설정할 수 있습니다.
<code>defaults write com.vmware.rtav IsDisabled 값</code>	실시간 오디오-비디오 기능 사용 여부를 지정합니다. 실시간 오디오-비디오는 기본적으로 사용되며 이 값이 적용되지 않습니다. 클라이언트에서 실시간 오디오-비디오를 사용하지 않으려면 이 값을 true로 설정합니다.

명령	설명
defaults read com.vmware.rtav	실시간 오디오-비디오 구성 설정을 표시합니다.
defaults delete com.vmware.rtav <i>설정</i>	실시간 오디오-비디오 구성 설정을 삭제합니다. 예: defaults delete com.vmware.rtav srcWCamFrameWidth

**참고** 프레임 속도는 1fps에서 최대 25fps까지, 해상도는 최대 1920x1080까지 조정할 수 있습니다. 일부 디바이스나 환경에서는 높은 프레임 속도에서의 높은 해상도가 지원되지 않을 수 있습니다.

## Mac 클라이언트 시스템에서 기본 웹캠 또는 마이크 구성

실시간 오디오-비디오 기능을 사용하면 클라이언트 시스템에 여러 개의 웹캠 또는 마이크가 있는 경우 그중 하나의 웹캠과 하나의 마이크만 원격 데스크톱에서 사용됩니다. Mac 기본 시스템을 사용하여 명령줄에서 기본적으로 사용할 웹캠과 마이크를 지정합니다.

실시간 오디오-비디오 기능을 사용하는 경우, 웹캠, 오디오 입력 디바이스 및 오디오 출력 디바이스를 USB 리디렉션 없이 사용할 수 있으며, 필요한 네트워크 대역폭 양이 대폭 감소됩니다. 아날로그 오디오 입력 디바이스도 지원됩니다.

대부분의 환경에서는 기본 마이크나 웹캠을 구성할 필요가 없습니다. 기본 마이크를 설정하지 않으면 클라이언트 시스템의 시스템 기본 설정에 설정된 기본 오디오 디바이스가 원격 데스크톱에서 사용됩니다. [Mac 클라이언트 시스템에서 기본 마이크 선택](#)의 내용을 참조하십시오. 기본 웹캠을 구성하지 않으면 시스템 목록에서 웹캠이 선택되어 원격 데스크톱에서 사용됩니다.

### 사전 요구 사항

- 기본 USB 웹캠을 구성하려는 경우 클라이언트 시스템에 USB 웹캠이 설치되어 있고 작동이 가능한지 확인하십시오.
- 기본 USB 마이크나 다른 유형의 마이크를 구성하려는 경우 클라이언트 시스템에 해당 마이크가 설치되어 있고 작동이 가능한지 확인하십시오.
- 원격 데스크톱에 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용하고 있는지 확인하십시오.

### 절차

- 1 Mac 클라이언트 시스템에서 웹캠이나 마이크 애플리케이션을 시작하여 카메라 디바이스 또는 오디오 디바이스 목록을 실시간 오디오-비디오 로그 파일에 트리거합니다.
  - a 웹캠이나 오디오 디바이스를 장착합니다.
  - b **애플리케이션** 폴더에서 **VMware Horizon Client**를 두 번 클릭하여 Horizon Client를 시작합니다.
  - c 호출을 시작한 다음 호출을 멈춥니다.

## 2 실시간 오디오-비디오 로그 파일에서 웹캠 또는 마이크에 대한 로그 항목을 찾습니다.

### a 텍스트 편집기에서 실시간 오디오-비디오 로그 파일을 엽니다.

실시간 오디오-비디오 로그 파일의 이름은 `~/Library/Logs/VMware/vmware-RTAV-pid.log`입니다. 여기서 *pid*는 현재 세션의 프로세스 ID입니다.

### b 장착된 웹캠과 마이크를 식별하는 항목을 실시간 오디오-비디오 로그 파일에서 검색합니다.

다음 예는 웹캠 항목이 실시간 오디오-비디오 로그 파일에 어떻게 표시되는지를 보여줍니다.

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() - 1 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=FaceTime HD
Camera (Built-in)   UserId=FaceTime HD Camera (Built-in)#0xfa20000005ac8509   SystemId=0xfa20000005ac8509
```

다음 예는 마이크 항목이 실시간 오디오-비디오 로그 파일에 어떻게 표시되는지를 보여줍니다.

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - 2 Device(s)
found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - Index=255
Name=Built-in Microphone   UserId=Built-in Microphone#AppleHDAEngineInput:1B,0,1,0:1
SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - Index=255
Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

## 3 실시간 오디오-비디오 로그 파일에서 기본으로 사용할 웹캠 또는 마이크를 찾아 해당 사용자 ID를 기록합니다.

사용자 ID는 로그 파일의 `UserId` = 문자열 다음에 나옵니다. 예를 들어 내장형 FaceTime 카메라의 사용자 ID는 FaceTime HD Camera (Built-in)이며 내장형 마이크의 사용자 ID는 Built-in Microphone입니다.

## 4 터미널(/Applications/Utilities/Terminal.app)에서 `defaults write` 명령을 사용하여 기본 웹캠과 마이크를 설정합니다.

옵션	조치
기본 웹캠 설정	<p><code>defaults write com.vmware.rtav srcWCamId "<i>webcam-userid</i>"</code>를 입력합니다. 여기서 <i>webcam-userid</i>는 실시간 오디오-비디오 로그 파일에서 검색한 기본 웹캠의 사용자 ID입니다. 예:</p> <pre>defaults write com.vmware.rtav srcWCamId "HD Webcam C525"</pre>
기본 마이크 설정	<p><code>defaults write com.vmware.rtav srcAudioInId "<i>audio-device-userid</i>"</code>를 입력합니다. 여기서 <i>audio-device-userid</i>는 실시간 오디오-비디오 로그 파일에서 검색한 기본 마이크의 사용자 ID입니다. 예:</p> <pre>defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"</pre>

- 5 (선택 사항) defaults read 명령을 사용하여 실시간 오디오-비디오 기능에 대한 변경 사항을 확인합니다.

예: `defaults read com.vmware.rtav`

이 명령은 모든 실시간 오디오-비디오 설정을 나열합니다.

이후에 원격 데스크톱과 연결하여 새 호출을 시작하면 클라이언트 시스템에서 구성한 기본 웹캠이나 마이크가 데스크톱에서 사용됩니다(사용할 수 있는 경우). 기본 웹캠과 마이크를 사용할 수 없으면 지원되는 다른 웹캠이나 마이크가 원격 데스크톱에서 사용됩니다.

## Linux 클라이언트 시스템에서 기본 마이크 선택

클라이언트 시스템에 여러 마이크가 있을 경우, 하나의 마이크만 Horizon 7 데스크톱에서 사용됩니다. 기본 마이크를 지정하려면 클라이언트 시스템에서 사운드 제어를 사용합니다.

실시간 오디오-비디오 기능을 통해, 오디오 입력 디바이스 및 오디오 출력 디바이스는 USB 리디렉션을 사용하지 않고 함께 작동하며, 필요한 네트워크 대역폭 양이 대폭 감소했습니다. 아날로그 오디오 입력 디바이스도 지원됩니다.

이 절차에서는 클라이언트 시스템의 사용자 인터페이스에서 기본 마이크를 선택하는 방법에 대해 설명합니다. 관리자가 구성 파일을 편집하여 기본 마이크를 구성할 수도 있습니다. [Linux 클라이언트 시스템에서 기본 웹캠 또는 마이크 선택](#)를 참조하십시오.

### 사전 요구 사항

- 클라이언트 시스템에 USB 마이크 또는 다른 유형의 마이크가 설치되어 있고 작동이 가능한지 확인하십시오.
- 원격 데스크톱에 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용하고 있는지 확인하십시오.

### 절차

- 1 Ubuntu 그래픽 사용자 인터페이스에서 **시스템 > 환경설정 > 사운드**를 선택합니다.

화면 상단의 도구 모음 오른쪽에서 **사운드** 아이콘을 클릭해도 됩니다.

- 2 사운드 환경설정 대화 상자에서 **입력** 탭을 클릭합니다.

- 3 기본 디바이스를 선택하고 **닫기**를 클릭합니다.

## Linux 클라이언트 시스템에서 기본 웹캠 또는 마이크 선택

실시간 오디오-비디오 기능을 사용하는 경우, 클라이언트 시스템에 여러 개의 웹캠 및 마이크가 있으면 Horizon 7 데스크톱에서는 그 중 하나의 웹캠 및 마이크만 사용할 수 있습니다. 구성 파일을 편집하면 기본으로 사용할 웹캠 및 마이크를 지정할 수 있습니다.

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

실시간 오디오-비디오 기능을 사용하는 경우, 웹캠, 오디오 입력 디바이스 및 오디오 출력 디바이스는 USB 리디렉션을 사용하지 않고도 작동할 수 있으며, 필요한 네트워크 대역폭 양이 대폭 감소합니다. 아날로그 오디오 입력 디바이스도 지원됩니다.

/etc/vmware/config 파일에서 속성을 설정하고 기본 디바이스를 지정하려면 특정 필드의 값을 확인해야 합니다. 로그 파일에서 이러한 필드의 값을 검색할 수 있습니다.

- 웹캠의 경우에는 rtav.srcWCamId 속성을 웹캠의 UserId 필드 값으로 설정하고 frtav.srcWCamName 속성을 웹캠의 Name 필드 값으로 설정합니다.

rtav.srcWCamName 속성은 rtav.srcWCamId 속성보다 우선 순위가 높습니다. 두 속성 모두 같은 웹캠을 지정해야 합니다. 속성에서 서로 다른 웹캠을 지정하면 rtav.srcWCamName으로 지정된 웹캠이 사용됩니다(있을 경우). 없을 경우에는 rtav.srcWCamId로 지정된 웹캠이 사용됩니다. 두 웹캠을 모두 찾을 수 없는 경우에는 기본 웹캠이 사용됩니다.

- 오디오 디바이스의 경우 rtav.srcAudioInId 속성을 Pulse Audio device.description 필드의 값으로 설정합니다.

### 사전 요구 사항

기본 웹캠, 기본 마이크 또는 이 두 가지를 모두 구성하는지 여부에 따라 이에 적절한 필수 조건 작업을 수행하십시오.

- 클라이언트 시스템에 USB 웹캠이 설치되어 있고 작동이 가능한지 확인하십시오.
- 클라이언트 시스템에 USB 마이크 또는 다른 유형의 마이크가 설치되어 있고 작동이 가능한지 확인하십시오.
- 원격 데스크톱에 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용하고 있는지 확인하십시오.

### 절차

- 1 클라이언트를 실행하고, 웹캠 또는 마이크 애플리케이션을 시작하여 클라이언트 로그에 카메라 디바이스 또는 오디오 디바이스 목록을 나열합니다.
  - a 사용할 웹캠 또는 오디오 디바이스를 연결합니다.
  - b vmware-view 명령을 사용하여 Horizon Client를 시작합니다.
  - c 호출을 시작한 다음 호출을 멈춥니다.

이 작업으로 로그 파일이 생성됩니다.



## 2 웹캠 또는 마이크에 대한 로그 항목을 찾습니다.

### a 텍스트 편집기로 디버그 로그 파일을 엽니다.

실시간 오디오-비디오 로그 메시지가 있는 로그 파일은 /tmp/vmware-**<사용자 이름>**/vmware-RTAV-**<pid>**.log에 있습니다. 클라이언트 로그는 /tmp/vmware-**<사용자 이름>**/vmware-view-**<pid>**.log에 있습니다.

### b 로그 파일을 검색하여 연결된 웹캠 및 마이크를 참조하는 로그 파일 항목을 찾습니다.

다음 예는 웹캠 선택에서 발췌한 내용을 보여줍니다.

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:0819)   UserId=UVC
Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.5   SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver   UserId=gspca main
driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7   SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=노트북용 Microsoft® LifeCam HD-6000
UserId=Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6
SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) - enumeration data
unavailable
```

다음 예는 오디오 디바이스 선택에서 발췌한 내용과 각각에 대한 현재 오디오 레벨을 보여줍니다.

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB Headset Analog
Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB 헤드셋 아날로그 모노')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of Microsoft LifeChat
LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
```

선택한 디바이스의 소스 오디오 레벨이 PulseAudio 기준을 충족하지 않거나, 소스가 100%(0dB)로 설정되지 않았거나, 선택한 소스 디바이스가 음소거된 경우 경고가 표시됩니다.

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*, const
pa_source_info*, int, void*) - Note, selected device channel volume: 0: 67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*, const
pa_source_info*, int, void*) - Note, selected device channel is muted
```

- 3 디바이스의 설명을 복사한 후 이를 사용하여 /etc/vmware/config 파일에 적절한 속성을 설정합니다.

웹캠의 경우, 노트북용 Microsoft® LifeCam HD-6000 및 노트북용 Microsoft® LifeCam HD-6000#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6을 복사하여 Microsoft 웹캠을 기본 웹캠으로 지정하고 아래와 같이 속성을 설정합니다.

```
rtav.srcWCamName = "Microsoft® LifeCam HD-6000 for Notebooks"
rtav.srcWCamId = "Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/
usb1/1-3/1-3.6"
```

이 예에서는 rtav.srcWCamId 속성을 "Microsoft"로 설정할 수도 있습니다. rtav.srcWCamId 속성은 부분 일치와 전체 일치를 모두 지원합니다. rtav.srcWCamName 속성은 전체 일치만 지원합니다. 오디오 디바이스의 경우 Logitech USB Headset Analog Mono를 복사하여 Logitech 헤드셋을 기본 오디오 디바이스로 지정하고 다음과 같이 속성을 설정합니다.

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

- 4 변경 내용을 저장하고 /etc/vmware/config 구성 파일을 닫습니다.
- 5 데스크톱 세션에서 로그오프하고 새 세션을 시작합니다.

## 실시간 오디오-비디오 그룹 정책 설정 구성

Horizon 7 데스크톱에서 실시간 오디오-비디오(RTAV)의 동작을 제어하는 그룹 정책 설정을 구성할 수 있습니다. 이러한 설정으로 가상 웹캠의 최대 프레임 속도 및 이미지 해상도가 결정됩니다. 이 설정을 통해 모든 사용자가 소비할 수 있는 최대 대역폭을 관리할 수 있습니다. 추가 설정은 RTAV 기능을 비활성화 또는 활성화합니다.

이러한 정책 설정을 구성하지 않아도 됩니다. 실시간 오디오-비디오는 클라이언트 시스템의 웹캠에 설정된 프레임 속도 및 이미지 해상도와 함께 작동합니다. 대부분의 웹캠 및 오디오 애플리케이션에서 기본 설정을 사용하는 것이 좋습니다.

실시간 오디오-비디오 실행 중 대역폭 사용에 대한 예는 [실시간 오디오-비디오 대역폭](#)을 참조하십시오.

이러한 정책 설정은 물리적 디바이스가 연결된 클라이언트 시스템이 아닌 Horizon 7 데스크톱에 영향을 미칩니다. 데스크톱에서 이러한 설정을 구성하려면 Active Directory에서 RTAV 그룹 정책 관리 템플릿(ADMX) 파일을 추가하십시오.

클라이언트 시스템에서 설정 구성에 대한 자세한 내용은 <http://kb.vmware.com/kb/2053644>의 VMware 기술 자료 문서, "Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients" (Horizon View 클라이언트의 실시간 오디오-비디오에 대한 프레임 속도 및 해상도 설정)를 참조하십시오.

## Active Directory에서 RTAV ADMX 템플릿 추가 및 설정 구성

ADMX 파일(`vdm_agent_rtav.admx`)의 정책 설정을 Active Directory의 GPO(그룹 정책 개체)에 추가하고 그룹 정책 개체 편집기에서 이 설정을 구성할 수 있습니다.

### 사전 요구 사항

- RTAV 설정 옵션이 데스크톱에 설치되어 있는지 확인합니다. 이 설정 옵션은 기본적으로 설치되지만 설치 중에 선택 취소할 수 있습니다. RTAV가 설치되어 있지 않으면 이 설정이 효과가 없습니다. Horizon Agent 설치에 대한 자세한 내용은 설치 문서를 참조하십시오.
- RTAV 그룹 정책 설정에 대해 Active Directory GPO가 생성되어 있는지 확인하십시오. GPO가 데스크톱이 포함된 OU에 링크되어 있어야 합니다. [Active Directory 그룹 정책 예제](#)를 참조하십시오.
- Active Directory 서버에서 Microsoft MMC와 그룹 정책 개체 편집기 스냅인을 사용할 수 있는지 확인하십시오.
- RTAV 그룹 정책 설정에 대한 내용을 숙지해야 합니다. [실시간 오디오-비디오 그룹 정책 설정](#)를 참조하십시오.

### 절차

- 1 Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`입니다. 여기서 `x.x.x`는 버전이고 `yyyyyyy`는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 파일의 압축을 풀고 ADMX 파일을 Active Directory 또는 RDS 호스트에 복사합니다.
  - a `vdm_agent_rtav.admx` 파일과 `ko-KR` 폴더를 Active Directory 또는 RDS 호스트의 `C:\Windows\PolicyDefinitions` 폴더에 복사합니다.
  - b (선택 사항) 언어 리소스 파일(`vdm_agent_rtav.adml`)을 Active Directory 또는 RDS 호스트의 `C:\Windows\PolicyDefinitions\`에 있는 적절한 하위 폴더에 복사합니다.
- 3 Active Directory 호스트에서 그룹 정책 관리 편집기를 열고 편집기에 템플릿 파일 경로를 입력합니다.

개별 RDS 호스트에서는 `gpedit.msc` 유틸리티를 사용하여 로컬 그룹 정책 편집기를 열 수 있습니다.

이 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > RTAV 구성 보기** 폴더에 있습니다.

## 다음에 수행할 작업

그룹 정책 설정을 구성하십시오.

## 실시간 오디오-비디오 그룹 정책 설정

RTAV(실시간 오디오-비디오) 그룹 정책 설정은 가상 웹캠의 최대 프레임 속도 및 최대 이미지 해상도를 제어합니다. 추가 설정을 통해 RTAV 기능을 사용하거나 사용하지 않도록 설정할 수 있습니다. 이러한 정책 설정은 물리적 디바이스가 연결된 클라이언트 시스템이 아니라 원격 데스크톱에 영향을 줍니다.

RTAV 그룹 정책 설정을 구성하지 않은 경우, RTAV에서는 클라이언트 시스템에 설정된 값을 사용합니다. 클라이언트 시스템에서 기본 웹캠 프레임 속도는 초당 15프레임입니다. 기본 웹캠 이미지 해상도는 320x240픽셀입니다.

해상도 그룹 정책 설정은 사용할 수 있는 최대 값을 결정합니다. 클라이언트 시스템에서 설정된 프레임 속도 및 해상도는 절댓값입니다. 예를 들어 최대 이미지 해상도에 대한 RTAV 설정을 640x480픽셀로 구성하는 경우 웹캠에는 클라이언트에서 최대 640x480픽셀로 설정된 모든 해상도를 표시합니다. 클라이언트에서 이미지 해상도를 640x480픽셀 이상의 값으로 설정하는 경우 클라이언트 해상도는 640x480픽셀로 제한됩니다.

일부 구성은 초당 25프레임에서 1920x1080 해상도의 최대 그룹 정책 설정을 충족하지 못할 수 있습니다. 주어진 해상도에 대해 구성으로 설정할 수 있는 최대 프레임 속도는 사용 중인 웹캠, 클라이언트 시스템 하드웨어, Horizon Agent 가상 하드웨어 및 사용 가능한 대역폭에 따라 달라집니다.

해상도 그룹 정책 설정은 사용자가 해상도 값을 설정하지 않은 경우에 사용되는 기본값을 결정합니다.

그룹 정책 설정	설명
Disable RTAV	이 설정을 사용하도록 설정하면 실시간 오디오-비디오 기능이 사용되지 않도록 설정됩니다. 이 설정이 구성되어 있지 않거나 사용하지 않도록 설정되어 있으면 실시간 오디오-비디오가 사용되도록 설정됩니다. 이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; View RTAV 구성</b> 폴더에 있습니다.
Max frames per second	웹캠이 프레임을 캡처할 수 있는 초당 최대 속도를 결정합니다. 이 설정을 사용하여 낮은 대역폭 네트워크 환경에서 웹캠 프레임 속도를 제한할 수 있습니다. 최솟값은 초당 1프레임입니다. 최대값은 초당 25프레임입니다. 이 설정이 구성되어 있지 않거나 사용하지 않도록 설정되어 있으면 최대 프레임 속도는 설정되지 않습니다. 실시간 오디오-비디오는 클라이언트 시스템의 웹캠에 대해 선택된 프레임 속도를 사용합니다. 기본적으로 클라이언트 웹캠은 초당 15프레임의 프레임 속도를 가지고 있습니다. 클라이언트 시스템에 구성된 설정이 없고 <b>초당 최대 프레임</b> 설정이 구성되어 있지 않거나 사용하지 않도록 설정되어 있는 경우, 웹캠은 초당 15프레임을 캡처합니다. 이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; View RTAV 구성 &gt; View RTAV 웹캠 설정</b> 폴더에 있습니다.

그룹 정책 설정	설명
Resolution - Max image width in pixels	<p>웹캠에서 캡처한 이미지 프레임의 최대 너비(픽셀 단위)를 결정합니다. 낮은 최대 이미지 너비를 설정하여 캡처된 프레임의 해상도를 낮추면 낮은 대역폭 네트워크 환경에서 이미지 환경을 향상시킬 수 있습니다.</p> <p>이 설정이 구성되어 있지 않거나 사용하지 않도록 설정되어 있으면 최대 이미지 너비는 설정되지 않습니다. RTAV는 클라이언트 시스템에서 설정된 이미지 너비를 사용합니다. 클라이언트 시스템의 웹캠 이미지에 대한 기본 너비는 320픽셀입니다.</p> <p>모든 웹캠 이미지의 최대 한도는 1920x1080픽셀입니다. 1920픽셀 이상의 값으로 이 설정을 구성하는 경우 효과적인 최대 이미지 너비는 1920픽셀입니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; View RTAV 구성 &gt; View RTAV 웹캠 설정</b> 폴더에 있습니다.</p>
Resolution - Max image height in pixels	<p>웹캠에서 캡처한 이미지 프레임의 최대 높이(픽셀 단위)를 결정합니다. 낮은 최대 이미지 높이를 설정하여 캡처된 프레임의 해상도를 낮추면 낮은 대역폭 네트워크 환경에서 이미지 환경을 향상시킬 수 있습니다.</p> <p>이 설정이 구성되어 있지 않거나 사용하지 않도록 설정되어 있으면 최대 이미지 높이는 설정되지 않습니다. RTAV는 클라이언트 시스템에서 설정된 이미지 높이를 사용합니다. 클라이언트 시스템의 웹캠 이미지에 대한 기본 높이는 240픽셀입니다.</p> <p>모든 웹캠 이미지의 최대 한도는 1920x1080픽셀입니다. 1080픽셀 이상의 값으로 이 설정을 구성하는 경우 효과적인 최대 이미지 높이는 1080픽셀입니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; View RTAV 구성 &gt; View RTAV 웹캠 설정</b> 폴더에 있습니다.</p>
Resolution - Default image resolution width in pixels	<p>웹캠에서 캡처한 이미지 프레임의 기본 해상도 너비(픽셀 단위)를 결정합니다. 이 설정은 사용자가 해상도 값을 지정하지 않은 경우에 사용됩니다.</p> <p>이 설정이 구성되어 있지 않거나 사용하지 않도록 설정되어 있으면 기본 이미지 너비는 320픽셀입니다.</p> <p>이 정책 설정을 사용하여 구성된 값은 View Agent 6.0 이상과 Horizon Client 3.0 이상을 함께 사용하는 경우에만 적용됩니다. 이전 버전의 View Agent와 Horizon Client에는 이 정책 설정이 영향을 주지 않으며 기본 이미지 너비는 320픽셀입니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; View RTAV 구성 &gt; View RTAV 웹캠 설정</b> 폴더에 있습니다.</p>
Resolution - Default image resolution height in pixels	<p>웹캠에서 캡처한 이미지 프레임의 기본 해상도 높이(픽셀 단위)를 결정합니다. 이 설정은 사용자가 해상도 값을 지정하지 않은 경우에 사용됩니다.</p> <p>이 설정을 구성하지 않거나 사용하지 않을 경우 기본 이미지 높이는 240픽셀입니다.</p> <p>이 정책 설정을 사용하여 구성된 값은 View Agent 6.0 이상과 Horizon Client 3.0 이상을 함께 사용하는 경우에만 적용됩니다. 이전 버전의 View Agent와 Horizon Client에는 이 정책 설정이 영향을 주지 않으며 기본 이미지 높이는 240픽셀입니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; View RTAV 구성 &gt; View RTAV 웹캠 설정</b> 폴더에 있습니다.</p>

## 실시간 오디오-비디오 대역폭

실시간 오디오-비디오 대역폭은 웹캠의 이미지 해상도 및 프레임 속도와 캡처되는 이미지 및 오디오 데이터에 따라 달라집니다.

**표 2-3. Horizon Client에서 Horizon Agent로 실시간 오디오-비디오 데이터를 전송하기 위한 샘플 대역폭 결과**에 나와 있는 샘플 테스트는 표준 웹캠 및 오디오 입력 디바이스가 장착된 View 환경에서 실시간 오디오-비디오가 사용하는 대역폭을 측정합니다. 이러한 테스트는 Horizon Client에서 Horizon Agent로 비디오 및 오디오 데이터를 전송하는 데 필요한 대역폭을 측정합니다. Horizon Client에서 데스크톱 세션을 실행하는 데 필요한 총 대역폭은 이 측정된 값보다 클 수 있습니다. 이러한 테스트에서 웹캠은 각 이미지 해상도에 대해 초당 15 프레임에서 이미지를 캡처합니다.

표 2-3. Horizon Client에서 Horizon Agent로 실시간 오디오-비디오 데이터를 전송하기 위한 샘플 대역폭 결과

이미지 해상도(너비 x 높이)	사용되는 대역폭(Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

## 스캐너 리디렉션 구성

스캐너 리디렉션을 사용하여 Horizon 7 사용자는 클라이언트 컴퓨터에 로컬로 연결된 스캔 및 이미지 생성 디바이스를 통해 원격 데스크톱과 애플리케이션의 정보를 스캔할 수 있습니다. 스캐너 리디렉션은 Horizon 6.0.2 이상 릴리스에서 사용할 수 있습니다.

스캐너 리디렉션은 TWAIN 및 WIA 형식과 호환 가능한 표준 스캔 및 이미지 생성 디바이스를 지원합니다.

스캐너 리디렉션 설정 옵션과 함께 Horizon Agent를 설치하면 추가 구성 작업을 수행하지 않아도 원격 데스크톱과 애플리케이션에서 이 기능이 작동합니다. 원격 데스크톱 또는 애플리케이션에서 스캐너 전용 드라이버를 구성할 필요가 없습니다.

기본값을 변경하여 특정 스캔 및 이미지 생성 애플리케이션 또는 환경에 적용하도록 그룹 정책 설정을 구성할 수 있습니다. 기능을 함께 사용하거나 사용하지 않도록 설정하는 정책을 설정할 수도 있습니다. ADMX 템플릿 파일을 사용하여 Active Directory 또는 개별 데스크톱에 스캐너 리디렉션 그룹 정책 설정을 설치할 수 있습니다. [스캐너 리디렉션 그룹 정책 설정 구성](#)를 참조하십시오.

스캔 데이터가 원격 데스크톱 또는 애플리케이션으로 리디렉션되는 경우 로컬 컴퓨터에서 스캔 또는 이미지 생성 디바이스에 액세스할 수 없습니다. 이와 반대로 디바이스가 로컬 컴퓨터에서 사용 중인 경우 원격 데스크톱 또는 애플리케이션에서 디바이스에 액세스할 수 없습니다.

## 스캐너 리디렉션에 대한 시스템 요구 사항

스캐너 리디렉션을 지원하려면 Horizon 7 배포가 특정 소프트웨어 및 하드웨어 요구 사항을 충족해야 합니다.

### Horizon 7 원격 데스크톱 또는 애플리케이션

이 기능은 단일 사용자 가상 시스템에 배포된 VDI 데스크톱, RDS 데스크톱 및 RDS 애플리케이션에서 지원됩니다.

스캐너 리디렉션 설정 옵션을 선택하고 View Agent 6.0.2 이상을 상위 또는 템플릿 가상 시스템이나 RDS 호스트에 설치해야 합니다.

Windows 데스크톱 및 Windows Server 게스트 운영 체제에서는 기본적으로 Horizon Agent 스캐너 리디렉션 설정 옵션이 선택되지 않습니다.

단일 사용자 가상 시스템 및 RDS 호스트(참고 사항이 표시되는 경우)에서 지원되는 게스트 운영 체제는 다음과 같습니다.

- 32비트 또는 64비트 Windows 7
- 32비트 또는 64비트 Windows 8.x
- 32비트 또는 64비트 Windows 10
- Windows Server 2008 R2(데스크톱 또는 RDS 호스트로 구성)
- Windows Server 2012 R2(데스크톱 또는 RDS 호스트로 구성)

---

**중요** 데스크톱 환경 기능은 Windows Server 게스트 운영 체제가 데스크톱 또는 RDS 호스트로 구성되었는지 여부와 상관없이 게스트 운영 체제에 설치되어야 합니다.

---

스캐너 디바이스 드라이버는 Horizon Agent가 설치된 데스크톱 운영 체제에 설치하지 않아도 됩니다.

#### Horizon Client 소프트웨어

Windows용 Horizon Client 3.2 이상 릴리스

#### Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

지원되는 운영 체제:

- 32비트 또는 64비트 Windows 7
- 32비트 또는 64비트 Windows 8.x
- 32비트 또는 64비트 Windows 10

스캐너 디바이스 드라이버가 설치되어 있어야 하며, 클라이언트 컴퓨터에서 스캐너를 작동할 수 있어야 합니다.

#### 스캔 디바이스 표준

TWAIN 또는 WIA

#### Horizon 7에 대한 디스플레이 프로토콜


PCoIP

RDP 데스크톱 세션에서는 스캐너 리디렉션이 지원되지 않습니다.

## 스캐너 리디렉션의 사용자 작업

스캐너 리디렉션을 사용하여 사용자는 클라이언트 컴퓨터에 연결된 물리적 스캐너 및 이미지 생성 디바이스를 원격 데스크톱 및 애플리케이션에서 스캔 작업을 수행하는 가상 디바이스로 조작할 수 있습니다.

사용자는 로컬로 연결된 클라이언트 컴퓨터에서 스캐너를 사용하는 방식과 거의 비슷하게 가상 스캐너를 조작할 수 있습니다.

- Horizon Agent와 함께 스캐너 리디렉션 옵션이 설치되면 스캐너 도구 트레이 아이콘()이 데스크톱에 추가됩니다. RDS 애플리케이션에서 도구 트레이 아이콘은 로컬 클라이언트 컴퓨터로 리디렉션됩니다.



스캐너 도구 트레이 아이콘은 사용할 필요가 없습니다. 스캔 리디렉션은 추가 구성 없이 작동합니다. 두 개 이상의 디바이스가 클라이언트 컴퓨터에 연결된 경우 아이콘을 사용하여 사용할 디바이스 변경과 같은 옵션을 구성할 수 있습니다.

- 스캐너 아이콘을 클릭하면 VMware Horizon용 스캐너 리디렉션 메뉴가 표시됩니다. 호환되지 않는 스캐너가 클라이언트 컴퓨터에 연결된 경우 메뉴 목록에 스캐너가 나타나지 않습니다.
- 기본적으로 스캔 디바이스는 자동으로 선택됩니다. TWAIN 및 WIA 스캐너는 개별적으로 선택됩니다. 하나의 TWAIN 스캐너와 하나의 WIA 스캐너를 동시에 선택할 수 있습니다.
- 로컬로 연결된 두 개 이상의 스캐너가 구성되어 있는 경우 기본적으로 선택된 스캐너가 아닌 다른 스캐너를 선택할 수 있습니다.
- WIA 스캐너는 **이미지 생성 디바이스** 아래에 있는 원격 데스크톱의 디바이스 관리자 메뉴에 표시됩니다. WIA 스캐너의 이름은 **VMware 가상 WIA 스캐너**입니다.
- VMware Horizon용 스캐너 리디렉션 메뉴에서 **환경설정** 옵션을 클릭하고 다양한 옵션(예: 스캐너 리디렉션 메뉴에서 웹캠 숨기기 및 기본 스캐너 선택 방법 결정)을 선택할 수 있습니다.

또한 Active Directory에서 스캐너 리디렉션 그룹 정책 설정을 구성하여 이러한 기능을 제어할 수 있습니다. [스캐너 리디렉션 그룹 정책 설정](#)의 내용을 참조하십시오.

- TWAIN 스캐너를 작동시키면 VMware Horizon용 TWAIN 스캐너 리디렉션 메뉴에 이미지 영역 선택, 색상/흑백/회색조 스캔 및 기타 공통 기능 선택과 같은 추가 옵션이 제공됩니다.
- 기본적으로 창을 표시하지 않는 TWAIN 스캔 소프트웨어에 대해 TWAIN 사용자 인터페이스 창을 표시하기 위해 VMware Horizon 스캐너 리디렉션 환경설정 대화상자에서 **항상 스캐너 설정 대화상자 표시** 옵션을 선택할 수 있습니다.

대부분의 TWAIN 스캔 소프트웨어는 기본적으로 TWAIN 사용자 인터페이스 창을 표시합니다. 이 소프트웨어의 경우 **항상 스캐너 설정 대화상자 표시** 옵션을 선택하는지 여부에 상관없이 창이 항상 표시됩니다.

**참고** 서로 다른 팜에서 호스팅되는 두 개의 RDS 애플리케이션을 실행하는 경우 클라이언트 컴퓨터에 두 개의 스캐너 리디렉션 도구 트레이 아이콘이 나타납니다. 일반적으로 하나의 스캐너만 클라이언트 컴퓨터에 연결됩니다. 이 경우 두 아이콘은 동일한 디바이스를 작동시키며 어떤 아이콘을 선택해도 상관 없습니다. 일부 경우에 로컬로 연결된 두 개의 스캐너가 있을 수 있으며 서로 다른 팜에서 실행되는 두 개의 RDS 애플리케이션을 실행할 수 있습니다. 이 경우 각 아이콘을 열어서 어떤 스캐너 리디렉션 메뉴가 어떤 RDS 애플리케이션을 제어하는지 확인해야 합니다.

리디렉션된 스캐너를 작동하기 위한 최종 사용자 지침은 “Windows용 VMware Horizon Client 사용” 문서를 참조하십시오.

## 스캐너 리디렉션 그룹 정책 설정 구성

Horizon 7 데스크톱 및 애플리케이션에서 스캐너 리디렉션의 동작을 제어하는 그룹 정책 설정을 구성할 수 있습니다. 이러한 정책 설정을 사용하여 사용자 데스크톱 및 애플리케이션의 VMware Horizon 스캐너 리디렉션 환경설정 대화상자에 제공되는 옵션을 Active Directory에서 중앙 집중식으로 제어할 수 있습니다.



이러한 정책 설정을 구성하지 않아도 됩니다. 스캐너 리디렉션은 원격 데스크톱과 클라이언트 시스템의 스캔 디바이스에 대해 구성된 기본 설정을 사용하여 작동합니다.

이러한 정책 설정은 원격 데스크톱과 애플리케이션에 적용되지만 실제 스캐너가 연결되어 있는 클라이언트 시스템에는 영향을 주지 않습니다. 데스크톱과 애플리케이션에서 이러한 설정을 구성하려면 Active Directory에 스캐너 리디렉션 그룹 정책 관리 템플릿(ADMX) 파일을 추가하십시오.

## Active Directory에 스캐너 리디렉션 ADMX 템플릿 추가

스캐너 리디렉션 ADMX 템플릿 파일(C:\Windows\PolicyDefinitions\W)의 정책 설정을 Active Directory의 GPO(그룹 정책 개체)에 추가하고 그룹 정책 개체 편집기에서 이 설정을 구성할 수 있습니다.

### 사전 요구 사항

- 스캐너 리디렉션 설정 옵션이 데스크톱과 RDS 호스트에 설치되어 있는지 확인합니다. 스캐너 리디렉션이 설치되어 있지 않은 경우 그룹 정책 설정이 아무런 영향을 주지 않습니다. Horizon Agent 설치에 대한 자세한 내용은 설치 문서를 참조하십시오.
- 스캐너 리디렉션 그룹 정책 설정에 대해 Active Directory GPO가 생성되어 있는지 확인합니다. GPO가 데스크톱과 RDS 호스트가 포함된 OU에 연결되어 있어야 합니다. [Active Directory 그룹 정책 예제](#)를 참조하십시오.
- Active Directory 서버에서 MMC와 그룹 정책 개체 편집기 스냅인을 사용할 수 있는지 확인합니다.
- 스캐너 리디렉션 그룹 정책 설정에 대한 내용을 숙지해야 합니다. [스캐너 리디렉션 그룹 정책 설정](#)을 참조하십시오.

### 절차

- 1 Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip입니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일의 압축을 풀고 ADMX 파일을 Active Directory 또는 RDS 호스트에 복사합니다.
  - a vdm\_agent\_scanner.admx 파일과 ko-KR 폴더를 Active Directory 또는 RDS 호스트의 C:\Windows\PolicyDefinitions 폴더에 복사합니다.
  - b (선택 사항) 언어 리소스 파일(vdm\_agent\_scanner.adml)을 Active Directory 또는 RDS 호스트의 C:\Windows\PolicyDefinitions\W에 있는 적절한 하위 폴더에 복사합니다.

- 3** Active Directory 호스트에서 그룹 정책 관리 편집기를 열고 편집기에 템플릿 파일 경로를 입력합니다.

개별 RDS 호스트에서는 gpedit.msc 유틸리티를 사용하여 로컬 그룹 정책 편집기를 열 수 있습니다.

이 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > 스캐너 리디렉션** 폴더에 있습니다.

대부분의 설정이 **사용자 구성 > 정책 > 관리 템플릿 > 스캐너 리디렉션** 폴더의 **사용자 구성** 폴더에도 추가됩니다.

다음에 수행할 작업

그룹 정책 설정을 구성하십시오.

## 스캐너 리디렉션 그룹 정책 설정

스캐너 리디렉션 그룹 정책 설정은 사용자 데스크톱 및 애플리케이션의 VMware Horizon 스캐너 리디렉션 환경설정 대화상자에 제공되는 옵션을 제어합니다.

스캐너 리디렉션 ADMX 템플릿 파일에는 컴퓨터 구성 및 사용자 구성 정책이 둘 다 포함되어 있습니다. 사용자 구성 정책을 사용하여 VDI 데스크톱, RDS 데스크톱 및 RDS 애플리케이션의 사용자에게 대해 서로 다른 구성을 설정할 수 있습니다. 서로 다른 사용자 구성 정책은 사용자 데스크톱 세션 및 애플리케이션이 동일한 RDS 호스트에서 실행 중인 경우에도 적용할 수 있습니다. 모든 설정은 그룹 정책 관리 편집기의 **VMware Horizon Agent 구성 > 스캐너 리디렉션** 폴더에 있습니다.

그룹 정책 설정	컴퓨터	사용자	설명
Disable functionality	X		스캐너 리디렉션 기능을 사용하지 않습니다. 이 설정을 사용하도록 설정하면 스캐너를 리디렉션할 수 없으며 사용자 데스크톱 및 애플리케이션의 스캐너 메뉴에 스캐너가 표시되지 않습니다. 이 설정을 사용하지 않도록 설정하거나 구성하지 않으면 스캐너 리디렉션이 작동하며 스캐너 메뉴에 스캐너가 표시됩니다.
Lock config	X		스캐너 리디렉션 사용자 인터페이스를 잠그고 사용자가 자신의 데스크톱 및 애플리케이션에서 구성 옵션을 변경하지 못하게 합니다. 이 설정을 사용하도록 설정하면 사용자는 자신의 데스크톱 및 애플리케이션의 트레이 메뉴에 제공되는 옵션을 구성할 수 없습니다. 사용자는 VMware Horizon 스캐너 리디렉션 환경설정 대화상자를 표시할 수 있지만 옵션이 비활성화되어 옵션을 변경할 수 없습니다. 이 설정을 사용하지 않도록 설정하거나 구성하지 않으면 사용자는 VMware Horizon 스캐너 리디렉션 환경설정 대화상자의 옵션을 구성할 수 있습니다.

그룹 정책 설정	컴퓨터	사용자	설명
Compression		X	<p>원격 데스크톱 또는 애플리케이션으로 이미지를 전송하는 동안 이미지 압축 비율을 설정합니다. 다음과 같은 압축 모드 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>사용 안 함.</b> 이미지 압축을 사용하지 않습니다.</li> <li>■ <b>무손실.</b> 이미지 품질이 떨어지지 않는 무손실(zlib) 압축을 사용합니다.</li> <li>■ <b>JPEG.</b> 품질이 떨어지는 JPEG 압축을 사용합니다. <b>JPEG 압축 품질</b> 필드에 이미지 품질 수준을 지정할 수 있습니다. JPEG 압축 품질은 0과 100 사이의 값이어야 합니다.</li> </ul> <p>이 설정을 사용하도록 설정하면 선택한 압축 모드가 이 정책의 영향을 받는 모든 사용자에게 대해 설정됩니다. 그러나 사용자는 VMware Horizon 스캐너 리디렉션 환경설정 대화상자의 <b>압축 옵션</b>을 변경하여 정책 설정을 재정의할 수 있습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 <b>JPEG</b> 압축 모드가 사용됩니다.</p>
Hide Webcam	X	X	<p>VMware Horizon 스캐너 리디렉션 환경설정 대화상자의 스캐너 선택 메뉴에 웹캠이 표시되지 않게 합니다.</p> <p>기본적으로 웹캠은 데스크톱 및 애플리케이션으로 리디렉션할 수 있습니다. 사용자는 웹캠을 선택하고 해당 웹캠을 가상 스캐너로 사용하여 이미지를 캡처할 수 있습니다.</p> <p>이 설정을 컴퓨터 구성 정책으로 사용하면 영향을 받는 컴퓨터의 모든 사용자에게 웹캠이 숨겨집니다. 사용자는 VMware Horizon 스캐너 리디렉션 환경설정 대화상자에서 <b>웹캠 숨기기</b> 옵션을 변경할 수 없습니다.</p> <p>이 설정을 사용자 구성 정책으로 사용하면 영향을 받는 모든 사용자에게 웹캠이 숨겨집니다. 그러나 사용자는 VMware Horizon 스캐너 리디렉션 환경설정 대화상자에서 <b>웹캠 숨기기</b> 옵션을 변경할 수 있습니다.</p> <p>컴퓨터 구성 및 사용자 구성 둘 다에서 이 설정을 사용하도록 설정하면 컴퓨터 구성의 <b>웹캠 숨기기</b> 설정이 영향을 받는 컴퓨터의 모든 사용자에게 대한 사용자 구성의 해당하는 정책 설정을 재정의합니다.</p> <p>정책 구성에서 이 설정을 사용하지 않도록 설정하거나 구성하지 않으면 <b>웹캠 숨기기</b> 설정은 해당하는 정책 설정(사용자 구성 또는 컴퓨터 구성) 또는 VMware Horizon 스캐너 리디렉션 대화상자의 사용자 선택에 의해 결정됩니다.</p>
Default Scanner	X	X	<p>스캐너 자동 선택을 중앙 집중식으로 관리할 수 있도록 합니다.</p> <p>스캐너 자동 선택 옵션은 TWAIN 및 WIA 스캐너에 대해 개별적으로 선택합니다. 다음과 같은 자동 선택 옵션 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>없음</b> 스캐너를 자동으로 선택하지 않습니다.</li> <li>■ <b>자동 선택</b> 로컬로 연결된 스캐너를 자동으로 선택합니다.</li> <li>■ <b>마지막으로 사용된 스캐너</b> 마지막으로 사용된 스캐너를 자동으로 선택합니다.</li> <li>■ <b>지정됨/지정된 스캐너</b> 텍스트 상자에 입력하는 스캐너 이름을 선택합니다.</li> </ul> <p>이 설정을 컴퓨터 구성 정책으로 사용하면 영향을 받는 컴퓨터의 모든 사용자에게 대한 스캐너 자동 선택 모드가 이 설정을 통해 결정됩니다. 사용자는 VMware Horizon 스캐너 리디렉션 환경설정 대화상자에서 <b>기본 스캐너</b> 옵션을 변경할 수 없습니다.</p> <p>이 설정을 사용자 구성 정책으로 사용하면 영향을 받는 모든 사용자에게 대한 스캐너 자동 선택 모드가 이 설정을 통해 결정됩니다. 그러나 사용자는 VMware Horizon 스캐너 리디렉션 환경설정 대화상자에서 <b>기본 스캐너</b> 옵션을 변경할 수 있습니다.</p> <p>컴퓨터 구성 및 사용자 구성 둘 다에서 이 설정을 사용하도록 설정하면 컴퓨터 구성의 스캐너 자동 선택 모드가 영향을 받는 컴퓨터의 모든 사용자에게 대한 사용자 구성의 해당하는 정책 설정을 재정의합니다.</p> <p>정책 구성에서 이 설정을 사용하지 않도록 설정하거나 구성하지 않으면 스캐너 자동 선택 모드는 해당하는 정책 설정(사용자 구성 또는 컴퓨터 구성) 또는 VMware Horizon 스캐너 리디렉션 대화상자의 사용자 선택에 의해 결정됩니다.</p>

## 직렬 포트 리디렉션 구성

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

직렬 포트 리디렉션은 Windows용 Horizon Client 3.4 이상 릴리스가 있는 Horizon 6 버전 6.1.1 이상 릴리스에서 사용할 수 있습니다.

Horizon Agent를 설치하고 직렬 포트 리디렉션 기능을 설정하면 추가 구성을 하지 않아도 원격 데스크톱에서 해당 기능을 사용할 수 있습니다. 예를 들어 원격 데스크톱에 이미 COM 포트가 있더라도 로컬 클라이언트 시스템의 COM1은 원격 데스크톱에서 COM1으로 리디렉션되고, COM2는 COM2로 리디렉션됩니다. 이미 원격 데스크톱에 COM 포트가 있는 경우에는 충돌을 피하기 위해 해당 COM 포트가 매핑됩니다. 예를 들어 원격 데스크톱에 이미 COM1 및 COM2가 있으면 클라이언트의 COM1은 기본적으로 COM3에 매핑됩니다. 원격 데스크톱에서 COM 포트를 구성하거나 디바이스 드라이버를 설치할 필요가 없습니다.

리디렉션된 COM 포트를 활성 상태로 만들려면 데스크톱 세션 동안 직렬 포트 도구 트레이 아이콘의 메뉴에서 **연결** 옵션을 선택합니다. 또한 사용자가 원격 데스크톱에 로그인할 때마다 자동으로 연결되도록 COM 포트 디바이스를 설정할 수도 있습니다. [직렬 포트 리디렉션의 사용자 작업을](#) 참조하십시오.

기본 구성을 변경하도록 그룹 정책 설정을 구성할 수 있습니다. 예를 들어 사용자가 COM 포트 매핑 또는 속성을 변경할 수 없도록 설정을 잠글 수 있습니다. 기능을 함께 사용하거나 사용하지 않도록 설정하는 정책을 설정할 수도 있습니다. ADMX 템플릿 파일을 사용하여 Active Directory 또는 개별 데스크톱에 직렬 포트 리디렉션 그룹 정책 설정을 설치할 수 있습니다. [직렬 포트 리디렉션 그룹 정책 설정 구성](#)을 참조하십시오.

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

## 직렬 포트 리디렉션에 대한 시스템 요구 사항

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

### 원격 데스크톱

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

단일 세션 가상 시스템에서 다음 게스트 운영 체제가 지원됩니다.

- 32비트 또는 64비트 Windows 7
- 32비트 또는 64비트 Windows 8.x
- 32비트 또는 64비트 Windows 10

- Windows Server 2008 R2(데스크톱으로 구성)
- Windows Server 2012 R2(데스크톱으로 구성)
- Windows Server 2016(데스크톱으로 구성)

이 기능은 현재 Windows Server RDS 호스트에서는 지원되지 않습니다.

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

### Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

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


### 디스플레이 프로토콜

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

RDP 데스크톱 세션에서는 VMware Horizon 직렬 포트 리디렉션이 지원되지 않습니다.

## 직렬 포트 리디렉션의 사용자 작업

사용자는 클라이언트 컴퓨터에 연결되어 있는 물리적 COM 포트 디바이스를 작동시키고 직렬 포트 가상화를 사용하여 디바이스를 원격 데스크톱에 연결할 수 있습니다. 이렇게 하면 타사 애플리케이션에서 디바이스에 액세스할 수 있습니다.

- Horizon Agent와 함께 직렬 포트 리디렉션 옵션이 설치되면 직렬 포트 도구 트레이 아이콘()이 원격 데스크톱에 추가됩니다. 게시된 애플리케이션의 경우 아이콘이 로컬 클라이언트 컴퓨터로 리디렉션됩니다.

이 아이콘은 필요한 Horizon Agent 버전 및 Windows용 Horizon Client를 사용하고 있으며 PCoIP를 통해 연결하는 경우에만 표시됩니다. Mac, Linux 또는 모바일 클라이언트에서 원격 데스크톱에 연결하는 경우에는 이 아이콘이 나타나지 않습니다.

이 아이콘을 사용하여 매핑된 COM 포트를 연결, 연결 해제 및 사용자 지정하기 위한 옵션을 구성할 수 있습니다.

- 직렬 포트 아이콘을 클릭하면 **VMware Horizon용 직렬 COM 리디렉션** 메뉴가 나타납니다.
- 기본적으로 로컬로 연결된 COM 포트는 원격 데스크톱의 해당 COM 포트에 매핑됩니다. 예: **COM3에 매핑된 COM1**. 매핑된 포트는 기본적으로 연결되어 있지 않습니다.

- 매핑된 COM 포트를 사용하려면 **VMware Horizon용 직렬 COM 리디렉션** 메뉴에서 **연결** 옵션을 수동으로 선택하거나, 그룹 정책 설정을 구성하는 과정 또는 이전 데스크톱 세션 중에 **자동 연결** 옵션을 설정해야 합니다. **자동 연결**은 원격 데스크톱 세션이 시작될 때 자동으로 연결되도록 매핑된 포트를 구성합니다.

- **연결** 옵션을 선택하면 리디렉션된 포트가 활성화됩니다. 원격 데스크톱의 게스트 운영 체제에 있는 디바이스 관리자에서 리디렉션된 포트는 **VMware Horizon용 직렬 포트 리디렉터(COMn)**로 표시됩니다.

COM 포트가 연결되면 타사 애플리케이션에서 해당 포트를 열 수 있습니다. 이 애플리케이션은 클라이언트 시스템에 연결된 COM 포트 디바이스와 데이터를 교환할 수 있습니다. 애플리케이션에서 포트가 열려 있는 동안에는 **VMware Horizon용 직렬 COM 리디렉션** 메뉴에서 포트 연결을 해제할 수 없습니다.

COM 포트 연결을 끊으려면 애플리케이션에서 포트를 닫거나 애플리케이션을 닫아야 합니다. 그런 후 **연결 해제** 옵션을 선택하여 포트 연결을 해제하고 물리적 COM 포트를 클라이언트 컴퓨터에서 사용할 수 있도록 설정할 수 있습니다.

- **VMware Horizon용 직렬 COM 리디렉션** 메뉴에서 리디렉션된 포트를 마우스 오른쪽 버튼으로 클릭하고 **포트 속성** 명령을 선택할 수 있습니다.

COM 속성 대화 상자에서 원격 데스크톱 세션이 시작될 때 자동으로 연결되도록 포트를 구성하고, DSR(Data Set Ready) 신호를 무시하고, **사용자 지정 포트 이름** 드롭다운 목록에서 포트를 선택하여 클라이언트의 로컬 포트를 원격 데스크톱의 다른 COM 포트에 매핑할 수 있습니다.

원격 데스크톱 포트가 중복된 것으로 표시될 수 있습니다. 예를 들면 **COM1(중복됨)**이 표시될 수 있습니다. 이 경우 가상 시스템은 ESXi 호스트의 가상 하드웨어에 있는 COM 포트에 구성됩니다. 가상 시스템의 중복된 포트에 매핑되어 있는 경우에도 리디렉션된 포트를 사용할 수 있습니다. 가상 시스템은 ESXi 호스트 또는 클라이언트 시스템의 포트를 통해 직렬 데이터를 수신합니다.

- 게스트 운영 체제의 디바이스 관리자에서 **속성 > 포트 설정** 탭을 사용하여 리디렉션된 COM 포트에 대한 설정을 구성할 수 있습니다. 예를 들면 기본 전송 속도 및 데이터 비트를 설정할 수 있습니다. 그러나 애플리케이션이 포트 설정을 지정하는 경우 디바이스 관리자에서 구성한 설정은 무시됩니다.

리디렉션된 직렬 COM 포트를 작동하기 위한 최종 사용자 지침은 "Windows용 VMware Horizon Client 사용" 문서를 참조하십시오.

## 직렬 포트 리디렉션 구성 지침

그룹 정책 설정을 통해 직렬 포트 리디렉션을 구성하고 사용자가 리디렉션된 COM 포트를 사용자 지정할 수 있는 범위를 제어할 수 있습니다. 선택 옵션은 조직의 사용자 역할 및 타사 애플리케이션에 따라 다릅니다.

그룹 정책 설정에 대한 자세한 내용은 [직렬 포트 리디렉션 그룹 정책 설정](#)에 나와 있습니다.

- 사용자가 동일한 타사 애플리케이션 및 COM 포트 디바이스를 실행하는 경우 리디렉션된 포트가 동일한 방식으로 구성되어 있는지 확인하십시오. 예를 들어 POS(Point-of-Sale) 디바이스를 사용하는 은행 또는 소매점에서는 모든 COM 포트 디바이스가 클라이언트 끝점의 동일한 포트에 연결되어야 하고 모든 포트는 원격 데스크톱의 리디렉션된 동일한 COM 포트에 매핑되어야 합니다.



클라이언트 포트를 리디렉션된 포트에 매핑하도록 **PortSettings** 정책 설정을 지정합니다.

**PortSettings**에서 **Autoconnect** 항목을 선택하여 리디렉션된 포트가 각 데스크톱 세션 맨 처음에 연결되도록 합니다. **Lock Configuration** 정책 설정을 사용하도록 설정하여 사용자가 포트 매핑을 변경하거나 포트 구성을 사용자 지정하지 못하도록 합니다. 이 시나리오에서 사용자는 수동으로 연결하거나 연결을 해제할 필요가 없으며 실수로 리디렉션된 COM 포트에서 타사 애플리케이션에 액세스하지 못하게 지정하는 경우도 발생할 수 없습니다.

- 사용자가 다양한 타사 애플리케이션을 사용하는 지식 근로자이며 해당 클라이언트 컴퓨터에서 로컬로 COM 포트를 사용할 수도 있는 경우 리디렉션된 COM 포트에 연결하고 연결을 해제할 수 있는지 확인하십시오.

기본 포트 매핑이 올바르지 않은 경우 **PortSettings** 정책 설정을 지정할 수 있습니다. 사용자의 요구 사항에 따라 **Autoconnect** 항목을 설정할 수도 있고 설정하지 않을 수도 있습니다. **Lock Configuration** 정책 설정을 사용하도록 설정하지 않도록 합니다.

- 타사 애플리케이션이 원격 데스크톱에 매핑된 COM 포트를 여는지 확인합니다.
- 디바이스에 대해 사용되는 전송 속도는 타사 애플리케이션이 사용하려고 하는 전송 속도와 같아야 합니다.
- 클라이언트 시스템에서 원격 데스크톱으로 최대 5개의 COM 포트를 리디렉션할 수 있습니다.

## 직렬 포트 리디렉션 그룹 정책 설정 구성

원격 데스크톱에서 직렬 포트 리디렉션의 동작을 제어하는 그룹 정책 설정을 구성할 수 있습니다. 이러한 정책 설정을 사용하여 중앙의 Active Directory에서 사용자 데스크톱의 **VMware Horizon용 직렬 COM 리디렉션** 메뉴에서 사용할 수 있는 옵션을 제어할 수 있습니다.

이러한 정책 설정을 구성하지 않아도 됩니다. 직렬 포트 리디렉션은 원격 데스크톱과 클라이언트 시스템의 리디렉션된 COM 포트에 대해 구성된 기본 설정을 사용하여 작동합니다.

이러한 정책 설정은 물리적 COM 포트 디바이스가 연결된 클라이언트 시스템이 아닌 원격 데스크톱에 영향을 줍니다. 데스크톱에서 이러한 설정을 구성하려면 Active Directory에서 직렬 포트 리디렉션 그룹 정책 관리 템플릿(ADMX) 파일을 추가하십시오.

### Active Directory에 직렬 포트 리디렉션 ADMX 템플릿 추가

직렬 포트 리디렉션 ADMX 파일(`vdm_agent_serialport.admx`)의 정책 설정을 Active Directory의 GPO(그룹 정책 개체)에 추가하고 그룹 정책 개체 편집기에서 이 설정을 구성할 수 있습니다.

#### 사전 요구 사항

- 직렬 포트 리디렉션 설정 옵션이 데스크톱에 설치되어 있는지 확인합니다. 직렬 포트 리디렉션이 설치되어 있지 않은 경우 그룹 정책 설정이 아무런 영향을 주지 않습니다. Horizon Agent 설치에 대한 자세한 내용은 설치 문서를 참조하십시오.
- 직렬 포트 리디렉션 그룹 정책 설정에 대해 Active Directory GPO가 생성되어 있는지 확인합니다. GPO가 데스크톱이 포함된 OU에 링크되어 있어야 합니다. [Active Directory 그룹 정책 예제](#)를 참조하십시오.

- Active Directory 서버에서 MMC와 그룹 정책 개체 편집기 스냅인을 사용할 수 있는지 확인합니다.
- 직렬 포트 리디렉션 그룹 정책 설정에 대한 내용을 숙지해야 합니다. [직렬 포트 리디렉션 그룹 정책 설정](#)를 참조하십시오.

## 절차

- 1 Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip입니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일의 압축을 풀고 ADMX 파일을 Active Directory 또는 RDS 호스트에 복사합니다.
  - a vdm\_agent\_serialport.admx 파일과 ko-KR 폴더를 Active Directory 또는 RDS 호스트의 C:\Windows\PolicyDefinitions 폴더에 복사합니다.
  - b (선택 사항) 언어 리소스 파일(vdm\_agent\_serialport.adml)을 Active Directory 또는 RDS 호스트의 C:\Windows\PolicyDefinitions\에 있는 적절한 하위 폴더에 복사합니다.

- 3 Active Directory 호스트에서 그룹 정책 관리 편집기를 열고 편집기에 템플릿 파일 경로를 입력합니다.

개별 RDS 호스트에서는 gpedit.msc 유틸리티를 사용하여 로컬 그룹 정책 편집기를 열 수 있습니다.

이 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > 직렬 COM** 폴더에 있습니다.

대부분의 설정이 **사용자 구성 > 정책 > 관리 템플릿 > 직렬 COM** 폴더의 **사용자 구성** 폴더에도 추가됩니다.

## 다음에 수행할 작업

그룹 정책 설정을 구성하십시오.

## 직렬 포트 리디렉션 그룹 정책 설정

직렬 포트 리디렉션 그룹 정책 설정은 원격 데스크톱의 **VMware Horizon용 직렬 COM 리디렉션** 메뉴에서 사용할 수 있는 옵션을 비롯하여 리디렉션된 COM 포트 구성을 제어합니다.

직렬 포트 리디렉션 ADMX 파일에는 컴퓨터 구성 및 사용자 구성 정책이 모두 포함되어 있습니다. 사용자 구성 정책을 사용하여 VDI 데스크톱의 지정된 사용자를 대상으로 다른 구성을 설정할 수 있습니다. 컴퓨터 구성에서 구성된 정책 설정은 사용자 구성에서 구성된 해당 설정보다 우선적으로 적용됩니다.



그룹 정책 설정	컴퓨터	사용자	설명
PortSettings1 PortSettings2 PortSettings3 PortSettings4 PortSettings5	X	X	<p>포트 설정은 클라이언트 시스템의 COM 포트와 원격 데스크톱의 리디렉션된 COM 포트 간 매핑을 확인하고 리디렉션된 COM 포트에 영향을 주는 기타 설정을 확인합니다. 리디렉션된 각 COM 포트를 개별적으로 구성합니다.</p> <p>5개의 포트 설정 정책 설정을 사용할 수 있으므로 클라이언트에서 원격 데스크톱으로 COM 포트를 최대 5개까지 매핑할 수 있습니다. 구성하려는 각 COM 포트에 대해 하나의 포트 설정 정책 설정을 선택합니다. 포트 설정 정책 설정을 사용하도록 설정하는 경우 리디렉션된 COM 포트에 영향을 주는 다음 항목을 구성할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>소스 포트 번호</b> 설정은 클라이언트 시스템에 연결된 물리적 COM 포트의 수를 지정합니다.</li> <li>■ <b>대상 가상 포트 번호</b> 설정은 원격 데스크톱에 있는 리디렉션된 가상 COM 포트의 수를 지정합니다.</li> <li>■ <b>자동 연결</b> 설정은 각 데스크톱 세션이 시작될 때 COM 포트를 리디렉션된 COM 포트에 자동으로 연결합니다.</li> <li>■ <b>IgnoreDSR</b> 설정을 사용하면 리디렉션된 COM 포트 디바이스는 DSR(Data Set Ready) 신호를 무시합니다.</li> <li>■ <b>포트 닫기 전 일시 중지(밀리초)</b> 설정은 사용자가 리디렉션된 포트를 닫은 후, 포트가 실제로 닫히기 전까지 대기하는 시간(밀리초)을 지정합니다. 특정 USB-직렬 어댑터의 경우 전송된 데이터가 유지되도록 하려면 이러한 시간 지연이 필요합니다. 이 설정은 문제 해결을 위한 것입니다.</li> <li>■ <b>Serial2USBModeChangeEnabled</b> 설정은 GlobalSat BU353 GPS 어댑터를 비롯하여 Prolific 칩셋을 사용하는 USB-직렬 어댑터에 적용되는 문제를 해결합니다. Prolific 칩셋 어댑터에 대해 이 설정을 사용하지 않도록 설정하면 연결된 디바이스가 데이터를 전송할 수는 있지만 수신할 수는 없습니다.</li> <li>■ <b>대기 마스크의 오류 사용 안 함</b> 설정은 COM 포트 마스크의 오류 값을 사용하지 않도록 설정합니다. 특정 애플리케이션에는 이러한 문제 해결 설정이 필요합니다. 자세한 내용은 <a href="http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx</a>의 WaitCommEvent 함수에 대한 Microsoft 설명서를 참조하십시오.</li> <li>■ <b>HandleBtDisappear</b> 설정은 BlueTooth COM 포트 동작을 지원합니다. 이 설정은 문제 해결을 위한 것입니다.</li> <li>■ <b>UsbToComTroubleShooting</b> 설정은 USB-직렬 포트 어댑터와 관련된 일부 문제를 해결합니다. 이 설정은 문제 해결을 위한 것입니다.</li> </ul> <p>특정 COM 포트에 대해 포트 설정 정책 설정을 사용하도록 설정하면 사용자는 리디렉션된 포트를 연결 및 연결 해제할 수 있지만 원격 데스크톱에 대한 포트 속성은 구성할 수 없습니다. 예를 들어 사용자는 데스크톱에 로그인할 때 포트가 자동으로 리디렉션되도록 포트를 설정하거나 DSR 신호를 무시할 수 없습니다. 이러한 속성은 그룹 정책 설정을 통해 제어됩니다.</p> <p><b>참고</b> 리디렉션된 COM 포트는 물리적 COM 포트가 클라이언트 시스템에 로컬로 연결되는 경우에만 연결되고 활성화됩니다. 클라이언트에 존재하지 않는 COM 포트를 매핑하면 리디렉션된 포트가 비활성으로 나타나며 원격 데스크톱의 도구 트레이 메뉴에서 사용할 수 없게 됩니다.</p> <p>포트 설정 정책 설정이 사용되지 않도록 설정되거나 구성되지 않으면 리디렉션된 COM 포트는 원격 데스크톱에서 사용자가 구성하는 설정을 사용합니다. <b>VMware Horizon용 직렬 COM 리디렉션</b> 메뉴 옵션은 활성 상태이며 사용할 수 있습니다.</p> <p>이러한 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; 직렬 COM &gt; PortSettings</b> 폴더에 있습니다.</p>
Local settings priority	X	X	원격 데스크톱에서 구성된 설정에 우선 순위를 부여합니다.

그룹 정책 설정	컴퓨터	사용자	설명
			<p>이 정책을 사용하도록 설정하면 사용자가 원격 데스크톱에서 구성하는 직렬 포트 리디렉션 설정이 그룹 정책 설정보다 우선합니다. 그룹 정책 설정은 원격 데스크톱에 구성된 설정이 없는 경우에만 적용됩니다.</p> <p>이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우 그룹 정책 설정이 원격 데스크톱에서 구성된 설정보다 우선합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; 직렬 COM</b> 폴더에 있습니다.</p>
Disable functionality	X		<p>직렬 포트 리디렉션 기능을 사용하지 않도록 설정합니다.</p> <p>이 설정을 사용하도록 설정하면 COM 포트는 원격 데스크톱으로 리디렉션되지 않습니다. 원격 데스크톱에 직렬 포트 도구 트레이 아이콘이 표시되지 않습니다.</p> <p>이 설정을 사용하지 않도록 설정하면 직렬 포트 리디렉션이 작동하고, 직렬 포트 도구 트레이 아이콘이 표시되고, <b>VMware Horizon용 직렬 COM 리디렉션</b> 메뉴에 COM 포트가 표시됩니다.</p> <p>이 설정이 구성되지 않으면 원격 데스크톱에 대해 로컬인 설정에 따라 직렬 포트 리디렉션의 사용 여부가 결정됩니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; 직렬 COM</b> 폴더에 있습니다.</p>
Lock configuration	X	X	<p>직렬 포트 리디렉션 사용자 인터페이스를 잠그고 사용자가 원격 데스크톱에서 구성 옵션을 변경할 수 없게 합니다.</p> <p>이 설정을 사용하도록 설정하면 사용자는 자신의 데스크톱의 도구 트레이 메뉴에 제공되는 옵션을 구성할 수 없습니다. 사용자는 <b>VMware Horizon용 직렬 COM 리디렉션</b> 메뉴를 표시할 수 있지만 옵션은 비활성 상태이며 변경할 수 없습니다.</p> <p>이 설정을 사용하지 않도록 설정하면 사용자는 <b>VMware Horizon용 직렬 COM 리디렉션</b> 메뉴에서 옵션을 구성할 수 있습니다.</p> <p>이 설정이 구성되지 않으면 원격 데스크톱의 로컬 프로그램 설정에 따라 사용자가 COM 포트 리디렉션 설정을 구성할 수 있는지 여부가 결정됩니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; 직렬 COM</b> 폴더에 있습니다.</p>
Bandwidth limit	X		<p>리디렉션된 직렬 포트와 클라이언트 시스템 간의 데이터 전송 속도 제한(킬로바이트/초)을 설정합니다.</p> <p>이 설정을 사용하도록 설정하는 경우 리디렉션된 직렬 포트와 클라이언트 사이의 최대 데이터 전송 속도를 결정하는 <b>대역폭 제한(킬로바이트/초)</b> 상자에서 값을 설정할 수 있습니다. 0 값은 대역폭 제한을 사용하지 않도록 설정합니다.</p> <p>이 설정을 사용하지 않도록 설정하면 대역폭 제한이 설정되지 않습니다.</p> <p>이 설정이 구성되지 않으면 원격 데스크톱의 로컬 프로그램 설정에 따라 대역폭 제한 설정 여부가 결정됩니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; 직렬 COM</b> 폴더에 있습니다.</p>

## USB-직렬 어댑터 구성

Prolific 칩셋을 사용하는 USB-직렬 어댑터가 직렬 포트 리디렉션 기능에 의해 원격 데스크톱으로 리디렉션되도록 구성할 수 있습니다.

Prolific 칩셋 어댑터에서 데이터가 제대로 전송되게 하려면 Active Directory 또는 개별 데스크톱 가상 시스템에서 직렬 포트 리디렉션 그룹 정책 설정을 사용하도록 설정할 수 있습니다.

Prolific 칩셋 어댑터 문제를 해결하도록 그룹 정책 설정을 구성하지 않으면 연결된 디바이스가 데이터를 전송할 수는 있지만 수신할 수는 없습니다.

클라이언트 시스템에서 정책 설정 또는 레지스트리 키를 구성할 필요가 없습니다.

#### 사전 요구 사항

- 직렬 포트 리디렉션 설정 옵션이 데스크톱에 설치되어 있는지 확인합니다. 직렬 포트 리디렉션이 설치되어 있지 않은 경우 그룹 정책 설정이 아무런 영향을 주지 않습니다. Horizon Agent 설치에 대한 자세한 내용은 설치 문서를 참조하십시오.
- 직렬 포트 리디렉션 ADMX 템플릿 파일이 Active Directory 또는 데스크톱 가상 시스템에 추가되어 있는지 확인합니다.
- **PortSettings** 그룹 정책 설정의 **Serial2USBModeChangeEnabled** 항목을 숙지하십시오. [직렬 포트 리디렉션 그룹 정책 설정](#)를 참조하십시오.

#### 절차

- 1 Active Directory 또는 가상 컴퓨터에서 그룹 정책 개체 편집기를 엽니다.
- 2 **컴퓨터 구성 > 정책 > 관리 템플릿 > 클래식 관리 템플릿 > VMware View Agent 구성 > 직렬 COM** 폴더로 이동합니다.
- 3 **PortSettings** 폴더를 선택합니다.
- 4 **PortSettings** 그룹 정책 설정을 선택하고 사용하도록 설정합니다.
- 5 소스 및 대상 COM 포트 번호를 지정하여 COM 포트를 매핑합니다.
- 6 **Serial2USBModeChangeEnabled** 확인란을 선택합니다.
- 7 **PortSettings** 정책 설정의 다른 항목을 필요에 맞게 구성합니다.
- 8 **확인**을 클릭하고 그룹 정책 개체 편집기를 닫습니다.

USB-직렬 어댑터는 원격 데스크톱으로 리디렉션될 수 있으며, 사용자가 다음 데스크톱 세션을 시작할 때 데이터를 성공적으로 수신할 수 있습니다.

## Windows Media MMR(멀티미디어 리디렉션)에 대한 액세스 관리

Horizon 7는 단일 사용자 시스템에서 실행되는 VDI 데스크톱 및 RDS 데스크톱에 Windows Media MMR 기능을 제공합니다.

MMR은 멀티미디어 스트림을 클라이언트 컴퓨터로 직접 전달합니다. MMR을 사용하면 멀티미디어 스트림이 처리됩니다. 즉, 클라이언트 시스템에서 디코딩됩니다. 클라이언트 시스템은 미디어 콘텐츠를 재생하여 ESXi 호스트에 대한 요청 부담을 덜어줍니다.

MMR 데이터는 애플리케이션 기반 암호화 없이 네트워크를 통해 전송되며 리디렉션되는 콘텐츠에 따라 중요한 데이터를 포함하고 있을 수 있습니다. 이 데이터가 네트워크에서 모니터링되는 것을 방지하려면 보안 네트워크 상에서만 MMR을 사용하십시오.

보안 터널을 사용하는 경우 Horizon Client와 View Secure Gateway 간 MMR 연결의 보안은 유지되지만 View Secure Gateway에서 데스크톱 시스템으로의 연결은 암호화되지 않습니다. 보안 터널이 사용되지 않으면 Horizon Client에서 데스크톱 시스템으로의 MMR 연결은 암호화되지 않습니다.

## Horizon 7에서 멀티미디어 리디렉션 사용

몇 가지 단계를 수행하여 보안이 유지되는 Horizon 7 네트워크에 연결되어 있고 로컬 멀티미디어 디코딩을 처리할 리소스가 충분한 Horizon Client 시스템만 MMR에 액세스할 수 있게 할 수 있습니다.

기본적으로 View Administrator의 전역 정책인 **MMR(멀티미디어 리디렉션)**은 **거부**로 설정됩니다.

MMR을 사용하려면 이 값을 **허용**으로 명시적으로 설정해야 합니다.

개별 데스크톱 풀 또는 특정 사용자에게 대해 **MMR(멀티미디어 리디렉션)** 정책을 전역으로 사용하거나 사용하지 않도록 설정하여 MMR에 대한 액세스를 제어할 수 있습니다.

Horizon Administrator에서 전역 정책을 설정하는 지침은 [Horizon 7 정책](#) 항목을 참조하십시오.

## Windows Media MMR에 대한 시스템 요구 사항

Windows Media MMR(멀티미디어 리디렉션)을 지원하려면 Horizon 7 배포가 특정 소프트웨어 및 하드웨어 요구 사항을 충족해야 합니다. Windows Media MMR은 Horizon 6.0.2 이상 릴리스에서 제공됩니다.

### View 원격 데스크톱

- 이 기능은 단일 사용자 가상 시스템 및 RDS 데스크톱에 배포된 가상 시스템 데스크톱에서 지원됩니다.

RDS 데스크톱에서 이 기능을 지원하려면 View Agent 6.1.1 이상이 필요합니다.

단일 사용자 시스템에서 이 기능을 지원하려면 View Agent 6.0.2 이상이 필요합니다.

- 다음 게스트 운영 체제가 지원됩니다.
  - 64비트 또는 32비트 Windows 10. Windows Media Player가 지원됩니다. 기본 플레이어 TV 및 동영상은 지원되지 않습니다.
  - Windows Server 2016은 기술 미리보기 기능입니다. Windows Media Player가 지원됩니다. 기본 플레이어 TV 및 동영상은 지원되지 않습니다.
  - 64비트 또는 32비트 Windows 7 SP1 Enterprise 또는 Ultimate(단일 사용자 시스템). Windows 7 Professional은 지원되지 않습니다.
  - 64비트 또는 32비트 Windows 8/8.1 Professional 또는 Enterprise(단일 사용자 시스템)
  - Windows Server 2008 R2(RDS 호스트로 구성)
  - Windows Server 2012 및 2012 R2(RDS 호스트로 구성)

- **3D 렌더링**은 데스크톱 풀에서 사용하거나 사용하지 않도록 설정할 수 있습니다.
- 사용자는 Windows Media Player 12 이상 또는 Internet Explorer 8 이상에서 비디오를 재생해야 합니다.

Internet Explorer를 사용하려면 보호 모드를 사용하지 않도록 설정해야 합니다. 인터넷 옵션 대화상자에서 **보안** 탭을 클릭하고 **보호 모드 사용**의 선택을 취소합니다.

## Horizon Client 소프트웨어

단일 사용자 시스템에서 Windows Media MMR을 지원하려면 Windows용 Horizon Client 3.2 이상 릴리스가 필요합니다.

## Horizon Client 컴퓨터 또는 클라이언트 액세스 디바이스

- 클라이언트는 64비트 또는 32비트 Windows 7, Windows 8/8.1 또는 Windows 10 운영 체제를 실행해야 합니다.

## 지원되는 미디어 형식

Windows Media Player에서 지원되는 미디어 형식이 모두 지원됩니다. 예: M4V, MOV, MP4, WMP, MPEG-4 Part 2, WMV 7, 8 및 9, WMA, AVI, ACE, MP3, WAV.

**참고** DRM 보호 콘텐츠는 Windows Media MMR을 통해 리디렉션되지 않습니다.

## Horizon 정책

Horizon Administrator에서 **MMR(멀티미디어 리디렉션)** 정책을 허용으로 설정합니다. 기본값은 **거부**입니다.

## 백엔드 방화벽

Horizon 7 배포에 DMZ 기반 보안 서버와 내부 네트워크 간의 백엔드 방화벽이 포함되어 있는 경우 해당 백엔드 방화벽이 데스크톱의 포트 9427에 대한 트래픽을 허용하는지 확인합니다.

## 네트워크 지연 시간을 기반으로 Windows Media MMR을 사용할지 여부 결정

기본적으로 Windows Media MMR은 Windows 8에서 실행되는 단일 사용자 데스크톱 및 Windows Server 2012 또는 2012 R2 이상에서 실행되는 RDS 데스크톱에서 네트워크 조건에 맞게 조정됩니다. Horizon Client와 원격 데스크톱 간의 네트워크 지연 시간이 29밀리초 이하인 경우 비디오가 Windows Media MMR을 통해 리디렉션됩니다. 네트워크 지연 시간이 30밀리초 이상인 경우 비디오가 리디렉션되지 않습니다. 대신 ESXi 호스트에서 렌더링되고 PCoIP를 통해 클라이언트로 전송됩니다.

이 기능은 Windows 8 이상 단일 사용자 데스크톱 및 Windows Server 2012 또는 2012 R2 이상 RDS 데스크톱에 적용됩니다. 사용자는 지원되는 모든 클라이언트 시스템, Windows 7 또는 Windows 8/8.1을 실행할 수 있습니다.

이 기능은 Windows 7 단일 사용자 데스크톱 또는 Windows Server 2008 R2 RDS 데스크톱에 적용되지 않습니다. 이러한 게스트 운영 체제에서 Windows Media MMR은 네트워크 지연 시간에 관계없이 항상 멀티미디어 리디렉션을 수행합니다.

데스크톱에서 RedirectionPolicy 레지스트리 설정을 구성하여 강제로 Windows Media MMR이 네트워크 지연 시간에 관계없이 멀티미디어 리디렉션을 수행하도록 이 기능을 재정의할 수 있습니다.

### 절차

1 원격 데스크톱에서 Windows 레지스트리 편집기를 시작합니다.

2 리디렉션 정책을 제어하는 Windows 레지스트리 키로 이동합니다.

원격 데스크톱에 구성하는 레지스트리 키는 Windows Media Player의 비트 버전에 따라 달라집니다.

옵션	설명
<b>64비트 Windows Media Player</b>	<ul style="list-style-type: none"> <li>64비트 데스크톱에서는 다음 레지스트리 키를 사용합니다. HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware tsmmr</li> </ul>
<b>32비트 Windows Media Player</b>	<ul style="list-style-type: none"> <li>32비트 데스크톱에서는 다음 레지스트리 키를 사용합니다. HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware tsmmr</li> <li>64비트 데스크톱에서는 다음 레지스트리 키를 사용합니다. HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware tsmmr</li> </ul>

3 RedirectionPolicy 값을 always로 설정합니다.

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

4 업데이트 값을 적용하려면 데스크톱에서 Windows Media Player를 다시 시작합니다.

## 클라이언트 드라이브 리디렉션에 대한 액세스 관리

클라이언트 드라이브 리디렉션을 사용하여 Horizon Client 3.5 이상과 View Agent 6.2 이상 또는 Horizon Agent 7.0 이상을 배포하면 폴더와 파일이 암호화가 제공되는 네트워크를 통해 전송됩니다. 클라이언트와 View Secure Gateway 간의 클라이언트 드라이브 리디렉션 연결 및 View Secure Gateway와 데스크톱 시스템 간의 연결은 안전합니다.

Horizon Client 4.2 또는 Horizon 7 버전 7.0.2 이상의 경우, VMware Blast Extreme이 사용하도록 설정되어 있으면 암호화를 사용하는 가상 채널을 통해 파일 및 폴더가 전송됩니다.

이전 클라이언트 또는 에이전트 릴리스에서는 클라이언트 드라이브 리디렉션 폴더 및 파일이 암호화 없이 네트워크 전반에서 전송되며 리디렉션되는 콘텐츠에 따라 중요한 데이터가 포함될 수 있습니다. 보안 터널이 사용되면 Horizon Client와 View Secure Gateway 간 클라이언트 드라이브 리디렉션 연결의 보안은 유지되지만 View Secure Gateway에서 데스크톱 시스템으로의 연결은 암호화되지 않습니다. 보안 터널을 사용하지 않도록 설정된 경우에는 Horizon Client에서 데스크톱 시스템으로의 클라이언트 드라이브 리디렉션 연결이 암호화되지 않습니다. 이 데이터를 네트워크에서 모니터링할 수 없게 하려면 Horizon Client가 버전 3.5보다 오래되었거나 에이전트가 버전 6.2보다 오래된 경우에 보안 네트워크에서만 클라이언트 드라이브 리디렉션을 사용합니다.

에이전트 설치 관리자에서 **클라이언트 드라이브 리디렉션** 설정 옵션은 기본적으로 선택되어 있습니다. 가장 좋은 방법은 사용자에게 이 기능이 필요한 경우에만 데스크톱에 **클라이언트 드라이브 리디렉션** 설정 옵션을 사용하도록 설정하는 것입니다.

## 그룹 정책을 사용하여 클라이언트 드라이브 리디렉션 사용 안 함

Active Directory에 있는 RDS 호스트와 원격 데스크톱에 대해 Microsoft 원격 데스크톱 서비스 그룹 정책 설정을 구성하여 클라이언트 드라이브 리디렉션을 사용하지 않도록 설정할 수 있습니다.

클라이언트 드라이브 리디렉션에 대한 자세한 사항은 "VMware Horizon Client 사용" 문서의 특정 데스크톱 클라이언트 디바이스 유형을 참조하십시오. 자세한 사항은 [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html)의 내용을 참조하십시오.

**참고** 이 설정은 로컬 레지스트리와 클라이언트 드라이브 리디렉션 기능을 사용하도록 설정하는 스마트 정책 설정을 재정의합니다.

### 사전 요구 사항

View 배포에 DMZ 기반 보안 서버와 내부 네트워크 간의 백엔드 방화벽이 포함되어 있는 경우 해당 백엔드 방화벽이 단일 사용자 및 RDS 데스크톱의 포트 9427에 대한 트래픽을 허용하는지 확인합니다. 클라이언트 드라이브 리디렉션을 지원하려면 포트 9427의 TCP 연결이 필요합니다.

Horizon Client 4.2 또는 Horizon 7 버전 7.0.2 이상의 경우 클라이언트 드라이브 리디렉션으로 가상 채널을 통해 데이터를 전송하기 때문에 VMware Blast Extreme이 사용하도록 설정된 경우에는 포트 9427을 열지 않아도 됩니다.

### 절차

- 1 그룹 정책 편집기에서 **컴퓨터 구성\정책\관리 템플릿\Windows 구성 요소\원격 데스크톱 서비스\원격 데스크톱 세션 호스트\디바이스 및 리소스 리디렉션**으로 이동합니다.

이 탐색 경로는 Windows Server 2012의 Active Directory에 사용됩니다. Windows 운영 체제에 따라 탐색 경로는 달라집니다.

- 2 **드라이브의 리디렉션을 허용하지 않음** 그룹 정책 설정을 사용하도록 설정합니다.

## 레지스트리 설정을 사용하여 클라이언트 드라이브 리디렉션 구성

Windows 레지스트리 키 설정을 사용하여 원격 데스크톱에서 클라이언트 드라이브 리디렉션 동작을 설정할 수 있습니다. 이 기능에는 Horizon Agent 7.0 이상 및 Horizon Client 4.0 이상이 필요합니다.

원격 데스크톱에서 클라이언트 드라이브 리디렉션 동작을 제어하는 Windows 레지스트리 설정은 다음 경로에 있습니다.

```
HKLM\Software\VMware, Inc.\VMware TSDR
```



원격 데스크톱에서 Windows 레지스트리 편집기를 사용하여 로컬 레지스트리 설정을 편집할 수 있습니다.

**참고** 로컬 레지스트리 설정보다 스마트 정책으로 설정한 클라이언트 리디렉션 정책의 우선 순위가 더 높습니다.

## 클라이언트 드라이브 리디렉션 사용 안 함

클라이언트 드라이브 리디렉션을 사용하지 않도록 설정하려면 `disabled`라는 새 문자열 값을 만들고 값을 `true`로 설정합니다.

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

기본값은 `false`(사용)입니다.

## 공유 폴더에 대한 쓰기 액세스 방지

원격 데스크톱과 공유된 모든 폴더에 대한 쓰기 액세스 권한을 방지하려면 `permissions`라는 새 문자열 값을 만들고 값을 `r`로 시작하면서 `rw`는 아닌 임의의 문자열로 설정합니다.

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

기본값은 `rw`(모든 공유 폴더를 읽고 쓸 수 있음)입니다.

## 특정 폴더 공유

특정 폴더를 원격 데스크톱과 공유하려면 `default shares`라는 새 키를 만들고 원격 데스크톱과 공유할 각 폴더에 대해 새 하위 키를 만듭니다. 각 하위 키에 대해 `name`이라는 새 문자열을 만들고 값을 공유할 폴더의 경로로 설정합니다. 다음 예에서는 `C:\Webbooks` 및 `C:\Spreadsheets` 폴더를 공유합니다.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1\name=C:\Webbooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\2\name=C:\Spreadsheets
```

`name`을 `*all`로 설정하면 모든 클라이언트 드라이브를 원격 데스크톱과 공유합니다. `*all` 설정은 Windows 클라이언트 시스템에서만 지원됩니다.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

클라이언트가 추가 폴더(즉, `default shares` 키를 지정하지 않은 폴더)를 공유하는 것을 방지하려면 `ForcedByAdmin`이라는 문자열 값을 만들고 값을 `true`로 설정합니다.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

값이 `true`이면 사용자가 Horizon Client에서 원격 데스크톱에 연결할 때 공유 대화 상자가 나타나지 않습니다. 기본값은 `false`(클라이언트에서 추가 폴더 공유 가능)입니다.

다음 예에서는 `C:\Webbooks` 및 `C:\Spreadsheets` 폴더를 공유하고, 두 폴더 모두를 읽기 전용으로 만들고, 클라이언트가 추가 폴더를 공유하지 못하도록 합니다.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```



```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\w1\name=C:\Webbooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\w2\name=C:\Spreadsheets
```

**참고** ForcedByAdmin 기능을 보안 기능 또는 공유 제어로 사용하지 마십시오. 사용자는 기본 공유 키로 지정되지 않은 폴더를 가리키는 기존 공유에 대해 링크를 생성하여 ForcedByAdmin=true 설정을 무시할 수 있습니다.

## 비즈니스용 Skype 구성

비즈니스용 Skype를 사용하면 가상 인프라에 부정적인 영향을 주거나 네트워크에 과부하를 주지 않고도 가상 데스크톱 내에서 최적화된 음성 및 영상 통화를 할 수 있습니다.

Skype 음성 및 영상 통화 동안 모든 미디어 처리는 가상 데스크톱 대신 클라이언트 시스템에서 수행됩니다.

비즈니스용 Skype를 사용하려면 Windows용 Horizon Client 설치 중에 클라이언트 시스템에 비즈니스용 Skype의 가상화 팩 기능을 설치해야 합니다. “Windows용 VMware Horizon Client 사용” 문서를 참조하십시오.

또한 Horizon 관리자는 Horizon Agent 설치 중에 가상 데스크톱에 비즈니스용 Skype 기능에 대한 가상화 팩을 설치해야 합니다.

## 비즈니스용 Skype 기능

비즈니스용 Skype는 다음과 같은 기능을 제공합니다.

- 지점 간 음성 통화
- 지점 간 비디오 통화
- 다이얼 패드를 통한 PSTN 호출
- 통화 전송, 전달, 음소거, 대기 및 다시 시작
- HID 명령
- 중재 서버를 통한 PSTN 호출
- Edge 서버를 통한 원격 연결 및 호출
- 통화 대기음
- 음성 메일 통합

## 비즈니스용 Skype 시스템 요구 사항

이 기능은 이러한 구성을 지원합니다.

표 2-4. 비즈니스용 Skype 시스템 요구 사항

시스템	요구 사항
Server	Lync Server 2013, 비즈니스용 Skype Server 2015, Office365
클라이언트	비즈니스용 Skype 2015 15.0.4675.1003 이상 Office 365 Plus 16.0.7571.2072 이상에 속하는 비즈니스용 Skype 2016 Office 2016 16.0.4534.1000 이상에 속하는 비즈니스용 Skype 2016
가상 데스크톱 운영 체제	Windows 7, Windows 8.1, Windows 10 영구 및 비영구 데스크톱. Windows 2008r2 데스크톱 및 Windows 2012r2 데스크톱도 지원됩니다.
클라이언트 시스템 운영 체제	Windows 7, Windows 8.1, Windows 10
디스플레이 프로토콜	VMware Blast 및 PCoIP
네트워크 포트	네이티브 비즈니스용 Skype 클라이언트에서 사용되는 것과 동일한 포트입니다. <a href="https://technet.microsoft.com/en-us/library/gg398833.aspx">https://technet.microsoft.com/en-us/library/gg398833.aspx</a> 에서 클라이언트 포트를 참조하십시오.
웹캠	비즈니스용 Skype에서 작동될 수 있는 동일한 디바이스입니다. <a href="https://technet.microsoft.com/en-us/office/dn947482.aspx">https://technet.microsoft.com/en-us/office/dn947482.aspx</a> 에 나열된 웹캠을 참조하십시오.
오디오 및 비디오 코덱	네이티브 비즈니스용 Skype 클라이언트에서 사용되는 것과 동일한 오디오 및 비디오 코덱입니다. <a href="https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&amp;MSPPErrors=-2147217396">https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&amp;MSPPErrors=-2147217396</a> 의 내용을 참조하십시오.
미디어 기능 팩	Windows 10 N 및 KN 버전용 원격 데스크톱에 설치해야 합니다. <a href="https://www.microsoft.com/en-us/download/details.aspx?id=48231">https://www.microsoft.com/en-us/download/details.aspx?id=48231</a> 에서 미디어 기능을 설치할 수 있습니다.

## 비즈니스용 Skype 제한 사항

비즈니스용 Skype에는 다음과 같은 제한 사항이 있습니다.

- E.911 호출을 할 수 없습니다.
- IPv6은 지원되지 않습니다.
- 벨 소리를 사용자 지정할 수 없습니다.
- 응답 그룹 호출, 통화 대기, 통화 대기 해제, 회사 번호로 전화는 지원되지 않습니다.
- 화이트보드, 갤러리 보기, 파노라마 웹캠 및 화면 공유는 현재 지원되지 않습니다.
- 통화를 녹음할 수 없습니다.
- 원격 데스크톱에서 최적화된 비즈니스용 Skype와 동시에 클라이언트 시스템의 Lync 또는 비즈니스용 Skype를 사용하는 것은 지원되지 않습니다.
- Skype 2015 클라이언트를 Lync 2013 서버에 연결할 경우 Lync 2013 클라이언트 UI가 지원되지 않습니다. 관리자는 서버에서 Skype 클라이언트 UI를 구성할 수 있습니다. <https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx>
- 두 명 이상의 사용자가 참여하는 오디오 및 비디오 회의는 현재 지원되지 않습니다.

- 모임 시작 기능은 지원되지 않습니다.
- 비디오 미리 보기 창에서 나열된 것과는 다른 카메라를 보려면 해당 디바이스를 선택하고 대화 상자를 닫은 후 다시 열어서 미리 봅니다.
- 원격 데스크톱에 비즈니스용 Skype를 설치할 때 사설망에 연결되면 설치 관리자는 해당 네트워크 프로파일에 대한 인바운드 및 아웃바운드 방화벽 규칙을 추가합니다. 도메인 네트워크에서 원격 데스크톱에 로그인한 후 비즈니스용 Skype를 사용하여 방화벽 예외를 표시합니다. 이 문제를 해결하려면 모든 네트워크 프로파일에 대한 방화벽 규칙에서 비즈니스용 Skype 클라이언트에 대한 방화벽 예외를 수동으로 추가합니다.
- 원격 데스크톱 운영 체제의 볼륨 컨트롤 옵션은 진행 중인 Skype 통화의 볼륨 수준에 영향을 주지 않습니다. Skype 통화에서 볼륨 컨트롤을 사용하거나 클라이언트 시스템에서 볼륨 컨트롤을 사용하여 볼륨을 변경합니다.

## URL 콘텐츠 리디렉션 구성

URL 콘텐츠 리디렉션 기능을 사용하면 특정 URL이 클라이언트 시스템 또는 원격 데스크톱이나 애플리케이션에서 열리도록 구성할 수 있습니다. Internet Explorer 주소 표시줄이나 애플리케이션에서 사용자가 입력하는 URL을 리디렉션할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- URL 콘텐츠 리디렉션 이해
- URL 콘텐츠 리디렉션 요구 사항
- Cloud Pod 아키텍처 환경에서 URL 콘텐츠 리디렉션 사용
- URL 콘텐츠 리디렉션 기능이 있는 Horizon Agent 설치
- 에이전트에서 클라이언트로의 리디렉션 구성
- 클라이언트에서 에이전트로의 리디렉션 구성
- URL 콘텐츠 리디렉션 제한
- 지원되지 않는 URL 콘텐츠 리디렉션 기능

### URL 콘텐츠 리디렉션 이해

URL 콘텐츠 리디렉션 기능은 원격 데스크톱 또는 애플리케이션에서 클라이언트로의 리디렉션 및 클라이언트에서 원격 데스크톱 또는 애플리케이션으로의 리디렉션을 지원합니다.

원격 데스크톱 또는 애플리케이션에서 클라이언트로 리디렉션하는 것은 에이전트에서 클라이언트로의 리디렉션이라고 합니다. 클라이언트에서 원격 데스크톱 또는 애플리케이션으로 리디렉션하는 것은 클라이언트에서 에이전트로의 리디렉션이라고 합니다.

#### 에이전트에서 클라이언트로의 리디렉션

에이전트에서 클라이언트로의 리디렉션을 사용하면 Horizon Agent는 URL을 Horizon Client로 보내 클라이언트 시스템의 해당 URL에서 프로토콜에 대한 기본 애플리케이션을 엽니다.

#### 클라이언트에서 에이전트로의 리디렉션

클라이언트에서 에이전트로의 리디렉션을 사용하면 Horizon Client는 사용자가 지정한 원격 데스크톱 또는 원격 애플리케이션을 열어 URL을 처리합니다. URL이 원격 데스크톱으로 리디렉션되면 링크가 해당 데스크톱의 프로토콜에 대한 기본 브라우저에서 열립니다. URL이 원격 애플리케이션으로 리디렉션되면 링크가 지정된 애플리케이션을 사용하여 열립니다. 최종 사용자에게 데스크톱 또는 애플리케이션 풀에 대한 권한이 있어야 합니다.

일부 URL은 원격 데스크톱 또는 애플리케이션에서 클라이언트로 리디렉션하고 다른 URL은 클라이언트에서 원격 데스크톱 또는 애플리케이션으로 리디렉션할 수 있습니다. HTTP, HTTPS, mailto 및 callto를 비롯한 다양한 프로토콜을 리디렉션할 수 있습니다.

## URL 콘텐츠 리디렉션 요구 사항

URL 콘텐츠 리디렉션 기능을 사용하려면 클라이언트 시스템, 원격 데스크톱 시스템 및 RDS 호스트가 특정 요구 사항을 충족해야 합니다.

### Windows 클라이언트

Windows용 Horizon Client 4.0 이상

클라이언트에서 에이전트로의 리디렉션을 사용하려면 Windows용 Horizon Client 설치 중에 URL 콘텐츠 리디렉션 기능을 사용하도록 설정해야 합니다. 에이전트에서 클라이언트로의 리디렉션을 사용하기 위해서는 Windows용 Horizon Client의 URL 콘텐츠 리디렉션 기능을 사용하도록 설정하지 않아도 됩니다.

### Mac 클라이언트

Mac용 Horizon Client 4.2 이상

Mac용 Horizon Client 4.2 또는 4.3에서 URL 콘텐츠 리디렉션은 기술 미리보기 기능이며 에이전트에서 클라이언트로의 리디렉션만 지원합니다. Mac용 Horizon Client 4.4 이상에서는 URL 콘텐츠 리디렉션이 공식적으로 지원되며 에이전트에서 클라이언트로 및 클라이언트에서 에이전트로의 리디렉션이 모두 지원됩니다.

### 데스크톱 가상 시스템 및 RDS 호스트

데스크톱 및 애플리케이션을 제공하는 원격 데스크톱 시스템 및 RDS 호스트의 Horizon Agent 7.0 이상

Horizon Agent 설치 중에 URL 콘텐츠 리디렉션 기능을 사용하도록 설정해야 합니다.

### 웹 브라우저

Internet Explorer 9, 10 및 11

### 디스플레이 프로토콜

VMware Blast 및 PCoIP

## Cloud Pod 아키텍처 환경에서 URL 콘텐츠 리디렉션 사용

Cloud Pod 아키텍처 환경이 있는 경우 로컬 URL 콘텐츠 리디렉션 설정 외에 전역 URL 콘텐츠 리디렉션 설정을 구성할 수 있습니다.

로컬 포트에서만 표시되는 로컬 URL 콘텐츠 리디렉션 설정과 달리, 전역 URL 콘텐츠 리디렉션 설정은 포트 페더레이션 전체에서 볼 수 있습니다. 전역 URL 콘텐츠 리디렉션 설정을 사용하면 클라이언트의 URL 링크를 전역 데스크톱 사용 권한 및 전역 애플리케이션 사용 권한과 같은 전역 리소스로 리디렉션할 수 있습니다.

사용자가 Horizon Client를 사용하여 포트 페더레이션의 연결 서버 인스턴스에 로그인하면 연결 서버 인스턴스는 사용자에게 할당된 로컬 및 전역 URL 콘텐츠 리디렉션 설정을 찾습니다. 로컬 및 전역 설정이 병합된 후 사용자가 클라이언트 시스템에서 URL을 클릭할 때마다 사용됩니다.

Cloud Pod 아키텍처 환경 구성 및 관리에 대한 자세한 내용은 “Horizon 7에서 Cloud Pod 아키텍처 관리” 문서를 참조하십시오.

## URL 콘텐츠 리디렉션 기능이 있는 Horizon Agent 설치

원격 데스크톱 또는 애플리케이션에서 클라이언트로의 URL 콘텐츠 리디렉션(에이전트에서 클라이언트로의 리디렉션) 또는 클라이언트에서 원격 데스크톱 또는 애플리케이션으로의 URL 콘텐츠 리디렉션(클라이언트에서 에이전트로의 리디렉션)을 사용하려면 Horizon Agent를 설치할 때 URL 콘텐츠 리디렉션 기능을 사용하도록 설정해야 합니다.

설치 관리자 파일을 두 번 클릭하는 대신, 명령 프롬프트 창에서 다음 명령을 실행하여 Horizon Agent 설치를 시작합니다.

```
VMware-viewagent-x86_64-y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

표시되는 메시지에 따라 설치를 완료합니다.

URL 콘텐츠 리디렉션 기능이 설치되었는지 확인하려면 `vmware-url-protocol-launch-helper.exe` 및 `vmware-url-filtering-plugin.dll` 파일이 `%PROGRAMFILES%\VMware\VMware View\Agent\bin\URLRedirection` 디렉토리에 있는지 확인하십시오. 또한 VMware Horizon View URL 필터링 플러그인 Internet Explorer 추가 기능이 사용되도록 설정되어 있는지도 확인하십시오.

## 에이전트에서 클라이언트로의 리디렉션 구성

에이전트에서 클라이언트로의 리디렉션을 사용하면 Horizon Agent는 URL을 Horizon Client로 보내 해당 URL에서 프로토콜에 대한 기본 애플리케이션을 엽니다.

에이전트에서 클라이언트로의 리디렉션을 사용하도록 설정하려면 다음 구성 작업을 수행하십시오.

- Horizon Agent에서 URL 콘텐츠 리디렉션 기능을 사용하도록 설정합니다. [URL 콘텐츠 리디렉션 기능이 있는 Horizon Agent 설치](#)를 참조하십시오.
- 원격 데스크톱 및 애플리케이션에 URL 콘텐츠 리디렉션 그룹 정책 설정을 적용합니다. [GPO에 URL 콘텐츠 리디렉션 ADMX 템플릿 추가](#)를 참조하십시오.
- 각 프로토콜에 대해 Horizon Agent에서 URL을 리디렉션하는 방법을 나타내도록 그룹 정책 설정을 구성합니다. [URL 콘텐츠 리디렉션 그룹 정책 설정](#)를 참조하십시오.

## GPO에 URL 콘텐츠 리디렉션 ADMX 템플릿 추가

URL 콘텐츠 리디렉션 ADMX 템플릿 파일(`urlRedirection-enUS.admx`)에는 URL 링크가 클라이언트에서 열리는지(에이전트에서 클라이언트로의 리디렉션) 또는 원격 데스크톱이나 애플리케이션에서 열리는지를(클라이언트에서 에이전트로의 리디렉션) 제어할 수 있는 설정이 포함되어 있습니다.

URL 콘텐츠 리디렉션 그룹 정책 설정을 원격 데스크톱 및 애플리케이션에 적용하려면 Active Directory 서버의 GPO에 ADMX 템플릿 파일을 추가합니다. 원격 데스크톱 또는 애플리케이션에서 클릭하는 URL 링크에 대한 규칙의 경우, GPO가 데스크톱과 RDS 호스트를 포함하는 OU에 반드시 연결되어 있어야 합니다.

Windows 클라이언트 컴퓨터가 포함된 OU에 연결된 GPO에 그룹 정책 설정을 적용할 수도 있지만 클라이언트에서 에이전트로의 리디렉션 구성하는 기본 방법은 vdmutil 명령줄 유틸리티를 사용하는 것입니다. macOS는 GPO를 지원하지 않으므로 Mac 클라이언트가 있는 경우에는 vmdutil을 사용해야 합니다.

### 사전 요구 사항

- Horizon Agent를 설치할 때 URL 콘텐츠 리디렉션 기능이 포함되는지 확인하십시오. [URL 콘텐츠 리디렉션 기능이 있는 Horizon Agent 설치](#)를 참조하십시오.
- URL 콘텐츠 리디렉션 그룹 정책 설정에 대해 Active Directory GPO가 생성되어 있는지 확인합니다.
- Active Directory 서버에서 MMC와 그룹 정책 관리 편집기 스냅인을 사용할 수 있는지 확인합니다.

### 절차

- 1 Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip입니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일의 압축을 풀고 URL 콘텐츠 리디렉션 ADMX 파일을 Active Directory 서버에 복사합니다.

a urlRedirection-enUS.admx 파일을 C:\Windows\PolicyDefinitions 폴더에 복사합니다.

b urlRedirection.adml 언어 리소스 파일을 C:\Windows\PolicyDefinitions 디렉토리의 해당 하위 폴더에 복사합니다.

예를 들어 EN 로캘의 경우 urlRedirection-enUS.adml 파일을 C:\Windows\PolicyDefinitions\en-US 폴더로 복사합니다.

- 3 Active Directory 서버에서 그룹 정책 관리 편집기를 엽니다.

URL 콘텐츠 리디렉션 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > VMware Horizon URL 리디렉션**에 설치됩니다.

### 다음에 수행할 작업

그룹 정책 설정을 구성하십시오.

## URL 콘텐츠 리디렉션 그룹 정책 설정

URL 콘텐츠 리디렉션 템플릿 파일에는 에이전트에서 클라이언트로의 리디렉션과 클라이언트에서 에이전트로의 리디렉션에 대한 규칙을 생성할 수 있는 그룹 정책 설정이 포함되어 있습니다. 템플릿 파일에

는 컴퓨터 구성 설정만 포함됩니다. 모든 설정은 그룹 정책 관리 편집기의 **VMware Horizon URL 리디렉션** 폴더에 있습니다.

다음 표에서는 URL 콘텐츠 리디렉션 템플릿 파일의 그룹 정책 설정에 대해 설명합니다.

표 3-1. URL 콘텐츠 리디렉션 그룹 정책 설정

설정	속성
IE Policy: Prevent users from changing URL Redirection plugin loading behavior	사용자가 URL 콘텐츠 리디렉션 기능을 사용하지 않도록 설정할 수 있는지 여부를 결정합니다. 이 설정은 기본적으로 구성되어 있지 않습니다.
IE Policy: Automatically enable URL Redirection plugin	새로 설치된 Internet Explorer 플러그인의 자동 활성화 여부를 결정합니다. 이 설정은 기본적으로 구성되어 있지 않습니다.
Url Redirection Enabled	URL 콘텐츠 리디렉션 기능이 사용되도록 설정되어 있는지 여부를 결정합니다. URL 콘텐츠 리디렉션 기능이 클라이언트 또는 에이전트에 설치되어 있더라도 이 설정을 사용하여 이 기능을 사용하지 않도록 설정할 수 있습니다. 이 설정은 기본적으로 구성되어 있지 않습니다.



설정	속성
Url Redirection Protocol 'http'	<p>HTTP 프로토콜을 사용하는 모든 URL에 대해 리디렉션할 URL을 지정합니다. 이 설정에는 다음과 같은 옵션이 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>brokerHostname</b> - URL을 원격 데스크톱 또는 애플리케이션으로 리디렉션할 때 사용할 연결 서버 호스트의 IP 주소 또는 정규화된 이름입니다.</li> <li>■ <b>remoteltem</b> - <b>agentRules</b>에 지정된 URL을 처리할 수 있는 원격 데스크톱 또는 애플리케이션 풀의 표시 이름입니다.</li> <li>■ <b>clientRules</b> - 클라이언트로 리디렉션되어야 하는 URL입니다. 예를 들어 <b>clientRules</b>를 <b>*.mycompany.com</b>으로 설정하면 텍스트 mycompany.com을 포함하는 모든 URL이 Windows 기반 클라이언트로 리디렉션되고 클라이언트의 기본 브라우저에서 열립니다.</li> <li>■ <b>agentRules</b> - <b>remoteltem</b>에 지정된 원격 데스크톱 또는 애플리케이션으로 리디렉션되어야 하는 URL입니다. 예를 들어 <b>agentRules</b>를 <b>*.mycompany.com</b>으로 "mycompany.com"을 포함하는 모든 URL이 원격 데스크톱 또는 애플리케이션으로 설정하면 리디렉션됩니다.</li> </ul> <p>또한 에이전트 규칙을 생성할 때는 <b>brokerHostname</b> 옵션을 사용하여 연결 서버 호스트의 IP 주소 또는 정규화된 도메인 이름을 지정하고 <b>remoteltem</b> 옵션을 사용하여 데스크톱 또는 애플리케이션 풀의 표시 이름을 지정해야 합니다.</p> <p><b>참고</b> 기본적인 클라이언트 규칙 구성 방법은 vdmutil 명령줄 유틸리티를 사용하는 것입니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
Url Redirection Protocol '[...]'	<p>HTTP 이외의 프로토콜(예: HTTPS, email 또는 callto)에 이 설정을 사용하십시오.</p> <p>옵션은 Url Redirection Protocol 'http'의 경우에도 같습니다.</p> <p>다른 프로토콜을 구성할 필요가 없는 경우에는 URL 콘텐츠 리디렉션 템플릿 파일을 Active Directory에 추가하기 전에 이 항목을 삭제하거나 주석 처리할 수 있습니다.</p> <p>HTTP 및 HTTPS 프로토콜에 대해서는 동일한 리디렉션 설정을 구성하는 것이 좋습니다. 이렇게 해야 사용자가 mycompany.com과 같이 부분적인 URL을 Internet Explorer에 입력할 때 해당 사이트가 HTTP에서 HTTPS로 자동 리디렉션되면 URL 콘텐츠 리디렉션 기능이 원하는 대로 작동합니다. 이 예에서 HTTPS에 대한 규칙은 설정하지만 HTTP에 대해 동일한 리디렉션 설정을 지정하지 않으면 사용자가 입력하는 부분 URL이 리디렉션되지 않습니다.</p> <p>이 설정은 기본적으로 구성되어 있지 않습니다.</p>

클라이언트에서 에이전트로의 리디렉션에서 기본 처리기가 없는 프로토콜을 구성하려면 이 프로토콜에 대한 그룹 정책 설정을 구성한 후에 이 프로토콜을 지정하는 URL을 리디렉션하기 전에 Horizon Client를 한 번 시작해야 합니다.

## URL 콘텐츠 리디렉션 규칙 생성을 위한 구문

클라이언트 또는 원격 데스크톱이나 애플리케이션에서 열리는 URL을 지정할 때 정규식을 사용할 수 있습니다. 여러 항목을 구분할 때는 세미콜론을 사용하십시오. 항목 간 공백은 허용되지 않습니다.

다음 표에서는 몇 가지 샘플 항목에 대해 설명합니다.

항목	설명
<b>.*</b>	모든 URL이 리디렉션되도록 지정합니다. 에이전트 규칙( <b>agentRules</b> 옵션)에 이 설정을 사용하면 모든 URL이 지정된 원격 데스크톱 또는 애플리케이션에서 열립니다. 클라이언트 규칙( <b>clientRules</b> 옵션)에 이 설정을 사용하면 모든 URL이 클라이언트로 리디렉션됩니다.
<b>.*.acme.com;*.example.com</b>	텍스트 <b>.acme.com</b> 또는 <b>example.com</b> 을 포함하는 모든 URL이 리디렉션되도록 지정합니다.
[공백 또는 비워 둠]	어떤 URL도 리디렉션되지 않도록 지정합니다. 예를 들어 <b>clientRules</b> 옵션을 비워 두면 어떤 URL도 클라이언트로 리디렉션되지 않습니다.

## 에이전트에서 클라이언트로의 리디렉션 그룹 정책 예

에이전트에서 클라이언트로의 리디렉션을 사용하여 리소스를 보존하거나 추가적인 보안 계층으로 활용할 수 있습니다. 예를 들어 직원들이 원격 데스크톱 또는 애플리케이션에서 작업 중이고 비디오 시청을 원할 경우 해당 URL을 클라이언트 시스템으로 리디렉션하여 데이터 센터의 부담을 덜 수 있습니다. 또는 보안을 위해 기업 네트워크 외부에서 작업하는 직원들을 대상으로 기업 네트워크 외부 위치를 가리키는 모든 URL이 직원의 자체 클라이언트 시스템에서 열리도록 할 수 있습니다.

예를 들어 회사와 관련이 없는 콘텐츠, 기업 네트워크를 가리키지 않는 모든 URL이 클라이언트 시스템에서 열리도록 리디렉션되는 규칙을 구성할 수 있습니다. 이 경우 정규 표현식을 포함하는 다음과 같은 설정을 사용할 수 있습니다.

### ■ **agentRules**: **.\*.mycompany.com**

이 규칙은 mycompany.com 텍스트가 포함된 URL이 지정된 원격 데스크톱 또는 애플리케이션(에이전트)에서 열리도록 리디렉션합니다.

### ■ **clientRules**: **.\***

이 규칙은 클라이언트에 대한 모든 URL이 기본 클라이언트 브라우저에서 열리도록 리디렉션합니다.

URL 콘텐츠 리디렉션 기능은 다음 프로세스를 사용하여 클라이언트 및 에이전트 규칙을 적용합니다.

- 1 사용자가 원격 애플리케이션 또는 데스크톱의 링크를 클릭하면 클라이언트 규칙을 먼저 확인합니다.
- 2 URL이 클라이언트 규칙과 일치하면 에이전트 규칙을 확인합니다.
- 3 에이전트 규칙과 클라이언트 규칙 간에 충돌이 있으면 링크가 로컬로 열립니다. 이 경우 URL은 에이전트 시스템에서 열립니다.
- 4 충돌하지 않으면 URL이 클라이언트로 리디렉션됩니다.

이 예에서 **mycompany.com**이 있는 URL이 모든 URL의 부분 집합이기 때문에 클라이언트 및 에이전트 규칙이 충돌합니다. 이러한 충돌 때문에 **mycompany.com**을 포함하는 URL은 로컬로 열립니다. 원격 데스크톱에서 URL에 **mycompany.com**이 있는 링크를 클릭하면 URL이 원격 데스크톱에서 열립니다. 클라이언트 시스템에서 URL에 **mycompany.com**이 있는 링크를 클릭하면 URL이 해당 클라이언트에서 열립니다.

## 클라이언트에서 에이전트로의 리디렉션 구성

클라이언트에서 에이전트로의 리디렉션을 사용하면 Horizon Client는 원격 데스크톱 또는 애플리케이션을 열어 사용자가 클라이언트에서 클릭하는 URL 링크를 처리합니다. 원격 데스크톱이 열려 있으면 URL의 프로토콜에 대한 기본 애플리케이션이 해당 URL을 처리합니다. 원격 애플리케이션이 열려 있으면 해당 애플리케이션이 URL을 처리합니다.

클라이언트에서 에이전트로의 리디렉션을 사용하도록 설정하려면 다음 구성 작업을 수행하십시오.

- Horizon Agent에서 URL 콘텐츠 리디렉션 기능을 사용하도록 설정합니다. [URL 콘텐츠 리디렉션 기능이 있는 Horizon Agent 설치](#)를 참조하십시오.
- (Windows 클라이언트만 해당) Windows용 Horizon Client에서 URL 콘텐츠 리디렉션 기능을 사용하도록 설정합니다. [URL 콘텐츠 리디렉션 기능이 있는 Windows용 Horizon Client 설치](#)를 참조하십시오.
- vdmutil 명령줄 유틸리티를 사용하여 각 프로토콜에 대해 Horizon Client가 URL을 리디렉션하는 방법을 나타내는 URL 콘텐츠 리디렉션 설정을 생성합니다. 자세한 내용은 [로컬 URL 콘텐츠 리디렉션 설정 생성](#) 또는 [전역 URL 콘텐츠 리디렉션 설정 생성](#)에 나와 있습니다.
- vdmutil 명령줄 유틸리티를 사용하여 URL 콘텐츠 리디렉션 설정을 Active Directory 사용자 또는 그룹에 할당합니다. [사용자 또는 그룹에 URL 콘텐츠 리디렉션 설정 할당](#)를 참조하십시오.
- URL 콘텐츠 리디렉션 설정을 확인합니다. [URL 콘텐츠 리디렉션 설정 테스트](#)를 참조하십시오.

**참고** 그룹 정책 설정을 사용하여 클라이언트에서 에이전트로의 리디렉션 규칙을 구성할 수 있으나 vdmutil 명령줄 유틸리티를 사용하는 방식이 기본적으로 사용됩니다. 자세한 내용은 [그룹 정책 설정을 사용하여 클라이언트에서 에이전트로의 리디렉션 구성](#)의 내용을 참조하십시오.

## URL 콘텐츠 리디렉션 기능이 있는 Windows용 Horizon Client 설치

Windows 클라이언트에서 원격 데스크톱 또는 애플리케이션으로의 URL 콘텐츠 리디렉션(클라이언트에서 에이전트로의 리디렉션)을 사용하려면 URL 콘텐츠 리디렉션 기능이 있는 Windows용 Horizon Client를 설치해야 합니다.

URL 콘텐츠 리디렉션 기능을 사용하도록 설정하려면 명령줄 옵션을 통해 Windows용 Horizon Client 설치 관리자를 사용해야 합니다. 설치 관리자 파일을 두 번 클릭하는 대신, 명령 프롬프트 창에서 다음 명령을 실행하여 설치를 시작합니다.

```
VMware-Horizon-Client-x86-y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

이 기능이 설치되었는지 확인하려면 vmware-url-protocol-launch-helper.exe 및 vmware-url-filtering-plugin.dll 파일이 %PROGRAMFILES%\VMware\VMware Horizon View Client 디렉토리에 있는지 확인하십시오. 또한 VMware Horizon View URL 필터링 플러그인 Internet Explorer 추가 기능이 설치되어 있는지도 확인하십시오.

**참고** Mac용 Horizon Client 4.4는 기본적으로 클라이언트에서 에이전트로의 리디렉션을 지원합니다. 추가 설치 단계는 필요하지 않습니다. Mac용 Horizon Client 4.2 및 4.3은 클라이언트에서 에이전트로의 리디렉션을 지원하지 않습니다.

## vdmutil 명령줄 유틸리티 사용

vdmutil 명령줄 인터페이스를 사용하여 클라이언트에서 에이전트로의 리디렉션에 대한 URL 콘텐츠 리디렉션 설정을 생성, 할당 및 관리할 수 있습니다.

### 명령 사용 방법

vdmutil 명령 구문은 Windows 명령 프롬프트에서 해당 작업을 제어합니다.

```
vdmutil 명령 옵션 [추가 옵션인수] ...
```

사용할 수 있는 추가 옵션은 명령 옵션에 따라 다릅니다.

기본적으로 vdmutil 명령 실행 파일의 경로는 C:\Program Files\VMware\VMware View\Server\tools\Wbin입니다. 명령줄에 경로를 입력하지 않으려면 PATH 환경 변수에 경로를 추가하십시오.

### 명령 인증

관리자 역할을 가진 사용자로 vdmutil 명령을 실행해야 합니다.

Horizon Administrator를 사용하여 사용자에게 관리자 역할을 할당할 수 있습니다. 자세한 내용은 "View 관리" 문서를 참조하십시오.

vdmutil 명령에는 인증에 사용할 사용자 이름, 도메인 및 암호를 지정하는 옵션이 있습니다. --help 및 --verbose를 제외한 모든 vdmutil 명령 옵션과 함께 이러한 인증 옵션을 사용해야 합니다.

표 3-2. vdmutil 명령 인증 옵션

옵션	설명
--authAs	연결 서버 인스턴스에서 인증을 받기 위한 Horizon 관리자의 사용자 이름입니다. <b>domain\username</b> 또는 UPN(사용자 계정 이름) 형식을 사용하지 마십시오.
--authDomain	--authAs 옵션에 지정된 Horizon 관리자의 정규화된 도메인 이름입니다.
--authPassword	--authAs 옵션에 지정된 Horizon 관리자의 암호입니다. 암호 대신 "*"를 입력하면 vdmutil 명령이 암호를 묻는 메시지를 표시하고 명령줄에서 중요 암호를 명령 기록에 남기지 않습니다.

예를 들어 다음 vdmutil 명령은 사용자 mydomain\johndoe에 로그인합니다.

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

### 명령 출력

vdmutil 명령은 작업이 성공하면 0을 반환하고 작업이 실패하면 0이 아닌 장애 관련 코드를 반환합니다. vdmutil 명령은 오류 메시지를 표준 오류로 기록합니다. 작업에서 출력을 생성하는 경우 또는 --verbose 옵션을 통해 자세한 정보 로깅이 사용되도록 설정된 경우 vdmutil 명령은 출력을 표준 출력에 영어로 기록합니다.

### URL 콘텐츠 리디렉션에 대한 옵션

다음 vdmutil 명령 옵션을 사용하여 URL 콘텐츠 리디렉션 설정을 생성, 할당 및 관리할 수 있습니다. 모든 옵션은 2개의 대시(--로 시작합니다.

표 3-3. URL 콘텐츠 리디렉션에 대한 vdmutil 명령 옵션

옵션	설명
--addGroupURLSetting	그룹을 특정 URL 콘텐츠 리디렉션 설정에 할당합니다.
--addUserURLSetting	사용자를 특정 URL 콘텐츠 리디렉션 설정에 할당합니다.
--createUrlSetting	URL 콘텐츠 리디렉션 설정을 생성합니다.
--deleteURLSetting	URL 콘텐츠 리디렉션 설정을 삭제합니다.
--disableURLSetting	URL 콘텐츠 리디렉션 설정을 사용하지 않도록 설정합니다.
--enableURLSetting	--disableURLSetting 옵션을 사용하여 이전에 사용되지 않도록 설정한 URL 콘텐츠 리디렉션 설정을 사용하도록 설정합니다.
--listURLSetting	연결 서버 인스턴스의 모든 URL 콘텐츠 리디렉션 설정을 나열합니다.
--readURLSetting	URL 콘텐츠 리디렉션 설정에 대한 정보를 표시합니다.
--removeGroupURLSetting	URL 콘텐츠 리디렉션 설정에서 그룹 할당을 제거합니다.
--removeUserURLSetting	URL 콘텐츠 리디렉션 설정에서 사용자 할당을 제거합니다.
--updateURLSetting	기존 URL 콘텐츠 리디렉션 설정을 업데이트합니다.

**vdmutil --help**를 입력하여 모든 vdmutil 옵션에 대한 구문 정보를 표시할 수 있습니다. 특정 옵션에 대한 자세한 구문 정보를 표시하려면 **vdmutil --option --help**를 입력합니다.

## 로컬 URL 콘텐츠 리디렉션 설정 생성

원격 데스크톱 또는 애플리케이션에서 열리도록 특정 URL을 리디렉션하는 로컬 URL 콘텐츠 리디렉션 설정을 생성할 수 있습니다. 로컬 URL 콘텐츠 리디렉션 설정은 로컬 포트에서만 볼 수 있습니다.

HTTP, HTTPS, mailto 및 callto를 비롯한 다양한 프로토콜을 구성할 수 있습니다.

HTTP 및 HTTPS 프로토콜에 대해서는 동일한 리디렉션 설정을 구성하는 것이 좋습니다. 이렇게 해야 사용자가 mycompany.com과 같이 부분적인 URL을 Internet Explorer에 입력할 때 해당 사이트가 HTTP에서 HTTPS로 자동 리디렉션되면 URL 콘텐츠 리디렉션 기능이 원하는 대로 작동합니다. 이 예에서 HTTPS에 대한 규칙은 설정하지만 HTTP에 대해 동일한 리디렉션 설정을 지정하지 않으면 사용자가 입력하는 부분 URL이 리디렉션되지 않습니다.

포트 페더레이션 내에서 볼 수 있는 전역 URL 콘텐츠 리디렉션 설정을 생성하려면 [전역 URL 콘텐츠 리디렉션 설정 생성](#)을 참조하십시오.

### 사전 요구 사항

vdmutil 명령줄 인터페이스 옵션 및 요구 사항을 파악하고 vdmutil 명령을 실행할 수 있는 충분한 권한이 있는지 확인합니다. [vdmutil 명령줄 유틸리티 사용](#)을 참조하십시오.

### 절차

- 1 연결 서버 인스턴스에 로그인합니다.

- 2 URL 콘텐츠 리디렉션 설정을 생성하려면 `--createUrlSetting` 옵션과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --createUrlSetting --urlSettingName <값> --urlRedirectionScope LOCAL
[--description <값>] [--urlScheme <값>] [--entitledApplication <값> | --entitledDesktop <값>] [--agentURLPattern <값>]
```

옵션	설명
<code>--urlSettingName</code>	URL 콘텐츠 리디렉션 설정의 고유한 이름입니다. 이름은 1 ~ 64자 사이일 수 있습니다.
<code>--urlRedirectionScope</code>	URL 콘텐츠 리디렉션 설정의 범위입니다. 해당 설정이 로컬 포트에만 표시되도록 하려면 LOCAL을 지정합니다.
<code>--description</code>	URL 콘텐츠 리디렉션 설정에 대한 설명입니다. 설명은 1 ~ 1024자 사이일 수 있습니다.
<code>--urlScheme</code>	URL 콘텐츠 리디렉션 설정이 적용되는 프로토콜(예: http, https, mailto 또는 callto)입니다.
<code>--entitledApplication</code>	지정된 URL을 여는 데 사용할 로컬 애플리케이션 풀의 표시 이름(예: iexplore-2012)입니다. 이 옵션을 사용하여 로컬 RDS 데스크톱 풀의 표시 이름을 지정할 수도 있습니다.
<code>--entitledDesktop</code>	지정된 URL을 여는 데 사용할 로컬 데스크톱 풀의 표시 이름(예: xx)입니다. RDS 데스크톱 풀의 경우 <code>--entitledApplication</code> 옵션을 사용하십시오.
<code>--agentURLPattern</code>	원격 데스크톱 또는 애플리케이션에서 열 URL을 지정하는 따옴표로 묶은 문자열입니다. 프로토콜 접두사를 포함해야 합니다. 와일드카드를 사용하여 여러 URL과 일치하는 URL 패턴을 지정할 수 있습니다.  예를 들어 "http://google.*"을 입력하면 google이라는 텍스트를 포함하는 모든 URL이 지정된 원격 데스크톱 또는 애플리케이션으로 리디렉션됩니다. .* (점 별)을 입력하면 모든 URL이 원격 데스크톱 또는 애플리케이션으로 리디렉션됩니다.

- 3 (선택 사항) 하나 이상의 프로토콜, URL 및 로컬 리소스를 생성된 URL 콘텐츠 리디렉션 설정에 추가하려면 `--updateURLSetting` 옵션과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --updateURLSetting --urlSettingName <값> --urlRedirectionScope LOCAL
[--description <값>] [--urlScheme <값>] [--entitledApplication <값> | --entitledDesktop <값>] [--agentURLPattern <값>]
```

이 옵션은 `vdmutil` 옵션과 함께 `--createUrlSetting` 명령을 사용하는 것과 같습니다.

## 예제: 로컬 URL 콘텐츠 리디렉션 설정 생성

다음 예에서는 url-filtering이라는 로컬 URL 콘텐츠 리디렉션 설정을 생성합니다. 이 설정은 텍스트 http://google.\*을 포함하는 모든 클라이언트 URL을 iexplore2012라는 애플리케이션 풀로 리디렉션합니다.

```
VdmUtil --createUrlSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

다음 예에서는 url-filtering 설정을 텍스트 `https://google.*`을 포함하는 모든 클라이언트 URL을 `iexplore2012`라는 애플리케이션 풀로 리디렉션하도록 업데이트합니다.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

다음 예에서는 url-filtering 설정을 텍스트 `mailto://*.mycompany.com`를 포함하는 모든 클라이언트 URL을 `Outlook2008`라는 애플리케이션 풀로 리디렉션하도록 업데이트합니다.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

## 다음에 수행할 작업

사용자 또는 그룹에 URL 콘텐츠 리디렉션 설정을 할당합니다. [사용자 또는 그룹에 URL 콘텐츠 리디렉션 설정 할당](#)를 참조하십시오.

## 전역 URL 콘텐츠 리디렉션 설정 생성

Cloud Pod 아키텍처 환경에서 작업하는 경우 포트 페더레이션의 포트에 있는 원격 데스크톱 또는 애플리케이션에서 열리도록 특정 URL을 리디렉션하는 전역 URL 콘텐츠 리디렉션 설정을 생성할 수 있습니다.

전역 URL 콘텐츠 리디렉션 설정은 포트 페더레이션 내에서 볼 수 있습니다. 전역 URL 콘텐츠 리디렉션 설정을 생성할 때 전역 데스크톱 사용 권한 및 전역 애플리케이션 사용 권한과 같은 전역 리소스로 URL을 리디렉션할 수 있습니다.

HTTP, HTTPS, mailto 및 callto를 비롯한 다양한 프로토콜을 구성할 수 있습니다.

HTTP 및 HTTPS 프로토콜에 대해서는 동일한 리디렉션 설정을 구성하는 것이 좋습니다. 이렇게 해야 사용자가 `mycompany.com`과 같이 부분적인 URL을 Internet Explorer에 입력할 때 해당 사이트가 HTTP에서 HTTPS로 자동 리디렉션되면 URL 콘텐츠 리디렉션 기능이 원하는 대로 작동합니다. 이 예에서 HTTPS에 대한 규칙은 설정하지만 HTTP에 대해 동일한 리디렉션 설정을 지정하지 않으면 사용자가 입력하는 부분 URL이 리디렉션되지 않습니다.

Cloud Pod 아키텍처 환경 구성 및 관리에 대한 자세한 내용은 "Horizon 7에서 Cloud Pod 아키텍처 관리" 문서를 참조하십시오.

로컬 URL 콘텐츠 리디렉션 설정을 생성하려면 [로컬 URL 콘텐츠 리디렉션 설정 생성](#)을 참조하십시오.

## 사전 요구 사항

`vdmutil` 명령줄 인터페이스 옵션 및 요구 사항을 파악하고 `vdmutil` 명령을 실행할 수 있는 충분한 권한이 있는지 확인합니다. [vdmutil 명령줄 유틸리티 사용](#)를 참조하십시오.

## 절차

**1** 포트 페더레이션의 연결 서버 인스턴스에 로그인합니다.



- 2 URL 콘텐츠 리디렉션 설정을 생성하려면 `--createUrlSetting` 옵션과 함께 `vdutil` 명령을 실행합니다.

```
vdutil --createUrlSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description 값] [--urlScheme 값] [--entitledApplication 값 | --entitledDesktop
값] [--agentURLPattern 값]
```

옵션	설명
<code>--urlSettingName</code>	URL 콘텐츠 리디렉션 설정의 고유한 이름입니다. 이름은 1 ~ 64자 사이일 수 있습니다.
<code>--urlRedirectionScope</code>	URL 콘텐츠 리디렉션 설정의 범위입니다. 해당 설정이 포트 페더레이션에서 보이도록 하려면 GLOBAL을 지정합니다.
<code>--description</code>	URL 콘텐츠 리디렉션 설정에 대한 설명입니다. 설명은 1 ~ 1024자 사이일 수 있습니다.
<code>--urlScheme</code>	URL 콘텐츠 리디렉션 설정이 적용되는 프로토콜(예: http, https, mailto 또는 callto)입니다.
<code>--entitledApplication</code>	지정된 URL을 여는 데 사용할 전역 애플리케이션 사용 권한의 표시 이름입니다.
<code>--entitledDesktop</code>	지정된 URL을 여는 데 사용할 전역 데스크톱 사용 권한의 표시 이름(예: GE-1)입니다.
<code>--agentURLPattern</code>	원격 데스크톱 또는 애플리케이션에서 열 URL을 지정하는 따옴표로 묶은 문자열입니다. 프로토콜 접두사를 포함해야 합니다. 와일드카드를 사용하여 여러 URL과 일치하는 URL 패턴을 지정할 수 있습니다.  예를 들어 "http://google.*"을 입력하면 google이라는 텍스트를 포함하는 모든 URL이 원격 데스크톱 또는 애플리케이션으로 리디렉션됩니다. *(점 별)을 입력하면 모든 URL이 원격 데스크톱 또는 애플리케이션으로 리디렉션됩니다.

- 3 (선택 사항) 하나 이상의 프로토콜, URL 및 전역 리소스를 생성된 URL 콘텐츠 리디렉션 설정에 추가하려면 `--updateURLSetting` 옵션과 함께 `vdutil` 명령을 실행합니다.

```
vdutil --updateURLSetting --urlSettingName 값 --urlRedirectionScope GLOBAL
[--description 값][--urlScheme 값][--entitledApplication 값 | --entitledDesktop
값] [--agentURLPattern 값]
```

이 옵션은 `--createUrlSetting` 옵션과 함께 `vdutil` 명령을 사용하는 것과 같습니다.

## 예제: 전역 URL 콘텐츠 리디렉션 설정 구성

다음 예에서는 Operations-Setting이라는 전역 URL 콘텐츠 리디렉션 설정을 생성합니다. 이 설정은 텍스트 `http://google.*`을 포함하는 모든 클라이언트 URL을 GAE1이라는 전역 애플리케이션 사용 권한으로 리디렉션합니다.

```
vdutil --createUrlSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```



다음 예에서는 Operations-Setting 설정을 텍스트 `https://google.*`을 포함하는 모든 URL도 GAE1이라는 전역 애플리케이션 사용 권한으로 리디렉션하도록 업데이트합니다.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

다음 예에서는 Operations-Setting 설정을 텍스트 `"mailto://*.mycompany.com"`을 포함하는 모든 URL을 GA2라는 전역 애플리케이션 사용 권한으로 리디렉션하도록 업데이트합니다.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

다음에 수행할 작업

사용자 또는 그룹에 URL 콘텐츠 리디렉션 설정을 할당합니다. [사용자 또는 그룹에 URL 콘텐츠 리디렉션 설정 할당](#)를 참조하십시오.

## 사용자 또는 그룹에 URL 콘텐츠 리디렉션 설정 할당

URL 콘텐츠 리디렉션 설정을 생성한 후에 Active Directory 사용자 또는 그룹에 할당할 수 있습니다.

사전 요구 사항

vdmutil 명령줄 인터페이스 옵션 및 요구 사항을 파악하고 vdmutil 명령을 실행할 수 있는 충분한 권한이 있는지 확인합니다. [vdmutil 명령줄 유틸리티 사용](#)를 참조하십시오.

절차

- ◆ 사용자에게 URL 콘텐츠 리디렉션 설정을 할당하려면 `--addUserURLSetting` 옵션을 사용하여 vdmutil 명령을 실행합니다.

```
vdmutil --addUserURLSetting --urlSettingName <URL> --userName <사용자>
```

옵션	설명
<code>--urlSettingName</code>	할당할 URL 콘텐츠 리디렉션 설정의 이름입니다.
<code>--userName</code>	domain\username 형식의 Active Directory 사용자 이름입니다.

- ◆ 그룹에 URL 콘텐츠 리디렉션 설정을 할당하려면 `--addGroupURLSetting` 옵션을 사용하여 vdmutil 명령을 실행합니다.

```
vdmutil --addGroupURLSetting --urlSettingName <URL> --groupName <그룹>
```

옵션	설명
<code>--urlSettingName</code>	할당할 URL 콘텐츠 리디렉션 설정의 이름입니다.
<code>--groupName</code>	domain\group 형식의 Active Directory 그룹 이름입니다.

## 예제: URL 콘텐츠 리디렉션 설정 할당

다음 예제에서는 url-filtering이라는 URL 콘텐츠 리디렉션 설정을 mydomainWjandoe라는 사용자에게 할당합니다.

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomainWjandoe
```

다음 예제에서는 url-filtering이라는 URL 콘텐츠 리디렉션 설정을 mydomainWusergroup라는 그룹에 할당합니다.

```
vdmutil --addGoupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomainWusergroup
```

다음에 수행할 작업

URL 콘텐츠 리디렉션 설정을 확인합니다. [URL 콘텐츠 리디렉션 설정 테스트](#)를 참조하십시오.

## URL 콘텐츠 리디렉션 설정 테스트

URL 콘텐츠 리디렉션 설정을 만들고 할당한 후에 특정 단계를 수행하여 설정이 제대로 작동하는지 확인하십시오.

사전 요구 사항

vdmutil 명령줄 인터페이스 옵션 및 요구 사항을 파악하고 vdmutil 명령을 실행할 수 있는 충분한 권한이 있는지 확인합니다. [vdmutil 명령줄 유틸리티 사용](#)을 참조하십시오.

절차

- 1 연결 서버 인스턴스에 로그인합니다.
- 2 --readURLSetting 옵션과 함께 vdmutil 명령을 실행합니다.

예:

```
vdmutil --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

이 명령을 실행하면 URL 콘텐츠 리디렉션 설정에 대한 자세한 정보가 표시됩니다. 예를 들어 url-filtering 설정에 대한 다음 명령 출력은 텍스트 google.\*이 포함된 HTTP 및 HTTPS URL이 클라이언트에서 iexplore2012라는 로컬 애플리케이션 폴로 리디렉션된다는 것을 보여줍니다.

```
URL Redirection setting url-filtering
Description                : null
Enabled                    : true
Scope of URL Redirection Setting : LOCAL
URL Scheme And Local Resource handler pairs
  URL Scheme               : http
  Handler type              : APPLICATION
  Handler Resource name    : iexplore2012
  URL Scheme               : https
  Handler type              : APPLICATION
```

```

Handler Resource name           : iexplore2012
AgentPatterns
  https://google.*
  http://google.*
ClientPatterns
  No client patterns configured

```

- 3 Windows 클라이언트 시스템에서 Horizon Client를 열고 연결 서버 인스턴스에 연결한 후 설정에 구성된 URL 패턴과 일치하는 URL을 클릭한 후 해당 URL이 예상대로 리디렉션되는지 확인합니다.
- 4 동일한 Windows 클라이언트 시스템에서 레지스트리 편집기(regedit)를 열고 `WComputer\HKEY_CURRENT_USER\Software\VMware, Inc.\VMware\VMWURLRedirection` 경로에서 레지스트리 키를 확인합니다.

설정에 지정된 각 프로토콜에 대한 키가 표시됩니다. 프로토콜을 클릭하면 해당 프로토콜과 연결된 규칙을 볼 수 있습니다. 예를 들어 `agentRules`는 리디렉션되는 URL을 표시하고, `brokerHostName`은 URL을 리디렉션할 때 사용되는 연결 서버 인스턴스의 IP 주소 또는 정규화된 호스트 이름을 표시하고, `remoteItem`은 리디렉션된 URL을 처리하는 데스크톱 또는 애플리케이션 풀의 표시 이름을 표시합니다.

## URL 콘텐츠 리디렉션 설정 관리

`vdmutil` 명령을 사용하여 URL 콘텐츠 리디렉션 설정을 관리할 수 있습니다.

모든 명령과 함께 `--authAs`, `--authDomain` 및 `--authPassword` 옵션을 지정해야 합니다. 자세한 내용은 [vdmutil 명령줄 유틸리티 사용](#)의 내용을 참조하십시오.

### 설정 표시

구성된 모든 URL 콘텐츠 리디렉션 설정의 이름을 나열하려면 `--listURLSetting` 옵션과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --listURLSetting
```

특정 URL 콘텐츠 리디렉션 설정에 대한 자세한 정보를 보려면 `--readURLSetting`과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --readURLSetting --urlSettingName value
```

### 설정 삭제

URL 콘텐츠 리디렉션 설정을 삭제하려면 `--deleteURLSetting` 옵션과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --deleteURLSetting --urlSettingName value
```

## 설정 사용 및 사용 안 함

URL 콘텐츠 리디렉션 설정을 사용하지 않도록 지정하려면 `--disableURLSetting` 옵션과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --disableURLSetting --urlSettingName value
```

사용되지 않도록 지정된 URL 콘텐츠 리디렉션 설정을 사용하도록 지정하려면 `--enableURLSetting` 옵션과 함께 `vdmutil`을 실행합니다.

```
vdmutil --enableURLSetting --urlSettingName value
```

## 설정에서 사용자 또는 그룹 제거

URL 콘텐츠 리디렉션 설정에서 사용자를 제거하려면 `--removeUserURLSetting` 옵션과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --removeUserURLSetting --urlSettingName <값> --userName <값>
```

URL 콘텐츠 리디렉션 설정에서 그룹을 제거하려면 `--removeGroupURLSetting` 옵션과 함께 `vdmutil` 명령을 실행합니다.

```
vdmutil --removeGroupURLSetting --urlSettingName <값> --userGroup <값>
```

사용자 또는 그룹 이름을 지정할 때는 `domain\username` 또는 `domain\groupname` 형식을 사용합니다.

## 그룹 정책 설정을 사용하여 클라이언트에서 에이전트로의 리디렉션 구성

URL 콘텐츠 리디렉션 ADMX 템플릿 파일(`urlRedirection-enUS.admx`)에는 클라이언트에서 원격 데스크톱 또는 애플리케이션으로 URL을 리디렉션하는 규칙(클라이언트에서 에이전트로의 리디렉션)을 생성하는 데 사용할 수 있는 그룹 정책 설정이 포함되어 있습니다.

**참고** 기본적인 클라이언트에서 에이전트로의 리디렉션 구성 방법은 `vdmutil` 명령줄 인터페이스를 사용하는 것입니다. GPO는 macOS에서 지원되지 않으므로 macOS 클라이언트가 있는 경우에는 클라이언트에서 에이전트로의 구성을 수행하기 위해 GPO를 사용할 수 없습니다.

클라이언트에서 에이전트로의 리디렉션에 대한 규칙을 생성하려면 **remoteItem** 옵션을 사용하여 원격 데스크톱 또는 애플리케이션 풀의 표시 이름을 지정하고, **agentRules** 옵션을 사용하여 원격 데스크톱 또는 애플리케이션으로 리디렉션되어야 하는 URL을 지정합니다. 또한 **brokerHostname** 옵션을 사용하여 URL을 원격 데스크톱 또는 애플리케이션으로 리디렉션할 때 사용할 연결 서버 호스트의 IP 주소 또는 정규화된 도메인 이름을 지정해야 합니다.

예를 들어 보안을 위해 기업 네트워크를 가리키는 모든 HTTP URL이 원격 데스크톱이나 애플리케이션에서 열리도록 할 수 있습니다. 이 경우 **agentRules** 옵션을 `.*.mycompany.com`으로 설정할 수 있습니다.

URL 콘텐츠 리디렉션 템플릿 파일 설치 지침에 대해서는 [GPO에 URL 콘텐츠 리디렉션 ADMX 템플릿 추가](#)를 참조하십시오.

## URL 콘텐츠 리디렉션 제한

URL 콘텐츠 리디렉션 기능의 동작으로 인해 예기치 않은 특정 결과가 발생할 수 있습니다.

- URL이 로컬을 기준으로 국가별 페이지를 열 경우 링크 소스는 열린 로컬 페이지를 확인합니다. 예를 들어 원격 데스크톱(에이전트 소스)이 일본의 데이터 센터에 있고 사용자의 컴퓨터가 미국에 있는 경우 URL이 에이전트에서 클라이언트 시스템으로 리디렉션되면 미국 클라이언트에서 일본어 페이지가 열립니다.
- 사용자가 웹 페이지에서 즐겨찾기를 만들면 리디렉션 후 즐겨찾기가 생성됩니다. 예를 들어 사용자가 클라이언트 시스템에서 링크를 클릭하고 URL이 원격 데스크톱(에이전트)으로 리디렉션되며 사용자가 해당 페이지에 대해 즐겨찾기를 생성하면 즐겨찾기가 해당 에이전트에서 생성됩니다. 다음 번에 클라이언트 시스템에서 사용자가 브라우저를 열 때 사용자는 클라이언트 시스템에 즐겨찾기가 있을 것으로 기대하겠지만 즐겨찾기는 원격 데스크톱(에이전트 소스)에 저장되어 있습니다.
- 사용자가 다운로드하는 파일이 브라우저가 URL을 여는 데 사용된 시스템에 나타납니다. 예를 들어 사용자가 클라이언트 시스템에서 링크를 클릭한 경우에는 URL이 원격 데스크톱으로 리디렉션됩니다. 링크를 클릭하면 파일이 다운로드되거나 링크가 사용자가 파일을 다운로드하는 웹 페이지에 대한 링크인 경우 파일이 클라이언트 시스템이 아닌 원격 데스크톱으로 다운로드됩니다.
- 동일한 시스템에 Horizon Agent 및 Horizon Client를 설치하는 경우 Horizon Agent 또는 Horizon Client 중 하나에서만 URL 콘텐츠 리디렉션을 사용하도록 설정할 수 있습니다. 이 시스템에서는 클라이언트에서 에이전트로의 리디렉션 또는 에이전트에서 클라이언트로의 리디렉션을 설정할 수 있지만 둘 다를 설정할 수는 없습니다.

## 지원되지 않는 URL 콘텐츠 리디렉션 기능

특정 상황에서는 URL 콘텐츠 리디렉션 기능이 작동하지 않습니다.

### 단축 URL

<https://goo.gl/abc>와 같은 단축 URL을 필터링 규칙에 따라 리디렉션할 수 있지만, 필터링 메커니즘에서 단축되지 않은 원래의 URL을 확인하지는 않습니다.

예를 들어 [acme.com](http://www.acme.com/some-really-long-path)이 포함된 URL, <http://www.acme.com/some-really-long-path>와 같은 원래 URL, <https://goo.gl/xyz>와 같은 원래 URL의 단축 URL을 리디렉션하는 규칙이 있을 경우, 원래 URL은 리디렉션되지만 단축 URL은 리디렉션되지 않습니다.

URL 단축에 가장 자주 사용되는 웹 사이트에서 URL을 차단하거나 리디렉션하는 규칙을 생성하여 이러한 제한을 해결할 수 있습니다.

### 내장된 HTML 페이지

내장된 HTML 페이지는 URL 리디렉션을 우회합니다. 예를 들어 사용자가 URL 리디렉션 규칙과 일치하지 않는 URL로 이동하는 경우가 여기에 해당됩니다. 페이지에 리디렉션 규칙과 일치하는 URL을 포함하는 내장된 HTML 페이지(iFrame 또는 인라인 프레임)가 있으면 URL 리디렉션 규칙이 작동하지 않습니다. 규칙은 최상위 URL에서만 작동합니다.

## 사용하지 않도록 설정된 Internet Explorer 플러그인

사용자가 Internet Explorer에서 InPrivate 브라우징으로 전환한 경우와 같이 Internet Explorer 플러그인을 사용하지 않도록 설정한 경우에는 URL 콘텐츠 리디렉션이 작동하지 않습니다. 사람들은 웹 페이지와 웹 페이지에서 다운로드한 파일이 자신의 컴퓨터에서 검색 및 다운로드 내역에 기록되지 않도록 비공개 검색을 사용합니다. URL 리디렉션 기능을 사용하려면 특정 Internet Explorer 플러그인을 사용하도록 설정해야 하지만 비공개 검색에서는 이러한 플러그인을 사용하지 않도록 설정하기 때문에 이러한 제한이 발생합니다.

GPO 설정을 사용하여 사용자가 플러그인을 사용하지 않도록 설정하지 못하게 함으로써 이러한 제한을 해결할 수 있습니다. 이러한 설정에는 [사용자가 추가 기능을 사용 또는 사용할 수 없도록 설정하는 것을 허용 안 함] 및 [새로 설치된 추가 기능을 자동으로 사용]이 포함됩니다. 그룹 정책 관리 편집기에서 해당 설정은 **컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > Internet Explorer**에 있습니다.

특히 Internet Explorer에서 이러한 제한을 해결하려면 GPO 설정을 사용하여 InPrivate 모드를 사용하지 않도록 설정하십시오. 이 설정은 "InPrivate 브라우징 끄기"라고 합니다. 그룹 정책 관리 편집기에서 해당 설정은 **컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > Internet Explorer > 개인 정보**에 있습니다.

이러한 해결 방법은 모범 사례로, 비공개 검색 이외의 상황에서 발생할 수 있는 리디렉션 문제를 방지할 수 있습니다.

## Windows 10 범용 애플리케이션이 프로토콜에 대한 기본 처리기인 경우

링크에 지정된 프로토콜에 대한 기본 처리기가 Windows 10 범용 애플리케이션일 경우 URL 리디렉션이 작동하지 않습니다. PC, 태블릿, 스마트폰으로 다운로드할 수 있도록 범용 Windows 플랫폼을 바탕으로 만들어진 범용 애플리케이션으로는 Microsoft Edge 브라우저, 메일, 지도, 사진, Groove 음악 등이 있습니다.

이러한 애플리케이션 중 하나가 기본 처리기인 링크를 클릭하면 URL이 리디렉션되지 않습니다. 예를 들어 사용자가 애플리케이션에서 e-메일 링크를 클릭하고 기본 e-메일 애플리케이션이 메일 범용 애플리케이션인 경우 링크에 지정된 URL이 리디렉션되지 않습니다.

다른 애플리케이션을 리디렉션하려는 URL 프로토콜의 기본 처리기로 지정하여 이러한 제한을 해결할 수 있습니다. 예를 들어, Edge가 기본 브라우저이면 Internet Explorer를 기본 브라우저로 설정합니다.

## 보안 부팅 사용 시스템

보안 부팅이 사용되도록 설정된 시스템의 경우 URL 콘텐츠 리디렉션 기능을 사용 안 함 상태로 둡니다. 이러한 시스템에서는 URL을 리디렉션할 수 없습니다. 해당 시스템으로 URL을 리디렉션할 수는 있습니다.

# 원격 데스크톱 및 애플리케이션에 서 USB 디바이스 사용

## 4

관리자는 원격 데스크톱에서 썸 플래시 드라이브, 카메라, VoIP(Voice-over-IP) 디바이스, 프린터와 같은 USB 디바이스를 사용하는 기능을 구성할 수 있습니다. 이 기능은 USB 리디렉션이라고 하며 Blast Extreme, PCoIP 또는 Microsoft RDP 디스플레이 프로토콜의 사용을 지원합니다. 원격 데스크톱 하나에서 최대 128개의 USB 디바이스를 수용할 수 있습니다.

RDS 데스크톱 및 애플리케이션에서 사용하기 위해 로컬로 연결된 USB 썸 플래시 드라이브 및 하드 디스크를 리디렉션할 수도 있습니다. 다른 유형의 스토리지 디바이스를 포함한 다른 유형의 USB 디바이스는 RDS 데스크톱 및 애플리케이션에서 지원되지 않습니다.

단일 사용자 시스템에 배포된 데스크톱 풀에서 이 기능을 사용하면 로컬 클라이언트 시스템에 연결된 대부분의 USB 디바이스를 원격 데스크톱에서 사용할 수 있습니다. 원격 데스크톱에서 iPad에 연결하여 이 디바이스를 관리할 수도 있습니다. 예를 들어 원격 데스크톱에 설치된 iTunes와 iPad를 동기화할 수 있습니다. Windows 및 Mac 컴퓨터 같은 일부 클라이언트 디바이스에서는 USB 디바이스가 Horizon Client의 메뉴에 나열됩니다. 디바이스를 연결 및 연결 해제하는 메뉴를 사용합니다.

대부분의 경우 USB 디바이스를 클라이언트 시스템과 원격 데스크톱 또는 애플리케이션에서 동시에 사용할 수 없습니다. 일부 유형의 USB 디바이스만 원격 데스크톱과 로컬 컴퓨터 간에 공유할 수 있습니다. 이러한 디바이스에는 스마트 카드 판독기와 키보드 및 포인팅 디바이스 같은 휴먼 인터페이스 디바이스가 포함됩니다.

관리자는 최종 사용자가 연결할 수 있는 USB 디바이스의 유형을 지정할 수 있습니다. 비디오 입력 디바이스 및 스토리지 디바이스와 같은 여러 디바이스 유형을 포함하는 복합 디바이스의 경우 관리자는 일부 클라이언트 시스템에서 하나의 디바이스(예: 비디오 입력 디바이스)는 허용되지만 다른 디바이스(예: 스토리지 디바이스)는 허용되지 않도록 디바이스를 분할할 수 있습니다.

USB 리디렉션 기능은 일부 클라이언트 유형에서만 이용 가능합니다. 특정 유형의 클라이언트에서 이 기능이 지원되는지 여부를 확인하려면, "VMware Horizon Client 사용" 문서에 포함된 기능 지원 매트릭스를 참조하여 지원되는 특정 유형의 데스크톱 또는 모바일 클라이언트 디바이스를 확인하십시오. 자세한 사항은 [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html)의 내용을 참조하십시오.

---

**중요** USB 리디렉션 기능을 배포할 때 USB 디바이스에 영향을 줄 수 있는 보안 취약점으로부터 조직을 보호하기 위한 단계를 수행할 수 있습니다. [보안 Horizon 7 환경에 USB 디바이스 배포](#)의 내용을 참조하십시오.

---

본 장은 다음 항목을 포함합니다.

### ■ USB 디바이스 유형의 제한 사항

- USB 리디렉션 설정 개요
- 네트워크 트래픽 및 USB 리디렉션
- USB 디바이스에 대한 자동 연결
- 보안 Horizon 7 환경에 USB 디바이스 배포
- 로그 파일을 사용하여 문제 해결 및 USB 디바이스 ID 확인
- USB 리디렉션 제어를 위한 정책 사용
- USB 리디렉션 문제 해결

## USB 디바이스 유형의 제한 사항

Horizon 7는 원격 데스크톱에서 사용할 수 있는 디바이스에 명시적으로 제한을 두지 않지만 네트워크 지연 시간 및 대역폭 같은 요인 때문에 일부 디바이스의 성능이 다른 디바이스보다 더 나을 수 있습니다. 기본적으로 일부 디바이스는 사용하지 못하도록 자동으로 필터링되거나 차단됩니다.

Windows, Linux 및 Mac 클라이언트에서 Horizon 6.0.1과 Horizon Client 3.1 이상을 함께 사용하면 클라이언트 시스템의 USB 3.0 포트에 USB 3.0 디바이스를 연결할 수 있습니다. USB 3.0 디바이스는 단일 스트림을 통해서만 지원됩니다. 이 릴리스에서는 다중 스트림 지원이 구현되지 않았기 때문에 USB 디바이스 성능은 향상되지 않습니다. 올바르게 작동하기 위해 일정하게 높은 처리량이 필요한 일부 USB 3.0 디바이스는 네트워크 지연으로 VDI 세션에서 작동하지 못할 수 있습니다.

이전 View 릴리스에서는 초고속 USB 3.0 디바이스가 지원되지 않지만 클라이언트 시스템에서 USB 3.0 디바이스를 USB 2.0에 꽂으면 종종 작동합니다. 그러나 클라이언트 시스템 마더보드에 장착한 USB 칩셋 유형에 따라 예외가 있을 수 있습니다.

다음 유형의 디바이스는 단일 사용자 시스템에 배포된 원격 데스크톱으로의 USB 리디렉션에 적합하지 않을 수 있습니다.

- 웹캠은 대개 60Mbps 이상의 대역폭을 필요로 하기 때문에 USB 리디렉션을 통해 지원되지 않습니다. 웹캠의 경우에는 실시간 오디오-비디오 기능을 사용할 수 있습니다.
- USB 오디오 디바이스의 리디렉션 가능 여부는 네트워크의 상태에 따라 달라질 수 있으며 안정적이지 않습니다. 일부 디바이스의 경우, 유휴 상태에서도 높은 데이터 처리량을 요구합니다. 실시간 오디오-비디오 기능이 설치되어 있으면 오디오 입력 및 출력 디바이스가 이 기능을 통해 문제없이 작동하기 때문에 해당 디바이스에 대해 USB 리디렉션을 사용하지 않아도 됩니다.
- USB CD/DVD 굽기는 지원되지 않습니다.
- 일부 USB 디바이스는 WAN을 사용하는 경우에는 특히 네트워크 지연 시간과 신뢰성에 따라 성능이 크게 달라질 수 있습니다. 예를 들어, USB 스토리지 디바이스의 읽기 요청을 1회 수행하려면 클라이언트와 원격 데스크톱 사이에 세 번의 왕복 통신이 필요합니다. 전체 파일을 읽는 데는 여러 번의 USB 읽기 작업이 필요할 수 있으며, 지연 시간이 길수록 왕복 시간이 더 오래 걸립니다.

파일 구조는 파일 형식에 따라 상당히 클 수 있습니다. 대용량 USB 디스크 드라이브는 데스크톱에 나타나는 데 수 분이 소요될 수 있습니다. USB 디바이스를 FAT 대신 NTFS로 포맷하면 초기 연결 시간을 줄이는 데 도움이 됩니다. 안정적이지 않은 네트워크 연결을 사용할 경우 재시도 횟수가 증가하여 성능이 저하될 수 있습니다.



마찬가지로 USB CD/DVD 판독기와 스캐너 및 터치 디바이스(예: 전자서명용 태블릿)는 WAN과 같은 숨어 있는 네트워크에서는 잘 작동하지 않습니다.

- USB 스캐너의 리디렉션은 네트워크 상태에 따라 달라지고 스캔이 완료되는 시간이 평소보다 오래 걸릴 수 있습니다.

다음 유형의 디바이스를 RDS 호스트의 게시된 데스크톱 또는 애플리케이션으로 리디렉션할 수 있습니다.

- USB 씬 플래시 드라이브
- USB 하드 디스크

Horizon 7 버전 7.0.2부터 서명 패드, 받아쓰기 퓌트 페달, 일부 Wacom 태블릿을 게시된 데스크톱 또는 애플리케이션으로 리디렉션할 수 있습니다. 이러한 디바이스는 Horizon 7 버전 7.0.2에서 기본적으로 사용되지 않도록 설정됩니다. 이러한 디바이스를 사용하도록 설정하려면 Windows 레지스트리 키 설정 ExcludeAllDevices 및 IncludeFamily를 경로 HKLM\Software\Policies\VMware, Inc\VMware VDM WAgent\WUSB에서 삭제하십시오. Horizon 7 버전 7.0.3 이상에서는 기본적으로 이러한 디바이스가 사용되도록 설정됩니다.

다른 유형의 USB 디바이스와 보안 스토리지 드라이브, USB CD-ROM 등의 다른 유형의 USB 스토리지 디바이스를 게시된 데스크톱 또는 애플리케이션으로 리디렉션할 수 없습니다.

## USB 리디렉션 설정 개요

최종 사용자가 USB 플래시 드라이브, 카메라, 헤드셋 등의 이동식 디바이스를 연결할 수 있도록 배포를 설정하려면 원격 데스크톱 또는 RDS 호스트와 클라이언트 디바이스 모두에 특정 구성 요소를 설치하고 USB 디바이스에 대한 전역 설정이 View Administrator에서 사용하도록 설정되었는지 확인해야 합니다.

이 체크리스트에는 엔터프라이즈 내 USB 리디렉션 설정을 위한 필수 작업과 선택적 작업이 모두 포함되어 있습니다.

USB 리디렉션 기능은 Windows 클라이언트, Mac 클라이언트, 파트너 제공 Linux 클라이언트 등의 일부 클라이언트 유형에서만 사용할 수 있습니다. 특정 유형의 클라이언트에서 이 기능이 지원되는지 확인하려면 "VMware Horizon Client 사용" 문서에 포함된 기능 지원 표를 참조하여 지원되는 특정 유형의 클라이언트 디바이스를 확인하십시오. 자세한 사항은 [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html)의 내용을 참조하십시오.

**중요** USB 리디렉션 기능을 배포할 때 USB 디바이스에 영향을 줄 수 있는 보안 취약점으로부터 조직을 보호하기 위한 단계를 수행할 수 있습니다. 예를 들어 그룹 정책 설정을 사용하여 일부 원격 데스크톱 및 사용자에게 USB 리디렉션을 사용하지 않도록 설정하거나 리디렉션 가능한 USB 디바이스 유형을 제한할 수 있습니다. [보안 Horizon 7 환경에 USB 디바이스 배포](#)의 내용을 참조하십시오.

- 1 원격 데스크톱 소스 또는 RDS 호스트에서 Horizon Agent 설치 마법사를 실행하는 경우 USB 리디렉션 구성 요소를 포함해야 합니다.

이 구성 요소는 기본적으로 선택 취소되어 있습니다. 설치하려면 이 구성 요소를 선택해야 합니다.

- 클라이언트 시스템에서 VMware Horizon Client 설치 마법사를 실행하는 경우 USB 리디렉션 구성 요소를 포함해야 합니다.

이 구성 요소는 기본적으로 포함되어 있습니다.

- 원격 데스크톱 또는 애플리케이션에서 USB 디바이스로의 액세스가 View Administrator에서 사용하도록 설정되었는지 확인합니다.

View Administrator에서 **정책 > 전역 정책**으로 이동하고 **USB 액세스**가 **허용**으로 설정되었는지 확인합니다.

- (선택 사항) Horizon Agent 그룹 정책을 구성하여 리디렉션할 수 있는 디바이스 유형을 지정합니다.

[USB 리디렉션 제어를 위한 정책 사용](#)의 내용을 참조하십시오.

- (선택 사항) 클라이언트 디바이스에서 유사한 설정을 구성합니다.

Horizon Client가 원격 데스크톱 또는 애플리케이션에 연결할 때 또는 최종 사용자가 USB 디바이스를 연결할 때 디바이스가 자동으로 연결되는지 여부를 구성할 수도 있습니다. 클라이언트 디바이스에서 USB 설정을 구성하는 방법은 디바이스 유형에 따라 다릅니다. 예를 들어, Windows 클라이언트 끝점의 경우에는 그룹 정책을 구성할 수 있지만 Mac 끝점의 경우에는 명령줄 명령을 사용합니다. 자세한 지침은 특정 클라이언트 디바이스 유형에 대한 "VMware Horizon Client 사용" 설명서를 참조하십시오.

- 최종 사용자가 원격 데스크톱 또는 애플리케이션에 연결하여 USB 디바이스를 로컬 클라이언트 시스템에 연결하도록 합니다.

USB 디바이스 드라이버가 원격 데스크톱 또는 RDS 호스트에 설치되어 있지 않은 경우 물리적 Windows 컴퓨터에서와 마찬가지로 게스트 운영 체제가 USB 디바이스를 감지하고 적합한 드라이버를 검색합니다.

## 네트워크 트래픽 및 USB 리디렉션

USB 리디렉션은 디스플레이 프로토콜(RDP 또는 PCoIP)에 독립적으로 작동하며 USB 트래픽은 대개 TCP 포트 32111을 사용합니다.

클라이언트 시스템과 원격 데스크톱 또는 애플리케이션 간의 네트워크 트래픽은 클라이언트 시스템이 회사 네트워크 내부에 있는지 여부 및 관리자가 보안을 설정한 방법에 따라 다양한 경로를 통해 이동할 수 있습니다.

- 클라이언트 시스템이 회사 네트워크 내부에 있어 클라이언트와 데스크톱 또는 애플리케이션을 직접 연결할 수 있는 경우에는 USB 트래픽이 TCP 포트 32111을 사용합니다.
- 클라이언트 시스템이 회사 네트워크 외부에 있는 경우, 클라이언트는 View 보안 서버를 통해 연결할 수 있습니다.

보안 서버는 DMZ에 상주하며 신뢰할 수 있는 네트워크 내 연결을 위한 프록시 호스트 역할을 합니다. 이 디자인은 공용 인터넷에서 View 연결 서버 인스턴스를 보호하고 보안 서버를 통해 보호되지 않은 모든 세션을 강제로 요청하여 추가 보안 계층을 제공합니다.

DMZ 기반 보안 서버를 배포하려면 클라이언트를 DMZ 내 보안 서버와 연결시키는 방화벽에서 일부 포트를 열어야 합니다. 또한 내부 네트워크의 View 연결 서버 인스턴스 및 보안 서버 간 통신을 위해 포트를 구성해야 합니다.

특정 포트에 대한 자세한 내용은 "View 아키텍처 계획 가이드"에서 "DMZ 기반 보안 서버의 방화벽 규칙"을 참조하십시오.

- 클라이언트 시스템이 회사 네트워크 외부에 있는 경우에는 View Administrator를 사용하여 HTTPS 보안 터널을 사용하도록 설정할 수 있습니다. 그러면 클라이언트는 사용자가 원격 데스크톱 또는 애플리케이션에 연결할 때 View 연결 서버 또는 보안 서버 호스트에 추가 HTTPS 연결을 생성합니다. 연결은 HTTPS 포트 443을 사용하여 보안 서버에 터널링되고, 이 서버에서 원격 데스크톱 또는 애플리케이션으로의 USB 트래픽에 필요한 연결에는 TCP 포트 32111이 사용됩니다. 이 터널을 사용할 때 USB 디바이스 성능이 약간 저하됩니다.

---

**참고** 제로 클라이언트를 사용하는 경우에는 TCP 32111 대신 PCoIP 가상 채널을 사용하여 USB 트래픽이 리디렉션됩니다. 데이터는 TCP/UDP 포트 4172를 사용하는 PCoIP 보안 게이트웨이를 통해 캡슐화되고 암호화됩니다. 제로 클라이언트만 사용할 때는 TCP 포트 32111을 열지 않아도 됩니다.

---

## USB 디바이스에 대한 자동 연결

일부 클라이언트 시스템에서는 관리자, 최종 사용자 또는 둘 모두가 원격 데스크톱에 대한 USB 디바이스 자동 연결을 구성할 수 있습니다. 자동 연결은 사용자가 클라이언트 시스템에 USB 디바이스를 연결하거나 클라이언트가 원격 데스크톱에 연결하는 경우에 실행될 수 있습니다.

스마트폰과 태블릿 같은 일부 디바이스의 경우에는 업그레이드 시 해당 디바이스가 시작되는 과정에서 연결이 끊어지기 때문에 자동 연결 기능이 필요합니다. 원격 데스크톱에 자동으로 다시 연결하도록 이러한 디바이스를 설정하지 않은 경우 업그레이드를 진행하는 동안 디바이스가 다시 시작되면 로컬 클라이언트 시스템에 대신 연결됩니다.

관리자가 클라이언트에 설정하거나, 최종 사용자가 Horizon Client 메뉴 항목을 사용하여 설정하는 자동 USB 연결 구성 속성은 USB 리디렉션에서 제외하도록 구성된 디바이스를 제외한 모든 USB 디바이스에 적용됩니다. 예를 들어, 일부 클라이언트 버전에서 웹캠과 마이크는 실시간 오디오-비디오 기능을 통해 더 효과적으로 작동하기 때문에 기본적으로 USB 리디렉션에서 제외됩니다. 경우에 따라서는 USB 디바이스가 기본적으로 리디렉션에서 제외되지 않고 관리자가 해당 디바이스를 명시적으로 리디렉션에서 제외해야 할 수 있습니다. 예를 들어, 다음과 같은 USB 디바이스 유형은 USB 리디렉션의 대상으로 적합하지 않으며 원격 데스크톱에 자동으로 연결되면 안 됩니다.

- USB 이더넷 디바이스. USB 이더넷 디바이스를 리디렉션할 경우, 해당 디바이스가 유일한 이더넷 디바이스면 클라이언트 시스템에서 네트워크에 연결하지 못할 수 있습니다.
- 터치 스크린 디바이스. 터치 스크린 디바이스를 리디렉션할 경우, 원격 데스크톱에서는 터치 입력은 수신하지만 키보드 입력은 수신하지 않습니다.

USB 디바이스를 자동 연결하도록 원격 데스크톱을 설정한 경우에는 터치 스크린 및 네트워크 디바이스 같은 특정 디바이스를 제외하도록 정책을 구성할 수 있습니다. 자세한 내용은 [USB 디바이스를 위한 필터 정책 설정 구성](#)의 내용을 참조하십시오.

Windows 클라이언트에서는 제외된 디바이스 이외의 모든 디바이스를 자동으로 연결하는 설정을 사용하는 대신 클라이언트에서 구성 파일을 편집하여 Horizon Client가 스마트폰이나 태블릿 같은 특정 디바이스만 원격 데스크톱에 다시 연결하도록 설정할 수 있습니다. 자세한 지침은 “Windows용 VMware Horizon Client 사용” 을 참조하십시오.

## 보안 Horizon 7 환경에 USB 디바이스 배포

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

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

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

## 모든 유형의 디바이스에 대한 USB 리디렉션 사용 안 함

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

각자의 상황에 맞게 다음의 전략 중에 선택하여 사용하십시오.

- Horizon Agent를 데스크톱 이미지 또는 RDS 호스트에 설치할 때 **USB 리디렉션** 설정 옵션의 선택을 취소합니다. (이 옵션은 기본적으로 선택 취소되어 있습니다.) 이 접근 방식은 데스크톱 이미지 또는 RDS 호스트에서 배포된 모든 원격 데스크톱 및 애플리케이션의 USB 디바이스에 대한 액세스를 방지합니다.
- Horizon Administrator에서 특정 풀에 대한 액세스를 거부하거나 허용하도록 **USB 액세스** 정책을 편집합니다. 이 접근 방식을 사용하면 데스크톱 이미지를 변경할 필요가 없으며 특정 데스크톱 및 애플리케이션 풀의 USB 디바이스에 대한 액세스를 제어할 수 있습니다.  
  
RDS 데스크톱 및 애플리케이션 풀에 대해 전역 **USB 액세스** 정책만 사용할 수 있습니다. 개별 RDS 데스크톱 또는 애플리케이션 풀에 대해서는 이 정책을 설정할 수 없습니다.
- View Administrator에서 데스크톱 또는 애플리케이션 풀 수준에서 정책을 설정한 후 **사용자 재정**의 설정을 선택하고 사용자를 선택하여 풀의 특정 사용자에게 대한 정책을 재정의할 수 있습니다.
- Horizon Agent 측 또는 클라이언트 측 중 상황에 맞게 Exclude All Devices 정책을 **true**로 설정합니다.

- 스마트 정책을 사용하여 **USB 리디렉션** Horizon 정책 설정을 사용하지 않도록 설정하는 정책을 만듭니다. 이 접근 방식을 사용하면 특정 조건이 충족된 경우에 특정 원격 데스크톱에서 USB 리디렉션을 사용하지 않도록 설정할 수 있습니다. 예를 들어, 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결하면 USB 리디렉션을 사용하지 않도록 설정하는 정책을 구성할 수 있습니다.

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

표 4-1. 모든 디바이스 제외 정책 결합 효과

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

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

이러한 정책은 Horizon Agent 구성 ADMX 템플릿 파일(vdm\_agent.admx)에 포함되어 있습니다.

## 특정 디바이스에 대해 USB 리디렉션을 사용하지 않도록 설정

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

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

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

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

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

```
ExcludeAllDevices    Enabled

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

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

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

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

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

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

```
ExcludeAllDevices    Enabled

IncludeDeviceFamily  o:storage
```

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

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

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

## 로그 파일을 사용하여 문제 해결 및 USB 디바이스 ID 확인

유용한 USB 로그 파일이 클라이언트 시스템과 원격 데스크톱 운영 체제 또는 RDS 호스트 모두에 있습니다. 두 위치에 있는 로그 파일을 문제 해결에 사용하십시오. 특정 디바이스의 제품 ID를 찾으려면 클라이언트 측 로그를 사용하십시오.

USB 디바이스 분할 또는 필터링을 구성하려는 경우 또는 특정 디바이스가 Horizon Client 메뉴에 나타나지 않는 이유를 확인하려는 경우에는 클라이언트 측 로그를 살펴보십시오. 클라이언트 로그는 USB 중재자와 Horizon View USB 서비스용으로 생성됩니다. Windows 및 Linux 클라이언트에서는 로깅을 기본적으로 사용하도록 설정됩니다. Mac 클라이언트에서는 로깅을 기본적으로 사용하지 않도록 설정됩니다. Mac 클라이언트에서 로깅을 사용하도록 설정하려면 “Mac용 VMware Horizon Client 사용” 문서를 참조하십시오.

USB 디바이스 분할 및 필터링을 위한 정책을 구성할 경우 일부 값을 설정하려면 USB 디바이스의 VID(벤더 ID)와 PID(제품 ID)가 필요합니다. VID 및 PID를 찾으려면 vid 및 pid와 결합된 제품 이름을 인터넷에서 검색하면 됩니다. 또는 Horizon Client가 실행 중일 때 USB 디바이스를 로컬 시스템에 연결한 후 클라이언트 측 로그 파일을 살펴볼 수 있습니다. 다음 표에서는 로그 파일의 기본 위치를 보여 줍니다.

표 4-2. 로그 파일 위치

클라이언트 또는 에이전트	로그 파일의 경로
Windows 클라이언트	%PROGRAMDATA%\VMware\WDM\logs\debug-*.txt C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log
Horizon Agent	%PROGRAMDATA%\VMware\WDM\logs\debug-*.txt
Mac 클라이언트	/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log /Library/Logs/VMware/vmware-usbarbitrator-xxxx.log
Linux 클라이언트	(기본 위치) /tmp/vmware-root/vmware-view-usbd-*.log

디바이스가 원격 데스크톱 또는 애플리케이션으로 리디렉션된 후 디바이스에 문제가 발생하면 클라이언트 측 로그와 에이전트 측 로그를 모두 검사하십시오.

## USB 리디렉션 제어를 위한 정책 사용

원격 데스크톱 또는 애플리케이션(Horizon Agent)과 Horizon Client 모두에 대한 USB 정책을 구성할 수 있습니다. 이러한 정책은 클라이언트 디바이스가 복합 USB 디바이스를 별도의 리디렉션 구성 요소로 분할해야 하는지 여부를 지정합니다. 디바이스를 분할하여 클라이언트가 리디렉션에 사용할 수 있도록 설정할 USB 디바이스 유형을 제한하고 Horizon Agent가 특정 USB 디바이스에 대해 클라이언트 컴퓨터로부터의 전달을 차단하도록 할 수 있습니다.

이전 버전의 Horizon Agent 또는 Horizon Client가 설치되어 있는 경우에는 USB 리디렉션 정책 기능의 일부를 사용할 수 없습니다. 표 4-3. [USB 정책 설정 호환성](#)에서는 Horizon 7가 다양한 Horizon Agent 및 Horizon Client 조합에 정책을 적용하는 방법을 보여 줍니다.



표 4-3. USB 정책 설정 호환성

Horizon Agent 버전	Horizon Client 버전	USB 정책 설정이 USB 리디렉션에 미치는 영향
5.1 이상	5.1 이상	Horizon Agent와 Horizon Client 모두에 USB 정책 설정을 적용할 수 있습니다. Horizon Agent USB 정책 설정을 사용하여 USB 디바이스가 데스크톱에 전달되지 않도록 할 수 있습니다. Horizon Agent는 Horizon Client로 디바이스 분할 및 필터링 정책 설정을 보낼 수 있습니다. Horizon Client USB 정책 설정을 사용하여 USB 디바이스가 클라이언트 컴퓨터에서 데스크톱으로 리디렉션되지 않도록 할 수 있습니다.  <b>참고</b> View Agent 6.1 이상 및 Horizon Client 3.3 이상에서는 이러한 USB 리디렉션 정책 설정이 RDS 데스크톱 및 애플리케이션과 단일 사용자 시스템에서 실행되는 원격 데스크톱에 적용됩니다.
5.1 이상	5.0.x 이하	USB 정책 설정이 Horizon Agent에만 적용됩니다. Horizon Agent USB 정책 설정을 사용하여 USB 디바이스가 데스크톱에 전달되지 않도록 할 수 있습니다. Horizon Client USB 정책 설정을 사용하여 클라이언트 컴퓨터에서 데스크톱으로 리디렉션될 수 있는 디바이스를 제어할 수 없습니다. Horizon Client가 Horizon Agent의 디바이스 분할 및 필터링 정책 설정을 수신할 수 없습니다. USB 리디렉션에 대한 Horizon Client의 기존 레지스트리 설정은 유효하게 유지됩니다.
5.0.x 이하	5.1 이상	USB 정책 설정이 Horizon Client에만 적용됩니다. Horizon Client USB 정책 설정을 사용하여 USB 디바이스가 클라이언트 컴퓨터에서 데스크톱으로 리디렉션되지 않도록 할 수 있습니다. Horizon Agent USB 정책 설정을 사용하여 USB 디바이스가 데스크톱에 전달되지 않도록 할 수 없습니다. Horizon Agent는 Horizon Client로 디바이스 분할 및 필터링 정책 설정을 보낼 수 없습니다.
5.0.x 이하	5.0.x 이하	USB 정책 설정이 적용되지 않습니다. USB 리디렉션에 대한 Horizon Client의 기존 레지스트리 설정은 유효하게 유지됩니다.

Horizon Client를 업그레이드할 경우 HardwareIdFilters와 같은 USB 리디렉션에 대한 기존 레지스트리 설정은 Horizon Client에 대한 USB 정책을 정의할 때까지 유효하게 유지됩니다.

클라이언트 측 USB 정책을 지원하지 않는 클라이언트 디바이스에서 Horizon Agent에 대한 USB 정책을 사용하여 클라이언트에서 데스크톱 또는 애플리케이션으로 전달할 수 있는 USB 디바이스를 제어할 수 있습니다.

## 복합 USB 디바이스를 위한 디바이스 분할 정책 설정 구성

복합 USB 디바이스는 비디오 입력 디바이스와 스토리지 디바이스 또는 마이크와 마우스 디바이스처럼 서로 다른 두 개 이상의 디바이스 조합으로 구성됩니다. 하나 이상의 구성 요소를 리디렉션에 사용하면 복합 디바이스를 해당 구성 요소 인터페이스로 분할하고 특정 인터페이스를 리디렉션에서 제외하고 필요한 인터페이스만 포함하면 됩니다.

복합 디바이스를 자동으로 분할하는 정책을 설정할 수 있습니다. 특정 디바이스에 대해 자동 디바이스 분할을 사용할 수 없거나 자동 분할 기능이 애플리케이션에서 필요로 하는 결과를 제공하지 못하는 경우에는 복합 디바이스를 수동으로 분할할 수 있습니다.

## 자동 디바이스 분할

자동 디바이스 분할을 사용하도록 설정한 경우 Horizon 7는 적용된 필터 규칙에 따라 복합 디바이스에서 기능 또는 디바이스 분할을 시도합니다. 예를 들어, 녹취용 마이크를 자동으로 분할하여 마우스 디바이스는 로컬 상태로 클라이언트에 두고 나머지 디바이스만 원격 데스크톱에 전달할 수 있습니다.



다음 표에서는 Allow Auto Device Splitting 설정의 값이 Horizon Client가 복합 USB 디바이스의 자동 분할 시도 여부에 어떤 영향을 주는지 보여 줍니다. 기본적으로 자동 분할은 사용하지 않도록 설정됩니다.

표 4-4. 자동 분할 사용 안 함 정책 결합 효과

Horizon Agent에서 자동 디바이스 분할 허용 정책	Horizon Client에서 자동 디바이스 분할 허용 정책	결합된 효율적 자동 디바이스 분할 허용 정책
Allow - Default Client Setting	<b>false</b> (자동 분할 사용 안 함)	자동 분할 사용 안 함
Allow - Default Client Setting	<b>true</b> (자동 분할 사용)	자동 분할 사용
Allow - Default Client Setting	정의되지 않음	자동 분할 사용
Allow - Override Client Setting	임의 또는 정의되지 않음	자동 분할 사용
정의되지 않음	정의되지 않음	자동 분할 사용 안 함

**참고** 이러한 정책은 Horizon Agent 구성 ADMX 템플릿 파일에 포함되어 있습니다. ADMX 템플릿 파일의 이름은 vdm\_agent.admx입니다.

기본적으로 Horizon 7는 자동 분할을 사용하지 않으며 복합 USB 디바이스의 오디오 출력, 키보드, 마우스 또는 스마트 카드 구성 요소를 리디렉션에서 제외합니다.

Horizon 7는 모든 필터 정책 설정을 적용하기 전에 디바이스 분할 정책 설정부터 적용합니다. 자동 분할을 사용하도록 설정했고 벤더 및 제품 ID를 지정하여 복합 USB 디바이스가 분할되지 않도록 명시적으로 제외하지 않을 경우 Horizon 7는 복합 USB 디바이스의 각 인터페이스를 검토하여 필터 정책 설정에 따라 제외할 인터페이스와 포함할 인터페이스를 결정합니다. 자동 디바이스 분할을 사용하지 않도록 설정했고 분할할 복합 USB 디바이스의 벤더 및 제품 ID를 명시적으로 지정하지 않은 경우 Horizon 7는 필터 정책 설정을 전체 디바이스에 적용합니다.

자동 분할을 사용하도록 설정한 경우 Exclude Vid/Pid Device From Split 정책을 사용하여 분할에서 제외할 복합 USB 디바이스를 지정할 수 있습니다.

## 수동 디바이스 분할

Split Vid/Pid Device 정책을 사용하여 분할할 복합 USB 디바이스의 벤더 및 제품 ID를 지정할 수 있습니다. 또한 리디렉션에서 제외할 복합 USB 디바이스 구성 요소의 인터페이스를 지정할 수 있습니다. Horizon 7는 이 방법으로 제외한 구성 요소에 대해 어떠한 필터 정책 설정도 적용하지 않습니다.

**중요** Split Vid/Pid Device 정책을 사용하는 경우 Horizon 7는 명시적으로 제외하지 않은 구성 요소를 자동으로 포함하지 않습니다. Include Vid/Pid Device와 같은 필터 정책을 지정하여 해당 구성 요소를 포함시켜야 합니다.

표 4-5. Horizon Agent의 디바이스 분할 정책 설정을 위한 분할 수정자에서는 Horizon Client에 동등한 디바이스 분할 정책 설정이 있는 경우 Horizon Client가 Horizon Agent 디바이스 분할 정책 설정을 어떻게 처리하는지 지정하는 수정자를 보여 줍니다. 이러한 수정자는 모든 디바이스 분할 정책에 적용됩니다.

표 4-5. Horizon Agent의 디바이스 분할 정책 설정을 위한 분할 수정자

수정자	설명
m(병합)	Horizon Client는 Horizon Client 디바이스 분할 정책 설정과 함께 Horizon Agent 디바이스 분할 정책 설정을 적용합니다.
o(제정의)	Horizon Client는 Horizon Client 디바이스 분할 정책 설정 대신 Horizon Agent 디바이스 분할 정책 설정을 사용합니다.

표 4-6. 디바이스 분할 정책 설정에 대한 분할 수정자 적용의 예에는 서로 다른 분할 수정자를 지정한 경우에 Horizon Client가 Exclude Device From Split by Vendor/Product ID에 대한 설정을 어떻게 처리하는지 보여 주는 예가 나와 있습니다.

표 4-6. 디바이스 분할 정책 설정에 대한 분할 수정자 적용의 예

Horizon Agent의 벤더/제품 ID별 분할에서 디바이스 제외	Horizon Client의 벤더/제품 ID별 분할에서 디바이스 제외	Horizon Client에서 사용하는 효율적 벤더/제품 ID별 분할에서 디바이스 제외 정책 설정
m:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX
m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY

Horizon Agent는 연결 측면에서 디바이스 분할 정책 설정을 적용하지 않습니다.

Horizon Client는 다음과 같은 우선 순위에 따라 디바이스 분할 정책 설정을 평가합니다.

- Exclude Vid/Pid Device From Split
- Split Vid/Pid Device

분할에서 디바이스를 제외하는 디바이스 분할 정책 설정은 디바이스를 분할하는 모든 정책 설정보다 우선합니다. 분할에서 제외할 인터페이스 또는 디바이스를 정의한 경우 Horizon Client는 일치하는 구성 요소 디바이스를 리디렉션 대상에서 제외합니다.

## 복합 USB 디바이스를 분할하는 정책 설정의 예

자동 분할 후 특정 벤더 및 제품 ID를 가진 디바이스를 제외하도록 데스크톱 분할 정책을 설정하고 이러한 정책을 클라이언트 컴퓨터에 전달합니다.

- Horizon Agent의 경우 Allow Auto Device Splitting 정책을 Allow - Override Client Setting로 설정합니다.
- Horizon Agent에 대해 Exclude VidPid From Split 정책을 o:vid-xxx\_pid-yyyy로 설정합니다. 여기서 xxx와 yyyy는 해당 ID입니다.

데스크톱의 자동 디바이스 분할을 허용하고 클라이언트 컴퓨터에서 특정 디바이스를 분할하기 위한 정책을 지정합니다.

- Horizon Agent의 경우 Allow Auto Device Splitting 정책을 Allow - Override Client Setting로 설정합니다.

- 클라이언트 디바이스에 대해 분할할 특정 디바이스를 포함하도록 Include Vid/Pid Device 필터 정책을 설정합니다(예: **vid-0781\_pid-554c**).
- 클라이언트 디바이스에 대해 인터페이스 00과 인터페이스 01이 리디렉션에서 제외되도록 지정된 복합 USB 디바이스를 분할하기 위해 Split Vid/Pid Device 정책을 **vid-0781\_pid-554c(exintf:00;exintf:01)**로 설정합니다.

## USB 디바이스를 위한 필터 정책 설정 구성

Horizon Agent와 Horizon Client에 대해 구성하는 필터 정책 설정에 따라 클라이언트 컴퓨터에서 원격 데스크톱 또는 애플리케이션으로 어떤 USB 디바이스를 리디렉션할 수 있는지가 결정됩니다. 일반적으로 USB 디바이스 필터링은 원격 데스크톱에서 대량의 스토리지 디바이스를 사용하지 못하게 하거나, 클라이언트 디바이스를 원격 데스크톱에 연결하는 USB와 이더넷 간 어댑터 같은 특정 유형의 디바이스를 전달하지 못하게 차단하기 위해 기업에서 주로 사용합니다.

데스크톱 또는 애플리케이션에 연결할 때 Horizon Client는 Horizon Agent USB 정책 설정을 다운로드한 후 Horizon Client USB 정책 설정과 함께 사용하여 클라이언트 컴퓨터에서 리디렉션할 수 있도록 허용할 USB 디바이스를 결정합니다.

Horizon 7는 모든 디바이스 분할 정책 설정을 적용한 후에 필터 정책 설정을 적용합니다. 복합 USB 디바이스를 분할한 경우 Horizon 7는 디바이스의 인터페이스 각각을 검사하여 필터 정책 설정에 따라 제외하거나 포함할 인터페이스를 결정합니다. 복합 USB 디바이스를 분할하지 않은 경우 Horizon 7는 전체 디바이스에 필터 정책 설정을 적용합니다.

디바이스 분할 정책은 Horizon Agent 구성 ADMX 템플릿 파일(vdm\_agent.admx)에 포함되어 있습니다.

## 에이전트가 강제로 적용하는 USB 설정의 상호 작용

다음 표에서는 Horizon Client에 동일한 필터 정책 설정이 존재할 경우 에이전트가 강제로 적용할 수 있는 설정에 대해 Horizon Client가 Horizon Agent 필터 정책 설정을 어떻게 처리하는지 지정하는 수정자를 보여 줍니다.

표 4-7. 에이전트가 강제로 적용할 수 있는 설정의 필터 수정자

수정자	설명
m(병합)	Horizon Client는 Horizon Client 필터 정책 설정과 함께 Horizon Agent 필터 정책 설정을 적용합니다. 부울이나 true/false 설정의 경우 클라이언트 정책이 설정되어 있지 않으면 에이전트 설정이 사용됩니다. 클라이언트 정책이 설정되어 있으면 Exclude All Devices 이외의 모든 에이전트 설정이 무시됩니다. Exclude All Devices 정책이 에이전트 측에 설정되어 있으면 이 정책이 클라이언트 설정보다 우선합니다.
o(재정의)	Horizon Client는 Horizon Client 필터 정책 설정 대신 Horizon Agent 필터 정책 설정을 사용합니다.

예를 들어, 다음의 에이전트 측 정책은 클라이언트 측의 모든 규칙을 재정의하며 VID-0911\_PID-149a 디바이스에만 포함 규칙이 적용됩니다.

```
IncludeVidPid: o:VID-0911_PID-149a
```

별표를 와일드카드 문자로 사용할 수도 있습니다(예: **o:vid-0911\_pid-\*\*\*\***).

**중요** **o** 또는 **m** 수정자 없이 에이전트 측을 구성하면 해당 구성 규칙은 잘못된 것으로 간주되어 무시됩니다.

## 클라이언트 해석 USB 설정의 상호 작용

다음 표에서는 Horizon Client가 클라이언트 해석 설정에 대해 Horizon Agent 필터 정책 설정을 어떻게 처리하는지 지정하는 수정자를 보여 줍니다.

표 4-8. 클라이언트 해석 설정의 필터 수정자

수정자	설명
Default (레지스트리 설정의 <b>d</b> )	Horizon Client 필터 정책 설정이 존재하지 않는 경우 Horizon Client는 Horizon Agent 필터 정책 설정을 사용합니다. Horizon Client 필터 정책 설정이 존재하는 경우 Horizon Client는 해당 정책 설정을 적용하고 Horizon Agent 필터 정책 설정은 무시합니다.
Override (레지스트리 설정의 <b>o</b> )	Horizon Client는 동등한 Horizon Client 필터 정책 설정 대신 Horizon Agent 필터 정책 설정을 사용합니다.

Horizon Agent는 연결 측면에서 클라이언트 해석 설정에 대한 필터 정책 설정을 적용하지 않습니다.

다음 표에서는 서로 다른 필터 수정자를 지정한 경우에 Horizon Client가 Allow Smart Cards의 설정을 처리하는 방법의 예를 보여 줍니다.

표 4-9. 클라이언트 해석 설정에 대한 필터 수정자 적용의 예

Horizon Agent의 스마트 카드 허용 설정	Horizon Client의 스마트 카드 허용 설정	Horizon Client에서 사용하는 유효한 스마트 카드 허용 정책 설정
Disable - Default Client Setting (레지스트리 설정의 <b>d:false</b> )	<b>true</b> (허용)	<b>true</b> (허용)
Disable - Override Client Setting (레지스트리 설정의 <b>o:false</b> )	<b>true</b> (허용)	<b>false</b> (사용 안 함)

Disable Remote Configuration Download 정책을 **true**로 설정하면 Horizon Client는 Horizon Agent에서 수신하는 모든 필터 정책 설정을 무시합니다.

다른 필터 정책 설정을 사용하도록 Horizon Client를 구성하거나 Horizon Agent에서 필터 정책 설정을 다운로드하지 못하게 Horizon Client를 사용하지 않도록 설정하더라도 Horizon Agent는 연결 측면에서 에이전트가 강제로 적용할 수 있는 설정의 필터 정책 설정을 항상 적용합니다. Horizon Client는 Horizon Agent가 디바이스 전달을 차단하고 있다는 것을 보고하지 않습니다.

## 설정 우선 순위

Horizon Client는 우선 순위에 따라 필터 정책 설정을 평가합니다. 리디렉션되지 않도록 일치하는 디바이스를 제외하는 필터 정책 설정은 디바이스를 포함하는 동일한 필터 정책 설정보다 우선합니다.

Horizon Client에 디바이스를 제외하는 필터 정책 설정이 없는 경우 Horizon Client 정책을 Exclude All Devices로 **설정하지 않는 한** 는 디바이스 리디렉션을 허용합니다. 그러나 Horizon Agent에 디바이스를 제외하는 필터 정책 설정을 구성한 경우 데스크톱 또는 애플리케이션은 디바이스를 리디렉션하려는 모든 시도를 차단합니다.

Horizon Client는 Horizon Agent 설정에 적용하는 수정자 값과 함께 Horizon Client 설정과 Horizon Agent 설정을 고려하여 우선 순위에 따라 필터 정책 설정을 평가합니다. 다음은 설정 우선 순위 목록이며, 여기서 항목 1이 우선 순위가 가장 높습니다.

- 1 Exclude Path
- 2 Include Path
- 3 Exclude Vid/Pid Device
- 4 Include Vid/Pid Device
- 5 Exclude Device Family
- 6 Include Device Family
- 7 Allow Audio Input Devices, Allow Audio Output Devices, Allow HIDBootable, Allow HID (Non Bootable and Not Mouse Keyboard), Allow Keyboard and Mouse Devices, Allow Smart Cards 및 Allow Video Devices
- 8 모든 USB 디바이스를 제외 또는 포함하도록 평가되는 결합된 효율적인 Exclude All Devices 정책

Exclude Path 및 Include Path 필터 정책 설정은 Horizon Client에만 설정할 수 있습니다. 개별 디바이스 제품군을 참조하는 Allow 필터 정책 설정은 우선 순위가 동일합니다.

벤더 및 제품 ID 값에 기반하여 디바이스를 제외하는 정책 설정을 구성할 경우, 디바이스가 속한 제품군에 Horizon Client 정책 설정을 구성하더라도 Allow는 벤더 및 제품 ID 값이 이 정책 설정과 일치하는 디바이스를 제외합니다.

정책 설정의 순서는 정책 설정 간 충돌을 해결합니다. 스마트 카드의 리디렉션을 허용하는 Allow Smart Cards를 구성할 경우, 더 높은 우선 순위의 제외 정책 설정이 있으면 이 설정이 무시됩니다. 예를 들어, 경로 또는 벤더 및 제품 ID 값이 일치하는 스마트 카드 디바이스를 제외하는 Exclude Vid/Pid Device 정책 설정이 구성되어 있거나 Exclude Device Family 디바이스 제품군까지 완전히 제외하는 smart-card 정책 설정이 구성되어 있을 수 있습니다.

Horizon Agent 필터 정책 설정을 구성한 경우 Horizon Agent는 원격 데스크톱 또는 애플리케이션에서 다음과 같은 우선 순위에 따라 필터 정책 설정을 평가하고 강제로 적용합니다. 이 목록에서 항목 1의 우선 순위가 가장 높습니다.

- 1 Exclude Vid/Pid Device
- 2 Include Vid/Pid Device
- 3 Exclude Device Family

#### 4 Include Device Family

#### 5 모든 USB 디바이스를 제외 또는 포함하도록 설정된, 에이전트가 강제로 적용할 수 있는 Exclude All Devices 정책

Horizon Agent는 연결 측면에서 이 제한된 필터 정책 설정 집합을 강제로 적용합니다.

Horizon Agent의 필터 정책 설정을 정의하여 관리되지 않는 클라이언트 컴퓨터를 위한 필터링 정책을 생성할 수 있습니다. 또한 이 기능을 사용하면 Horizon Client의 필터 정책 설정이 리디렉션을 허용하더라도 클라이언트 컴퓨터에서 전달되지 않도록 디바이스를 차단할 수 있습니다.

예를 들어, Horizon Client에 디바이스를 리디렉션할 수 있는 정책을 구성한 경우 Horizon Agent에 디바이스를 제외하는 정책을 구성하면 Horizon Agent가 해당 디바이스를 차단합니다.

### USB 디바이스를 필터링하는 정책 설정의 예

이 예에 사용된 벤더 ID와 제품 ID는 예제일 뿐입니다. 특정 디바이스의 벤더 ID와 제품 ID를 확인하는 방법에 대한 자세한 내용은 [로그 파일을 사용하여 문제 해결 및 USB 디바이스 ID 확인](#) 항목을 참조하십시오.

- 클라이언트에서 특정 디바이스가 리디렉션되지 않도록 제외:

```
Exclude Vid/Pid Device: Vid-0341_Pid-1a11
```

- 모든 스토리지 디바이스가 이 데스크톱 또는 애플리케이션 풀로 리디렉션되지 않도록 차단. 에이전트 측 설정 사용:

```
Exclude Device Family: o:storage
```

- 데스크톱 풀의 모든 사용자에게 오디오 및 비디오 디바이스를 차단하여 이러한 디바이스를 실시간 오디오-비디오 기능에 대해 항상 사용할 수 있도록 합니다. 에이전트 측 설정 사용::

```
Exclude Device Family: o:video;audio
```

벤더 및 제품 ID별로 특정 디바이스를 제외하는 방법도 사용할 수 있습니다.

- 클라이언트에서 특정 디바이스 하나만 제외하고 모든 디바이스가 리디렉션되지 않도록 차단:

```
Exclude All Devices: true
Include Vid/Pid Device: Vid-0123_Pid-abcd
```

- 최종 사용자에게 문제가 될 수 있는 특정 업체의 모든 디바이스 제외. 에이전트 측 설정 사용:

```
Exclude Vid/Pid Device: o:Vid-0341_Pid-*
```

- 클라이언트에서 특정 디바이스 두 개만 포함하고 다른 모든 디바이스 제외:

```
Exclude All Devices: true
Include Vid/Pid Device: Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
```

## USB 디바이스 제품군

Horizon Client 또는 View Agent 또는 Horizon Agent의 USB 필터링 규칙을 만들 때 제품군을 지정할 수 있습니다.

**참고** 일부 디바이스는 디바이스 제품군을 보고하지 않습니다.

표 4-10. USB 디바이스 제품군

디바이스 제품군 이름	설명
audio	임의의 오디오 입력 또는 오디오 출력 디바이스.
audio-in	마이크와 같은 오디오 입력 디바이스.
audio-out	확성기 및 헤드폰과 같은 오디오 출력 디바이스.
bluetooth	Bluetooth 연결 디바이스.
comm	모뎀 및 유선 네트워크 어댑터와 같은 통신 디바이스.
hid	키보드 및 포인팅 디바이스를 제외한 휴먼 인터페이스 디바이스.
hid-bootable	키보드 및 포인팅 디바이스를 제외한, 부팅 중에 사용할 수 있는 휴먼 인터페이스 디바이스.
imaging	스캐너와 같은 이미징 디바이스.
keyboard	키보드 디바이스.
mouse	마우스와 같은 포인팅 디바이스.
other	지정된 제품군이 없습니다.
pda	개인용 디지털 디바이스.
physical	물리적 피드백 조이스틱과 같은 물리적 피드백을 이용하는 디바이스.
printer	인쇄 디바이스.
security	지문 판독기와 같은 보안 디바이스.
smart-card	스마트 카드 디바이스.
storage	플래시 드라이브 및 외부 하드 디스크 드라이브와 같은 대용량 스토리지 디바이스.
unknown	알려진 제품군이 없습니다.
vendor	벤더 특정 기능을 가진 디바이스.
video	비디오 입력 디바이스.
wireless	무선 네트워크 어댑터.
wusb	무선 USB 디바이스.

## Horizon Agent 구성 ADMX 템플릿에서의 USB 설정

USB 정책 설정은 Horizon Agent와 Horizon Client 모두에 대해 정의할 수 있습니다. 연결 시 Horizon Client는 Horizon Agent에서 USB 정책 설정을 다운로드한 후 Horizon Client USB 정책 설정과 함께 사용하여 클라이언트 컴퓨터에서 리디렉션할 수 있는 디바이스를 결정합니다.

Horizon Agent 구성 ADMX 템플릿 파일에는 USB 리디렉션을 포함하여 Horizon Agent의 인증 및 환경 구성 요소와 관련된 정책 설정이 포함됩니다. ADMX 템플릿 파일의 이름은 `vdm_agent.admx`입니다. 이 설정은 컴퓨터 수준에서 적용됩니다. Horizon Agent는 컴퓨터 수준의 GPO에서 설정을 우선적으로 읽고, 그 이외에는 `HKLM\Software\Policies\VMware, Inc.\VMware VDMWAgent\USB`의 레지스트리에서 읽습니다.

## USB 디바이스 분할 구성 설정

다음 표에는 Horizon Agent 구성 ADMX 템플릿 파일의 복합 USB 디바이스 분할을 위한 각 정책 설정이 설명되어 있습니다. 이러한 모든 설정은 그룹 정책 관리 편집기의 **VMware Horizon Agent 구성 > USB 구성 보기 > 클라이언트 다운로드 가능한 설정만** 폴더에 있습니다. Horizon Agent에서는 이러한 설정을 강제로 적용하지 않습니다. Horizon Agent는 병합(m) 또는 재정의(o) 수정자를 지정했는지에 따라 해석 및 강제 적용을 위해 설정을 Horizon Client에 전달합니다. Horizon Client는 이 설정을 사용하여 복합 USB 디바이스를 해당 구성 요소 디바이스로 분할할지 여부와 구성 요소 디바이스를 리디렉션에 사용하지 못하도록 제외할지 여부를 결정합니다. Horizon에서 복합 USB 디바이스 분할을 위해 정책을 적용하는 방식에 대한 설명은 [복합 USB 디바이스를 위한 디바이스 분할 정책 설정 구성](#)에 나와 있습니다.

표 4-11. Horizon Agent 구성 템플릿: 디바이스 분할 설정

설정	속성
Allow Auto Device Splitting 속성: AllowAutoDeviceSplitting	복합 USB 디바이스의 자동 분할을 허용합니다. 기본값은 정의되어 있지 않으며 <b>false</b> 와 같습니다.
Exclude Vid/Pid Device from Split 속성: SplitExcludeVidPid	공급업체 및 제품 ID별로 지정된 복합 USB 디바이스를 분할에서 제외합니다. 설정 형식은 <code>{m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</code> 입니다. ID 번호를 16진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다. 예: <b>o:vid-0781_pid-55**</b> 기본 값은 정의되어 있지 않습니다.
Split Vid/Pid Device 속성: SplitVidPid	공급업체 및 제품 ID별로 지정된 복합 USB 디바이스의 구성 요소를 개별 디바이스로 처리합니다. 설정 형식은 다음과 같습니다. <code>{m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])</code> 또는 <code>{m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])</code> <code>exintf</code> 키워드를 사용하면 인터페이스 번호를 지정하여 구성 요소를 리디렉션에서 제외할 수 있습니다. ID 번호는 16진수로, 인터페이스 번호는 앞에 0이 표시되는 10진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다. 예: <b>o:vid-0781_pid-554c(exintf:01;exintf:02)</b> <b>참고</b> Horizon 7는 명시적으로 제외하지 않은 구성 요소를 자동으로 포함시키지 않습니다. Include Vid/Pid Device과 같은 필터 정책을 지정하여 해당 구성 요소를 포함시켜야 합니다. 기본 값은 정의되어 있지 않습니다.



## Horizon Agent가 강제로 적용하는 USB 설정

다음 표에는 Horizon Agent 구성 ADMX 템플릿 파일에서 각 에이전트가 강제로 적용하는 USB 정책 설정이 설명되어 있습니다. 이러한 모든 설정은 그룹 정책 관리 편집기의 **VMware Horizon Agent 구성 > USB 구성 보기** 폴더에 있습니다. Horizon Agent는 설정을 사용하여 USB 디바이스가 호스트 시스템으로 전달될 수 있는지 여부를 결정합니다. 또한 Horizon Agent는 병합(m) 또는 재정의(o) 수정자를 지정했는지에 따라 해석 및 강제 적용을 위해 설정을 Horizon Client에 전달합니다. Horizon Client는 이 설정을 사용하여 USB 디바이스를 리더렉션에 사용할 수 있는지 여부를 결정합니다. Horizon Agent는 사용자가 지정하고 에이전트가 강제로 적용하는 정책 설정을 항상 시행하기 때문에 그로 인해 Horizon Client에 설정한 정책이 무효화될 수 있습니다. Horizon 7에서 USB 디바이스 필터링에 대한 정책을 적용하는 방식에 대한 설명은 [USB 디바이스를 위한 필터 정책 설정 구성](#)에 나와 있습니다.

표 4-12. Horizon Agent 구성 템플릿: 에이전트가 강제로 적용하는 설정

설정	속성
Exclude All Devices 속성: ExcludeAllDevices	<p>모든 USB 디바이스가 전달되지 않도록 제외합니다. <b>true</b>로 설정되면 기타 정책 설정을 사용하여 특정 디바이스 또는 디바이스 제품군을 전달할 수 있습니다. <b>false</b>로 설정되면 기타 정책 설정을 사용하여 특정 디바이스 또는 디바이스 제품군이 전달되지 않도록 방지할 수 있습니다.</p> <p><b>true</b>로 설정하고 Horizon Client에 전달할 경우, 이 설정은 항상 Horizon Client의 설정을 재정의합니다. 이 설정에 병합(m) 또는 재정의(o) 수정자를 사용할 수 없습니다.</p> <p>기본값은 정의되어 있지 않으며 <b>false</b>와 같습니다.</p>
Exclude Device Family 속성: ExcludeFamily	<p>디바이스 제품군이 전달되지 않도록 제외합니다. 설정 형식은 {m o}:family_name_1[:family_name_2]...입니다.</p> <p>예: <b>o:bluetooth;smart-card</b></p> <p>자동 디바이스 분할을 사용하도록 지정한 경우, Horizon 7는 복합 USB 디바이스의 각 인터페이스의 디바이스 제품군을 검사하여 제외할 인터페이스를 결정합니다. 자동 디바이스 분할을 사용하지 않도록 설정한 경우, Horizon 7는 전체 복합 USB 디바이스의 디바이스 제품군을 검토합니다.</p> <p>기본 값은 정의되어 있지 않습니다.</p>
Exclude Vid/Pid Device 속성: ExcludeVidPid	<p>지정된 벤더 및 제품 ID가 있는 디바이스가 전달되지 않도록 제외합니다. 설정 형식은 {m o}:vid-xxx1_pid-yyy2[:vid-xxx2_pid-yyy2]...입니다.</p> <p>ID 번호를 16진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다.</p> <p>예: <b>m:vid-0781_pid-****;vid-0561_pid-554c</b></p> <p>기본 값은 정의되어 있지 않습니다.</p>
Include Device Family 속성: IncludeFamily	<p>전달될 수 있는 디바이스 제품군을 포함합니다. 설정 형식은 {m o}:family_name_1[:family_name_2]...입니다.</p> <p>예: <b>m:storage</b></p> <p>기본 값은 정의되어 있지 않습니다.</p>
Include Vid/Pid Device 속성: IncludeVidPid	<p>지정된 벤더 및 제품 ID가 있는 디바이스가 전달되도록 포함합니다. 설정 형식은 {m o}:vid-xxx1_pid-yyy2[:vid-xxx2_pid-yyy2]...입니다.</p> <p>ID 번호를 16진수로 지정해야 합니다. 와일드카드 문자(*)를 ID의 개별 자릿수 대신 사용할 수 있습니다.</p> <p>예: <b>o:vid-0561_pid-554c</b></p> <p>기본 값은 정의되어 있지 않습니다.</p>

## 클라이언트 해석 USB 설정

다음 표에는 Horizon Agent 구성 ADMX 템플릿 파일의 각 클라이언트 해석 정책 설정이 설명되어 있습니다. 이러한 모든 설정은 그룹 정책 관리 편집기의 **VMware Horizon Agent 구성 > USB 구성 보기 > 클라이언트 다운로드 가능한 설정만** 폴더에 있습니다. Horizon Agent에서는 이러한 설정을 강제로 적용하지 않습니다. Horizon Agent는 해석 및 강제 적용을 위해 설정을 Horizon Client에 전달합니다. Horizon Client는 이 설정을 사용하여 USB 디바이스를 리디렉션에 사용할 수 있는지 여부를 결정합니다.

표 4-13. Horizon Agent 구성 템플릿: 클라이언트 해석 설정

설정	속성
Allow Audio Input Devices 속성: AllowAudioIn	오디오 입력 디바이스가 전달되도록 허용합니다. 기본값은 정의되어 있지 않으며 <b>true</b> 와 같습니다.
Allow Audio Output Devices 속성: AllowAudioOut	오디오 출력 디바이스가 전달되도록 허용합니다. 기본값은 정의되어 있지 않으며 <b>false</b> 와 같습니다.
Allow HID-Bootable 속성: AllowHIDBootable	부팅 시 사용할 수 있는 키보드 또는 마우스(HID 부팅 가능 디바이스라고도 부름) 이외의 입력 디바이스가 전달되도록 허용합니다. 기본값은 정의되어 있지 않으며 <b>true</b> 와 같습니다.
Allow Other Input Devices	HID 부팅 가능 디바이스 또는 통합된 포인팅 디바이스가 있는 키보드 이외의 입력 디바이스가 전달되도록 허용합니다. 기본 값은 정의되어 있지 않습니다.
Allow Keyboard and Mouse Devices 속성: AllowKeyboardMouse	통합된 포인팅 디바이스(마우스, 트랙볼 또는 터치 패드)가 있는 키보드가 전달되도록 허용합니다. 기본값은 정의되어 있지 않으며 <b>false</b> 와 같습니다.
Allow Smart Cards 속성: AllowSmartcard	스마트 카드 디바이스가 전달되도록 허용합니다. 기본값은 정의되어 있지 않으며 <b>false</b> 와 같습니다.
Allow Video Devices 속성: AllowVideo	비디오 디바이스가 전달되도록 허용합니다. 기본값은 정의되어 있지 않으며 <b>true</b> 와 같습니다.

## USB 리디렉션 문제 해결

Horizon Client의 USB 리디렉션에 다양한 문제가 발생할 수 있습니다.

### 문제

Horizon Client의 USB 리디렉션이 원격 데스크톱에서 로컬 디바이스를 사용할 수 있도록 만드는 데 실패하거나 Horizon Client의 리디렉션에 사용할 수 있는 디바이스가 나타나지 않습니다.

### 원인

다음은 USB 리디렉션이 올바르게 또는 예상대로 작동하는 데 실패하게 되는 원인입니다.

- 디바이스가 복합 USB 디바이스이고 포함된 디바이스 중 하나가 기본적으로 차단되어 있습니다. 예를 들어, 마우스 디바이스가 기본적으로 차단되어 있으므로 마우스가 포함된 받아쓰기 디바이스도 기본적으로 차단되어 있습니다. 이 문제를 해결하려면 "Horizon 7에서 원격 데스크톱 기능 구성" 문서에서 "복합 USB 디바이스에 대한 디바이스 분할 정책 설정 구성"을 참조하십시오.

- USB 리디렉션은 원격 데스크톱 및 애플리케이션을 배포하는 Windows Server 2008 RDS 호스트에서 지원되지 않습니다. USB 리디렉션은 View Agent 6.1 이상이 설치된 Windows Server 2012 RDS 호스트에서 USB 스토리지 디바이스에 대해서만 지원됩니다. USB 리디렉션은 단일 사용자 데스크톱으로 사용되는 Windows Server 2008 R2 및 Windows Server 2012 R2 시스템에서 지원됩니다.
- RDS 데스크톱 및 애플리케이션에서는 USB 플래시 드라이브와 하드 디스크만 지원됩니다. 다른 유형의 USB 디바이스와 보안 스토리지 드라이브, USB CD-ROM 등의 다른 유형의 USB 스토리지 디바이스를 RDS 데스크톱 또는 애플리케이션으로 리디렉션할 수 없습니다.
- 리디렉션에는 웹캠이 지원되지 않습니다.
- USB 오디오 디바이스의 리디렉션 가능 여부는 네트워크의 상태에 따라 달라질 수 있으며 안정적이지 않습니다. 일부 디바이스의 경우, 유휴 상태에서도 높은 데이터 처리량을 요구합니다.
- USB 리디렉션은 부트 디바이스에 지원되지 않습니다. USB 디바이스에서 부팅되는 Windows 시스템에서 Horizon Client를 실행하고 이 디바이스를 원격 데스크톱으로 리디렉션할 경우 로컬 운영 체제는 응답하지 않거나 사용할 수 없습니다. <http://kb.vmware.com/kb/1021409> 항목을 참조하십시오.
- 기본적으로 Windows용 Horizon Client에서는 리디렉션을 위해 키보드, 마우스, 스마트 카드 및 오디오 출력 디바이스를 선택할 수 없습니다. <http://kb.vmware.com/kb/1011600> 항목을 참조하십시오.
- RDP는 콘솔 세션의 USB HID 또는 스마트 카드 판독기의 리디렉션을 지원하지 않습니다. <http://kb.vmware.com/kb/1011600> 항목을 참조하십시오.
- Windows Mobile Device Center는 RDP 세션의 USB 디바이스 리디렉션을 방지할 수 있습니다. <http://kb.vmware.com/kb/1019205> 항목을 참조하십시오.
- 일부 USB HID의 경우 마우스 포인터 위치를 업데이트하도록 가상 시스템을 구성해야 합니다. <http://kb.vmware.com/kb/1022076> 항목을 참조하십시오.
- 일부 오디오 디바이스는 정책 설정 또는 레지스트리 설정으로 변경해야 할 수 있습니다. <http://kb.vmware.com/kb/1023868> 항목을 참조하십시오.
- 네트워크 지연으로 인해 디바이스 상호 작용이 느려지거나 로컬 디바이스와 상호 작용하도록 설계되었기 때문에 애플리케이션이 중지된 것처럼 보일 수 있습니다. USB 디스크 드라이브가 많이 크면 Windows Explorer에 나타나는 데 몇 분 정도 걸릴 수 있습니다.
- FAT32 파일 시스템 형식 USB 플래시 카드가 저속 로드됩니다. <http://kb.vmware.com/kb/1022836> 항목을 참조하십시오.
- 로컬 시스템의 프로세스 또는 서비스는 원격 데스크톱 또는 애플리케이션에 연결되기 전에 디바이스를 열었습니다.
- 리디렉션된 USB 디바이스는 데스크톱 또는 애플리케이션에 디바이스를 사용할 수 있다고 표시되어도 데스크톱 또는 애플리케이션 세션을 다시 연결할 경우 작동을 중지합니다.
- USB 리디렉션이 Horizon Administrator에서 사용되지 않도록 설정되었습니다.
- 게스트에서 USB 리디렉션 드라이버가 누락되거나 사용되지 않도록 설정되었습니다.

## 해결책

- ◆ 사용 가능한 경우, 프로토콜로 RDP 대신 PCoIP를 사용하십시오.
- ◆ 임시로 연결을 끊은 후 리디렉션된 디바이스가 사용할 수 없게 되거나 작동을 중지한 경우 디바이스를 제거했다가 다시 연결하여 리디렉션을 다시 시도하십시오.
- ◆ Horizon Administrator에서 **정책 > 전역 정책**으로 이동하고 View 정책에서 USB 액세스가 **허용**으로 설정되었는지 확인합니다.
- ◆ 게스트 측 로그의 ws\_vhub 클래스 항목 및 클라이언트 측 로그의 vmware-view-usbd 클래스 항목을 관찰합니다.

사용자가 관리자가 아닌 경우 또는 USB 리디렉션 드라이버가 설치되지 않았거나 작동하지 않는 경우, 이러한 클래스를 가진 항목은 로그에 작성됩니다. 이러한 로그 파일의 위치에 대해서는 "Horizon 7에서 원격 데스크톱 기능 구성" 문서에서 "로그 파일을 사용하여 문제 해결 및 USB 디바이스 ID 확인"을 참조하십시오.

- ◆ 게스트에서 디바이스 관리자를 열고 범용 직렬 버스 컨트롤러를 확장한 다음 해당 드라이버가 누락된 경우 VMware View 가상 USB 호스트 컨트롤러 및 VMware View 가상 USB 허브 드라이버를 다시 설치하거나, 사용하지 않도록 설정된 경우 다시 사용하도록 설정합니다.

# 데스크톱 풀 및 애플리케이션 풀의 정책 구성

## 5

정책을 구성하여 데스크톱 풀과 애플리케이션 풀, 시스템 및 사용자의 동작을 제어할 수 있습니다. 클라이언트 세션의 정책은 Horizon Administrator를 사용하여 설정합니다. Active Directory 그룹 정책 설정을 사용하면 Horizon Agent 및 Windows용 Horizon Client의 동작을 제어하고 단일 사용자 시스템, RDS 호스트, PCoIP 또는 VMware Blast에 영향을 주는 기능을 제어할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- Horizon Administrator에서 정책 설정
- 스마트 정책 사용
- Active Directory 그룹 정책 사용
- Horizon 7 그룹 정책 관리 템플릿 파일 사용
- Horizon 7 ADMX 템플릿 파일
- Active Directory에 ADMX 템플릿 파일 추가
- Horizon Agent 구성 ADMX 템플릿 설정
- PCoIP 정책 설정
- VMware Blast 정책 설정
- 원격 데스크톱 서비스 그룹 정책 사용
- 위치 기반 인쇄 설정
- Active Directory 그룹 정책 예제

## Horizon Administrator에서 정책 설정

클라이언트 세션의 정책은 Horizon Administrator를 사용하여 구성합니다.

이러한 정책을 설정하여 특정 사용자, 특정 데스크톱 풀 또는 모든 클라이언트 세션 사용자에게 영향을 줄 수 있습니다. 특정 사용자 및 데스크톱 풀에 영향을 주는 정책을 사용자 수준 정책 및 데스크톱 풀 수준 정책이라고 합니다. 모든 세션 및 사용자에게 영향을 주는 정책은 전역 정책이라고 합니다.

사용자 수준 정책은 동등한 데스크톱 풀 수준 정책 설정에서 설정을 상속합니다. 마찬가지로 데스크톱 풀 수준 정책은 동등한 전역 정책 설정에서 설정을 상속합니다. 데스크톱 풀 수준 정책 설정은 동등한 전역 정책 설정보다 우선합니다. 사용자 수준 정책 설정은 동등한 전역 및 데스크톱 풀 수준 정책 설정보다 우선합니다.

낮은 수준의 정책 설정은 동일한 높은 수준의 설정보다 더 또는 덜 제한적일 수 있습니다. 예를 들어, 전역 정책을 **거부**로 설정하고 동등한 데스크톱 풀 수준 정책을 **허용**으로 설정할 수 있으며, 그 반대도 가능합니다.

---

**참고** RDS 데스크톱 및 애플리케이션 풀에 대해 전역 정책만 사용할 수 있습니다. RDS 데스크톱 및 애플리케이션 풀에 대해 사용자 수준 정책이나 풀 수준 정책을 설정할 수 없습니다.

---

## 전역 정책 설정 구성

전역 정책을 구성해 모든 클라이언트 세션 사용자의 동작을 제어할 수 있습니다.

### 사전 요구 사항

정책 설명을 숙지하십시오. [Horizon 7 정책](#)를 참조하십시오.

### 절차

- 1 Horizon Administrator에서 **정책 > 전역 정책**을 선택합니다.
- 2 **View 정책** 창에서 **정책 편집**을 클릭합니다.
- 3 변경 사항을 저장하려면 **확인**을 클릭합니다.

## 데스크톱 풀 정책 구성

특정 데스크톱 풀에 적용할 데스크톱 수준 정책을 구성할 수 있습니다. 데스크톱 수준 정책 설정은 동등한 전역 정책 설정보다 우선합니다.

### 사전 요구 사항

정책 설명을 숙지하십시오. [Horizon 7 정책](#)를 참조하십시오.

### 절차

- 1 Horizon Administrator에서 **카탈로그 > 데스크톱 풀**을 선택합니다.
- 2 데스크톱 풀 ID를 두 번 클릭하고 **정책** 탭을 클릭합니다.  
**정책** 탭은 현재 정책 설정을 표시합니다. 동등한 전역 설정에서 설정을 상속한 경우에는 **데스크톱 풀 정책** 옆에 **상속**이 표시됩니다.
- 3 **View 정책** 창에서 **정책 편집**을 클릭합니다.
- 4 변경 사항을 저장하려면 **확인**을 클릭합니다.

## 사용자를 위한 정책 구성

특정 사용자에게 적용할 사용자 수준 정책을 구성할 수 있습니다. 사용자 수준 정책 설정은 동등한 전역과 데스크톱 풀 수준 정책 설정보다 항상 우선합니다.

### 사전 요구 사항

정책 설명을 숙지하십시오. [Horizon 7 정책](#)를 참조하십시오.

### 절차

- 1 Horizon Administrator에서 **카탈로그 > 데스크톱 풀**을 선택합니다.
- 2 데스크톱 풀 ID를 두 번 클릭하고 **정책** 탭을 클릭합니다.  
**정책** 탭은 현재 정책 설정을 표시합니다. 동등한 전역 설정에서 설정을 상속한 경우에는 **데스크톱 풀 정책** 열에 **상속**이 표시됩니다.
- 3 **사용자 재정의**를 클릭한 다음 **사용자 추가**를 클릭합니다.
- 4 사용자를 찾으려면 **추가**를 클릭하고 사용자 이름 또는 설명을 입력한 다음 **찾기**를 클릭합니다.
- 5 목록에서 사용자를 한 명 이상 선택하고 **확인**을 클릭한 후 **다음**을 클릭합니다.  
개별 정책 추가 대화 상자가 나타납니다.
- 6 Horizon 정책을 구성하고 **마침**을 클릭하여 변경 내용을 저장합니다.

## Horizon 7 정책

모든 클라이언트 세션에 영향을 주는 Horizon 7 정책을 구성하거나 특정 데스크톱 풀 또는 사용자에게 영향을 주도록 정책을 적용할 수 있습니다.

[표 5-1. Horizon 정책](#)에서는 각 Horizon 7 정책 설정에 대해 설명합니다.

표 5-1. Horizon 정책

정책	설명
MMR(멀티미디어 리디렉션)	<p>클라이언트 시스템을 위해 MMR이 사용되도록 설정되어 있는지 확인합니다.</p> <p>MMR은 TCP 소켓을 통해 직접 원격 데스크톱의 특정 코덱에서 멀티미디어 데이터를 클라이언트 시스템에 전달하는 Windows Media Foundation 필터입니다. 그런 다음 데이터는 재생되는 클라이언트 시스템에서 바로 디코딩됩니다.</p> <p>기본값은 <b>거부</b>입니다.</p> <p>클라이언트 시스템에 로컬 멀티미디어 디코딩을 처리하는 리소스가 충분하지 않은 경우 <b>거부</b> 설정을 그대로 둡니다.</p> <p>멀티미디어 리디렉션(MMR) 데이터는 애플리케이션 기준 암호화 없이 네트워크를 통해 전송되며 리디렉션되는 콘텐츠에 따라 중요한 데이터가 포함될 수 있습니다. 이 데이터가 네트워크에서 모니터링되는 것을 방지하려면 보안 네트워크 상에서만 MMR을 사용하십시오.</p>
USB 액세스	<p>원격 데스크톱에서 클라이언트 시스템에 연결된 USB 디바이스를 사용할 수 있는지 여부를 결정합니다.</p> <p>기본값은 <b>허용</b>입니다. 보안상의 이유를 위해 외부 디바이스의 사용을 막으려면 설정을 <b>거부</b>로 변경하십시오.</p>
PCoIP 하드웨어 가속	<p>PCoIP 디스플레이 프로토콜의 하드웨어 가속을 사용하도록 설정할지 여부를 확인하고 PCoIP 사용자 세션에 할당된 가속 우선 순위를 지정합니다.</p> <p>이 설정은 PCoIP 하드웨어 가속 디바이스가 원격 데스크톱을 호스팅하는 물리적 컴퓨터에 있는 경우에만 적용됩니다.</p> <p>기본값은 <b>중간</b> 우선 순위에서 <b>허용</b>입니다.</p>

## 스마트 정책 사용

스마트 정책을 사용하여 특정 원격 데스크톱의 USB 리디렉션, 가상 인쇄, 클립보드 리디렉션, 클라이언트 드라이브 리디렉션, PCoIP 디스플레이 프로토콜 기능의 동작을 제어하는 정책을 만들 수 있습니다. 스마트 정책을 사용하여 게시된 애플리케이션의 동작을 제어하는 정책을 생성할 수도 있습니다.

스마트 정책을 사용하면 특정 조건이 충족된 경우에만 적용되는 정책을 만들 수 있습니다. 예를 들어, 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결한 경우 클라이언트 드라이브 리디렉션 기능을 사용하지 않도록 설정하는 정책을 구성할 수 있습니다.

## 스마트 정책 요구 사항

스마트 정책을 사용하려면 Horizon 7 환경이 특정한 요구 사항을 충족해야 합니다.

- 스마트 정책으로 관리할 원격 데스크톱에 Horizon Agent 7.0 이상 및 VMware User Environment Manager 9.0 이상을 설치해야 합니다.
- 사용자는 Horizon Client 4.0 이상을 사용하여 스마트 정책으로 관리하는 원격 데스크톱에 연결해야 합니다.

## User Environment Manager 설치

스마트 정책을 사용하여 원격 데스크톱에서 원격 데스크톱 기능의 동작을 제어하려면 원격 데스크톱에 User Environment Manager 9.0 이상을 설치해야 합니다.



VMware 다운로드 페이지에서 User Environment Manager 설치 관리자를 다운로드할 수 있습니다. User Environment Manager로 관리할 각 원격 데스크톱에 VMware UEM FlexEngine 클라이언트 구성 요소를 설치해야 합니다. User Environment Manager 환경을 관리할 데스크톱에 임의의 User Environment Manager 관리 콘솔 구성 요소를 설치할 수 있습니다.

연결된 클론 풀의 경우 연결된 클론의 기본 이미지로 사용하는 상위 가상 시스템에 User Environment Manager를 설치합니다. RDS 데스크톱 풀의 경우 RDS 데스크톱 세션을 제공하는 RDS 호스트에 User Environment Manager를 설치합니다.

User Environment Manager 시스템 요구 사항과 전체 설치 지침은 "User Environment Manager 관리자 가이드" 문서를 참조하십시오.

## User Environment Manager 구성

원격 데스크톱 기능에 대해 스마트 정책을 만들려면 먼저 User Environment Manager를 구성해야 합니다.

User Environment Manager를 구성하려면 "User Environment Manager 관리자 가이드"에 있는 구성 지침을 따릅니다. 다음 구성 단계는 그 문서에 설명된 정보를 보완합니다.

- 원격 데스크톱에 VMware UEM FlexEngine 클라이언트 구성 요소를 구성할 때 FlexEngine 로그인 및 로그오프 스크립트를 만듭니다. 로그인 스크립트에 **-HorizonViewMultiSession -r** 매개 변수를 사용하고 로그오프 스크립트에 **-HorizonViewMultiSession -s** 매개 변수를 사용합니다.

---

**참고** 로그인 스크립트로 원격 데스크톱에서 다른 애플리케이션을 시작하지 마십시오. 추가 로그인 스크립트는 원격 데스크톱 로그인을 최대 10분까지 지연시킬 수 있습니다.

---

- 원격 데스크톱에서 동기적으로 로그인 스크립트 실행을 설정하여 사용자 그룹 정책을 사용하도록 설정합니다. 이 설정은 사용자 구성\정책\관리 템플릿\시스템\스크립트 폴더에 있습니다.
- 원격 데스크톱에서 컴퓨터 시동 및 로그인 시 항상 네트워크 대기 컴퓨터 그룹 정책 설정을 사용하도록 설정합니다. 이 설정은 컴퓨터 구성\관리 템플릿\시스템\로그온 폴더에 있습니다.
- Windows 8.1 원격 데스크톱에 대해 로그인 스크립트 지연 구성 컴퓨터 그룹 정책 설정을 사용하지 않도록 설정합니다. 이 설정은 컴퓨터 구성\관리 템플릿\시스템\그룹 정책 폴더에 있습니다.
- 사용자가 데스크톱 세션에 다시 연결할 때 Horizon 스마트 정책 설정을 새로 고치도록 하려면 User Environment Manager 관리 콘솔을 사용하여 트리거된 작업을 생성합니다. 트리거를 **세션 다시 연결**로 설정하고, 작업을 **사용자 환경 새로 고침**으로 설정하고, 새로 고칠 **Horizon 스마트 정책**을 선택합니다.

---

**참고** 사용자가 원격 데스크톱에 로그인해 있는 동안 트리거된 작업을 만든 경우, 트리거된 작업을 적용하려면 사용자가 데스크톱에서 로그오프해야 합니다.

---

## Horizon 스마트 정책 설정

Horizon 스마트 정책을 생성하면 User Environment Manager에서 원격 데스크톱 기능의 동작을 제어할 수 있습니다.

표 5-2. Horizon 스마트 정책 설정에서는 User Environment Manager에서 Horizon 스마트 정책을 정의할 때 선택할 수 있는 설정에 대해 설명합니다.

표 5-2. Horizon 스마트 정책 설정

설정	설명
USB 리디렉션	USB 리디렉션이 원격 데스크톱에서 사용되도록 설정되었는지 확인합니다. USB 리디렉션 기능을 사용하면 사용자가 썸 플래시 드라이브, 카메라, 프린터와 같이 로컬로 연결된 USB 디바이스를 원격 데스크톱에서 사용할 수 있습니다.
인쇄	가상 인쇄가 원격 데스크톱에서 사용되도록 설정되었는지 확인합니다. 가상 인쇄 기능을 사용하면 가상 프린터나 클라이언트 컴퓨터에 연결된 USB 프린터를 통해 원격 데스크톱에서 사용자가 인쇄할 수 있습니다.
클립보드	<p>클립보드 리디렉션이 허용되는 방향을 결정합니다. 다음 값 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>사용 안 함.</b> 클립보드 리디렉션은 양방향 모두에서 사용하도록 설정되어 있지 않습니다.</li> <li>■ <b>모두 허용.</b> 클립보드 리디렉션이 사용되도록 설정되었습니다. 사용자는 클라이언트 시스템에서 원격 데스크톱으로, 그리고 원격 데스크톱에서 클라이언트 시스템으로 복사 및 붙여넣기를 할 수 있습니다.</li> <li>■ <b>클라이언트에서 에이전트로 복사 허용.</b> 사용자는 클라이언트 시스템에서 원격 데스크톱으로 복사 및 붙여넣기를 할 수 있습니다.</li> <li>■ <b>에이전트에서 클라이언트로 복사 허용.</b> 사용자는 원격 데스크톱에서 클라이언트 시스템으로만 복사 및 붙여넣기를 할 수 있습니다.</li> </ul>
클라이언트 드라이브 리디렉션	<p>원격 데스크톱에서 클라이언트 드라이브 리디렉션을 사용하도록 설정되어 있는지 여부와 공유 드라이브 및 폴더가 쓰기 가능한지 여부를 결정합니다. 다음 값 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>사용 안 함.</b> 클라이언트 드라이브 리디렉션은 원격 데스크톱에서 사용하도록 설정되어 있지 않습니다.</li> <li>■ <b>모두 허용.</b> 클라이언트 드라이브 및 폴더는 원격 데스크톱과 공유되며 읽기 및 쓰기가 가능합니다.</li> <li>■ <b>읽기 전용.</b> 클라이언트 드라이브 및 폴더는 원격 데스크톱과 공유되며 읽기는 가능하지만 쓰기는 가능하지 않습니다.</li> </ul> <p>이 설정을 구성하지 않을 경우 공유 드라이브와 폴더의 쓰기 가능 여부는 로컬 레지스트리 설정에 따라 결정됩니다. 자세한 내용은 <a href="#">레지스트리 설정을 사용하여 클라이언트 드라이브 리디렉션 구성</a>의 내용을 참조하십시오.</p>
대역폭 프로파일	<p>원격 데스크톱에서 PCoIP 및 Blast 세션에 대한 대역폭 프로파일을 구성합니다. LAN과 같이 미리 정의된 대역폭 프로파일을 선택할 수 있습니다. 미리 정의된 대역폭 프로파일을 선택하면 에이전트가 링크 용량보다 높은 속도로 전송을 시도할 수 없습니다. 기본 프로파일을 선택할 경우의 최대 대역폭은 초당 90000킬로비트입니다.</p> <p>자세한 내용은 <a href="#">대역폭 프로파일 참조</a>의 내용을 참조하십시오.</p>
HTML Access 파일 전송	클라이언트와 에이전트 간의 HTML 파일 전송을 결정합니다.

일반적으로 User Environment Manager에서 원격 데스크톱 기능에 대해 구성한 Horizon 스마트 정책 설정이 이와 동등한 레지스트리 키 및 그룹 정책 설정을 재정의합니다.

## 대역폭 프로파일 참조

스마트 정책에서는 대역폭 프로파일 정책 설정을 사용하여 원격 데스크톱의 PCoIP 또는 Blast 세션에 대한 대역폭 프로파일을 구성할 수 있습니다.

표 5-3. 대역폭 프로파일

대역폭 프로파일	최대 세션 BW(Kbps)	최소 세션 BW(Kbps)	BTL 사 용	최대 초기 이미지 품질	최소 이미지 품질	최대 FPS	최대 오디오 BW(Kbps)	이미지 품질 성 능
고속 LAN	900000	100	예	100	50	60	1600	50
LAN	900000	100	예	90	50	30	1600	50
전용 WAN	900000	100	아니요	80	40	30	500	50
광대역 WAN	5000	100	아니요	70	40	20	500	50
저속 WAN	2000	100	아니요	70	30	15	200	25
초저속 연결	1000	100	아니요	70	30	5	90	0

## Horizon 스마트 정책 정의에 조건 추가

User Environment Manager에서 Horizon 스마트 정책을 정의할 때 정책을 적용하기 위해 충족해야 할 조건을 추가할 수 있습니다. 예를 들어, 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결한 경우에만 클라이언트 드라이브 리디렉션 기능을 사용하지 않도록 설정하는 조건을 추가할 수 있습니다.

동일한 원격 데스크톱 기능에 대해 여러 개의 조건을 추가할 수 있습니다. 예를 들어, 사용자가 HR 그룹 구성원인 경우에 로컬 인쇄를 사용하도록 설정하는 조건 하나와 원격 데스크톱이 Win7 풀에 있는 경우 로컬 인쇄를 사용하도록 설정하는 조건 하나를 추가할 수 있습니다.

User Environment Manager 관리 콘솔에서의 조건 추가 및 편집에 대한 자세한 내용은 “User Environment Manager 관리자 가이드”를 참조하십시오.

## Horizon Client 속성 조건 사용

사용자가 원격 데스크톱에 연결 또는 다시 연결하면 Horizon Client가 클라이언트 컴퓨터에 대한 정보를 수집하고 연결 서버가 해당 정보를 원격 데스크톱에 전송합니다. Horizon Client 속성 조건을 Horizon 정책 정의에 추가하여 원격 데스크톱이 수신하는 정보를 기반으로 정책이 적용되는 시기를 제어할 수 있습니다.

**참고** Horizon Client 속성 조건은 사용자가 PCoIP 디스플레이 프로토콜이나 VMware Blast 디스플레이 프로토콜을 사용하여 원격 데스크톱을 실행한 경우에만 적용됩니다. 사용자가 RDP 디스플레이 프로토콜로 원격 데스크톱을 실행한 경우에는 Horizon Client 속성 조건이 적용되지 않습니다.

**표 5-4. Horizon Client 속성 조건에 대해 미리 정의된 속성**에서는 Horizon Client 속성 조건을 사용할 때 **속성** 드롭다운 메뉴에서 선택할 수 있는 미리 정의된 속성을 설명합니다. 미리 정의된 각 속성은 ViewClient\_ 레지스트리 키에 해당됩니다.

표 5-4. Horizon Client 속성 조건에 대해 미리 정의된 속성

속성	해당 레지스트리 키	설명
클라이언트 위치	ViewClient_Broker_GatewayLocation	<p>사용자의 클라이언트 시스템 위치를 지정합니다. 올바른 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>■ 내부 - 사용자가 회사 네트워크 내부에서 원격 데스크톱에 연결한 경우에만 정책 적용</li> <li>■ 외부 - 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결한 경우에만 정책 적용</li> </ul> <p>연결 서버나 보안 서버 호스트의 게이트웨이 위치 설정에 대한 내용은 "View 관리" 문서를 참조하십시오.</p> <p>Access Point 장치의 게이트웨이 위치 설정에 대한 자세한 내용은 "Unified Access Gateway 배포 및 구성" 문서를 참조하십시오.</p>
실행 태그	ViewClient_Launch_Matched_Tags	<p>태그를 하나 이상 지정합니다. 태그가 여러 개인 경우 쉽표 또는 세미콜론으로 구분하십시오. 정책은 원격 데스크톱 또는 애플리케이션을 실행하도록 한 태그가 지정된 태그 중 하나와 일치하는 경우에만 적용됩니다.</p> <p>연결 서버 인스턴스 및 데스크톱 풀에 태그를 할당하는 것과 관련된 자세한 내용은 설치 문서를 참조하십시오.</p>
풀 이름	ViewClient_Launch_ID	<p>데스크톱 또는 애플리케이션 풀 ID를 지정합니다. 이 정책은 원격 데스크톱 또는 애플리케이션을 실행할 때 사용자가 선택한 데스크톱 또는 애플리케이션 풀의 ID가 지정된 데스크톱 또는 애플리케이션 풀 ID와 일치하는 경우에만 적용됩니다. 예를 들어, 사용자가 Win7 풀을 선택했고 이 속성이 Win7으로 설정되어 있으면 정책이 적용됩니다.</p> <p><b>참고</b> 동일한 RDS 호스트 세션에서 둘 이상의 애플리케이션 풀이 실행되면 해당 값은 Horizon Client에서 첫 번째로 실행되는 애플리케이션의 ID입니다.</p>

**속성** 드롭다운 메뉴는 텍스트 상자이기도 하며, 텍스트 상자에 ViewClient\_ 레지스트리 키를 수동으로 입력할 수 있습니다. 레지스트리 키를 입력할 때 ViewClient\_ 접두사를 포함할 수 있습니다. 예를 들어, ViewClient\_Broker\_URL을 지정하려면 Broker\_URL을 입력합니다.

원격 데스크톱에서 Windows 레지스트리 편집기(regedit.exe)를 사용하여 ViewClient\_ 레지스트리 키를 볼 수 있습니다. Horizon Client는 단일 사용자 시스템에 배포된 원격 데스크톱의 시스템 레지스트리 경로 HKEY\_CURRENT\_USER\WVolatile Environment에 클라이언트 컴퓨터 정보를 작성합니다. RDS 세션에서 배포된 원격 데스크톱의 경우 Horizon Client는 시스템 레지스트리 경로 HKEY\_CURRENT\_USER\WVolatile Environment\Wx에 클라이언트 컴퓨터 정보를 작성합니다. 여기서 x는 RDS 호스트의 세션 ID입니다.

## 다른 조건 사용

User Environment Manager 관리 콘솔에서는 다양한 조건을 제공합니다. 다음 조건은 원격 데스크톱 기능의 정책을 만들 때 특히 유용합니다.

<b>그룹 구성원</b>	이 조건을 사용하여 사용자가 특정 그룹의 구성원인 경우에만 정책을 적용하도록 구성할 수 있습니다.
<b>원격 디스플레이 프로토콜</b>	이 조건을 사용하여 사용자가 특정 디스플레이 프로토콜을 선택한 경우에만 정책을 적용하도록 구성할 수 있습니다. 조건 설정에는 RDP, PCoIP 및 Blast가 포함됩니다.
<b>IP 주소</b>	이 조건을 사용하여 사용자가 회사 네트워크의 내부/외부에서 연결한 경우에만 정책을 적용하도록 구성할 수 있습니다. 조건 설정을 사용하여 내부 IP 주소 범위나 외부 IP 주소 범위를 지정합니다.

---

**참고** Horizon Client 속성 조건에서 **클라이언트 위치** 속성을 사용할 수도 있습니다.

---

사용 가능한 모든 조건에 대한 설명은 “User Environment Manager 관리자 가이드” 문서를 참조하십시오.

## User Environment Manager에 Horizon 스마트 정책 생성

User Environment Manager 관리 콘솔을 사용하여 User Environment Manager에 Horizon 스마트 정책을 생성합니다. Horizon 스마트 정책을 정의할 때, 스마트 정책을 적용하기 위해 충족해야 할 조건을 추가할 수 있습니다.

### 사전 요구 사항

- User Environment Manager를 설치 및 구성합니다. 자세한 내용은 [User Environment Manager 설치](#) 및 [User Environment Manager 구성](#)에 나와 있습니다.
- Horizon 스마트 정책 설정을 익힙니다. [Horizon 스마트 정책 설정](#)의 내용을 참조하십시오.
- Horizon 스마트 정책 정의에 추가할 수 있는 조건을 익힙니다. [Horizon 스마트 정책 정의에 조건 추가](#)의 내용을 참조하십시오.

User Environment Manager 관리 콘솔 사용에 대한 완전한 정보를 보려면 “User Environment Manager 관리자 가이드” 문서를 참조하십시오.

### 절차

- 1 User Environment Manager 관리 콘솔에서 **사용자 환경** 탭을 선택하고 트리 보기에서 **Horizon 스마트 정책**을 클릭합니다.

기존 Horizon 스마트 정책 정의는 Horizon 스마트 정책 창에 나타납니다(있는 경우).

- 2 **Horizon 스마트 정책**을 마우스 오른쪽 버튼으로 클릭하고 **Horizon 스마트 정책 정의 만들기**를 선택하여 새 스마트 정책을 생성합니다.

Horizon 스마트 정책 대화상자가 표시됩니다.

### 3 설정 탭을 선택하고 스마트 정책 설정을 정의합니다.

- a 일반 설정 섹션에서 **이름** 텍스트 상자에 스마트 정책의 이름을 입력합니다.

예를 들어 스마트 정책이 클라이언트 드라이브 리디렉션 기능에 영향을 준다면 스마트 정책 이름을 CDR로 지정할 수 있습니다.

- b Horizon 스마트 정책 설정 섹션에서 스마트 정책에 포함할 원격 데스크톱 기능 및 설정을 선택합니다.

여러 개의 원격 데스크톱 기능을 선택할 수 있습니다.

### 4 (선택 사항) 스마트 정책에 조건을 추가하려면 **조건** 탭을 선택하고 **추가**를 클릭한 다음 조건을 선택합니다.

스마트 정책 정의에 여러 조건을 추가할 수 있습니다.

### 5 **저장**을 클릭하여 스마트 정책을 저장합니다.

User Environment Manager에서는 사용자가 원격 데스크톱에 연결하거나 다시 연결할 때마다 Horizon 스마트 정책을 처리합니다.

User Environment Manager에서는 스마트 정책 이름에 따라 여러 스마트 정책을 알파벳 순서로 처리합니다. Horizon 스마트 정책은 Horizon 스마트 정책 창에 알파벳 순으로 표시됩니다. 스마트 정책이 충돌하는 경우에는 마지막으로 처리한 스마트 정책의 우선 순위가 높습니다. 예를 들어 Sue라는 사용자가 USB 리디렉션을 사용할 수 있도록 설정하는 Sue라는 스마트 정책이 있고 Win7이라는 이름의 데스크톱 풀에 대해 USB 리디렉션을 사용하지 않도록 설정하는 Pool이라는 스마트 정책이 있는 경우, Win7 데스크톱 풀에 있는 원격 데스크톱에 Sue가 연결하면 USB 리디렉션 기능이 사용되도록 설정됩니다.

## Active Directory 그룹 정책 사용

Microsoft Windows 그룹 정책을 사용하여 원격 데스크톱을 최적화 및 보호하고 Horizon 7 구성 요소 동작을 제어하며 위치 기반 인재를 구성할 수 있습니다.

그룹 정책은 Active Directory 환경의 컴퓨터 및 원격 사용자를 구성하고 집중 관리하는 Microsoft Windows 운영 체제 기능입니다.

그룹 정책 설정은 그룹 정책 개체(GPO)라는 엔터티에 포함됩니다. GPO는 Active Directory 개체와 연결됩니다. 도메인 전체 수준에서 GPO를 Horizon 7 구성 요소에 적용하여 Horizon 7 환경의 다양한 영역을 제어할 수 있습니다. GPO가 적용되고 나면 GPO 설정은 지정한 구성 요소의 로컬 Windows 레지스트리에 저장됩니다.

Microsoft Windows Group Policy Object Editor를 사용하여 그룹 정책 설정을 관리합니다. Group Policy Object Editor는 Microsoft Management Console(MMC) 스냅인입니다. MMC는 Microsoft Group Policy Management Console(GPMC)의 일부입니다. GPMC 설치 및 사용에 대한 정보는 Microsoft TechNet 웹 사이트를 참조하십시오.

## 원격 데스크톱의 OU 생성

원격 데스크톱 전용 OU(조직 단위)를 Active Directory에 생성합니다.

그룹 정책 설정이 원격 데스크톱과 같은 도메인에 속해 있는 다른 Windows 서버나 워크스테이션에 적용되지 않게 하려면 Horizon 7 그룹 정책에 대한 GPO를 생성한 후 원격 데스크톱이 포함된 OU에 연결하십시오.

OU 및 GPO 생성에 대한 자세한 내용은 Microsoft TechNet 웹 사이트에서 Microsoft Active Directory 설명서를 참조하십시오.

## 원격 데스크톱에 대해 루프백 처리를 사용하도록 설정

기본적으로 Active Directory의 사용자 개체에 적용되는 GPO 집합에서 사용자의 정책 설정을 가져옵니다. 그러나 Horizon 7 환경에서는 사용자가 로그인하는 컴퓨터에 기반해 사용자에게 GPO가 적용됩니다.

루프백 처리를 사용하도록 설정하면 Active Directory에서의 위치에 관계없이 특정 컴퓨터에 로그인한 모든 사용자에게 일관된 정책 집합이 적용됩니다.

루프백 처리를 사용하도록 설정하는 자세한 방법은 Microsoft Active Directory 설명서를 참조하십시오.

---

**참고** 루프백 처리는 Horizon 7에서 GPO를 처리하는 한 가지 방법일 뿐입니다. 다른 방법으로 구현해야 하는 경우도 있습니다.

---

## Horizon 7 그룹 정책 관리 템플릿 파일 사용

Horizon 7에서는 몇 가지 구성 요소 관련 그룹 정책 관리 ADMX 템플릿 파일을 제공합니다. ADMX 템플릿 파일의 정책 설정을 Active Directory의 새 GPO 또는 기존 GPO에 추가하여 원격 데스크톱 및 애플리케이션을 최적화하고 보호할 수 있습니다.

Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip이라는 번들형 .zip 파일에서 사용할 수 있습니다. 여기서 x.x.x는 버전이고 yyyyyy는 빌드 번호입니다. <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 파일을 다운로드할 수 있습니다. Desktop & End-User Computing에서 번들형 .zip 파일이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

Horizon 7 ADMX 템플릿 파일에는 컴퓨터 구성 및 사용자 구성 그룹 정책 모두가 포함됩니다.

- 컴퓨터 구성 정책은 데스크톱에 연결하는 사용자에게 관계없이 모든 원격 데스크톱에 적용되는 정책을 설정합니다.
- 사용자 구성 정책은 사용자가 연결하는 원격 데스크톱 또는 애플리케이션에 관계없이 모든 사용자에게 적용할 정책을 설정합니다. 사용자 구성 정책은 동일한 컴퓨터 구성 정책보다 우선합니다.

Microsoft Windows는 데스크톱이 시작될 때와 사용자가 로그인할 때 정책을 적용합니다.

## Horizon 7 ADMX 템플릿 파일

Horizon 7 ADMX 템플릿 파일은 Horizon 7 구성 요소를 제어하고 최적화하기 위한 그룹 정책 설정을 제공합니다.



표 5-5. Horizon ADMX 템플릿 파일

템플릿 이름	템플릿 파일	설명
Horizon Agent 구성	vdm_agent.admx	Horizon Agent의 환경 구성 요소 및 인증과 관련된 정책 설정이 포함됩니다.
Horizon Client 구성	vdm_client.admx	Windows용 Horizon Client와 관련된 정책 설정이 들어 있습니다. 연결 서버 호스트 도메인 외부에서 연결하는 클라이언트는 Horizon Client에 적용된 정책의 영향을 받지 않습니다. "Windows용 VMware Horizon Client 사용" 문서를 참조하십시오.
VMware Horizon URL 리디렉션	urlRedirection-enUS.admx	URL 콘텐츠 리디렉션 기능과 관련된 정책 설정이 포함되어 있습니다. 이 템플릿을 원격 데스크톱 풀 또는 애플리케이션 풀의 GPO에 추가하면 원격 데스크톱이나 애플리케이션 내부에서 클릭하는 특정 URL 링크를 Windows 기반 클라이언트로 리디렉션하고 클라이언트 측 브라우저에서 열 수 있습니다. 이 템플릿을 클라이언트 측 GPO에 추가하면, 사용자가 Windows 기반 클라이언트 시스템에서 특정 URL을 클릭할 때 해당 URL을 원격 데스크톱이나 애플리케이션에서 열 수 있습니다. <a href="#">장 3 URL 콘텐츠 리디렉션 구성</a> 및 "Windows용 VMware Horizon Client 사용" 문서를 참조하십시오.
연결 서버 구성	vdm_server.admx	연결 서버와 관련된 정책 설정이 포함됩니다. "View 관리" 설명서를 참조하십시오.
View 일반 구성	vdm_common.admx	모든 Horizon 구성 요소에 일반적인 정책 설정이 포함됩니다. "View 관리" 설명서를 참조하십시오.
PCoIP 세션 변수	pcoip.admx	PCoIP 디스플레이 프로토콜과 관련된 정책 설정이 들어 있습니다.
PCoIP 클라이언트 세션 변수	pcoip.client.admx	Windows용 Horizon Client에 영향을 주는 PCoIP 디스플레이 프로토콜과 관련된 정책 설정이 들어 있습니다. "Windows용 VMware Horizon Client 사용" 문서를 참조하십시오.
Horizon Persona Management 구성	ViewPM.admx	Horizon Persona Management와 관련된 정책 설정이 포함되어 있습니다. "Horizon 7에서 가상 데스크톱 설정" 문서를 참조하십시오.
원격 데스크톱 서비스	vmware_rds.admx	원격 데스크톱 서비스와 관련된 정책 설정이 들어 있습니다. <a href="#">원격 데스크톱 서비스 그룹 정책 사용</a> 을 참조하십시오.



템플릿 이름	템플릿 파일	설명
실시간 오디오-비디오 구성	vdm_agent_rtav.admx	실시간 오디오-비디오 기능과 함께 사용되는 웹캠과 관련된 정책 설정이 포함되어 있습니다. <a href="#">실시간 오디오-비디오 그룹 정책 설정</a> 을 참조하십시오.
스캐너 리디렉션	vdm_agent_scanner.admx	게시된 데스크톱 및 애플리케이션에서 사용하기 위해 리디렉션되는 스캔 디바이스와 관련된 정책 설정이 포함되어 있습니다. <a href="#">스캐너 리디렉션 그룹 정책 설정</a> 을 참조하십시오.
직렬 포트 리디렉션	vdm_agent_serialport.admx	가상 데스크톱에서 사용하기 위해 리디렉션되는 직렬(COM) 포트와 관련된 정책 설정이 포함되어 있습니다. <a href="#">직렬 포트 리디렉션 그룹 정책 설정</a> 을 참조하십시오.

## Active Directory에 ADMX 템플릿 파일 추가

Horizon 7 ADMX 파일의 특정 원격 데스크톱 기능에 대한 정책 설정을 Active Directory의 GPO(그룹 정책 개체)에 추가할 수 있습니다.

### 사전 요구 사항

- 정책을 적용하는 원격 데스크톱 기능에 대한 설정 옵션이 데스크톱 및 RDS 호스트에 설치되어 있는지 확인하십시오. 원격 데스크톱 기능이 설치되어 있지 않은 경우 그룹 정책 설정이 아무런 영향을 주지 않습니다. Horizon Agent 설치에 대한 자세한 내용은 설치 문서를 참조하십시오.
- 그룹 정책 설정을 적용할 원격 데스크톱 기능에 대한 GPO를 만들고 RDS 호스트를 포함하는 OU에 연결합니다.
- Active Directory에 추가하려는 ADMX 템플릿 파일의 이름을 확인하십시오. [Horizon 7 ADMX 템플릿 파일](#)을 참조하십시오.
- Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.

Windows 2012, Windows 2008 및 Windows 2003 Active Directory 버전에 따라 그룹 정책 관리 콘솔을 여는 방법이 다릅니다. [Horizon 7 그룹 정책에 대한 GPO 생성](#)을 참조하십시오.

### 절차

- 1 Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip입니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일의 압축을 풀고 ADMX 파일을 Active Directory 또는 RDS 호스트에 복사합니다.
  - a .admx 파일과 ko-KR 폴더를 Active Directory 또는 RDS 호스트의 %systemroot%\PolicyDefinitions 폴더에 복사합니다.
  - b 언어 리소스 파일(.adml)을 Active Directory 또는 RDS 호스트의 %systemroot%\PolicyDefinitions\에 있는 적절한 하위 폴더에 복사합니다.
- 3 Active Directory 호스트에서 그룹 정책 관리 편집기를 열고, 설치 후에 편집기에 나타나는 템플릿 파일 경로를 입력합니다.

개별 RDS 호스트에서는 gpedit.msc 유틸리티를 사용하여 로컬 그룹 정책 편집기를 열 수 있습니다.

다음에 수행할 작업

그룹 정책 설정을 구성하십시오.

## Horizon Agent 구성 ADMX 템플릿 설정

Horizon Agent 구성 ADMX 템플릿 파일(vdm\_agent.admx)에는 Horizon Agent의 인증 및 환경 구성 요소와 관련된 정책 설정이 포함됩니다.

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

다음 표에는 USB 디바이스에서 사용되는 설정을 제외한 Horizon Agent 구성 ADMX 템플릿 파일의 정책 설정이 설명되어 있습니다. 템플릿에는 컴퓨터 구성 및 사용자 구성 설정 모두가 포함됩니다. 사용자 구성 설정은 동일한 컴퓨터 구성 설정보다 우선합니다.

표 5-6. Horizon Agent 구성 템플릿 설정

설정	컴퓨터	사용자	속성
AllowDirectRDP	X		<p>Horizon Client 디바이스 이외의 클라이언트가 RDP를 사용하여 원격 데스크톱에 직접 연결할 수 있는지 여부를 결정합니다. 이 설정을 사용하지 않도록 설정한 경우 에이전트는 Horizon Client를 통해 Horizon에서 관리하는 연결만 허용합니다.</p> <p>Mac용 Horizon Client에서 원격 데스크톱에 연결할 경우 AllowDirectRDP 설정을 사용하지 않도록 설정하지 마십시오. 이 설정이 사용되지 않도록 설정된 경우, 액세스가 거부됨 오류와 함께 연결이 실패합니다.</p> <p>기본적으로 사용자가 Horizon 7 데스크톱 세션에 로그인한 동안에는 Horizon 7 외부에서 RDP를 사용하여 가상 시스템에 연결할 수 있습니다. RDP 연결이 설정되면 Horizon 7 데스크톱 세션이 종료되고 사용자가 저장하지 않은 데이터와 설정은 손실될 수 있습니다. 외부 RDP 연결이 닫힐 때까지 사용자는 데스크톱에 로그인할 수 없습니다. 이러한 상황이 발생하지 않도록 방지하려면 AllowDirectRDP 설정을 비활성화합니다.</p> <p><b>중요</b> 각 데스크톱의 게스트 운영 체제에 Windows 원격 데스크톱 서비스가 실행 중이어야 합니다. 이 설정을 사용하여 사용자가 데스크톱에 대한 직접 RDP 연결을 설정하지 못하도록 할 수 있습니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
AllowSingleSignon	X		<p>사용자를 데스크톱과 애플리케이션에 연결하는 데 SSO(단일 로그인)를 사용할지 여부를 결정합니다. 이 설정이 사용하도록 설정되어 있으면 사용자가 서버에 로그인할 때 자격 증명을 한 번만 입력하면 됩니다. 이 설정을 사용하지 않도록 설정된 경우, 사용자는 원격 연결이 설정될 때 다시 인증해야 합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
CommandsToRunOnConnect	X		<p>처음 세션이 연결될 때 실행될 명령 스크립트 또는 명령 목록을 지정합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>자세한 내용은 <a href="#">Horizon 데스크톱에서 명령 실행</a>에 나와 있습니다.</p>
CommandsToRunOnDisconnect	X		<p>세션 연결이 끊어진 후 실행해야 하는 명령 목록 또는 명령 스크립트를 지정합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>자세한 내용은 <a href="#">Horizon 데스크톱에서 명령 실행</a>에 나와 있습니다.</p>

설정	컴퓨터	사용자	속성
CommandsToRunOnReconnect	X		<p>연결이 끊긴 후 세션이 다시 연결될 때 실행될 명령 스크립트 또는 명령 목록을 지정합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>자세한 내용은 <a href="#">Horizon 데스크톱에서 명령 실행</a>에 나와 있습니다.</p>
ConnectionTicketTimeout	X		<p>Horizon 연결 티켓이 유효한 시간을 초로 지정합니다.</p> <p>Horizon Client 디바이스는 에이전트에 연결할 때 확인 및 Single Sign-On을 위해 연결 티켓을 사용합니다. 보안상의 이유로 연결 티켓은 제한된 시간 동안 유효합니다. 사용자가 원격 데스크톱에 연결할 경우 연결 티켓 시간 초과 기간 또는 세션 시간 초과 내에 인증이 실행되어야 합니다. 이 설정이 구성되지 않을 경우 기본 시간 초과 기간은 900초입니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p>
CredentialFilterExceptions	X		<p>CredentialFilter 에이전트 로드에서 허용되지 않는 실행 파일을 지정합니다. 파일 이름에는 경로 또는 접미사가 포함될 수 없습니다. 세미콜론을 사용하여 여러 파일 이름을 구분합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p>
Disable Time Zone Synchronization	X	X	<p>Horizon 데스크톱의 표준 시간대와 연결된 클라이언트의 표준 시간대를 동기화할지 여부를 결정합니다. Horizon Client 구성 정책의 표준 시간대 전달 사용 안 함 설정을 사용하지 않도록 설정되지 않은 경우에만 사용 설정이 적용됩니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하지 않도록 설정됩니다.</p>
DPI Synchronization	X	X	<p>원격 세션의 시스템 전체 DPI 설정을 조정합니다. 이 설정이 구성되지 않았거나 사용하도록 설정된 경우에는 원격 세션의 시스템 전체 DPI 설정이 클라이언트 운영 체제의 해당 DPI 설정과 일치하도록 설정됩니다. 이 설정이 사용하지 않도록 설정된 경우에는 원격 세션의 시스템 전체 DPI 설정이 변경되지 않습니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 구성되어 있지 않습니다.</p> <p><b>참고</b> 이 설정은 버전 7.0.2 이상과 Horizon Client 4.2 이상이 설치된 Windows 클라이언트에만 적용됩니다.</p>

설정	컴퓨터	사용자	속성
Enable multi-media acceleration	X		<p>MMR(멀티미디어 리디렉션)을 원격 데스크톱에서 사용하도록 설정할지를 결정합니다.</p> <p>MMR은 TCP 소켓을 통해 원격 시스템의 특정 코덱에서 클라이언트로 멀티미디어 데이터를 직접 전달하는 Windows Media Foundation 필터입니다. 그런 다음 데이터는 재생되는 클라이언트에서 바로 디코딩됩니다. 클라이언트의 리소스가 부족하여 로컬 멀티미디어 디코딩을 처리할 수 없는 경우 MMR을 사용하지 않도록 설정할 수 있습니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
Force MMR to use software overlay	X		<p>MMR은 더 나은 성능을 위해 하드웨어 오버레이를 사용하여 비디오를 재생하려고 합니다. 여러 디스플레이를 사용할 때는 하드웨어 오버레이가 디스플레이 중 하나, 즉 기본 디스플레이 또는 WMP가 시작된 디스플레이에만 존재합니다. WMP를 다른 디스플레이로 끌어오면 비디오는 검은색 사각형으로 나타납니다. MMR이 모든 디스플레이에서 작동하는 소프트웨어 오버레이를 강제로 사용하도록 하려면 이 옵션을 사용하십시오.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 구성되어 있지 않습니다.</p>
Single sign-on retry timeout	X		<p>단일 로그인에 다시 시도되기까지 경과되는 시간(밀리초)을 지정합니다. 단일 로그인 다시 시도를 사용하지 않도록 설정하려면 이 값을 0으로 설정합니다. 기본값은 5,000밀리초입니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 구성되어 있지 않습니다.</p>
ShowDiskActivityIcon	X		<p>이 설정은 본 릴리스에서 지원되지 않습니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p>
Toggle Display Settings Control	X		<p>클라이언트 세션에서 PCoIP 디스플레이 프로토콜을 사용할 경우 <b>디스플레이</b> 제어판에서 <b>설정</b> 탭이 사용되지 않도록 설정되었는지 확인합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>

설정	컴퓨터	사용자	속성
UnAuthenticatedAccessEnabled			<p>인증되지 않은 액세스 기능을 사용하거나 사용하지 않도록 설정합니다. 이 설정이 사용되도록 지정되면 인증되지 않은 액세스 사용자가 AD 자격 증명 없이도 Horizon Client에서 게시된 애플리케이션에 액세스할 수 있습니다. 이 설정이 사용되지 않도록 지정되면 인증되지 않은 액세스 사용자가 AD 자격 증명 없이 Horizon Client에서 게시된 애플리케이션에 액세스할 수 없습니다.</p> <p>이 설정이 적용되려면 RDS 호스트를 재부팅해야 합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 구성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
Send updates for empty or offscreen windows	X		<p>클라이언트가 비어 있는 창 또는 화면 밖에 있는 창에 대한 업데이트를 수신할지를 지정합니다. 이 설정을 사용하지 않도록 설정하면 2x2픽셀보다 작거나 완전히 화면 밖에 있는 창에 대한 정보는 클라이언트로 전송되지 않습니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Unity Touch 및 호스팅된 애플리케이션</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하지 않도록 설정됩니다.</p>
Enable Unity Touch	X		<p>Unity Touch 기능을 원격 데스크톱에서 사용하도록 설정할지를 결정합니다. Unity Touch는 Horizon에서 원격 애플리케이션의 제공을 지원하고 모바일 디바이스 사용자가 Unity Touch 사이드바에서 애플리케이션에 액세스하게 해줍니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Unity Touch 및 호스팅된 애플리케이션</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
Enable system tray redirection for Hosted Apps	X		<p>사용자가 원격 애플리케이션을 실행하는 동안 시스템 트레이 리디렉션 사용하도록 설정되었는지 확인합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Unity Touch 및 호스팅된 애플리케이션</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p>
Enable user profile customization for Hosted Apps	X	X	<p>원격 애플리케이션이 사용될 때 사용자 프로파일을 사용자 지정할지를 지정합니다. 이 설정이 사용되도록 설정되면 사용자 프로파일이 생성되고, Windows 테마가 사용자 지정되고, 시작 애플리케이션이 등록됩니다.</p> <p>이 컴퓨터 구성 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Unity Touch 및 호스팅된 애플리케이션</b> 폴더에 있습니다. 사용자 구성 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 보안 &gt; Unity Touch 및 호스팅된 애플리케이션</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용하지 않도록 설정됩니다.</p>

설정	컴퓨터	사용자	속성
Limit usage of Windows hooks	X		<p>원격 애플리케이션 또는 Unity Touch가 사용될 때 대부분의 후크는 사용되지 않도록 설정됩니다. 이 설정은 OS 수준 후크가 설정될 경우 호환성 문제가 발생하는 애플리케이션을 위한 것입니다. 예를 들어 이 설정을 사용하도록 설정하면 대부분의 Windows 활성 액세스 가능성 및 in-process 후크를 사용할 수 없게 됩니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Unity Touch 및 호스팅된 애플리케이션</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용되지 않도록 설정됩니다. 즉, 모든 기본 설정 후크가 사용됩니다.</p>
Accept SSL encrypted framework channel		X	<p>SSL 암호화된 프레임워크 채널을 사용하도록 설정합니다. 다음 옵션을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>사용 안 함</b> - SSL을 사용하지 않도록 설정합니다.</li> <li>■ <b>사용</b> - SSL을 사용하도록 설정합니다. 레거시 클라이언트가 SSL 없이 연결할 수 있습니다.</li> <li>■ <b>강제 적용</b> - SSL을 사용하도록 설정합니다. 레거시 클라이언트 연결을 거부합니다.</li> </ul> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; Agent 보안</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 구성되어 있지 않습니다. 기본값은 <b>사용</b>입니다.</p>
Default Proxy Server	X		<p>프록시 서버에 대한 기본 Internet Explorer 연결 설정입니다. [인터넷 옵션] &gt; [LAN 설정]에서 사용할 프록시 서버를 지정합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware 클라이언트 IP 투명성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용되도록 설정되어 있지 않습니다.</p>
Enable	X		<p>VMware 클라이언트 IP 투명성을 사용하도록 설정합니다. Internet Explorer에 대한 원격 연결은 원격 데스크톱 시스템의 IP 주소 대신 클라이언트의 IP 주소를 사용합니다. 이 설정은 다음 로그인 시 적용됩니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware 클라이언트 IP 투명성</b> 폴더에 있습니다.</p> <p>[VMware 클라이언트 IP 투명성] 사용자 지정 설정 옵션이 Horizon Agent 설치 관리자에서 선택되면 이 설정이 기본적으로 사용되도록 설정됩니다.</p>
Default auto detect proxy	X		<p>기본 Internet Explorer 연결 설정입니다. [인터넷 옵션] &gt; [LAN 설정]에서 <b>자동으로 설정 검색</b>을 켭니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware 클라이언트 IP 투명성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용되도록 설정되어 있지 않습니다.</p>

설정	컴퓨터	사용자	속성
Set proxy for Java applet	X		<p>Java 애플릿에 대한 프록시를 설정합니다. 다음 옵션을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>Java 프록시에 대해 클라이언트 IP 투명성 사용</b> - 원격 연결이 Java 애플릿에 대해 원격 데스크톱 시스템의 IP 주소가 아닌 클라이언트의 IP 주소를 사용하도록 지시합니다.</li> <li>■ <b>Java 프록시에 대해 직접 연결 사용</b> - 직접 연결을 사용하여 Java 애플릿에 대한 브라우저 설정을 우회합니다.</li> <li>■ <b>Java 프록시에 대해 기본값 사용</b> - 원래의 Java 프록시 설정을 복원합니다.</li> </ul> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware 클라이언트 IP 투명성</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 사용되도록 설정되어 있지 않습니다.</p>
Enable flash multi-media redirection	X		<p>Flash 리디렉션을 에이전트에서 사용하도록 설정할지를 지정합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware FlashMMR</b> 폴더에 있습니다.</p>
Minimum rect size to enable FlashMMR	X		<p>Flash 리디렉션을 사용하도록 설정할 최소 직사각형 크기를 지정합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware FlashMMR</b> 폴더에 있습니다.</p> <p>기본 너비는 320픽셀이고 기본 높이는 200픽셀입니다.</p>
Definition for FlashMMR url list usage		X	<p>URL이 Flash 리디렉션을 사용하도록 하는 화이트리스트 또는 사용하지 않도록 하는 블랙리스트 규칙을 정의합니다.</p> <p><b>FlashMMR URL 목록 사용 정의</b> 드롭다운 메뉴에서 <b>화이트리스트 목록 사용</b>을 선택하는 경우 URL 목록의 URL만 Flash 리디렉션을 사용하도록 설정됩니다.</p> <p><b>FlashMMR URL 목록 사용 정의</b> 드롭다운 메뉴에서 <b>블랙리스트 목록 사용</b>을 선택하는 경우 URL 목록의 URL은 Flash 리디렉션을 사용할 수 없습니다.</p> <p>Hosts Url list to enable FlashMMR 그룹 정책 설정에서 URL 목록을 지정합니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware FlashMMR</b> 폴더에 있습니다.</p> <p>이 설정은 기본적으로 화이트리스트를 지정합니다.</p>
Hosts Url list to enable FlashMMR		X	<p>Definition for FlashMMR url list usage 그룹 정책 설정에 따라 Flash 리디렉션을 사용하거나 사용하지 않도록 설정된 URL 목록을 지정합니다.</p> <p><b>http://</b> 또는 <b>https://</b>를 포함해야 합니다. 정규식을 사용할 수 있습니다. 예를 들어, <b>https://*.google.com</b> 및 <b>http://www.cnn.com</b>을 지정할 수 있습니다.</p> <p>이 설정은 그룹 정책 관리 편집기의 <b>VMware View Agent 구성 &gt; VMware FlashMMR</b> 폴더에 있습니다.</p>



**참고** Connect using DNS Name 설정은 Horizon 6 버전 6.1 릴리스에서 제거되었습니다. Horizon 7 LDAP 특성 **pae-PreferDNS**를 설정하여 데스크톱 시스템 및 RDS 호스트의 주소를 클라이언트 및 게이트웨이로 전송할 때 Horizon 연결 서버가 DNS 이름에 우선 순위를 부여하도록 요구할 수 있습니다. “View 설치” 문서의 “Horizon 연결 서버가 주소 정보를 반환하는 경우 DNS 이름에 우선 순위 부여”를 참조하십시오.

## Horizon Agent에 대한 USB 설정

Horizon Agent 구성 ADMX 템플릿에서의 USB 설정을 참조하십시오.

## 원격 데스크톱에 전송한 클라이언트 시스템 정보

사용자가 원격 데스크톱에 연결 또는 다시 연결하면 Horizon Client가 클라이언트 시스템에 대한 정보를 수집하고 연결 서버가 해당 정보를 원격 데스크톱에 전송합니다.

Horizon Agent는 단일 사용자 시스템에 배포된 원격 데스크톱의 시스템 레지스트리 경로 HKCU\Wolative Environment에 클라이언트 컴퓨터 정보를 작성합니다. RDS 세션에서 배포된 원격 데스크톱의 경우 Horizon Agent는 시스템 레지스트리 경로 HKCU\Wolative Environment\X에 클라이언트 컴퓨터 정보를 작성합니다. 여기서 X는 RDS 호스트의 세션 ID입니다.

Horizon Client가 원격 데스크톱 세션 내부에서 실행 중인 경우에는 가상 시스템 정보 대신 실제 클라이언트 정보를 원격 데스크톱으로 전송합니다. 예를 들어 사용자가 클라이언트 시스템에서 원격 데스크톱에 연결하고, 원격 데스크톱 내부에서 Horizon Client를 실행하고, 다른 원격 데스크톱에 연결하면 두 번째 원격 데스크톱으로 실제 클라이언트 시스템의 IP 주소가 전송됩니다. 이 기능은 중첩 모드나 이중 홈 시나리오라고도 합니다. Horizon Client에서는 1로 설정된 ViewClient\_Nested\_Passthrough를 클라이언트 시스템 정보와 함께 중첩 모드 정보를 전송하는 것을 알립니다.

**참고** Horizon Client 4.1에서는 클라이언트 시스템 정보가 초기 프로토콜 연결의 두 번째 홈 데스크톱에 전달됩니다. Horizon Client 4.2 이상에서는 첫 번째 홈 프로토콜 연결이 끊겼다가 다시 연결된 경우에도 클라이언트 시스템 정보가 업데이트됩니다.

Horizon Agent CommandsToRunOnConnect, CommandsToRunOnReconnect 및 CommandsToRunOnDisconnect 그룹 정책 설정에 명령을 추가해 사용자가 데스크톱에 연결 및 재연결할 때 시스템 레지스트리에서 해당 정보를 읽는 명령 또는 명령 스크립트를 실행할 수 있습니다. 자세한 내용은 [Horizon 데스크톱에서 명령 실행](#)에 나와 있습니다.

**표 5-7. 클라이언트 시스템 정보**에서는 클라이언트 시스템 정보를 포함하는 레지스트리 키를 설명하고 이를 지원하는 데스크톱 및 클라이언트 시스템 유형 목록을 보여줍니다. **중첩 모드 지원** 열에 [예]가 표시되면 두 번째 홈 데스크톱에 가상 시스템의 정보 대신 실제 클라이언트 정보를 전송하는 것입니다.

표 5-7. 클라이언트 시스템 정보

레지스트리 키	설명	중첩 모드 지원	지원되는 데스크톱	지원되는 클라이언트 시스템
ViewClient_IP_Address	클라이언트 시스템의 IP 주소.	예	VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_MAC_Address	클라이언트 시스템의 MAC 주소.	예	VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android
ViewClient_Machine_Name	클라이언트 시스템의 시스템 이름.	예	VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Machine_Domain	클라이언트 시스템의 도메인.	예	VDI(단일 사용자 시스템) RDS	Windows, Windows 스토어
ViewClient_LoggedOn_Username	클라이언트 시스템에 로그인할 때 사용한 사용자 이름.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac
ViewClient_LoggedOn_Domainname	클라이언트 시스템에 로그인할 때 사용한 도메인 이름.		VDI(단일 사용자 시스템) RDS	Windows, Windows 스토어 Linux 및 Mac 클라이언트의 경우 ViewClient_Machine_Domain을 참조하십시오. Linux와 Mac 계정은 Windows 도메인에 바인딩되지 않으므로 Linux 또는 Mac 클라이언트에 .ViewClient_LoggedOn_Domainname을 지정하지 않습니다.
ViewClient_Type	클라이언트 시스템의 썬 클라이언트 이름 또는 운영 체제 유형.	예	VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Broker_DNS_Name	View 연결 서버 인스턴스의 DNS 이름.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.
ViewClient_Broker_URL	View 연결 서버 인스턴스의 URL.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.

레지스트리 키	설명	중첩 모드 지원	지원되는 데스크톱	지원되는 클라이언트 시스템
ViewClient_Broker_Tunneled	View 연결 서버의 터널 연결 상태를 true(사용) 또는 false(사용 안 함)로 설정할 수 있습니다.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.
ViewClient_Broker_Tunnel_URL	터널 연결을 사용하는 경우 View 연결 서버 터널 연결의 URL.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.
ViewClient_Broker_Remote_IP_Address	View 연결 서버 인스턴스에 나타나는 클라이언트 시스템의 IP 주소.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.
ViewClient_TZID	Olson 표준 시간대 ID. 표준 시간대 동기화를 사용하지 않으려면 Horizon AgentDisable Time Zone Synchronization 그룹 정책 설정을 사용하도록 설정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Windows_Timezone	GMT 표준시. 표준 시간대 동기화를 사용하지 않으려면 Horizon AgentDisable Time Zone Synchronization 그룹 정책 설정을 사용하도록 설정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Windows 스토어
ViewClient_Broker_DomainName	View 연결 서버에 인증하는 데 사용되는 도메인 이름.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.
ViewClient_Broker_UserName	View 연결 서버에 인증하는 데 사용되는 사용자 이름.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.
ViewClient_Client_ID	라이선스 키에 대한 링크로 사용되는 Unique Client HardwareId를 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어

레지스트리 키	설명	중첩 모드 지원	지원되는 데스크톱	지원되는 클라이언트 시스템
ViewClient_Displays.Number	클라이언트에서 사용 중인 모니터 수를 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Displays.Topology	클라이언트에 있는 디스플레이의 배열, 해상도 및 크기를 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Keyboard.Type	클라이언트에서 사용 중인 키보드 유형을 지정합니다. 예: 일본어, 한국어.		VDI(단일 사용자 시스템) RDS	Windows
ViewClient_Launch_SessionType	세션 유형을 지정합니다. 유형은 데스크톱 또는 애플리케이션일 수 있습니다.		VDI(단일 사용자 시스템) RDS	값은 Horizon Client에서 수집되는 것이 아니라 View 연결 서버에서 직접 전송됩니다.
ViewClient_Mouse.Identifier	마우스 유형을 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows
ViewClient_Mouse.NumButtons	마우스에서 지원되는 버튼 수를 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows
ViewClient_Mouse.SampleRate	PS/2 마우스의 입력 샘플 속도(초당 보고 횟수)를 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows
ViewClient_Protocol	사용 중인 프로토콜을 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Language	운영 체제 언어를 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Launch_Matched_Tags	태그를 하나 이상 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Launch_ID	데스크톱 또는 애플리케이션 풀 고유 ID를 지정합니다.		VDI(단일 사용자 시스템) RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어
ViewClient_Broker_Farm_ID	RDS 호스트에 있는 데스크톱 또는 애플리케이션 풀의 팜 ID를 지정합니다.		RDS	Windows, Linux, Mac, Android, iOS, Windows 스토어

**참고** 표 5-7. 클라이언트 시스템 정보의 ViewClient\_LoggedOn\_Username 및

ViewClient\_LoggedOn\_Domainname 정의는 Windows용 Horizon Client 2.2 이상 릴리스에 적용됩니다.

Windows용 Horizon Client 5.4 이하 릴리스의 경우 ViewClient\_LoggedOn\_Username은 Horizon Client에 입력된 사용자 이름을 전송하고 ViewClient\_LoggedOn\_Domainname은 Horizon Client에 입력된 도메인 이름을 전송합니다.

Windows용 Horizon Client 2.2는 Windows용 Horizon Client 5.4보다 최신 릴리스입니다. Horizon Client 2.2부터는 Windows용 릴리스 번호가 다른 운영 체제 및 디바이스의 Horizon Client 릴리스와 일치합니다.

## Horizon 데스크톱에서 명령 실행

Horizon Agent CommandsToRunOnConnect, CommandsToRunOnReconnect 및 CommandsToRunOnDisconnect 그룹 정책 설정을 사용하여 사용자가 연결, 다시 연결 및 연결 해제할 때 Horizon 데스크톱에서 명령 및 명령 스크립트를 실행할 수 있습니다.

명령이나 명령 스크립트를 실행하려면 그룹 정책 설정의 명령 목록에 스크립트의 파일 경로 또는 명령 이름을 추가하십시오. 예:

date

C:\WScripts\Wmyscript.cmd

콘솔 액세스가 필요한 스크립트를 실행하려면 뒤에 공백이 있는 -C 또는 -c 옵션을 추가합니다. 예:

-c C:\WScripts\Wcli\_clip.cmd

-C e:\wprocexp.exe

지원되는 파일 형식에는 .CMD, .BAT 및 .EXE가 포함됩니다. .VBS 파일은 cscript.exe 또는 wscript.exe로 구문 분석되지 않는 경우 실행되지 않습니다. 예:

-C C:\WINDOWS\system32\wscript.exe C:\WScripts\checking.vbs

-C 또는 -c 옵션을 포함한 문자열의 총 길이는 260자를 초과하면 안 됩니다.

## PCoIP 정책 설정

PCoIP ADMX 템플릿 파일에는 PCoIP 디스플레이 프로토콜에 관련된 정책 설정이 포함되어 있습니다. ADMX 템플릿 파일의 이름은 pcoip.admx입니다. 관리자가 재정의할 수 있는 기본값으로 설정을 구성하거나 재정의할 수 없는 값으로 설정을 구성할 수 있습니다.

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

PCoIP 세션 변수 ADMX 템플릿 파일에는 다음 2개의 하위 범주가 포함됩니다.

#### 재정의 가능한 관리자 기본값

PCoIP 정책 설정 기본값을 지정합니다. 이러한 설정은 관리자가 재정의할 수 있습니다. 이러한 설정으로 레지스트리 키 값이 HKLM\Software\W\Policies\W\Teradici\W\PCoIP\Wpcoip\_admin\_defaults에 작성됩니다. 이러한 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 가능한 관리자 기본값** 폴더에 있습니다.

#### 재정의 불가능한 관리자 설정

재정의 가능한 관리자 기본값과 동일한 설정이 포함되어지만 이러한 설정은 관리자가 재정의할 수 없습니다. 이러한 설정으로 레지스트리 키 값이 HKLM\Software\W\Policies\W\Teradici\W\PCoIP\Wpcoip\_admin에 작성됩니다. 이러한 모든 설정은 그룹 정책 관리 편집기의 **사용자 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 불가능한 관리자 설정** 폴더에 있습니다.

템플릿에는 컴퓨터 구성 및 사용자 구성 설정 모두가 포함됩니다.

## 비정책 레지스트리 키

로컬 시스템 설정이 적용되어야 하고 HKLM\Software\W\Policies\W\Teradici 아래에 지정될 수 없는 경우 로컬 시스템 설정은 HKLM\Software\W\Teradici의 레지스트리 키에 지정될 수 있습니다. 동일한 레지스트리 키가 HKLM\Software\W\Policies\W\Teradici에 지정되는 것과 같이 HKLM\Software\W\Teradici에 지정될 수 있습니다. 동일한 레지스트리 키가 두 개의 위치 모두에 있는 경우 HKLM\Software\W\Policies\W\Teradici의 설정이 로컬 시스템 값을 재정의합니다.

## PCoIP 일반 설정

PCoIP ADMX 템플릿 파일은 PCoIP 이미지 품질, USB 디바이스 및 네트워크 포트와 같은 일반적인 설정을 구성하는 그룹 정책 설정을 포함합니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 가능한 관리자 기본값** 폴더에 있습니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **사용자 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 불가능한 관리자 설정** 폴더에도 있습니다.

표 5-8. PCoIP 일반 정책 설정

설정	설명
Configure PCoIP event log cleanup by size in MB	<p>PCoIP 이벤트 로그 정리 작업을 크기(MB)에 따라 구성할 수 있습니다.</p> <p>이 정책을 구성하면 해당 설정은 정리를 수행하기 전까지의 로그 파일 최대 크기를 제어합니다. <math>m</math>을 0이 아닌 값으로 설정하면 <math>m</math>MB 이상인 로그 파일이 자동으로 삭제됩니다. 설정 값이 0이면 크기별 파일 정리가 수행되지 않음을 나타냅니다.</p> <p>이 정책을 사용하지 않도록 설정하거나 구성하지 않은 경우, 크기별 이벤트 로그 정리 작업의 기본값은 100MB입니다.</p> <p>로그 파일 정리는 세션을 시작할 때 한 번 수행됩니다. 변경된 설정은 다음 세션부터 적용됩니다.</p>
Configure PCoIP event log cleanup by time in days	<p>PCoIP 이벤트 로그 정리 작업을 일수에 따라 구성할 수 있습니다.</p> <p>이 정책을 구성하면 해당 설정에 지정된 일수가 지나면 로그 파일을 정리하도록 제어됩니다. <math>n</math>을 0이 아닌 값으로 설정하면 <math>n</math>일보다 오래된 로그 파일이 자동으로 삭제됩니다. 설정 값이 0이면 일수에 따라 파일 정리가 수행되지 않음을 나타냅니다.</p> <p>이 정책을 사용하지 않도록 설정하거나 구성하지 않은 경우, 이벤트 정리 작업의 기본값은 7일입니다.</p> <p>로그 파일 정리는 세션을 시작할 때 한 번 수행됩니다. 변경된 설정은 다음 세션부터 적용됩니다.</p>
Configure PCoIP event log verbosity	<p>PCoIP 이벤트 로그의 자세한 표시 수준을 설정합니다. 값의 범위는 0(최대한 간단하게)~3(최대한 자세하게)입니다.</p> <p>이 설정을 사용하도록 설정하면 자세한 표시 수준을 0에서 3까지 설정할 수 있습니다. 이 설정을 구성하지 않거나 사용하지 않도록 설정하면 이벤트 로그의 자세한 표시 수준이 2로 기본 설정됩니다.</p> <p>활성 PCoIP 세션 도중 이 설정을 수정하면 새 설정이 즉시 적용됩니다.</p>

설정	설명
Configure PCoIP image quality levels	<p>네트워크 정체 기간 중 PCoIP에서 이미지를 렌더링하는 방식을 제어합니다. <b>최저 이미지 품질</b>, <b>최고 초기 이미지 품질</b> 및 <b>최대 프레임 비율</b> 값은 네트워크 대역폭 제한 환경을 미세하게 제어할 수 있도록 상호작용합니다.</p> <p><b>최저 이미지 품질</b> 값을 사용하여 제한된 대역폭 시나리오를 위해 이미지 품질 및 프레임 비율을 조정합니다. 값을 30과 100 사이에서 지정할 수 있습니다. 기본값은 40입니다. 더 낮은 값을 사용하면 프레임 비율이 높아지지만 품질 디스플레이는 더 낮아질 수 있습니다. 값이 높아지면 이미지 품질도 높아지지만 네트워크 대역폭이 제한될 때 프레임 비율이 더 낮아질 수 있습니다. 네트워크 대역폭이 제한되지 않는 경우, PCoIP는 이 값과 상관없이 최대 품질을 유지합니다.</p> <p><b>최고 초기 이미지 품질</b> 값을 사용하면 디스플레이 이미지의 변경된 영역에 대한 초기 품질을 제한하여 PCoIP에 필요한 네트워크 대역폭 피크가 줄어듭니다. 값을 30과 100 사이에서 지정할 수 있습니다. 기본값은 80입니다. 값이 낮아지면 내용 변경의 이미지 품질이 저하되고 피크 대역폭 요구 사항이 감소합니다. 값이 높아지면 내용 변경의 이미지 품질이 높아지고 피크 대역폭 요구 사항이 증가합니다. 변경되지 않은 영역은 이 값에 상관없이 점차 결합 없는(완벽한) 품질을 형성합니다. 80 이하의 값일 때 사용 가능한 대역폭을 가장 잘 사용합니다.</p> <p><b>최저 이미지 품질</b> 값은 <b>최고 초기 이미지 품질</b> 값을 초과할 수 없습니다.</p> <p><b>최대 프레임 비율</b> 값을 사용하면 초당 화면 업데이트 수를 제한하여 사용자당 소비한 평균 대역폭을 관리할 수 있습니다. 초당 프레임 1개에서 120개 사이의 값을 지정할 수 있습니다. 기본값은 30입니다. 값이 높아지면 대역폭을 많이 사용할 수 있지만 불규칙 신호가 적어져서 비디오와 같은 이미지 변경에서 전환이 더 매끄러워집니다. 값이 낮아지면 대역폭을 적게 사용하지만 불규칙 신호는 더 많아집니다.</p> <p>이러한 이미지 품질 값은 소프트웨어 호스트에만 적용되며 소프트웨어 클라이언트에 영향을 주지 않습니다.</p> <p>이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우 기본값이 사용됩니다.</p> <p>활성 PCoIP 세션 도중 이 설정을 수정하면 새 설정이 즉시 적용됩니다.</p>
Configure frame rate vs image quality preference	<p>프레임 속도 및 이미지 품질 환경설정을 0(최고 프레임 속도)에서 100(최고 이미지 품질)까지로 구성합니다. 이 정책을 사용하지 않도록 설정하거나 구성하지 않은 경우의 기본 설정은 50입니다.</p> <p>값이 높을수록(최대: 100) 프레임 속도가 고르지 못하더라도 높은 이미지 품질을 선호하는 것을 의미합니다. 값이 낮을수록(최소: 0) 이미지 품질이 떨어지더라도 원활한 프레임 속도를 선호하는 것을 의미합니다.</p> <p>이 설정은 최대 이미지 품질 수준과 최소 이미지 품질 수준을 결정하는 <b>Configure PCoIP image quality levels GPO</b>와 함께 사용할 수도 있습니다. <b>Frame rate and image quality preference</b>는 각 프레임의 이미지 품질 수준을 조정하지만, <b>Configure PCoIP image quality levels GPO</b>에서 구성한 최대/최소 품질 수준 임계값을 넘을 수는 없습니다.</p> <p>실행 중에 이 정책이 변경되면 즉시 적용될 수 있습니다.</p>



설정	설명
Configure PCoIP session encryption algorithms	<p>세션 협상 중 PCoIP 끝점에 의해 보급된 암호화 알고리즘을 제어합니다. 확인란 중 하나를 선택하면 연결된 암호화 알고리즘이 사용되지 않도록 설정됩니다. 적어도 한 개의 알고리즘을 사용하도록 설정해야 합니다.</p> <p>이 설정은 에이전트 및 클라이언트 모두에 적용됩니다. 끝점은 사용하는 실제 세션 암호화 알고리즘을 협상합니다. FIPS140-2 승인된 모드가 사용되도록 설정된 경우, <b>AES-128-GCM 암호화 사용 안 함</b> 값이 항상 재정의되어 AES-128-GCM 암호화가 사용되도록 설정됩니다.</p> <p>지원되는 암호화 알고리즘을 우선 순위에 따라 나열하면 SALSA20/12-256, AES-GCM-128 및 AES-GCM-256이며, 기본적으로 지원되는 모든 암호화 알고리즘을 이 끝점에서 협상에 사용할 수 있습니다.</p> <p>양쪽 끝점이 세 가지 알고리즘 모두를 지원하도록 구성되어 있고 연결에 SG(Security Gateway)가 사용되지 않는 경우에는 SALSA20 알고리즘이 협상 및 사용됩니다. 그러나 연결에 SG가 사용되면 SALSA20은 사용하지 않도록 자동으로 설정되고 AES128이 협상 및 사용됩니다. 양쪽 끝점 중 하나 또는 SG에서 SALSA20을 사용하지 않도록 설정하고, 다른 끝점에서 AES128을 사용하지 않도록 설정하면 AES256이 협상 및 사용됩니다.</p>

설정	설명
Configure PCoIP USB allowed and unallowed device rules	<p>PCoIP 세션을 위해 인증된 USB 디바이스 및 Teradici 펌웨어를 실행하는 제로 클라이언트를 사용하는 인증되지 않은 USB 디바이스를 지정합니다. PCoIP 세션에 사용된 USB 디바이스가 USB 인증 테이블에 나타나야 합니다. USB 비인증 케이블에 나타나는 USB 디바이스는 PCoIP 세션에서 사용될 수 있습니다.</p> <p>최대 10개의 USB 인증 규칙 및 최대 10개의 USB 비인증 규칙을 정의할 수 있습니다. 여러 규칙을 세로 막대( ) 문자로 구분하십시오.</p> <p>각 규칙은 공급업체 ID(VID) 및 제품 ID(PID)가 조합된 것일 수 있습니다. 또는 규칙에 USB 디바이스의 클래스가 설명될 수 있습니다. 클래스 규칙은 전체 디바이스 클래스, 단일 하위 클래스 또는 하위 클래스 내 프로토콜을 허용하거나 허용하지 않을 수 있습니다.</p> <p>VID/PID 규칙 조합의 형식은 <b>1xxxxyyyy</b>입니다. 여기서 <b>xxxx</b>는 16진수 형식의 VID이며 <b>yyyy</b>는 16진수 형식의 PID입니다. 예를 들어, VID <b>0x1a2b</b> 및 PID <b>0x3c4d</b>가 있는 디바이스를 인증 또는 차단하는 규칙은 <b>11a2b3c4d</b>입니다. 클래스 규칙의 경우, 다음 형식 중 하나를 사용합니다.</p> <p><b>모든 USB 디바이스 허용</b>      형식: <b>23XXXXX</b> 예: <b>23XXXXX</b></p> <p><b>특정 클래스 ID가 있는 USB 디바이스 허용</b>      형식: <b>22c/assXXX</b> 예: <b>22aaXXX</b></p> <p><b>특정 하위 클래스 허용</b>      형식: <b>21c/ass-subc/assXX</b> 예: <b>21aabbXX</b></p> <p><b>특정 프로토콜 허용</b>      형식: <b>20c/ass-subclass-protocol</b> 예: <b>20aabbcc</b></p> <p>예를 들어, USB HID(마우스 및 키보드) 디바이스(클래스 ID 0x03) 및 웹캠(클래스 ID 0x0e)을 허용하는 USB 인증 문자열은 <b>2203XXXX 220eXXXX</b>입니다. USB 대용량 스토리지 디바이스(클래스 ID 0x08)를 허용하지 않는 USB 비인증 문자열은 <b>2208XXXX</b>입니다.</p> <p>빈 USB 인증 문자열은 인증된 USB 디바이스가 없다는 뜻입니다. 빈 USB 비인증 문자열은 금지된 USB 디바이스가 없다는 뜻입니다.</p> <p>이 설정은 Horizon Agent에만 적용되며 원격 데스크톱이 Teradici 펌웨어를 실행하는 제로 클라이언트를 가진 세션에 있는 경우에만 적용됩니다. 디바이스 사용은 끝점 사이에서 협상됩니다.</p> <p>기본적으로 모든 디바이스가 허용되고 허용되지 않은 디바이스는 없습니다.</p>

설정	설명
Configure PCoIP virtual channels	<p>PCoIP 세션에서 작동할 수 있는 가상 채널 및 작동할 수 없는 가상 채널을 지정합니다. 또한 이 설정은 PCoIP 호스트에서 클립보드 처리를 사용하지 않도록 설정할지 여부를 결정합니다.</p> <p>PCoIP 세션에서 사용되는 가상 채널은 가상 채널 인증 목록에 나타나야 합니다. 인증되지 않은 가상 채널 목록에 나타나는 가상 채널은 PCoIP 세션에서 사용될 수 없습니다.</p> <p>PCoIP 세션에서 사용하기 위해 최대 15개의 가상 채널을 지정할 수 있습니다.</p> <p>여러 채널 이름을 세로 막대( ) 문자로 구분하십시오. 예를 들어, mksvchan 및 vdp_rdpvcbridge 가상 채널을 허용하는 가상 채널 인증 문자열은 <code>mksvchan vdp_vdpvcbridge</code>입니다.</p> <p>채널 이름이 세로 막대 또는 백슬래시(\) 문자를 포함할 경우, 그 앞에 백슬래시 문자를 삽입합니다. 예를 들어, 채널 이름 <code>awk ward\channel</code>을 <code>awk\\ward\\channel</code>로 입력하십시오.</p> <p>인증된 가상 채널 목록이 빈 경우, 모든 가상 채널이 허용되지 않습니다. 인증되지 않은 가상 채널 목록이 빈 경우, 모든 가상 채널이 허용됩니다.</p> <p>가상 채널 설정은 에이전트 및 클라이언트 모두에 적용됩니다. 가상 채널을 사용하려면 에이전트 및 클라이언트 모두에서 가상 채널을 사용하도록 설정해야 합니다.</p> <p>가상 채널 설정에는 PCoIP 호스트에서 원격 클립보드 처리를 사용하지 않도록 설정할 수 있는 개별 확인란이 있습니다. 이 값은 에이전트에만 적용됩니다.</p> <p>기본적으로 클립보드 처리를 포함한 모든 가상 채널이 사용되도록 설정됩니다.</p>
Configure the PCoIP transport header	<p>PCoIP 전송 헤더를 구성하고 전송 세션 우선 순위를 설정합니다.</p> <p>PCoIP 전송 헤더는 모든 PCoIP UDP 패킷에 추가(전송 헤더가 사용하도록 설정되어 있고 양쪽 모두에서 지원하는 경우에만 해당)되는 32비트 헤더입니다. PCoIP 전송 헤더는 네트워크 디바이스가 네트워크 정체를 처리할 때 더 효율적으로 우선 순위를 지정하거나 QoS를 결정할 수 있도록 지원합니다. 기본적으로 전송 헤더를 사용하도록 설정되어 있습니다.</p> <p>전송 세션 우선 순위는 PCoIP 전송 헤더에 보고되는 PCoIP 세션 우선 순위를 결정합니다. 네트워크 디바이스가 지정된 전송 세션 우선 순위에 따라 더 효율적으로 우선 순위를 지정하거나 QoS를 결정할 수 있도록 합니다.</p> <p>Configure the PCoIP transport header 설정을 사용하도록 설정한 경우 다음 전송 세션 우선 순위를 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ 높음</li> <li>■ 중간(기본값)</li> <li>■ 낮음</li> <li>■ 정의되지 않음</li> </ul> <p>PCoIP 에이전트와 클라이언트가 전송 세션 우선 순위 값을 협상합니다. PCoIP 에이전트가 전송 세션 우선 순위 값을 지정하면 세션이 에이전트에서 지정한 세션 우선 순위를 사용합니다. 클라이언트에서만 전송 세션 우선 순위를 지정한 경우 세션이 클라이언트에서 지정한 세션 우선 순위를 사용합니다. 에이전트와 클라이언트 모두 전송 세션 우선 순위를 지정하지 않았거나 <b>정의되지 않은 우선 순위</b>가 지정된 경우 세션이 기본 값인 <b>중간</b> 우선 순위를 사용합니다.</p>

설정	설명
Configure the TCP port to which the PCoIP host binds and listens	<p>소프트웨어 PCoIP 호스트로 바인딩된 TCP 에이전트 포트를 지정합니다.</p> <p>TCP 포트 값은 에이전트에서 바인딩하려고 시도하는 기본 TCP 포트를 지정합니다. TCP 포트 범위 값은 기본 포트를 사용할 수 없을 경우 시도할 추가 포트의 수를 결정합니다. 포트 범위는 1에서 10 사이여야 합니다.</p> <p>범위는 기본 포트에서 기본 포트 및 포트 범위의 합계까지 스패합니다. 예를 들어, 기본 포트가 4172이고 포트 범위가 10인 경우, 범위는 4172에서 4182까지 스패합니다.</p> <p>재시도 포트 범위 크기를 0으로 설정하지 마십시오. 이 값을 0으로 설정하면 사용자가 PCoIP 디스플레이 프로토콜을 사용하여 데스크톱에 로그인할 때 연결 장애가 발생합니다. Horizon Client에서 이 데스크톱의 디스플레이 프로토콜을 현재 사용할 수 없습니다. 시스템 관리자에게 문의하십시오라는 오류 메시지를 표시합니다.</p> <p>이 설정은 Horizon Agent에만 적용됩니다.</p> <p>단일 사용자 시스템의 경우 View 4.5 이상에서는 기본 TCP 포트가 기본적으로 4172입니다. View 4.0.x 및 그 이전 버전의 경우 기본 포트는 기본적으로 50002입니다. 기본적으로 포트 범위는 1입니다.</p> <p>RDS 호스트에서는 기본 TCP 포트가 기본적으로 4173이며, RDS 호스트에서 PCoIP를 사용하는 경우에는 각 사용자 연결마다 개별 PCoIP 포트가 사용됩니다. RDS에서 설정하는 기본 포트 범위는 예상되는 최대 동시 사용자 연결 수를 모두 지원할 정도로 범위가 넓습니다.</p> <p><b>중요</b> 이 정책 설정을 사용하여 RDS 호스트의 기본 포트 범위를 변경하거나, TCP 포트 값을 기본값인 4173 이외의 값으로 변경하지 않는 것이 좋습니다. TCP 포트 값을 4172로 설정하지 않는 것이 가장 중요합니다. 이 값을 4172로 다시 설정하면 RDS 세션에서 PCoIP의 성능에 영향을 줄 수 있습니다.</p>

설정	설명
Configure the UDP port to which the PCoIP host binds and listens	<p>소프트웨어 PCoIP 호스트로 바인딩된 UDP 에이전트 포트를 지정합니다.</p> <p>UDP 포트 값은 에이전트에서 바인딩하려고 시도하는 기본 UDP 포트를 지정합니다. UDP 포트 범위 값은 기본 포트를 사용할 수 없을 경우 시도할 추가 포트의 수를 결정합니다. 포트 범위는 1에서 10 사이여야 합니다.</p> <p>재시도 포트 범위 크기를 0으로 설정하지 마십시오. 이 값을 0으로 설정하면 사용자가 PCoIP 디스플레이 프로토콜을 사용하여 데스크톱에 로그인할 때 연결 장애가 발생합니다. Horizon Client에서 이 데스크톱의 디스플레이 프로토콜을 현재 사용할 수 없습니다. 시스템 관리자에게 문의하십시오.</p> <p>범위는 기본 포트에서 기본 포트 및 포트 범위의 합계까지 스패합니다. 예를 들어, 기본 포트가 4172이고 포트 범위가 10인 경우, 범위는 4172에서 4182까지 스패합니다.</p> <p>이 설정은 Horizon Agent에만 적용됩니다.</p> <p>단일 사용자 시스템의 경우 기본적으로 기본 UDP 포트는 View 4.5 이상에서는 4172이고, View 4.0.x 및 이전 버전에서는 50002입니다. 기본적으로 포트 범위는 10입니다.</p> <p>RDS 호스트에서는 기본 UDP 포트가 기본적으로 4173이며, RDS 호스트에서 PCoIP를 사용하는 경우에는 각 사용자 연결마다 개별 PCoIP 포트가 사용됩니다. RDS에서 설정하는 기본 포트 범위는 예상되는 최대 동시 사용자 연결 수를 모두 지원할 정도로 범위가 넓습니다.</p> <p><b>중요</b> 이 정책 설정을 사용하여 RDS 호스트의 기본 포트 범위를 변경하거나, UDP 포트 값을 기본값인 4173 이외의 값으로 변경하지 않는 것이 좋습니다. UDP 포트 값을 4172로 설정하지 않는 것이 가장 중요합니다. 이 값을 4172로 설정하면 RDS 세션에서 PCoIP의 성능에 영향을 줄 수 있습니다.</p>
Enable access to a PCoIP session from a vSphere console	<p>vSphere Client 콘솔이 활성 PCoIP 세션을 표시하고 데스크톱에 입력을 보내도록 허용할지 여부를 결정합니다.</p> <p>기본적으로 클라이언트가 PCoIP를 통해 연결되면 vSphere Client 콘솔 화면이 비어 있고 콘솔에서 입력을 보낼 수 없습니다. 기본 설정에서는 PCoIP 원격 세션이 활성화될 때 악성 사용자가 사용자의 데스크톱을 보거나 호스트에 로컬로 입력을 제공할 수 없습니다.</p> <p>이 설정은 Horizon Agent에만 적용됩니다.</p> <p>이 설정을 사용하지 않거나 구성되지 않은 경우, 콘솔 액세스가 허용되지 않습니다. 이 설정을 사용할 경우, 콘솔에 PCoIP 세션이 표시되며 콘솔 입력이 허용됩니다.</p> <p>이 설정이 사용되도록 설정되면 Windows 7 가상 시스템이 하드웨어 v8인 경우에만 Windows 7 시스템에서 실행 중인 PCoIP 세션을 콘솔에서 표시할 수 있습니다. 하드웨어 v8은 ESXi 5.0 이상에서만 사용할 수 있습니다. 반대로 Windows 7 시스템에 대한 콘솔 입력은 가상 시스템이 하드웨어 버전인 경우 허용됩니다.</p>
Enable/disable audio in the PCoIP session	<p>오디오가 PCoIP 세션에서 사용되도록 설정되었는지 확인합니다. 양 끝점에 오디오가 사용되도록 설정되어 있어야 합니다. 이 설정이 사용되도록 설정된 경우, PCoIP 오디오가 허용됩니다. 이 설정이 사용되지 않도록 설정된 경우 PCoIP 오디오가 사용되지 않도록 설정됩니다. 이 설정이 구성되지 않은 경우, 오디오가 기본적으로 사용되도록 설정됩니다.</p>

설정	설명
Enable/disable microphone noise and DC offset filter in PCoIP session	<p>PCoIP 세션 중 마이크 입력을 위해 마이크 노이즈 및 DC 오프셋 필터를 사용하도록 설정할지 여부를 결정합니다.</p> <p>이 설정은 Horizon Agent 및 Teradici 오디오 드라이버에만 적용됩니다.</p> <p>이 설정이 구성되지 않은 경우, Teradici 오디오 드라이버는 기본적으로 마이크 노이즈 및 DC 오프셋 필터를 사용합니다.</p>
Turn on PCoIP user default input language synchronization	<p>PCoIP 세션의 사용자를 위한 기본 입력 언어가 PCoIP 클라이언트 끝점의 기본 입력 언어와 동기화되었는지 확인합니다. 이 설정이 사용되도록 설정된 경우, 동기화가 허용됩니다. 이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우, 동기화가 허용되지 않습니다.</p> <p>이 설정은 Horizon Agent에만 적용됩니다.</p>
Configure SSL Connections to satisfy Security Tools	<p>SSL 세션 협상 연결의 설정 방법을 지정합니다.</p> <p>포트 스캐너를 충족하려면 이 'SSL 연결 구성' 설정을 사용하도록 설정하고 Horizon Agent에서 다음 작업을 완료하십시오.</p> <ol style="list-style-type: none"> <li>1 Microsoft 관리 콘솔에서 올바르게 명명되고 서명된 인증서를 로컬 시스템의 컴퓨터 계정에 대한 개인 저장소에 저장한 후 내보낼 수 있는 상태로 표시합니다.</li> <li>2 해당 인증서에 서명한 인증 기관에 대한 인증서를 신뢰할 수 있는 루트 인증서 저장소에 저장합니다.</li> <li>3 VMware View 5.1 및 이하 버전에 대한 연결을 사용하지 않도록 설정합니다.</li> <li>4 인증서 저장소에서만 인증서를 로드하도록 Horizon Agent를 구성합니다. 로컬 시스템에 대한 개인 저장소가 사용될 경우 1 및 2단계에서 다른 저장소 위치를 사용하지 않았으면 인증서 저장소 이름을 "MY" 및 "ROOT"(큰따옴표 제외)로 변경하지 않고 그대로 둡니다.</li> </ol> <p>결과 PCoIP Server는 포트 스캐너와 같은 Security Tools를 충족합니다.</p>
Configure SSL Protocols	<p>암호화된 SSL 연결이 설정되기 전에 특정 프로토콜의 사용을 제한하는 OpenSSL 프로토콜을 구성합니다. 프로토콜 목록은 콜론으로 구분된 하나 이상의 openssl 문자열로 구성됩니다. 모든 암호 문자열은 대소문자를 구분합니다.</p> <p>기본값은 'TLS1.1:TLS1.2'입니다.</p> <p>즉, TLS v1.1 및 TLS v1.2는 사용하도록 설정하고 SSL v2.0, SSLv3.0 및 TLS v1.0은 사용하지 않도록 설정함을 의미합니다.</p> <p>이 설정은 Horizon Agent 및 Horizon Client 둘 다에 적용됩니다.</p> <p>양쪽 모두에 설정된 경우 OpenSSL 프로토콜 협상 규칙을 따릅니다.</p>

## PCoIP 클립보드 설정

Horizon PCoIP ADMX 템플릿 파일에는 복사 및 붙여넣기 작업의 클립보드 설정을 구성하는 그룹 정책 설정이 포함되어 있습니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 가능한 관리자 기본값** 폴더에 있습니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **사용자 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 불가능한 관리자 설정** 폴더에도 있습니다.

표 5-9. PCoIP 클립보드 정책 설정

설정	설명
Configure clipboard memory size on server (in kilobytes)	<p>서버의 클립보드 메모리 크기 값을 킬로바이트 단위로 나타낸 값입니다. 클라이언트에도 클립보드 메모리 크기 값이 있습니다. 세션이 설정되면 서버는 클립보드 메모리 크기 값을 클라이언트로 보냅니다. 유효 클립보드 메모리 크기 값은 클라이언트와 서버의 클립보드 메모리 크기 값 중에서 작은 쪽입니다.</p> <p>지정할 수 있는 최솟값은 512킬로바이트이고 최댓값은 16,384킬로바이트입니다. 0을 지정하거나 값을 지정하지 않을 경우, 기본 서버 클립보드 메모리 크기는 1,024킬로바이트입니다.</p> <p>이 설정은 버전 7.0.1 이상과 Horizon Client 4.1 이상이 설치된 Windows, Linux 및 Mac 클라이언트에만 적용됩니다. 이전 릴리스에서의 클립보드 메모리 크기는 1MB입니다.</p> <p><b>참고</b> 클립보드 메모리 크기가 크면 네트워크에 따라 성능이 저하될 수 있습니다. VMware에서는 클립보드 메모리 크기를 16MB보다 크지 않은 값으로 설정할 것을 권장합니다.</p>
Configure clipboard redirection	<p>클립보드 리디렉션이 허용되는 방향을 결정합니다. 다음 값 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>클라이언트에서 에이전트로만 활성화</b>(클라이언트 시스템에서 원격 데스크톱으로 복사하여 붙여넣기만 가능)</li> <li>■ <b>양방향으로 비활성화</b></li> <li>■ <b>양방향으로 활성화</b></li> <li>■ <b>에이전트에서 클라이언트로만 활성화</b>(클라이언트 시스템에서 원격 데스크톱으로 복사하여 붙여넣기만 가능)</li> </ul> <p>클립보드 리디렉션이 가상 채널로 구현됩니다. 가상 채널이 사용되지 않도록 설정된 경우, 리디렉션이 작동하지 않습니다.</p> <p>이 설정은 Horizon Agent에만 적용됩니다.</p> <p>이 설정이 비활성화되어 있거나 구성되어 있지 않을 경우 기본값은 <b>클라이언트에서 에이전트로만 활성화</b>입니다.</p>
Filter text out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 서식 있는 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter images out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 이미지 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>

설정	설명
Filter Microsoft Office text data out of the incoming clipboard data	클라이언트에서 에이전트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 형식 데이터(BIFF12 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	클라이언트에서 에이전트로 가는 클립보드 데이터에서 Microsoft Office Chart 및 Smart Art 데이터(Art::GVML ClipFormat)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Microsoft Text Effects data out of the incoming clipboard data	클라이언트에서 에이전트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 효과 데이터(HTML 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter text out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Rich Text Format data out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 서식 있는 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter images out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 이미지 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Microsoft Office text data out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 형식 데이터(BIFF12 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.



설정	설명
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 Microsoft Office Chart 및 Smart Art 데이터(Art::GVML ClipFormat)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Microsoft Text Effects data out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 효과 데이터(HTML 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.

## PCoIP 대역폭 설정

Horizon PCoIP ADMX 템플릿 파일에는 PCoIP 대역폭 특성을 구성하는 그룹 정책 설정이 포함되어 있습니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 가능한 관리자 기본값** 폴더에 있습니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **사용자 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 불가능한 관리자 설정** 폴더에도 있습니다.

표 5-10. Horizon PCoIP 세션 대역폭 변수

설정	설명
Configure the maximum PCoIP session bandwidth	<p>PCoIP 세션에서 초당 킬로비트로 최대 대역폭을 지정합니다. 대역폭은 모든 이미지, 오디오, 가상 채널, USB 및 컨트롤 PCoIP 트래픽을 포함합니다.</p> <p>예상되는 동시 PCoIP 세션 수를 고려하여 이 값을 끝점이 연결되는 링크의 전체 용량으로 설정합니다. 예를 들어 4Mbit/s 인터넷 연결을 통해 연결하는 단일 사용자 VDI 구성(단일 PCoIP 세션)의 경우 이 값을 4Mbit로 설정하거나 다른 네트워크 트래픽에서 사용할 수 있는 양을 남겨 두기 위해 4Mbit보다 10% 적게 설정합니다. 여러 개의 동시 PCoIP 세션에서 링크를 공유하여 여러 VDI 사용자 또는 단일 RDS 구성을 형성할 것으로 예상되는 경우 그에 따라 설정을 조정할 수도 있습니다. 하지만 이 값을 낮게 설정하면 각 활성 세션의 최대 대역폭이 제한됩니다.</p> <p>이 값을 설정하면 에이전트가 링크 용량보다 더 높은 비율로 전송하지 못하도록 하여 과도한 패킷 손실 및 열악한 사용자 환경으로 이어지는 것을 방지합니다. 이 값은 대칭형입니다. 클라이언트 및 에이전트가 클라이언트 및 에이전트 쪽에 설정된 두 값 중 더 낮은 값을 강제로 사용하도록 합니다. 예를 들어 클라이언트에서 4Mbit/s 최대 대역폭 설정이 구성되어도 에이전트가 더 낮은 비율을 사용하여 전송하도록 강제됩니다.</p> <p>이 설정을 사용하지 않거나 끝점에 구성되지 않은 경우 끝점은 대역폭 제한을 부과하지 않습니다. 이 설정이 구성된 경우 설정은 끝점의 최대 대역폭 제약(초당 킬로비트)으로 사용됩니다.</p> <p>이 설정이 구성되지 않은 경우 기본값은 초당 900000 킬로비트입니다.</p> <p>이 설정은 Horizon Agent 및 클라이언트에 적용됩니다. 두 개의 끝점에서 설정이 다른 경우, 더 낮은 값이 사용됩니다.</p>
Configure the PCoIP session bandwidth floor	<p>PCoIP 세션으로 예약된 대역폭을 위해 초당 킬로비트로 더 낮은 제한을 지정합니다.</p> <p>이 설정은 끝점을 위해 예상된 최소 대역폭 전송률을 구성합니다. 이 설정을 사용하여 끝점을 위해 대역폭을 예약할 경우, 사용자는 대역폭을 사용할 수 있을 때까지 기다릴 필요가 없습니다(세션 응답을 항상시킴).</p> <p>모든 끝점을 위해 예약된 총 대역폭을 초과 가입하지 않았는지 확인하십시오. 구성에서 모든 연결을 위한 대역폭 총의 합계는 네트워크 용량을 초과하지 않아야 합니다.</p> <p>기본값은 0으로, 이는 최소 대역폭이 예약되어 있지 않음을 의미합니다. 이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우 예약된 최소 대역폭이 없습니다.</p> <p>이 설정은 Horizon Agent 및 클라이언트에 적용되지만 이 설정이 구성된 끝점에만 영향을 줍니다.</p> <p>활성 PCoIP 세션 도중 이 설정을 수정하면 변경 사항이 즉시 적용됩니다.</p>
Configure the PCoIP session MTU	<p>PCoIP 세션의 UDP 패킷을 위해 MTU(최대 전송 단위) 크기를 지정합니다. MTU 크기는 IP 및 UDP 패킷 머리글을 포함합니다. TCP는 표준 MTU 발견 메커니즘을 사용하여 MTU를 설정하며 이 설정으로 영향을 받지 않습니다. 최대 MTU 크기는 1500바이트입니다. 최소 MTU 크기는 500바이트입니다. 기본값은 1300바이트입니다.</p> <p>일반적으로 MTU 크기를 변경할 필요가 없습니다. 비정상적인 네트워크 설치로 인해 PCoIP 패킷 조각화가 발생할 경우 이 값을 변경하십시오.</p> <p>이 설정은 Horizon Agent 및 클라이언트에 적용됩니다. 두 개의 끝점에서 MTU 크기 설정이 다른 경우, 가장 작은 크기가 사용됩니다.</p> <p>이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우 클라이언트는 Horizon Agent와의 협상에서 기본값을 사용합니다.</p>

설정	설명
Configure the PCoIP session audio bandwidth limit	<p>PCoIP 세션에서 오디오(사운드 재생)에 사용될 수 있는 최대 대역폭을 지정합니다.</p> <p>오디오 처리는 오디오에 사용된 대역폭을 모니터링합니다. 현재 대역폭을 이 용한 경우 처리 과정에서 가능한 최고의 오디오를 제공하는 오디오 압축 알고리즘을 선택합니다. 대역폭 제한이 설정된 경우, 처리 과정에서 대역폭 제한에 도달할 때까지 압축 알고리즘 선택을 변경하여 품질이 저하됩니다. 최소 품질 오디오가 지정된 대역폭 제한 내에서 제공되지 않는다면 오디오가 사용되지 않도록 설정됩니다.</p> <p>압축되지 않은 고품질의 스테레오 오디오 재생을 허용하려면 이 값을 1600kbit/s보다 높게 설정하십시오. 450kbit/s 이상의 값은 고품질의 압축된 스테레오 오디오 재생을 허용합니다. 50kbit/s 및 450kbit/s 사이의 값을 사용하면 오디오는 FM 라디오 및 통화 품질 사이의 범위를 갖게 됩니다. 50kbit/s 보다 낮은 값으로는 오디오가 재생되지 않을 수 있습니다.</p> <p>이 설정은 Horizon Agent에만 적용됩니다. 이 설정이 적용되기 전에 양 끝점에서 오디오를 사용하도록 설정해야 합니다.</p> <p>또한 이 설정은 USB 오디오에 영향을 주지 않습니다.</p> <p>이 설정이 사용되지 않도록 설정되거나 구성되지 않은 경우, 초당 500킬로비트의 기본 오디오 대역폭 제한은 선택된 오디오 압축 알고리즘을 제약하도록 구성됩니다. 이 설정이 구성된 경우, 이 값은 초당 500킬로비트의 기본 오디오 대역폭 제한을 사용하여 초당 킬로비트로 측정됩니다.</p> <p>이 설정은 View 4.6 이상에 적용됩니다. 이전 버전의 View에는 적용되지 않습니다.</p> <p>활성 PCoIP 세션 도중 이 설정을 수정하면 변경 사항이 즉시 적용됩니다.</p>
Turn off Build-to-Lossless feature	<p>PCoIP 프로토콜의 무손실 빌드 기능을 사용할지 여부를 지정합니다. 이 기능은 기본적으로 사용되지 않습니다.</p> <p>이 설정을 사용하도록 설정하거나 구성하지 않은 경우 무손실 빌드 기능은 기본적으로 사용되지 않으며, 이미지와 기타 데스크톱 및 애플리케이션 콘텐츠는 무손실 상태로 빌드되지 않습니다. 대역폭이 제한된 네트워크 환경에서 무손실 빌드 기능을 사용하지 않도록 설정하면 대역폭을 절감할 수 있습니다.</p> <p>이 설정을 사용하지 않도록 설정하면 무손실 빌드 기능이 사용됩니다. 무손실 빌드 기능은 이미지와 기타 데스크톱 및 애플리케이션 콘텐츠를 무손실 상태로 빌드해야 하는 환경에서 사용하도록 설정하는 것이 좋습니다.</p> <p>활성 PCoIP 세션 도중 이 설정을 수정하면 변경 사항이 즉시 적용됩니다.</p> <p>PCoIP 무손실 빌드 기능에 대한 자세한 내용은 <a href="#">PCoIP 무손실 빌드 기능</a>에 나와 있습니다.</p>

## PCoIP 키보드 설정

View PCoIP ADMX 템플릿 파일에는 키보드 사용에 영향을 주는 PCoIP 설정을 구성하는 그룹 정책 설정이 포함되어 있습니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 가능한 관리자 기본값** 폴더에 있습니다.

이러한 모든 설정은 그룹 정책 관리 편집기의 **사용자 구성 > 정책 > 관리 템플릿 > PCoIP 세션 변수 > 재정의 불가능한 관리자 설정** 폴더에도 있습니다.

표 5-11. 키보드에 대한 Horizon PColP 세션 변수

설정	설명
Disable sending CAD when users press Ctrl+Alt+Del	<p>이 정책을 사용하도록 설정한 경우 사용자는 PColP 세션 중에 SAS(Secure Attention Sequence)를 원격 데스크톱에 보낼 때 Ctrl+Alt+Del 대신 Ctrl+Alt+Insert를 눌러야 합니다.</p> <p>Ctrl+Alt+Del 키를 눌러 클라이언트 끝점을 잠그고 SAS를 호스트 및 게스트 모두에게 보낼 때 사용자가 혼동할 경우 이 설정을 사용하도록 설정할 수 있습니다.</p> <p>이 설정은 Horizon Agent에만 적용되며 클라이언트에는 아무런 영향을 주지 않습니다.</p> <p>이 정책을 구성하지 않거나 사용하지 않도록 설정한 경우에는 사용자가 Ctrl+Alt+Del 또는 Ctrl+Alt+Insert를 눌러 SAS를 원격 데스크톱에 보낼 수 있습니다.</p>
Use alternate key for sending Secure Attention Sequence	<p>SAS(Secure Attention Sequence)를 보내기 위해 Insert 키 대신 대체 키를 지정합니다.</p> <p>이 설정을 사용하면 PColP 세션 중 원격 데스크톱 내부에서 실행되는 가상 시스템에서 사용할 수 있도록 Ctrl+Alt+Ins 키 순서를 보존할 수 있습니다. 예를 들어, 사용자는 PColP 데스크톱 내부에서 vSphere Client를 시작하고 vCenter Server의 가상 시스템에서 콘솔을 열 수 있습니다. Ctrl+Alt+Ins 순서가 vCenter Server 가상 시스템의 게스트 운영 체제 내에서 사용될 경우, Ctrl+Alt+Del SAS가 가상 시스템에 전송됩니다. 이 설정에서 Ctrl+Alt+ 대체 키 순서가 허용되어 Ctrl+Alt+Del SAS를 PColP 데스크톱으로 보냅니다.</p> <p>이 설정이 사용되도록 설정된 경우, 드롭다운 메뉴에서 대체 키를 선택해야 합니다. 설정을 사용하도록 설정하고 값을 지정하지 않은 상태로 둘 수 없습니다.</p> <p>이 설정이 사용되도록 설정되거나 구성되지 않은 경우, Ctrl+Alt+Ins 키 순서가 SAS로 사용됩니다.</p> <p>이 설정은 Horizon Agent에만 적용되며 클라이언트에는 아무런 영향을 주지 않습니다.</p>

## PColP 무손실 빌드 기능

제한된 네트워크 상태에서도 최적의 전체 사용자 환경을 제공하는 인코딩 접근법인 점진적 빌드 또는 무손실 빌드를 사용하도록 PColP 디스플레이 프로토콜을 구성할 수 있습니다. 이 기능은 기본적으로 사용되지 않습니다.

무손실 빌드 기능은 손실 이미지라고 불리는 고도로 압축된 초기 이미지를 제공하며, 이 이미지는 점진적으로 전체 무손실 상태로 빌드됩니다. 무손실 상태란 이미지가 원래의 고화질로 나타난다는 뜻입니다.

LAN에서 PColP는 항상 무손실 압축을 사용하여 텍스트를 표시합니다. 무손실 빌드 기능이 켜져 있는 경우 세션당 사용 가능한 대역폭이 1Mbps 아래로 떨어지면 PColP가 처음에 손실 텍스트 이미지를 표시했다가 빠르게 무손실 상태로 이미지를 빌드합니다. 이 방법을 사용하면 네트워크 상태가 변화하더라도 데스크톱이 응답성을 유지할 수 있으며 가능한 한 최상의 이미지를 표시하여 사용자에게 최적의 환경을 제공할 수 있습니다.

무손실 빌드 기능에는 다음과 같은 특징이 있습니다.

- 이미지 품질을 동적으로 조정
- 느린 네트워크에서 이미지 품질 감소
- 화면 업데이트 지연을 감소시켜 응답성 유지
- 네트워크의 지체가 해소될 경우 최대의 이미지 품질로 복귀

Turn off Build-to-Lossless feature 그룹 정책 설정을 사용하지 않도록 설정하여 무손실 빌드 기능을 설정할 수 있습니다. [PCoIP 대역폭 설정](#)의 내용을 참조하십시오.

## VMware Blast 정책 설정

VMware Blast 그룹 정책 ADMX 템플릿 파일 vdm\_blast.admx에는 VMware Blast 디스플레이 프로토콜에 대한 정책 설정이 포함되어 있습니다. 정책이 적용되고 나면 설정이 레지스트리 키 HKLM\Software\W\Policies\VMware, Inc.\VMware Blast\Wconfig에 저장됩니다.

이러한 설정은 HTML Access와 모든 Horizon Client에 적용됩니다.

표 5-12. VMware Blast 정책 설정

설정	설명
Max Session Bandwidth	VMware Blast 세션에 대해 초당 킬로비트(kbps)로 최대 대역폭을 지정합니다. 대역폭은 모든 이미지, 오디오, 가상 채널, USB 및 VMware Blast 제어 트래픽을 포함합니다. 기본값은 1Gbps입니다.
Min Session Bandwidth	VMware Blast 세션에 대해 예약된 최소 대역폭을 초당 킬로비트(kbps)로 지정합니다. 기본값은 256kbps입니다.
Max Bandwidth Slope for the Kbps Per Megapixel	VMware Blast 세션에 대해 예약된 최소 대역폭 기울기를 초당 킬로비트(kbps)로 지정합니다. 최솟값은 100입니다. 최댓값은 100000입니다. 기본값은 6200입니다.
Max Frame Rate	화면 업데이트의 최대 속도를 지정합니다. 사용자가 소비하는 평균 대역폭을 관리하려면 이 설정을 사용합니다. 기본값은 초당 30회 업데이트입니다.
UDP Protocol	UDP 프로토콜과 TCP 프로토콜 중에서 어느 것을 사용할지 지정합니다. 기본값은 UDP 프로토콜을 사용하는 것입니다. 이 설정을 사용하려면 레지스트리 키가 있는 Horizon Agent 시스템을 재부팅해야 합니다. 항상 TCP 프로토콜을 사용하는 HTML Access에는 이 설정이 적용되지 않습니다.
H264	H.264 인코딩과 JPEG/PNG 인코딩 중에서 어느 것을 사용할지 지정합니다. 기본값은 H.264 인코딩을 사용하는 것입니다.
PNG	이 설정을 사용하도록 설정하거나 구성하지 않으면 원격 세션에 PNG 인코딩을 사용할 수 있습니다. 이 설정을 사용하지 않도록 설정하면 JPEG/PNG 모드의 인코딩에 JPEG 인코딩만 사용됩니다. 이 정책은 H.264 인코더가 활성 상태일 때는 적용되지 않습니다. 이 설정은 기본적으로 구성되어 있지 않습니다. 이 설정은 7.0.2 이상에 적용됩니다.
Screen Blanking	데스크톱에 활성 세션이 있을 때 데스크톱 VM의 콘솔에 사용자에게 보이는 실제 데스크톱을 표시할지 아니면 빈 화면을 표시할지 지정합니다. 기본값은 빈 화면을 표시하는 것입니다.
Cookie Cleanup Interval	비활성 세션과 연결된 쿠키가 삭제되는 빈도(밀리초)를 결정합니다. 기본값은 100ms입니다.

설정	설명
Image Quality	<p>원격 디스플레이의 이미지 품질을 지정합니다. 두 개의 낮은 품질 설정, 두 개의 높은 품질 설정, 중간 품질 설정 하나를 지정할 수 있습니다. 낮은 품질 설정은 스크롤이 발생하는 경우와 같이 자주 변경되는 화면 영역에 사용됩니다. 높은 품질 설정은 더 정적이어서 이미지 품질이 더 좋은 화면 영역에 사용됩니다. 다음과 같은 설정을 지정할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>낮은 JPEG 품질</b>(사용 가능한 값 범위: 1 - 100, 기본값: 25)</li> <li>■ <b>낮은 JPEG 크로마 서브샘플링</b>(사용 가능한 값 범위: 4:1:0(최저), 4:1:1, 4:2:0, 4:2:2 및 4:4:4(최고), 기본값: 4:1:0)</li> <li>■ <b>중간 JPEG 품질</b>(사용 가능한 값 범위: 1 - 100, 기본값: 35)</li> <li>■ <b>높은 JPEG 품질</b>(사용 가능한 값 범위: 1 - 100, 기본값: 90)</li> <li>■ <b>높은 JPEG 크로마 서브샘플링</b>(사용 가능한 값 범위: 4:1:0(최저), 4:1:1, 4:2:0, 4:2:2 및 4:4:4(최고), 기본값: 4:4:4)</li> </ul>
H.264 Quality	<p>H.264 인코딩을 사용하도록 구성된 원격 디스플레이의 이미지 품질을 지정합니다. 무손실 압축에서 이미지를 얼마나 제어할지를 결정하는 최소 및 최대 양자화 값을 지정할 수 있습니다. 최소 양자화 값을 지정하면 최고 이미지 품질로 설정됩니다. 최대 양자화 값을 지정하면 최저 이미지 품질로 설정됩니다. 다음과 같은 설정을 지정할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>H264maxQP</b>(사용 가능한 값 범위: 0-51, 기본값: 36)</li> <li>■ <b>H264minQP</b>(사용 가능한 값 범위: 0-51, 기본값: 10)</li> </ul> <p>최상의 이미지 품질을 얻으려면 양자화 값을 사용 가능한 값 범위의 +5 또는 -5 이내로 설정합니다.</p>
HTTP Service	<p>보안 서버와 Access Point 장치 및 데스크톱 사이의 보안 통신(HTTPS)에 사용되는 포트를 지정합니다. 이 포트를 열어 두려면 방화벽을 구성해야 합니다. 기본값은 22443입니다.</p>
Audio playback	<p>원격 데스크톱에 대한 오디오 재생의 사용 여부를 지정합니다. 이 설정은 오디오 재생을 사용하도록 설정하는 데 사용하는 것입니다.</p>
Configure clipboard redirection	<p>클립보드 리디렉션에 허용할 수 있는 동작을 지정합니다. 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>■ <b>양방향으로 활성화</b></li> <li>■ <b>양방향으로 비활성화</b></li> <li>■ <b>클라이언트에서 서버로만 활성화</b>(클라이언트에서 데스크톱으로만 복사/붙여넣기가 가능합니다.)</li> <li>■ <b>서버에서 클라이언트로만 활성화</b>(데스크톱에서 클라이언트로만 복사/붙여넣기가 가능합니다.)</li> </ul> <p>기본값은 <b>클라이언트에서 서버로만 활성화</b>입니다.</p>
Clipboard memory size on server(in kilobytes)	<p>서버의 클립보드 메모리 크기 값을 킬로바이트 단위로 나타낸 값입니다. 클라이언트에도 클립보드 메모리 크기 값이 있습니다. 세션이 설정되면 서버는 클립보드 메모리 크기 값을 클라이언트로 보냅니다. 유효 클립보드 메모리 크기 값은 클라이언트와 서버의 클립보드 메모리 크기 값 중에서 작은 쪽입니다.</p> <p>지정할 수 있는 최솟값은 512킬로바이트이고 최댓값은 16,384킬로바이트입니다. 0을 지정하거나 값을 지정하지 않을 경우, 기본 서버 클립보드 메모리 크기는 1,024킬로바이트입니다.</p> <p>이 설정은 버전 7.0.1 이상과 Horizon Client 4.1 이상이 설치된 Windows, Linux 및 Mac 클라이언트에만 적용됩니다. 이전 릴리스에서의 클립보드 메모리 크기는 1MB입니다.</p> <p><b>참고</b> 클립보드 메모리 크기가 크면 네트워크에 따라 성능이 저하될 수 있습니다. VMware에서는 클립보드 메모리 크기를 16MB보다 크지 않은 값으로 설정할 것을 권장합니다.</p>
Keyboard locale synchronization	<p>클라이언트 키보드 로캘 목록 및 기본 키보드 로캘을 원격 데스크톱 또는 애플리케이션에 동기화할지 여부를 지정합니다. 이 설정이 사용되도록 설정되면 동기화가 됩니다. 이 설정은 Horizon Agent에만 적용됩니다.</p> <p><b>참고</b> 이 기능은 Windows용 Horizon Client에 대해서만 지원됩니다.</p>

설정	설명
Configure file transfer	<p>원격 데스크톱과 HTML Access 클라이언트 사이에서 파일을 전송할 때 허용 가능한 동작을 지정합니다. 다음 값 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>업로드 및 다운로드 모두 사용 안 함</b></li> <li>■ <b>업로드 및 다운로드 모두 사용</b></li> <li>■ <b>파일 업로드만 사용</b>(사용자는 클라이언트 시스템에서 원격 데스크톱으로만 파일을 업로드할 수 있습니다.)</li> <li>■ <b>파일 다운로드만 사용</b>(사용자는 원격 데스크톱에서 클라이언트 시스템으로만 파일을 다운로드할 수 있습니다.)</li> </ul> <p>기본값은 <b>파일 업로드만 사용</b>입니다.</p> <p>이 설정은 버전 7.0.1 이상과 HTML Access 4.1 이상에만 적용됩니다.</p>
Filter text out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 서식 있는 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter images out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 이미지 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter Microsoft Office text data out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 형식 데이터 (BIFF12 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 Microsoft Office Chart 및 Smart Art 데이터 (Art::GVML ClipFormat)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter Microsoft Text Effects data out of the incoming clipboard data	<p>클라이언트에서 에이전트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 효과 데이터 (HTML 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter text out of the outgoing clipboard data	<p>에이전트에서 클라이언트로 가는 클립보드 데이터에서 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>
Filter Rich Text Format data out of the outgoing clipboard data	<p>에이전트에서 클라이언트로 가는 클립보드 데이터에서 서식 있는 텍스트 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다.</p> <p>이 설정은 버전 7.0.2 이상에 적용됩니다.</p>



설정	설명
Filter images out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 이미지 데이터를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Microsoft Office text data out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 형식 데이터 (BIFF12 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 Microsoft Office Chart 및 Smart Art 데이터 (Art::GVML ClipFormat)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.
Filter Microsoft Text Effects data out of the outgoing clipboard data	에이전트에서 클라이언트로 가는 클립보드 데이터에서 Microsoft Office 텍스트 효과 데이터 (HTML 형식)를 필터링할지를 지정합니다. 이 설정이 사용하도록 설정되어 있고 확인란이 선택되어 있으면 데이터가 필터링됩니다. 이 설정이 사용하지 않도록 설정되어 있거나 구성되지 않은 경우에는 데이터가 허용됩니다. 이 설정은 버전 7.0.2 이상에 적용됩니다.

## VMware Blast 정책 설정 적용

클라이언트 세션 동안 다음 VMware Blast 정책이 변경되면 Horizon Client에서는 변경 내용을 감지한 후 즉시 새 설정을 적용합니다.

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

다른 모든 VMware Blast 정책의 경우 Microsoft GPO 업데이트 규칙이 적용됩니다. GPO는 수동으로 또는 Horizon Agent 시스템을 다시 시작하여 업데이트할 수 있습니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.

## VMware Blast에 대해 무손실 압축 사용

VMware Blast 디스플레이 프로토콜을 사용하도록 설정하여 점진적 빌드 또는 무손실 빌드라고 하는 인코딩 접근 방법을 사용할 수 있습니다. 이 기능은 손실 이미지라고 불리는 고도로 압축된 초기 이미지를 제공하며, 이 이미지는 점진적으로 전체 무손실 상태로 빌드됩니다. 무손실 상태란 이미지가 원래의 고화질로 나타난다는 뜻입니다.



VMware Blast에 대해 무손실 압축을 사용하도록 설정하려면 에이전트 시스템의 Windows 레지스트리에 있는 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config 폴더에서 EncoderBuildToPNG 키를 1로 설정합니다. 기본값은 0(사용 안 함)입니다. 이는 코덱이 무손실 형식인 PNG로 빌드되지 않음을 의미합니다.

EncoderBuildToPNG 키에 대한 구성 변경은 즉시 진행됩니다.

**참고** VMware Blast에 대해 무손실 압축을 사용하도록 설정하면 대역폭 및 CPU 사용량이 증가합니다. 무손실 압축이 필요한 경우 VMware Blast 대신 PCoIP 디스플레이 프로토콜을 사용하는 것이 좋습니다. PCoIP에 대해 무손실 압축을 구성하는 방법에 대한 자세한 내용은 [PCoIP 무손실 빌드 기능](#)을 참조하십시오.

## 원격 데스크톱 서비스 그룹 정책 사용

RDS(원격 데스크톱 서비스) 그룹 정책을 사용하면 RDS 호스트와 RDS 데스크톱 및 애플리케이션 세션의 구성과 성능을 제어할 수 있습니다. Horizon 7는 Horizon 7에서 지원하는 Microsoft RDS 그룹 정책이 포함된 ADMX 파일을 제공합니다.

Microsoft 그룹 정책보다는 Horizon 7 ADMX 파일에서 제공하는 이에 해당하는 그룹 정책을 사용하는 것이 좋습니다. 그 이유는 Horizon 7 그룹 정책은 Horizon 7 배포를 지원하도록 검증되었기 때문입니다.

## RDS 디바이스 단위 CAL 스토리지 구성

RDS 디바이스 단위 CAL 스토리지 옵션을 구성하여 CAL을 저장할 위치를 지정할 수 있습니다. 이 기능을 사용하면 CAL의 저장 여부를 결정할 수 있습니다.

Horizon RDS 배포에 Windows Server 2008과 Windows Server 2012 시스템이 모두 있는 경우와 같이, 디바이스 단위 CAL 기본 사용량보다 더 많이 사용해야 하는 경우가 있을 수 있습니다. 이 기능을 사용하면 Horizon RDS 배포에서 CAL을 효과적으로 사용할 수 있습니다. 즉, 이 기능은 발급된 라이선스를 저장하고 클라이언트에서 RDS 호스트에 연결하려고 할 때 라이선스를 제공하며, 라이선스 업그레이드가 있을 경우 다시 라이선스를 저장하여 이 목표를 달성합니다.

RDS 디바이스 단위 CAL은 Horizon Administrator에서 구성하거나 Horizon LDAP 데이터베이스에서 수동으로 구성할 수 있습니다.

### 절차

- 1 Horizon Administrator에서 **View 구성 > 전역 설정**을 클릭합니다.
- 2 [일반] 창에서 **편집**을 클릭합니다.

### 3 RDS 디바이스 단위 CAL 스토리지 옵션 드롭다운 메뉴에서 다음 구성 중 하나를 선택합니다.

옵션	설명
브로커에만 저장	디바이스 단위 CAL이 브로커에만 저장됩니다. <a href="#">참고</a> LDAP 항목, cs-enablerdslicensing=true 및 sendRdsLicense=false.
클라이언트와 브로커 모두에 저장	디바이스 단위 CAL이 클라이언트와 브로커 모두에 저장됩니다. <a href="#">참고</a> LDAP 항목 cs-enablerdslicensing=true 및 sendRdsLicense=true.
디바이스 단위 CAL을 저장하지 않음	디바이스 단위 CAL이 어느 위치에도 저장되지 않습니다. <a href="#">참고</a> LDAP 항목, cs-enablerdslicensing=false 및 sendRdsLicense=false.

### 4 확인을 클릭합니다.

## Active Directory에 원격 데스크톱 서비스 ADMX 파일 추가

Horizon 7 RDS ADMX 파일의 정책 설정을 Active Directory의 GPO(그룹 정책 개체)에 추가할 수 있습니다. 개별 RDS 호스트에 RDS ADMX 파일을 설치할 수도 있습니다.

#### 사전 요구 사항

- RDS 그룹 정책 설정에 대한 GPO를 생성하고 RDS 호스트를 포함하는 OU에 연결합니다.
- Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.

Windows 2012, Windows 2008 및 Windows 2003 Active Directory 버전에 따라 그룹 정책 관리 콘솔을 여는 방법이 다릅니다. [Horizon 7 그룹 정책에 대한 GPO 생성](#)을 참조하십시오.

#### 절차

- 1 Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip입니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일의 압축을 풀고 RDS ADMX 파일을 Active Directory 또는 RDS 호스트에 복사합니다.
  - a vmware\_rdsh.admx 및 vmware\_rdsh\_server.admx 파일과 ko-KR 폴더를 Active Directory 또는 RDS 호스트의 C:\Windows\PolicyDefinitions 폴더에 복사합니다.
  - b (선택 사항) 언어 리소스 파일 vmware\_rdsh.adml 및 vmware\_rdsh\_server.adml을 Active Directory 또는 RDS 호스트의 C:\Windows\PolicyDefinitions\에 있는 적절한 하위 폴더에 복사합니다.

### 3 Active Directory 호스트에서 그룹 정책 관리 편집기를 엽니다.

개별 RDS 호스트에서는 gpedit.msc 유틸리티를 사용하여 로컬 그룹 정책 편집기를 열 수 있습니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트** 폴더에 설치됩니다.

또한 일부 Horizon 7 RDS 그룹 정책 설정은 **사용자 구성 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트** 폴더에 설치됩니다.

### 4 (선택 사항) 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 폴더에서 그룹 정책 설정을 구성합니다.

## RDS 애플리케이션 호환성 설정

RDS 애플리케이션 호환성 그룹 정책 설정은 Windows Installer 호환성, 원격 데스크톱 IP 가상화, 네트워크 어댑터 선택, RDS 호스트 IP 주소의 사용 등을 제어합니다.

표 5-13. RDS 애플리케이션 호환성 그룹 정책 설정

설정	설명
Turn off Windows Installer RDS Compatibility	<p>이 정책 설정은 완전히 설치된 애플리케이션에 대해 Windows Installer RDS 호환성을 사용자별로 실행할지 여부를 지정합니다. Windows Installer는 한 번에 하나의 <b>msiexec</b> 프로세스 인스턴스를 실행하도록 허용합니다. Windows Installer RDS 호환성은 기본적으로 설정됩니다.</p> <p>이 정책 설정을 사용하는 경우 Windows Installer RDS 호환성이 사용되지 않고 한 번에 하나의 <b>msiexec</b> 프로세스 인스턴스만 실행할 수 있습니다.</p> <p>이 정책 설정을 사용하지 않거나 구성하지 않는 경우 Windows Installer RDS 호환성이 사용되며, 사용자 애플리케이션 설치당 여러 개의 요청이 대기열에 추가되어 <b>msiexec</b> 프로세스에서 순서대로 이를 처리합니다.</p>
Turn on Remote Desktop IP Virtualization	<p>이 정책 설정은 원격 데스크톱 IP 가상화의 사용 여부를 지정합니다.</p> <p>원격 데스크톱 IP 가상화는 기본적으로 사용되지 않습니다.</p> <p>이 정책 설정을 사용하는 경우 원격 데스크톱 IP 가상화가 사용됩니다. 이 설정을 적용할 모드를 선택할 수 있습니다. 프로그램마다 모드를 사용하려면 가상 IP 주소를 사용할 프로그램 목록을 입력해야 합니다. 프로그램 사이에 빈 줄 없이 한 줄에 하나의 프로그램을 입력합니다. 예:</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <pre>explorer.exe mstsc.exe</pre> </div> <p>이 정책 설정을 사용하지 않거나 구성하지 않는 경우 원격 데스크톱 IP 가상화가 사용되지 않습니다.</p>

설정	설명
Select the network adapter to be used for Remote Desktop IP Virtualization	<p>이 정책 설정은 가상 IP 주소에 사용될 네트워크 어댑터의 IP 주소와 네트워크 마스크를 지정합니다. IP 주소와 네트워크 마스크는 CIDR(클래스 없는 인터넷 도메인 라우팅 형식) 형식으로 입력해야 합니다. 예: 192.0.2.96/24.</p> <p>이 정책 설정을 사용하는 경우 지정한 IP 주소와 네트워크 마스크를 사용하여 가상 IP 주소에 사용되는 네트워크 어댑터가 선택됩니다.</p> <p>이 정책 설정을 사용하지 않거나 구성하지 않는 경우 원격 데스크톱 IP 가상화가 사용되지 않습니다. 원격 데스크톱 IP 가상화가 작동하기 위해서는 네트워크 어댑터를 반드시 구성해야 합니다.</p>
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	<p>이 정책 설정은 세션에서 가상 IP 주소를 사용할 수 없을 때 RDS 호스트의 IP 주소를 사용할지 여부를 지정합니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 가상 IP를 사용할 수 없으면 RDS 호스트의 IP 주소를 사용하지 않습니다. 세션에서는 네트워크 연결을 할 수 없게 됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않는 경우 가상 IP를 사용할 수 없으면 RDS 호스트의 IP 주소를 사용합니다.</p>

## RDS 연결 설정

RDS 연결 그룹 정책 설정을 사용하면 사용자가 RDS 호스트의 세션에 연결하기 위한 정책을 설정할 수 있습니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 연결** 폴더에 설치됩니다.

Horizon 7 RDS 그룹 정책 설정은 **사용자 구성 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 연결** 폴더에도 설치됩니다.

표 5-14. RDS 연결 그룹 정책 설정

설정	설명
Automatic reconnection	<p>원격 데스크톱 연결 클라이언트가 네트워크 연결이 일시적으로 끊어졌을 때 RDS 호스트의 세션에 자동으로 다시 연결하도록 허용할지 여부를 지정합니다. 기본적으로 최대 20번의 다시 연결 시도가 5초 간격으로 수행됩니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 데스크톱 연결을 실행하는 모든 클라이언트에서 해당 네트워크 연결이 끊어질 때마다 자동 다시 연결을 시도합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 클라이언트의 자동 다시 연결이 금지됩니다.</p> <p>이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 자동 다시 연결이 지정되지 않습니다. 하지만 사용자가 원격 데스크톱 연결의 <b>고급</b> 탭에서 <b>연결이 끊어지면 다시 연결</b> 확인란을 사용하여 자동 다시 연결을 구성할 수 있습니다.</p>
Allow users to connect remotely using Remote Desktop Services	<p>이 정책 설정은 원격 데스크톱 서비스를 사용하여 컴퓨터에 대한 원격 액세스를 구성합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 대상 컴퓨터에 있는 원격 데스크톱 사용자 그룹의 구성원인 사용자가 원격 데스크톱 서비스를 사용하여 대상 컴퓨터에 원격으로 연결할 수 있습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 사용자가 원격 데스크톱 서비스를 사용하여 대상 컴퓨터에 원격으로 연결할 수 없습니다. 대상 컴퓨터에서 현재 연결은 유지하지만 새로 들어오는 연결은 허용하지 않습니다.</p> <p>이 정책 설정을 구성하지 않는 경우에는 원격 데스크톱 서비스에서 대상 컴퓨터의 원격 데스크톱 설정을 사용하여 원격 연결을 허용할지 여부를 결정합니다. 이 설정은 <b>시스템 속성</b>의 <b>원격</b> 탭에 있습니다. 기본적으로 원격 연결은 허용되지 않습니다.</p> <p><b>참고</b> 컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; 원격 데스크톱 서비스 &gt; 원격 데스크톱 세션 호스트 &gt; 보안 폴더에 있는 "네트워크 수준 인증을 사용하여 원격 연결에 대한 사용자 인증 필요" 정책 설정을 구성하면 원격 데스크톱 서비스를 사용하여 원격으로 연결할 수 있는 클라이언트를 제한할 수 있습니다. 원격 데스크톱 세션 호스트 구성 도구의 <b>네트워크 어댑터</b> 탭에 있는 [최대 연결 수] 옵션을 구성하거나 컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; 원격 데스크톱 서비스 &gt; 원격 데스크톱 세션 호스트 &gt; 연결 폴더에 있는 "연결 개수 제한" 정책 설정을 구성하여 동시에 연결할 수 있는 사용자 수를 제한할 수 있습니다.</p>

설정	설명
Deny logoff of an administrator logged in to the console session	<p>이 정책 설정은 서버 콘솔에 원격으로 연결하려고 하는 관리자가 현재 콘솔에 로그인된 관리자를 로그오프할 수 있는지 여부를 결정합니다.</p> <p>이 정책은 현재 연결된 관리자가 다른 관리자에게 의해 로그오프되지 않도록 하려는 경우에 유용합니다. 연결된 관리자가 로그오프되면 이전에 저장되지 않은 데이터는 모두 손실됩니다.</p> <p>이 정책 설정을 사용하도록 설정하면 연결된 관리자 로그오프가 허용되지 않습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 연결된 관리자 로그오프가 허용됩니다.</p> <p><b>참고</b> 이 콘솔 세션을 세션 0이라고도 합니다. 콘솔 액세스 권한은 컴퓨터 필드 이름의 원격 데스크톱 연결 또는 명령줄에서 /console 스위치를 사용하여 확보할 수 있습니다.</p>
Configure keep-alive connection interval	<p>이 정책 설정을 사용하여 RDS 호스트의 세션 상태가 클라이언트 상태와 일치되도록 하는 연결 유지 간격을 입력할 수 있습니다.</p> <p>클라이언트가 RDS 호스트에서 연결이 끊어지면 클라이언트가 RDS 호스트에서 실제로 연결 해제되었더라도 RDS 호스트의 세션은 연결 해제된 상태로 변경되지 않고 활성 상태로 유지될 수 있습니다. 클라이언트가 동일한 RDS 호스트에 다시 로그인하면 새 세션이 설정되고(RDS 호스트가 여러 세션을 허용하도록 구성된 경우) 원래 세션은 여전히 활성 상태를 유지할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 연결 유지 간격을 입력해야 합니다. 연결 유지 간격에 따라 서버가 세션 상태를 확인하는 빈도(분)가 결정됩니다. 입력할 수 있는 값 범위는 1~999,999입니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 연결 유지 간격이 설정되지 않고 서버는 세션 상태를 확인하지 않습니다.</p>
Limit number of connections	<p>원격 데스크톱 서비스가 서버에 대한 동시 연결 수를 제한할지 여부를 지정합니다.</p> <p>이 설정을 사용하여 서버에서 활성 상태일 수 있는 원격 데스크톱 서비스 세션의 수를 제한할 수 있습니다. 이 수를 초과하면 연결을 시도하는 추가 사용자는 서버가 사용 중이므로 나중에 다시 시도하라는 오류 메시지를 받습니다. 세션 수를 제한하면 더 적은 수의 세션이 시스템 리소스를 요구하므로 성능이 향상됩니다. 기본적으로 RDS 호스트는 제한없는 수의 원격 데스크톱 서비스 세션을 허용하며, 관리용 원격 데스크톱은 2개의 원격 데스크톱 서비스 세션을 허용합니다.</p> <p>이 설정을 사용하려면 서버에 대해 최댓값으로 지정하려는 연결 수를 입력합니다. 제한없는 수의 연결을 지정하려면 999999를 입력합니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 최대 연결 수는 Windows 버전 및 서버에서 실행되는 원격 데스크톱 서비스 모드에 따라 지정된 수로 제한됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 연결 수에 대한 제한이 그룹 정책 수준에서 적용되지 않습니다.</p> <p><b>참고</b> 이 설정은 원격 데스크톱 세션 호스트 역할 서비스가 설치된 Windows 운영 체제가 실행되는 서버에 해당하는 RDS 호스트에서 사용하도록 고안되었습니다.</p>

설정	설명
Set rules for remote control of Remote Desktop Services user sessions	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 세션에서 허용되는 원격 제어 수준을 지정합니다.</p> <p>이 정책 설정을 사용하여 2가지 원격 제어 수준인 세션 보기 또는 모든 권한 중 하나를 선택할 수 있습니다. 세션 보기 권한이 있으면 원격 제어 사용자가 세션을 볼 수 있습니다. 모든 권한이 있으면 관리자는 세션과 상호 작용할 수 있습니다. 원격 제어는 사용자 권한을 사용하거나 사용하지 않고 설정할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 관리자는 지정된 규칙에 따라 사용자의 원격 데스크톱 서비스 세션과 원격으로 상호 작용할 수 있습니다. 이러한 규칙을 설정하려면 [옵션] 목록에서 원하는 수준의 제어 및 사용 권한을 선택합니다. 원격 제어를 사용하지 않도록 설정하려면 "원격 제어 사용하지 않음"을 선택합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 제어 규칙은 원격 데스크톱 세션 호스트 구성 도구의 <b>원격 제어</b> 탭에 제공되는 설정에 따라 결정됩니다. 기본적으로 원격 제어 사용자는 사용자의 권한이 있는 세션에 대해 모든 권한을 갖습니다.</p> <p><b>참고</b> 이 정책 설정은 컴퓨터 구성 및 사용자 구성 둘 다에 표시됩니다. 두 정책 설정이 모두 구성되면 컴퓨터 구성 정책 설정이 우선적으로 적용됩니다.</p>
Restrict Remote Desktop Services users to a single Remote Desktop Services session	<p>이 정책 설정을 사용하여 사용자를 단일 원격 데스크톱 서비스 세션으로 제한합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 데스크톱 서비스를 사용하여 원격으로 로그인하는 사용자는 해당 서버의 단일 세션(활성 또는 연결 해제 상태)으로 제한됩니다. 사용자가 연결 해제된 상태로 세션을 나가면 다음 로그인 시 해당 세션에 자동으로 다시 연결됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 사용자는 원격 데스크톱 서비스를 사용하여 제한없는 수의 동시 원격 연결을 만들 수 있습니다.</p> <p>이 정책 설정을 구성하지 않으면 원격 데스크톱 세션 호스트 구성 도구의 "사용자당 세션을 하나로 제한" 설정에 따라 사용자가 단일 원격 데스크톱 서비스 세션으로 제한되는지 결정됩니다.</p>

설정	설명
Allow remote start of unlisted programs	<p>이 정책 설정을 사용하여 원격 사용자가 원격 데스크톱 서비스 세션을 시작할 때 RDS 호스트에서 모든 프로그램을 시작할 수 있는지 또는 RemoteApp 프로그램 목록에 나열된 프로그램만 시작할 수 있는지를 지정합니다.</p> <p>RemoteApp 관리자 도구를 통해 RemoteApp 프로그램 목록을 생성하여 RDS 호스트에서 원격으로 시작할 수 있는 프로그램을 제어할 수 있습니다. 기본적으로 사용자가 원격 데스크톱 서비스 세션을 시작할 때 RemoteApp 프로그램 목록에 있는 프로그램만 시작할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 사용자는 원격 데스크톱 서비스 세션을 시작할 때 RDS 호스트의 모든 프로그램을 시작할 수 있습니다. 예를 들어 원격 사용자는 원격 데스크톱 연결 클라이언트를 사용하여 연결할 때 프로그램의 실행 파일 경로를 지정하여 프로그램을 시작할 수 있습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 사용자는 원격 데스크톱 서비스 세션을 시작할 때 RemoteApp 관리자의 RemoteApp 프로그램 목록에 나열된 프로그램만 시작할 수 있습니다.</p>
Turn off Fair Share CPU Scheduling	<p>CPU FSS(Fair Share Scheduling)는 세션 수와 각 세션에 요구되는 프로세서 시간을 기준으로 동일한 RDS 호스트의 모든 원격 데스크톱 서비스 세션에 프로세서 시간을 동적으로 분배합니다.</p> <p>이 정책 설정을 사용하는 경우 CPU FSS(Fair Share Scheduling)가 사용되지 않습니다.</p> <p>이 정책 설정을 사용하지 않거나 구성하지 않는 경우 CPU FSS(Fair Share Scheduling)가 사용됩니다.</p>

## RDS 디바이스 및 리소스 리디렉션 설정

RDS 디바이스 및 리소스 리디렉션 그룹 정책 설정은 원격 데스크톱 서비스 세션에서 클라이언트 컴퓨터의 디바이스와 리소스에 대한 액세스를 제어합니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 디바이스 및 리소스 리디렉션** 폴더에 설치됩니다.

Horizon 7 RDS 그룹 정책 설정은 **사용자 구성 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 디바이스 및 리소스 리디렉션** 폴더에도 설치됩니다.



표 5-15. RDS 디바이스 및 리소스 리디렉션 그룹 정책 설정

설정	설명
Allow audio and video playback redirection	<p>이 정책 설정을 사용하여 사용자가 원격 데스크톱 서비스 세션에서 원격 컴퓨터의 오디오 및 비디오 출력을 리디렉션할 수 있는 여부를 지정합니다.</p> <p>사용자는 RDS(원격 데스크톱 연결)의 [로컬 리소스] 탭에서 원격 오디오 설정을 구성하여 원격 컴퓨터의 오디오 출력을 재생할 위치를 지정할 수 있습니다. 사용자는 원격 컴퓨터 또는 로컬 컴퓨터에서 원격 오디오를 재생하도록 선택할 수 있습니다. 또한 오디오를 재생하지 않도록 선택할 수도 있습니다. 비디오 재생은 원격 데스크톱 프로토콜(.rdp) 파일에서 videoplayback 설정을 사용하여 구성할 수 있습니다. 기본적으로 비디오 재생은 사용되도록 설정됩니다.</p> <p>기본적으로 오디오 및 비디오 재생 리디렉션이 Windows Server 2008 R2, Windows Server 2008 또는 Windows Server 2003을 실행하는 컴퓨터에 연결될 때는 허용되지 않습니다. 기본적으로 오디오 및 비디오 재생 리디렉션이 Windows 7, Windows Vista 또는 Windows XP Professional을 실행하는 컴퓨터에 연결될 때 허용됩니다.</p> <p>이 정책 설정을 사용하도록 설정하면 오디오 및 비디오 재생 리디렉션이 허용됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 오디오 재생 리디렉션이 RDC에서 지정되거나 비디오 재생이 .rdp 파일에서 지정되더라도 오디오 및 비디오 재생 리디렉션이 허용되지 않습니다.</p> <p>이 정책 설정을 구성하지 않으면 원격 데스크톱 세션 호스트 구성 도구의 [클라이언트 설정] 탭에 제공되는 오디오 및 비디오 재생 설정에 따라 오디오 및 비디오 재생 리디렉션이 허용될지 여부가 결정됩니다.</p>
Allow audio recording redirection	<p>이 정책 설정을 사용하여 사용자가 원격 데스크톱 서비스 세션에서 원격 컴퓨터에 오디오를 녹음할 수 있는 여부를 지정합니다.</p> <p>사용자는 RDS(원격 데스크톱 연결)의 [로컬 리소스] 탭에서 원격 오디오 설정을 구성하여 원격 컴퓨터에 오디오를 녹음할 수 있는지 여부를 지정할 수 있습니다. 사용자는 기본 제공 마이크와 같은 로컬 컴퓨터의 오디오 입력 디바이스를 사용하여 오디오를 녹음할 수 있습니다.</p> <p>기본적으로 오디오 녹음 리디렉션은 Windows Server 2008 R2가 실행되는 컴퓨터에 연결할 경우에는 허용되지 않습니다. 기본적으로 오디오 녹음 리디렉션은 Windows 7이 실행되는 컴퓨터에 연결할 때 허용됩니다.</p> <p>이 정책 설정을 사용하도록 설정하면 오디오 녹음 리디렉션이 허용됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하는 경우 오디오 녹음 리디렉션이 RDC에 지정되었더라도 오디오 녹음 리디렉션은 허용되지 않습니다.</p> <p>이 정책 설정을 구성하지 않으면 원격 데스크톱 세션 호스트 구성 도구의 [클라이언트 설정] 탭에 제공되는 오디오 녹음 설정에 따라 오디오 녹음 리디렉션이 허용될지 여부가 결정됩니다.</p>

설정	설명
Limit audio playback quality	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 세션에 대한 오디오 재생 품질을 제한합니다. 오디오 재생 품질을 제한하면 특히 느린 링크를 통한 연결 성능을 향상시킬 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 높음, 중간 또는 동적 중에서도 하나를 선택할 수 있습니다. [높음]을 선택하면 오디오는 압축되지 않고 최소의 지연 시간으로 전송됩니다. 이 경우 많은 양의 대역폭이 필요합니다. [중간]을 선택하면 오디오는 약간 압축되고 사용 중인 코덱에 따라 결정되는 최소의 지연 시간으로 전송됩니다. [동적]을 선택하면 오디오는 원격 연결의 대역폭에 따라 결정되는 수준만큼 압축되어 전송됩니다.</p> <p>이 정책 설정을 사용하여 원격 컴퓨터에 지정하는 오디오 재생 품질은 클라이언트 컴퓨터에 구성된 오디오 재생 품질에 관계없이 원격 데스크톱 서비스 세션에서 사용될 수 있는 최대 품질입니다. 예를 들어 클라이언트 컴퓨터에 구성된 오디오 재생 품질이 원격 컴퓨터에 구성된 오디오 재생 품질보다 높으면 더 낮은 수준의 오디오 재생 품질이 사용됩니다.</p> <p>오디오 재생 품질은 원격 데스크톱 프로토콜(.rdp) 파일의 audioqualitymode 설정을 사용하여 클라이언트 컴퓨터에서 구성할 수 있습니다. 기본적으로 오디오 재생 품질은 [동적]으로 설정됩니다.</p>
Do not allow clipboard redirection	<p>원격 데스크톱 서비스 세션 동안 원격 컴퓨터와 클라이언트 컴퓨터 간에 클립보드 내용(클립보드 리디렉션) 공유 금지 여부를 지정합니다.</p> <p>이 설정을 사용하여 사용자가 클립보드 데이터를 원격 컴퓨터 및 로컬 컴퓨터 간에 리디렉션하지 못하게 할 수 있습니다. 기본적으로 원격 데스크톱 서비스는 클립보드 리디렉션을 허용합니다.</p> <p>이 설정을 사용하도록 설정하면 사용자가 클립보드 데이터를 리디렉션할 수 없습니다.</p> <p>이 설정을 사용하지 않도록 설정하는 경우 원격 데스크톱 서비스는 항상 클립보드 리디렉션을 허용합니다.</p> <p>이 설정을 구성하지 않으면 그룹 정책 수준에서 클립보드 리디렉션이 지정되지 않습니다. 하지만 관리자는 원격 데스크톱 세션 호스트 구성 도구를 사용하여 클립보드 리디렉션을 여전히 사용하지 않도록 설정할 수 있습니다.</p>
Do not allow COM port redirection	<p>원격 데스크톱 서비스 세션의 원격 컴퓨터에서 클라이언트 COM 포트로의 데이터 리디렉션을 금지할지 여부를 지정합니다.</p> <p>이 설정을 사용하여 원격 데스크톱 서비스 세션에 로그인된 상태에서 COM 포트 주변 장치로의 데이터 리디렉션 또는 로컬 COM 포트 매핑을 금지할 수 있습니다. 기본적으로 원격 데스크톱 서비스는 이 COM 포트 리디렉션을 허용합니다.</p> <p>이 설정을 사용하도록 설정하면 사용자가 로컬 COM 포트에 서버 데이터를 리디렉션할 수 없습니다.</p> <p>이 설정을 사용하지 않도록 설정하는 경우 원격 데스크톱 서비스는 항상 COM 포트 리디렉션을 허용합니다.</p> <p>이 설정을 구성하지 않으면 그룹 정책 수준에서 COM 포트 리디렉션이 지정되지 않습니다. 하지만 관리자는 원격 데스크톱 세션 호스트 구성 도구를 사용하여 COM 포트 리디렉션을 여전히 사용하지 않도록 설정할 수 있습니다.</p>

설정	설명
Do not allow drive redirection	<p>원격 데스크톱 서비스 세션에서 클라이언트 드라이브의 매핑을 금지할지 여부를 지정합니다(드라이브 리디렉션).</p> <p>기본적으로 RD 세션 호스트 서버는 연결 시 클라이언트 드라이브를 자동으로 매핑합니다. 매핑된 드라이브는 Windows 탐색기 또는 컴퓨터의 세션 폴더에서 &lt;컴퓨터 이름&gt;의 &lt;드라이브 문자&gt; 형식으로 나타납니다. 이 설정을 사용하여 이 동작을 재정의할 수 있습니다.</p> <p>이 설정을 사용하도록 설정하면 원격 데스크톱 서비스 세션에서 클라이언트 드라이브 리디렉션이 허용되지 않습니다.</p> <p>이 설정을 사용하지 않도록 설정하는 경우 클라이언트 드라이브 리디렉션은 항상 허용됩니다.</p> <p>이 설정을 구성하지 않으면 그룹 정책 수준에서 클라이언트 드라이브 리디렉션이 지정되지 않습니다. 하지만 관리자는 원격 데스크톱 세션 호스트 구성 도구를 사용하여 클라이언트 드라이브 리디렉션을 여전히 사용하지 않도록 설정할 수 있습니다.</p>
Do not allow LTP Port redirection	<p>원격 데스크톱 서비스 세션 동안 클라이언트 LPT 포트로의 데이터 리디렉션을 금지할지 여부를 지정합니다.</p> <p>이 설정을 사용하여 로컬 LPT 포트를 매핑하고 원격 컴퓨터의 데이터를 로컬 LPT 포트 주변 장치로 리디렉션하지 못하게 할 수 있습니다. 기본적으로 원격 데스크톱 서비스는 이 LPT 포트 리디렉션을 허용합니다.</p> <p>이 설정을 사용하도록 설정하면 원격 데스크톱 서비스 세션의 사용자가 서버 데이터를 로컬 LPT 포트에 리디렉션할 수 없습니다. 이 설정을 사용하지 않도록 설정하는 경우 LPT 포트 리디렉션은 항상 허용됩니다.</p> <p>이 설정을 구성하지 않으면 그룹 정책 수준에서 LPT 포트 리디렉션이 지정되지 않습니다. 하지만 관리자는 원격 데스크톱 세션 호스트 구성 도구를 사용하여 로컬 LPT 포트 리디렉션을 여전히 사용하지 않도록 설정할 수 있습니다.</p>
Do not allow supported Plug and Play device redirection	<p>이 정책 설정을 사용하여 Windows 휴대용 장치와 같은 지원되는 플러그 앤 플레이 디바이스에서 원격 데스크톱 서비스 세션의 원격 컴퓨터로의 리디렉션을 제어합니다.</p> <p>기본적으로 원격 데스크톱 서비스는 지원되는 플러그 앤 플레이 디바이스의 리디렉션을 허용합니다. 사용자는 원격 데스크톱 연결의 [로컬 리소스] 탭에 있는 "자세히" 옵션을 사용하여 원격 컴퓨터로 리디렉션할 지원되는 플러그 앤 플레이 디바이스를 선택할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 사용자는 지원되는 플러그 앤 플레이 디바이스를 원격 컴퓨터로 리디렉션할 수 없습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 이 정책 설정을 구성하지 않으면 사용자는 지원되는 플러그 앤 플레이 디바이스를 원격 컴퓨터로 리디렉션할 수 있습니다.</p> <p><b>참고</b> 원격 데스크톱 세션 호스트 구성 도구의 [클라이언트 설정] 탭에서 지원되는 플러그 앤 플레이 디바이스의 리디렉션을 허용하지 않을 수 있습니다. <b>컴퓨터 구성 &gt; 관리 템플릿 &gt; 시스템 &gt; 장치 설치 &gt; 장치 설치 제한</b> 폴더의 정책 설정을 사용하여 특정 유형의 지원되는 플러그 앤 플레이 디바이스에 대한 리디렉션을 허용하지 않을 수 있습니다.</p>

설정	설명
Do not allow smart card device redirection	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 세션의 스마트 카드 디바이스에 대한 리디렉션을 제어합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 데스크톱 서비스 사용자는 스마트 카드를 사용하여 원격 데스크톱 서비스 세션에 로그인할 수 없습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 스마트 카드 디바이스 리디렉션이 허용됩니다. 기본적으로 원격 데스크톱 서비스는 연결 시 자동으로 스마트 카드 디바이스를 리디렉션합니다.</p> <p><b>참고</b> 클라이언트 컴퓨터는 Microsoft Windows 2000 Server 이상 또는 Microsoft Windows XP Professional 이상에서 실행되어야 하며 대상 서버가 도메인에 가입되어야 합니다.</p>
Allow time zone redirection	<p>클라이언트 컴퓨터가 표준 시간대 설정을 원격 데스크톱 서비스 세션에 리디렉션할지 여부를 결정합니다.</p> <p>이 정책 설정을 사용하는 경우 표준 시간대 리디렉션을 사용할 수 있는 클라이언트가 표준 시간대 정보를 서버로 보냅니다. 이렇게 하면, 서버의 기준 시간을 사용하여 현재 세션 시간(현재 세션 시간 = 서버 기준 시간 + 클라이언트 표준 시간대)이 계산됩니다.</p> <p>이 정책 설정을 사용하지 않거나 구성하지 않으면 클라이언트 컴퓨터에서 표준 시간대 정보를 리디렉션하지 않으며 세션 표준 시간대가 서버 표준 시간대와 같습니다.</p>

## RDS 라이선싱 설정

RDS 라이선싱 그룹 정책 설정은 RDS 라이선스 서버를 찾는 순서, 문제 알림을 표시할지 여부, RDS CAL(클라이언트 액세스 라이선스)에 사용자 단위 또는 디바이스 단위 라이선싱을 사용할지 여부 등을 제어합니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 라이선스** 폴더에 설치됩니다.

표 5-16. RDS 라이선싱 그룹 정책 설정

설정	설명
Use the specified Remote Desktop license servers	<p>이 정책 설정으로 RDS 호스트 서버가 원격 데스크톱 라이선스 서버를 찾는 순서를 지정할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 RDS 호스트 서버는 사용자가 지정한 라이선스 서버를 먼저 찾으려고 시도합니다. 지정된 라이선스 서버를 찾을 수 없는 경우 RDS 호스트 서버는 자동 라이선스 서버 검색을 시도합니다.</p> <p>자동 라이선스 서버 검색 프로세스에서 Windows Server 기반 도메인의 RDS 호스트 서버는 다음 순서에 따라 라이선스 서버에 연결하려고 시도합니다.</p> <ol style="list-style-type: none"> <li>1 원격 데스크톱 세션 호스트 구성 도구에 지정된 라이선스 서버</li> <li>2 Active Directory 도메인 서비스에 게시된 라이선스 서버</li> <li>3 RDS 호스트와 같은 도메인에 있는 도메인 컨트롤러에 설치된 라이선스 서버</li> </ol> <p>이 정책 설정을 사용하도록 설정하지 않거나 구성하지 않는 경우 RDS 호스트는 원격 데스크톱 세션 호스트 구성 도구에 지정된 라이선스 서버 검색 모드를 사용합니다.</p>
Hide notifications about RD Licensing problems that affect the RD Session Host server	<p>이 정책 설정은 RDS 호스트에 영향을 주는 RD 라이선스에 문제가 있을 경우 RDS 호스트에 알림을 표시할지 여부를 지정합니다.</p> <p>기본적으로 RDS 호스트에 영향을 주는 RD 라이선스에 문제가 있을 경우 로컬 관리자로 로그인하면 RDS 호스트에 알림이 표시됩니다. 또한 해당하는 경우 RDS 호스트의 라이선스 유예 기간이 만료되기까지 남은 일수를 알려 주는 알림도 표시됩니다.</p> <p>이 정책 설정을 사용하는 경우 RDS 호스트에 이러한 알림이 표시되지 않습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않는 경우 로컬 관리자로 로그인하면 RDS 호스트에 이러한 알림이 표시됩니다.</p>
Set the Remote Desktop licensing mode	<p>이 정책 설정으로 이 RDS 호스트에 연결하는 데 필요한 RDS CAL(원격 데스크톱 서비스 클라이언트 액세스 라이선스) 유형을 지정할 수 있습니다.</p> <p>이 정책 설정을 사용하여 사용자 단위 또는 디바이스 단위의 두 가지 라이선스 모드 중에 하나를 선택할 수 있습니다.</p> <p>사용자 단위 라이선스 모드를 사용하려면 이 RDS 호스트에 연결하는 각 사용자 계정에 RDS 사용자 단위 CAL이 있어야 합니다.</p> <p>디바이스 단위 라이선스 모드를 사용하려면 이 RDS 호스트에 연결하는 각 디바이스에 RDS 디바이스 단위 CAL이 있어야 합니다.</p> <p>이 정책 설정을 사용하는 경우 이 설정에서 지정된 라이선스 모드가 원격 데스크톱 세션 호스트 설치 중에 지정된 라이선스 모드 또는 원격 데스크톱 세션 호스트 구성 도구에 지정된 라이선스 모드보다 우선적으로 적용됩니다.</p> <p>이 정책 설정을 사용하지 않거나 구성하지 않는 경우 원격 데스크톱 세션 호스트 역할 서비스 설치 중에 지정된 라이선스 모드 또는 원격 데스크톱 세션 호스트 구성 도구에 지정된 라이선스 모드가 사용됩니다.</p>

## RDS 프린터 리디렉션 설정

RDS 프린터 리디렉션 그룹 정책 설정을 사용하면 프린터 리디렉션에 대한 정책을 구성할 수 있습니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 프린터 리디렉션** 폴더에 설치됩니다.

Horizon 7 RDS 그룹 정책 설정은 **사용자 구성 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 프린터 리디렉션** 폴더에도 설치됩니다.

표 5-17. RDS 프린터 리디렉션 그룹 정책 설정

설정	설명
Do not set default client printer to be default printer in a session	<p>이 정책 설정을 사용하여 클라이언트 기본 프린터를 RDS 호스트의 세션에서 기본 프린터로 자동으로 설정할지 여부를 지정합니다.</p> <p>기본적으로 원격 데스크톱 서비스는 클라이언트 기본 프린터를 RDS 호스트의 세션에서 기본 프린터로 자동으로 지정합니다. 이 정책 설정을 사용하여 이 동작을 재정의할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 기본 프린터는 원격 컴퓨터에 지정된 프린터가 됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 RDS 호스트는 연결 시에 클라이언트 기본 프린터를 자동으로 매핑하고 기본 프린터로 설정합니다.</p> <p>이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 기본 프린터가 지정되지 않습니다. 하지만 관리자는 원격 데스크톱 세션 호스트 구성 도구를 사용하여 클라이언트 세션에 대한 기본 프린터를 구성할 수 있습니다.</p>
Do not allow client printer redirection	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 세션에서 클라이언트 프린터의 매핑을 금지할지 여부를 지정합니다.</p> <p>이 정책 설정을 사용하여 사용자가 원격 컴퓨터의 인쇄 작업을 로컬(클라이언트) 컴퓨터에 연결된 프린터로 리디렉션하지 못하게 할 수 있습니다. 기본적으로 원격 데스크톱 서비스는 이 클라이언트 프린터 매핑을 허용합니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 사용자는 원격 데스크톱 서비스 세션에서 원격 컴퓨터의 인쇄 작업을 로컬 클라이언트 프린터로 리디렉션할 수 없습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하는 경우 사용자는 클라이언트 프린터를 매핑하여 인쇄 작업을 리디렉션할 수 있습니다.</p> <p>이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 클라이언트 프린터 매핑이 지정되지 않습니다. 하지만 관리자는 원격 데스크톱 세션 호스트 구성 도구를 사용하여 클라이언트 프린터 매핑을 여전히 사용하지 않도록 설정할 수 있습니다.</p>

설정	설명
Use Remote Desktop Easy Print printer driver first	<p>이 정책 설정을 사용하여 모든 클라이언트 프린터를 설치할 때 먼저 원격 데스크톱 간편 인쇄 프린터 드라이버를 사용할지 여부를 지정합니다.</p> <p>이 정책 설정을 사용하도록 설정하거나 구성하지 않으면 RDS 호스트는 먼저 원격 데스크톱 간편 인쇄 프린터 드라이버를 사용하여 모든 클라이언트 프린터를 설치하려고 합니다. 어떤 이유로든 원격 데스크톱 간편 인쇄 프린터 드라이버를 사용할 수 없으면 클라이언트 프린터와 일치하는 RDS 호스트의 프린터 드라이버가 사용됩니다. RDS 호스트에 클라이언트 프린터와 일치하는 프린터 드라이버가 없으면 해당 클라이언트 프린터를 원격 데스크톱 세션에 사용할 수 없습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 RDS 호스트는 클라이언트 프린터 설치에 적합한 프린터 드라이버를 찾으려고 합니다. RDS 호스트에 클라이언트 프린터와 일치하는 프린터 드라이버가 없으면 RDS 호스트는 원격 데스크톱 간편 인쇄 드라이버를 사용하여 클라이언트 프린터를 설치하려고 합니다. 어떤 이유로든 원격 데스크톱 간편 인쇄 프린터 드라이버를 사용할 수 없으면 해당 클라이언트 프린터를 원격 데스크톱 서비스 세션에 사용할 수 없습니다.</p> <p><b>참고</b> “클라이언트 프린터의 리디렉션을 허용하지 않음” 정책 설정을 사용하도록 설정하는 경우 “원격 데스크톱 간편 인쇄 프린터 드라이버 우선 사용” 정책 설정은 무시됩니다.</p>

설정	설명
Specify RD Session Host Server fallback printer driver behavior	<p>이 정책 설정을 사용하여 RDS 호스트 폴백 프린터 드라이버 동작을 지정합니다.</p> <p>기본적으로 RDS 호스트 폴백 프린터 드라이버는 사용되지 않도록 설정됩니다. RDS 호스트에 클라이언트 프린터와 일치하는 프린터 드라이버가 없으면 원격 데스크톱 서비스 세션에 사용할 수 있는 프린터가 없습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 폴백 프린터 드라이버가 사용되도록 설정되며 기본 동작은 RDS 호스트가 적절한 프린터 드라이버를 찾는 것입니다. 프린터 드라이버를 찾을 수 없으면 해당 클라이언트의 프린터를 사용할 수 없습니다. 이 기본 동작을 변경하도록 선택할 수 있습니다. 사용 가능한 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>■ Do nothing if one is not found. 프린터 드라이버 불일치가 나타나면 RDS 호스트는 적절한 드라이버를 찾으려고 합니다. 프린터 드라이버를 찾을 수 없으면 해당 클라이언트의 프린터를 사용할 수 없습니다. 기본 동작입니다.</li> <li>■ Default to PCL if one is not found. 적절한 프린터 드라이버를 찾을 수 없으면 기본적으로 PCL(프린터 제어 언어) 폴백 프린터 드라이버가 사용됩니다.</li> <li>■ Default to PS if one is not found. 적절한 프린터 드라이버를 찾을 수 없으면 기본적으로 PS(PostScript) 폴백 프린터 드라이버가 사용됩니다.</li> <li>■ Show both PCL and PS if one is not found. 적절한 드라이버를 찾을 수 없으면 PS 및 PCL 기반 폴백 프린터 드라이버가 둘 다 표시됩니다.</li> </ul> <p>이 정책 설정을 사용하지 않도록 설정하면 RDS 호스트 폴백 드라이버는 사용되지 않도록 설정되고 RDS 호스트는 폴백 프린터 드라이버를 사용하려고 시도하지 않습니다.</p> <p>이 정책 설정을 구성하지 않으면 폴백 프린터 드라이버 동작은 기본적으로 해제됩니다.</p> <p><b>참고</b> "클라이언트 프린터의 리디렉션을 허용하지 않음" 설정이 사용되도록 설정되면 이 정책 설정은 무시되고 폴백 프린터 드라이버는 사용되지 않도록 설정됩니다.</p>
Redirect only the default client printer	<p>이 정책 설정을 사용하여 기본 클라이언트 프린터가 원격 데스크톱 서비스 세션에서 리디렉션되는 유일한 프린터인지 여부를 지정합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 데스크톱 서비스 세션에서 기본 클라이언트 프린터만 리디렉션됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 데스크톱 서비스 세션에서 모든 클라이언트 프린터가 리디렉션됩니다.</p>

## RDS 프로파일 설정

RDS 프로파일 그룹 정책 설정은 원격 데스크톱 서비스 세션의 로밍 프로파일 및 홈 디렉토리 설정을 제어합니다.



표 5-18. RDS 프로파일 그룹 정책 설정

설정	설명
Limit the size of the entire roaming user profile cache	<p>이 정책 설정으로 로컬 드라이브에 있는 전체 로밍 사용자 프로파일 캐시 크기를 제한할 수 있습니다. 이 정책 설정은 원격 데스크톱 세션 호스트 역할 서비스가 설치되어 있는 컴퓨터에만 적용됩니다.</p> <p><b>참고</b> 개별 사용자 프로파일의 크기를 제한하려면 <b>사용자 구성\정책\관리 템플릿\시스템\사용자 프로파일</b>에 있는 Limit profile size 정책 설정을 사용하십시오.</p> <p>이 정책 설정을 사용하는 경우 전체 로밍 사용자 프로파일 캐시에 대한 모니터링 간격(분)과 최대 크기(GB)를 지정해야 합니다. 모니터링 간격에 따라 전체 로밍 사용자 프로파일 캐시의 크기를 확인하는 빈도가 결정됩니다. 전체 로밍 사용자 프로파일 캐시의 크기가 지정된 최대 크기를 초과하면 전체 로밍 사용자 프로파일 캐시의 크기가 지정된 최대 크기보다 작아질 때까지 가장 오래된(가장 오래 전에 액세스한) 로밍 사용자 프로파일이 삭제됩니다.</p> <p>이 정책 설정을 사용하지 않거나 구성하지 않는 경우 로컬 드라이브의 전체 로밍 사용자 프로파일 캐시 크기에 제한이 설정되지 않습니다.</p> <p><b>참고:</b> <b>컴퓨터 구성\정책\관리 템플릿\시스템\사용자 프로파일</b>에 있는 Prevent Roaming Profile changes from propagating to the server 정책 설정이 사용되도록 설정될 경우 이 정책 설정이 무시됩니다.</p>
Set Remote Desktop Services User Home Directory	<p>원격 데스크톱 서비스에서 지정한 네트워크 공유 또는 로컬 디렉토리 경로를 원격 데스크톱 서비스 세션의 사용자 홈 디렉토리 루트로 사용할지 여부를 지정합니다.</p> <p>이 설정을 사용하려면 위치 드롭다운 목록에서 홈 디렉토리(네트워크 또는 로컬)의 위치를 선택합니다. 디렉토리를 네트워크 공유로 지정하려면 <b>\\\\컴퓨터 이름\공유 이름</b> 형식으로 홈 디렉토리 루트 경로를 입력한 후 네트워크 공유를 매핑할 드라이브 문자를 선택합니다.</p> <p>홈 디렉토리를 로컬 컴퓨터에 유지하려면 환경 변수나 줄임표를 사용하지 않고 <b>드라이브:W경로</b>(따옴표 사용 안 함) 형식으로 홈 디렉토리 루트 경로를 입력하십시오. 원격 데스크톱 서비스에서는 로그인할 때 사용자 별칭을 자동으로 추가하므로 사용자 별칭에 대한 자리 표시자를 지정하지 마십시오.</p> <p><b>참고</b> 로컬 경로를 지정할 경우 드라이브 문자 필드는 무시됩니다. 로컬 경로를 지정하고 홈 디렉토리 루트 경로에 네트워크 공유 이름을 입력한 경우에 원격 데스크톱 서비스는 네트워크 위치에 사용자 홈 디렉토리를 지정합니다.</p> <p>상태를 사용으로 설정한 경우 원격 데스크톱 서비스는 로컬 컴퓨터 또는 네트워크의 지정한 위치에 사용자의 홈 디렉토리를 만듭니다. 각 사용자의 홈 디렉토리 경로는 지정한 홈 디렉토리 루트 경로 및 사용자 별칭입니다.</p> <p>상태를 사용 안 함 또는 구성되지 않음으로 설정하면 서버의 지정된 위치에 사용자의 홈 디렉토리가 만들어집니다.</p>

설정	설명
Use mandatory profiles on the RD Session Host server	<p>이 정책 설정으로 원격 데스크톱 서비스가 RDS 호스트에 원격으로 연결되어 있는 모든 사용자에게 필수 프로파일을 사용할지 여부를 지정할 수 있습니다.</p> <p>이 정책 설정을 사용하는 경우 원격 데스크톱 서비스는 Set path for Remote Desktop Services Roaming User Profile 정책 설정에 지정되어 있는 경로를 필수 사용자 프로파일의 루트 폴더로 사용합니다. RDS 호스트에 원격으로 연결되어 있는 모든 사용자가 같은 사용자 프로파일을 사용합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않는 경우 RDS 호스트에 원격으로 연결되어 있는 사용자가 필수 사용자 프로파일을 사용하지 않게 됩니다.</p> <p><b>참고</b> 이 정책 설정을 사용하려면 Set path for Remote Desktop Services Roaming User Profile 정책 설정도 사용하도록 구성해야 합니다.</p>
Set path for Remote Desktop Services Roaming User Profile	<p>이 정책 설정으로 원격 데스크톱 서비스가 로밍 사용자 프로파일에 사용하는 네트워크 경로를 지정할 수 있습니다.</p> <p>기본적으로 원격 데스크톱 서비스는 모든 사용자 프로파일을 RDS 호스트에 로컬로 저장합니다. 이 정책 설정을 통해 사용자 프로파일을 한 곳에 저장할 수 있는 네트워크 공유를 지정하여 사용자가 사용자 프로파일에 네트워크 공유를 사용하도록 구성된 모든 RDS 호스트의 세션에 대해 같은 프로파일에 액세스하도록 할 수 있습니다.</p> <p>이 정책 설정을 사용하는 경우 원격 데스크톱 서비스는 지정된 경로를 모든 사용자 프로파일에 대한 루트 디렉토리로 사용합니다. 프로파일은 각 사용자의 계정 이름을 가진 하위 폴더에 있습니다.</p> <p>이 정책 설정을 구성하려면 <b>\\\\컴퓨터 이름\공유 이름</b> 형식으로 네트워크 공유에 대한 경로를 입력합니다. 사용자가 로그인하여 프로파일이 만들어지면 원격 데스크톱 서비스가 자동으로 자리 표시자를 추가하므로 사용자 계정 이름에 자리 표시자를 지정하지 마십시오. 지정된 네트워크 공유가 없으면 원격 데스크톱 서비스는 RDS 호스트에 오류 메시지를 표시하고 사용자 프로파일을 RDS 호스트에 로컬로 저장합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않는 경우 사용자 프로파일은 RDS 호스트에 로컬로 저장됩니다. 사용자 계정 속성 대화 상자의 원격 데스크톱 서비스 프로파일 탭에서 사용자의 프로파일 경로를 구성할 수 있습니다.</p> <p><b>참고:</b></p> <ol style="list-style-type: none"> <li>1 정책 설정을 통해 사용 가능해진 로밍 사용자 프로파일은 원격 데스크톱 서비스 연결에만 적용됩니다. 사용자에게 Windows 로밍 사용자 프로파일이 구성되어 있을 수도 있습니다. 원격 데스크톱 서비스 세션에서는 원격 데스크톱 서비스 로밍 사용자 프로파일이 항상 우선합니다.</li> <li>2 RDS 호스트에 원격으로 연결되어 있는 모든 사용자에게 필수 원격 데스크톱 서비스 로밍 사용자 프로파일을 구성하려면 <b>컴퓨터 구성\관리 템플릿\Windows 구성 요소\원격 데스크톱 서비스\RD 세션 호스트\프로파일</b>에 있는 Use mandatory profiles on the RD Session Host server 정책 설정과 함께 이 정책 설정을 사용하십시오. Set path for Remote Desktop Services Roaming User Profile 정책 설정에 지정되어 있는 경로는 필수 프로파일을 포함해야 합니다.</li> </ol>

## RDS 연결 서버 설정

RDS 연결 서버 그룹 정책 설정을 사용하면 사용자가 연결 서버에 대한 정책을 설정할 수 있습니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > RD 연결 브로커** 폴더에 설치됩니다.

표 5-19. RDS 연결 서버 그룹 정책 설정

설정	설명
Join RD Connection Broker	<p>이 정책 설정을 사용하여 RDS 호스트가 RDS 호스트에 설치된 연결 서버의 팜에 가입해야 하는지 여부를 지정합니다. RDS 호스트의 연결 서버는 사용자 세션을 추적하고 사용자 로드 밸런싱된 RDS 팜의 기존 세션에 다시 연결할 수 있도록 합니다. RDS 호스트의 연결 서버에 참여하려면 원격 데스크톱 세션 호스트 역할 서비스가 RDS 호스트에 설치되어야 합니다. 이 정책 설정이 사용되도록 설정되면 RDS 호스트는 "RD 연결 브로커 팜 이름 구성" 설정에 지정된 팜에 가입합니다. 해당 팜은 "RD 연결 브로커 서버 이름 구성" 정책 설정에 지정되어 있는 연결 서버에 존재합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 RDS 호스트는 연결 서버의 팜에 가입하지 않으므로 사용자 세션 추적이 수행되지 않습니다. 이 설정을 사용하지 않도록 설정하면 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 RDS 호스트를 연결 서버에 가입할 수 없습니다.</p> <p>이 정책 설정이 구성되지 않으면 설정이 그룹 정책 수준에서 지정되지 않습니다. 이 경우 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 RDS 호스트에서 연결 서버에 가입하도록 RDS 호스트를 구성할 수 있습니다.</p> <p><b>참고</b></p> <ol style="list-style-type: none"> <li>이 설정을 사용하도록 설정하는 경우 "RD 연결 브로커 팜 이름 구성" 및 "RD 연결 브로커 서버 이름 구성" 정책 설정을 사용하도록 설정하거나 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 이러한 설정을 구성해야 합니다.</li> <li>Windows Server 2008의 경우 이 정책 설정은 Windows Server 2008 Standard 이상에서 지원됩니다.</li> </ol>
Configure RD Connection Broker farm name	<p>이 정책 설정을 사용하여 RDS 호스트에 대한 연결 서버에서 가입할 팜의 이름을 지정합니다. 연결 서버는 팜 이름을 사용하여 같은 RDS 팜에 있는 RDS 호스트를 확인합니다. 따라서 동일한 로드 밸런싱된 팜의 모든 RDS 호스트에 대해 동일한 팜 이름을 사용해야 합니다. 팜 이름은 Active Directory 도메인 서비스의 이름과 일치할 필요가 없습니다.</p> <p>새 팜 이름을 지정하면 새 팜이 RDS 호스트에 대한 연결 서버에 생성됩니다. 기존 팜 이름을 지정하는 경우 RDS 호스트는 RDS 호스트의 연결 서버에서 해당 팜에 가입합니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 RDS 호스트에 대한 연결 서버에 팜의 이름을 지정해야 합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 팜 이름이 그룹 정책에 의해 지정되지 않습니다. 이 경우 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 팜 이름을 조정할 수 있습니다.</p> <p><b>참고</b> Windows Server 2008의 경우 이 정책 설정은 Windows Server 2008 Standard 이상에서 지원됩니다. 이 설정은 그룹 정책, 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 "RD 연결 브로커 가입" 및 "RD 연결 브로커 서버 이름 구성"이 둘 다 사용되도록 설정하지 않고 구성하지 않으면 적용되지 않습니다.</p>

설정	설명
Use IP Address Redirection	<p>이 정책 설정을 사용하여 클라이언트 디바이스가 로드 밸런싱된 RDS 팜의 기존 원격 데스크톱 서비스 세션에 다시 연결할 때 사용할 리디렉션 방법을 지정합니다. 이 설정은 원격 데스크톱의 연결 서버가 아닌 RDS 호스트의 연결 서버를 사용하도록 구성된 RDS 호스트에 적용됩니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 데스크톱 서비스 클라이언트는 RDS 호스트의 연결 서버를 쿼리하고 세션이 존재하는 RDS 호스트의 IP 주소를 사용하여 기존 세션으로 리디렉션됩니다. 이 리디렉션 방법을 사용하려면 클라이언트 컴퓨터가 IP 주소로 팜의 RDS 호스트에 직접 연결할 수 있어야 합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 RDS 호스트의 IP 주소가 클라이언트로 전송되지 않습니다. 대신 IP 주소가 토큰에 포함됩니다. 클라이언트가 로드 밸런서에 다시 연결되면 라우팅 토큰을 사용하여 클라이언트를 팜의 올바른 RDS 호스트에 있는 기존 세션으로 리디렉션합니다. 네트워크 로드 밸런싱 솔루션이 RDS 호스트 연결 서버 라우팅 토큰의 사용을 지원하며 클라이언트가 로드 밸런싱된 팜의 RDS 호스트에 IP 주소로 직접 연결되지 않게 하려는 경우에만 이 설정을 사용하지 않도록 설정하십시오.</p> <p>이 정책 설정을 구성하지 않으면 원격 데스크톱 세션 호스트 구성 도구의 "IP 주소 리디렉션 사용" 설정이 사용됩니다. 기본적으로 원격 데스크톱 세션 호스트 구성 도구의 이 설정은 사용하도록 설정됩니다.</p> <p><b>참고</b> Windows Server 2008의 경우 이 정책 설정은 Windows Server 2008 Standard 이상에서 지원됩니다.</p>

설정	설명
Configure RD Connection Broker Server name	<p>이 정책 설정을 사용하여 RDS 호스트가 로드 밸런싱된 RDS 팜에 대한 사용자 세션을 추적하고 리디렉션하는 데 사용하는 연결 서버를 지정합니다. 지정된 RDS 호스트에서 연결 서버 서비스가 실행되고 있어야 합니다. 로드 밸런싱된 팜의 모든 RDS 호스트는 동일한 연결 서버를 사용해야 합니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 해당 호스트 이름, IP 주소 또는 정규화된 도메인 이름을 사용하여 RDS 호스트에 대한 연결 서버를 지정해야 합니다. 유효하지 않은 연결 서버에 대해 이름 또는 IP 주소를 지정하면 RDS 호스트의 이벤트 뷰어에 오류 메시지가 로깅됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 RDS 호스트 연결 서버 이름 또는 IP 주소를 조정할 수 있습니다.</p> <p><b>참고</b></p> <ul style="list-style-type: none"> <li>■ Windows Server 2008의 경우 이 정책 설정은 Windows Server 2008 Standard에서 지원됩니다.</li> <li>■ 이 정책 설정은 "RD 연결 브로커 가입" 정책 설정을 사용하도록 설정하지 않거나 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 RDS 호스트가 RDS 호스트의 연결 서버에 가입되도록 구성하지 않으면 적용되지 않습니다.</li> <li>■ RDS 팜의 연결 서버에서 사용 설정된 세션의 활성 구성원이 되려면 팜의 각 RDS 호스트에 대한 컴퓨터 계정이 RDS 호스트에 대한 연결 서버의 "세션 디렉토리 컴퓨터" 로컬 그룹의 구성원이어야 합니다.</li> </ul>
Use RD Connection Broker load balancing	<p>이 정책 설정을 사용하여 RDS 호스트의 연결 서버에서 로드 밸런싱 기능을 사용하여 RDS 팜의 서버 간에 로드 밸런스를 조정할지 여부를 지정합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 RDS 호스트의 연결 서버가 기존 세션이 없는 사용자를 최소 세션만 있는 팜의 RDS 호스트로 리디렉션합니다. 기존 세션이 있는 사용자에 대한 리디렉션 동작은 영향을 받지 않습니다. 서버가 RDS 호스트의 연결 서버를 사용하도록 구성되면 기존 세션이 있는 사용자는 해당 세션이 있는 RDS 호스트로 리디렉션됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 기존 세션이 없는 사용자는 연결되는 첫 번째 RDS 호스트에 로그인됩니다.</p> <p>이 정책 설정을 구성하지 않으면 원격 데스크톱 세션 호스트 구성 도구 또는 터미널 서비스 WMI 제공자를 사용하여 RDS 호스트가 RDS 호스트에 대한 연결 서버 로드 밸런싱에 참여하도록 구성할 수 있습니다.</p> <p><b>참고</b> 이 정책 설정을 사용하도록 설정하는 경우 "RD 연결 브로커 가입", "RD 연결 브로커 팜 이름 구성" 및 "RD 연결 브로커 서버 이름 구성" 정책 설정도 사용하도록 설정해야 합니다.</p>

## RDS 원격 세션 환경 설정

RDS 원격 세션 환경 그룹 정책 설정은 원격 데스크톱 서비스 세션의 사용자 인터페이스 구성을 제어합니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 원격 세션 환경** 폴더에 설치됩니다.

Horizon 7 RDS 그룹 정책 설정은 **사용자 구성 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 원격 세션 환경** 폴더에 설치됩니다.

표 5-20. RDS 원격 세션 환경 그룹 정책 설정

설정	설명
Limit maximum color depth	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 연결에 대한 최대 색 해상도(색 농도)를 지정합니다.</p> <p>이 정책 설정을 사용하면 RDP를 통해 연결의 색 농도 제한을 설정할 수 있습니다. 색 농도를 제한하면 특히 느린 링크에서 연결 성능이 향상되며 서버 로드가 줄어듭니다.</p> <p>이 정책 설정을 사용하도록 설정하면 지정한 색 농도는 RDP를 통한 사용자 연결에 허용되는 최대 색 농도입니다. 연결에 대한 실제 색 농도는 클라이언트 컴퓨터에서 사용할 수 있는 색 지원에 따라 결정됩니다. “클라이언트 호환 가능”을 선택하면 클라이언트에서 지원하는 최대 색 농도가 사용됩니다.</p> <hr/> <p><b>참고</b> 색 농도 24비트는 Windows XP Professional 및 Windows Server 2003에서만 지원됩니다.</p> <hr/> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않는 경우 연결할 때 사용자가 더 낮은 수준을 지정하지 않으면, 연결에 대한 색 농도는 원격 데스크톱 세션 호스트 구성 도구의 [클라이언트 설정] 탭에 있는 “최대 색 농도 제한” 설정에 의해 결정됩니다.</p>
Enforce Removal of Remote Desktop Wallpaper	<p>데스크톱 배경 무늬를 원격 데스크톱 서비스를 통해 연결되는 원격 클라이언트에 표시할지 여부를 지정합니다.</p> <p>이 설정을 사용하여 원격 데스크톱 서비스 세션 동안 배경 무늬를 제거할 수 있습니다. 기본적으로 Windows XP Professional은 클라이언트 구성에 따라 원격 데스크톱을 통해 연결되는 원격 클라이언트에 배경 무늬를 표시합니다. 자세한 내용은 원격 데스크톱 연결 옵션의 [고급] 탭을 참조하십시오. 기본적으로 Windows Server 2003이 실행되는 서버는 원격 데스크톱 서비스 세션에 배경 무늬를 표시하지 않습니다.</p> <p>이 설정을 사용하도록 설정하면 원격 데스크톱 서비스 세션에 배경 무늬가 전혀 나타나지 않습니다.</p> <p>이 설정을 사용하지 않도록 설정하면 클라이언트 구성에 따라 원격 데스크톱 세션에 배경 무늬가 표시될 수 있습니다.</p> <p>이 설정을 구성하지 않으면 기본 동작이 적용됩니다.</p>

설정	설명
Configure RemoteFX	<p>이 정책 설정을 사용하여 RD 가상화 호스트(원격 데스크톱 가상화 호스트) 및 RDS 호스트 둘 다에서 RemoteFX의 가용성을 제어합니다.</p> <p>RD 가상화 호스트에 배포될 경우 RemoteFX는 GPU(그래픽 처리 장치) 또는 하드웨어를 사용하여 서버의 콘텐츠를 렌더링함으로써 풍부한 사용자 환경을 제공합니다. 기본적으로 RD 가상화 호스트용 RemoteFX는 서버 쪽 GPU 또는 하드웨어를 사용하여 LAN 연결 및 RDP 7.1을 통해 풍부한 사용자 환경을 제공합니다. RDS 호스트에 배포될 경우 RemoteFX는 하드웨어 가속 압축 체계를 사용하여 풍부한 사용자 환경을 제공합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 RemoteFX는 LAN 연결 및 RDP 7.1을 통해 풍부한 사용자 환경을 제공하는 데 사용됩니다. 이 정책 설정을 사용하도록 설정하지 않으면 RemoteFX가 사용되지 않도록 설정됩니다.</p> <p>이 정책 설정을 구성하지 않으면 기본 동작이 사용됩니다. 기본적으로 RD 가상화 호스트용 RemoteFX는 사용되도록 설정되고 RDS 호스트용 RemoteFX는 사용되지 않도록 설정됩니다.</p>
Limit maximum display resolution	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 세션을 표시하는 데 사용되는 각 모니터에서 사용할 수 있는 최대 디스플레이 해상도를 지정합니다. 원격 세션을 표시하는 데 사용되는 해상도를 제한하면 특히 느린 링크에서 연결 성능이 향상되며 서버 로드를 줄일 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 해상도 너비 및 높이를 지정해야 합니다. 지정된 해상도는 원격 데스크톱 서비스 세션을 표시하는 데 사용되는 각 모니터에서 사용할 수 있는 최대 해상도입니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 각 모니터에서 원격 데스크톱 서비스 세션을 표시하는 데 사용할 수 있는 최대 해상도는 원격 데스크톱 세션 호스트 구성 도구의 [디스플레이 설정] 탭에 지정된 값에 따라 결정됩니다.</p>
Limit maximum number of monitors	<p>이 정책 설정을 사용하여 사용자가 원격 데스크톱 서비스 세션을 표시하는 데 사용할 수 있는 모니터 수를 제한합니다. 원격 데스크톱 서비스 세션을 표시하는 모니터의 수를 제한하면 특히 느린 링크에서 연결 성능이 향상되며 서버 로드를 줄일 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 원격 데스크톱 서비스 세션을 표시하는 데 사용할 수 있는 모니터 수를 지정할 수 있습니다. 1부터 10까지의 수를 지정할 수 있습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 데스크톱 서비스 세션을 표시하는 데 사용할 수 있는 모니터 수는 원격 데스크톱 세션 호스트 구성 도구의 [디스플레이 설정] 탭에 있는 "세션당 최대 모니터 수 제한" 상자에 지정한 값에 따라 결정됩니다.</p>



설정	설명
Remove "Disconnect" option from Shut Down dialog	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 세션의 [Windows 종료] 대화 상자에서 "연결 해제" 옵션을 제거합니다. 이 정책 설정을 사용하여 사용자가 이러한 익숙한 방법으로 RDS 호스트에서 클라이언트 연결을 해제하지 못하도록 할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 [Windows 종료] 대화 상자의 드롭다운 목록에 "연결 해제"가 옵션으로 나타나지 않습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 [Windows 종료] 대화 상자의 목록에서 "연결 해제"가 제거되지 않습니다.</p> <hr/> <p><b>참고</b> 이 정책 설정은 [Windows 종료] 대화 상자에만 영향을 줍니다. 사용자는 다른 방법을 사용하여 원격 데스크톱 서비스 세션에서 연결을 해제할 수 없습니다. 이 정책 설정은 서버에서 연결이 해제된 세션도 금지합니다. <b>컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; 원격 데스크톱 서비스 &gt; RD 세션 호스트 &gt; 세션 시간 제한</b> 폴더에서 "연결 끊어진 세션에 시간 제한 설정"을 구성하여 연결이 끊어진 세션이 서버에서 활성 상태를 유지하는 시간을 제어할 수 있습니다.</p> <hr/>
Optimize visual experience when using RemoteFX	<p>이 정책 설정을 사용하여 RemoteFX를 사용하는 RDS(원격 데스크톱 연결) 연결에서 원격 사용자에게 제공될 시각적 환경을 지정합니다. 이 정책을 사용하여 네트워크 대역폭 사용량과 전달되는 그래픽 환경 유형을 균형 있게 조정할 수 있습니다.</p> <p>사용자의 요구 사항에 따라, 화면 캡처 속도를 줄여 네트워크 대역폭 사용량을 줄일 수 있습니다. 또한 이미지 품질을 줄여(수행되는 이미지 압축 크기 증가) 네트워크 대역폭 사용량을 줄일 수 있습니다.</p> <p>평균 대역폭 네트워크보다 더 높을 경우 화면 캡처 속도 및 이미지 품질에 대해 더 높은 설정을 선택하여 대역폭 사용량을 최대화할 수 있습니다.</p> <p>기본적으로 RemoteFX를 사용하는 원격 데스크톱 연결 세션은 LAN 상태와 환경의 균형을 이루도록 최적화됩니다. 이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 RemoteFX를 사용하는 원격 데스크톱 연결 세션은 중간 화면 캡처 속도 및 중간 이미지 압축 설정을 선택한 것과(기본 동작) 같아집니다.</p> <hr/>

설정	설명
Set compression algorithm for RDP data	<p>이 정책 설정을 사용하여 사용할 RDP(원격 데스크톱 프로토콜) 압축 알고리즘을 지정합니다.</p> <p>기본적으로 서버는 서버의 하드웨어 구성을 기준으로 하는 RDP 압축 알고리즘을 사용합니다.</p> <p>이 정책 설정을 사용하도록 지정하면 사용할 RDP 압축 알고리즘을 지정할 수 있습니다. 메모리를 덜 사용하기 위해 최적화된 알고리즘을 선택하는 경우 이 옵션은 덜 메모리 집약적이지만 더 많은 네트워크 대역폭을 사용합니다. 네트워크 대역폭을 덜 사용하기 위해 최적화된 알고리즘을 선택하는 경우 이 옵션은 네트워크 대역폭을 덜 사용하지만 좀 더 메모리 집약적입니다. 또한 메모리 사용량과 네트워크 대역폭의 균형을 유지하는 세 번째 옵션을 사용할 수 있습니다.</p> <p>RDP 압축 알고리즘을 사용하지 않도록 선택할 수도 있습니다. RDP 압축 알고리즘을 사용하지 않도록 선택하면 더 많은 네트워크 대역폭이 사용되므로 네트워크 트래픽을 최적화하도록 고안된 하드웨어 디바이스를 사용 중인 경우에만 권장됩니다. RDP 압축 알고리즘을 사용하지 않도록 선택하더라도 일부 그래픽 데이터는 여전히 압축됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 기본 RDP 압축 알고리즘이 사용됩니다.</p>
Optimize visual experience for Remote Desktop Services sessions	<p>이 정책 설정을 사용하여 원격 데스크톱 서비스 세션에서 원격 사용자에게 제공되는 시각적 환경을 지정합니다. 그런 후에 원격 컴퓨터의 원격 세션은 이러한 시각적 환경을 지원하도록 최적화됩니다.</p> <p>기본적으로 원격 데스크톱 서비스 세션은 Silverlight 또는 Windows Presentation Foundation을 사용하는 애플리케이션 등의 풍부한 멀티미디어에 맞게 최적화됩니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 데스크톱 서비스 세션을 최적화하려는 시각적 환경을 선택해야 합니다. 풍부한 멀티미디어 또는 텍스트 중에서 선택할 수 있습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 데스크톱 서비스 세션이 풍부한 멀티미디어에 맞게 최적화됩니다.</p>

설정	설명
<p>Start a program on connection</p>	<p>연결할 때 지정된 프로그램을 자동으로 실행하도록 원격 데스크톱 서비스를 구성합니다.</p> <p>이 설정을 사용하여 사용자가 원격 컴퓨터에 로그인할 때 자동으로 실행될 프로그램을 지정할 수 있습니다.</p> <p>기본적으로 원격 데스크톱 서비스 세션은 서버 관리자나 사용자가 클라이언트 연결을 구성할 때 이 설정으로 지정하지 않으면 전체 Windows 바탕 화면에 대한 액세스를 제공합니다. 이 설정을 사용하도록 설정하면 서버 관리자 또는 사용자가 설정한 "시작 프로그램" 설정이 재정의됩니다. 시작 메뉴 및 Windows 바탕 화면이 표시되지 않으며, 사용자가 프로그램을 나가면 세션이 자동으로 로그오프됩니다.</p> <p>이 설정을 사용하려면 프로그램 경로 및 파일 이름에서 사용자가 로그인할 때 실행될 실행 파일의 정규화된 경로 및 파일 이름을 입력합니다. 필요한 경우 작업 디렉토리에 프로그램에 대한 시작 디렉토리의 정규화된 경로를 입력합니다. 작업 디렉토리를 비워 두면 프로그램은 기본 작업 디렉토리를 사용하여 실행됩니다. 지정된 프로그램 경로, 파일 이름 또는 작업 디렉토리가 유효한 디렉토리의 이름이 아닌 경우 RDS 호스트 연결은 오류 메시지를 나타내며 실패합니다.</p> <p>상태가 [사용]으로 설정되면 원격 데스크톱 서비스 세션은 지정된 프로그램을 자동으로 실행하고 지정된 작업 디렉토리(또는 작업 디렉토리가 지정되지 않은 경우 프로그램 기본 디렉토리)를 프로그램의 작업 디렉토리로 사용합니다.</p> <p>상태가 [사용 안 함] 또는 [구성되지 않음]으로 설정되면 서버 관리자나 사용자가 다르게 지정하지 않은 경우 원격 데스크톱 서비스 세션은 전체 데스크톱에서 시작됩니다. 자세한 내용은 "사용자가 로그인할 때 다음 프로그램 실행: 컴퓨터 구성 &gt; 관리 템플릿 &gt; 시스템 &gt; 로그인" 폴더의 정책 설정"을 참조하십시오.</p> <p><b>참고</b> 이 설정은 컴퓨터 구성 및 사용자 구성 둘 다에 표시됩니다. 두 설정이 모두 구성되면 컴퓨터 구성 설정이 사용자 구성 설정을 재정의합니다.</p>
<p>Always show desktop on connection</p>	<p>이 정책 설정은 클라이언트가 원격 컴퓨터에 연결되거나 초기 프로그램을 실행할 수 있게 되면 바탕 화면이 항상 표시되는지 여부를 결정합니다. 이 설정을 사용하여 초기 프로그램이 기본 사용자 프로파일, 원격 데스크톱 연결, 원격 데스크톱 서비스 클라이언트 또는 그룹 정책을 통해 이미 지정되었더라도 클라이언트가 원격 컴퓨터에 연결된 후에 바탕 화면이 표시되도록 할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 클라이언트가 원격 컴퓨터에 연결될 때 항상 바탕 화면이 표시됩니다. 이 정책 설정은 초기 프로그램 정책 설정을 재정의합니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 클라이언트가 원격 컴퓨터에 연결한 후에 원격 컴퓨터에서 실행되는 초기 프로그램을 지정할 수 있습니다. 초기 프로그램을 지정하지 않으면 클라이언트가 원격 컴퓨터에 연결한 후에 원격 컴퓨터에 항상 바탕 화면이 표시됩니다.</p> <p><b>참고</b> 이 정책 설정이 사용되도록 설정되면 "연결 시 프로그램 시작" 정책 설정이 무시됩니다.</p>

설정	설명
Allow desktop composition for remote desktop sessions	<p>이 정책 설정을 사용하여 원격 데스크톱 세션에 대해 바탕 화면 구성이 허용되는지 여부를 지정합니다. 이 정책 설정은 RemoteApp 세션에는 적용되지 않습니다.</p> <p>바탕 화면 구성은 원격 데스크톱 세션에 대해 반투명 창과 같은 Windows Aero의 사용자 인터페이스 요소를 제공합니다. Windows Aero에는 추가 시스템 및 대역폭 리소스가 필요하므로 원격 데스크톱 세션에 대해 바탕 화면 구성을 허용하면 특히 느린 링크에서 연결 성능이 저하되고 원격 컴퓨터의 로드가 늘어날 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 원격 데스크톱 세션에 대해 바탕 화면 구성이 허용됩니다. 클라이언트 컴퓨터에서 RDC(원격 데스크톱 연결)의 [고급] 탭에서 또는 원격 데스크톱 프로토콜 (.rdp) 파일에서 "바탕 화면 구성 허용" 설정을 사용하여 바탕 화면 구성을 구성할 수 있습니다. 또한 클라이언트 컴퓨터에는 Windows Aero 기능을 지원하기 위해 필요한 하드웨어가 있어야 합니다.</p> <hr/> <p><b>참고</b> 원격 데스크톱 세션에 Windows Aero 기능을 사용할 수 있도록 하려면 원격 컴퓨터에서 추가 구성이 필요할 수 있습니다. 예를 들어 데스크톱 경험 기능을 원격 컴퓨터에 설치하고 원격 컴퓨터의 최대 색 농도를 픽셀당 32비트로 설정해야 합니다. 또한 원격 컴퓨터에서 테마 서비스를 시작해야 합니다.</p> <hr/> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 바탕 화면 구성이 RDC 또는 .rdp 파일에서 사용되도록 설정되더라도 원격 데스크톱 세션에 대해 허용되지 않습니다.</p>

설정	설명
Do not allow font smoothing	<p>이 정책 설정을 사용하여 원격 연결에 대해 글꼴 다듬기가 허용되는지 여부를 지정합니다.</p> <p>글꼴 다듬기는 원격 연결에 대해 ClearType 기능을 제공합니다. ClearType은 특히 LCD 모니터를 사용할 때 컴퓨터 글꼴이 깨끗하고 매끄럽게 표시되도록 하는 기술입니다. 글꼴 다듬기를 수행하려면 추가 대역폭 리소스가 필요하므로 원격 연결에 대해 글꼴 다듬기를 허용하지 않으면 특히 느린 링크에서 연결 성능이 향상될 수 있습니다.</p> <p>기본적으로 원격 연결에 대해 글꼴 다듬기가 허용됩니다. RDC(원격 데스크톱 연결)의 [고급] 탭에서 또는 원격 데스크톱 프로토콜(.rdp) 파일에서 "글꼴 다듬기 허용" 설정을 사용하여 글꼴 다듬기를 구성할 수 있습니다.</p> <p>이 정책 설정을 사용하도록 설정하면 RDC 또는 .rdp 파일에서 글꼴 다듬기를 사용하도록 설정하는 경우에도 원격 연결에 대해 글꼴 다듬기가 허용되지 않습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 연결에 대해 글꼴 다듬기가 허용됩니다.</p>
Remove Windows Security item from Start menu	<p>원격 데스크톱 클라이언트의 설정 메뉴에서 Windows 보안 항목을 제거할지 여부를 지정합니다. 이 설정을 사용하면 경험이 부족한 사용자가 실수로 원격 데스크톱 서비스에서 로그오프하는 것을 방지할 수 있습니다.</p> <p>상태를 사용으로 설정하면 시작 메뉴의 설정에 Windows 보안이 표시되지 않습니다. 따라서 사용자는 Ctrl+Alt+End와 같은 보안 주의 키 시퀀스를 입력해야 클라이언트 컴퓨터에서 Windows 보안 대화 상자를 열 수 있습니다.</p> <p>상태를 사용 안 함 또는 구성하지 않음으로 설정하면 Windows 보안이 설정 메뉴에 계속 표시됩니다.</p>

## RDS 보안 설정

RDS Security Group 정책 설정은 로컬 관리자의 사용 권한 사용자 지정에 대한 허용 여부를 제어합니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 보안** 폴더에 설치됩니다.

표 5-21. RDS Security Group 정책 설정

설정	설명
Server Authentication Certificate Template	<p>이 정책 설정을 사용하여 RDS 호스트를 인증하기 위해 자동으로 선택되는 인증서를 결정하는 인증서 템플릿의 이름을 지정합니다. SSL(TLS 1.0)이 RDP 연결 중에 클라이언트와 RDS 호스트 간의 보안 통신에 사용될 경우 RDS 호스트를 인증하는 데 인증서가 필요합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 인증서 템플릿 이름을 지정해야 합니다. RDS 호스트를 인증하기 위한 인증서가 자동으로 선택될 경우 지정된 인증서 템플릿을 사용하여 생성한 인증서만 고려됩니다. 특정 인증서가 선택되지 않은 경우에만 자동 인증서 선택이 발생합니다.</p> <p>지정된 인증서 템플릿으로 생성한 인증서를 찾을 수 없으면 RDS 호스트는 인증서 등록 요청을 실행하고 해당 요청이 완료될 때까지 현재 인증서를 사용합니다. 지정된 인증서 템플릿으로 생성한 인증서가 2개 이상 있으면 곧 만료될 예정이며 RDS 호스트의 현재 이름과 일치하는 인증서가 선택됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 기본적으로 RDS 호스트를 인증하는 데 자체 서명된 인증서가 사용됩니다. 원격 데스크톱 호스트 구성 도구의 [일반] 탭에서 RDS 호스트를 인증하는 데 사용할 수 있는 특정 인증서를 선택할 수 있습니다.</p> <p><b>참고</b> RDS 호스트를 인증하는 데 사용할 특정 인증서를 선택하는 경우 해당 인증서는 이 정책 설정보다 우선합니다.</p>
Set client connection encryption level	<p>RDP(원격 데스크톱 프로토콜) 연결 동안 클라이언트와 RDS 호스트 간 보안 통신을 위해 특정 암호화 수준을 사용하도록 요구할지 여부를 지정합니다.</p> <p>이 설정을 사용하도록 설정하면 원격 연결 동안 클라이언트와 RDS 호스트 간의 모든 통신에 이 설정에 지정된 암호화 방법을 사용해야 합니다. 기본적으로 암호화 수준은 [높음]으로 설정됩니다. 다음 암호화 방법을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>High.</b> [높음] 설정은 강력한 128비트 암호화를 사용하여 클라이언트에서 서버로, 서버에서 클라이언트로 전송되는 데이터를 암호화합니다. 128비트 클라이언트(예: 원격 데스크톱 연결을 실행하는 클라이언트)만 포함하는 환경에서는 이 암호화 수준을 사용합니다. 이 암호화 수준을 지원하지 않는 클라이언트는 RDS 호스트 서버에 연결할 수 없습니다.</li> <li>■ <b>Client Compatible.</b> [클라이언트 호환 가능] 설정은 클라이언트에서 지원하는 최대 키 강도에서 클라이언트와 서버 간에 전송되는 데이터를 암호화합니다. 128비트 암호화를 지원하지 않는 클라이언트가 포함된 환경에서는 이 암호화 수준을 사용합니다.</li> <li>■ <b>Low.</b> [낮음] 설정은 56비트 암호화를 사용하여 클라이언트에서 서버로 전송되는 데이터만 암호화합니다.</li> </ul> <p>이 설정을 사용하지 않도록 설정하거나 구성하지 않으면 RDS 호스트와의 원격 연결에 사용할 암호화 수준이 그룹 정책을 통해 적용되지 않습니다. 하지만 원격 데스크톱 세션 호스트 구성 도구를 사용하여 이러한 연결에 필요한 암호화 수준을 구성할 수 있습니다.</p> <p><b>중요</b> FIPS 규격은 <b>컴퓨터 구성 &gt; Windows 설정 &gt; 보안 설정 &gt; 로컬 정책 &gt; 보안 옵션</b> 폴더의 "시스템 암호화: 암호화, 해시, 서명에 FIPS 호환 알고리즘 사용" 정책 설정을 통해 또는 원격 데스크톱 세션 호스트 구성의 "FIPS 규격" 설정을 통해 구성할 수 있습니다. FIPS 규격 설정은 Microsoft 암호화 모듈을 사용하여 FIPS(Federal Information Processing Standard) 140-1 암호화 알고리즘을 통해 클라이언트에서 서버로 및 서버에서 클라이언트</p>

설정	설명
Always prompt for password upon connection	<p>원격 데스크톱 서비스가 연결 시 항상 클라이언트에 암호를 요구할지 여부를 지정합니다.</p> <p>이 설정을 사용하여 원격 데스크톱 연결 클라이언트에서 이미 암호를 제공한 경우에도 원격 데스크톱 서비스에 로그인하는 사용자에게 암호를 요구할 수 있습니다.</p> <p>기본적으로 원격 데스크톱 서비스는 사용자가 원격 데스크톱 연결 클라이언트에서 암호를 입력하여 자동으로 로그인할 수 있도록 합니다.</p> <p>이 설정을 사용하도록 설정하면 사용자는 원격 데스크톱 연결 클라이언트에서 해당 암호를 제공하여 원격 데스크톱 서비스에 자동으로 로그인할 수 없습니다. 로그인하기 위해 암호를 입력하라는 메시지가 표시됩니다.</p> <p>이 설정을 사용하지 않도록 설정하면 사용자는 항상 원격 데스크톱 연결 클라이언트에서 해당 암호를 제공하여 원격 데스크톱 서비스에 자동으로 로그인할 수 있습니다.</p> <p>이 정책 설정을 구성하지 않으면 그룹 정책 수준에서 자동 로그인이 지정되지 않습니다. 하지만 관리자는 원격 데스크톱 세션 호스트 구성 도구를 사용하여 여전히 암호를 입력하도록 요구할 수 있습니다.</p>
Require secure RPC communication	<p>RDS 호스트가 모든 클라이언트와의 보안 RPC 통신을 요구할지 또는 비보안 통신을 허용할지를 지정합니다.</p> <p>이 설정을 사용하여 인증되고 암호화된 요청만 허용하여 RPC 통신의 보안을 강화할 수 있습니다.</p> <p>이 설정을 사용하도록 설정하면 원격 데스크톱 서비스는 보안 요청을 지원하는 RPC 클라이언트의 요청을 수락하며 신뢰할 수 없는 클라이언트와의 비보안 통신을 허용하지 않습니다.</p> <p>이 설정을 사용하지 않도록 설정하면 원격 데스크톱 서비스는 항상 모든 RPC 트래픽에 대한 보안을 요청합니다. 그러나 요청에 응답하지 않는 RPC 클라이언트에 대해 비보안 통신이 허용됩니다.</p> <p>이 설정을 구성하지 않을 경우 비보안 통신이 허용됩니다.</p> <p><b>참고</b> 원격 데스크톱 서비스를 관리 및 구성하는 데 RPC 인터페이스가 사용됩니다.</p>

설정	설명
Require use of specific security layer for remote (RDP) connections	<p>RDP(원격 데스크톱 프로토콜) 연결 동안 클라이언트와 RDP 호스트 간 보안 통신을 위해 특정 보안 계층을 사용하도록 요구할지 여부를 지정합니다.</p> <p>이 설정을 사용하도록 설정하면 원격 연결 동안 클라이언트와 RDS 호스트 간의 모든 통신에 이 설정에 지정된 보안 방법이 사용되어야 합니다. 다음 보안 방법을 사용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>■ <b>Negotiate.</b> 협상 방법은 클라이언트가 지원하는 가장 안전한 방법을 적용합니다. TLS(전송 계층 보안) 버전 1.0이 지원되는 경우 RDS 호스트를 인증하는 데 사용됩니다. TLS가 지원되지 않으면 기본 RDP(원격 데스크톱 프로토콜) 암호화가 통신 보안 유지에 사용되지만 RDS 호스트는 인증되지 않습니다.</li> <li>■ <b>RDP.</b> RDP 방법은 기본 RDP 암호화를 사용하여 클라이언트와 RDS 호스트 간 통신의 보안을 유지합니다. 이 설정을 선택하면 RDS 호스트가 인증되지 않습니다.</li> <li>■ <b>SSL (TLS 1.0).</b> SSL 방법을 사용하려면 TLS 1.0을 통해 RDS 호스트를 인증해야 합니다. TLS가 지원되지 않으면 연결이 실패합니다.</li> </ul> <p>이 설정을 사용하지 않도록 설정하거나 구성하지 않으면 RDS 호스트에 대한 원격 연결에 사용할 보안 방법이 그룹 정책을 통해 적용되지 않습니다. 하지만 원격 데스크톱 세션 호스트 구성 도구를 사용하여 이러한 연결에 필요한 보안 방법을 구성할 수 있습니다.</p>



설정	설명
Require user authentication for remote connections by using Network	<p>이 정책 설정을 사용하여 네트워크 수준 인증을 통해 RDS 호스트에 대한 원격 연결을 위해 사용자 인증을 요구할지 여부를 지정합니다. 이 정책 설정은 사용자 인증이 원격 연결 프로세스의 초반에 발생하도록 하여 보안을 강화합니다.</p> <p>이 정책 설정을 사용하도록 설정하면 네트워크 수준 인증을 지원하는 클라이언트 컴퓨터만 RDS 호스트에 연결할 수 있습니다.</p> <p>클라이언트 컴퓨터가 네트워크 수준 인증을 지원하는지 여부를 결정하려면 클라이언트 컴퓨터에서 원격 데스크톱 연결을 시작하고, [원격 데스크톱 연결] 대화 상자의 왼쪽 상단 모서리에 있는 아이콘을 클릭합니다. [원격 데스크톱 연결 정보] 대화 상자에서 “네트워크 수준 인증이 지원됩니다.”라는 문구를 찾습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 RDS 호스트에 대한 원격 연결을 허용하기 전에 사용자 인증에 네트워크 수준 인증이 필요하지 않습니다.</p> <p>원격 데스크톱 세션 호스트 구성 도구를 사용하거나 [시스템 속성]의 [원격] 탭에서 사용자 인증에 네트워크 수준 인증이 필요하다고 지정할 수 있습니다.</p> <p><b>중요</b> 이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 사용자 인증이 원격 연결 프로세스의 후반부에 발생하므로 보안이 약화됩니다.</p>
Do not allow local administrators to customize permissions	<p>관리자가 원격 데스크톱 세션 호스트 구성 도구에서 보안 권한을 사용자 지정할 수 없도록 할지 여부를 지정합니다.</p> <p>이 설정을 사용하여 관리자가 원격 데스크톱 세션 호스트 구성 도구의 사용 권한 탭에서 사용자 그룹을 변경할 수 없도록 할 수 있습니다. 기본적으로 관리자는 이러한 변경을 수행할 수 있습니다.</p> <p>상태를 사용으로 설정하면 원격 데스크톱 세션 호스트 구성 도구의 사용 권한 탭을 사용하여 연결당 보안 설명자를 사용자 지정하거나 기존 그룹에 대한 기본 보안 설명자를 변경할 수 없습니다. 모든 보안 설명자는 읽기 전용으로 됩니다.</p> <p>상태를 사용 안 함 또는 구성되지 않음으로 설정하면 서버 관리자에게 원격 데스크톱 세션 호스트 구성 도구의 사용 권한 탭에 있는 사용자 보안 설명자에 대한 모든 읽기/쓰기 권한이 부여됩니다.</p> <p><b>참고</b> 사용자 액세스를 관리하기 위한 기본 방법은 사용자를 원격 데스크톱 사용자 그룹에 추가하는 것입니다.</p>

## RDS 세션 시간 제한

RDS 세션 시간 제한 그룹 정책 설정을 사용하여 RDS 호스트의 세션에 대한 시간 제한 정책을 설정할 수 있습니다.

Horizon 7 RDS 그룹 정책 설정은 **컴퓨터 구성 > 정책 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 세션 시간 제한** 폴더에 설치됩니다.

Horizon 7 RDS 그룹 정책 설정은 **사용자 구성 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 세션 시간 제한** 폴더에도 설치됩니다.

표 5-22. RDS 세션 시간 제한 그룹 정책 설정

설정	설명
Set time limit for disconnected sessions	<p>이 정책 설정을 사용하여 연결이 끊긴 원격 데스크톱 서비스 세션에 대한 시간 제한을 구성합니다.</p> <p>이 정책 설정을 사용하여 연결이 끊긴 세션이 서버에서 활성 상태를 유지하는 최대 시간을 지정할 수 있습니다. 기본적으로 원격 데스크톱 서비스는 사용자가 로그오프하고 세션을 종료하지 않고도 원격 데스크톱 서비스 세션에서 연결을 해제할 수 있도록 합니다.</p> <p>세션이 연결 해제된 상태일 때 실행 중인 프로그램은 사용자가 더 이상 능동적으로 연결되지 않더라도 활성 상태를 유지합니다. 기본적으로 이러한 연결 해제된 세션은 서버에서 시간 제한 없이 계속 유지됩니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 연결이 끊긴 세션이 지정된 시간 후에 서버에서 삭제됩니다. 연결이 끊긴 세션이 제한없는 시간 동안 유지되도록 하는 기본 동작을 적용하려면 "안함"을 선택합니다. 콘솔 세션이 있는 경우 연결이 끊긴 세션 시간 제한이 적용되지 않습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 연결이 끊긴 세션이 제한없는 시간 동안 유지됩니다. 원격 데스크톱 세션 호스트 구성 도구의 [세션] 탭에서 연결이 끊긴 세션에 대한 시간 제한을 지정할 수 있습니다.</p> <p><b>참고</b> 이 정책 설정은 컴퓨터 구성 및 사용자 구성 둘 다에 표시됩니다. 두 정책 설정이 모두 구성되면 컴퓨터 구성 정책 설정이 우선적으로 적용됩니다.</p>
Set time limit for active but idle Remote Desktop Services sessions	<p>이 정책 설정을 사용하여 자동으로 연결이 끊기기 전에 사용자 입력 없이 활성 원격 데스크톱 서비스 세션이 유휴 상태를 유지할 수 있는 최대 시간을 지정합니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 [유휴 세션 제한] 드롭다운 목록에서 원하는 시간 제한을 선택해야 합니다. 원격 데스크톱 서비스는 지정된 시간 후에 자동으로 활성이면서 유휴 상태인 세션의 연결을 끊습니다. 사용자가 세션 연결이 끊기기 2분 전에 경고를 수신합니다. 이 경우 아무 키나 누르거나 마우스를 사용하여 세션을 계속 활성 상태로 유지할 수 있습니다. 콘솔 세션이 있는 경우 유휴 세션 시간 제한이 적용되지 않습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 데스크톱 서비스는 세션이 제한없는 시간 동안 활성이면서 유휴 상태를 유지할 수 있습니다. 원격 데스크톱 세션 호스트 구성 도구의 [세션] 탭에서 활성이면서 유휴 상태인 세션에 대한 시간 제한을 지정할 수 있습니다.</p> <p>시간 제한에 도달할 때 원격 데스크톱 서비스가 세션 연결을 끊지 않고 종료되도록 하려면 <b>컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; 원격 데스크톱 서비스 &gt; 원격 데스크톱 세션 호스트 &gt; 세션 시간 제한</b> 폴더에서 "시간 제한에 도달하면 세션 종료" 정책 설정을 구성할 수 있습니다.</p> <p><b>참고</b> 이 정책 설정은 컴퓨터 구성 및 사용자 구성 둘 다에 표시됩니다. 두 정책 설정이 모두 구성되면 컴퓨터 구성 정책 설정이 우선적으로 적용됩니다.</p>

설정	설명
Set time limit for active Remote Desktop Services sessions	<p>이 정책 설정을 사용하여 자동으로 연결이 끊기기 전에 원격 데스크톱 서비스 세션이 활성 상태를 유지할 수 있는 최대 시간을 지정합니다.</p> <p>이 정책 설정을 사용하도록 설정하는 경우 [활성 세션 제한] 그룹다운 목록에서 원하는 시간 제한을 선택해야 합니다. 원격 데스크톱 서비스는 지정된 시간 후에 자동으로 활성 세션의 연결을 끊습니다. 사용자는 원격 데스크톱 서비스 세션의 연결이 끊기기 2분 전에 경고를 받으며 이를 통해 사용자는 열린 파일을 저장하고 프로그램을 닫을 기회를 얻게 됩니다. 콘솔 세션이 있는 경우 활성 세션 시간 제한이 적용되지 않습니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 원격 데스크톱 서비스는 세션이 제한없는 시간 동안 활성 상태를 유지할 수 있습니다. 원격 데스크톱 세션 호스트 구성 도구의 [세션] 탭에서 활성 세션에 대한 시간 제한을 지정할 수 있습니다.</p> <p>시간 제한에 도달할 때 원격 데스크톱 서비스가 세션 연결을 끊지 않고 종료되도록 하려면 <b>컴퓨터 구성 &gt; 관리 템플릿 &gt; Windows 구성 요소 &gt; 원격 데스크톱 서비스 &gt; 원격 데스크톱 세션 호스트 &gt; 세션 시간 제한</b> 폴더에서 "시간 제한에 도달하면 세션 종료" 정책 설정을 구성할 수 있습니다.</p> <p><b>참고</b> 이 정책 설정은 컴퓨터 구성 및 사용자 구성 둘 다에 표시됩니다. 두 정책 설정이 모두 구성되면 컴퓨터 구성 정책 설정이 우선적으로 적용됩니다.</p>

설정	설명
Terminate session when time limits are reached	<p>시간 초과된 원격 데스크톱 서비스 세션의 연결을 끊지 않고 종료할지 여부를 지정합니다.</p> <p>이 설정을 사용하여 활성 또는 유휴 세션에 대한 시간 제한에 도달한 후에 원격 데스크톱 서비스가 세션을 종료하도록 지정할 수 있습니다(즉, 사용자가 로그오프되고 세션이 서버에서 삭제됨). 기본적으로 원격 데스크톱 서비스는 시간 제한에 도달하는 세션의 연결을 끊습니다.</p> <p>시간 제한은 서버 관리자가 또는 그룹 정책을 통해 로컬로 설정합니다. "활성 원격 데스크톱 서비스 세션에 대한 시간 제한 설정" 및 "활성 상태지만 유휴 원격 데스크톱 서비스 세션에 시간 제한 설정" 설정을 참조하십시오.</p> <p>이 설정을 사용하도록 설정하면 원격 데스크톱 서비스가 시간 초과 제한에 도달하는 모든 세션을 종료합니다.</p> <p>이 설정을 사용하지 않도록 설정하면 원격 데스크톱 서비스는 서버 관리자가 다르게 지정하더라도 항상 시간 초과된 세션의 연결을 끊습니다.</p> <p>이 설정을 구성하지 않을 경우 원격 데스크톱 서비스는 로컬 설정에서 다르게 지정되더라도 시간 초과된 세션의 연결을 끊습니다.</p> <p><b>참고</b> 이 설정은 연결 또는 네트워크 상태로 인해 발생하는 시간 초과 이벤트가 아닌, 원격 데스크톱 세션 호스트 구성 도구 또는 그룹 정책 관리 콘솔에서 고의로 설정한 시간 초과 제한에만 적용됩니다. 또한 이 설정은 컴퓨터 구성 및 사용자 구성 둘 다에 표시됩니다. 두 설정이 모두 구성되면 컴퓨터 구성 설정이 우선합니다.</p>
Set time limit for logoff of RemoteApp sessions	<p>이 정책 설정을 사용하여 세션이 RDS 호스트에서 로그오프되기 전에 연결이 끊긴 상태를 유지하는 기간을 지정합니다.</p> <p>기본적으로 사용자가 원격 애플리케이션을 닫으면 세션은 RDS 호스트에서 연결이 끊깁니다.</p> <p>이 정책 설정을 사용하도록 설정하면 사용자가 원격 애플리케이션을 닫을 때 원격 애플리케이션 세션은 지정된 시간 제한에 도달할 때까지 연결이 끊긴 상태를 유지합니다. 지정된 시간 제한에 도달하면 원격 애플리케이션 세션이 RDS 호스트에서 로그오프됩니다. 사용자가 시간 제한에 도달하기 전에 원격 애플리케이션을 시작하면 RDS 호스트에서 연결이 끊긴 세션에 다시 연결됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하거나 구성하지 않으면 사용자가 원격 애플리케이션을 닫을 때 RDS 호스트에서 세션 연결이 끊어집니다.</p> <p><b>참고</b> 이 정책 설정은 컴퓨터 구성 및 사용자 구성 둘 다에 표시됩니다. 두 정책 설정이 모두 구성되면 컴퓨터 구성 정책 설정이 우선적으로 적용됩니다.</p>

## RDS 임시 폴더 설정

RDS 연결 그룹 정책 설정은 원격 데스크톱 서비스 세션에 사용되는 임시 폴더의 생성과 삭제를 제어합니다.

표 5-23. RDS 임시 폴더 그룹 정책 설정

설정	설명
Do not delete temp folder upon exit	<p>로그오프 시 원격 데스크톱 서비스가 사용자의 세션별 임시 폴더를 보존하는지 여부를 지정합니다.</p> <p>이 설정을 사용하면 사용자가 세션에서 로그오프하더라도 사용자의 세션별 임시 폴더를 원격 컴퓨터에 유지할 수 있습니다. 기본적으로 원격 데스크톱 서비스는 로그오프 시 사용자의 임시 폴더를 삭제합니다.</p> <p>상태를 사용으로 설정하면 사용자가 세션에서 로그오프해도 해당 사용자의 세션별 임시 폴더가 보존됩니다.</p> <p>상태를 사용 안 함으로 설정하면 원격 데스크톱 세션 호스트 구성 도구에서 관리자가 설정을 다르게 지정했더라도 사용자가 로그오프하면 임시 폴더가 삭제됩니다.</p> <p>상태를 구성되지 않음으로 설정한 경우 서버 관리자가 달리 지정하지 않는 한, 원격 데스크톱 서비스는 로그오프 시 원격 컴퓨터에서 임시 폴더를 삭제합니다.</p> <p><b>참고</b> 이 설정은 서버에서 세션별 임시 폴더가 사용 중인 경우에만 적용됩니다. 즉, “세션별 임시 폴더를 사용하지 않음” 설정을 사용하는 경우에는 이 설정이 아무런 영향도 미치지 않습니다.</p>
Do not use temporary folders per session	<p>이 정책 설정을 사용하면 원격 데스크톱 서비스가 세션별 임시 폴더를 생성하지 못합니다.</p> <p>이 정책 설정을 사용하면 원격 컴퓨터에 각 세션에 대한 임시 폴더가 생성되지 않게 할 수 있습니다. 기본적으로 원격 데스크톱 서비스는 사용자가 원격 컴퓨터에 유지하는 활성 세션 각각에 대해 별도의 임시 폴더를 생성합니다. 이러한 임시 폴더는 원격 컴퓨터에서 사용자 프로파일 폴더 아래의 임시 폴더에 생성되며 sessionid를 이름으로 사용합니다.</p> <p>이 정책 설정을 사용하는 경우 세션별 임시 폴더가 생성되지 않습니다. 그 대신 원격 컴퓨터에서 실행되는 모든 세션의 사용자 임시 파일이 원격 컴퓨터에 있는 사용자 프로파일 폴더 아래의 공용 임시 폴더에 저장됩니다.</p> <p>이 정책 설정을 사용하지 않도록 설정하면 원격 데스크톱 세션 호스트 구성 도구에서 다르게 지정하더라도 세션별 임시 폴더가 항상 생성됩니다.</p> <p>이 정책 설정을 구성하지 않으면 원격 데스크톱 세션 호스트 구성 도구에서 달리 지정하지 않는 한, 세션별 임시 폴더가 생성됩니다.</p>

## 위치 기반 인쇄 설정

위치 기반 인쇄 기능은 사용자가 View 데스크톱에서 로컬 및 네트워크 프린터로 인쇄하도록 설정하여 View 데스크톱에 물리적으로 가까운 클라이언트 시스템인 프린터를 매핑합니다.

위치 기반 인쇄 기능을 사용하여 IT 조직은 끝점 클라이언트 디바이스에서 가장 가까운 프린터에 View 데스크톱을 매핑할 수 있습니다. 예를 들어 의사는 병실 사이를 이동하기 때문에 의사가 문서를 인쇄할 때마다 가장 가까운 프린터로 인쇄 작업이 전송됩니다.

위치 기반 인쇄 기능은 Windows, Mac, Linux 및 모바일 클라이언트 디바이스에서 사용할 수 있습니다.

Horizon 6.0.1 이상에서 위치 기반 인쇄는 다음 원격 데스크톱 및 애플리케이션에서 지원됩니다.

- Windows Desktop 및 Windows Server 시스템을 포함한 단일 사용자 시스템에 배포된 데스크톱
- RDS 호스트가 가상 시스템인 RDS 호스트에 배포된 데스크톱
- 호스팅된 애플리케이션
- 원격 데스크톱 내부의 Horizon Client에서 시작된 호스팅된 애플리케이션

Horizon 6.0 이전에서 위치 기반 인쇄는 단일 사용자, Windows Desktop 시스템에 배포된 데스크톱에서 지원됩니다.

위치 기반 인쇄 기능을 사용하려면 Horizon Agent와 함께 데스크톱에 가상 인쇄 설정 옵션을 설치하고 올바른 프린터 드라이버도 설치해야 합니다.

**컴퓨터 구성** 아래 **소프트웨어 설정** 폴더의 Microsoft Group Policy Object Editor에 있는 AutoConnect Map Additional Printers for VMware View라는 Active Directory 그룹 정책 설정을 구성하여 위치 기반 인쇄를 설정합니다.

---

**참고** AutoConnect Map Additional Printers for VMware View는 컴퓨터 특정 정책입니다. 컴퓨터 특정 정책은 데스크톱에 연결하는 사람에 관계없이 모든 View 데스크톱에 적용됩니다.

---

AutoConnect Map Additional Printers for VMware View는 이름 변환 테이블로 구현됩니다. 테이블 각 행을 사용하여 특정 프린터를 식별하고 해당 프린터의 번역 규칙을 정의합니다. 번역 규칙은 프린터가 특정 클라이언트 시스템의 View 데스크톱에 매핑되었는지 여부를 결정합니다.

사용자가 View 데스크톱에 연결될 경우 View는 테이블의 각 프린터와 연결된 번역 규칙과 클라이언트 시스템을 비교합니다. 클라이언트 시스템이 프린터의 모든 번역 규칙 세트를 만족하거나 프린터에 연결된 번역 규칙이 없는 경우 View는 사용자 세션 중 View 데스크톱에 프린터를 매핑합니다.

클라이언트 시스템의 IP 주소, 이름 및 MAC 주소 그리고 사용자 이름 및 그룹을 기반으로 번역 규칙을 정의할 수 있습니다. 특정 프린터에 하나의 번역 규칙 또는 여러 번역 규칙 조합을 지정할 수 있습니다.

View 데스크톱에 프린터를 매핑하는 데 사용된 정보는 HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\WthinprintWtpautoconnect의 View 데스크톱 레지스트리 항목에 저장됩니다.

## 위치 기반 인쇄를 위한 프린터 설정

Horizon 6.0.2 이상에서 위치 기반 인쇄를 위한 프린터 설정은 사용자가 데스크톱에서 로그아웃하거나 연결을 끊은 후에도 유지됩니다. 예를 들어 사용자는 흑백 모드를 사용하도록 위치 기반 프린터를 설정할 수 있습니다. 사용자가 데스크톱에서 로그아웃하고 다시 로그인하면 위치 기반 프린터는 흑백 모드를 계속 사용합니다.

호스팅되는 애플리케이션의 전체 세션에 프린터 설정을 저장하려면 사용자는 애플리케이션의 인쇄 대화상자에서 위치 기반 프린터를 선택하고 선택한 프린터를 마우스 오른쪽 버튼으로 클릭한 다음 **인쇄 환경설정**을 선택해야 합니다. 프린터 설정은 사용자가 애플리케이션의 인쇄 대화상자에서 프린터를 선택하고 **환경설정** 버튼을 클릭하는 경우 저장되지 않습니다.

Microsoft의 권장 사항인 프린터 드라이버의 DEVMODE 확장 부분이 아닌 프린터 드라이버의 개인용 공간에 설정이 저장되는 경우 위치 기반 프린터의 지속적 설정은 지원되지 않습니다. 지속적 설정을 지원하려면 프린터 드라이버의 DEVMODE 부분에 설정이 저장된 프린터를 배포하십시오.

## 위치 기반 인쇄 그룹 정책 DLL 파일 등록

위치 기반 인쇄를 위해 그룹 정책 설정을 구성하려면 TPVMGPOACmap.dll DLL 파일을 등록해야 합니다.

VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyyy.zip이라는 이름으로 함께 제공되는 .zip 파일에서 TPVMGPOACmap.dll의 32비트 및 64비트 버전을 사용할 수 있습니다. 여기서 x.x.x는 버전이고 yyyyyyyy는 빌드 번호입니다. VMware Horizon의 6 다운로드 사이트에서 파일을 다운로드할 수 있습니다.

이전 View 릴리스는 View 연결 서버 호스트에 있는 `install_directory\VMware\VMware View\Server\Wextras\GroupPolicyFiles\ThinPrint` 디렉토리에서 TPVMGPOACmap.dll의 32비트 및 64비트 버전을 제공합니다.

### 절차

- 1 TPVMGPOACmap.dll의 적절한 버전을 Active Directory 서버 또는 그룹 정책 구성에 사용할 도메인 컴퓨터에 복사하십시오.
- 2 regsvr32 유틸리티를 사용하여 TPVMGPOACmap.dll 파일을 등록합니다.

예: `regsvr32 "C:\TPVMGPOACmap.dll"`

### 다음에 수행할 작업

위치 기반 인쇄를 위해 그룹 정책 설정을 구성하십시오.

## 위치 기반 인쇄 그룹 정책 구성

위치 기반 인쇄를 설정하려면 AutoConnect Map Additional Printers for VMware View 그룹 정책 설정을 구성합니다. 그룹 정책 설정은 Horizon 데스크톱에 프린터를 매핑하는 이름 변환 테이블입니다.

### 사전 요구 사항

- 그룹 정책 구성에 사용하는 도메인 컴퓨터 또는 Active Directory 서버에서 Microsoft MMC와 그룹 정책 개체 편집기 스냅인을 사용할 수 있는지 확인하십시오.
- 그룹 정책 구성에 사용하는 도메인 컴퓨터 또는 Active Directory 서버에 TPVMGPOACmap.dll을 등록하십시오. [위치 기반 인쇄 그룹 정책 DLL 파일 등록](#)을 참조하십시오.
- AutoConnect Map Additional Printers for VMware View 그룹 정책 설정 구문을 숙지하십시오. [위치 기반 인쇄 그룹 정책 설정 구문](#)을 참조하십시오.
- 위치 기반 그룹 정책 설정에 대한 GPO를 생성하고 Horizon 데스크톱을 포함하는 OU에 연결하십시오. Horizon 그룹 정책에 대한 GPO 생성 방법의 예는 [Horizon 7 그룹 정책에 대한 GPO 생성](#)에 나와 있습니다.
- 가상 인쇄 설정 옵션이 Horizon Agent와 함께 데스크톱에 설치되었는지 확인합니다. TP 자동 연결 서비스와 TP VC 게이트웨이 서비스가 데스크톱 운영 체제에 설치되어 있는지 확인하면 됩니다.

- Horizon 데스크톱에서 프린터로 인쇄 작업을 직접 전송하기 때문에 데스크톱에 필요한 프린터 드라이버가 설치되어 있는지 확인하십시오.

## 절차

- 1 Active Directory 서버에서 GPO를 편집합니다.

AD 버전	탐색 경로
Windows 2003	<ol style="list-style-type: none"> <li>a 시작 &gt; 모든 프로그램 &gt; 관리 도구 &gt; <b>Active Directory 사용자 및 컴퓨터</b>를 선택합니다.</li> <li>b Horizon 데스크톱을 포함하는 OU를 마우스 오른쪽 버튼으로 클릭하고 <b>속성</b>을 선택합니다.</li> <li>c <b>그룹 정책</b> 탭에서 <b>열기</b>를 클릭하여 그룹 정책 관리 플러그인을 엽니다.</li> <li>d 오른쪽 창에서 위치 기반 인쇄 그룹 정책 설정용으로 생성한 GPO를 마우스 오른쪽 단추로 클릭하고 <b>편집</b>을 선택합니다.</li> </ol>
Windows 2008	<ol style="list-style-type: none"> <li>a 시작 &gt; 관리 도구 &gt; <b>그룹 정책 관리</b>를 선택합니다.</li> <li>b 도메인을 확장하고 위치 기반 인쇄 그룹 정책 설정에 대해 생성한 GPO를 마우스 오른쪽 버튼으로 클릭한 다음 <b>편집</b>을 선택합니다.</li> </ol>

**그룹 정책 개체 편집기** 창이 나타납니다.

- 2 컴퓨터 구성을 확장하고 **소프트웨어 설정** 폴더를 연 다음 **VMware View용 추가 프린터 자동 연결 매핑**을 선택합니다.

- 3 정책 창에서 **추가 프린터 자동 연결 매핑 구성**을 두 번 클릭합니다.

**VMware View용 추가 프린터 자동 연결 매핑** 창이 나타납니다.

- 4 그룹 정책 설정을 사용하려면 **사용**을 선택합니다.

그룹 정책 창에 변환 테이블 머리글과 단추가 나타납니다.

**중요** **사용 안 함**을 선택하면 모든 테이블 항목이 삭제됩니다. 예방 조치로 나중에 가져올 수 있도록 구성을 저장하십시오.

- 5 Horizon 데스크톱에 매핑하려는 프린터를 추가하고 관련 변환 규칙을 정의하십시오.

- 6 변경 사항을 저장하려면 **확인**을 클릭합니다.

## 위치 기반 인쇄 그룹 정책 설정 구문

원격 데스크톱에 프린터를 매핑하려면 AutoConnect Map Additional Printers for VMware View 그룹 정책 설정을 사용합니다.

AutoConnect Map Additional Printers for VMware View은 프린터를 식별하고 관련된 변환 규칙을 정의하는 이름 변환 테이블입니다. 표 5-24. 변환 테이블 열 및 값에서는 변환 테이블 구문을 설명합니다.

위치 기반 인쇄는 원격 데스크톱에 로컬 프린터를 매핑하지만, UNC 경로를 사용하여 구성된 네트워크 프린터 매핑은 지원하지 않습니다.



표 5-24. 변환 테이블 열 및 값

열	설명
IP Range	<p>클라이언트 시스템의 IP 주소 범위를 지정하는 변환 규칙입니다.</p> <p>특정 범위에서 IP 주소를 지정하려면 다음 표기법을 사용합니다.</p> <p><b><i>ip_address-ip_address</i></b></p> <p>예: <b>10.112.116.0-10.112.119.255</b></p> <p>특정 서브넷에서 모든 IP 주소를 지정하려면 다음 표기법을 사용합니다.</p> <p><b><i>ip_address/subnet_mask_bits</i></b></p> <p>예: <b>10.112.4.0/22</b></p> <p>이 표기법은 사용 가능한 IPv4 주소를 10.112.4.1에서 10.112.7.254로 지정합니다.</p> <p>임의의 IP 주소에 맞추려면 별표를 입력하십시오.</p>
Client Name	<p>컴퓨터 이름을 지정하는 변환 규칙입니다.</p> <p>예: <b>Mary's Computer</b></p> <p>임의의 컴퓨터 이름에 맞추려면 별표를 입력하십시오.</p>
Mac Address	<p>MAC 주소를 지정하는 변환 규칙입니다. GPO 편집기에서는 클라이언트 시스템에서 사용하는 형식과 동일한 형식을 사용해야 합니다. 예:</p> <ul style="list-style-type: none"> <li>■ Windows 클라이언트는 다음과 같이 하이픈을 사용합니다. <b>01-23-45-67-89-ab</b></li> <li>■ Linux 클라이언트는 다음과 같이 콜론을 사용합니다. <b>01:23:45:67:89:ab</b></li> </ul> <p>임의의 MAC 주소에 맞추려면 별표를 입력하십시오.</p>
User/Group	<p>사용자 또는 그룹 이름을 지정하는 변환 규칙입니다.</p> <p>특정 사용자 또는 그룹을 지정하려면 다음 표기법을 사용합니다.</p> <p><b><i>\\domain\user_or_group</i></b></p> <p>예: <b>\\mydomain\Mary</b></p> <p>FQDN(정규화된 도메인 이름)은 도메인 이름에 대해 지원되는 표기법이 아닙니다. 임의의 사용자 또는 그룹 이름을 지정하려면 별표를 입력하십시오.</p>
Printer Name	<p>원격 데스크톱에 매핑된 프린터 이름입니다.</p> <p>예: <b>PRINTER-2-CLR</b></p> <p>매핑된 이름과 클라이언트 시스템에 있는 프린터 이름을 맞추지 않아도 됩니다.</p> <p>프린터는 클라이언트 디바이스에 대해 로컬로 존재해야 합니다. UNC 경로의 네트워크 프린터 매핑은 지원되지 않습니다.</p>
Printer Driver	<p>프린터에서 사용하는 드라이버 이름입니다.</p> <p>예: <b>HP Color LaserJet 4700 PS</b></p> <p><b>중요</b> 데스크톱에서 프린터로 인쇄 작업을 직접 전송하기 때문에 데스크톱에 프린터 드라이버를 설치해야 합니다.</p>
IP Port/ThinPrint Port	<p>네트워크 프린터의 경우 프린터 IP 주소는 <b>IP_</b>로 표시됩니다.</p> <p>예: <b>IP_10.114.24.1</b></p> <p>기본 포트는 9100입니다. IP 주소에 포트 번호를 추가하여 기본값이 아닌 포트를 지정할 수 있습니다.</p> <p>예: <b>IP_10.114.24.1:9104</b></p>
Default	<p>프린터가 기본 프린터인지 여부를 표시합니다.</p>

열 머리글 위에 있는 단추를 사용해 행을 추가, 삭제, 이동하고 테이블 항목을 저장 및 내보낼 수 있습니다. 각 단추는 바로 가기 키와 동일합니다. 마우스를 각 단추 위로 가져가면 단추에 대한 설명 및 동일한 바로 가기 키를 확인할 수 있습니다. 예를 들어, 테이블 끝에 행을 삽입하려면 첫 번째 테이블 단추를 클릭하거나 Alt+A를 누르십시오. 테이블 항목을 내보내고 저장하려면 마지막 단추 2개를 클릭합니다.

표 5-25. 위치 기반 인쇄 그룹 정책 설정 예제에서는 변환 테이블 행 두 개를 예로 보여줍니다.

표 5-25. 위치 기반 인쇄 그룹 정책 설정 예제

IP 범위	클라이언트 이름	Mac 주소	사용자/그룹	프린터 이름	프린터 드라이버	IP 포트/ ThinPrint 포트	기본값
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.14 0-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

모든 변환 규칙 열에 별표가 나타나기 때문에 첫 번째 행에 지정된 네트워크 프린터가 모든 클라이언트 시스템의 원격 데스크톱에 매핑됩니다. 클라이언트 시스템의 IP 주소가 10.112.116.140부터 10.112.116.145 범위에 있는 경우에만 두 번째 행에 지정된 네트워크 프린터가 원격 데스크톱에 매핑됩니다.

## Active Directory 그룹 정책 예제

원격 데스크톱 세션을 전달하는 Horizon 7 시스템에 대한 OU를 생성한 다음 해당 OU에 하나 이상의 GPO를 연결하면 Horizon 7에서 Active Directory 그룹 정책을 구현할 수 있습니다. 이러한 GPO를 사용하여 Horizon 7 시스템에 그룹 정책 설정을 적용할 수 있습니다.

정책 설정이 도메인의 모든 컴퓨터에 적용되는 경우 도메인에 GPO를 직접 연결할 수 있습니다. 하지만 대부분의 배포에서는 개별 OU에 GPO를 연결하여 정책이 도메인의 모든 컴퓨터에서 처리되는 상황을 방지하는 것이 권장되는 모범 사례입니다.

Active Directory 서버 또는 도메인에 있는 모든 컴퓨터에서 정책을 구성할 수 있습니다. 이 예제에서는 Active Directory 서버에 직접 정책을 구성하는 방법을 보여줍니다.

**참고** 모든 Horizon 7 환경이 동일한 것은 아니기 때문에 조직에 맞는 정책을 구성하려면 다른 단계를 수행해야 할 수도 있습니다.

## Horizon 7 시스템을 위한 OU 생성

동일한 Active Directory 도메인의 다른 Windows 컴퓨터에 영향을 주지 않고 Horizon 7 시스템에 원격 데스크톱 세션을 제공할 그룹 정책을 적용하려면 해당 Horizon 7 시스템 전용으로 사용할 OU를 생성하십시오. 전체 Horizon 7 배포용으로 OU 한 개를 생성하거나, 단일 사용자 시스템과 RDS 호스트용으로 각각의 OU를 생성할 수 있습니다.

## 절차

- 1 Active Directory 서버에서 **시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터**를 선택합니다.
- 2 Horizon 7 시스템이 포함되어 있는 도메인을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 조직 단위**를 선택합니다.
- 3 OU 이름을 입력하고 **확인**를 클릭합니다.  
새 OU가 왼쪽 창에 표시됩니다.
- 4 새 OU에 Horizon 7 시스템을 추가하려면
  - a 왼쪽 창에서 **컴퓨터**를 클릭합니다.  
도메인의 모든 컴퓨터 개체가 오른쪽 창에 표시됩니다.
  - b 오른쪽 패널에서 Horizon 7 시스템을 나타내는 컴퓨터 개체 이름을 마우스 오른쪽 버튼으로 클릭하고 **이동**을 선택합니다.
  - c OU를 선택하고 **확인**을 클릭합니다.  
OU를 선택하면 오른쪽 창에 Horizon 7 시스템이 표시됩니다.

## 다음에 수행할 작업

Horizon 7 그룹 정책에 대한 GPO를 생성합니다.

## Horizon 7 그룹 정책에 대한 GPO 생성

Horizon 7 구성 요소와 위치 기반 인쇄에 대한 그룹 정책을 포함하는 GPO를 생성하고 Horizon 7 시스템의 OU에 연결하십시오.

## 사전 요구 사항

- Horizon 7 시스템의 OU를 생성합니다.
- Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.

## 절차

- 1 Active Directory 서버에서 그룹 정책 관리 콘솔을 엽니다.

AD 버전	탐색 경로
Windows 2012	서버 관리자 > 도구 > 그룹 정책 관리를 선택합니다.
Windows 2008	시작 > 관리 도구 > 그룹 정책 관리를 선택합니다.
Windows 2003	<ol style="list-style-type: none"> <li>a 시작 &gt; 모든 프로그램 &gt; 관리 도구 &gt; Active Directory 사용자 및 컴퓨터를 선택합니다.</li> <li>b Horizon 7 시스템이 포함되어 있는 OU를 마우스 오른쪽 버튼으로 클릭하고 <b>속성</b>을 선택합니다.</li> <li>c <b>그룹 정책</b> 탭에서 <b>열기</b>를 클릭하여 그룹 정책 관리 플러그인을 엽니다.</li> </ol>

- 2 도메인을 확장하고 Horizon 7 시스템이 포함되어 있는 OU를 마우스 오른쪽 버튼으로 클릭한 다음 **이 도메인에서 GPO를 만들어 여기에 연결**을 선택합니다.

Windows 2003 Active Directory에서는 이 옵션을 **GPO를 만들어 여기에 연결**이라고 합니다.

- 3 GPO 이름을 입력하고 **확인**을 클릭합니다.

새 GPO가 왼쪽 창 OU 아래에 표시됩니다.

- 4 (선택 사항) OU의 특정 Horizon 7 시스템에만 GPO를 적용하려면 다음을 수행하십시오.

a 왼쪽 창에서 GPO를 선택합니다.

b **보안 필터링 > 추가**를 선택합니다.

c Horizon 7 시스템의 컴퓨터 이름을 입력하고 **확인**을 클릭합니다.

보안 필터링 창에 Horizon 7 시스템이 나타납니다. 이들 시스템에만 GPO 설정이 적용됩니다.

다음에 수행할 작업

그룹 정책의 GPO에 Horizon ADMX 템플릿을 추가하십시오.

## GPO에 Horizon 7 ADMX 템플릿 파일 추가

게시된 데스크톱과 애플리케이션에 Horizon 7 구성 요소 그룹 정책 설정을 적용하려면 GPO에 해당 ADMX 템플릿 파일을 추가해야 합니다.

사전 요구 사항

- Horizon 7 구성 요소 그룹 정책 설정에 대한 GPO를 생성하고 Horizon 7 시스템이 포함된 OU에 연결합니다.
- Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.

Windows 2012, Windows 2008 및 Windows 2003 Active Directory 버전에 따라 그룹 정책 관리 콘솔을 여는 방법이 다릅니다. [Horizon 7 그룹 정책에 대한 GPO 생성](#)을 참조하십시오.

절차

- 1 Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip입니다. 여기서 x.x.x는 버전이고 yyyyyy는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일의 압축을 풀고 ADMX 파일을 Active Directory 또는 RDS 호스트에 복사합니다.
  - a .admx 파일과 ko-KR 폴더를 Active Directory 또는 RDS 호스트의 %systemroot%\PolicyDefinitions 폴더에 복사합니다.
  - b 언어 리소스 파일(.adml)을 Active Directory 또는 RDS 호스트의 %systemroot%\PolicyDefinitions\에 있는 적절한 하위 폴더에 복사합니다.
- 3 Active Directory 호스트에서 그룹 정책 관리 편집기를 열고, 설치 후에 편집기에 나타나는 템플릿 파일 경로를 입력합니다.
 

개별 RDS 호스트에서는 gpedit.msc 유틸리티를 사용하여 로컬 그룹 정책 편집기를 열 수 있습니다.

#### 다음에 수행할 작업

그룹 정책 설정을 구성하고 Horizon 7 시스템에 대한 루프백 처리를 사용하도록 설정합니다.

## 원격 데스크톱에 대해 루프백 처리를 사용하도록 설정

컴퓨터에 일반적으로 적용되는 사용자 구성 설정을 해당 컴퓨터에 로그인하는 모든 사용자에게 적용하려면 루프백 처리를 사용하도록 설정하십시오.

#### 사전 요구 사항

- Horizon 7 구성 요소 그룹 정책 설정에 대한 GPO를 생성하고 Horizon 7 시스템이 포함된 OU에 연결합니다.
  - Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.
- Windows 2012, Windows 2008 및 Windows 2003 Active Directory 버전에 따라 그룹 정책 관리 콘솔을 여는 방법이 다릅니다. [Horizon 7 그룹 정책에 대한 GPO 생성](#)을 참조하십시오.

#### 절차

- 1 Active Directory 서버에서 그룹 정책 관리 콘솔을 엽니다.
- 2 도메인을 확장하고 그룹 정책 설정에 대해 생성했던 GPO를 오른쪽 클릭하고 **편집**을 선택합니다.
- 3 **그룹 정책 편집기**에서 **컴퓨터 구성 > 정책 > 관리 템플릿: 정책 정의 > 시스템 > 그룹 정책**으로 이동합니다.
- 4 오른쪽 창에서 **사용자 그룹 정책 루프백 처리 모드**를 두 번 클릭합니다.
- 5 **사용**을 선택한 다음 **모드** 드롭다운 메뉴에서 루프백 처리 모드를 선택합니다.

옵션	조치
병합	컴퓨터 및 사용자 GPO에 포함되어 있는 사용자 정책 설정을 조합해 적용합니다. 충돌이 발생하면 컴퓨터 GPO가 우선합니다.
교체	컴퓨터와 관련된 GPO에서 전체 사용자 정책을 정의합니다. 사용자와 관련된 GPO는 모두 무시됩니다.

**6** 변경 사항을 저장하려면 **확인**을 클릭합니다.

## Active Directory 그룹 정책 예제

원격 데스크톱 세션을 전달하는 Horizon 7 시스템에 대한 OU를 생성한 다음 해당 OU에 하나 이상의 GPO를 연결하면 Horizon 7에서 Active Directory 그룹 정책을 구현할 수 있습니다. 이러한 GPO를 사용하여 Horizon 7 시스템에 그룹 정책 설정을 적용할 수 있습니다.

정책 설정이 도메인의 모든 컴퓨터에 적용되는 경우 도메인에 GPO를 직접 연결할 수 있습니다. 하지만 대부분의 배포에서는 개별 OU에 GPO를 연결하여 정책이 도메인의 모든 컴퓨터에서 처리되는 상황을 방지하는 것이 권장되는 모범 사례입니다.

Active Directory 서버 또는 도메인에 있는 모든 컴퓨터에서 정책을 구성할 수 있습니다. 이 예제에서는 Active Directory 서버에 직접 정책을 구성하는 방법을 보여줍니다.

---

**참고** 모든 Horizon 7 환경이 동일한 것은 아니기 때문에 조직에 맞는 정책을 구성하려면 다른 단계를 수행해야 할 수도 있습니다.

---

### Horizon 7 시스템을 위한 OU 생성

동일한 Active Directory 도메인의 다른 Windows 컴퓨터에 영향을 주지 않고 Horizon 7 시스템에 원격 데스크톱 세션을 제공할 그룹 정책을 적용하려면 해당 Horizon 7 시스템 전용으로 사용할 OU를 생성하십시오. 전체 Horizon 7 배포용으로 OU 한 개를 생성하거나, 단일 사용자 시스템과 RDS 호스트용으로 각각의 OU를 생성할 수 있습니다.

#### 절차

- 1 Active Directory 서버에서 **시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터**를 선택합니다.
- 2 Horizon 7 시스템이 포함되어 있는 도메인을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 조직 단위**를 선택합니다.
- 3 OU 이름을 입력하고 **확인**을 클릭합니다.  
새 OU가 왼쪽 창에 표시됩니다.

#### 4 새 OU에 Horizon 7 시스템을 추가하려면

- a 왼쪽 창에서 **컴퓨터**를 클릭합니다.  
도메인의 모든 컴퓨터 개체가 오른쪽 창에 표시됩니다.
- b 오른쪽 패널에서 Horizon 7 시스템을 나타내는 컴퓨터 개체 이름을 마우스 오른쪽 버튼으로 클릭하고 **이동**을 선택합니다.
- c OU를 선택하고 **확인**을 클릭합니다.  
OU를 선택하면 오른쪽 창에 Horizon 7 시스템이 표시됩니다.

#### 다음에 수행할 작업

Horizon 7 그룹 정책에 대한 GPO를 생성합니다.

## Horizon 7 그룹 정책에 대한 GPO 생성

Horizon 7 구성 요소와 위치 기반 인쇄에 대한 그룹 정책을 포함하는 GPO를 생성하고 Horizon 7 시스템의 OU에 연결하십시오.

#### 사전 요구 사항

- Horizon 7 시스템의 OU를 생성합니다.
- Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.

#### 절차

- 1 Active Directory 서버에서 그룹 정책 관리 콘솔을 엽니다.

AD 버전	탐색 경로
Windows 2012	서버 관리자 > 도구 > 그룹 정책 관리를 선택합니다.
Windows 2008	시작 > 관리 도구 > 그룹 정책 관리를 선택합니다.
Windows 2003	<ol style="list-style-type: none"> <li>a 시작 &gt; 모든 프로그램 &gt; 관리 도구 &gt; Active Directory 사용자 및 컴퓨터를 선택합니다.</li> <li>b Horizon 7 시스템이 포함되어 있는 OU를 마우스 오른쪽 버튼으로 클릭하고 <b>속성</b>을 선택합니다.</li> <li>c <b>그룹 정책</b> 탭에서 <b>열기</b>를 클릭하여 그룹 정책 관리 플러그인을 엽니다.</li> </ol>

- 2 도메인을 확장하고 Horizon 7 시스템이 포함되어 있는 OU를 마우스 오른쪽 버튼으로 클릭한 다음 **이 도메인에서 GPO를 만들어 여기에 연결**을 선택합니다.

Windows 2003 Active Directory에서는 이 옵션을 **GPO를 만들어 여기에 연결**이라고 합니다.

- 3 GPO 이름을 입력하고 **확인**를 클릭합니다.

새 GPO가 왼쪽 창 OU 아래에 표시됩니다.



**4** (선택 사항) OU의 특정 Horizon 7 시스템에만 GPO를 적용하려면 다음을 수행하십시오.

- a 왼쪽 창에서 GPO를 선택합니다.
- b **보안 필터링 > 추가**를 선택합니다.
- c Horizon 7 시스템의 컴퓨터 이름을 입력하고 **확인**을 클릭합니다.

보안 필터링 창에 Horizon 7 시스템이 나타납니다. 이들 시스템에만 GPO 설정이 적용됩니다.

다음에 수행할 작업

그룹 정책의 GPO에 Horizon ADMX 템플릿을 추가하십시오.

## GPO에 Horizon 7 ADMX 템플릿 파일 추가

게시된 데스크톱과 애플리케이션에 Horizon 7 구성 요소 그룹 정책 설정을 적용하려면 GPO에 해당 ADMX 템플릿 파일을 추가해야 합니다.

사전 요구 사항

- Horizon 7 구성 요소 그룹 정책 설정에 대한 GPO를 생성하고 Horizon 7 시스템이 포함된 OU에 연결합니다.
- Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.

Windows 2012, Windows 2008 및 Windows 2003 Active Directory 버전에 따라 그룹 정책 관리 콘솔을 여는 방법이 다릅니다. [Horizon 7 그룹 정책에 대한 GPO 생성](#)을 참조하십시오.

절차

- 1** Horizon 7 GPO 번들 .zip 파일을 <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 다운로드합니다.

Desktop & End-User Computing에서 GPO 번들이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이 파일의 이름은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip입니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다. Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 이 파일에서 제공됩니다.

- 2** VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일의 압축을 풀고 ADMX 파일을 Active Directory 또는 RDS 호스트에 복사합니다.

- a .admx 파일과 ko-KR 폴더를 Active Directory 또는 RDS 호스트의 %systemroot%\WPolicyDefinitions 폴더에 복사합니다.
- b 언어 리소스 파일(.adml)을 Active Directory 또는 RDS 호스트의 %systemroot%\WPolicyDefinitions\에 있는 적절한 하위 폴더에 복사합니다.

- 3 Active Directory 호스트에서 그룹 정책 관리 편집기를 열고, 설치 후에 편집기에 나타나는 템플릿 파일 경로를 입력합니다.

개별 RDS 호스트에서는 gpedit.msc 유틸리티를 사용하여 로컬 그룹 정책 편집기를 열 수 있습니다.

다음에 수행할 작업

그룹 정책 설정을 구성하고 Horizon 7 시스템에 대한 루프백 처리를 사용하도록 설정합니다.

## 원격 데스크톱에 대해 루프백 처리를 사용하도록 설정

컴퓨터에 일반적으로 적용되는 사용자 구성 설정을 해당 컴퓨터에 로그인하는 모든 사용자에게 적용하려면 루프백 처리를 사용하도록 설정하십시오.

사전 요구 사항

- Horizon 7 구성 요소 그룹 정책 설정에 대한 GPO를 생성하고 Horizon 7 시스템이 포함된 OU에 연결합니다.
- Active Directory 서버에서 그룹 정책 관리 기능을 사용할 수 있는지 확인합니다.

Windows 2012, Windows 2008 및 Windows 2003 Active Directory 버전에 따라 그룹 정책 관리 콘솔을 여는 방법이 다릅니다. [Horizon 7 그룹 정책에 대한 GPO 생성](#)를 참조하십시오.

절차

- 1 Active Directory 서버에서 그룹 정책 관리 콘솔을 엽니다.
- 2 도메인을 확장하고 그룹 정책 설정에 대해 생성했던 GPO를 오른쪽 클릭하고 **편집**을 선택합니다.
- 3 **그룹 정책 편집기**에서 **컴퓨터 구성 > 정책 > 관리 템플릿: 정책 정의 > 시스템 > 그룹 정책**으로 이동합니다.
- 4 오른쪽 창에서 **사용자 그룹 정책 루프백 처리 모드**를 두 번 클릭합니다.
- 5 **사용**을 선택한 다음 **모드** 드롭다운 메뉴에서 루프백 처리 모드를 선택합니다.

옵션	조치
<b>병합</b>	컴퓨터 및 사용자 GPO에 포함되어 있는 사용자 정책 설정을 조합해 적용합니다. 충돌이 발생하면 컴퓨터 GPO가 우선합니다.
<b>교체</b>	컴퓨터와 관련된 GPO에서 전체 사용자 정책을 정의합니다. 사용자와 관련된 GPO는 모두 무시됩니다.

- 6 변경 사항을 저장하려면 **확인**을 클릭합니다.