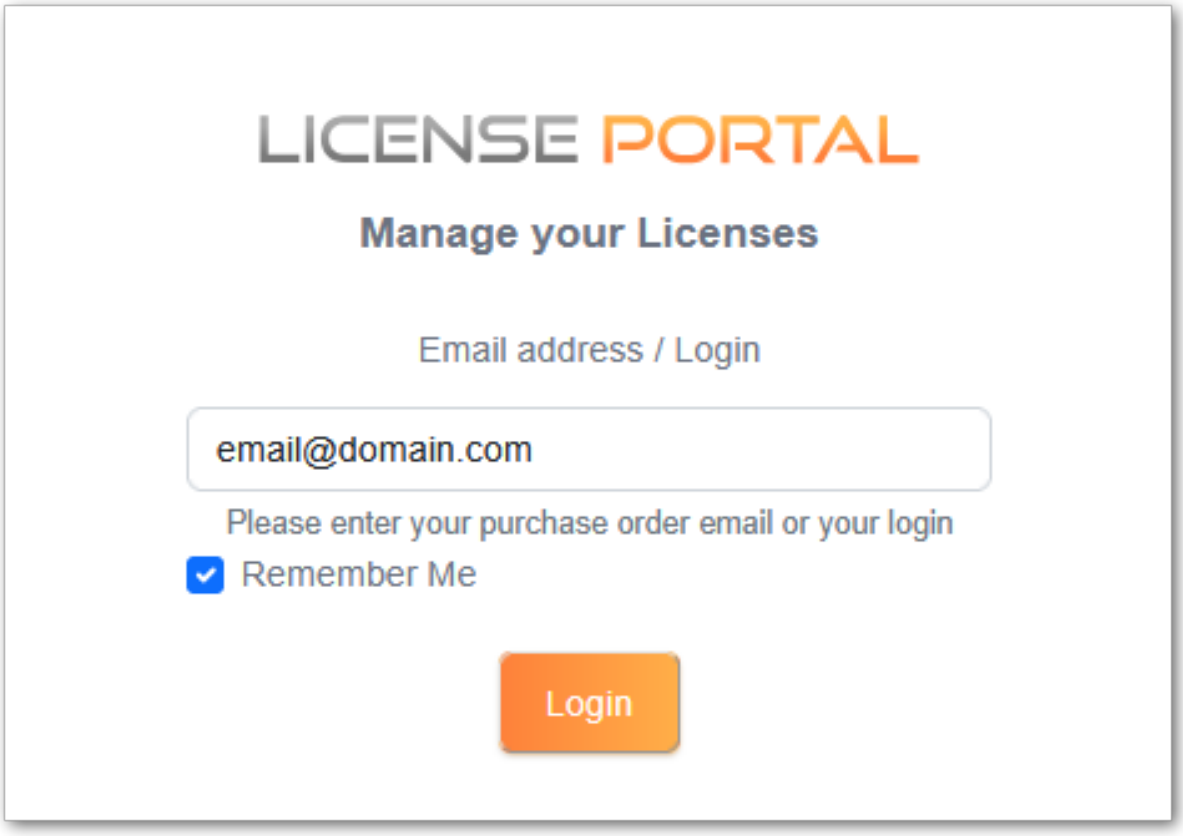
TSplus 영구 라이센스 활성화 (오프라인)

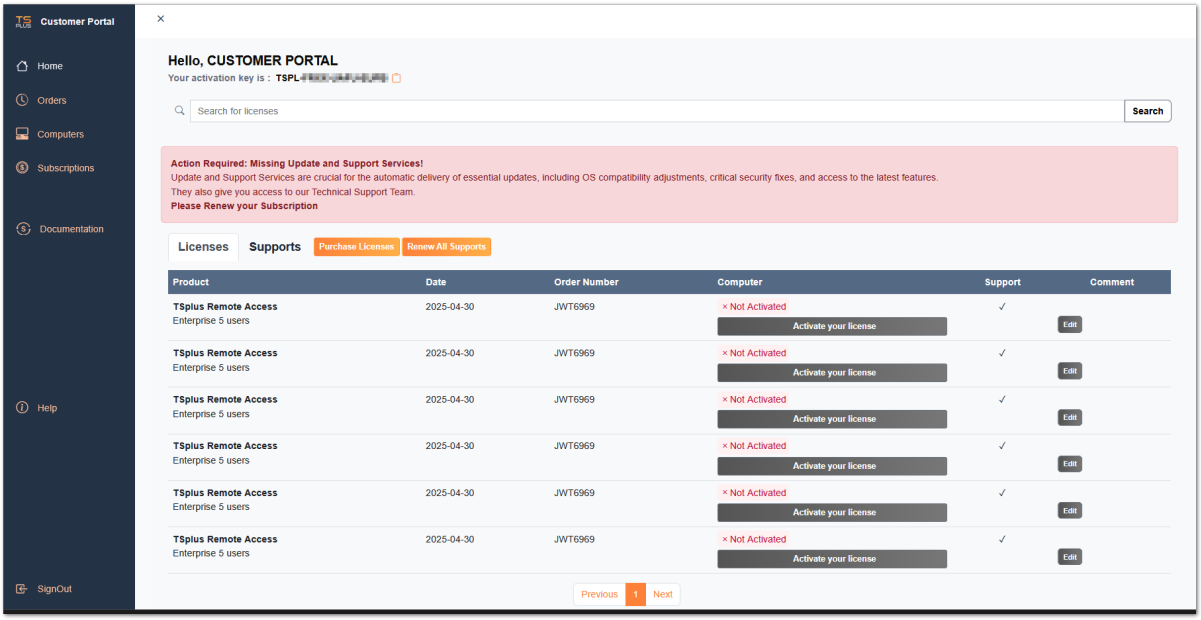
귀하의 활성화 키를 검색하십시오

라이센스를 주문할 때, 저희에게 연결하세요. 라이센스 포털 이메일 주소와 주문 번호를 입력하세요.

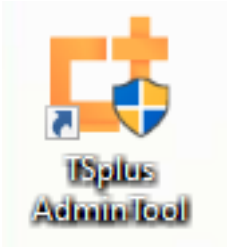


고객 포털 사용자 가이드 다운로드 사용 방법에 대한 자세한 정보는 다음을 참조하십시오.

귀하의 활성화 키는 대시보드 상단에 표시됩니다:



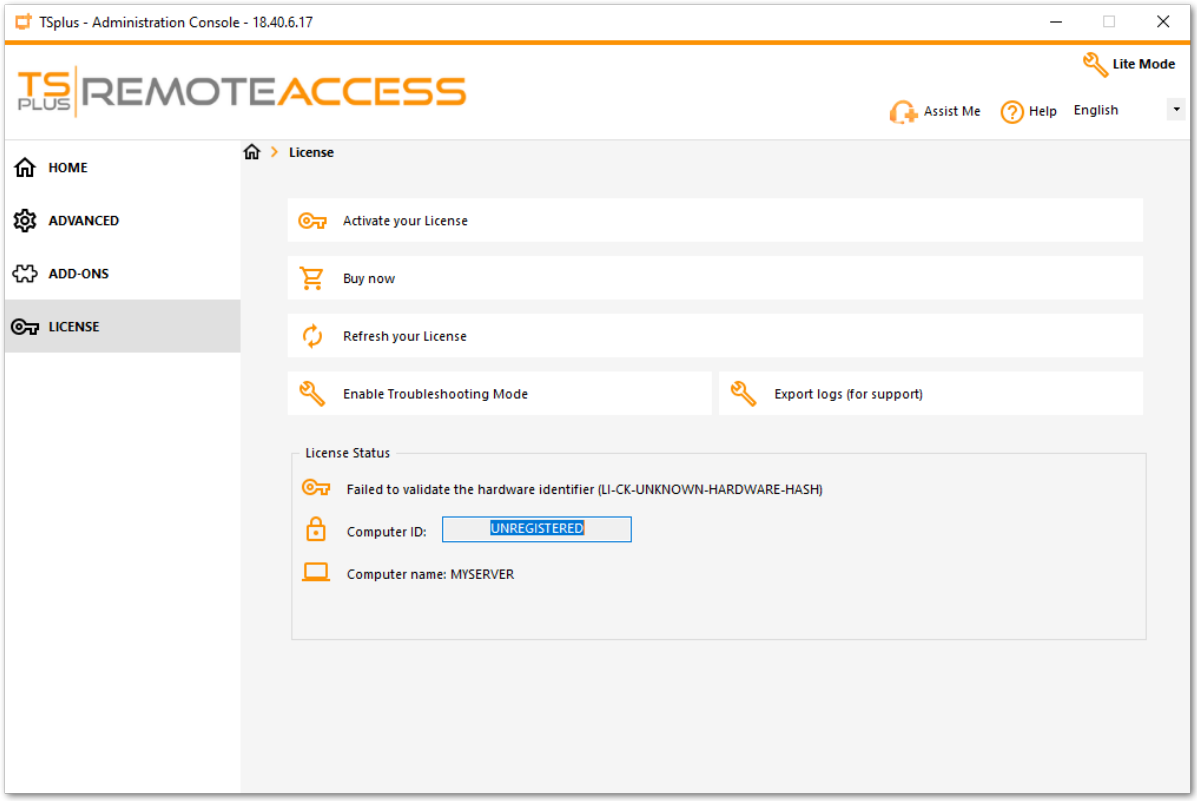
바탕 화면에서 관리자 도구를 찾으세요.



관리자 도구 바로가기를 찾을 수 없는 경우, TSplus를 다운로드하는 데 사용된 관리자 계정의 바탕 화면 폴더에 있어야 합니다. 또한 이 경로에서 TSplus 폴더를 찾을 수 있습니다: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

두 번 클릭한 후 라이센스 탭을 클릭하세요.

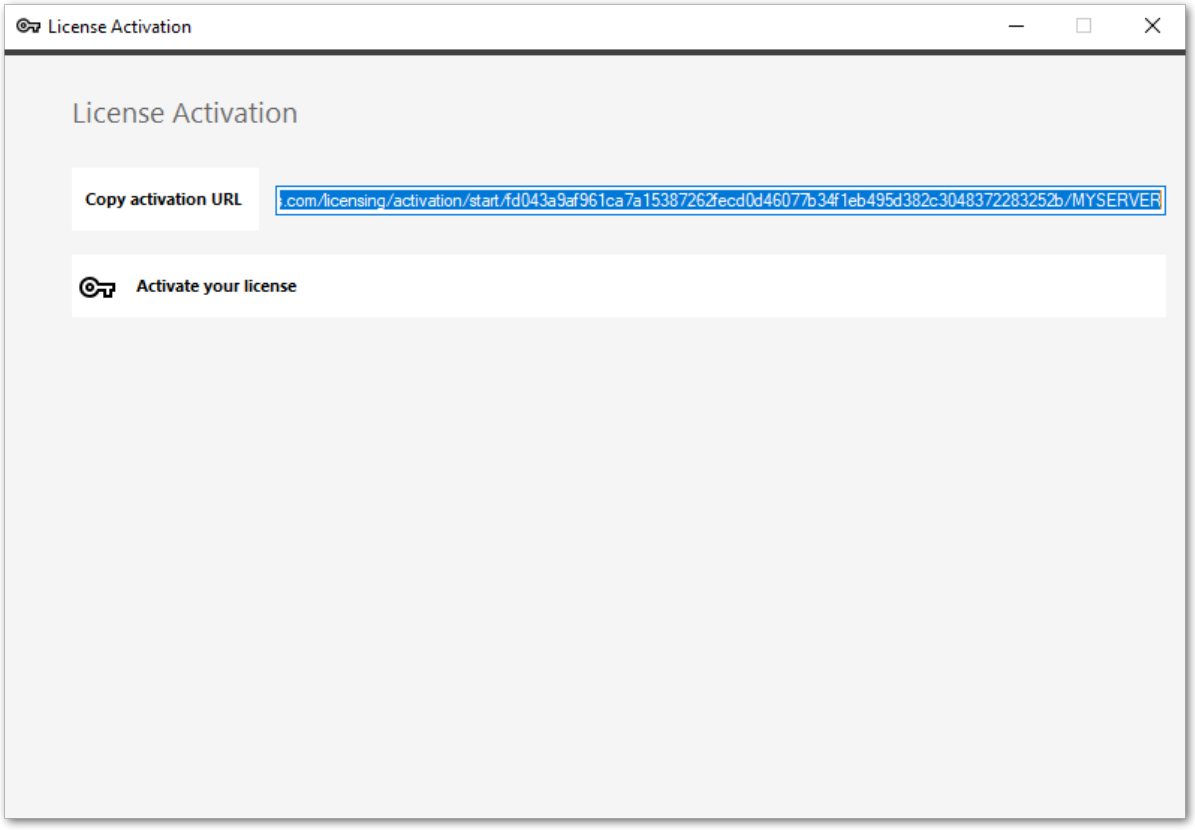
여기에서 TSplus 라이센스의 상태와 컴퓨터 ID 및 컴퓨터 이름 "UNREGISTERED"를 확인할 수 있습니다.



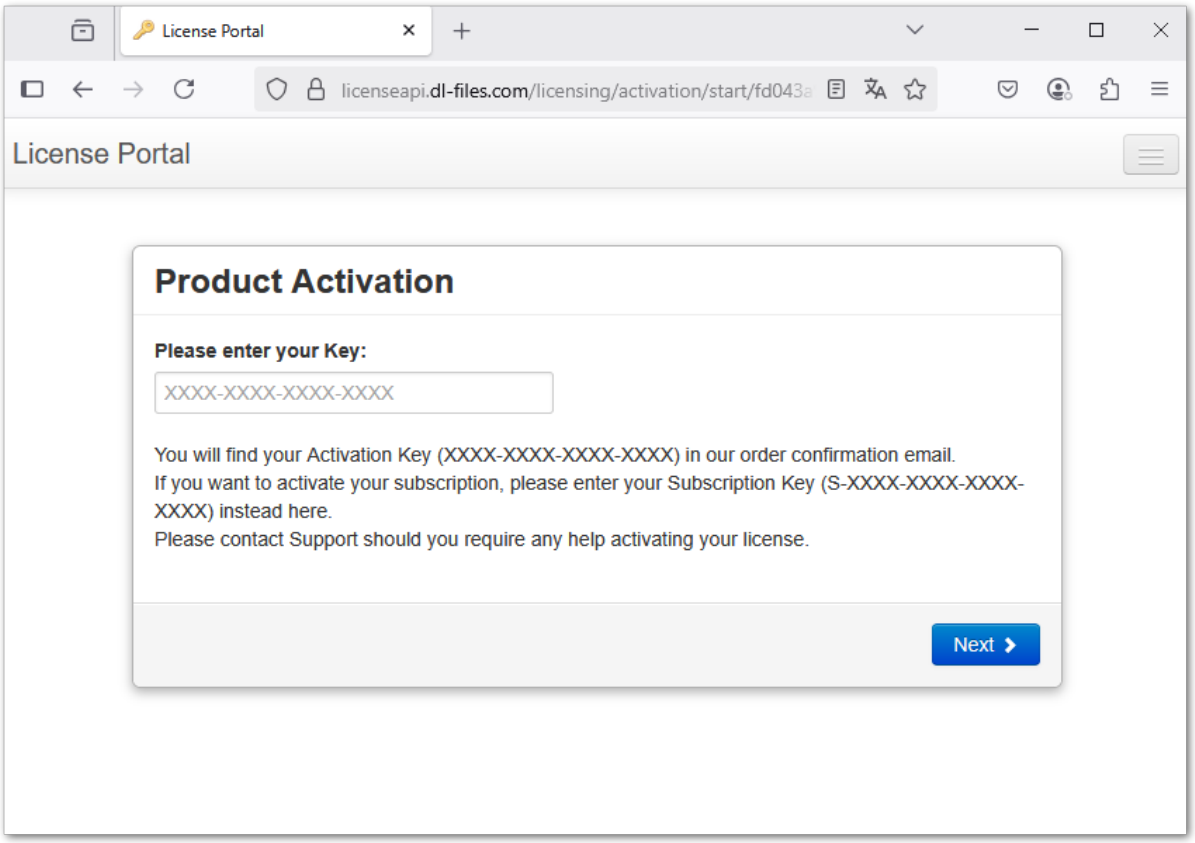
오프라인 TSplus 서버에서 라이센스를 활성화하세요.

“라이센스 활성화” 버튼을 클릭하세요. 팝업이 나타나고 꽤 긴 URL 주소가 표시됩니다.

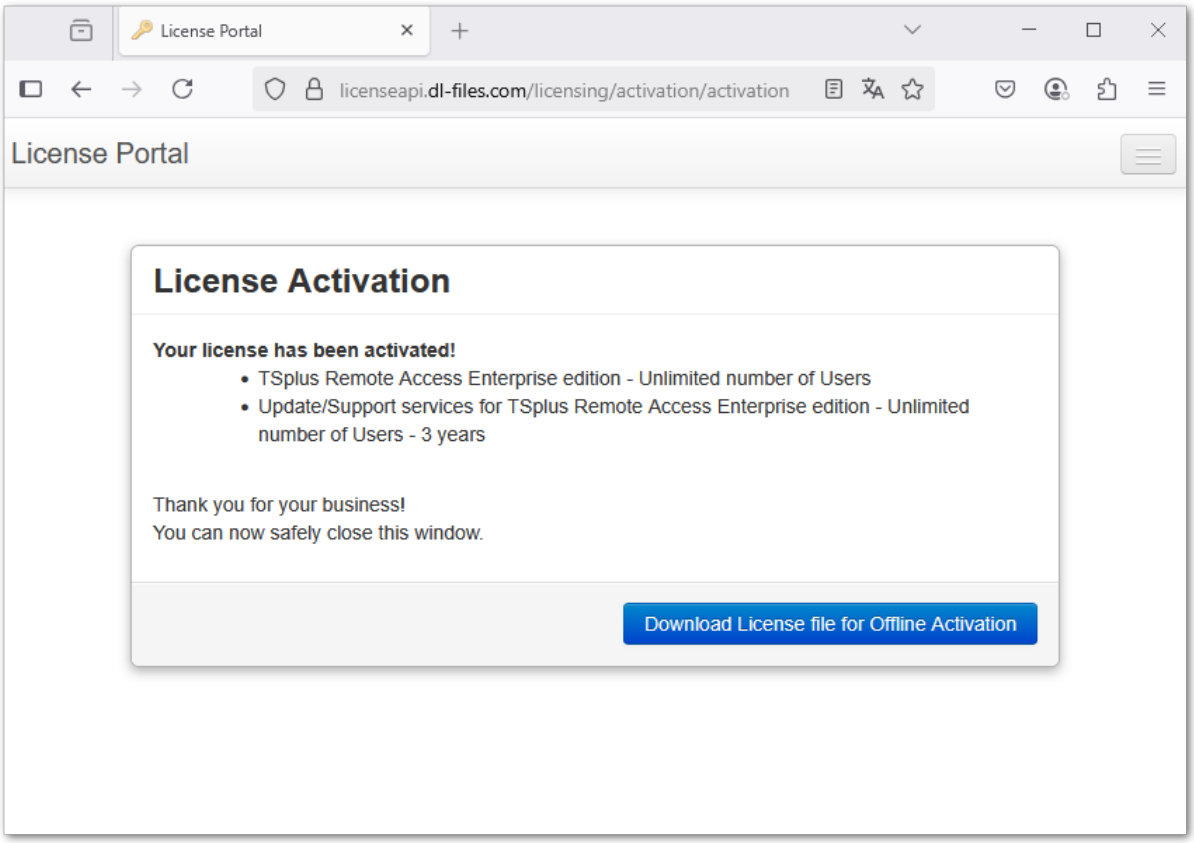
이 URL을 인터넷에 연결된 컴퓨터 브라우저에 복사하여 라이센스 파일을 가져오세요:



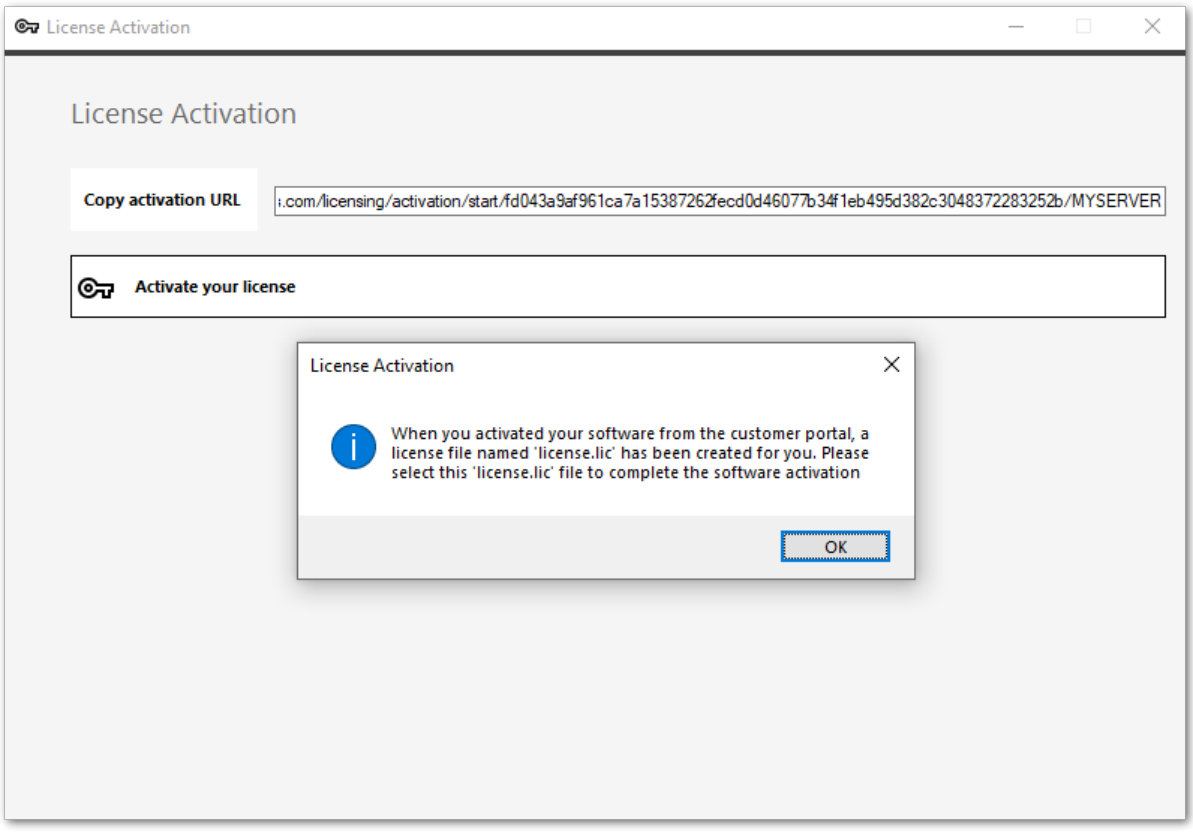
활성화 키를 입력하세요:

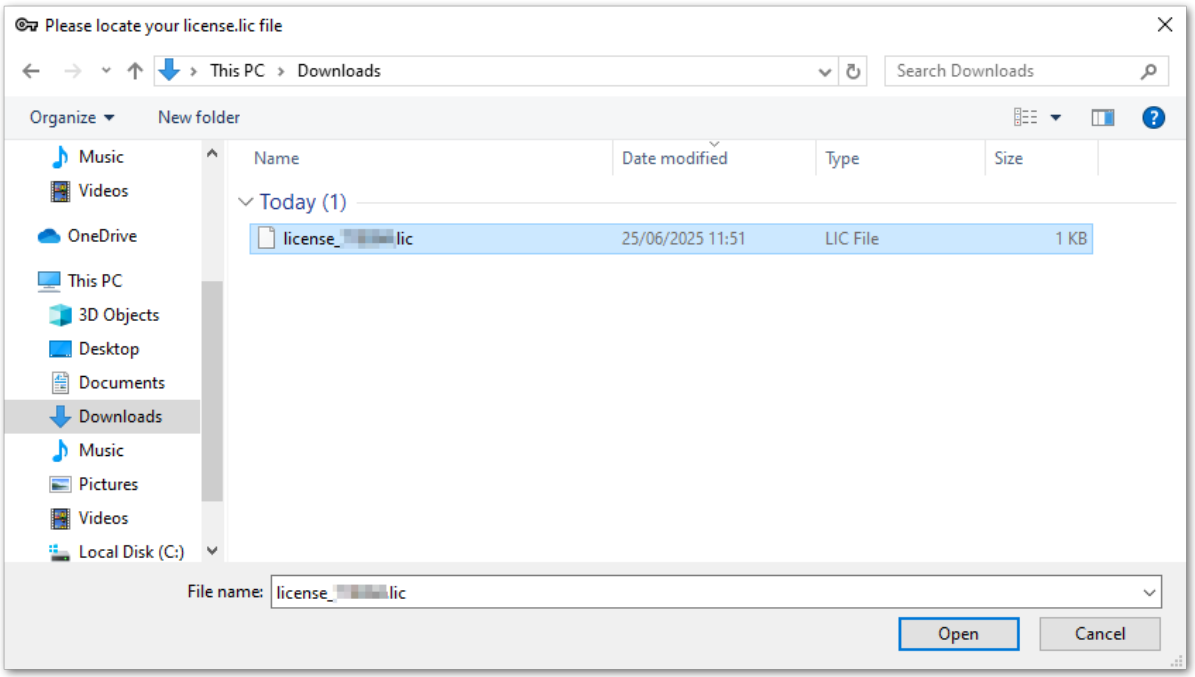


귀하의 라이센스가 확인됩니다. 해당 버튼을 클릭하여 라이센스 파일을 다운로드하십시오.

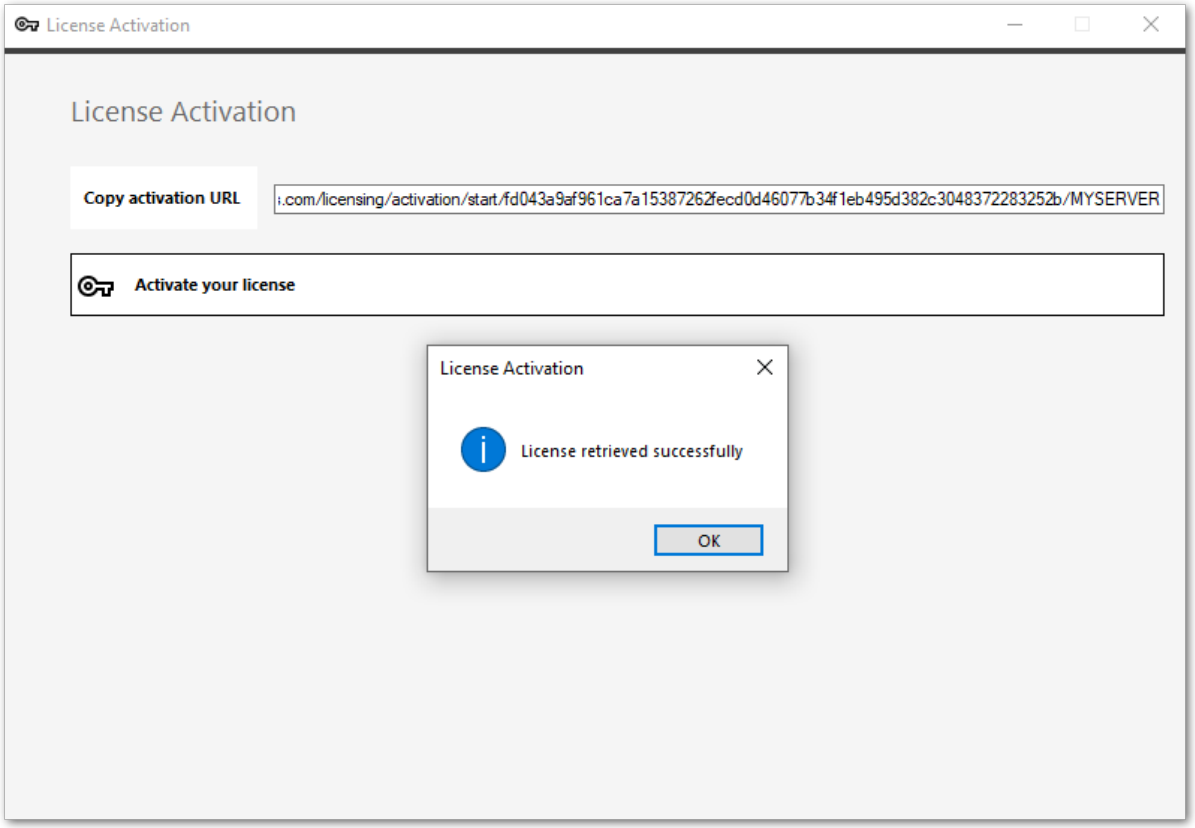


이 라이센스 파일은 오프라인 활성화 프로세스를 완료하기 위해 서버에 다시 복사되어야 합니다.





라이센스가 성공적으로 검색되었음을 확인하는 메시지가 표시됩니다:

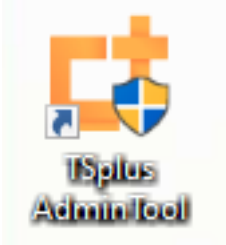


해당 라이센스/지원 항목을 선택하여 활성화해야 하며, 모든 제품/지원이 이제 활성화되었다는 확인 메시지가 표시됩니다.

참고 사항 여전히 TSplus 레거시 버전용 라이센스 포털에서 license.lic 파일을 다운로드할 수 있습니다. 고객 포털 사용자 가이드 다운로드 .

TSplus 라이센스 활성화 (온라인) 영구 또는 구독.

바탕 화면에서 관리자 도구 찾기 :

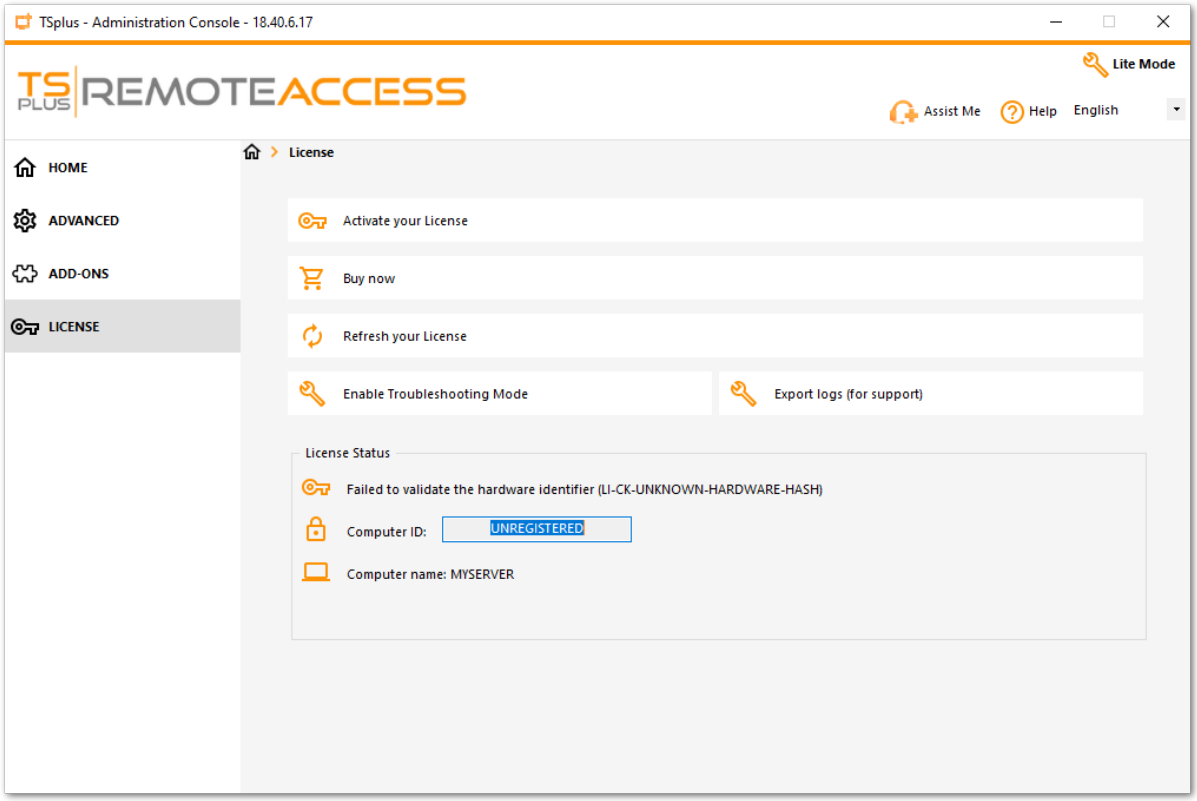


- 관리자 도구 바로가기를 찾을 수 없는 경우, TSplus를 다운로드하는 데 사용된 관리자 계정의 바탕 화면 폴더에 있어야 합니다. 또한 이 경로에서 TSplus 폴더를 찾을 수 있습니다: 'C:\Program Files (x86)\TSplus\UserDesktop\files'.

두 번 클릭한 후 라이센스 탭을 클릭하세요.

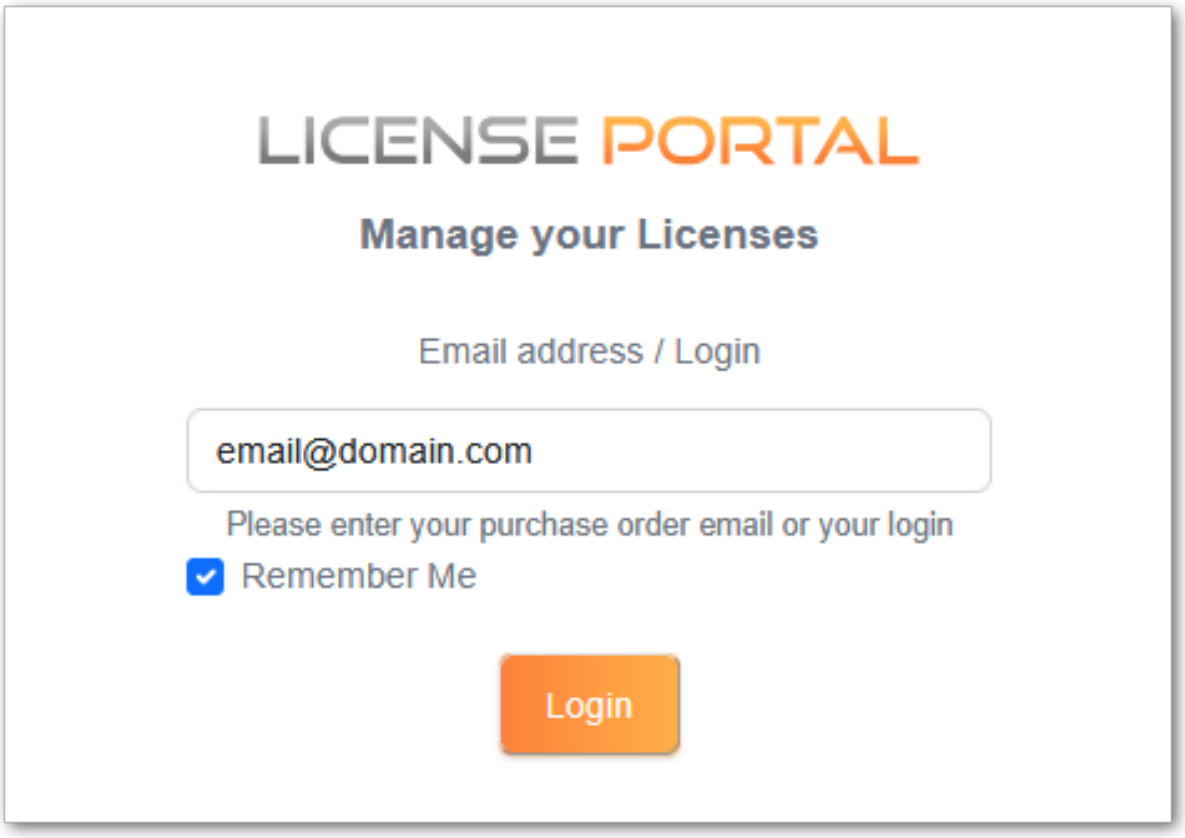
여기에서 TSplus 라이센스의 상태와 컴퓨터 ID 및 컴퓨터 이름을 확인할 수 있습니다.

서버에 "UNREGISTERED"가 표시되면 인터넷에 연결되어 있지 않다는 의미이며, 계속 진행하기 전에 서버의 웹 액세스를 확인해야 합니다.



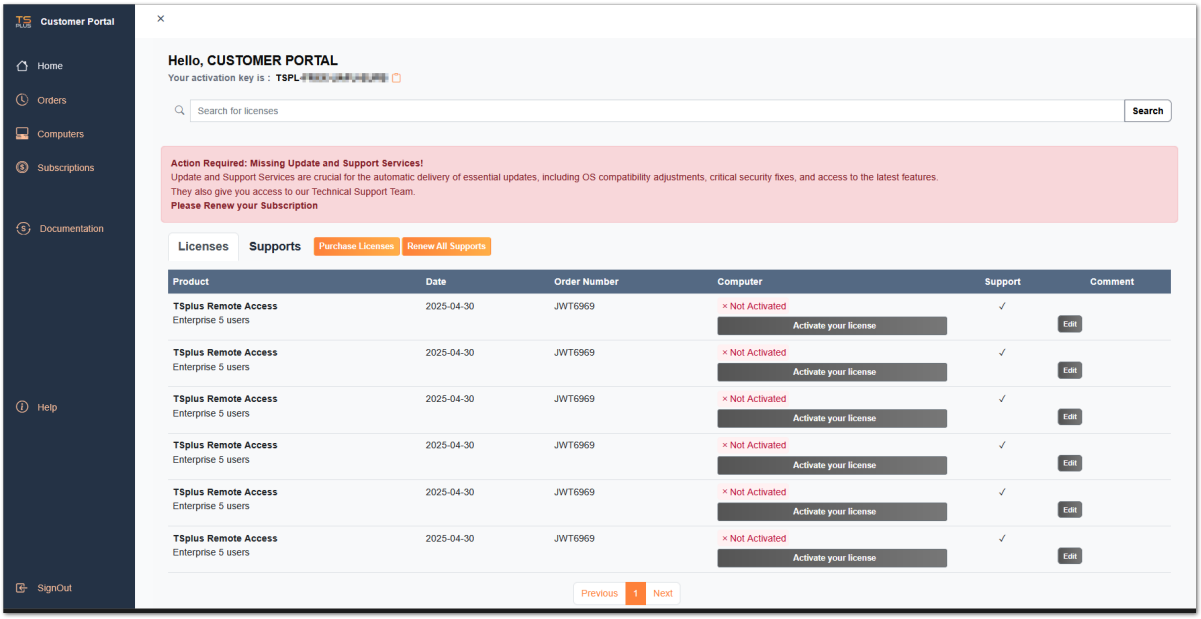
온라인 TSplus 서버에서 라이센스를 활성화하세요.

라이센스를 주문할 때, 저희에게 연결하세요. 라이센스 포털 이메일 주소와 주문 번호를 입력하세요:



고객 포털 사용자 가이드 다운로드 사용 방법에 대한 자세한 정보는 다음을 참조하십시오.

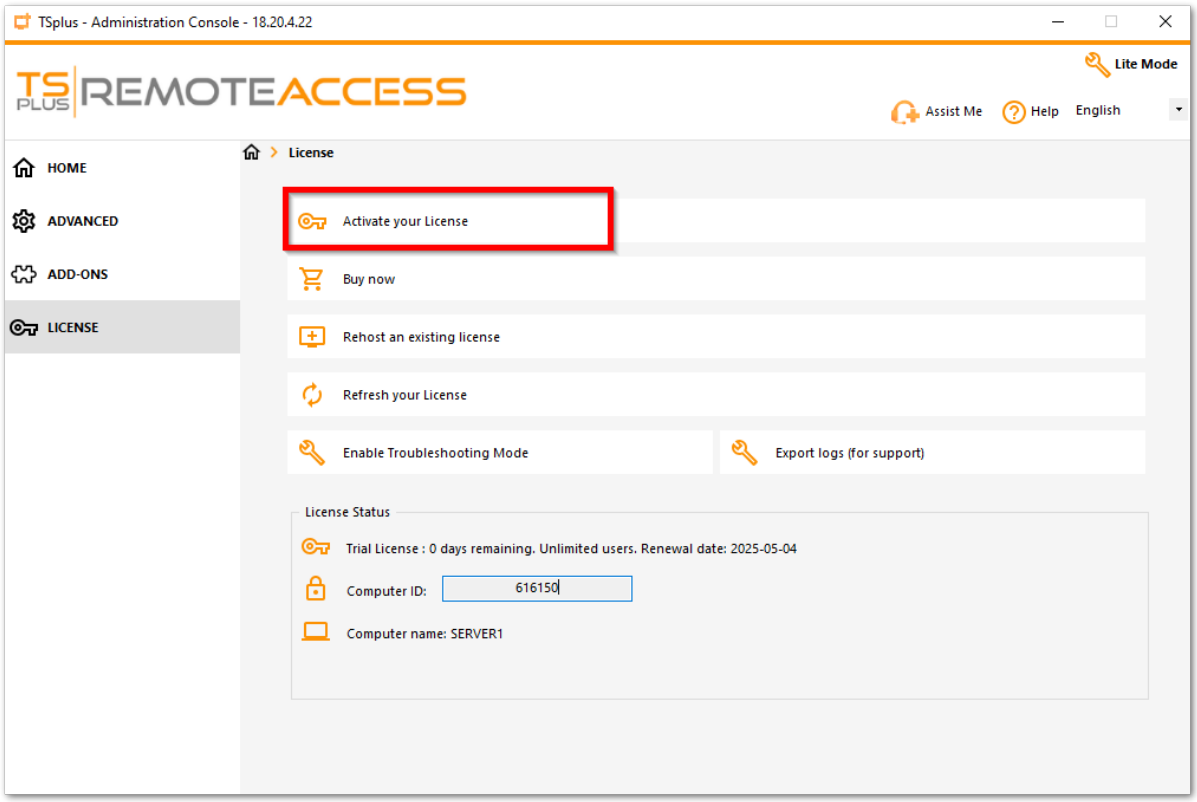
귀하의 활성화 키는 대시보드 상단에 표시됩니다:

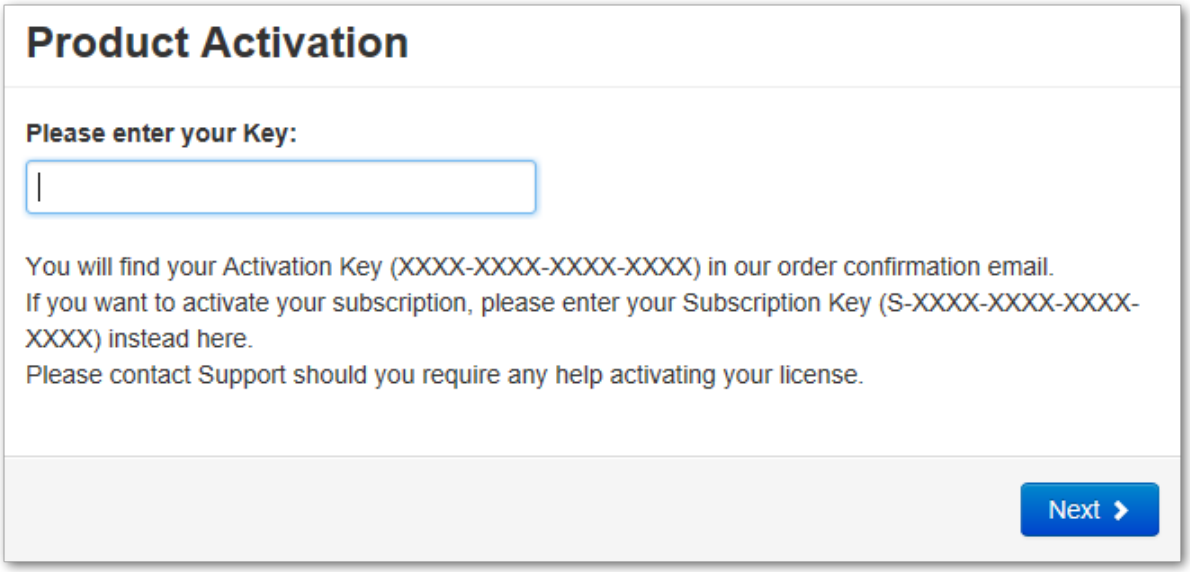


관리 도구의 라이센스 타일로 이동한 후 "라이센스 활성화" 버튼을 클릭하고, 이 활성화 키를 입력한 다음 "다음"을 클릭할 수 있습니다.

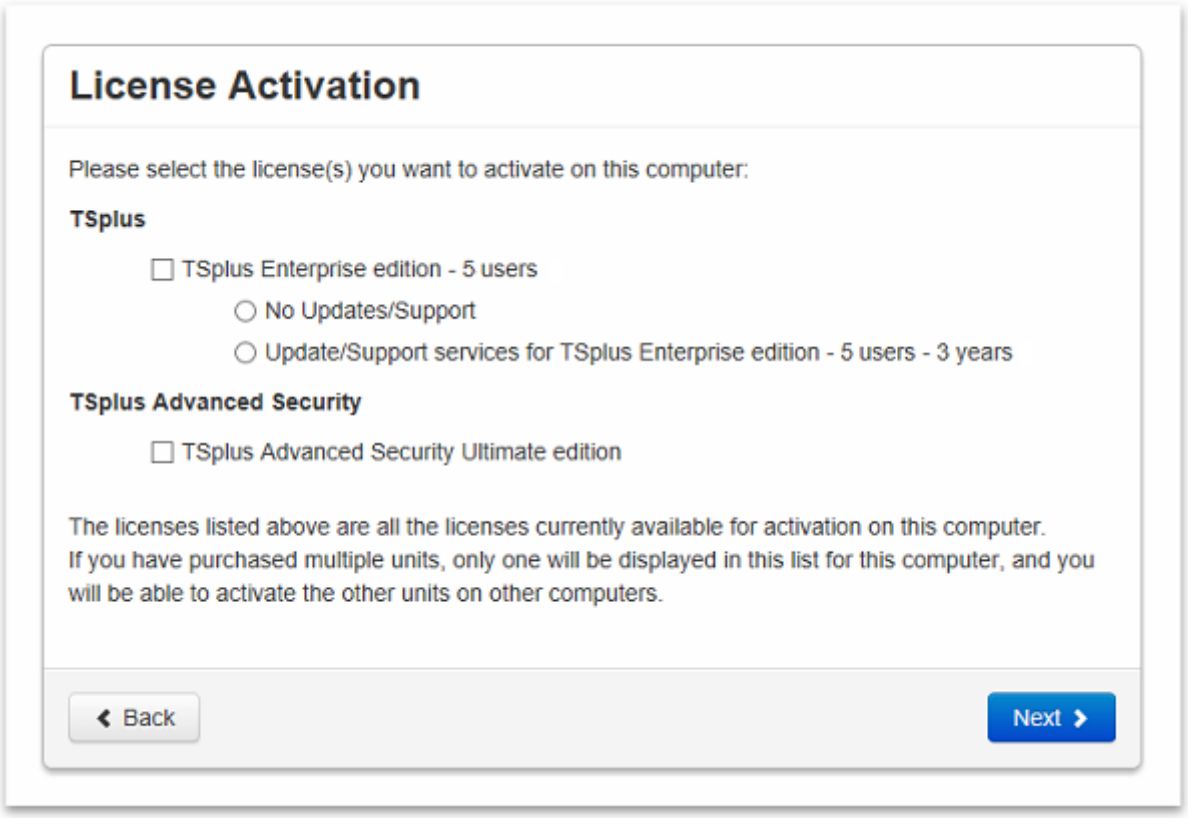
영구 활성화 키를 찾을 수 있습니다. **(XXXX-XXXX-XXXX-XXXX)** 주문 확인 이메일에서.

구독을 활성화하려면 구독 키를 입력해 주십시오. **(S-XXXX-XXXX-XXXX-XXXX)** .

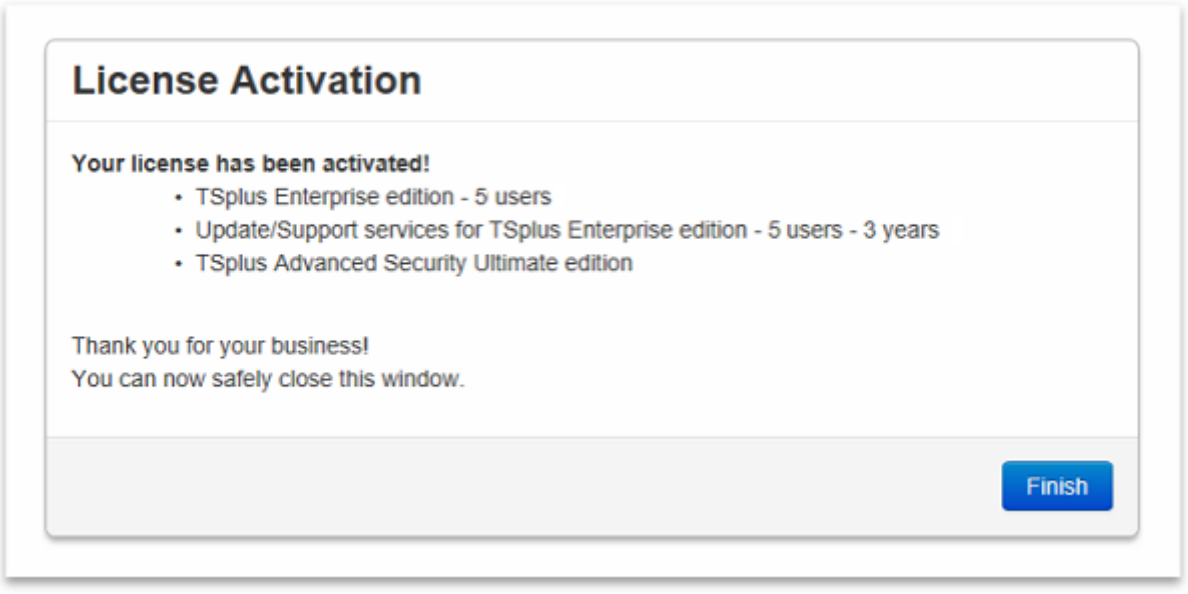




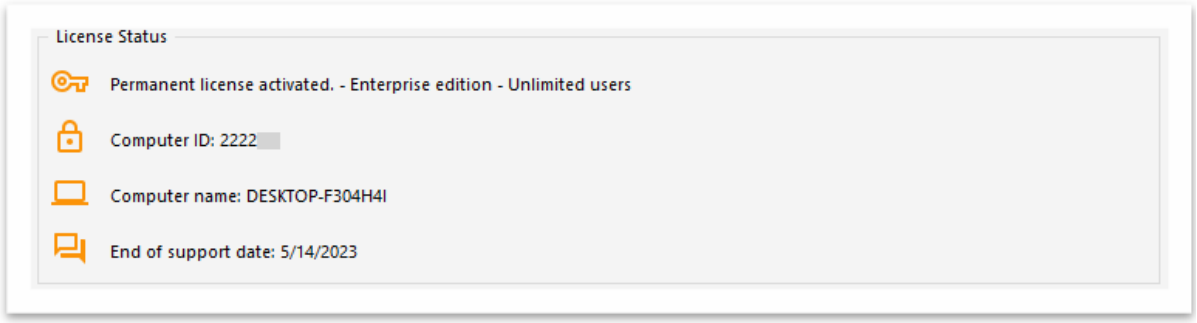
이 활성화 키에 할당된 모든 사용 가능한 라이센스/지원 목록을 받게 됩니다. 즉, 아직 활성화되지 않은 모든 라이센스/지원입니다.



하나 이상의 항목을 선택하고 “다음” 버튼을 클릭하십시오. 여러 제품/지원 항목을 선택하여 동시에 여러 제품을 활성화할 수 있습니다.



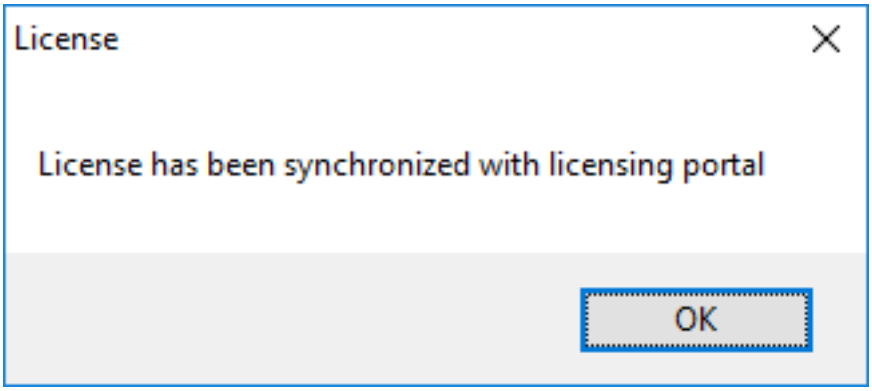
모든 제품/지원이 이제 활성화되었습니다(이 예에서는 TSplus와 지원, TSplus Advanced Security가 동시에 활성화되었습니다).





페이지 하단의 해당 버튼을 클릭하여 라이선스 데이터를 새로 고치면, 라이선스 포털과 정보를 동기화합니다.





참고 사항 여전히 TSplus 레거시 버전용 라이센스 포털에서 license.lic 파일을 다운로드할 수 있습니다. 고객 포털 사용자 가이드 다운로드 .

활성화 문제:

페이지 오류 또는 "다음" 버튼이 작동하지 않습니다. 다음은 몇 가지 해결책입니다.

라이선스 활성화 중에 안티바이러스를 비활성화하고 방화벽 및 안티바이러스 설정을 확인하세요.

이 링크를 클릭하여 브라우저에서 OK 메시지를 확인하세요:
https://licenseapi.dl-files.com/licensing/ping

안티바이러스 프로그램에 문제가 있는 경우, 다음 디렉토리를 제외하는 절차입니다: C:\Program Files (x86)\TSplus 및 C:\wsession

업데이트를 위해 바이러스 백신 및 방화벽에서 허용할 URL: setup.dl-files.com dl-files.com secure-download-file.com

라이센스 / 텔레메트리: 93.88.241.55 업데이트: 51.254.22.117 TSplus 호환성 업데이트 / 업데이트 확인 / 변경 로그 보기: 83.166.153.206

포트 허용: (포트 3389는 WAN에서 RDP용, 포트 80은 HTTP용, 포트 443은 HTTPS용)

인터넷 보안 설정을 확인하세요
제어판 > 인터넷 옵션 > 사용자 지정 수준 스크립트 > 활성 스크립트 > 사용 설정

치명적인 경고 코드 40 70

각 동기화 또는 업데이트 시도 중 이벤트 뷰어에서 치명적인 경고 코드 40/70 TLS를 발견하면.

일부 TLS 암호화 스위트가 비활성화될 수 있습니다. [무료 소프트웨어와 같은] 사용할 수 있습니다. **IIS Crypto 4.0** 확인하고 활성화합니다.

지원 라이센스 활성화

TSplus의 15버전은 연간 지원 계약을 처리하는 새로운 쉽고 간편한 방법을 도입했습니다.

지원 구독은 영구 라이선스에만 제공됩니다. 구독 라이선스에는 업데이트가 포함됩니다.

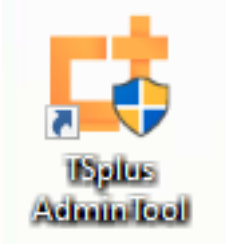
지원 서비스에는 전 세계적인 티켓/이메일 지원 서비스, 포럼 접근, 라이센스 재호스팅, FAQ 및 튜토리얼 지원이 포함됩니다.

업데이트 서비스에는 업데이트 코드의 제공, 새로운 릴리스, 패치 및 업데이트를 설치하고 사용할 권리가 포함됩니다.

우리는 매일 TSplus를 향상시키고 모든 알려진 문제를 해결하기 위해 투자하고 있습니다. 따라서 모든 고객에게 TSplus 설치를 최신 상태로 유지할 것을 권장합니다. 연간 요금은 비싸지 않으며, 저희 스토어 페이지에서 확인할 수 있습니다.

첫 번째 단계

바탕 화면에서 관리 도구 찾기 :



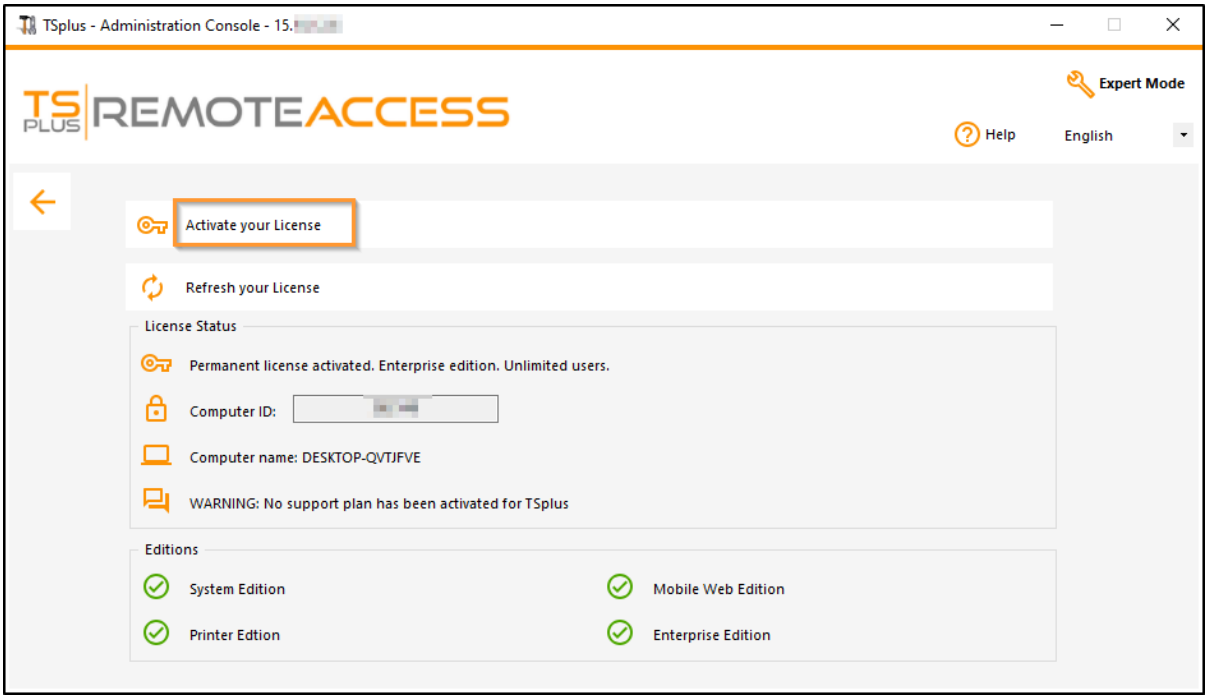
두 번 클릭한 다음 라이센스 타일을 클릭하세요.

- 관리자 도구 바로가기를 찾을 수 없는 경우, TSplus를 다운로드하는 데 사용된 관리자 계정의 바탕 화면 폴더에 있어야 합니다. 또한 이 경로에서 TSplus 폴더를 찾을 수 있습니다: 'C:\Program Files (x86)\TSplus\UserDesktop\files'.

라이센스 탭을 클릭하세요. 이제 일련 번호를 볼 수 있습니다.

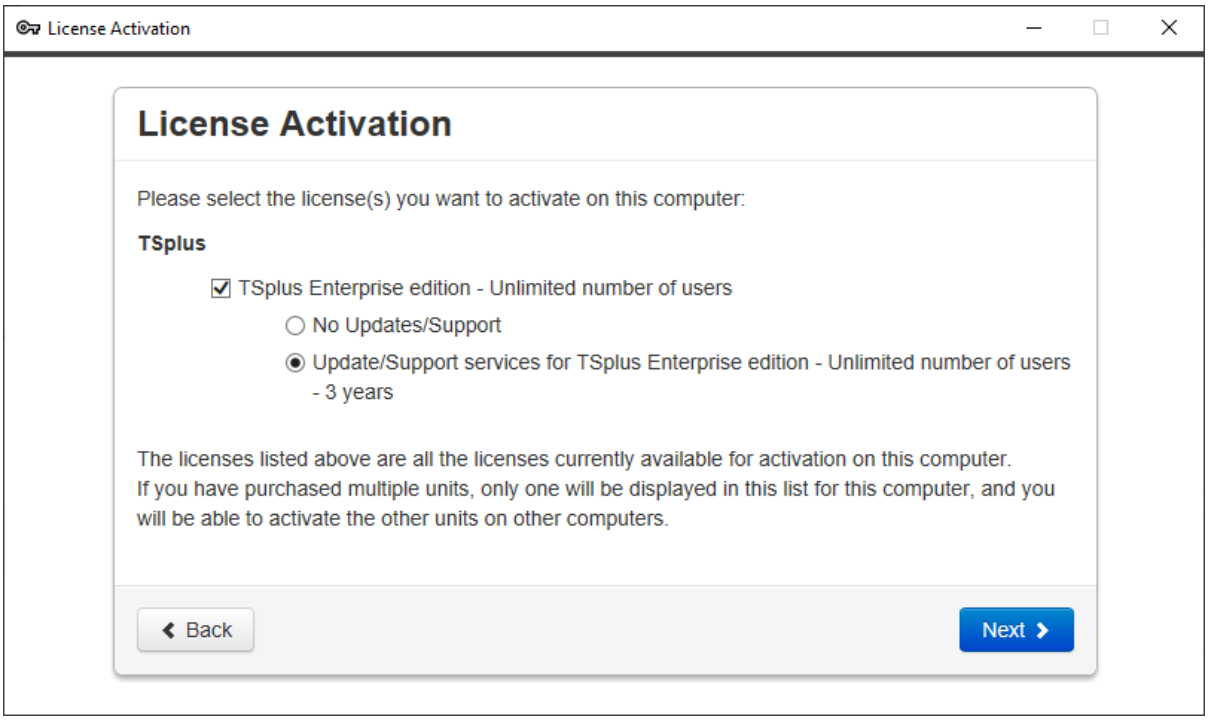
2단계

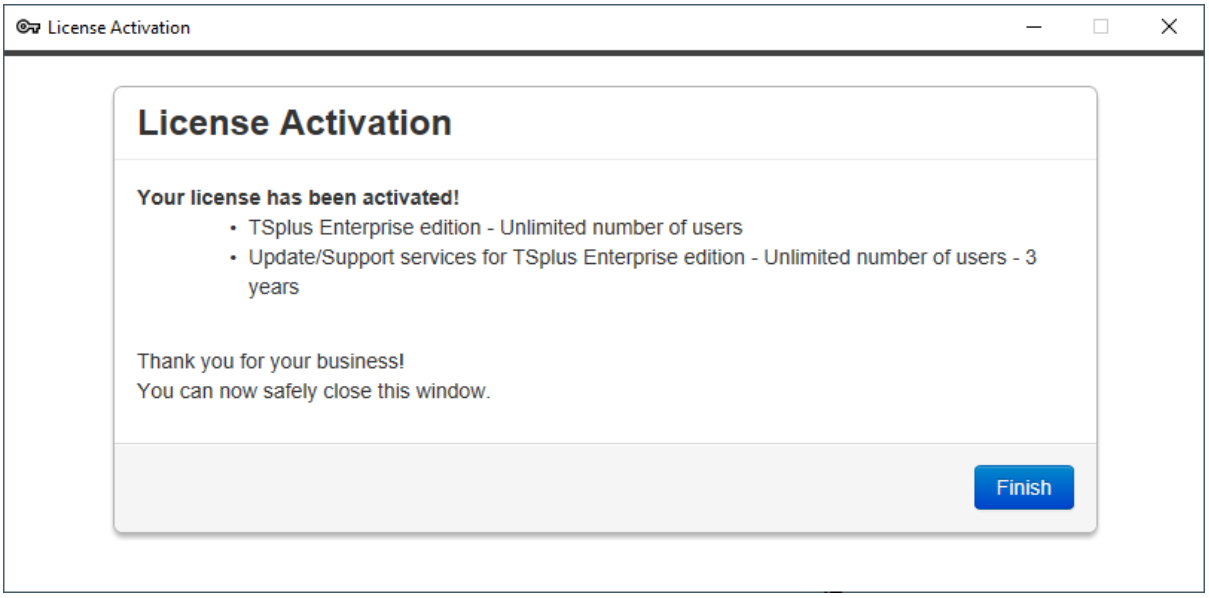
“라이센스 활성화” 타일을 클릭하고 활성화 키를 입력하세요.



3단계

그런 다음 "지원 기간 연장"을 선택하십시오:



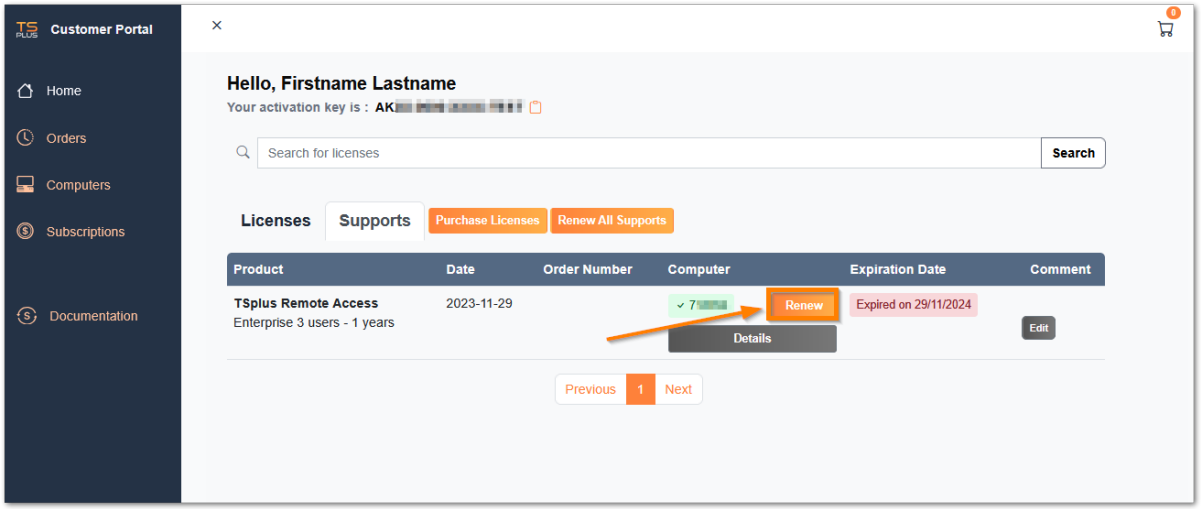


업데이트/지원 구독 연장

라이선스 포털에 액세스하세요: https://license.tsplus.net/login
구매 이메일 주소
비밀번호: “원하는 구매 주문 번호”

그런 다음 지원 탭으로 이동하여 컴퓨터 ID를 입력하십시오(관리 도구의 라이센스 탭에서 확인할 수 있음).

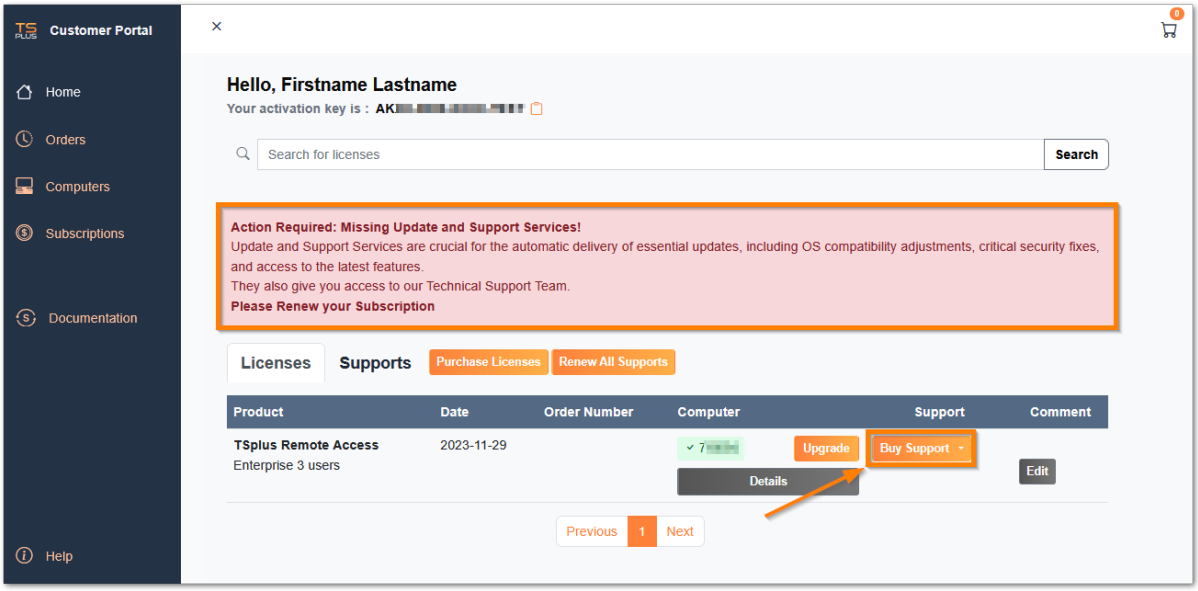
그런 다음 "갱신" 버튼을 클릭하여 1년, 2년 또는 3년 지원 기간을 선택하십시오.



라이센스에 대한 지원 구독이 없으면 라이센스 탭에 다음과 같은 메시지가 표시됩니다.

조치 필요: 업데이트 및 지원 서비스 누락!

지원 구독을 "지원 구매" 버튼을 클릭하여 직접 구매할 수 있습니다.



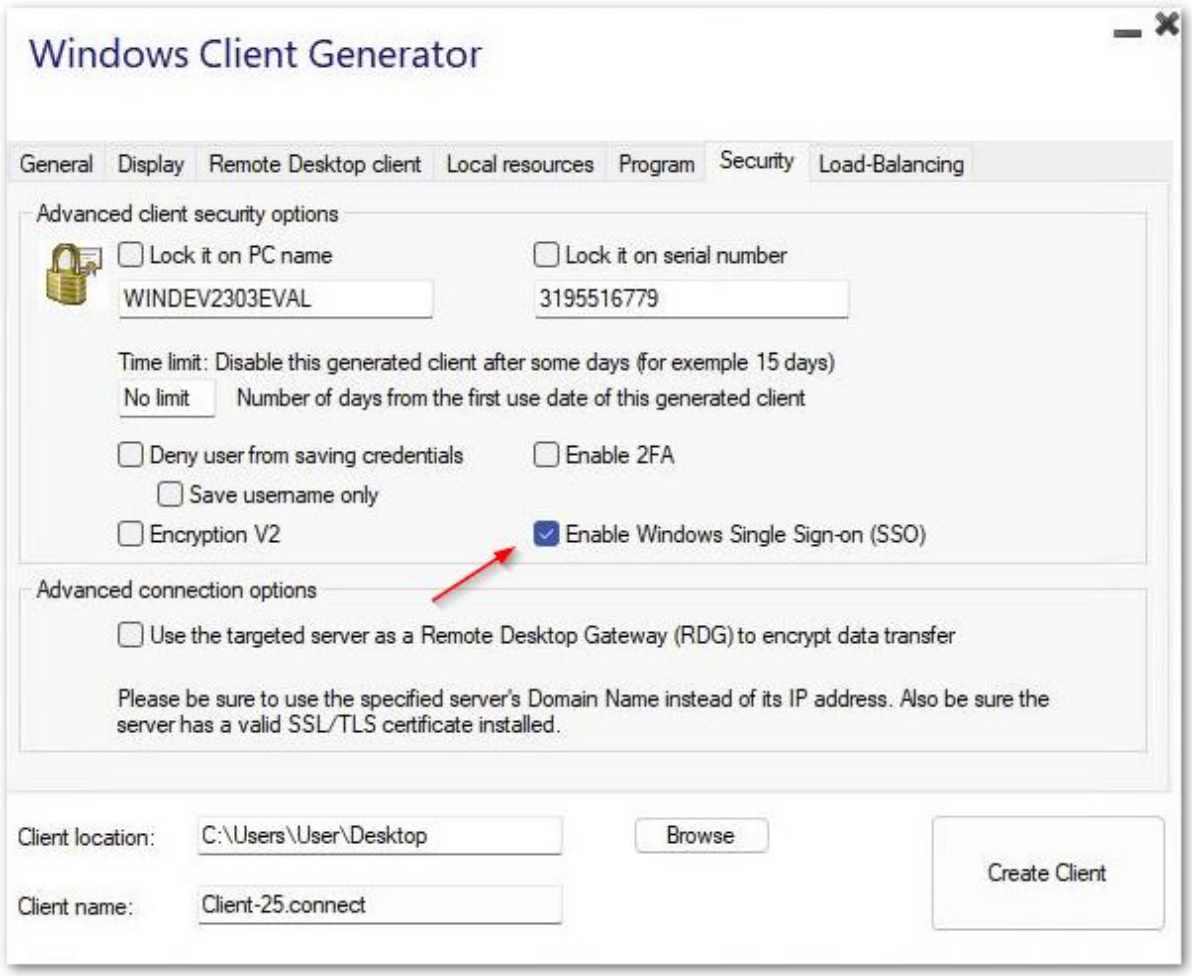
액티브 디렉토리 싱글 사인온

생성된 클라이언트에 대해 Windows SSO 인증을 활성화하려면:

도메인에 가입된 서버에서 TSplus Remote Access를 최신 버전으로 업데이트하십시오.

클라이언트 생성기에서 클라이언트를 생성하고 “보안” 탭에서 “싱글 사인 온(SSO) 활성화” 상자를 체크합니다.

도메인에 가입된 머신에서 생성된 클라이언트를 사용하여 연결합니다.



Windows 원격 데스크톱 클라이언트를 통한 그룹 정책 구성 단일 로그인(SSO)

도메인 컨트롤러에서:

1. 그룹 정책 관리 콘솔을 엽니다.

2. 조직 단위(OU)에서 그룹 정책 개체(GPO)를 적용해야 하는 곳을 마우스 오른쪽 버튼으로 클릭하고 “이 도메인에서 GPO 만들기 및 여기에 링크…”를 선택합니다.

3. GPO의 이름을 지정하고(예: SSO_RDS_MY_SERVER) “확인”을 클릭합니다.

4. 생성된 정책을 마우스 오른쪽 버튼으로 클릭하고 “편집”을 선택합니다.

5. 다음 위치로 이동하십시오: “컴퓨터 구성 / 정책 / 관리 템플릿 / 시스템 / 자격 증명 위임.”

6. “기본 자격 증명 위임 허용”을 두 번 클릭하여 설정을 엽니다.

7. 설정을 활성화하고 “표시…”를 클릭하십시오.

8. 값 필드에 서버를 TERMSRV/server_fully_qualified_domain_name 형식으로 입력하고 “확인”을 클릭합니다.

9. “적용”과 “확인”을 클릭하여 창을 닫습니다. 클라이언트 머신에서:

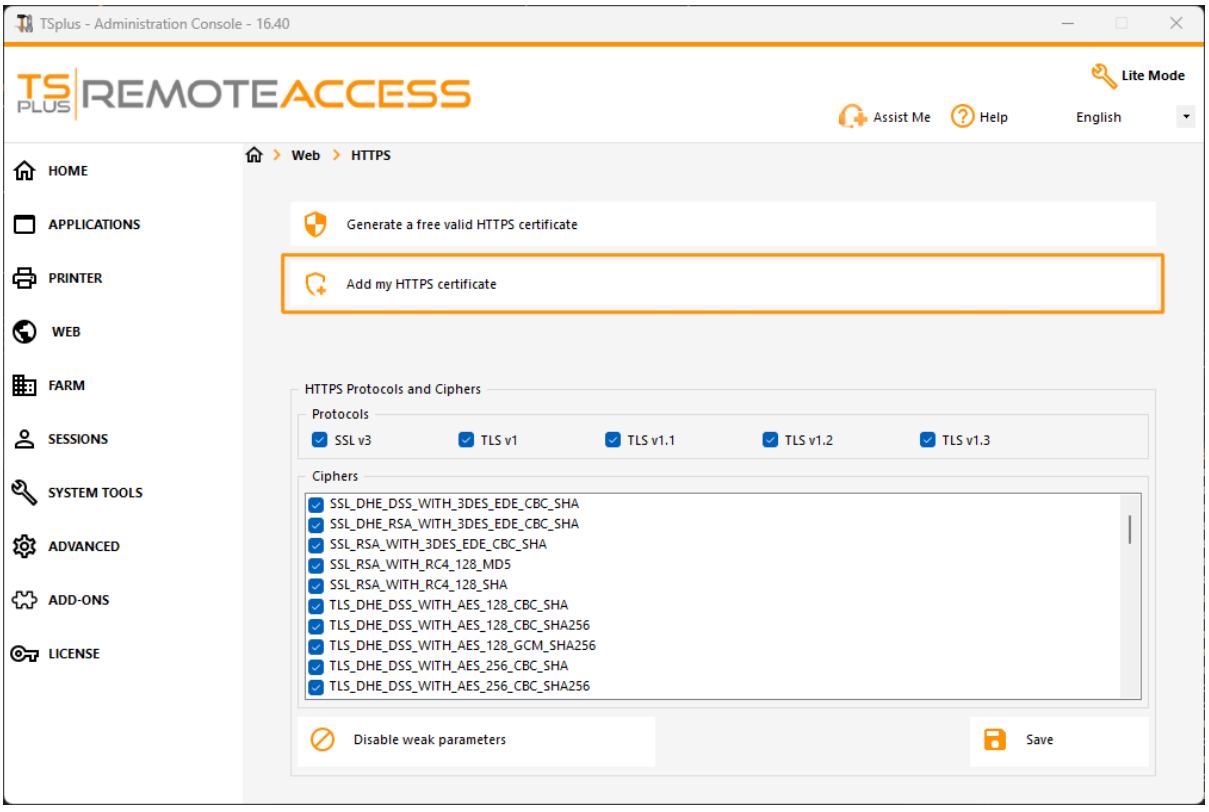
10. 그룹 정책을 업데이트하려면 다음 명령을 관리자 권한으로 실행하십시오: gpupdate /force.

HTTPS 및 SSL 제3자 인증서

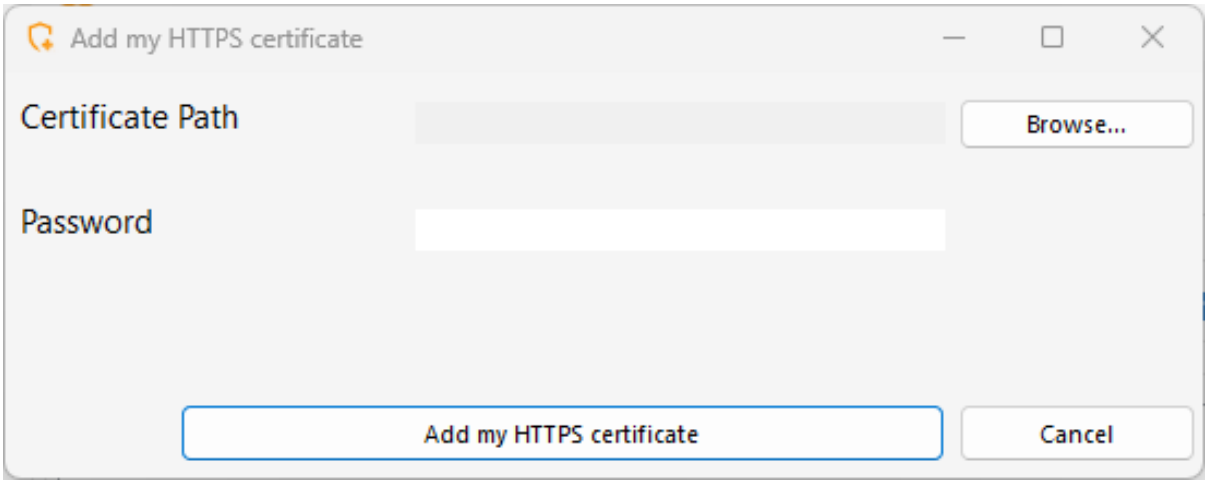
자신의 인증서를 추가하세요

유효한 HTTPS 인증서가 이미 있는 경우 웹 서버에 추가할 수 있습니다.

TSPlus AdminTool을 열고 “Web” 탭을 클릭한 다음 “HTTPS” 메뉴로 이동하여 아래 스크린샷에 표시된 대로 “내 HTTPS 인증서 추가”를 클릭합니다.



인증서를 선택할 수 있는 창이 열립니다:



귀하의 인증서 파일은 “.pfx” 형식을 사용해야 합니다.

비밀번호로 보호된 인증서가 있는 경우, 해당 필드에 입력할 수 있습니다.

“내 인증서 추가” 버튼을 클릭하여 인증서를 추가하세요.

인증서를 수동으로 갱신해야 한다는 점에 유의하시기 바랍니다.

추가 링크

신뢰할 수 있는 SSL 인증서 공급업체:

- 고대디
- DigiCert

당신은 도구나 온라인 사이트를 사용하여 .pem 파일을 pfx 형식으로 변환할 수 있습니다. 예를 들어, 이 사이트에서: https://www.sslshopper.com/ssl-converter.html

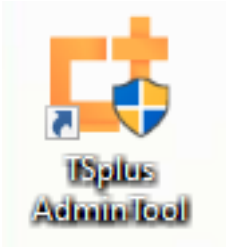
이것을 사용할 수 있습니다 SSL 서버 테스트 도구 웹 포털의 HTTPS에서 좋은 품질을 검증하기 위해.

TSplus 관리 도구 개요

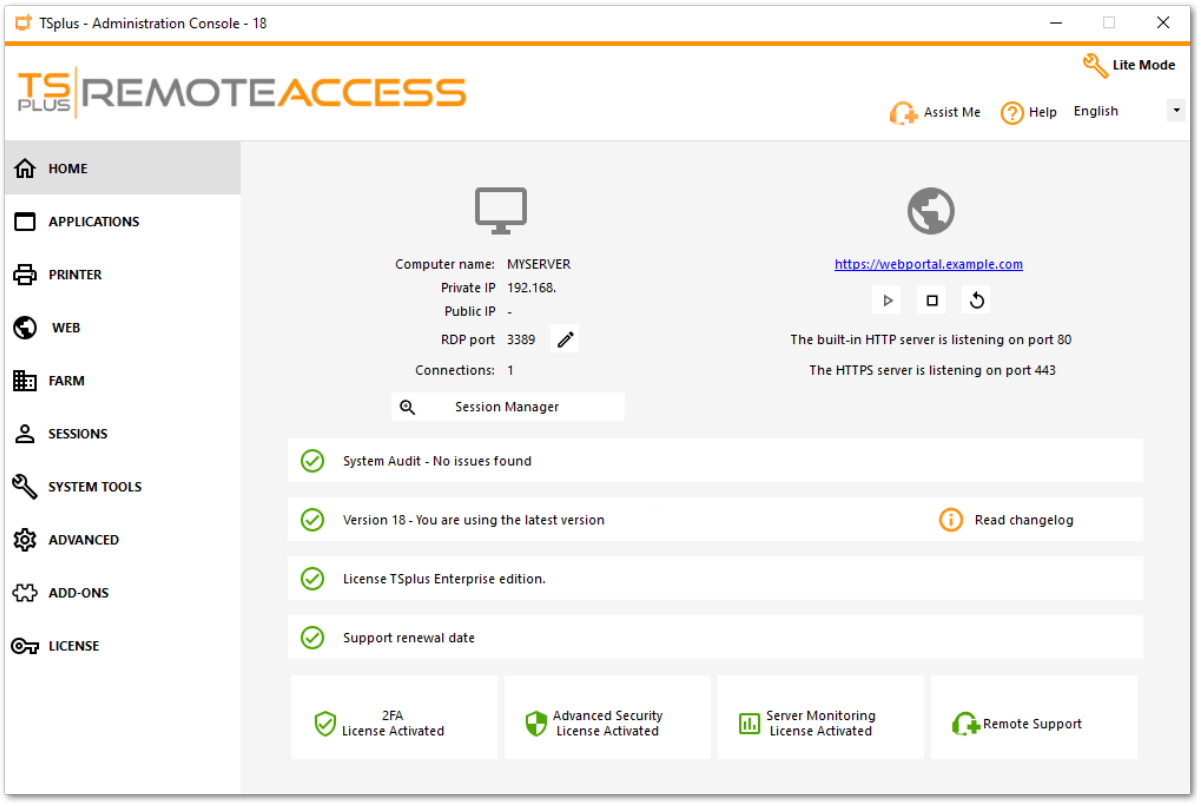
후에 TSplus 설치 서버가 즉시 준비됩니다.

그러나, 당신은 **모든 시스템 매개변수를 사용자 정의하십시오.** 강력한 관리자 도구와 함께.

바탕 화면에 생성된 다음 아이콘을 클릭하십시오:



관리자 도구가 다음과 같이 표시됩니다:

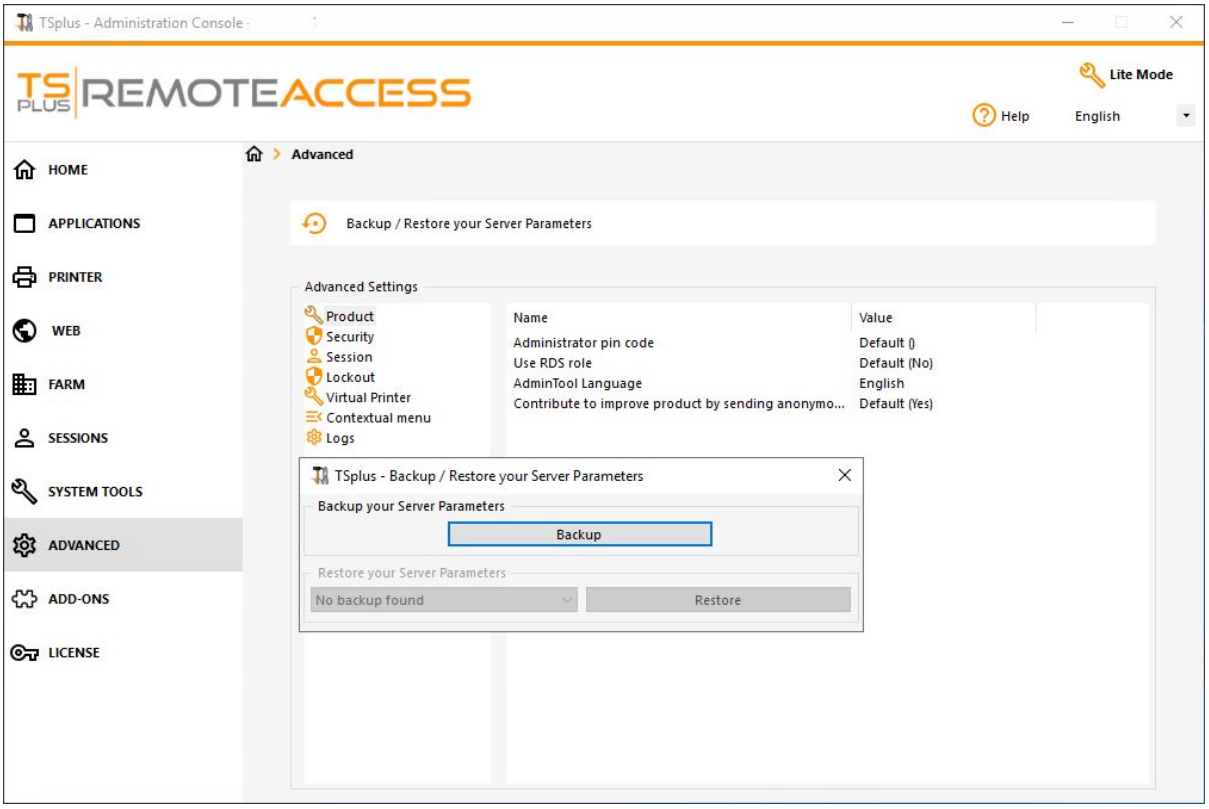


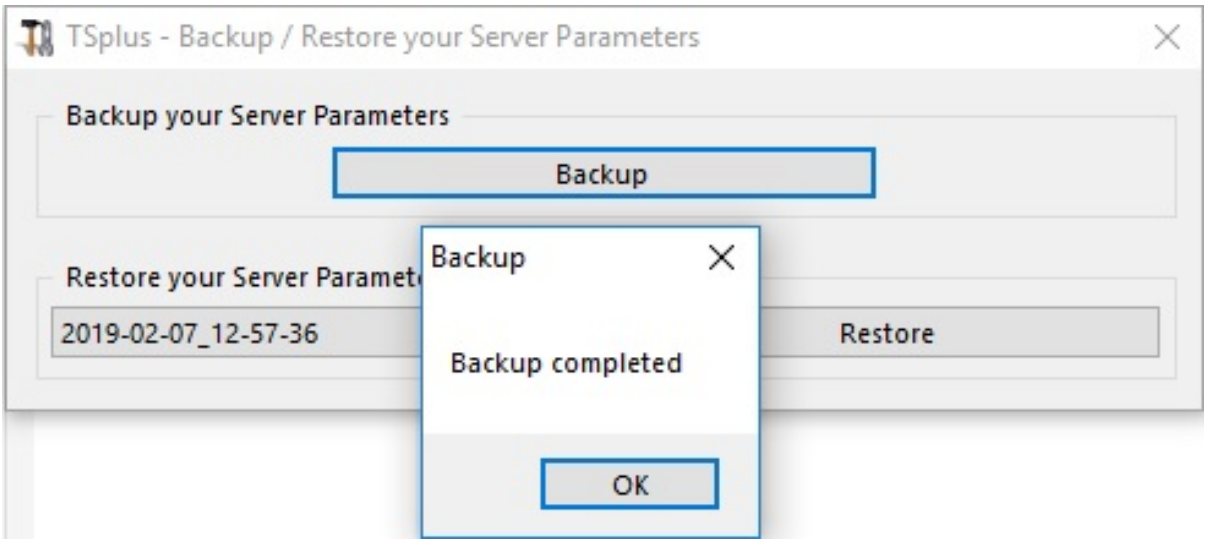
TSplus Admin Tool의 기능에 대해 빠르게 도움을 받고 싶으신가요? 그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!

백업 및 복원

버전 14부터 **고급** 탭, TSplus 설정을 구성할 수 있습니다.

TSplus 데이터 및 설정을 백업하거나 복원하려면 상단의 “백업/복원” 버튼을 클릭하세요.





명령어 사용법은 아래에 설명되어 있습니다:

- **백업** :

admintool.exe /backup [선택적 디렉토리 경로]

기본적으로 백업은 TSplus 보안 설정 폴더에 위치한 아카이브 디렉토리에 생성됩니다. 그러나 백업은 지정된 폴더에 저장될 수 있습니다. 상대 경로와 절대 경로가 허용됩니다.

- **복원** :

admintool.exe /restore [백업 디렉토리 경로]

지정된 백업 디렉토리에는 /backup 명령으로 생성된 데이터 및 설정 폴더가 포함되어야 합니다.

명령줄을 사용하는 것을 좋아하고 다른 명령줄이 무엇인지 궁금하다면, 이곳으로 가십시오. 특정 문서)

아래 단계를 따라 컴퓨터 A에서 컴퓨터 B로 TSplus를 마이그레이션하세요:

1. 컴퓨터 A에서 백업 버튼을 클릭하여 새 백업을 생성하십시오. 설정 및 데이터는 C:\Backupparam 폴더에 위치한 아카이브 디렉토리에 저장됩니다.

2. 새로 생성된 백업 폴더(예: backup-2021-01-29_15-01-29라는 이름)와 모든 내용을 컴퓨터 A의 아카이브 디렉토리에서 컴퓨터 B의 아카이브 디렉토리로 복사합니다.

3. 컴퓨터 B에서 백업 / 복원 창의 "복원" 섹션에서 복원할 관련 백업 이름을 선택합니다.

4.

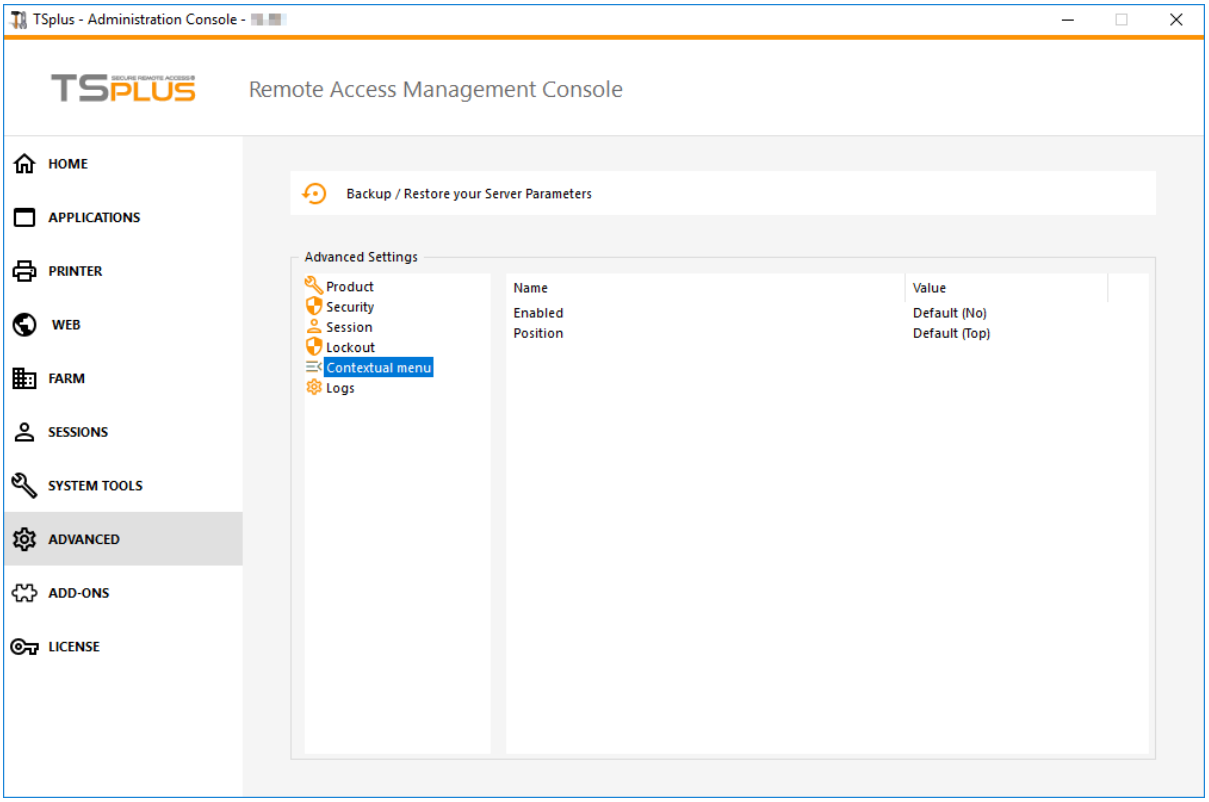
그런 다음 설정만 복원하기 위해 Restore Settings Only를 클릭합니다. 또는 모든 데이터와 설정을 복원하기 위해 Restore를 클릭할 수 있으며, 이는 마이그레이션에는 권장되지 않지만 컴퓨터 A에서 TSplus를 복원하는 데 유용합니다.

5.
TSplus 기능에 의해 설정이 다시 로드되는 데 최대 2분 정도 기다려 주십시오.

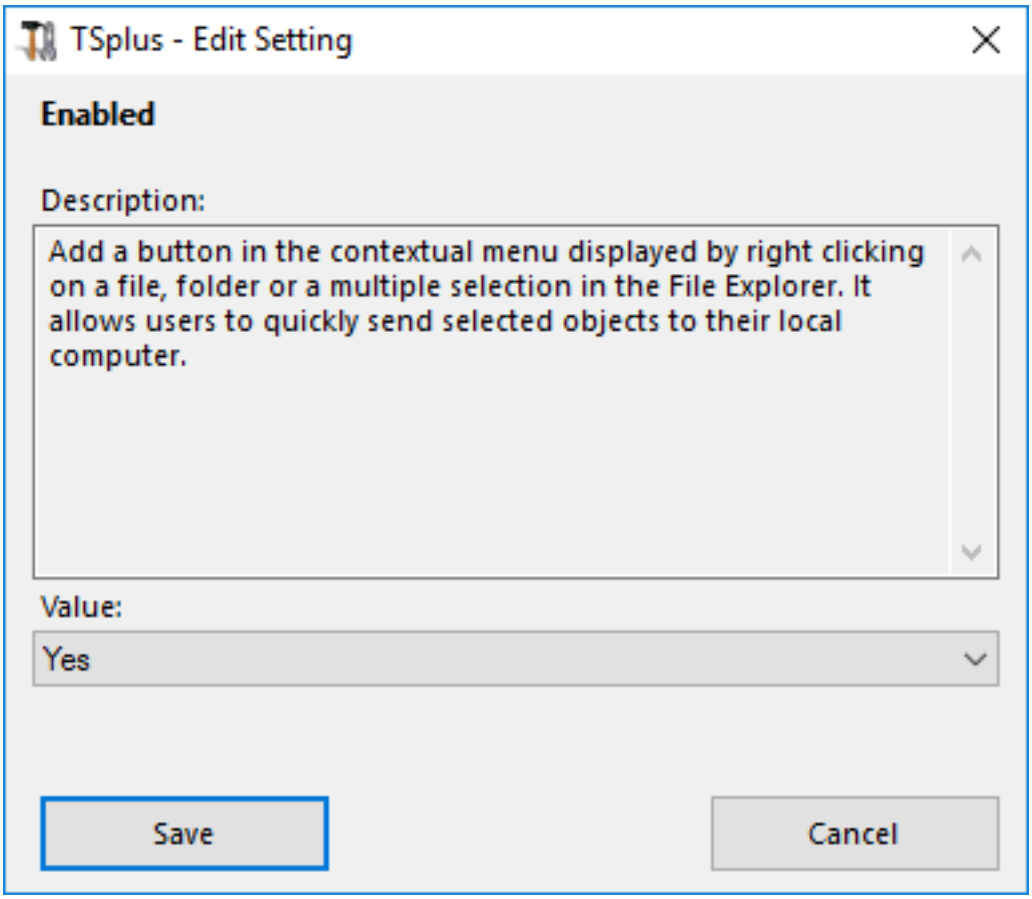
고급 기능 - 컨텍스트 메뉴

개요

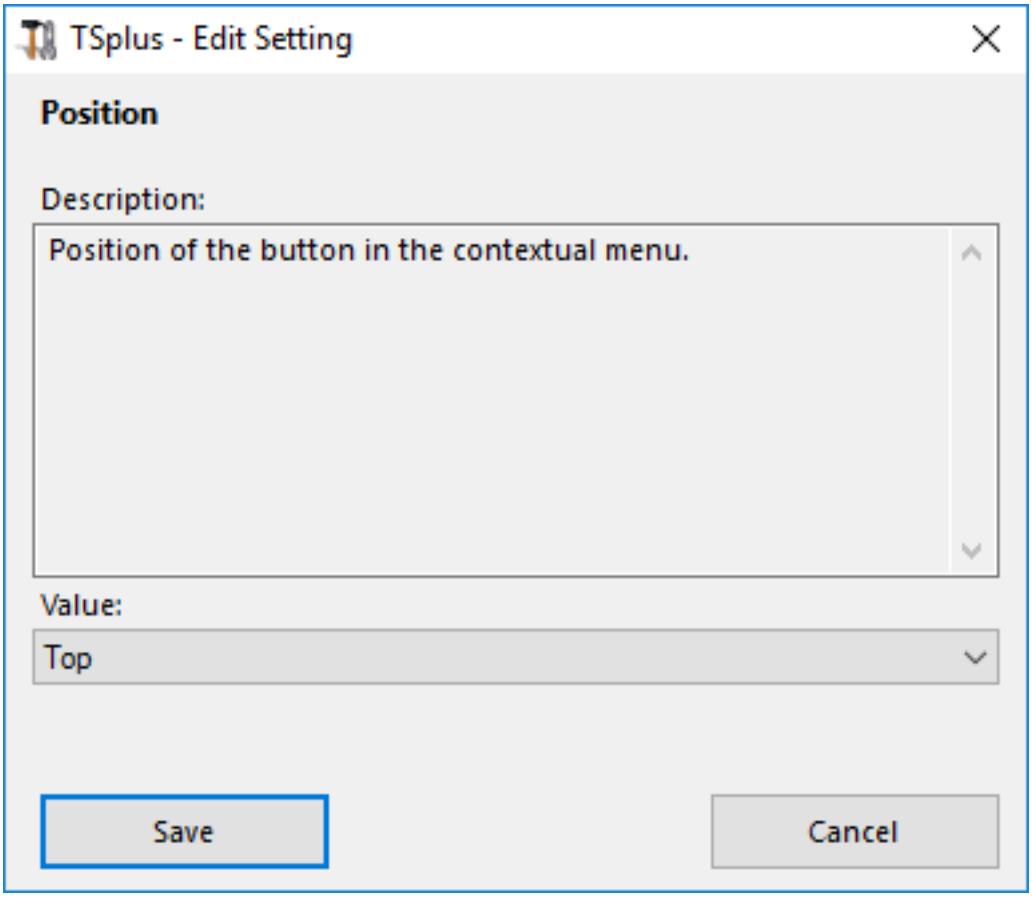
TSplus 버전 12.50부터 새로운 **"클라이언트에게 보내기" 메뉴** 고급 > 컨텍스트 메뉴 탭에서 활성화할 수 있어 클라이언트 워크스테이션으로 파일을 쉽게 전송할 수 있습니다. 이 기능은 모든 연결 방법과 함께 작동합니다.



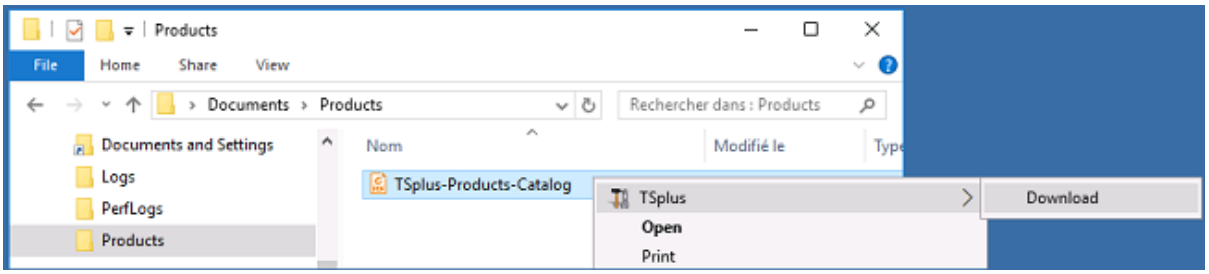
기본적으로 이 기능은 비활성화되어 있습니다. "예" 값을 선택한 다음 "저장"을 클릭하여 활성화하십시오.



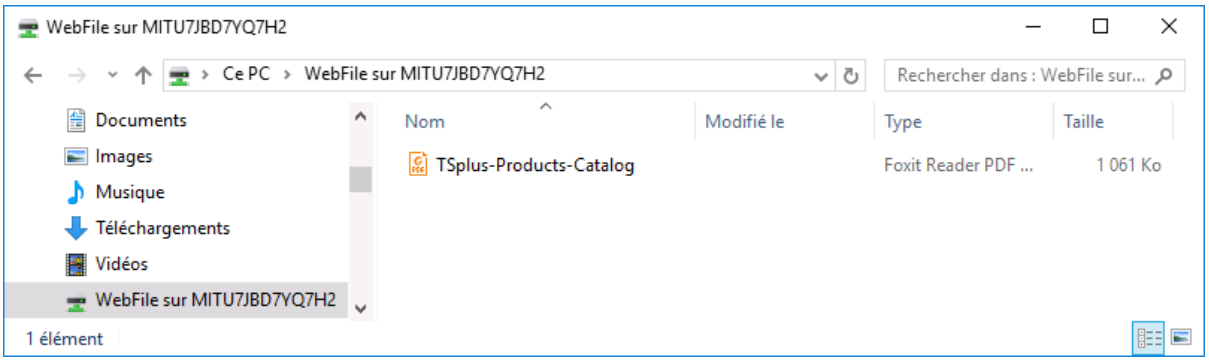
위치도 변경할 수 있습니다. 기본적으로 상단에 표시됩니다:



이것은 마우스 오른쪽 버튼 클릭 컨텍스트 메뉴입니다. 원하는 폴더나 파일을 선택하고, 마우스 오른쪽 버튼을 클릭한 후, “TSplus” 탭을 선택하고 “다운로드”를 클릭하면 됩니다.



웹파일 폴더와 웹 브라우저의 "다운로드" 폴더에서 다운로드를 찾을 수 있습니다.

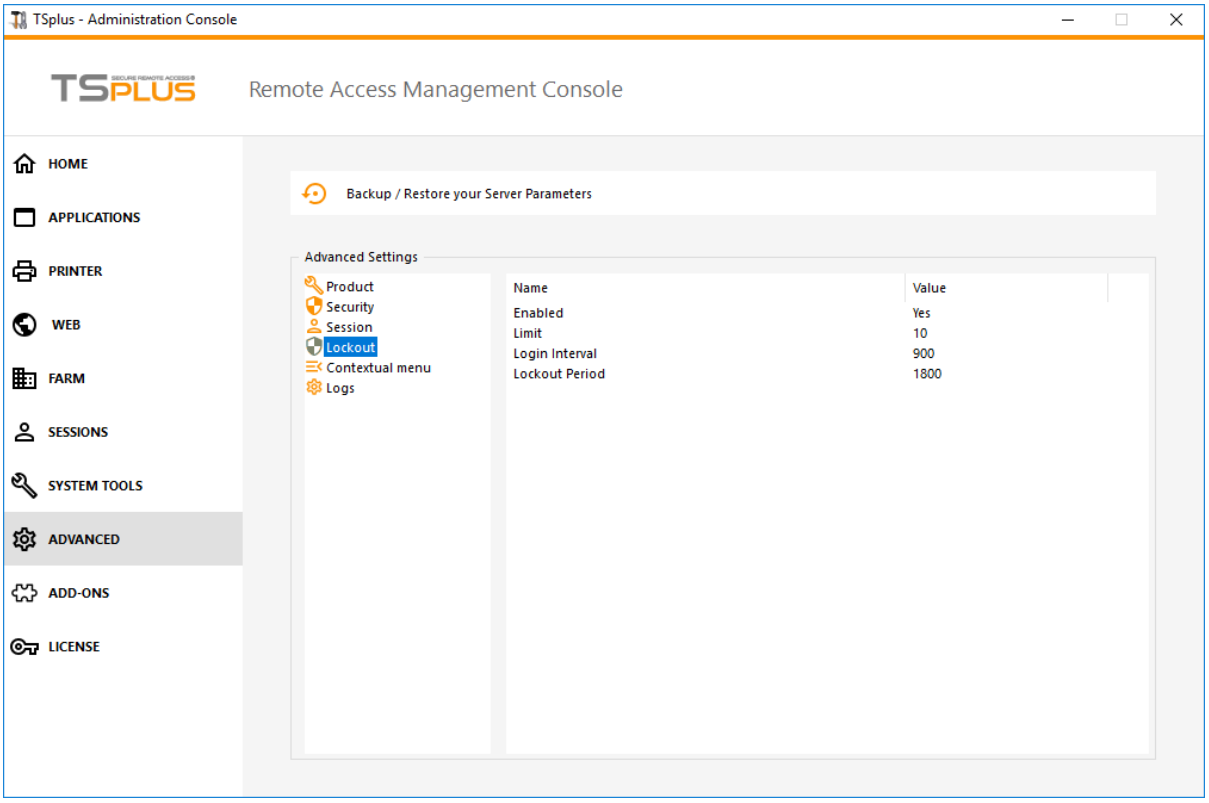


각 다운로드된 폴더는 자동으로 zip 파일로 압축됩니다.

고급 기능 - 잠금

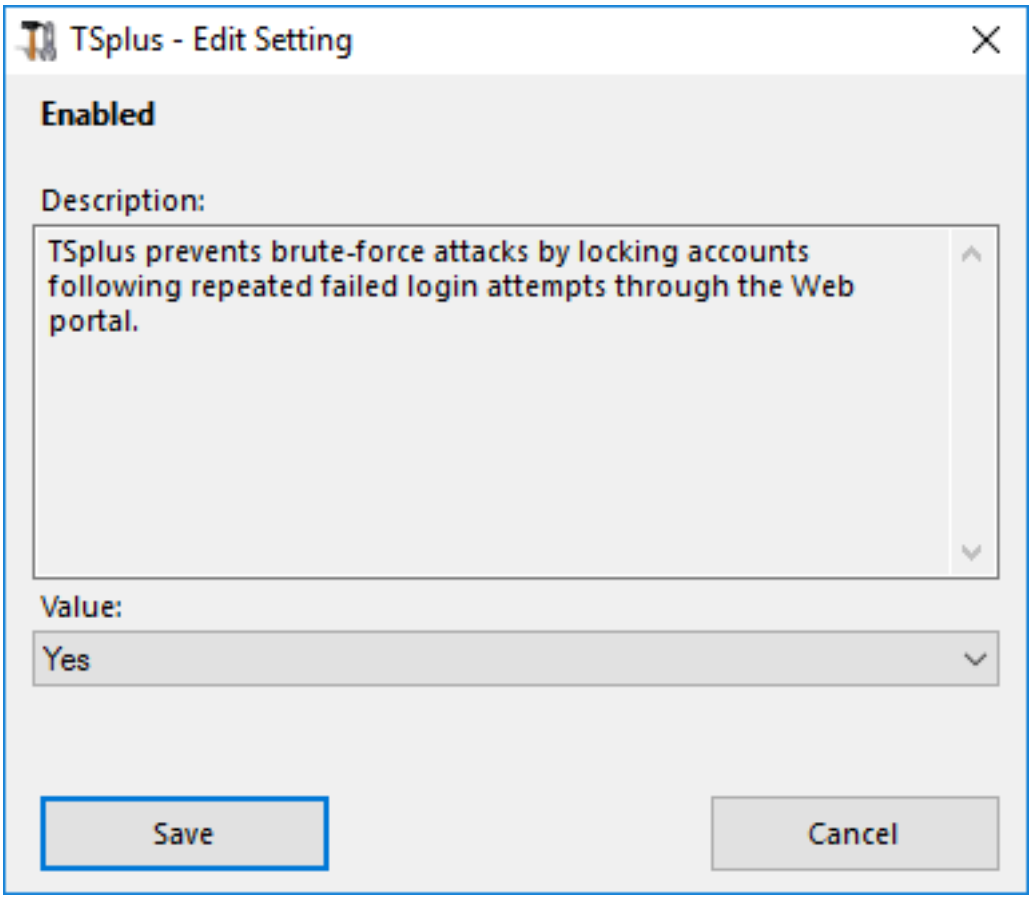
개요

이 탭에서 사용을 활성화/비활성화하고 구성할 수 있습니다. TSplus 잠금 설정.



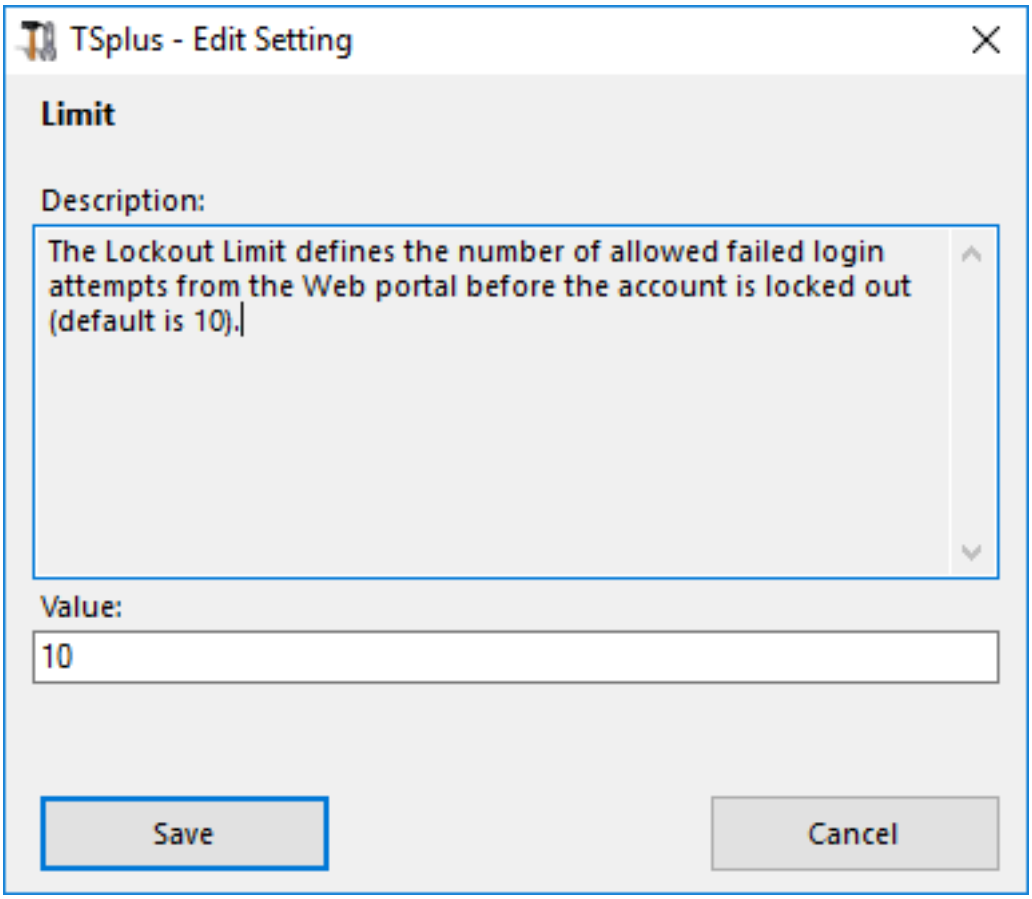
잠금 기능 활성화/비활성화

잠금 기능은 기본적으로 활성화되어 있습니다. 이 창에서 값을 "예"에서 "아니오"로 변경하여 비활성화할 수 있으며, 그 후 저장을 클릭하십시오.



한계

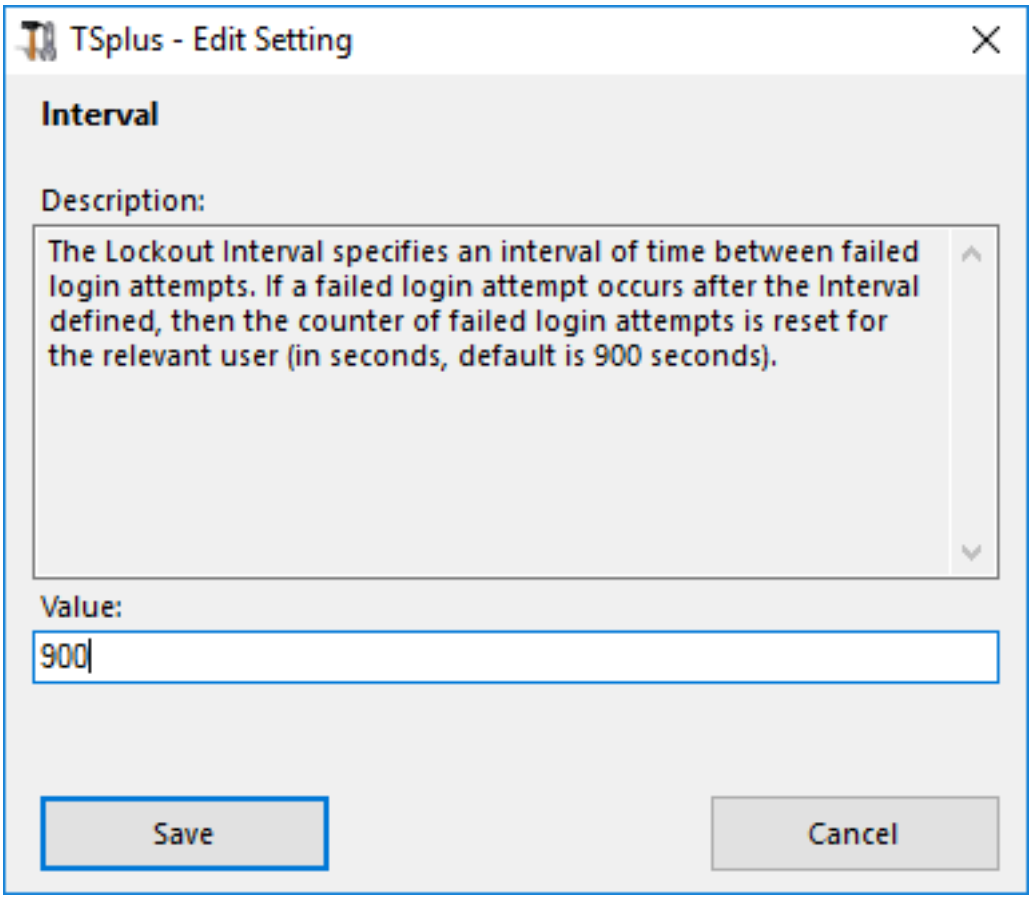
잠금 제한은 계정이 잠기기 전에 웹 포털에서 허용된 실패한 로그인 시도의 수를 정의합니다(기본값은 10입니다). 원하는 값을 해당 필드에 입력하고 저장을 클릭하여 이 값을 수정할 수 있습니다.



간격

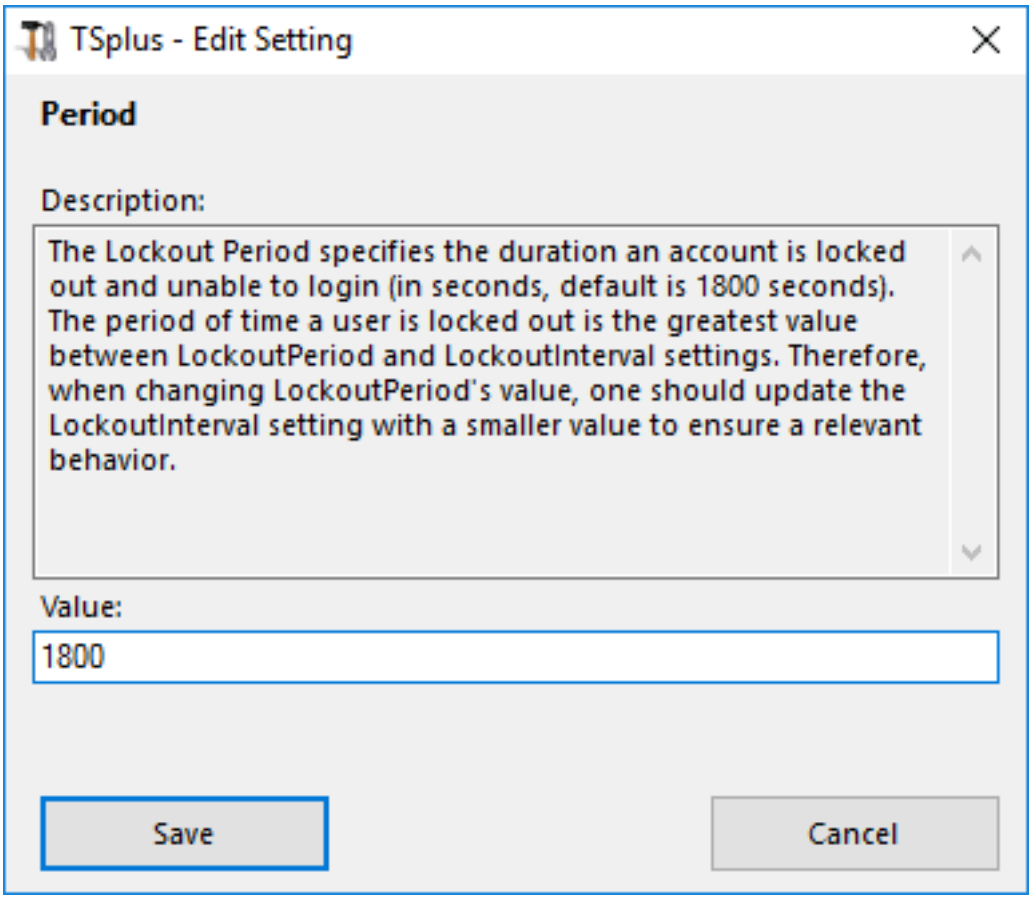
잠금 간격은 실패한 로그인 시도 사이의 시간 간격을 지정합니다.

로그인 시도가 정의된 간격 이후에 실패하면 해당 사용자의 실패한 로그인 시도 카운터가 초기화 됩니다(초 단위, 기본값은 900초입니다). 원하는 값을 해당 필드에 입력하고 저장을 클릭하여 이 값을 수정할 수 있습니다.



기간

잠금 기간은 계정이 잠겨 로그인할 수 없는 기간(초 단위, 기본값은 1800초)을 지정합니다. 사용자가 잠금되는 기간은 LockoutPeriod와 LockoutInterval 설정 중 가장 큰 값입니다. 따라서 LockoutPeriod의 값을 변경할 때는 관련된 동작을 보장하기 위해 LockoutInterval 설정을 더 작은 값으로 업데이트해야 합니다. 원하는 값을 해당 필드에 입력하고 저장을 클릭하여 이 값을 수정할 수 있습니다.


TSplus - Edit Setting
Period
Description:
The Lockout Period specifies the duration an account is locked out and unable to login (in seconds, default is 1800 seconds). The period of time a user is locked out is the greatest value between LockoutPeriod and LockoutInterval settings. Therefore, when changing LockoutPeriod's value, one should update the LockoutInterval setting with a smaller value to ensure a relevant behavior.
Value:
1800
Save
Cancel

고급 기능 - 로그

개요

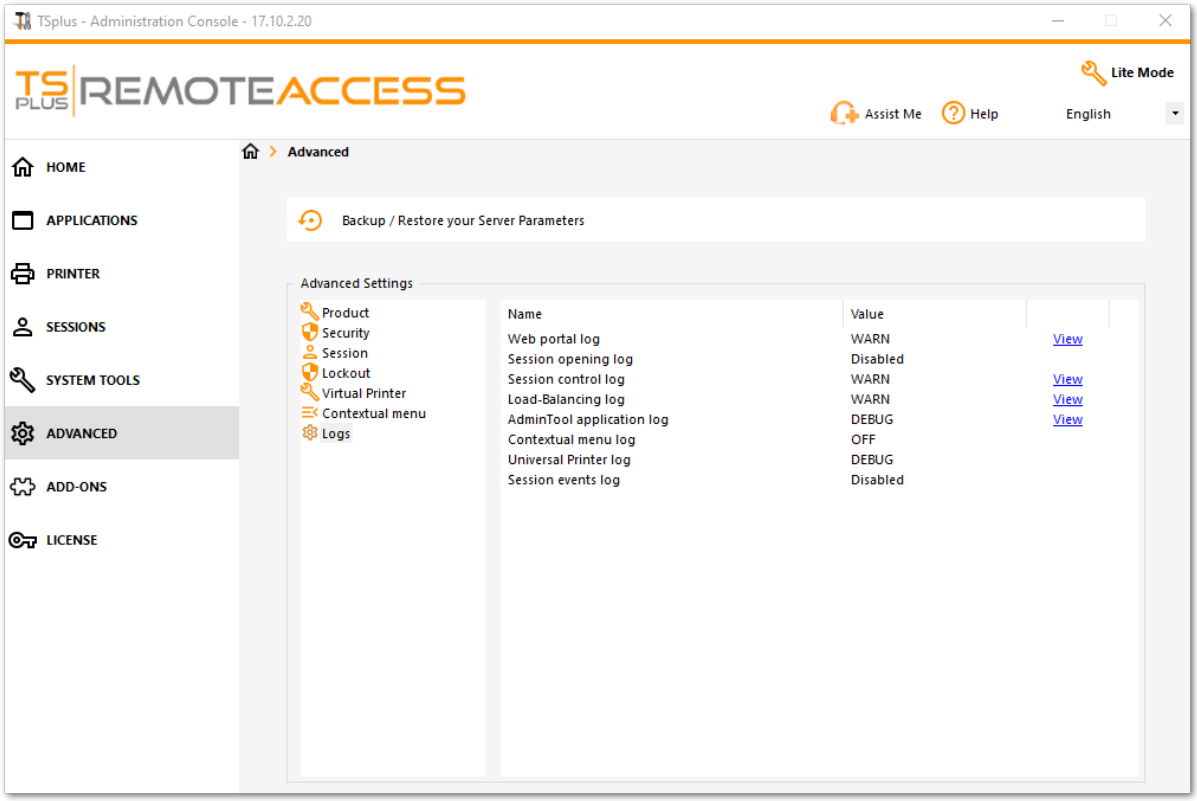
이 탭에서 TSplus 로그 설정을 구성할 수 있습니다.

기본적으로 TSplus는 성능 문제를 피하기 위해 로그를 생성하지 않습니다.

로그는 TSplus에서 발생한 오류의 원인을 더 쉽게 찾기 위해 존재하며, 다음과 같이 활성화할 수 있습니다:

- 이동하다 C:\wsession
- 'Trace' 폴더를 생성합니다. 로그는 사용자별로 자동으로 그곳에 생성됩니다.

관리 도구 > 고급 > 로그에서 로그 생성을 활성화해야 합니다.



로그의 종류는 5가지입니다:

- 웹 포털 로그,
- 세션 열기 로그,
- 세션 제어 로그,
- 부하 분산 로그 및
- 관리자 도구 애플리케이션(인터페이스) 로그.

로그 수준은 다양한 구성 요소에 해당하며, 문제에 따라 어떤 값을 입력해야 하는지 지원 팀이 알려줄 것입니다.

다음은 다양한 로그 파일 이름과 위치입니다:

- 웹 포털 로그: “C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\hb.log”

- 세션 열기 로그: “C:\wsession\trace”
- 세션 제어 로그: “C:\Program Files (x86)\TSplus\UserDesktop\files\APSC.log”
- 로드 밸런싱 로그: “C:\Program Files (x86)\TSplus\UserDesktop\files\svcenterprise.log”
- AdminTool 애플리케이션 로그: “C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.log”
- RDS-Knight / TSplus Advanced Security: “C:\Program Files (x86)\TSplus-Security\logs”

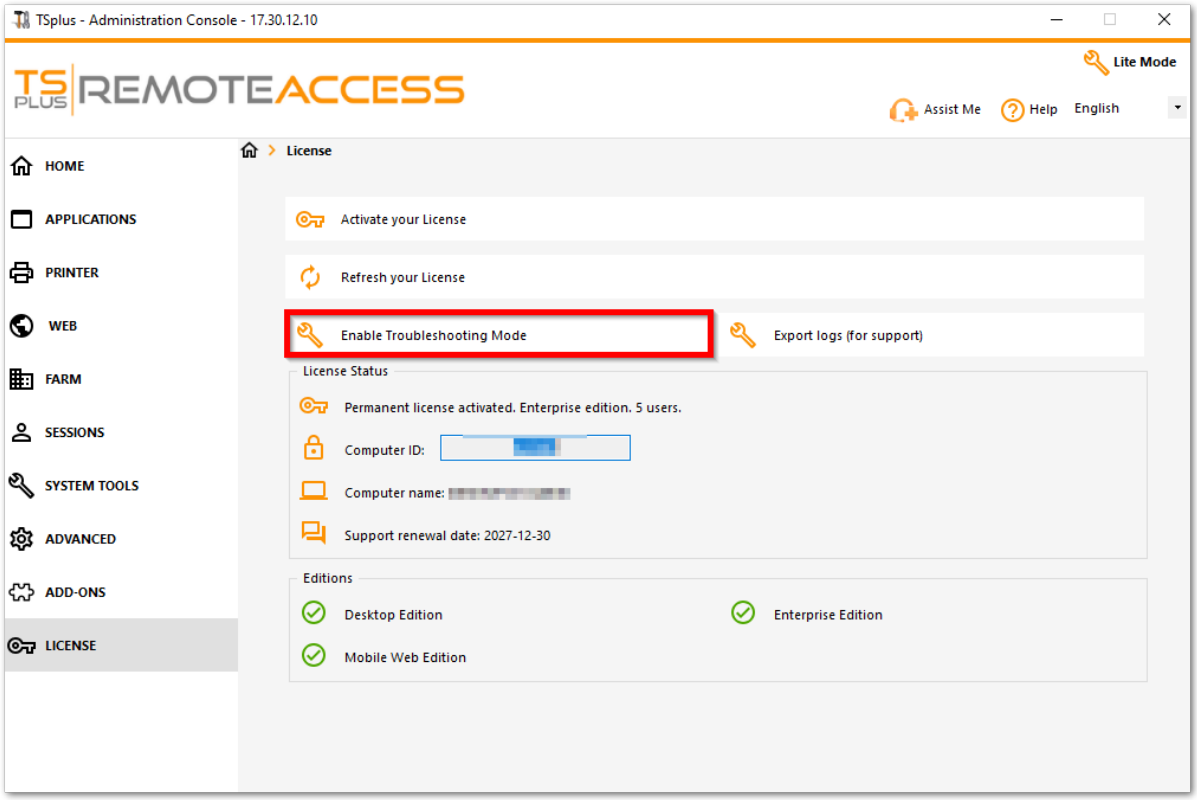
클라이언트 측에서 다음 레지스트리 키를 추가하여 연결 클라이언트의 로그를 활성화할 수 있습니다:

HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\ConnectionClient “Debug”=“true”

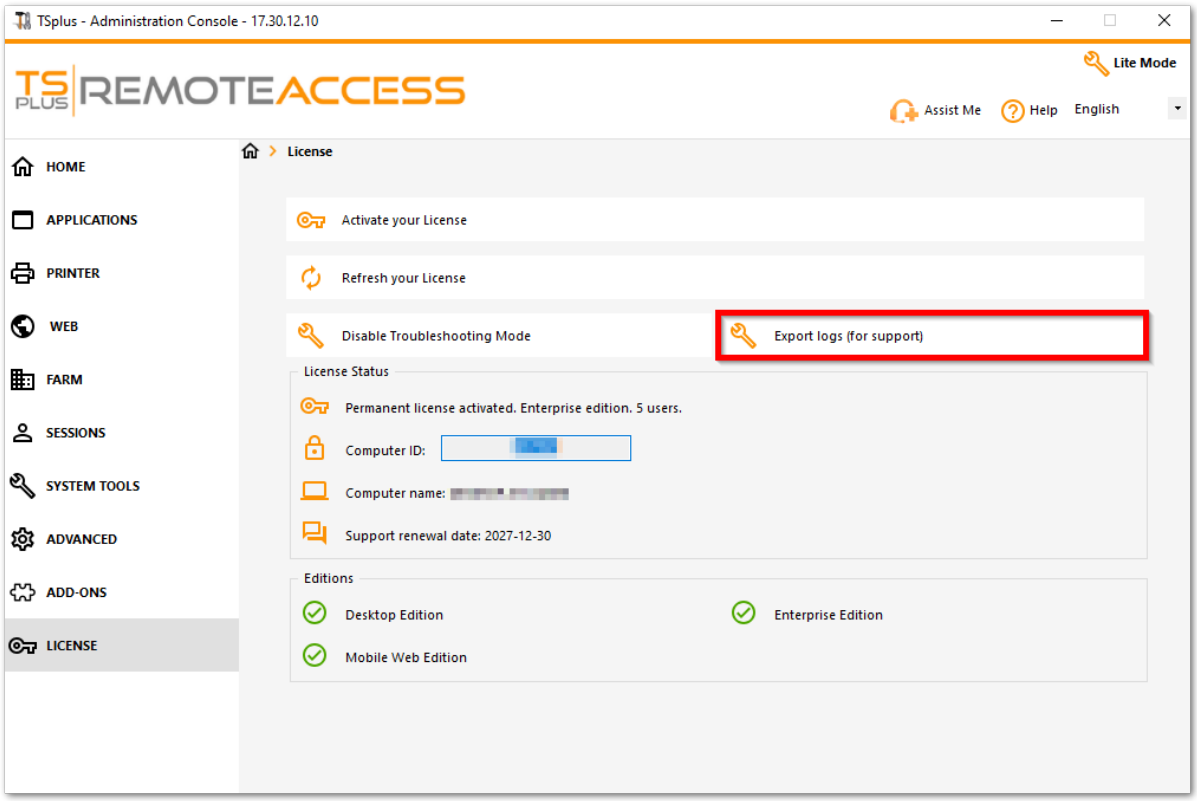
로그는 C:\Users에 있습니다. RDP6\logs 디렉토리는 설치가 사용자별인 경우이며, 모든 사용자에 대한 설치인 경우 C:\Program Files (x86)\Connection Client\RDP6\logs 디렉토리입니다.

문제 해결 모드 활성화

“라이센스” 탭으로 이동하십시오. 클릭하십시오. **문제 해결 모드 활성화** 버튼.



문제를 재현한 후 클릭하세요 **지원용 로그 내보내기** 지원 팀에 로그를 이메일로 전송하는 버튼.



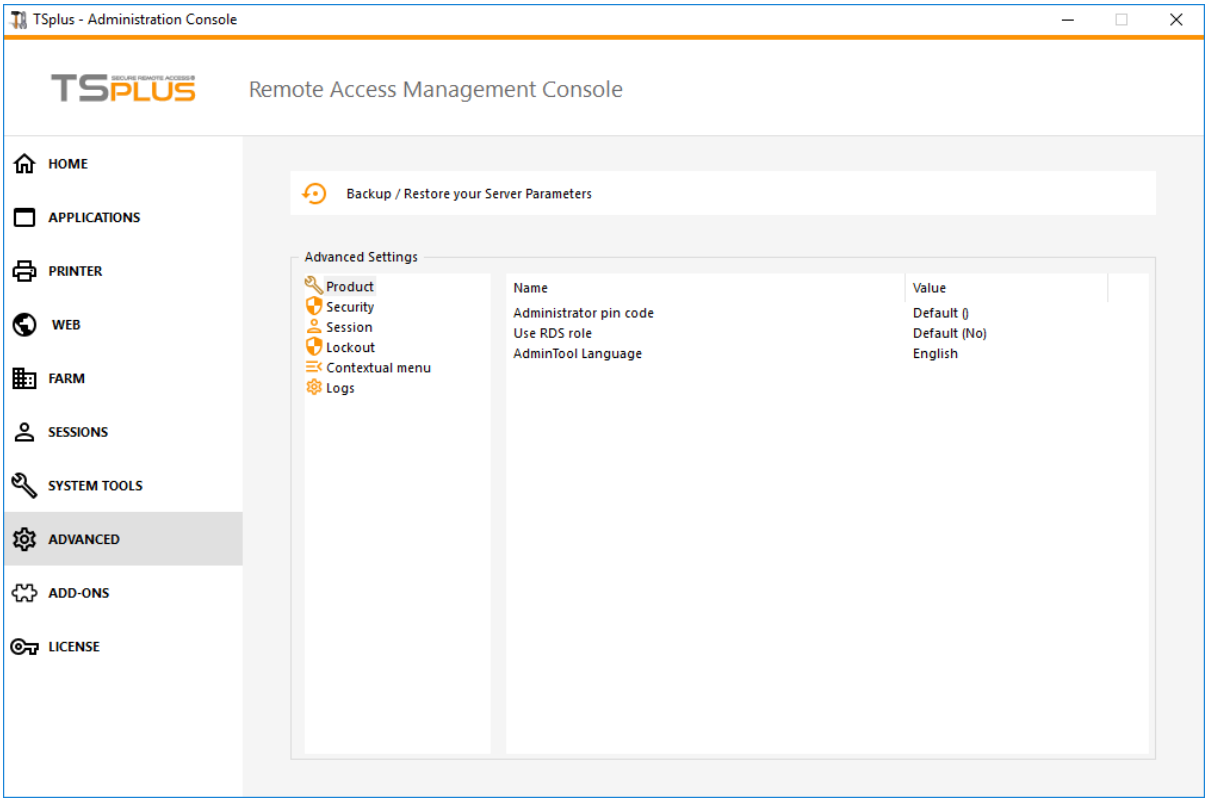


전송할 파일의 형식은 **.zip.logs** 파일과 비밀번호로 보호됩니다. **비밀번호** .

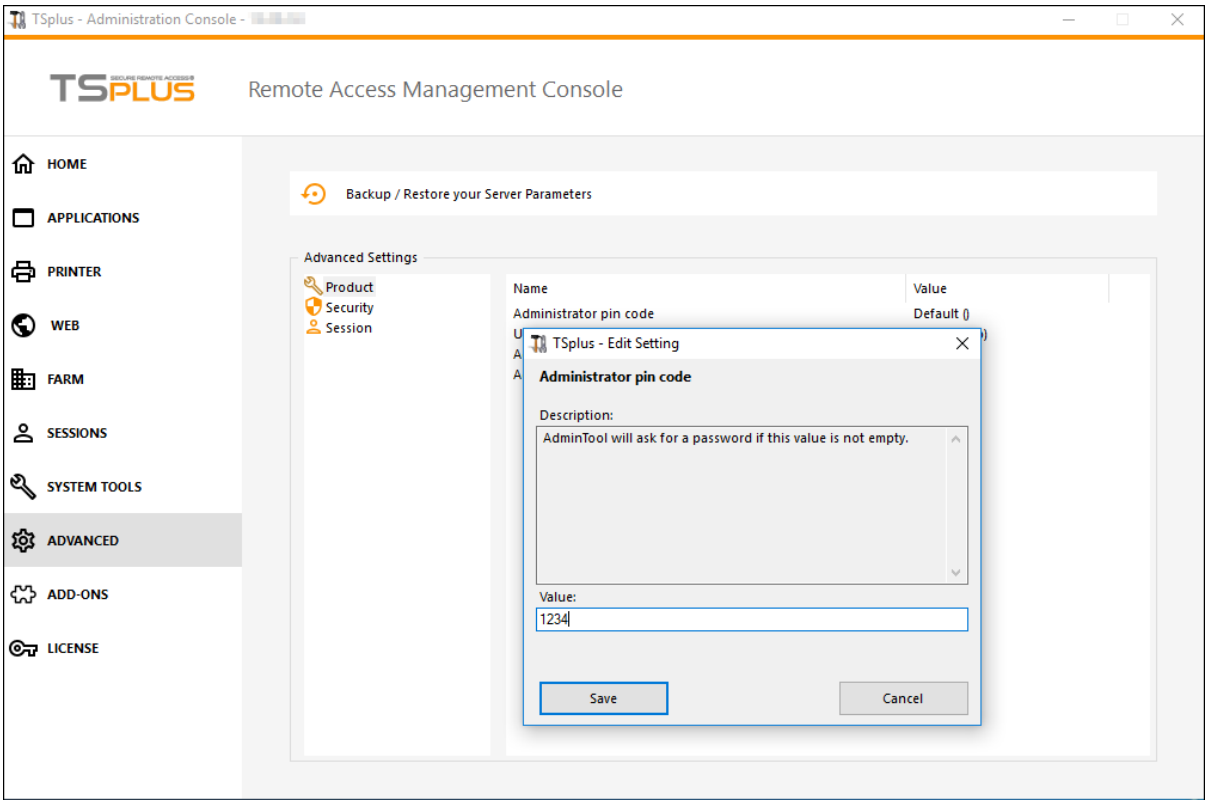
고급 기능 - 제품

개요

이 탭에서는 AdminTool Pincode를 추가하여 TSplus 설정을 수정하고, Windows RDS 역할을 사용하며, AdminTool의 배경 색상과 언어를 사용자 정의할 수 있습니다.



관리자는 제품 설정의 AdminTool 고급 탭에서 매 시작 시 요청되는 PIN 코드를 설정하여 관리자 도구 접근을 보호할 수 있습니다.

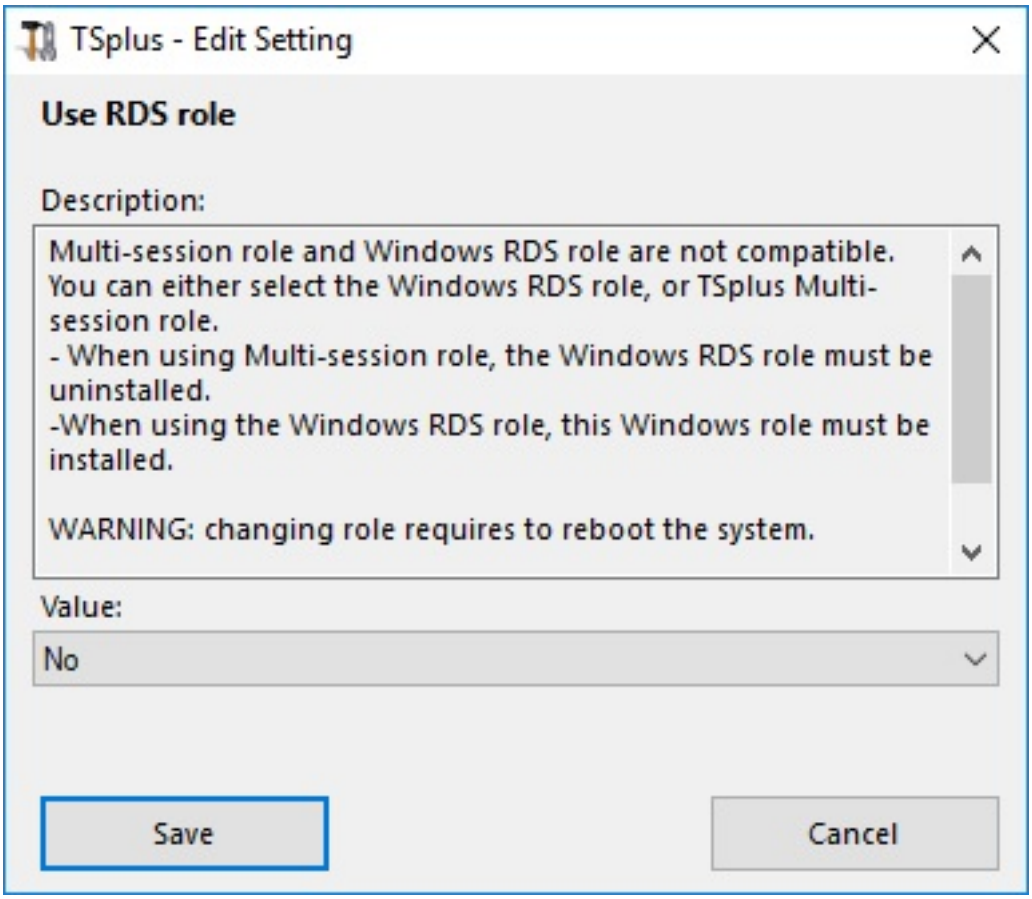


RDS 역할 사용

다중 세션 역할과 Windows RDS 역할은 호환되지 않습니다. Windows RDS 역할 또는 TSplus 다중 세션 역할 중 하나를 선택할 수 있습니다.

- Multi-session 역할을 사용할 때, Windows RDS 역할은 제거해야 합니다.
- Windows RDS 역할을 사용할 때, 이 Windows 역할은 설치되어 있어야 합니다.

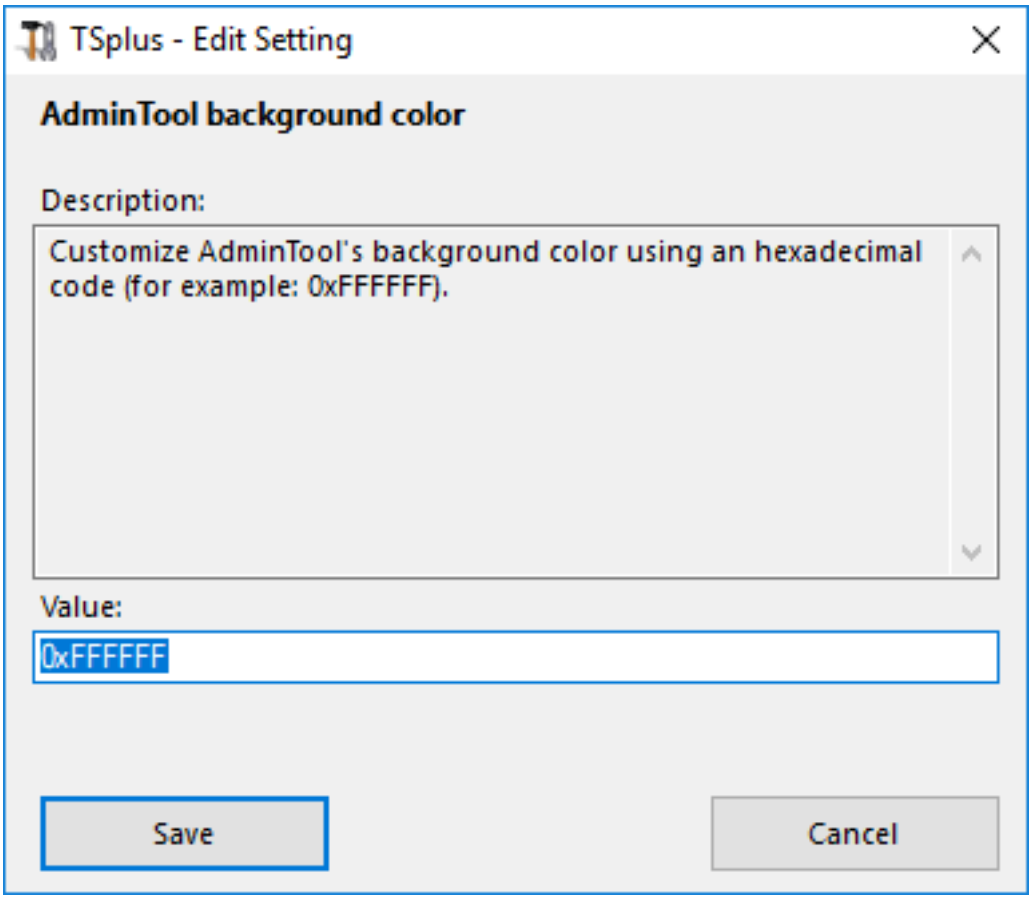
경고 역할 변경은 시스템을 재부팅해야 합니다. Windows 원격 데스크톱을 선택할 때는 한 번에 한 사용자만 워크스테이션 시스템에 허용됩니다.



Windows RDS 역할을 사용하려면 "예" 값을 선택하고 저장하십시오.

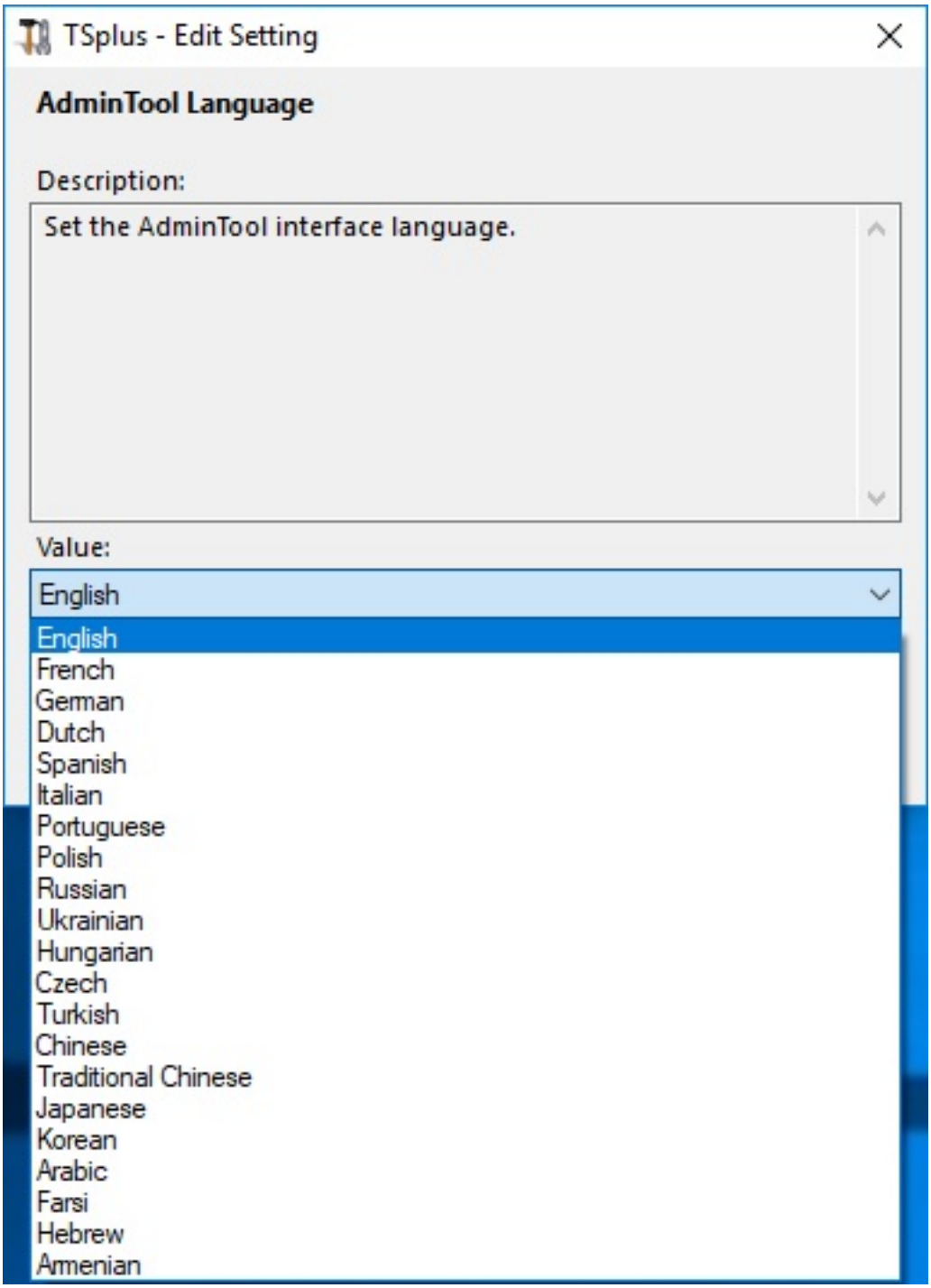
관리자 도구 배경색 수정

AdminTool의 배경 색상을 16진수 코드(예: 0xFFFFFF)를 사용하여 사용자 정의하십시오.



관리자 도구 언어 수정

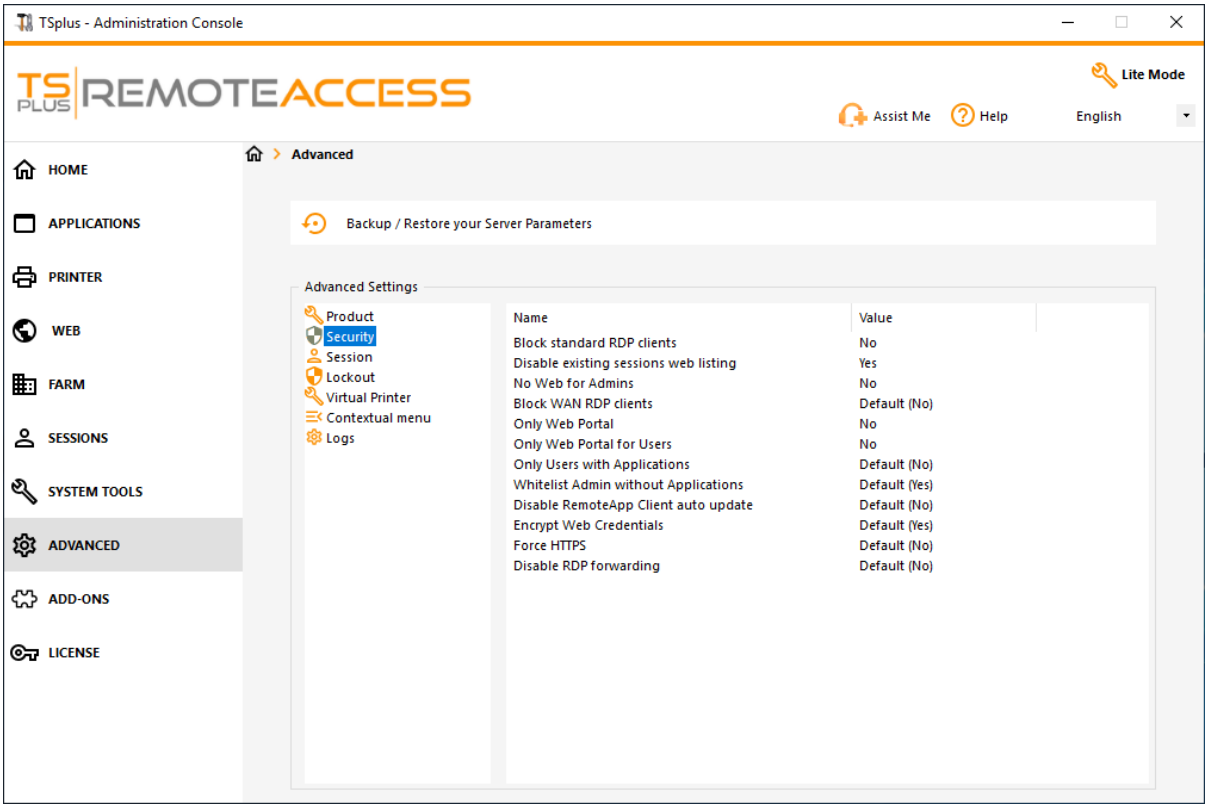
관리 도구를 위해 21개 중에서 선호하는 언어를 선택하세요.


TSplus - Edit Setting
AdminTool Language
Description:
Set the AdminTool interface language.
Value:
English
English
French
German
Dutch
Spanish
Italian
Portuguese
Polish
Russian
Ukrainian
Hungarian
Czech
Turkish
Chinese
Traditional Chinese
Japanese
Korean
Arabic
Farsi
Hebrew
Armenian

고급 기능 - 보안

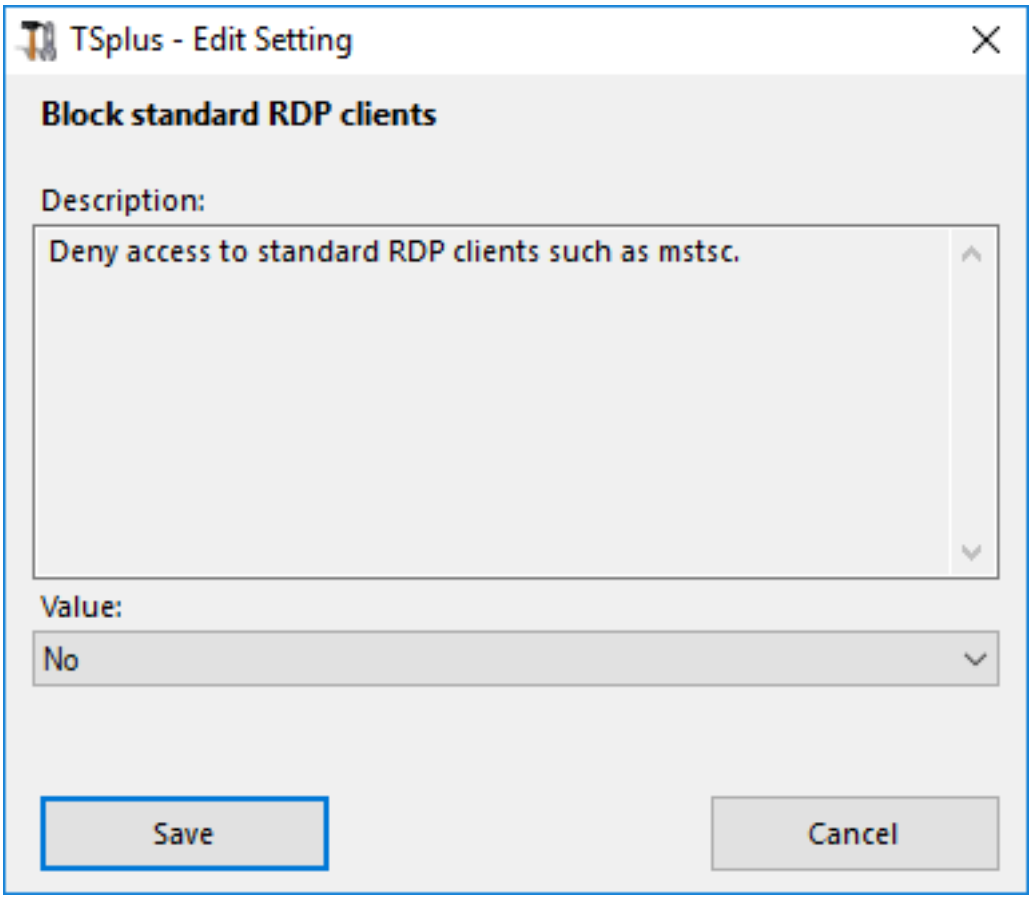
개요

고급 기능의 보안 섹션에서 사용자의 연결 유형을 차단, 비활성화 또는 사용자 정의할 수 있습니다.



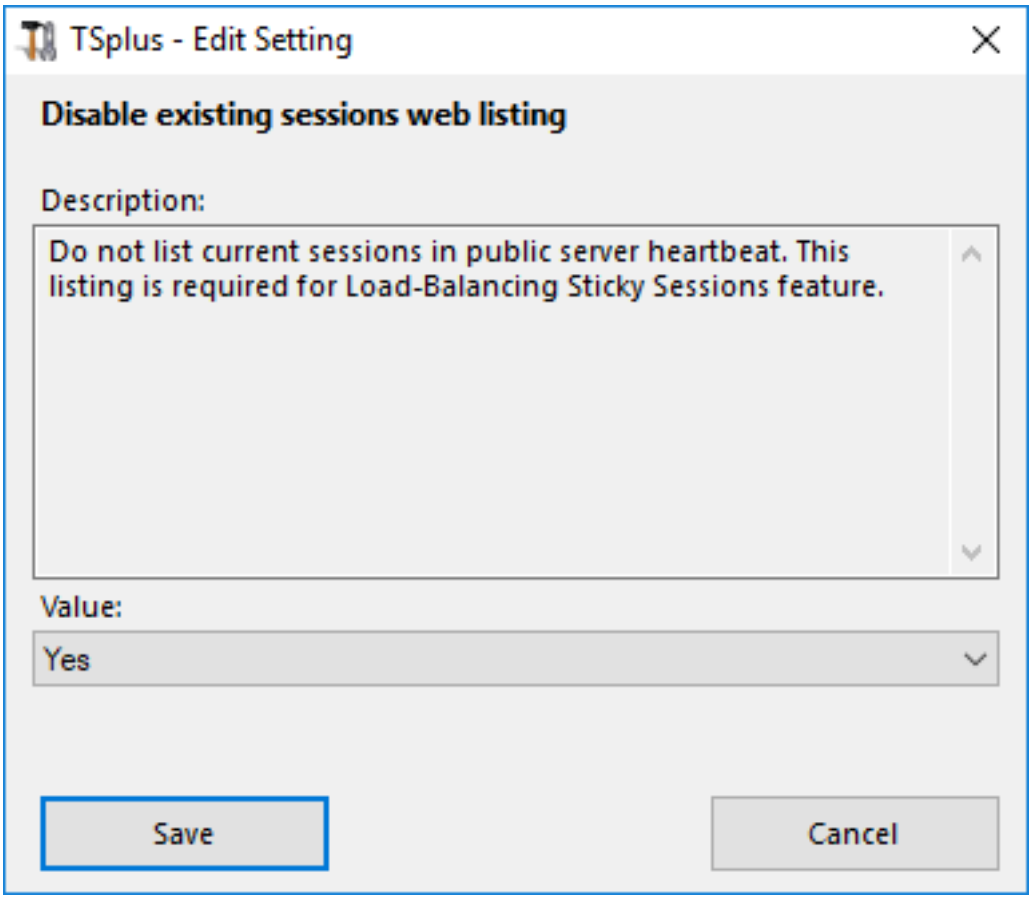
표준 RDP 클라이언트 차단

“예” 값을 선택하면 mstsc와 같은 표준 RDP 클라이언트에 대한 액세스를 사용자에게 거부할 수 있습니다.



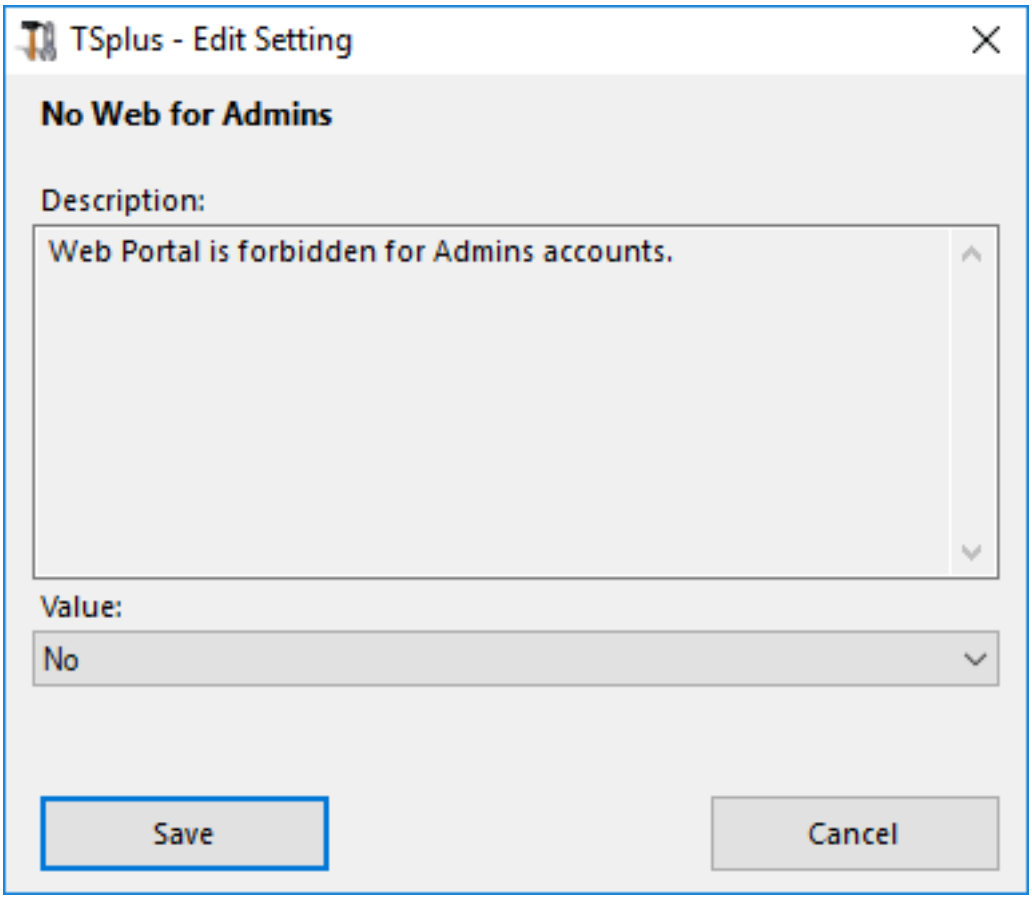
기존 세션 웹 목록 비활성화

이 목록은 로드 밸런싱 스티키 세션 기능에 필요하며 기본적으로 활성화되어 있습니다. 비활성화하려면 이 창에서 "아니오" 값을 선택한 다음 저장을 클릭하십시오.



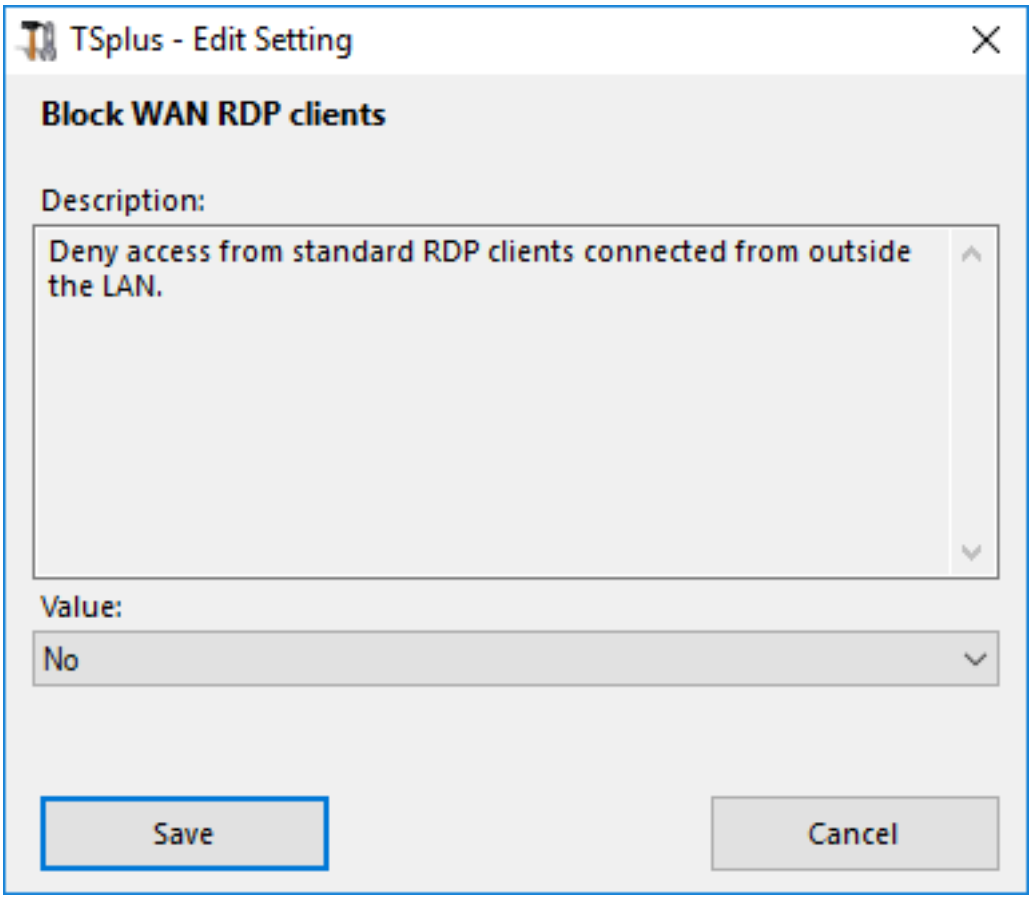
관리자를 위한 웹 없음

관리자를 위한 웹 포털을 비활성화하려면 "예" 값을 선택하십시오:



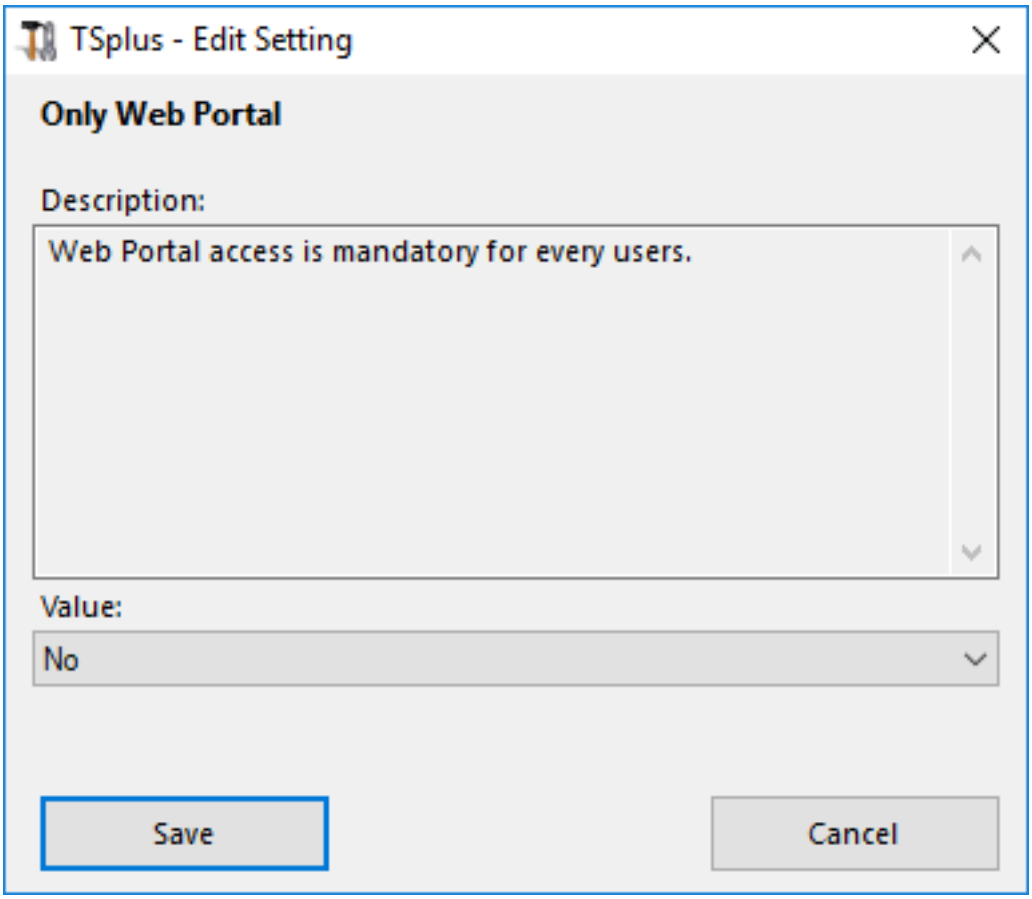
WAN RDP 클라이언트 차단

표준 RDP 클라이언트가 LAN 외부에서 연결되는 것을 차단하려면 "예" 값을 선택하십시오.



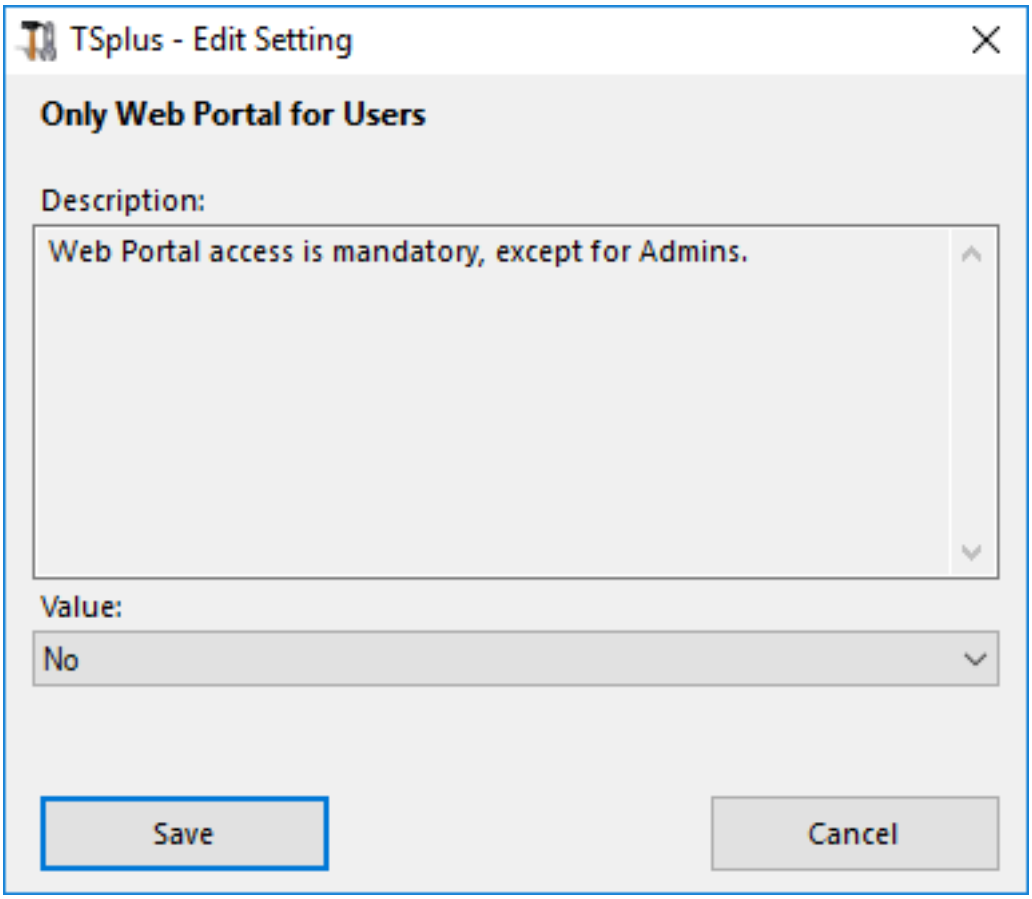
웹 포털만

모든 사용자가 "예" 값을 선택하여 웹 포털 접근을 의무화하십시오.



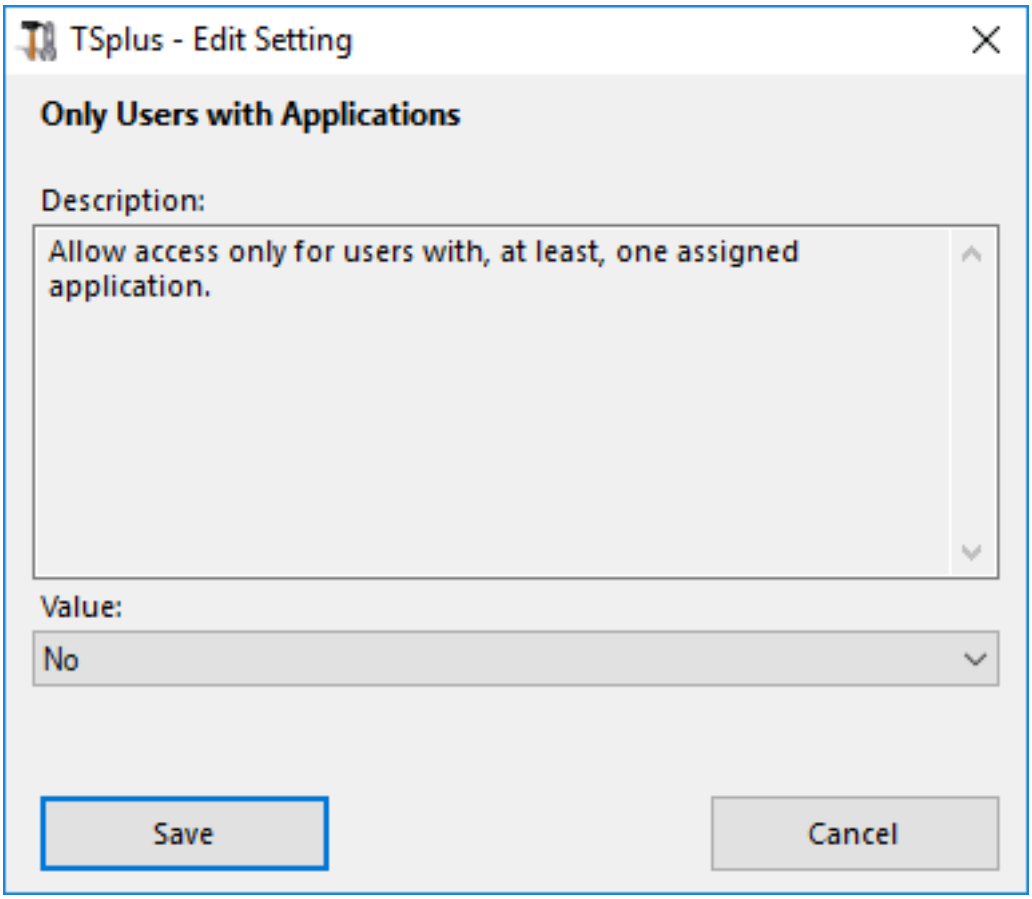
사용자를 위한 유일한 웹 포털

모든 사용자에 대해 웹 포털 접근을 의무화하고, 관리자를 제외하려면 "예" 값을 선택하십시오.



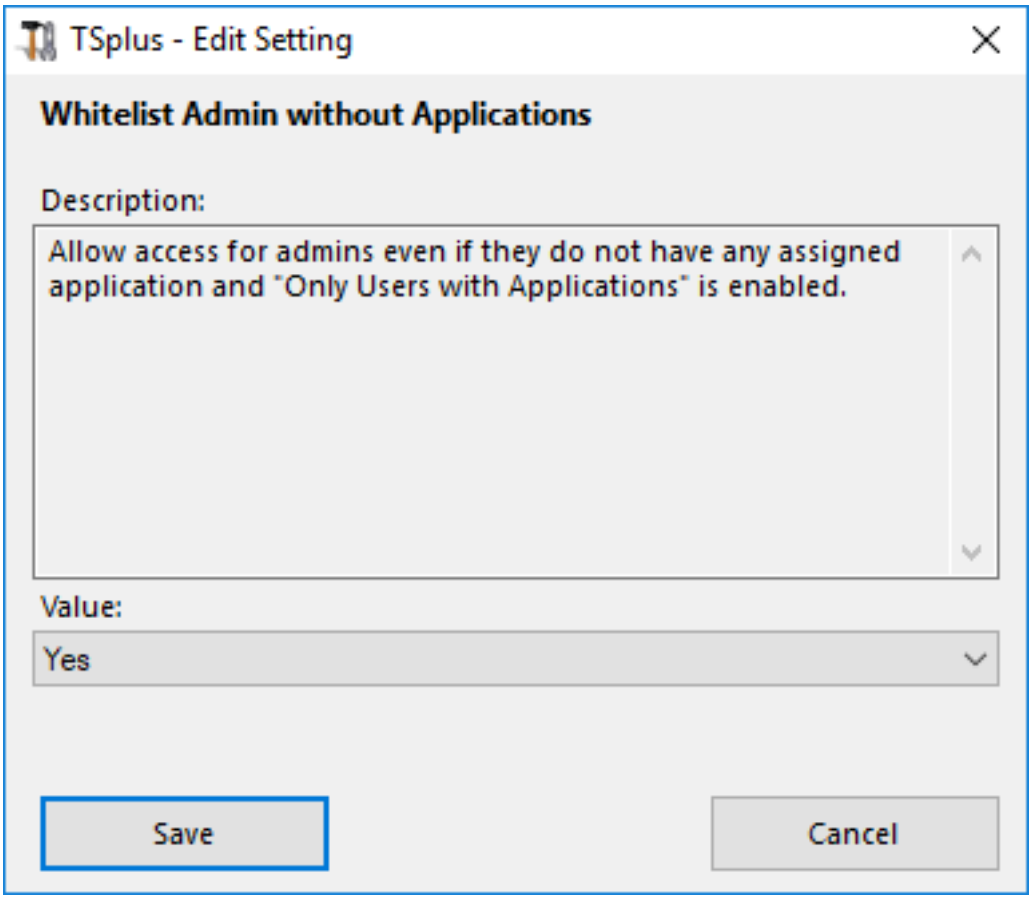
응용 프로그램이 있는 사용자만

사용자에게 할당된 애플리케이션이 하나 이상 있는 경우에만 접근을 허용하려면 "예" 값을 선택하십시오.



응용 프로그램이 없는 화이트리스트 관리자

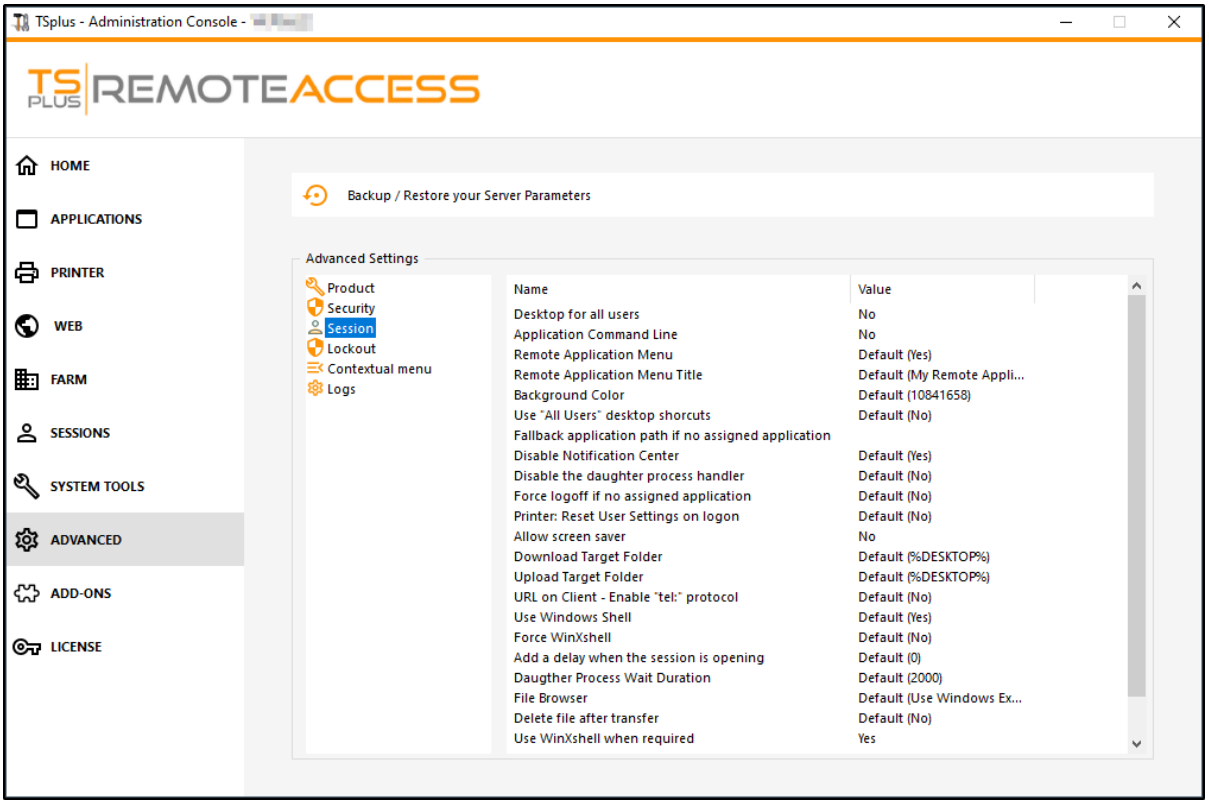
관리자에게 할당된 애플리케이션이 없더라도 접근을 허용하고 “애플리케이션이 있는 사용자만”이 활성화되어 있습니다. 이 기능은 기본적으로 활성화되어 있습니다. 비활성화하려면 이 창에서 “아니오” 값을 선택한 후 저장을 클릭하십시오.


TSplus - Edit Setting
Whitelist Admin without Applications
Description:
Allow access for admins even if they do not have any assigned application and "Only Users with Applications" is enabled.
Value:
Yes
Save
Cancel

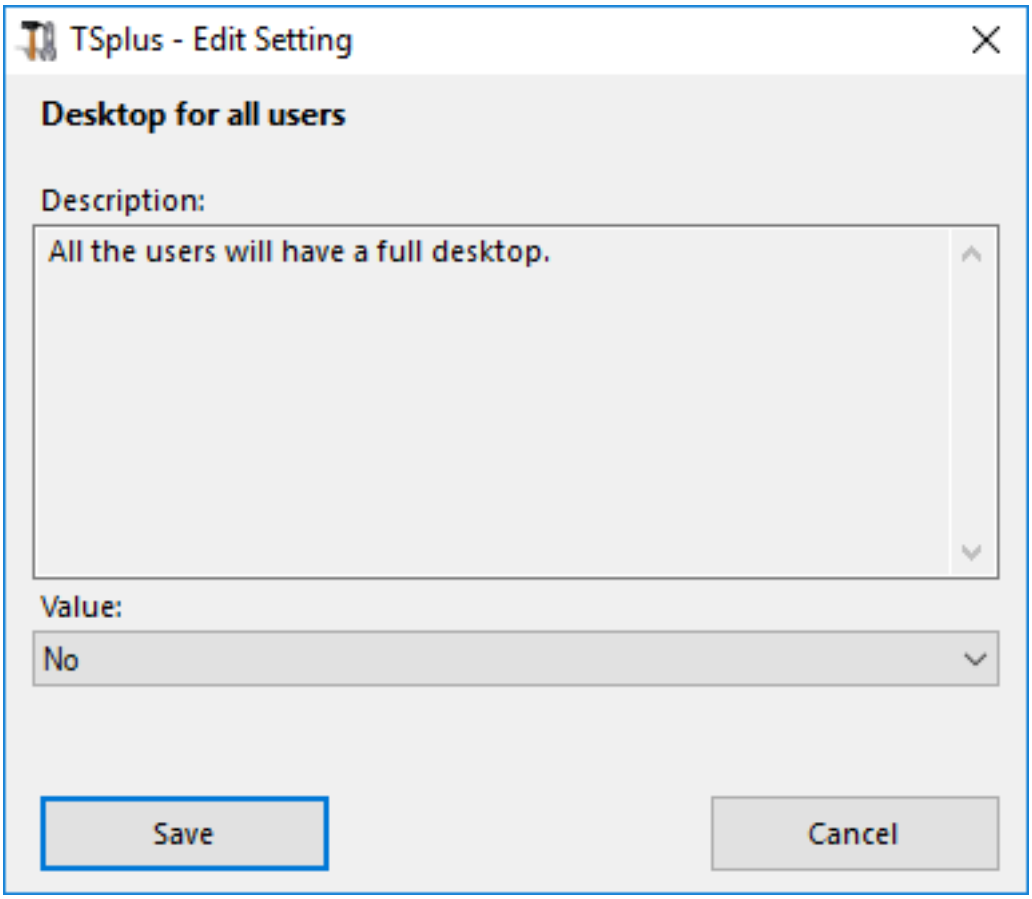
고급 기능 - 세션

개요

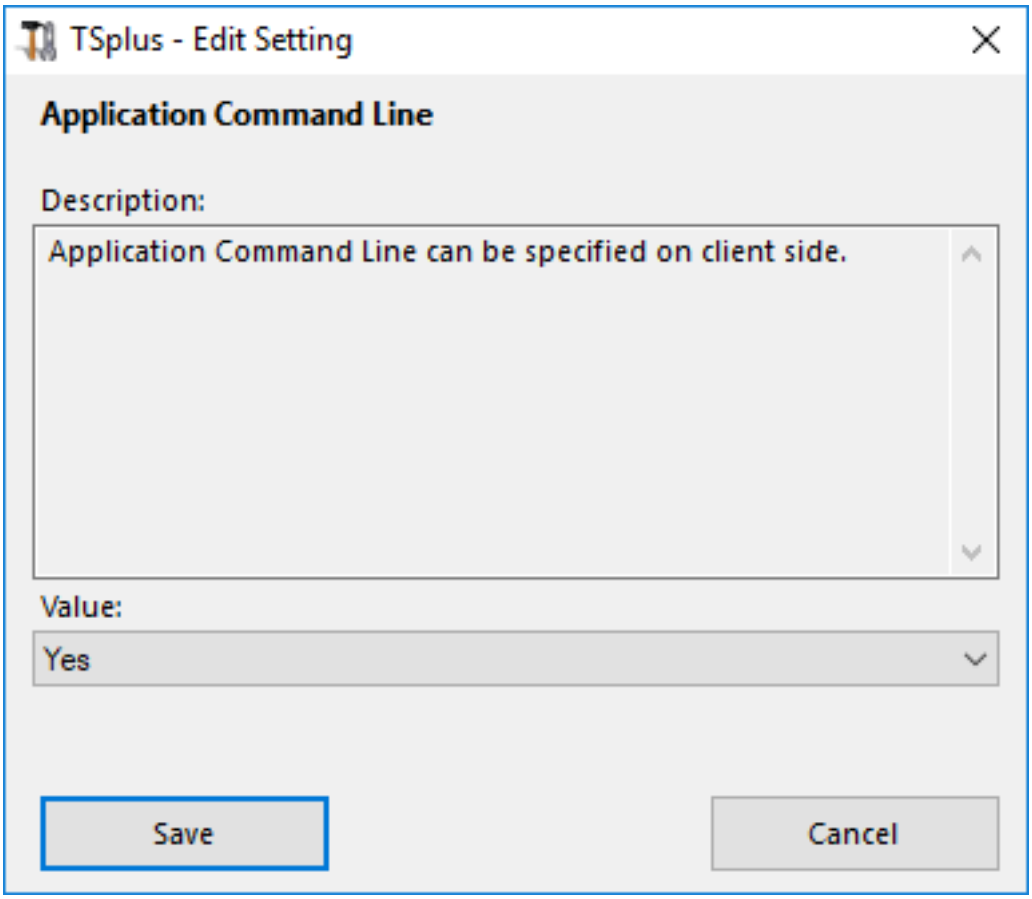
이 고급 탭의 이 섹션에서는 사용자 권한 및 세션의 측면을 구성할 수 있습니다.



모든 사용자를 위해 전체 데스크탑을 활성화하려면 이 창에서 "예" 값을 선택한 후 저장을 클릭하십시오.

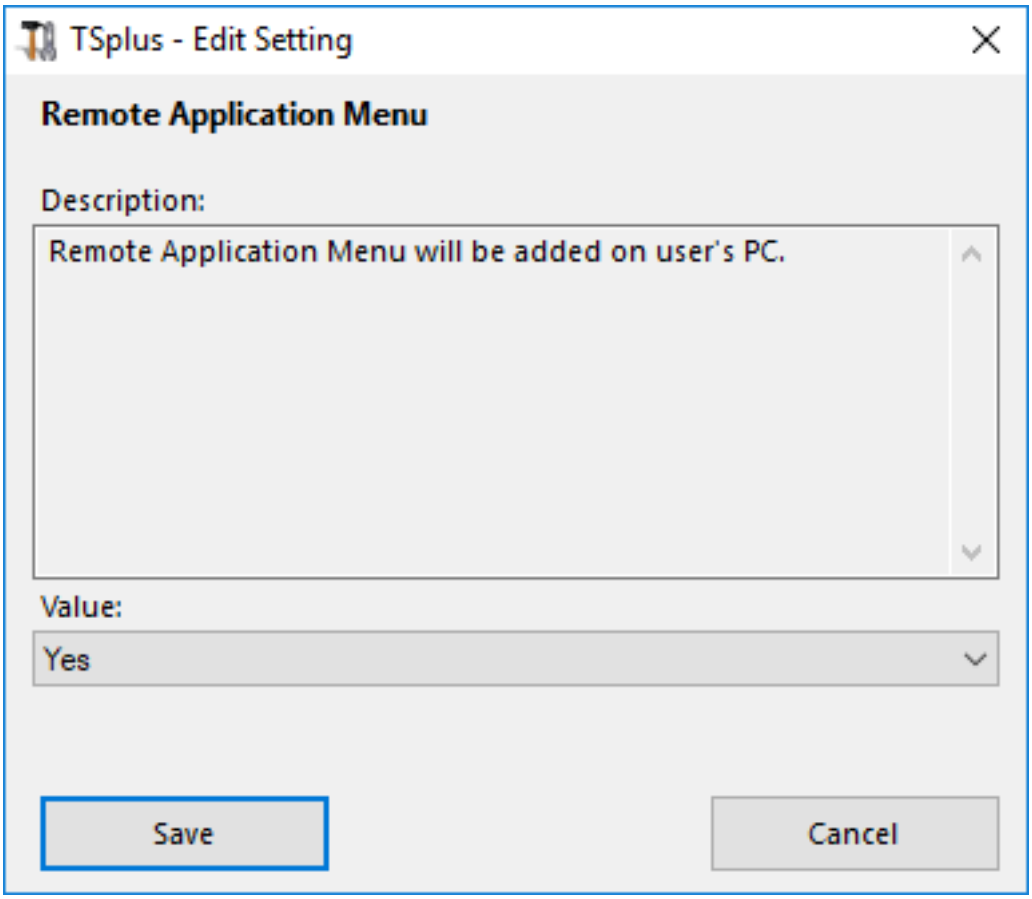


클라이언트 측에서 애플리케이션 명령줄을 지정할 수 있습니다. 이 기능은 기본적으로 활성화되어 있습니다. 비활성화하려면 이 창에서 "아니요" 값을 선택한 다음 저장을 클릭하십시오.



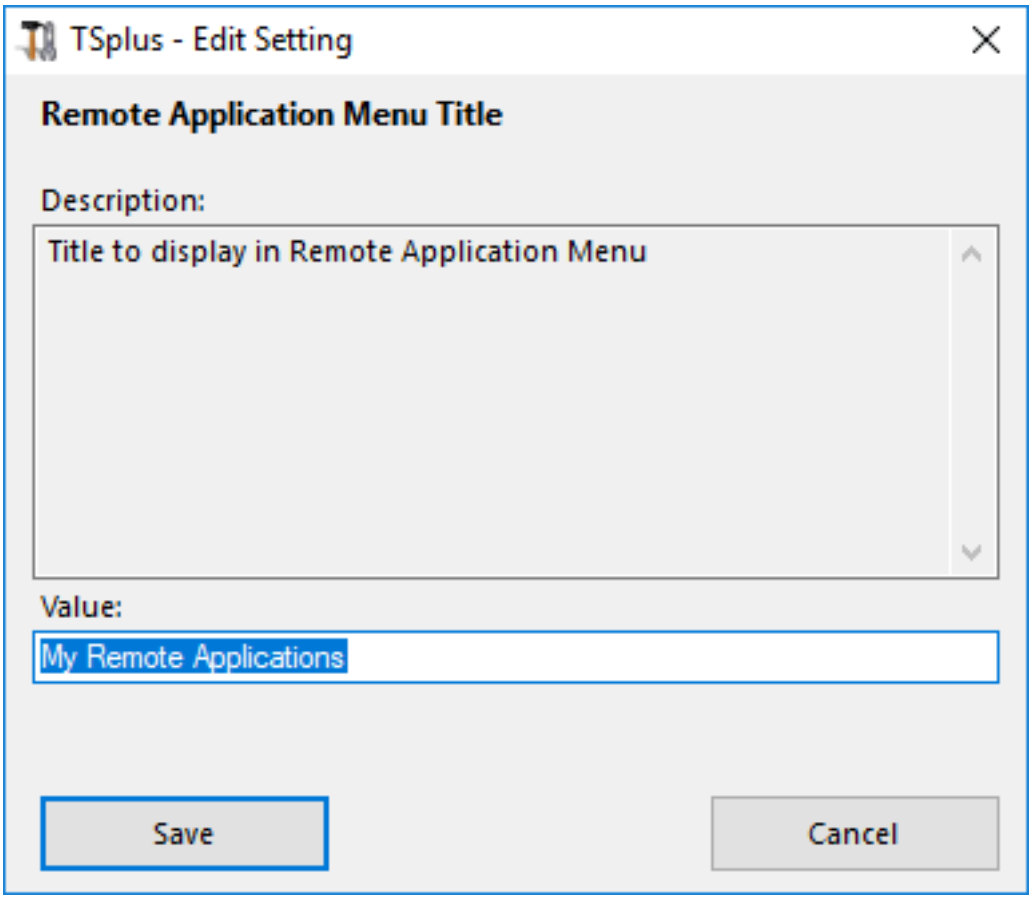
원격 애플리케이션 메뉴

원격 애플리케이션 메뉴가 사용자의 PC에 추가됩니다. 이 기능은 기본적으로 활성화되어 있습니다. 비활성화하려면 이 창에서 "아니오" 값을 선택한 후 저장을 클릭하십시오.



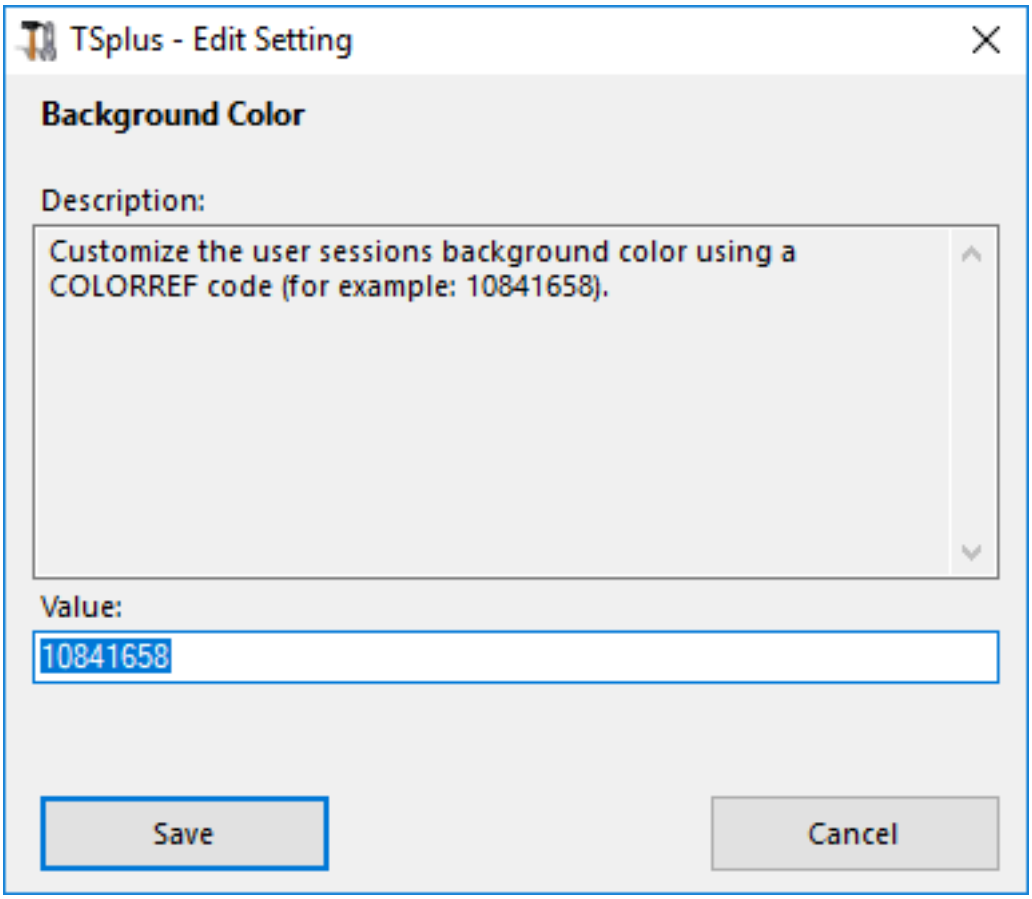
원격 애플리케이션 메뉴 제목

원격 애플리케이션 메뉴의 제목을 수정할 수 있습니다. 기본 제목은 "내 원격 애플리케이션"입니다. 수정하려면 원하는 제목을 입력한 후 저장을 클릭하세요.



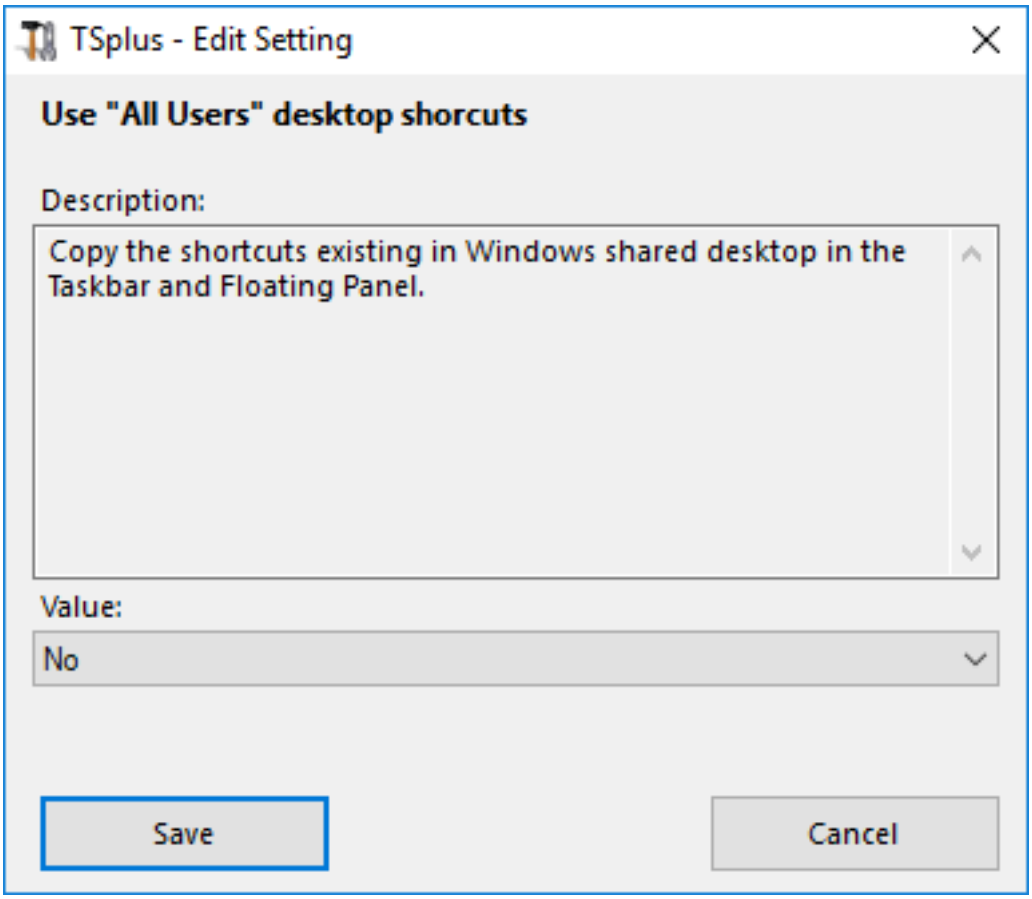
배경 색상

사용자 세션의 배경 색상을 COLORREF 코드(예: 기본값은 10841658)로 사용자 지정합니다.



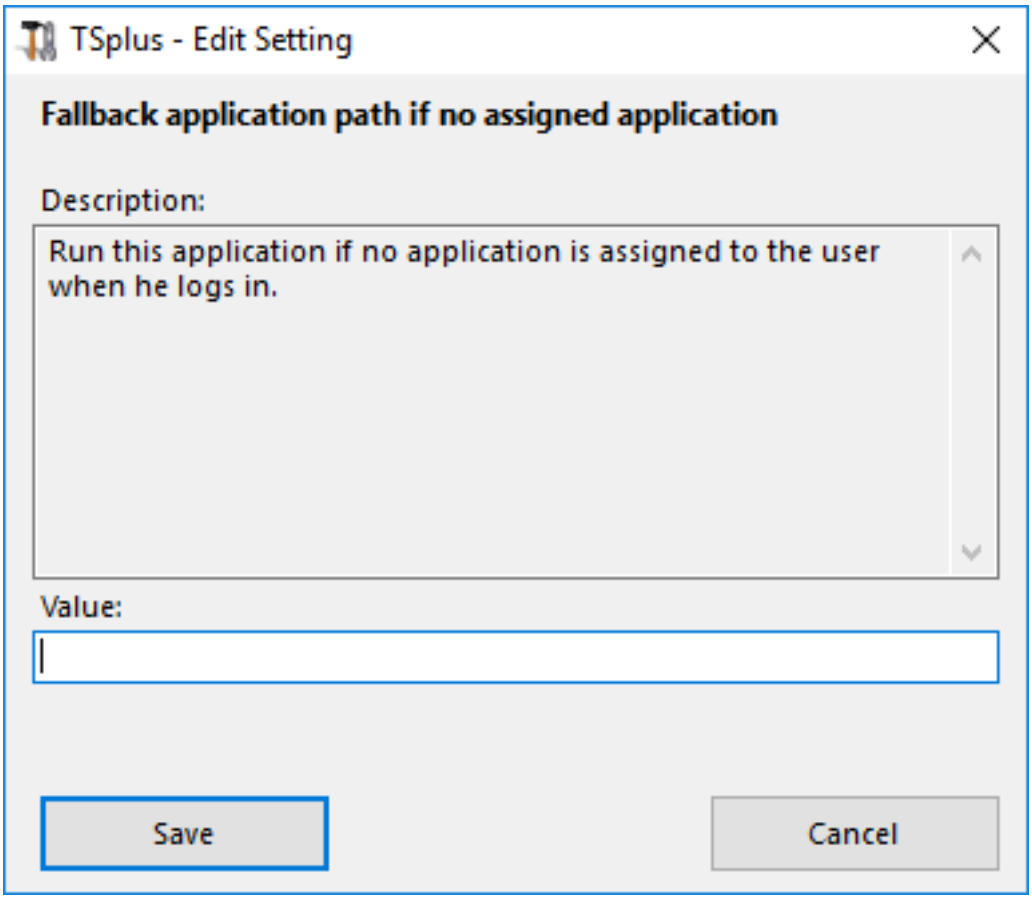
“모든 사용자” 데스크탑 바로가기를 사용하세요

Windows 공유 데스크탑에 있는 바로 가기를 작업 표시줄과 플로팅 패널에 복사합니다. 이 창에서 "예" 값을 선택하여 이 기능을 활성화한 후 저장을 클릭합니다.



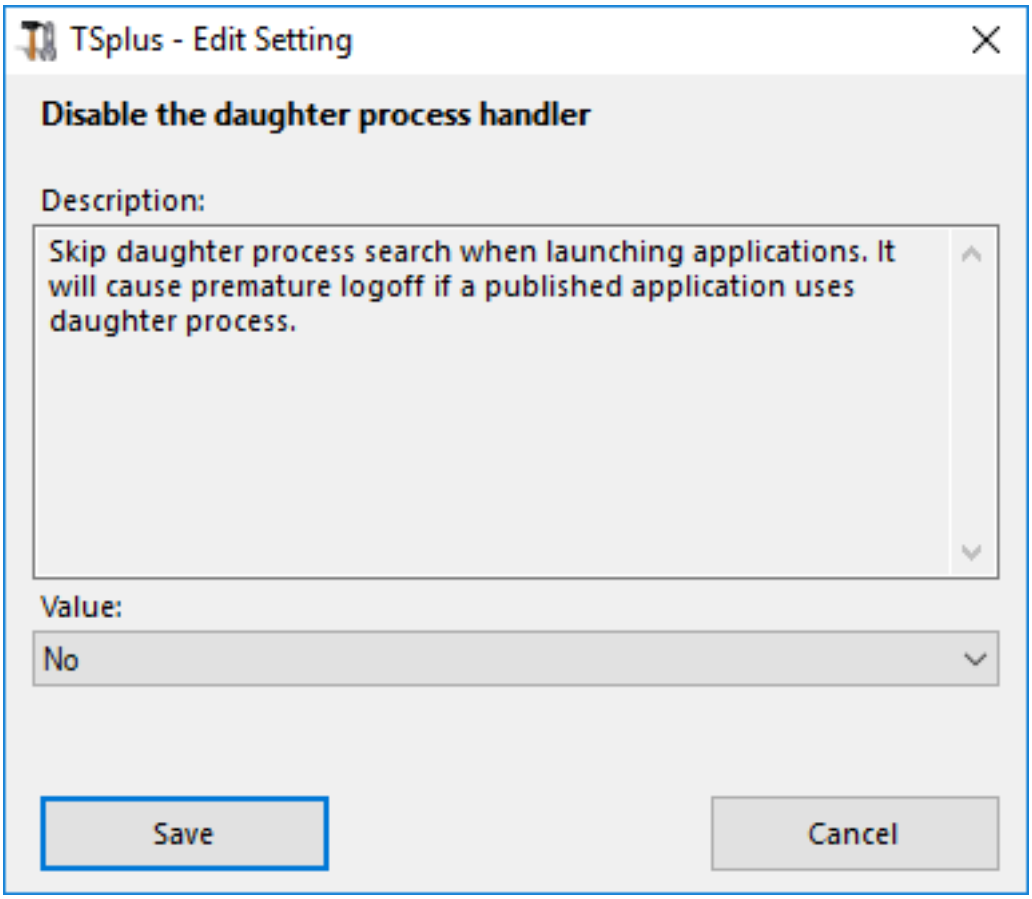
할당된 애플리케이션이 없을 경우 대체 애플리케이션 경로

이 애플리케이션은 사용자가 로그인할 때 사용자에게 할당된 애플리케이션이 없으면 실행됩니다. 기본적으로 값이 없습니다. 이 창에 "예" 값을 입력한 후 이 기능을 활성화하고 저장을 클릭하십시오.



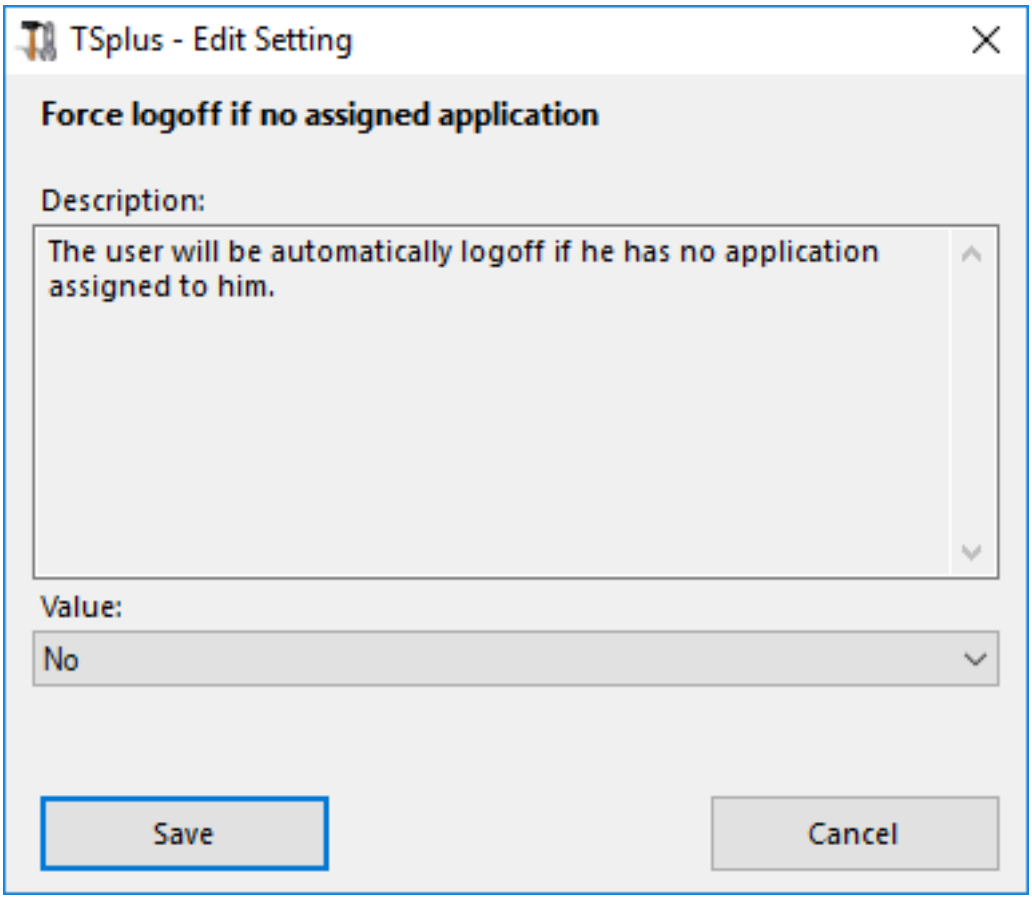
딸 프로세스 핸들러 비활성화

응용 프로그램을 시작할 때 자식 프로세스 검색을 건너뜁니다. 게시된 응용 프로그램이 자식 프로세스를 사용할 경우 조기 로그오프가 발생합니다. 이 기능은 기본적으로 비활성화되어 있습니다. 이 창에서 "예" 값을 선택하여 이 기능을 활성화한 후 저장을 클릭하십시오.



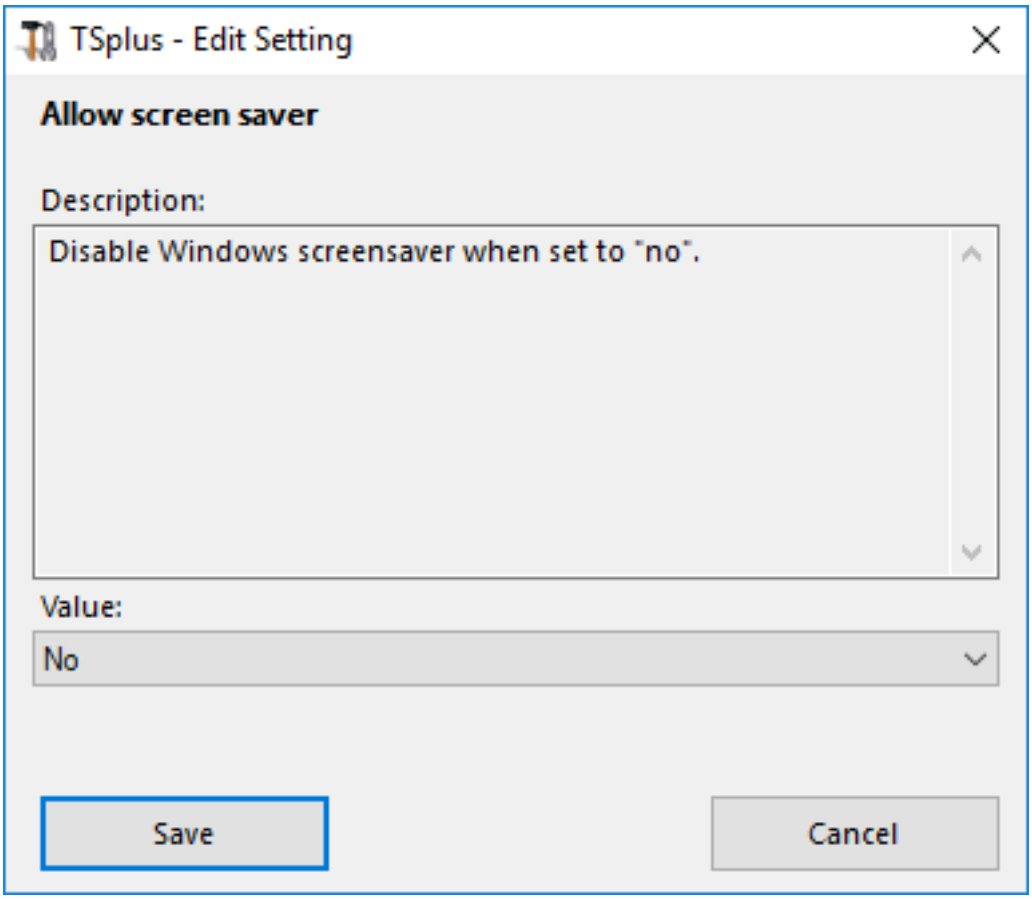
할당된 애플리케이션이 없으면 강제 로그오프

사용자에게 할당된 애플리케이션이 없으면 자동으로 로그오프됩니다. 이 기능은 기본적으로 비활성화되어 있습니다. 이 창에서 "예" 값을 선택한 후 저장을 클릭하여 이 기능을 활성화하십시오.



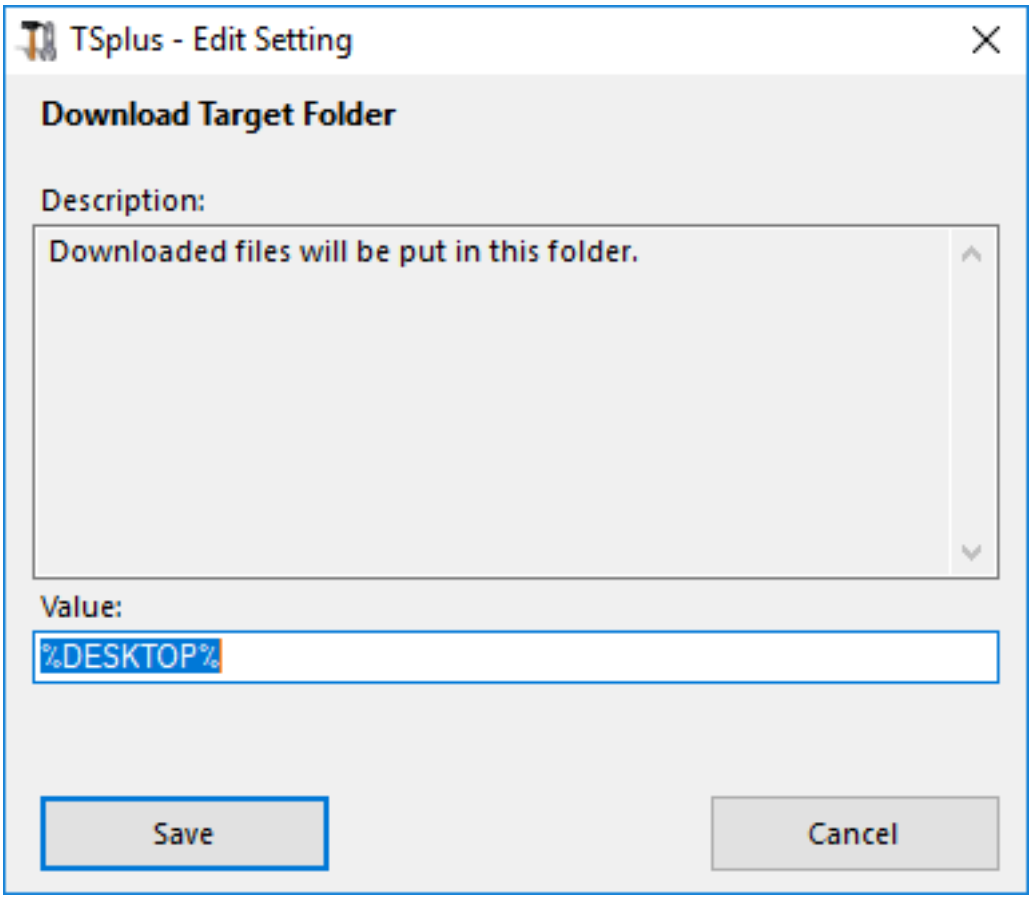
화면 보호기 허용

이 기능은 기본적으로 비활성화되어 있습니다. 이 창에서 "예" 값을 선택하여 Windows 화면 보호기를 활성화한 다음 저장을 클릭하십시오.



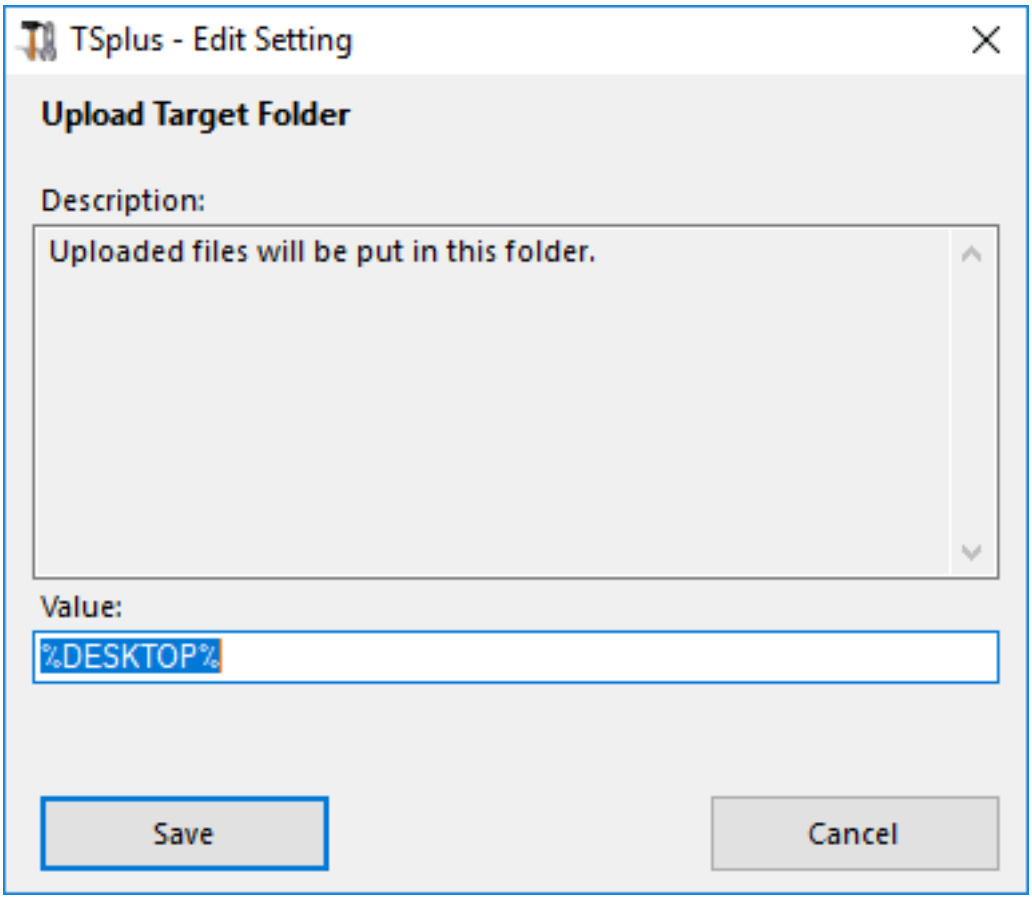
다운로드 대상 폴더

다운로드한 파일은 기본적으로 바탕화면에 저장됩니다. 수정하려면 원하는 다운로드 폴더의 경로를 입력한 후 저장을 클릭하세요.



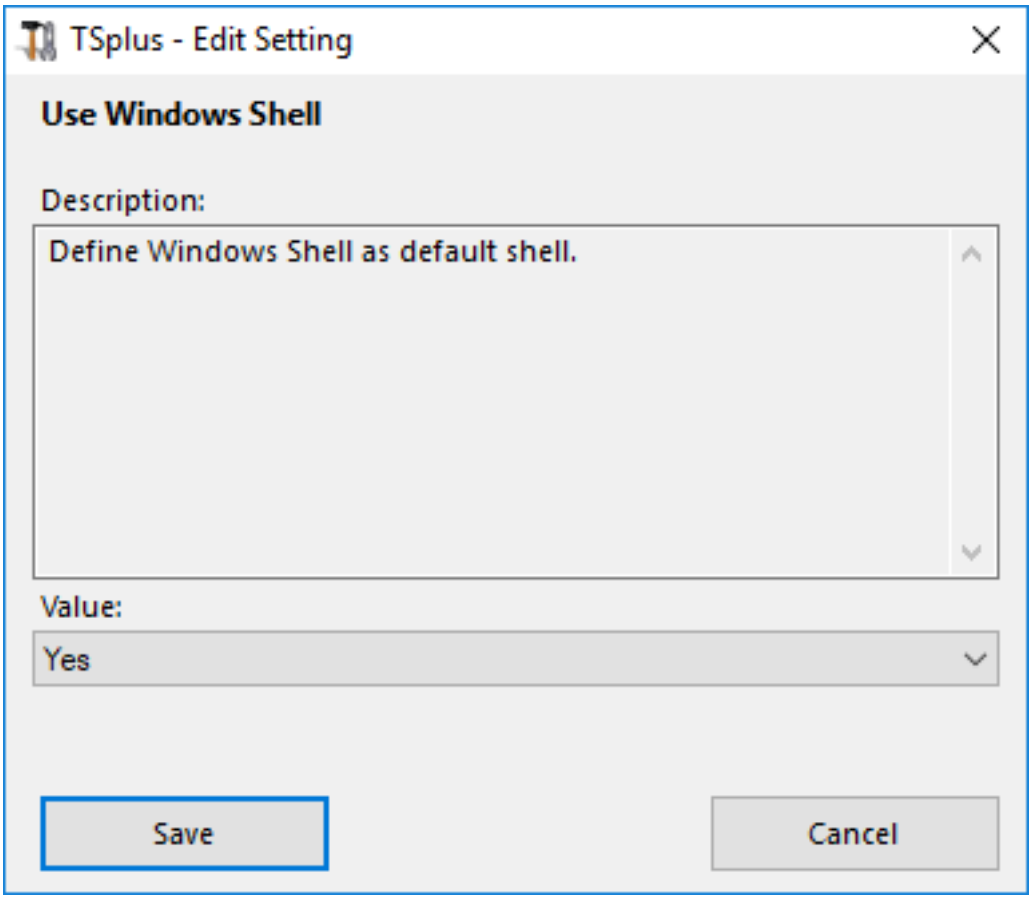
업로드 대상 폴더

업로드된 파일은 이 폴더에 저장됩니다. 수정하려면 원하는 업로드 폴더의 경로를 입력한 후 저장을 클릭하세요.



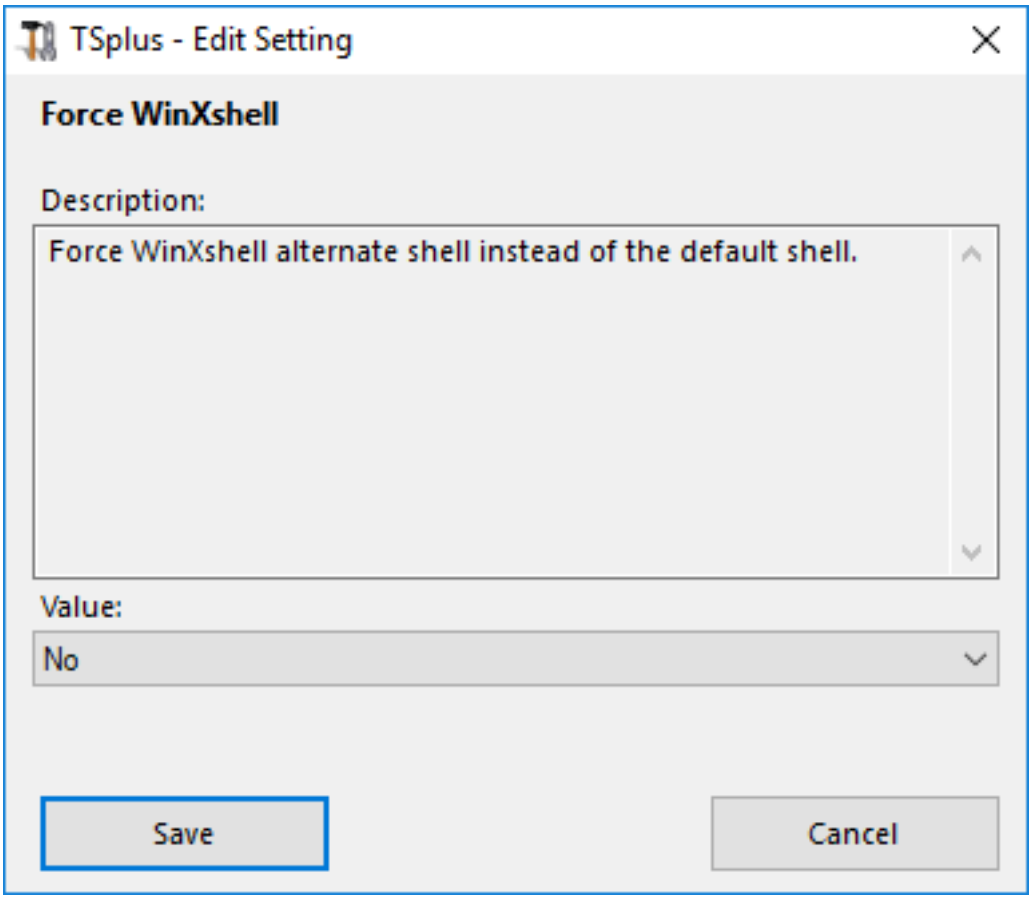
Windows 셸 사용

Windows Shell을 기본 셸로 정의합니다. 이 기능은 기본적으로 활성화되어 있습니다. 비활성화하려면 이 창에서 "아니오" 값을 선택한 다음 저장을 클릭하십시오.



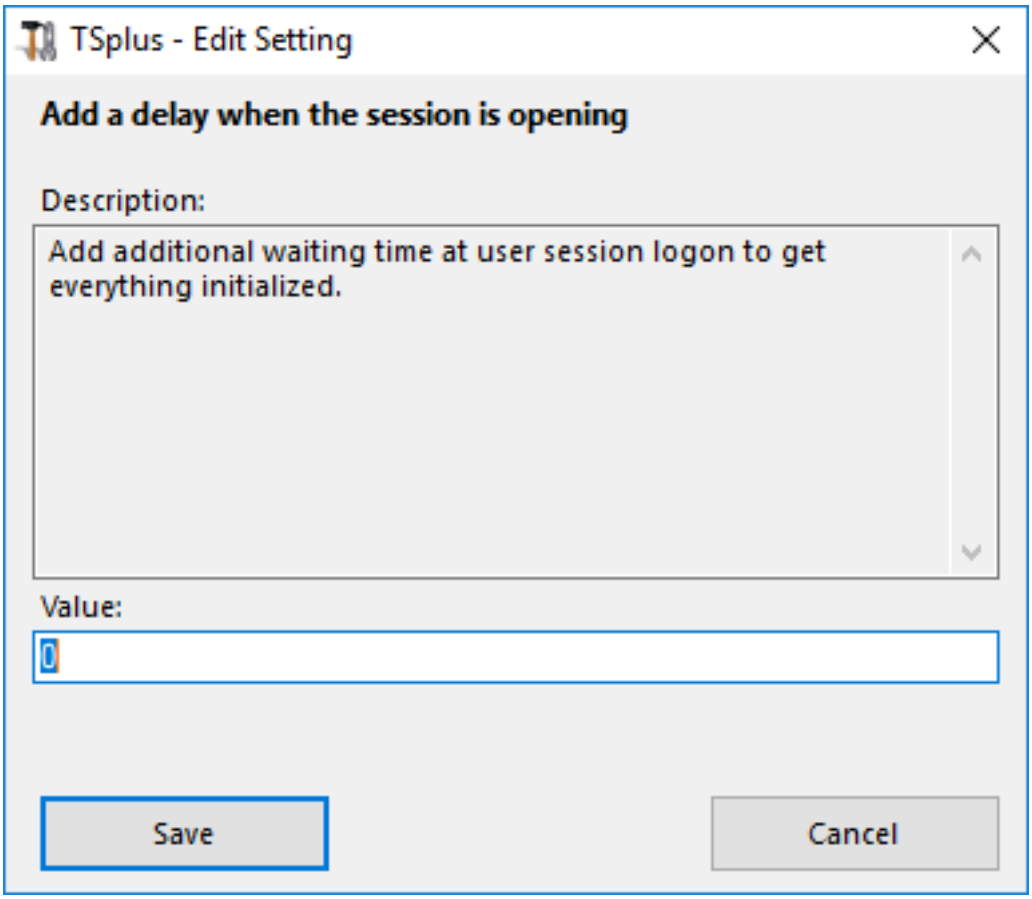
WinXshell 강제 실행

이 기능은 기본적으로 비활성화되어 있습니다. 이 창에서 "예" 값을 선택하여 기본 셸 대신 WinXshell 대체 셸을 강제로 사용한 후 저장을 클릭하십시오.



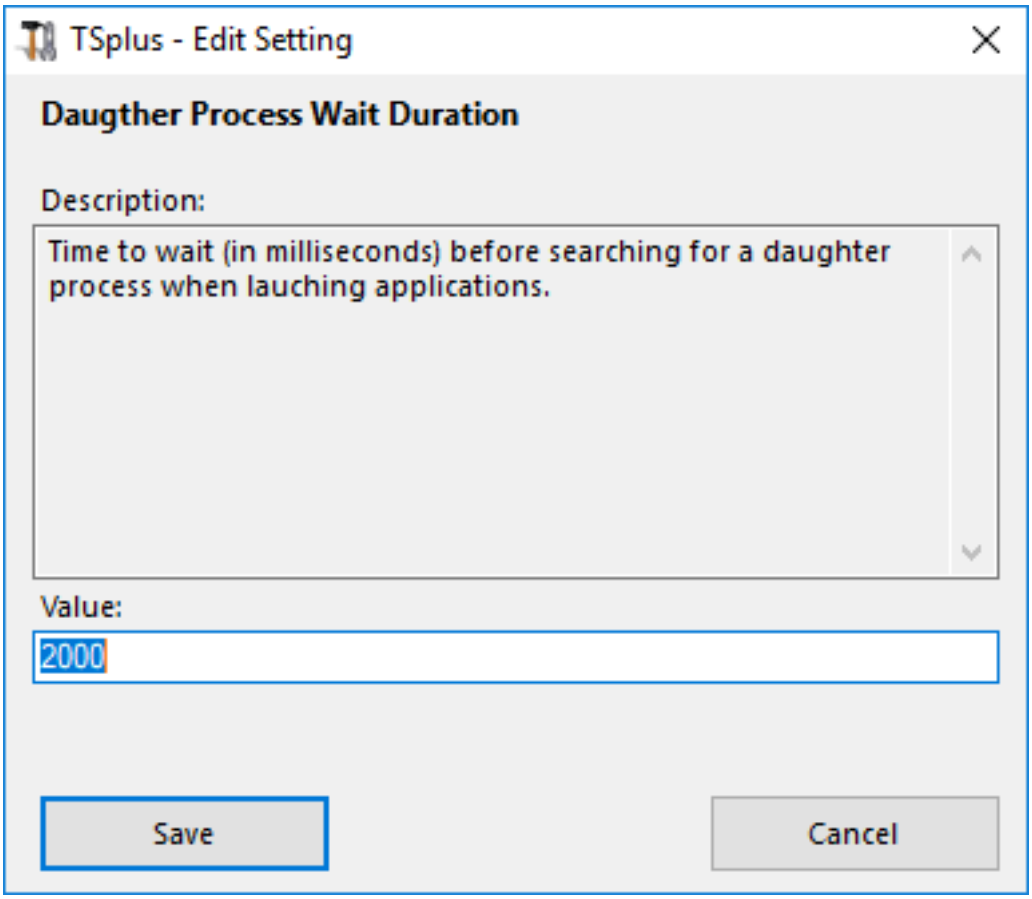
세션이 열릴 때 지연 추가

사용자 세션 로그온 시 모든 것이 초기화되도록 추가 대기 시간을 추가하십시오. 기본값은 0입니다. 수정하려면 원하는 값을 입력한 후(초 단위) 저장을 클릭하십시오.



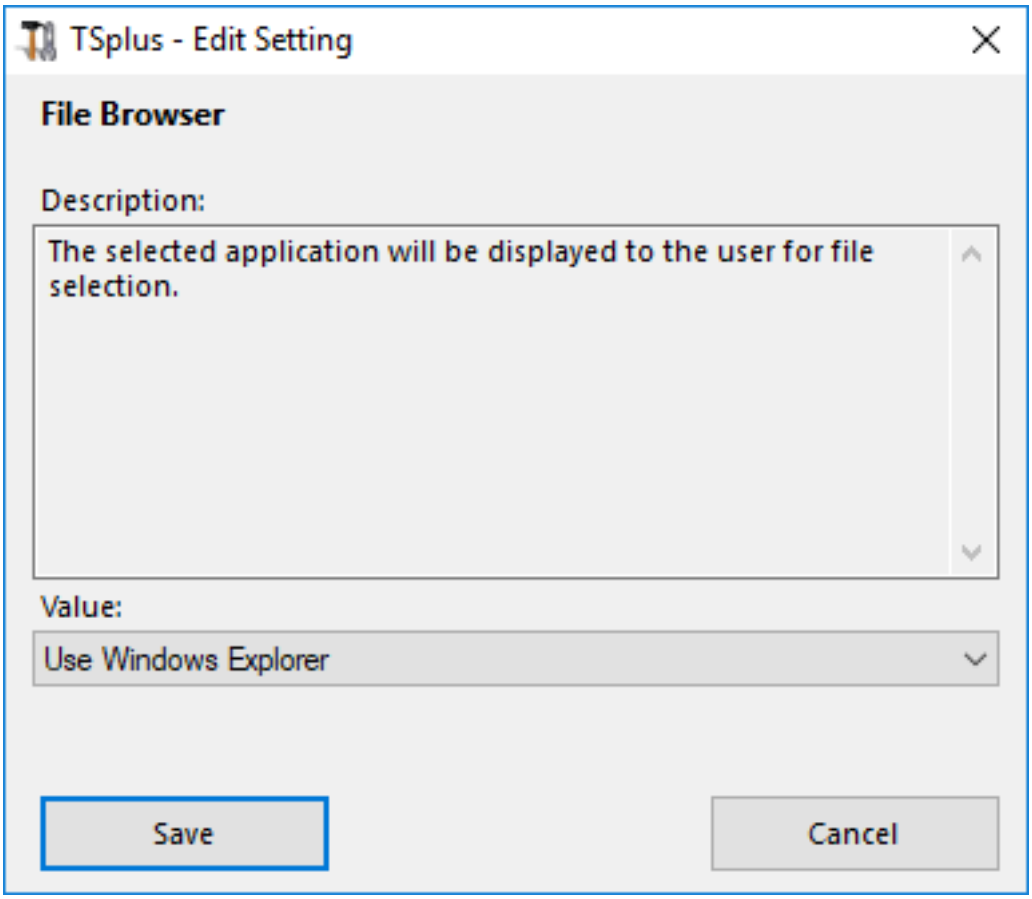
자식 프로세스 대기 시간

응용 프로그램을 시작할 때 자식 프로세스를 검색하기 전에 대기할 시간(밀리초).



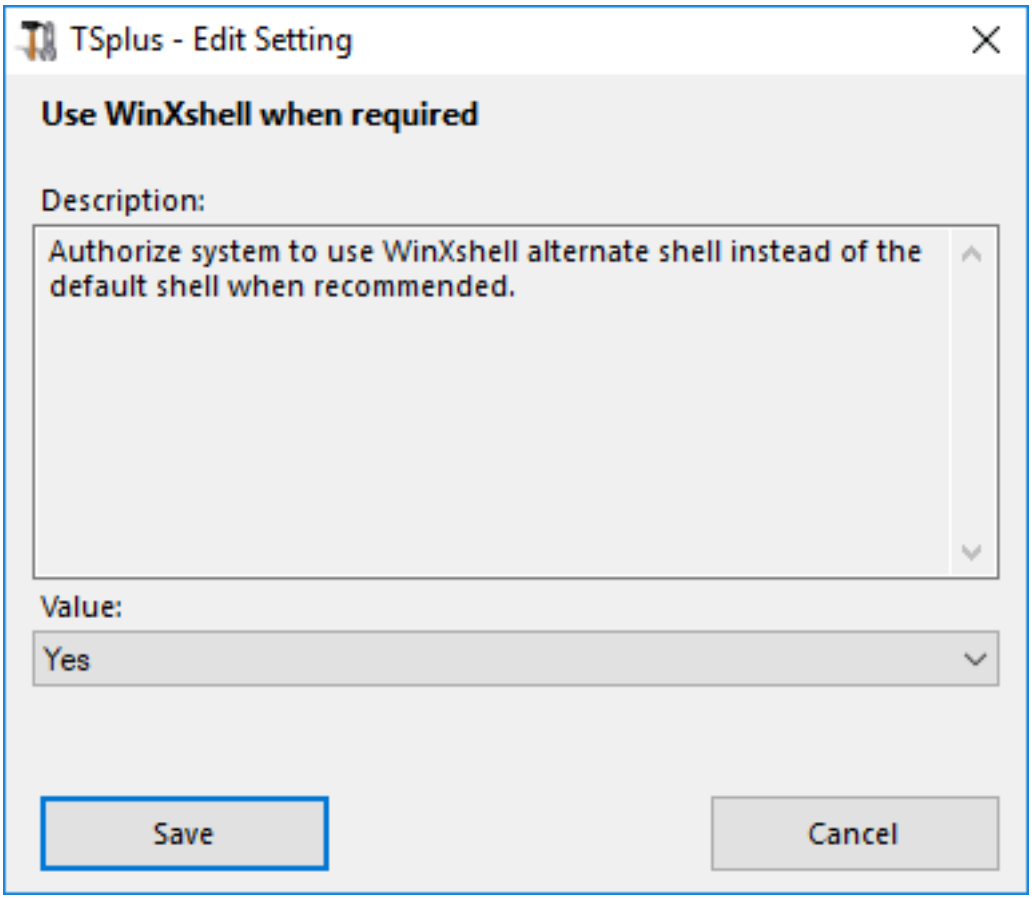
파일 탐색기

선택한 애플리케이션이 파일 선택을 위해 사용자에게 표시됩니다. 기본 브라우저는 Windows 탐색기입니다. TSplus 파일 브라우저를 선택한 후 저장을 클릭하여 사용할 수 있습니다.



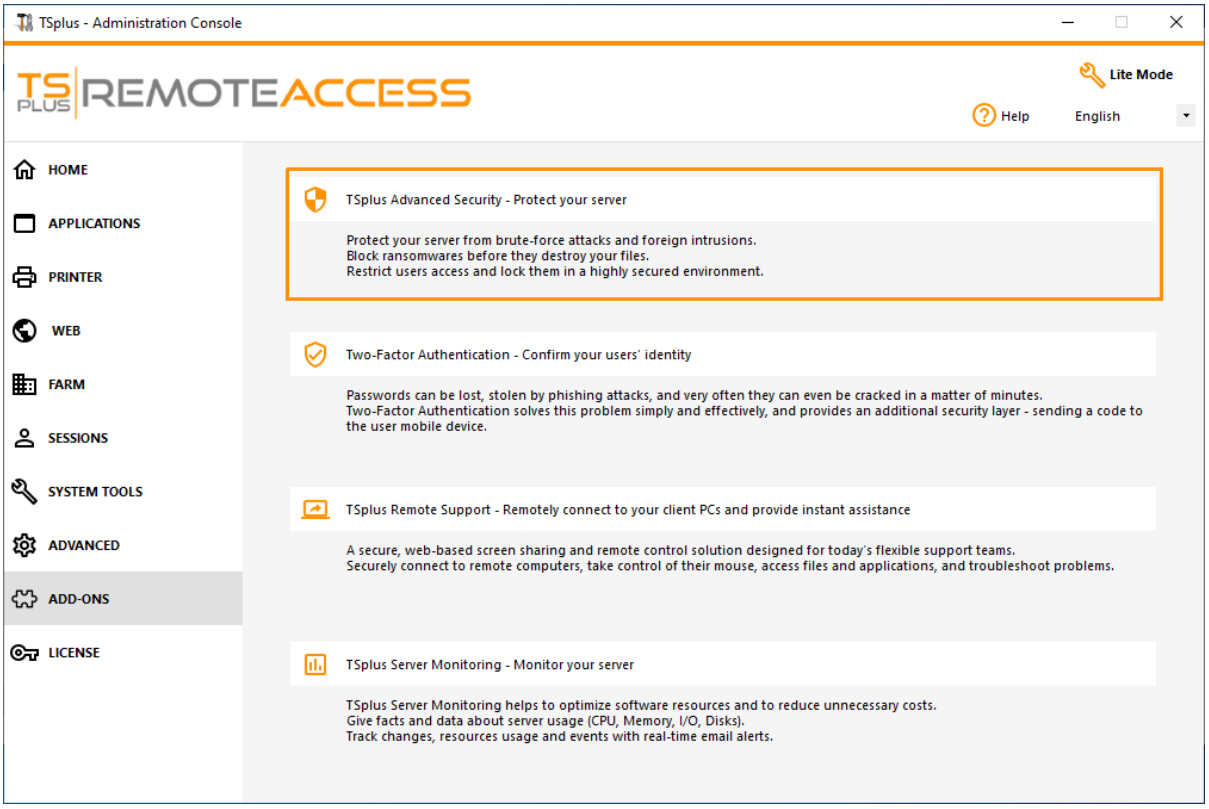
WinXshell이 필요할 때 사용하세요.

시스템이 기본 셸 대신 WinXshell 대체 셸을 사용하도록 권한을 부여합니다. 이 기능은 기본적으로 활성화되어 있습니다. 비활성화하려면 이 창에서 "아니오" 값을 선택한 다음 저장을 클릭하십시오.


TSplus - Edit Setting
Use WinXshell when required
Description:
Authorize system to use WinXshell alternate shell instead of the default shell when recommended.
Value:
Yes
Save
Cancel

TSplus 고급 보안

TSplus Advanced Security는 TSplus AdminTool의 Add-On으로 제공되며 Add-Ons 탭에서 사용할 수 있습니다.

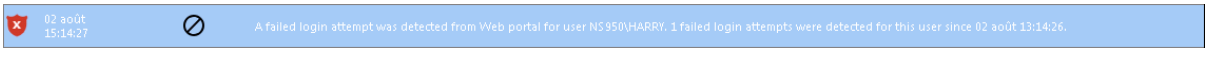


전체 문서를 찾을 수 있습니다. 이 페이지에서 .

잠금 이벤트

TSplus 잠금 귀하의 TSplus 서버에서 웹 로그인 시도 실패를 모니터링합니다.

TSplus Advanced Security는 아래 예와 같은 웹 포털 실패 시도 후 잠금 이벤트를 표시합니다.



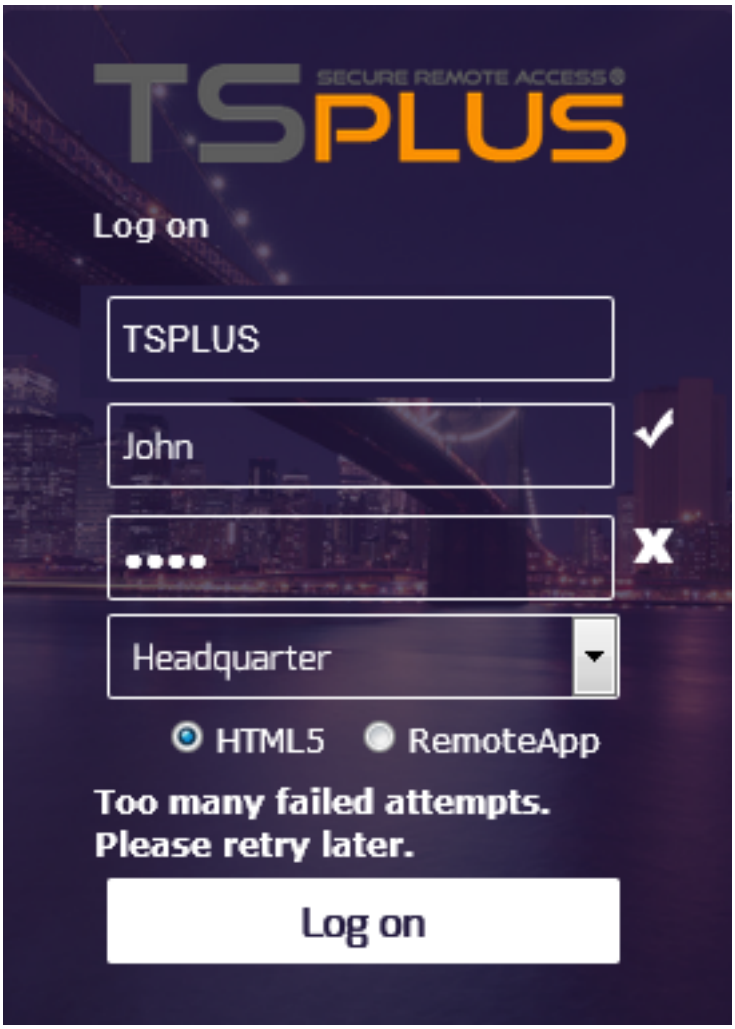
“웹 포털에서 사용자 … 에 대한 로그인 실패 시도가 감지되었습니다. 이 사용자에 대해 1회의 로그인 실패 시도가 감지되었습니다…”

Bruteforce Protection은 해커, 네트워크 스캐너 및 관리자의 로그인과 비밀번호를 추측하려는 브루트포스 로봇으로부터 공용 서버를 보호할 수 있게 해줍니다. 현재 로그인 및 비밀번호 사전을 사용하여, 이들은 매 분마다 수백에서 수천 번 서버에 로그인하려고 자동으로 시도할 것입니다. 이 기능에 대한 자세한 내용은 여기에서 확인하세요. 이 페이지 .

웹 포털에서

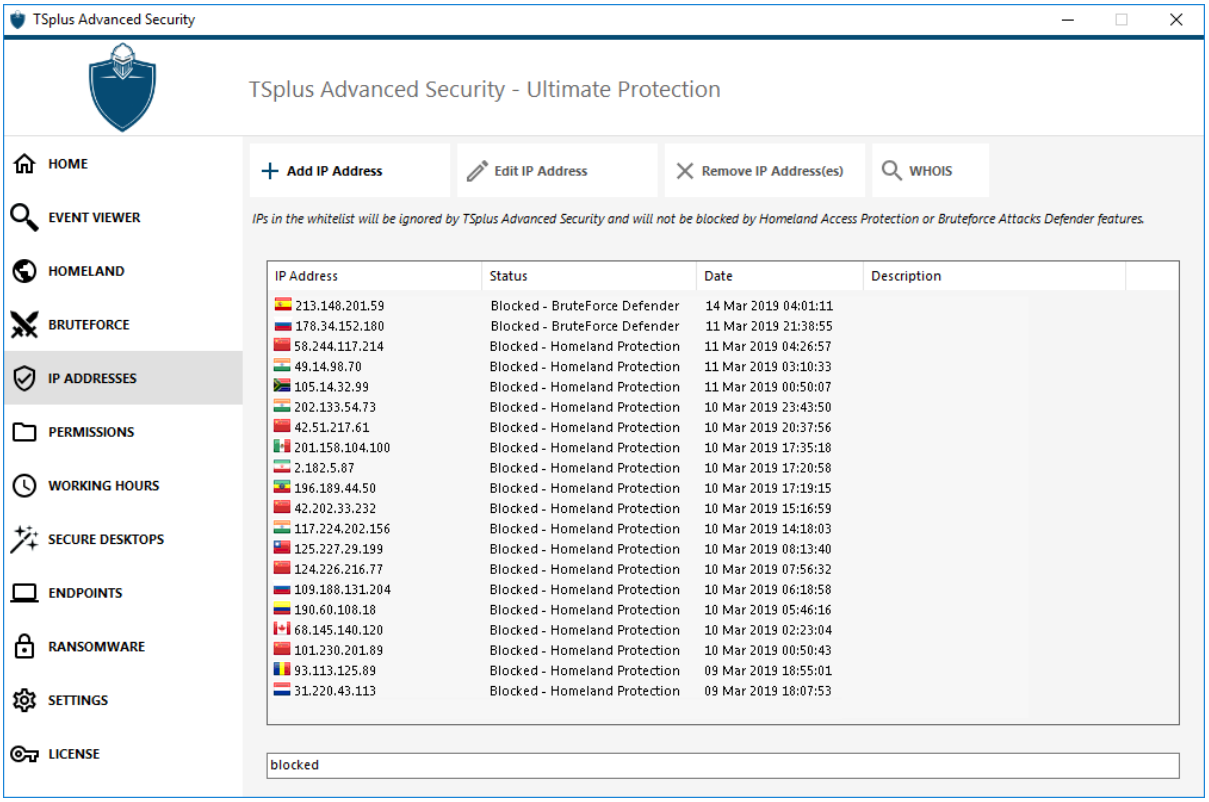
웹 포털에서 사용자가 잘못된 자격 증명을 입력할 때 브루트 포스 공격이 차단됩니다.

10분 동안 10회 시도한 후, 웹 포털은 사용자가 20분 동안 로그인하는 것을 금지합니다.



기본 설정으로, [ ]에서 사용자 정의할 수 있습니다. BruteForce 보호 탭 TSplus 고급 보안 관리 도구입니다.

TSplus Advanced Security Ultimate Protection의 IP 주소 타일에서 모든 차단된 연결 및 로그를 확인할 수 있습니다.



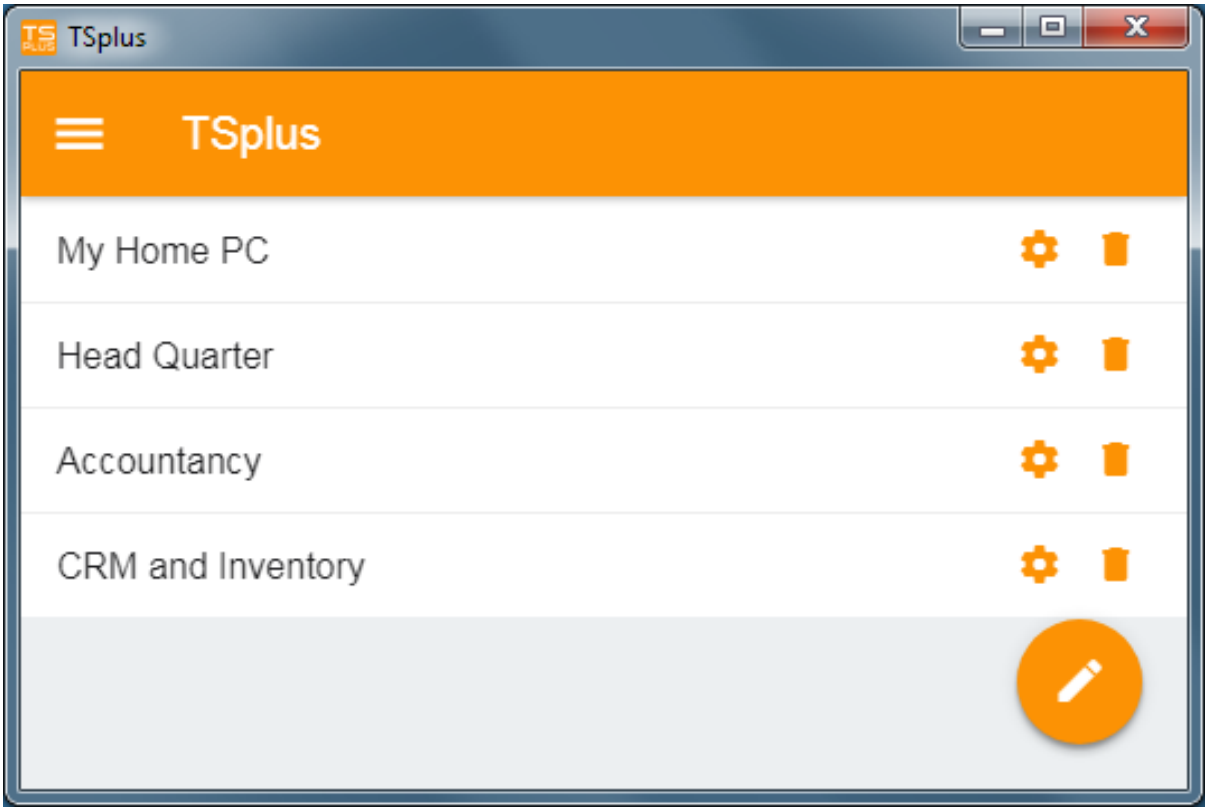
이 기능은 첫 번째 웹 포털 연결 후에 표시되고 활성화됩니다.

TSplus Advanced Security에 대한 전체 문서가 제공됩니다. 이 페이지에서 .

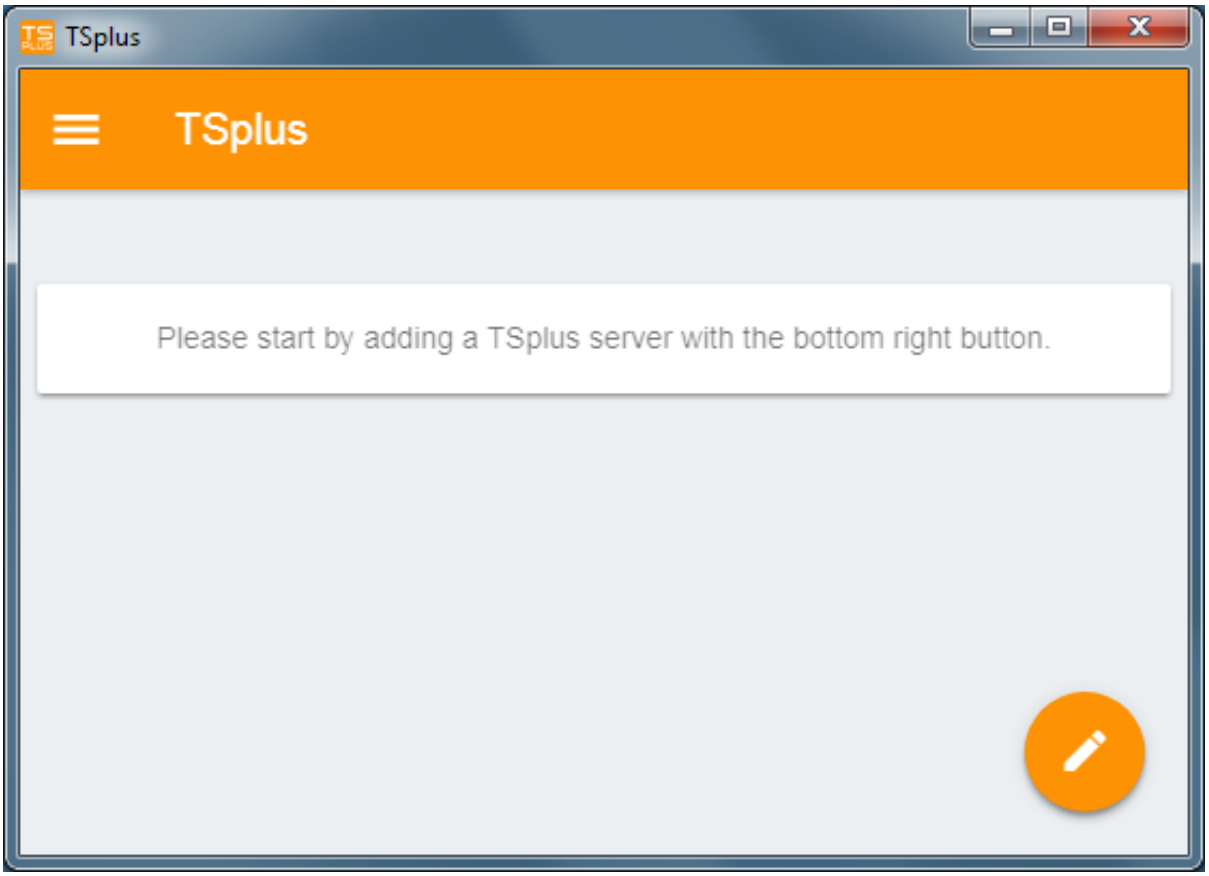
TSplus 앱 구성

서버 관리

사용자 인터페이스와 구성은 간단하고 직관적입니다.



먼저, 오른쪽 하단 버튼을 클릭하여 TSplus 서버를 추가하세요:

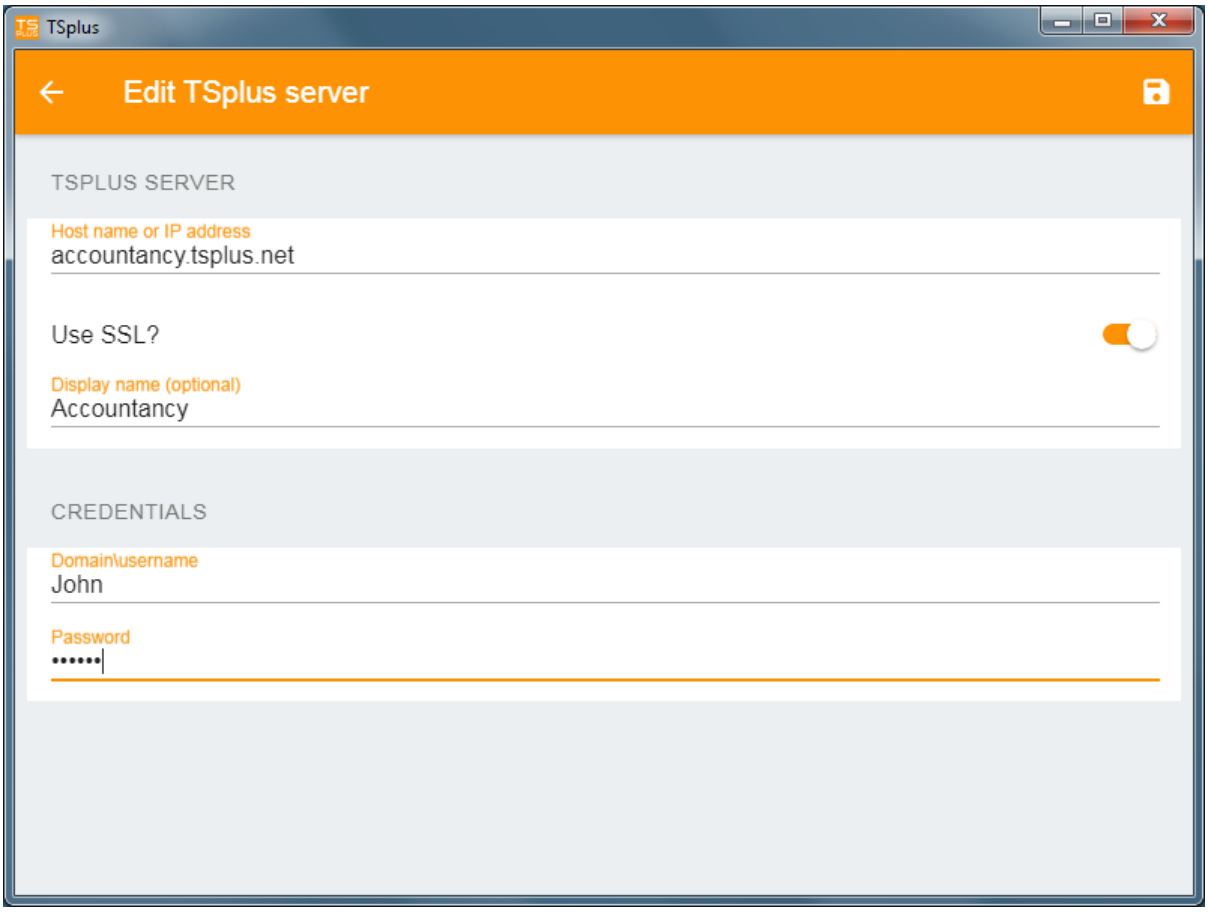


그런 다음 서버 정보를 추가하고 구성하십시오:

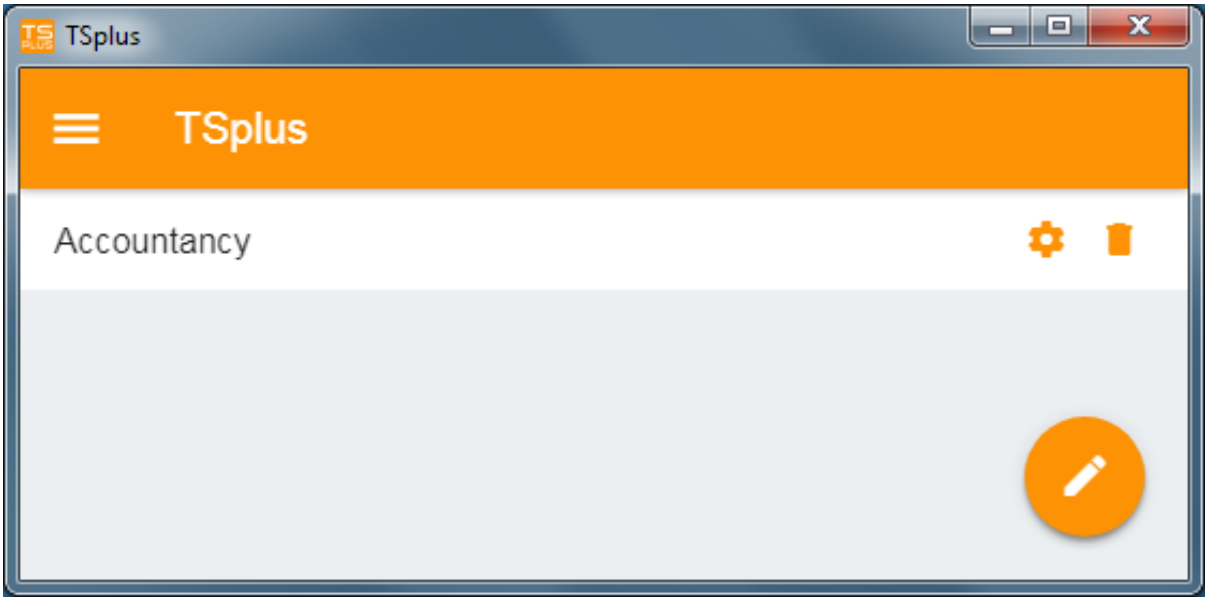
- 호스트 이름 또는 IP 주소를 입력하세요.
- SSL은 기본적으로 비활성화되어 있지만, 활성화하도록 선택할 수 있습니다.

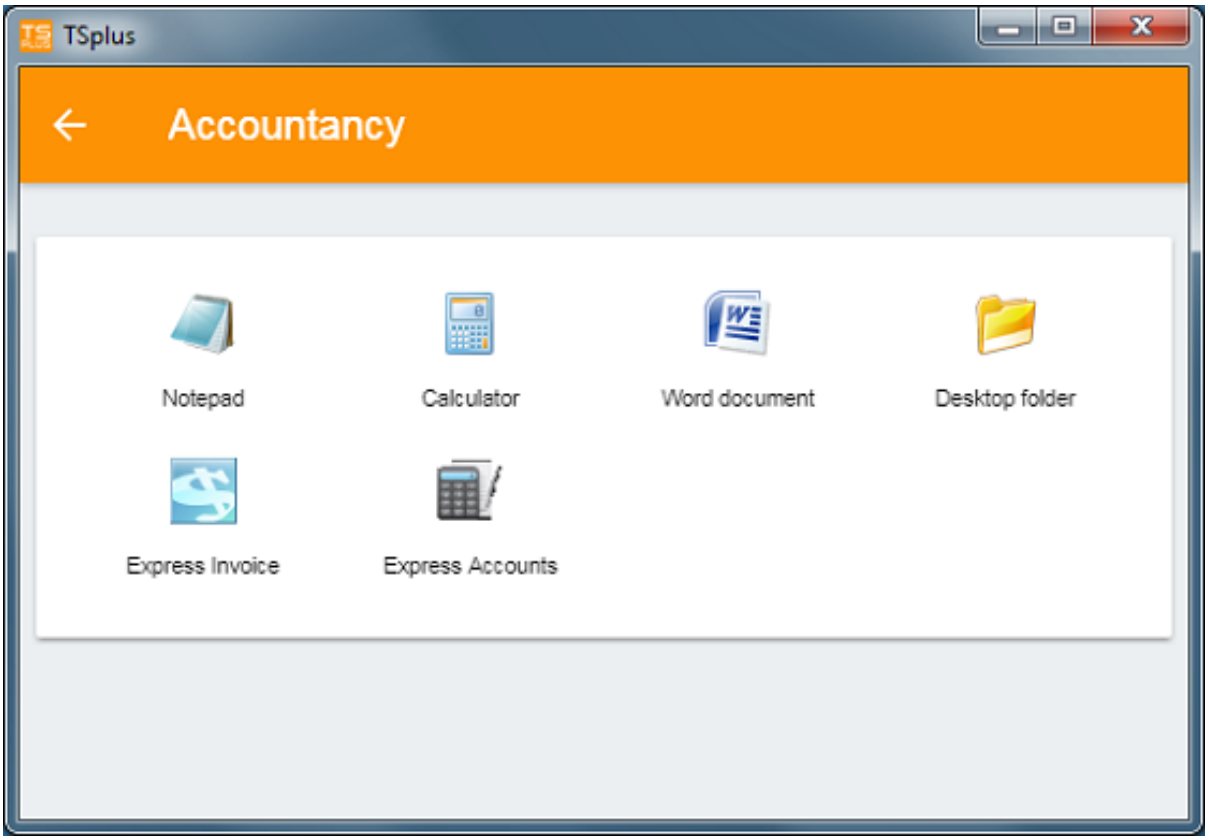
경고: SSL 활성화는 TSplus 서버에 유효한 SSL 인증서를 설치한 경우에만 작동합니다. 확인하세요. 이 문서 자세한 정보는 다음과 같습니다.

- 표시 이름을 입력하세요. (선택 사항)
- 사용자의 자격 증명과 도메인 또는 사용자 이름 및 비밀번호를 입력하세요.
- HTTPS 프로토콜을 사용하는 경우, 구성된 주소에 포트를 입력해야 합니다. appportal.mydomain.com:443



그런 다음 오른쪽 상단 버튼을 클릭하여 저장하십시오. 이제 서버를 클릭하여 애플리케이션에 액세스할 수 있습니다.





인쇄

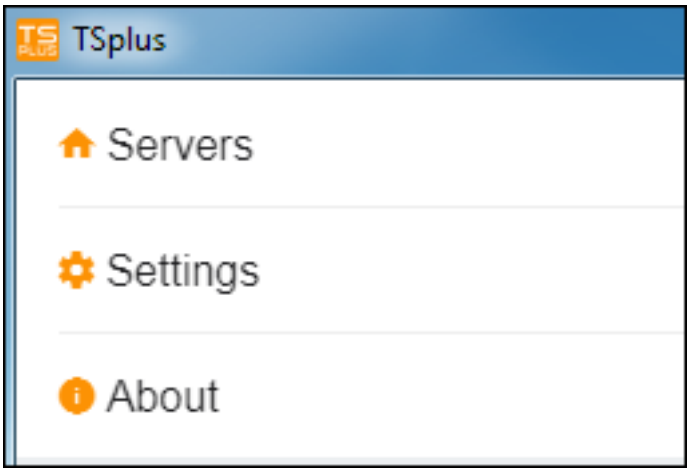
로컬 프린터에서 쉽게 인쇄할 수 있습니다. 유니버설 프린터 .

TSplus App 11.40 버전 이후로, 인쇄된 문서는 기본 PDF 리더 앱으로 열립니다.

설정 및 버전

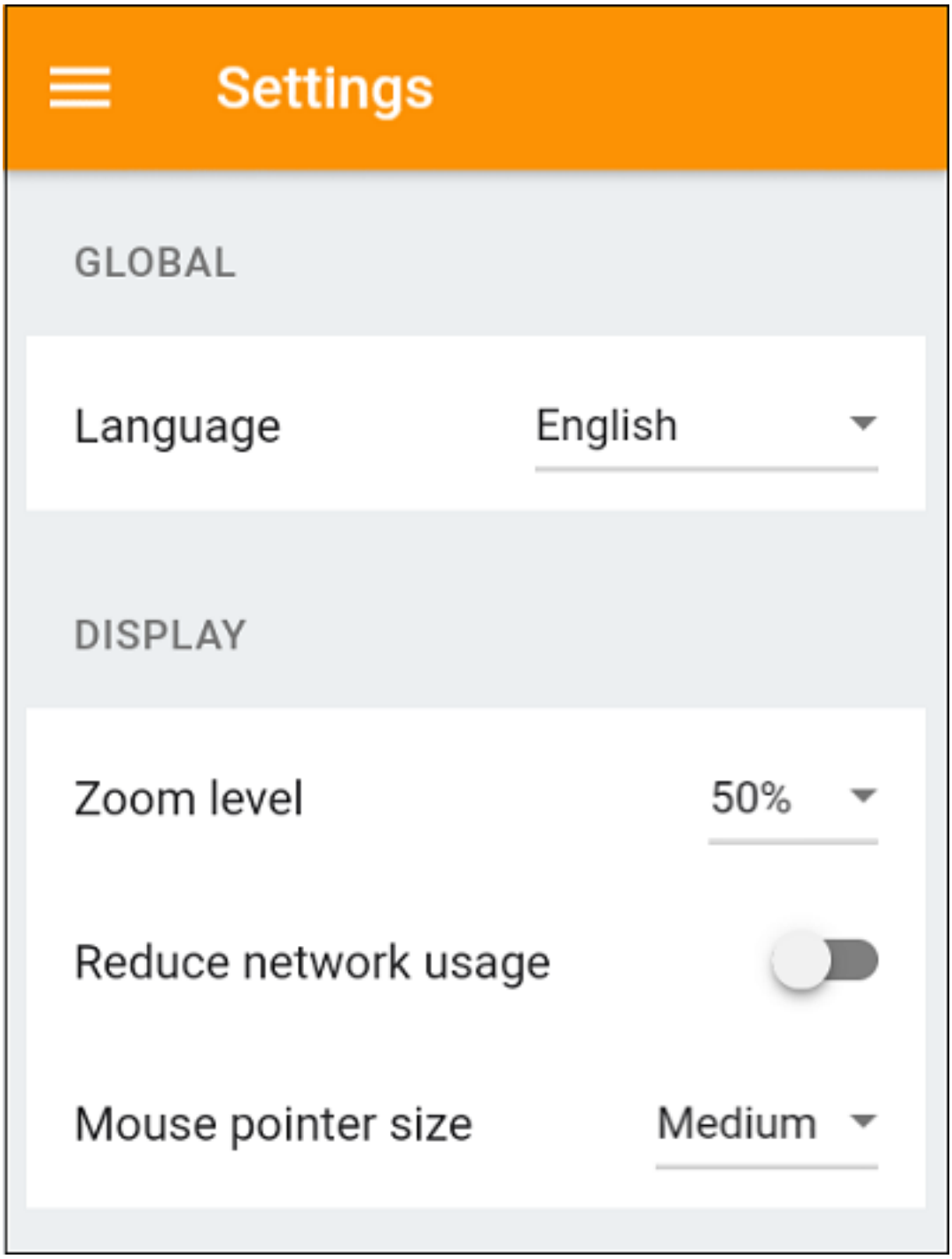
왼쪽 상단 메뉴에서 다음을 수행할 수 있습니다:

- 서버 관리
- 설정을 관리하세요
- 법적 정보는 정보 섹션에서 확인하시고, 귀하의 TSplus 앱 버전을 확인하십시오.



설정

설정 창에서 다양한 설정을 사용할 수 있습니다:



- 언어를 변경할 수 있습니다.
- 디스플레이 설정을 조정하여 편리하게 확대/축소 수준을 변경하고, 네트워크 사용량을 줄이거나 3가지 마우스 포인터 크기(작음, 중간, 큼) 중에서 선택하세요.

2FA 인증

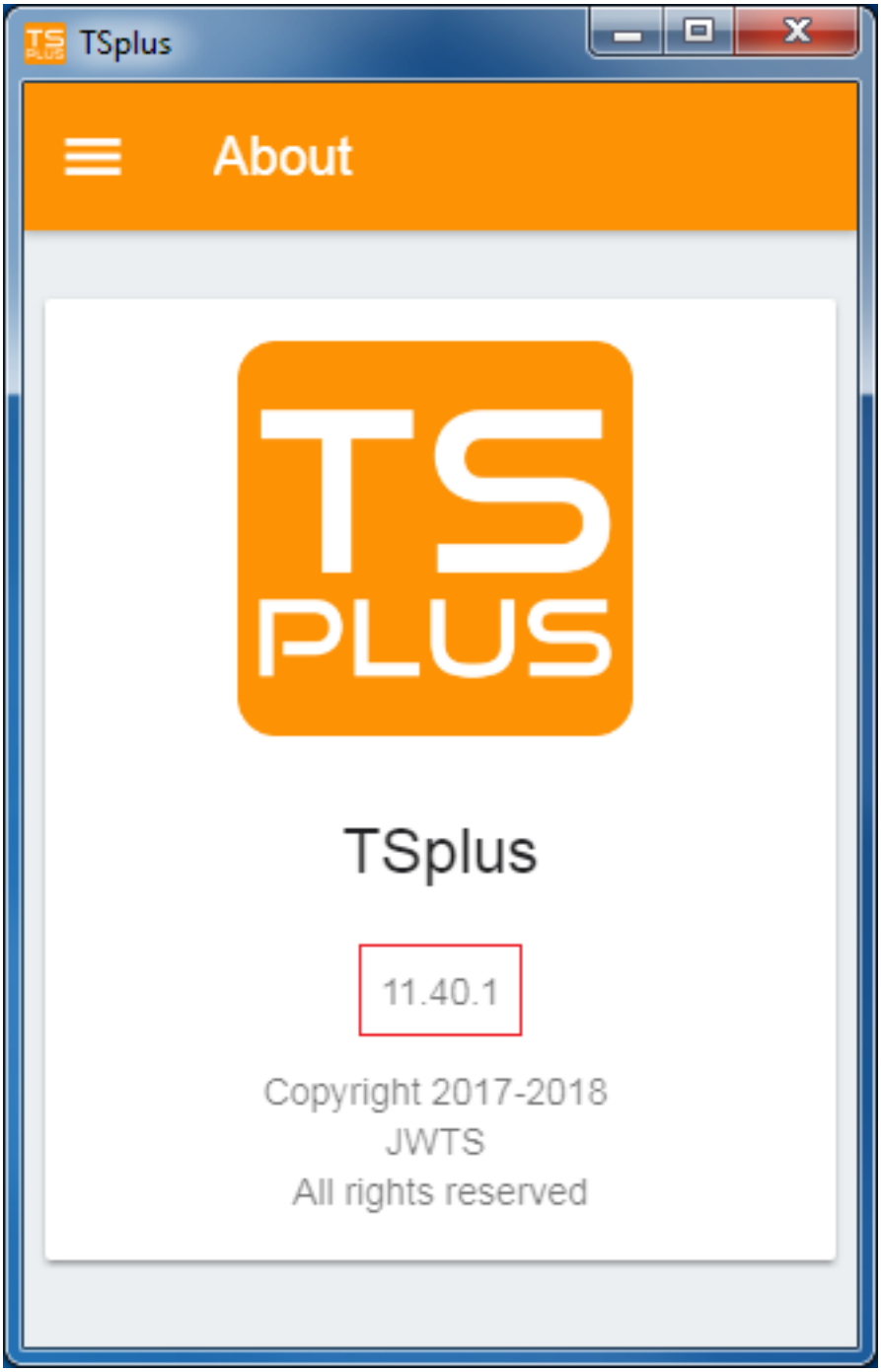
안드로이드 앱은 2FA와 호환됩니다.

앱은 사용자 계정이 2FA를 사용하도록 설정된 경우 2FA 코드를 요청합니다.

모바일 앱에서 활성화할 수 없으며, 먼저 웹 포털에서 2FA를 구성해야 합니다.

버전

정보 탭에서 법적 정보와 현재 TSplus 앱 버전을 확인할 수 있습니다.



TSplus 앱

TSplus 앱을 사용하면 언제 어디서나 모든 장치에서 TSplus 서버에 연결할 수 있습니다!

TSplus처럼 태블릿과 스마트폰에서 Windows 데스크탑 및 비즈니스 애플리케이션으로 빠르고 안정적인 원격 연결을 제공합니다.

애플리케이션과 비즈니스 데이터를 실시간으로 액세스하고 필요한 모든 문서와 사진을 가장 가까운 로컬 프린터에서 쉽게 인쇄하세요.

TSplus 앱은 2FA와 호환됩니다.



자세한 정보와 다운로드 링크는 저희 웹사이트의 앱 페이지로 가세요.

하드웨어 요구 사항 및 운영 체제

TSplus 앱은 다음 운영 체제를 지원하는 모바일 및 태블릿에서 사용할 수 있습니다: iOS, Android 4.4 버전 이상 및 Linux.

안드로이드 버전

iOS 버전

사전 요구 사항

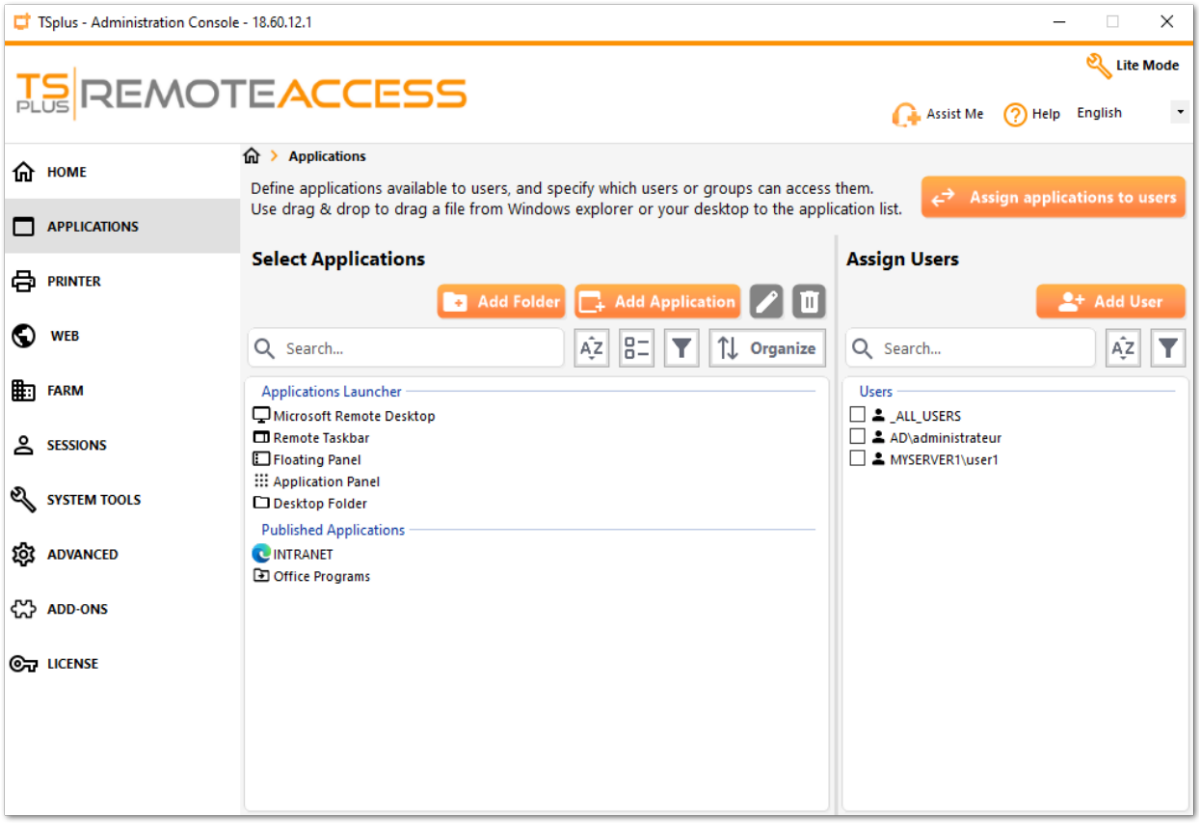
- 호스트 사이트는 TSplus 모바일 웹 또는 엔터프라이즈 시스템이어야 합니다.
- 11.30 이상의 릴리스는 이 호스트에 설치되어야 합니다.

사용자 또는 그룹에 애플리케이션 할당

한 번 당신이 일부 애플리케이션을 게시했습니다. , 하나 이상의 사용자 및/또는 그룹에 할당할 수 있습니다.

사용자 또는 그룹을 애플리케이션에 할당

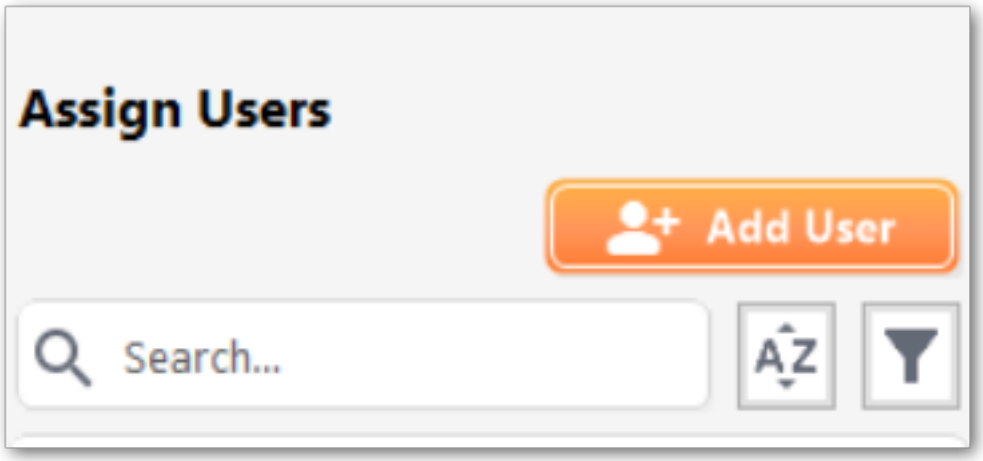
모든 할당은 AdminTool의 "응용 프로그램" 섹션의 오른쪽 패널에서 수행되어야 합니다. 이 오른쪽 패널은 현재 응용 프로그램이 할당된 모든 사용자와 그룹을 보여줍니다.



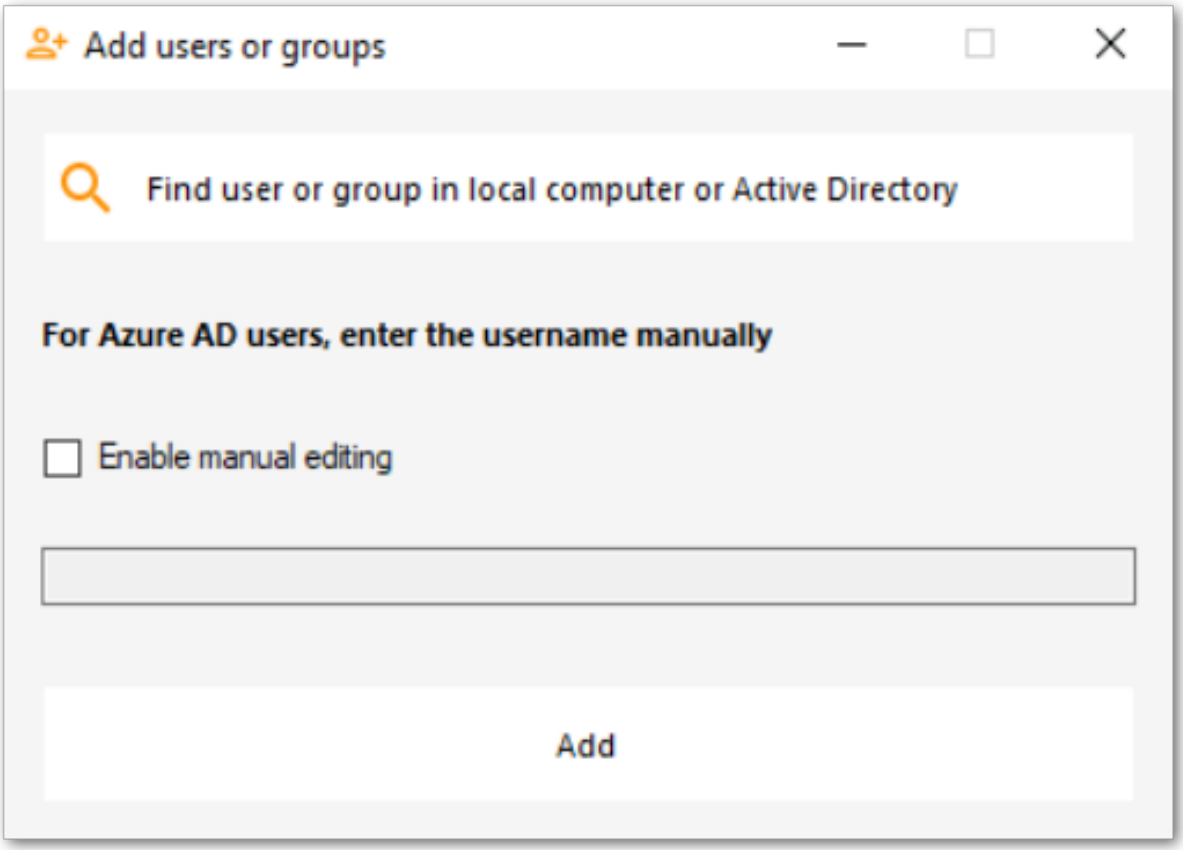
사용자 또는 그룹을 할당하려면 먼저 애플리케이션을 할당할 사용자/그룹을 추가해야 합니다.

사용자 또는 그룹 추가

사용자 또는 그룹을 추가하려면 "사용자 추가" 아이콘 버튼을 클릭하십시오.



이 인터페이스가 표시되며, 사용자/그룹 선택기를 통해 사용자 또는 그룹을 찾거나 추가하려는 사용자/그룹의 이름을 직접 입력할 수 있습니다.
로컬 또는 Active Directory 사용자는 로컬 또는 Active Directory 사용자 또는 그룹 찾기 버튼을 사용하여 선택해야 합니다.
외부 사용자만 텍스트 상자에 직접 입력할 수 있습니다.



_ALL_USERS 특수 사용자 이름

사용자 목록에서 항상 “_ALL_USERS” 사용자를 찾을 수 있습니다. 이 사용자는 Windows 사용자가 아니라 가상 사용자입니다. 애플리케이션을 선택하고 “_ALL_USERS” 사용자 이름을 선택하면 해당 애플리케이션이 모든 사용자에게 제공됩니다.

사용자 또는 그룹을 애플리케이션에 할당

사용자가 추가되면, 다음과 같이 애플리케이션을 할당합니다:

1. 왼쪽 패널에서 사용자에게 할당할 애플리케이션을 선택합니다.
2. 오른쪽 패널에서 해당 사용자의 사용자 이름 옆에 있는 상자를 선택하여 선택한 애플리케이션을 해당 사용자에게 할당합니다.

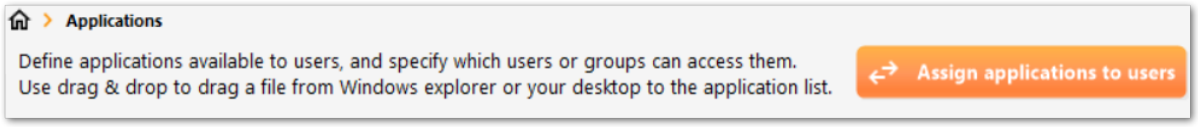
예: 사용자가 "benjamin"에게 메모장을 할당하려면 왼쪽에서 "메모장" 애플리케이션을 선택하고 오른쪽에서 사용자 이름 "benjamin" 옆의 상자를 체크하면 됩니다.

사용자를 할당 해제하려면 사용자 이름 옆의 상자를 간단히 선택 해제하면 됩니다.

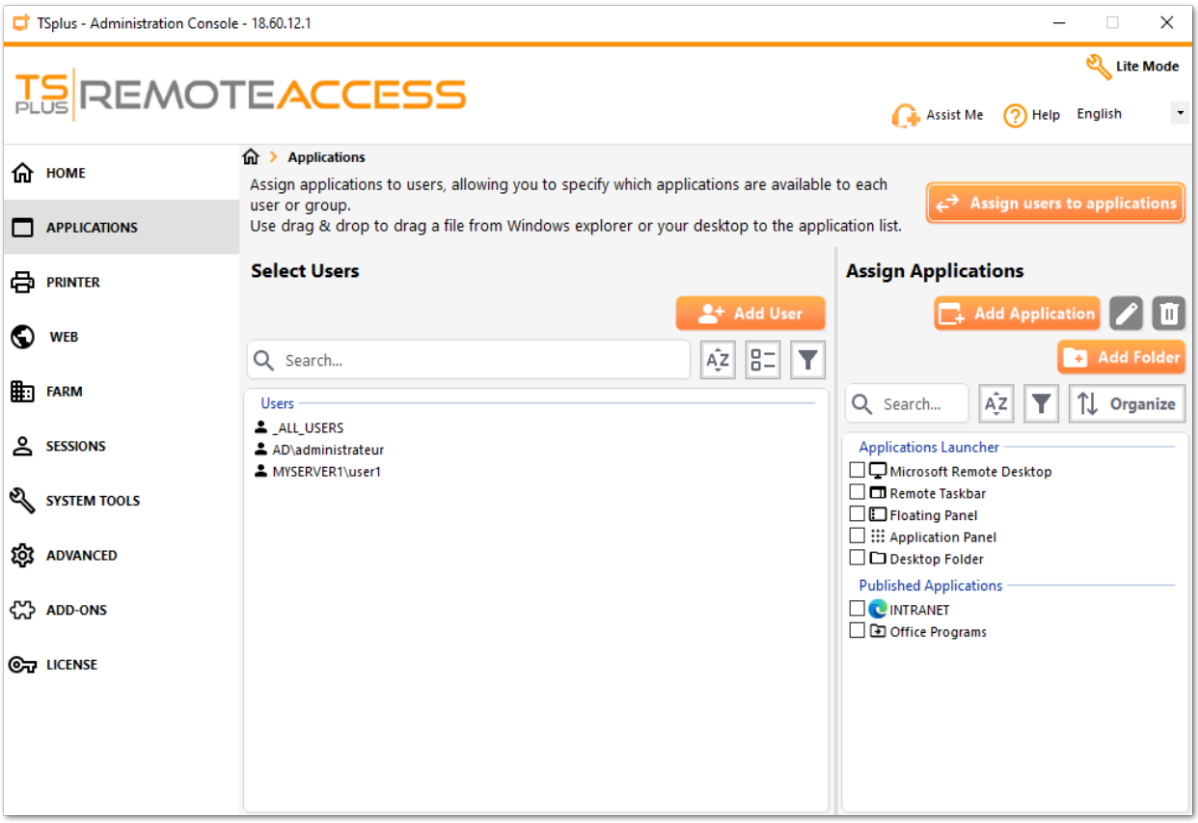
이 작업은 다중 선택을 지원합니다.
이것은 여러 응용 프로그램을 선택할 수 있으며, 응용 프로그램을 한 번에 하나씩 할당할 필요가 없음을 의미합니다.

사용자 또는 그룹에 애플리케이션 할당

사용자 또는 그룹을 선택하고 애플리케이션을 할당하려면 "사용자에게 애플리케이션 할당"을 클릭하면 됩니다.



이것은 왼쪽과 오른쪽 패널을 뒤집을 것입니다.



버튼을 클릭한 후, 사용자가 애플리케이션을 할당하기 위해:

1. 왼쪽 패널에서 애플리케이션에 할당할 사용자 또는 그룹을 선택합니다.
2. 오른쪽 패널에서 선택한 사용자 또는 그룹을 해당 애플리케이션에 할당하기 위해 애플리케이션 이름 옆의 상자를 확인합니다.

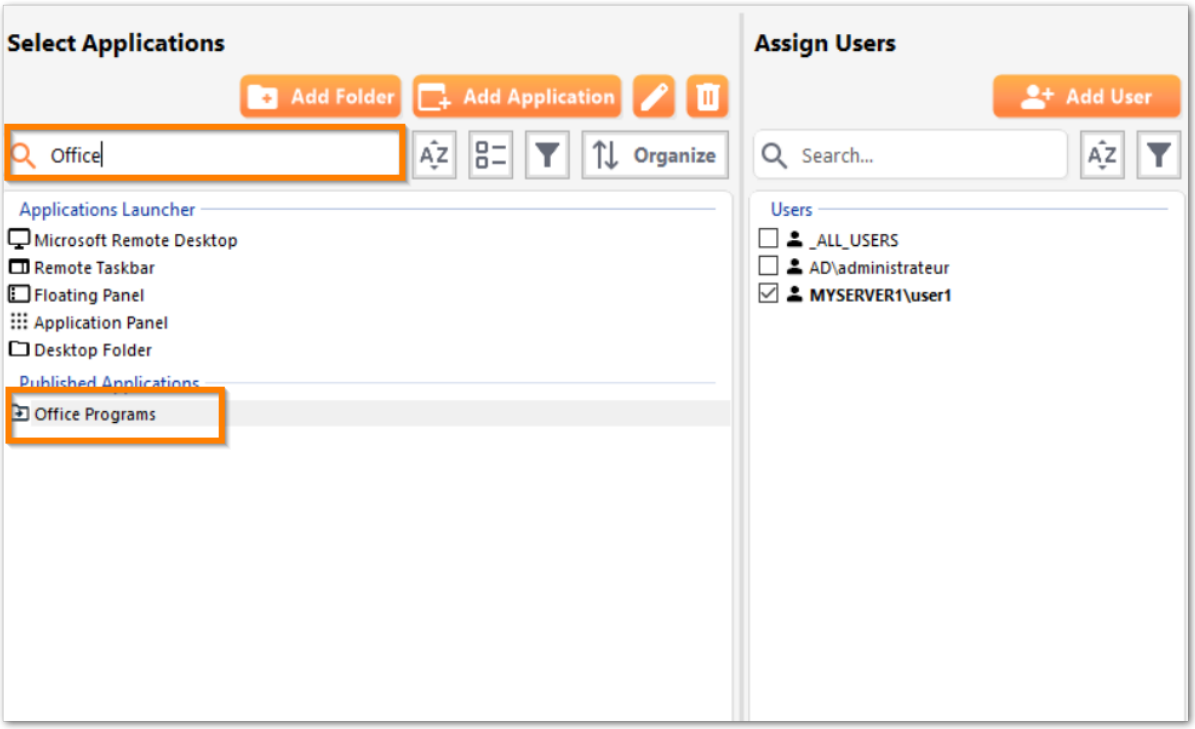
예: 사용자인 "benjamin"에게 메모장을 할당하려면 왼쪽에서 사용자 "benjamin"을 선택하고 오른쪽에서 애플리케이션 이름 "notepad" 옆의 상자를 체크하면 됩니다.

응용 프로그램의 할당을 해제하려면 응용 프로그램 이름 옆의 상자를 단순히 선택 해제하면 됩니다.

이 작업은 다중 선택을 지원합니다.
이것은 여러 사용자를 선택할 수 있으며, 사용자를 한 번에 하나씩 할당할 필요가 없음을 의미합니다.

검색 및 필터

사용자 할당 관리를 용이하게 하기 위해 검색창과 필터링 버튼이 제공되어 사용자만 또는 그룹만 표시할 수 있습니다.



필터 버튼을 사용하여 할당된/할당되지 않은 애플리케이션(또는 보기 전환 시 할당된/할당되지 않은 사용자)만 표시되도록 할 수 있습니다.
이것은 애플리케이션이 할당된 많은 사용자나 단순히 많은 게시된 애플리케이션이 있는 경우 할당을 관리하는 데 도움이 될 것입니다.

내장 웹 서버 관리

귀하의 원격 데스크톱 서버는 사용 가능하고 접근이 용이하며 안전해야 합니다. 그렇기 때문에 TSplus는 상태 및 작업을 쉽게 관리할 수 있도록 도와주는 내장 웹 서버를 활용합니다.

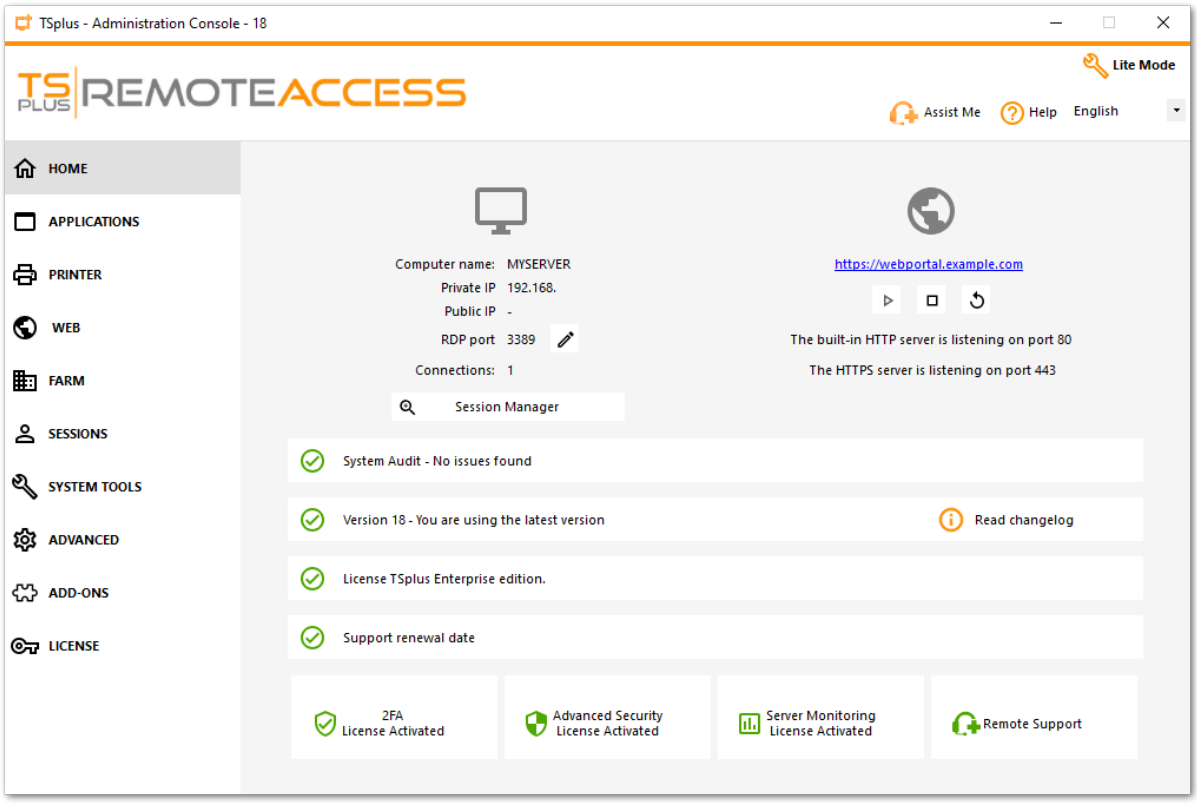
관리자 도구에서 관리 콘솔을 사용할 수 있습니다. 이 관리 콘솔을 통해 Terminal Service Plus에 내장된 웹 서버의 상태를 보고 구성할 수 있습니다.

당신이 TSplus 설치 웹 서버는 기본적으로 포트 80과 443에서 수신 대기하고 있습니다. 정의된 포트가 사용 가능하고 서버에 Java가 설치되어 있는지 확인하십시오.

보세요 비디오 웹 기능에 대해.

웹 서버 구성 요소 상태

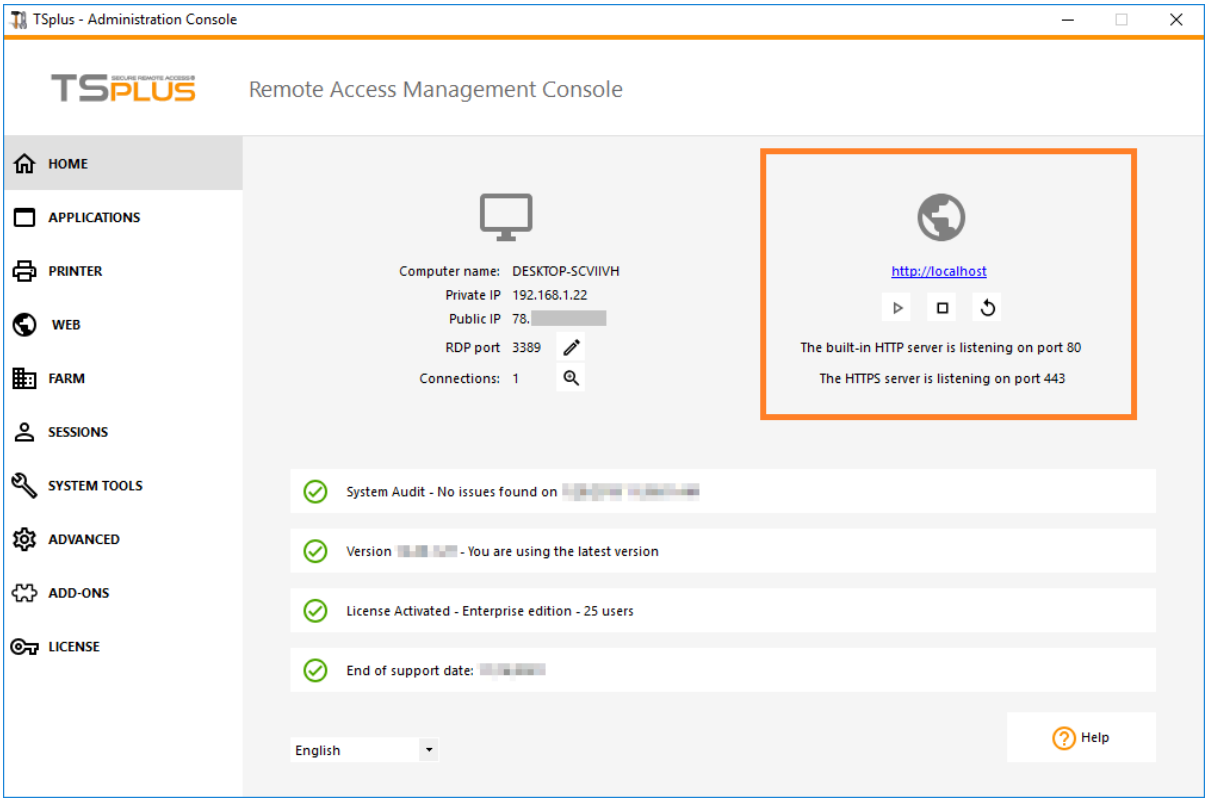
웹 서버 주요 구성 요소의 상태가 AdminTool 홈 대시보드에 표시됩니다.



포트 고려사항 (로컬 머신 및 방화벽 / 라우터)

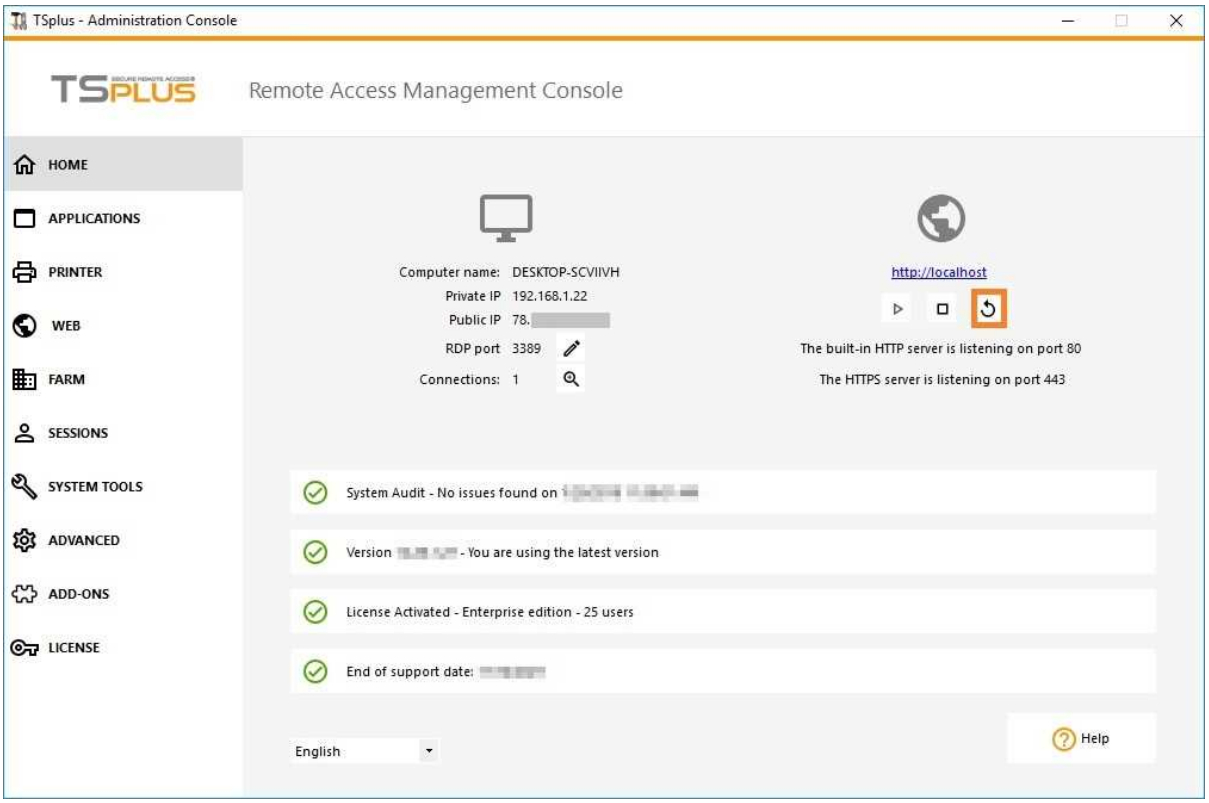
Terminal Service Plus는 포트 80 또는 포트 443 중 하나만 열려 있으면 됩니다.

포트 3389는 닫힌 상태로 유지할 수 있습니다.

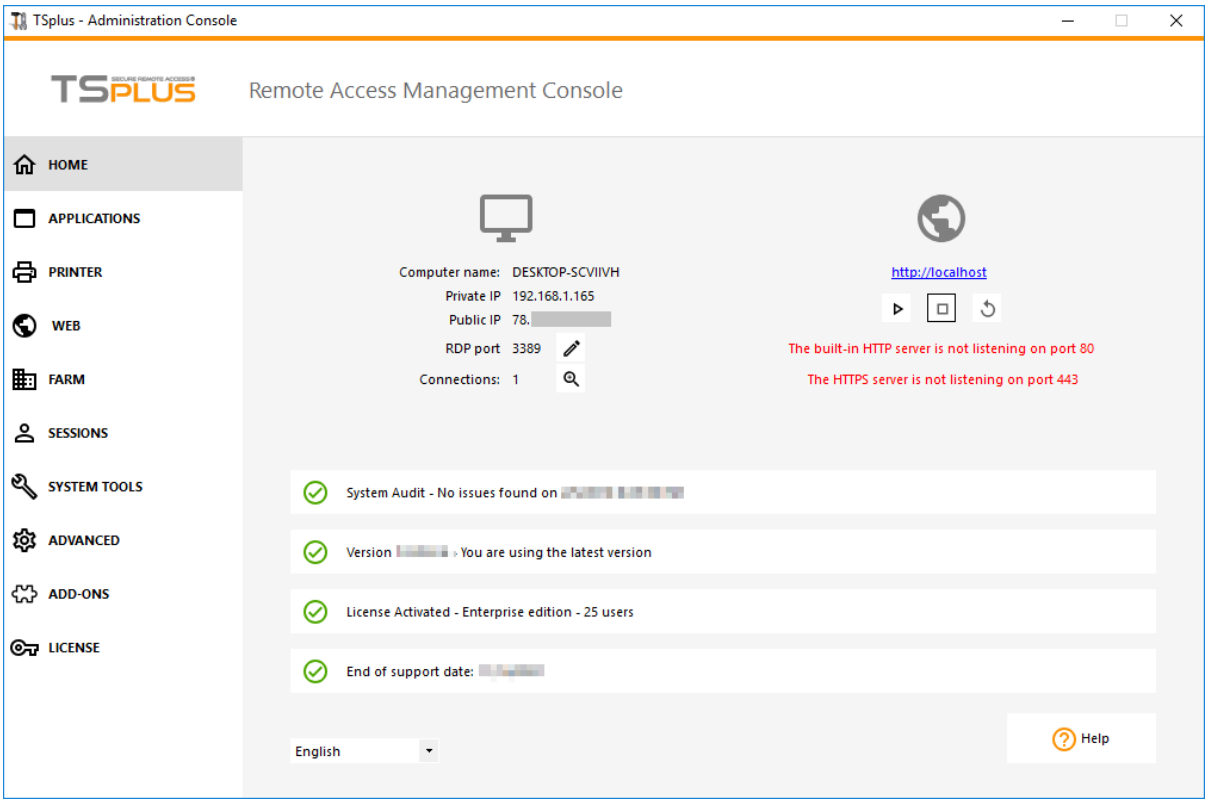


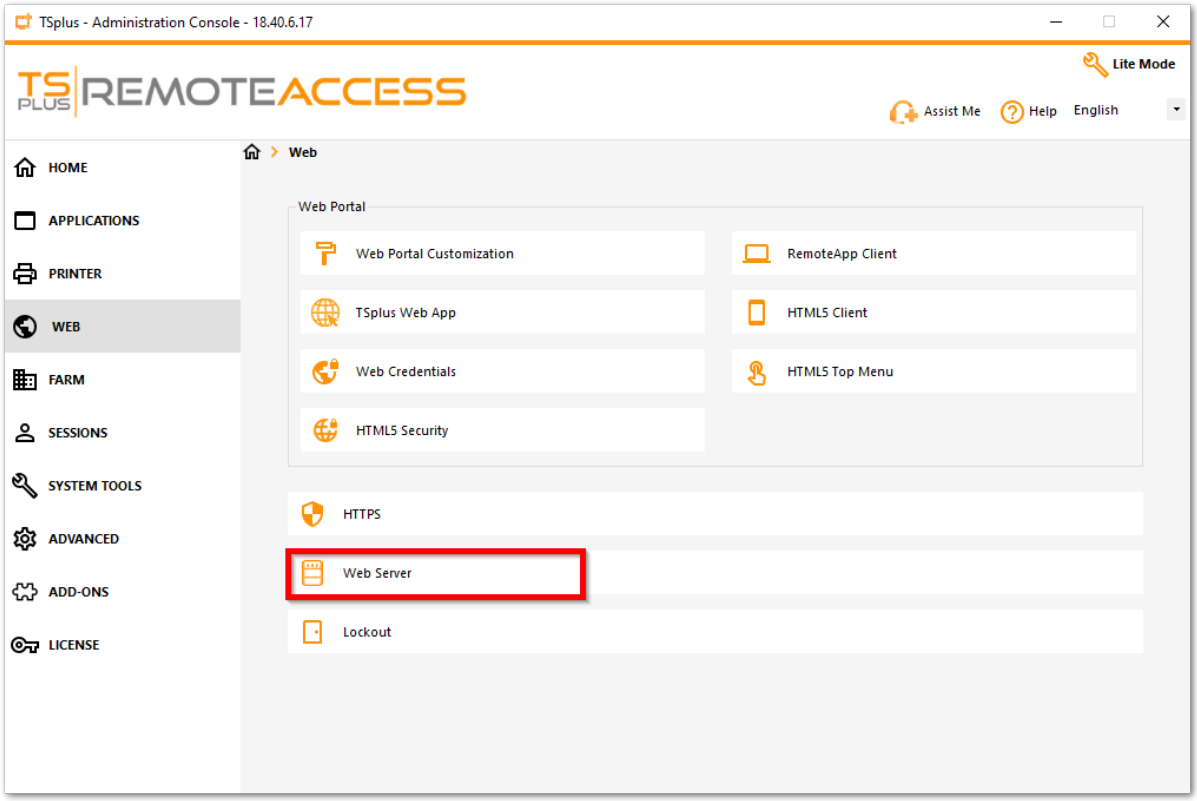
웹 서버 서비스를 다시 시작 / 중지

서비스가 실행되고 있지 않으면, 오른쪽에 있는 화살표로 표시된 “웹 서버 재시작 버튼”을 클릭하여 웹 서버를 재시작해야 할 수 있습니다. 웹 서버가 재시작되면 서비스가 다시 실행되어야 합니다.



"웹 서버 중지" 버튼을 클릭하면 중앙에 위치한 웹 서버가 중지됩니다. HTTP 및 HTTPS 서버 상태가 빨간색으로 표시되어 HTTP / HTTPS 서비스가 중지되었음을 나타냅니다.





설치 중 또는 언제든지 웹 - 웹 서버 탭을 클릭하여 포트를 변경할 수 있습니다. 이 탭에서 다른 HTTP 웹 서버를 사용하도록 선택하고, 웹 서버 루트 경로 및 HTTP/HTTPS 포트 번호를 수정할 수 있습니다. 이러한 포트가 변경하기 전에 사용 가능해야 합니다: 충돌이 발생하면 TSplus 웹 서버가 작동하지 않습니다. 여기 서버의 애플리케이션에서 사용될 수 있는 TCP 포트의 비포괄적인 목록입니다. 이러한 수정이 완료되면 저장을 클릭하고 AdminTool이 재시작됩니다.

###http 전용 비활성화 또는 https에서 http 사용

보세요 이 문서 이 주제에 대한 자세한 정보는.

자세한 정보는 **서버 사용자 정의** 그리고 **환경 설정** 이 페이지를 참조하세요:

웹 포털 사용자 정의 , 웹 애플리케이션 포털 , 웹 자격 증명 .

보안 강화를 위한 암호 스위트 선택

개요

TLS/SSL, HTTPS 뒤에 있는 보안,은 연결을 보호하고 암호화하며 인증하기 위해 여러 가지 다른 알고리즘을 사용할 수 있습니다.

서버와 클라이언트 간의 합의에 따라 사용할 알고리즘의 선택은 각 측에서 사용 가능한 알고리즘에 따라 결정됩니다.

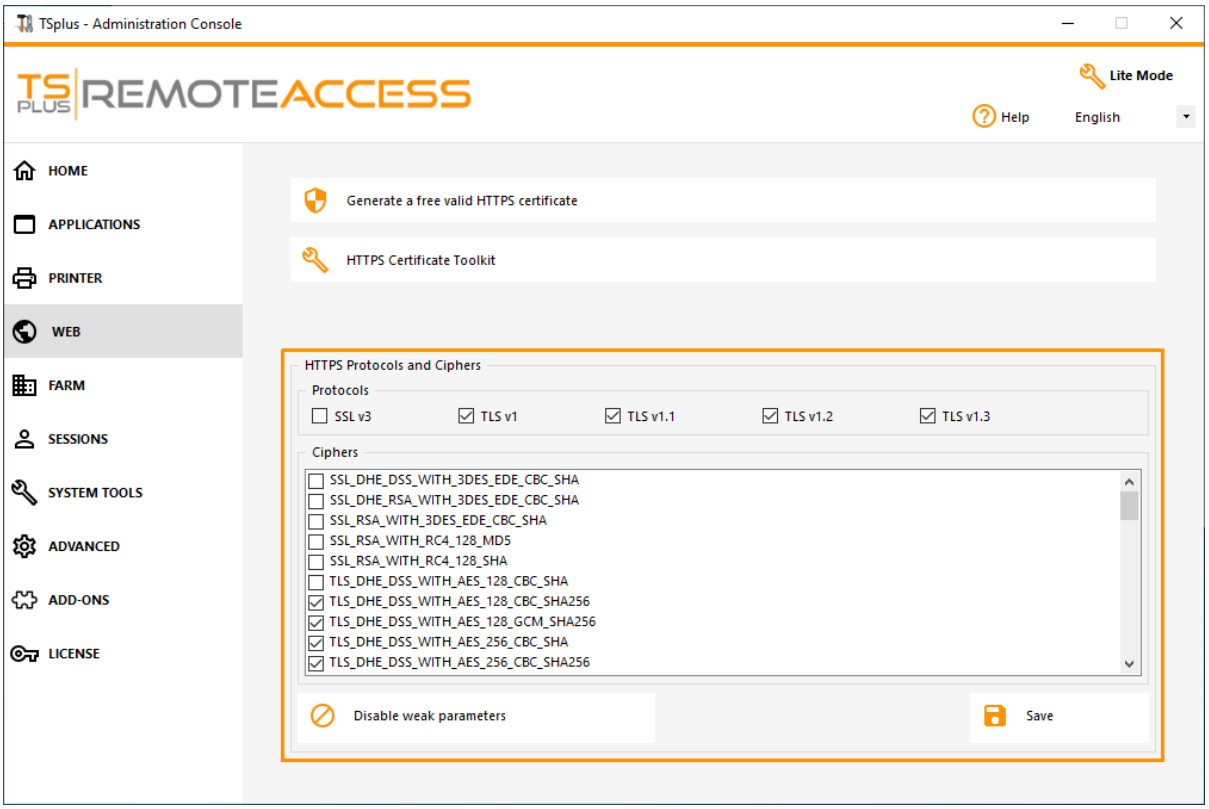
암호 모음은 인증, 암호화, 메시지 인증 및 키 교환 알고리즘의 명명된 조합입니다.

Terminal Service Plus 서버는 다양한 암호화 스위트를 처리할 수 있습니다. 그 중 일부는 다른 것보다 더 안전하지만, 일부 오래된/레거시 브라우저는 연결을 위해 상대적으로 약한 알고리즘을 요구할 수 있습니다.

이것이 Terminal Service Plus가 사용자가 활성화할 암호 모음을 선택할 수 있도록 하는 이유입니다. 물론, Terminal Service Plus는 가장 약한 알고리즘을 비활성화하는 쉬운 설정도 제공하여 연결 보안을 강화합니다.

HTTPS 프로토콜 및 암호 선택

Terminal Service Plus 암호 선택을 보려면 Terminal Service Plus AdminTool을 열고 “Web - HTTPS” 탭을 클릭하세요. 그곳에서 HTTPS 프로토콜과 암호를 볼 수 있습니다.



암호 모음 활성화/비활성화

암호 모음을 쉽게 활성화하려면 해당 체크박스를 선택하고 비활성화하려면 체크를 해제하면 됩니다.

선택이 완료되면 "저장"을 클릭하세요.

이것은 귀하의 선택을 저장하고 Terminal Service Plus 내장 웹 서버에서 새 구성을 다시 로드합니다. 귀하의 새로운 암호 모음 선택은 서버에 대한 모든 새로운 연결에 즉시 적용됩니다.

권장 암호 스위트 선택

대부분의 관리자에게는 “약한 매개변수 비활성화” 버튼을 클릭한 다음 “저장” 버튼을 클릭하여 권장 암호 모음 선택을 사용하는 것을 권장합니다.

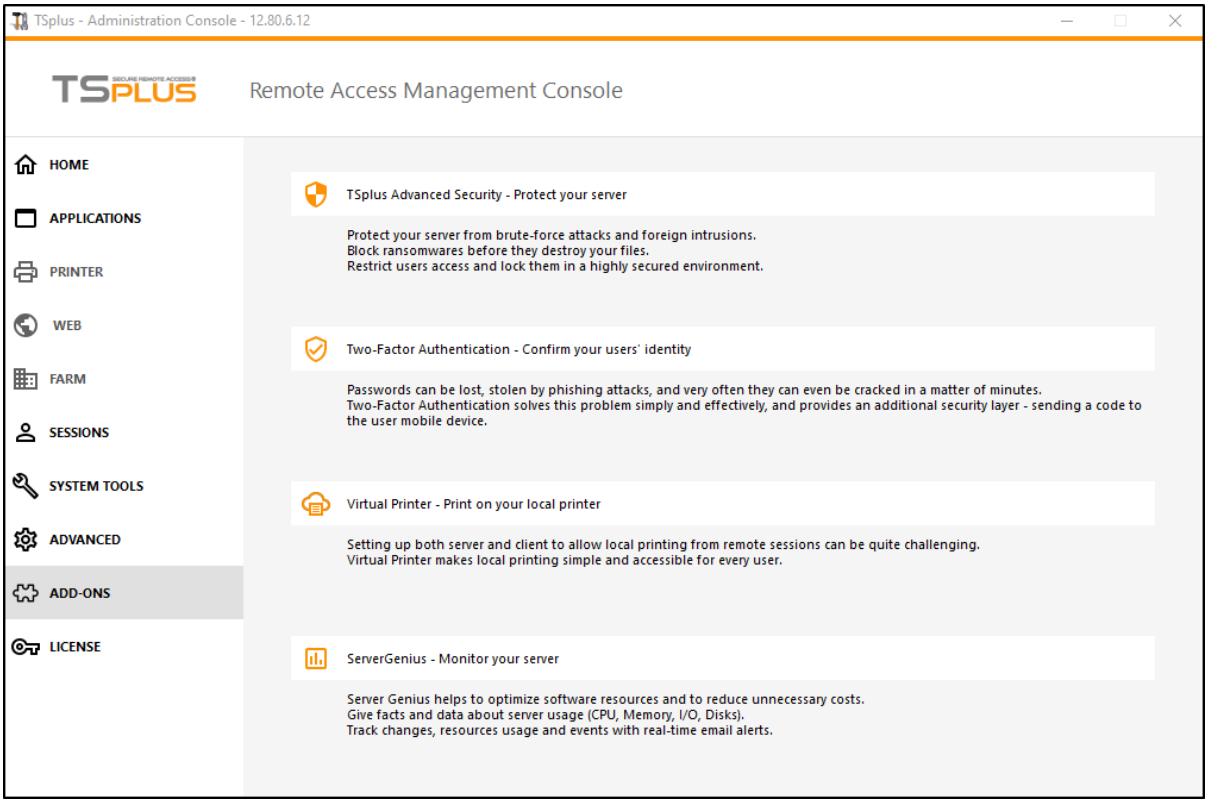
이 작업은 현재 약한 것으로 알려진 모든 암호 모음을 비활성화합니다.

확인할 수 있습니다. SSL Labs 온라인 테스트 도구 약한 암호 스위트 없이 최대 등급 A를 받을 수 있어야 합니다!

클릭하여 도움말 - 관리 도구 - 추가 기능

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

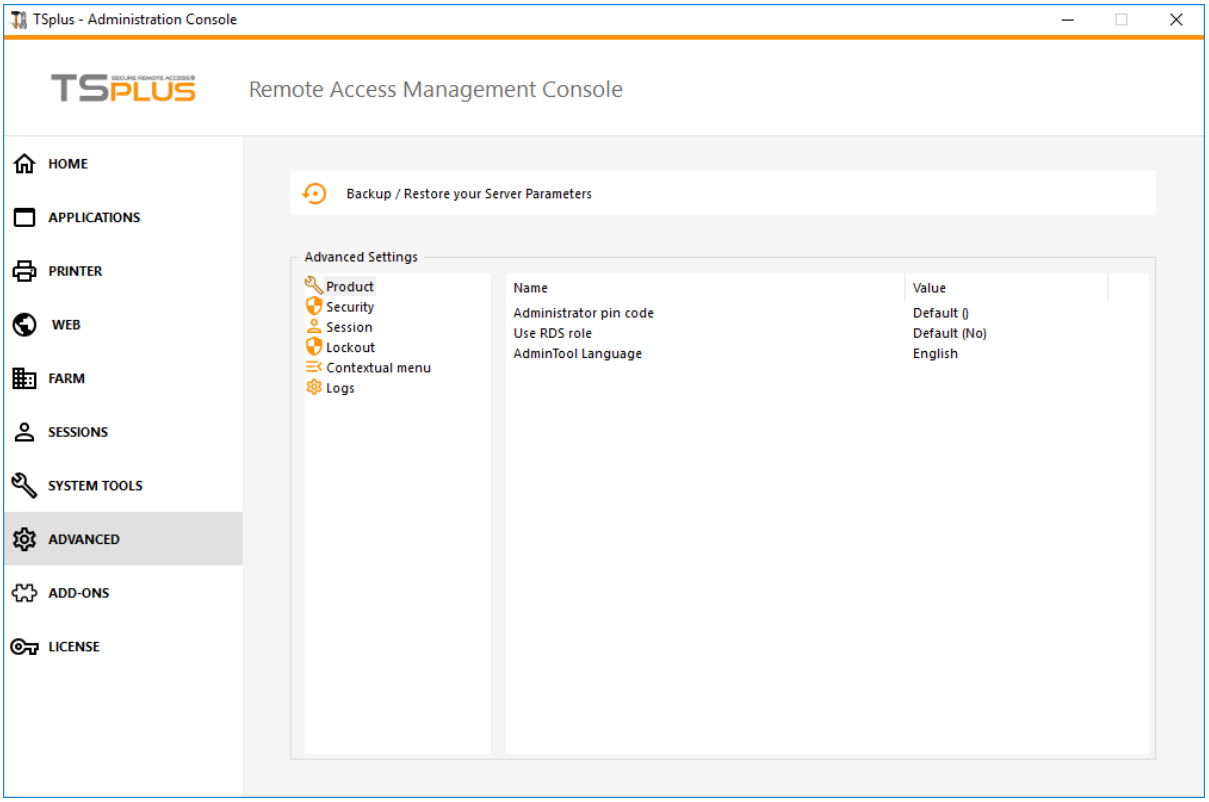
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움 요청 - 관리 도구 - 고급

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

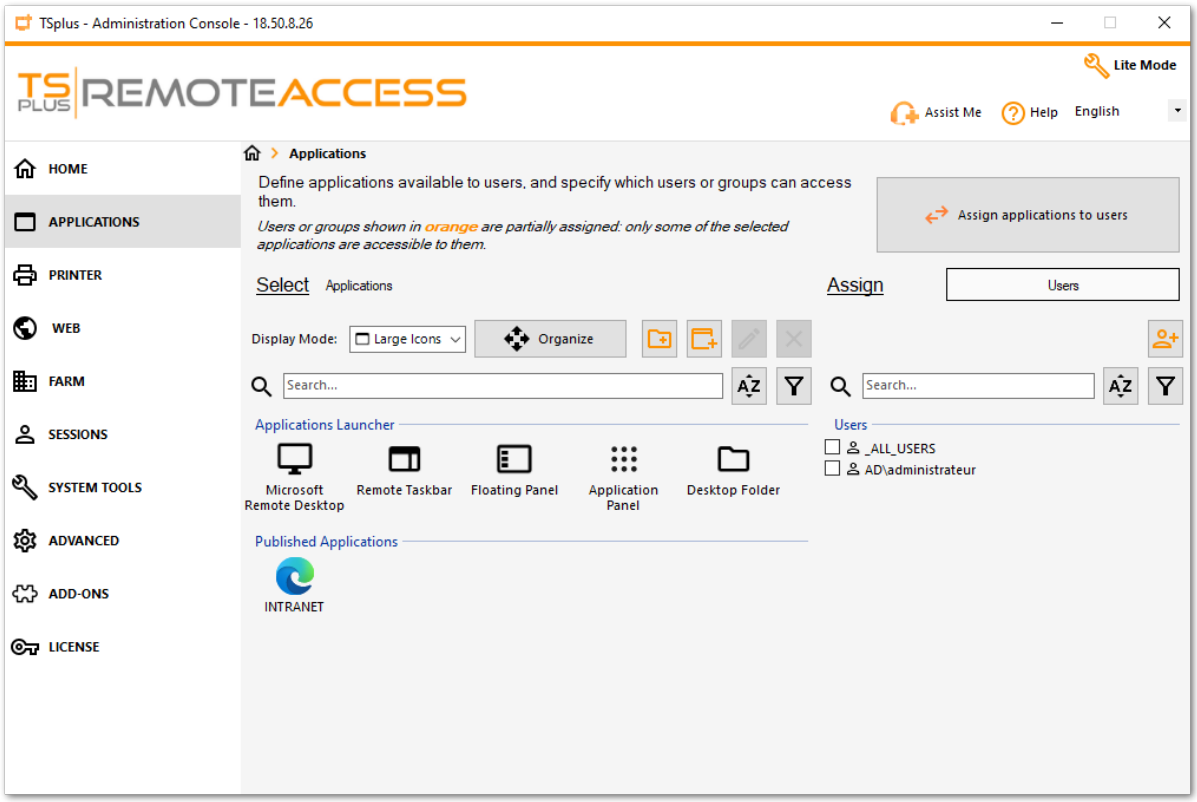
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움말 - 관리 도구 - 애플리케이션

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

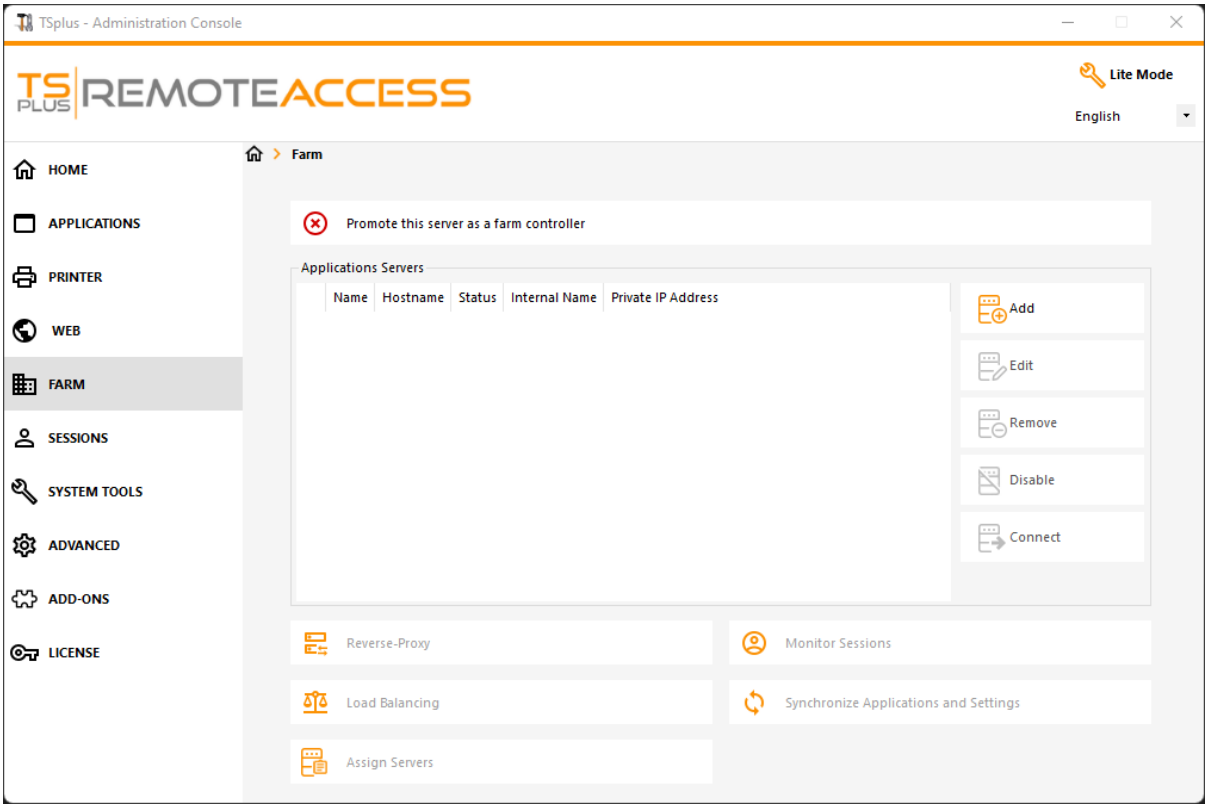
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움 요청 - 관리 도구 - 농장

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

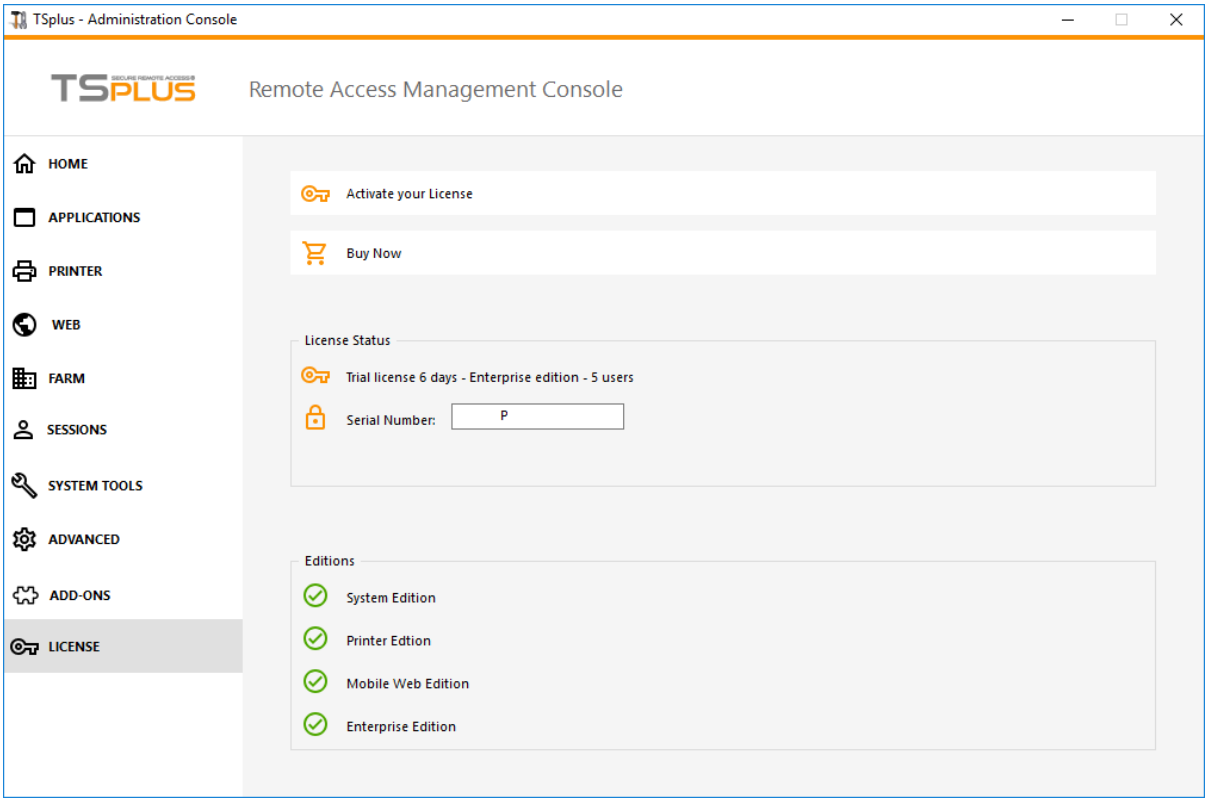
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움 요청 - 관리 도구 - 라이센스

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

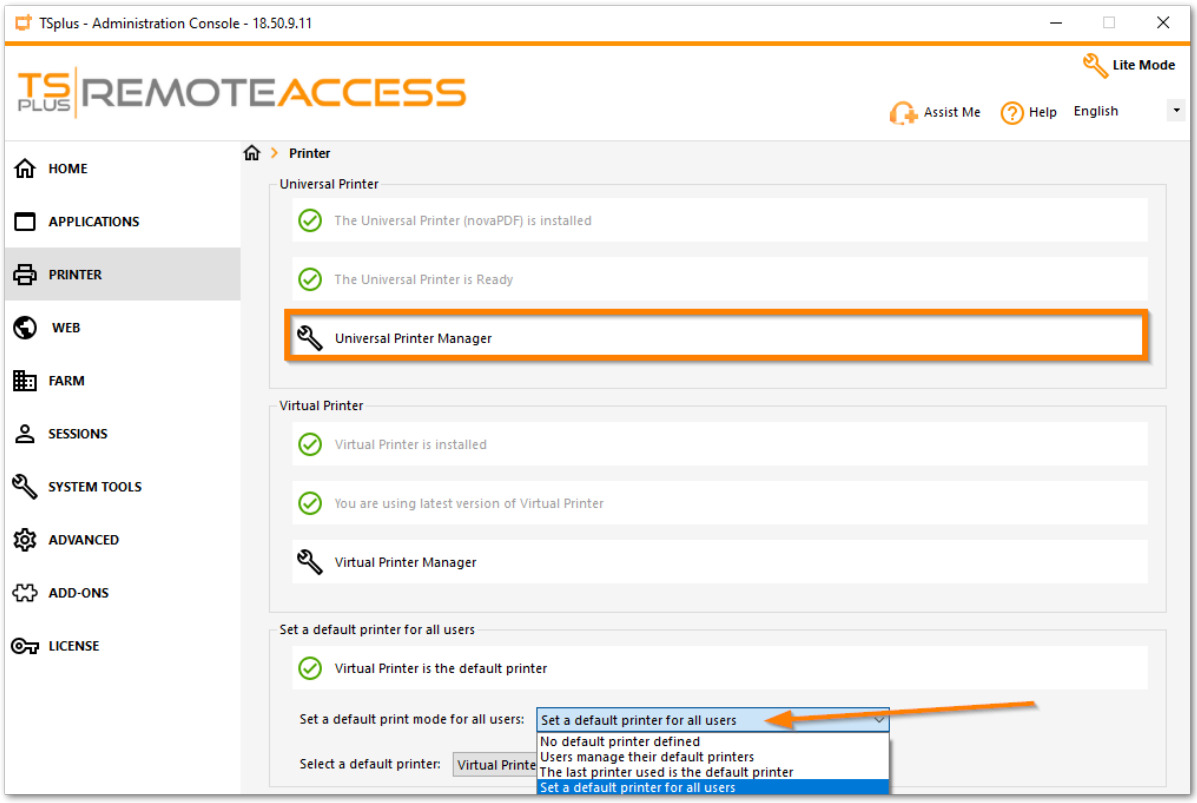
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움말 - 관리 도구 - 프린터

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움말 - 관리 도구 - 보안

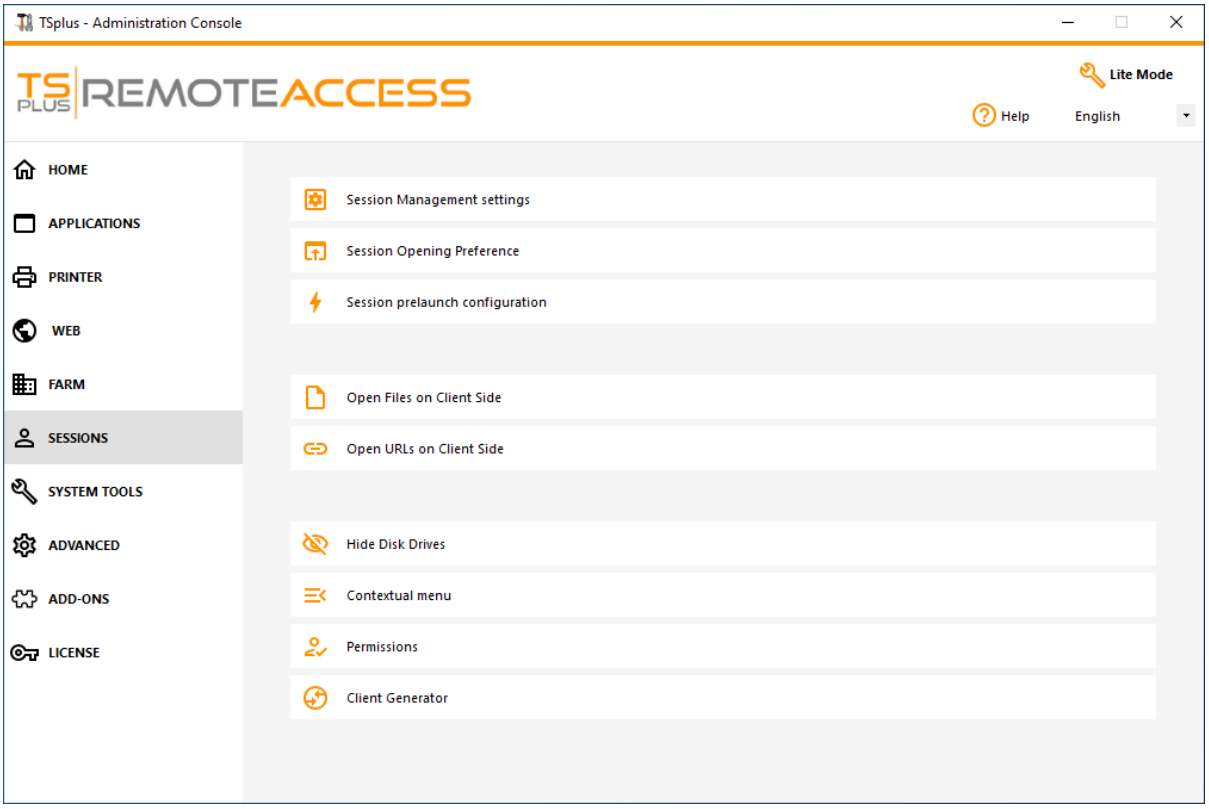
터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!

클릭하여 도움말 - 관리 도구 - 세션

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

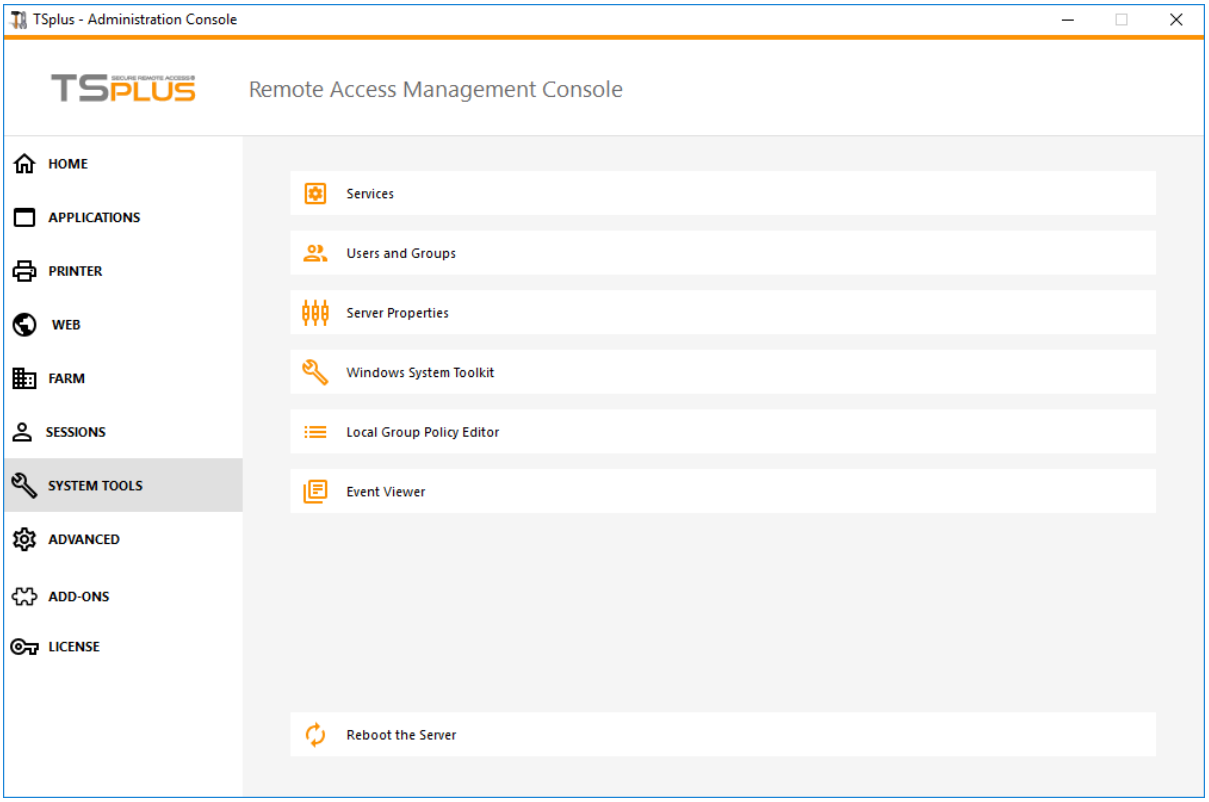
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움 요청 - 관리 도구 - 시스템

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

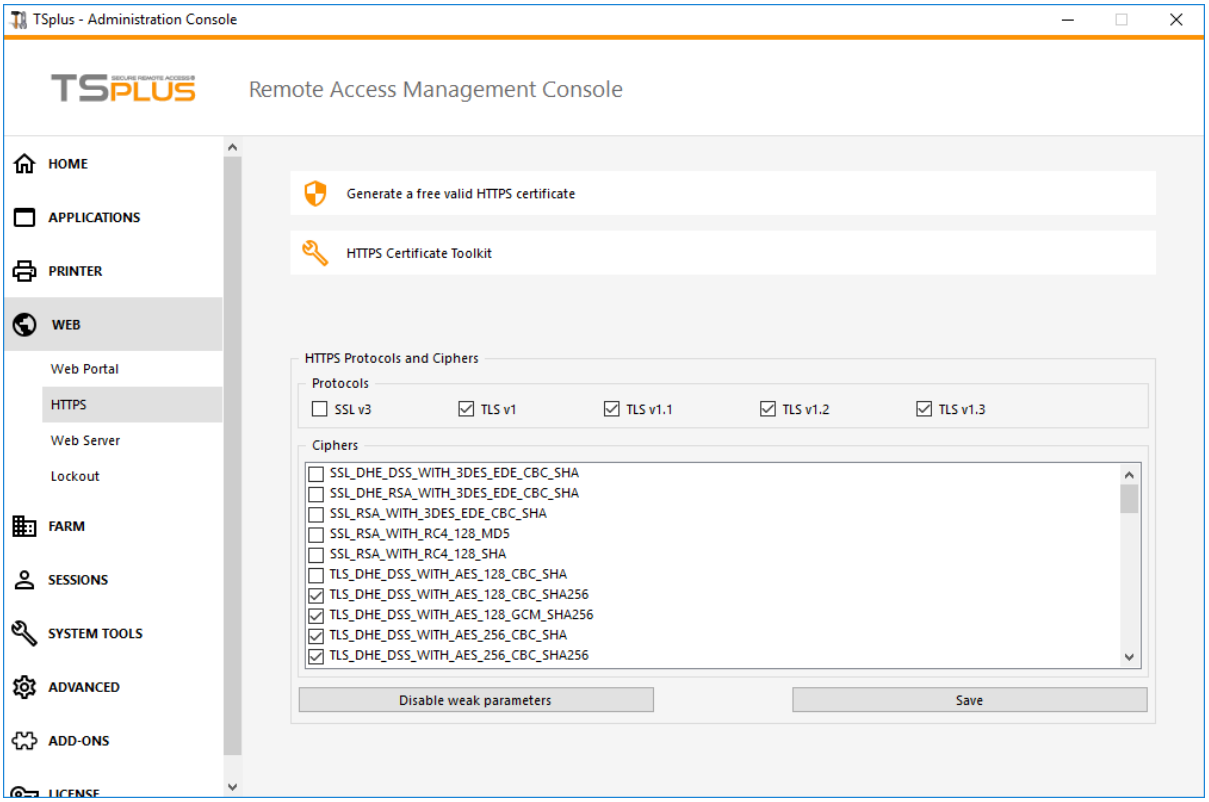
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움 요청 - 관리 도구 - 웹

터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

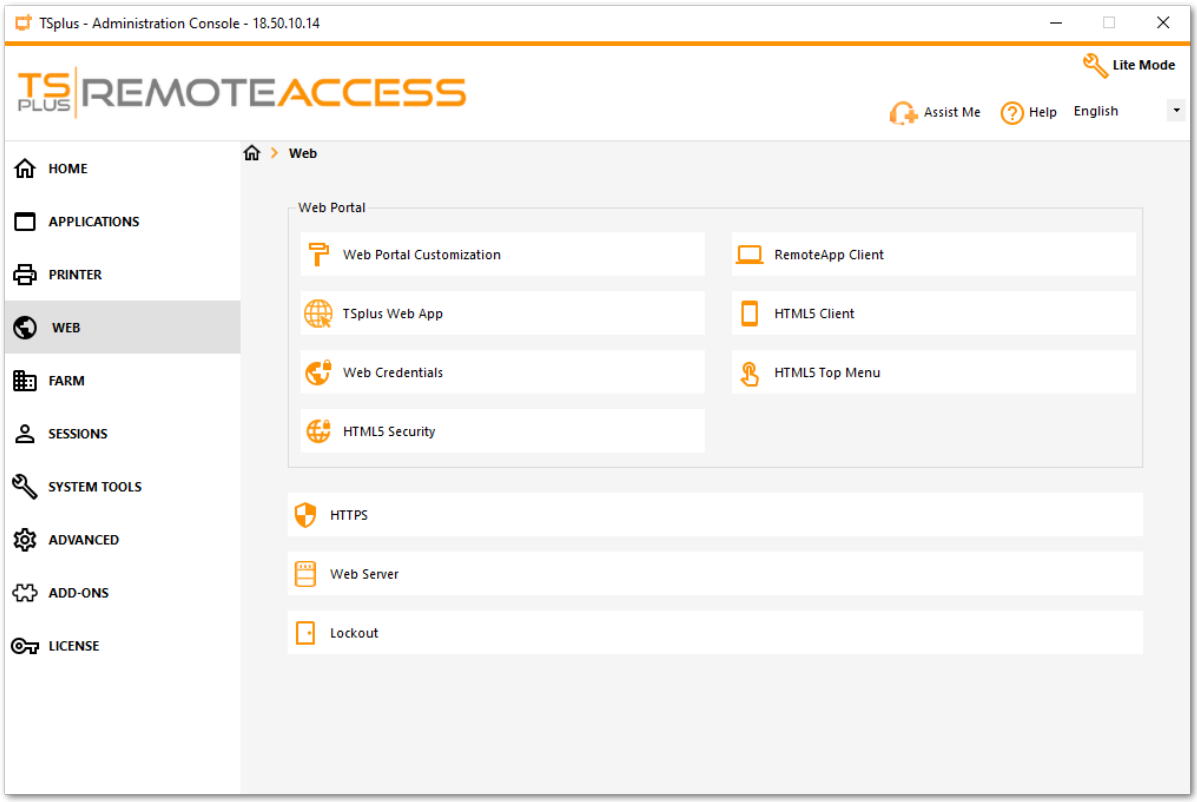
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!



클릭하여 도움 요청 - 관리 도구 - 웹

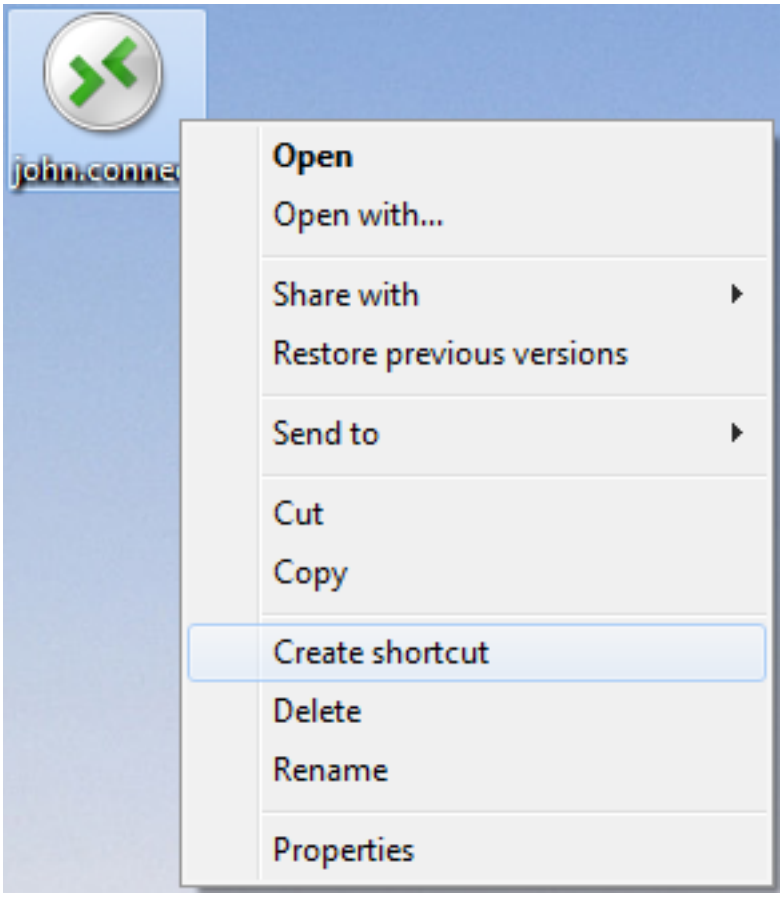
터미널 서비스 플러스 관리 도구의 기능에 대해 빠르게 도움을 받고 싶으신가요?

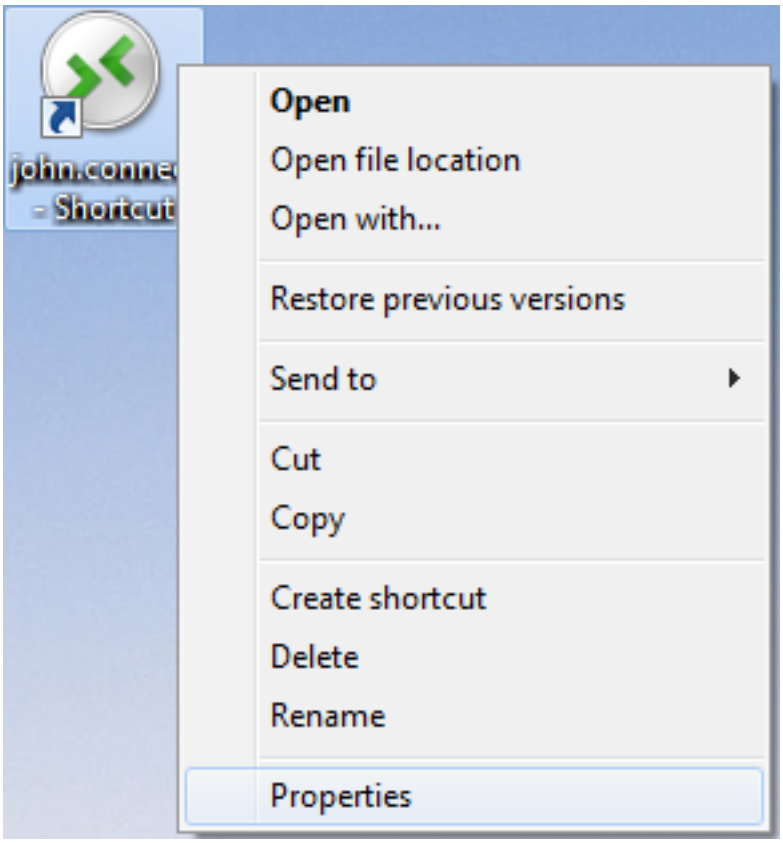
그냥 **타일이나 탭을 클릭하세요** 일치하는 도움말로 가기!

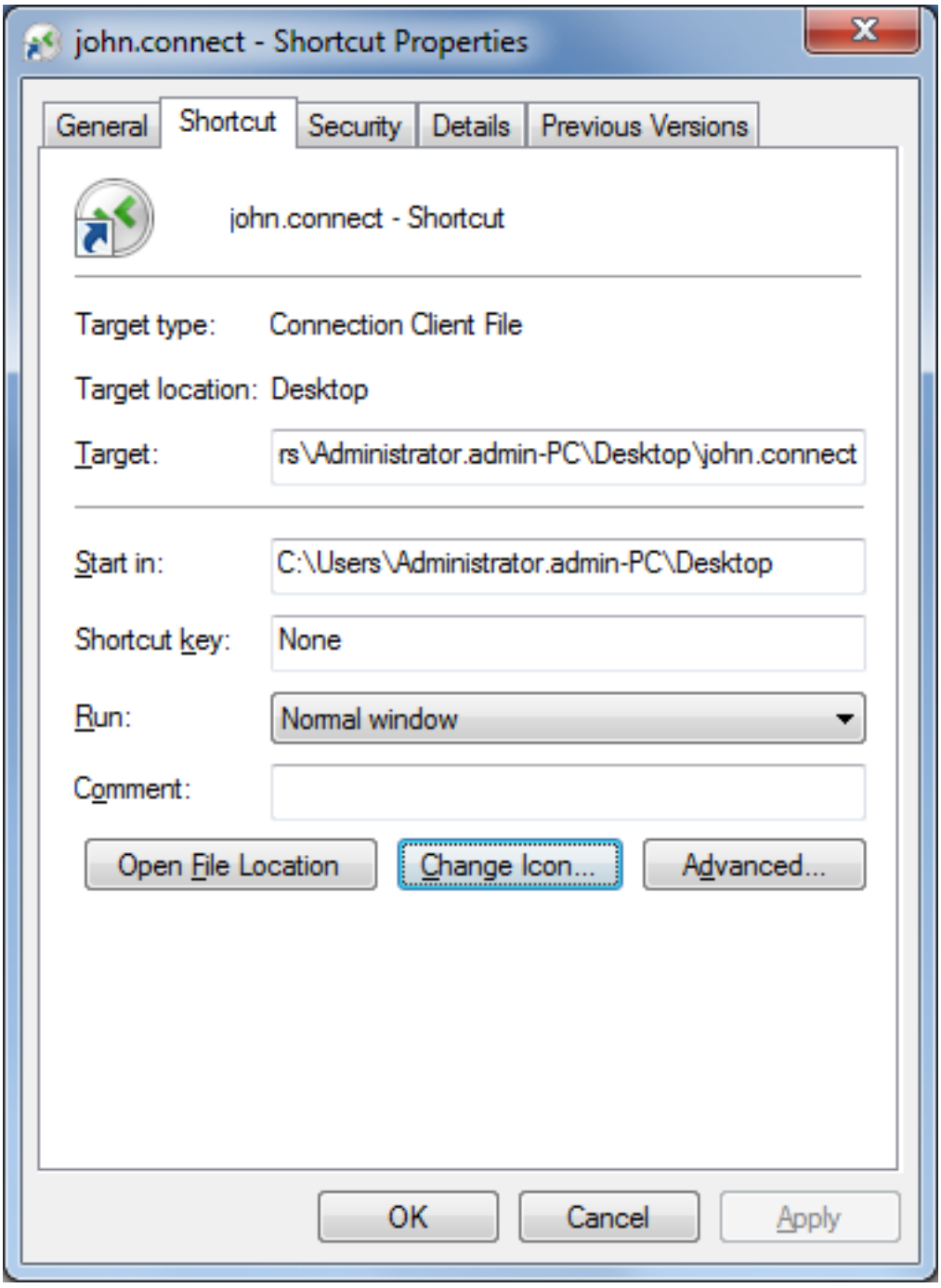


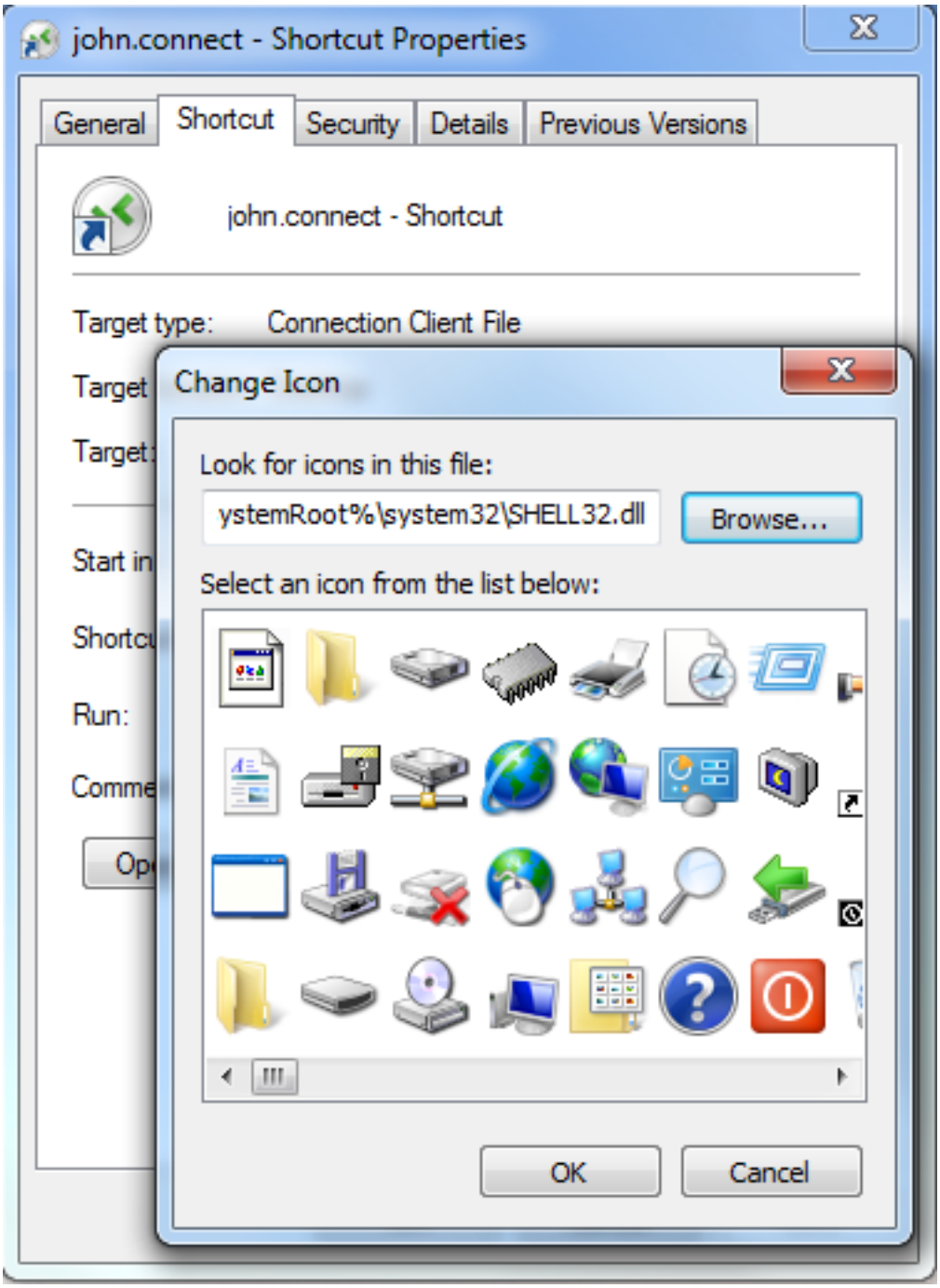
TSplus 클라이언트 아이콘 수정 방법

클라이언트의 아이콘을 변경하려면 클라이언트의 바로 가기를 만들고 바로 가기 속성으로 이동하면 됩니다.




john.connec
- Shortcut
Open
Open file location
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties


john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type: Connection Client File
Target location: Desktop
Target: rs\Administrator.admin-PC\Desktop\john.connect
Start in: C:\Users\Administrator.admin-PC\Desktop
Shortcut key: None
Run: Normal window
Comment:
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply

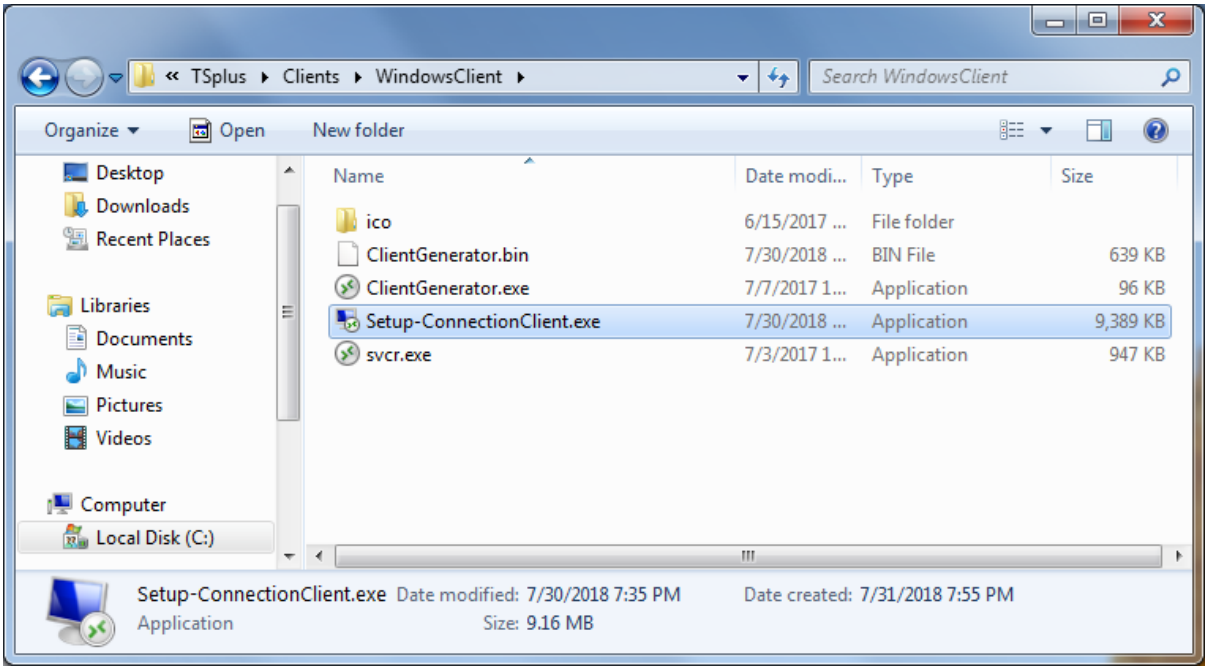

john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type:
Connection Client File
Target
Target:
Start in
Shortcu
Run:
Comme
Op
Change Icon
Look for icons in this file:
ystemRoot%\system32\SHELL32.dll
Browse...
Select an icon from the list below:
OK
Cancel

TSplus 클라이언트 설정 프로그램

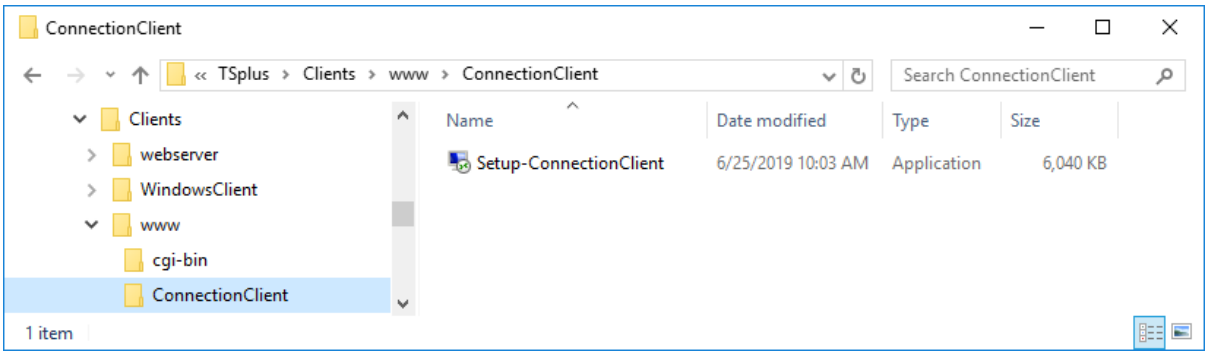
설치

클라이언트 측에서, **각 사용자는 필수 조건으로 "Setup-ConnectionClient.exe"라는 서명된 프로그램을 실행해야 합니다.** .

이 프로그램은 귀하의 서버, TSplus 프로그램 폴더에 있습니다: C:\Program Files (x86)\TSplus\Clients\WindowsClient:



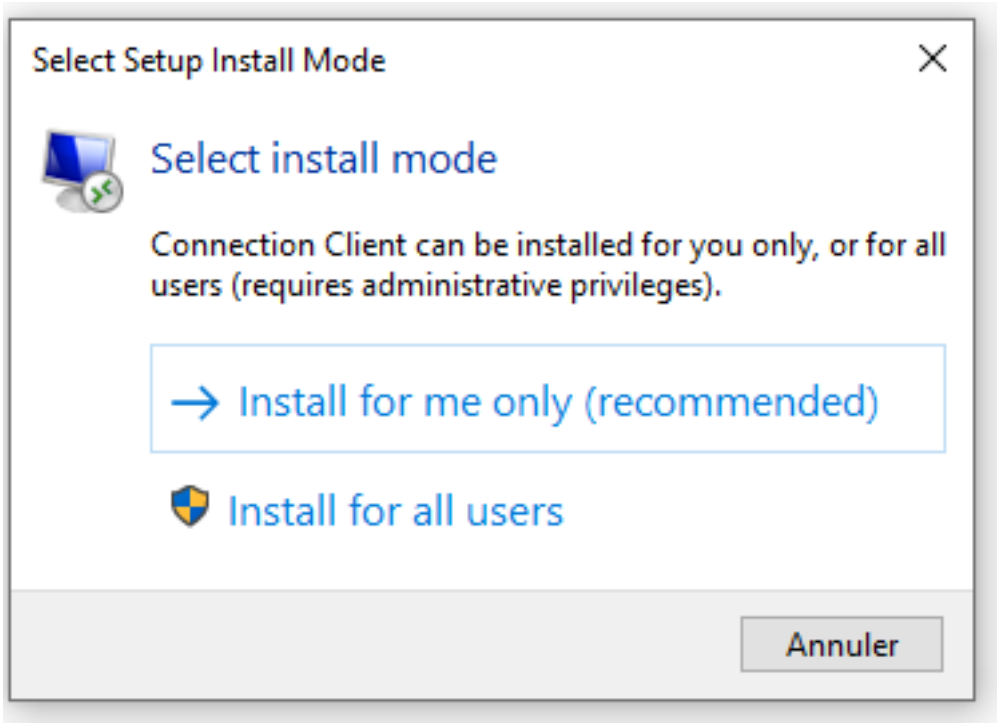
C:\Program Files (x86)\TSplus\Clients\www\ConnectionClient에 또한 제공되므로, 사용자는 웹 서버 주소에서 프로그램을 한 번만 실행하면 됩니다. http://xxxxxxxxxx/ConnectionClient/Setup-ConnectionClient.exe



또는 다운로드 중입니다 .

모든 사용자에게 설치

이제 모든 사용자를 위한 연결 클라이언트를 설치할 수 있습니다. 이는 설치가 완료되면 컴퓨터의 모든 사용자가 이를 활용할 수 있으며, 웹 포털에서 원격 앱 모드로 연결하거나 생성된 .connect 클라이언트 파일을 사용하여 연결할 수 있음을 의미합니다.



이 팝업이 나타나려면 이미 Connection Client가 설치되어 있지 않아야 합니다. 또한 명령줄을 사용하여 설치하는 동안 /ALLUSERS 또는 /CURRENTUSER 인수를 사용하여 모든 사용자 또는 현재 사용자에 대해 설치할 모드를 지정할 수 있습니다.

노트 TSplus 12.40부터 클라이언트 설정 프로그램과 원격 앱 클라이언트 설정 하나의 단일 설정으로 배포할 수 있도록 통합되었으므로, Connection Client Setup을 다운로드하면 RemoteApp Client를 별도로 다운로드할 필요가 없습니다.

sysprep을 사용한 서버 복제

요구 사항

클론된 가상 머신을 사용할 때, 고유한 TSplus Remote Access 설치를 보장하고 라이센스 문제를 피하기 위해 컴퓨터 이름과 디스크 볼륨 ID를 수정하는 것이 중요합니다.

컴퓨터 이름 고려사항

컴퓨터 이름은 이미지 자체의 Windows 레지스트리에 저장됩니다. 이미지를 적용하기 전에 수정하면 Windows 부팅 시 Sysprep에 의해 덮어씌워집니다. 그러나 이름을 미리 정의할 수 있습니다. Unattended.xml 답변 파일. 보기 Microsoft 문서 자세한 내용은.

컴퓨터 이름을 설정하려면 다음 섹션을 내부에 추가하십시오. 마이크로소프트-윈도우-셸-설정 :

```
    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
        <ComputerName>%COMPUTERNAME%ComputerName>
    component>
```

볼륨 ID 고려사항

볼륨 ID는 디스크 파티션과 연결되어 있으며, OS 이미지와는 관련이 없습니다. 이미지를 적용하기 전에 변경할 수 있으며, 변경 사항은 유지됩니다. 사용하십시오. volumeid.exe Sysinternals에서 제공됨 Microsoft Sysinternals 윈도우가 부팅되기 전에.

배포 단계

새 가상 머신을 sysprepped 이미지에서 배포할 때, Windows는 첫 부팅 시 Out-Of-Box Experience (OOBE)에 들어가 구성 설정을 요청합니다.

배포를 위한 권장 단계:

1. **WinPE로 부팅** – 시스템을 Windows로 부팅하지 않고 준비합니다.
2. **볼륨 ID 설정** – 이미지를 적용하기 전에 변경하여 지속되도록 하세요.
3. **sysprepped 이미지를 배포하십시오** – DISM을 사용하여 이미지를 적용합니다. C: .
4. **컴퓨터 이름을 오프라인으로 설정** – 마운트된 이미지 내에서 레지스트리를 편집합니다.
5. **복사한 Unattended.xml 파일** – OOBE 구성을 자동화합니다. 이 파일은 배포 전에 스크립트를 사용하여 동적으로 수정할 수 있습니다.
6. **첫 부팅 스크립트 생성** – 최종 구성을 단 한 번의 재부팅으로 완료하십시오.
7. **Windows로 재부팅** – Windows는 지정된 구성을 사용하여 최종화됩니다.
8. **원격 액세스 라이센스 재설정** – 다음 명령을 실행하십시오:

터미널 창

AdminTool.exe /license /reset

이것은 라이센스를 재설정하고 새로운 라이센스를 적용합니다.

배포 스크립트

아래에 관련된 WinPE 배포 스크립트를 찾으십시오.

터미널 창

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"    # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive

<# 3. Load Registry Offline to Set Computer Name #>
Write-Host "Modifying Registry to Set Computer Name..."
reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
reg unload HKLM\TempSys

<# 4. Ensure Unattended Setup is Used #>
Write-Host "Copying Unattended File..."
Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

<# 5. Set the First Boot Script for Final Configurations #>
Write-Host "Creating First Boot Script..."
$FirstBootScript = @"
Write-Host "Finalizing Configuration..."
Rename-Computer -NewName "$ComputerName" -Force
Restart-Computer -Force
"@
Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

Write-Host "Deployment Complete! Rebooting into Windows..."
```

```
Write-Host "================================================"
Write-Host "  Computer Name: $ComputerName"
Write-Host "  Volume ID: $VolumeID"
Write-Host "  Image Applied to: $ApplyDrive"
Write-Host "================================================"

<# Reboot into Windows #>
wpeutil reboot
```

라이센스 활성화

배포 후 라이센스를 활성화하면 가상 머신에 대한 새로운 컴퓨터 ID가 생성됩니다. 이 컴퓨터 ID는 머신이 평가판 또는 라이센스 활성화를 요청할 때 라이센스 포털에 의해 생성됩니다. 클론된 가상 머신의 경우 라이센스 활성화가 필수입니다. 활성화 키 또는 볼륨 라이센스 키를 사용하십시오. **오프라인 설정은 허용되지 않습니다** 보안 문제로 인해. 자세한 활성화 단계는 다음을 참조하십시오. TSplus 명령어 목록 .

결론

이 가이드는 TSplus Remote Access로 클론된 가상 머신을 배포할 때의 주요 고려 사항을 설명합니다. 시스템을 올바르게 구성하고 라이센스를 부여하기 위한 필수 단계를 제공하며, 귀하의 필요와 요구 사항에 맞게 조정되어야 합니다.

명령줄

우리는 소프트웨어의 유연성과 효율성을 향상시키기 위해 설계된 포괄적인 명령줄 도구 세트를 제공하게 되어 기쁩니다. 이러한 도구는 사용자가 다양한 기능을 스크립트하고 자동화할 수 있도록 하여 소프트웨어를 특정 요구 사항과 작업 흐름에 맞게 조정할 수 있게 합니다.

가능성을 탐색하고 명령줄 옵션으로 경험을 최적화하세요.

다음 명령줄을 관리자 권한으로 실행하면 됩니다. 참고로, AdminTool.exe와 TwoFactor.Admin.exe (2FA 추가 기능)는 여기 위치해야 합니다: **C:\Program Files (x86)\TSplus\UserDesktop\files**

백업 데이터 및 설정: /백업

구문:

AdminTool.exe /backup [선택적경로] [매개변수]

설명:

명령 /백업 TSplus 데이터 및 설정을 백업하는 데 사용됩니다.

기본적으로 백업은 아카이브 디렉토리(C:\Backupparam)에 생성됩니다.

매개변수:

- 선택적 경로 다른 디렉토리에 백업하기 위해 기본 디렉토리와는 다른 경로를 사용할 수 있습니다. 상대 경로와 절대 경로가 허용됩니다.
- /침묵 이 매개변수가 언급되면 백업이 조용히 수행됩니다.

예시:

AdminTool.exe /backup AdminTool.exe /backup “c:/TSplus/CustomBackupFolder” /silent

자세한 정보는 다음을 참조하십시오. TSplus - 백업 설정

데이터 및 설정 복원: 복원

구문:

AdminTool.exe /restore [백업 경로] [매개변수]

설명:

명령 복원 TSplus 데이터 및 설정을 복원하는 데 사용됩니다.

지정된 백업 디렉토리에는 /backup 명령으로 생성된 데이터 및 설정 폴더가 포함되어야 합니다.

매개변수:

- 백업 경로 백업 폴더가 위치한 경로입니다.
- /침묵 이 매개변수가 언급되면 복원이 조용히 수행됩니다.

예시:

AdminTool.exe /restore “C:/Backupparam” /silent AdminTool.exe /restore “C:/TSplus/CustomBackupFolder” /silent

자세한 정보는 다음을 참조하십시오. TSplus - 백업 설정

웹서버: /webstop , /webstart 그리고 웹 재시작

구문:

AdminTool.exe /webstop

AdminTool.exe /webstart

AdminTool.exe /webrestart

설명:

명령 /webstop 웹 서버를 중지하는 데 사용됩니다.

명령 /webstart 웹 서버를 시작하는 데 사용됩니다.

명령 웹 재시작 웹 서버를 재시작하는 데 사용됩니다.

매개변수:

없음

업데이트: /업데이트

구문:

AdminTool.exe /update [옵션]

설명:

명령 업데이트 TSplus Remote Access 및 잠재적으로 Advanced Security를 업데이트하는 데 사용됩니다.

매개변수:

- 옵션
  :
  - /추가 기능 이 옵션을 사용하면 새로운 버전이 있을 경우 Advanced Security도 업데이트됩니다.

예시:

AdminTool.exe /update /addons

Windows 호환성 업데이트 적용: 업데이트 커널

구문:

svcac.exe /updatekernel [/silent]

svcac.exe는 여기 위치해야 합니다: **C:\Program Files (x86)\TSplus**

설명:

명령 업데이트 커널 Windows 호환성 업데이트를 적용하는 데 사용됩니다.

이 자동 업데이트는 TSplus Remote Access가 새로운 Windows 업데이트와 호환되도록 보장하며, TSplus Remote Access의 최신 버전을 다운로드하고 재설치할 필요를 피합니다.

Windows 호환성 업데이트는 매일 발생할 수 있습니다. TSplus Remote Access는 강제 업데이트를 허용합니다. 이는 호환성이 깨진 것처럼 보일 때 유용하며, 정기 업데이트 일정 외부에서 최신 TSplus Remote Access 패치를 가져와야 할 때 필요합니다.

유효한 라이센스가 필요하여 호환성 업데이트를 가져올 수 있습니다. 체험 라이센스가 만료되었거나 라이센스가 유효하지 않은 경우 오류 메시지 상자가 표시됩니다. 문제가 예상치 못한 경우 이 오류 메시지의 스크린샷과 함께 지원 팀에 문의해 주시기 바랍니다.

매개변수:

- /침묵 이 매개변수를 제공하여 조용히 업데이트하십시오. 메시지 상자가 표시되지 않습니다.

유니버설 프린터 설치: /유니버설 프린터 설치

구문:

universalprintermanagement.exe /InstallUniversalPrinter

universalprintermanagement.exe는 여기 위치해 있습니다: **C:\Program Files (x86)\TSplus\UserDesktop\files**

설명:

명령 /유니버설 프린터 설치 유니버설 프린터를 설치하는 데 사용됩니다.

이것은 이전에 설치된 경우 기존의 유니버설 프린터를 제거하므로 깨끗한 설치입니다.

매개변수:

없음

이 작업을 수동으로 수행할 수도 있습니다. 확인해 주세요. 유니버설 프린터

유니버설 프린터 제거: 유니버설 프린터 제거

구문:

universalprintermanagement.exe /RemoveUniversalPrinter

universalprintermanagement.exe는 여기 위치해 있습니다: **C:\Program Files (x86)\TSplus\UserDesktop\files**

설명:

명령 유니버설 프린터 제거 Universal Printer를 제거하는 데 사용됩니다.

매개변수:

없음

이 작업을 수동으로 수행할 수도 있습니다. 확인해 주세요. 유니버설 프린터

프록시 서버 구성: /프록시 /설정

구문:

AdminTool.exe /proxy /set [매개변수]

설명:

명령 /프록시 /설정 인터넷 접속을 위한 프록시 서버를 구성하는 데 사용됩니다.

매개변수:

- /호스트 대상 호스트는 미리 정의된 값("ie" 또는 "none")이거나 사용자 정의 값(예: 127.0.0.1 또는 proxy.company.org)일 수 있습니다. 이 매개변수는 필수입니다.
- /포트 프록시 서버에 연결하는 데 사용되는 포트 번호입니다. 호스트 이름 값이 사용자 정의 값인 경우 필수입니다.
- /사용자 이름 프록시 서버에 연결할 사용자 이름. 이 설정은 선택 사항입니다.
- /비밀번호 사용자 이름이 정의된 경우 사용자의 비밀번호를 제공해야 합니다. 그러나 그 값은 비어 있을 수 있습니다.

예시:

AdminTool.exe /proxy /set /host proxy.company.org /port 80 /username dummy /password pass@word1

AdminTool.exe /proxy /set /host ie

자세한 정보는 다음을 참조하십시오. 인터넷 액세스를 위한 프록시 서버 구성 방법은 무엇인가요?

웹 자격 증명 양식 열기: /webcredentials

구문:

AdminTool.exe /webcredentials

설명:

명령 /webcredentials 단일 창에서 웹 자격 증명 인터페이스를 실행합니다(관리 도구 > 웹 > 웹 자격 증명에서 수행하는 것처럼).

매개변수:

없음

웹 자격 증명 만들기: /webcredentials-add

구문:

AdminTool.exe /webcredentials-add [웹로그인] [웹비밀번호] [윈도우로그인] [윈도우비밀번호] [최대동시세션]

설명:

명령 /webcredentials-add 웹 자격 증명을 생성하는 데 사용됩니다(관리 도구 > 웹 > 웹 자격 증명에서 수행하는 것처럼).

매개변수:

- 웹 로그인 생성하려는 웹 로그인입니다.
- 웹 비밀번호 연관된 웹 비밀번호입니다. 비어 있는 자격 증명일 수 있습니다. 이를 위해 빈 비밀번호를 나타내기 위해 이중 따옴표 ""를 사용하십시오.
- 윈도우 로그인 해당 사용자의 Windows 로그인.
- 윈도우 비밀번호 Windows 비밀번호.
- 최대 동시 세션 (선택 사항): 이 사용자의 최대 동시 세션 수.

예시:

AdminTool.exe /webcredentials-add johndoe passwordABCD johnWinuser johnWinpassword 4

자세한 정보는 다음을 참조하십시오. 웹 자격 증명

웹 자격 증명 제거: /webcredentials-remove

구문:

AdminTool.exe /webcredentials-remove [웹로그인]

설명:

명령 /webcredentials-remove 기존 웹 자격 증명을 제거하는 데 사용됩니다(관리 도구 > 웹 > 웹 자격 증명에서 수행하는 것처럼).

매개변수:

- 웹 로그인 제거하려는 웹 로그인입니다.

예시:

AdminTool.exe /webcredentials-remove johndoe

자세한 정보는 다음을 참조하십시오. 웹 자격 증명

세션 관리자 열기: /세션 관리자

구문:

AdminTool.exe /sessionmanager

설명:

명령 /세션 관리자 단일 크기의 창에서 세션 관리자를 실행합니다(관리 도구 > 홈 > 세션 관리자에서 수행하는 것처럼).

매개변수:

없음

열린 세션 모니터: /farm-sessions-monitor

구문:

AdminTool.exe /farm-sessions-monitor

설명:

명령 /farm-sessions-monitor 농장 관리자의 세션 모니터를 단일 크기의 창에서 실행합니다(관리 도구 > 농장 > 세션 모니터링에서 수행하는 것처럼).

매개변수:

없음

로드 밸런싱 관리자 열기: /농장-부하균형

구문:

AdminTool.exe /farm-loadbalancing

설명:

명령 /농장-부하균형 단일 크기의 창에서 농장 관리자의 로드 밸런싱 관리자를 실행합니다(관리 도구 > 농장 > 로드 밸런싱에서 수행하는 것처럼).

매개변수:

없음

시스템 감사 실행: /시스템 감사

구문:

AdminTool.exe /systemaudit

설명:

명령 /시스템 감사 시스템 감사를 실행합니다(관리 도구 > 홈 > 시스템 감사 > 시스템 감사 실행에서 수동으로 수행하는 것처럼).

매개변수:

없음

라이선스 활성화: /활성화

구문:

AdminTool.exe /activate [licensePath]

설명:

명령 활성화 원격 액세스 라이센스를 활성화하는 데 사용되며, 라이센스 파일을 사용합니다.

매개변수:

- 라이센스 경로 라이선스 파일의 경로

예시:

AdminTool.exe /activate “C:\Program Files (x86)\TSplus\license.lic”

가상 머신 클로닝 후 라이센스 재설정: 재설정

구문:

AdminTool.exe /license /reset

설명:

서버를 복제할 때 AdminTool의 '라이센스' 탭에 컴퓨터 ID가 표시되지 않거나 "잘못된 하드웨어 식별자."라는 오류 메시지가 표시될 수 있습니다. 명령 재설정 클론 서버에서 라이센스를 초기화하여 설치된 TSplus 제품에 대해 새로운 라이센스를 할당할 수 있도록 하는 것을 목표로 합니다.

중요한 사항:

1. 새로운 TSplus 라이센스는 새로운 활성화 키를 사용하여 활성화해야 합니다.
2. 비클론 머신에서 /license /reset 명령을 사용하지 마십시오. 이는 라이센스 할당을 영구적으로 방지합니다. 진행하기 전에 항상 머신의 상태를 확인하십시오.

클론된 서버에서 라이센스를 재설정하는 단계:

1.
   클론된 서버에서 관리자 세션을 엽니다.

2.
   HDD 볼륨 일련 번호를 변경하십시오.

- 실행하십시오 볼륨 현재 볼륨 일련 번호(VSN)를 표시하는 명령입니다. 결과는 다음과 같아야 합니다: 74F8-9C08 .
- 볼륨 ID 유틸리티를 다운로드하고 설치하세요. 여기 .
- 명령을 실행하십시오: volumeid C: 84F8-9C08 관리자로서 드라이브 VSN을 변경합니다. 이 예제에서는 디스크 C:의 VSN을 변경했으며, 이전 VSN의 첫 번째 문자만 변경하여 새 VSN을 지정했습니다.
- 참고: 이 단계는 중요합니다. 특정 Windows Server 버전은 SysPrep을 사용하더라도 클론 중에 새 볼륨 일련 번호를 생성하지 않습니다.

3.

복제된 서버의 이름을 바꾸고 재시작하십시오.

4. 관리 도구에서 라이센스 재설정:

- 관리자 권한으로 명령 프롬프트를 엽니다.
- 이 명령을 사용하여 AdminTool 실행 파일이 포함된 디렉토리로 이동하십시오: cd "C:\Program Files (x86)\TSplus\UserDesktop\files"
- 다음 명령을 실행하십시오: AdminTool.exe /license /reset

5. 재설정을 확인하십시오.

- 명령을 실행한 후 '라이센스' 탭에 다음 오류가 표시되어야 합니다: 라이센스 파일을 읽지 못했습니다(예상치 못한 파일 형식).

6. 새 라이센스를 활성화하세요.

- '라이센스' 탭에서 '라이센스 활성화'를 클릭하고 새로운 활성화 키를 입력하여 필요한 라이센스와 지원을 활성화합니다.

예시:

AdminTool.exe /license /reset TSplus-Security.exe /license /reset ServerMonitoring.exe /license /reset

---

볼륨 라이센스 활성화: /vl /활성화

구문:

AdminTool.exe /vl /activate [라이센스키] [매개변수]

명령 vl /activate 볼륨 라이센스를 활성화하는 데 사용됩니다.

매개변수:

- 라이센스 키 라이센스 키를 활성화하기 위한 형식: AAAA-BBBB-CCCC-DDDD
- /사용자 1에서 50까지의 숫자 중 하나 또는 "무제한"
- /에디션 “데스크탑”, “모바일웹” 또는 “기업”
- /지원 연수 0에서 3까지의 모든 숫자.
- /댓글 라이선스 포털에 라이선스에 첨부할 주석을 지정합니다.

예시:

AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “이것은 댓글입니다”

자세한 정보는 다음을 참조하십시오. 볼륨 라이선스 문서

볼륨 라이센스 활성화 및 비활성화: /vl /enable 그리고 /vl /비활성화

구문:

AdminTool.exe /vl /enable [라이센스키]

AdminTool.exe /vl /disable [licensekey]

설명:

명령 vl /enable 볼륨 라이센스를 활성화하는 데 사용됩니다.

명령 vl /disable 볼륨 라이센스를 비활성화하는 데 사용됩니다.

매개변수:

- 라이센스 키 라이센스 키를 활성화/비활성화하기 위한 형식: AAAA-BBBB-CCCC-DDDD

예시:

AdminTool.exe /vl /enable VOLU-MELI-CENS-EKEY

AdminTool.exe /vl /disable VOLU-MELI-CENS-EKEY

자세한 정보는 다음을 참조하십시오. 서버에서 라이센스를 활성화/비활성화하는 방법은 무엇인가요?

볼륨 라이센스 업데이트: /vl /업데이트

구문:

AdminTool.exe /vl /update [licensekey] [parameters]

설명:

명령 vl /업데이트 볼륨 라이선스의 사용자에게 업데이트하는 데 사용됩니다.

매개변수:

- 라이센스 키 라이센스 키 업데이트를 위한 형식: AAAA-BBBB-CCCC-DDDD
- /사용자 1에서 50까지의 숫자 중 하나 또는 "무제한"

예시:

AdminTool.exe /vl /update /users 2 AdminTool.exe /vl /update /users unlimited

자세한 정보는 다음을 참조하십시오. 서버에서 볼륨 라이선스의 사용자를 업데이트하는 방법은 무엇인가요?

볼륨 라이센스 키에 대한 남은 라이센스 크레딧 표시: /vl /크레딧-라이센스

구문:

AdminTool.exe /vl /credits-license [licensekey] [parameters]

설명:

명령 vl /credits-license 볼륨 라이센스 키와 관련된 남은 라이센스 크레딧을 표시하는 데 사용됩니다.

매개변수:

- 라이센스 키 볼륨 라이센스 키, 이 형식: AAAA-BBBB-CCCC-DDDD
- /로그인 파트너의 로그인 정보를 제공하십시오.
- /에디션 고급 보안 및 서버 모니터링 제품에 대한 선택적 에디션 매개변수를 제공합니다.
- /침묵 명령을 조용히 실행합니다.

출력은 사용자 수준 환경 변수에 저장됩니다. 볼륨 라이선스 크레딧 값을 읽어야 할 수 있습니다. 볼륨 라이선스 크레딧 다른 프로세스에서 명령을 사용하여 에코 %VOLUME_LICENSE_CREDITS% .

예시:

AdminTool.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE TSplus-Security.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE /edition Essentials /silent

자세한 정보는 다음을 참조하십시오. 볼륨 라이센스 키의 남은 라이센스 크레딧을 어떻게 표시하나요?

볼륨 라이센스 키에 대한 남은 지원 크레딧 표시: /vl /크레딧-지원

구문:

AdminTool.exe /vl /credits-support [licensekey] [parameters]

설명:

명령 vl /크레딧-지원 볼륨 라이센스 키와 관련된 남은 지원 크레딧을 표시하는 데 사용됩니다.

매개변수:

- 라이센스 키 볼륨 라이센스 키, 이 형식: AAAA-BBBB-CCCC-DDDD
- /로그인 파트너의 로그인 정보를 제공하십시오.
- /에디션 고급 보안 및 서버 모니터링 제품에 대한 선택적 에디션 매개변수를 제공합니다.
- /침묵 명령을 조용히 실행합니다.

출력은 사용자 수준 환경 변수에 저장됩니다. 볼륨 라이선스 크레딧 값을 읽어야 할 수 있습니다. 볼륨 라이선스 크레딧 다른 프로세스에서 명령을 사용하여 에코 %VOLUME_LICENSE_CREDITS% .

예시:

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE TSplus-Security.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE /edition Essentials

자세한 정보는 다음을 참조하십시오. 볼륨 라이센스 키에 대한 남은 지원 크레딧을 표시하는 방법은 무엇인가요?

2FA - 재설정: /resetuser

구문:

TwoFactor..Admin.exe /resetuser [user1] [user2] … [userN]

설명:

명령 /resetuser 2FA 사용자를 재설정하는 데 사용되며, 사용자 인터페이스를 통해 수행하는 대신 (여기에서 인터페이스에서 수행할 수 있습니다: TwoFactor.Admin > 사용자 관리 > 재설정)

매개변수:

- user1 user2 ... userN 사용자 비밀번호를 재설정하려는 도메인 이름(단순한 공백으로 구분)

예시:

TwoFactor.Admin.exe /resetuser johndoe jackrussell chuckbartowski

자세한 정보는 다음을 참조하십시오. 사용자 구성 재설정

2FA - 사용자 추가: 사용자 추가

구문:

TwoFactor.Admin.exe /addusers [userInfos1] [userInfos2] … [userInfosN]

설명:

명령 사용자 추가 여기에서 사용자 인터페이스를 통해 사용자별로 수행하는 대신 여러 2FA 사용자를 추가하는 데 사용됩니다(여기에서 인터페이스에서 수행할 수 있습니다: TwoFactor.Admin > 사용자 관리 > 사용자 추가).

매개변수:

- userInfos1 userInfos2 ... userInfosN
  사용자를 추가하려는 사용자에 대한 정보입니다. 이 정보는 세미콜론으로 구분된 다음 필드로 구성됩니다.
  - 도메인 이름 (필수): 추가할 사용자의 도메인 이름
  - 수신 방법 (선택 사항): 확인 코드를 수신하는 방법. 다음 값 중 하나여야 합니다: SMS, 앱, 이메일 또는 사용자 선택. 앱이 기본값입니다.
  - 모바일폰 (선택 사항): 추가할 사용자의 전화번호
  - 이메일 (선택 사항): 추가할 사용자의 이메일

예시:

TwoFactor.Admin.exe /addusers johndoe jackrussell;LetTheUserChoose chuckbartowski;전화; +33101010101; abcd@efgh.com 사만다카터;이메일;;

자세한 정보는 다음을 참조하십시오. 사용자 및 그룹 추가

2FA - 그룹 추가: /addgroups

구문:

TwoFactor.Admin.exe /addgroups [group1] [group2] … [groupN]

설명:

명령 /addgroups 여기에서 사용자 인터페이스를 통해 그룹별로 수행하는 대신 여러 2FA 그룹을 추가하는 데 사용됩니다(여기에서 인터페이스에서 수행할 수 있습니다: TwoFactor.Admin > 사용자 관리 > 그룹 추가).

매개변수:

- 그룹1 그룹2 ... 그룹N 추가하려는 그룹의 이름.

예시:

TwoFactor.Admin.exe /addgroups group1 group2 group3

자세한 정보는 다음을 참조하십시오. 사용자 및 그룹 추가

2FA - 사용자 목록: /getusers

구문:

TwoFactor.Admin.exe /getusers

설명:

명령 /getusers 2FA 관리 콘솔에 구성된 모든 사용자/그룹의 목록을 가져오는 데 사용됩니다. 이 사용자/그룹 목록의 JSON 표현이 반환되며, 예를 들어 PowerShell 스크립트에서 사용할 수 있습니다.

이 목록은 인터페이스에서 확인할 수 있습니다: TwoFactor.Admin > 사용자 관리.

매개변수:

없음

2FA - 그룹 추가: /사용자삭제

구문:

TwoFactor.Admin.exe /deleteuser [도메인 이름] [사용자 유형]

설명:

명령 /사용자삭제 사용자가 2FA 구성에서 제거되도록 하는 데 사용됩니다(이는 인터페이스에서 여기에서 수행할 수 있습니다: TwoFactor.Admin > 사용자 관리 > 제거).

매개변수:

- 도메인 이름 사용자 또는 제거할 그룹의 이름.
- 사용자 유형 삭제할 객체의 유형. 값은 "user" 또는 "group"이어야 합니다.

예시:

TwoFactor.Admin.exe /deleteuser “이것은 그룹 이름입니다” 그룹 TwoFactor.Admin.exe /deleteuser administrator 사용자

자세한 정보는 다음을 참조하십시오. 사용자 및 그룹 제거

Windows 자격 증명 관리자에 자격 증명을 추가하거나 업데이트하십시오: /windowscredential-addorupdate

구문:

AdminTool.exe /windowscredential-addorupdate

또는

AdminTool.exe /windowscredential-addorupdate csvFilePath

설명:

명령 /windowscredential-addorupdate 새로운 Windows 자격 증명을 Windows 자격 증명 관리자에 추가하거나 기존 자격 증명을 업데이트하는 데 사용됩니다. 도메인, 사용자 이름 및 비밀번호를 지정하여 개별적으로 자격 증명을 제공하거나 CSV 파일에서 여러 항목을 일괄 처리할 수 있습니다.

이 명령은 SSO와 함께 웹 포털을 위한 SAML을 통한 외부 인증을 구성하는 데 유용합니다.

매개변수:

- **단일 자격 증명 모드**

- 도메인 (필수): 사용자가 Active Directory의 일부인 경우 도메인 이름, 또는 사용자가 로컬 사용자일 경우 머신 이름
- 사용자 이름 (필수): Windows 계정 사용자 이름
- 비밀번호 (필수): Windows 계정 비밀번호

- **대량 모드 (CSV 파일)**

  - csv 파일 경로 (필수): 추가하거나 업데이트할 하나 이상의 자격 증명이 포함된 CSV 파일의 경로

예시

Active Directory 사용자용:

AdminTool.exe /windowscredential-addorupdate COMPANY johndoe SecurePassword123

로컬 사용자용:

AdminTool.exe /windowscredential-addorupdate MACHINE-NAME janedoe SecurePassword123

CSV 파일에서 자격 증명을 일괄 추가하거나 업데이트하려면:

AdminTool.exe /windowscredential-addorupdate C:\\credentials\\users.csv

---

Windows 자격 증명 관리자에서 자격 증명 제거: /windowscredential-remove

구문:

AdminTool.exe /windowscredential-remove 사용자 이름

또는

AdminTool.exe /windowscredential-remove csvFilePath

설명:

명령 /windowscredential-remove Windows 자격 증명을 제거하는 데 사용됩니다. 대상을 지정하여 단일 자격 증명을 제거하거나 CSV 파일을 사용하여 여러 자격 증명을 일괄적으로 제거할 수 있습니다.

매개변수:

- **단일 자격 증명 모드:**
-

대상 (필수): 자격 증명의 대상 이름, 일반적으로 도메인 또는 서버 이름

- **대량 모드 (CSV 파일):**

  - csv 파일 경로 (필수): 제거할 사용자 이름이 포함된 CSV 파일의 경로. 파일이 존재해야 합니다.

예시:

AdminTool.exe /windowscredential-remove COMPANY

AdminTool.exe /windowscredential-remove C:\credentials\remove_users.csv

웹 포털 기능을 넘어 웹 액세스 페이지를 완전히 사용자 정의하는 방법은 무엇인가요?

개요

사용하여 웹 포털 Terminal Service Plus 웹 액세스 페이지를 광범위하게 사용자 정의할 수 있습니다.

그러나 경우에 따라 이것만으로는 충분하지 않습니다. 이러한 경우에는 Webmaster Toolkit에서 생성된 Web Access Page를 직접 수정하여 Web Portal 기능을 넘어 Web Access Page를 완전히 사용자 정의할 수 있습니다.

경고, 이 문서는 숙련된 웹 개발자만을 위한 것입니다.

필수 설정 생성

웹 액세스 페이지에 필수 설정을 포함하려면, 웹 액세스 페이지를 생성하는 것으로 시작하는 것이 좋습니다. 웹 포털 .

파일 위치

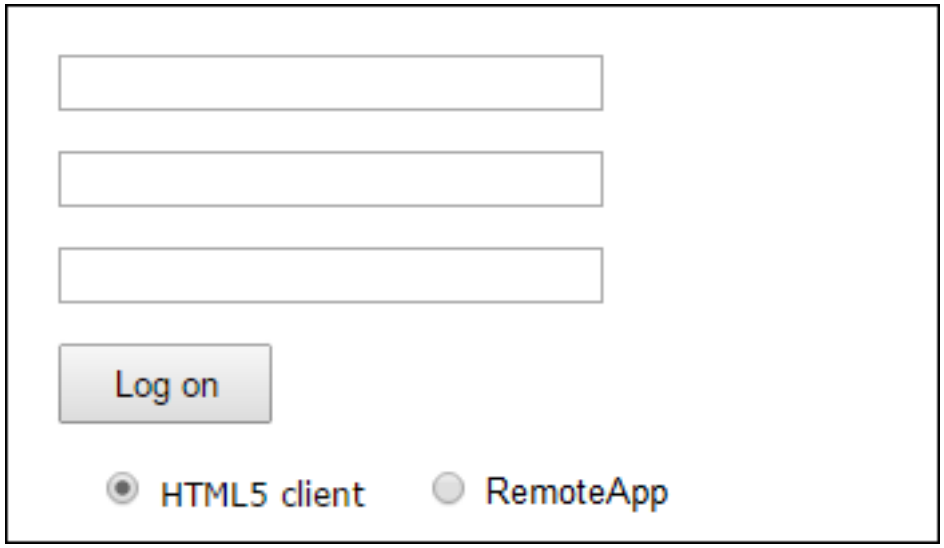
웹 액세스 페이지는 “C:\Program Files (x86)\TSplus\Clients\www” 폴더에 생성됩니다. 예를 들어 페이지 이름으로 “index”를 선택하면 이 폴더에 “index.html”이라는 이름의 파일이 생성됩니다. 이는 표준 HTML 파일이므로 HTML, JavaScript 및 CSS 프로그래밍 언어에 대한 모든 지식을 사용하여 사용자 정의 페이지를 개발할 수 있습니다.

모든 파일 포함은 "C:\Program Files (x86)\TSplus\Clients\www" 폴더를 기준으로 작성됩니다. 예를 들어, 주요 CSS 스타일 파일은 "C:\Program Files (x86)\TSplus\Clients\www\software\common.css"에 위치하므로, 다음 줄을 통해 HTML 웹 액세스 페이지 파일에 포함됩니다:

최소 웹 액세스 페이지

HTML 파일에서 생성된 웹 포털 기본 설정을 시작으로, 최소한의 웹 액세스 페이지로 축소할 것입니다. 메모장이나 Notepad++와 같은 텍스트 편집기를 사용하는 것을 권장합니다. 아니다 Word를 사용하세요.

작업 후 아래 스크린샷과 같이 보일 것입니다:



먼저, 당신은 그 사이에 있는 모든 것을 유지해야 합니다.
그리고 HTML 태그:

- 브라우저가 캐시를 지우도록 강제하는 메타 태그
- .js 파일 포함
- 자바스크립트 설정 선언

그런 다음 'body'와 '/body' HTML 태그 사이의 내용을 다음 몇 줄로 줄일 수 있습니다:

HTML5 클라이언트 원격 앱

웹 브라우저에서 웹 페이지를 새로 고치면 위 스크린샷의 최소 페이지를 얻을 수 있습니다.

변경된 파일을 저장한 후 브라우저의 캐시를 지우는 것을 권장합니다.

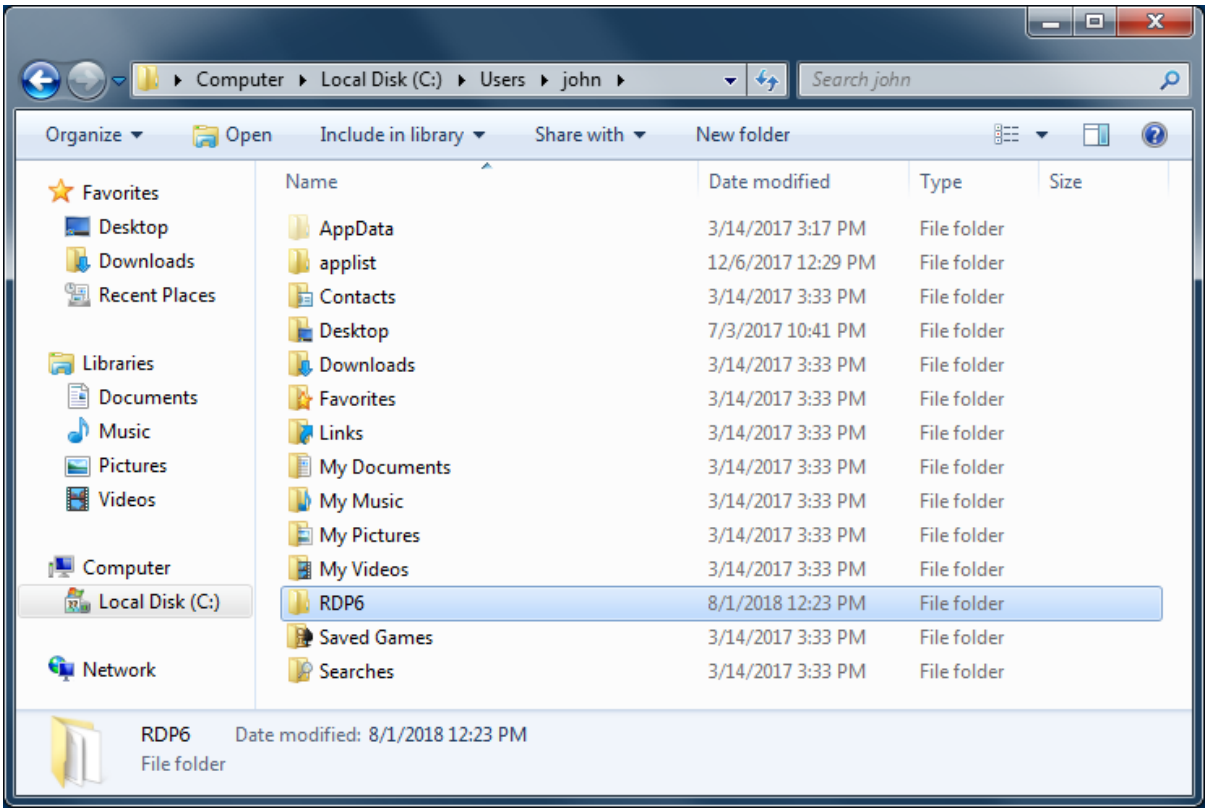
마지막으로, 이제 당신에게 달려 있습니다!

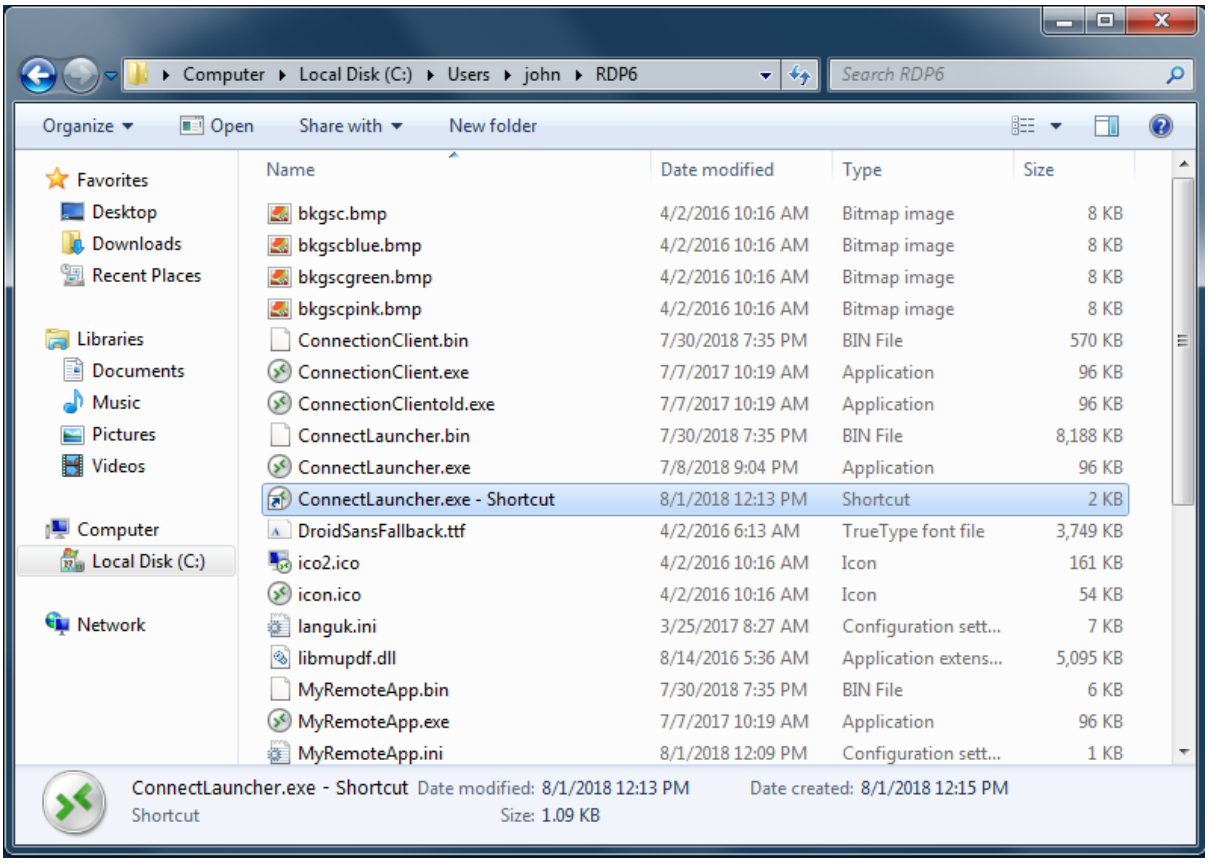
JavaScript 함수에 대한 호출을 특정 이벤트와 주어진 식별자(id="…")로 유지하는 한, 완전히 사용자 정의된 웹 액세스 페이지가 잘 작동할 것입니다!

생성된 클라이언트의 매개변수를 편집하거나 삭제하십시오.

연결 클라이언트의 매개변수를 변경하고 싶은 이유는 여러 가지가 있습니다: TSplus 서버 IP 주소가 변경되었거나, 프린터 리디렉션을 추가해야 하거나, 범용 프린터 설정을 변경해야 하는 경우 등입니다…

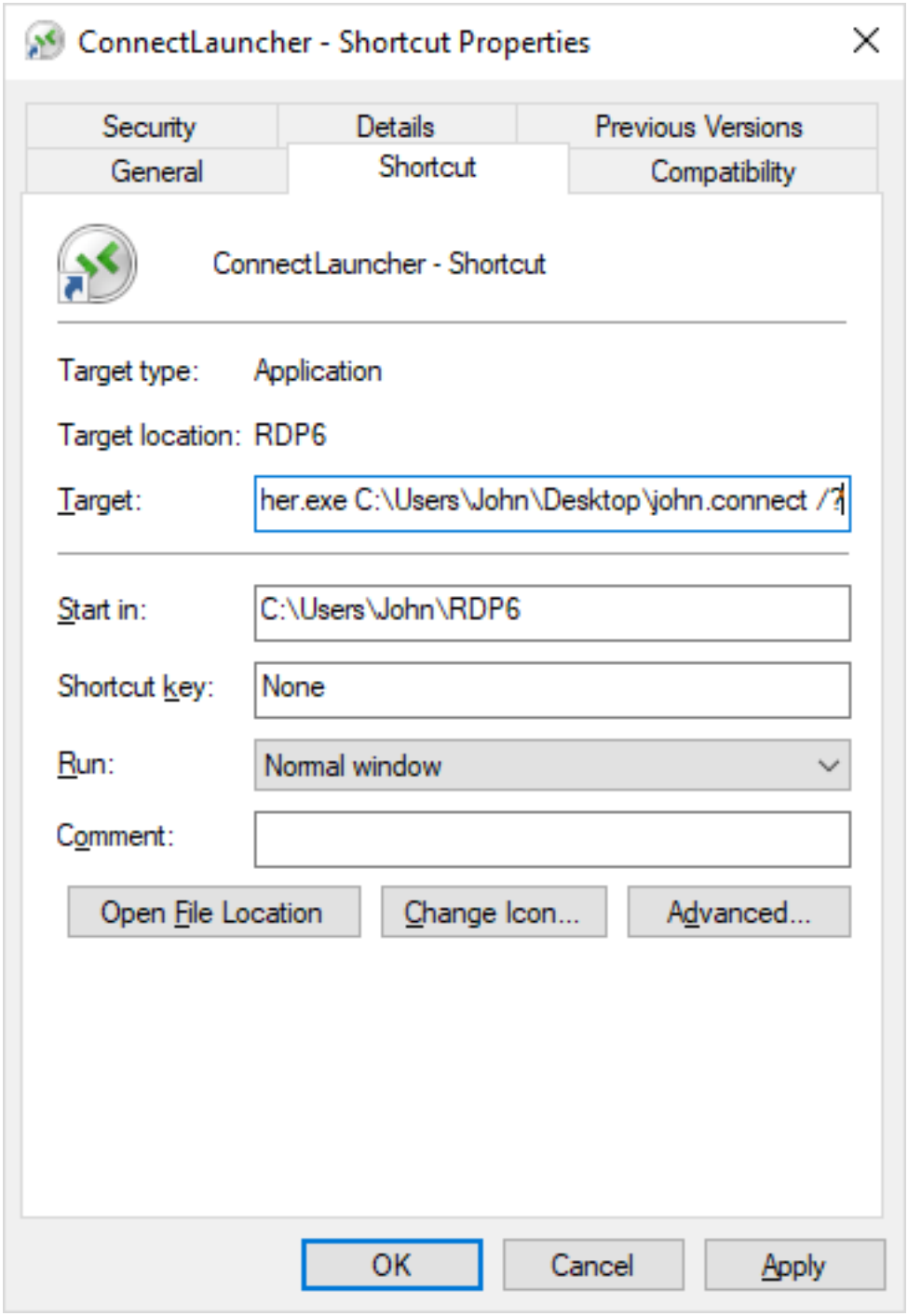
- 먼저 사용자 프로필의 RDP6 폴더에 있는 ConnectLauncher.exe 파일의 바로 가기를 만들어야 합니다.



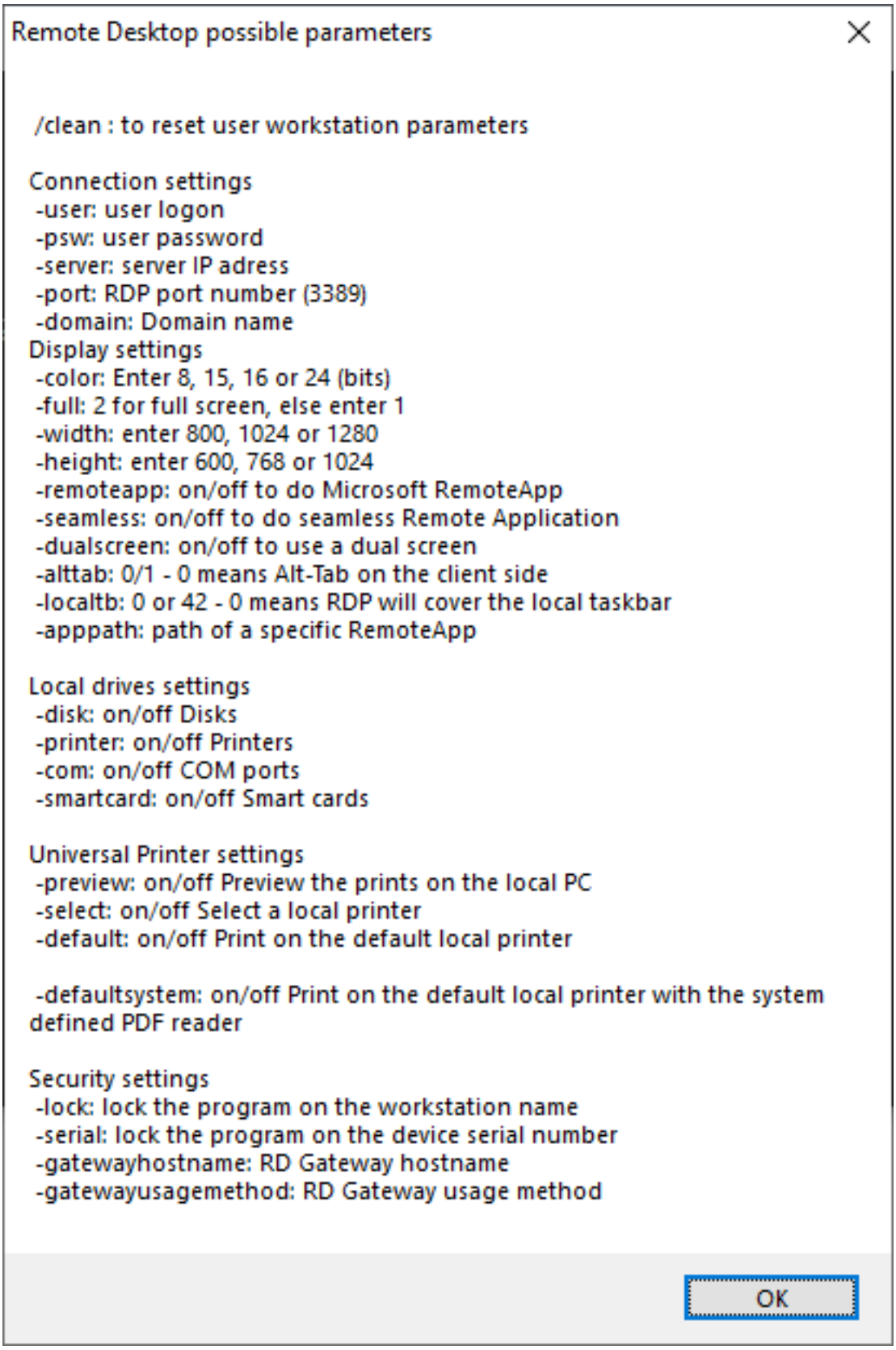


.

- 그런 다음, 그것을 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다. "대상" 필드의 끝에 마우스를 놓고 클라이언트의 경로 뒤에 "/?"를 입력합니다. 예: C:\Users\John\Desktop\clientname.connect /?":

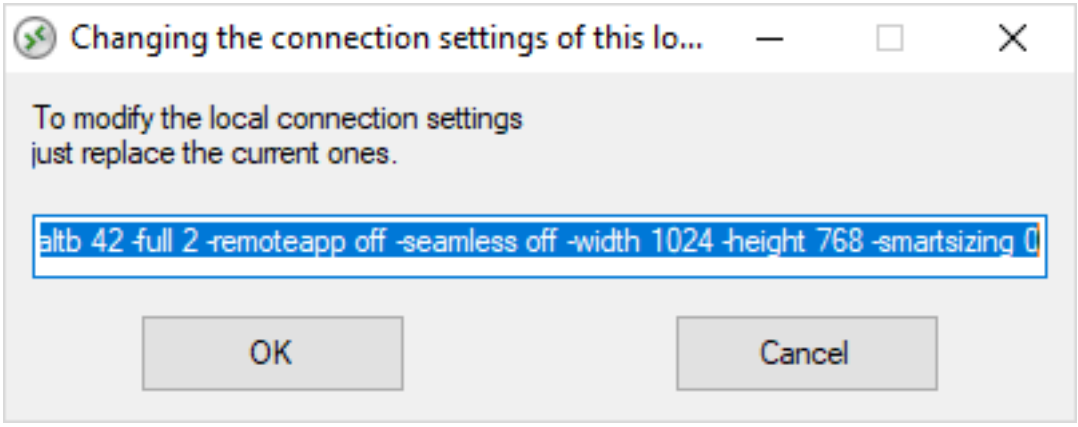


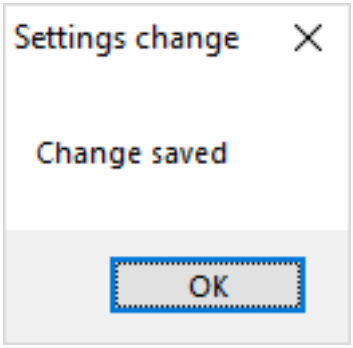
이제 확인을 클릭하고 바로 가기를 두 번 클릭하세요. 전환 목록이 나타납니다:



확인 버튼을 클릭하면 모든 매개변수 목록이 작은 창에 나타납니다.

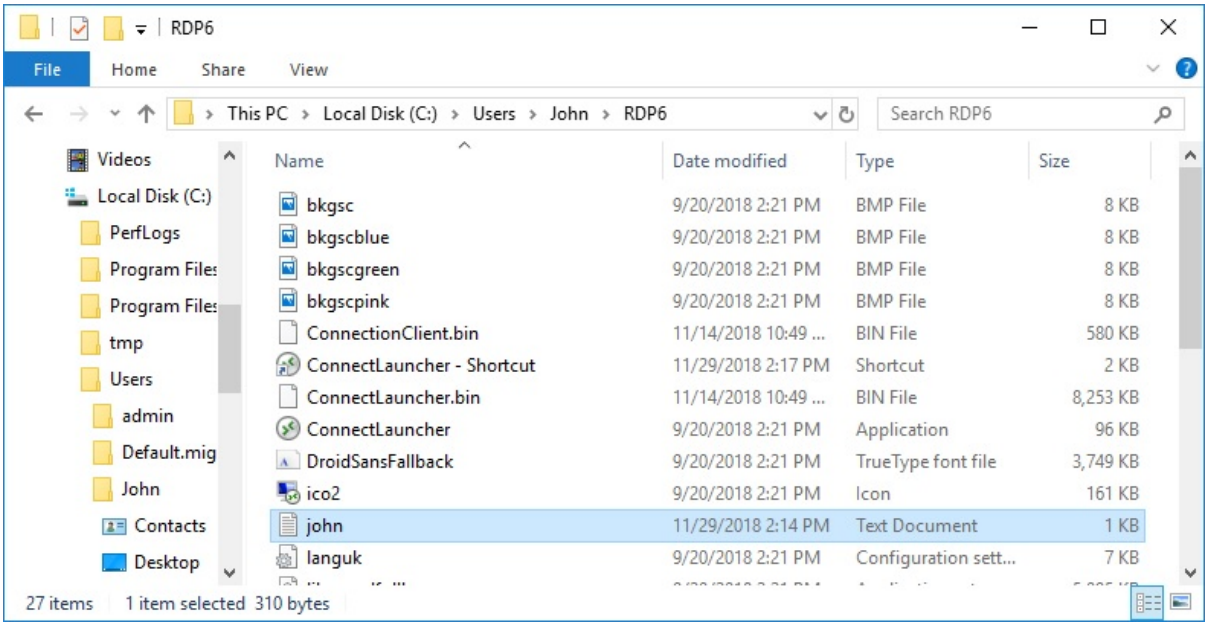
이제 선호도에 맞게 수정할 수 있으며, 변경 사항을 적용하려면 로그오프한 후 다시 로그인해야 합니다.





생성된 클라이언트의 매개변수를 정리하십시오.

클라이언트를 최소한 한 번 실행한 후, RDP6 폴더에 위치한 client.txt 파일을 삭제하여 매개변수를 정리할 수 있습니다.



Active Directory 도메인에서 Windows 통합 인증 활성화

이 가이드는 웹 포털에서 그룹 관리 서비스 계정(gMSA)과 함께 Windows 통합 인증(케르베로스/NTLM)을 구성하기 위해 제공됩니다.

각 회사의 네트워크 및 아키텍처의 고유한 특성으로 인해 이 문서를 따르면서 발생하는 문제에 대한 지원을 제공할 수 없습니다. Windows 통합 인증을 사용하는 웹 포털에 대한 기술 요구 사항을 충족하지만, 구현은 귀하의 책임입니다.

도메인 구성

Active Directory 환경은 Kerberos 또는 NTLM 인증을 지원해야 합니다.

관리 서비스 계정(gMSA) 설정

웹 포털 서비스를 설치하고 실행하십시오. **도메인 관리 서비스 계정** 대신 도메인 관리자 계정.

필수 조건

- Active Directory 스키마 수준: **Windows Server 2012** 또는 이후 (gMSA에 필요)
- 최소한 하나의 도메인 컨트롤러가 실행 중입니다. **Windows Server 2012** 또는 이후
- KDS 루트 키 생성됨 (일회성 설정)
- 회원 가입 **도메인 관리자** 또는 **계정 운영자** 계정을 생성하기 위해

KDS 루트 키를 생성합니다(아직 생성되지 않은 경우).

도메인 컨트롤러에서 권한 상승된 PowerShell 세션에서 실행:

터미널 창

```
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

이로 인해 루트 키가 즉시 사용 가능해집니다.

gMSA 생성

사용하다 New-ADServiceAccount :

터미널 창

```
New-ADServiceAccount `
  -Name "WebPortalSvc" `
  -DNSHostName "WebPortalSvc.domain.local" `
  -PrincipalsAllowedToRetrieveManagedPassword "YourServerGroup" `
  -Enabled $true
```

- 이름 gMSA 계정 이름
- DNS호스트이름 계정의 FQDN
- 관리되는 비밀번호를 검색할 수 있는 원칙 컴퓨터/그룹이 이 gMSA를 사용할 수 있습니다.

관리자 권한 부여 (선택 사항 / 필요에 따라)

기본적으로 gMSA는 특별한 권한이 없습니다.

도메인 수준 액세스 부여(선택 사항):

터미널 창

```
Add-ADGroupMember -Identity "Domain Admins" -Members "WebPortalSvc$"
```

로컬 관리자/로그온 권한 부여(필요한 경우):

터미널 창

```
Add-ADGroupMember -Identity "Administrateurs" -Members "WebPortalSvc$"
```

중요: 후행 `$` gMSA 계정 참조에 AD에서 필요합니다.

재부팅 요구 사항

재부팅이 필요합니다. 서비스 계정을 계속 설치하거나 사용하기 전에 정책을 새로 고치십시오.

대상 서버에 gMSA 설치

각 gMSA를 사용할 서버에서 실행:

터미널 창

```
Install-ADServiceAccount -Identity "WebPortalSvc"
```

테스트 설치:

터미널 창

```
Test-ADServiceAccount -Identity "WebPortalSvc"
```

gMSA를 사용하도록 서비스 구성

1. 부여 **서비스로 로그인** 계정으로:

   - 그룹 정책 편집기 열기
   - 이동: 컴퓨터 구성 > Windows 설정 > 보안 설정 > 로컬 정책 > 사용자 권한 할당
   - 열기 서비스로 로그인
   - 추가 DOMAIN\WebPortalSvc$

2. 웹 포털 파일/폴더에 대한 NTFS 권한을 보장하십시오:

   - 응용 프로그램 폴더/실행 파일을 마우스 오른쪽 버튼으로 클릭 > 속성 > 보안
   - 추가 DOMAIN\WebPortalSvc$
   - 최소한 부여하십시오 **읽기 및 실행** (또는 **전체 제어** 배포에 따라 필요한 경우

3.

서비스 ID 구성:

- 계정: DOMAIN\WebPortalSvc$
- 비밀번호: **빈칸을 남겨두세요**

서비스 주체 이름(SPN) 구성

웹 서비스는 Kerberos에 등록되어야 합니다.

도메인 컨트롤러에서 실행:

터미널 창

```
setspn -A HTTP/webserver.domain.com DOMAIN\WebPortalSvc
```

서버 FQDN 및 계정으로 교체하십시오.

웹 포털 호스팅 서버가 HTTP.sys를 사용하는 경우, 머신 계정에 대해 SPN을 등록하십시오.

터미널 창

```
setspn -S HTTP/portal.hiyoko.com:8008 WIN-HLBO0AGABB7
setspn -S HTTP/portal.hiyoko.com:8009 WIN-HLBO0AGABB7
```

클라이언트 머신에서 네트워크 구성

도메인에 가입된 클라이언트를 올바른 서브넷에 배치하려면:

1. 올바른 네트워크 인터페이스 식별
2. 기존 정적 IP 제거(잘못된 경우)
3. 정적 IP, 서브넷 마스크 및 DNS/DC 서브넷과 일치하는 기본 게이트웨이를 할당합니다.
4. DNS 서버 주소 설정

중요: 도메인 컨트롤러와 클라이언트에 정적 IP 주소를 할당하십시오. 보안 정책 동기화는 이 맥락에서 기계가 동일한 서브넷에 있어야 합니다.

필요한 클라이언트 연결 허용

UDP/TCP 53 차단될 수 있으며, 이는 DNS 쿼리를 방지합니다.

문제 해결 단계

DNS 서버 상태 확인

도메인 컨트롤러에서:

터미널 창

net start DNS

DNS 서비스가 실행 중인지 확인하십시오.

DNS 서버 IP 확인

클라이언트에서:

터미널 창

```
ipconfig /all
```

DNS 서버 IP가 도메인 컨트롤러 IP와 일치하는지 확인하십시오.

기본 연결 테스트

클라이언트에서:

터미널 창

```
ping <DC_IP_Address>
```

핑이 실패하면 네트워크/방화벽 라우팅 문제를 해결하십시오.

방화벽 규칙 확인

클라이언트와 서버에서 인바운드/아웃바운드 UDP/TCP 53이 허용되도록 하십시오.

nslookup으로 테스트

터미널 창

nslookup domain.com <DC_IP_Address>

이것이 작동하면 기본 DNS 서버가 잘못 구성되었거나 도달할 수 없을 수 있습니다.

이벤트 뷰어 검토

도메인 컨트롤러에서 DNS 관련 오류를 확인하십시오.

Windows 통합 인증을 위한 Mozilla Firefox 구성

Firefox는 기본적으로 WIA를 사용하지 않습니다.

1단계: 신뢰할 수 있는 협상 URI

1. 파이어폭스 열기
2. 이동하다 about:config
3. 경고 수락
4. 설정
   network.negotiate-auth.trusted-uris
   귀하의 도메인, 예를 들어:
   - intranet.domain.com, domain.com

2단계: 신뢰할 수 있는 NTLM URI

설정 네트워크.자동-ntlm-인증.신뢰할 수 있는-uri 같은 도메인 목록으로.

3단계: Kerberos 위임 URI(필요한 경우)

설정 network.negotiate-auth.delegation-uris Please provide the text you would like to have translated into Korean.

- domain.com

4단계: 브라우저 재시작

Firefox를 재시작하여 변경 사항을 적용하십시오.

Windows 통합 인증을 위한 Google Chrome 구성

Chrome은 Windows/시스템 인증 설정을 사용합니다.

그룹 정책을 통해 (권장)

1. Chrome ADMX 템플릿 다운로드:
   - https://chromeenterprise.google/policies/

2. 복사
   chrome.admx
   그리고
   chrome.adml
   로:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\ko-KR

3. 열기 gpedit.msc
4. 이동:
   - 컴퓨터 구성 > 관리 템플릿 > Google > Google Chrome

5. 인트라넷 사이트에 대한 통합 인증을 활성화하고 신뢰할 수 있는 사이트를 구성하십시오:
   - intranet.domain.com, domain.com

6. 정책 적용:

터미널 창

gpupdate /force

다른 방법

다른 방법(Chrome 명령줄 스위치 및 플래그)은 이 맥락에서 성공적이지 않았습니다.

Microsoft Edge를 Windows 통합 인증에 맞게 구성하십시오.

Edge는 Microsoft Edge 정책과 Windows 보안 영역 설정을 사용합니다.

인트라넷 영역에서 자동 로그온 활성화

1. 인터넷 옵션 열기
2. 보안 탭 > 로컬 인트라넷 > 사용자 정의 수준
3. 아래
   사용자 인증
   , 설정:
   - 인트라넷 존에서만 자동 로그온

GPO를 통해 Edge 정책 구성

1단계: Edge ADMX 템플릿 설치

1. 다운로드:
   - https://www.microsoft.com/ko-kr/edge/business/download

2. 복사
   msedge.admx
   그리고
   msedge.adml
   로:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\ko-KR

2단계: 정책 설정 편집

1. 열기 gpedit.msc
2. 이동:

- 컴퓨터 구성 > 관리 템플릿 > Microsoft Edge

3. 활성화:
   - Microsoft Edge가 자격 증명을 위임할 수 있는 서버 목록을 구성합니다.

4. 신뢰할 수 있는 서버 구성:
   - intranet.domain.com, domain.com

3단계: 정책 적용

터미널 창

```
gpupdate /force
```

다른 방법

이 맥락에서 다른 방법(엣지 명령줄 스위치 및 플래그)은 성공적이지 않았습니다.

통합 인증 문제 해결

Kerberos 티켓 확인

Windows 클라이언트에서:

터미널 창

```
klist
```

티켓을 확인해야 합니다. HTTP/webserver.domain.com .

캐시된 자격 증명/티켓 지우기

터미널 창

```
klist purge
```

SPN 등록 확인

도메인 컨트롤러에서:

터미널 창

```
setspn -L serviceaccount
```

확인하십시오 HTTP/webserver.domain.com 목록에 있습니다.

Firefox에서 Kerberos 디버깅

Firefox를 로깅 모드로 시작:

터미널 창

```
set NSPR_LOG_MODULES=negotiateauth:5
set NSPR_LOG_FILE=%USERPROFILE%\Desktop\firefox.log
start firefox.exe
```

리뷰 firefox.log 인증 오류에 대해.

Chrome 정책 확인

Chrome에서 열기:

chrome://policy

확인하십시오 AuthServerWhitelist 그리고 AuthNegotiateDelegateWhitelist 적용됩니다.

엣지 정책 확인

Edge에서 열기:

edge://policy

확인하십시오 AuthServerWhitelist 그리고 AuthNegotiateDelegateWhitelist 적용됩니다.

생애 주기 종료 버전 1-12

Remote Access v12 (및 이전 모든 버전)은 모든 Windows 컴퓨터에서 작동을 중지합니다.
서비스 중단은 2026년 1월에 시작되어 4월에 완전 중단될 때까지 점진적으로 연장됩니다.

LTS 버전 또는 최신 버전으로 업데이트하려면 다음이 필요합니다. **활성 지원 구독** 귀하의 라이센스를 위해. 만약 그렇지 않다면, 귀하의 라이센스 포털에서 지원 구독에 가입하고 귀하의 .LIC 파일로 Admintool에서 라이센스를 업데이트하여 업데이트의 혜택을 받으시기 바랍니다.

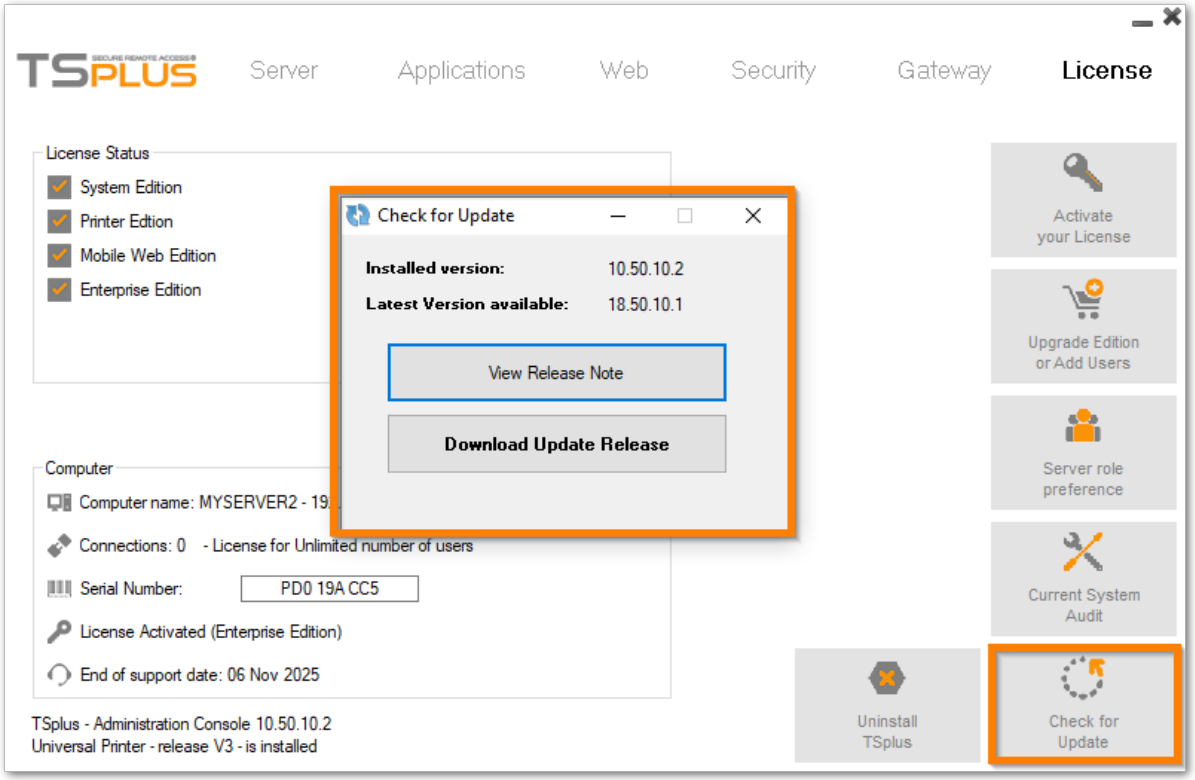
지원 구독을 추가할 수 없거나 오류 메시지를 받는 경우,
우리에게 연락하십시오. 지원 문의 제공:

- 귀하의 라이센스 번호는 PXX XXX XXX 형식입니다. 라이센스 탭의 Admintool에서 볼 수 있습니다.
- 귀하의 라이센스 구매 인보이스
- 귀하의 지원 구독 청구서

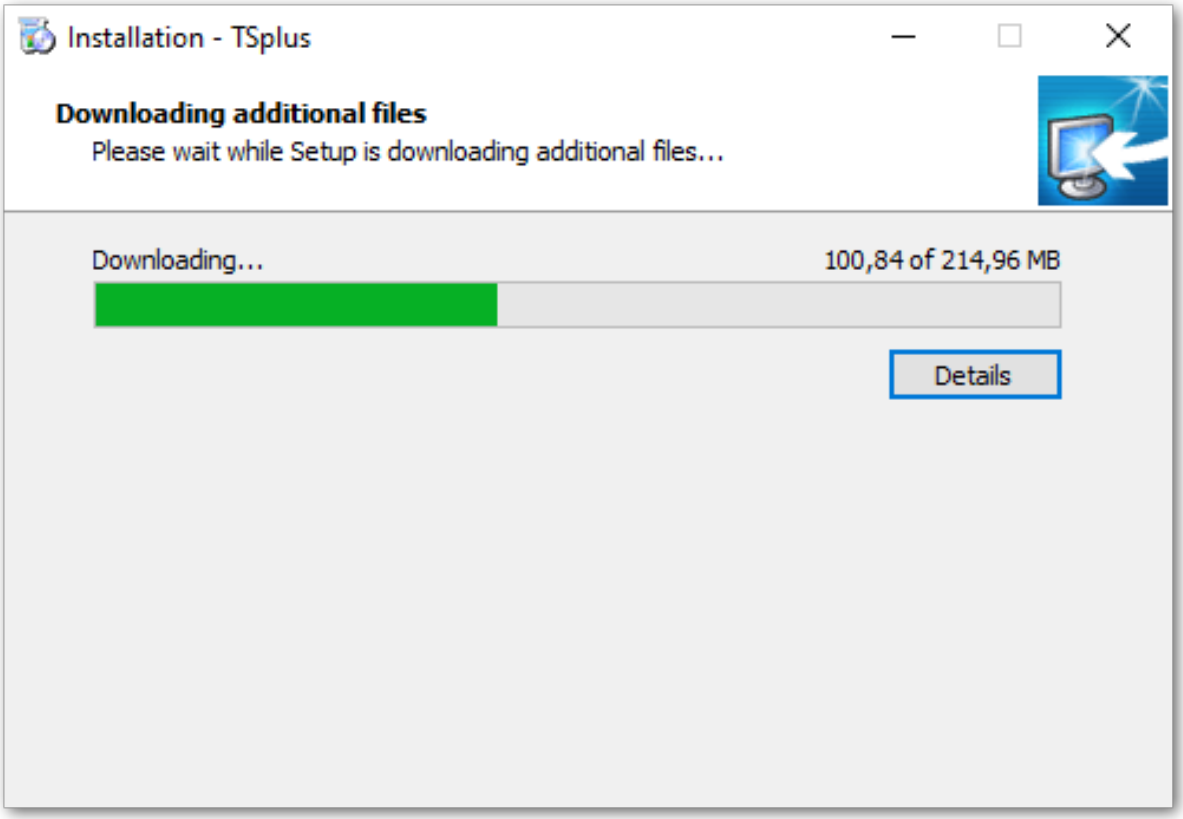
버전 v10 업데이트 중

LTS 대신 최신 버전을 설치하려면 페이지로 이동하세요. LTS)

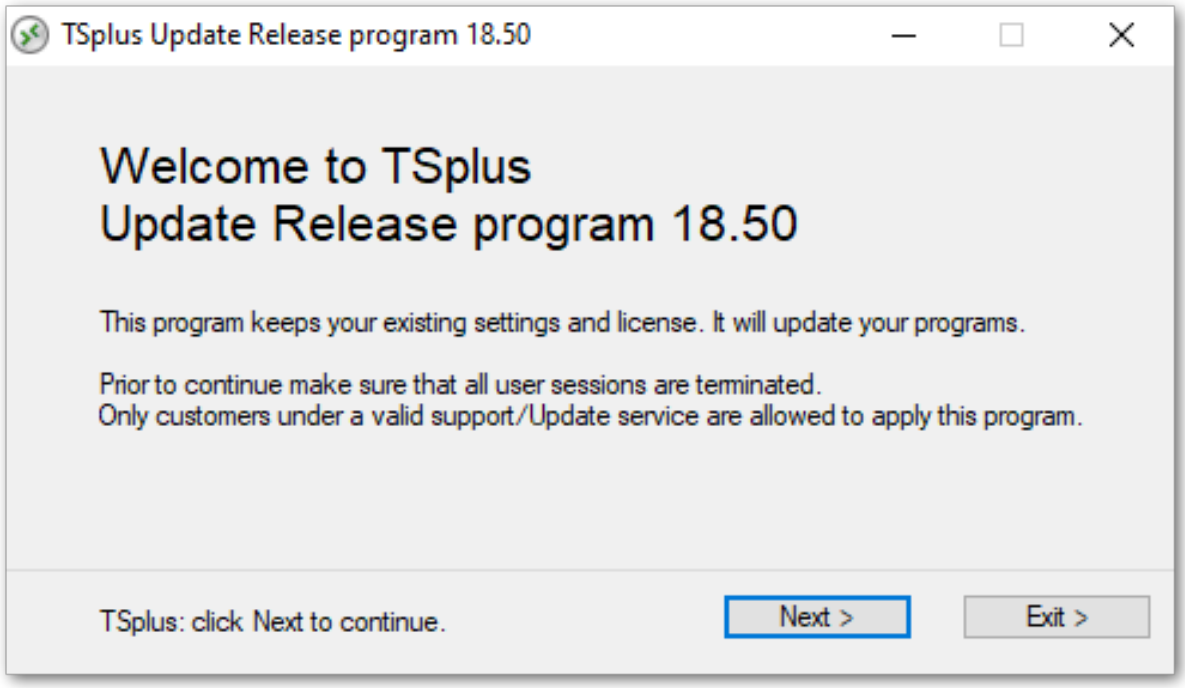
온라인 버전 10에서 다음 필드를 클릭하여 다운로드하십시오. **UpdateRelease.exe**
또한 다운로드할 수 있습니다 UpdateRelease.exe 업데이트 절차를 시작하려면.



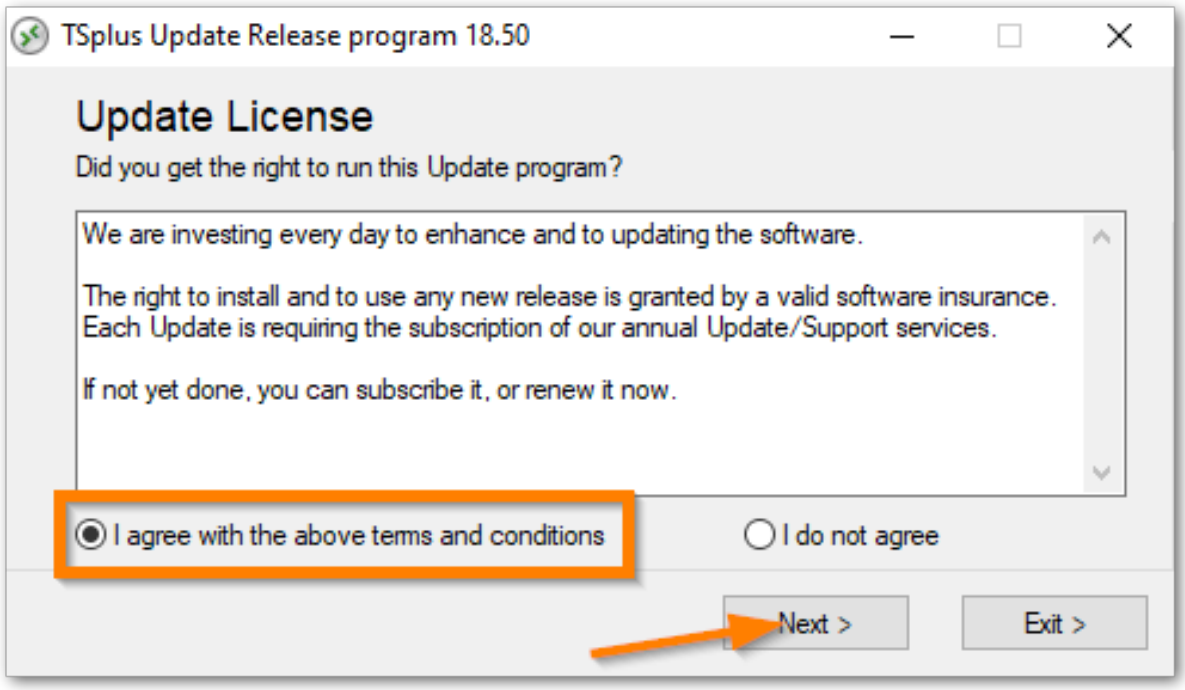
업데이트 파일인 updaterelease.exe를 다운로드하고 실행하세요.



업데이트 프로그램이 나타납니다.



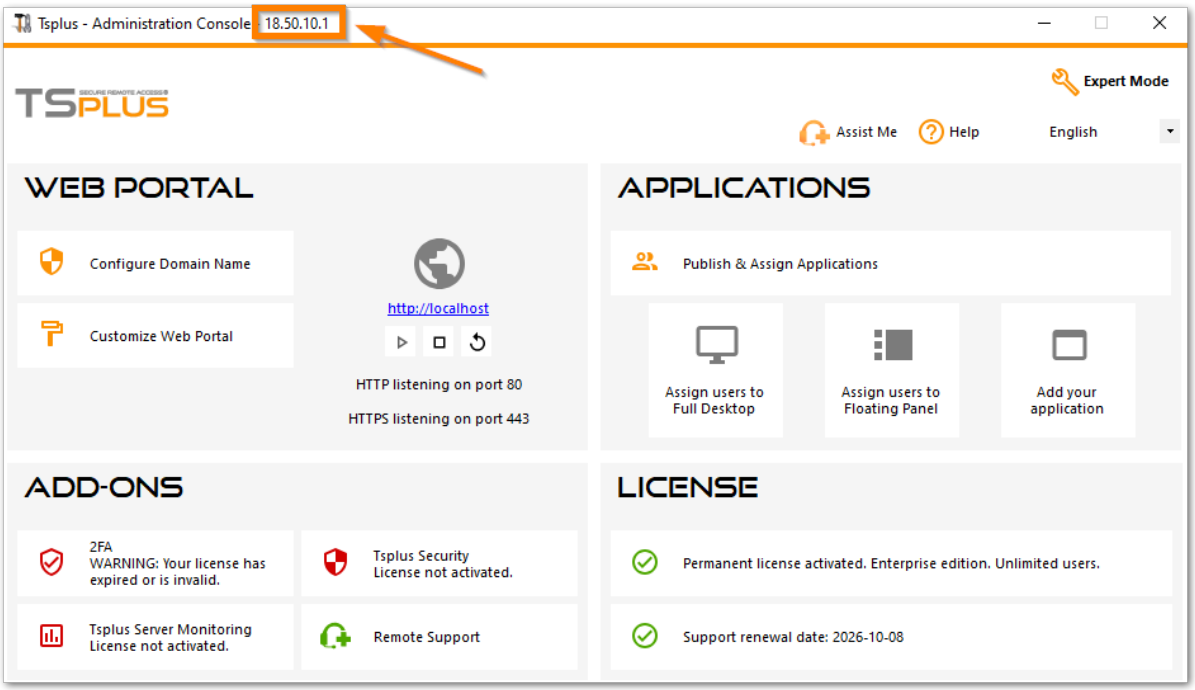
약관에 동의하고 클릭하세요
다음



모든 단계를 따르고 마이그레이션이 끝난 후 서버를 재시작하십시오.

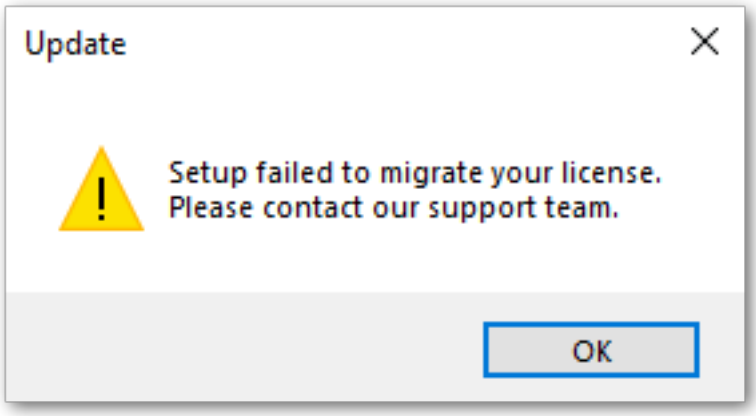
- 완료되면, **서버를 재시작하십시오** 업데이트를 완료하려면.

관리자 도구를 시작합니다. 축하합니다, 이제 버전 19에 있습니다.



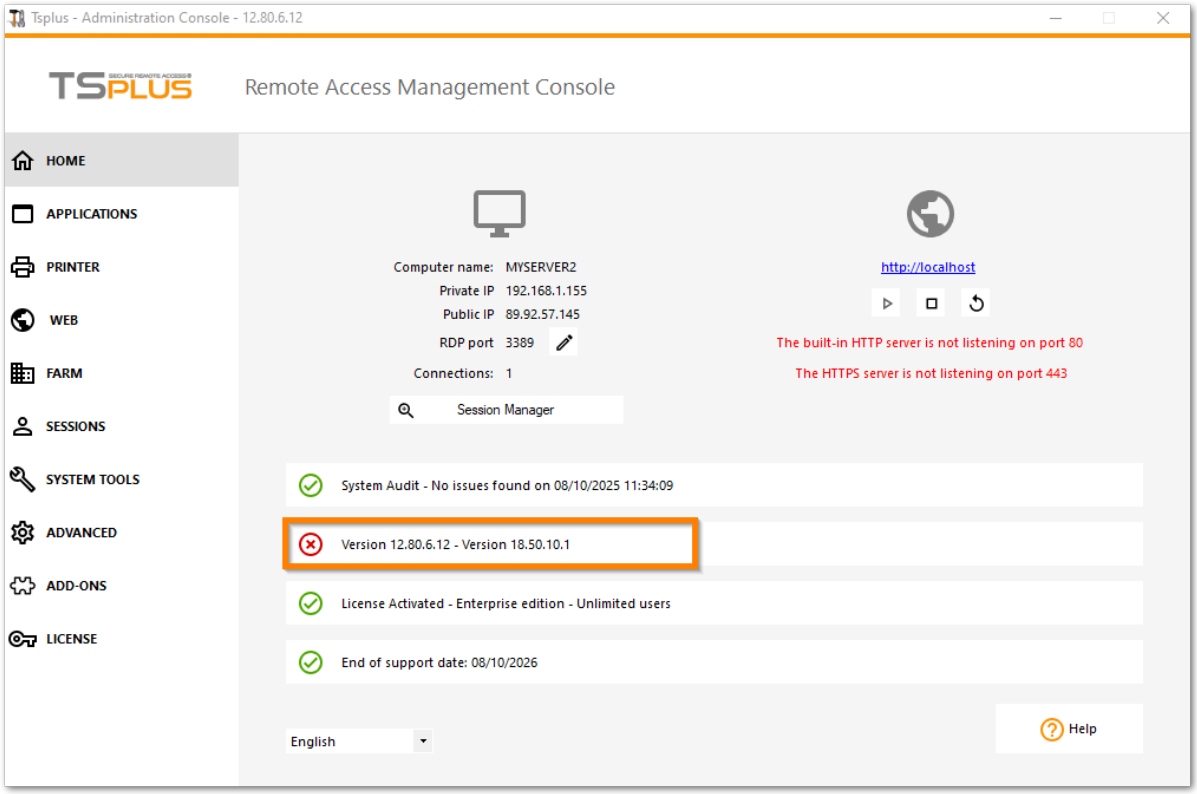
오류 메시지 v10

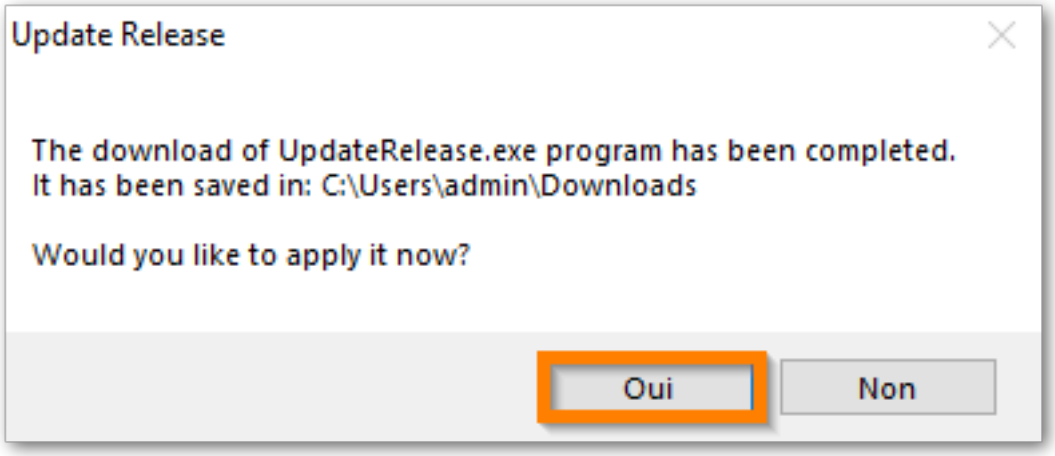
이 오류 메시지를 받으면,
지원 문의
원격 액세스를 제거하려면 라이센스 번호를 PXX XXX XXX 형식으로 제공해 주시고, 지원 구매 인보이스의 증명도 함께 제출해 주시기 바랍니다.

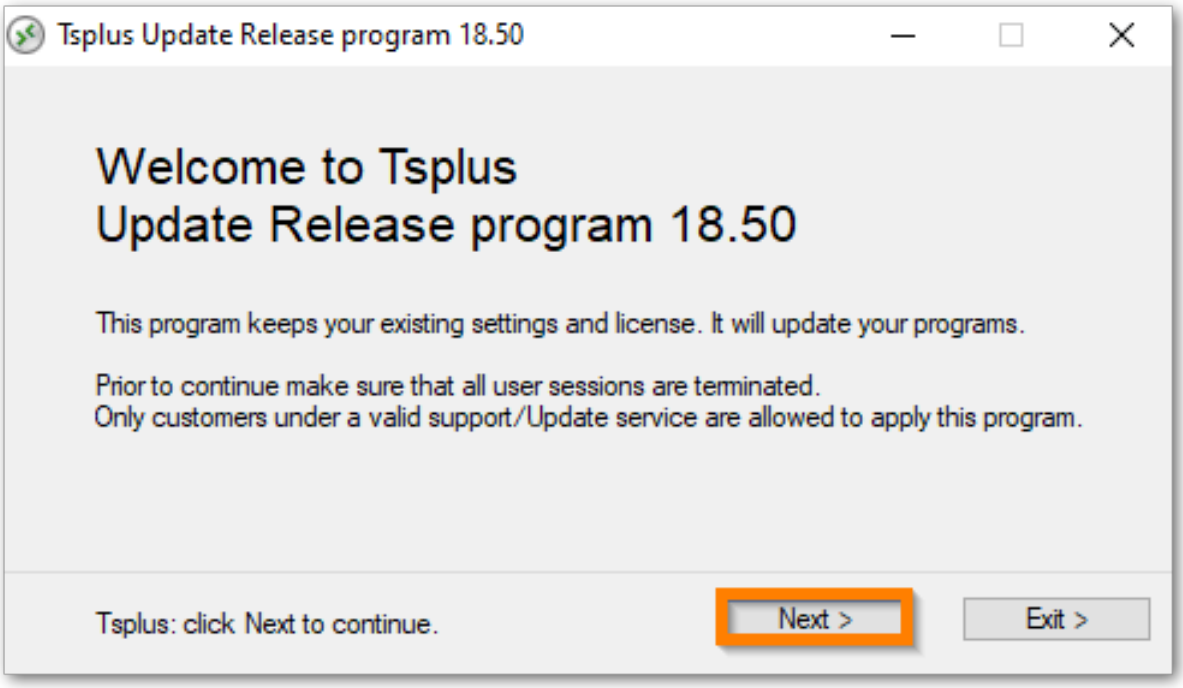


버전 v12 업데이트

온라인 버전 12에서 다음 필드를 클릭하여 다운로드하십시오. **UpdateRelease.exe**
또한 다운로드할 수 있습니다 UpdateRelease.exe 업데이트 절차를 시작하려면.

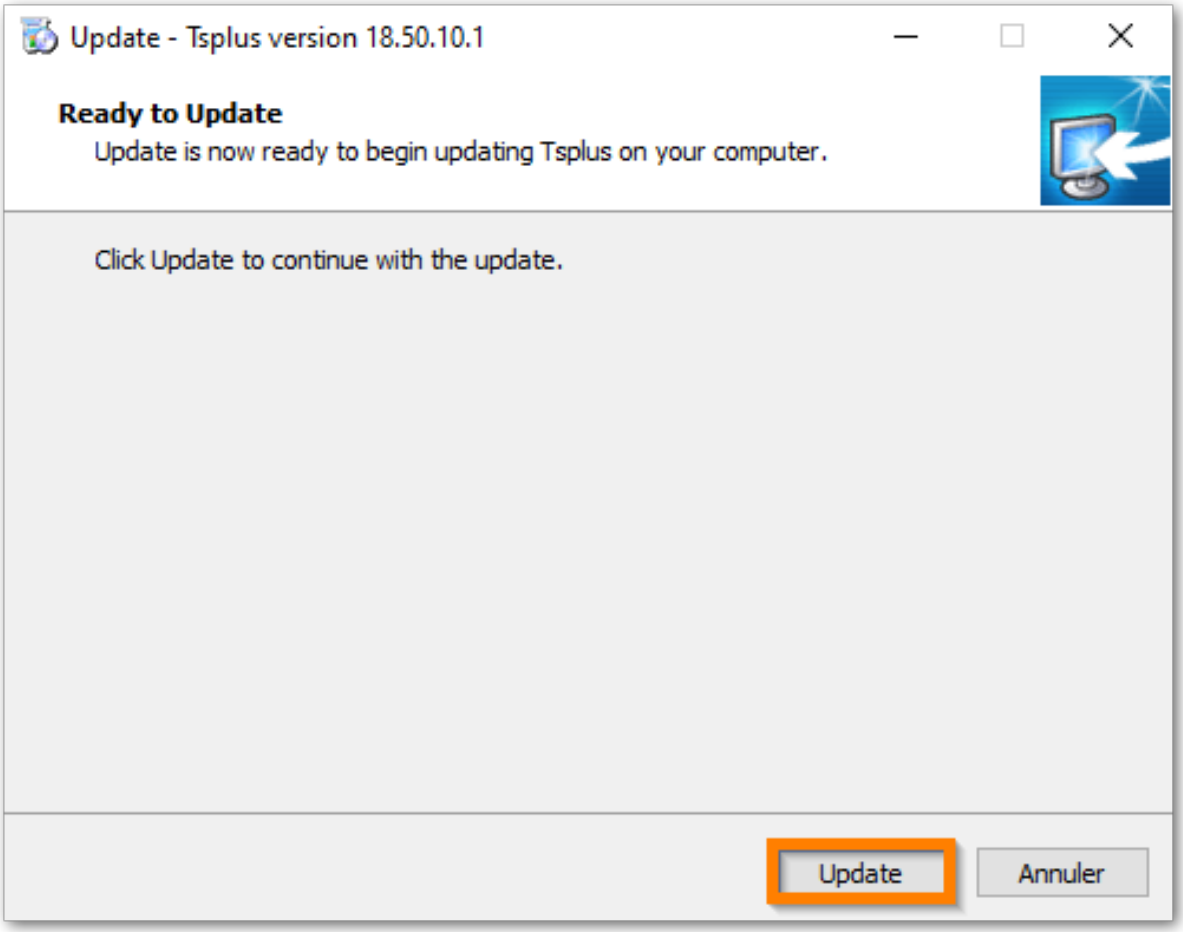

Tsplus - Administration Console - 12.80.6.12
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Computer name: MYSERVER2
Private IP 192.168.1.155
Public IP 89.92.57.145
RDP port 3389
Connections: 1
Session Manager
http://localhost
The built-in HTTP server is not listening on port 80
The HTTPS server is not listening on port 443
System Audit - No issues found on 08/10/2025 11:34:09
Version 12.80.6.12 - Version 18.50.10.1
License Activated - Enterprise edition - Unlimited users
End of support date: 08/10/2026
English
Help

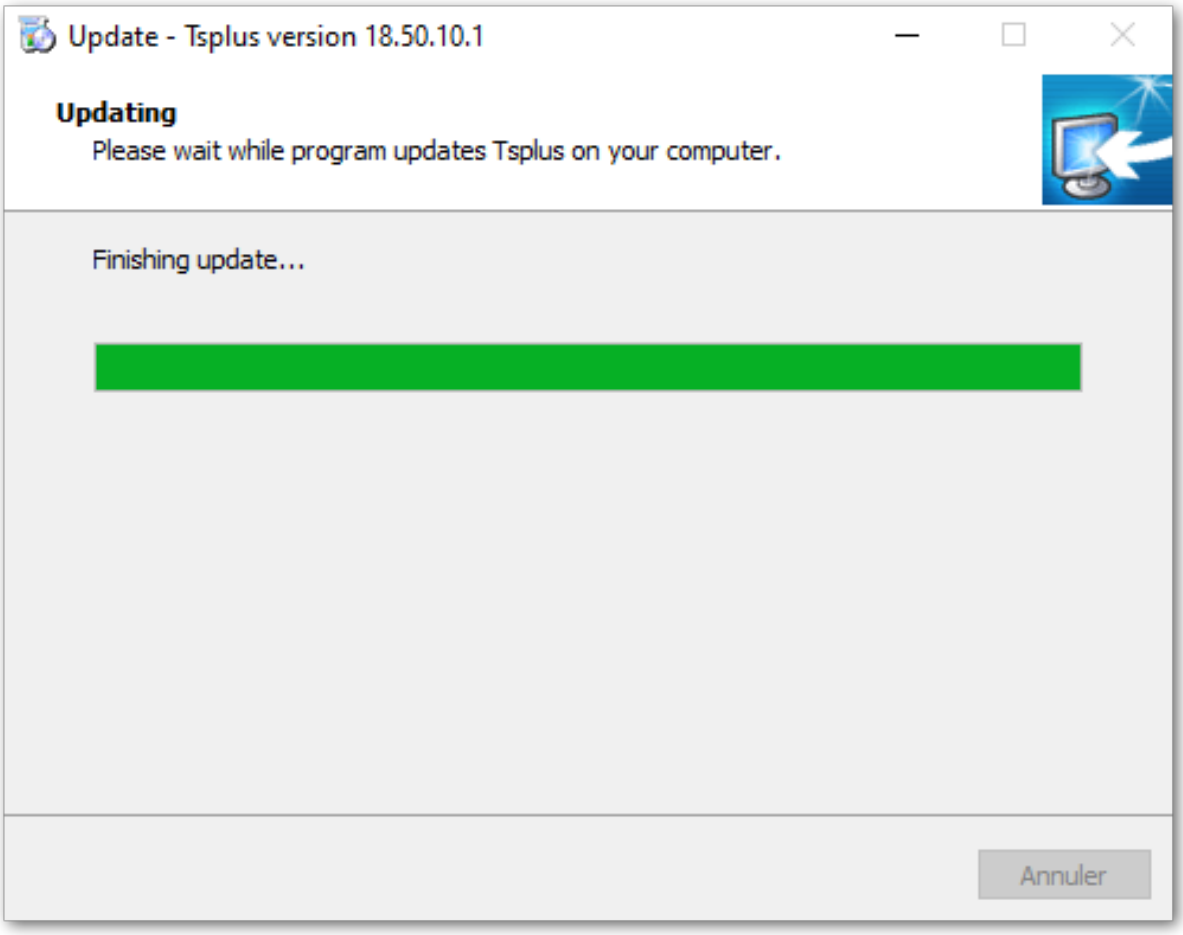

Update Release
The download of UpdateRelease.exe program has been completed.
It has been saved in: C:\Users\admin\Downloads
Would you like to apply it now?
Oui
Non



- 약관에 동의하고 다음을 클릭하세요.

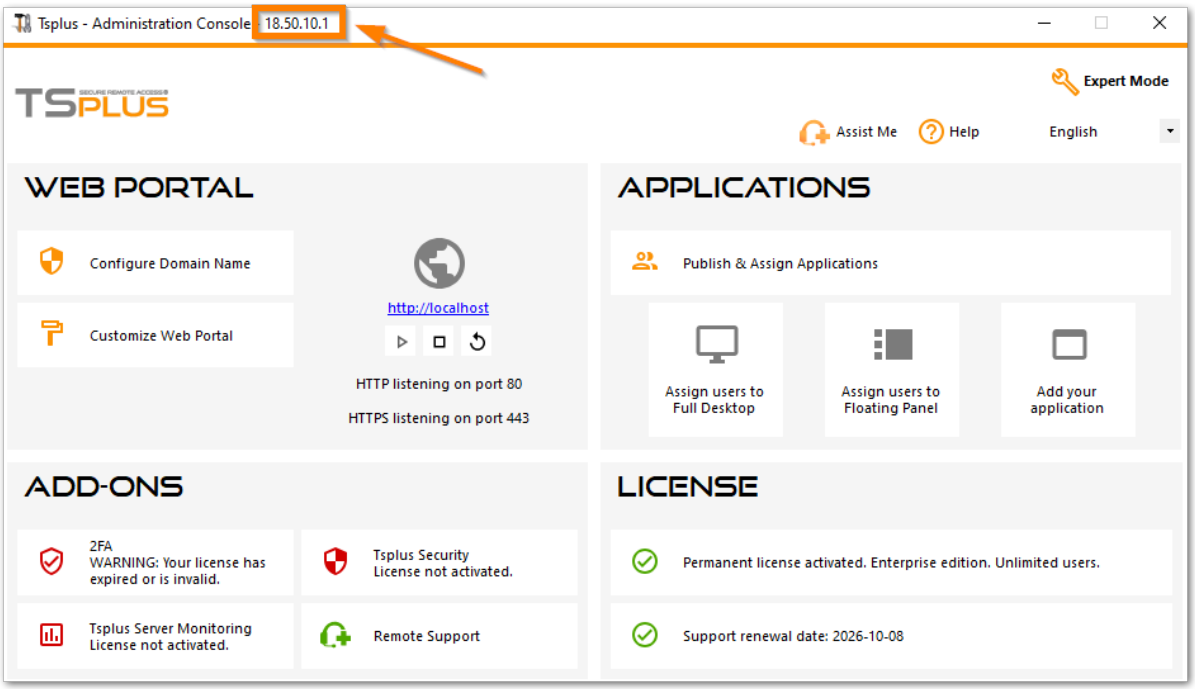
다운로드가 완료되면 클릭하십시오.
업데이트
프로세스를 시작하려면.





- 완료되면, **서버를 재시작하십시오** 업데이트를 완료하려면.

관리자 도구를 시작합니다. 축하합니다, 이제 버전 19에 있습니다.



오류 메시지 v12

이 오류 메시지를 받으면, 지원 문의 원격 액세스를 제거하려면.
라이센스 번호를 PXX XXX XXX 형식으로 제공해 주시고, 지원 구매 인보이스의 증명도 함께 제출해 주시기 바랍니다.

HTTPS 프로토콜 강제 적용

표준 케이스

Terminal Service Plus 버전 9.20부터 HTTP를 사용하는 모든 웹 요청을 HTTPS 보안 프로토콜로 리디렉션할 수 있습니다.

서버에서 이 기능을 활성화하려면 “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” 파일을 편집(또는 생성)하고 다음 줄을 추가하십시오:

disable_http_only=true

파일을 저장하고 Terminal Service Plus 웹 서버를 재시작하십시오 (AdminTool > Web > 웹 서버 재시작 또는 구성 다시 읽기 접근). http://127.0.0.1/w0j3?settings.bin).

이 기능이 활성화되면 다음의 안전하지 않은 웹 페이지로 이동해 볼 수 있습니다:

http://your-server

그리고 요청을 안전한 웹 포털 페이지로 자동으로 리디렉션합니다:

https://your-server

특수 사례: 사용자 정의 웹 포트

HTTPS를 제공하기 위해 특정 포트를 사용하고 있다면, “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” 파일을 수정하고 위에 설명된 줄 대신 다음 줄을 사용하세요:

disable_http_only=“domain.com:4431”

여기서 domain.com은 귀하의 서버 호스트 이름이고 4431은 귀하의 HTTPS 사용자 지정 포트입니다.

파일을 저장하고 Terminal Service Plus 웹 서버를 재시작하십시오 (AdminTool > Web > 웹 서버 재시작).

이 기능이 활성화되면 다음의 안전하지 않은 웹 페이지로 이동해 볼 수 있습니다:

http://domain.com

그리고 요청을 안전한 웹 포털 페이지로 자동으로 리디렉션합니다:

https://domain.com:4431

코멘트: 보안이 보장되지 않더라도 http 포트에서 ssl/https를 비활성화하려면 settings.bin 파일을 편집하고 다음을 추가하십시오: disable_ssl_on_http=true, 저장하고 서버를 재시작하십시오.

https에서 http 비활성화

기본적으로 접근이 허용됩니다. https://my-domain.com , https://my-domain.com:80 , http://my-domain.com:443 그래서 포트 443에서 http를 허용하거나 포트 80에서 https를 허용할 수 있으며, 이는 보안에 영향을 미치지 않으며 웹소켓 지원이 불가능할 때 저하된 xhr-연결로 쉽게 되돌릴 수 있게 합니다. 그러나 이를 비활성화하려면 settings.bin 파일을 편집하고 다음 줄을 추가하십시오.

disable_http_on_https=true

그런 다음 Terminal Service Plus 웹 서버를 재시작하십시오 (AdminTool > Web > 웹 서버 재시작 또는 구성 다시 읽기) http://127.0.0.1/w0j3?settings.bin)

HTTPS 시행 및 무료 SSL 인증서 검증

이 HTTPS Enforcement 기능은 우리의 모든 제품과 완벽하게 호환됩니다. 무료 SSL 인증서 기능.

서버에 연결하기 위해 웹 포털 사용을 강제합니다.

터미널 서비스 플러스 버전 6.60부터 mstsc.exe(또는 기타 RDP 클라이언트)를 사용하여 열린/리디렉션된 포트(80 또는 443)를 통해 연결하려는 모든 시도를 차단/비활성화할 수 있습니다.

이 기능은 Terminal Service Plus Web Portal에서만 액세스를 허용하며 포트 80/443에서 다른 RDP 연결을 비활성화합니다.

서버에서 이 기능을 활성화하려면 C:\Program Files (x86)\TSplus\UserDesktop\files\AppControl.ini 파일을 편집하고 다음 변수를 추가/수정하십시오.

보안 RDP 분할기 차단=예

로드 밸런싱

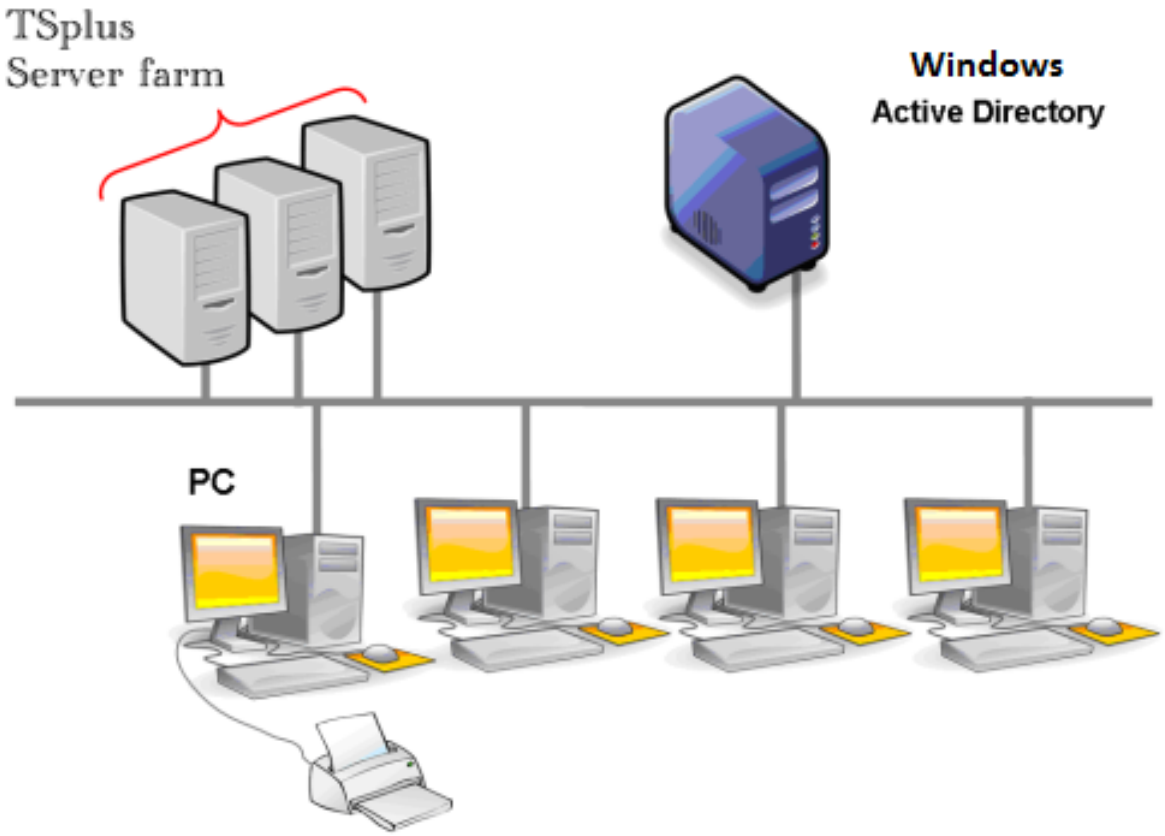
사전 요구 사항

이 기능을 사용하면 로드 밸런스 환경을 관리할 수 있습니다.

모든 사용자의 부하가 귀하의 서버 간에 분산된다는 의미입니다. 작업 부하는 귀하의 팜에 있는 모든 서버 간에 공유됩니다.

로드 밸런싱은 로드 밸런싱을 통해 무제한의 서버를 사용할 수 있게 하며, 엔터프라이즈 에디션(서버당 하나의 유효 라이센스)에서 사용할 수 있습니다. 이 매우 강력하고 고급 기능은 많은 수의 사용자/서버를 배포해야 할 때 사용됩니다.

중요: 로드 밸런싱을 단순히 활성화하면 사용자가 구성된 서버에 관계없이 농장의 가장 덜 로드된 서버로 리디렉션됩니다. 로드 밸런싱과 서버 할당을 모두 사용하려는 경우 "할당된 서버에서 로드 밸런스" 체크박스를 선택해야 합니다.



일반적으로 50명의 동시 사용자를 위해 하나의 서버를 사용하는 것을 권장합니다.
서버의 성능과 사용자의 애플리케이션 리소스 소비에 따라 +50명의 사용자를 초과할 수 있습니다.

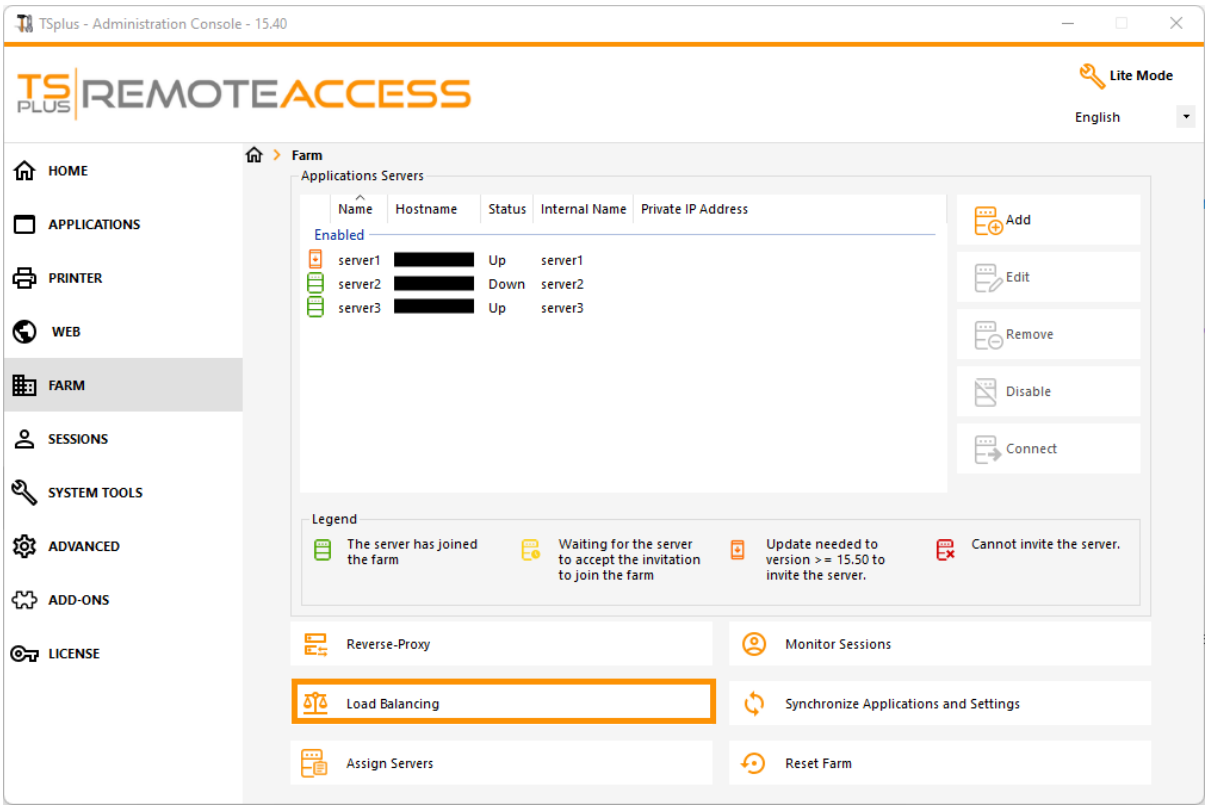
생성된 클라이언트 및 웹 액세스

로드 밸런싱 클러스터에 연결하는 방법은 세 가지가 있습니다:

- 사용하는 **생성된 클라이언트** 실행 가능한 프로그램, 생성된 의해 휴대용 클라이언트 생성기)
- 사용하는 **웹 포털 액세스** 웹 포털 기본 설정 창에서 활성화하여.
- 함께 TSplus 앱 모바일 장치에서.

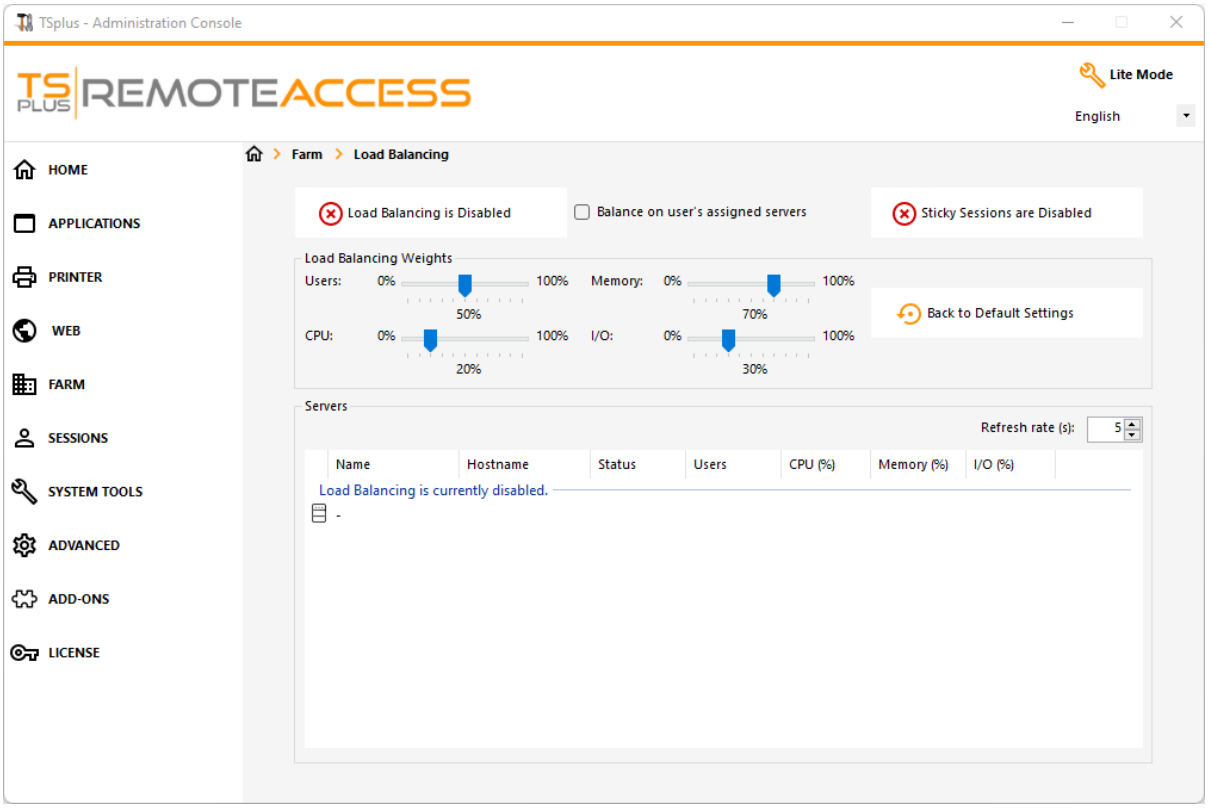
로드 밸런싱 기본 창

로드 밸런싱 관리자는 AdminTool의 Farm 탭에서 찾을 수 있습니다.



이 창에서는 로드 밸런싱을 구성할 수 있습니다. 로드 밸런싱된 서버 팜의 모든 서버가 나열되며, 로드 밸런싱을 활성화, 비활성화 및 구성할 수 있습니다(자세한 내용은 아래 참조).

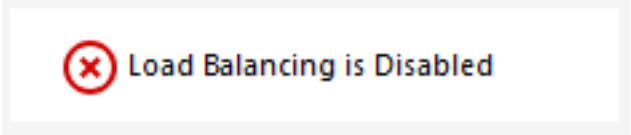
아래 그림의 버튼을 클릭하여 해당 정보를 확인하세요:



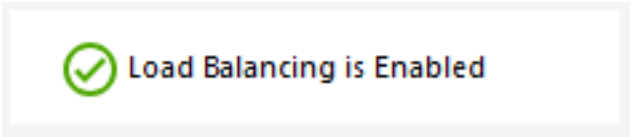
로드 밸런싱 창 상단에 큰 버튼이 표시됩니다:

- 이 버튼은 로드 밸런싱의 현재 상태를 표시합니다.
- 클릭하면 현재 상태에 따라 로드 밸런싱을 활성화하거나 비활성화합니다.

로드 밸런싱이 활성화되었을 때의 버튼입니다. **비활성화됨** 클릭하면 활성화됩니다.



로드 밸런싱이 활성화되었을 때의 버튼입니다. **활성화됨** 클릭하면 비활성화됩니다.



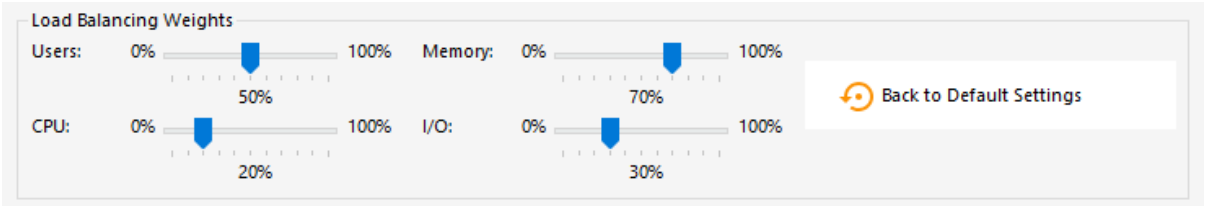
로드 밸런싱은 서버를 어떻게 선택하나요?

부하 분산이 활성화되면 사용자는 연결 시점에 덜 부하가 걸린 서버로 전송됩니다.

서버의 부하가 가장 적은 서버를 결정하기 위해, 여러 성능 지표 간의 가중 평균을 사용하여 각 서버의 부하를 계산합니다.

- 연결된 사용자 수
- 프로세서 사용량
- 메모리 사용량
- 디스크 사용량

이 지표의 가중치(중요도)를 다음 슬라이더를 사용하여 수정할 수 있습니다:



이 슬라이더를 사용하면 로드 밸런싱을 미세 조정하고 자신의 요구에 맞게 최적화할 수 있습니다. 예를 들어, 사용자가 큰 메모리 요구 사항이 있는 비즈니스 애플리케이션을 실행하는 경우 "메모리" 슬라이더를 사용하여 로드 계산에서 RAM의 영향을 증가시키는 것이 좋습니다.

이 값을 "기본 설정으로 돌아가기" 버튼을 클릭하여 재설정할 수도 있습니다.

서버의 부하 계산은 어떻게 이루어지나요?

각 서버의 부하는 사용자를 어떤 서버로 보낼지 결정하기 위해 필요할 때 계산됩니다.

이 계산을 위해 우리는 a를 사용합니다. **가중 평균** 4개의 하드웨어 메트릭스 사이.

4개의 슬라이더를 사용하여 이러한 각 지표에 더 많은 (또는 더 적은) 비중을 부여할 수 있습니다.

- 사용자 : 연결된 사용자 수
- CPU : 비활성 프로세서 시간의 비율
- 메모리 : 사용된 메모리의 비율
- I/O : 비활성 디스크 시간의 비율

예를 들어, "메모리" 슬라이더를 오른쪽에 두고 다른 모든 슬라이더를 왼쪽에 두면 각 서버의 부하는 사용된 메모리의 비율만을 거의 사용하여 계산됩니다. 그리고 귀하의 사용자는 가장 많은 사용 가능한 메모리가 있는 서버로 전송됩니다.

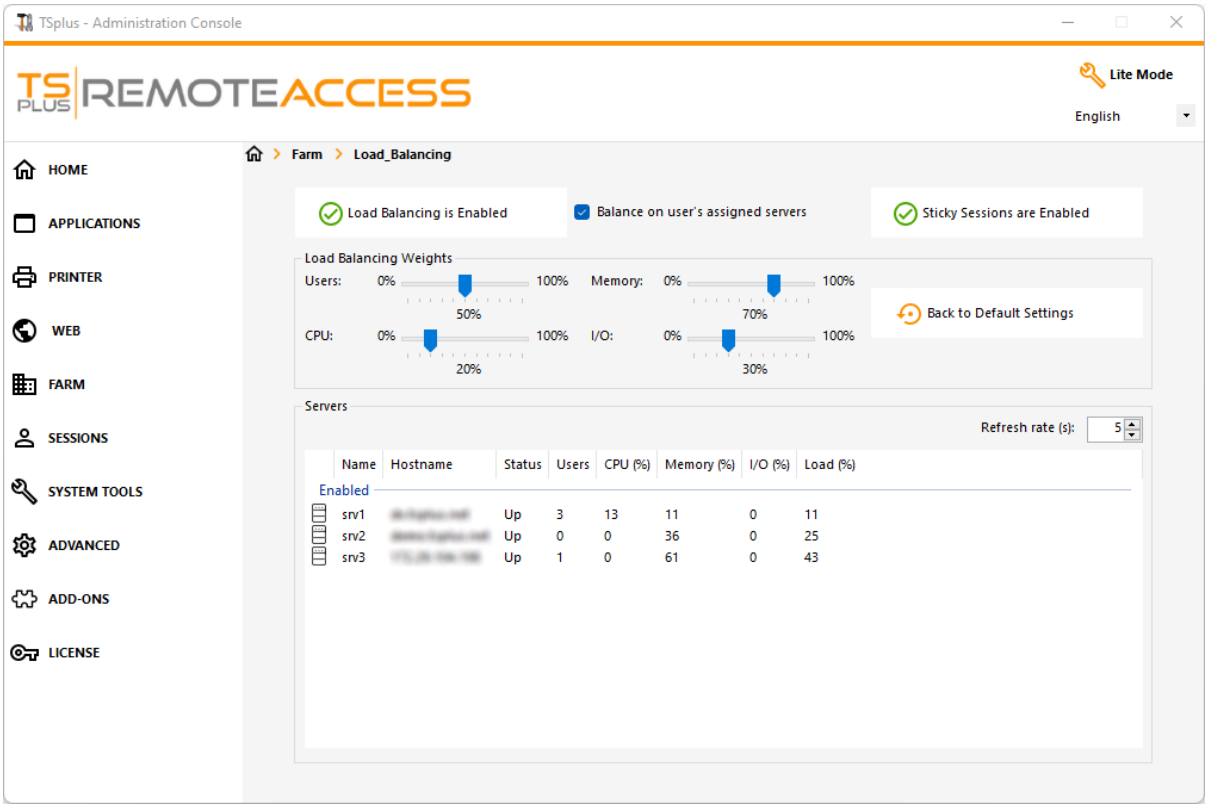
- 슬라이더가 완전히 왼쪽에 있을 때, 하중 계산에 사용되는 무게는 1이 됩니다.
- 슬라이더가 완전히 왼쪽에 있을 때, 하중 계산에 사용되는 무게는 100이 됩니다.

또한, 특정 서버의 부하는 [사용된 자원 / 총 자원] 비율에 따라 달라집니다; 따라서 서버 A가 서버 B보다 두 배 더 강력하다면, 서버 A에는 서버 B보다 두 배 더 많은 사용자가 전송되어야 합니다 (모든 다른 조건이 동일할 경우).

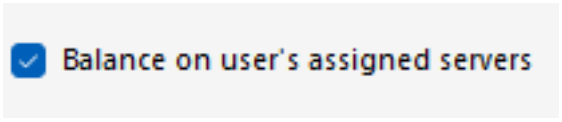
로드 밸런스 서버 상태 목록과 각 서버의 성능 지표에 대한 세부 정보를 확인할 수 있습니다.

서버는 귀하의 구성에 따라 덜 부하가 걸린 것부터 가장 부하가 걸린 것까지 정렬됩니다.

로드 밸런스 서버 상태 목록은 자동으로 새로 고쳐집니다. 이 자동 새로 고침은 연결이 사용할 수 없게 되면 중지됩니다. "서버" 상자의 오른쪽 상단에서 새로 고침 속도를 변경할 수 있습니다.



로드 밸런싱은 사용자가 할당된 서버에서 직접 수행할 수도 있습니다. **사용자가 할당된 서버에서 균형 조정** .
결과적으로, 이러한 특정 서버가 회계 사용자에게 할당되면 회계 부서 서버에서 회계 사용자만을 위한 로드 밸런싱을 수행할 수 있습니다.



로드 밸런싱 창의 오른쪽 버튼을 클릭하여 스티키 세션 기능을 활성화할 수 있습니다.



활성화 **기존 세션 웹 목록** 로드 밸런싱 스티키 세션 기능에 필요합니다.

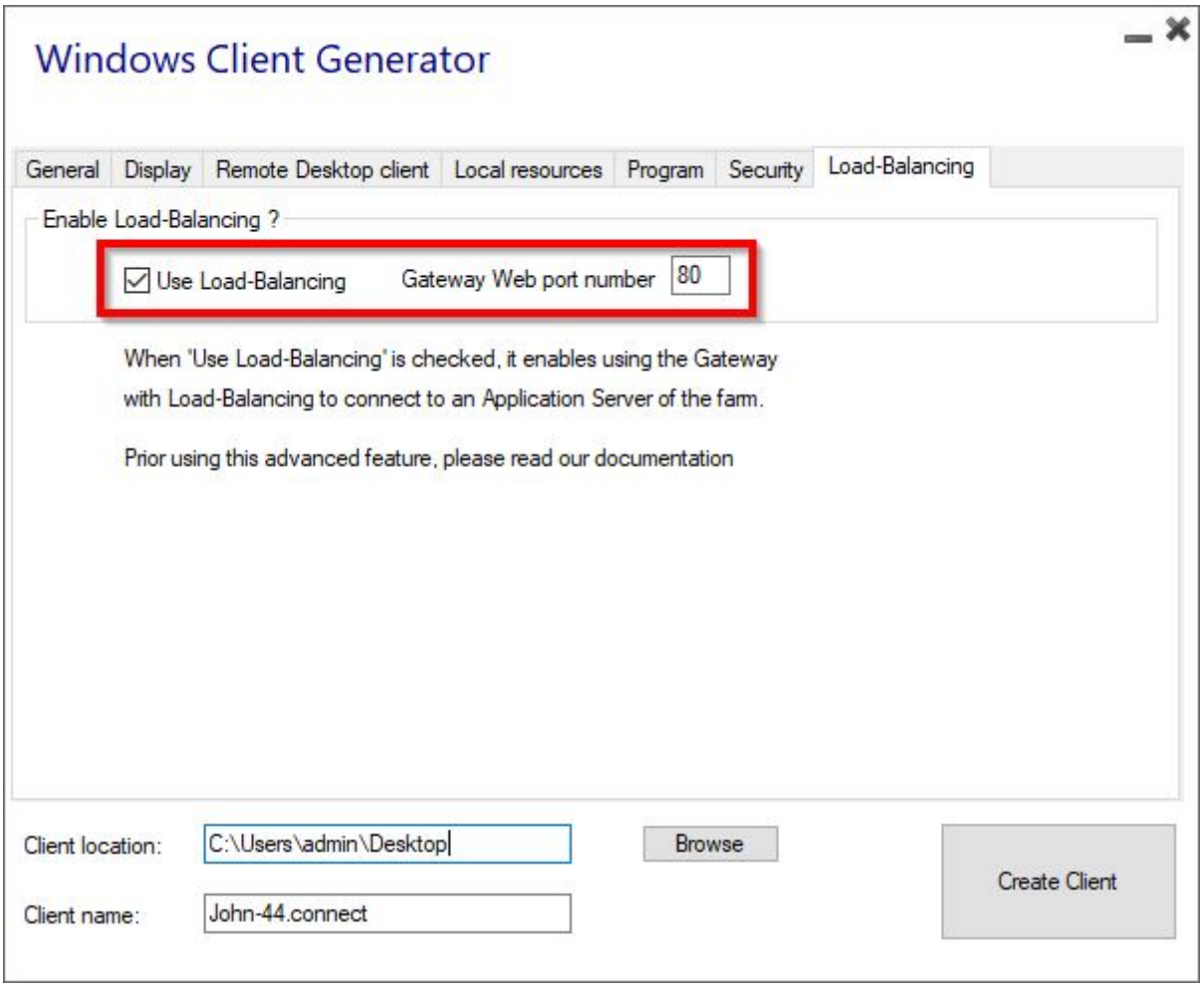
연결이 끊어진 세션에 재연결할 수 있도록 하여 다른 서버에서 새 세션을 여는 대신 사용할 수 있습니다.

활성화하려면 **기존 세션 웹 목록** 다음 설정을 하십시오. 설정 “아니오”.

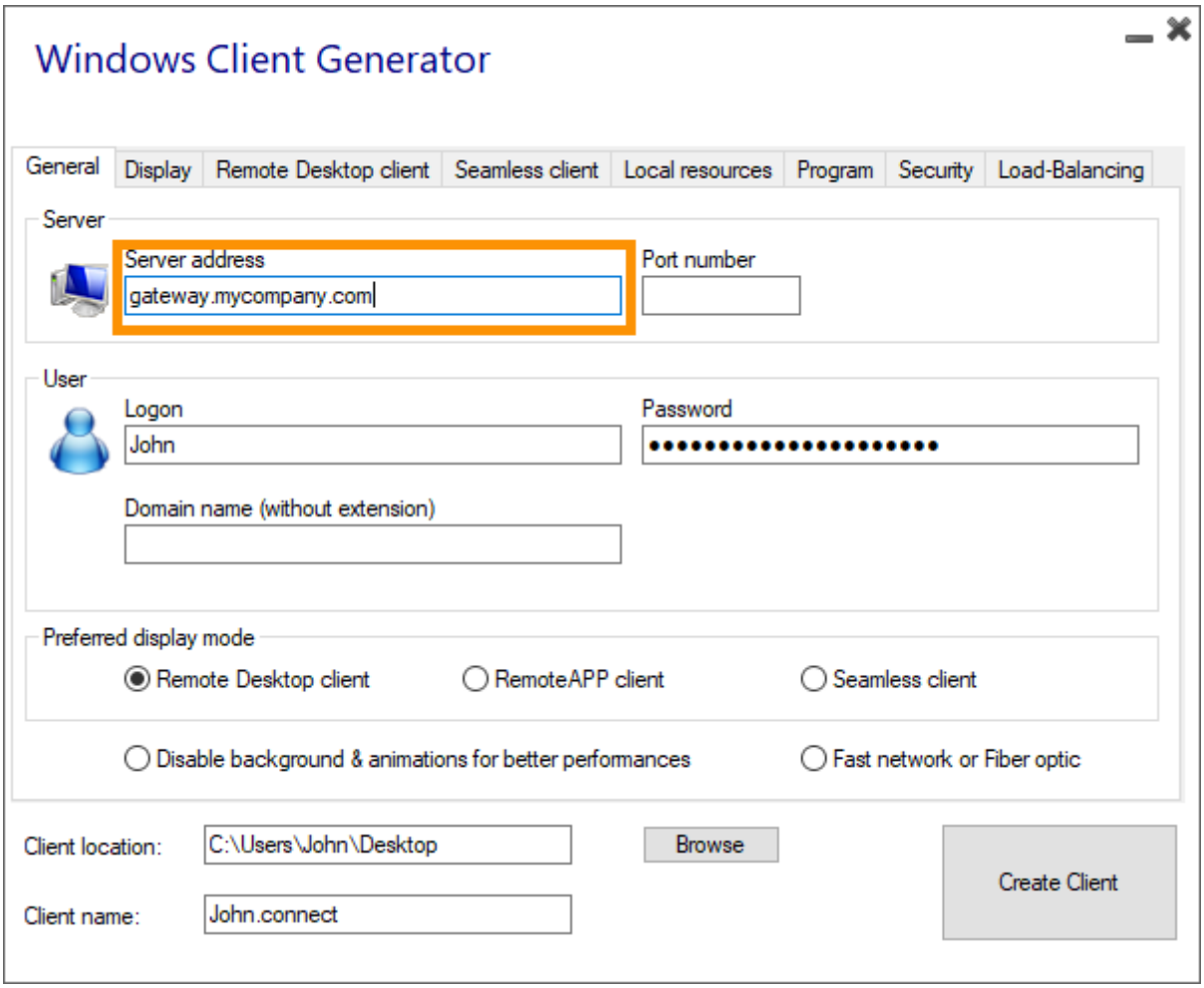
연결 클라이언트를 이용한 로드 밸런싱

생성하고 싶다면 연결 클라이언트 **사용자가 덜 부하가 걸린 서버에 연결하기 위해** 당신은 필요할 것입니다. 클라이언트 생성기 "안에 로드 밸런싱 탭하여:

- "로드 밸런싱 사용" 체크박스를 확인하세요.
- "Gateway Web 포트 번호" 필드에 Gateway Server에서 사용하는 HTTP 또는 HTTPS 포트를 입력하십시오.



- 게이트웨이 서버의 공용 IP 주소 또는 호스트 이름을 "서버" 필드에 직접 사용하십시오.


Windows Client Generator
General
Display
Remote Desktop client
Seamless client
Local resources
Program
Security
Load-Balancing
Server
Server address
gateway.mycompany.com
Port number
User
Logon
John
Password
Domain name (without extension)
Preferred display mode
Remote Desktop client
RemoteAPP client
Seamless client
Disable background & animations for better performances
Fast network or Fiber optic
Client location:
C:\Users\John\Desktop
Browse
Client name:
John.connect
Create Client

농장 관리자 API

서버 팜에 대한 포괄적인 관리 기능을 제공하도록 설계된 강력한 API를 제공하게 되어 기쁩니다.

이 API는 기존 인프라와 소프트웨어를 원활하게 통합할 수 있게 해주며, 사용자 정의 스크립트를 사용하여 서버 작업을 관리하고 자동화할 수 있도록 합니다.

우리의 강력하고 다재다능한 API를 통해 소프트웨어의 모든 잠재력을 발견하세요.

요구 사항

농장 관리자 API를 쿼리하기 위해, 귀하의 서버는 다음이 필요합니다:

- 유효한 SSL/TLS 인증서를 가지고 있습니다.
- 포트 19956에서 열려야 합니다.
- 귀하의 인증서가 적용되는 도메인을 사용하여 연락할 수 있습니다.

사용 예시

예를 들어, 관리자는 사용할 수 있습니다. `농장 > 서버 목록 가져오기` 모든 서버의 포괄적인 목록을 검색하는 기능으로, 재고 관리를 간소화합니다. `농장 > 농장 초기화` 기능은 새로운 서버 팜의 빠른 설정을 가능하게 하여 원활한 배포 프로세스를 보장합니다. 사용자별 서버 관리를 위해, `사용자에게 할당된 서버 목록` 기능은 서버 할당을 추적하고 관리하는 데 도움이 됩니다.

부하 분산 시나리오에서, the `로드 밸런싱 > 서버 선택` 그리고 `로드 밸런싱 > 다시 로드` 기능은 동적 서버 선택 및 로드 밸런서 구성의 재로드를 가능하게 하여 리소스 분배 및 성능을 최적화합니다. `리버스 프록시 > 새로 고침` 기능은 프록시 설정에 대한 변경 사항이 다운타임 없이 적용되도록 보장합니다. 또한, `서버 > 추가` 그리고 `서버 > 편집` 기능은 농장에서 서버의 원활한 추가 및 수정을 용이하게 합니다.

관리자는 이를 활용하여 운영을 더욱 향상시킬 수 있습니다. `설정 > 목록 설정` 그리고 `설정 > 설정 적용` 서버 팜 전반에 걸쳐 구성 설정을 검색하고 적용하는 기능.

세션 관리를 위해, `세션 > 연결 끊기` 그리고 `세션 > 로그오프` 기능은 사용자 세션의 제어된 종료를 허용합니다. `세션 > 사용자 세션 목록` 활동 세션에 대한 자세한 보기를 제공하여 모니터링 목적으로 사용합니다.

이 강력한 API 기능을 활용함으로써 서버 관리 프로세스의 자동화, 효율성 및 제어를 더욱 향상시켜 인프라의 최적 성능과 신뢰성을 보장할 수 있습니다.

문서화

이 API의 전체 문서는 여기에서 찾을 수 있습니다 : API 문서

개요

개요 및 명명

TSplus Farm 기능의 목표는 관리자가 단일 서버에서 모든 TSPlus 서버를 관리할 수 있도록 하는 것입니다. 이 서버는 다음과 같이 언급될 수 있습니다. **농장 제어기** .

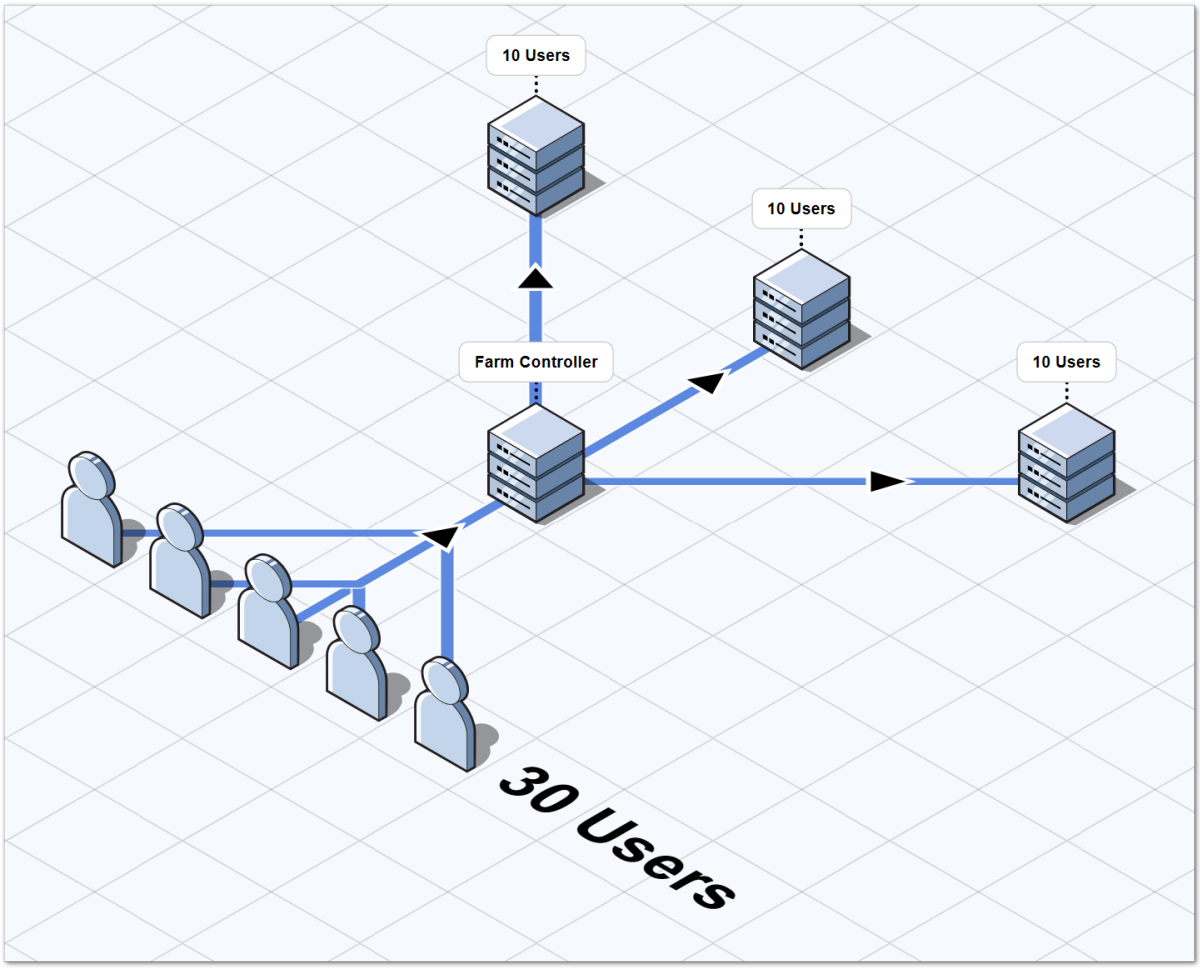
Farm의 TSplus 서버는 다음과 같이 명명됩니다. **애플리케이션 서버** 서버.

이 농장 컨트롤러는 애플리케이션 서버로 농장이 채워지면 또한 하나의가 될 것입니다. **게이트웨이 서버** 농장 기능 중 하나라도 활성화하면 다음과 같은:

- Load balancing
- 리버스 프록시
- 서버 할당

이 게이트웨이 서버는 기본적으로 "로드 밸런싱" 또는 "서버 할당"이 활성화될 때 모든 사용자의 주요 진입점이 됩니다.

마지막으로, 이 Farm Controller는 애플리케이션 서버를 모니터링하고, Farm Controller에서 애플리케이션 및 고급 설정과 같은 TSplus 관련 설정을 애플리케이션 서버로 쉽게 전송할 수 있도록 해줍니다.



TSplus 서버 아키텍처 농장

TSplus 서버 팜을 배포하는 두 가지 옵션이 있습니다:

옵션 1 모든 서버는 공인 IP 주소를 가지고 있으며 인터넷에서 접근할 수 있습니다.

또는

옵션 2 인터넷에서 접근할 수 있는 것은 오직 게이트웨이 포털뿐입니다. 게이트웨이 서버는 "리버스 프록시 역할"을 제공하고 있습니다.

두 가지 옵션 모두:

- 모든 서버는 동일한 TSplus 구성을 가지고 있습니다.
- 모든 서버는 동일한 HTTP/HTTPS 포트를 가지고 있습니다.
- 새로운 애플리케이션을 게시하려면 AdminTool에서 사용자/사용자 그룹에 추가하기만 하면 됩니다.

물론, 이 애플리케이션이 대상 애플리케이션 서버에 설치되어 있는지 확인하세요.

모든 웹 액세스 유형은 특정 구성 없이 사용할 수 있습니다: RemoteApp 및 HTML5 클라이언트.

옵션 1 - 모든 서버는 고유한 공인 IP 주소를 가지고 있으며 인터넷에서 접근할 수 있습니다.

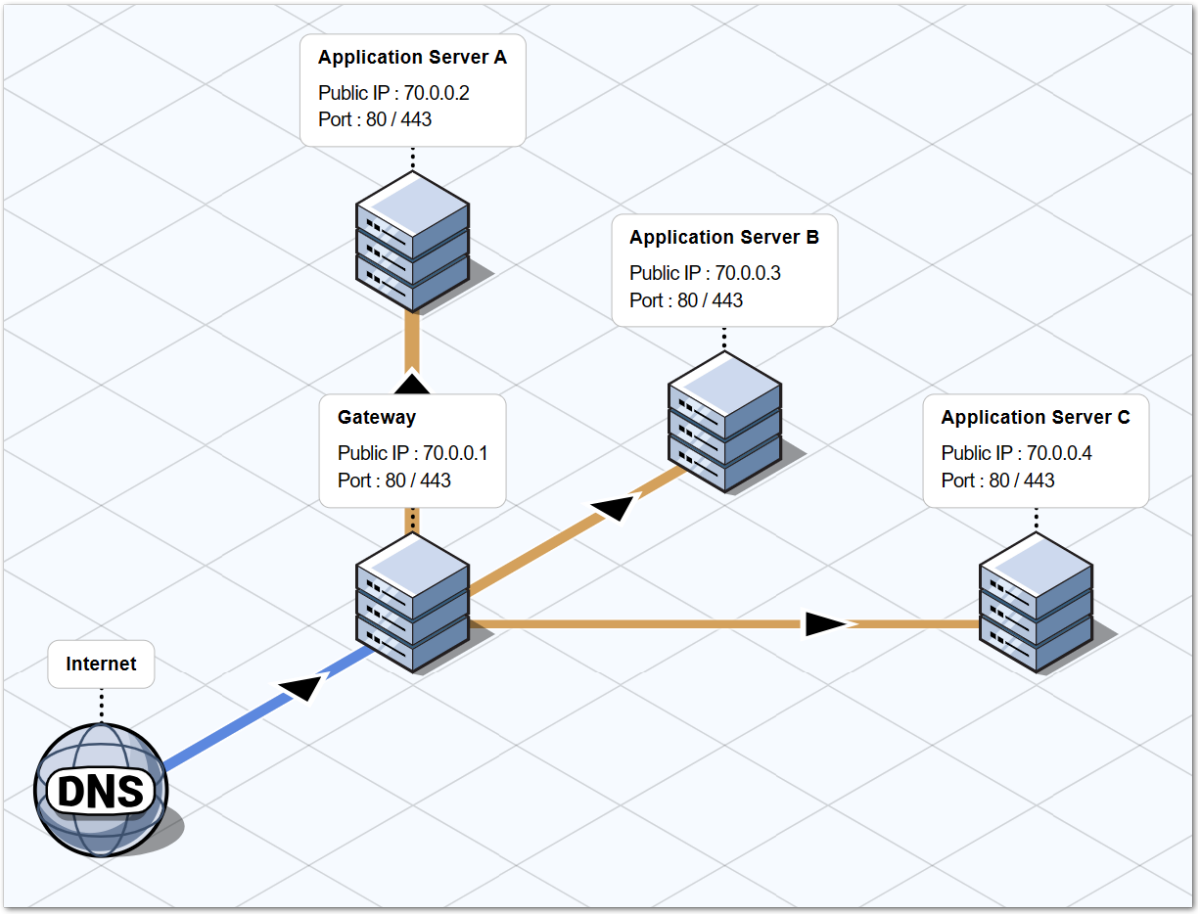
이것은 Terminal Service Plus Gateway를 사용하는 데 권장되는 아키텍처입니다.

이 아키텍처는 모범 사례를 따르며 IT 관리자가 환경을 산업화할 수 있도록 합니다.

- 모든 서버는 동일한 Terminal Service Plus 구성을 가지고 있습니다.
- 모든 서버는 동일한 HTTP/HTTPS 포트를 가지고 있습니다.
- 새로운 애플리케이션 서버를 배포하는 것은 몇 분이면 충분합니다(단지 게이트웨이 서버의 AdminTool에서 서버를 팜에 추가하기만 하면 됩니다).

이 아키텍처를 사용하면 특정 구성 없이 모든 액세스 유형을 사용할 수 있습니다: Remoteapp 및 HTML5 클라이언트.

이 아키텍처는 아래 다이어그램에 설명되어 있습니다.



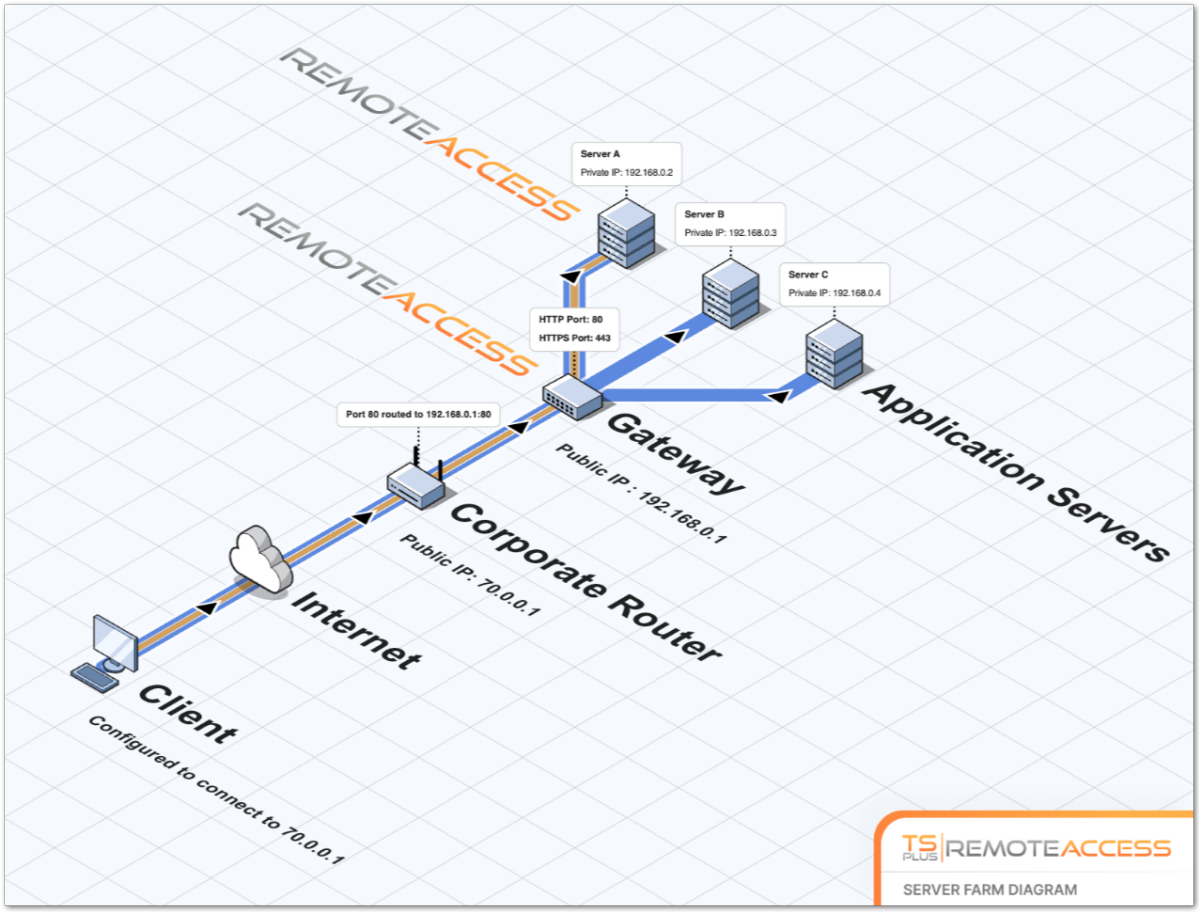
-
-
  -

옵션 2: 인터넷에서 접근할 수 있는 것은 Gateway Portal 뿐이며 "리버스 프록시 역할"이 포함됩니다.

Terminal Service Plus Gateway는 1개의 공인 IP 주소만으로도 설정할 수 있습니다.

게이트웨이는 모든 외부 연결 요청을 사용 가능한 서버로 리디렉션합니다. 부하 분산 기능을 사용하지 않으면 사용자는 할당된 서버에 연결됩니다.

이 아키텍처는 아래 다이어그램에 설명되어 있습니다.



리버스 프록시 역할에 대한 자세한 내용은 다음을 참조하십시오. 리버스 프록시 기능 문서 .

릴리스 역사

- API 1.5 (TSplus 15.50과 함께 출시됨)
  - 통합 리버스 프록시, 로드 밸런싱 및 애플리케이션 서버 할당 구성
  - 응용 프로그램/설정 간의 동기화가 농장 컨트롤러와 모든 응용 프로그램 서버 간에 추가되었습니다.

- API 1.4 (TSplus 10.10과 함께 출시됨)
  - 로드 밸런싱 중앙 집중 모니터링
  - TSplus 로드 밸런싱 관리자에서 서버 활성화/비활성화
  - 다국어 번역 (TSplus 언어가 사용됩니다)
  - 여러 설정 추가 + 표시 버그 수정됨

- API 1.3 (TSplus 9.70과 함께 출시됨)
  - 설정 중앙 집중 모니터링 및 관리 (전역 설정 / 플로팅 패널 / RemoteApp 클라이언트 / HTML5 클라이언트)

- API 1.2 (TSplus 9.60과 함께 출시됨)
  - 농장 관리자
  - 서버 중앙 집중 관리 (추가/제거)
  - 세션 중앙 집중 모니터링 및 관리 (메시지/연결 끊기/로그오프)

- API 1.1 (TSplus 9.30과 함께 출시됨)
  - 로드 밸런싱 내부
  - 로드 밸런싱 스티키 세션

필수 조건

하드웨어 요구 사항

농장 컨트롤러 및 애플리케이션 서버는 표준입니다. 터미널 서비스 플러스 요구 사항 하드웨어 용.

운영 체제 요구 사항

농장 컨트롤러 및 애플리케이션 서버는 다음 운영 체제 중 하나를 사용해야 합니다:

- 윈도우 **7 프로**
- 윈도우 **8/8.1 프로**
- 윈도우 **10 프로**
- 윈도우 **11 프로**
- 윈도우 **서버 2008 SP2/스몰 비즈니스 서버 SP2 또는 2008 R2 SP1**
- 윈도우 **서버 2012 또는 2012 R2**
- 윈도우 **서버 2016**
- 윈도우 **서버 2019**
- 윈도우 **서버 2022**
- 윈도우 **서버 2025**

32비트와 64비트 아키텍처가 모두 지원됩니다.

네트워크 요구 사항

모든 애플리케이션 서버는 팜 컨트롤러에서 접근 가능해야 합니다.

보다 구체적으로, Farm Controller는 API 포트(기본값 19955)의 모든 Application Server에 요청을 발행하며, 이 포트는 Farm Controller와 Application Servers 사이에 있는 방화벽에서 열려 있어야 합니다.

Farm Controller와 Application Servers 간의 네트워크 지연 시간은 낮아야 합니다. 200 ms 이하의 지연 시간이 권장되며, 2,000 ms 이하의 지연 시간이 필요합니다.

소프트웨어 요구 사항

.NET 2.0 이상이 필요합니다 - 이는 Terminal Service Plus Farm을 지원하는 모든 운영 체제에서 기본적으로 호환 가능한 .NET 버전이 활성화되어 있으므로 문제가 되지 않아야 합니다.

터미널 서비스 플러스 라이센스 및 버전 요구 사항

Terminal Service Plus는 Farm Controller와 모든 Application Server에서 "Enterprise" 에디션이어야 합니다.

모든 서버는 또한 동일한 버전의 Terminal Service Plus를 실행해야 합니다.

구성 요구 사항

농장 컨트롤러와 애플리케이션 서버는 동일한 날짜/시간이 설정되어 있어야 합니다. 이미 설정되지 않았다면 모든 서버의 Windows 시계를 인터넷 시간 서버와 동기화하는 것이 강력히 권장됩니다.

사용자 요구 사항

Active Directory는 **아니다** 필수적이지만, Active Directory가 있는 경우 도메인 관리자는 Terminal Service Plus Farm Manager를 사용하기 위해 Farm Controller의 로컬 관리자여야 합니다.

리버스 프록시

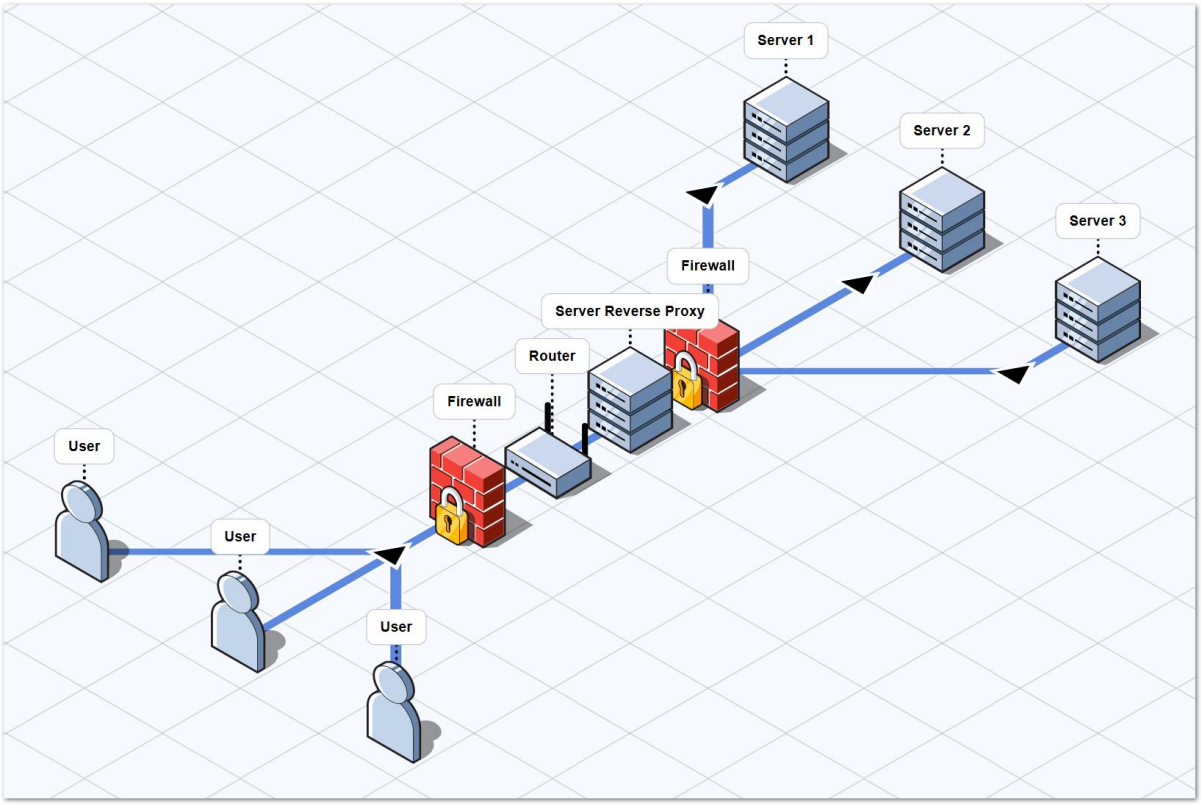
개요

이 기능은 TSplus Enterprise Edition에서 사용할 수 있습니다.

리버스 프록시 시스템은 관련 서버가 모든 클라이언트에 의해 연락받을 수 있도록 중개 역할을 합니다.

리버스 프록시를 사용하는 장점은 간단합니다: TSplus 서버 수만큼 포트 리디렉션 규칙을 생성할 필요가 없습니다.

로드 밸런싱 기능을 사용하든 사용하지 않든, 리버스 프록시를 사용하여 연결하려면 이를 활성화해야 합니다. TSplus에서는 로드 밸런싱된 TSplus 서버 농장에 대한 고유한 액세스 지점을 제공합니다.

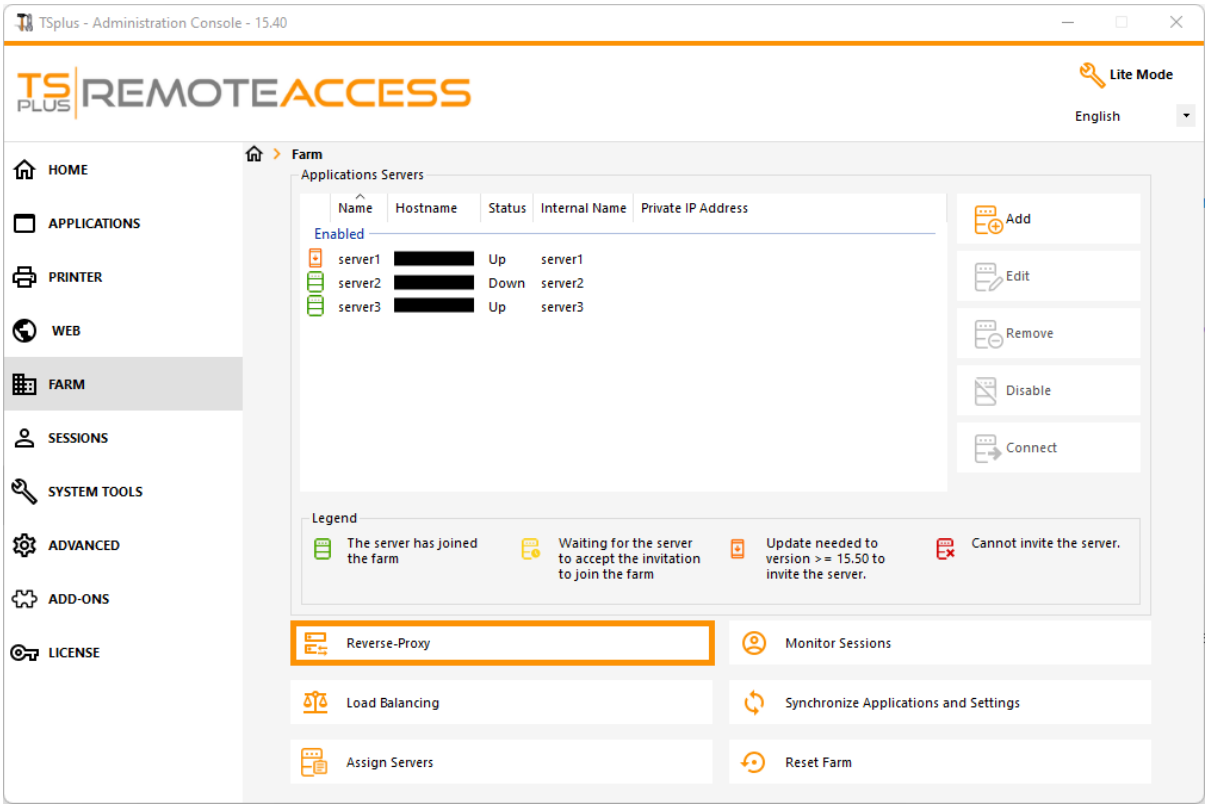


이 독특한 액세스 포인트는 귀하의 게이트웨이 서버 TSplus 웹 포털이 될 것입니다.

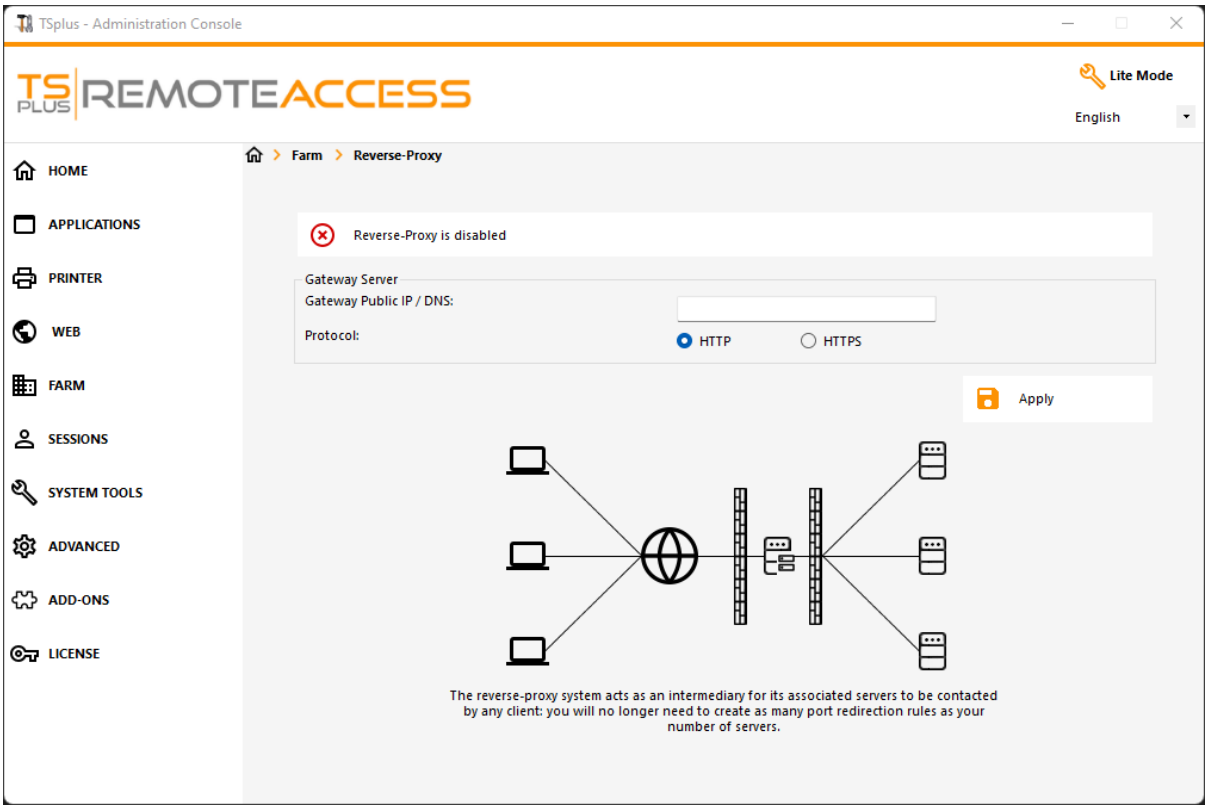
이 서버에 원격으로 접근할 예정이므로, 라우터에서 하나의 포트 리디렉션 규칙을 설정해야 합니다. 이는 선호에 따라 http 또는 https 포트를 포함해야 하며(기본 포트는 http의 경우 80, https의 경우 443입니다).

구성

FARM 탭을 통해 Reverse Proxy 구성 인터페이스에 접근할 수 있습니다.



리버스 프록시 버튼을 클릭하세요.



- “리버스 프록시 비활성화” 버튼을 클릭하여 활성화하십시오.

- 게이트웨이 공용 IP는 고정된 유효한 IP 주소 또는 도메인 이름으로 설정해야 합니다.

- HTTP 또는 HTTPS를 선택하여 선호하는 연결 방법을 설정하십시오. 귀하의 팜 서버는 사용 중인 연결 방법에 따라 포트 80 또는 443에서 서로 통신할 수 있어야 합니다. 또한 Windows 방화벽이 이러한 포트를 차단하지 않도록 하는 것이 중요합니다.

구성을 완료한 후 "적용"을 클릭하여 이러한 리버스 프록시 설정을 저장하십시오.

게이트웨이 서버를 통한 애플리케이션 서버 접근

한 번 활성화되고 작동하면, 리버스 프록시 기능을 사용하여 다음과 같이 형식화된 특별한 URL을 사용하여 애플리케이션 서버에 접근할 수 있습니다:
1 :// **2** : **3** /~~ **4**
함께:

- (1): 구성된 리버스 프록시 프로토콜
- 게이트웨이 서버의 공용 IP 주소 또는 도메인 이름
- (3): 구성된 리버스 프록시 프로토콜과 연결된 게이트웨이 서버 웹 포트
- (4): 리버스 프록시에서 사용하는 애플리케이션 서버의 내부 이름

예를 들어, 가정할 때:

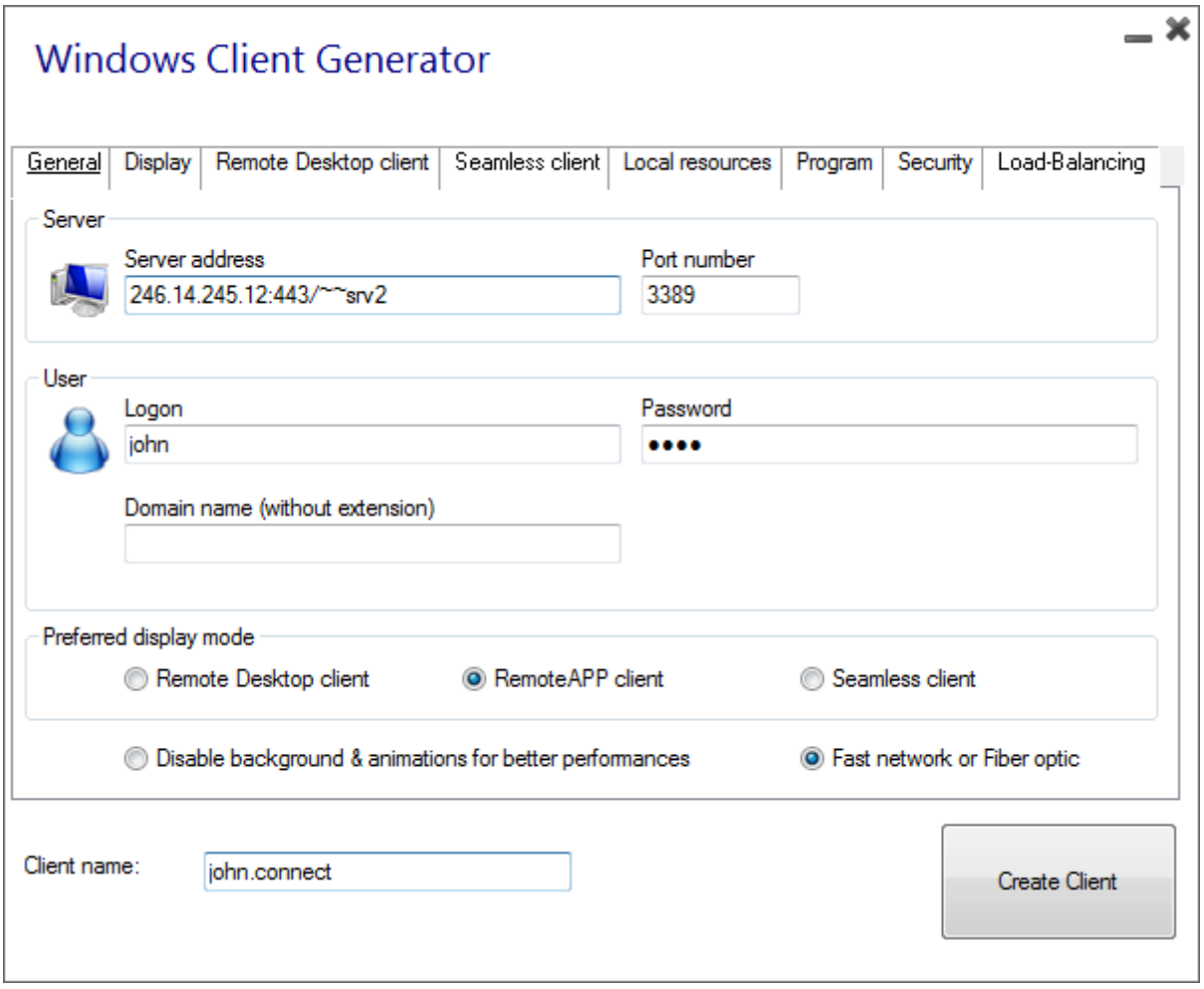
- 구성된 리버스 프록시 프로토콜은 HTTPS입니다.
- 귀하의 게이트웨이 서버는 공용 IP 1.1.1.1을 가지고 있습니다.
- 귀하의 게이트웨이 서버는 HTTPS 포트 443을 사용하고 있습니다.
- 연결하려는 대상 애플리케이션 서버는 내부 이름 “srv2”를 사용합니다.

대상 애플리케이션 서버에 도달하기 위해 사용할 특별한 URL은 다음과 같습니다. 1.1.1.1:443/~~srv2

결과적으로, 이 특별한 URL을 사용하여 이 애플리케이션 서버의 웹 포털에 접근할 수 있습니다.

이 특정 애플리케이션 서버에 게이트웨이 서버를 통해 연결할 수 있는 연결 클라이언트를 생성할 수도 있습니다. 연결 클라이언트 생성기에서 서버 주소 필드에 특별한 URL을 사용하기만 하면 됩니다.

예를 들어:



서버 할당

개요

농장 컨트롤러는 게이트웨이 서버 역할을 하여 사용자가 연결할 때 농장의 특정 애플리케이션 서버로 리디렉션할 수 있습니다. 사용자는 하나 이상의 서버를 사용자 / 로컬 그룹 / Active Directory 그룹에 할당할 수 있습니다.

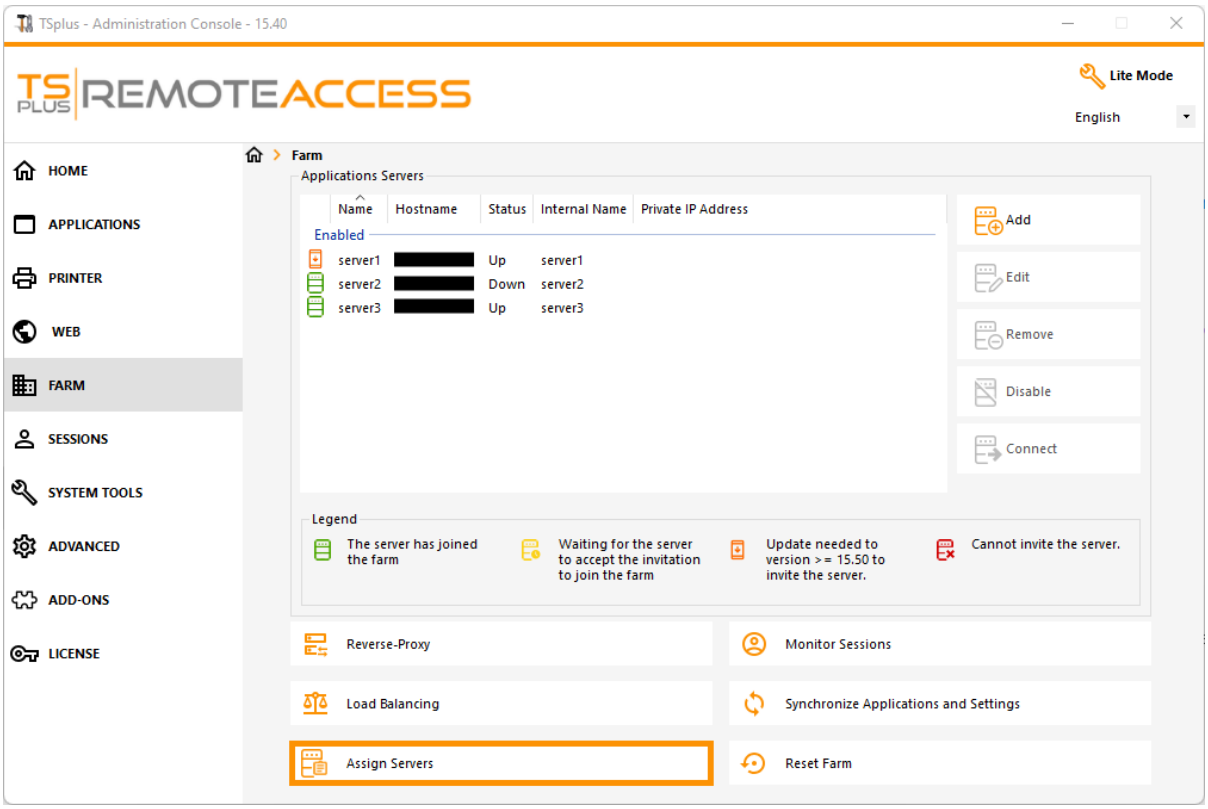
중요: 서버 할당은 TSplus 웹 포털에서만 작동하며, 연결 클라이언트에서는 작동하지 않습니다.

사용자에게 할당된 서버가 여러 개 있는 경우, 그는 자신에게 할당된 서버 목록에서 접근하고자 하는 서버를 선택할 수 있습니다.

농장이 도메인 내에 있는 경우, 게이트웨이는 그의 AD 자격 증명을 사용하고 사용자는 싱글 사인온(SSO)으로 연결됩니다.

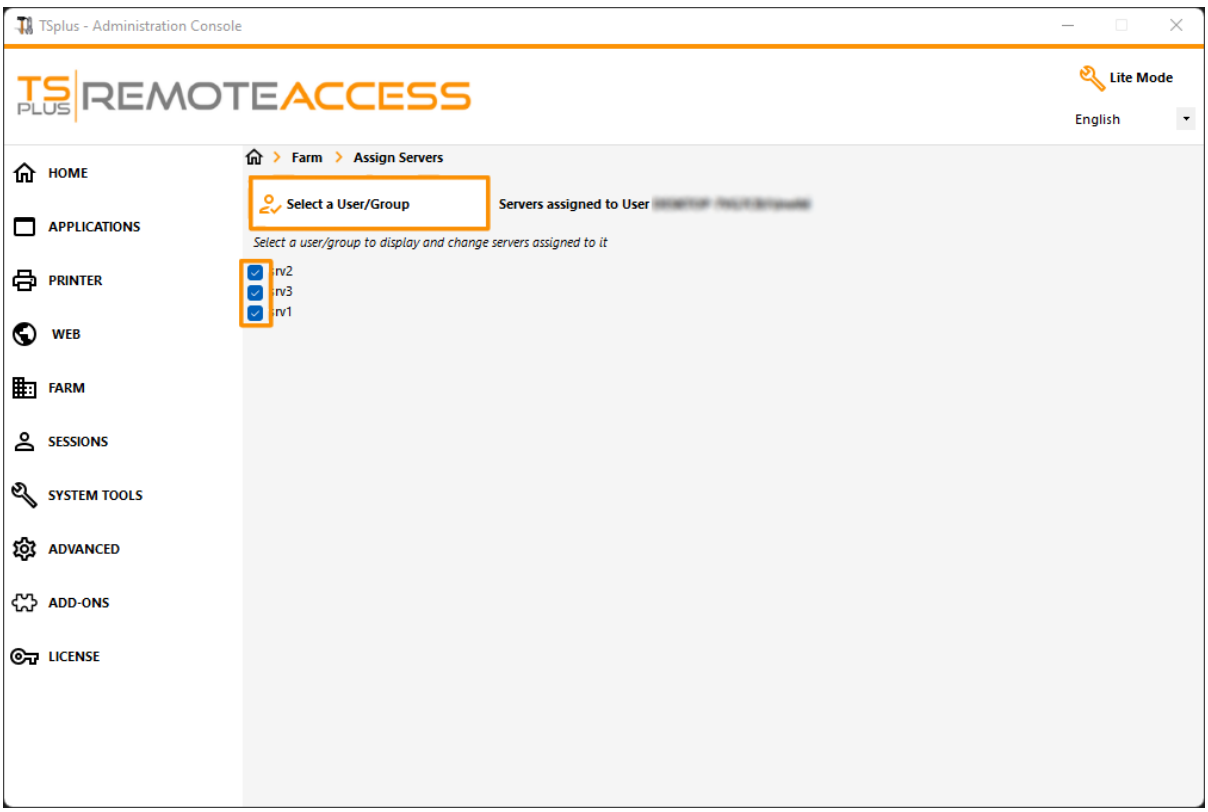
그렇지 않으면 각 서버에서 동일한 로컬 자격 증명을 가져야 합니다.

서버를 할당하려면 “서버 할당” 버튼을 클릭하십시오.



사용자에게 서버를 할당하려면 “사용자/그룹 선택” 버튼으로 서버를 선택한 다음 “서버” 목록에서 서버의 체크박스를 선택하면 됩니다.

사용자에게 할당된 서버를 제거하려면 "서버" 목록에서 서버의 체크박스를 간단히 선택 해제하면 됩니다.

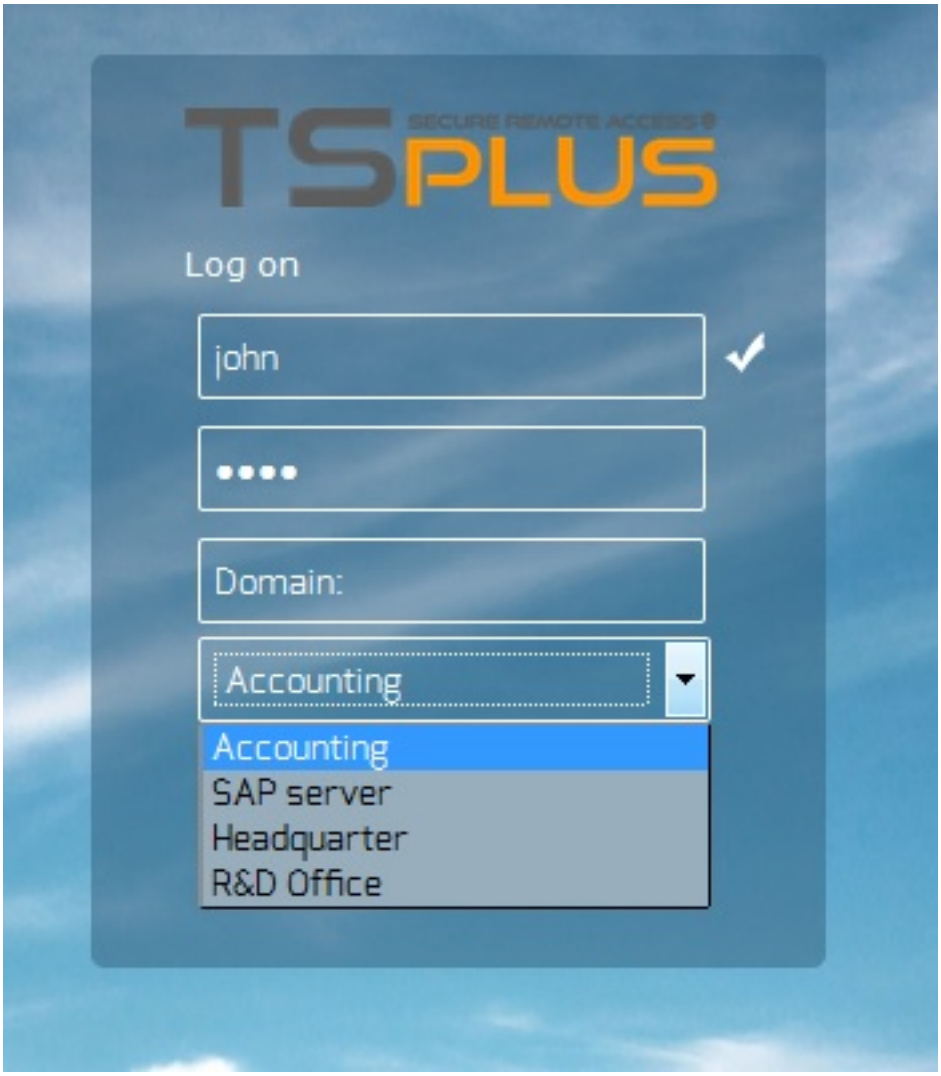


중요한 사항

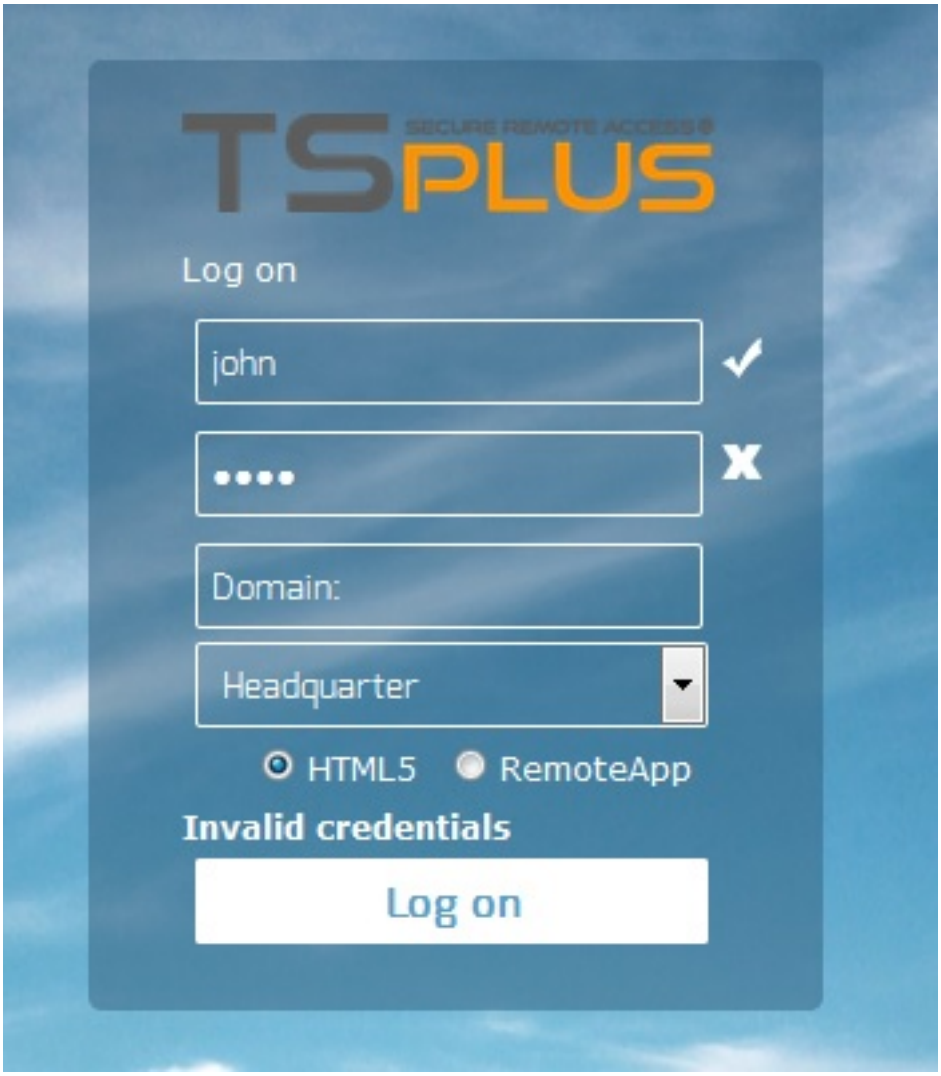
- 위의 예는 도메인 또는 작업 그룹에 대한 것입니다.
- 작업 그룹을 사용하는 경우 사용자의 로그인은 할당한 각 애플리케이션 서버에서 동일해야 합니다.
- 이 서버 할당 기능은 로드 밸런싱 기능과 동시에 구성하고 사용할 수 있으며, 이를 통해 팜 컨트롤러가 할당된 서버에서 로드 밸런싱을 수행할 수 있습니다. 이를 위해 로드 밸런싱을 활성화하고 "할당된 서버에서 로드 밸런싱" 옵션을 선택하십시오.
- 서버 할당 기능과 로드 밸런싱이 모두 활성화된 경우, 로드 밸런싱 구성에서 "할당된 서버에서 로드 밸런싱" 옵션이 활성화되지 않은 한, 게이트웨이 서버는 사용자를 할당된 서버와 관계없이 가장 덜 로드된 서버로 리디렉션합니다.

사용자가 게이트웨이에 연결할 때 받을 수 있는 예시

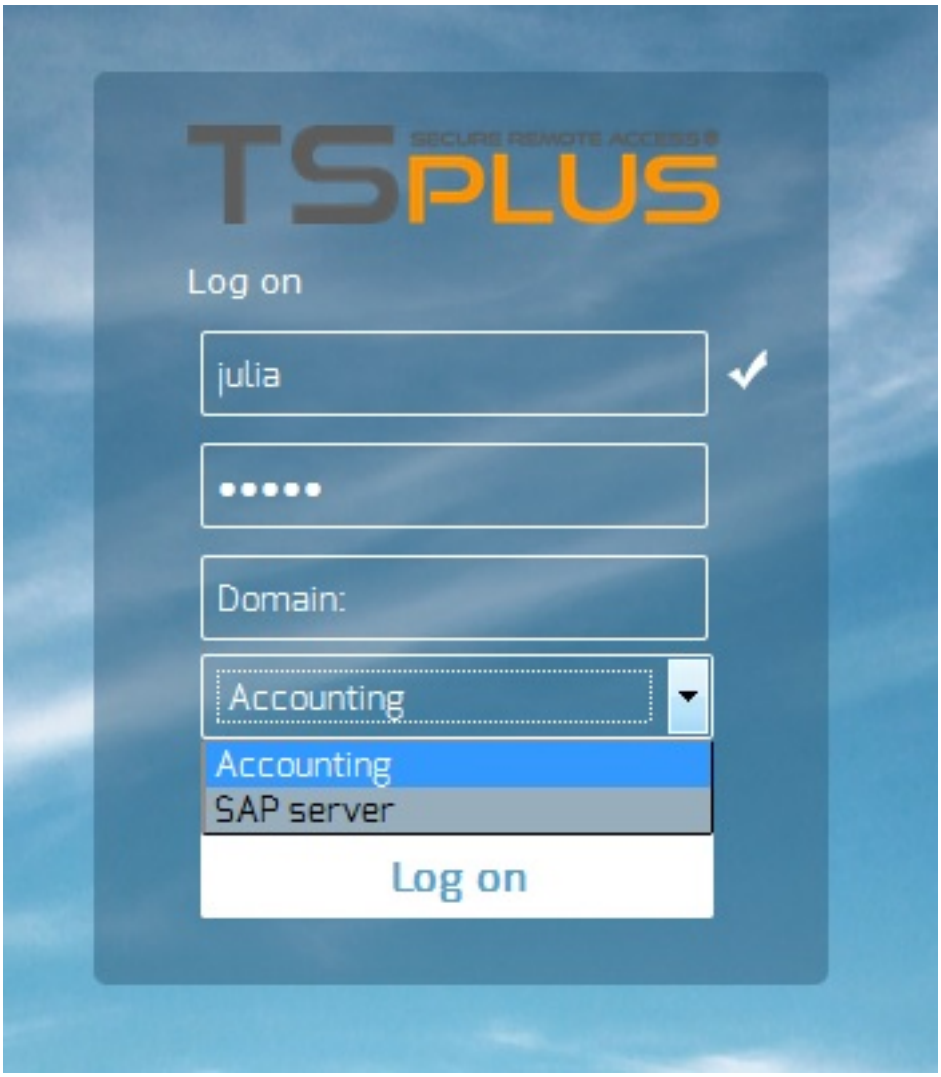
존은 서버를 선택할 수 있습니다. 그가 원하는 서버에 자동 로그온을 할 것입니다:



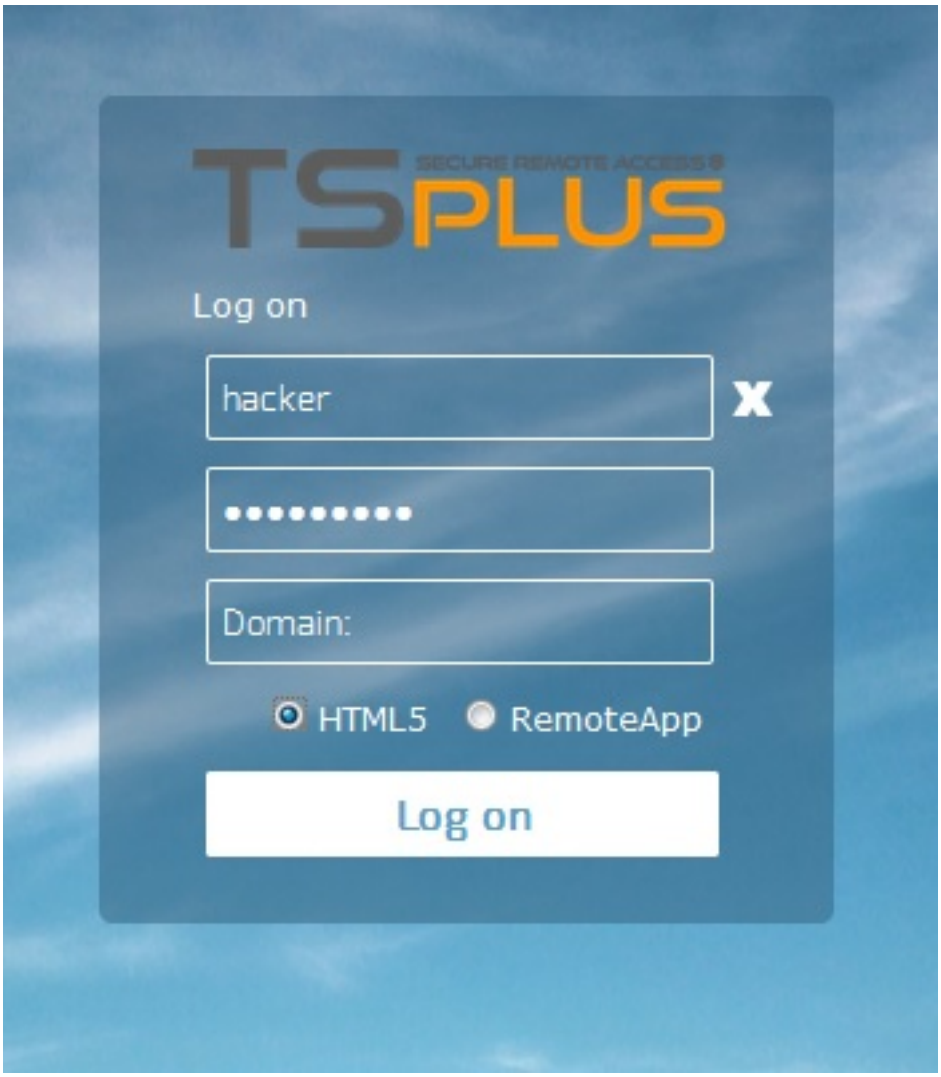
잘못된 비밀번호를 입력하면 존은 비밀번호를 다시 입력해야 합니다.



줄리아는 가능한 서버의 다른 목록을 가지고 있습니다:



누군가 게이트웨이를 해킹하려고 합니다. 그는 어떤 서버도 보지 못하고 게이트웨이는 그의 웹 접근을 차단합니다.

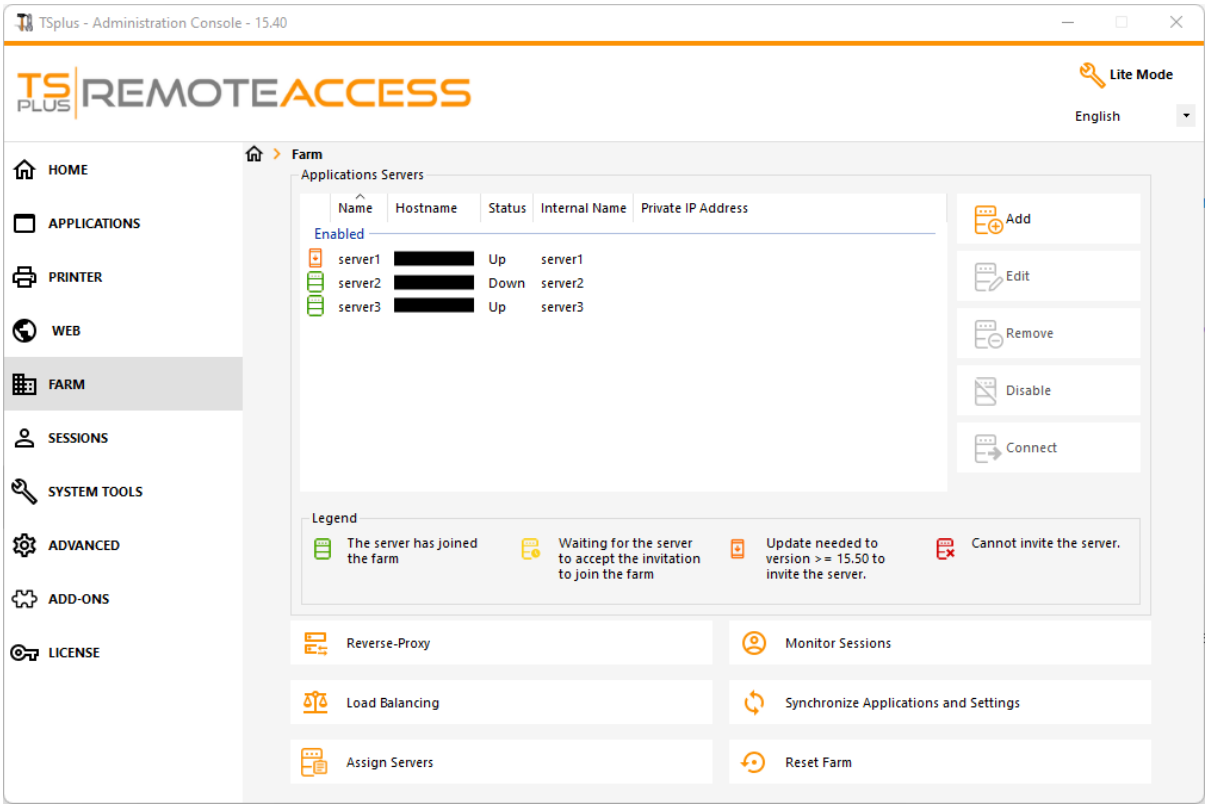

TSPLUS
SECURE REMOTE ACCESS
Log on
hacker
Domain:
HTML5
RemoteApp
Log on

농장 설정

개요

팜을 만들려면 TSplus AdminTool에서 애플리케이션 서버를 추가하기만 하면 됩니다.

관리 도구의 "Farm" 섹션에서 애플리케이션 서버를 관리할 수 있습니다.



이 창에서 여러 작업을 수행할 수 있습니다.

- “ 추가 새로운 애플리케이션 서버 추가
- “ 편집 선택한 서버를 편집합니다.
- “ 제거하다 선택한 서버를 농장에서 영구적으로 제거합니다(나중에 “추가” 버튼으로 다시 추가할 수 있습니다).
- “ 비활성화/활성화 선택한 서버를 일시적으로 비활성화하거나 활성화합니다(사용자는 이 서버에 연결할 수 없습니다).

- “ 연결하다 기본 RDP 클라이언트를 열고 선택한 서버에 자동으로 연결합니다. MSTSC에 자격 증명이 저장되어 있으면 사용되며, 그렇지 않으면 자격 증명을 입력해야 합니다.

서버에서 오른쪽 클릭하여 표시되는 컨텍스트 메뉴를 통해 이러한 작업에도 접근할 수 있습니다.

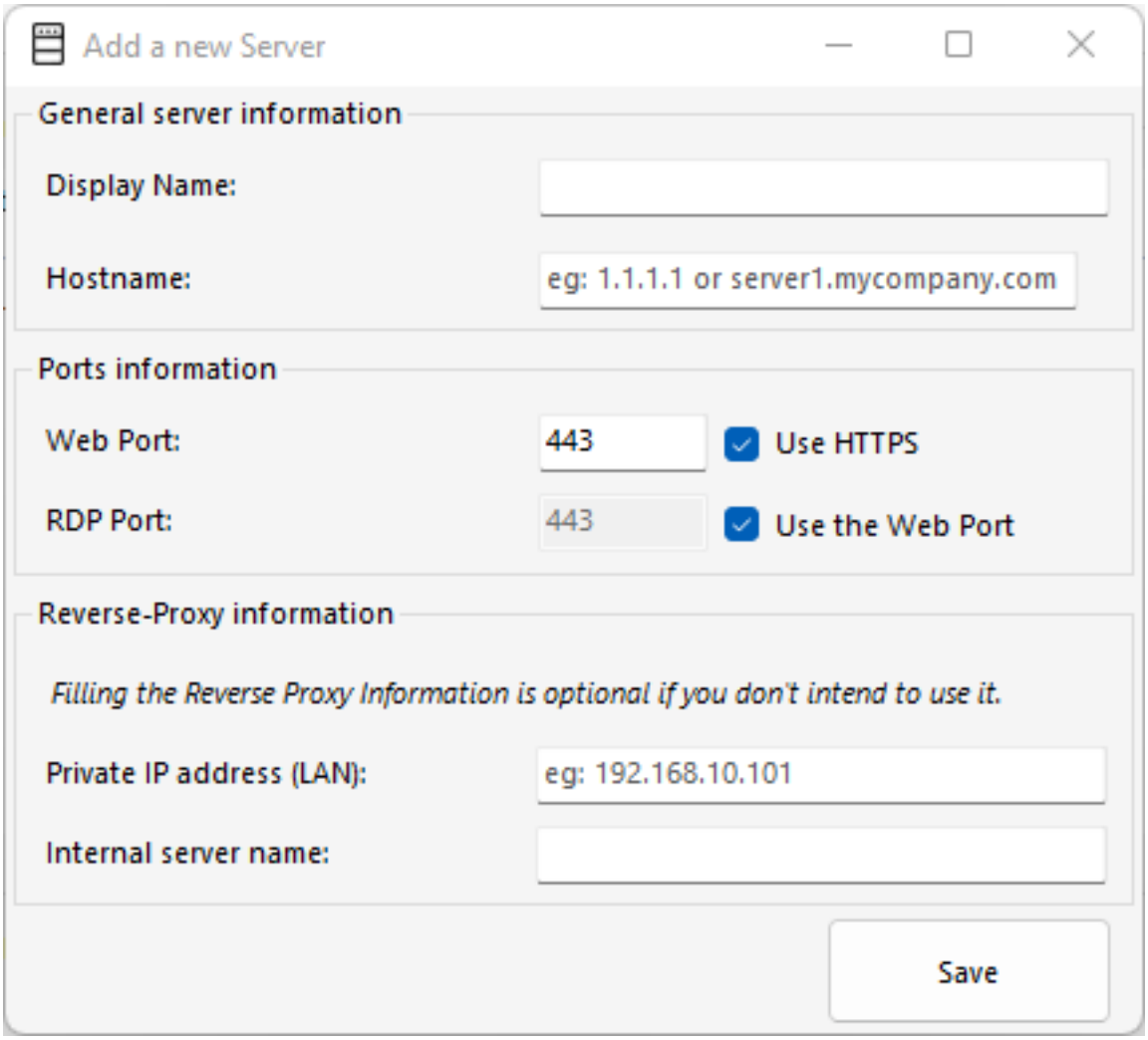
하단 패널에서 애플리케이션 서버가 추가된 후 사용할 수 있는 주요 농장 기능에 대한 빠른 액세스를 찾을 수 있습니다:

- “로드 밸런싱”: 게이트웨이 서버에서 연결하는 사용자를 농장의 가장 덜 부하가 걸린 서버로 리디렉션할 수 있습니다.
- “리버스 프록시”: 게이트웨이 서버만 노출할 수 있으며, 애플리케이션 서버에 URL을 사용하여 접근할 수 있게 합니다. https://gateway-server-domain-or-ip-address/~~application-server-internal-name
- “서버 할당”: 게이트웨이 서버에서 연결할 때 사용자와 그룹이 사용할 수 있는 애플리케이션 서버를 제한할 수 있으며, 여러 서버가 할당된 경우 사용자가 연결할 서버를 선택할 수 있습니다.
- 세션 모니터링 * 현재 세션을 모니터링하고 연결 끊기, 로그오프, 메시지 전송, 세션 보기 또는 세션 제어와 같은 작업을 신속하게 수행할 수 있습니다.
- 응용 프로그램 및 설정 동기화 * 선택한 애플리케이션 서버에 모든 고급 설정 및 게시된 애플리케이션을 푸시할 수 있습니다.
- “Reset Farm”: 농장을 재설정할 수 있으며, 이는 모든 서버를 제거하고 “리버스 프록시”, “로드 밸런싱” 및 “서버 할당” 구성과 같은 모든 농장 기능 구성을 재설정합니다.

* 이 기능은 보안상의 이유로 농장에 완전히 가입한 애플리케이션 서버에서만 접근할 수 있으며, 이는 애플리케이션 서버 측에서 농장 컨트롤러가 보낸 초대를 먼저 수락해야 함을 의미합니다.

농장에 애플리케이션 서버 추가

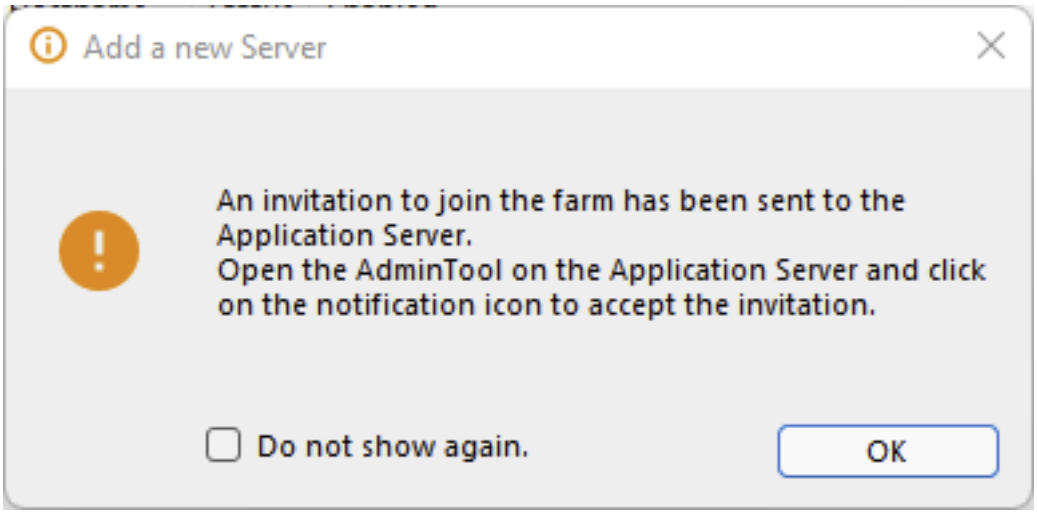
애플리케이션 서버를 추가하려면 "추가" 버튼을 클릭하십시오. 다음 창이 표시됩니다.



디스플레이 이름과 호스트 이름을 지정해야 합니다(포트 번호 없이 IP 또는 도메인 이름을 입력할 수 있습니다).
Reverse Proxy 정보 필드를 입력하는 것은 Reverse Proxy 기능을 현재 사용하지 않는 경우에만 선택 사항입니다.
내부 이름이 비어 있을 경우 전체 서버 구성을 용이하게 하기 위해 사용 가능한 표시 이름으로 자동으로 채워집니다.

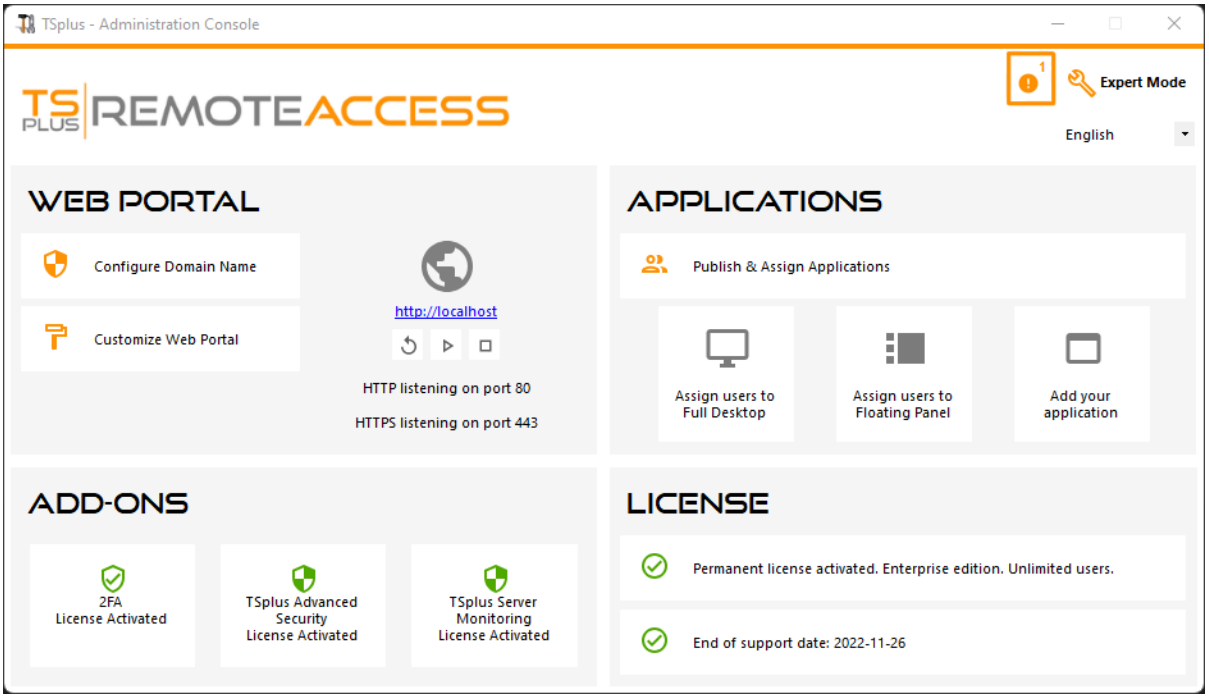
중요: RDP 포트 옵션 "웹 포트 사용"은 애플리케이션 서버의 웹 서버에서 제공하는 RDP 포트 포워딩 기능(기본적으로 활성화됨)을 활용하고 싶다는 것을 지정합니다.
결과적으로, "웹 포트 사용" 옵션을 사용하려면 추가된 애플리케이션 서버에서 AdminTool > 고급 > 보안의 "RDP 포워딩 비활성화" 옵션이 "아니오"로 설정되어 있는지 확인하십시오.

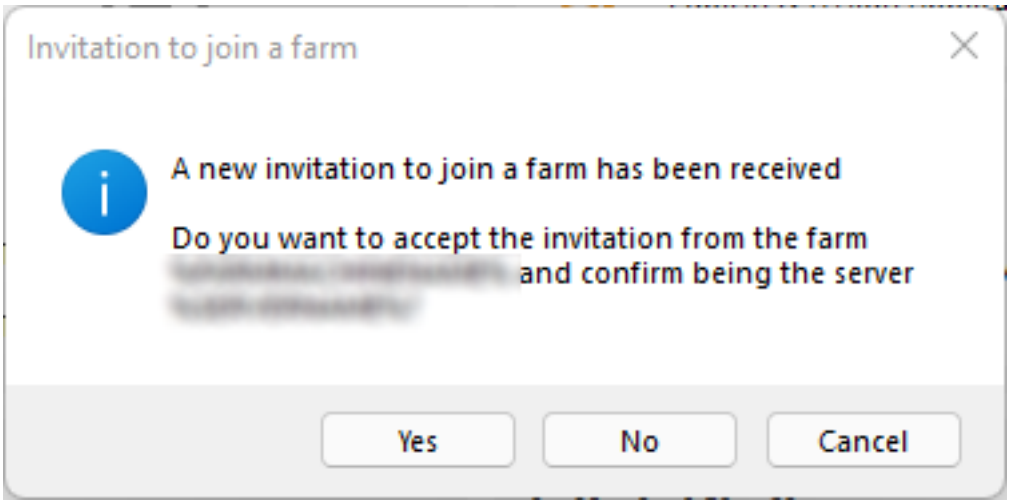
애플리케이션 서버 세부 정보를 입력한 후 "저장" 버튼을 클릭하십시오. 추가된 애플리케이션 서버에 농장에 가입하라는 초대가 전송됩니다.



응용 프로그램 서버 측에서 이 초대를 수락하는 것은 보안상의 이유로 "세션 모니터링" 및 "응용 프로그램 및 설정 동기화"를 사용하려면 필수입니다.
그러나 "리버스 프록시", "로드 밸런싱" 및 "서버 할당" 기능만 사용해야 하는 경우에는 필요하지 않습니다.

초대 수락을 위해 관리자 세션을 엽니다. **애플리케이션 서버에서** 농장에 추가했습니다. TSplus AdminTool의 오른쪽 상단 모서리에 있는 경고 버튼을 클릭한 다음 "예"를 클릭하세요.





농장 컨트롤러 측에서는 농장의 애플리케이션 서버 목록을 볼 수 있습니다. 이들은 색상 아이콘으로 표시된 세 가지 상태를 가질 수 있습니다.

- 

  가입됨 응용 프로그램 서버가 초대를 수락하여 농장에 완전히 가입했습니다.

-

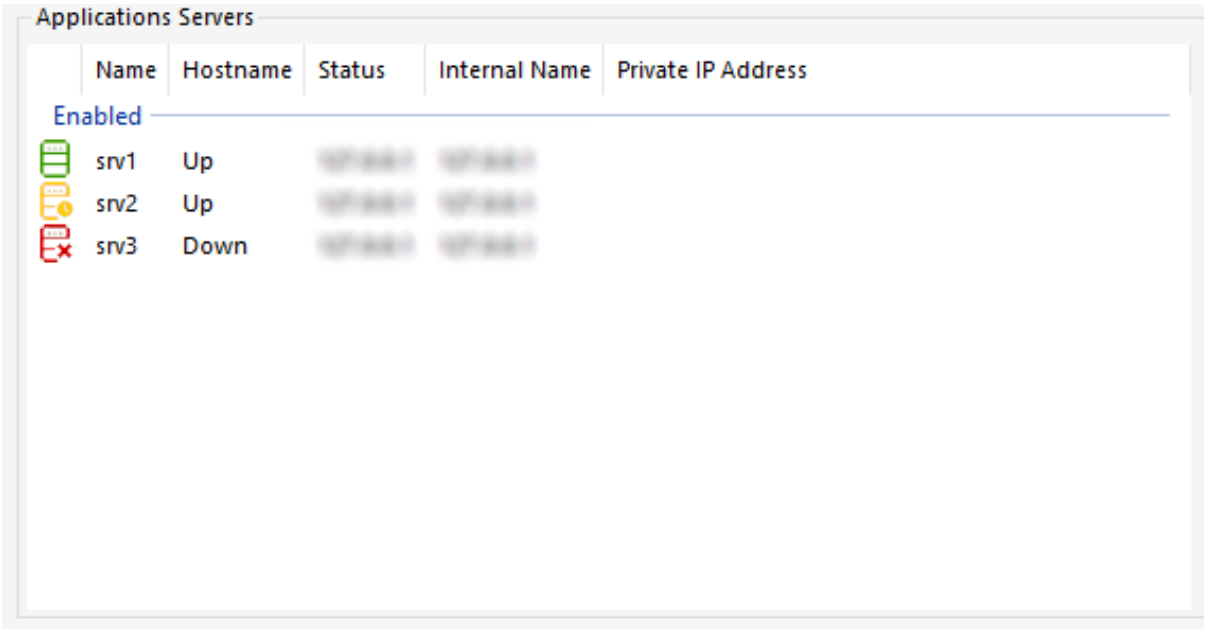
  대기 중 응용 프로그램 서버가 농장에 부분적으로 참여했으며, 응용 프로그램 서버가 초대를 수락하기를 기다리고 있습니다.

- 

  업데이트 필요 응용 프로그램 서버가 부분적으로 팜에 가입했지만, 서버가 TSplus Remote Access 버전 < 15.50을 사용하고 있기 때문에 초대를 보낼 수 없습니다.

- 

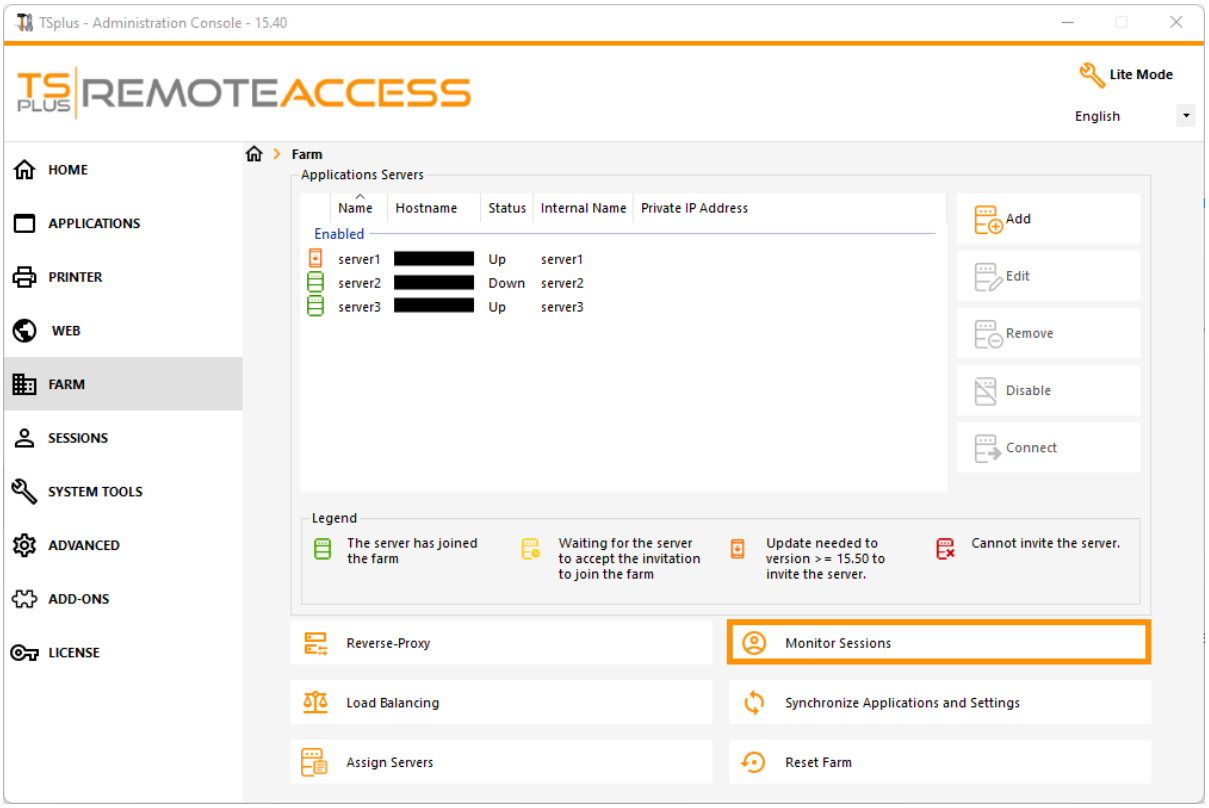
  도달할 수 없음 응용 프로그램 서버가 부분적으로 팜에 가입했지만, 서버에 접근할 수 없기 때문에 초대장을 보낼 수 없습니다.


Applications Servers
Name
Hostname
Status
Internal Name
Private IP Address
Enabled
srv1
Up
srv2
Up
srv3
Down

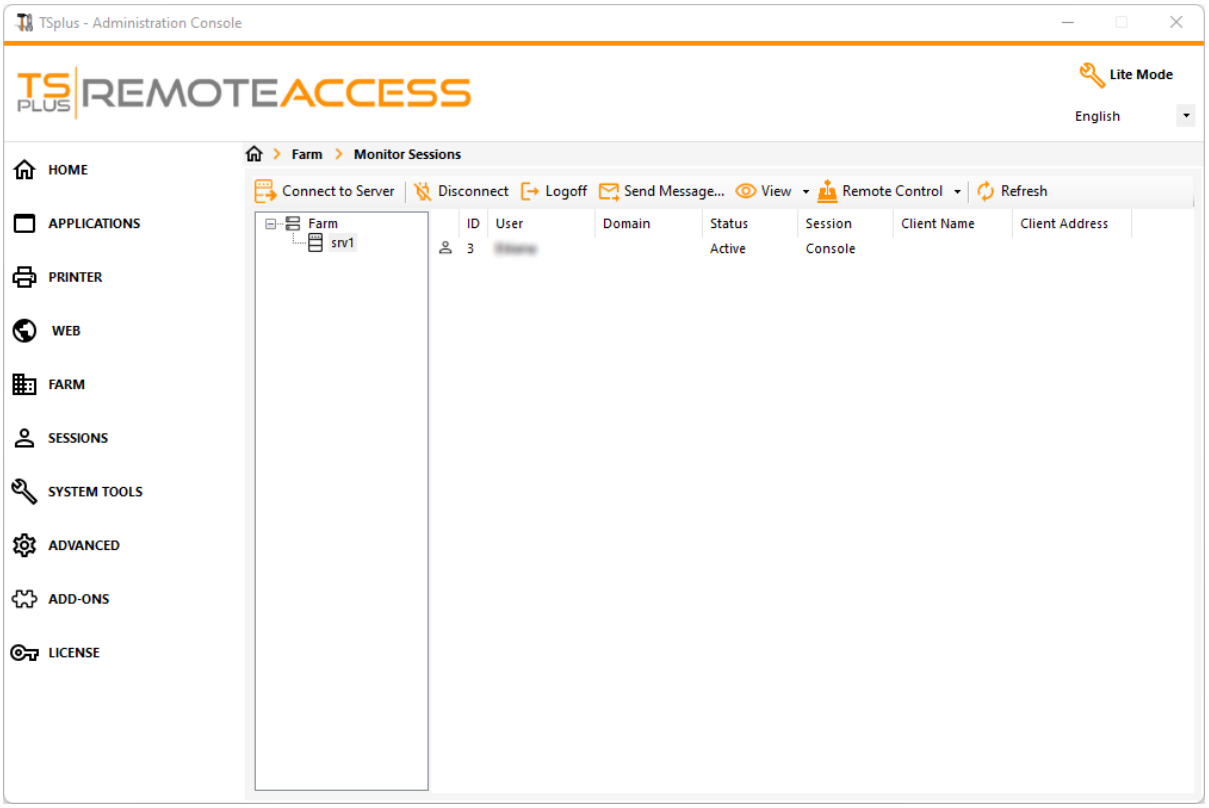
세션 모니터링

개요

FARM 탭을 통해 모니터링 세션 인터페이스에 접근할 수 있습니다:



“세션 모니터링” 버튼을 클릭하여 다음 탭을 표시합니다:



이 탭에서는 농장의 모든 애플리케이션 서버에서 사용자 세션 목록을 볼 수 있습니다.
왼쪽 패널에서 애플리케이션 서버를 클릭하여 선택하고 현재 활성 사용자 세션을 표시합니다. 표시되면 하나 이상의 세션을 선택하고 다음 버튼 중 하나를 클릭하여 여러 작업을 수행할 수 있습니다.

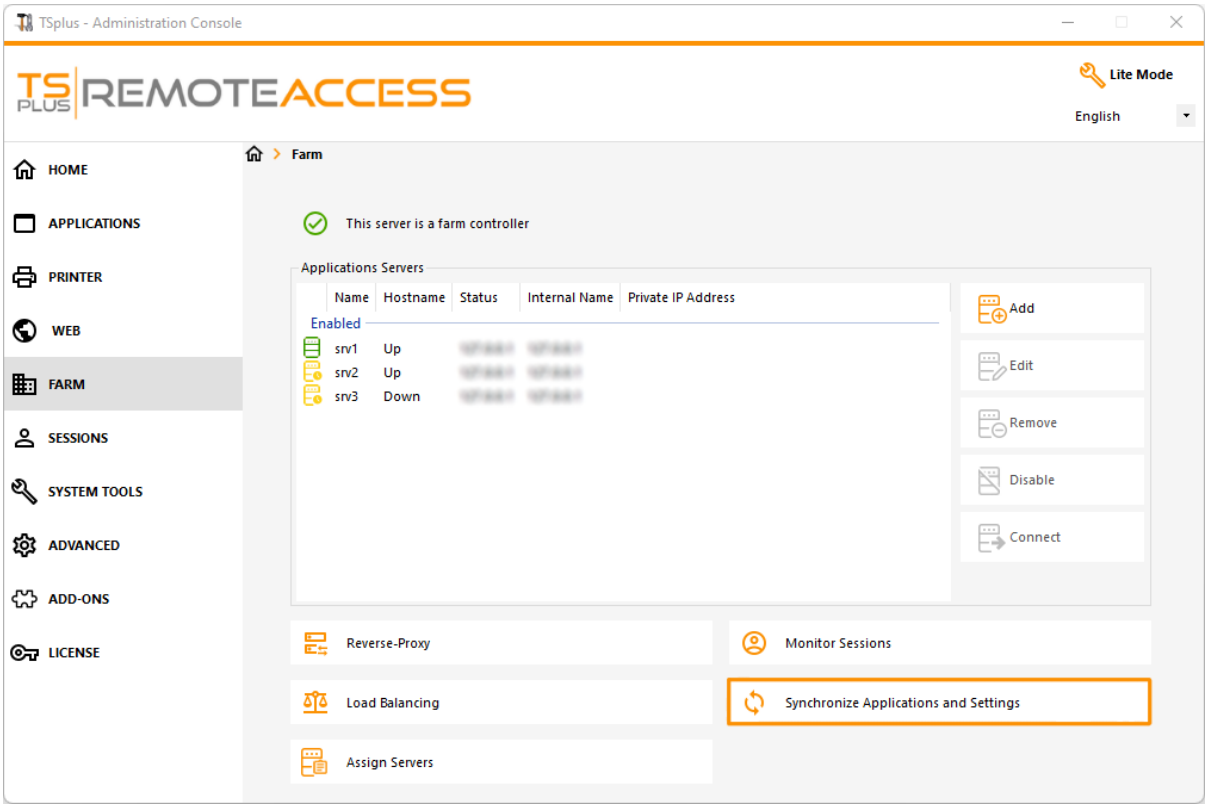
- “연결 끊기”: 선택한 사용자 세션을 연결 끊기 (사용자는 여전히 자신의 세션에 다시 연결할 수 있습니다).
- “Logoff”: 선택한 사용자 세션을 로그 오프합니다(저장되지 않은 모든 수정 사항이 손실되며, 애플리케이션이 갑자기 종료됩니다).
- “메시지 보내기”: 제목과 텍스트를 입력할 수 있는 창을 표시한 후, 이 메시지를 선택한 사용자 세션에 전송합니다.
- “보기”: 선택한 사용자 세션을 권한과 함께/없이 보기.
- “원격 제어”: 선택한 사용자 세션을 권한이 있거나 없는 상태에서 원격으로 제어합니다.
- “새로 고침”: 선택한 서버의 사용자 세션 목록을 완전히 새로 고칩니다.

* 세션을 보거나 제어하려면 **권한 없이** 당신은 필요할 것입니다 **응용 프로그램 서버에서 세션을 보고 및/또는 제어하려는 다음 GPO를 변경하십시오.** .
GPO 위치: 컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 > 연결 .
GPO 키: 원격 데스크톱 서비스 사용자 세션의 원격 제어 규칙 설정

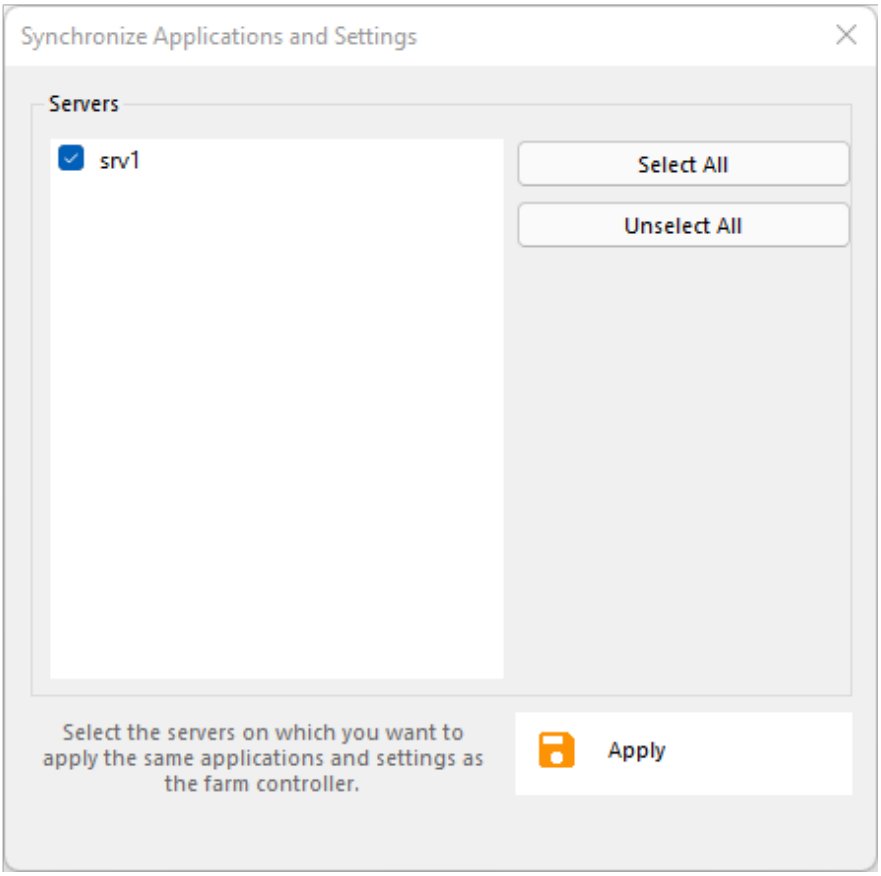
사용자 세션 목록은 5초마다 자동으로 새로 고쳐집니다. 선택한 서버가 사용 불가능해지면 이 자동 새로 고침이 중지됩니다. "새로 고침" 버튼을 클릭하면 자동 새로 고침이 재개됩니다.

응용 프로그램 및 설정 동기화

개요

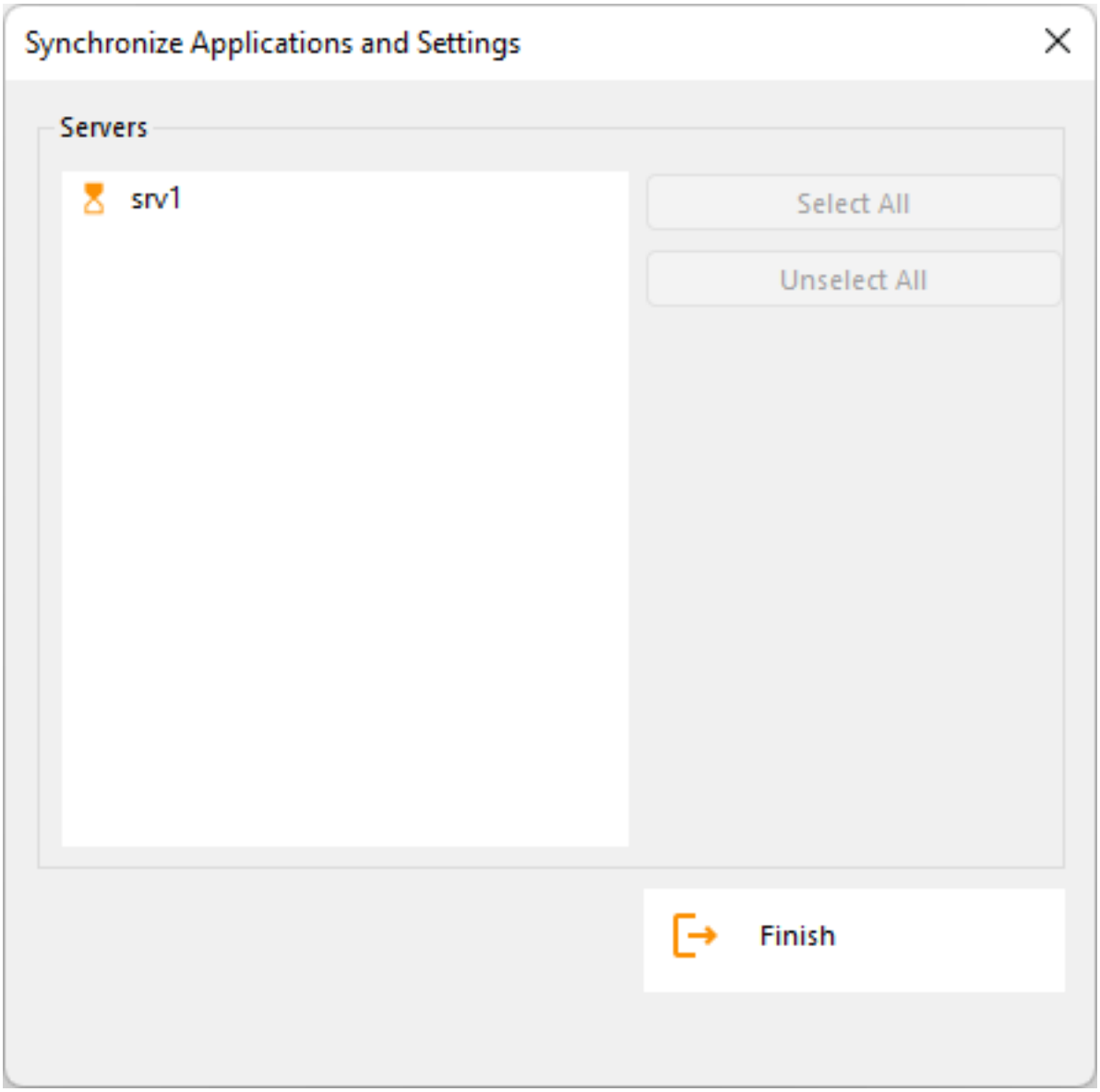


“응용 프로그램 및 설정 동기화” 버튼을 클릭하여 다음 창을 표시합니다.



모든 서버를 확인하여 Farm Controller와 동일한 설정을 적용하고 동일한 애플리케이션을 게시한 다음 "적용"을 클릭하십시오.

다음 창이 표시되어 작업 진행 상황을 모니터링할 수 있습니다:


Synchronize Applications and Settings
Servers
srv1
Select All
Unselect All
Finish

사용자와 서버 간의 빠르고 쉬운 파일 전송

개요

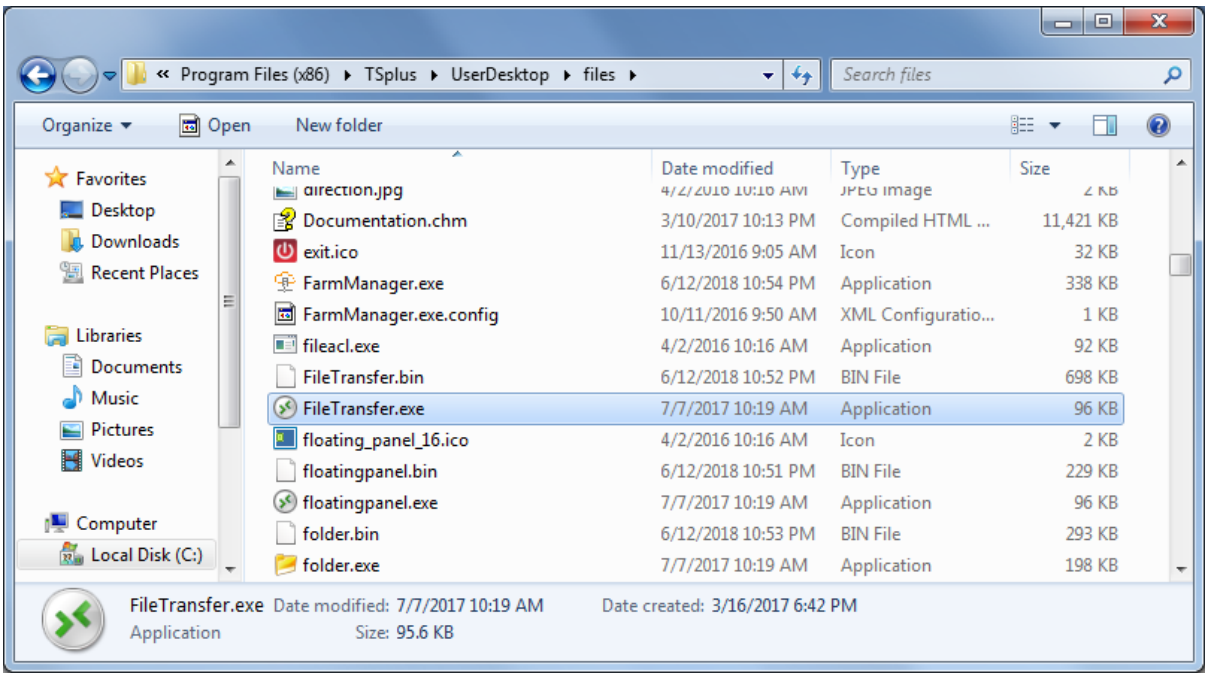
TSplus는 파일 전송을 위한 독특한 방법을 포함합니다:

- 로컬 사용자 워크스테이션에서 사용자 원격 데스크톱으로
- TSplus 서버에서 로컬 사용자 데스크탑으로

파일 전송이 가상 채널을 기반으로 하기 때문에 파일 복사보다 훨씬 빠르며, 수행할 수 있습니다. **로컬 사용자 디스크 드라이브가 매핑되지 않은 경우에도** .

파일 전송 프로그램 및 생성된 클라이언트

파일 전송 프로그램은 TSplus 프로그램 폴더에 위치하며, 이름은 “FileTransfer.exe”이고 다음 경로에 있습니다: “UserDesktop\files”



파일 전송

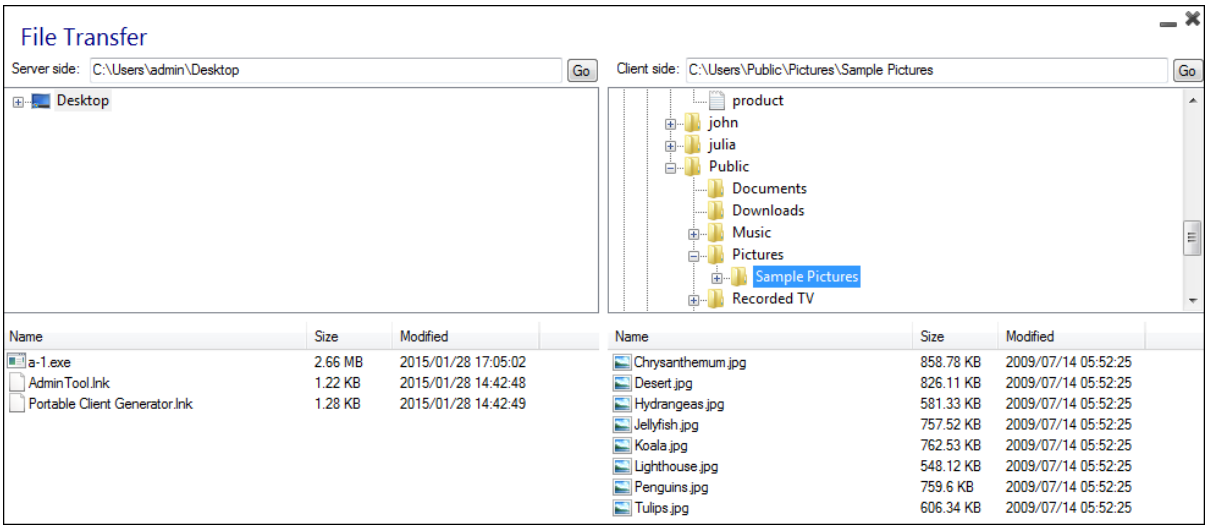
파일 전송은 매우 쉽습니다.

먼저 파일 전송을 시작합니다(예: TSplus 플로팅 패널 사용).

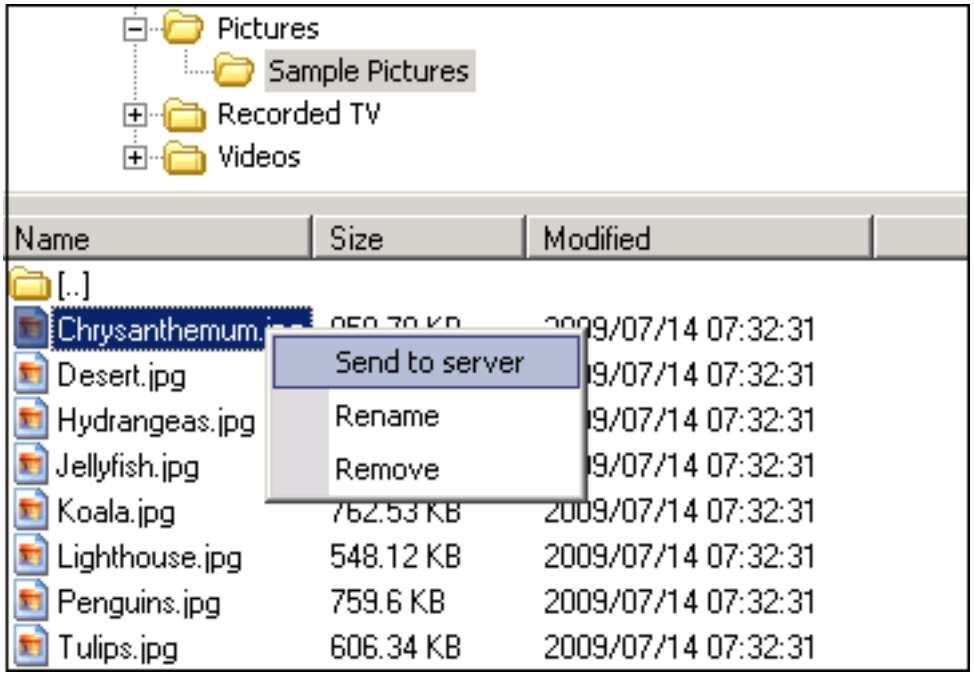


그런 다음 폴더 트리를 사용하여 파일로 이동하십시오:

- 서버의 폴더와 파일은 다음에 있습니다. **창의 왼쪽 부분 (서버 측)**
- 로컬 워크스테이션의 폴더와 파일은 다음에 있습니다. **창의 오른쪽 부분 (클라이언트 측)**



마지막으로, 전송하려는 파일을 오른쪽 클릭하고 “서버로 전송” (또는 “클라이언트로 전송”)을 클릭하세요:



파일 전송은 로컬 워크스테이션에서 서버로, 그리고 서버에서 로컬 워크스테이션으로도 작동합니다.

노트 HTML5 세션에서 파일 전송 유틸리티를 사용할 때, 서버에서 클라이언트로만 파일을 전송할 수 있습니다. 선호해 주세요. HTML5 상단 메뉴 방법 서버에 파일을 업로드하고 클라이언트로 다운로드하며 파일 전송 목록을 관리할 수 있는 곳.

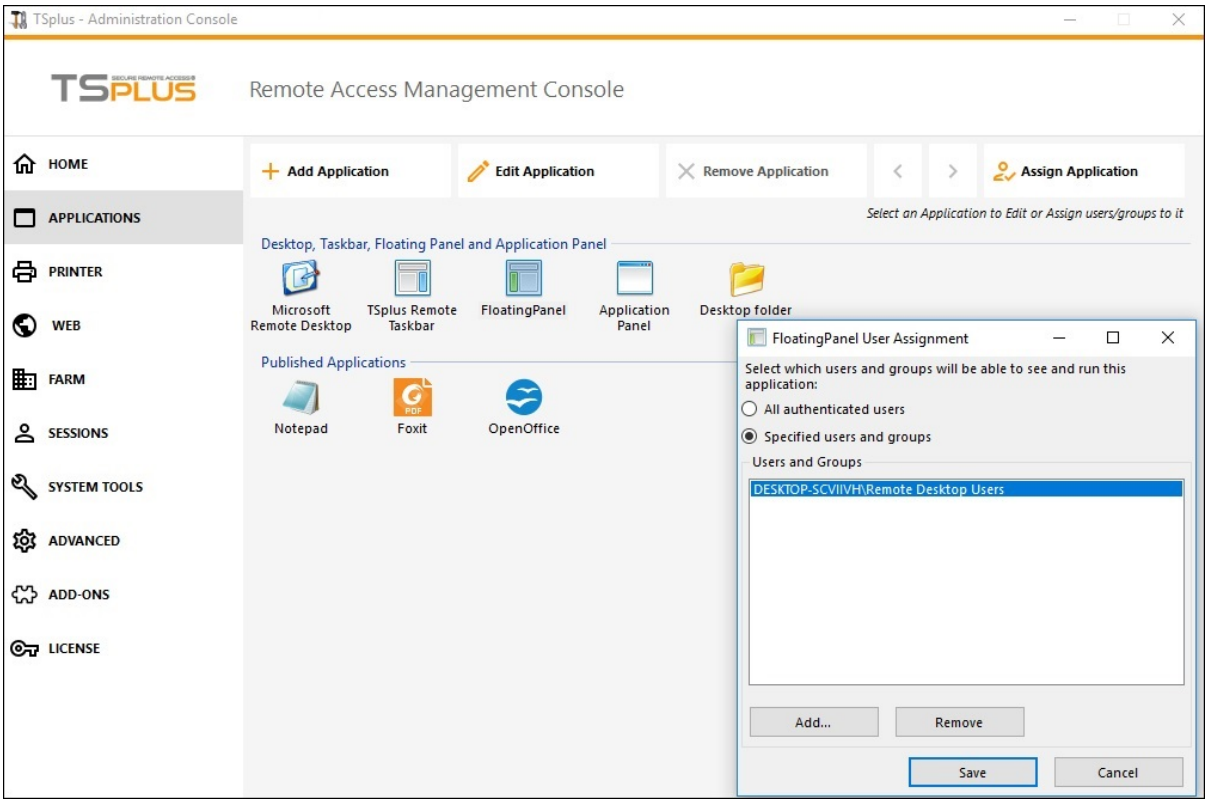
플로팅 패널 및 애플리케이션 패널

사용자 또는 그룹을 위해 플로팅 패널 또는 애플리케이션 패널을 활성화하도록 선택할 수 있습니다.

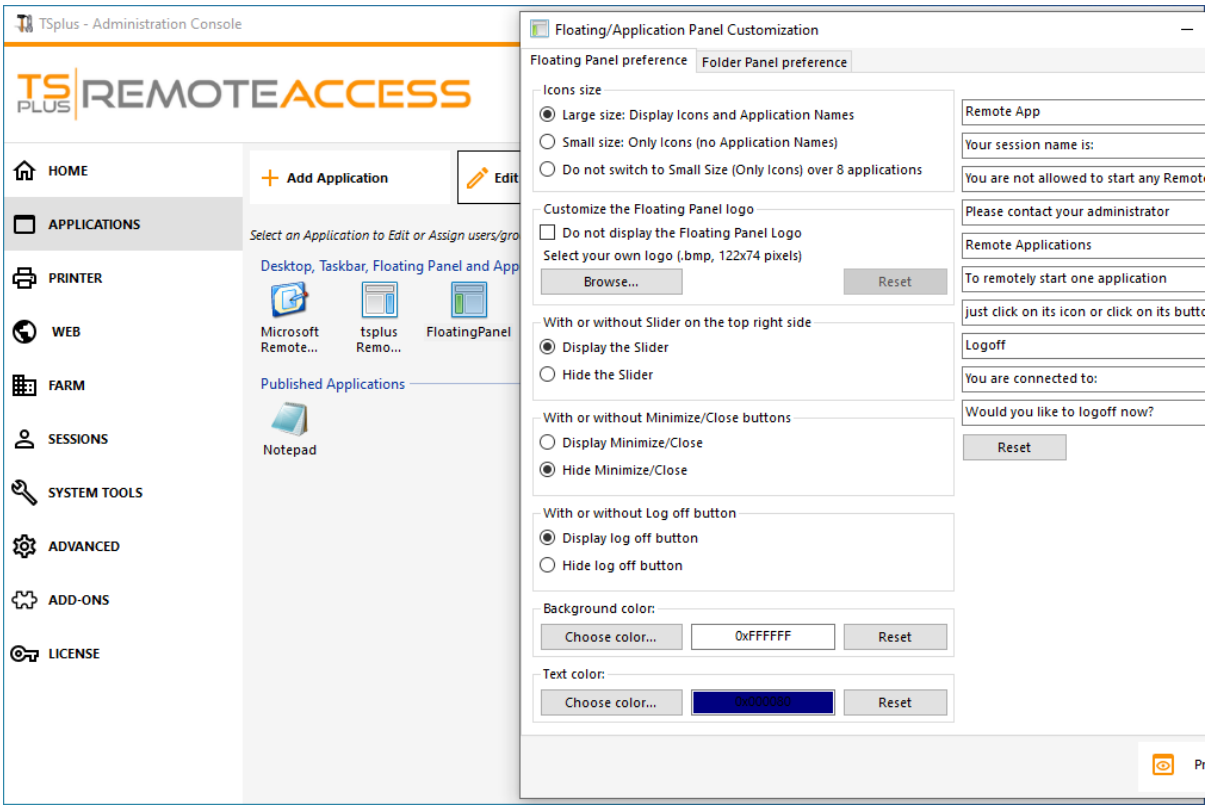
이 두 가지 애플리케이션 게시 방법은 모든 연결 방법에 대해 사용할 수 있습니다.

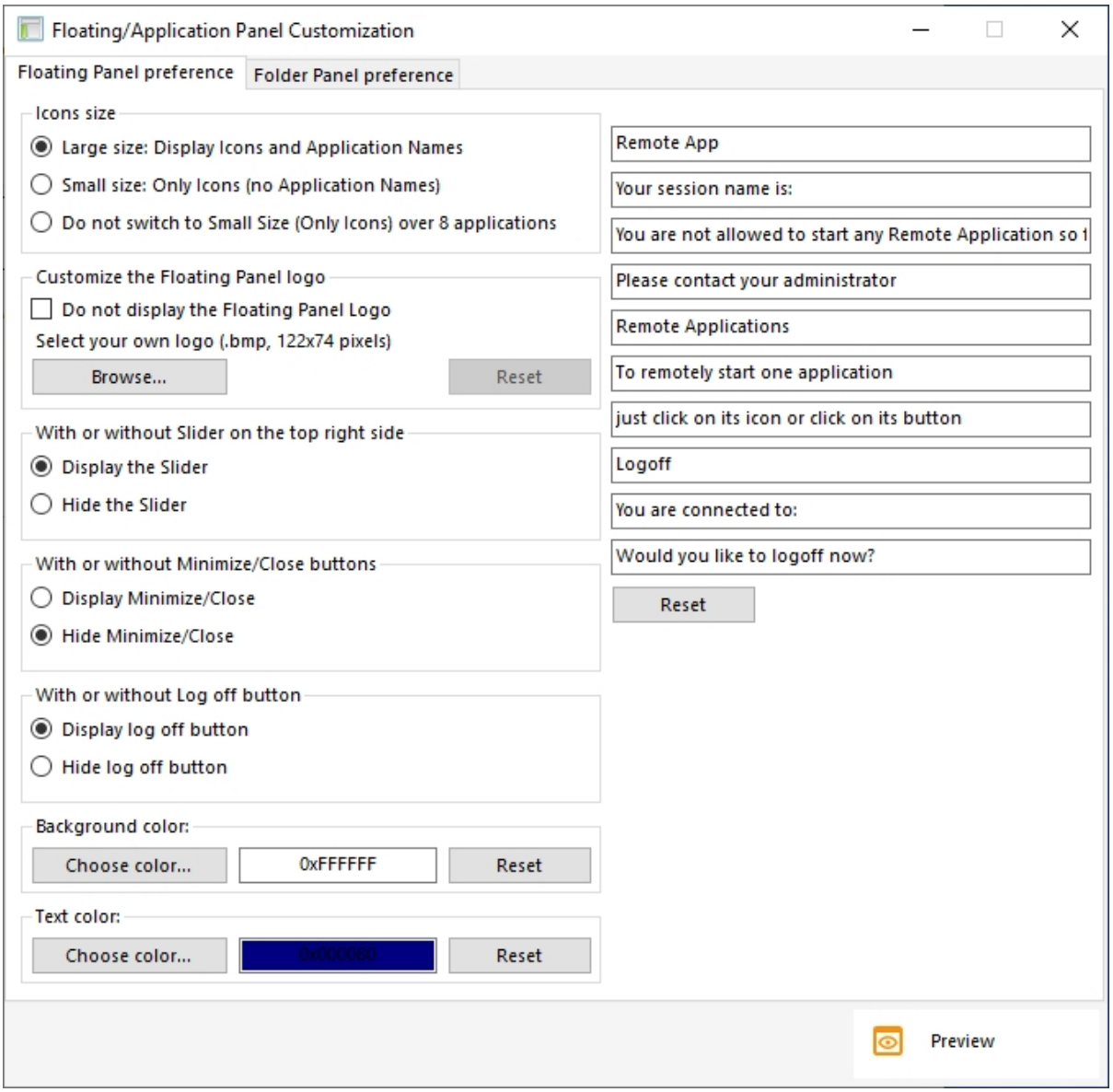
할당된 애플리케이션으로 활성화되면 사용자 화면의 중간 왼쪽에서 애플리케이션의 미니 드롭다운 목록 또는 플로팅 패널을 볼 수 있습니다(TSplus 사용자에게 매우 유용합니다):

애플리케이션으로 지정하십시오:



플로팅 패널을 선택한 다음, 편리하게 플로팅 패널을 사용자 정의할 수 있도록 “애플리케이션 편집” 타일을 클릭하세요.


TSplus - Administration Console
TS PLUS REMOTEACCESS
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Add Application
Edit
Select an Application to Edit or Assign users/gro
Desktop, Taskbar, Floating Panel and App
Microsoft Remote...
tsplus Remo...
FloatingPanel
Published Applications
Notepad
Floating/Application Panel Customization
Floating Panel preference
Folder Panel preference
Icons size
Large size: Display Icons and Application Names
Small size: Only Icons (no Application Names)
Do not switch to Small Size (Only Icons) over 8 applications
Customize the Floating Panel logo
Do not display the Floating Panel Logo
Select your own logo (.bmp, 122x74 pixels)
Browse...
Reset
With or without Slider on the top right side
Display the Slider
Hide the Slider
With or without Minimize/Close buttons
Display Minimize/Close
Hide Minimize/Close
With or without Log off button
Display log off button
Hide log off button
Background color:
Choose color...
0xFFFFFF
Reset
Text color:
Choose color...
Reset
Remote App
Your session name is:
You are not allowed to start any Remot
Please contact your administrator
Remote Applications
To remotely start one application
just click on its icon or click on its butt
Logoff
You are connected to:
Would you like to logoff now?
Reset



이러한 다양한 옵션을 통해 최종 사용자의 경험을 사용자 정의할 수 있습니다.

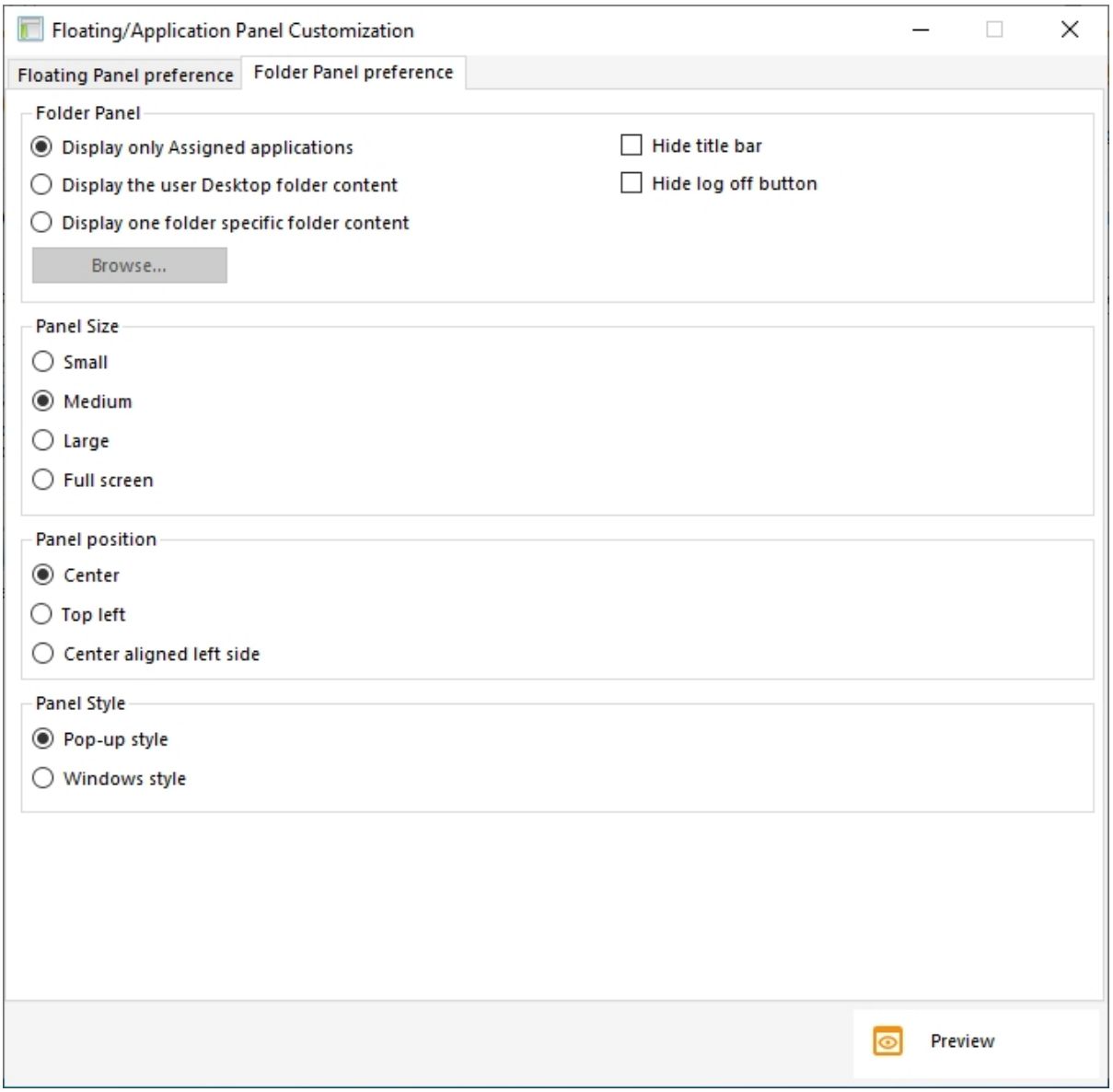
여기에서 다양한 플로팅 패널 표시 옵션을 설정할 수 있습니다.

- 표시된 텍스트를 수정하십시오.
- 선택한 크기를 선택하세요. 대형과 소형 중에서 아이콘만 표시할 수 있습니다.
- 로고 추가하기,
- 배경과 텍스트의 색상을 사용자 정의하세요.
- 슬라이더를 표시할지 말지,
- 최소화/닫기 버튼을 표시할지 여부
- 로그오프 아이콘 표시 여부…

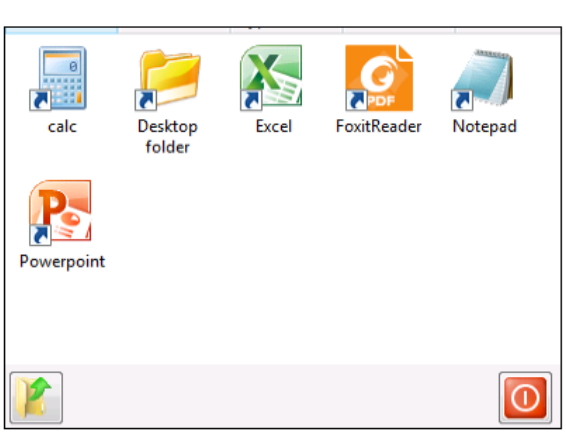


주의해 주십시오 8개 이상의 애플리케이션이 있을 경우, 플로팅 패널이 자동으로 소형으로 전환됩니다. 여전히 애플리케이션 이름을 표시하고 싶다면, "8개 이상의 애플리케이션에서 소형으로 전환하지 않기(아이콘만)"를 선택하세요.

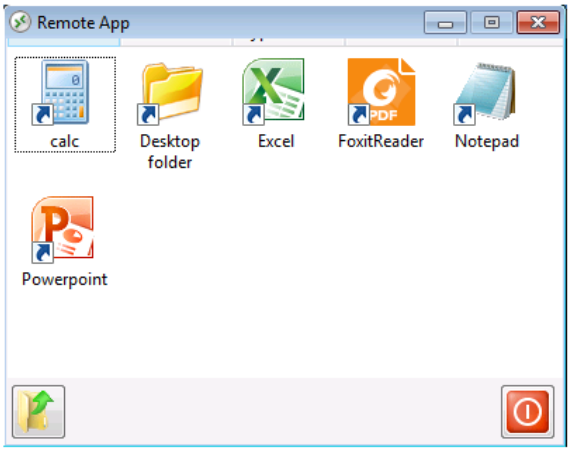
그 **폴더 패널** 사용자가 할당된 애플리케이션, 사용자 바탕 화면 폴더 또는 세션 내 특정 폴더의 내용을 다양한 표시 옵션으로 표시할 수 있도록 사용자 정의할 수 있습니다.



폴더 패널의 크기, 위치 및 스타일(팝업 또는 윈도우)을 편리하게 변경할 수 있습니다:



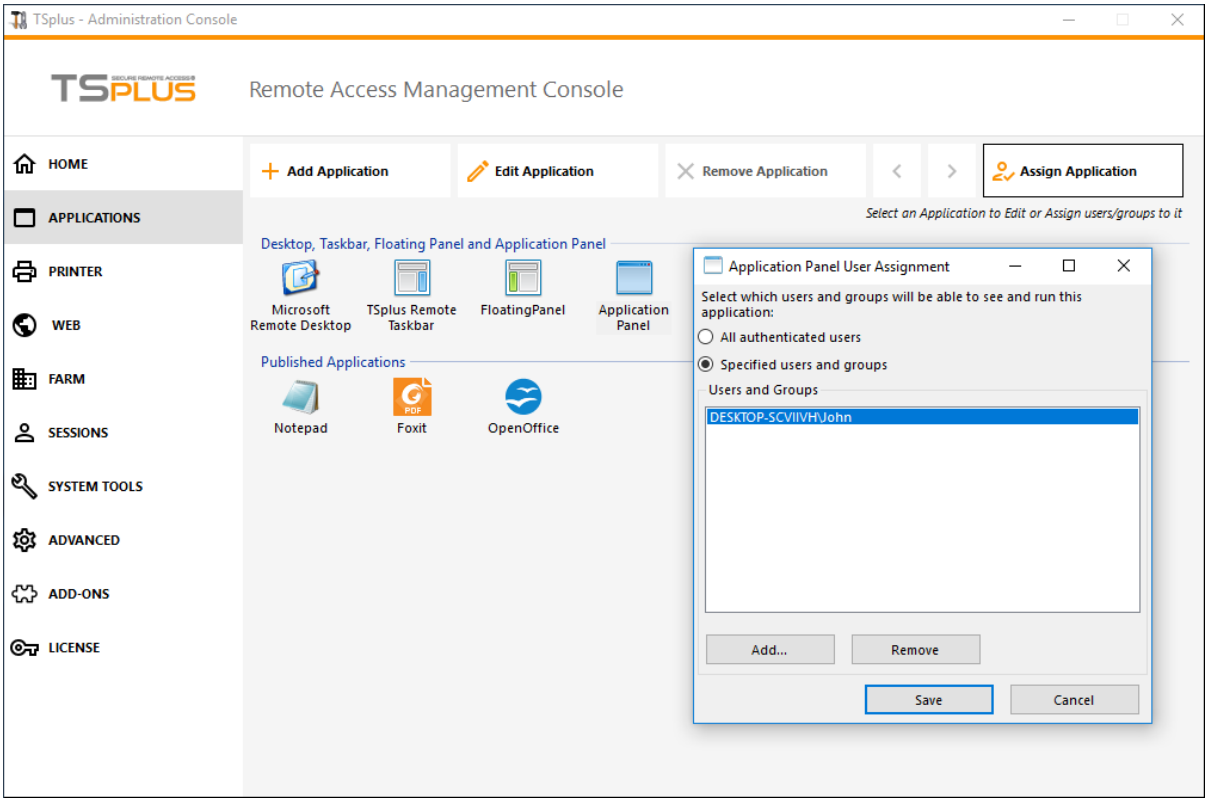
Pop-up style



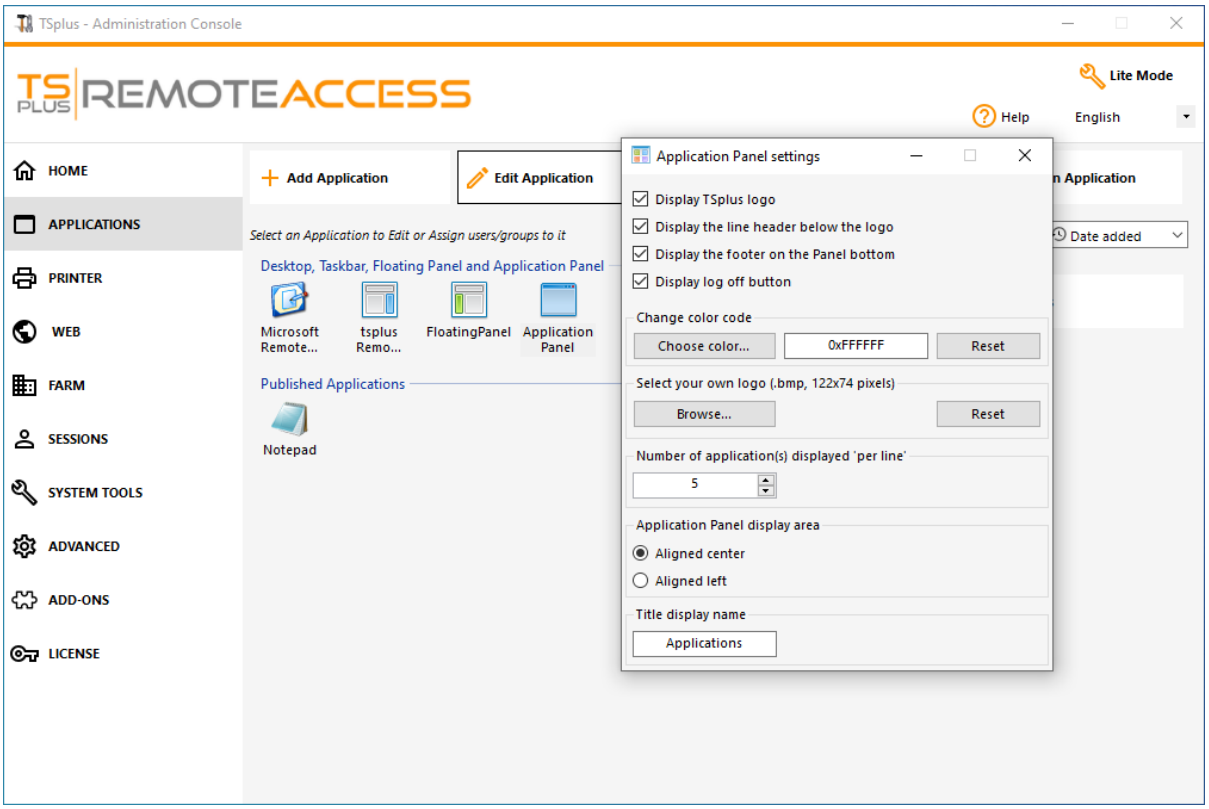
Windows style

응용 프로그램 패널은 웹 응용 프로그램 포털과 정확히 같은 방식으로 표시된 응용 프로그램을 구

성할 수 있는 가능성을 제공합니다. 단, 이를 단순히 한 사용자 또는 그룹에 할당함으로써 가능합니다.



관리자는 TSplus 로고 또는 자신의 로고를 표시하도록 선택하고, 로고 아래에 선 헤더와 바닥글을 표시하며, 색상을 변경하거나 해당 상자를 선택 해제하여 아무것도 표시하지 않도록 선택하여 사용자 정의할 수 있습니다. 또한, 한 줄에 표시되는 애플리케이션 수를 입력하여 행과 열로 표시되는 애플리케이션 수를 조정할 수 있으며, 애플리케이션 패널의 정렬 및 이름도 조정할 수 있습니다.



예를 들어, TSplus 로고와 함께 한 열에 여섯 개의 앱을 로고 없이 표시하거나 두 열과 세 줄로 표시합니다.


Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

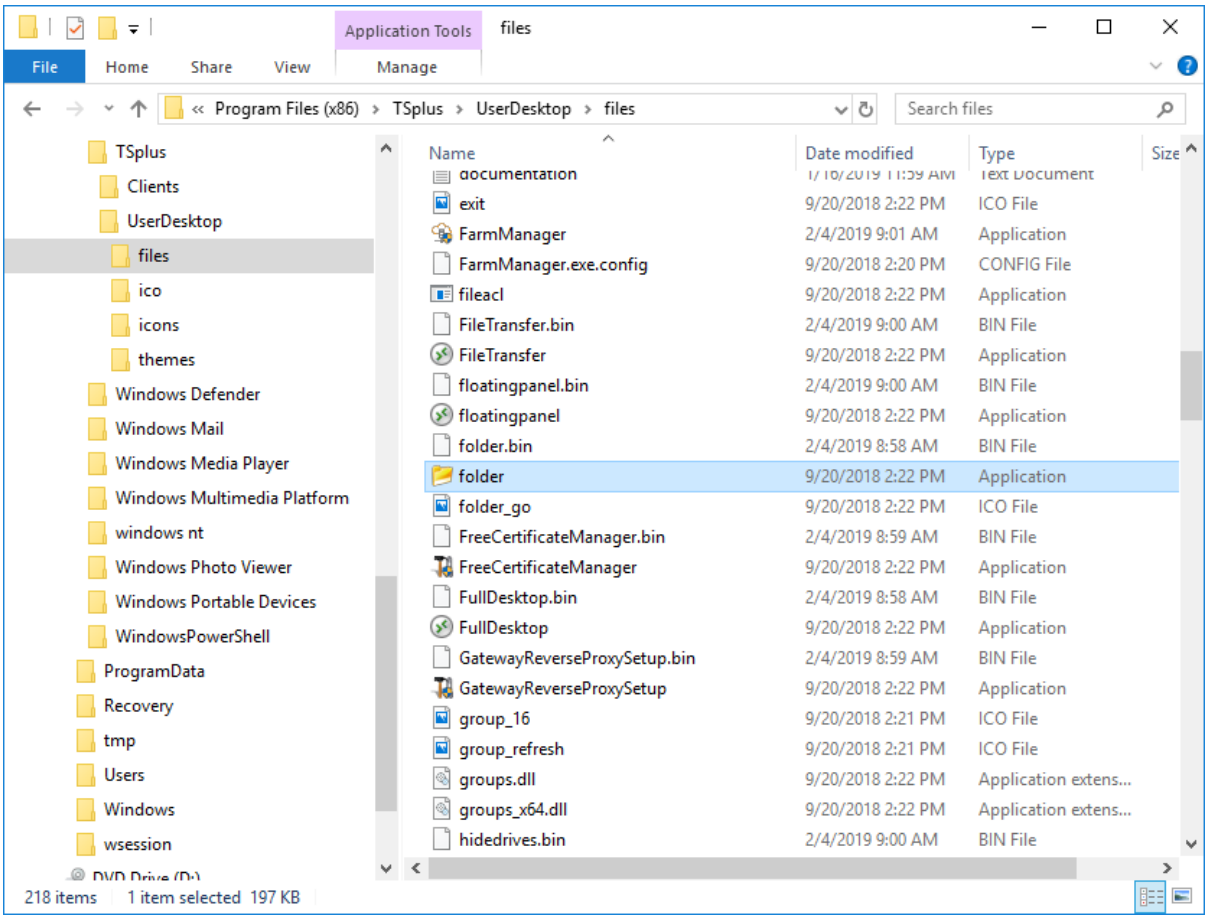

TSPLUS
Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

보안 폴더 공유 - Folder.exe

폴더 애플리케이션은 사용자가 사용할 수 있도록 제공할 폴더의 내용을 안전하게 표시합니다.

먼저, 공유하려는 애플리케이션이나 문서가 있는 서버에 폴더를 만드세요.

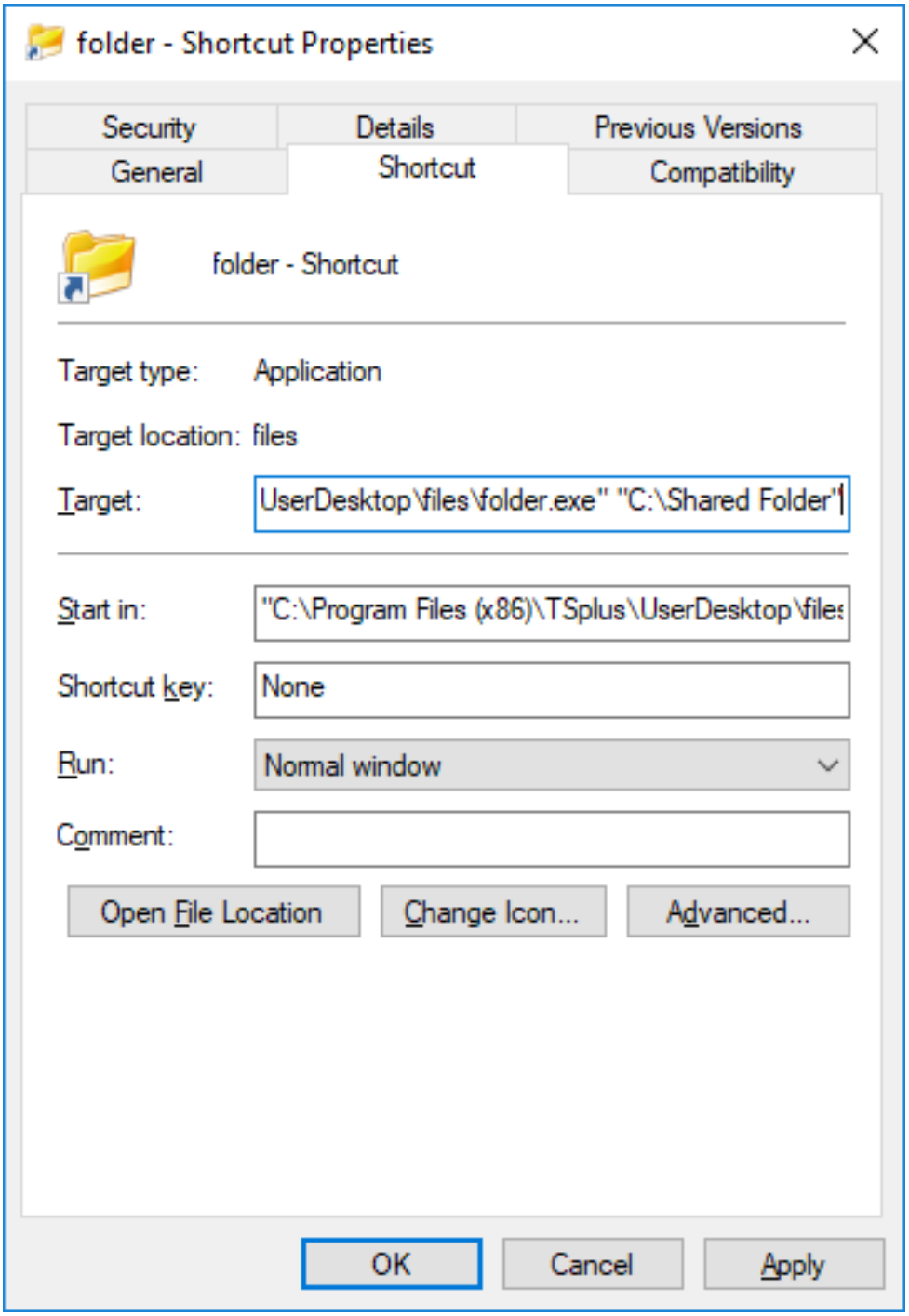
explorer.exe를 열고 C:\Program Files\tsplus\UserDesktop\files에서 folder.exe 애플리케이션을 찾으세요.



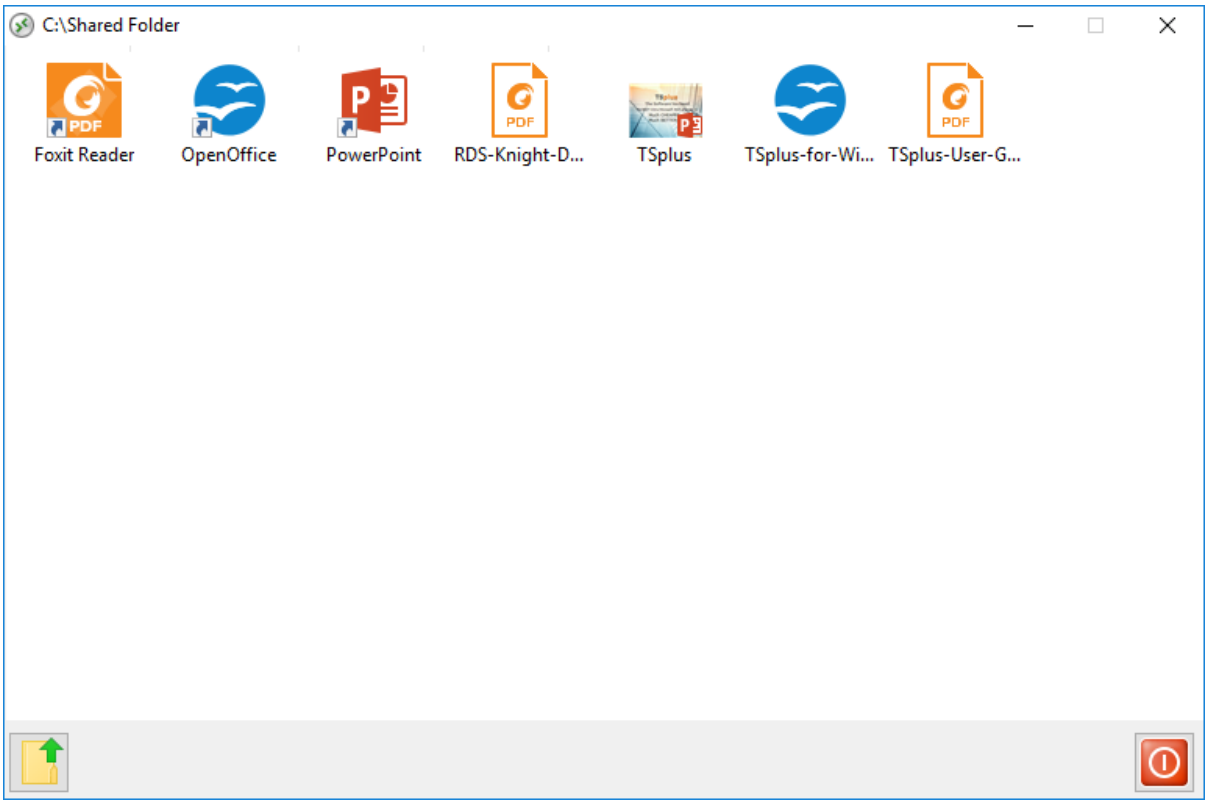
이 파일의 바로 가기를 만드세요. 바로 가기를 마우스 오른쪽 버튼으로 클릭하여 속성을 편집하세요.

그런 다음 원래 대상 경로 뒤에 "대상" 줄에 애플리케이션 폴더의 경로를 입력하여 바로 가기의 대상 경로를 수정합니다. 예:

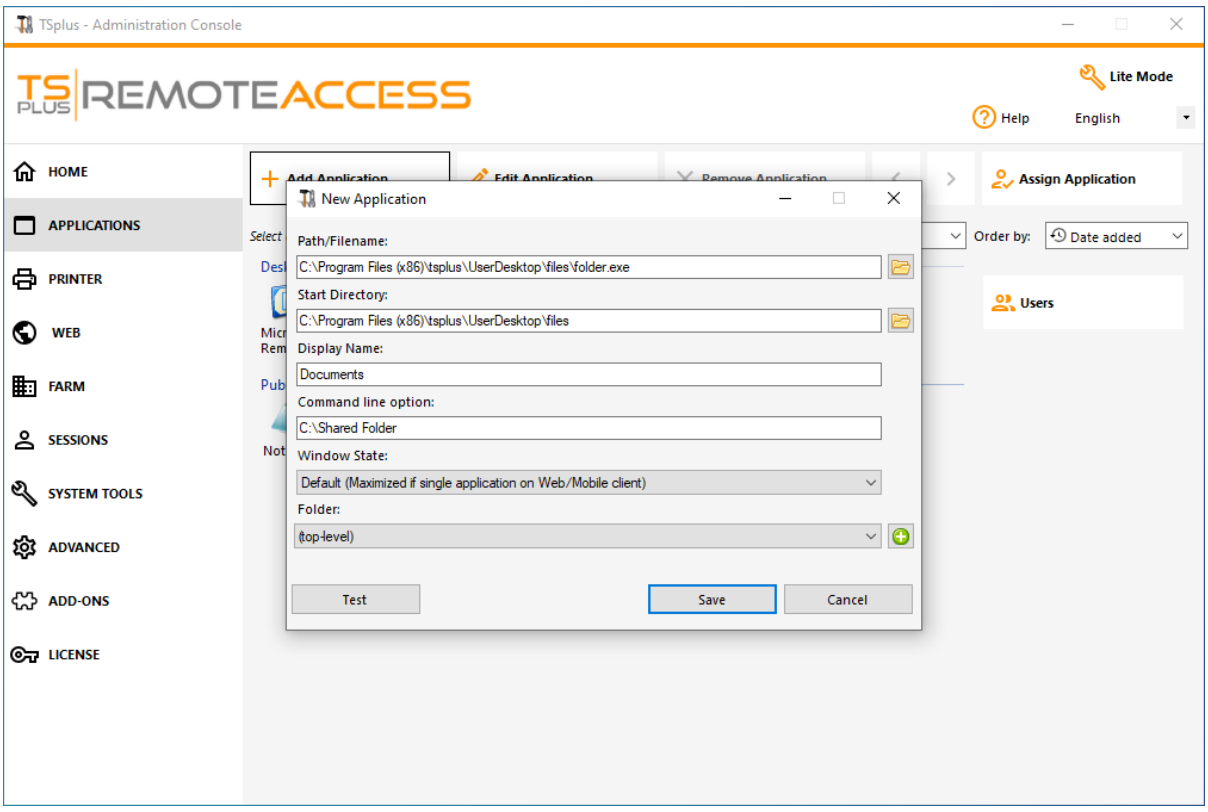
“C:\Program Files\tsplus\UserDesktop\files\folder.exe” “C:\공유 폴더”



폴더.exe 바로가기를 열면 다음과 같이 보여야 합니다(자신의 문서와 애플리케이션으로):



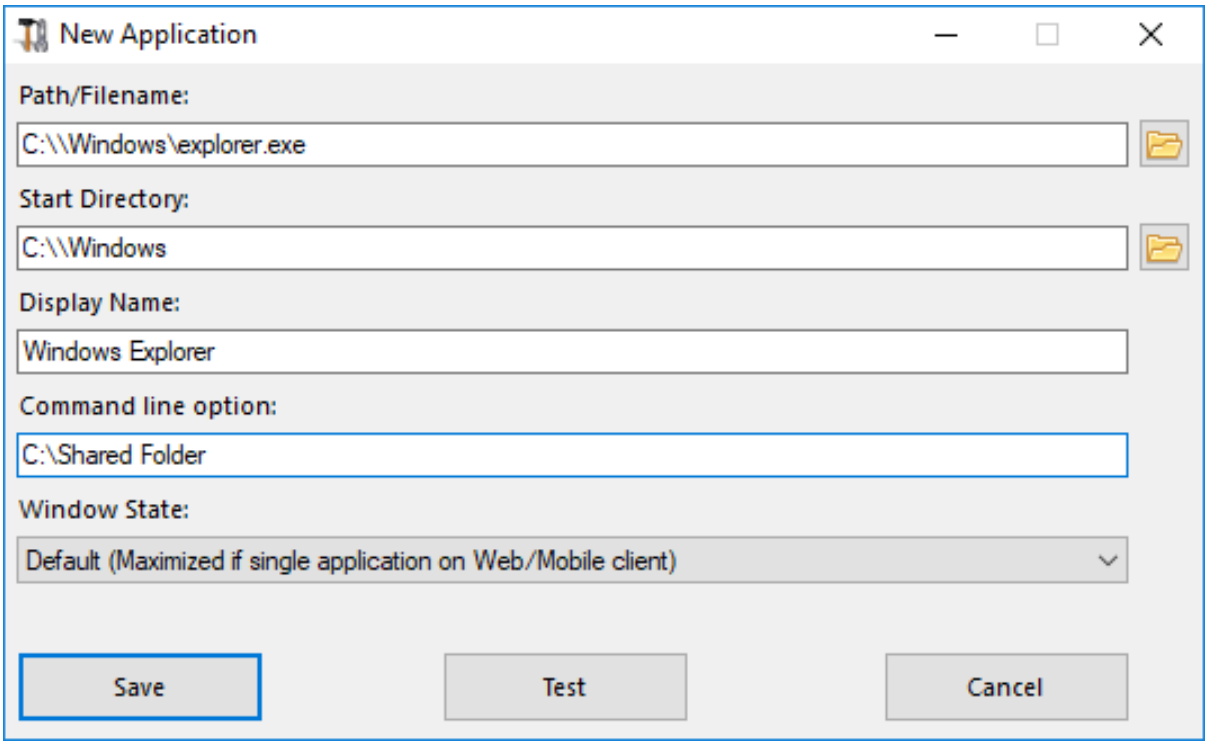
이 바로가는 경로는 사용자의 프로필 바탕화면 폴더에 복사할 수 있으며, 또는 사용자를 위한 애플리케이션으로 폴더.exe를 게시할 수 있습니다. 최신 방법을 선택하는 경우, 명령줄 옵션 섹션에서 폴더의 경로를 지정해야 합니다.



문서 폴더를 공유하는 대안 방법이 있습니다.

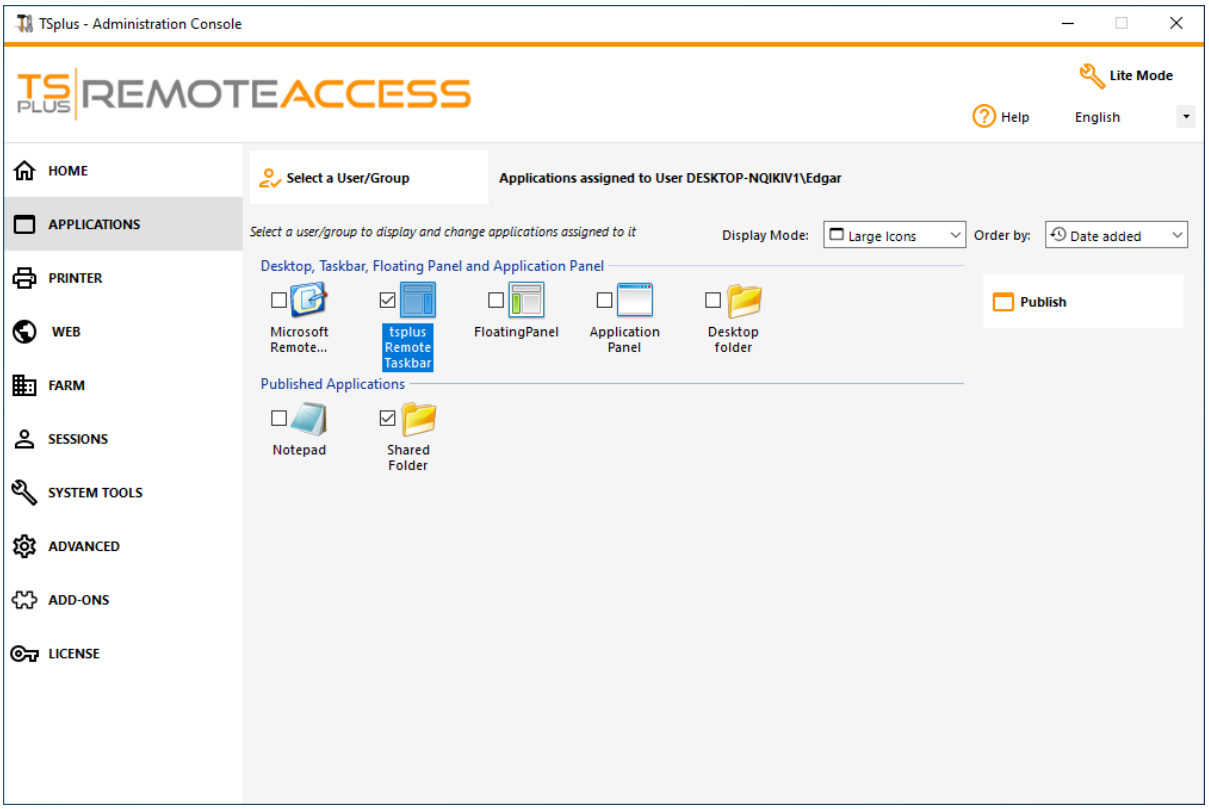
공유 폴더를 고유한 애플리케이션으로 게시하기:

새로운 애플리케이션을 추가합니다. 표시 이름에 공유 폴더의 이름이나 원하는 이름을 입력하세요. "경로/파일 이름" 필드 오른쪽에 있는 찾아보기 버튼을 클릭하고 C:\Windows\explorer.exe를 찾습니다. 시작 디렉터리는 explorer.exe의 경로로 자동으로 채워집니다. 명령줄 옵션 필드에 공유 폴더의 경로를 입력하세요. 로컬 폴더나 UNC 경로를 사용하는 네트워크 공유 폴더일 수 있습니다 (예: \data\shared folder). 아래 필드에 공유 폴더 정보를 입력하세요.

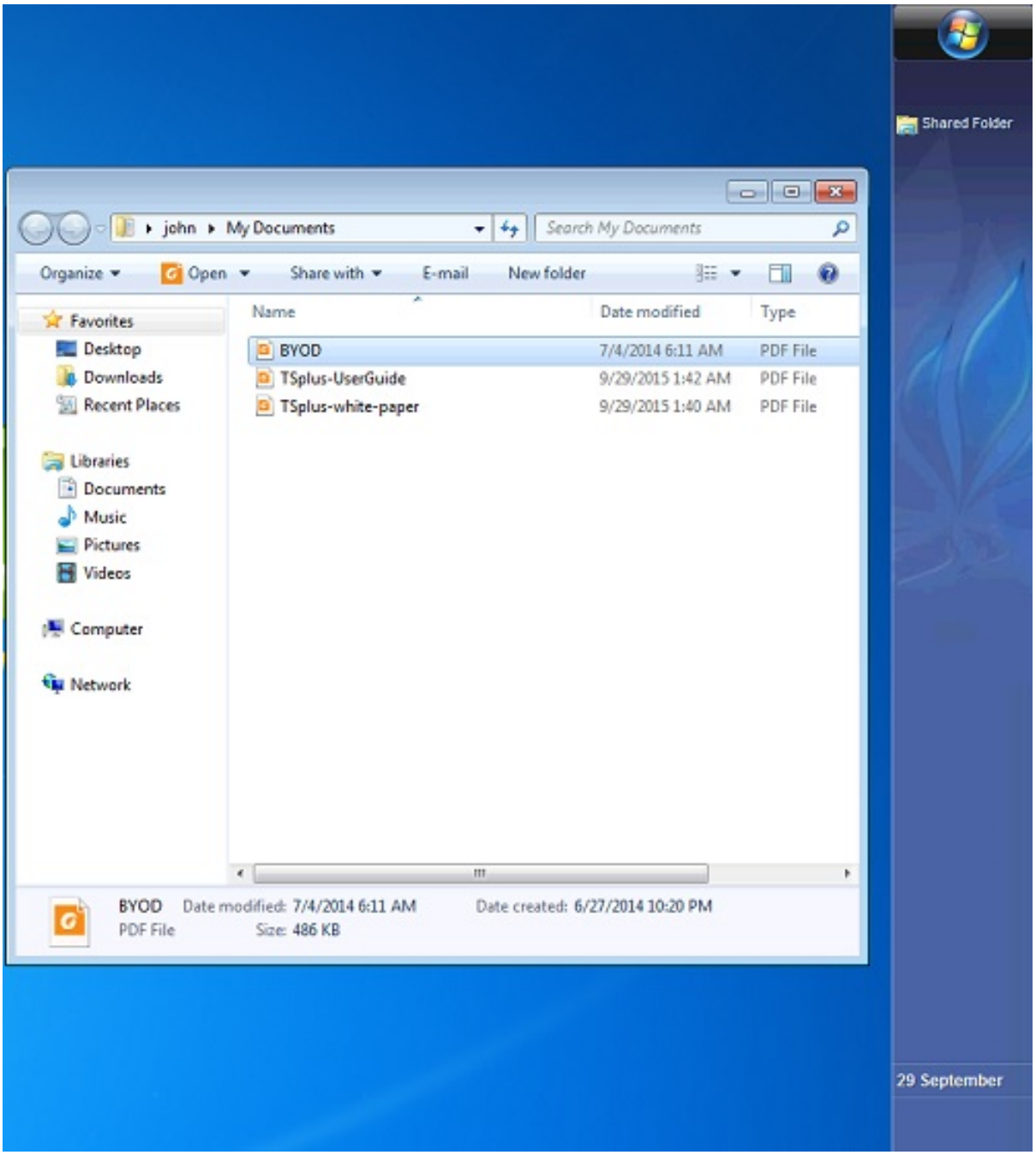


그런 다음 "저장"을 클릭하십시오.

“사용자” 탭을 클릭하세요. 사용자를 선택하고 TSplus Remote Taskbar 및 Shared Folder 상자를 확인하세요.

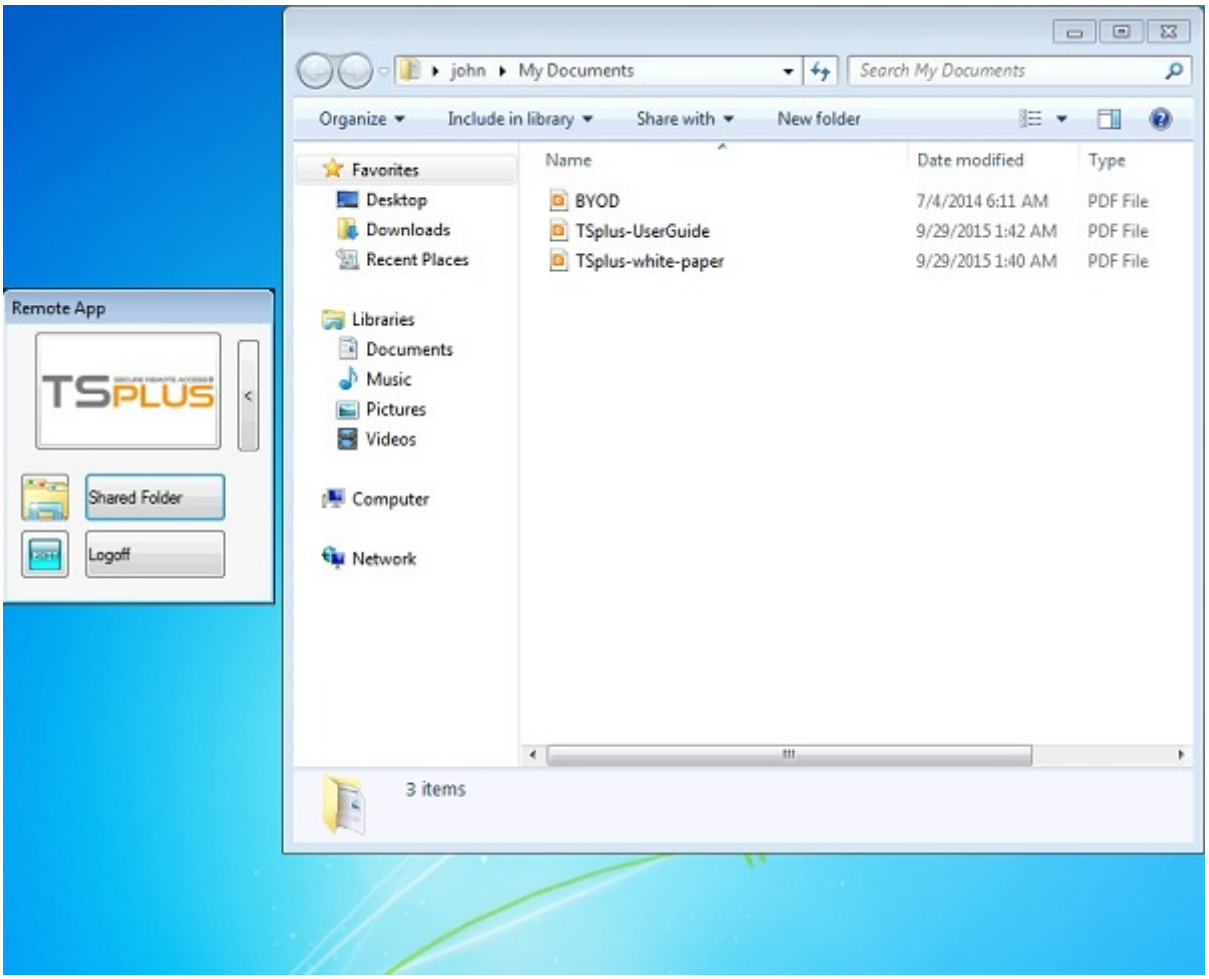


세션을 rdp 클라이언트로 열면 공유 폴더 애플리케이션이 있는 TSplus 작업 표시줄이 표시됩니다.



이 작업은 플로팅 패널로도 수행할 수 있습니다. 관리 도구를 열고 "응용 프로그램 할당" 탭을 클릭하십시오. 플로팅 패널 및 공유 폴더 상자를 선택하십시오.

여기 결과입니다:


Remote App
TSPLUS
Shared Folder
Logoff
john ▸ My Documents
Search My Documents
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
BYOD
7/4/2014 6:11 AM
PDF File
TSplus-UserGuide
9/29/2015 1:42 AM
PDF File
TSplus-white-paper
9/29/2015 1:40 AM
PDF File
3 items

무료 및 설치가 쉬운 HTTPS 인증서

개요

https://demo.tsplus.net/software/html5.html?user=demo&pwd=demo&program=c:\\windows\\system32\\notepad.exe&startupdir=c:\\windows\\system32¶ms=

3번의 마우스 클릭으로 자동으로 갱신되고 TSplus 내장 웹 서버에 자동으로 구성된 유효한 보안 인증서를 받을 수 있습니다.

이 기능은 사용합니다 렛츠 인크립트 무료 및 안전한 HTTPS 인증서를 귀하의 HTTPS 연결에 제공하기 위해.

필수 조건

귀하의 TSplus 서버가 무료 인증서 관리자를 사용하기 전에 이러한 요구 사항을 충족하는지 확인하십시오.

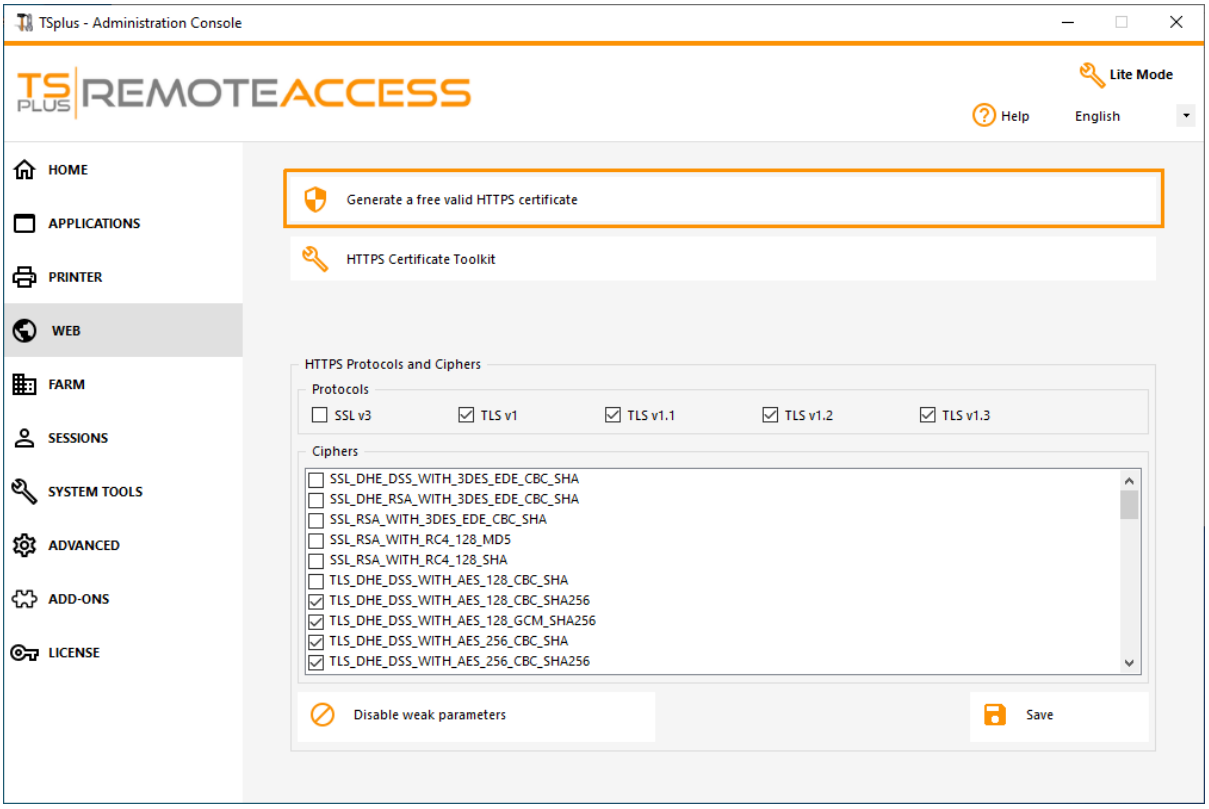
- 당신은 반드시 **TSplus 내장 웹 서버를 사용하여 HTTP를 위해 포트 80에서 수신 대기합니다.** 이것은 Let's Encrypt 도메인 소유권 검증 프로세스에 의해 요구됩니다.
- 당신의 **서버의 도메인 이름에 접근할 수 있어야 합니다.** 공용 인터넷에서. 이는 귀하가 도메인의 실제 소유자임을 확인하는 데 필요합니다.
- 당신은 반드시 **이 프로그램을 게이트웨이 서버 또는 독립형 서버에서 실행하고, 애플리케이션 서버에서는 실행하지 마십시오.** (공용 인터넷에서 접근할 수 있고 공용 도메인 이름이 있는 경우는 제외합니다.)

IP 주소에 대한 인증서를 받을 수 없습니다. 공용이든 사설이든 관계없이.

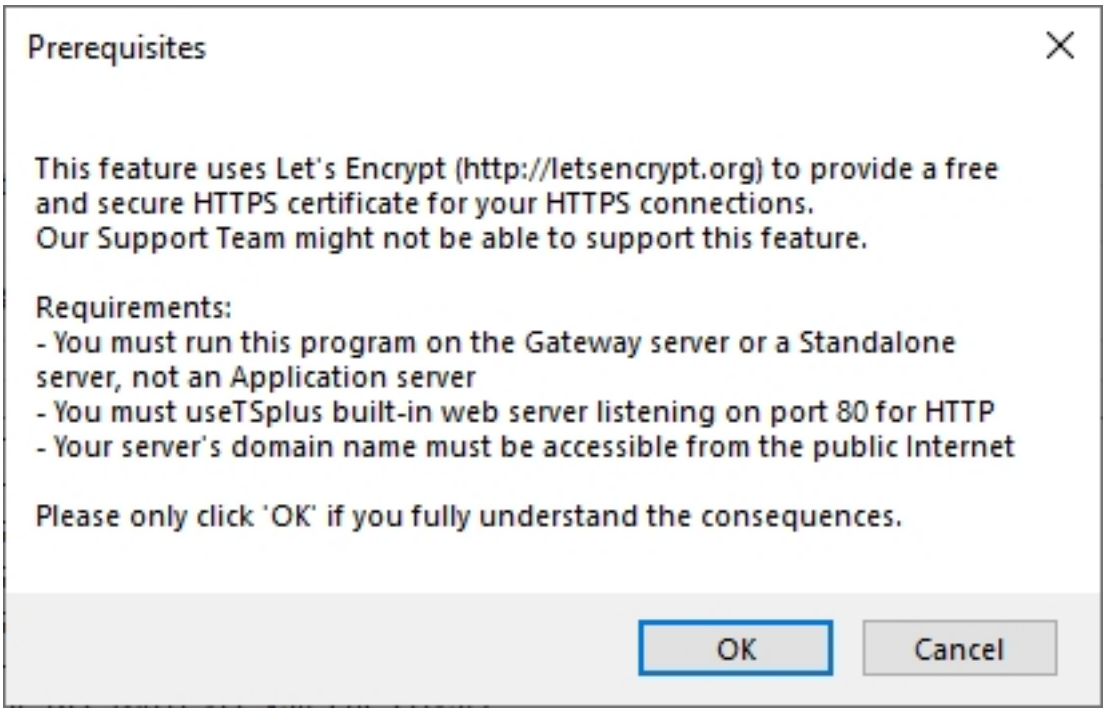
내부 도메인 이름(즉, 귀하의 개인 네트워크 내에서만 해결되는 도메인)에 대한 인증서를 받을 수 없습니다.

무료 인증서 관리자 GUI

TSplus 무료 인증서 관리자 GUI를 열려면 TSplus AdminTool을 열고 “웹 - HTTPS” 탭을 클릭한 다음 아래 스크린샷에 표시된 “무료 유효한 HTTPS 인증서 생성”을 클릭하십시오.



무료 인증서 관리자 GUI가 열리고 아래 스크린샷에 표시된 대로 필수 조건에 대해 알려줍니다.



서버가 모든 요구 사항을 충족하는지 주의 깊게 읽고 확인한 후 “확인” 버튼을 클릭하십시오.

1단계: 이메일을 입력하세요

이 이메일은 스팸으로 사용되지 않습니다. 실제로 이 이메일은 TSplus나 인증서 발급자인 Let’s Encrypt를 제외한 어떤 제3자에게도 전송되지 않습니다.

필요한 경우에만 서비스 약관에 따라 연락을 드릴 것입니다.

2단계: 서버의 도메인 이름을 입력하세요

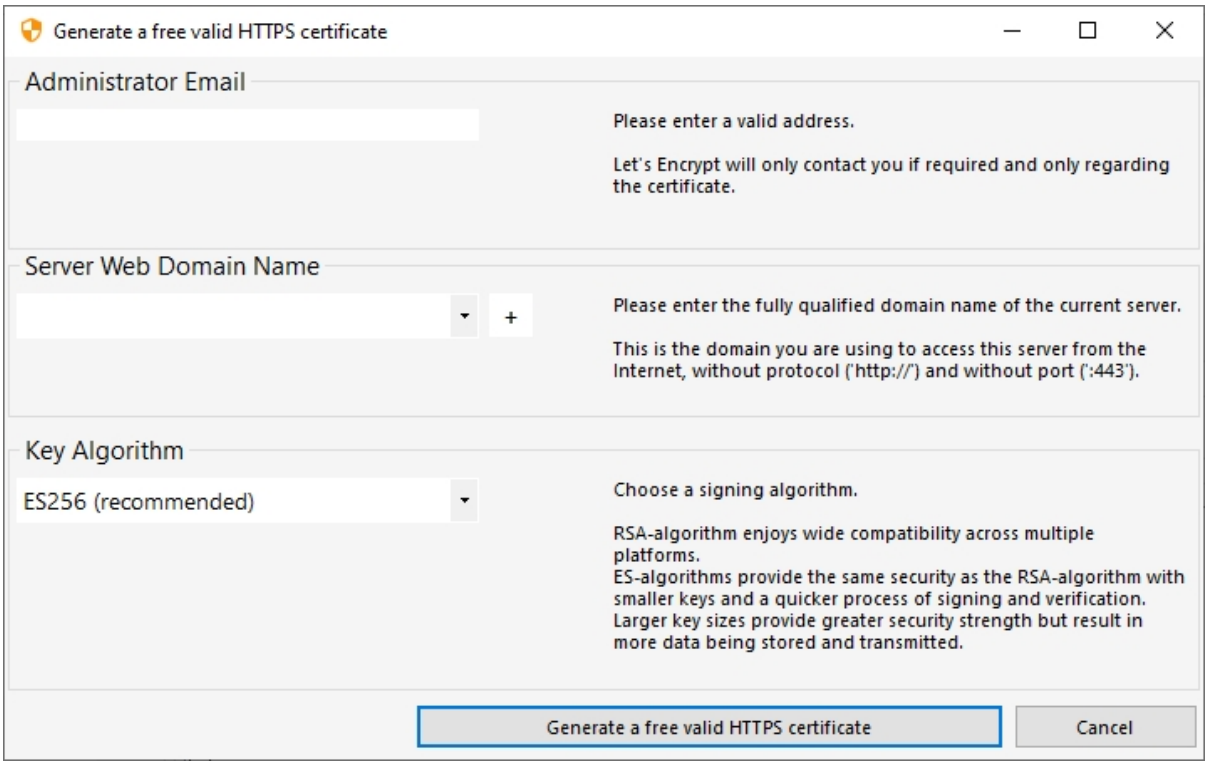
이것은 공용 인터넷에 접근 가능한 도메인 이름으로, gateway.your-company.com과 같은 것입니다. ”+” 버튼을 클릭한 후 다른 도메인 이름이나 서브도메인 이름을 추가할 수도 있습니다.

GUI에서 설명한 대로 프로토콜 접두사 및/또는 포트 접미사를 추가하지 말고, 깨끗한 도메인 이름만 입력하십시오.

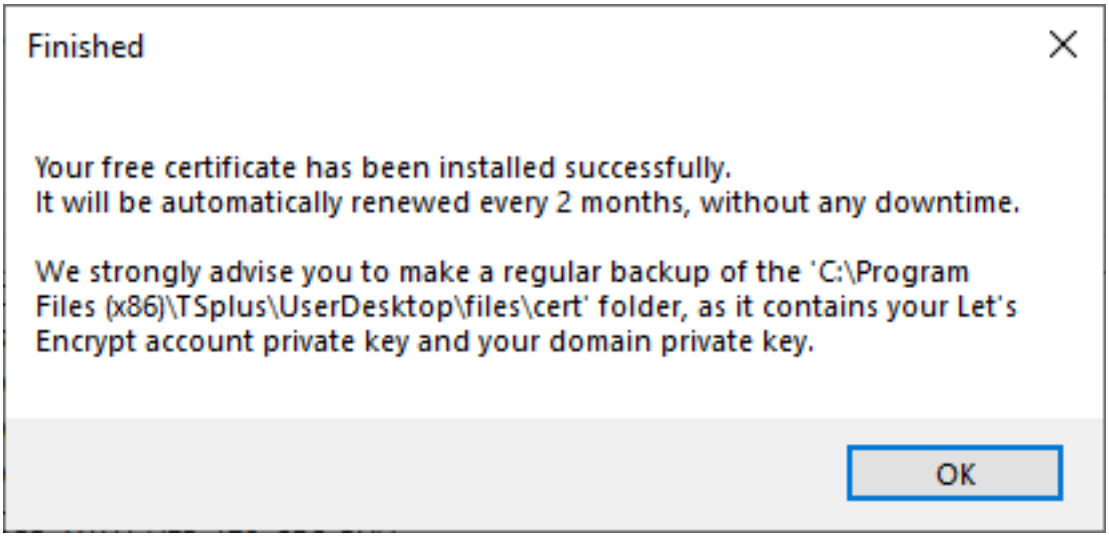
이 도메인 이름에 대해 인증서가 생성되며, 이 도메인 이름에서 호스팅되는 웹 페이지에서만 유효합니다. 사용자가 귀하의 웹 포털에 연결하는 경우 https://server1.example.com:1234 서버 1.example.com을 입력해야 합니다.

3단계: 키 알고리즘 선택

키 쌍을 생성하고 디지털 서명 작업을 수행하는 데 사용됩니다.



인증서를 즐기세요!



TSplus 무료 인증서 관리자는 이제 모든 데이터를 사용하여 Let's Encrypt와 연결하고, 입력한 도메인 이름을 실제로 소유하고 있는지 확인하며, 일치하는 유효한 인증서를 받을 것입니다.

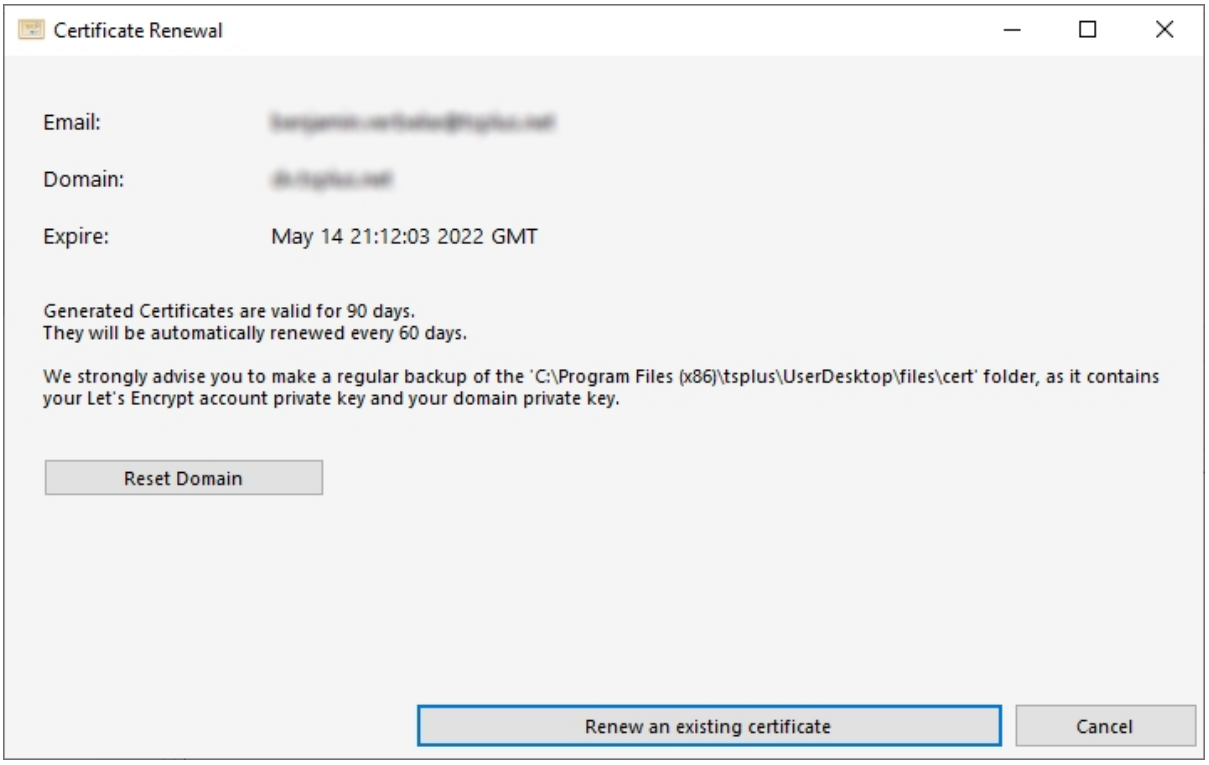
프로그램이 인증서를 수신하면, 모든 필요한 파일 형식 변환을 자동으로 처리하고 새로운 인증서를 모든 새로운 연결에 적용하기 위해 TSplus 내장 웹 서버를 부드럽게 다시 로드합니다. 웹 서버는 **아니다** 재시작되었고 연결이 중단되지 않았습니다.

인증서 갱신

Let’s Encrypt 인증서는 90일 동안 유효합니다. 유효 기간은 2028년까지 절반인 45일로 단축되며, 업계의 나머지 부분도 마찬가지입니다.

TSplus는 안전을 위해 15일마다 인증서를 자동으로 갱신합니다. Windows 서버가 재부팅될 때마다 확인이 이루어지며, 그 후 매 24시간마다 확인됩니다.

무료 인증서 관리자 도구를 열어 인증서를 수동으로 갱신할 수 있습니다. 아래 스크린샷에 표시된 대로 인증서의 도메인 이름과 만료 날짜가 표시됩니다.



수동으로 인증서를 갱신하려면 “다음” 버튼을 클릭하기만 하면 됩니다.

이 창의 "도메인 재설정" 버튼은 SSL 인증서를 삭제하고 인증서 관리자를 사용하기 전의 원래 상태로 웹 서버를 재구성합니다.

모범 사례

오류가 발생하지 않으면, TSplus는 매 15일마다 인증서를 자동으로 갱신합니다. 우리는 당신이 **45일마다 확인하십시오.** 귀하의 인증서가 자동으로 갱신되었음을 알려드립니다. Let's Encrypt는 현재 90일 동안 유효한 인증서를 발급하며, 이는 2028년까지 45일로 줄어들 것입니다.

우리는 또한 당신에게 권장합니다. **매달 최소한 한 번 백업하십시오.** 다음 폴더 및 그 하위 폴더:

C:\Program Files (x86)\TSplus\UserDesktop\files.lego

이것은 귀하의 Let’s Encrypt 계정 개인 키와 인증서의 키 쌍을 포함하는 내부 폴더입니다.

문제 해결

오류 발생 시 지원팀에 문의하시고 다음 로그 파일을 이메일로 보내주십시오.

C:\Program Files (x86)\TSplus\UserDesktop\files.lego\logs\cli.log

이 로그 파일(그리고 아마도 같은 폴더에 있는 다른 로그 파일들)은 우리 지원 팀이 문제를 조사하고 더 잘 이해하는 데 도움이 될 것입니다.

이전에 사용했던 인증서를 복원하려면 폴더로 이동:

C:\Program Files (x86)\TSplus\Clients\webserver

모든 “cert.jks” 파일이 포함됩니다. 이들은 “키 저장소” 파일이며 우리는 절대 삭제하지 않고, 단지 비활성화된 날짜와 시간으로 이름을 변경합니다.

오류 코드

- 오류 801: 무료 인증서 관리자가 귀하의 Let's Encrypt 계정을 등록할 수 없습니다. 인터넷 연결을 확인하십시오. 귀하의 이메일이 이미 Let's Encrypt에 등록되어 있지 않은지 확인하십시오. 다른 이메일로 다시 시도하십시오.

- 오류 802 및 오류 803: 무료 인증서 관리자가 Let's Encrypt 서비스 약관 URL 주소를 가져올 수 없습니다. 이는 차단되지 않는 오류입니다: 계속 진행하고 Let's Encrypt 서비스 약관을 수락할 수 있습니다 - 물론 먼저 브라우저에서 읽어보는 것을 잊지 마세요.

- 오류 804: 무료 인증서 관리자가 Let’s Encrypt 서비스 약관에 대한 귀하의 동의를 Let’s Encrypt 서버와 확인할 수 없습니다. 인터넷 연결을 확인하십시오. 다시 시도하십시오.

- 오류 805 및 오류 806: 무료 인증서 관리자가 인증서 생성(오류 805) 또는 인증서 갱신(오류 806) 중에 입력한 도메인을 소유하고 있는지 확인할 수 없습니다. 모든 전제 조건을 다시 확인하십시오. 인터넷 연결을 확인하십시오. 웹 서버가 포트 80에서 수신 대기 중인지 확인하십시오. IIS 또는 Apache와 같은 타사 웹 서버를 사용하지 않는지 확인하십시오. 도메인 이름이 공용 인터넷에서 접근 가능한지 확인하십시오.

HTTPS 인증서 명령줄

인증서 구성 파일 준비

"C:\Program Files (x86)\TSplus\UserDesktop\files\cert" 폴더 안에 "FreeCertificateManager.ini"라는 이름의 파일이 아직 존재하지 않는 경우 생성하십시오. 텍스트 편집기 및/또는 Windows 파일 탐색기가 끝에 ".txt" 확장자를 추가하지 않도록 하십시오.

파일을 편집하고 다음 형식으로 작성하거나 업데이트한 후 저장하십시오:

설정

이메일 = your.email@company.com

domain = your-server-domain-name.company.com

인증서 생성

서버 관리자 권한으로 다음 명령을 실행하십시오:

C:\Program Files (x86)\TSplus\UserDesktop\files\cert\CertificateManager.exe" /create

이 명령이 성공적으로 실행되기 위해서는:

- "FreeCertificateManager.ini" 파일이 존재해야 하며 예상 형식을 사용해야 합니다.
- 귀하의 TSplus Remote Access 서버는 가동 중이어야 합니다.
- 귀하의 TSplus Remote Access 웹 포털은 프로토콜과 함께 사용 가능해야 합니다.

인터넷 공용 네트워크의 포트 80에서 HTTP, TSplus HTTPS 인증서 제공자가 이를 사용하여 서버 도메인 이름을 검증합니다.

인증서 갱신

인증서가 구성되고 생성되면, TSplus Remote Access는 만료되지 않도록 매 두 달마다 자동으로 갱신합니다.

타사 인증서 추가

"C:\Program Files (x86)\TSplus\UserDesktop\files\cert" 폴더 안에 인증서 비밀번호만 포함된 "certpassword.txt"라는 이름의 파일을 생성합니다. 서버 관리자 권한으로 다음 명령을 실행합니다:

C:\Program Files (x86)\TSplus\UserDesktop\files\cert\CertificateManager.exe /add your-certificate-path

TSplus Advanced Security를 사용하고 있다면 기능이 작동하도록 지리적 보호 기능을 일시적으

로 비활성화해야 할 수 있습니다. 명령을 실행한 후 비밀번호 파일을 삭제할 수 있습니다.

RDP 접근을 차단하고 게이트웨이 서버에서 HTTP를 허용합니다.

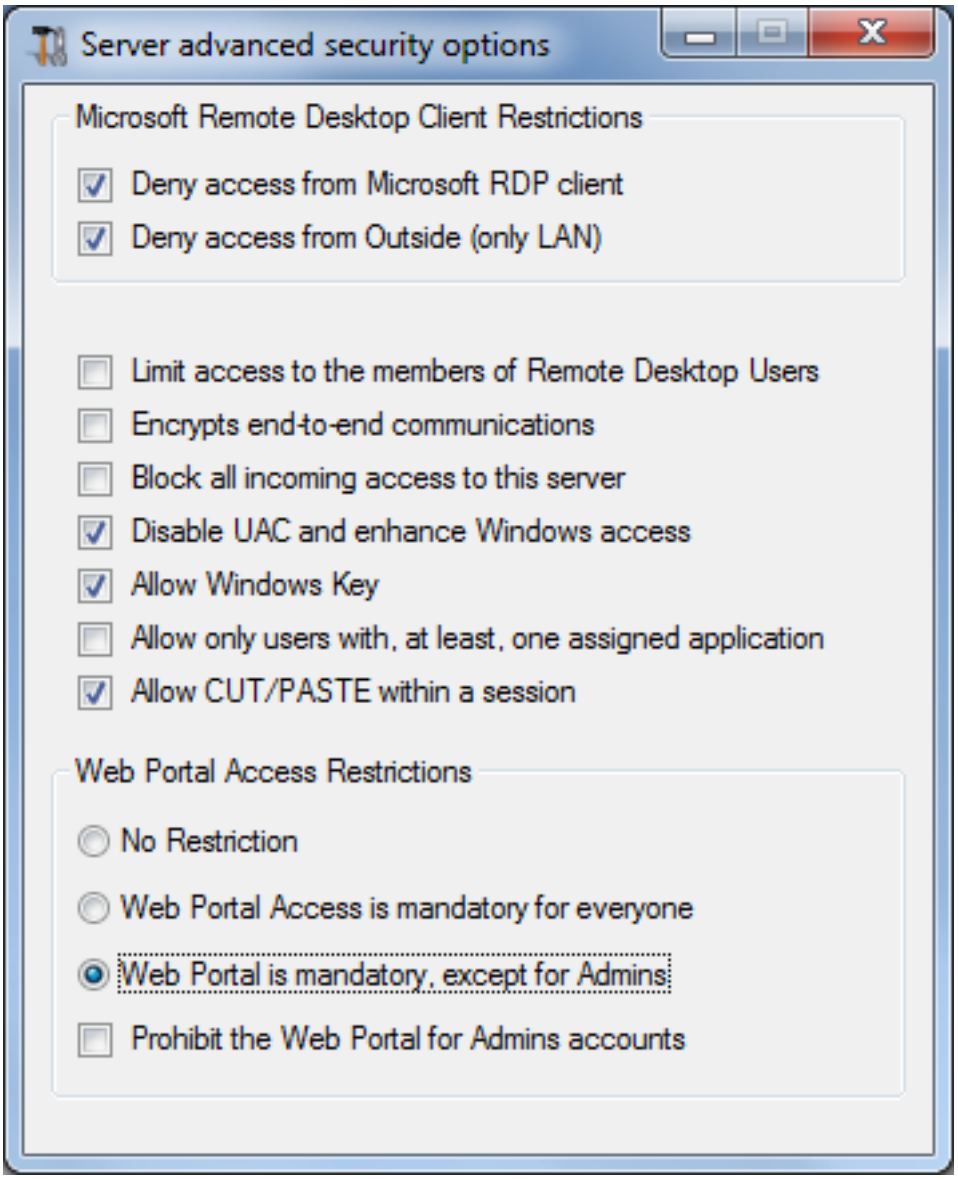
게이트웨이 서버에 접근하는 방법은 2가지가 있습니다:

- HTML5 / HTML
- RDP 세션 (게이트웨이 IP/DNS – 포트 번호)

HTML/HTML5 잠금 설정 방법

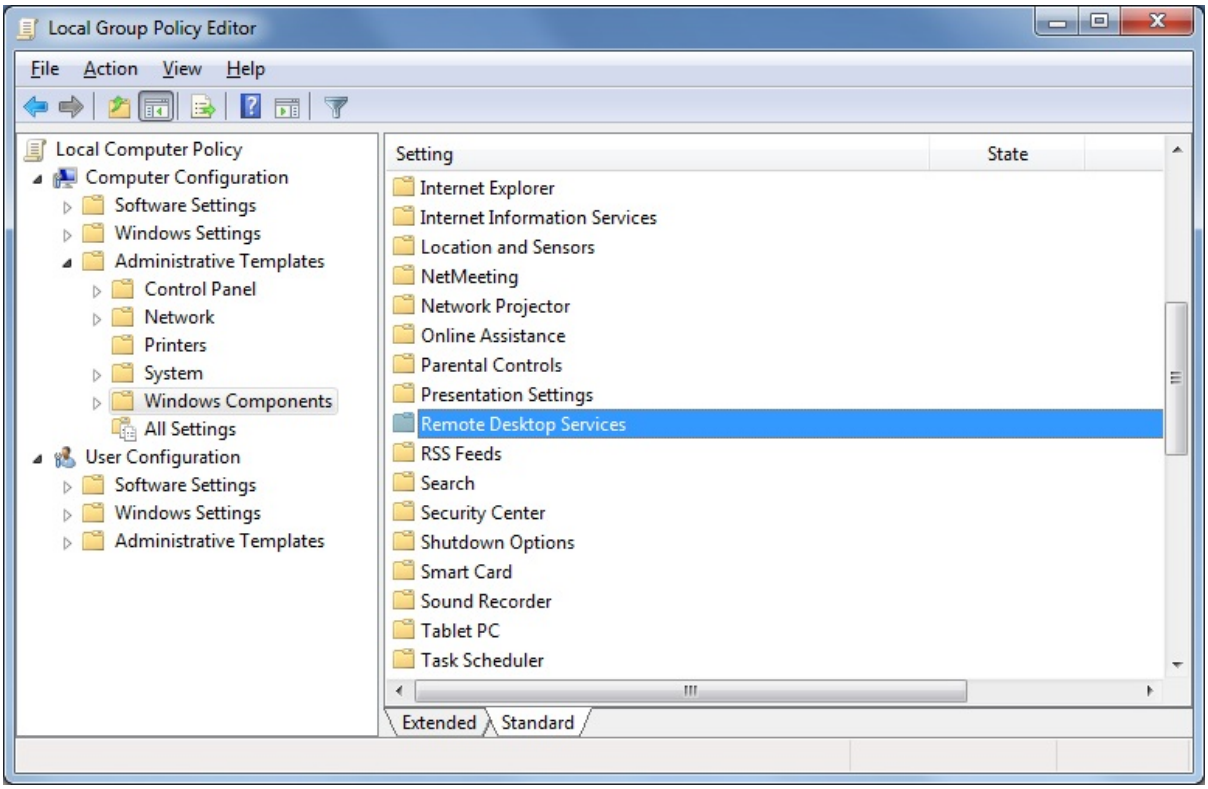
mstsc를 PORT 번호와 함께 사용하여 TSplus 애플리케이션 / 게이트웨이 서버에 RDP로 접속할 수 있습니다.

그러나 Gateway Server의 TSplus Admin Console에 위치한 이러한 고급 보안 도구를 사용하면, 보안 타일/탭으로 이동한 다음 고급 보안 옵션 타일을 클릭하여…

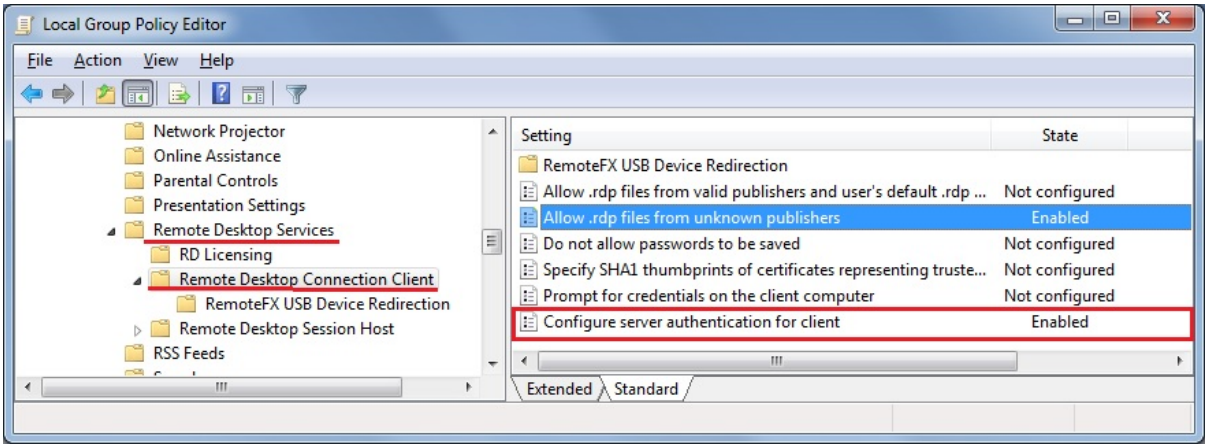


접속이 RDP로 연결하려고 할 때 거부됩니다. 이 동작을 피하기 위해, 게이트웨이 서버에서 다음을 수행해야 합니다:

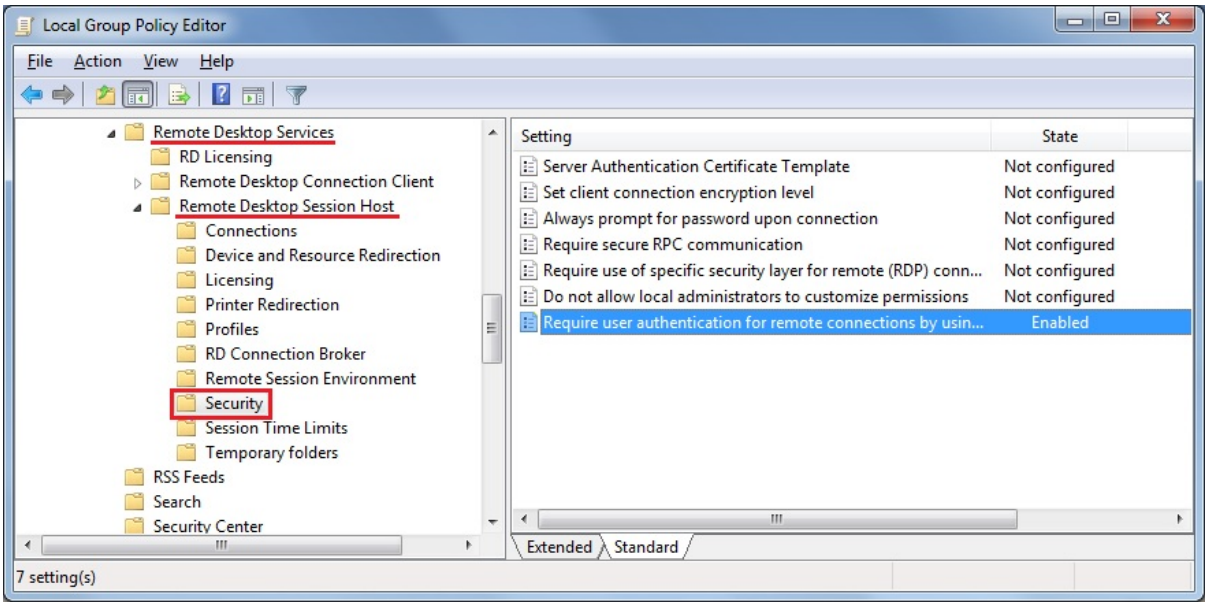
- Gpedit.msc로 이동한 다음, 컴퓨터 구성에서 관리 템플릿 폴더를 클릭하고, Windows 구성 요소 폴더와 원격 데스크톱 서비스에서 클릭합니다.



- 그런 다음 원격 데스크톱 연결 클라이언트 폴더를 클릭하고 “알 수 없는 게시자에서 .rdp 파일 허용” 설정을 두 번 클릭하여 활성화하고, “클라이언트에 대한 서버 인증 구성”도 활성화합니다.



- 원격 데스크톱 클라이언트 메뉴에서 원격 데스크톱 세션 호스트 폴더를 클릭한 다음 보안 폴더를 클릭합니다. "네트워크 수준 인증을 사용하여 원격 연결에 대한 사용자 인증 요구" 설정을 활성화합니다.

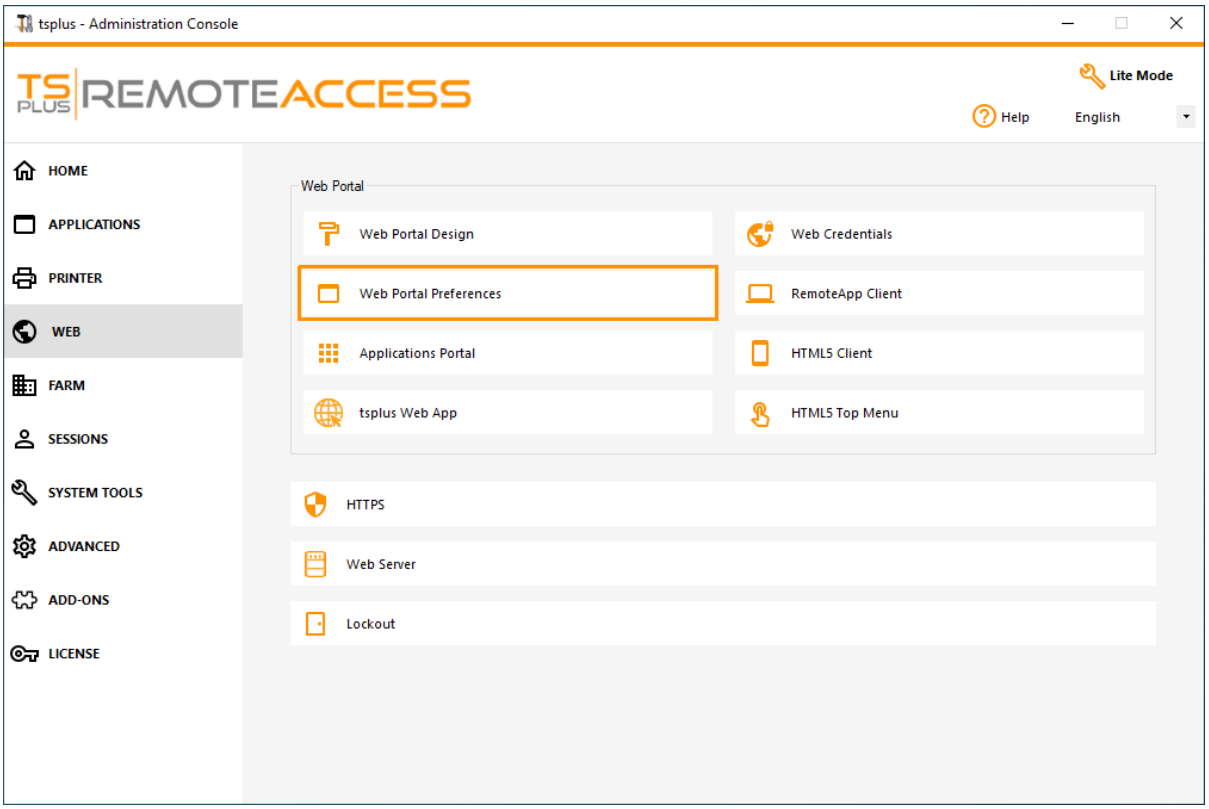

Local Group Policy Editor
File Action View Help
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment
Security
Session Time Limits
Temporary folders
RSS Feeds
Search
Security Center
Setting
State
Server Authentication Certificate Template
Not configured
Set client connection encryption level
Not configured
Always prompt for password upon connection
Not configured
Require secure RPC communication
Not configured
Require use of specific security layer for remote (RDP) conn...
Not configured
Do not allow local administrators to customize permissions
Not configured
Require user authentication for remote connections by usin...
Enabled
Extended
Standard
7 setting(s)

게이트웨이 서버를 수동으로 활성화/비활성화합니다.

개요

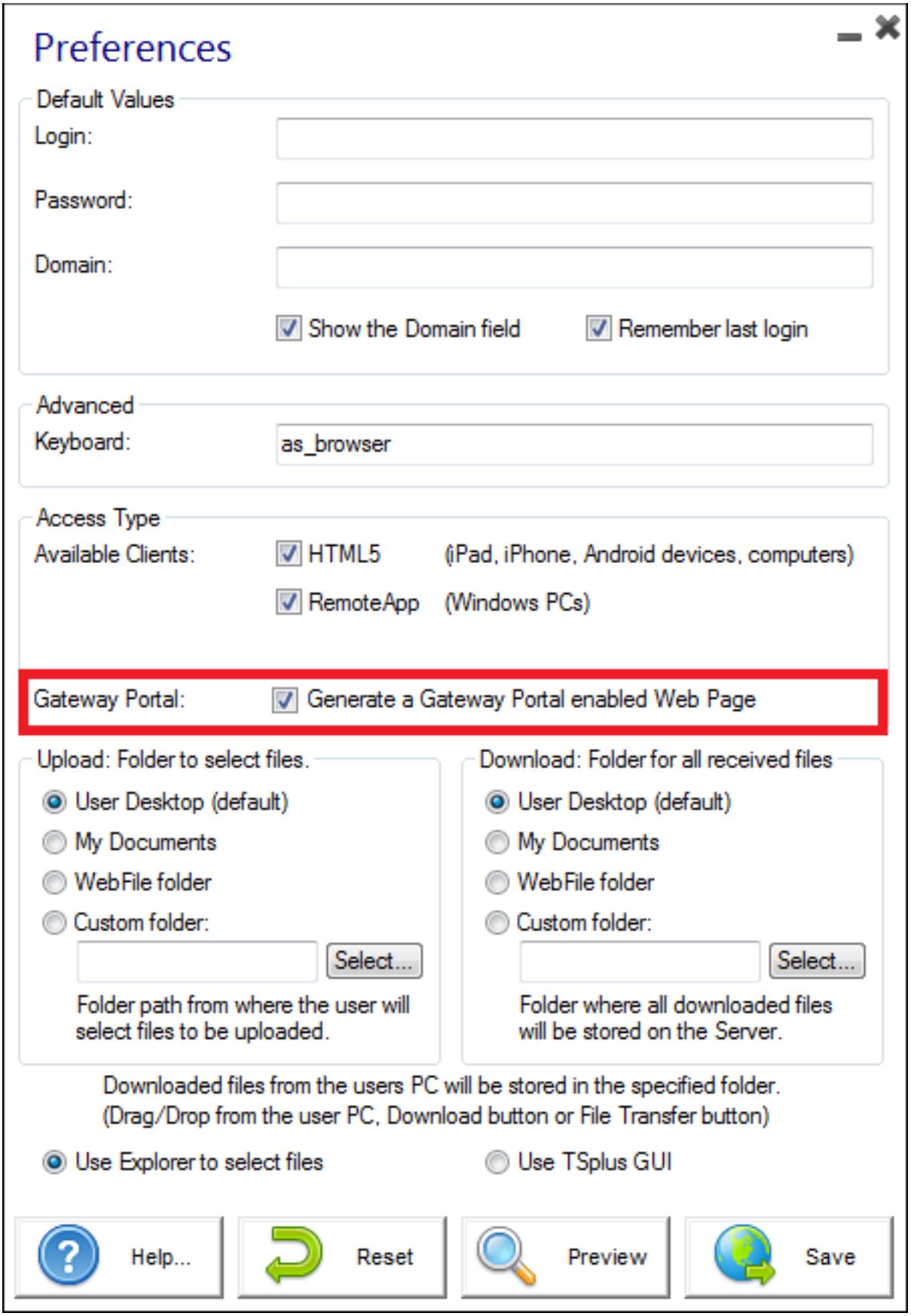
농장 구성에 따라 농장 컨트롤러는 자동으로 자신의 웹 포털 설정을 변경하여 게이트웨이 서버가 됩니다. 사용자가 Farm Controller의 TSplus 웹 포털에서 연결할 수 있도록 하여 Farm Controller 자체에 직접 연결하지 않고 Farm의 애플리케이션 서버 중 하나에 연결할 수 있습니다.

그러나 이 동작을 수동으로 변경하려면 "WEB" 타일을 클릭한 다음 웹 포털 기본 설정 버튼을 클릭하면 됩니다.



- 게이트웨이 포털이 농장 컨트롤러(현재 구성 중인 서버)의 게이트웨이 서버가 되어 사용자를 농장의 애플리케이션 서버로 리디렉션하려면 "게이트웨이 포털이 활성화된 웹 페이지 생성" 상자를 선택하십시오.

- “게이트웨이 포털이 농장 컨트롤러 자체로 리디렉션되어 농장 구성을 우회하도록 하려면 '게이트웨이 포털이 활성화된 웹 페이지 생성' 상자의 선택을 해제하십시오.”



“저장”을 클릭하여 이 설정을 저장하십시오.

하드웨어 식별자 및 클론 서버

1- 하드웨어 식별자 변경.

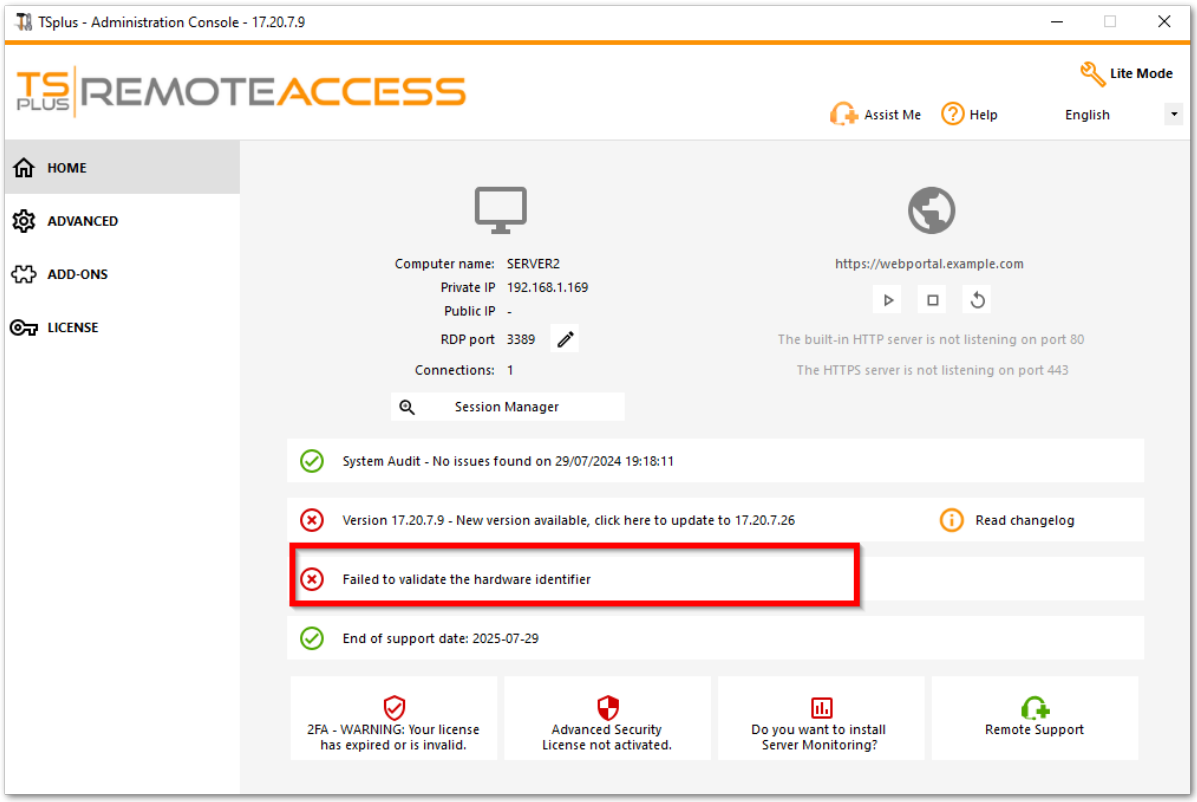
클로닝 또는 업데이트 후 하드웨어 식별자 수리.

경고: 하드웨어 식별자 유효성 검사에 실패했습니다.

물리 서버를 가상 머신으로 마이그레이션하거나 커널 Microsoft 업데이트를 수행한 후, 라이센스 상태가 새로운 하드웨어에서 하드웨어 식별자 유효성 검사 실패로 변경됩니다.

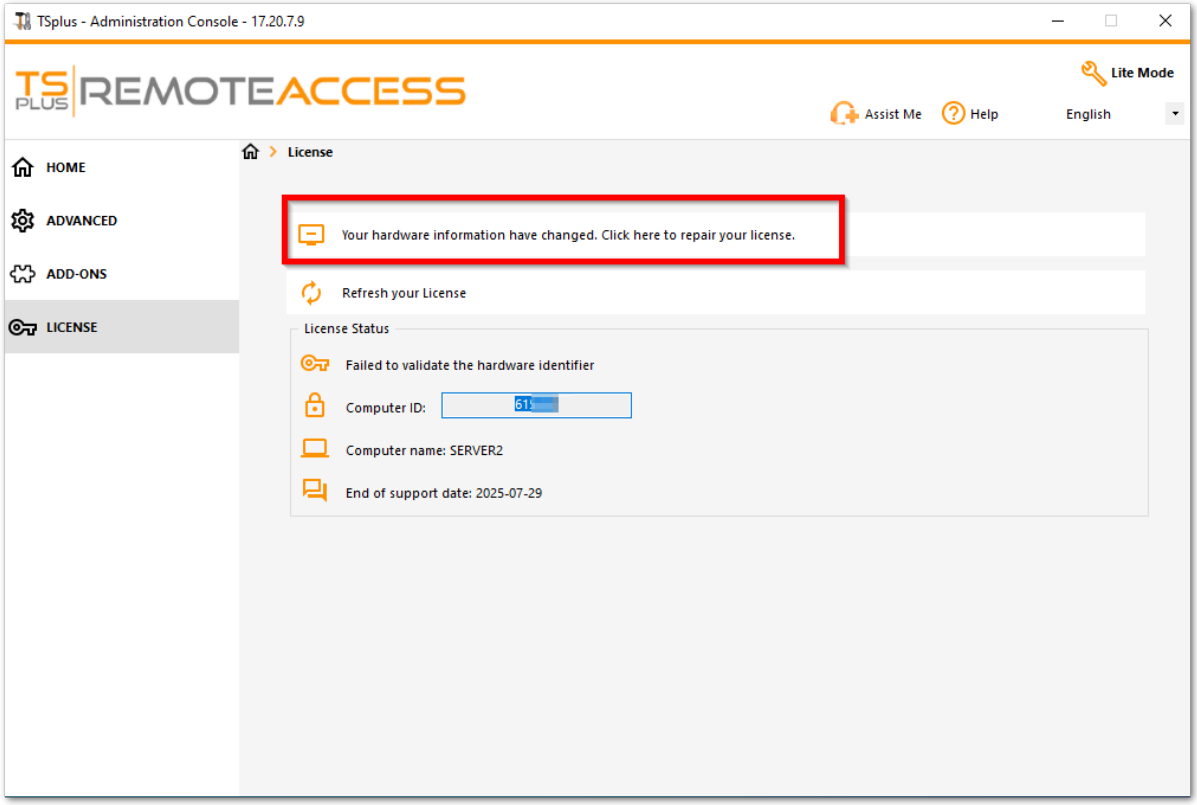
이 메시지는 TSplus가 동일한 컴퓨터 ID와 동일한 이름을 가진 한 서버에서 다른 서버로 복사된 라이센스 충돌을 감지했기 때문에 나타납니다.
새 서버의 이름을 변경할 것을 권장합니다 (예: SERVER1 > SERVER2)

- 서버를 재시작하세요



창을 클릭하여 라이센스 페이지로 이동하십시오.

그런 다음 "귀하의 하드웨어 정보가 변경되었습니다. 라이센스를 복구하려면 여기를 클릭하십시오." 탭을 클릭하십시오.



라이센스 복원 팝업이 열려 라이센스를 복원할 수 있습니다.

사례 1: 지원이 없습니다!
재호스팅은 불가능하므로 원래 서버에서 지원 구독을 신청하고 마이그레이션 작업을 다시 시작해야 합니다.
문제가 발생할 경우, 지원 문의 귀하의 컴퓨터 ID와 활성화 키를 입력하십시오.

사례 2: 이미 6개월 동안 재호스팅을 하셨습니다!
메시지: 지난 6개월 동안 이 컴퓨터를 이미 재호스팅했습니다. 라이센스 재호스팅에 도움이 필요하시면 지원팀에 문의하시기 바랍니다.

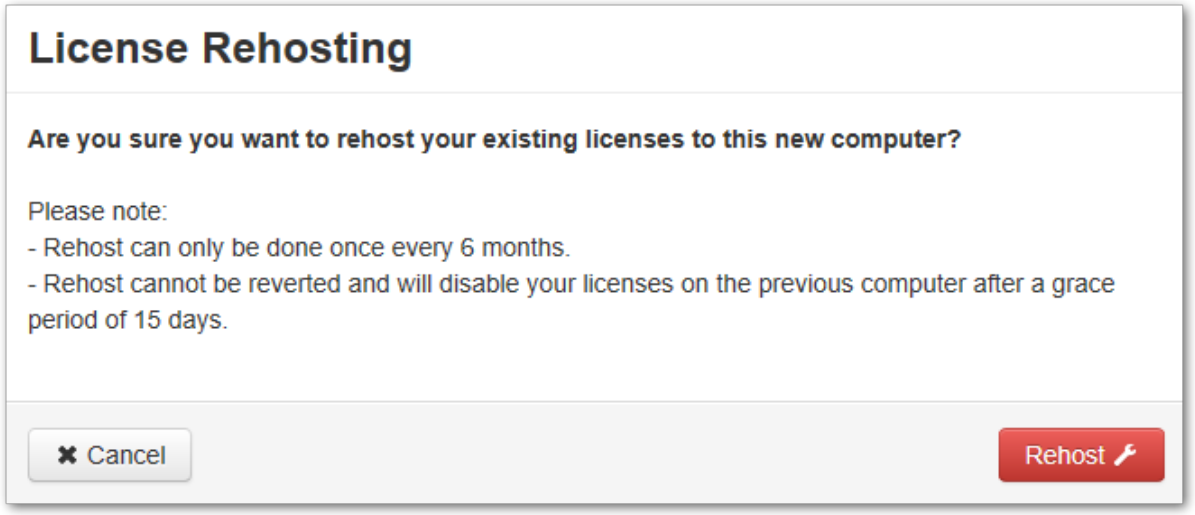
재호스팅은 따라서 불가능할 것입니다. 지원 문의 귀하의 컴퓨터 ID와 활성화 키를 입력하십시오.

사례 3: 지원이 있습니다!
다음 메시지가 나타납니다: 이 새로운 컴퓨터에서 기존 라이센스를 재호스팅 하시겠습니까?

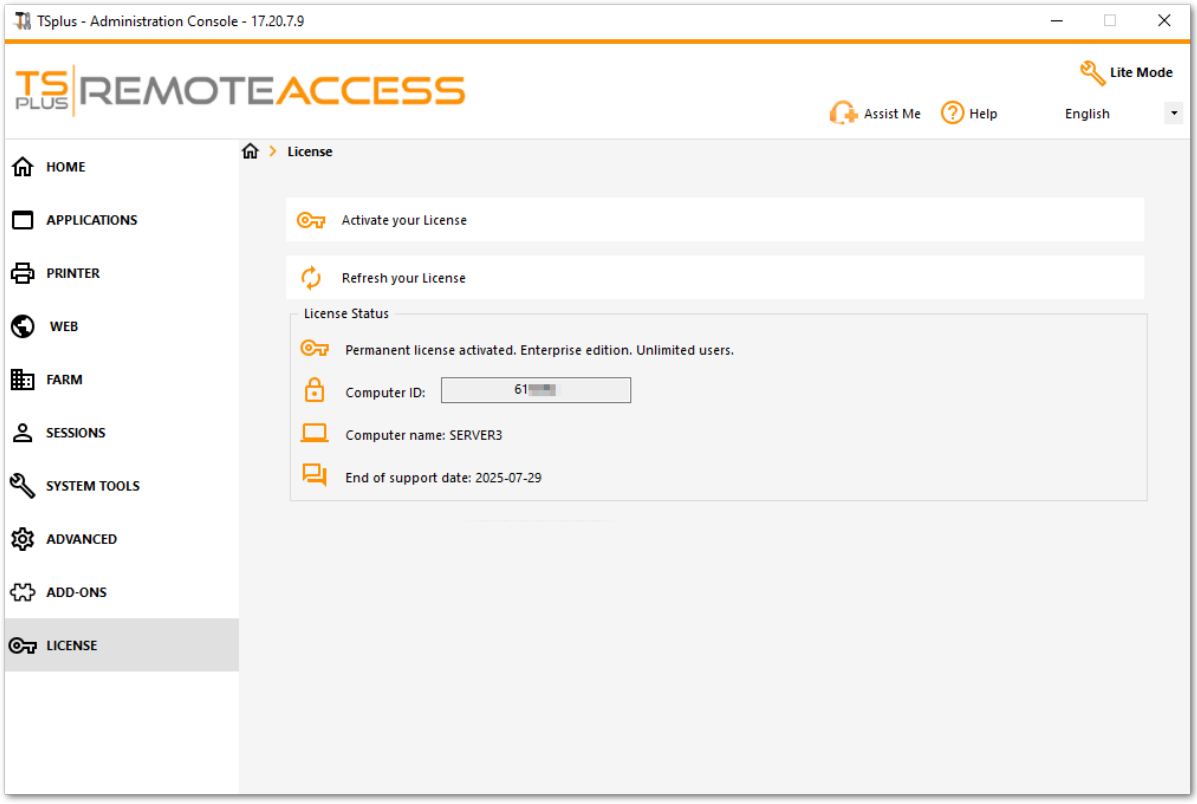
다음 사항에 유의하십시오:

- 재호스팅은 6개월에 한 번만 수행할 수 있습니다.
- 재호스팅은 취소할 수 없으며 15일의 유예 기간 후 이전 컴퓨터에서 라이센스가 비활성화됩니다.

클릭하세요 **"재호스팅"** 버튼

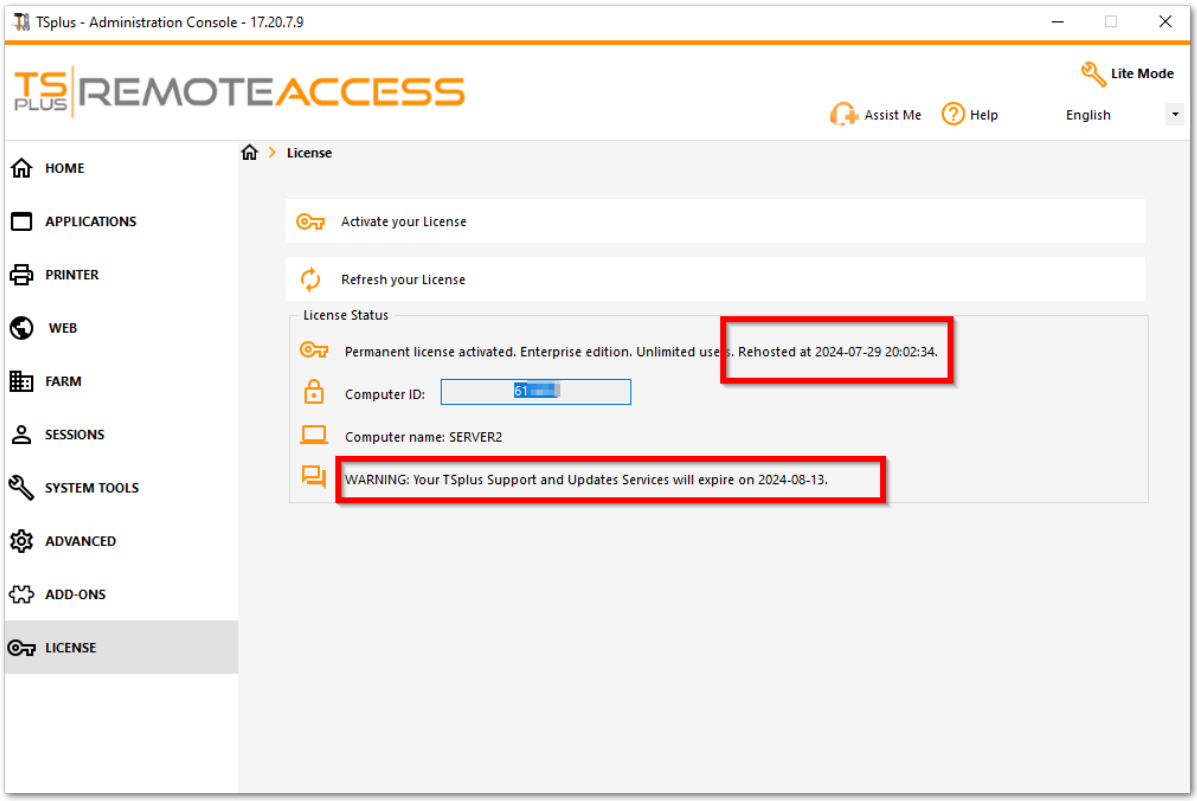


귀하의 라이센스가 재호스팅되었습니다!



노트: 이전 서버에는 재호스팅 날짜와 이전 서버 사용 기간 종료일(15일)이 표시된 메시지가 나타

납니다.



업데이트 실패:
업데이트 릴리스를 실행하고 서버를 재시작한 후 문제가 해결되었는지 확인하십시오.

- 다운로드하십시오 업데이트 릴리스

서버를 복제하면서 기존 서버를 유지하고 새로운 라이센스를 활성화합니다.

요구 사항

클론된 가상 머신을 사용할 때, 고유한 TSplus Remote Access 설치를 보장하고 라이센스 문제를 피하기 위해 컴퓨터 이름과 디스크 볼륨 ID를 수정하는 것이 중요합니다.

컴퓨터 이름 고려사항

컴퓨터 이름은 이미지 자체의 Windows 레지스트리에 저장됩니다. 이미지를 적용하기 전에 수정하면 Windows 부팅 시 Sysprep에 의해 덮어씌워집니다. 그러나 이름을 미리 정의할 수 있습니다. Unattended.xml 답변 파일. 보기 Microsoft 문서 자세한 내용은.

컴퓨터 이름을 설정하려면 다음 섹션을 내부에 추가하십시오. 마이크로소프트-윈도우-셸-설정 :

```
    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
        <ComputerName>%COMPUTERNAME%ComputerName>
    component>
```

볼륨 ID 고려사항

볼륨 ID는 디스크 파티션과 연결되어 있으며, OS 이미지와는 관련이 없습니다. 이미지를 적용하기 전에 변경할 수 있으며, 변경 사항은 유지됩니다. 사용하십시오. volumeid.exe Sysinternals에서 제공됨 Microsoft Sysinternals 윈도우가 부팅되기 전에.

배포 단계

새 가상 머신을 sysprepped 이미지에서 배포할 때, Windows는 첫 부팅 시 Out-Of-Box Experience (OOBE)에 들어가 구성 설정을 요청합니다.

배포를 위한 권장 단계:

1. **WinPE로 부팅** – 시스템을 Windows로 부팅하지 않고 준비합니다.
2. **볼륨 ID 설정** – 이미지를 적용하기 전에 변경하여 지속되도록 하세요.
3. **sysprepped 이미지를 배포하십시오** – DISM을 사용하여 이미지를 적용합니다. C: .
4. **컴퓨터 이름을 오프라인으로 설정** – 마운트된 이미지 내에서 레지스트리를 편집합니다.
5. **복사한 Unattended.xml 파일** – OOBE 구성을 자동화합니다. 이 파일은 배포 전에 스크립트를 사용하여 동적으로 수정할 수 있습니다.

6. **첫 부팅 스크립트 생성** – 최종 구성을 단 한 번의 재부팅으로 완료하십시오.
7. **Windows로 재부팅** – Windows는 지정된 구성을 사용하여 최종화됩니다.
8. **원격 액세스 라이센스 재설정** – 다음 명령을 실행하십시오:

터미널 창

```
AdminTool.exe /license /reset
```

이것은 라이센스를 재설정하고 새로운 라이센스를 적용합니다.

배포 스크립트

아래에 관련된 WinPE 배포 스크립트를 찾으십시오.

터미널 창

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"     # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive
```

```
    <# 3. Load Registry Offline to Set Computer Name #>
    Write-Host "Modifying Registry to Set Computer Name..."
    reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
    reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
    reg unload HKLM\TempSys

    <# 4. Ensure Unattended Setup is Used #>
    Write-Host "Copying Unattended File..."
    Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

    <# 5. Set the First Boot Script for Final Configurations #>
    Write-Host "Creating First Boot Script..."
    $FirstBootScript = @"
    Write-Host "Finalizing Configuration..."
    Rename-Computer -NewName "$ComputerName" -Force
    Restart-Computer -Force
    "@
    Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

    Write-Host "Deployment Complete! Rebooting into Windows..."
    Write-Host "================================================"
    Write-Host "  Computer Name: $ComputerName"
    Write-Host "  Volume ID: $VolumeID"
    Write-Host "  Image Applied to: $ApplyDrive"
    Write-Host "================================================"

    <# Reboot into Windows #>
    wpeutil reboot
```

라이센스 활성화

배포 후 라이센스를 활성화하면 가상 머신에 대한 새로운 컴퓨터 ID가 생성됩니다. 이 컴퓨터 ID는 머신이 평가판 또는 라이센스 활성화를 요청할 때 라이센스 포털에 의해 생성됩니다. 클론된 가상 머신의 경우 라이센스 활성화가 필수입니다. 활성화 키 또는 볼륨 라이센스 키를 사용하십시오.

오프라인 설정은 허용되지 않습니다 보안 문제로 인해. 자세한 활성화 단계는 다음을 참조하십시오. TSplus 명령어 목록 .

결론

이 가이드는 TSplus Remote Access로 클론된 가상 머신을 배포할 때의 주요 고려 사항을 설명합니다. 시스템을 올바르게 구성하고 라이센스를 부여하기 위한 필수 단계를 제공하며, 귀하의 필요와 요구 사항에 맞게 조정되어야 합니다.

웹 서버를 여러 네트워크 카드에 바인딩하는 방법

개요

일부 사용 사례에서는 Terminal Service Plus 웹 서버가 여러 네트워크 카드에서 수신 대기해야 할 수 있습니다. 예를 들어, 서버가 여러 다른 네트워크에 속하는 경우입니다.

이 기능은 이 특정 요구를 충족합니다.

여러 네트워크 카드에 웹 서버 바인딩

Terminal Service Plus 웹 서버를 여러 네트워크 카드에 바인딩하려면 다음이 필요합니다:

- “C:\Program Files (x86)\TSplus\Clients\webserver” 폴더에 “settings.bin” 파일을 생성합니다.
- 다음 줄을 추가하여 바인딩하려는 모든 네트워크 카드의 로컬 IP 주소를 모두 입력하십시오. 예를 들어:

  bind_nic=“127.0.0.3”,“127.0.0.4”
- 웹 서버를 재시작하십시오 (AdminTool > Web > 웹 서버 재시작) 변경 사항을 적용하기 위해

Terminal Service Plus 웹 서버는 이제 모든 바인딩된 네트워크 카드(우리의 예시에서는 바인딩이 127.0.0.3, 127.0.0.4 및 127.0.0.1로 자동으로 이루어질 것입니다)로부터의 모든 쿼리를 수신 대기합니다.

사용자 정의 HTTP 헤더 추가 방법

필수 조건

이 기능은 매우 기술적이며 이 문서는 기술 전문가만을 위한 것입니다.

HTTP 프로토콜과 HTTP 헤더에 익숙해야 합니다.

개요

일부 사용 사례에서는 Terminal Service Plus 웹 서버가 표준 HTTP 헤더 외에 하나 이상의 사용자 정의 HTTP 헤더를 반환해야 할 수 있습니다.

이 기능은 이 특정 요구를 충족합니다.

사용자 정의 HTTP 헤더 설정

자신만의 사용자 정의 HTTP 헤더를 추가하려면 다음이 필요합니다:

- “C:\Program Files (x86)\TSplus\Clients\webserver” 폴더에 “headers.bin” 파일을 생성합니다.
- 사용자 정의 헤더를 새 줄로 구분하여 추가하십시오. 예: header1=X-Frame-Options
- 웹 서버를 재시작하십시오 (AdminTool > Web > 웹 서버 재시작) 변경 사항을 적용하기 위해

Terminal Service Plus 서버는 이제 표준 HTTP 헤더 외에 이 사용자 정의 HTTP 헤더로 모든 쿼리에 응답합니다.

HTML 페이지 및 사용자 정의

제공된 HTML 페이지는 Notepad 또는 Notepad++로 편집하여 사용자 인터페이스를 사용자 정의할 수 있습니다.

index.html 페이지

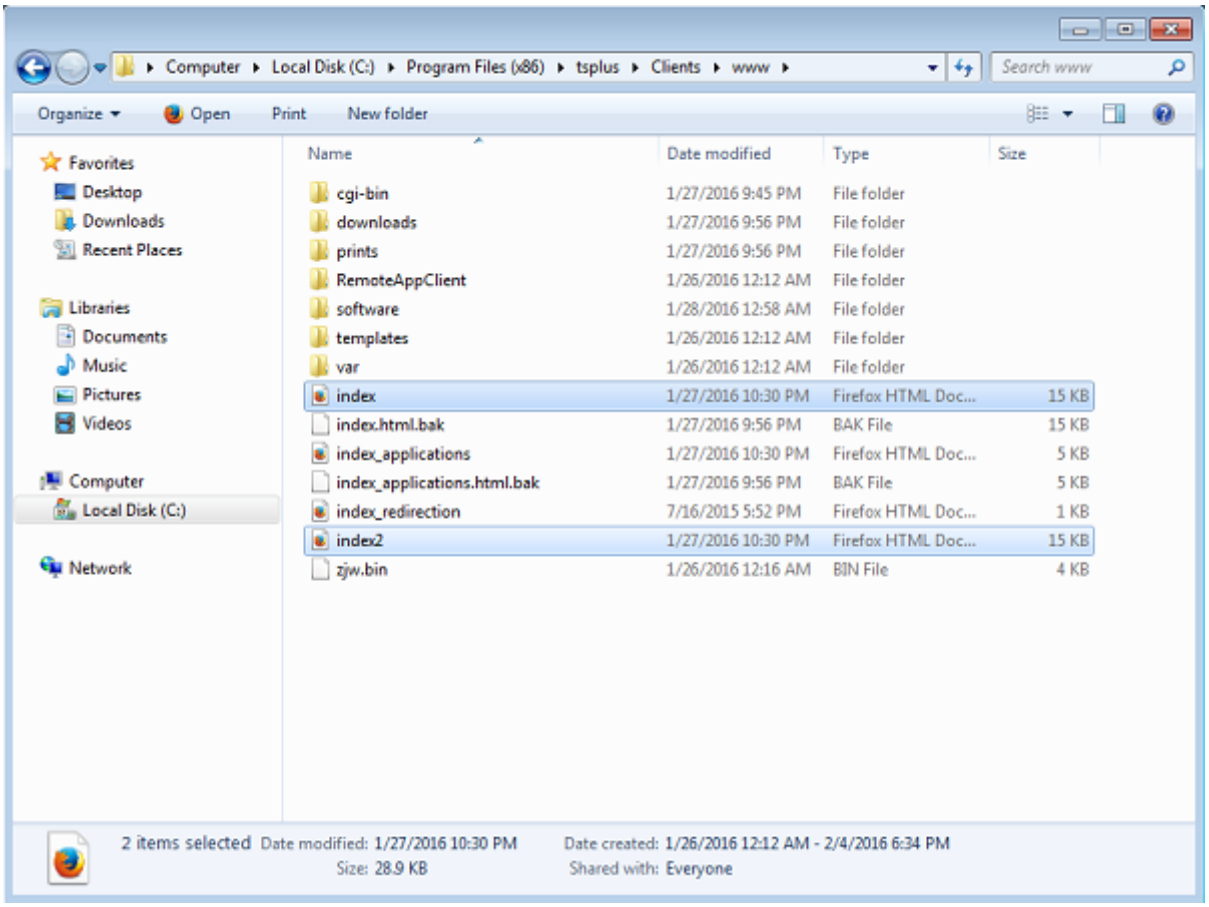
index.html은 웹 서버 루트 폴더 경로에 있습니다.

C:\Program Files (x86)\TSplus\Clients\www

Index.html 페이지는 기본 웹 페이지입니다. 이는 \www\ 폴더에 위치한 연결 페이지에 대한 링크가 있는 프론트엔드 포털 페이지와 같습니다.

이 웹 페이지는 여러 구성 및/또는 로그인 정보를 허용하기 위해 복사하고 이름을 변경할 수 있습니다.

예를 들어 index.html을 복사하여 index2.html로 이름을 바꾸면 이 페이지는 이 URL을 사용하여 사용할 수 있습니다. http://localhost/index2.html



주의: “index.html” 파일 이름을 “index2.html”로 변경하고 Web Applications Portal을 사용하는 경우, 이 파일에서 다음 변수를 변경해야 합니다: “page_configuration[“applications_portal”] = “index_applications.html””을 “index2_applications.html”로 변경한 후 “index_applications.html” 파일 이름을 “index_2applications.html”로 변경하십시오.

기본 index.html에는 가능한 모든 옵션이 포함되어 있습니다:

- 응용 프로그램에 대한 RemoteApp 액세스, 웹 브라우저 외부의 연결
- 모든 장치에서 HTML5를 사용한 연결
- 로컬 인쇄 설정

웹 탭의 웹 포털 기본 설정 타일에서 웹 포털 디자인 기능을 통해 헤더와 푸터를 변경할 수 있습니다.

index.html 웹 페이지를 편집하면 다양한 설정에 접근할 수 있습니다.

// ---------- 액세스 구성 ----------

var user = ""; // 원격 서버에 연결할 때 사용할 로그인 (이 페이지에 입력된 로그인 사용하려면 ""로 두세요)

var pass = ""; // 원격 서버에 연결할 때 사용할 비밀번호 (이 페이지에 입력된 비밀번호를 사용하려면 ""로 두십시오)

var domain = ""; // 원격 서버에 연결할 때 사용할 도메인 (이 페이지에 입력된 도메인을 사용하려면 ""로 두십시오)

var server = "127.0.0.1"; // 연결할 서버 (이 페이지에서 선택한 서버와 로컬호스트를 사용하려면 ""로 두십시오)

var port = ""; // 연결할 포트 (이 페이지에서 선택한 서버의 포트와 로컬호스트를 사용하려면 ""로 두세요)

var lang = "as_browser"; // 사용할 언어

var serverhtml5 = “127.0.0.1”; // HTML5 클라이언트를 사용할 때 연결할 서버

var porthtml5 = “3389”; // HTML5 클라이언트를 사용할 때 연결할 포트

var cmdline = ""; // 연결되면 서버의 클립보드에 넣을 선택적 텍스트

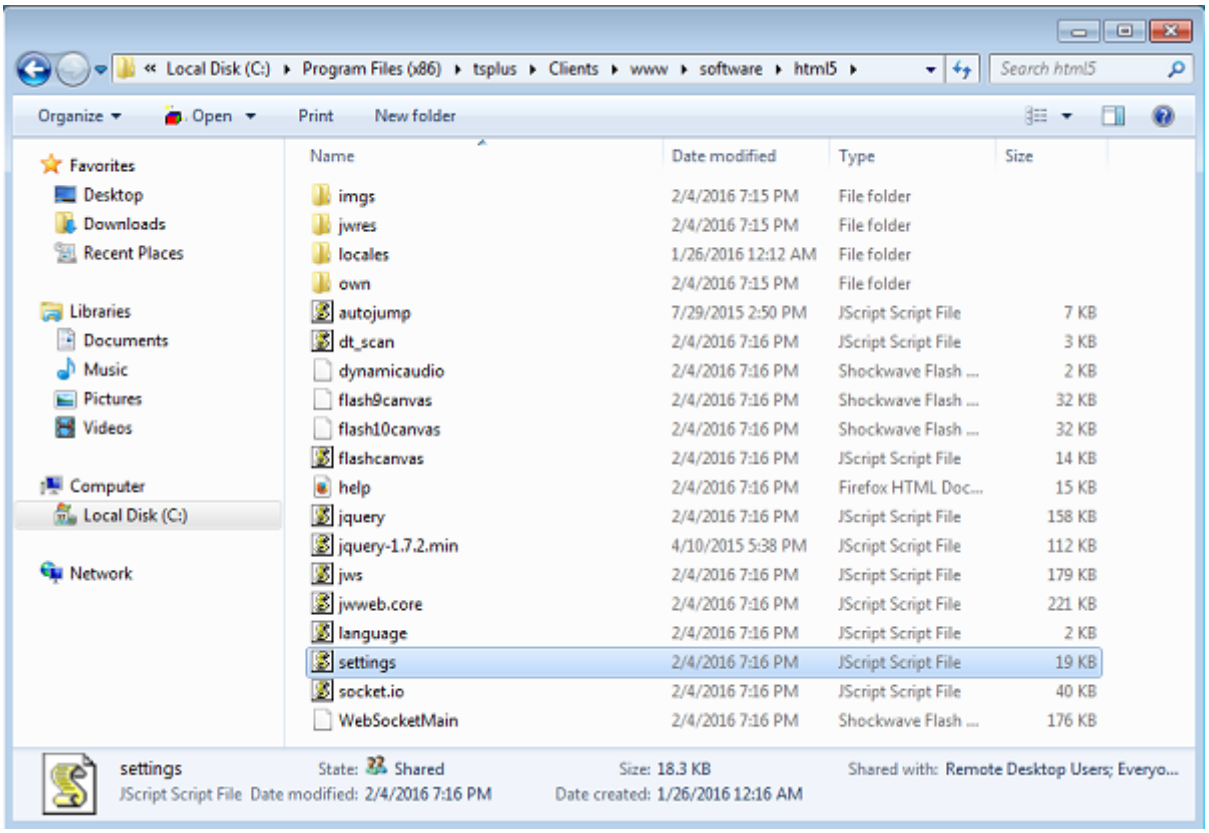
// ---------- 액세스 구성 종료 ----------

예를 들어, 로그인/비밀번호를 편집하여 데모/Psw로 설정하겠습니다:

var user = "데모"; var pass = "비밀번호";

이렇게 하면 포털을 방문할 때마다 미리 채워진 자격 증명이 표시됩니다.

또 다른 매우 중요한 구성 파일은 **settings.js** C:\Program Files (x86)\TSplus\Clients\www\software\html5:



이 파일에는 브라우저 탭이 닫힐 경우 소리 비활성화, 클립보드 사용 또는 세션 재연결 허용과 같은 HTML5 웹 클라이언트에 대한 다양한 설정이 포함되어 있습니다.

- 클립보드 비활성화:

W.clipboard = "예"; //또는 "아니오"

- 소리를 비활성화하는 것은 이 설정으로 수행됩니다:

W.playsound = false;

- 모바일 장치의 기본 해상도 변경:

W.viewportwidth = "1024" - 높이는 브라우저에 의해 계산됩니다.

- 원격 연결을 위한 HTTPS 강제 적용

W.forcealways_ssl = true;

- 브라우저 탭이 닫힐 때 세션 재연결 허용:

W.send_logoff = false;

- 브라우저 탭을 닫지 못하도록 경고 팝업 추가:

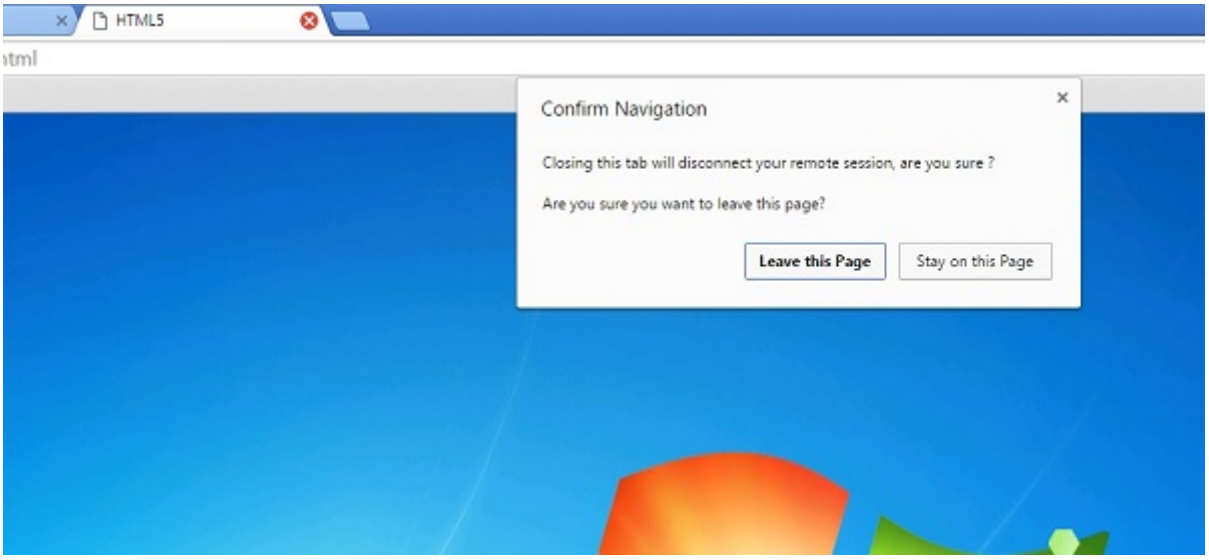
“W.pageUnloadMessage = "" ” 매개변수를 검색하십시오.

아래에 사용할 메시지의 예를 설정했습니다:

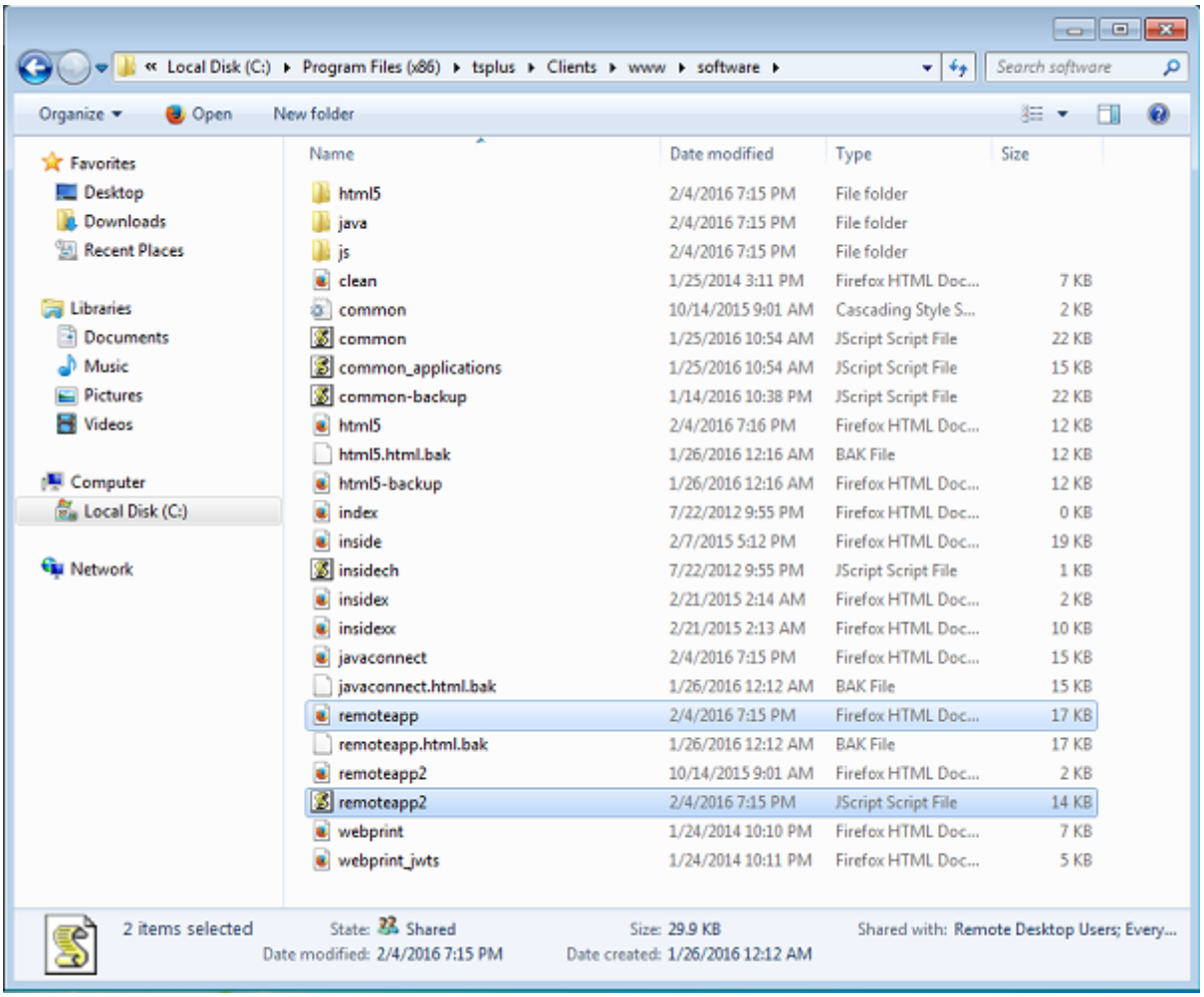
W.pageUnloadMessage = “이 탭을 닫으면 원격 세션이 끊어집니다. 확실합니까?”; //페이지가 언로드될 때 반환할 대화상자.

//1. 중요한 공지, 모든 브라우저에서 자체 대화 상자는 지원되지 않습니다.

//2. HTML 표준은 페이지 새로 고침과 페이지 닫기 동작을 구분하지 않으므로, 페이지 새로 고침 시에도 대화 상자가 팝업됩니다.



원격 앱 웹 페이지에 대한 일반 설정은 소프트웨어 폴더의 두 개의 다른 파일에 저장됩니다. **remoteapp.html** 그리고 **remoteapp2.js** .



사용 가능한 설정의 예가 있는 **remoteapp2.js** :

// 원격 데스크톱 서버

var remoteapp2_server = ”; var remoteapp2_port = ‘443’;

윈도우 인증

var remoteapp2_user = ”; var remoteapp2_psw = ”; var remoteapp2_domain = ”;

// 선택적 명령줄 매개변수

var remoteapp2_apppath = ”;

// 원격 앱 모드

var remoteapp2_wallp = '녹색'; var remoteapp2_remoteapp = '켜짐';

// 화면

var remoteapp2_color = '32';

var remoteapp2_full = '2';

var remoteapp2_width = ”;

var remoteapp2_height = ”;

var remoteapp2_scale = '100';

var remoteapp2_smartsizing = ‘1’;

var remoteapp2_dualscreen = '꺼짐';

var remoteapp2_span = '꺼짐';

디스크 매핑(인쇄를 위해 필요)

var remoteapp2_disk = ‘1’;

// 인쇄

var remoteapp2_printer = '꺼짐';

var remoteapp2_preview = '끄기';

var remoteapp2_default = '켜기';

var remoteapp2_select = '꺼짐';

하드웨어

var remoteapp2_com = '0';

var remoteapp2_smartcard = '0';

var remoteapp2_serial = '꺼짐';

var remoteapp2_usb = 'off';

var remoteapp2_sound = '켜기';

var remoteapp2_directx = '끄기';

// 잡다한 사항

var remoteapp2_alttab = '0';

var remoteapp2_firewall = '1';

```
var remoteapp2_localtb = ‘32’;

var remoteapp2_lock = 'off';

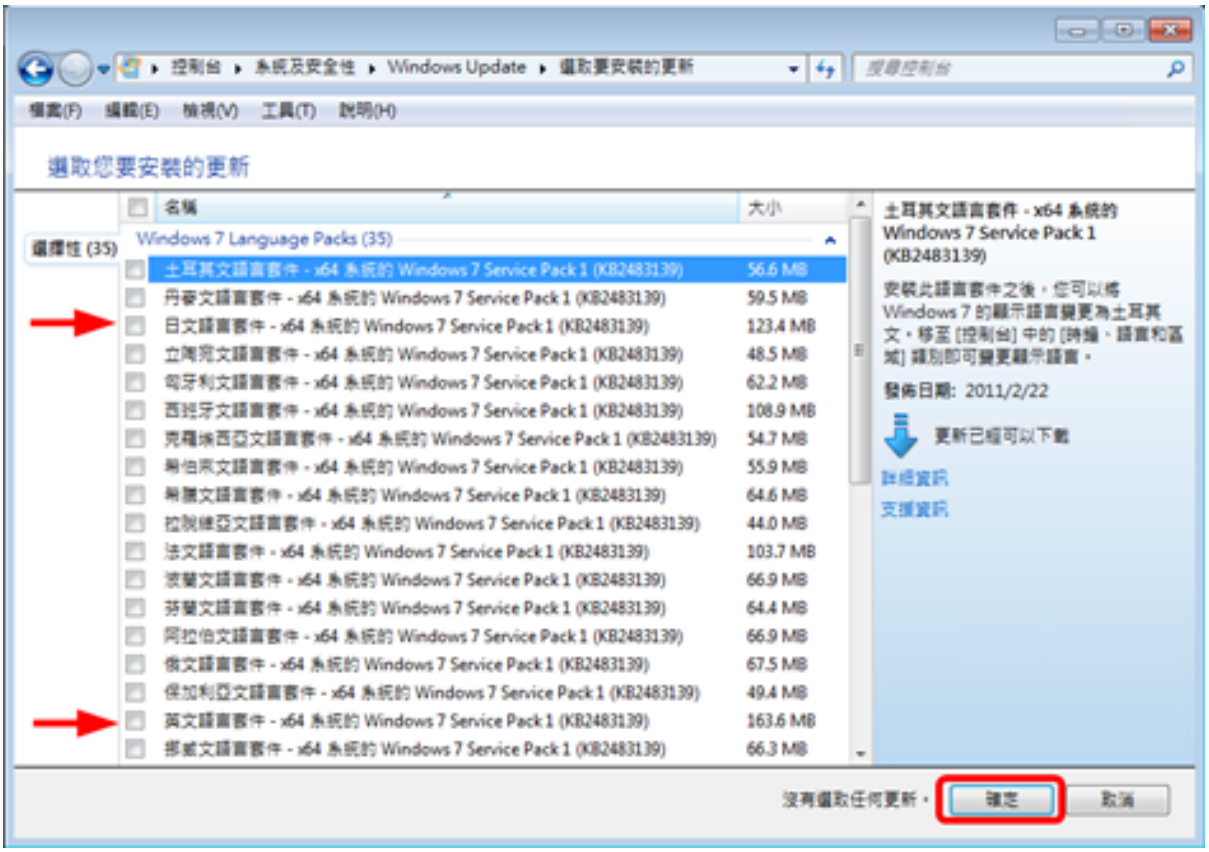
var remoteapp2_rdp5 = 'off';

var remoteapp2_reset = 'off';
```

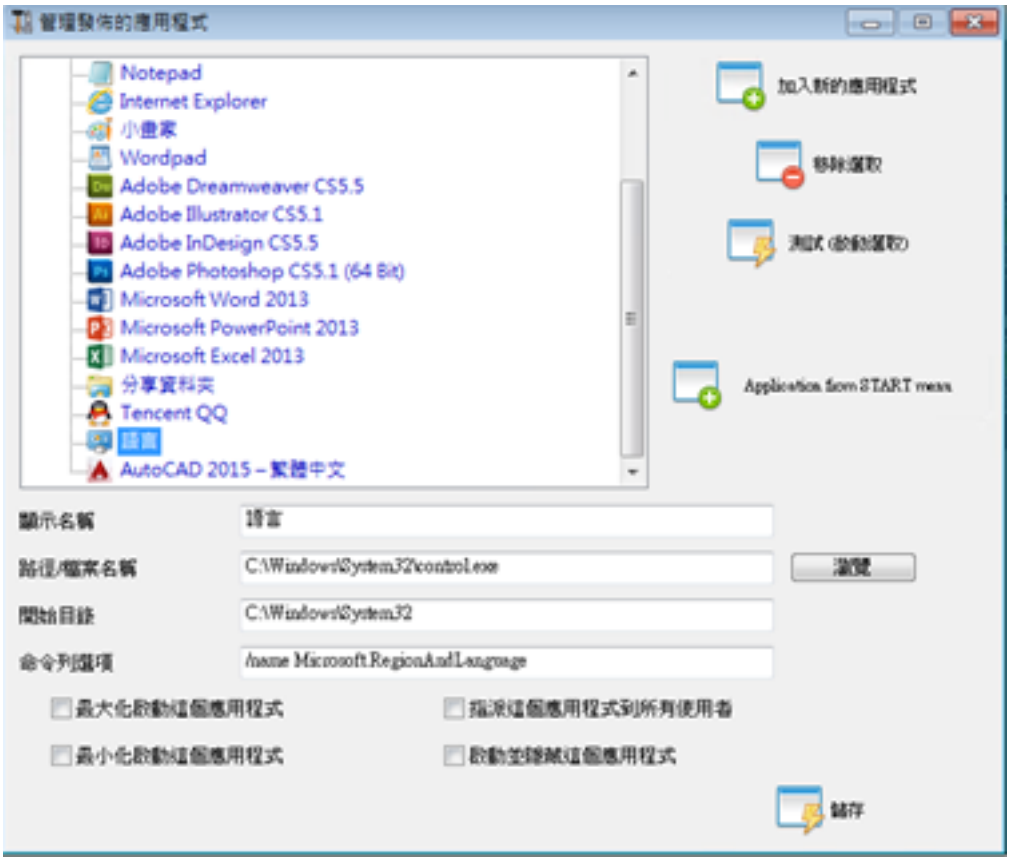
HTML5 : 중국어로 언어 변경

Windows 7 Enterprise 또는 Ultimate / Windows 8 Enterprise 또는 Professional이 필요합니다. 한 시스템에서 다국어를 사용하려면.

시스템에 필요한 모든 언어를 설치할 수 있습니다.



사용자가 UI의 O/S 언어를 변경하고 IME(입력기)를 추가할 수 있도록 언어 애플릿을 게시할 수 있습니다.

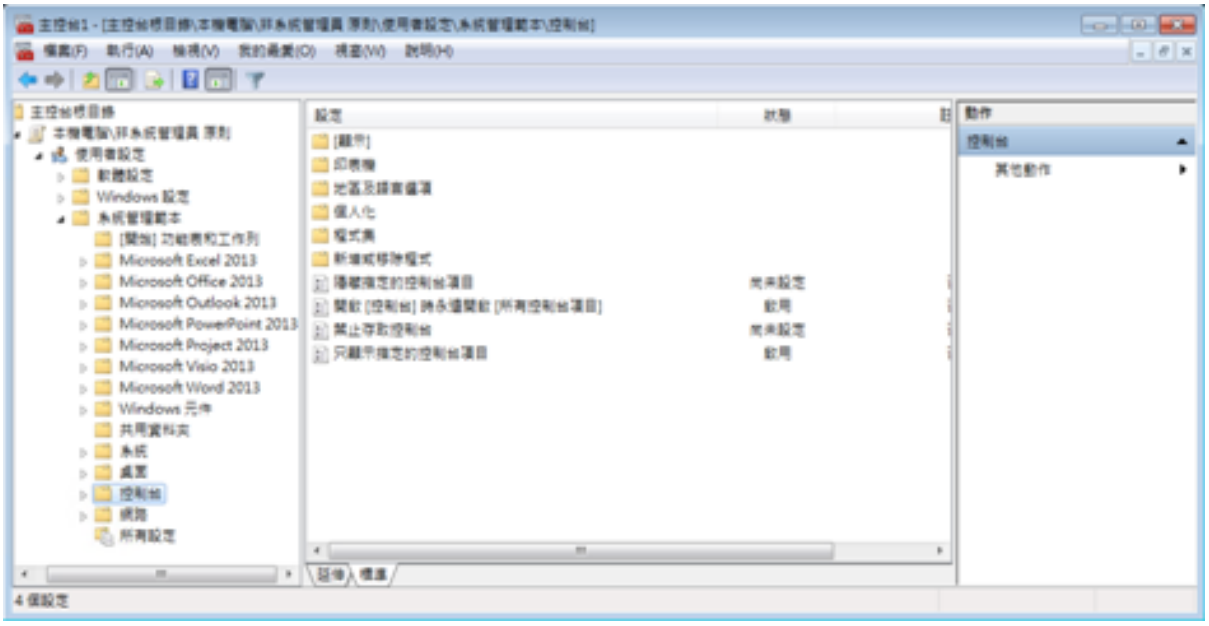


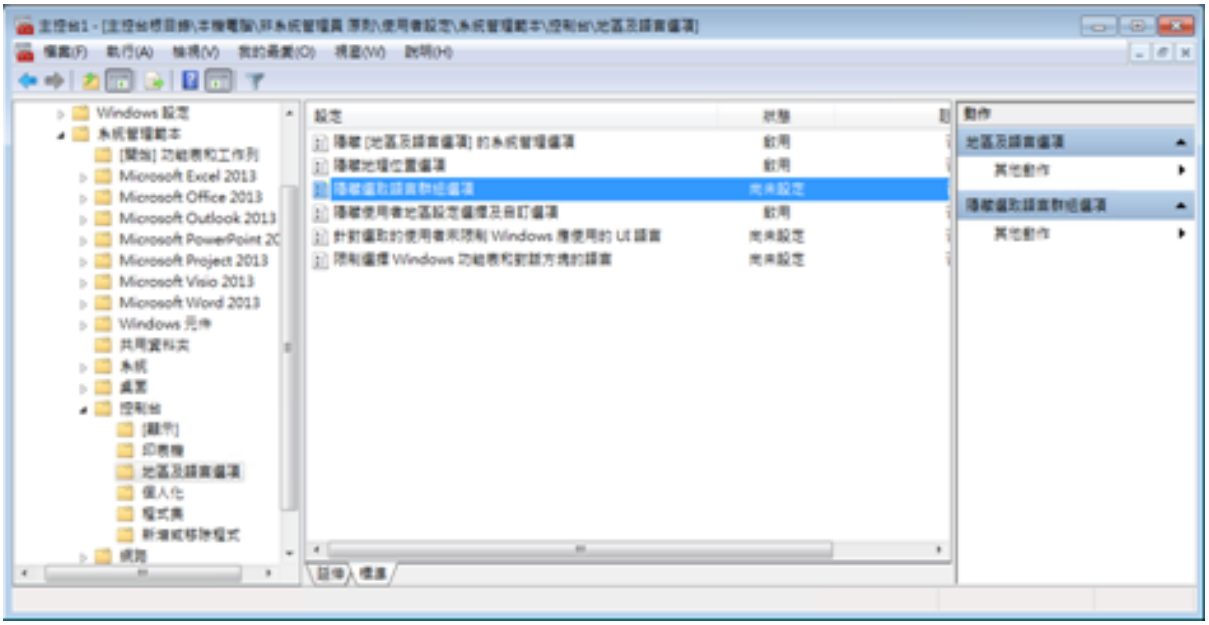
Windows 7의 경우: control /name Microsoft.RegionAndLanguage

Windows 8의 경우: control /name Microsoft.Language

전체 목록: http://pcsupport.about.com/od/tipstricks/tp/control-panel-applets-list.htm

선택 사항: 이것은 GPO를 통해 사용자의 제어판 동작을 제한하는 방법입니다.

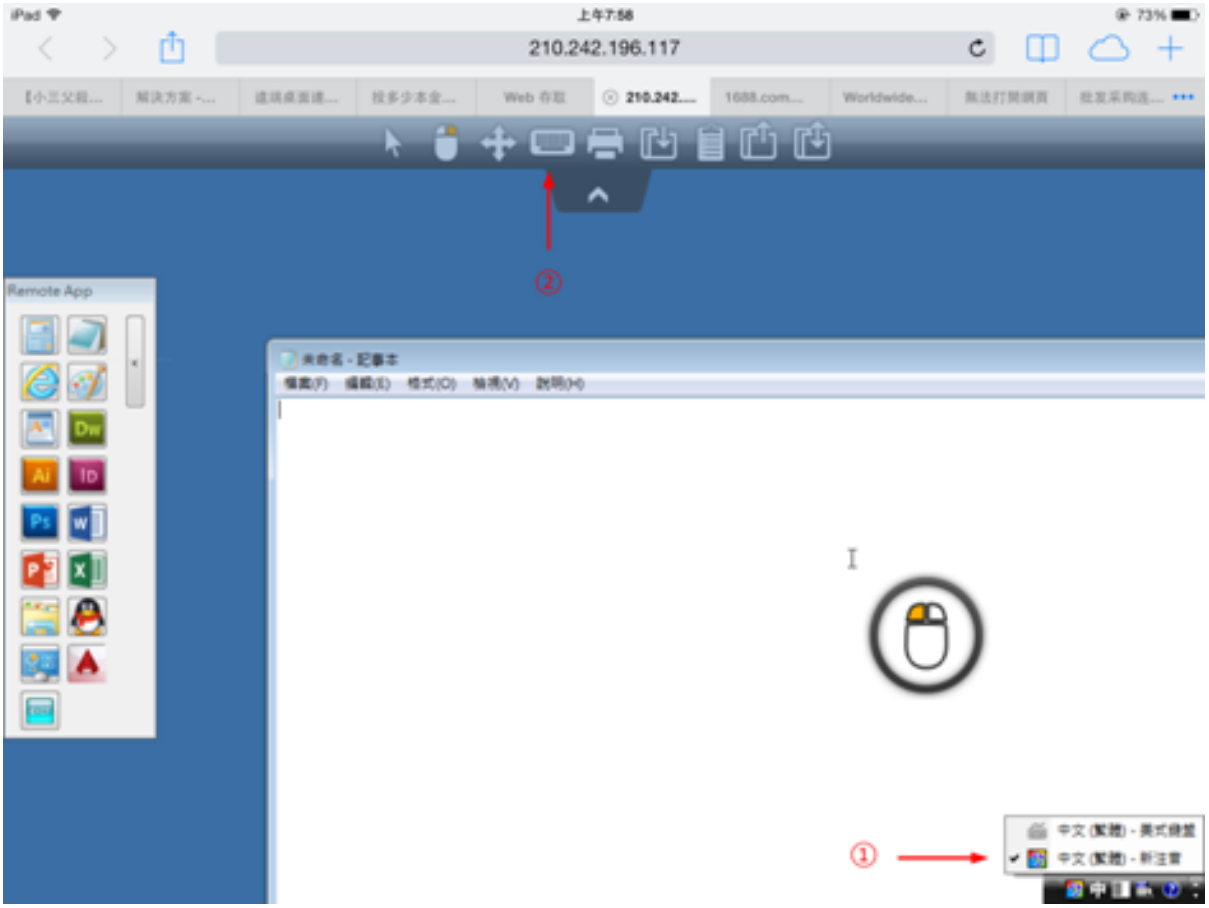




사용자는 이 설정을 변경한 후 효과를 보려면 로그아웃하고 다시 로그인해야 합니다.



사용자는 먼저 중국어 문자를 입력하기 위해 중국어 IME를 선택해야 합니다.


210.242.196.117
Remote App
②
①


210.242.196.117
中文中
中 中文 中國 巾 申 申請 申請人 甲 由 內 內 四 而 p 內
.?123
上一個
確認
下一個
換行


210.242.196.117
中 種 重 鐘 終 腫 仲 蟲 冢 忠 眾 踵 鍾 衷 塚 忪 众 潼 僮 狆
確認
.?123
一聲
.?123

HTML5 클라이언트: 웹소켓과 XHR의 차이점은 무엇인가요?

웹소켓은 순차적 순서 없이 및 http 헤더 없이 데이터를 수신/전송하는 데 사용할 수 있는 지속적인 연결입니다.

Xhr-polling은 HTTP 헤더로 새 요청을 생성하고 HTTP 헤더로 응답을 기다리며, 또한 순차적인 순서를 유지합니다.

이렇게 하면 XHR 데이터 흐름은 항상 다음과 같습니다:

HTTP_HEADER_REQUEST -> HTTP_HEADER_ANSWER HTTP_HEADER_REQUEST -> HTTP_HEADER_ANSWER 그리고 계속해서

데이터를 다운로드하기 전에 HTTP_HEADER로 요청해야 하므로 이름이 xhr-polling입니다.

웹소켓 데이터 흐름은 다음과 같이 보일 수 있습니다:

프레임_데이터_전송 프레임_데이터_전송 프레임_데이터_수신 프레임_데이터_전송 프레임_데이터_수신 프레임_데이터_수신

또한 특별한 순차적 순서 없이 및 http 헤더 데이터 없이 무작위 데이터 전송/수신입니다.

그로 인해 대부분의 알려진 리버스 프록시에서 Websockets 지원이 부족하여 리버스 프록시와의 사용이 불가능해지지만, xhr 전송의 절반은 Apache 리버스 프록시와 함께 작동할 수 있습니다.

또한 참조: HTML5 클라이언트: 지원되는 브라우저

HTML5 클라이언트: 모바일 장치에서 RDP 세션 해상도

대부분의 장치, 특히 모바일 전화에서 일반적인 화면 해상도는 320x480이지만, 이는 RDP 세션을 생성하기에는 명백히 충분하지 않습니다.

따라서 해상도는 너비 800으로 미리 설정되었습니다. 해상도의 높이는 숨겨진 브라우저의 기본 논리에 의해 재계산됩니다. 너비가 높을수록 높이가 커집니다.

- 예를 들어, 표준 해상도는 320x480입니다. 이제 뷰포트를 800으로 설정하면 브라우저가 높이 값을 800x904로 다시 계산합니다. 너비를 1280으로 설정하면 1280x1160이 됩니다.

높이와 너비는 장치의 가로/세로 모드에 따라 다르며, 예를 들어 800x904 또는 904x800 등입니다. 각 브라우저는 RDP 화면을 장치의 뷰포트에 맞추기 위해 자체 논리에 따라 이를 재계산할 수 있으며, 동일한 장치에서 사용하더라도 브라우저에 따라 다를 수 있습니다.

높이를 수동으로 설정하면 장치의 뷰포트 비율이 깨지고 최종 RDP 세션이 포트 뷰에서 벗어나게 되며, 이러한 영역에 도달하려면 원하는 위치로 스크롤해야 합니다.

- 따라서 높이를 수동으로 설정하지 않고 장치가 자동으로 높이를 선택하도록 하는 것이 권장됩니다.

높이가 더 필요하면 너비를 늘리세요!

모바일 전화 기기에서 테스트한 결과, 너비에 대한 좋은 값은 800이었습니다. 그러나 주의해야 할 점이 있습니다: 대부분의 모바일 전화의 CPU는 보통 느리기 때문에 높이를 증가시키면 CPU 부하가 증가합니다. 태블릿 기기에서는 CPU가 더 빠르므로 너비를 1280과 같은 더 높은 값으로 설정하고 기기가 높이에 대한 값을 다시 계산하도록 허용하는 것이 좋습니다.

일부 브라우저(예: FireFox 모바일)가 페이지 로딩 후 뷰포트를 설정하는 것을 허용하지 않기 때문에 이 값은 Clients\www\software\html5.html 파일에 고정되어 설정되었습니다.

예를 들어 다음과 같이 변경하십시오:

너비를 늘리면서 동시에 브라우저의 기본 내부 논리에 의해 높이가 재계산됩니다.

두 번째 예로, 이를 다음과 같이 변경합니다:

뷰포트 영역이 깨지고 RDP 세션이 화면에 맞지 않을 것입니다.

HTML5 클라이언트: URL 주소의 매개변수

원격 서버에 연결하기 위해 Terminal Service Plus HTML5 클라이언트를 사용할 때, 기본 매개변수를 무시하기 위해 URL 주소에 여러 매개변수를 지정할 수 있습니다.

- 사용자 로그인
- 사용자 비밀번호
- 실행할 프로그램
- 프로그램 실행을 위한 시작 디렉토리
- 프로그램을 실행하기 위한 명령줄

특정 애플리케이션 실행

여기 사용자 "demo"의 원격 세션을 열기 위한 전체 URL 주소의 예가 있습니다. 비밀번호는 "demo"이며 세션이 열릴 때 표준 메모장을 시작합니다.

https://demo.tsplus.net/software/html5.html?user=demo&pwd=demo&program=c:\\windows\\system32\\notepad.exe&startupdir=c:\\windows\\system32¶ms=

URL 주소에서 모든 슬래시 문자가 반복되어야 함을 유의하시기 바랍니다. **4회** .

모든 매개변수를 동시에 지정할 필요는 없습니다: 지정하지 않은 매개변수는 기본 설정 값이 적용됩니다.

웹 자격 증명으로 연결

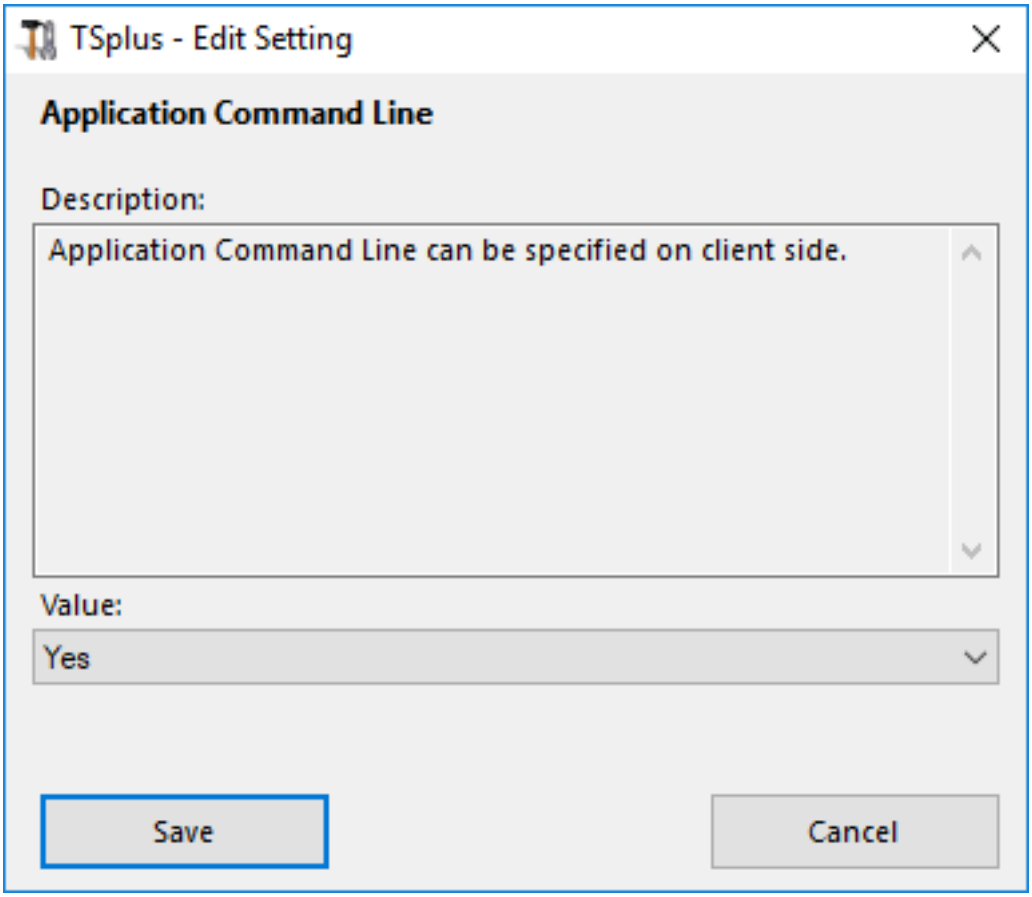
사용하려면 웹 자격 증명 연결하려면 웹 로그인 앞에 "@"를 추가하여 URL에 전달할 수 있습니다.

여기 "demo" 비밀번호로 웹 자격 증명 "1234"와 함께 애플리케이션 패널로 원격 세션을 열기 위한 URL 주소의 예가 있습니다.

https://demo.tsplus.net/software/html5.html?user=@1234&pwd=demo

사용자 기본 애플리케이션에 대한 이 사용을 제한합니다.

사용자에 대한 애플리케이션 명령줄을 비활성화하려면 다음으로 이동하십시오. 고급 —> 세션 탭 관리 도구에서 "응용 프로그램 명령줄" 설정을 두 번 클릭하고 값을 "아니오"로 설정합니다.



HTML5 클라이언트: 지원되는 브라우저

HTML5 클라이언트를 사용할 때 시작 시 브라우저에 빨간 경고가 표시되면

브라우저가 Websockets를 지원하지 않거나 브라우저가 Canvas를 지원하지 않음을 의미합니다.

이 기술을 지원하지 않는 브라우저는 IE6, IE7, IE8, IE9이며 이러한 기능을 에뮬레이트하기 위해 FLASH가 필요합니다.

웹소켓 및 캔버스를 지원하는 브라우저

브라우저	캔버스	웹소켓
파이어폭스	전체	버전 4부터 시작하는 전체
크롬	전체	PC에서 가장 많이 알려진 버전에서 전체 사용 가능
오페라	전체	최신 버전에서 전체 사용 가능
IE6	플래시	플래시(에뮬레이션 및 프록시 지원 없음)
	플래시	프록시 지원이 포함된 XHR
IE7	플래시	플래시(에뮬레이션 및 프록시 지원 없음)
	플래시	프록시 지원이 포함된 XHR
IE8	플래시	플래시(에뮬레이션 및 프록시 지원 없음)
	플래시	프록시 지원이 포함된 XHR
IE9	플래시	플래시(에뮬레이션 및 프록시 지원 없음)
	플래	프록시 지원이 포함된 XHR

	시	
IE10	전체	전체
안드로이드 네이티브	전체	XHR
오페라 모바일	전체	최신 버전에서 전체 사용 가능
파이어폭스 모바일	전체	전체
사파리 모바일	전체	최신 버전에서 iOS4까지 전체 지원, 그렇지 않으면 XHR을 통해 에뮬레이션됩니다.

또한 참조: 웹소켓과 XHR의 차이점은 무엇인가요?

브라우저가 페이지를 HTTPS 주소로 자동으로 새로 고치는 경우

웹소켓 전송이 지원되지 않음을 의미합니다. 이는 여러 Android 네이티브 모바일 브라우저에서 발생하는 경우입니다.

브라우저가 자동으로 XHR 전송으로 전환되기 때문입니다.

하지만 이 전송이 HTTP 프로토콜로 장거리에서 이루어지기 때문에 각 요청은 새로운 연결을 생성합니다. 새로운 연결을 생성하는 것은 매우 느리고 불안정합니다(초당 최대 20개의 새로운 연결). 따라서 이러한 불안정을 피하기 위해 프로그램은 페이지가 자동으로 HTTPS 주소로 새로 고쳐져 HTTPS 연결을 강제하도록 설계되었습니다.

물리적으로도 대부분 지속적인 보안 연결을 얻고 장거리에서 훨씬 더 안정적입니다. 따라서 브라우저의 논리는 HTTP 프로토콜을 사용할 때처럼 새로운 연결을 생성하는 대신 이미 설정된 SSL 연결을 재사용합니다.

이 동작은 다음 옵션을 통해 변경할 수 있습니다. 이 옵션은 TSplus 프로그램 폴더의 다음 경로에 있는 setting.js 파일에 있습니다: Clients\www\software\html5\settings.js:

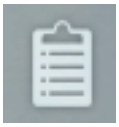
forcesslforxhr = false;

하지만 XHR 모드에서 SSL 사용을 비활성화하는 것은 절대 권장되지 않습니다.

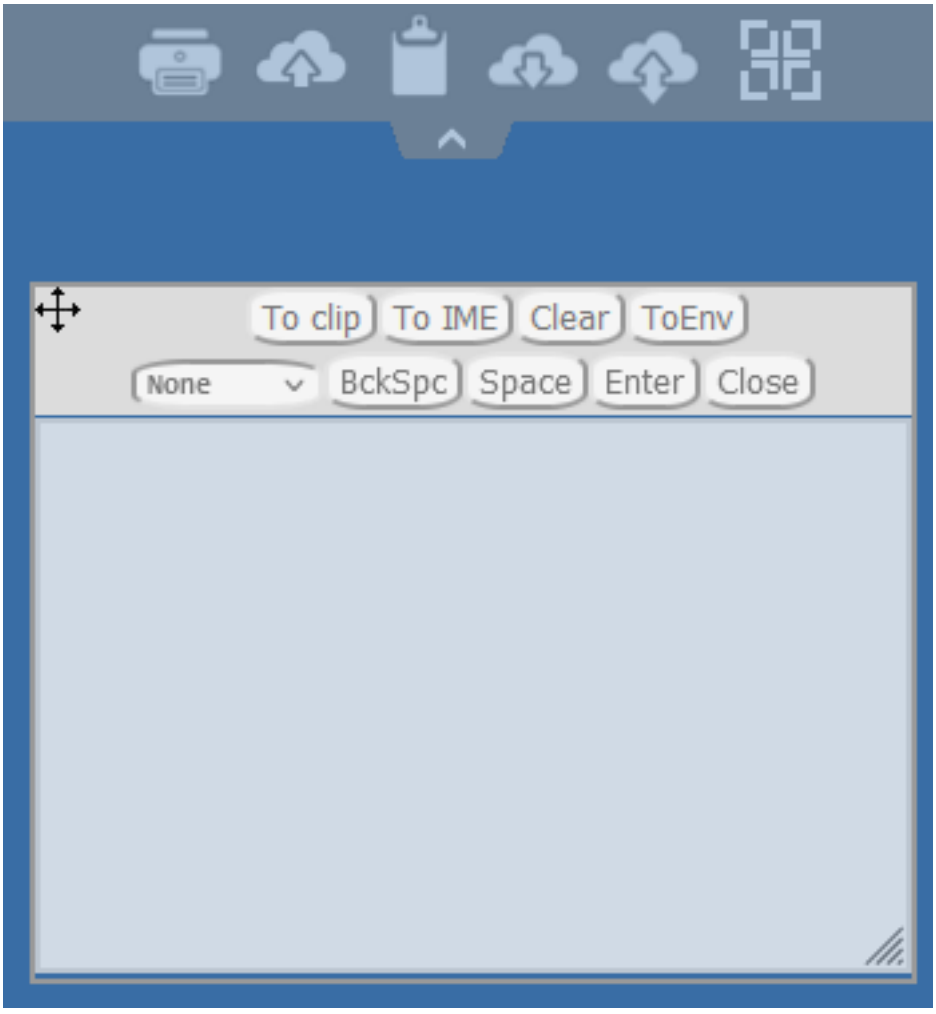
“C:\Program Files (x86)\TSplus\Clients\www\software\html5” 폴더에 “settings.js”라는 파일이 없으면, 귀하의 TSplus 버전이 오래된 것이며 이 문서는 적용되지 않습니다. 먼저 시스템을 업데이트하거나 지원팀에 문의하시기 바랍니다.

HTML5 클라이언트: 클립보드 사용

클립보드는 HTML5 상단 메뉴에서 이 아이콘과 함께 찾을 수 있습니다:



대부분의 브라우저는 보안상의 이유로 구형 MSIE 브라우저를 제외하고는 직접 클립보드 읽기 및 쓰기를 지원하지 않습니다.



여기 다양한 작업이 있습니다:

- **클립하기** RDP 세션에 텍스트 영역의 내용을 전송하고 끝에 Ctrl+V를 생성하여 텍스트를 RDP 세션 안에 넣습니다 (귀하의 환경은 영향을 받지 않습니다!!!)

- **IME로 이동** 텍스트 영역의 문자를 키 입력으로 변환하고 키보드를 사용한 것처럼 전송합니다. (이 버튼은 RDP 세션 앱 내에서 클립보드 텍스트 입력이 지원되지 않는 곳에 텍스트를 넣고 싶을 때 필요합니다.)

- **ToEnv** 텍스트 영역의 텍스트를 브라우저 외부의 자신의 클립보드(원격 데스크톱 세션이 아닌 자신의 환경)에 넣으려고 시도합니다!!!! 자신의 클립보드에 텍스트를 추가하는 것은 특권이 있는 작업이므로 클릭하여 실행해야 합니다.

- **클립하기** 보안상 자신의 브라우저 외부에 텍스트를 추가하지 않고 rdp-clip+ctrl/v 작업을 처리하는 방법으로 언급된 대로, 원하지 않을 때 자신의 클립보드에 텍스트를 넣는 것은 매우 어리석기 때문에 "ToEnv"를 사용하십시오. 이 동작은 요청에 따라 변경되지 않고 그대로 유지됩니다.

- **백스페이스** RDP 세션으로 BACKSPACE 버튼 명령을 전송합니다 (귀하의 앱은 포커스를 유지하고 Backspace 버튼 동작을 지원해야 합니다)

- **공간** RDP 세션으로 전송하는 Space 버튼 명령 (귀하의 앱은 포커스를 유지하고 Space 버튼 동작을 지원해야 합니다)

- **입력** RDP 세션으로 Enter 버튼 명령을 전송합니다 (귀하의 앱은 포커스를 받아야 하며 Enter 버튼 동작을 지원해야 합니다)

세션에서 텍스트를 클립보드로 복사하려면 Ctrl+C를 사용하고 클립보드에서 텍스트를 삽입하려면 Ctrl+V를 사용하세요.

하지만 Ctrl+C로 텍스트를 복사할 때 주의하세요. Ctrl+C 버튼을 누른 후 잠시 기다렸다가 버튼을 놓아야 합니다. 요청한 클립보드 텍스트가 이 키 조합을 놓은 후에 도착하면 텍스트가 환경 클립보드에 추가되지 않습니다. 이렇게 하면 Ctrl+C로 시작된 네이티브 브라우저 클립보드 복사 지원을 사용합니다.

대안으로 당신은 **클립보드 메뉴 사용** RDP 세션 클립보드에서 텍스트를 복사하고 삽입합니다.

거기에서 RDP 세션 클립보드에 텍스트를 삽입하거나 클립보드에 추가하고 RDP 세션 측에서 Ctrl+C를 자동으로 실행하여 텍스트를 삽입할 수 있습니다. 클립보드 메뉴는 작업 메뉴 또는 Shift + F11을 통해 열 수 있습니다.

- RDP 세션 내에서 마우스로 클립보드를 복사하면 텍스트가 브라우저로 전송되고 브라우저 포커스를 벗어나면 클립보드 메뉴가 자동으로 나타나 클립보드 텍스트가 있었음을 알리고 이를 클립보드 환경에 추가하지 않았음을 알려줍니다.

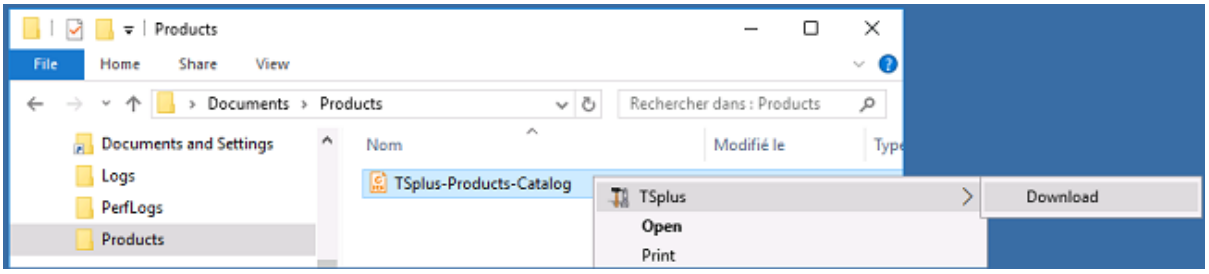
이 동작을 피하려면 Clients 폴더에 다음 줄을 설정하십시오. 기본 경로는 다음과 같습니다: C:\Program Files(x86)\tsplus\Clients\www\software\html5\settings.js

openonclipblur = false;

“C:\Program Files (x86)\TSplus\Clients\www\software\html5” 폴더에 “settings.js”라는 파일이 없으면, 귀하의 TSplus 버전이 오래된 것이며 이 문서는 적용되지 않습니다. 먼저 시스템을 업데이트하거나 지원팀에 문의하시기 바랍니다.

HTML5 클라이언트: 파일 전송 사용

파일 전송은 TSplus에서 여러 가지 방법으로 수행할 수 있습니다: 12.50 버전부터, **서버에서 로컬 PC로 파일을 다운로드할 수 있는 컨텍스트 메뉴가 제공됩니다.** :



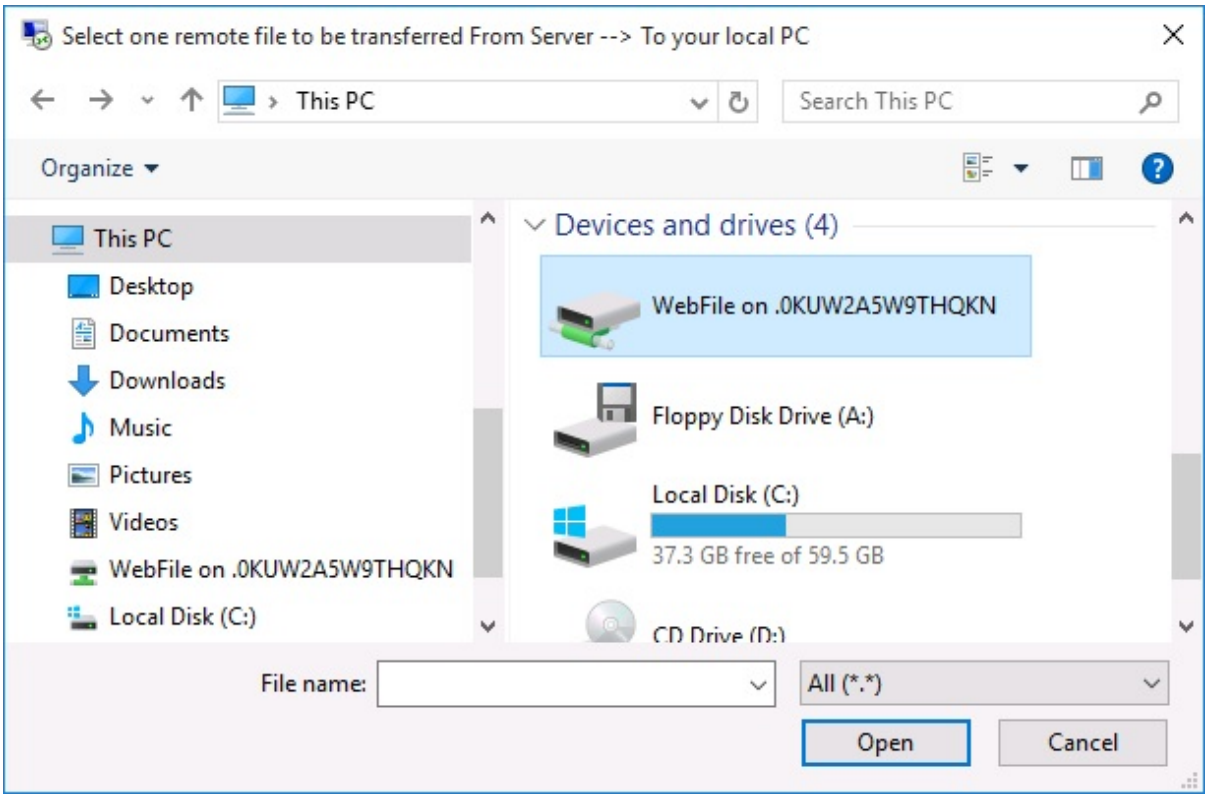
자세한 정보는 다음에서 확인할 수 있습니다. 이 문서 .

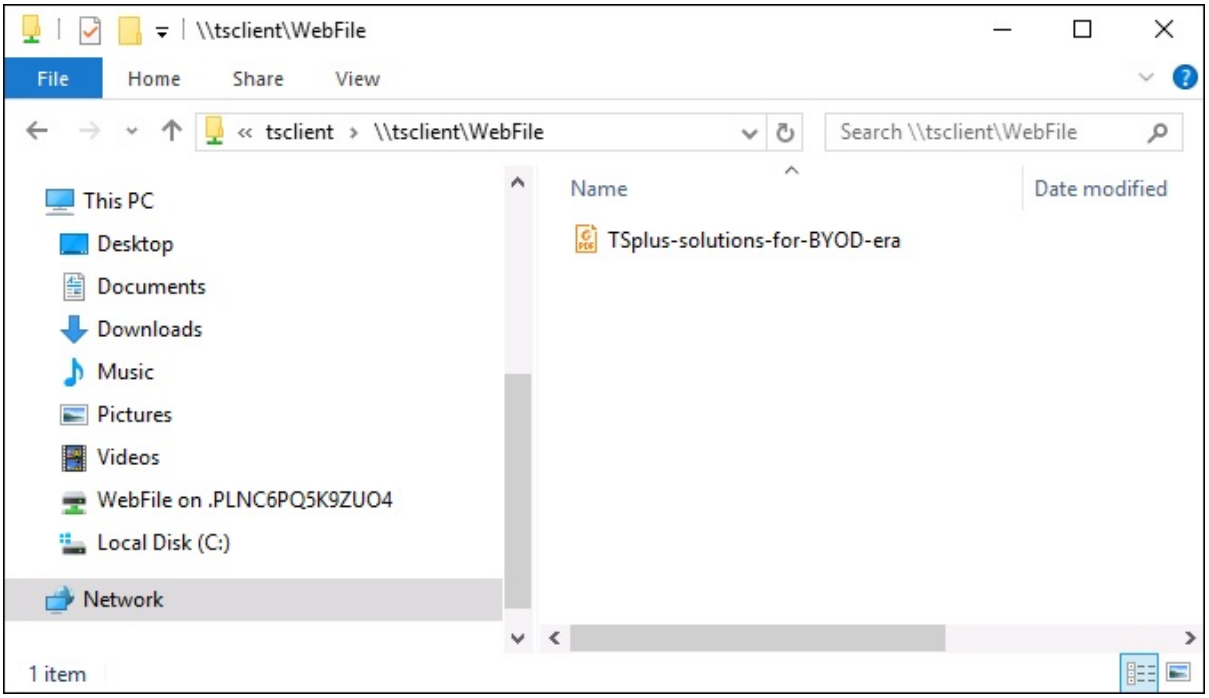
상단 메뉴를 사용하여 파일 전송:



실제 RDP 세션과 달리 브라우저는 하드 드라이브에 직접 접근할 수 없으며, 파일 전송은 에뮬레이션됩니다.

게이트웨이의 하위 폴더가 RDP 세션에 WebFile 장치로 마운트됩니다. RDP 세션 내에서 "WebFile"을 클릭하거나 " \\tsclient\WebFile"을 직접 호출하여 탐색기를 통해 접근할 수 있습니다.

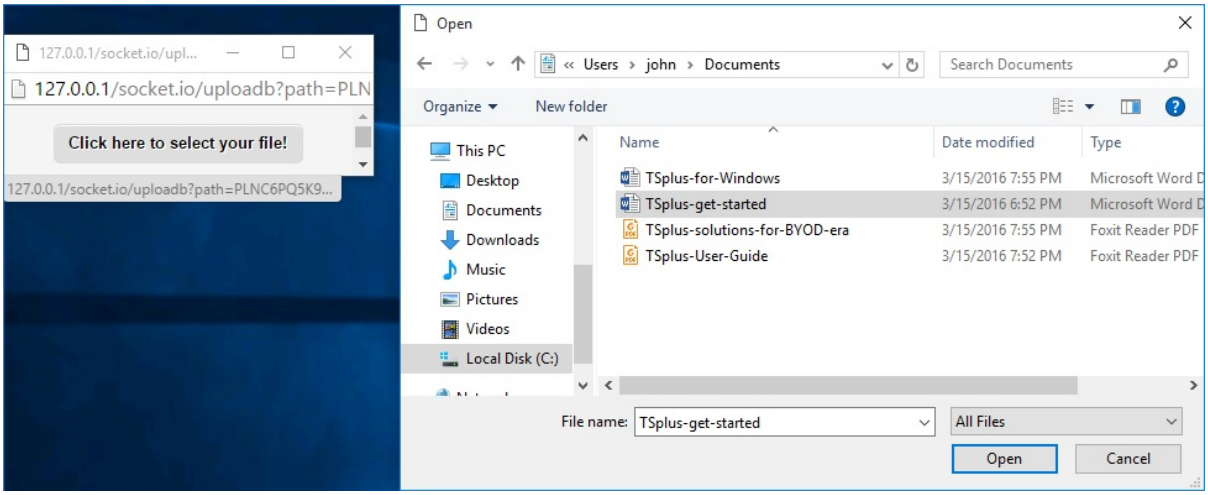




파일을 전송할 수 있는 3가지 다른 방법이 있습니다:

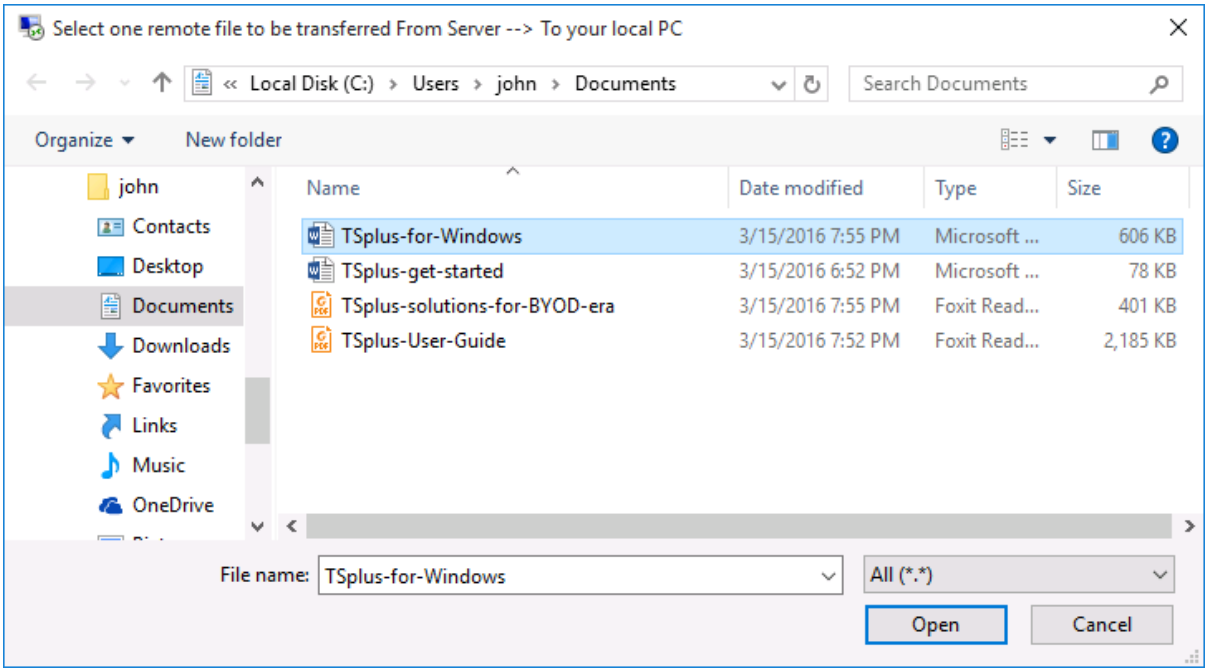
- 로컬 컴퓨터에서 서버로:



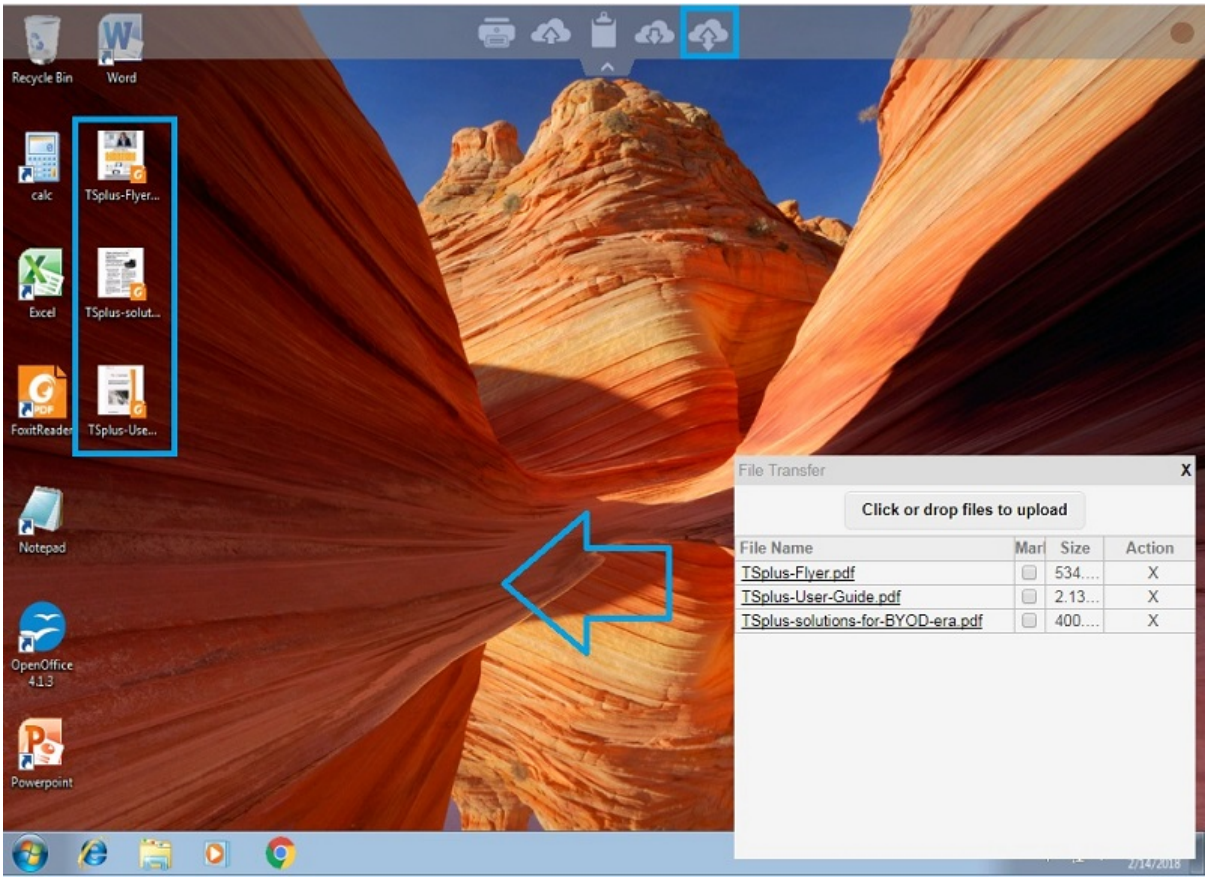


- 서버에서 로컬 컴퓨터로:



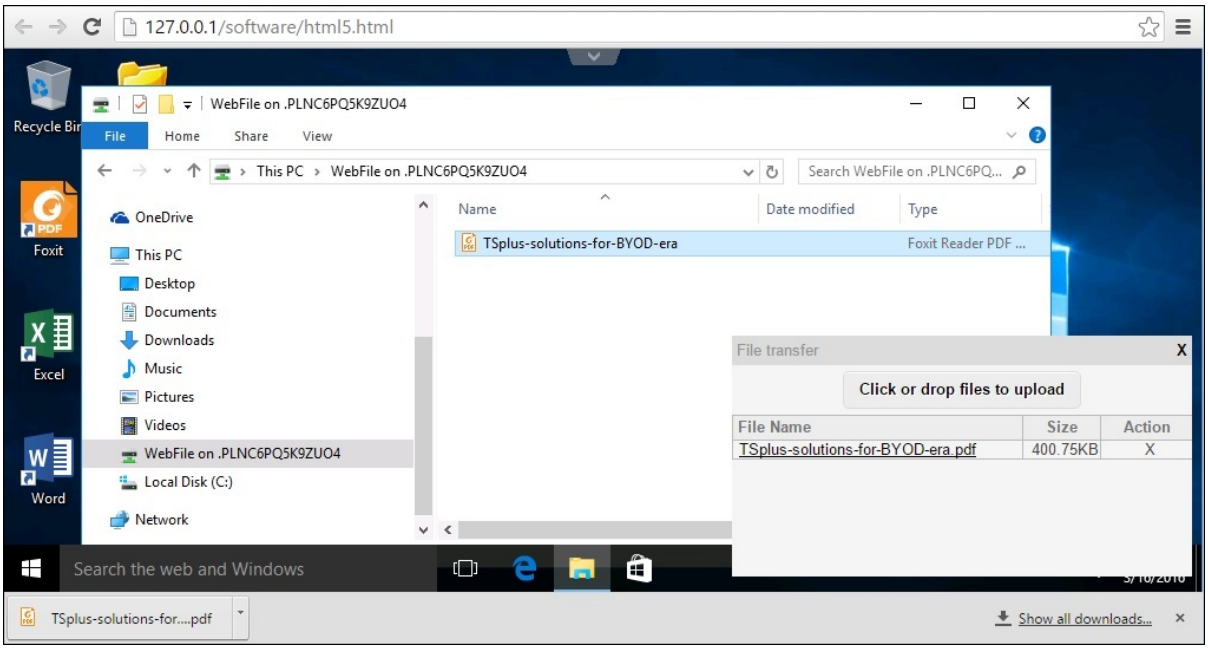


- 로컬 컴퓨터에서 서버로 파일을 전송할 수 있는 파일 관리자, 전송된 파일의 기록 포함:

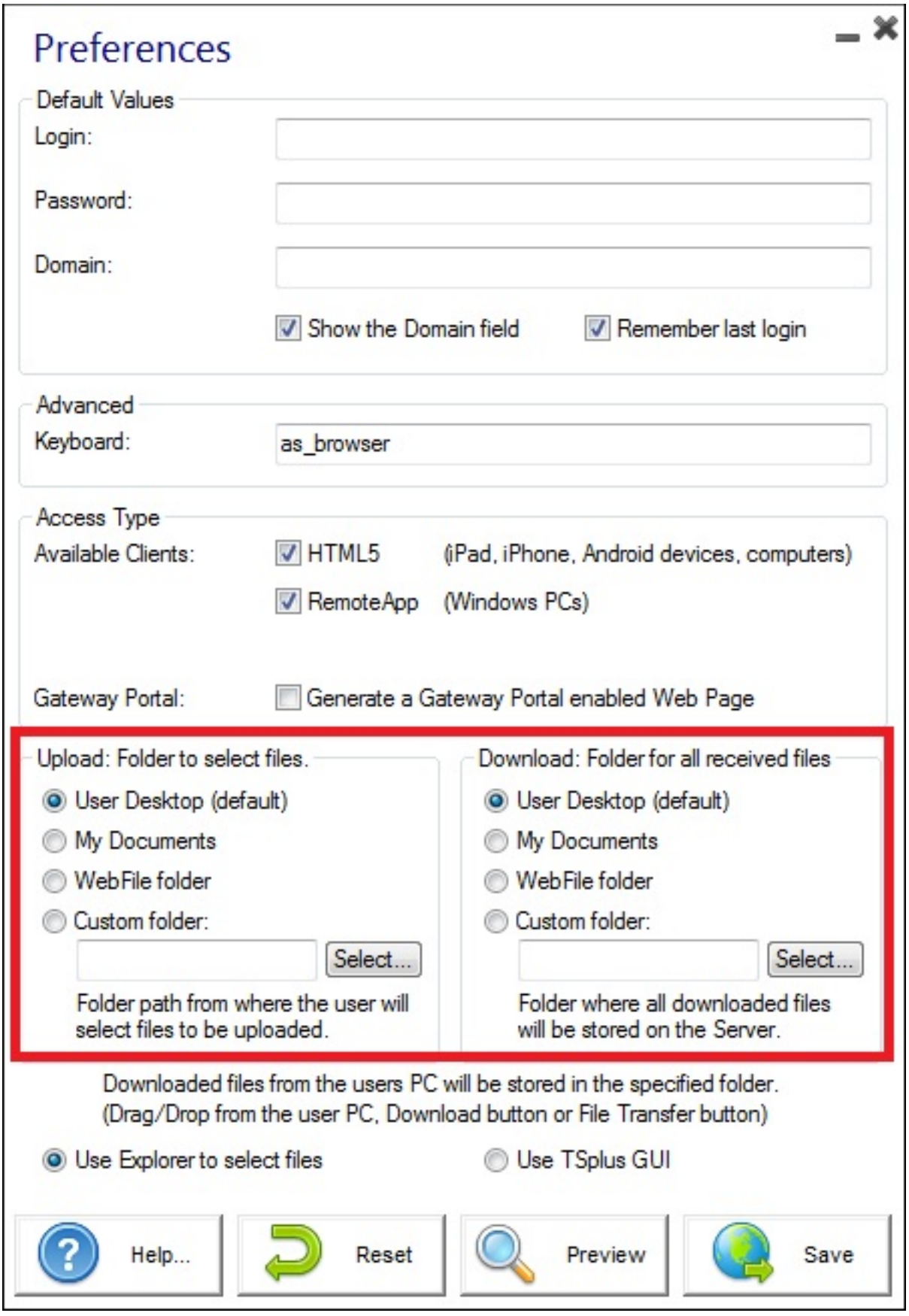


브라우저 측에서 파일은 브라우저의 목록 메뉴 안에 표시됩니다. 작업 메뉴를 통해 또는 Shift + F12로 열 수 있습니다.

- 파일 탐색기를 사용하여 WebFile 폴더에 파일을 복사하면, 이로 인해 WebFile 폴더에 새 파일이 생성되었다는 이벤트가 자동으로 발생하고 브라우저 메뉴가 자동으로 열리거나 새로 고쳐져 새 파일을 표시합니다.



사용자 지정 폴더를 사용할 때, 이 폴더가 클라이언트와 서버 측에 존재하는지 확인하십시오. 관리 도구의 웹 탭에서 웹 포털 기본 설정 타일에서 업로드/다운로드 대상 폴더를 설정할 수 있습니다.



이 동작을 피하고 싶다면 기본 경로인 C:\Program Files (x86)\tsplus\Clients\www\software\html5\settings.js 파일에서 다음 줄을 설정하세요:

dropboxonnewfile = 0;

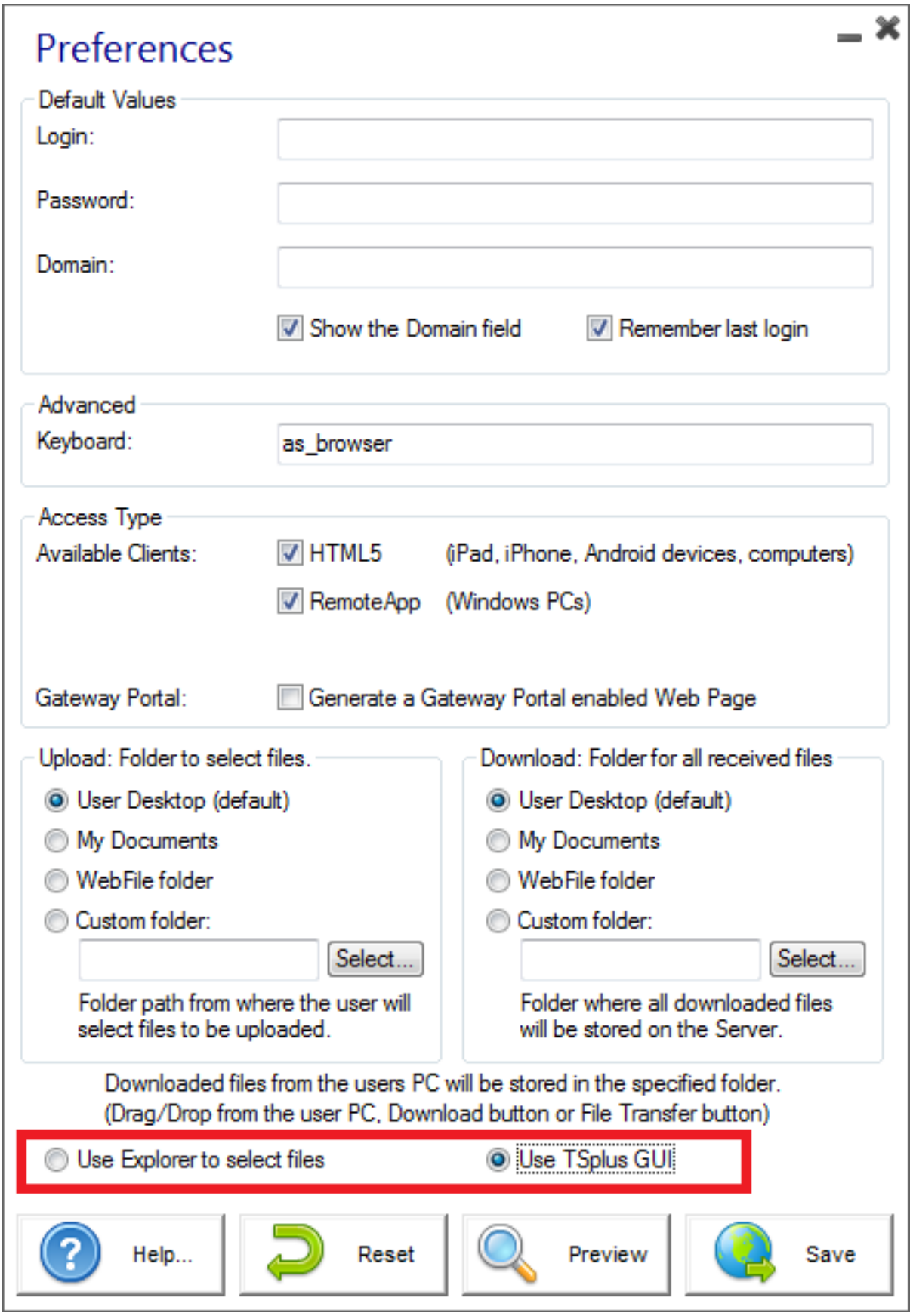
추가로 설정할 수 있습니다:

공유폴더 = “예”;

공유 폴더를 표시하고 다른 사용자와 파일을 공유합니다(기본적으로 비활성화됨).

“C:\Program Files (x86)\TSplus\Clients\www\software\html5” 폴더에 “settings.js”라는 파일이 없다면, 귀하의 TSplus 버전이 오래된 것이며 이 문서는 적용되지 않습니다. 먼저 시스템을 업데이트하거나 지원팀에 문의하시기 바랍니다.

- 기본적으로 파일 전송에 탐색기가 사용됩니다. "TSplus GUI 사용"을 선택하면 서버에서 클라이언트로 파일을 직접 다운로드할 수 있으며, 웹파일 폴더에 파일을 복사할 수 있습니다.


Preferences
Default Values
Login:
Password:
Domain:
Show the Domain field
Remember last login
Advanced
Keyboard:
as_browser
Access Type
Available Clients:
HTML5
(iPad, iPhone, Android devices, computers)
RemoteApp
(Windows PCs)
Gateway Portal:
Generate a Gateway Portal enabled Web Page
Upload: Folder to select files.
User Desktop (default)
My Documents
WebFile folder
Custom folder:
Select...
Folder path from where the user will select files to be uploaded.
Download: Folder for all received files
User Desktop (default)
My Documents
WebFile folder
Custom folder:
Select...
Folder where all downloaded files will be stored on the Server.
Downloaded files from the users PC will be stored in the specified folder.
(Drag/Drop from the user PC, Download button or File Transfer button)
Use Explorer to select files
Use TSplus GUI
Help...
Reset
Preview
Save

HTML5 클라이언트: 모바일 장치에서 제스처 사용 (터치)

화면 영역 사용:

1. 화면에서 쉽게 터치 = 마우스가 터치한 위치로 이동하고 왼쪽 마우스 클릭
2. 빠른 두 번 탭하면 화면에서 마우스가 터치한 위치로 이동하고 왼쪽 마우스 버튼이 두 번 클릭됩니다.
3. 화면에서 1초 동안 터치하고 유지하면 마우스가 터치한 위치로 이동하고 오른쪽 마우스 클릭이 됩니다.
4. 커서 영역 외부를 터치하고 이동하면 세션 프레임이 스크롤됩니다. (이는 특히 핀치 확대 후 스크롤을 위한 기본 브라우저 동작입니다.)
5. 커서 영역을 터치하고 이동 = 마우스 커서만 이동
6. 커서 영역 안에서 두 번 탭하고 이동 = 왼쪽 마우스 버튼을 누르고 마우스를 이동합니다. 창 이동, 요소 이동, 크기 조정에 유용합니다.
7. 화면을 두 번 탭(커서 영역 외부)하고 손가락을 아래/위로 이동 = 중간 마우스 스크롤링 페이지 스크롤이나 PDF 보기 시 유용합니다.
8. 두 손가락으로 핀치 확대 = RDP 세션 프레임 확대 (이것은 기본 브라우저 동작입니다)

마우스 패드 영역 사용 - 마우스 패드 중앙 지점의 추가 기능:

1. 중간에서 쉽게 터치 = 왼쪽 마우스 클릭
2. 중간을 두 번 탭 = 왼쪽 마우스 더블 클릭
3. 중간에서 터치하고 이동 = 마우스 이동 및 마우스 패드 이동
4. 터치하고 1초 동안 유지하면 = 오른쪽 마우스 클릭

키보드 모드 켜짐:

1. 화면에서 쉽게 터치하면 포커스가 잃어지고 키보드가 비활성화됩니다 (이것은 기본 브라우저의 동작입니다) 하지만 이것은 마우스 이동과 왼쪽 마우스 클릭을 발생시킵니다.
2. 빠른 더블 탭 = 마우스 이동 및 왼쪽 마우스 클릭(키보드 비활성화 없이) 커서를 재배치하고, 다른 문자에 포커스를 설정하며, 동시에 키보드 모드에 유지하는 데 유용합니다.
3. 위에 설명된 마우스 패드의 기능

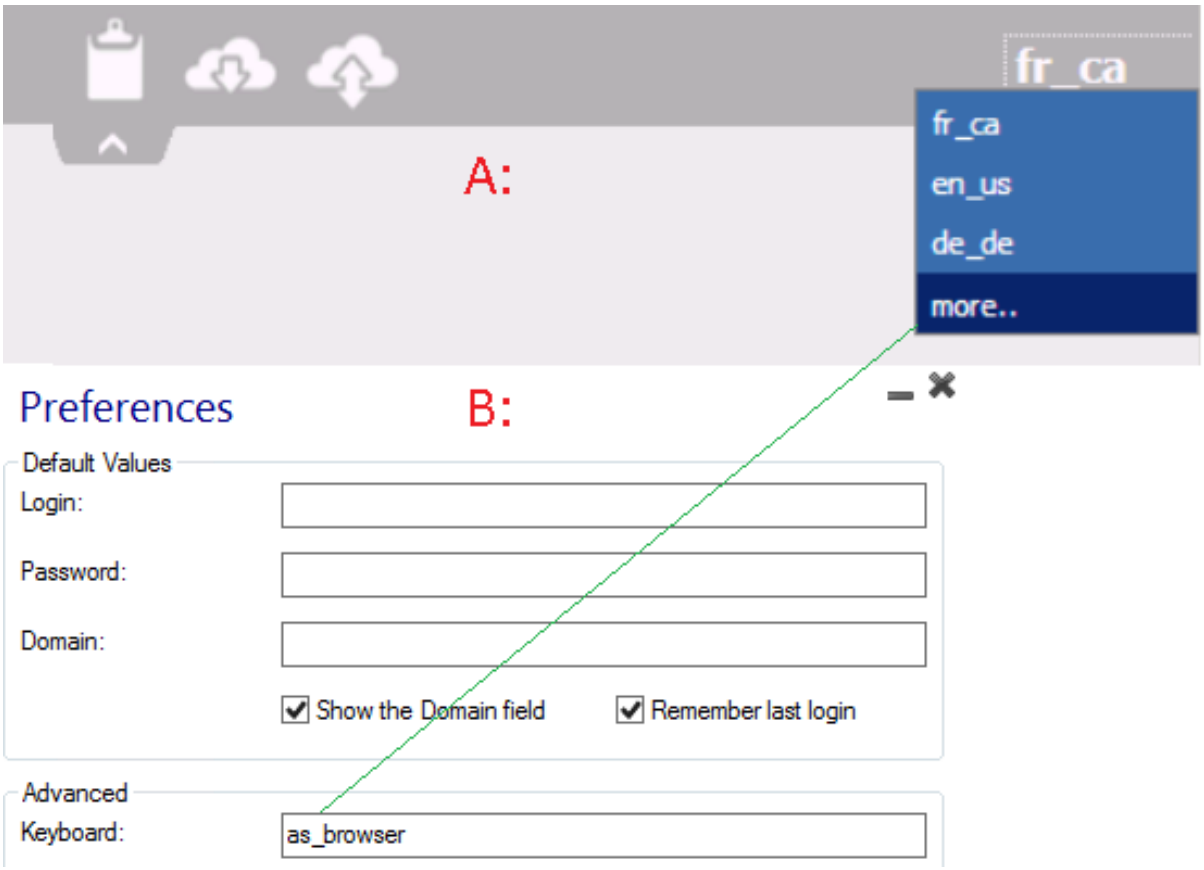
HTML5 클라이언트: 두 가지 언어 사용

기본적으로 HTML5 클라이언트는 브라우저의 기본 언어를 인식하려고 시도한 다음 RDP 세션 내에서 이를 사용합니다. 이 동작은 태그 "as_browser"에 의해 제어됩니다. 그러나 http://에서 사용 가능한 언어 태그의 전체 목록을 찾을 수 있습니다. 당신의 서버 /software/language.html 아래의 "지역"

고정 언어를 설정할 수 있는 선택권이 있습니다. **A:** 클라이언트별로 HTML5 상단 메뉴에서 직접.

	Language	Locale	Value
○	Portal	as_portal	
○	Browser	as_browser	
○	Gateway	as_gateway	
○	Arabic	ar_ar	1025
○	Arabic (Algeria)	ar_dz	5121
○	Assamese	as_as	1101
○	Azeri (Cyrillic)	az_cy	2092
○	Azeri (Latin)	az_lt	1068
○	Belarusian	be_be	1059
○	Bulgarian	bg_bg	1026
○	Bengali	bn_bn	1093
○	Tibetan	bo_bo	1105
○	Bosnian (Cyrillic)	bs_cy	8218
○	Bosnian (Latin)	bs_lt	5146
○	Catalan	ca_ca	1027
○	Czech	cs_cs	1029
○		cs_cz	1029
○	Welsh	cy_gb	1106
○	Danish	da_da	1030
○		da_dk	1030
○	German (Swiss)	de_ch	2055
○	German	de_de	1031
○	Divehi	dv_dv	1125
○	Greek	el_el	1032
○		el_gr	1032
○	English (Canada)	en_ca	1105

B: 관리자 도구 GUI에서 설정하여 모든 사용자에게 적용되도록 포털에서 또는 설정할 수 있습니다.



다른 언어를 기본으로 설정하면 세션을 다시 시작해야 합니다.

기억하세요: 사용할 때 **HTML5 클라이언트** 여러 언어 시나리오에서는 Web-HTML5-RDP 세션 내에서 사용되는 언어가 실제로 PC/Laptop/Mac 등에 설정된 언어와 동기화되어 있는지 확인하십시오. 그렇지 않으면 모든 언어 맵에서 표현되고 교차되는 일부 문자가 다른 언어에 대해 실제로 전송되는 스캔 코드로 인해 잘못된 문자를 생성할 수 있습니다. 또한, 웹 세션 내에서 언어를 영어에서 독일어로 변경한 경우 PC/Laptop/Mac에서도 독일어로 변경해야 한다는 의미입니다.

HTML5 클라이언트: 브라우저 창을 최대화하는 방법

개요

RDP 프로토콜은 재연결 없이 연결된 상태에서 크기를 조정하는 것을 허용하지 않습니다.

Terminal Service Plus HTML5 클라이언트에 연결하여 최상의 경험을 얻을 수 있습니다. 최대화된 브라우저 **.**

그러나 브라우저 창을 가능한 한 크게 만들고 싶다면 HTML5 창을 최대 크기로 열도록 "강제"할 수 있습니다(하지만 인터넷 브라우저 보안 제한으로 인해 "최대화된" 창으로는 열 수 없습니다).

브라우저 창 최대화

파일 “Clients\www\software\common.js”를 Terminal Service Plus 디렉토리에서 수정해야 합니다. Notepad++와 같은 텍스트 편집기를 사용하는 것이 좋습니다. 아니다 Word를 사용하세요.

브라우저 창이 화면을 모두 사용하도록 하려면 "window.open"이 포함된 줄을 수정하고 다음 텍스트를 추가해야 합니다:

터미널 창

"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(screen.availHeight-(55))

이것은 IE/Chrome/Firefox/Safari가 화면 크기로 창을 열 수 있게 해줍니다(Windows 바를 제외한 크기). 불행히도 웹 브라우저가 "전체 화면" Windows 유형에서 창을 "최대화"하도록 강제하는 것은 불가능합니다.

파일을 열고 “window.open(”을 검색하세요.

그런 다음 괄호 앞에 새 항목을 추가하십시오.

터미널 창

```
window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
```

다음과 같이 됩니다:

터미널 창

```
window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

그리고 다시:

터미널 창

```
tmpwin = window.open(p, '_blank'); //Chrome needs _blank
```

다음과 같이 됩니다:

터미널 창

```
tmpwin = window.open(p, '_blank',
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55))); //Chrome needs _blank
```

그리고 다시:

터미널 창

```
success = window.open(p, k);
```

다음과 같이 됩니다:

터미널 창

```
success = window.open(p, k,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

마지막으로:

터미널 창

```
cpwin = window.open("about:blank", n);
```

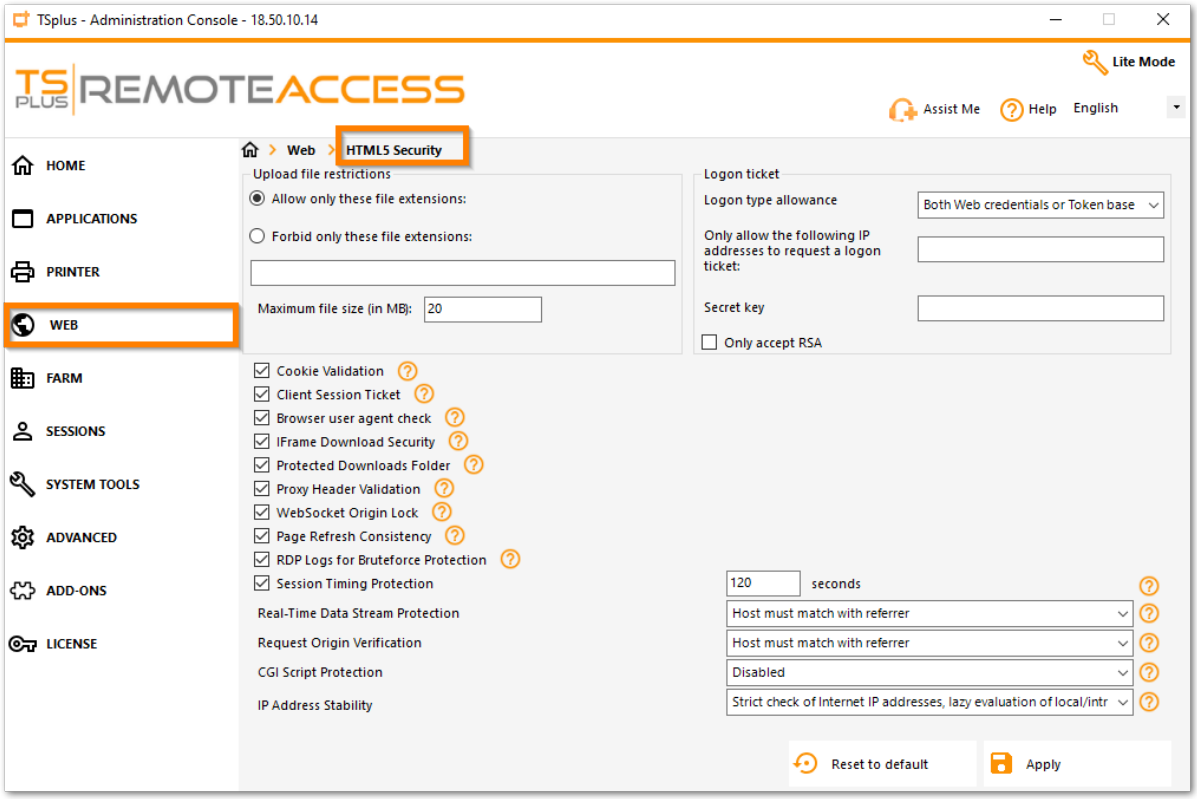
다음과 같이 됩니다:

터미널 창

```
cpwin = window.open("about:blank", n,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

HTML5 보안

HTML5 보안 탭에서 웹 설정을 관리할 수 있습니다.



추가 보안이 필요하시면 저희의 [보안]을 확인하고 다운로드할 수 있습니다. Advanced Security .

HTML5 서버 메모리 사용량

Terminal Service Plus HTML5 Server는 JAVA에서 실행됩니다. JAVA가 메모리를 처리하는 방식을 이해하면 Terminal Service Plus HTML5 Server의 메모리 사용을 이해하는 데 도움이 됩니다.

할당된 메모리

Java가 실행될 때, 컴퓨터의 물리적 메모리의 25%를 할당하려고 합니다. 이 메모리는 "할당"되지만 직접 사용되지는 않으며, Windows 작업 관리자에서 볼 수 있는 실제 메모리 사용량은 아닙니다.

JAVA 플랫폼: 32비트 vs 64비트

이 두 플랫폼 간에는 큰 차이점이 하나 있습니다:

- JAVA 32비트는 정의상 4GB 이상의 RAM을 처리할 수 없습니다. 사용 가능한 모든 메모리의 25%를 할당하므로, 4GB의 물리적 메모리가 있다고 가정할 때 최대 1GB를 할당합니다. 물리적 메모리가 2GB만 있는 경우에는 500MB만 할당합니다.
- JAVA 64비트는 4GB보다 훨씬 더 많은 용량을 처리할 수 있습니다(이론적으로 최대 16GB까지). 엑사 바이트이므로 할당된 메모리는 물리적 메모리에만 의존하게 됩니다.

JAVA 메모리 관리

JAVA는 "가상 머신"입니다. 이는 JAVA가 메모리 관리를 스스로 처리한다는 것을 의미합니다. JAVA가 일부 메모리를 할당하면, 더 이상 필요하지 않더라도 시스템에 자동으로 반환하지 않습니다. 이는 성능상의 이유로, 메모리 할당 및 해제는 CPU 집약적인 작업이기 때문입니다.

JAVA는 일반적으로 시스템에 반환하기 전에 사용되지 않는 메모리의 큰 덩어리를 기다립니다. 이 큰 덩어리의 크기는 컴퓨터 물리적 메모리의 크기에 직접적으로 의존합니다. 컴퓨터의 물리적 메모리가 많을수록 JAVA에 의해 할당되는 메모리도 많아집니다.

터미널 서비스 플러스 HTML5 서버 메모리 사용량

이 모든 기술적 세부사항은 사용자가 Windows 작업 관리자를 열고 Terminal Service Plus HTML5 Server가 많은 메모리를 사용한다고 생각하거나 JAVA 32비트가 JAVA 64비트보다 적은 메모리

를 사용한다고 생각하는 이유입니다.

실제로 Terminal Service Plus HTML5 Server에서 실제로 사용되는 메모리는 열려 있는 HTML5 세션의 수와 직접적으로 관련이 있습니다. 컴퓨터의 사용 가능한 메모리가 많을수록 더 많은 HTML5 세션을 열 수 있습니다.

HTML5 세션 메모리 사용량

HTML5 세션에서 사용되는 메모리는 사용자 활동(사용된 애플리케이션 및 프로그램, 워드/엑셀 대 드로잉 집약적인 프로그램)과 Terminal Service Plus HTML5 서버와 클라이언트 컴퓨터 간에 설정된 연결 방법에 따라 달라집니다.

일반적인 사용 사례에서 HTML5 세션은 30MB의 메모리를 사용합니다(표준 사용, 이진 웹소켓 연결). 최악의 경우, 세션은 최대 100MB의 메모리를 사용할 수 있습니다(집중 사용, 구형 브라우저를 위한 "XHR" 폴백 연결).

HTTP 및 HTTPS 서버 수신 손실

각 Java 오류 로그는 작동을 위한 충분한 네이티브 메모리를 나타냅니다.

문제는 사실 꽤 간단합니다.
HTML5 세션이 시작되면 보고된 값에 따라 충분한 메모리가 있습니다.
그런 다음 RDP 세션 내에서 알 수 없는 프로그램을 시작하고 모든 기본 메모리를 자신을 위해 훔칩니다.

Java가 다시 요청할 때 갑자기 더 이상 사용할 수 없게 되어 이 메모리 부족 오류가 발생합니다.

- Java 실행 환경이 계속 실행될 수 있도록 메모리가 부족합니다.
- 네이티브 메모리 할당(mmap)이 234881024 바이트를 매핑하는 데 실패했습니다. 오류 세부정보: 가상 공간 G1# 가능한 이유:
- 시스템에 물리적 RAM 또는 스왑 공간이 부족합니다. 이 프로세스는 압축된 Oops가 활성화된 상태로 실행되고 있으며, Java 힙이 네이티브 힙의 성장을 차단할 수 있습니다.

가능한 솔루션:

- 시스템의 메모리 부하를 줄이십시오.
- 물리적 메모리 또는 스왑 공간 증가# 스왑 지원 저장소가 가득 찼는지 확인하십시오.
- Java 힙 크기 줄이기 (-Xmx/-Xms)
- Java 스레드 수 감소 # Java 스레드 스택 크기 감소 (-Xss)
- -XX:ReservedCodeCacheSize=의 더 큰 코드 캐시를 설정합니다.

JVM은 제로 기반 압축 Oops 모드에서 실행되고 있으며, 이 모드에서는 Java 힙이 처음 32GB 주소 공간에 배치됩니다. Java 힙의 기본 주소는 네이티브 힙 성장의 최대 한계입니다.
사용해 주세요 **-XX:HeapBaseMinAddress**

잠재적으로, 처음부터 Java에 더 많은 네이티브 메모리를 할당하고 시스템에 메모리를 반환하지 않도록 강제하여 자신에게 할당할 수 있습니다.
그러나 이 경우 RDP 세션에서 실행 중인 프로그램이 메모리가 부족해질 수 있으며, 전체 시스템이 중단될 수 있습니다.

하지만 여전히 시도해 볼 수 있습니다.

1.
   다음 파일을 메모장으로 열고 수정하십시오: *\Clients\webserver\runwebserver.ini

2.
   거기에서 다음과 같은 명령줄 설정을 찾을 수 있습니다.

터미널 창

-Djdk.tls.ephemeralDHKeySize=matched -Djdk.tls.rejectClientInitiatedRenegotiation=true -Dorg.jboss.netty.epollBugWorkaround=true -XX:+UseG1GC -XX:MinHeapFreeRatio=10 -XX:MaxHeapFreeRatio=10 **********
and so on

3. runwebserver.ini 파일의 전체 줄을 제거하고 그 자리에 다음을 추가하십시오:

터미널 창

-server -javaagent:"%~dp0httpwebs.jar" -Djdk.tls.ephemeralDHKeySize=matched -Djdk.tls.rejectClientInitiatedRenegotiation=true -Dorg.jboss.netty.epollBugContourn=true --add-opens java.prefs/java.util.prefs=ALL-UNNAMED --add-opens java.base/java.lang.reflect=ALL-UNNAMED --add-opens java.base/sun.security.ssl=ALL-UNNAMED --add-opens java.base/java.nio=ALL-UNNAMED --add-opens java.base/jdk.internal.ref=ALL-UNNAMED --add-exports java.prefs/java.util.prefs=ALL-UNNAMED ---add-exports java.base/java.lang.reflect=ALL-UNNAMED --add-exports java.base/sun.security.ssl=ALL-UNNAMED --add-exports java.base/

jdk.internal.ref=ALL-UNNAMED --add-exports java.base/java.nio=ALL-UNNAMED

4. HTML5 서버를 AdminTool GUI를 통해 재시작하여 변경 사항을 적용하십시오.
   하지만 그렇게 하기 전에 web server\runwebserver.bat 파일의 속성에 읽기 전용 속성이 설정되어 있지 않은지 확인하십시오. 그렇지 않으면 AdminTool GUI가 재시작 후 runwebserver.bat를 조정할 수 없습니다.

대부분의 경우, 이것으로 충분해야 합니다. Java가 메모리를 사용하면 시스템에 반환하는 대신 다른 용도로 할당합니다. 따라서 html5service.exe의 메모리 사용량은 시스템의 사용 가능한 메모리의 70%에 이를 수 있습니다. 이 경우, Java는 충돌을 멈춰야 합니다. 그러나 다른 프로그램이 많은 메모리를 소비하고 있다면 대신 충돌할 수 있습니다. 그런 경우, 우리는 무력합니다; Java HTML 서버와 다른 프로그램을 실행할 수 있는 충분한 메모리가 있는지 확인해야 합니다.

Java에는 -XX:+AggressiveHeap이라는 옵션이 있어 Java 가상 머신 자체의 메모리 할당을 개선할 수 있으며, 따라서 *\webserver\runwebserver.ini의 최종 내용에 영향을 줄 수 있습니다.

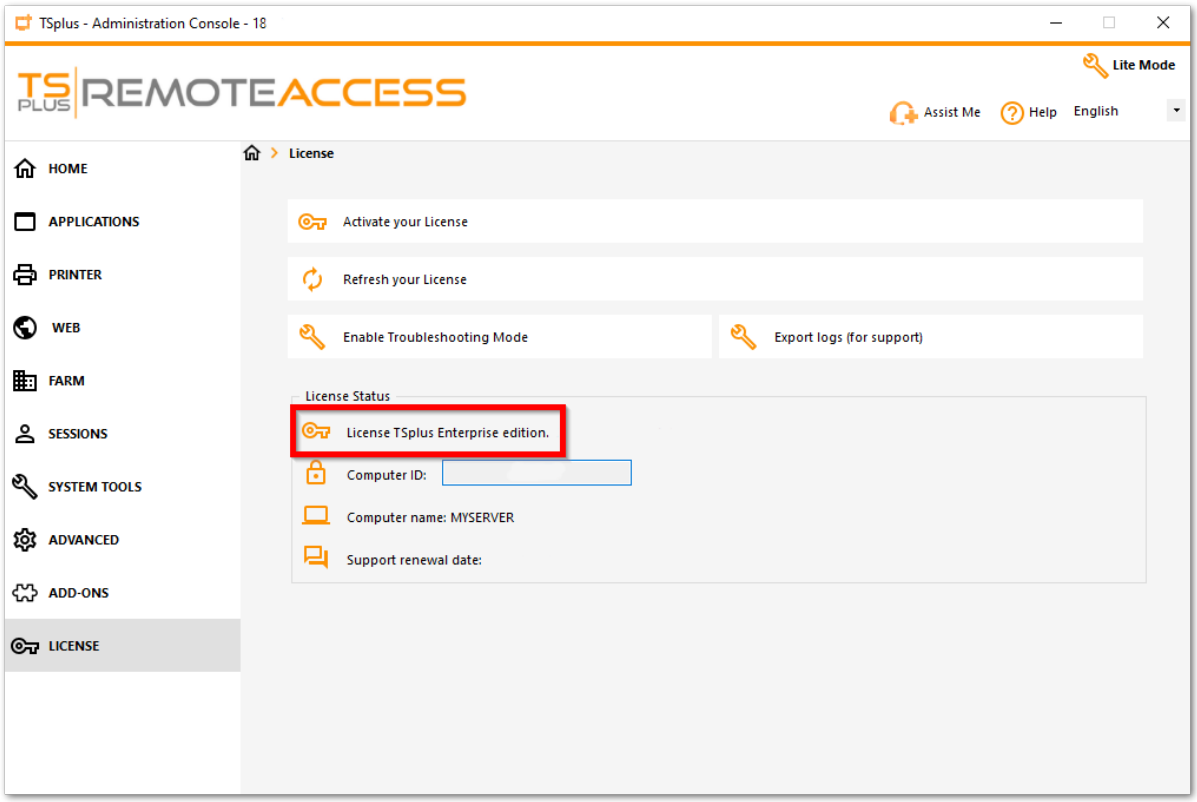
이것은 다음과 같이 보일 수 있습니다:

터미널 창

-XX:+AggressiveHeap -server -javaagent:"%~dp0httpwebs.jar" -Djdk.tls.ephemeralDHKeySize=matched -Djdk.tls.rejectClientInitiatedRenegotiation=true -Dorg.jboss.netty.epollBugWorkaround=true --add-opens java.prefs/java.util.prefs=ALL-UNNAMED --add-opens java.base/java.lang.reflect=ALL-UNNAMED --add-opens java.base/sun.security.ssl=ALL-UNNAMED --add-opens java.base/java.nio=ALL-UNNAMED --add-opens java.base/jdk.internal.ref=ALL-UNNAMED --add-exports java.prefs/ java.util.prefs=ALL-UNNAMED --add-exports java.base/java.lang.reflect=ALL-UNNAMED --add

귀하의 TSplus 에디션을 식별하는 방법

라이센스 타일의 일련 번호 아래에서 구매한 라이센스 유형과 연결 수 옆에 있는 사용자 수를 확인할 수 있습니다.



TSplus는 더 명확성을 얻기 위해 이전 라이센스를 하나로 통합했습니다. 시스템 및 프린터 에디션은 다음으로 이전되었습니다. **Desktop Edition** .

Desktop Edition

기본 기능:

- TSplus 관리자 도구 (AdminTool),

- 동시 연결 지원,
- 사용자 및/또는 그룹별 애플리케이션 제어,
- TSplus 원격 작업 표시줄 및/또는 TSplus 플로팅 패널,
- 원격 데스크톱 액세스,
- TSplus 휴대용 클라이언트 생성기,
- 원격 앱 연결 클라이언트,
- RDP 프로토콜을 완전히 준수합니다.
- 듀얼 스크린 지원, 양방향 사운드, Windows 버전과 호환될 때 RemoteFX,
- 로컬 및 원격 연결 지원,
- 워크그룹 및 Active Directory 사용자 지원,
- 장치/디스크 리디렉션.
- 가상 프린터는 특정 드라이버를 설치할 필요 없이 모든 위치에서 인쇄할 수 있게 해주며 프린터 리디렉션을 허용합니다.

모바일 웹 에디션

모든 시스템 및 프린터 에디션 기능 외에 다음을 수행할 수 있습니다:

- 모든 웹 브라우저에서 TSplus HTTP 웹 서버로 연결하세요.

- 모든 웹 브라우저에서 TSplus HTTPS 웹 서버 및 SSH 서버를 통한 완전히 안전한 연결
- HTML 페이지에는 Windows 및 HTML5 웹 액세스 클라이언트가 포함됩니다.
- iPhone/iPad 및 Android 기기에서 쉽게 연결할 수 있으며, 또한 TSplus 모바일 앱 ,
- TSplus의 사용하기 쉬운 웹마스터 툴킷으로 로그인 웹 페이지를 사용자 정의하세요.
- TSplus 웹 애플리케이션 포털을 통해 사용자는 웹 브라우저 내에서 애플리케이션 목록에 접근할 수 있습니다.
- Windows 자격 증명 대신, TSplus 웹 자격 증명은 사용자가 이메일이나 핀 코드만으로 연결할 수 있도록 합니다.
- 유니버설 프린터를 사용하면 특정 프린터 드라이버를 설치하지 않고도 어떤 위치에서든 인쇄할 수 있습니다.

Enterprise Edition

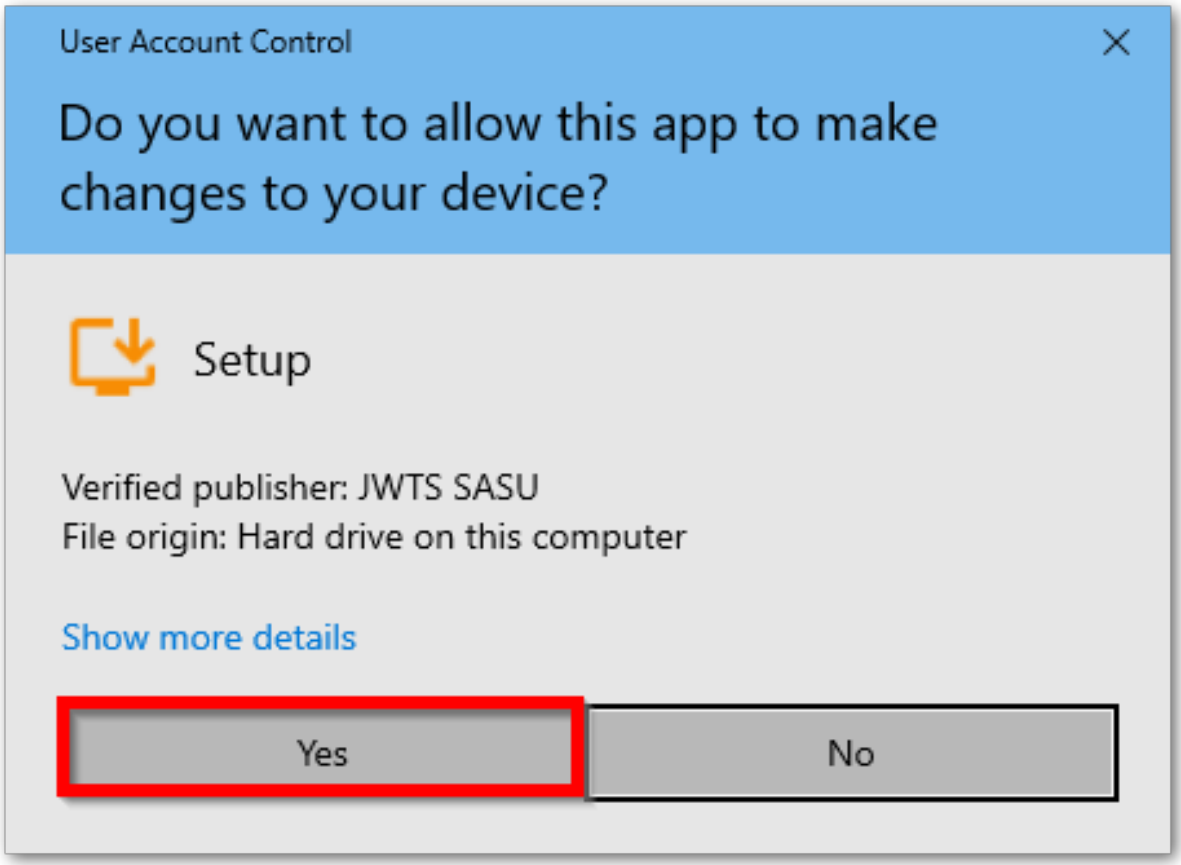
이전의 모든 기능에 이러한 기능이 추가됩니다:

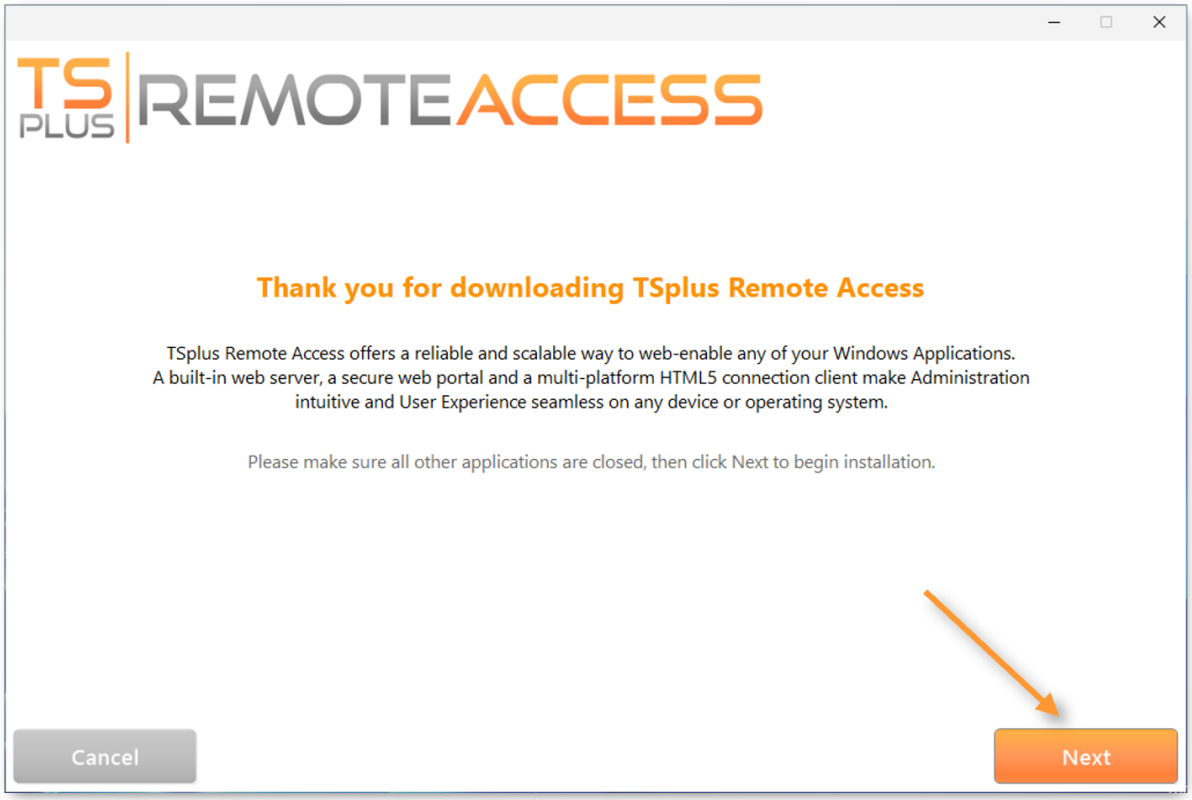
- 각 TSplus 팜 내에서 무제한 서버를 지원합니다(서버당 하나의 라이센스가 필요함).
- 수천 명의 사용자가 확장 가능한 로드 밸런스 아키텍처에서 동시에 작업하고 있습니다.
- 모든 TSplus 서버에 접근할 수 있는 단일 기업 포털,
- 사용자 또는 사용자 그룹에 하나 이상의 애플리케이션 서버를 할당할 수 있는 기능,
- 로드 밸런싱 및 장애 조치 지원이 포함되어 있습니다.

- 추가 보안 계층을 추가할 수 있는 가능성 TSplus 2FA 추가 기능 .

TSplus Remote Access v19 설치

실행 TSplus Remote Access 설치 프로그램 그리고 나서 **설치 단계를 따르십시오.** .
귀하의 로컬 관리자 비밀번호는 TSplus Remote Access의 첫 번째 재시작 후에 필요합니다.





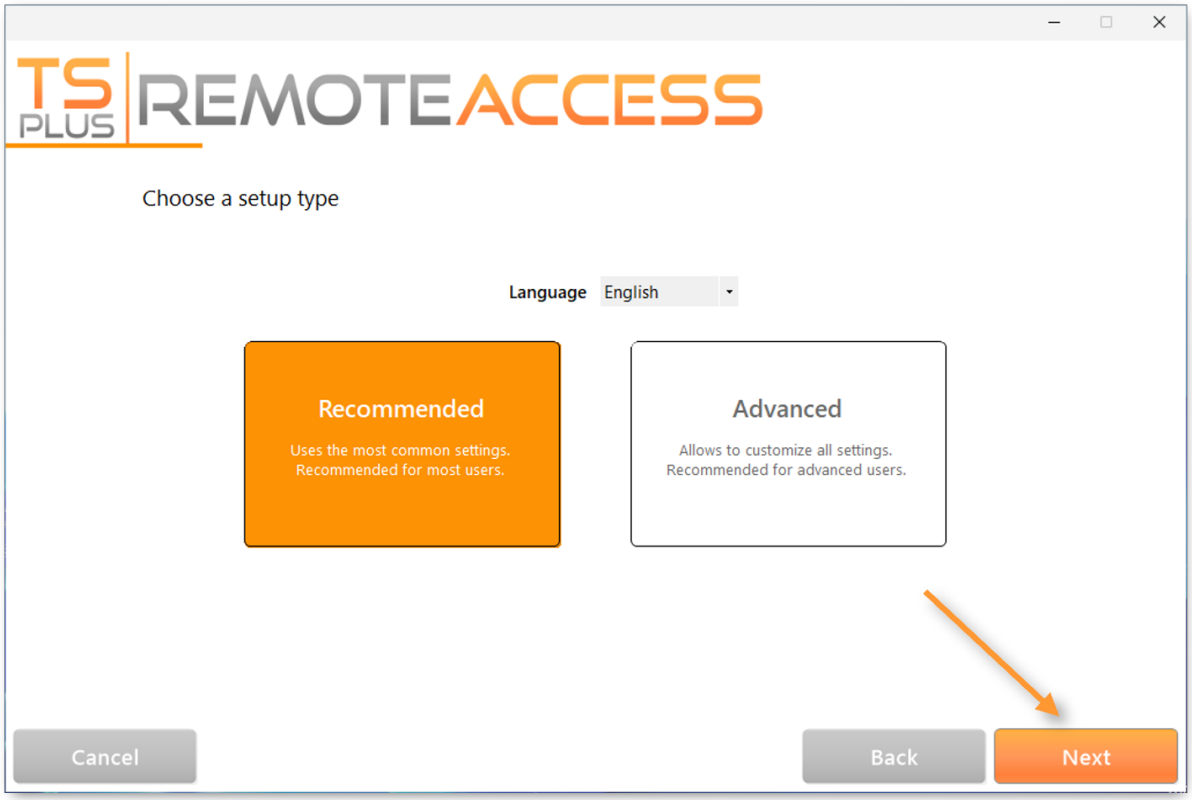
그런 다음 언어를 선택할 수 있습니다(나중에 변경 가능).

그런 다음 해당 상자를 선택하여 두 가지 사용자 정의 옵션을 선택할 수 있습니다: **추천** 또는 **고급**

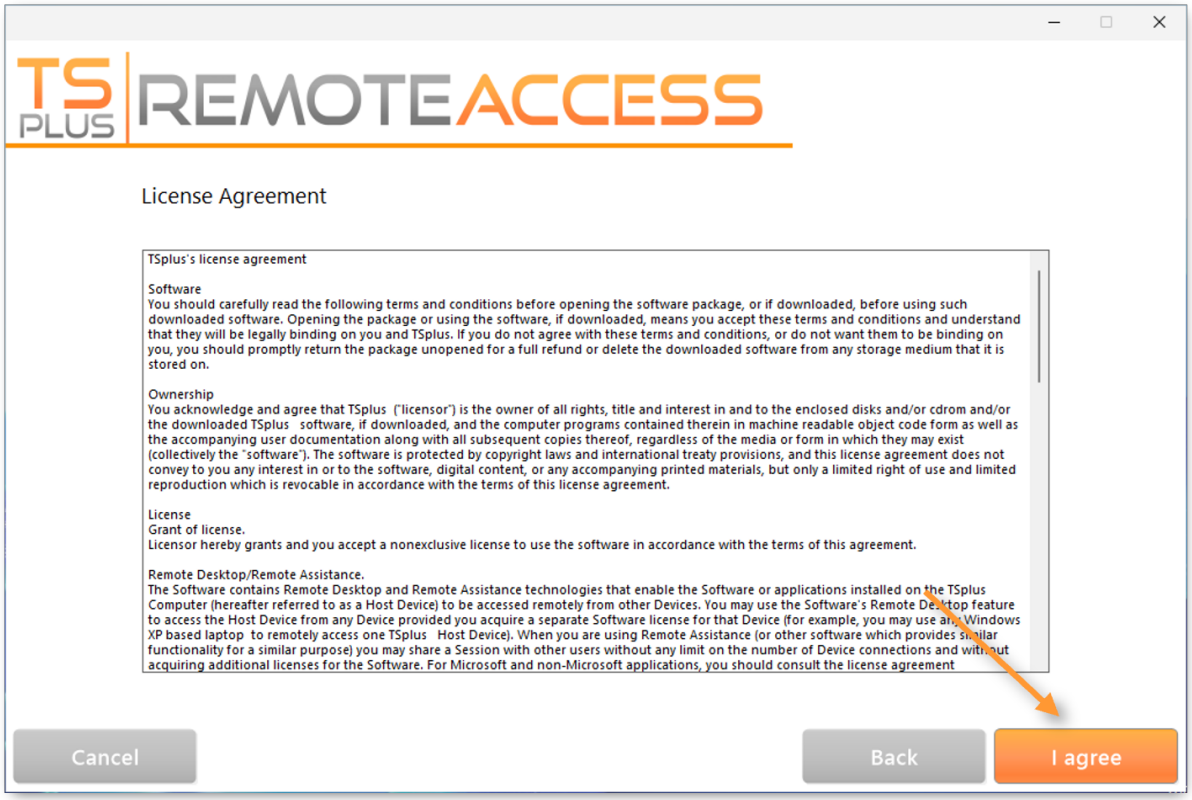
고급 옵션을 사용하면 다음을 수행할 수 있습니다:

- TSplus Advanced Security를 설치하지 않음.
- 사용자 정의 프록시 설정을 사용하십시오.
- 설치하지 않는 설치 프로그램만 다운로드하십시오.
- 기본 포트 변경(권장하지 않음).

다음 클릭.



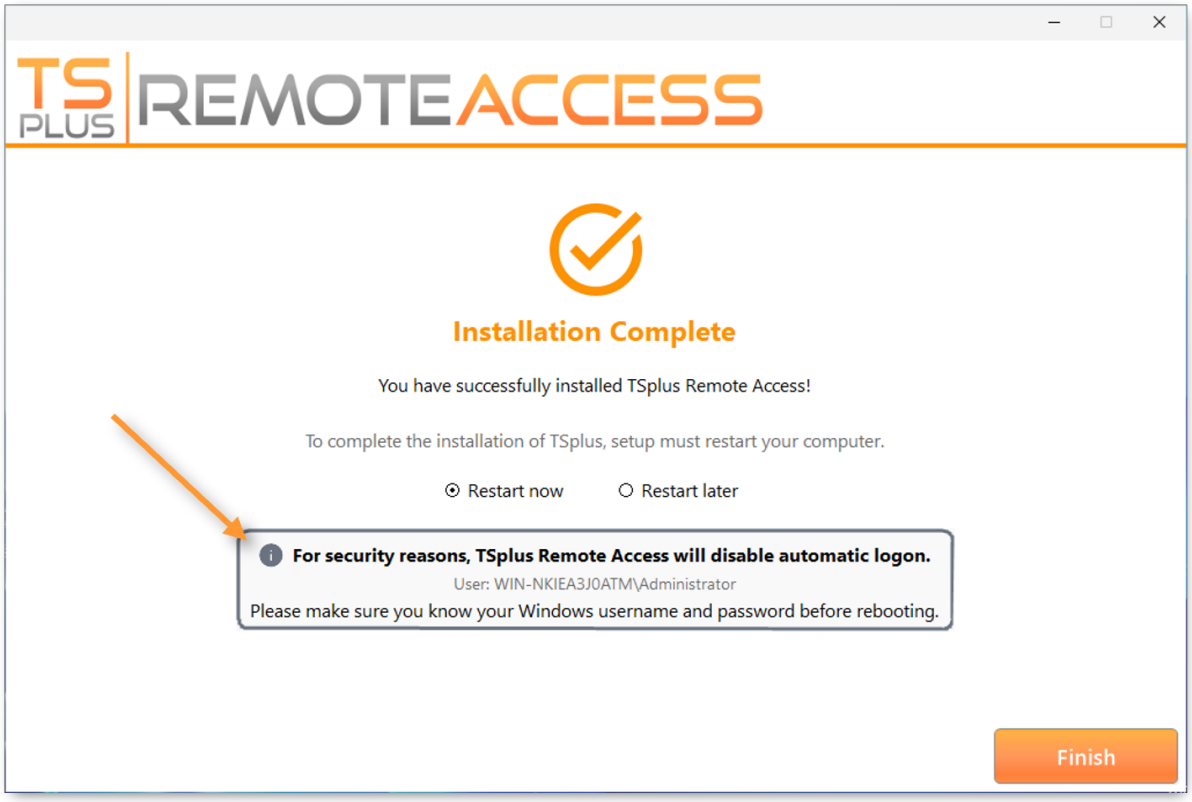
클릭하세요 “나는 계약에 동의합니다.”



프로그램을 다운로드하고 설치하는 중입니다. 잠시 기다려 주십시오.



그런 다음 TSplus 로고가 나타나고 설치 완료에 대한 정보가 포함된 창이 표시됩니다.

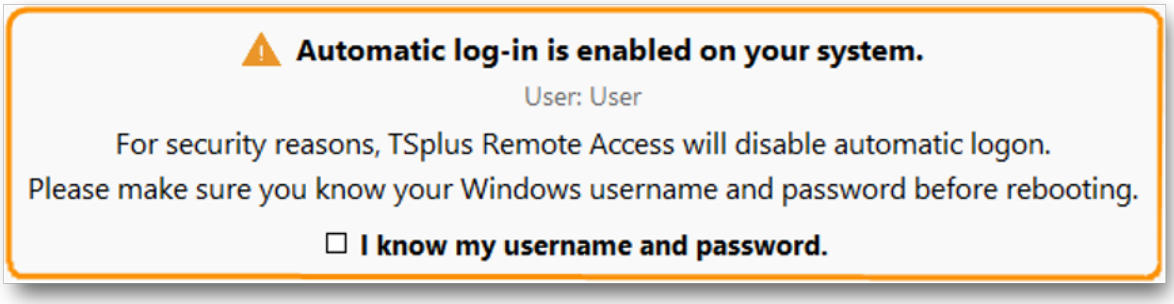


☐ 중요 공지

보안상의 이유로, **TSPlus 원격 액세스** 각 로그인 시 사용자 이름과 비밀번호를 수동으로 입력해야 합니다.

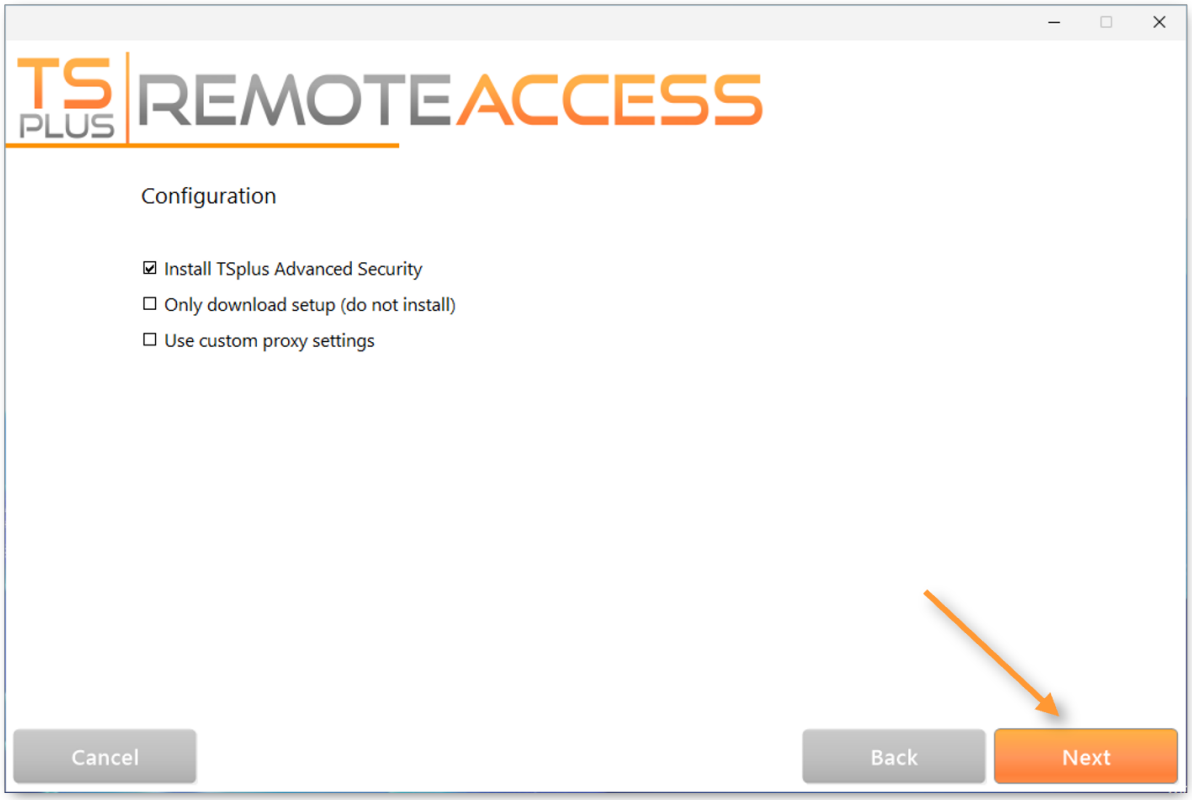
시스템을 재시작하기 전에 자격 증명을 알고 있는지 확인하여 잠기는 것을 피하십시오.

만약
자동 로그인
시스템에서 활성화되면, 설치 프로그램은 사용자 이름과 비밀번호를 알고 있음을 확인하라는 경고 팝업을 표시합니다.



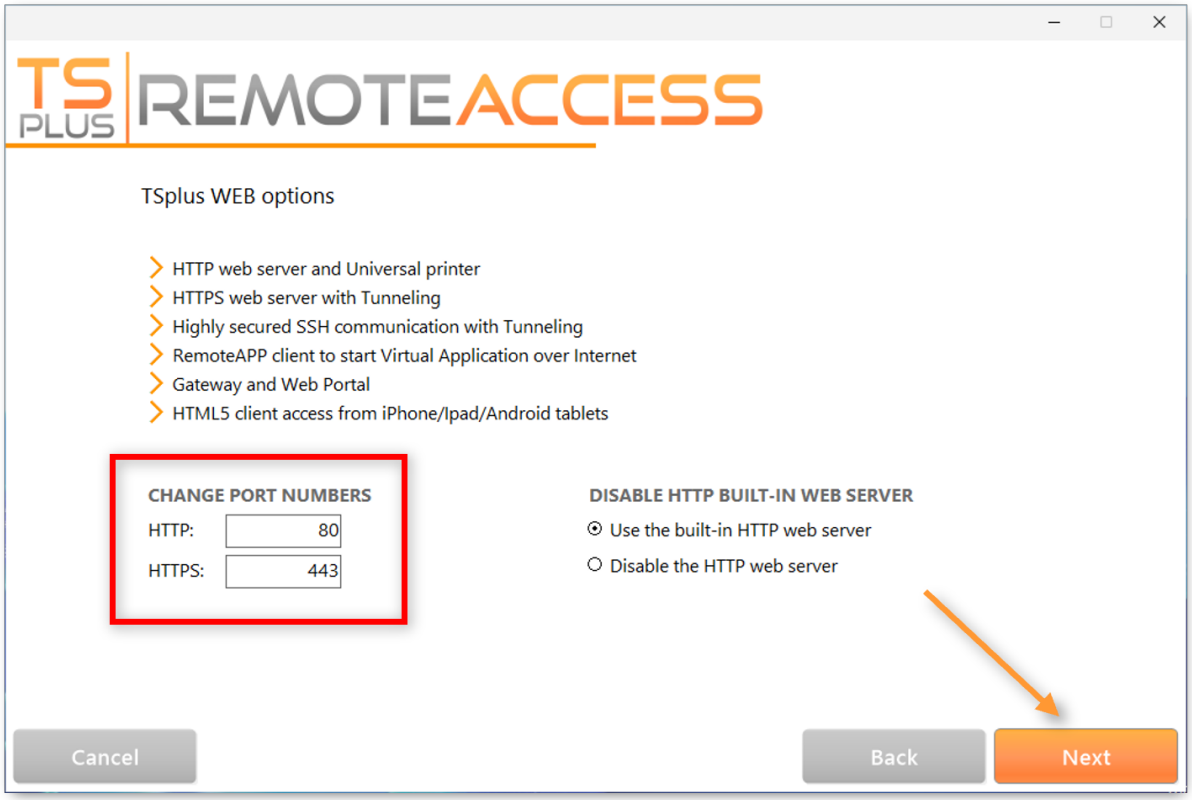
TSplus를 사용하려면 시스템을 재부팅해야 합니다. 체험 기간은 15일 동안 전체 제품과 5명의 동시 사용자를 제공합니다.

아래 단계는 TSplus Remote Access 설치를 확인하는 경우에만 진행하십시오. **고급 모드** .

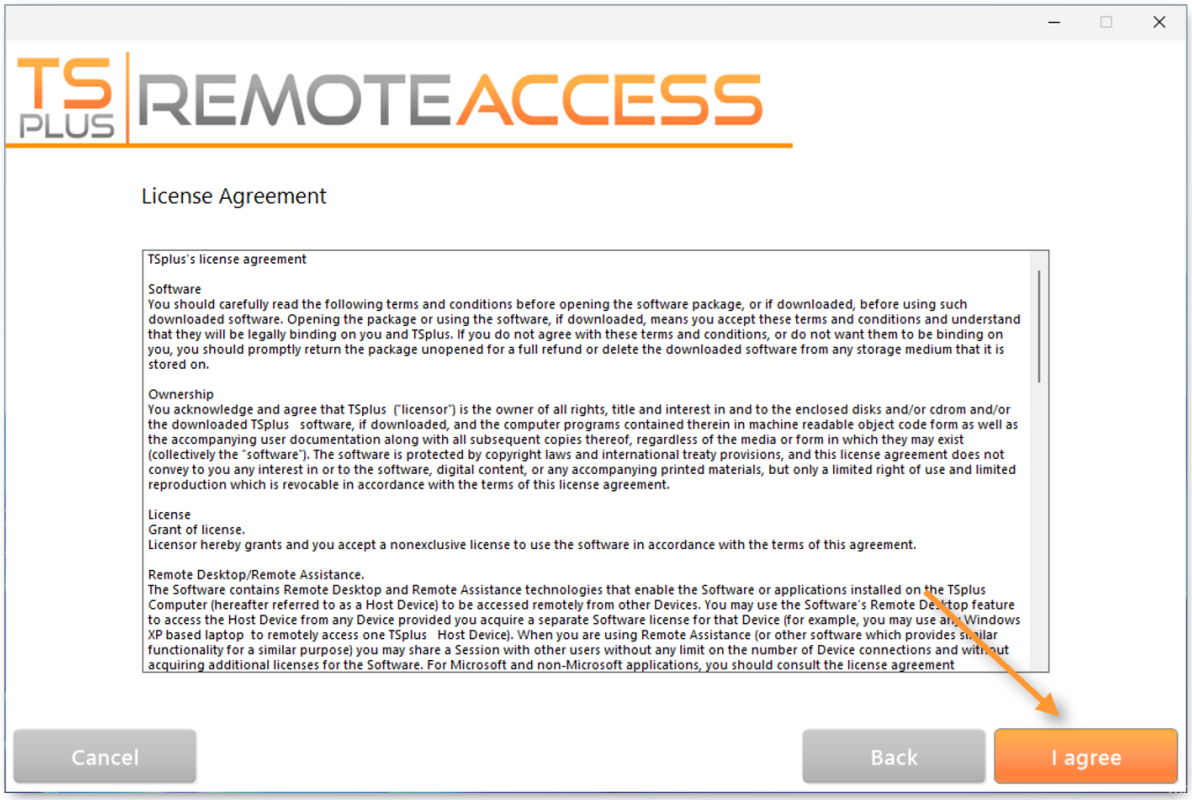


웹 서버는 기본적으로 포트 80과 443에서 수신 대기하고 있습니다. TSplus 기본 설치 설정을 수락할 것을 권장합니다. 우리의 경험에 따르면, 대부분의 생산 문제는 Windows 보안 기능으로 인해 발생합니다.

설치 중이나 언제든지 원하는 경우 이러한 포트를 수정할 수 있습니다. 관리 도구의 내장 웹 서버 관리 정의된 포트가 사용 가능하고 서버에 Java가 설치되어 있는지 확인하십시오.



클릭하세요 “나는 계약에 동의합니다.”



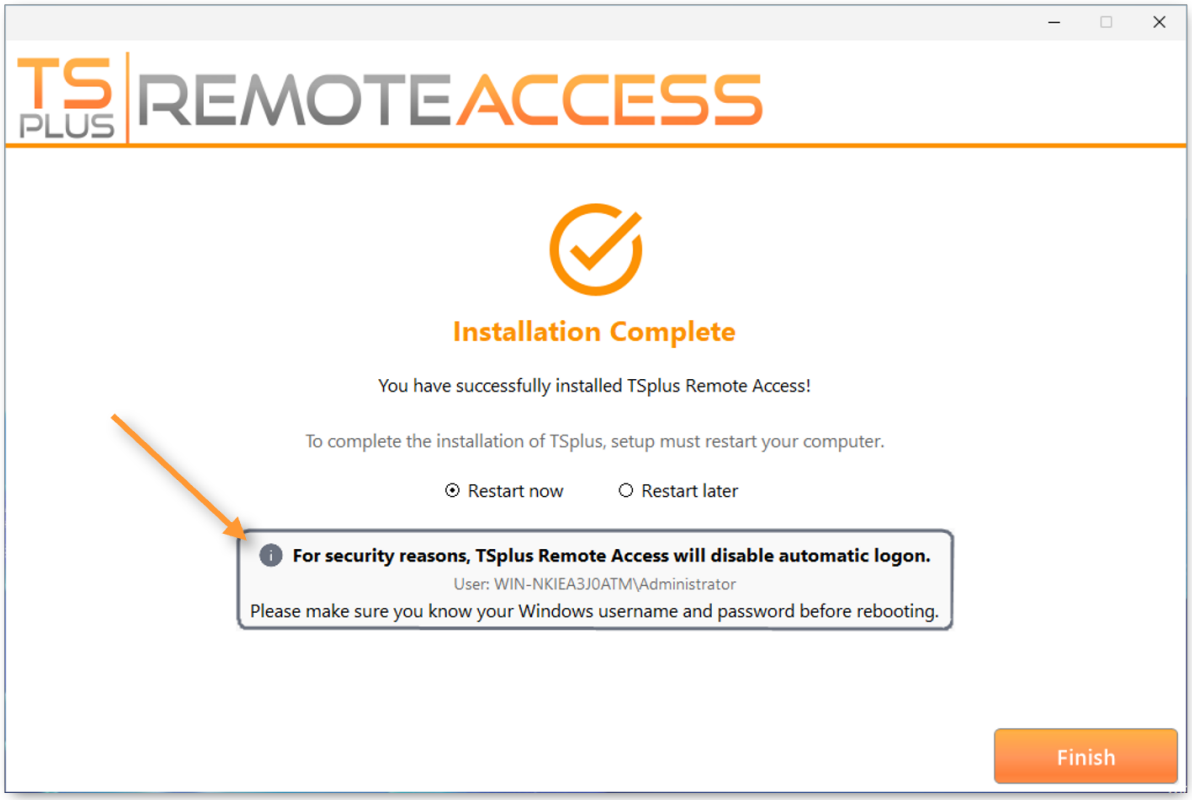
진행 표시줄이 나타나고 프로세스의 진행 상황을 따라갈 수 있습니다:



- TSplus 11.40 버전 이후로 설치할 선택권이 있습니다. TSplus 고급 보안 우리의 강력한 보안 추가 기능, 궁극적인 시험 버전(모든 보안 기능을 2주 동안 무료로 사용할 수 있음)을 귀하의 TSplus 시스템에:

이 제품에 대한 자세한 정보는 TSplus Advanced Security에 대한 페이지를 참조하십시오. 문서화 .

그런 다음 TSplus 로고가 나타나고 설치 완료에 대한 정보가 포함된 창이 표시됩니다.

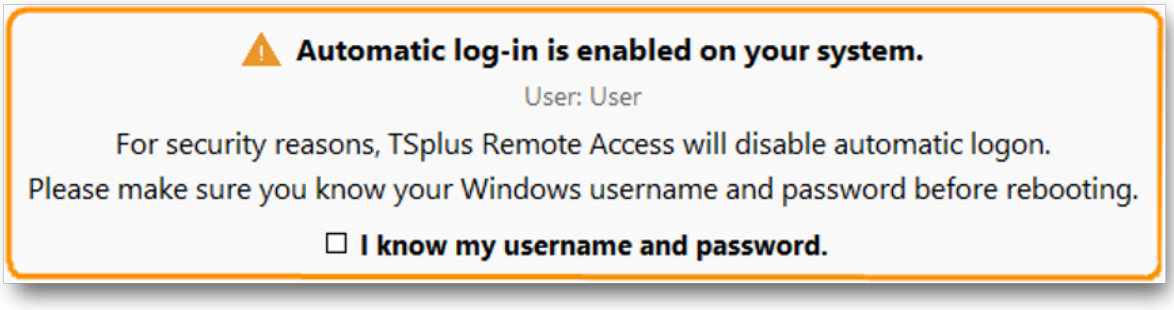


☐ 중요 공지

보안상의 이유로, **TSPlus 원격 액세스** 각 로그인 시 사용자 이름과 비밀번호를 수동으로 입력해야 합니다.

시스템을 재시작하기 전에 자격 증명을 알고 있는지 확인하여 잠기는 것을 피하십시오.

만약
자동 로그인
시스템에서 활성화되면, 설치 프로그램은 사용자 이름과 비밀번호를 알고 있음을 확인하라는 경고 팝업을 표시합니다.



TSplus를 사용하려면 시스템을 재부팅해야 합니다. 체험 기간은 15일 동안 전체 제품과 5명의 동시 사용자를 제공합니다.

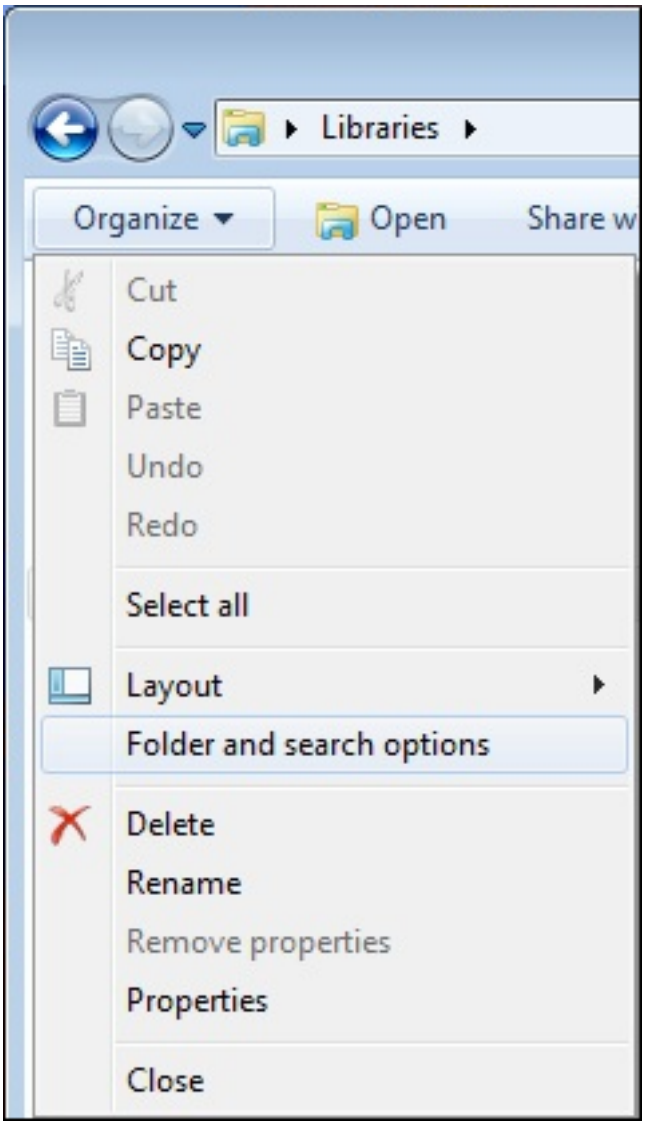
TSplus 세션 내에서 논리 드라이브를 마운트하는 방법

이 튜토리얼에서는 다음과 같은 측면을 다룰 것입니다:

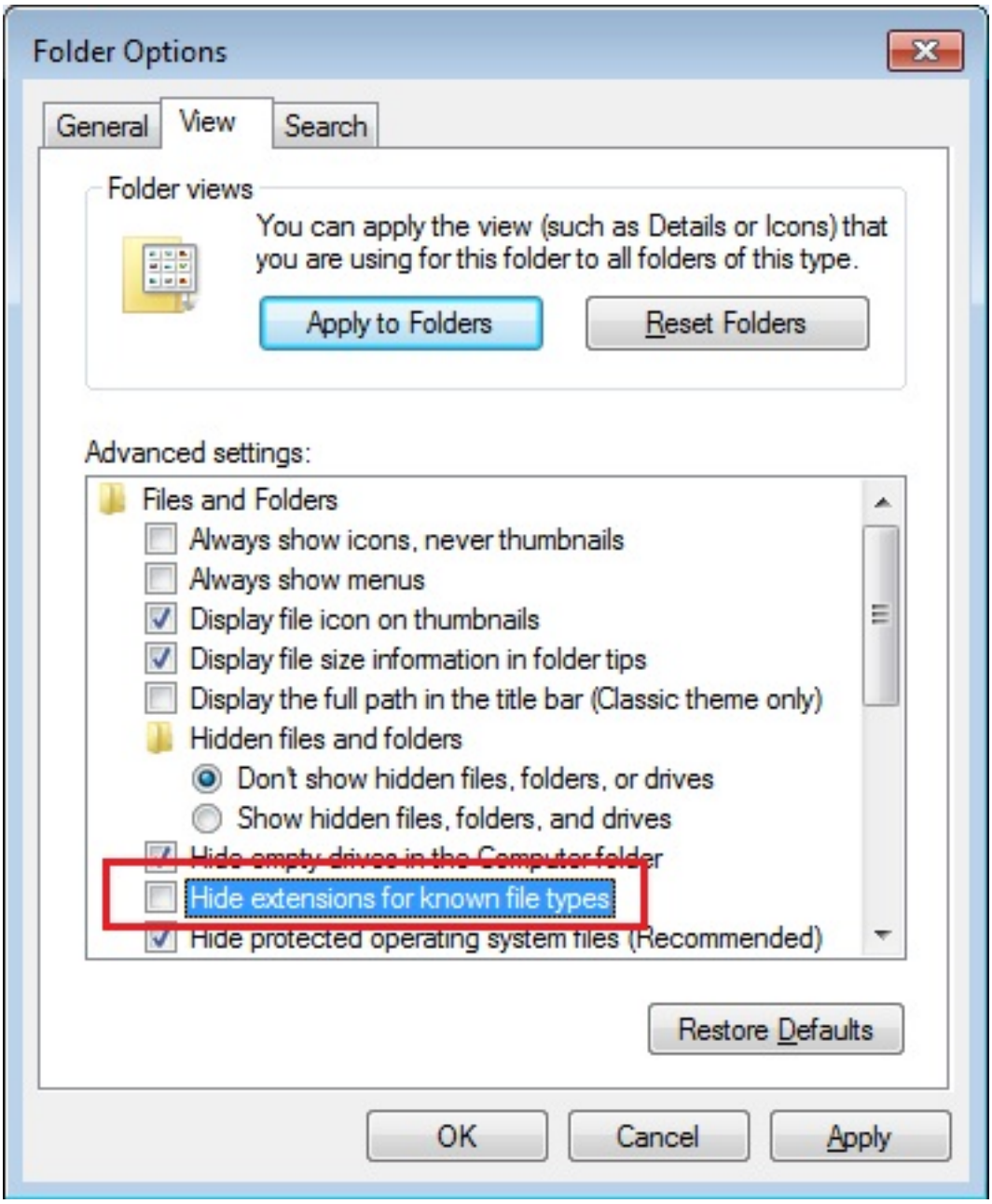
- 로그온 스크립트를 배포하고 여러 로그온 스크립트 시나리오를 만드는 방법.
- 세션 내에서 클라이언트 또는 서버 측에서 특정 폴더를 마운트합니다.

사용자에게 논리적 가상 드라이브에 폴더를 게시하려면 이 절차를 따르십시오:

스크립트를 만들기 전에 Windows 탐색기를 열고 "폴더 및 검색 옵션"을 클릭하십시오.



그런 다음 보기 탭을 클릭하고 "알려진 유형에 대한 확장자 숨기기" 상자의 선택을 해제하십시오.

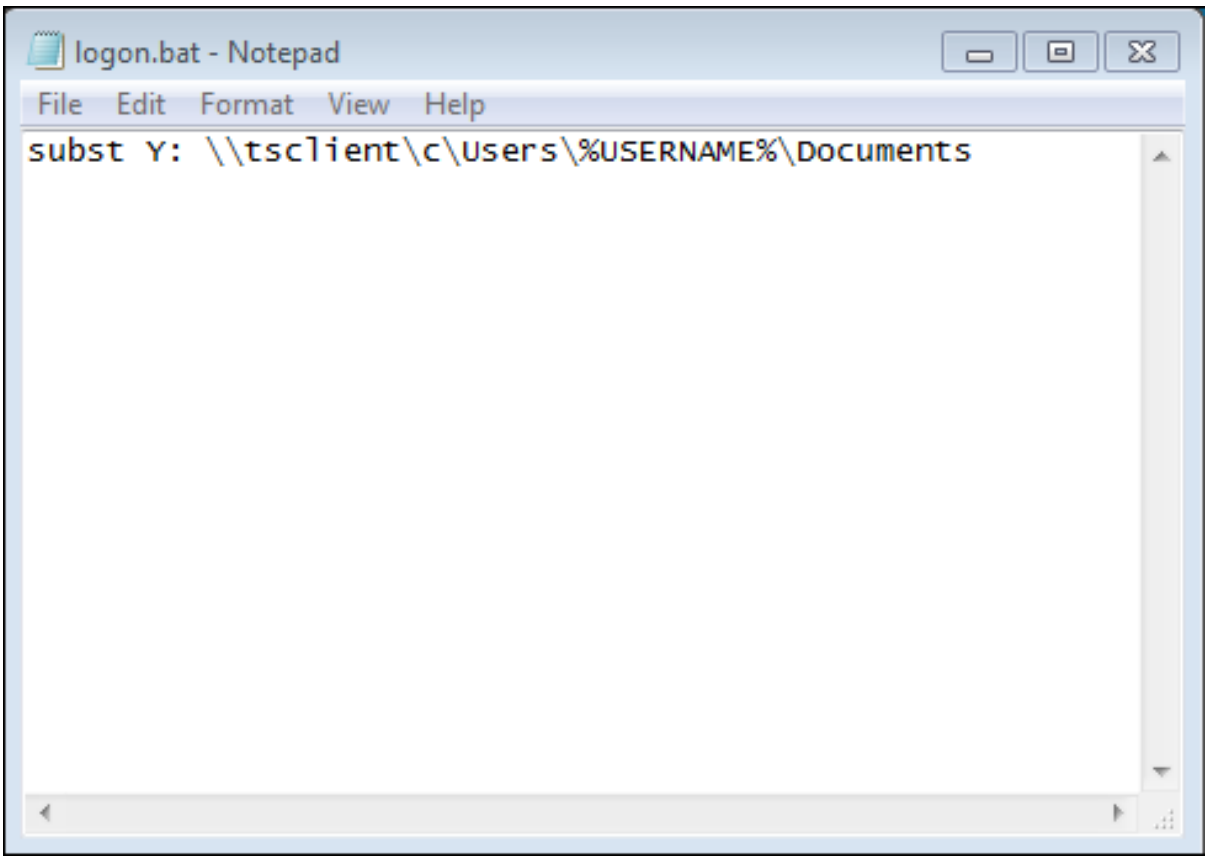


텍스트 문서를 만들고 확장자를 “logon.bat”로 변경합니다.



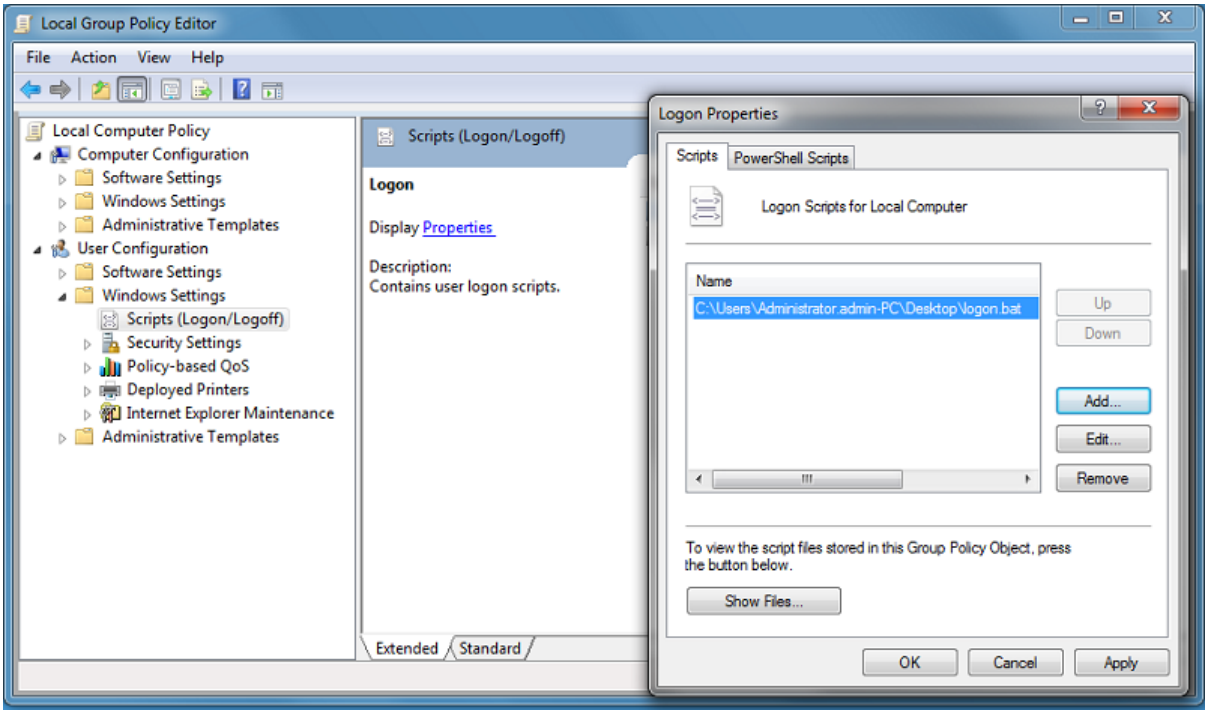
파일 내에서 예를 들어 이 명령을 입력하여 Folder.exe 폴더를 게시하십시오:

“subst Y: \tsclient\C\Users%USERNAME%\Documents”

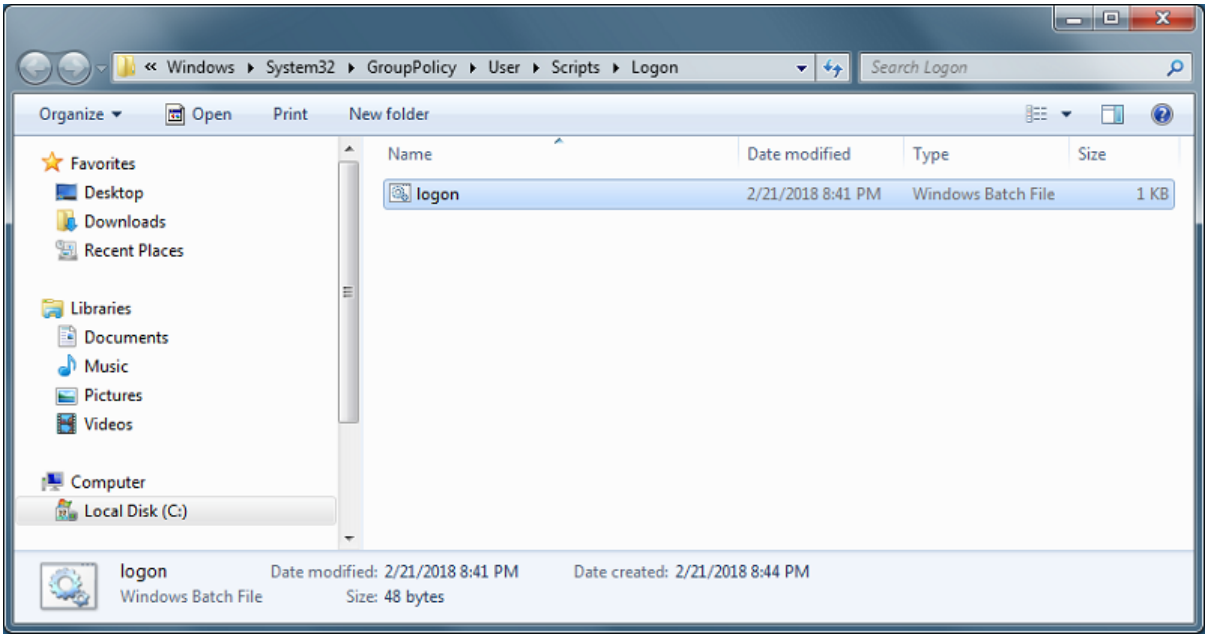


그런 다음 시작 메뉴에서 검색 작업 표시줄에 gpedit.msc를 입력합니다. 우리는 이 서버에 연결하는 모든 사용자가 스크립트를 실행하도록 로컬 정책을 사용할 것입니다.

사용자의 구성 메뉴로 들어간 다음 Windows 설정으로 이동하고 마지막으로 스크립트(로그온/로그오프)로 들어갑니다. 로그온 스크립트를 두 번 클릭한 다음 "추가"를 클릭하고 "찾아보기"를 클릭합니다.

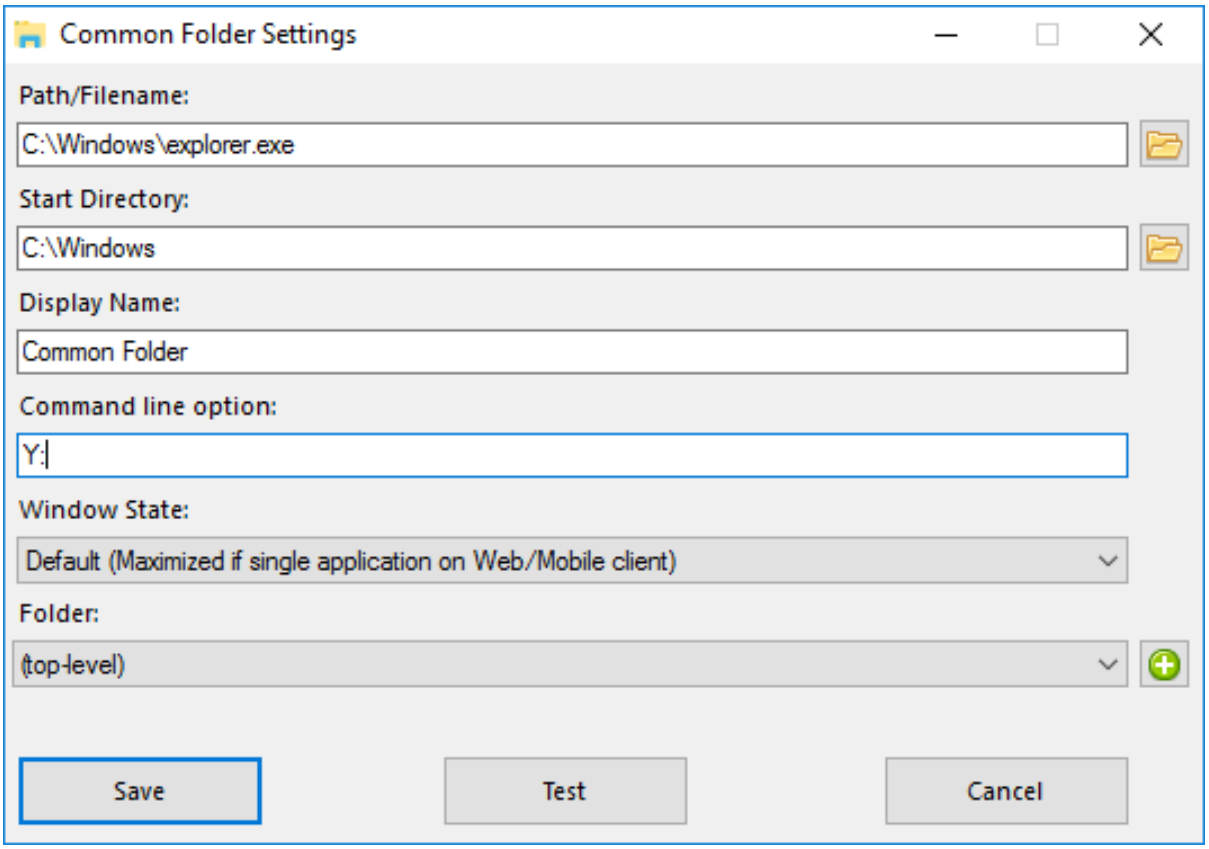


그런 다음 Logon Properties 창에서 "Show Files" 버튼을 클릭하고 logon.bat 스크립트를 정책 편집기에서 제공하는 경로인 "C:\Windows\System32\GroupPolicy\User\Scripts\Logon"에 복사합니다.



- 이 스크립트가 모든 사용자에게 실행되도록 하려면 C:\ProgramData에 이 logon.bat 파일을 복사할 수 있습니다.
- 각 사용자에 대해 특정 로그인 스크립트가 필요하면 C:\Users\Username\AppData\Roaming에 스크립트를 복사하십시오.

이 Y 드라이브를 사용자 세션에 어떻게 나타나게 할 수 있나요? 이를 달성하는 방법은 여러 가지가 있습니다. 관리 도구 내에서 새 응용 프로그램을 생성하고 이를 사용자에게 할당하면 바로 가기가 세션에 나타납니다.


Common Folder Settings
Path/Filename:
C:\Windows\explorer.exe
Start Directory:
C:\Windows
Display Name:
Common Folder
Command line option:
Y:
Window State:
Default (Maximized if single application on Web/Mobile client)
Folder:
(top-level)
Save
Test
Cancel


CommonFolder

mstsc.exe로 세션에 연결하는 경우 옵션 메뉴로 이동하는 것을 잊지 마세요. 로컬 리소스 탭에서 로컬 장치 및 리소스 아래의 "더보기"를 클릭한 다음 "드라이브" 체크박스를 선택하세요.

비관리자 사용자에게만 이 스크립트를 할당하려면 다음을 따르십시오. 튜토리얼 .

폴더의 접근을 보호하려면, 게시하는 방법에 대한 문서를 참조하세요. 보안 폴더 .

로그온 티켓 및 로드 밸런싱

게이트웨이 서버에서 로그온 티켓 생성

게이트웨이에서 로그인 티켓을 생성할 수 있습니다:

/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

하지만 게이트웨이 서버 자체에만 연결할 수 있습니다.

응용 프로그램 서버에서 로그인 티켓 생성

리버스 프록시화된 애플리케이션 서버에서 로그인 티켓을 생성할 수도 있습니다:

/srv4/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

(~~srv4가 TSplus 리버스 프록시에서 구성된 애플리케이션 서버의 내부 이름이라고 가정할 때)

하지만 이 특정 애플리케이션 서버에만 연결할 수 있습니다.

로그온 티켓 및 로드 밸런싱

로그온 티켓과 로드 밸런싱을 사용하려면 먼저 추가 HTTP 요청을 수행하는 것이 좋습니다.

https://your-gateway-server.com/cgi-bin/hb.exe?action=lb&l=LOGIN&d=DOMAIN&t=TIMESTAMP

이것은 이렇게 대답을 반환합니다:

로드밸런싱-온|앱 서버 4|your-gateway-server.com/~~srv4|https|443|

이 답변을 파싱하여 TSplus Load-Balancer가 이 특정 사용자에게 연결할 것을 권장하는 애플리케이션 서버를 검색할 수 있습니다.

즉, 부하가 덜 걸린 서버를 TSplus 팜에서 추천하며, TSplus 게이트웨이에 스티키 세션이 활성화되어 있으면 기존의 활성 세션을 고려합니다.

이 특정 애플리케이션 서버에서 로그인 티켓을 생성한 후 사용자에게 연결할 수 있습니다.

이것은 TSplus 웹 포털 로그인 페이지에서 수행된 http 요청입니다.

사용자 세션을 열기 위한 로그인 티켓 사용

이제 유효한 로그인 티켓이 있으므로, 이 URL로 브라우저 창을 열어 이 티켓을 사용하여 사용자 세션을 열 수 있습니다:

https://your-gateway-server.com/~~srv4/software/html5.html?user=*xxxxxxxx

“xxxxxxxx”은 로그인 티켓입니다.

장기 지원 버전

TSplus 지원 및 업데이트 서비스에 가입했지만 TSplus의 최신 기능 및 개선 사항에 관심이 없는 고객은 TSplus LTS(장기 지원) 버전을 설치할 수 있습니다.

TSplus LTS (장기 지원) 버전은 소프트웨어 유지 관리 기간을 연장하며, 소프트웨어 배포의 위험, 비용 및 중단을 줄이기 위해 소프트웨어 업데이트 빈도를 줄입니다. 또한 소프트웨어의 신뢰성을 높입니다.

또한, TSplus LTS(장기 지원)는 새로운 기능을 받지 않습니다.

TSplus 생애 주기

TSplus 표준 버전은 꽤 자주 출시되며 최신 릴리스는 항상 고객에게 제공되는 최상의 솔루션입니다: 모든 알려진 버그가 수정되고 새로운 기능이 매우 자주 제공됩니다.

매년 초에 새로운 주요 TSplus 버전이 출시됩니다.

2019년 1월부터 TSplus는 “LTS”라는 이름의 장기 지원 버전으로도 제공됩니다. 모든 새로운 주요 버전에서 TSplus는 이전 버전의 안정적인 LTS 버전을 게시하며, 이 버전은 2년 동안 지원됩니다.

TSplus LTS의 장점과 한계

TSplus LTS는 여러 가지 이점이 있습니다:

- 보안 수정 및 Windows 업데이트 호환성 외에는 업데이트가 없습니다.
- 업데이트할 때 동작이나 기능에 변화가 없습니다.
- 주어진 LTS의 두 개의 마이너 버전 간 업데이트 시 위험 감소
- 최소 2년 이상 지원됨

TSplus LTS에도 한계와 제약이 있습니다:

- 고객은 지원 및 업데이트 서비스(활성 지원 및 업데이트 서비스 없이는 라이센스를 활성화할 수 없음)를 구매해야 합니다.
- 전혀 새로운 기능이 없습니다 (지속적으로 많은 업데이트와 새로운 기능을 받는 TSplus 표준 버전과 비교할 때).

고객님께서는 최첨단 솔루션의 혜택을 누리기 위해 TSplus 표준 버전을 사용하시기를 권장합니다.

TSplus LTS 링크

TSplus LTS 18 (2026-01부터 2028-01까지 지원됨:)

- 변경 로그
- 설정 새 서버에 TSplus를 설치하려면
- 업데이트 릴리스 기존 TSplus 설치를 업데이트하려면
- LTS18 문서

TSplus LTS 17 2025-01부터 2027-01까지 지원됨:

- 변경 로그
- 설정 새 서버에 TSplus를 설치하려면
- 업데이트 릴리스 기존 TSplus 설치를 업데이트하려면
- LTS17 문서

TSplus LTS 16 (2024-01부터 2026-01까지 지원): **지원 종료**

TSplus LTS 15 (2023년 1월부터 2025년 1월까지 지원): **지원 종료**

TSplus LTS 14 (2021-12부터 2023-12까지 지원됨): **지원 종료**

TSplus LTS 12 (2019-12부터 2022-12까지 지원됨): **지원 종료**

TSplus LTS 11 (2018-12부터 2021-12까지 지원됨): **지원 종료**

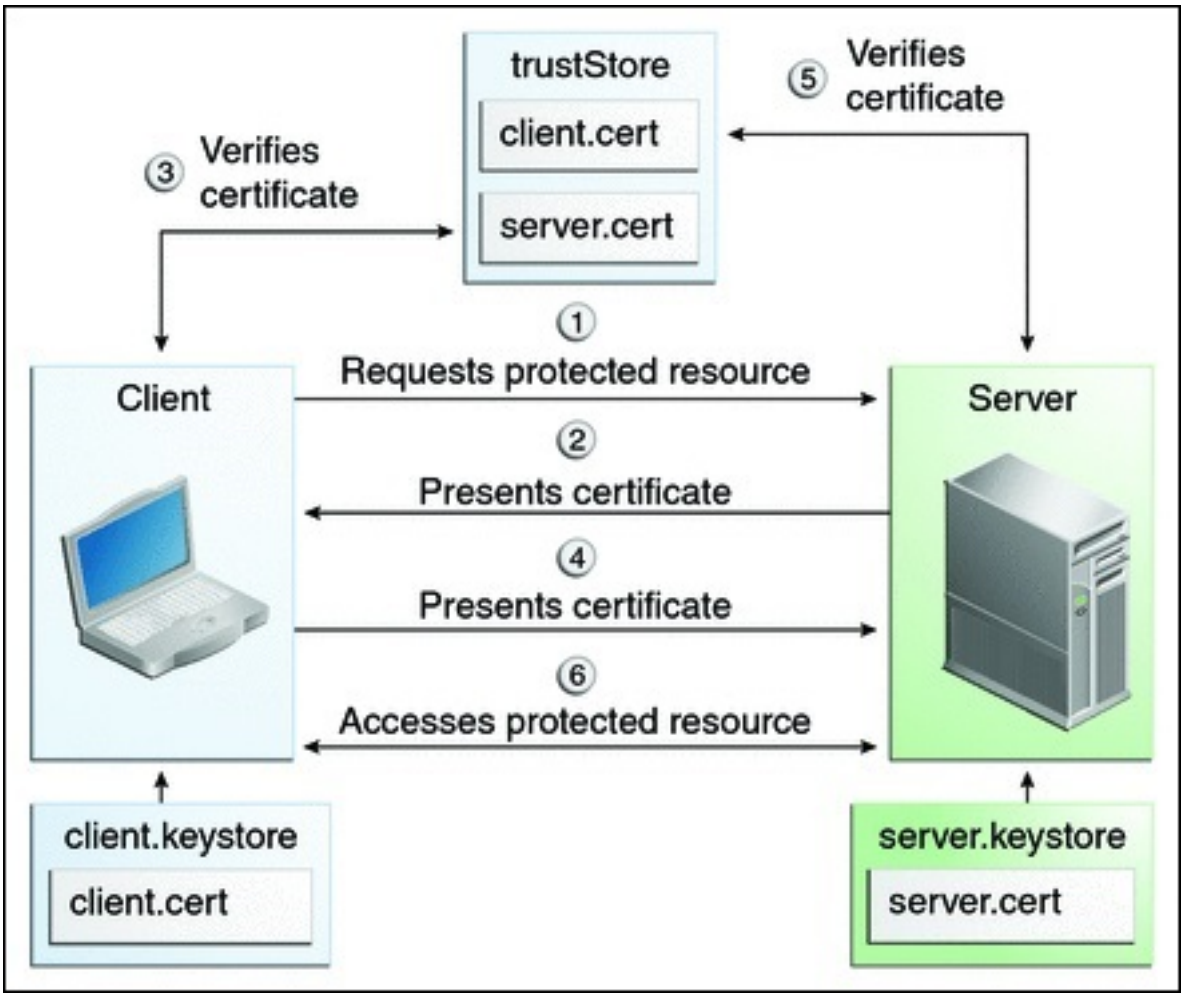
상호 SSL 인증 활성화

상호 인증이란 무엇인가요?

많은 사람들이 추가 보안을 기대하고 있으며 상호 인증은 이미 Terminal Service Plus에서 지원됩니다. 일반적으로 은행이나 정부 기관에서 구현됩니다.

그것이 무엇인지 이해하기 위해, 우리는 표준 SSL 프로세스와 비교할 수 있습니다. 여기서 사용자의 웹 브라우저가 SSL 연결을 허용하는지 확인하기 위해 추가 검사를 추가합니다. 서버 측 SSL 인증서가 무엇인지 알고 있습니다. 이 인증서가 웹 브라우저에 가져와져서 이 특정 웹 브라우저가 연결을 생성하는 데 신뢰할 수 있도록 한다고 상상해 보십시오. 통신의 첫 번째 단계에서 웹 브라우저는 클라이언트 역할을 하고 두 번째 단계에서는 그 반대입니다. 결국 클라이언트 웹 브라우저와 웹 서버 양쪽 모두 권한을 수락하고 연결을 시작할 수 있습니다.

보다 완전한 정의: 상호 SSL 인증 또는 인증서 기반 상호 인증은 두 당사자가 제공된 디지털 인증서를 검증하여 서로를 인증하는 것을 의미하며, 이를 통해 양 당사자는 서로의 신원을 확신할 수 있습니다. 기술 용어로는 클라이언트(웹 브라우저 또는 클라이언트 애플리케이션)가 서버(웹사이트 또는 서버 애플리케이션)에 자신을 인증하고, 그 서버 또한 신뢰할 수 있는 인증 기관(CA)에서 발급한 공개 키 인증서/디지털 인증서를 검증하여 클라이언트에게 자신을 인증하는 것을 의미합니다. 인증이 디지털 인증서에 의존하기 때문에 Verisign 또는 Microsoft Certificate Server와 같은 인증 기관은 상호 인증 프로세스의 중요한 부분입니다.



TSplus에서 활성화하기

TSplus 내장 웹 서버는 상호 인증을 설정할 수 있게 해줍니다.

상호 인증을 활성화하려면 이 프로세스를 따르십시오:

최신 Java Development Kit (JDK)를 설치해야 합니다. 이는 다음에서 사용할 수 있습니다. http://java.com > 다운로드 > JDK.

1. 다음 파일을 Notepad로 생성하고 편집하십시오: C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin

이 3줄을 추가하세요:

disable_http_only=true disable_print_polling=true force_mutual_auth_on_https=true

2. cert.jks 제거

"C:\Program Files (x86)\TSplus\Clients\webserver"에서 cert.jks 파일을 볼 수 있습니다. 이를 "C:\Program Files (x86)\TSplus\Clients"에 복사하십시오. "C:\Program Files (x86)\TSplus\Clients\webserver\cert.jks"를 제거하십시오.

3. 배치 파일 만들기

‘C:\Program Files (x86)\TSplus\Clients’에 배치 파일을 생성합니다. 예를 들어 “createcertuser.bat”와 같은 설정으로 생성합니다.

@rem 다음 줄의 주석을 제거하면 새로 self signed cert.jks를 생성할 수 있습니다. @rem keytool -genkey -v -alias jwts -keyalg RSA -validity 3650 -keystore cert.jks -storepass secret -keypass secret -dname “CN=localhost, OU=my_ou, O=my_org, L=my_city, ST=my_state, C=MY” @keytool -genkey -v -alias AliasUser1 -keyalg RSA -storetype PKCS12 -keystore forBrowserUser1.p12 -dname “CN=some_name, OU=some_ou, O=some_org, L=Paris, ST=FR, C=FR” -storepass mypassword -keypass mypassword @keytool -export -alias AliasUser1 -keystore forBrowserUser1.p12 -storetype PKCS12 -storepass mypassword -rfc -file forCertUser1.cer @keytool -alias AliasCertUser2 -import -v -file forCertUser1.cer -keystore cert.jks -storepass secret @del forCertUser1.cer

이 작업은 브라우저의 키 쌍을 생성한 후 웹 브라우저에서 "cert.jks"로 인증서 키 쌍을 자동으로 가져옵니다.

4. 새로 생성된 수정된 “cert.jks”를 복원합니다.

“C:\Program Files (x86)\TSplus\Clients\cert.jks”를 “C:\Program Files (x86)\TSplus\Clients\webserver”로 복사한 후 웹 서버를 재시작하십시오.

5. 인증서 가져오기 및 테스트

제공된 배치 예제는 테스트 파일 “BrowserUser1.p12”를 생성했어야 합니다. HTTPS 주소를 열면 보안 메시지가 표시되고 웹 서버 페이지에 접근할 수 없습니다. Chrome 또는 IE를 사용하면 이 ‘BrowserUser1.p12’ 파일을 클릭하여 Windows 기본 키 저장소에 인증서를 가져올 수 있습니다. FireFox를 사용하면 설정으로 가서 인증서 폴더 아래에 이 “BrowserUser1.p12” 파일을 가져와야 합니다.

올바르게 가져오면 HTTPS 주소에 접근할 수 있습니다.

관리자는 각 사용자에 대해 별도의 키 쌍 파일을 생성할 수 있습니다.

예를 들어:

forBrowserUser1.p12 forBrowserUser2.p12 forBrowserUser3.p12

그는 이 인증서를 cert.jks로 내보낼 수 있습니다. 한 사용자의 접근을 비활성화하려면 "cert.jks"에서 이 사용자를 삭제하기만 하면 됩니다. 그렇게 하면 사용자는 권한을 잃게 되고 더 이상 웹 서버에 접근할 수 없습니다.

이 상호 인증은 HTTPS 연결에만 영향을 미치며, HTTP 연결은 명령줄로 금지됩니다: settings.bin>disable_http_only=true

클라이언트 측에서 파일 열기

개요

이 기능은 강력한 기능입니다. 파일 확장자에 따라 클라이언트 측에서 서버에 위치한 문서를 열 수 있습니다.

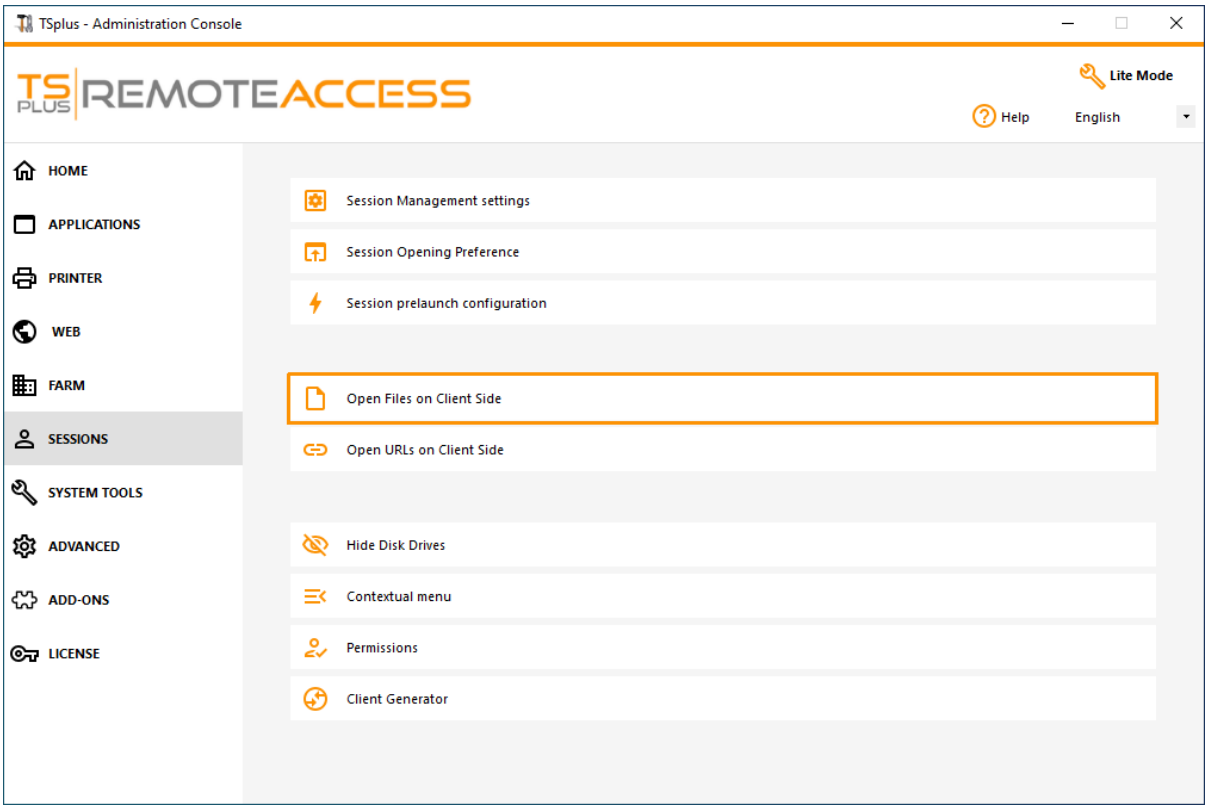
예를 들어, 서버에 Office가 설치되어 있지 않아도 Microsoft Office Word 문서를 열 수 있습니다.

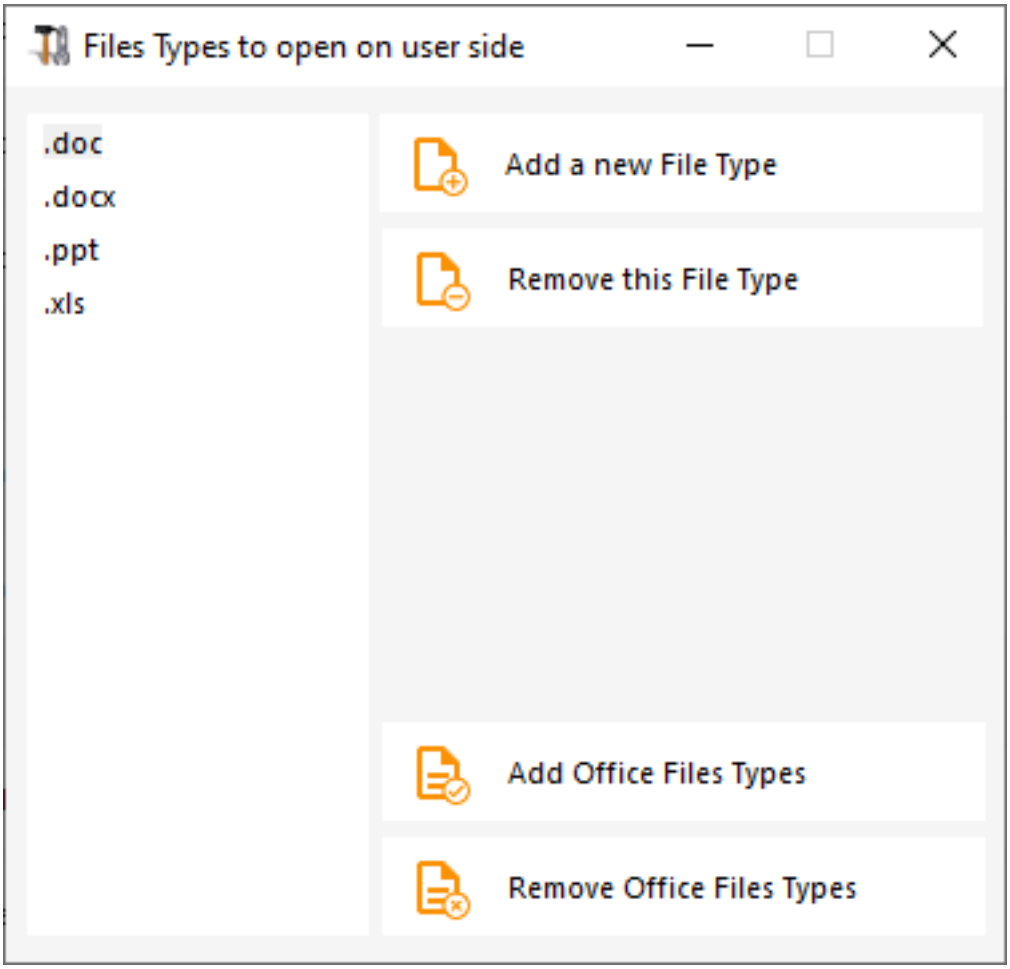
사용자 측에서 .docx (또는 .xlsx) 문서가 자동으로 업로드되며, 로컬 Office를 사용하여 열립니다.

클라우드 서버에서 애플리케이션을 호스팅하고 애플리케이션이 Excel, Access 또는 Word 문서를 생성하는 경우, 이 기능은 서버에서 Office 라이센스에 대해 걱정할 필요가 없도록 합니다.

클라이언트 측에서 열 파일 유형 구성하기

클라이언트 측에서 파일 열기라는 항목은 AdminTool의 세션 - 설정 탭에 있습니다. 클릭하면 구성 창이 표시됩니다.





“새 파일 형식 추가” 버튼을 사용하면 목록에 확장자(예: Microsoft Office Word 2007-2010의

“.docx”)를 추가할 수 있습니다.

이 목록에 있는 확장자를 가진 모든 파일은 클라이언트 측에서 열립니다. Terminal Service Plus 연결 클라이언트 중 하나를 사용하여:

- 생성된 Terminal Service Plus 클라이언트(원격 앱 또는 RDP)
- Terminal Service Plus 웹 포털에서의 모든 Windows 연결
- Terminal Service Plus 웹 포털의 모든 HTML5 연결

경고: 이 기능은 다음에 대해 지원되지 않습니다:

- 모든 RDP 클라이언트(예: mstsc)

문제 해결

클라이언트 측에서 열도록 파일 유형을 구성했지만 작동하지 않는 경우(즉, 파일이 여전히 자신의 컴퓨터에서 열리는 경우) Windows 컨텍스트 메뉴의 "다음으로 열기" 목록을 확인할 것을 권장합니다.

- 파일을 마우스 오른쪽 버튼으로 클릭하십시오.
- “열기” 메뉴 항목을 클릭하십시오.
- 이 목록에 여러 응용 프로그램이 있는 경우 "기본 프로그램 선택"을 클릭하고 "OpenOnClient.exe"를 선택하십시오.

이 Terminal Service Plus 훌륭한 도구는 컴퓨터를 사용하는 모든 사용자에게 구성 적용을 하지만, 다음 규칙을 염두에 두시기 바랍니다:

- Windows는 각 사용자가 이 기본 열기 프로그램을 원하는 다른 프로그램으로 변경할 수 있도록 허용합니다.
- HTML5 연결 클라이언트를 사용하면 파일이 로컬 브라우저에 의해 다운로드되고 관리됩니다. 일부 브라우저는 특정 방식으로 일부 파일 유형을 처리하므로 브라우저의 설정도 두 번 확인해야 합니다.

이 규칙은 Open On Client 기능을 사용할 때 발생하는 대부분의 문제를 설명합니다. 따라서 기본 프로그램을 확인하는 것부터 시작할 것을 권장합니다.

- 서버에 로그인한 사용자용
- 클라이언트의 사용자용
- 클라이언트의 브라우저용 (HTML5 사용 시)

클라이언트 측에서 URL 열기

개요

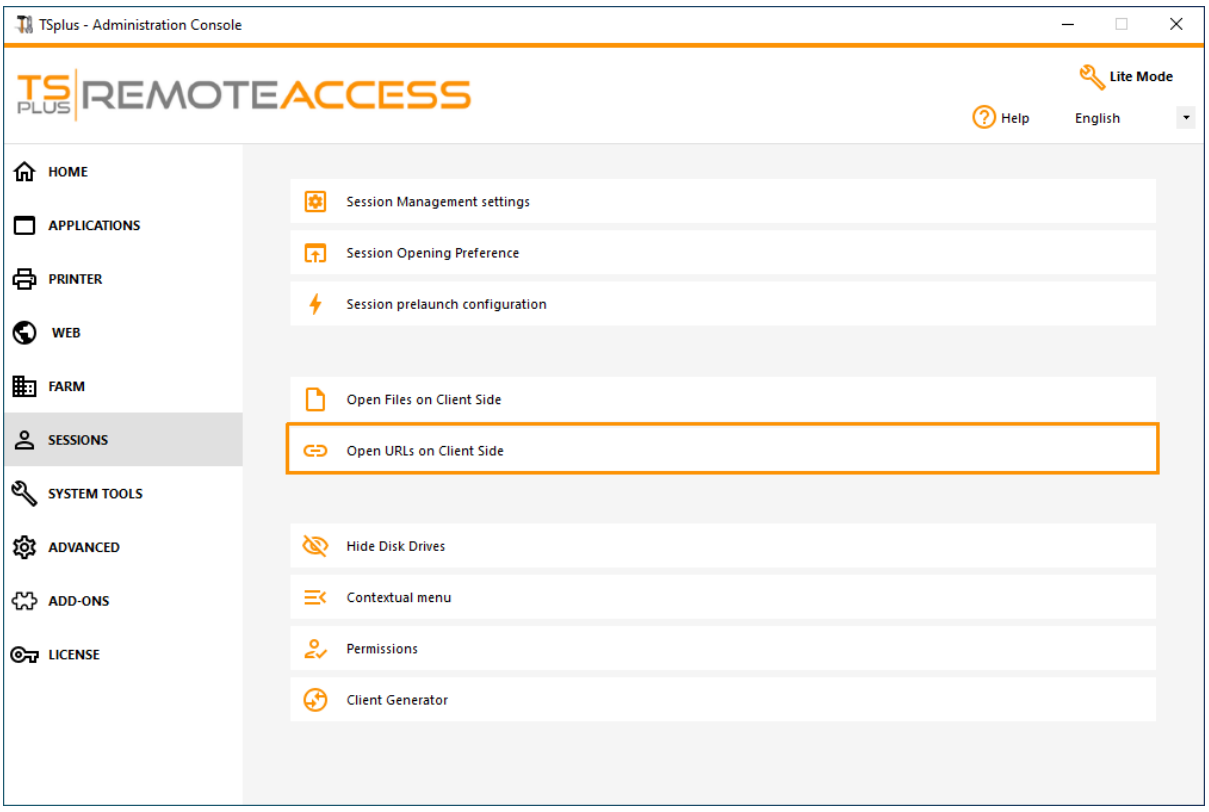
이 기능은 강력합니다. 클라이언트 측에서 서버에 위치한 모든 웹사이트 링크와 웹사이트 바로가기를 열 수 있습니다.

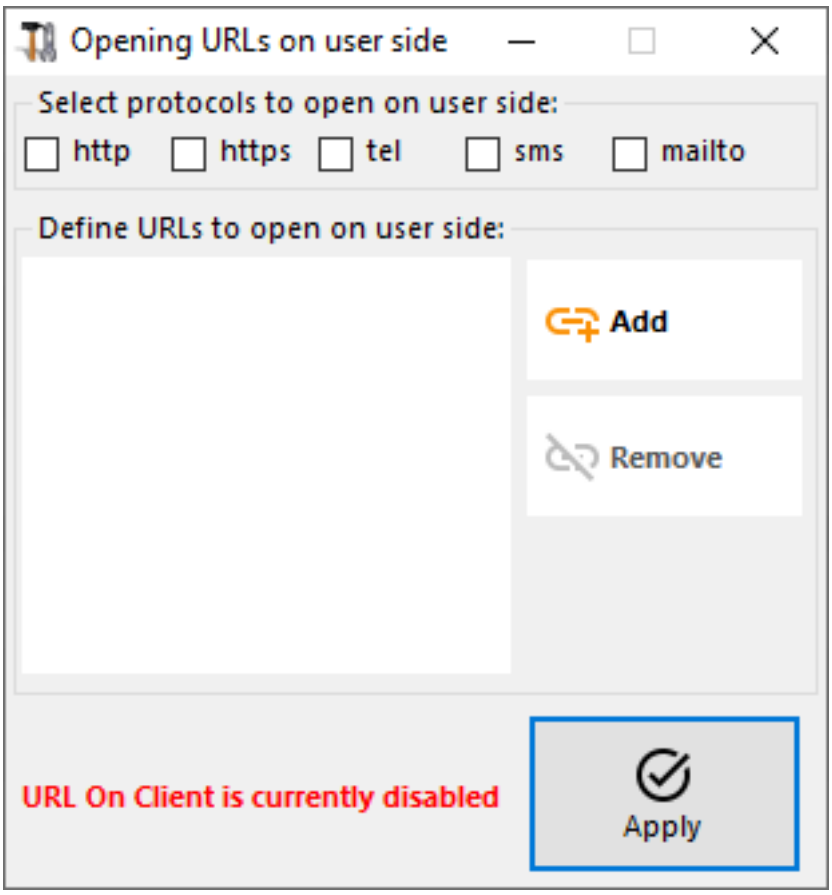
예를 들어, 클라이언트에서 YouTube 비디오를 직접 열 수 있으므로 서버의 대역폭과 CPU 전력을 많이 절약할 수 있습니다.

웹 주소(URL)는 자동으로 사용자 측으로 전송되며, 여기서 로컬 기본 브라우저가 사용되어 열립니다.

이 기능을 서버에서 활성화하기

“클라이언트 측에서 URL 열기” 타일은 AdminTool의 “세션 - 설정” 탭에 위치해 있습니다. 클릭하면 구성 창이 표시됩니다.





Http 및 https 프로토콜 상자는 기본적으로 선택되어 있지 않습니다.
해당 상자를 선택하여 tel, sms 및 mailto 프로토콜을 활성화할 수 있습니다.

그런 다음 "적용" 버튼을 클릭하여 이 기능을 서버의 모든 사용자에게 활성화할 수 있습니다.

이 기능을 완전히 활성화하려면 모든 사용자가 이 기능을 사용하기 전에 세션을 재시작해야 합니다(로그오프한 후 로그인).

모든 웹 링크와 단축키는 클라이언트 측에서 열립니다. Terminal Service Plus 연결 클라이언트 중 하나를 사용하여:

- 생성된 Terminal Service Plus 클라이언트(원격 앱 또는 RDP)
- Terminal Service Plus 웹 포털에서의 모든 Windows 연결
- Terminal Service Plus 웹 포털의 모든 HTML5 연결.

경고: 이 기능은 다음에 대해 지원되지 않습니다:

- 모든 RDP 클라이언트(예: mstsc).

웹 브라우저 동작 (웹 포털):

일부 웹 브라우저 —특히 iOS 장치에서— 우리 애플리케이션에서 링크가 자동으로 열리는 것을 허용하지 않습니다. 이러한 경우 클릭 가능한 링크가 표시되어 사용자가 수동으로 원하는 목적지에 접근할 수 있습니다.



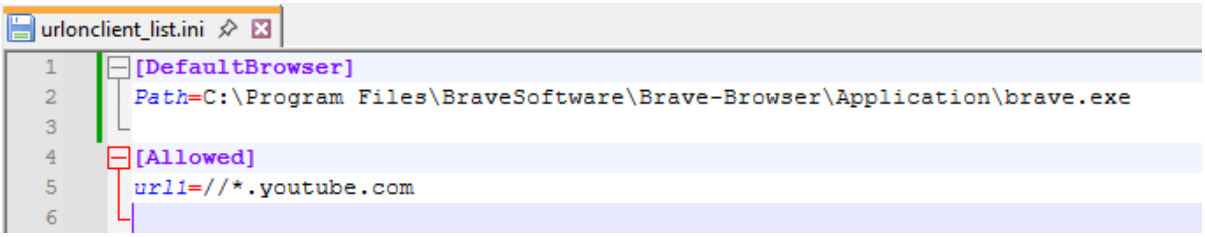
서버 기본 웹 브라우저 변경

클라이언트 측에서 열도록 정의되지 않은 모든 URL는 Microsoft Edge 또는 Internet Explorer를 사용하여 서버 측에서 계속 열립니다. 서버 측에서 사용되는 기본 웹 브라우저를 변경하려면 구성 파일을 편집해야 합니다. **urlonclient_list.ini** TSPlus 설치 폴더에 위치합니다.

정확한 위치(정확한 설치 경로에 따라)는 다음과 같아야 합니다: C:\Program Files (x86)\TSplus\UserDesktop\files\urlonclient_list.ini .

새 섹션 "DefaultBrowser"를 파일에 추가하고, 원하는 웹 브라우저의 경로 값을 가진 "Path" 항목을 추가해야 합니다. 이렇게:

[DefaultBrowser]
Path=C:\Path\To\Your\Favorite\WebBrowser.exe



기본 브라우저를 Brave로 설정하기

☐ **c:\wsession\URLonClient.exe로 firefox.exe를 교체한 경우**

서버 측에서 Firefox를 기본 웹 브라우저로 설정하려면:

- old firefox.exe 파일을 firefox-real.exe로 이름 변경하세요.
- 새 실행 파일 이름을 사용하십시오. **urlonclient_list.ini** 파일 :

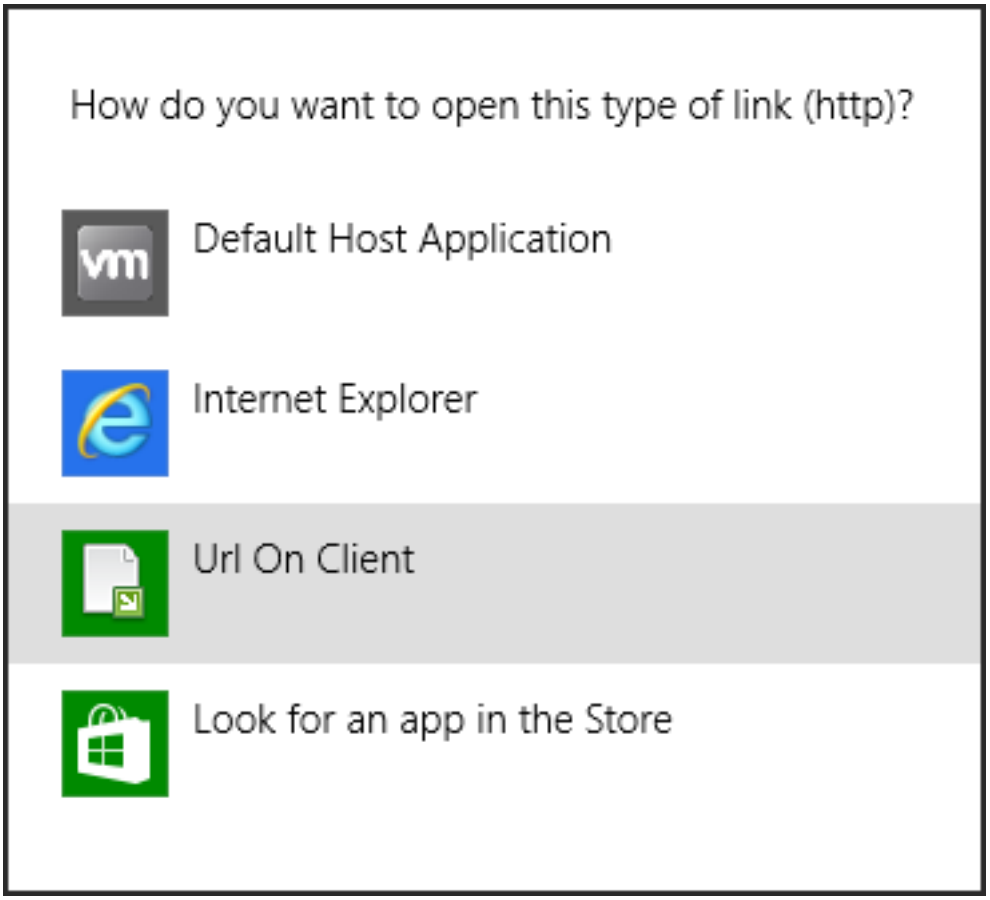
[DefaultBrowser]
Path=C:\Program Files\Mozilla Firefox\firefox-real.exe

Windows 8 및 8.1

Windows 8부터 Microsoft는 사용자의 기본 브라우저 자동 변경을 금지했습니다.

이것이 바로 기능이 서버에서 활성화되면 모든 사용자가 기본 브라우저를 요청받을 때 '클라이언

트에서 Url'을 선택해야 하는 이유입니다.



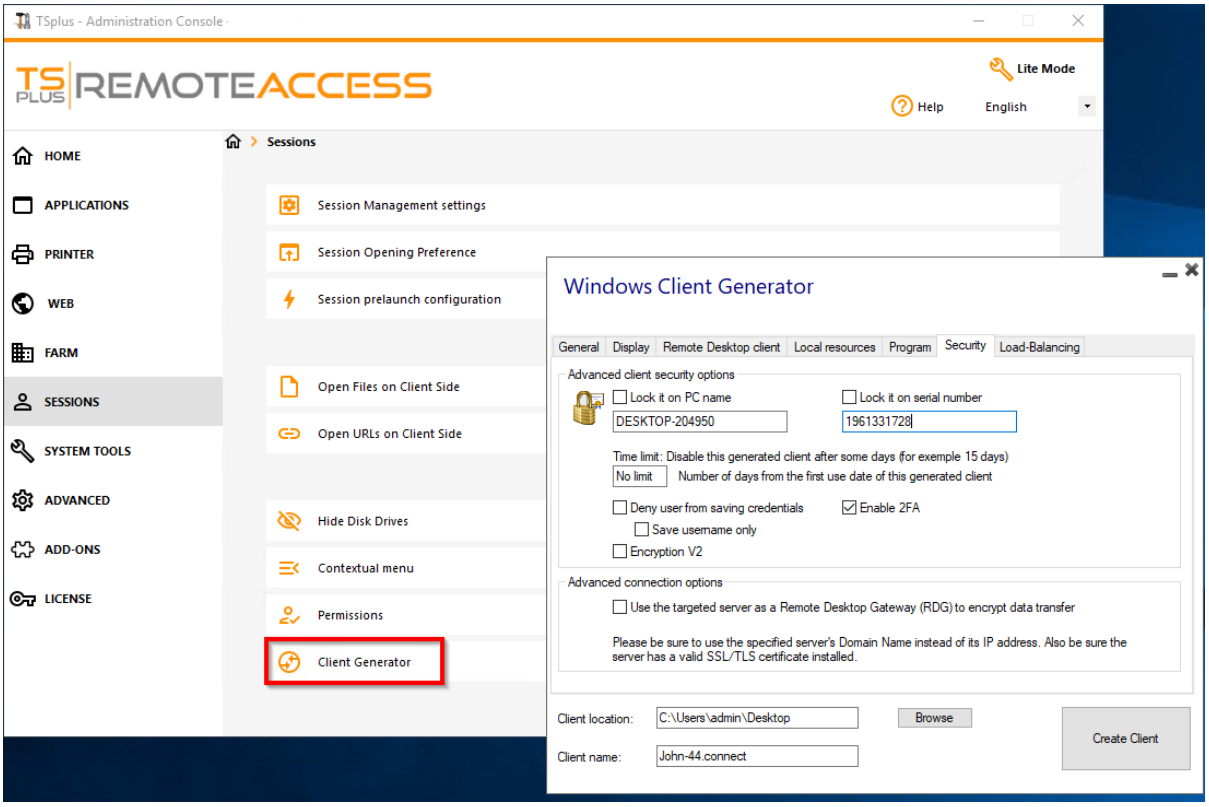
이 창은 사용자가 웹 링크를 처음 열 때만 표시됩니다. 불행히도, 이는 Microsoft Windows 정책이며 우리는 어떤 우회 방법도 알지 못합니다.

휴대용 클라이언트 생성기

TSplus는 기본적으로 Portable Client Generator에 대한 아이콘을 생성합니다.



관리 도구의 세션 탭에서도 접근할 수 있습니다.



사용자가 데스크탑이나 USB 메모리에 복사하여 휴대용으로 사용할 수 있는 2종류의 연결 클라이

언트를 생성할 수 있습니다.

노트 연결 클라이언트는 Mac 컴퓨터와 호환되지 않습니다.

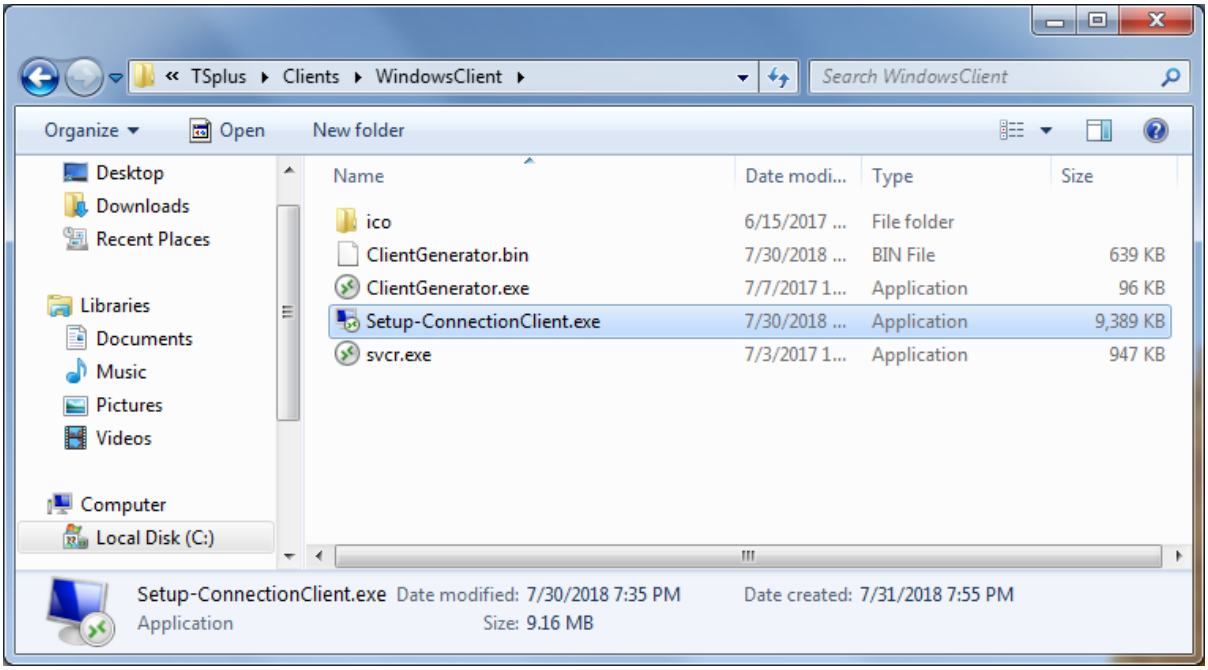
TSplus 11.40 출시 이후, 클라이언트 생성기가 숫자 서명으로 재설계되어 잘못된 양성 반응을 일으키는 안티바이러스 프로그램을 피할 수 있게 되었습니다.

대신 “.exe” 프로그램 대신 새로운 클라이언트 생성기는 “.connect” 확장자를 가진 평면 암호화 파일을 생성하고 있습니다.

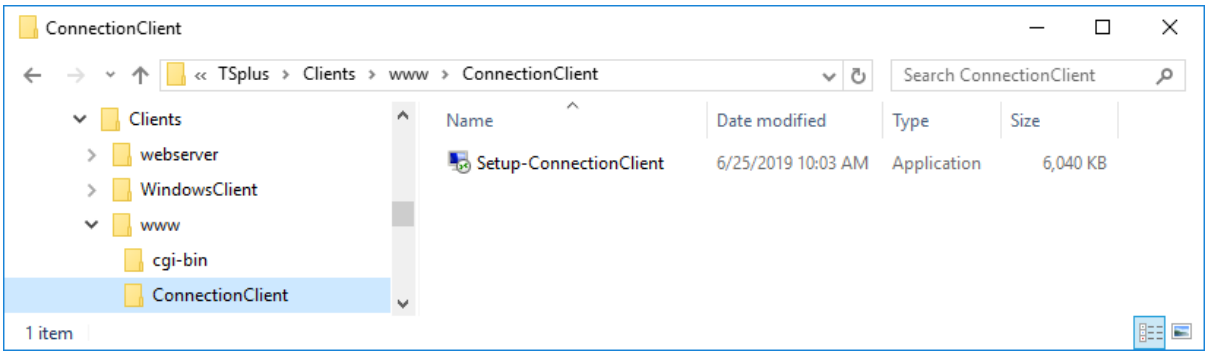


클라이언트 측의 전제 조건

클라이언트 측에서 각 사용자는 필수 조건으로 “Setup-ConnectionClient.exe”라는 서명된 프로그램을 실행해야 합니다. 이 프로그램은 귀하의 서버의 TSplus 프로그램 폴더에 있습니다: TSplus\Clients\WindowsClient:



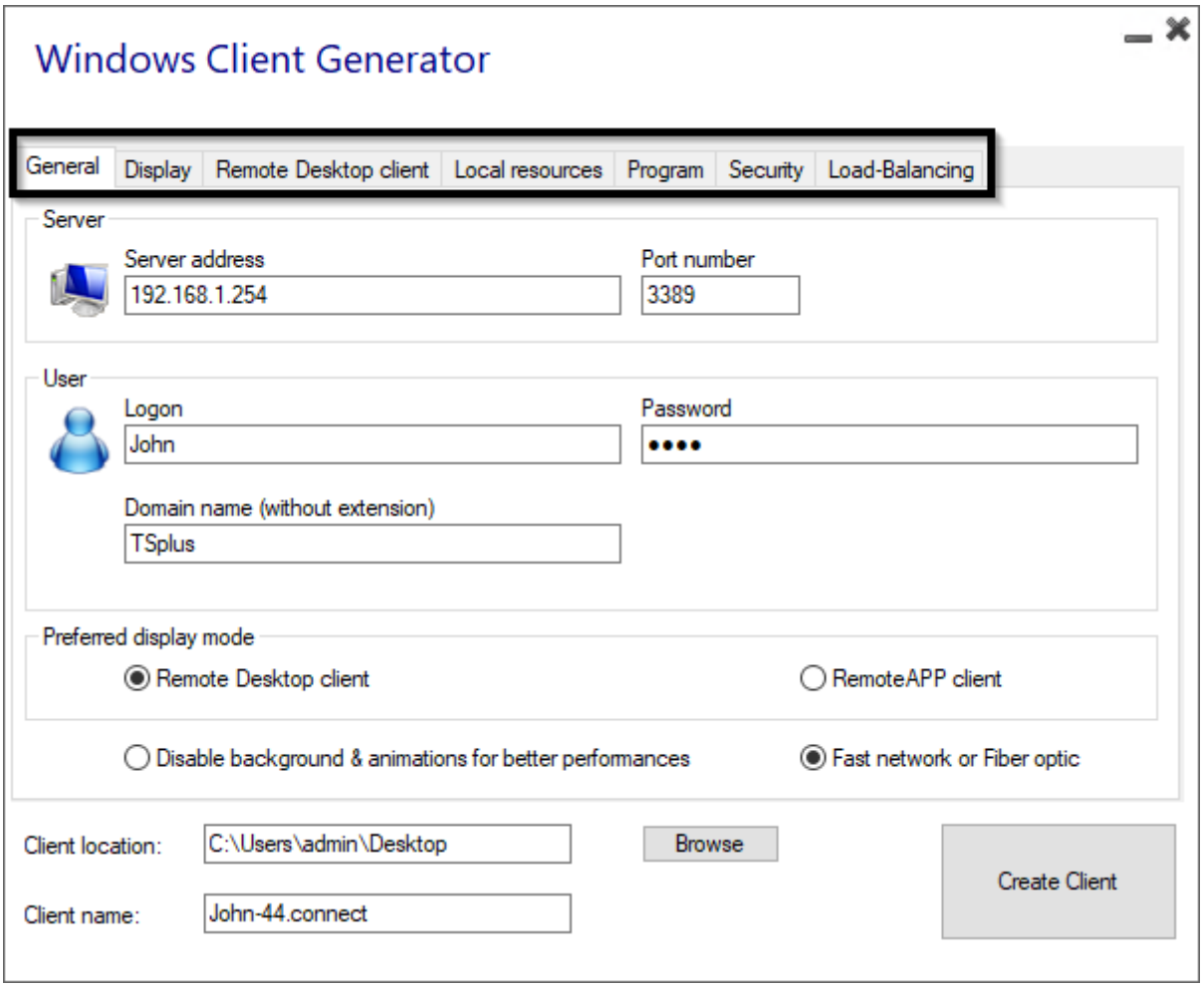
또는 TSplus\Clients\www 폴더에서:



또는 다운로드 중입니다 .

상세 개요

클릭하세요 **탭** 해당 정보로 이동하려면:



클라이언트 생성기를 실행하면 첫 번째로 표시되는 탭은 일반 탭입니다. 여기에서 시작하는 데 필요한 모든 필수 연결 설정을 찾을 수 있습니다.

- **서버 주소:** 클라이언트가 연결할 서버의 IP 주소를 입력하세요.
- **포트 번호:** 서버 포트 번호를 입력하세요. 기본값은 3389입니다.
- **사용자 이름 및 비밀번호:** 사용자 이름과 비밀번호를 입력하면 클라이언트 프로그램이 각 세션마다 사용자가 다시 입력하도록 요청하지 않습니다.

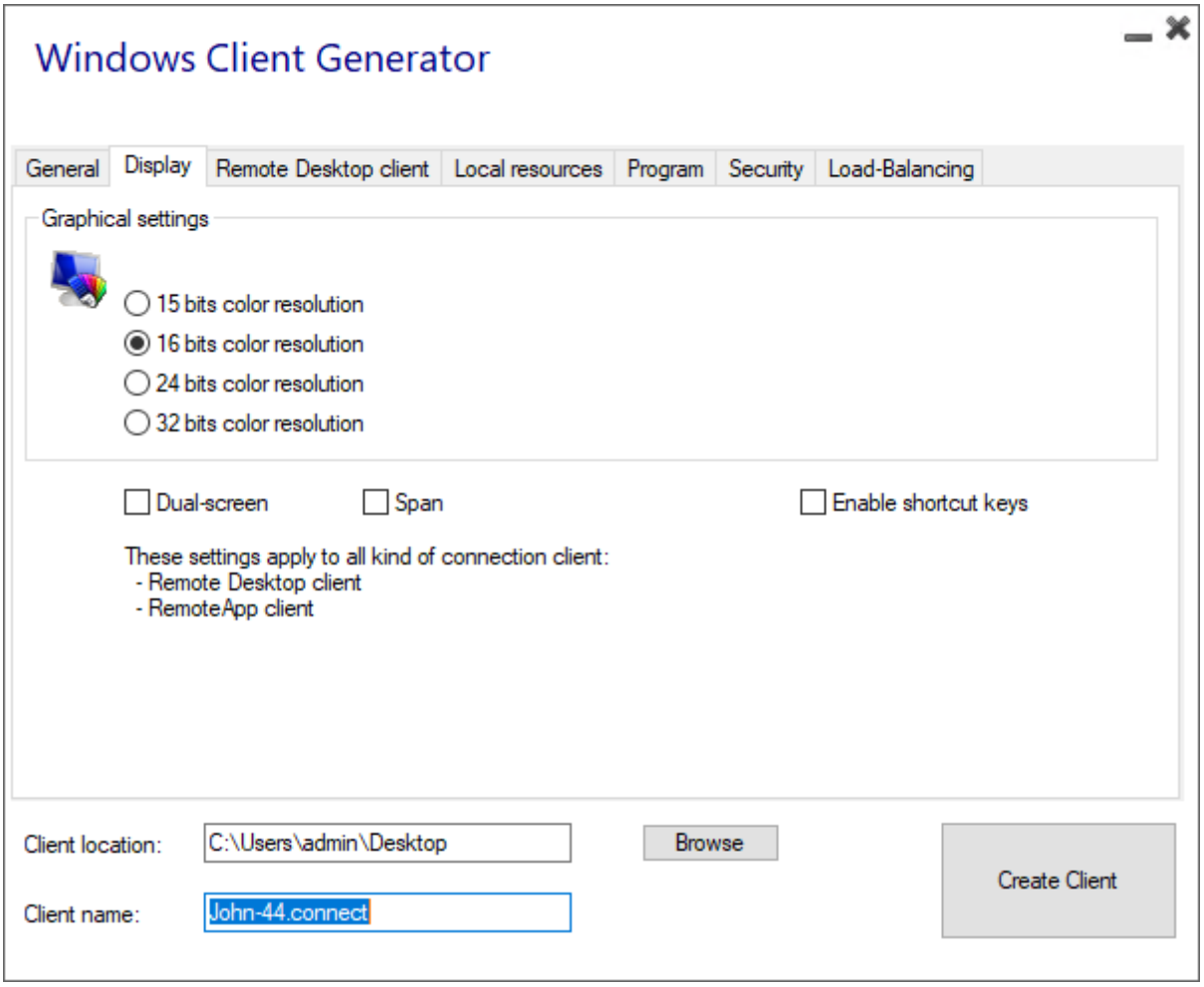
이 로그온/비밀번호 저장을 재설정하려면 Remote Desktop Client의 바로 가기를 생성하고 편집한 후 추가해야 합니다. -재설정 켜기 대상 필드의 끝에서 전환합니다.

자격 증명

- 자격 증명을 저장하고 싶지 않다면 Portable Client Generator의 로그인 필드에 "nosavecredential"을 입력하세요.
- 사용자 이름, 비밀번호 및 도메인 이름이 있는 로그인 창을 표시하고 싶지 않다면, 비밀번호 필드에 "nopassword"를 입력하면 됩니다.
- 자동 로그인을 활성화하려면 사용자 이름 필드에 *SSO를 입력하세요. 클라이언트 프로그램은 첫 번째 연결 시 사용자 이름과 비밀번호만 요청합니다. 이 정보는 사용자의 워크스테이션에 저장되어 사용자가 다시는 본인을 확인할 필요가 없습니다.
- 세션의 로그온으로 현재 로컬 사용자 이름을 표시하려면 로그온 필드에 ** 또는 %USERNAME%을 입력하십시오.

- **도메인 이름:** 도메인 이름이 있으면 입력하세요.
- **선호하는 표시 모드:** 다음 옵션 중에서 선호하는 디스플레이 모드를 선택할 수 있습니다:
  - 그 클래식 원격 데스크톱 원격 세션 환경을 표시합니다.
  - 그 마이크로소프트 RemoteApp 연결 클라이언트 원격 애플리케이션을 로컬에 설치된 것처럼 표시합니다. 최소화된 애플리케이션에 비해 더 나은 그래픽 성능을 제공합니다.

- **네트워크 속도** 네트워크 속도에 따라 두 가지 옵션 중에서 선택할 수 있습니다.
  - 저속 네트워크에 대한 배경 표시 및 그래픽 애니메이션 비활성화.
  - 광섬유 또는 빠른 네트워크에 대한 배경 디스플레이 및 그래픽 애니메이션을 활성화합니다.
- **클라이언트 위치:** 생성된 클라이언트의 위치를 정의하십시오.
- **클라이언트 이름:** 고객의 이름을 원하는 대로 지정할 수 있습니다.

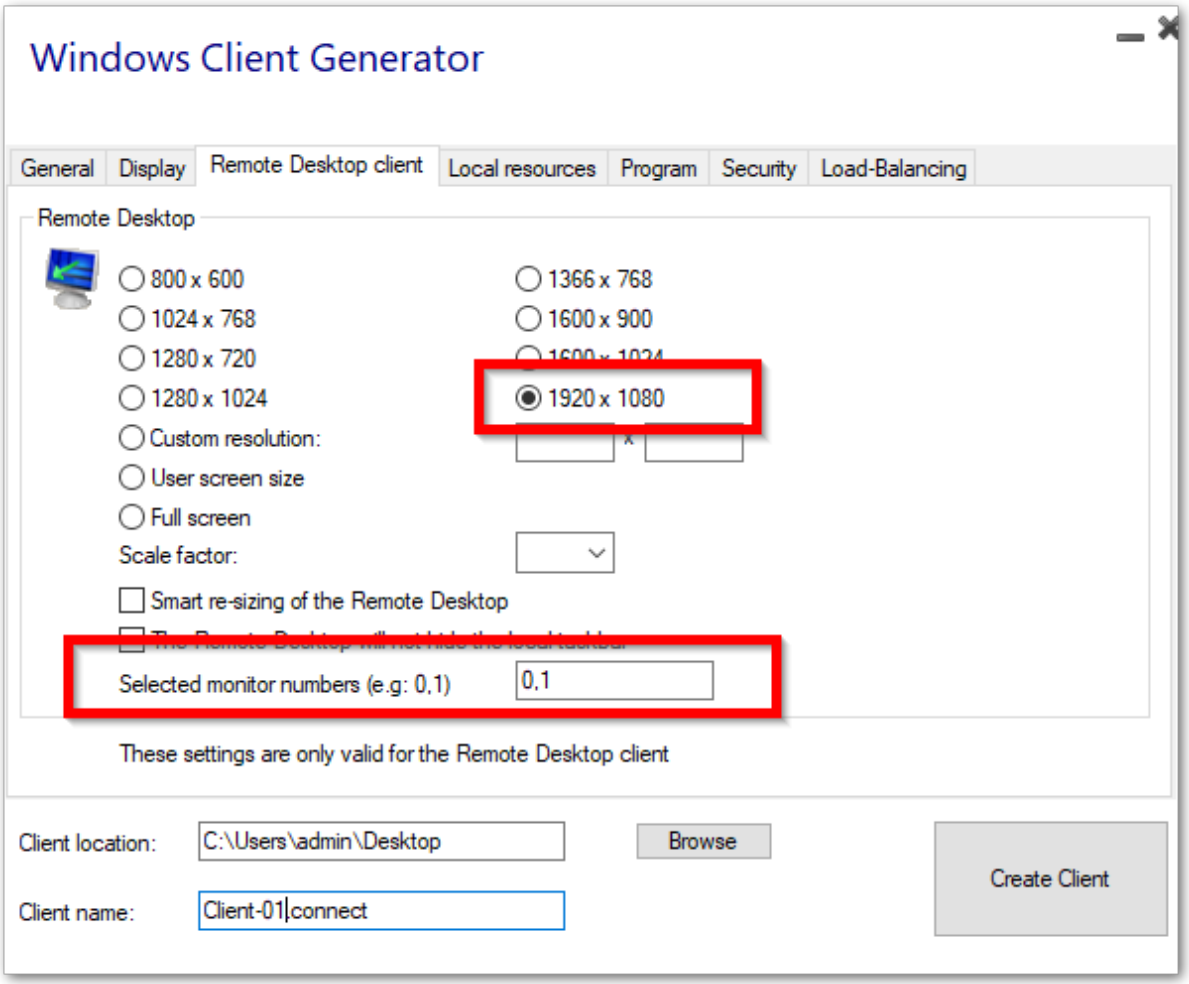


이 탭에서는 색상과 세션 화면 해상도를 변경할 수 있습니다.

세션을 듀얼 스크린에 맞게 조정할 수 있으며, 스팬 유무에 따라 가능합니다. 스팬 옵션을 사용하면 세션을 두 화면에 걸쳐 확장할 수 있습니다.

세션에서 TAB 키의 사용을 허용할 수 있습니다.

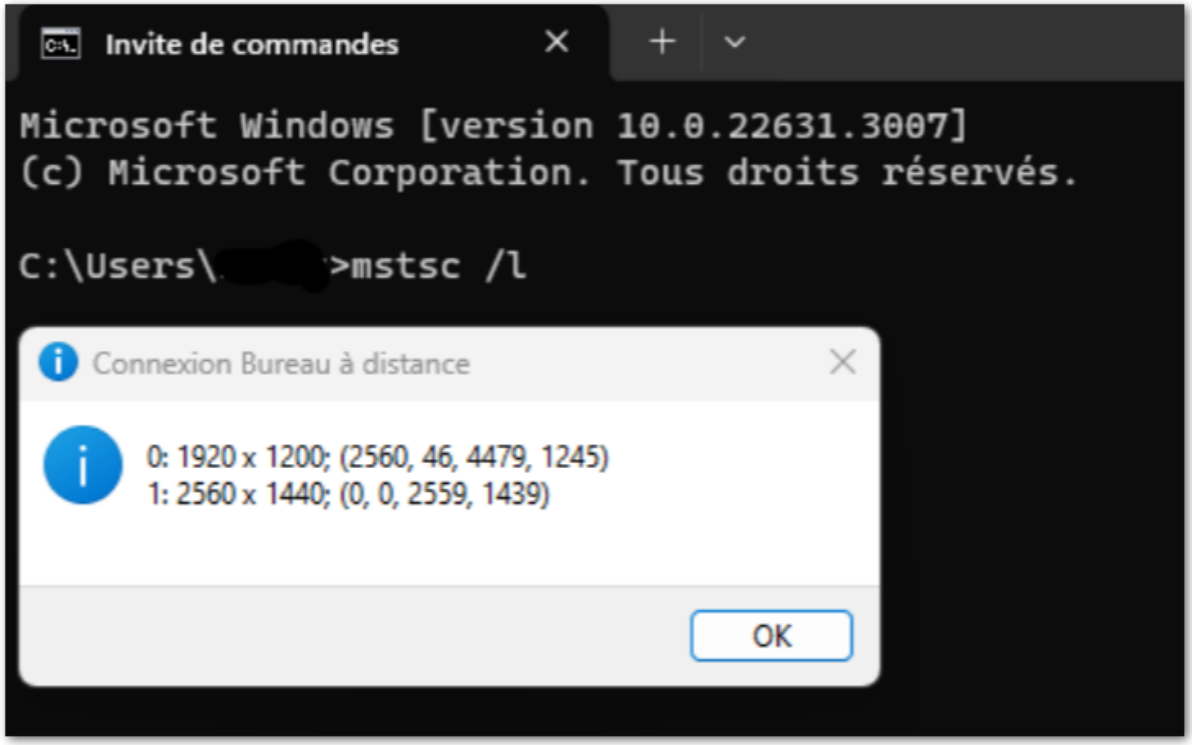
이 탭에서 사용자가 활성화할 해상도를 선택할 수 있습니다:



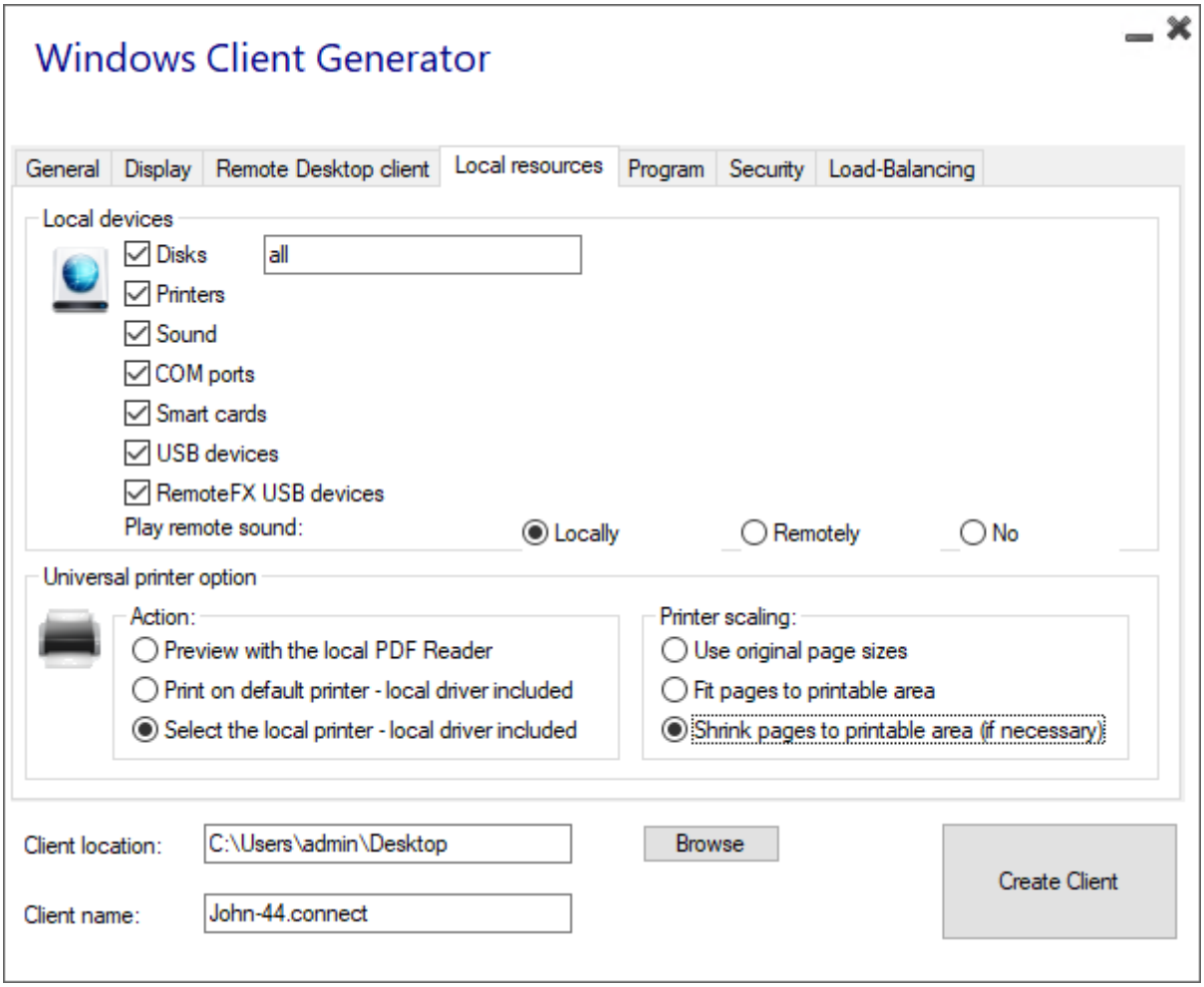
원격 데스크톱의 스마트 크기 조정을 활성화하려면 상자를 선택할 수 있으며, 원격 데스크톱이 로컬 작업 표시줄을 숨기거나 겹치지 않도록 하려면 원하지 않는 경우 선택할 수 있습니다.

화면 선택 옵션

이것은 RDP 세션에 사용할 모니터를 지정할 수 있게 해줍니다. 필드는 사용할 화면 번호 목록으로 채워야 합니다(쉼표, 공백 또는 세미콜론으로 구분).



화면 번호를 식별하려면 명령을 실행하기만 하면 됩니다. **mstsc /l**



로컬 리소스 탭은 원격 세션에서 리디렉션할 수 있는 모든 장치를 모읍니다.

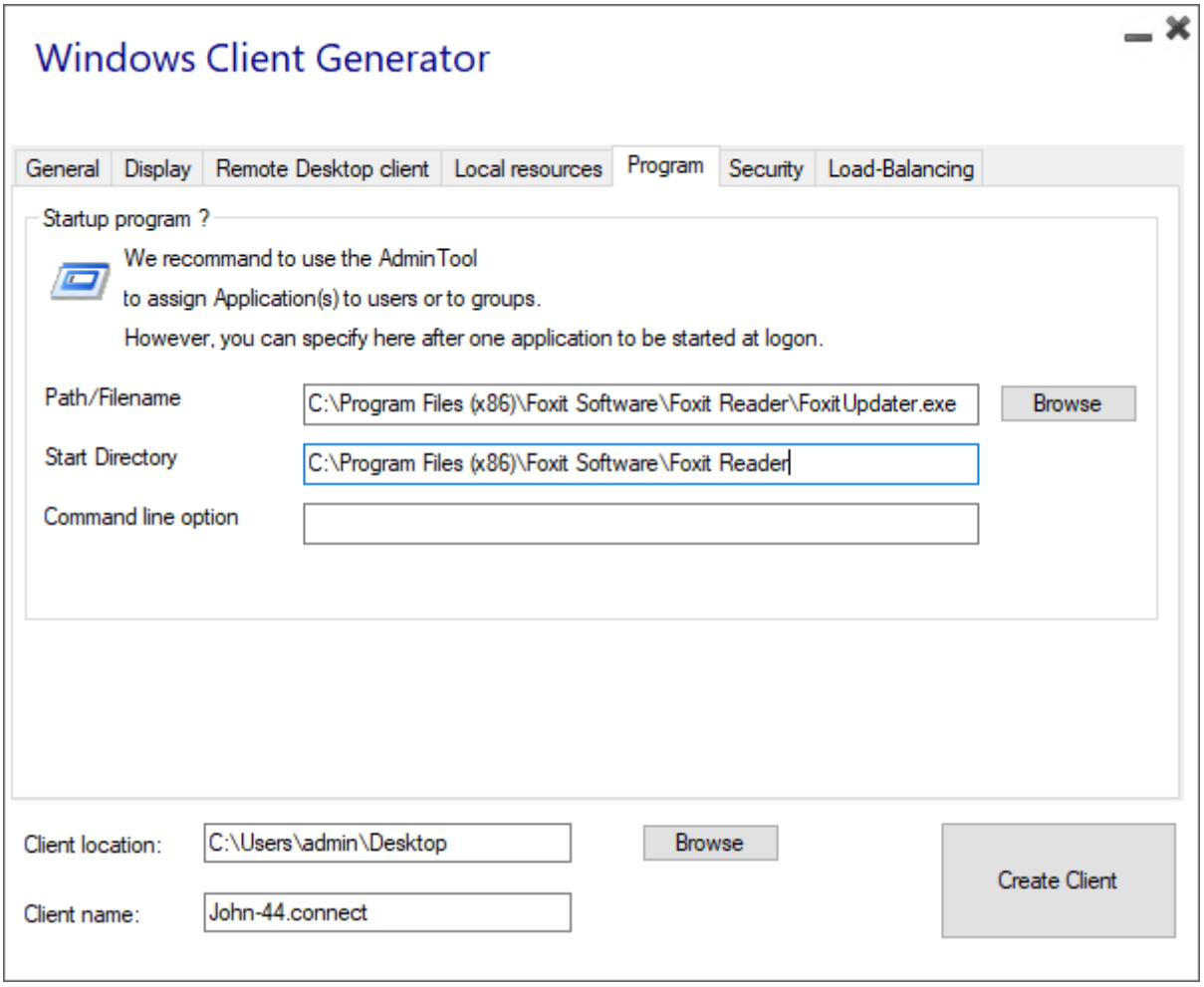
편집 가능한 필드 옆에 **디스크** 박스는 원격 세션에서 사용 가능한 디스크를 지정할 수 있습니다. 디스크의 각 문자를 쉼표로 구분하기만 하면 됩니다 (C :, E: ...). 디스크 박스가 선택되고 지정된 디스크가 없으면 모든 디스크가 원격 세션에 포함됩니다.

프린터 LPT 포트에 해당하며, COM 포트는 직렬 포트에 해당합니다. TSplus 11.50 버전부터 이러한 로컬 장치는 기본적으로 선택됩니다.

아래에서 보편적인 프린터로 인쇄할 옵션을 선택할 수 있습니다:

- **로컬 PDF 리더 미리보기:** 문서는 PDF로 변환되며 로컬 Acrobat Reader가 파일을 엽니다. 사용자는 이를 인쇄하거나 로컬 디스크 드라이브에 복사본을 저장할 수 있습니다.
- **사용자의 기본 프린터에 인쇄:** 문서는 사용자 기본 프린터(로컬 인쇄 드라이버가 TSplus 연결 클라이언트에 포함됨)로 자동으로 전송됩니다.
- **로컬 프린터 선택:** 사용자는 자신의 로컬 프린터 중 하나를 선택할 수 있습니다(로컬 인쇄 드라이버는 TSplus 연결 클라이언트에 포함되어 있습니다).

PDF 리더가 설치되어 있지 않은 경우 Foxit Reader 사용을 권장합니다.



포터블 클라이언트 생성기를 통해 시작 응용 프로그램을 설정하고 경로, 디렉터리 및 매개변수를 지정할 수 있습니다. 11.30 릴리스부터 가능합니다.

그러나 원하는 애플리케이션을 할당하기 위해 AdminTool을 사용하는 것을 권장합니다.

TSplus는 사용자의 연결을 안전하게 유지하기 위해 두 가지 추가 물리적 보안 계층을 제공합니다.

연결은 USB 키의 ID에 잠글 수 있으며, 컴퓨터 이름에 잠글 수 있거나 두 가지 보안 계층을 동시에 사용할 수 있습니다.

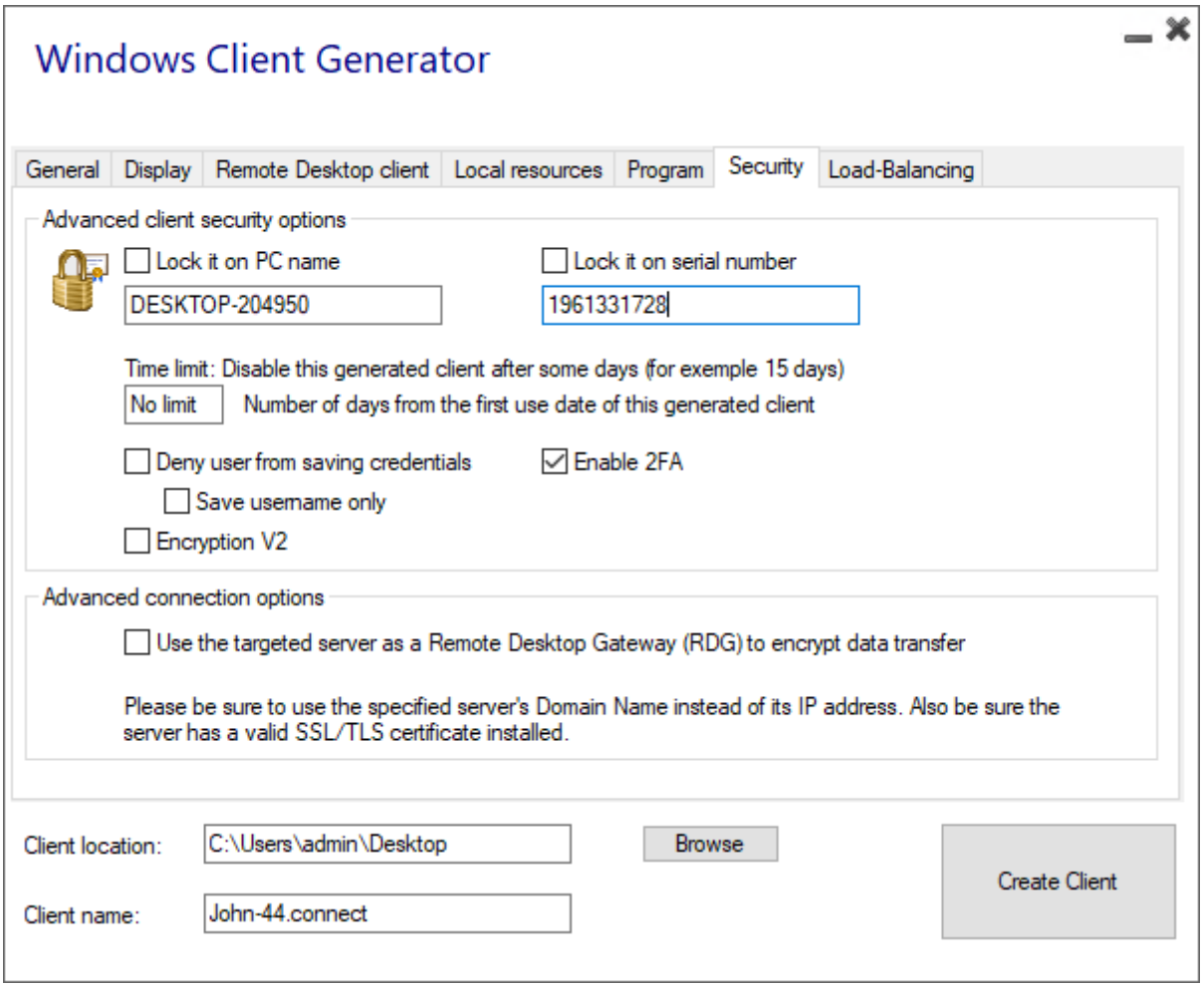
고급 클라이언트 보안 옵션

- **USB 키에 잠겨 있는 경우** 사용자는 USB 키를 삽입하고 관리자가 그곳에 배치한 연결 프로그램을 사용하여 자격을 갖춘 모든 Windows 컴퓨터에서 연결을 시작할 수 있습니다.
- **컴퓨터 이름에 잠겨 있는 경우** 사용자는 해당 사용자의 휴대용 클라이언트 연결을 위해 서버에 등록된 컴퓨터에서만 성공적으로 연결할 수 있습니다. 두 가지 보안 옵션이 모두 사용되는 경우, 사용자는 특정 장치에서만 연결할 수 있으며, 올바른 사전 구성된 USB 키가 있는 경우에만 가능합니다.

연결 클라이언트를 USB 키에 잠그려면 다음 위치에 있는 클라이언트 생성기를 복사하면 됩니다: C:\Program Files (x86)\TSplus\Clients\WindowsClient

이제 클라이언트 생성기를 두 번 클릭하고 보안 탭에 위치한 일련 번호 상자의 잠금을 확인하십시오. 완료되면 USB 키에서 클라이언트 생성기를 삭제할 수 있습니다.

새로 생성된 연결 클라이언트는 바탕 화면에 배치됩니다. USB 키로 다시 복사하는 것을 잊지 마세요! 이후 USB 키에 복사한 클라이언트 생성기는 삭제할 수 있습니다.



- 당신은 정의할 수 있습니다 **시간 제한** 생성된 클라이언트의 첫 사용 날짜부터 시간 제한 상자에 값을 입력하여. (기본적으로 "제한 없음"으로 설정됨).

- 아래의 상자들은 당신이 할 수 있는 것을 가능하게 합니다:

  - 생성된 클라이언트에 대한 자격 증명을 저장하는 기능을 표시하지 않습니다.
    - 사용자 이름만 저장합니다.
    - 암호화 V2 사용.

2단계 인증 지원

클라이언트 생성기가 지원합니다 **이중 인증** 버전 15.30.3.15부터 이중 인증 지원도 필요합니다. **모바일 웹 에디션 이상** .

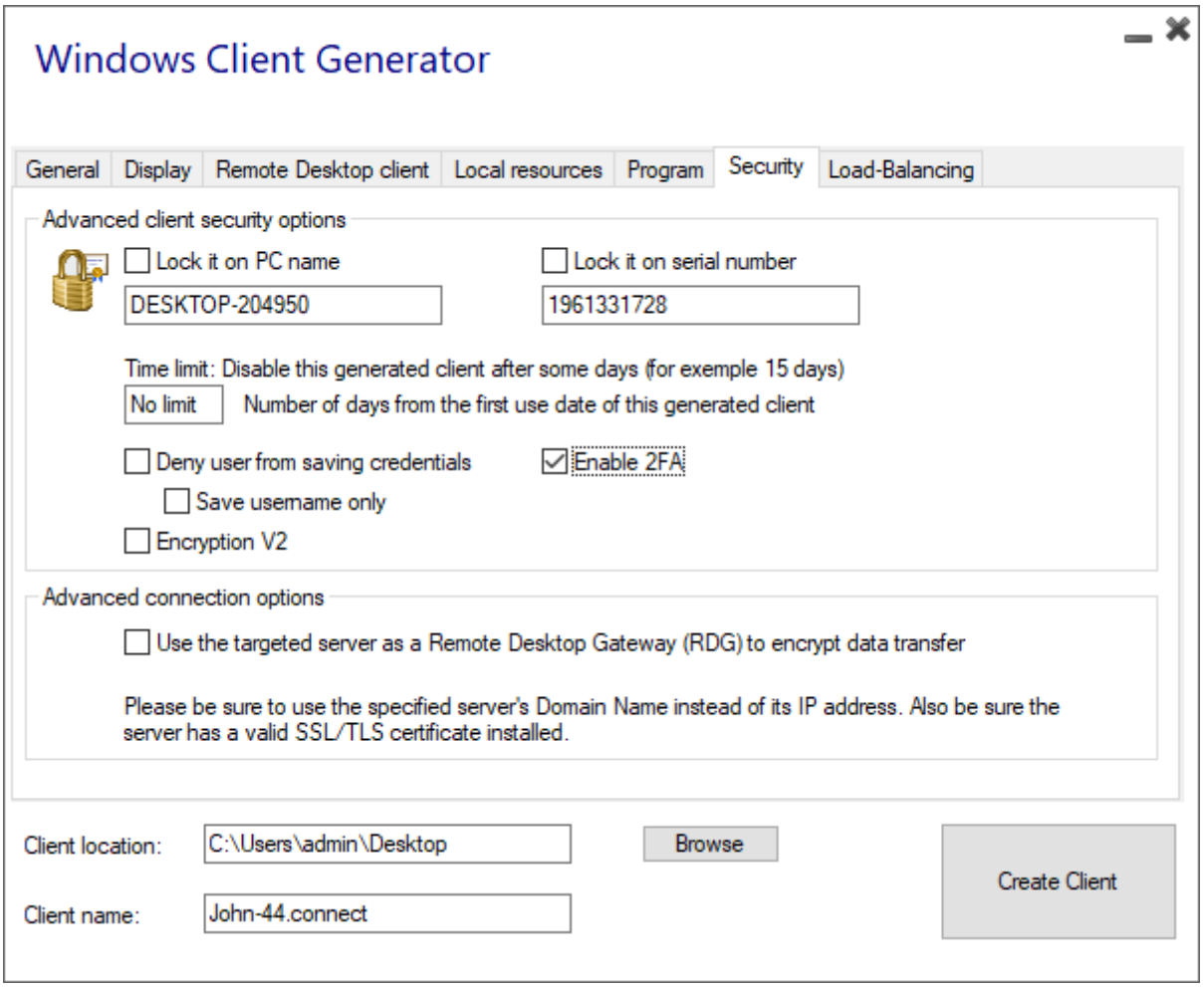
참조해 주십시오 이중 인증 문서 페이지 사용자의 TSplus Remote Access 설치에서 사용자 및 그룹에 대해 이중 인증을 구성하고 활성화하는 방법에 대한 자세한 정보는 다음을 참조하십시오.

다음 클라이언트에 대해 이중 인증을 활성화하기 위한 추가 요구 사항을 참고하시기 바랍니다:

- 연결 클라이언트는 HTTPS 포트를 사용하여 웹 포털에 대해 인증 코드를 검증합니다. 따라서, **웹 포털은 정상적으로 작동해야 합니다.** 클라이언트 머신의 HTTPS 포트를 통해 접근할 수 있습니다.
- 웹 포털의 HTTPS 포트가 수정되면, 이중 인증이 활성화된 클라이언트를 다시 생성해야 합니다. 이전에 생성된 클라이언트는 이중 인증을 검증하는 데 실패할 것입니다.

버전 15.30.3.15부터, 이전에 생성된 클라이언트와 2FA 지원이 활성화되지 않은 새 클라이언트는 이전과 동일하게 작동합니다. **사용자가 명시적인 2FA 지원 없이 생성된 클라이언트를 사용하여 로그인하려고 시도하면, 로그인은 거부됩니다.** 이중 인증이 불가능하므로 실패할 것입니다.

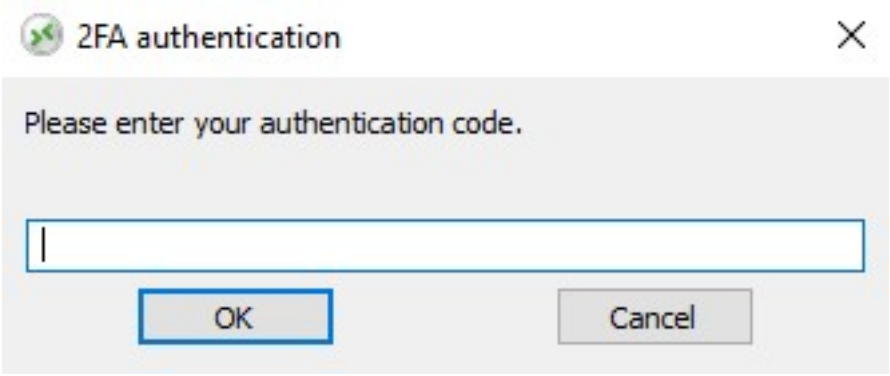
2단계 인증을 추가하려면 확인하십시오. **2FA 활성화** 클라이언트 파일을 생성하기 전에 체크박스를 선택하십시오. 그 결과, Remote Access 애플리케이션 서버에 연결할 때 이중 인증이 검증됩니다. 애플리케이션 서버에서 이중 인증이 활성화되어 있고 연결하는 사용자가 구성되지 않은 경우, 연결이 거부됩니다.



2FA 지원을 나중에 생성된 클라이언트에 추가하는 것은 지원되지 않습니다. 예를 들어, 생성된 .connect 파일에 대해 명령줄을 통해 2FA 지원을 추가하는 것은 지원되지 않습니다.

사용자가 인증기 앱에서 자신의 계정을 설정하면, 비밀번호와 인증기 앱 또는 SMS로 제공된 코드

를 사용하여 연결할 수 있습니다.



고급 연결 옵션

대상 서버가 특정하고 접근 가능한 도메인 이름과 유효한 SSL/TLS 인증서를 설치한 경우, "대상 서버를 원격 데스크톱 게이트웨이(RDG)로 사용하여 데이터 전송을 암호화합니다."를 활성화할 수 있습니다.

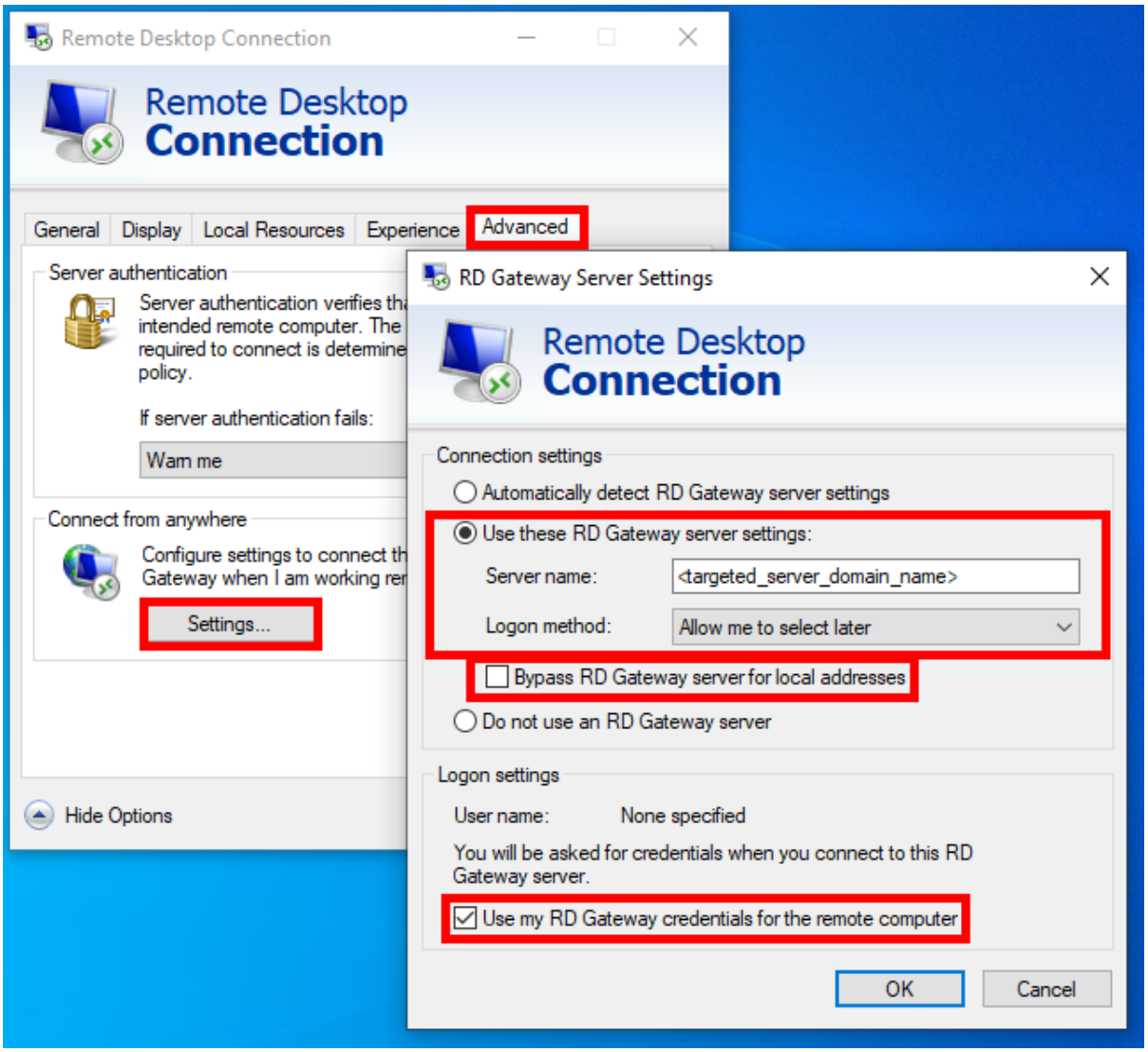
이 옵션은 연결 중 RDP 데이터 전송을 TLS 캡슐화를 사용하여 암호화하여 데이터 암호화 측면에서 모든 VPN에 적합한 대안이 되도록 합니다.

RD 게이트웨이에 연결하려면 대신 mstsc를 사용하세요.

이 기능은 위에서 언급한 전제 조건이 충족되면 생성된 클라이언트를 사용하지 않고 mstsc 구성으로도 사용할 수 있습니다.

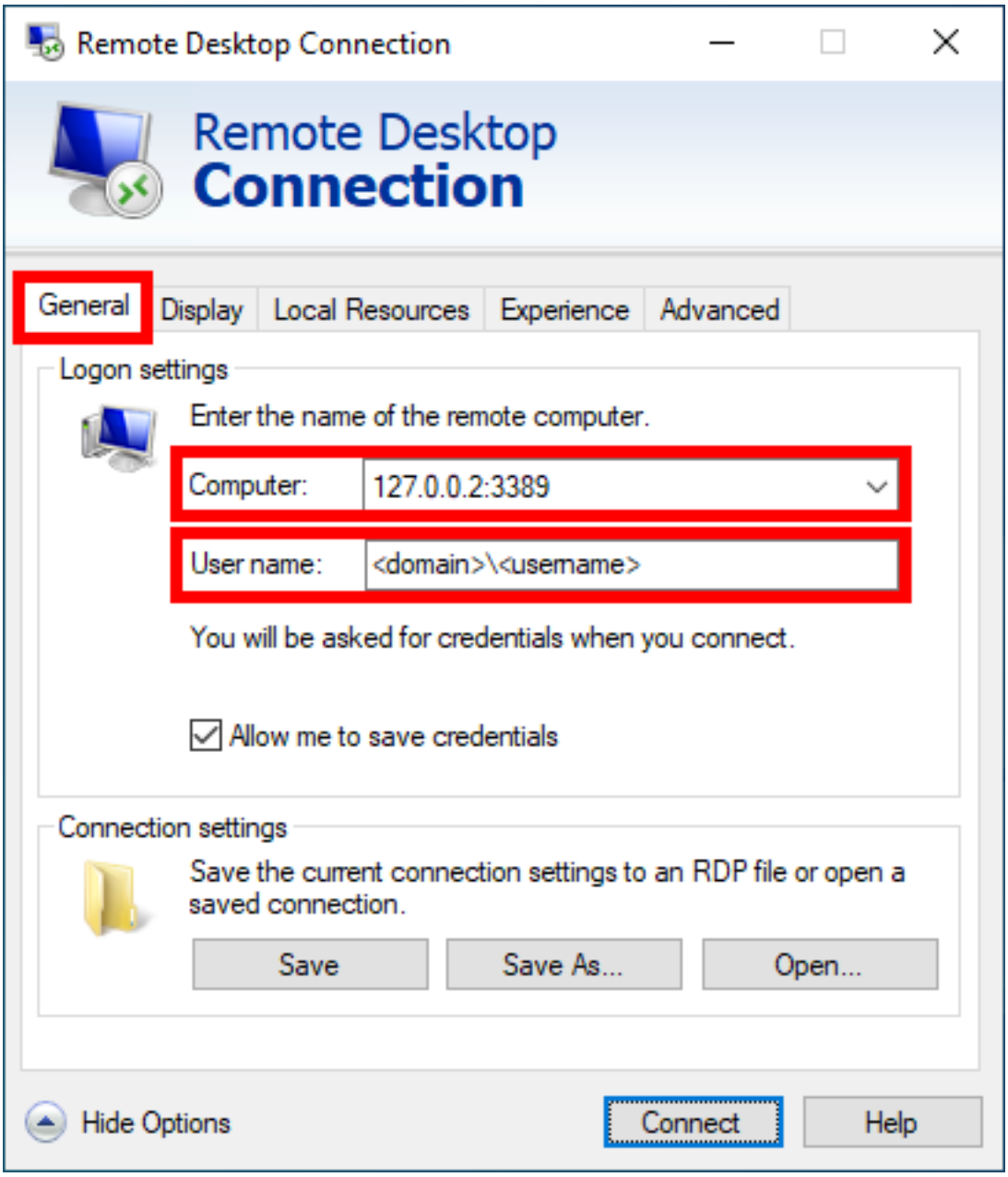
먼저 고급 탭으로 이동한 다음 "어디서나 연결" 섹션에서 "설정"을 클릭하고 원격 데스크톱 게이트웨이를 구성합니다.

- “이 RD 게이트웨이 서버 설정 사용” 옵션 선택
- 서버 이름을 대상 서버 도메인 이름(https:// 없이)으로 교체합니다.
- 로그온 방법 “나중에 선택할 수 있도록 허용” 선택
- “로컬 주소에 대한 RD 게이트웨이 서버 우회” 옵션 선택 해제
- "원격 컴퓨터에 대한 RD 게이트웨이 자격 증명 사용" 옵션을 선택합니다.
- “OK”을 클릭하여 이러한 설정을 저장합니다.



그런 다음 "일반" 탭으로 이동하고:

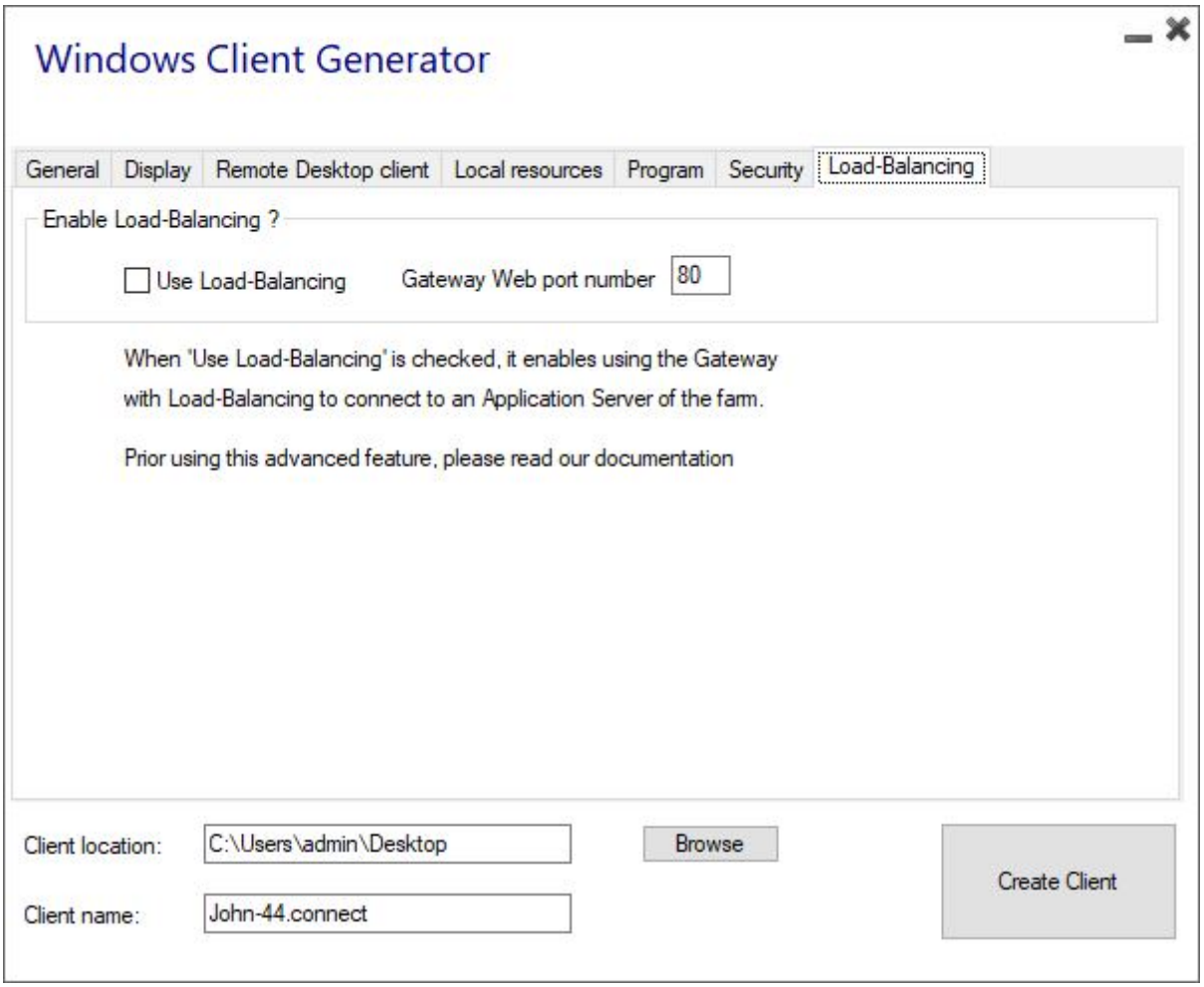
- 컴퓨터 이름을 "127.0.0.2:3389"로 바꾸고, 다른 포트를 사용하는 경우 "3389" 포트를 변경하세요.
- 사용자가 연결하려는 사용자 이름으로 사용자 이름을 바꾸십시오 (**중요: 도메인을 지정하는 것은 필수입니다.**)
- “연결”을 클릭하세요

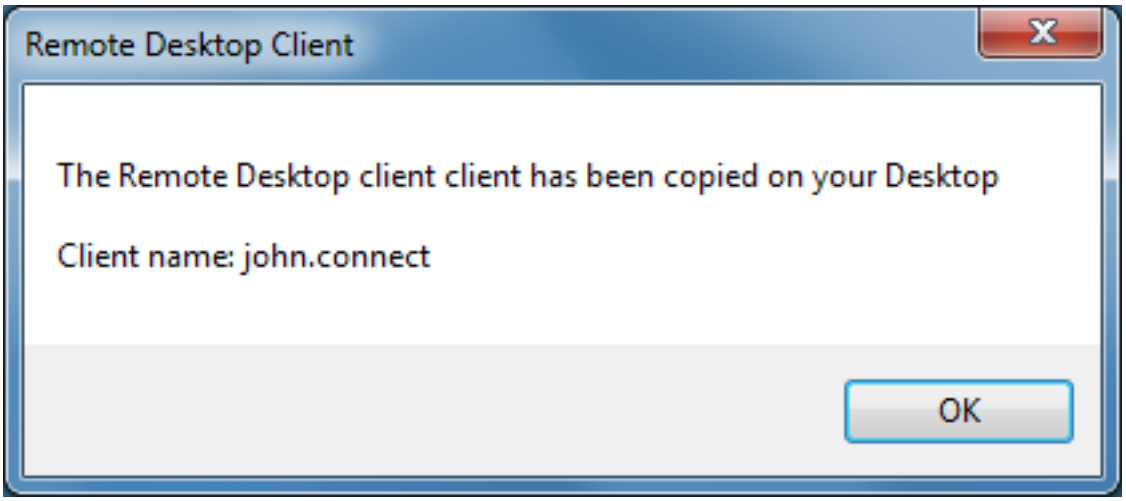


로드 밸런싱을 활성화하여 농장의 한 서버에 연결할 수도 있습니다.

서버에서 로드 밸런싱 기능을 활성화하지 않았다면 "로드 밸런싱 사용" 상자를 체크하지 마십시오.

게이트웨이 웹 포트를 입력해야 하며, 이는 농장의 모든 서버에서 사용되는 기본 웹 포트와 동일해야 합니다.





클라이언트 맞춤화가 가능합니다. 해당 문서는 다음을 참조하십시오. 클라이언트 아이콘 수정하는 방법 그리고 매개변수를 편집하거나 삭제하십시오. .

클라이언트 측에서 다음 레지스트리 키를 추가하여 연결 클라이언트의 로그를 활성화할 수 있습니다:

HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\ConnectionClient “Debug”=“true”

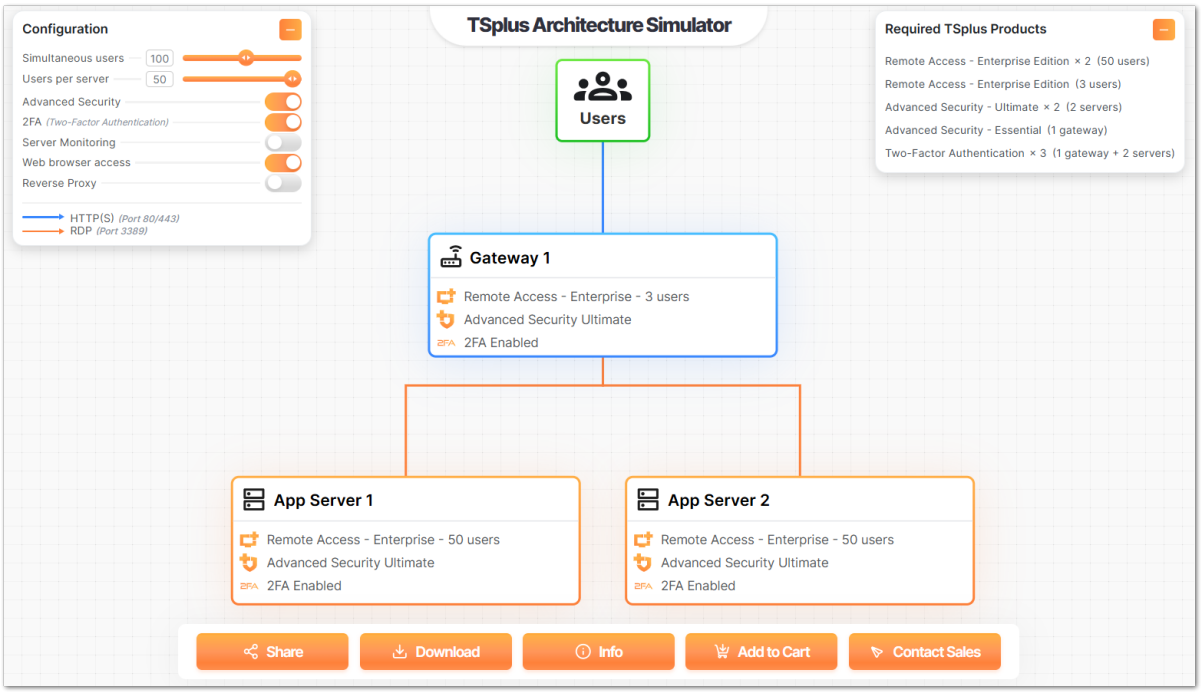
로그는 C:\Users에 있습니다. RDP6\logs 디렉토리는 설치가 사용자별인 경우이며, 모든 사용자에 대한 설치인 경우 C:\Program Files (x86)\Connection Client\RDP6\logs 디렉토리입니다.

TSplus Remote Access 전제 조건

아키텍처 시뮬레이터

온라인에서 아키텍처를 구성하여 저희 소프트웨어와 추가 기능을 선택하는 데 도움을 주십시오.

TSplus 아키텍처 시뮬레이터



1. 하드웨어

TSplus Remote Access Server 최소 요구 사항:

사용자 수	Windows 2008에서 2025 또는 7에서 11 Pro
3 - 5	I5 이상 하나의 CPU 2 GHZ 최소 : 4 GB RAM 권장 : 8 GB RAM

10	I5 이상 하나의 CPU 2 GHZ 최소 : 8 GB RAM 권장 : 16 GB RAM
25	하나의 CPU I7 또는 제온 최소 : 16 GB RAM 권장 사항: 32 GB RAM
50 이상	32 GB 듀얼 CPU - 시스템 전용 SSD 디스크 최소: 32 GB RAM 권장 사항: 64 GB RAM

10년 이하의 CPU를 사용하는 것을 권장합니다.

RAM 사용에 관해서는 설치된 OS, 동시 사용자 수 및 그들에게 할당된 애플리케이션에 따라 달라질 것입니다.

각 서버(물리적 또는 가상 서버)는 최대 50명의 동시 사용자를 처리할 수 있습니다. 50명 이상의 동시 세션을 위해서는 TSplus Remote Access Enterprise Edition에서 제공하는 로드 밸런싱 기능이 있는 서버 팜을 사용하는 것을 권장합니다.

참고: 귀하의 하드웨어의 정확한 사양은 귀하의 애플리케이션이 소비하는 리소스(CPU/RAM/디스크)의 종류에 따라 달라집니다.

오직 **x86 및 x64** 아키텍처가 지원됩니다.
ARM32 및 ARM64 아키텍처는 지원되지 않습니다.

2. 운영 체제

귀하의 하드웨어는 아래의 운영 체제 중 하나를 사용해야 합니다:

- 윈도우 **7 프로**
- 윈도우 **8/8.1 프로**
- 윈도우 **10 프로**
- 윈도우 **11 프로**
- 윈도우 **서버 2008 SP2/스몰 비즈니스 서버 SP2 또는 2008 R2 SP1**
- 윈도우 **서버 2012 또는 2012 R2**
- 윈도우 **서버 2016**
- 윈도우 **서버 2019**
- 윈도우 **서버 2022**
- 윈도우 **서버 2025**

32비트와 64비트 아키텍처가 모두 지원됩니다.

필요한 프레임워크는 **.NET 버전 4.7.2** 모든 지원되는 Windows 버전용.

원격 액세스 버전	최소 Windows 버전
19, LTS 18, LTS 17, LTS 16, LTS 15	Windows 7 서비스 팩 1 Windows Server 2008 R2 서비스 팩 1
LTS 14	윈도우 비스타 Windows Server 2008

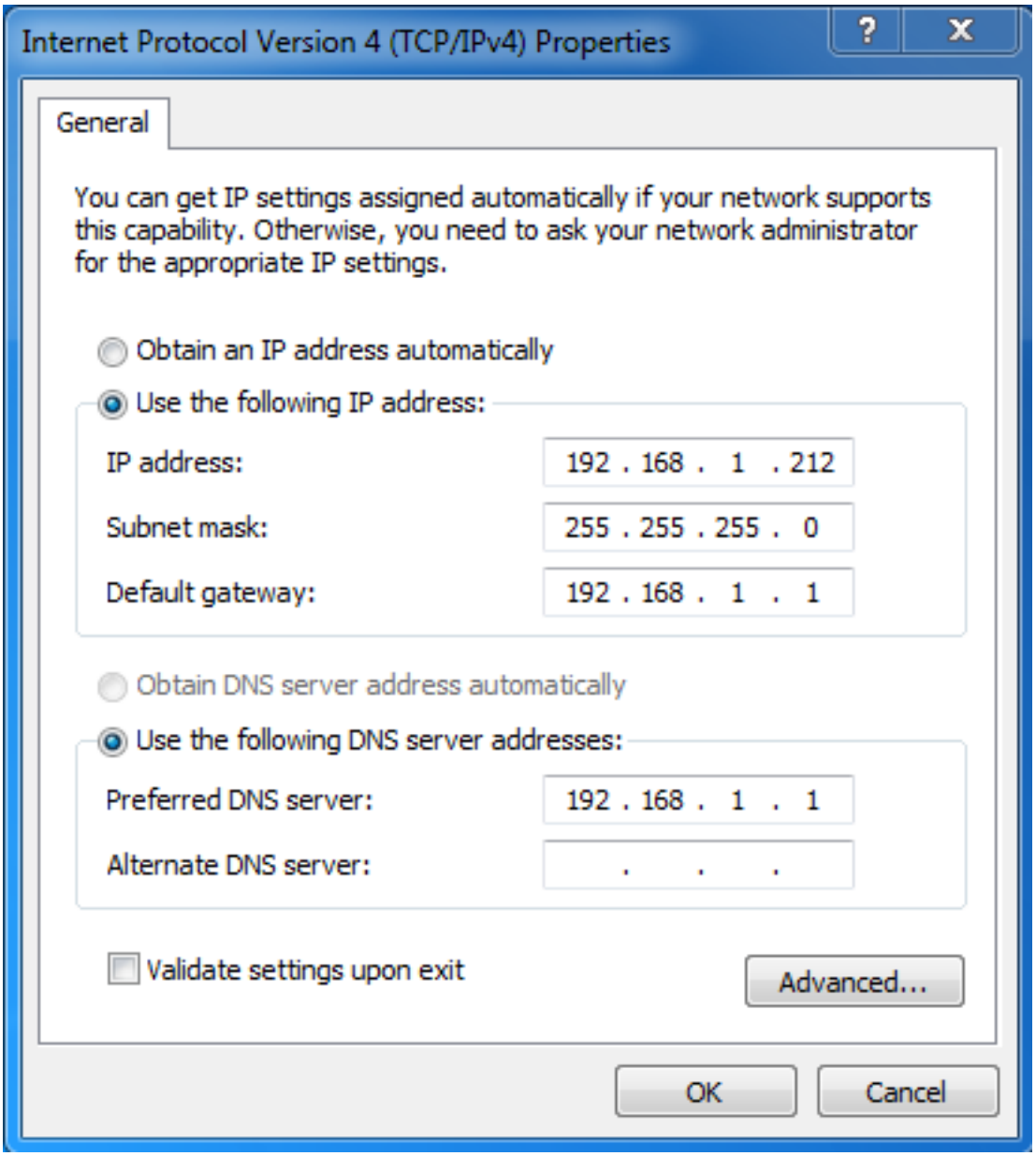
- Windows Server OS에 Remote Access를 설치할 경우, TSplus Remote Access를 설치하기 전에 RDS/Terminal Services 및 RDS/Terminal Services Licensing 역할이 설치되지 않았는지 확인하십시오.

이 역할이 현재 설치되어 있다면, 제거하고 재부팅하십시오.

- Windows Home Editions는 지원되지 않습니다.
- Windows Server 2016에서는 원격 데스크톱 액세스를 위해 최대 15개의 세션이 허용됩니다.
- Windows Server 2016, 2019, 2022 Essentials Edition은 TSplus Remote Access 사용을 지원하지 않으며 권장되지 않습니다.
- TSplus Remote Access 내장 웹 서버가 필요합니다 **Java OpenJDK 17 이상.** .

3. 네트워크 매개변수

원격 액세스 서버는 정적 개인 IP 주소를 가져야 합니다:



원격 액세스 (광역 네트워크 - WAN)

- 고속 인터넷 연결과 정적 공인 IP 주소를 권장합니다. 정적 IP 주소가 없는 경우, 다음과 같은 동적 DNS 서비스를 사용하는 것을 고려하십시오.
- TCP RDP 포트(기본값 3389)는 방화벽에서 양방향으로 열려 있어야 합니다.

3. 보안

2024년 초부터,
TSplus는 신뢰 체인에서 Let's Encrypt의 변경 사항에 맞추어 자동 SSL/TLS 인증서 생성 메커니즘을 업데이트했습니다: **"DST Root CA X3"** 루트가 교체되었습니다 **ISRG 루트 X1** .

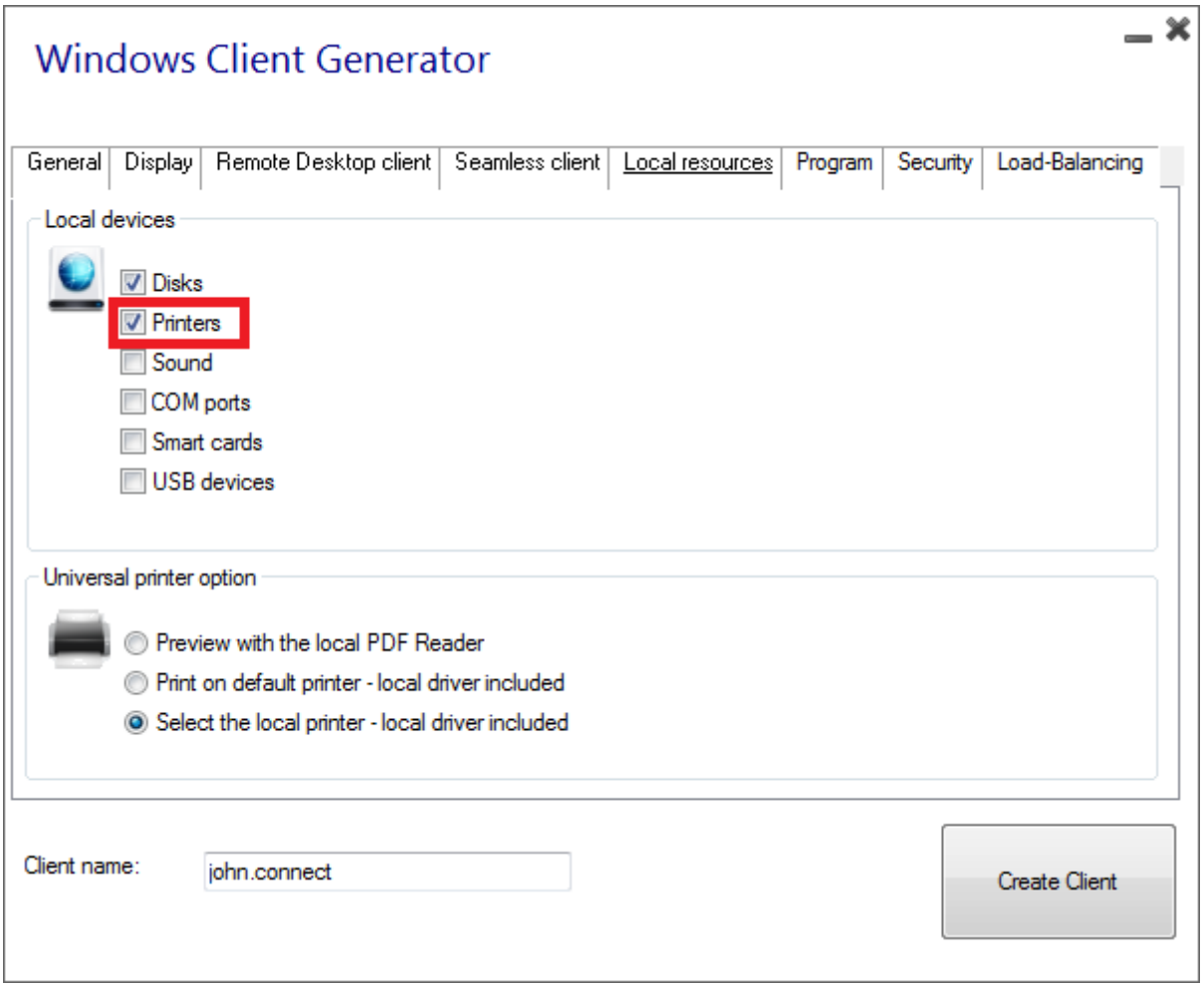
클라이언트나 워크스테이션이 새 인증서를 인식하지 못하는 경우, 추가해야 할 수 있습니다.
ISRG 루트 X1 Windows 신뢰할 수 있는 인증서 저장소로.

TSplus는 와일드카드 인증서와 함께 작동하며 안전한 원격 연결을 위해 TLS 프로토콜을 지원합니다.

표준 RDP 프린터 매핑 기능으로 인쇄하기

이것은 원격 데스크톱 사용자들에 의해 일반적으로 사용되며, Microsoft 터미널 서비스와 동일한 기능을 제공합니다.

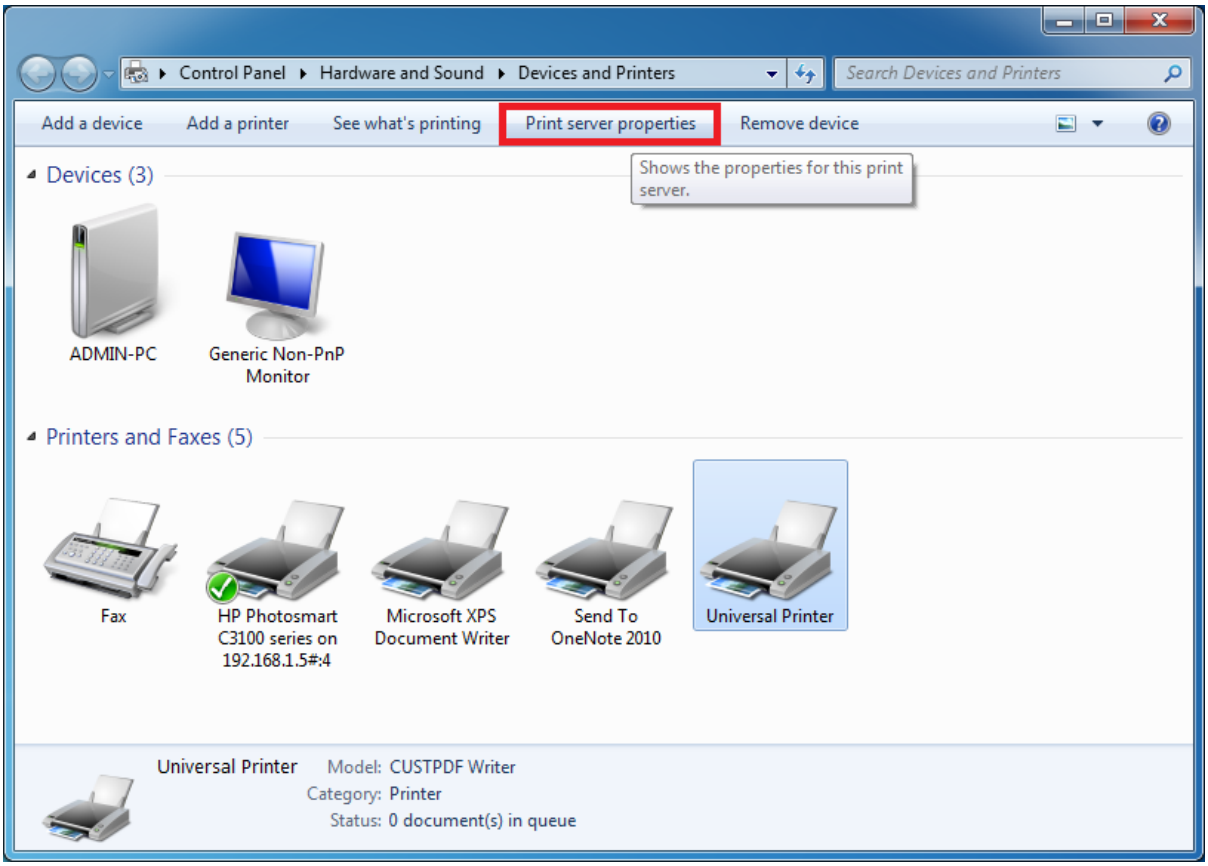
이국적인 프린터를 사용할 계획이라면 클라이언트 생성기의 로컬 리소스 탭에서 프린터에 대한 체크박스를 반드시 확인하세요.



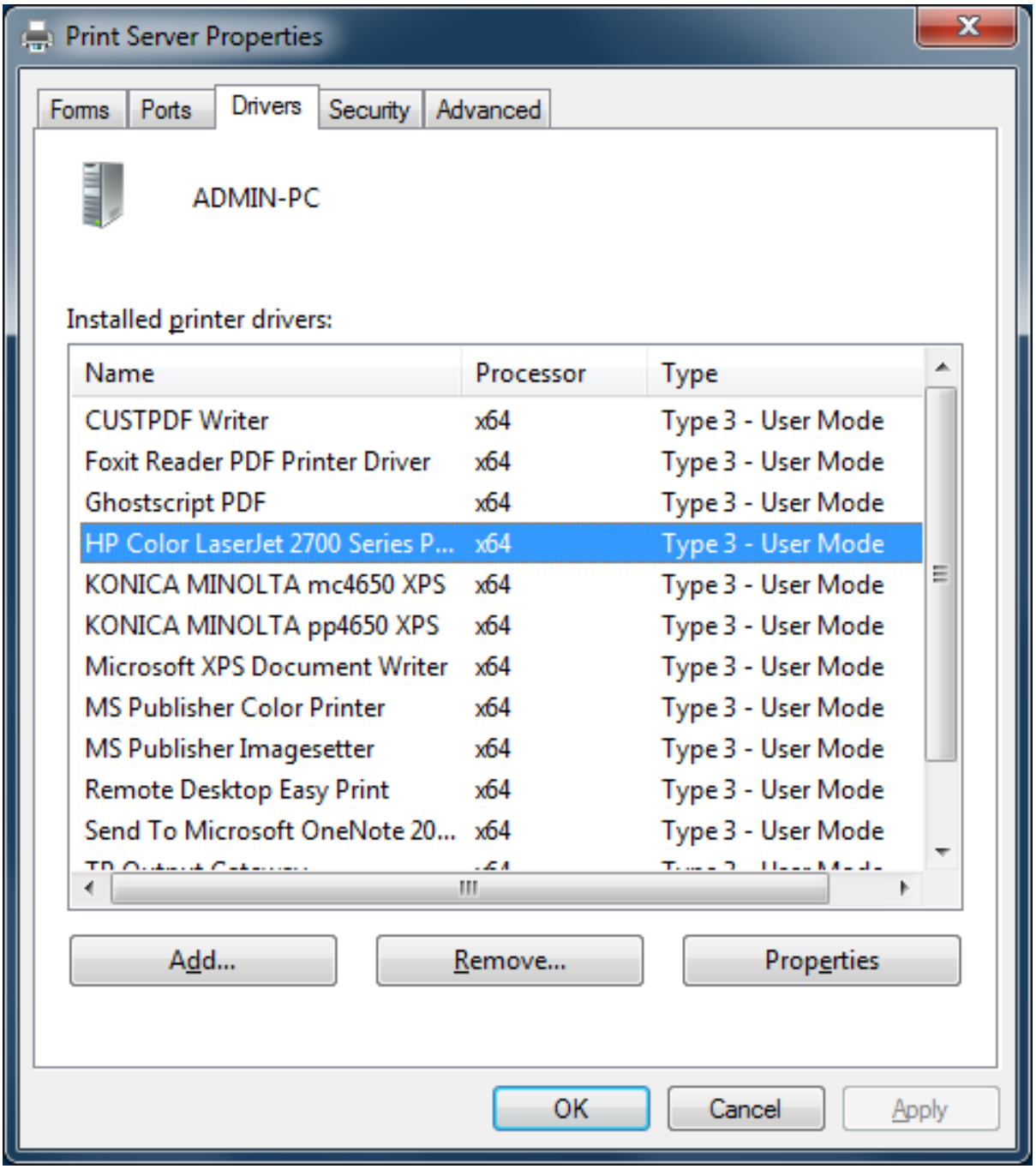
대부분의 경우 클라이언트와 서버 모두에 동일한 버전의 프린터 드라이버를 설치해야 제대로 작동합니다.

이것은 서버가 Windows 2008 64비트이고 클라이언트 컴퓨터가 Windows XP 32비트를 실행하는 경우, 서버에 32비트 XP 프린터 드라이버를 설치해야 함을 의미합니다.

시작 메뉴를 클릭한 다음 장치 및 프린터를 클릭합니다. 프린터를 클릭하면 창 상단에 인쇄 서버 속성 버튼이 표시됩니다.



프린트 서버 속성에서 드라이버 탭을 클릭하여 클라이언트 드라이버를 수동으로 추가합니다. (이 경우, Windows XP 32비트 드라이버를 설치하고 있습니다.)



프린터 제조업체 웹사이트의 정보와 드라이버를 사용하여 프린터 드라이버를 직접 설치할 수도 있습니다.

- 하드웨어 매뉴얼을 확인하여 터미널 서버 환경에서의 설치 절차를 확인하는 것이 좋습니다.
- USB 프린터를 사용하고 있다면, 리디렉션된 프린터와의 최대 호환성을 보장하기 위해 클라이언트 컴퓨터의 RDP 프로토콜을 RDP 버전 6 이상으로 업데이트했는지 확인하세요.

최고의 결과를 얻으려면 USB 프린터를 사용하지 않는 것이 좋습니다. COM 또는 LPT 프린터를 사용할 때 호환성과 신뢰성이 향상됩니다.

일부 이국적인 프린터, 예를 들어 라벨 프린터나 영수증 프린터는 TSplus 세션에서 리디렉션하는 데 적합하지 않을 수 있으므로, RDS 또는 터미널 서버 환경에서 호환성 및 설치 절차에 대해 항상 하드웨어 제조업체에 확인해야 합니다. 이 경우 TSplus와 매우 유사합니다.

TSplus Remote Access v19: 빠른 시작 가이드

필수 조건 :

서버에서 :

- **운영 체제:** Microsoft Windows 7에서 11까지 또는 Windows Server 2008R2에서 2025까지 최소 2GB의 RAM이 필요합니다.
- TSplus는 Windows Home Editions에 Remote Access 설치를 지원하지 않습니다.
- 운영 체제 **필수** C: 드라이브에 있습니다.
- Java Runtime Environment. Java가 이미 설치되어 있지 않은 경우, Remote Access는 설치 중에 OpenJDK를 설치합니다.
- Windows Server 운영 체제에 Remote Access를 설치하는 경우 RDS/Terminal Services 및 RDS/Terminal Services 라이선스 역할이 있는지 확인하십시오. **설치되지 않음** TSplus Remote Access를 설치하기 전에.
- 귀하의 Remote Access 서버는 정적 개인 IP 주소를 가져야 합니다.
- 외부 액세스를 위해, 귀하의 서버는 정적 공용 IP 주소 또는 동적 DNS 공급자가 있어야 합니다.
- TSplus Remote Access 내장 웹 서버가 필요합니다 **Java OpenJDK 17 이상.** .

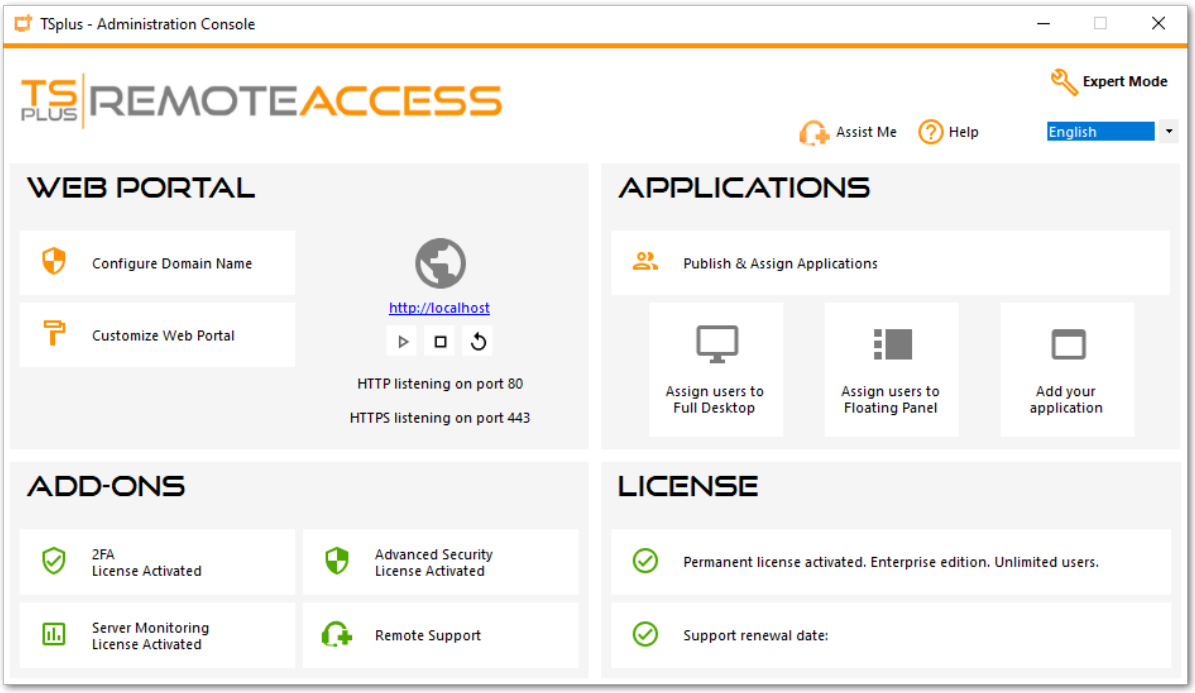
클라이언트에서 :

- **운영 체제:** Microsoft Windows 7에서 11까지의 버전이 완전히 지원됩니다.
- MacOS에서는 모든 Mac RDP 클라이언트나 TSplus HTML5 클라이언트를 사용할 수 있습니다.
- Linux에서는 Rdesktop 또는 TSplus HTML5 클라이언트를 사용할 수 있습니다.
- 자바 런타임 환경.
- PDF 리더 (예: Foxit Reader 또는 Acrobat DC)

자세한 전제 조건은 다음을 참조하십시오. 문서

참고:

Remote Access 버전 15부터 관리 콘솔의 모양이 변경되었습니다. A **라이트 모드** 그리고 하나 **전문 모드** 두 가지 인터페이스 스타일 간에 전환할 수 있습니다. 관리자는 관리 콘솔의 오른쪽 상단 모서리에 있는 버튼을 클릭하여 전환할 수 있습니다.



1단계: 설치.

참고:

원격 액세스의 평가판 버전은 모든 기능이 포함된 엔터프라이즈 에디션입니다. 최대 5명의 동시 사용자를 위해 15일 동안 라이선스가 부여됩니다.

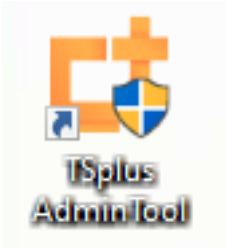
TSplus Remote Access 설치는 간단한 과정입니다. 웹사이트에서 다운로드하고 Setup-TSplus.exe 프로그램을 실행하기만 하면 됩니다.

파일이 압축 해제되어 복사됩니다:

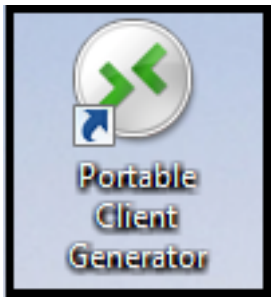
- C:\Program Files\TSplus (32비트 시스템)
- C:\Program Files(x86)\TSplus (64비트 시스템).

설치가 완료되면 설치 프로그램이 재부팅을 요청합니다.

재부팅 후 바탕 화면에 2개의 새로운 아이콘이 표시됩니다:



AdminTool은 Remote Access를 사용하기 위해 필요한 도구입니다.

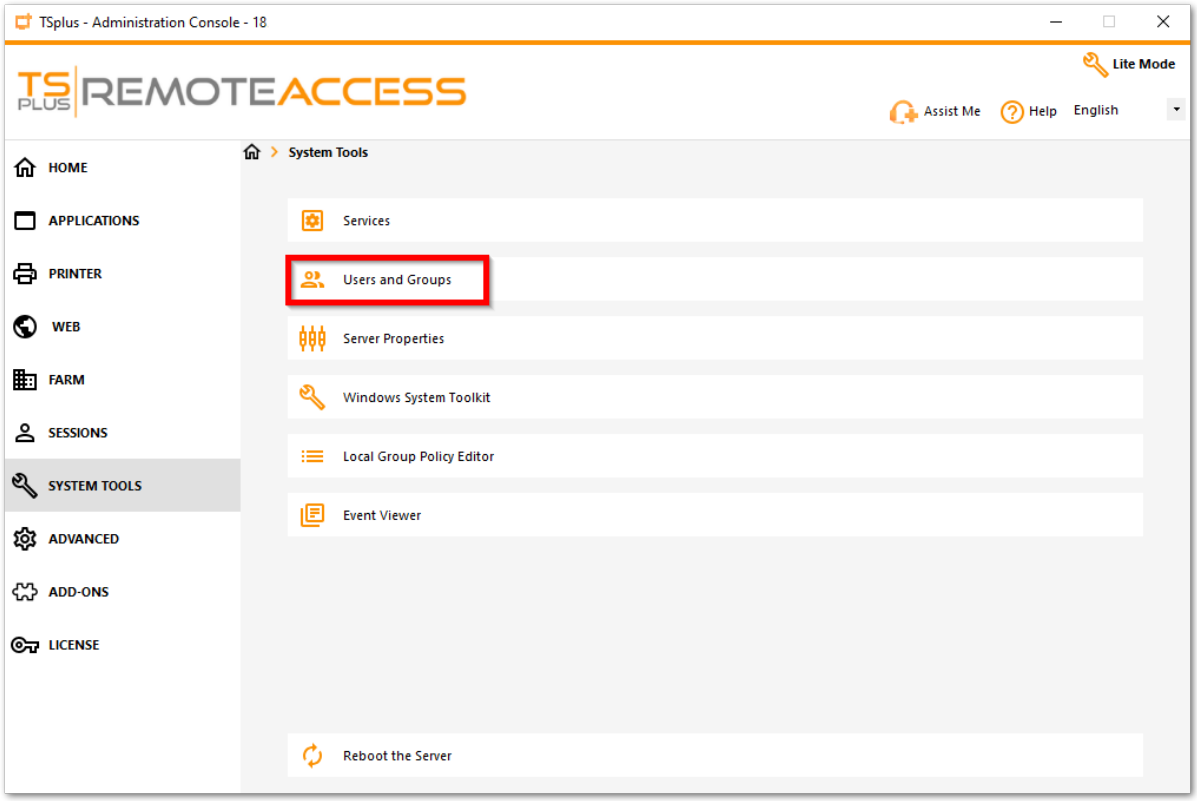


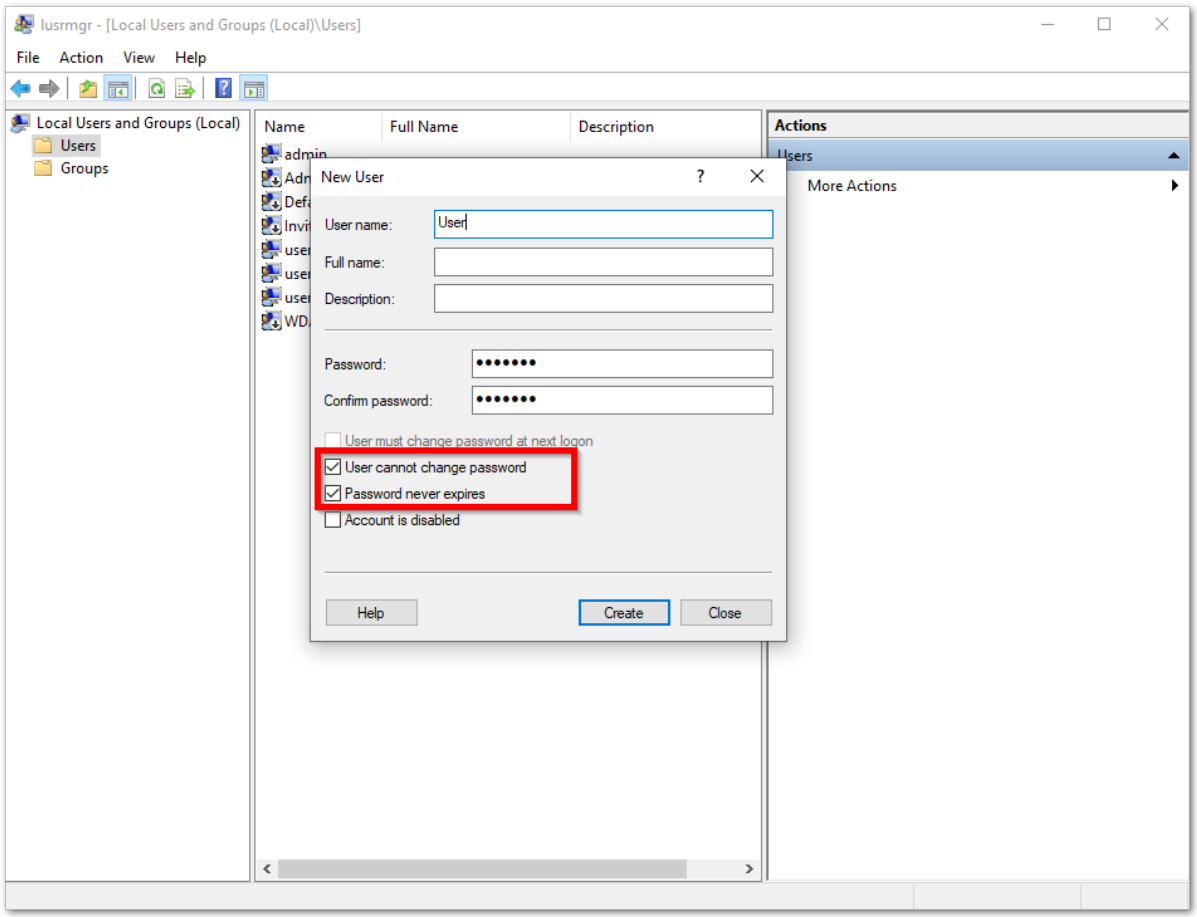
휴대용 클라이언트 생성기는 사용자를 위한 Remote Access 연결 클라이언트를 생성하는 데 사용됩니다.

보세요 문서 전체 설치 지침을 참조하십시오.

2단계: 사용자 생성.

재부팅 후, Remote Access Server는 거의 준비가 완료되었습니다. 이제 사용자를 생성하겠습니다. 시작하려면 AdminTool을 엽니다. 그런 다음 System Tools 탭으로 이동하여 "Users and Groups"를 클릭합니다. 그러면 Local Users and Groups 창으로 이동합니다.





각 사용자는 사용자 이름과 비밀번호를 가져야 합니다. 사용자를 생성할 때 "사용자는 다음 로그인 시 비밀번호를 변경해야 함"이라는 상자를 주의 깊게 확인하세요. 사용자가 첫 로그인 시 비밀

번호를 변경하지 않도록 하려면 이 상자의 선택을 해제하고 "비밀번호가 만료되지 않음" 또는 "사용자가 비밀번호를 변경할 수 없음"을 선택하세요.

3단계: 귀하의 필요에 가장 적합한 클라이언트를 선택하십시오.

원격 액세스는 Windows 원격 데스크톱 프로토콜과 호환됩니다. 모든 사용자는 표준 원격 데스크톱 연결 클라이언트(mstsc.exe) 또는 RDP 호환 클라이언트를 사용하여 로컬 또는 원격으로 연결할 수 있습니다. 원격 액세스의 고급 기능(원격 앱, 유니버설 프린터 등)을 완전히 활용하려면 생성된 클라이언트 또는 원격 액세스 웹 포털을 사용할 수 있습니다.

원격 액세스는 매우 유연한 솔루션이며 세션을 여는 여러 가지 방법을 제공합니다:

- **클래식 원격 데스크톱 연결** (MSTSC.EXE).
- **휴대용 TSplus RDP 클라이언트** 원격 연결을 위해 창 모드 환경을 표시하며, Windows 작업 표시줄에서 최소화할 수 있습니다.
- **MS RemoteAPP 클라이언트** 네이티브 MS RemoteApp을 사용하여 애플리케이션을 표시합니다.
- **윈도우 클라이언트** TSplus 웹 포털을 통해.
- **HTML5 클라이언트** TSplus 웹 포털을 통해.

이 클라이언트는 사용자에게 다음과 같은 경험을 제공합니다:

원격 데스크톱 연결(mstsc.exe)

- **연결** 연결은 매우 표준적인 것입니다. 이 유형의 연결에서는 유니버설 프린터가 지원되지 않습니다.

- **디스플레이** 사용자는 Remote Desktop 창 내에서 자신의 세션을 볼 수 있습니다. 이 데스크탑은 사용자의 데스크탑 폴더의 내용을 표시합니다.

  관리자가 AdminTool로 특정 애플리케이션을 할당한 경우, 이러한 애플리케이션만 표시됩니다(작업 표시줄 없음, 바탕 화면 없음).

TSplus RDP 생성 클라이언트 .

이것은 독특한 TSplus 솔루션으로, 로컬 및 원격 사용자가 하나의 전용 프로그램을 사용하여 연결할 수 있도록 합니다.

연결 프로그램, 고급 기능인 유니버설 프린팅, 사용자에게 매우 간단하면서도 높은 수준의 보안을 유지하는 휴대성을 포함합니다.

TSplus 클라이언트 생성기 사용에 대한 자세한 내용은 다음을 참조하십시오. 이 문서

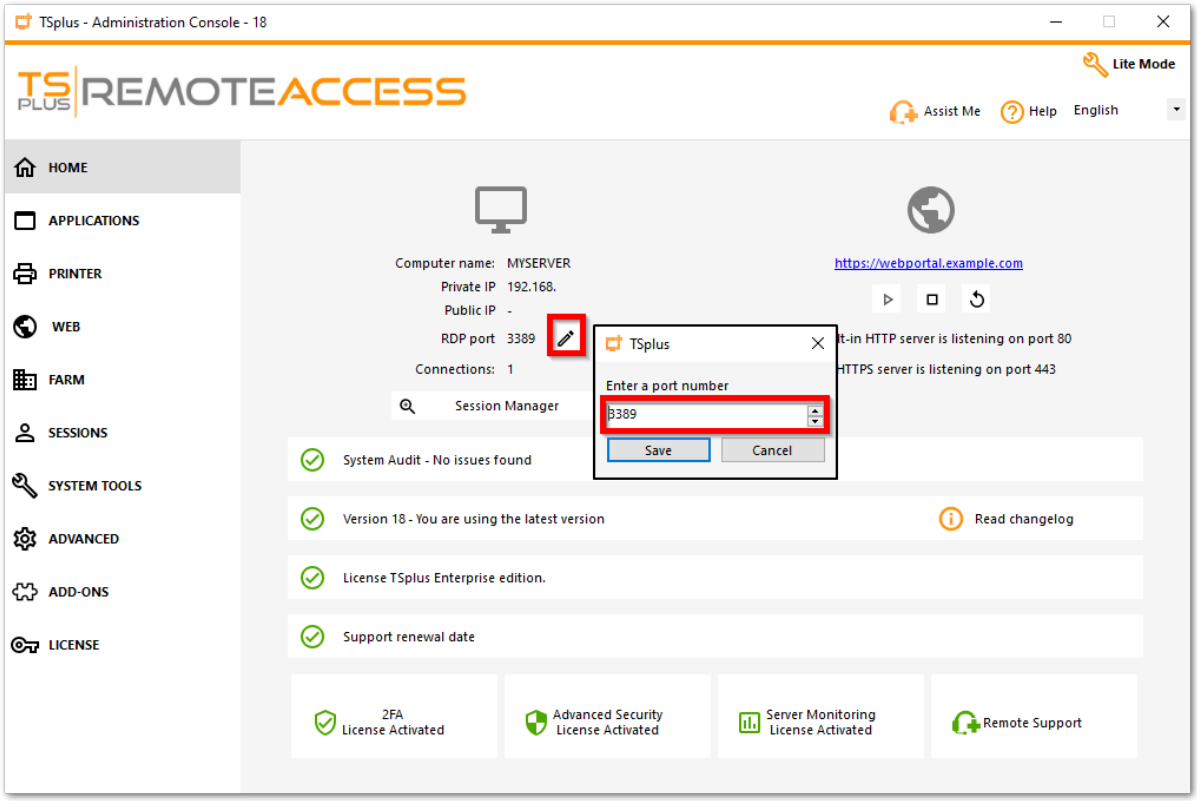
TSplus RemoteApp에서 생성된 클라이언트 .

원격 애플리케이션은 로컬 애플리케이션처럼 보이고 작동합니다. 고전적인 원격 데스크톱 창 대신, 원격 데스크톱 창을 최소화할 필요 없이 로컬 애플리케이션과 원격 애플리케이션 간에 자유롭게 전환할 수 있습니다.

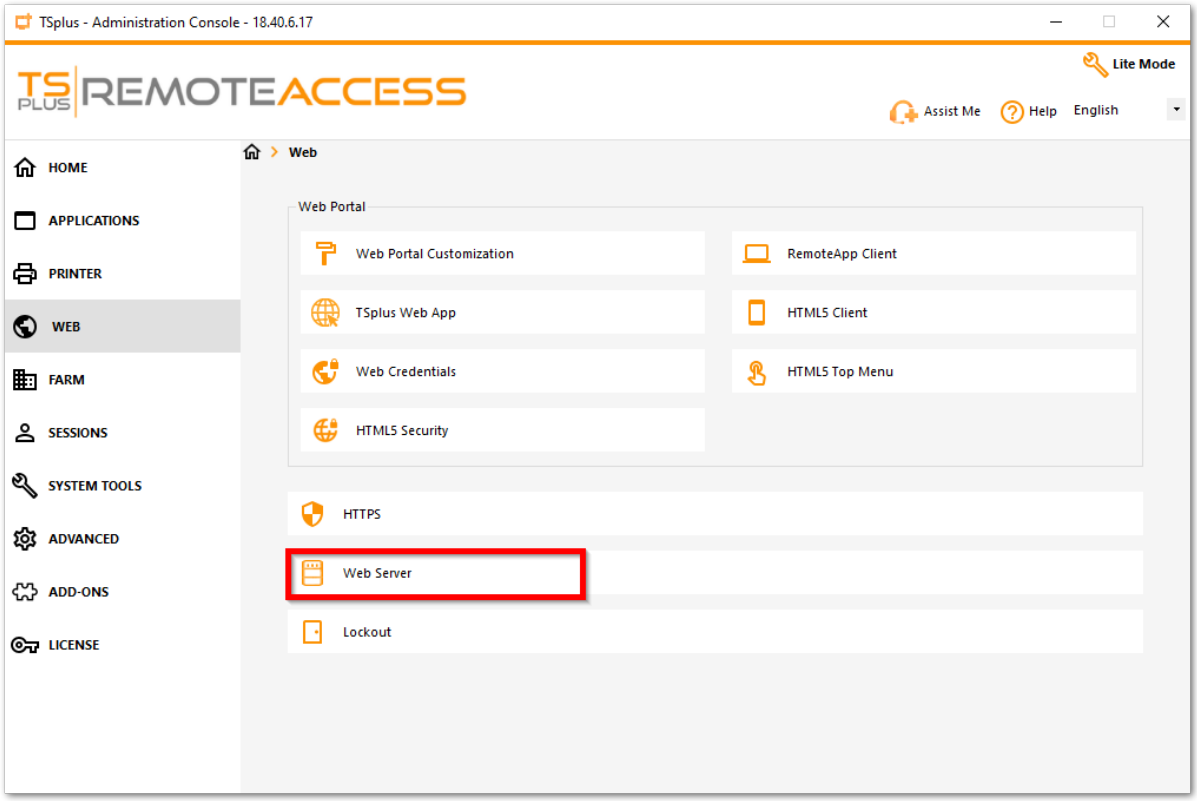
이 클라이언트에 대한 자세한 정보는 다음을 참조하십시오. 이 문서 .

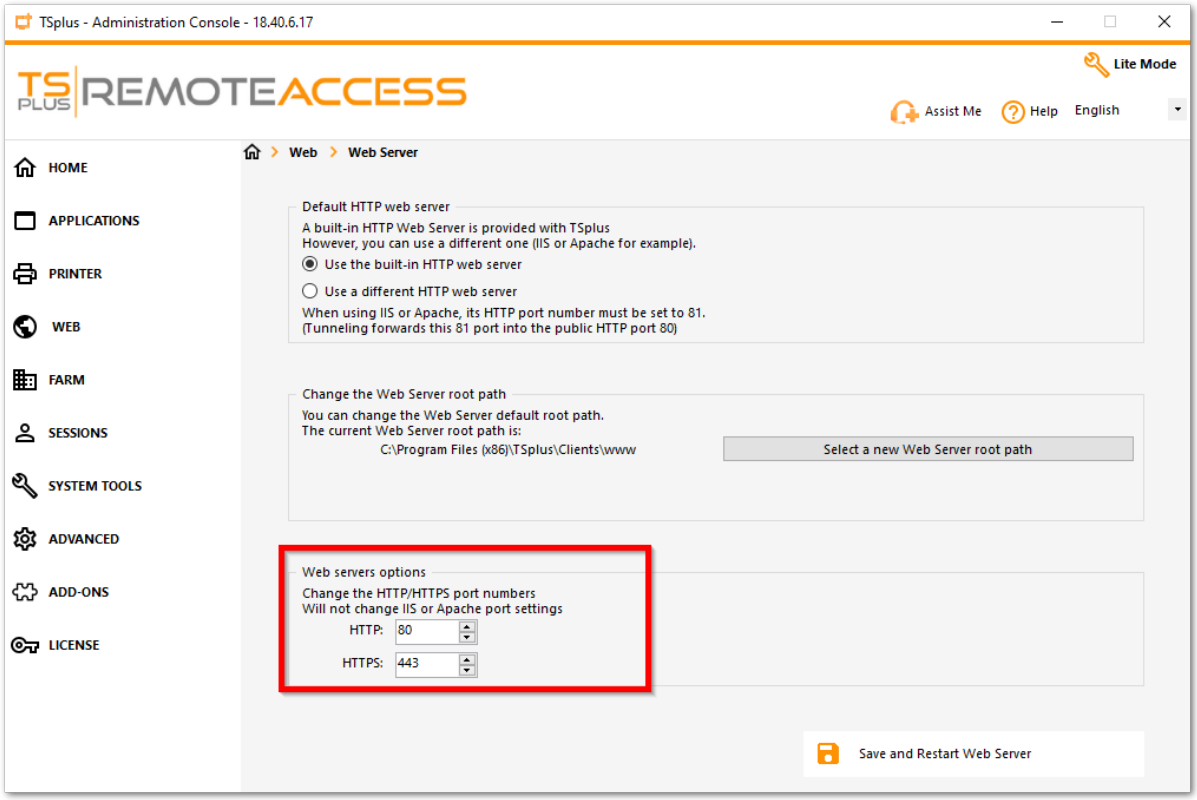
원격 위치에서 TSplus Remote Access 서버에 액세스하기

로컬 네트워크 외부에서 Remote Access 서버에 접근하려면 선호하는 연결 방법에 따라 3389/80/443 포트의 포트 포워딩 또는 포트 리디렉션 규칙을 만들어야 합니다. 홈 탭에서 RDP 포트를 변경할 수 있습니다.



80/443 포트는 웹 서버 탭에서 변경할 수 있습니다:





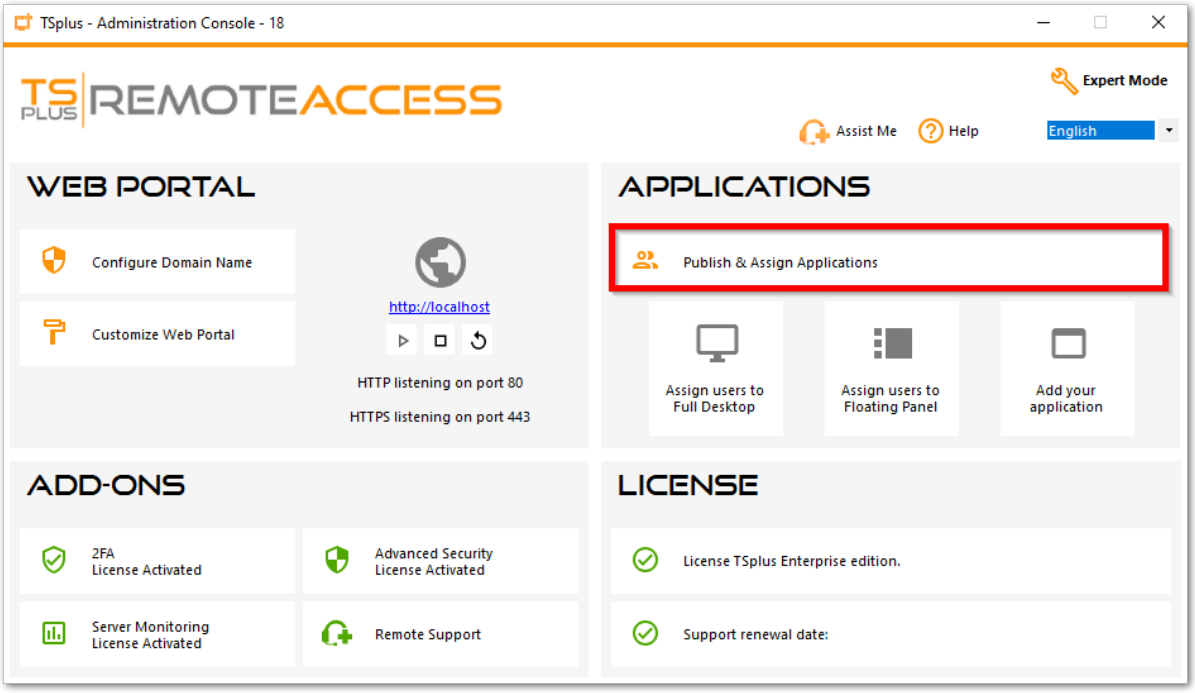
4단계: 애플리케이션 게시 및 애플리케이션 제어.

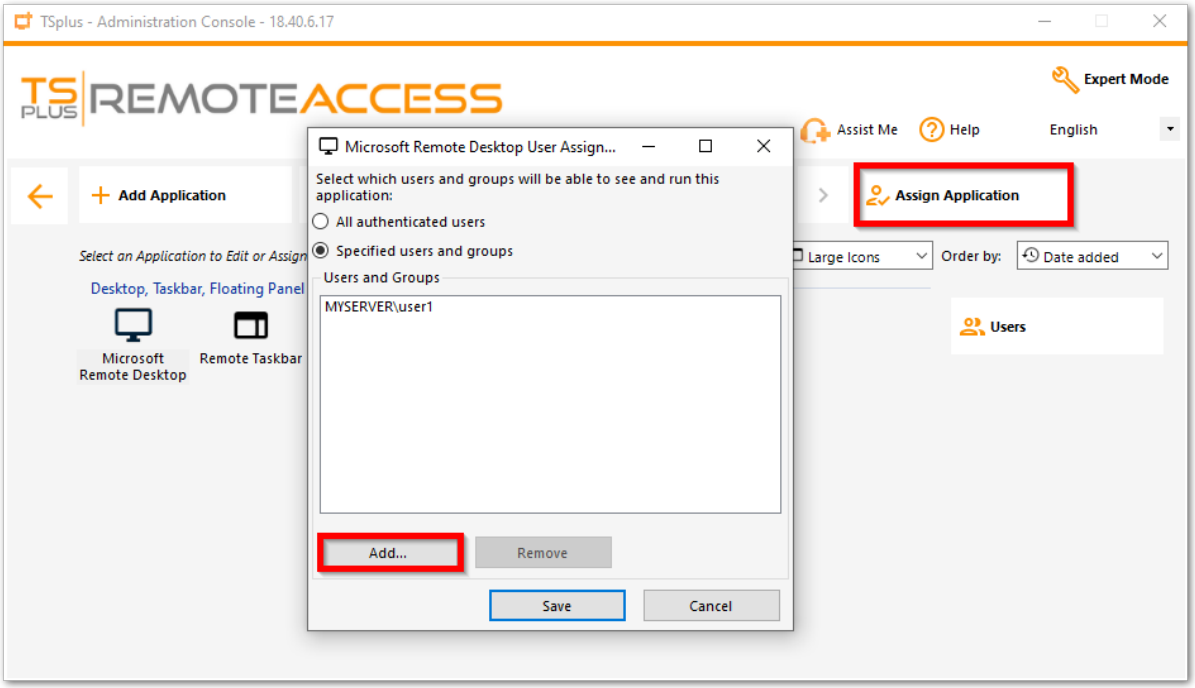
원격 액세스 관리 도구에서 사용자 또는 그룹에 응용 프로그램을 할당할 수 있습니다.

- 사용자에게 하나의 애플리케이션을 할당하면, 그들은 이 애플리케이션만 볼 수 있습니다.

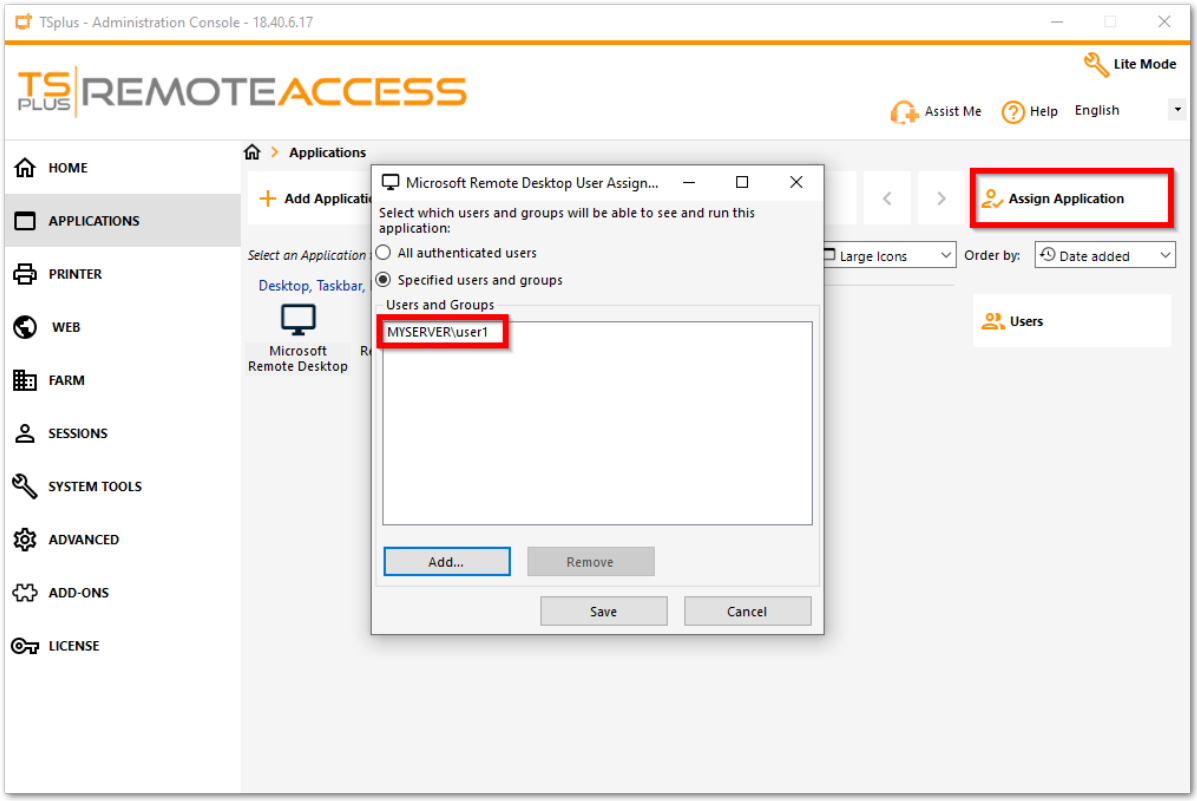
- 그들에게 여러 응용 프로그램을 표시하기 위해 TSplus 작업 표시줄, 플로팅 패널 또는 응용 프로그램 패널을 할당할 수도 있습니다.
- 전체 원격 데스크톱을 게시할 수도 있습니다.

이제 사용 가능합니다.
라이트 모드
홈 탭에서.





또는 이동하십시오 **전문 모드** > 앱 탭에서 앱을 추가, 편집, 삭제 및 할당합니다.



이 예제에서 관리자는 사용자 'John'이 TSplus 작업 표시줄을 받기로 결정했습니다. 이 문서 자세한 정보는 다음과 같습니다.

TSplus Remote Access를 이용해 주셔서 감사합니다!

TSplus 라이센스 재호스팅

온라인 재호스팅

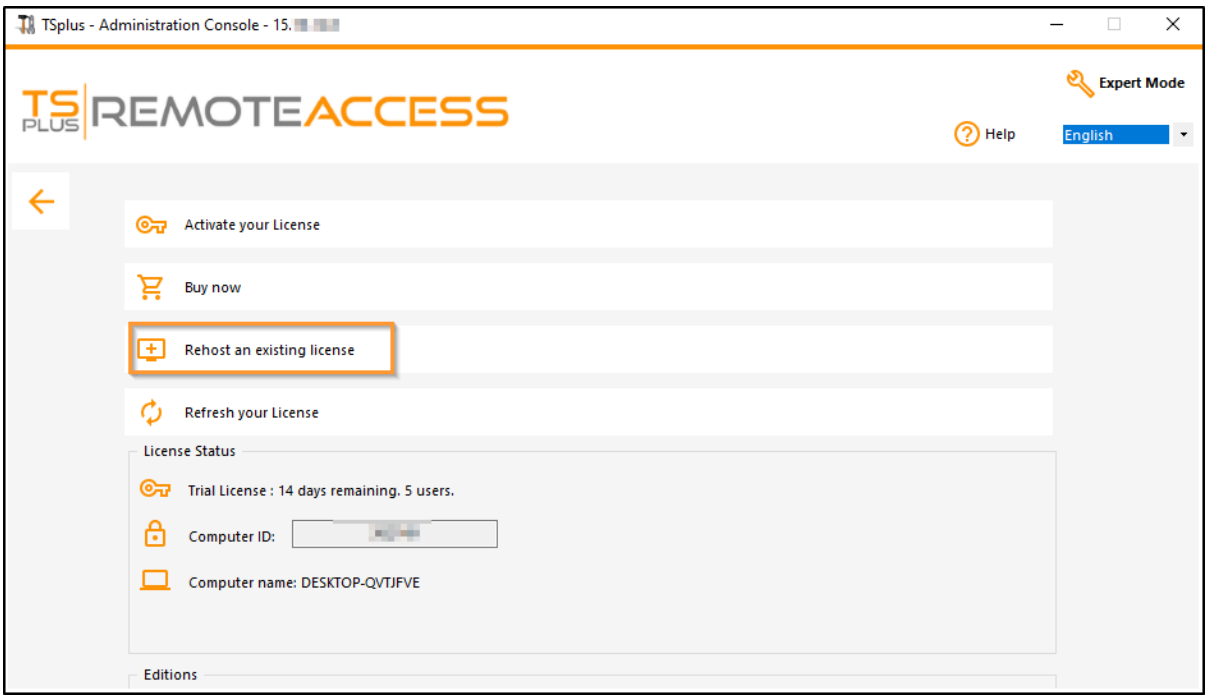
온라인 활성화는 한 달에 한 번 승인됩니다.

필수 조건: 라이센스를 재호스팅하려면 활성 지원 구독이 필요합니다.

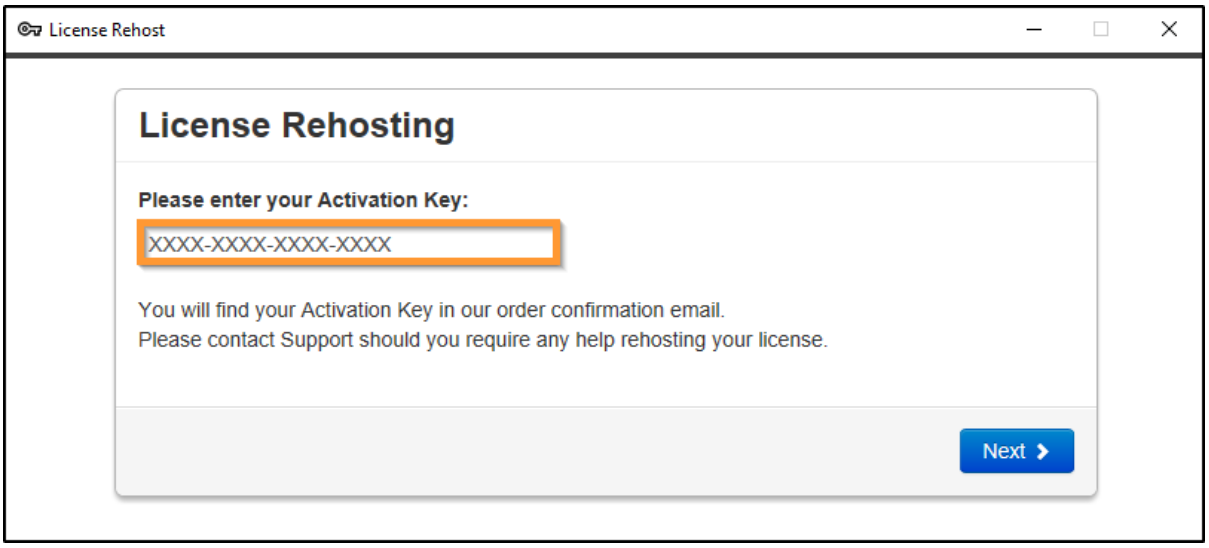
비클론 원격 액세스를 새 컴퓨터 ID를 생성하기 위해 새로운 버전을 설치해야 합니다.

서버를 복제하고 Remote Access를 클론한 경우, 다음 페이지로 이동해 주시기 바랍니다: 서버 복제

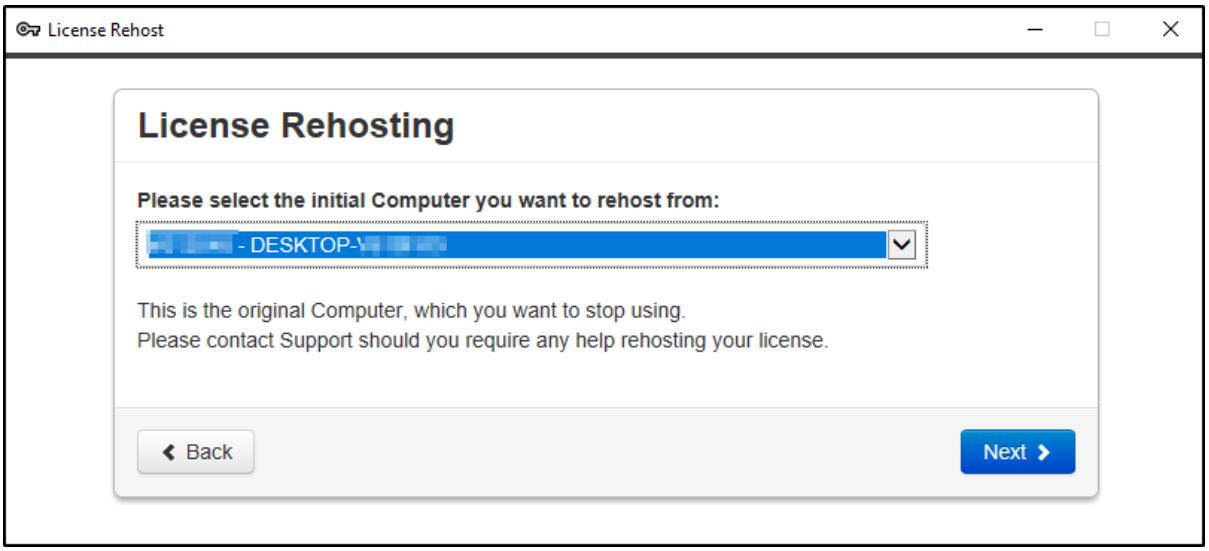
새 서버에서 “라이센스” 탭으로 이동 “기존 라이센스 재호스팅”을 클릭하십시오.



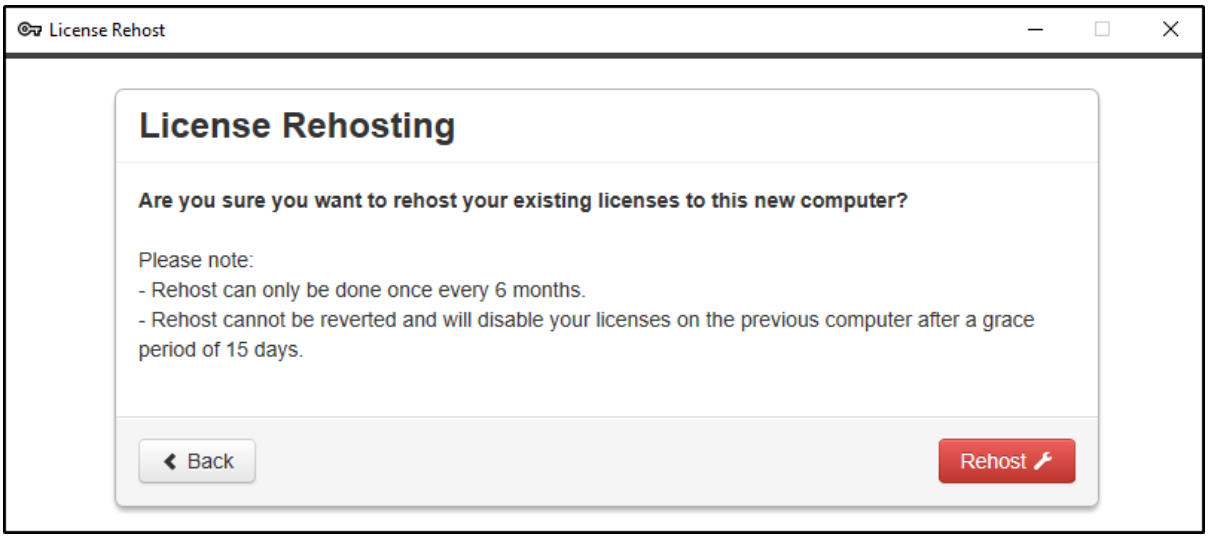
활성화 키를 입력하세요:



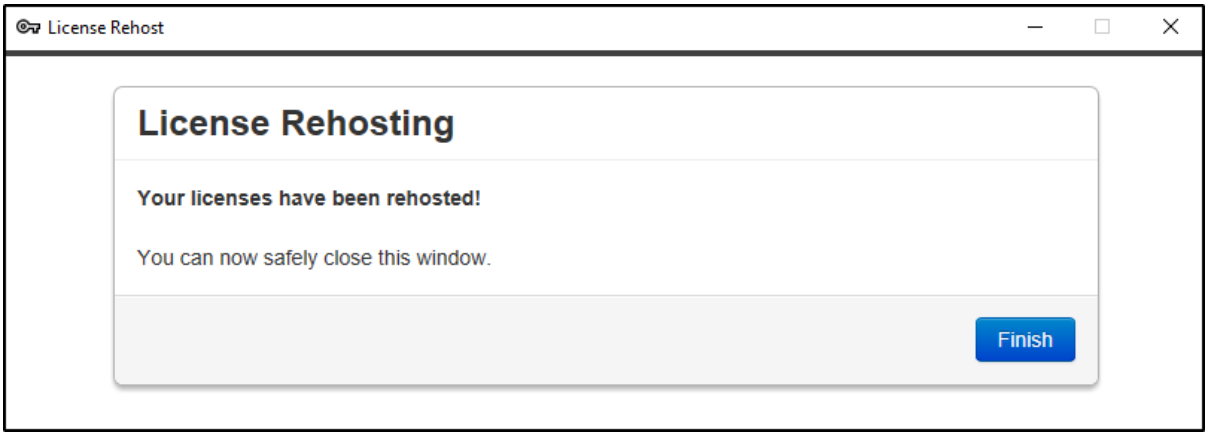
재호스팅할 초기 컴퓨터를 선택하세요.



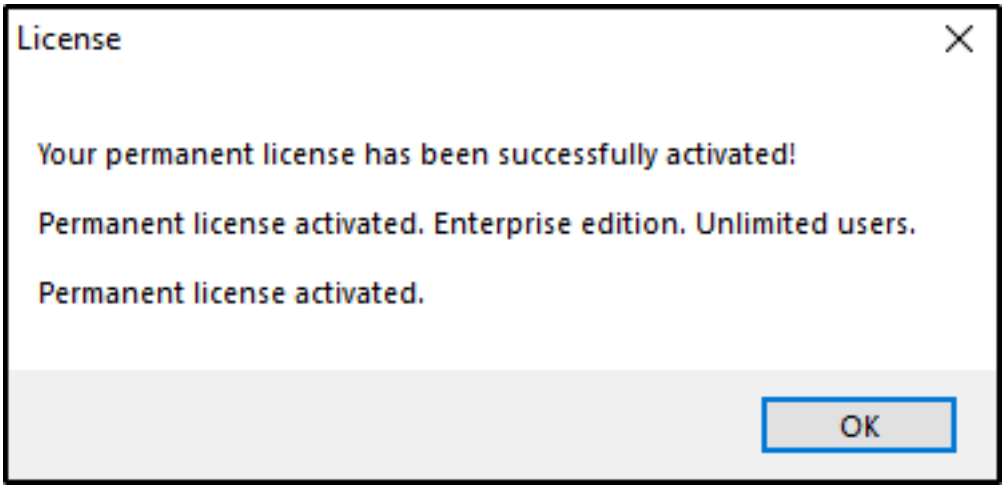
재호스팅 확인



라이선스 재호스팅이 완료되었습니다.

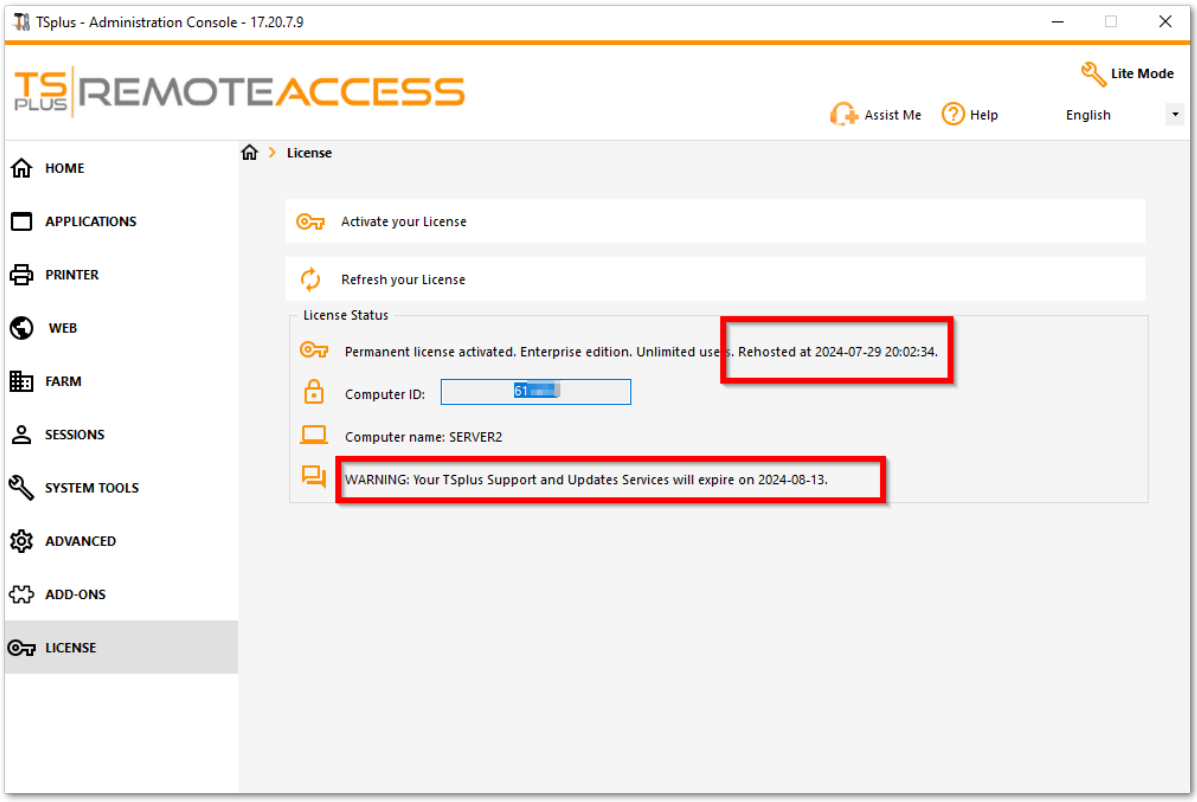


잠시 기다려 주십시오. AdminTool이 동기화되어 창이 나타날 때까지 기다려 주십시오.



라이센스가 성공적으로 활성화되었습니다!

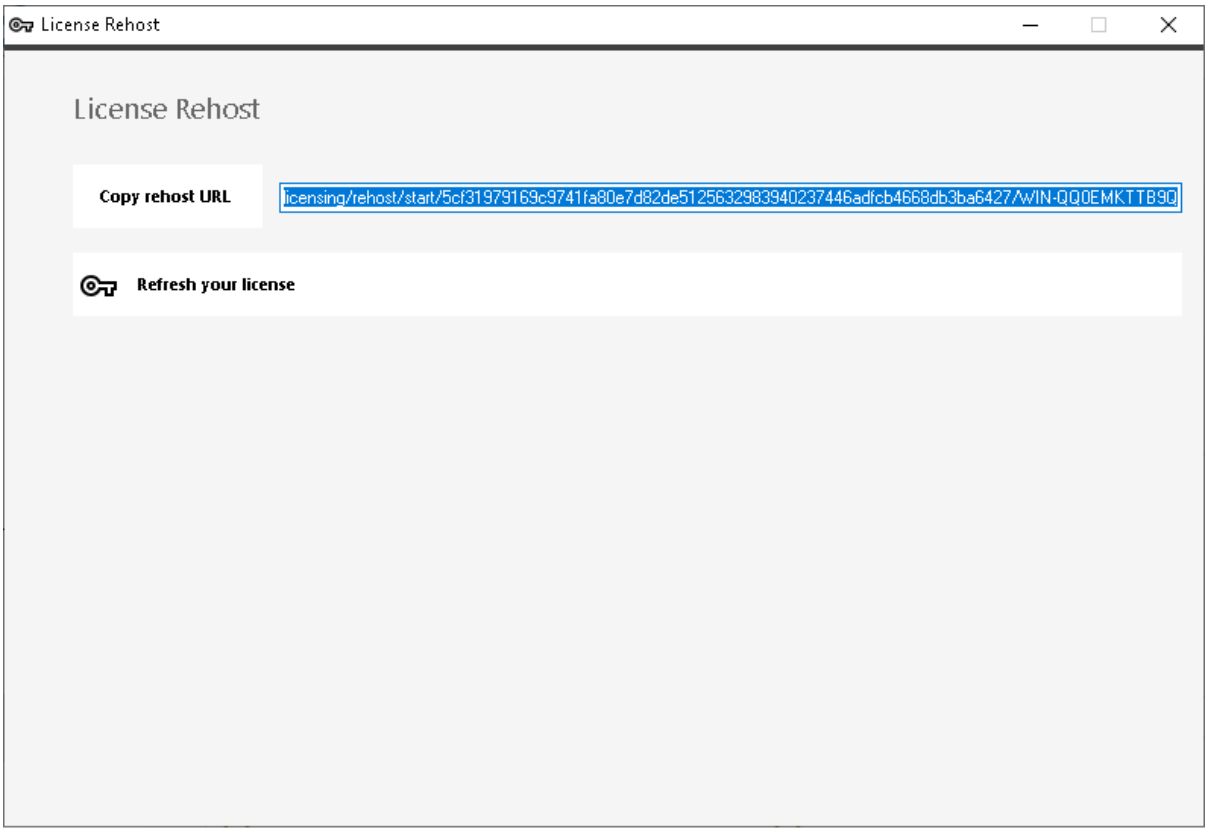
노트: 재호스팅 날짜와 사용 종료 날짜가 포함된 메시지가 이전 서버에 표시됩니다. 재호스팅 후에도 이전 서버는 여전히 작동합니다. **15일** 전환을 도와드리기 위해.



오프라인 재호스팅

오프라인 활성화는 재호스팅 라이센스에 대해서도 수행할 수 있습니다.

서버에 인터넷 연결이 없을 때, '기존 라이선스 재호스팅' 버튼이 오프라인 재호스팅 페이지를 표시합니다:



오프라인 활성화와 동일한 프로세스입니다.

iPhone / iPad / Android 기기에서의 원격 연결

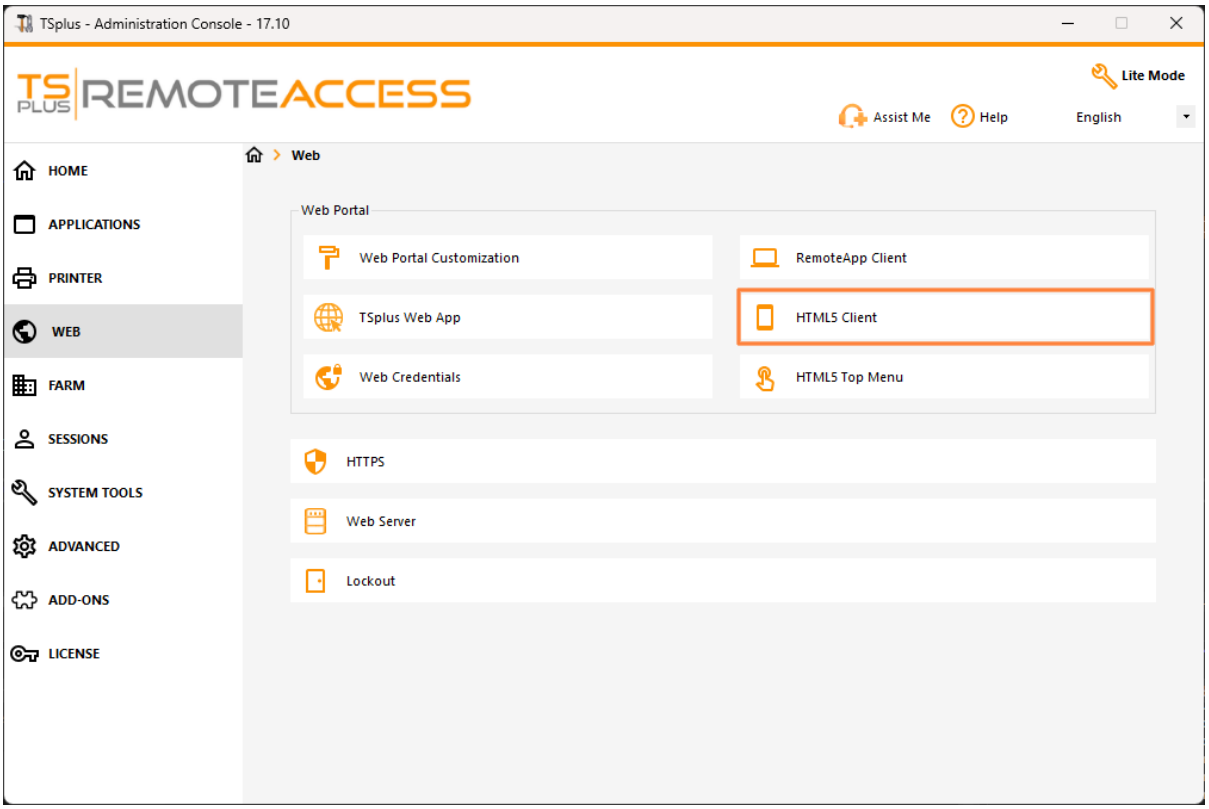
모바일 장치에서 HTML5 기술을 지원하는 모든 브라우저를 통해 Terminal Service Plus 서버에 연결할 수 있습니다.

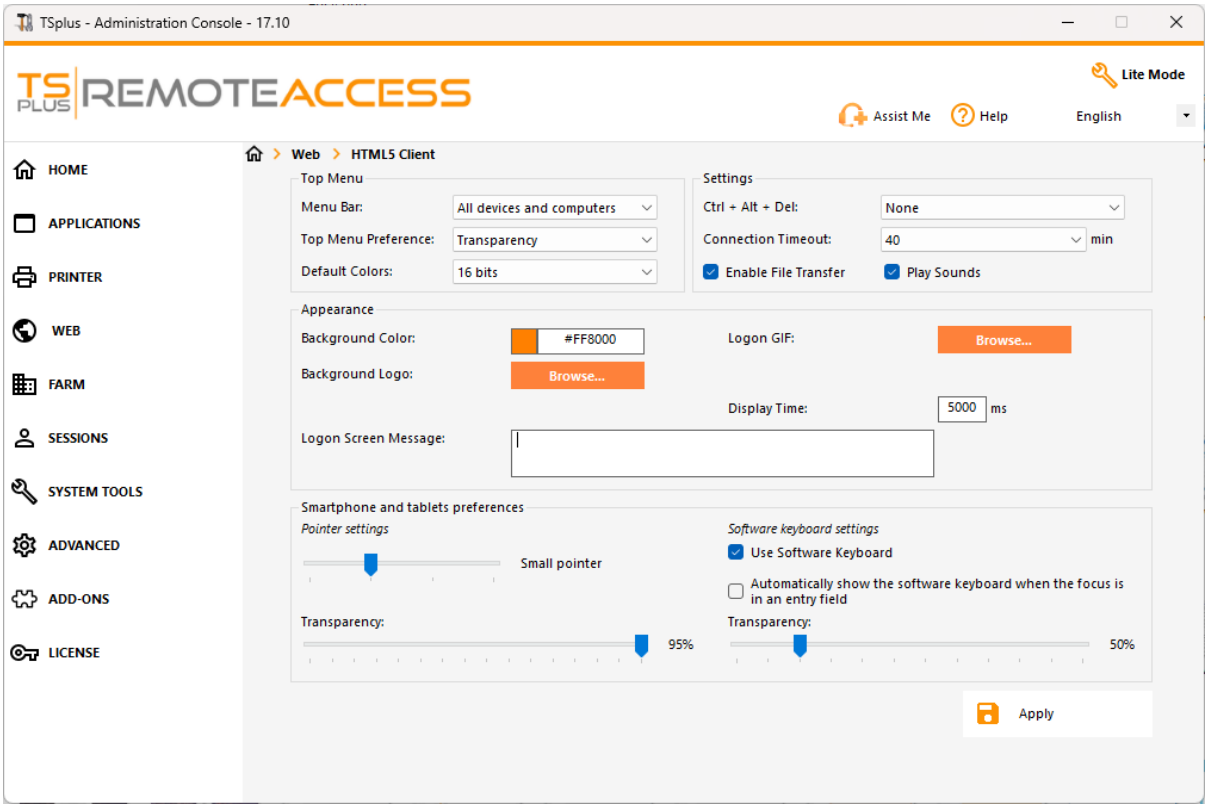
- 아이폰
- 아이패드
- 안드로이드 스마트폰
- 안드로이드 태블릿

모바일 장치에 대한 기본 설정을 편집하십시오.

11.20 버전 출시 이후, TSplus HTML5 클라이언트는 스마트폰이나 태블릿에서도 최상의 사용자 경험을 제공하기 위해 크게 향상되었습니다. 키보드는 입력 필드에 포커스가 있을 때 자동으로 팝업되도록 재설계되었습니다. 마우스 포인터는 버튼과 필드를 선택하기 쉽게 재설계되었으며, 스마트폰의 왼쪽 또는 하단 경계에 위치해 있어도 가능합니다.

모바일 장치나 컴퓨터에 대한 다양한 HTML5 설정을 Web Tab의 HTML5 클라이언트 타일에서 설정할 수 있습니다.





- 모든 장치와 컴퓨터 또는 모바일 장치에 대해서만 메뉴 바를 표시합니다.
- 파일 전송 활성화 또는 비활성화.
- 특정 유형의 장치에서 Ctrl + Alt + Del 단축키를 허용합니다.
- 투명성과 불투명성 사이에서 좋아하는 상단 메뉴 표시를 선택하세요.
- 그래픽 색상 비트 수.

- 연결 시간 초과, 클라이언트가 다시 연결하기를 기다리는 동안 세션이 활성 상태로 유지되는 최대 기간(초). 0은 시간 초과를 비활성화합니다.
- 경고 메시지 표시 또는 숨기기.
- 소리를 활성화하거나 비활성화합니다.
- 가장 좋아하는 배경 색상을 선택하세요.
- 배경에 로고를 추가하세요.
- 로그온 화면 메시지와 애니메이션 GIF, 그리고 밀리초 단위의 표시 시간을 변경합니다.

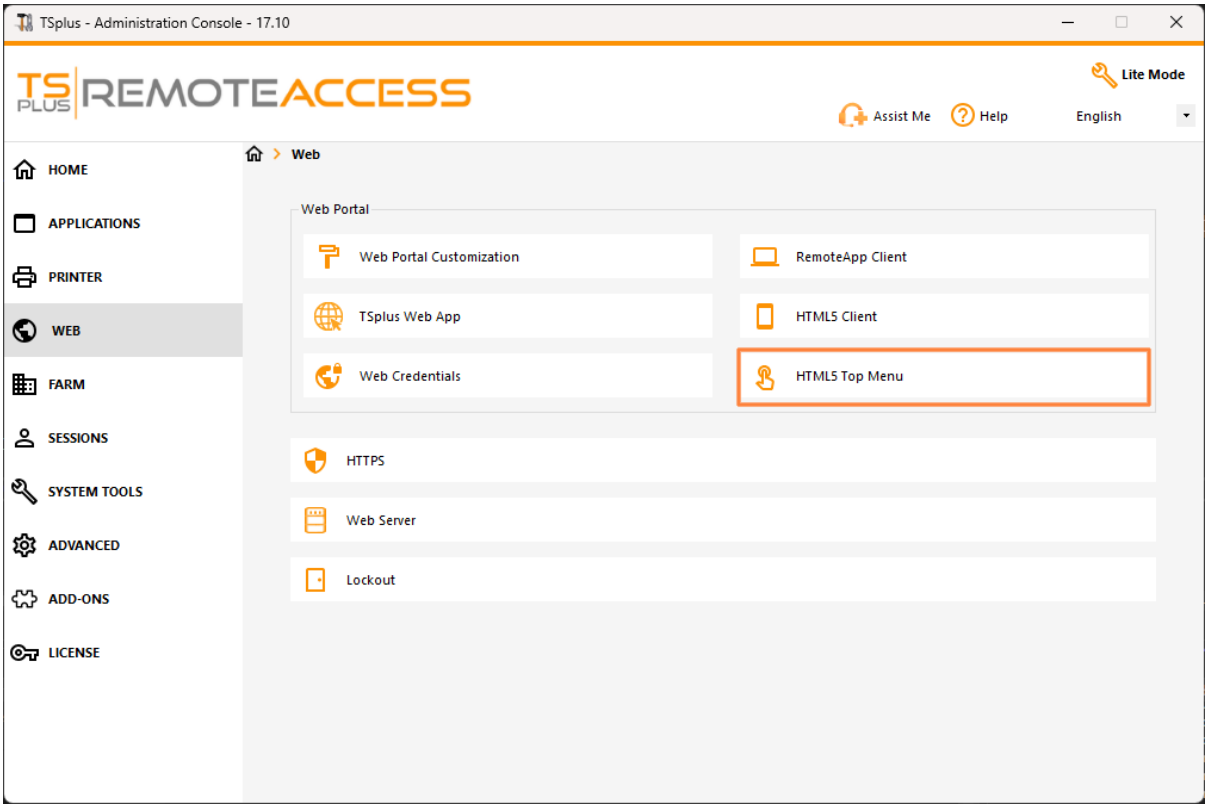
스마트폰 및 태블릿 기본 설정 :

- 관리자가 소프트웨어 키보드를 사용하는 경우, 입력 필드가 숨겨질 때 애플리케이션이 위로 이동하며 사용자는 여전히 입력하고 있는 내용을 볼 수 있습니다.

- 관리자는 마우스 포인터의 크기를 작게, 중간으로 또는 크게 선택하거나 아예 마우스 포인터를 사용하지 않을 수 있습니다. 이는 사용자가 자신의 애플리케이션 내에서 직관적으로 탐색할 수 있도록 합니다.

- 그는 마우스와 키보드의 투명도 수준도 선택할 수 있습니다.

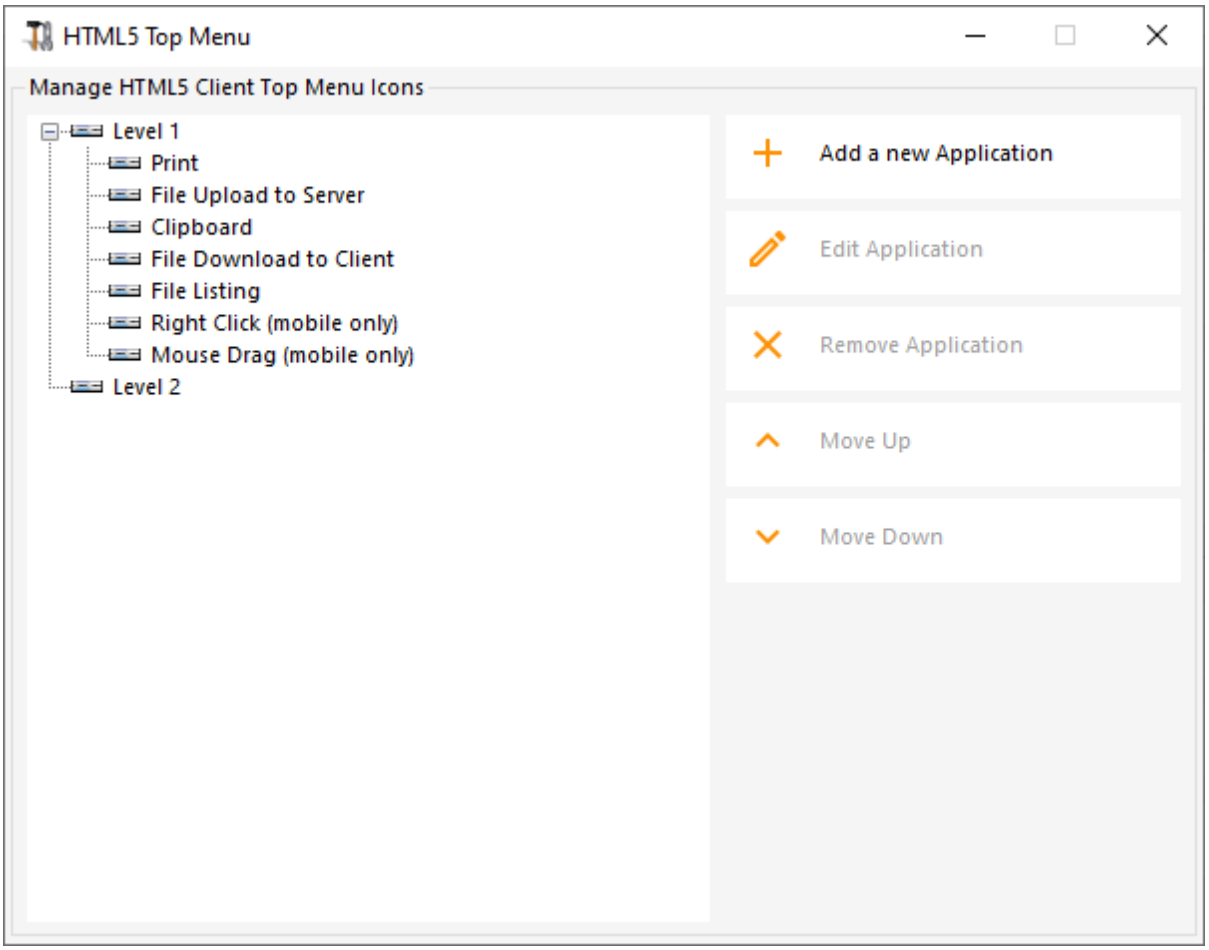
HTML5 상단 메뉴 탭에서 HTML5의 상단 메뉴 첫 번째 또는 두 번째 수준에 표시될 애플리케이션을 추가할 수 있습니다.



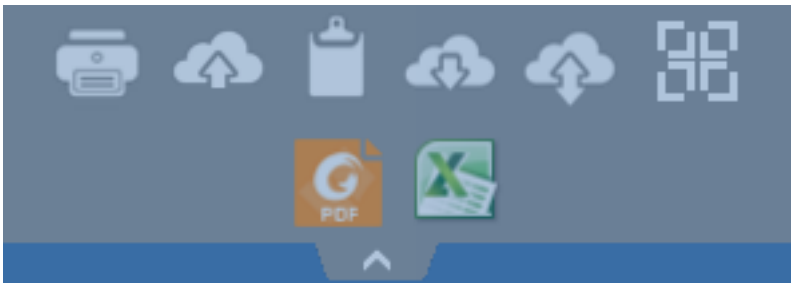
1단계에서는 통합된 HTML5 기능인 인쇄, 파일 전송 및 클립보드를 찾을 수 있습니다. (이 기능에 대한 자세한 정보는 이 페이지로 이동하세요:)

HTML5용 유니버설 프린터 , 파일 전송 사용 그리고 클립보드 사용 .)

이 예에서 Foxit과 Excel은 2단계에 게시됩니다:



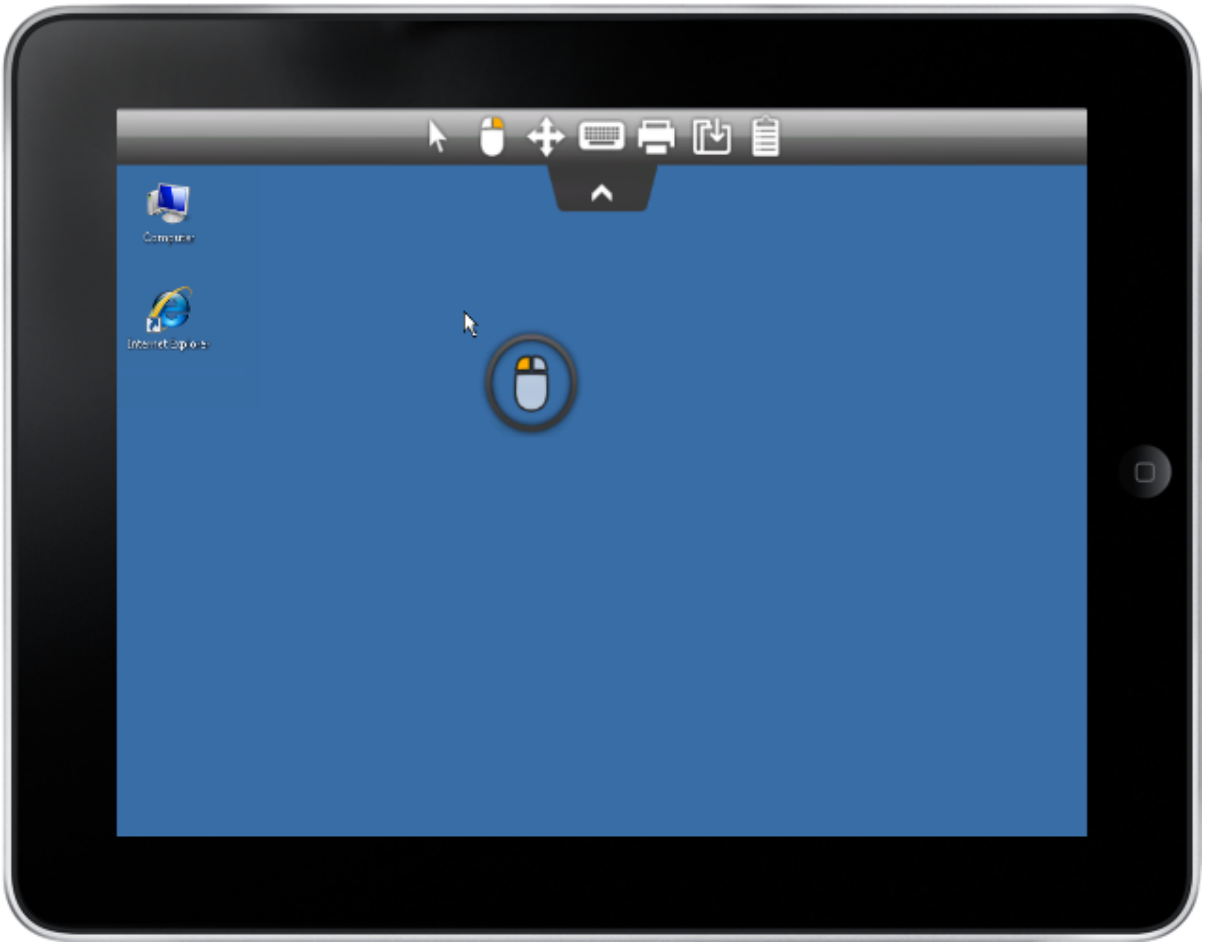
통합 기능에서 HTML5 세션의 상단 메뉴 아래에서 찾을 수 있습니다.



또한, 오른쪽 상단 아이콘을 사용하여 세션을 전체 화면으로 전환할 수 있습니다.

터미널 서비스 플러스 내장 HTML5 클라이언트 사용자에게 태블릿과 모바일 장치에서 완전히

새로운 메뉴를 제공합니다. 이 새로운 메뉴를 통해 사용자는 모바일 키보드와 오른쪽 클릭에 쉽게 접근할 수 있을 뿐만 아니라 파일 공유 및 우리의 독특한 유니버설 프린팅 기능에도 접근할 수 있습니다!



참조해 주십시오 이 문서 미니 마우스와 키보드 사용 방법에 대한 내용입니다.

언어 선택

이제 상단 메뉴 오른쪽의 언어 버튼으로 언어를 변경할 수 있습니다:



이 메뉴에서 원하는 특정 국가의 언어를 선택할 수 있습니다:

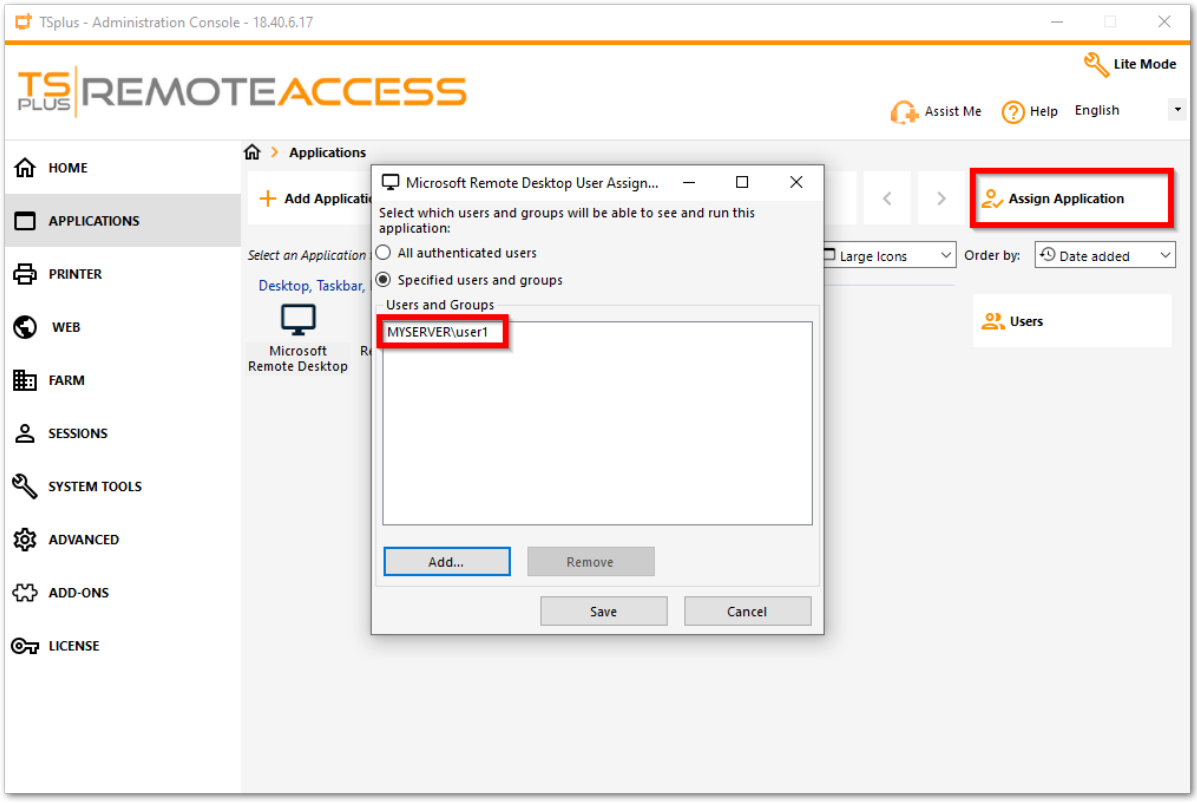
	Language	Locale	Value
◯	Portal	as_portal	
◯	Browser	as_browser	
◯	Gateway	as_gateway	
◯	Arabic	ar_ar	1025
◯	Belarusian	be_be	1059
◯	Bulgarian	bg_bg	1026
◯	Bengali	bn_bn	1093
◯	Bosnian (Cyrillic)	bs_cyrl_ba	8218
◯	Bosnian (Latin)	bs_latn_ba	5146
◯	Catalan	ca_ca	1027
◯	Czech	cs_cs	1029
◯		cs_cz	1029
◯	Welsh	cy_gb	1106
◯	Danish	da_da	1030
◯		da_dk	1030
◯	German (Swiss)	de_ch	2055
◯	German	de_de	1031
◯	Divehi	dv_dv	1125
◯	Greek	el_el	1032
◯		el_gr	1032
◯	English (Canada)	en_ca	4105

원격 작업 표시줄 및 바탕화면 테마

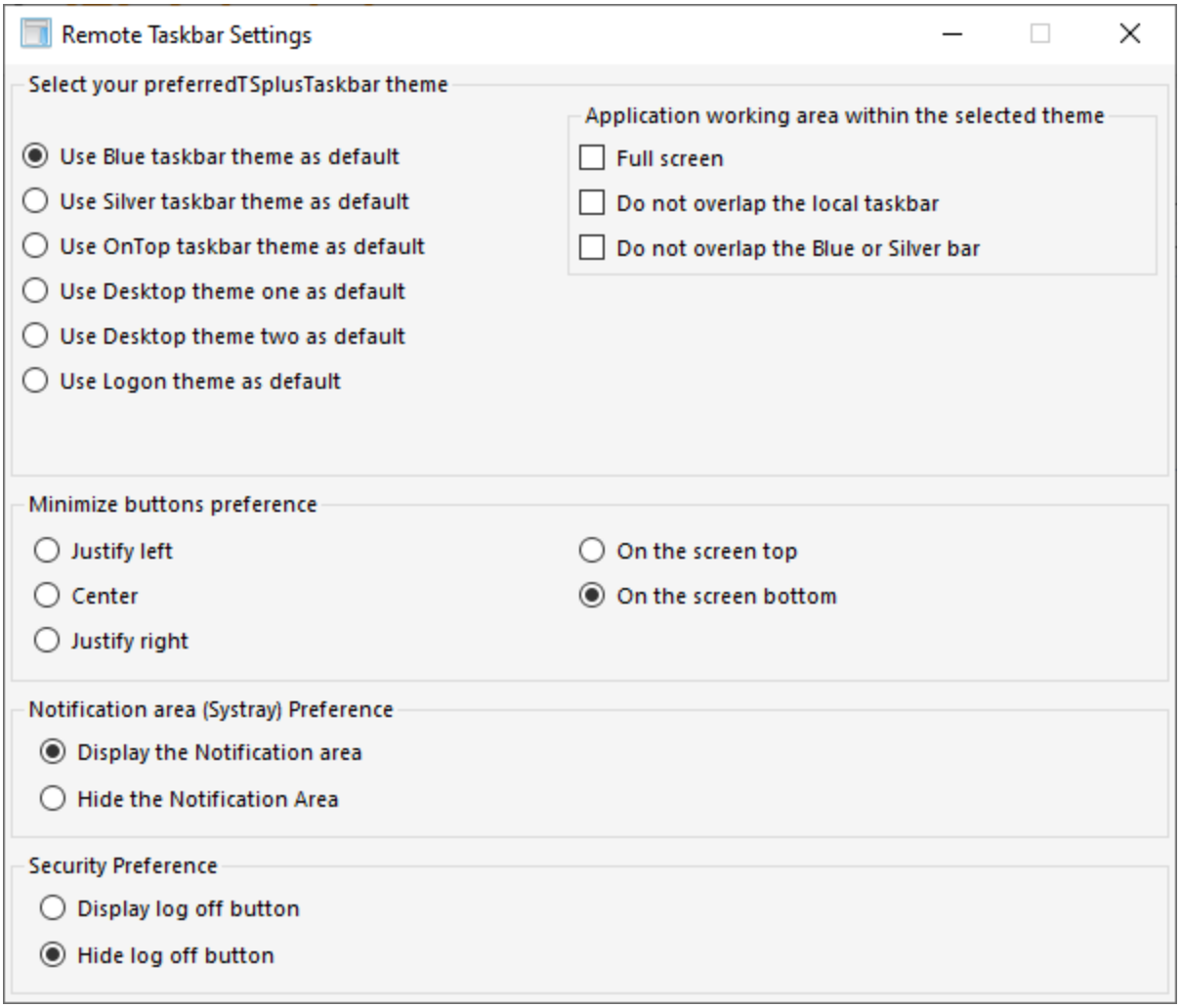
서버의 관리자 도구

관리자 도구를 사용하면 관리자가 애플리케이션을 할당할 때 4가지 표시 모드 중에서 선택할 수 있습니다. 마이크로소프트 원격 데스크톱 , 원격 작업 표시줄 , 플로팅 패널 또는 응용 프로그램 패널 원격 작업 표시줄, 플로팅 및 애플리케이션 패널은 모든 연결 방법에서 사용할 수 있습니다.

사용자에게 애플리케이션을 할당할 때 TSplus 원격 작업 표시줄을 활성화할 수 있습니다. 사용자는 TSplus 작업 표시줄에서 한 번의 클릭으로 원격 애플리케이션을 실행할 수 있으며 여전히 전체 로컬 데스크탑을 사용할 수 있습니다. 원격 작업 표시줄을 사용자나 그룹에 할당하려면 두 번 클릭하거나 선택한 다음 "애플리케이션 할당" 타일을 클릭하면 됩니다.



관리자는 사용자가 세션을 열 때 볼 기본 원격 데스크톱 테마를 쉽게 결정할 수 있습니다. TSplus 원격 작업 표시줄을 선택한 다음 "응용 프로그램 편집"을 클릭하십시오.

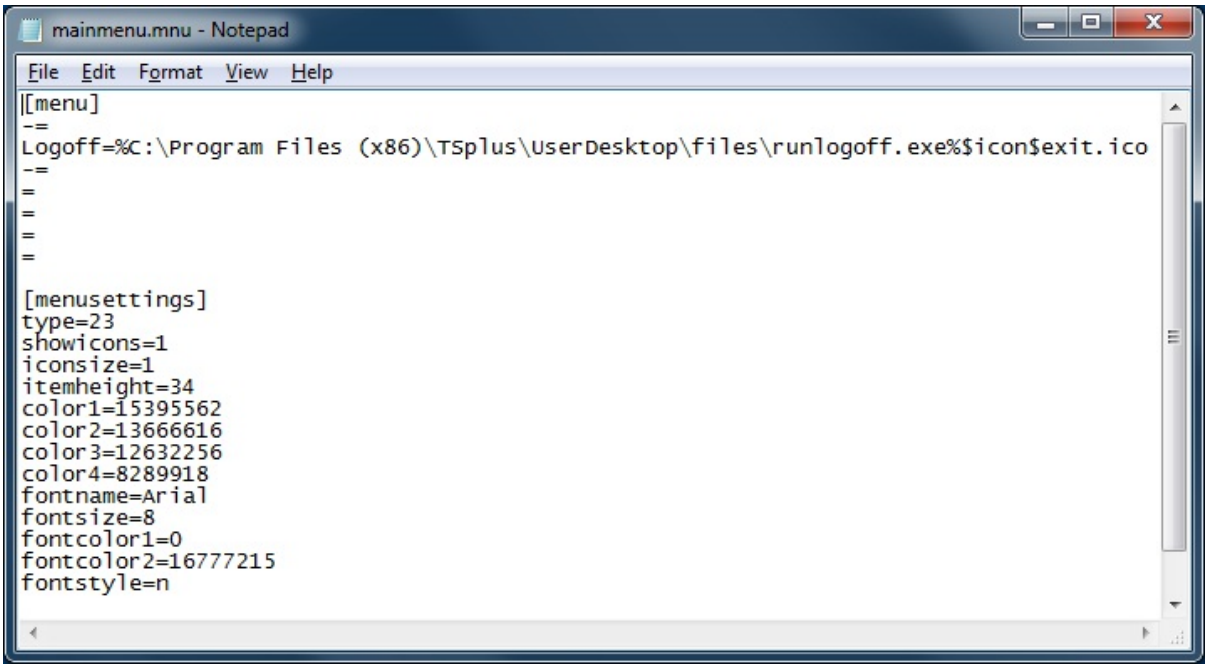


- 관리자만 자신의 사용자에 대한 테마를 선택할 수 있습니다.
- 그는 최대화된 애플리케이션을 전체 화면 모드로 표시하거나 TSplus 작업 표시줄과 Silver 또는 Blue 작업 표시줄이 겹치지 않도록 선택할 수 있습니다.
- 작업 표시줄의 최소화된 버튼 위치는 변경할 수 있습니다(화면 상단, 하단, 오른쪽, 왼쪽 또는 중앙).

  관리자는 기본 하단 대신 사용자 화면 상단에 표시하도록 결정할 수도 있습니다.
- Systray 아이콘은 “알림 영역 숨기기” 원을 선택하여 숨길 수 있습니다.
- TSplus 12.60 버전부터 로그오프 버튼을 숨길 수 있습니다.

사용자 메뉴를 편집함으로써 관리자는 애플리케이션과 기능을 추가/제거할 수 있습니다. 사용자 메뉴의 맞춤화는 쉽습니다.

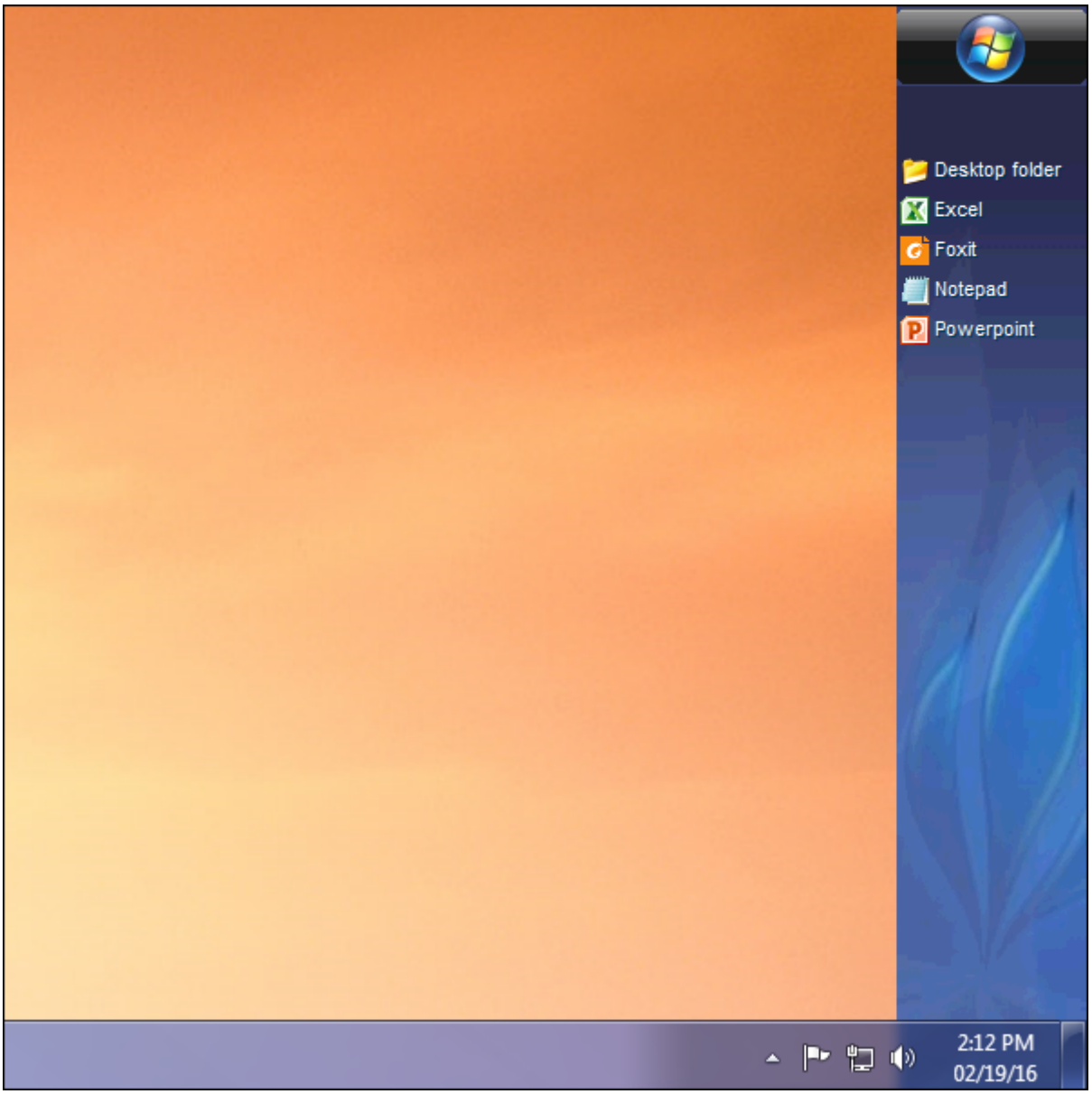
사용자 메뉴의 내용(Program Files/TSplus/UserDesktop/mainmenu.mnu에 위치)은 관리자가 메모장을 사용하여 수정할 수 있습니다.



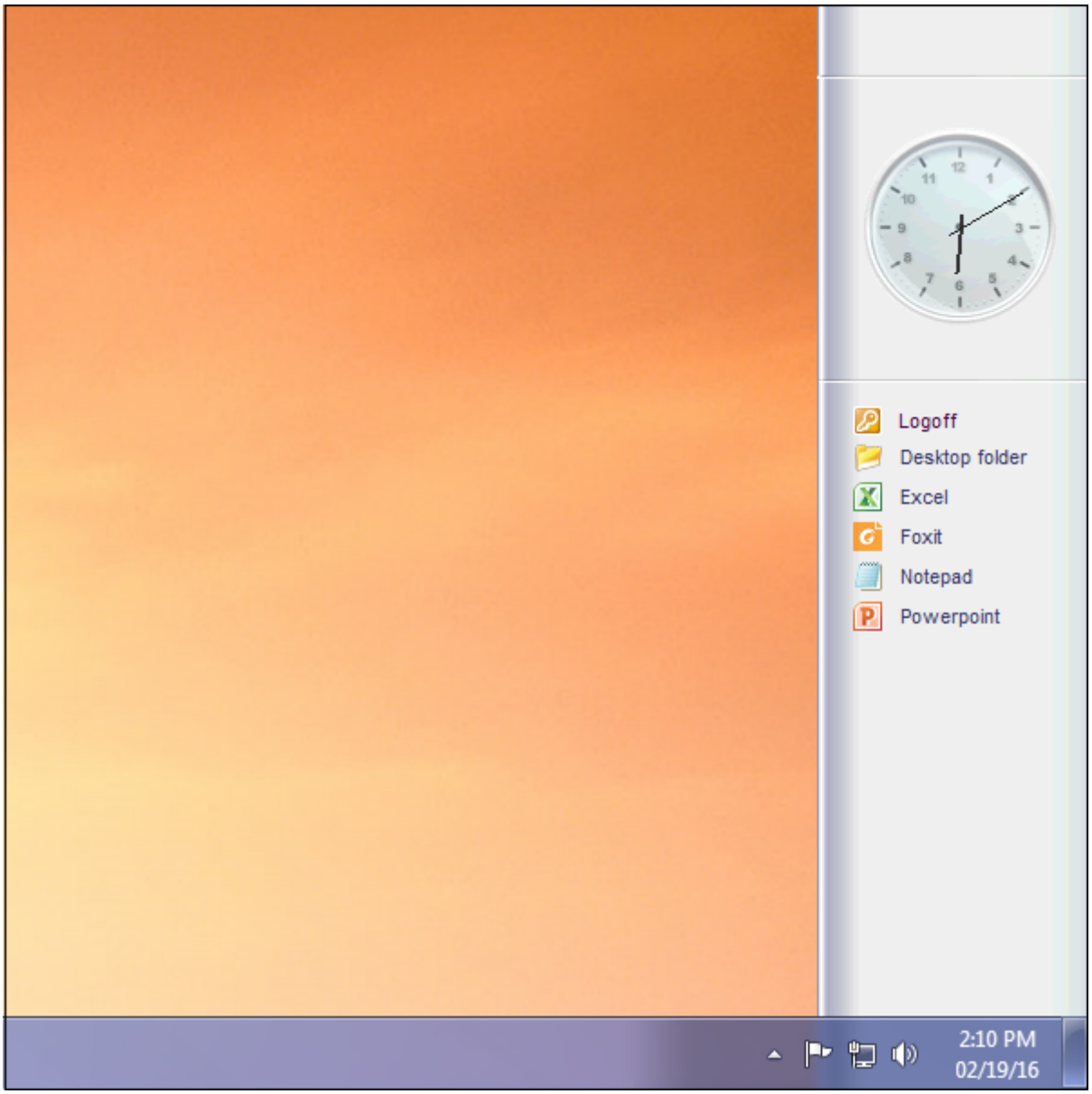
관리자 도구의 애플리케이션 타일에서 관리자는 3가지 다른 스타일의 원격 데스크탑 TSplus 작업 표시줄을 선택할 수 있습니다.

사용자는 TSplus 작업 표시줄에서 한 번의 클릭으로 원격 애플리케이션을 실행할 수 있으며 여전히 전체 로컬 데스크탑을 사용할 수 있습니다.

오른쪽 파란색 테마 작업 표시줄



오른쪽 실버 테마 작업 표시줄



상단 작업 표시줄



위로 가기

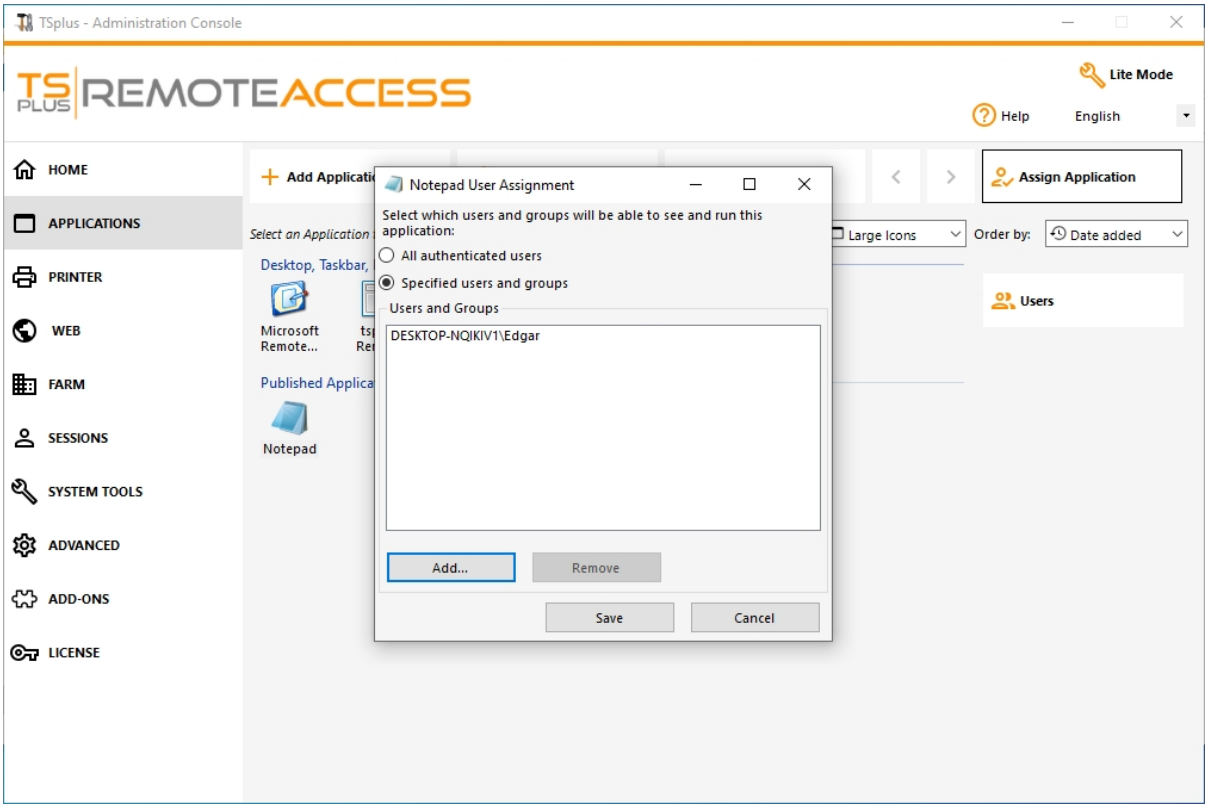
AdminTool을 사용하면 관리자가 사용자가 세션을 열 때 볼 기본 Remote Desktop 테마를 쉽게 결

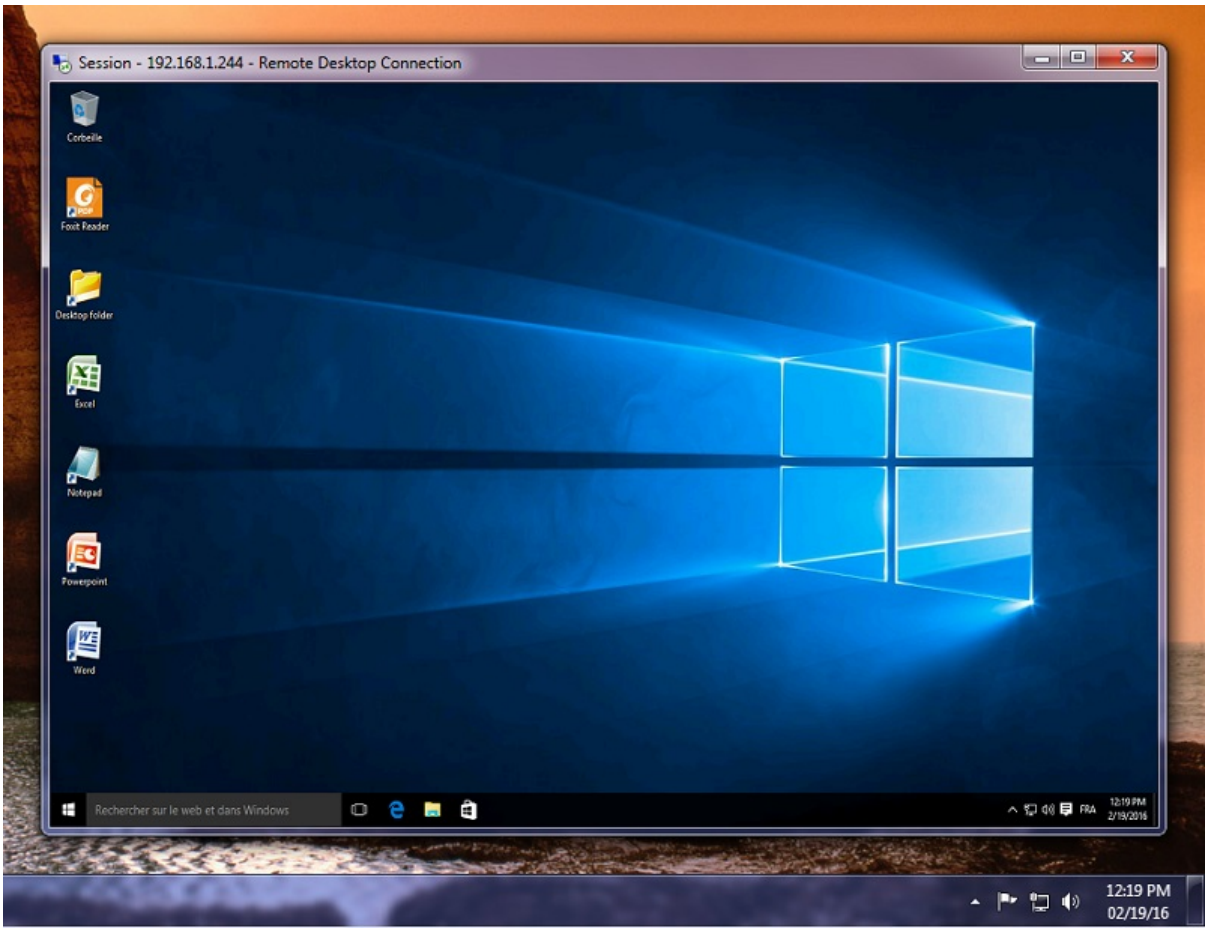
정할 수 있습니다. 그는 전체 화면 Remote Desktop의 4가지 다른 스타일 중에서 선택할 수 있습니다. 표준 Microsoft Remote Desktop도 선호하는 경우 사용할 수 있습니다.

이 TSplus 데스크탑은 전체 화면 데스크탑이기 때문에, 전용 얇은 클라이언트, RDP 기반 클라이언트 또는 웹 페이지나 TSplus 원격 데스크탑 클라이언트에서 세션이 열릴 때 사용자의 디스플레이가 완전히 채워집니다.

표준 원격 데스크톱에 대한 이점이 있습니다. 서버 보안을 강화합니다(시작 버튼이나 데스크톱의 전체 제어가 없습니다).

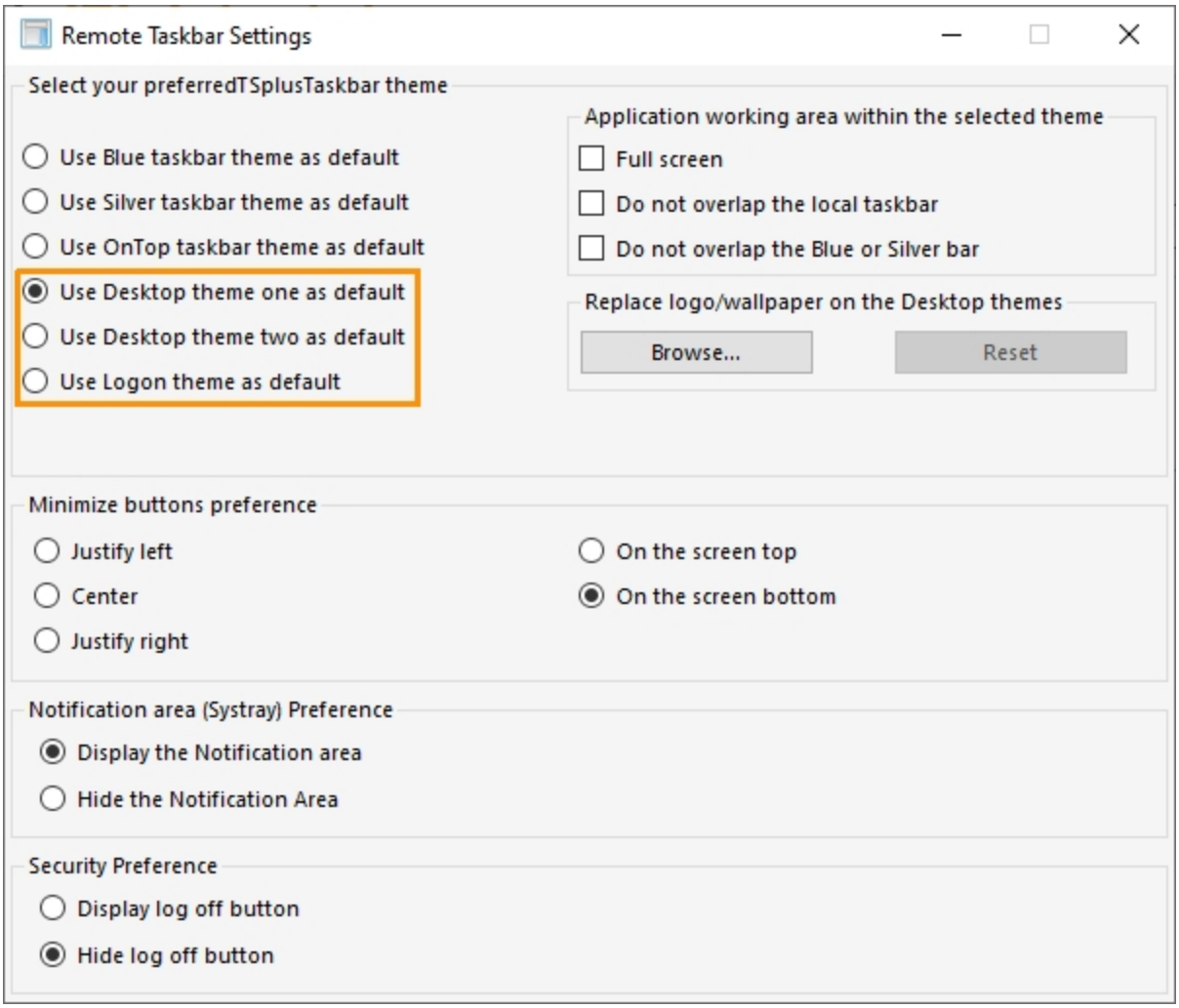
표준 Microsoft 원격 데스크톱





- 사용자는 시작 버튼과 데스크탑에 대한 완전한 제어를 포함한 전체 데스크탑을 가지고 있습니다.
- 완전한 데스크톱에 할당하려면 Microsoft Remote Desktop 애플리케이션을 할당하면 됩니다.

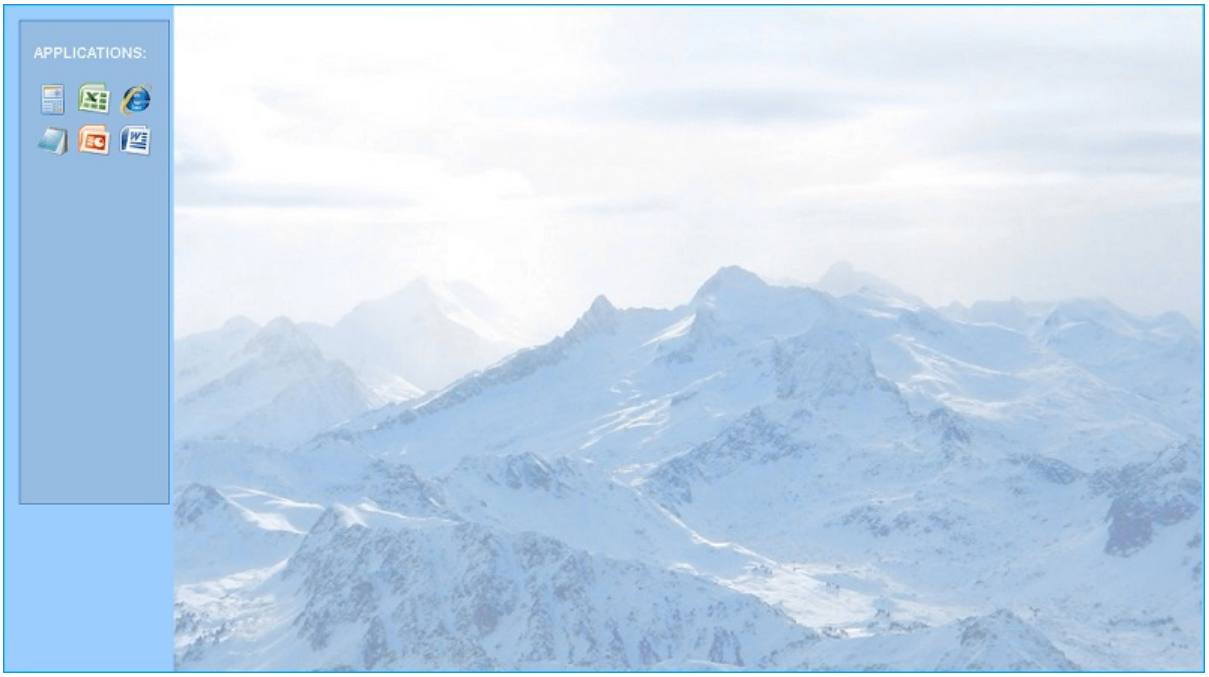
바탕 화면 테마를 변경하려면 TSplus Remote Taskbar를 할당하고 제안된 3가지 테마 중에서 선택해야 합니다.



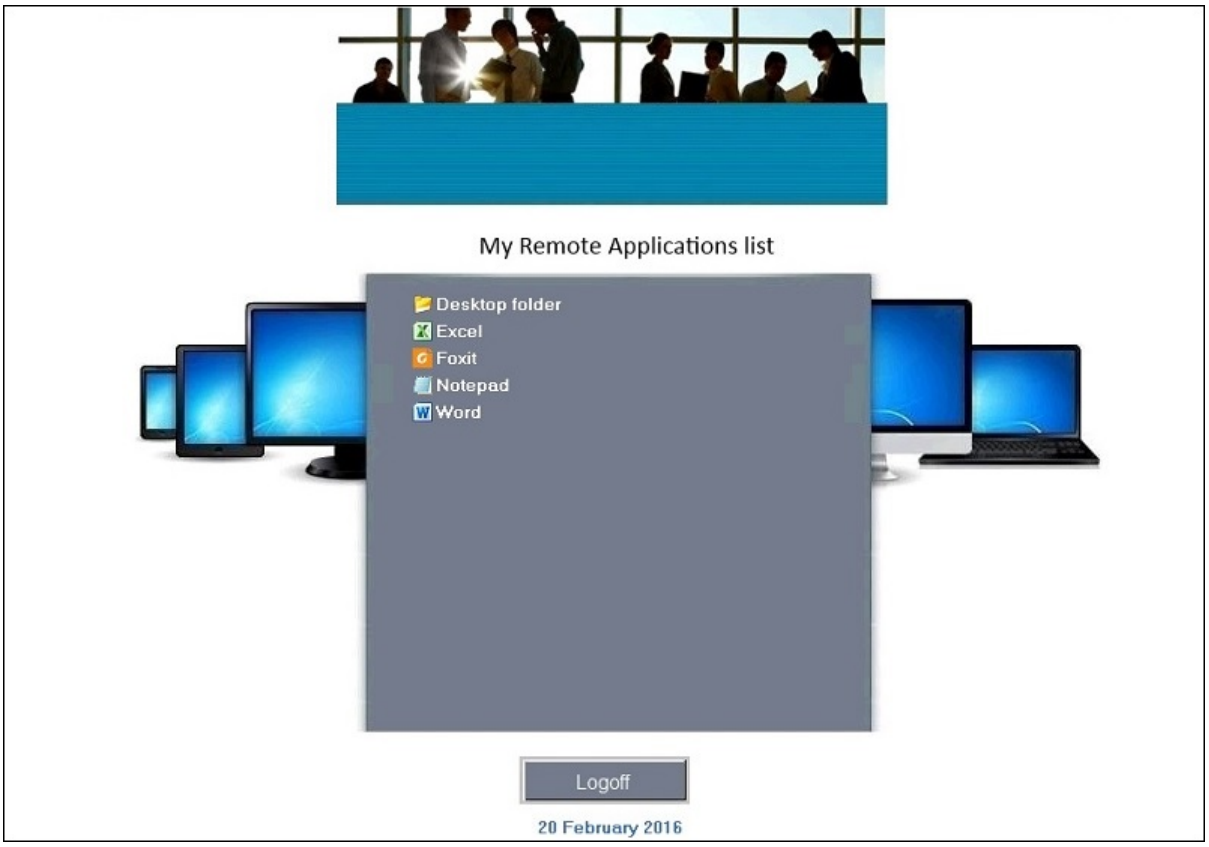
TSplus 데스크탑 테마 하나



TSplus 데스크탑 테마 두



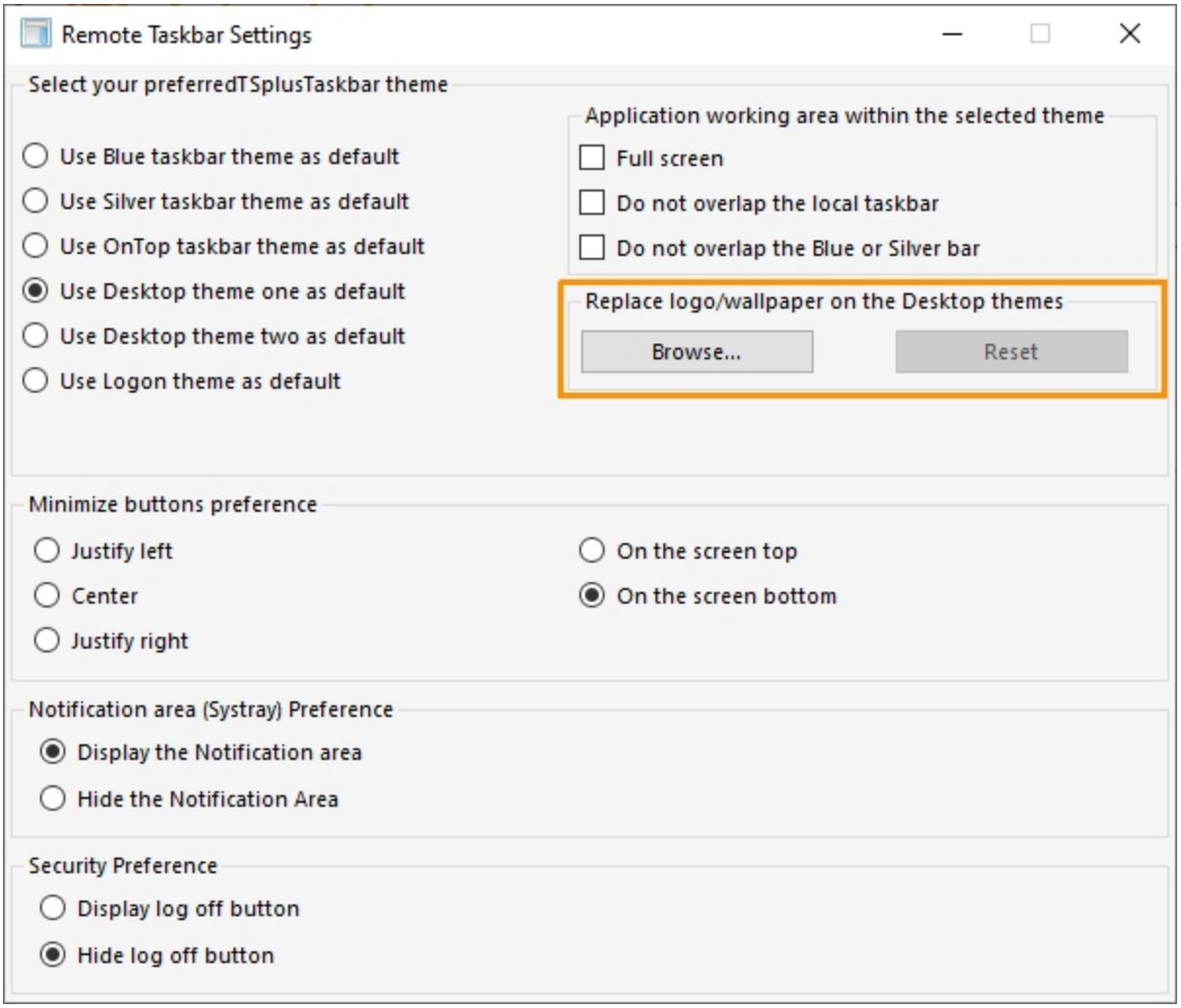
TSplus 로그인 테마



맞춤형 테마

각 테마에 대해 관리자는 이를 사용자 정의할 수 있으며, 예를 들어 기업 로고를 표시할 수 있습니

다. 그는 또한 데스크탑 테마 중 하나를 선택하고 로고/배경화면 교체 버튼을 클릭하여 자신의 데스크탑 배경화면을 추가할 수 있습니다. 예를 들어 .jpg 파일을 선택할 수 있습니다.



- 바탕화면 테마 중 하나를 선택하고 교체 로고/배경화면 버튼을 클릭하여 .jpg 파일을 선택하면 자신만의 바탕화면 배경을 추가할 수 있습니다.


APPLICATIONS:
15 June 17

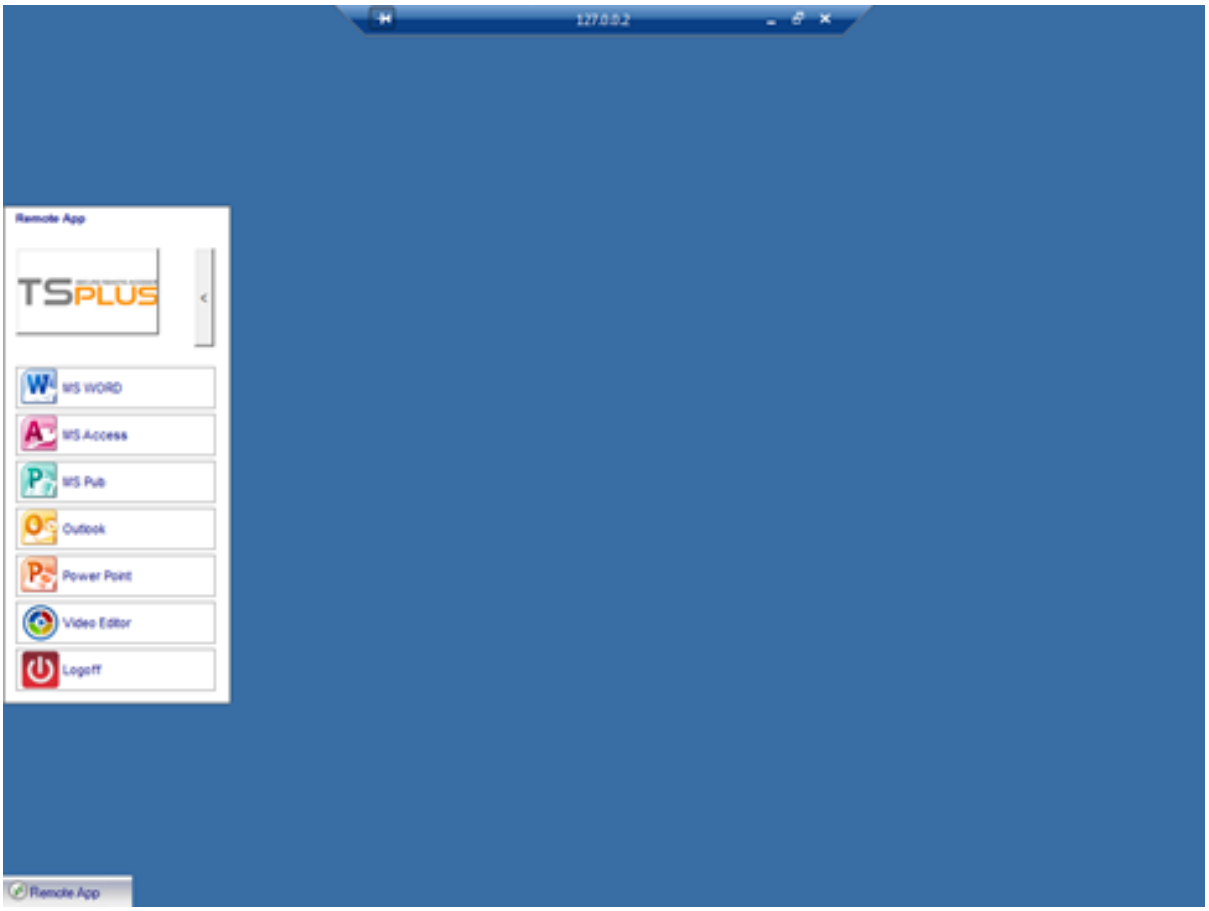
클라이언트의 RemoteApp 기능

과거에 생성된 TSplus Portable 클라이언트는 사용자가 애플리케이션을 시작하는 일반적인 방법이었습니다. 10.50 릴리스는 도입합니다. **알림 영역의 아이콘** 각 사용자에게 모든 원격 애플리케이션 목록을 제공합니다. 이 애플리케이션 목록 내에서 사용자는 시작할 애플리케이션을 선택할 수 있습니다.

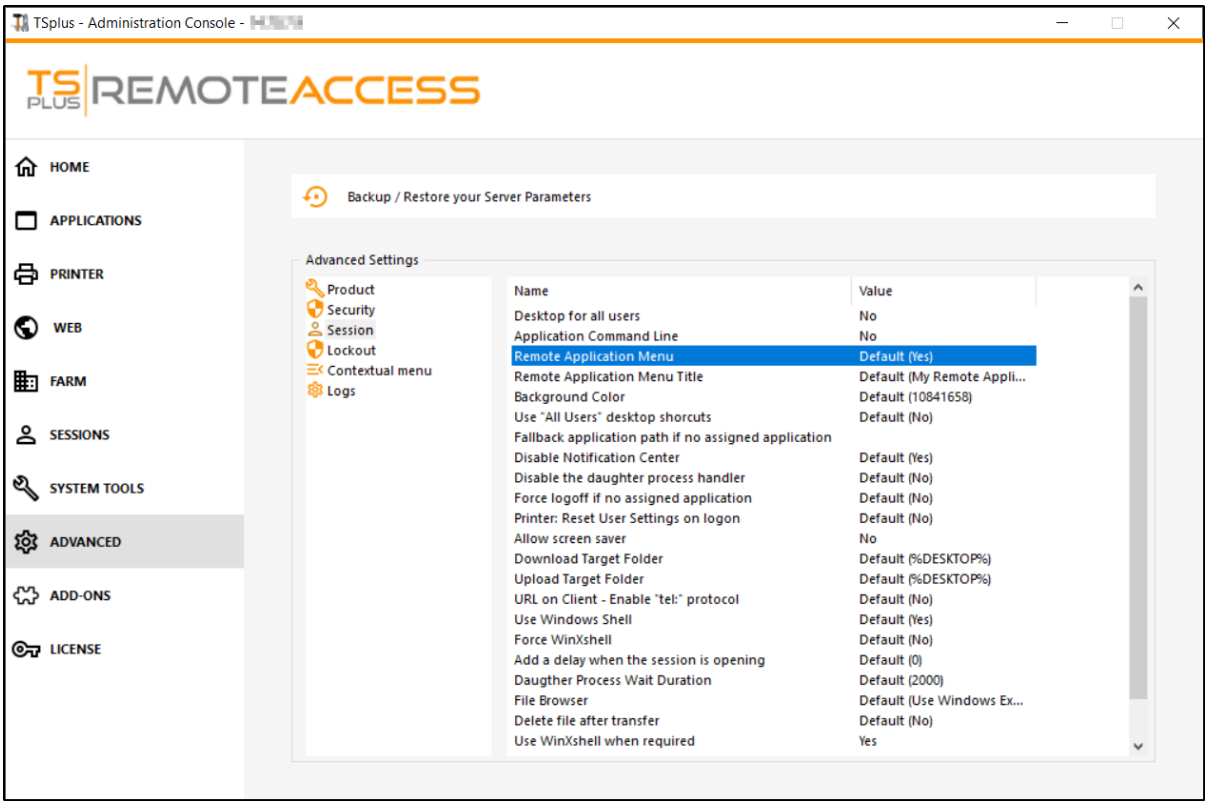
관리자가 사용자에게 원격 애플리케이션(“RemoteApps”라고 함)을 제공하는 새로운 방법입니다. 특히, 클라이언트에서 RemoteApp은 서버에 직접 설치된 애플리케이션을 사용자에게 제공할 수 있는 간단한 게시 프로세스를 가능하게 하며, RemoteApp 프로그램이 로컬 프로그램과 나란히 실행될 수 있도록 하고, 사용자가 RemoteApp 프로그램을 쉽게 찾고 실행할 수 있도록 맞춤형 “런처” 애플리케이션과의 통합을 제공합니다.

사용자 애플리케이션 목록도 나타납니다. **시작 메뉴** 아래 **모든 프로그램** 폴더에 있는 **내 원격 애플리케이션** 이 새로운 놀라운 TSplus 기능을 배포하는 것은 간단합니다: 관리자가 새로운 연결 클라이언트를 생성하고 AdminTool을 통해 이를 허용했습니다. 이 가이드는 관리자가 이 새로운 기능을 활성화할 때 어떤 일이 발생할지 단계별로 설명하고, 사용자에게 새로 생성된 연결 클라이언트를 제공할 것입니다.

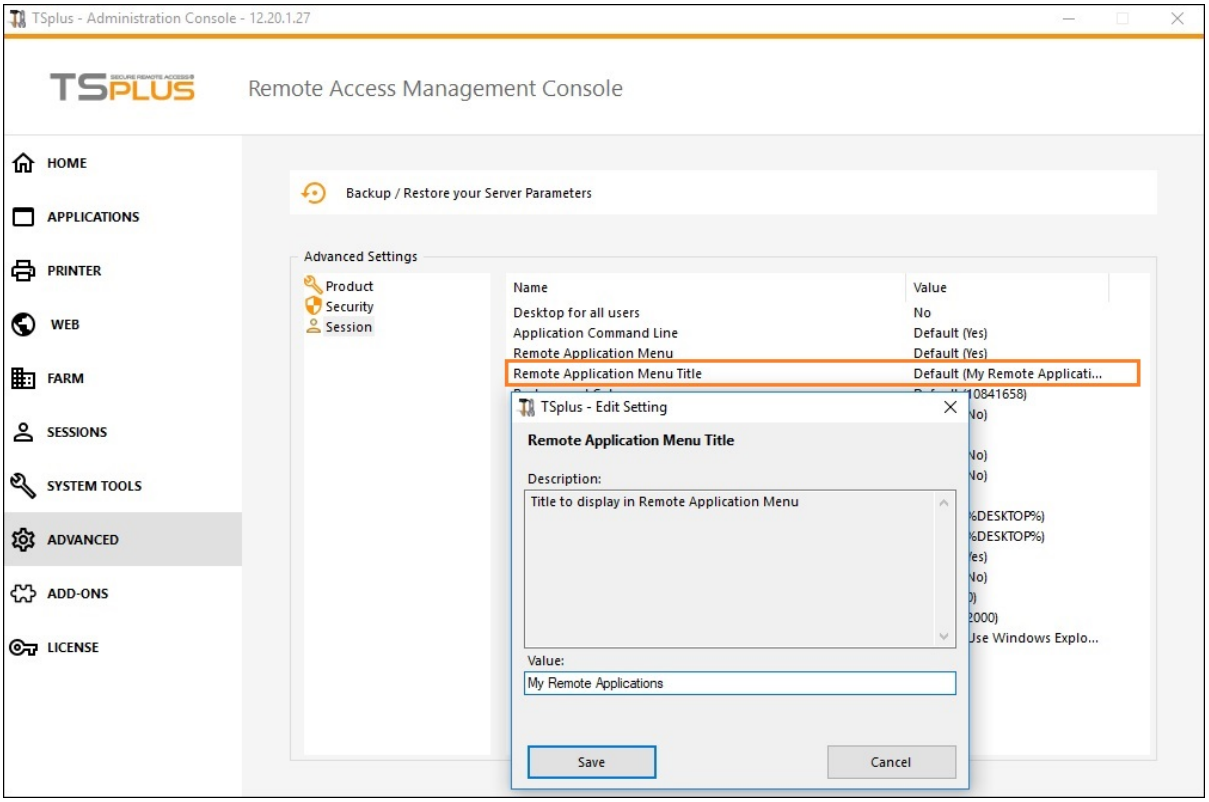
사용자 "Laura"는 TSplus를 사용하여 원격 애플리케이션에 접근하고 있습니다. 이를 위해 그녀는 생성된 클라이언트 이름을 사용하고 있습니다. **LauraPortableClient.exe** 그녀가 자신의 PC에서 실행할 때 다음과 같은 결과를 얻습니다:



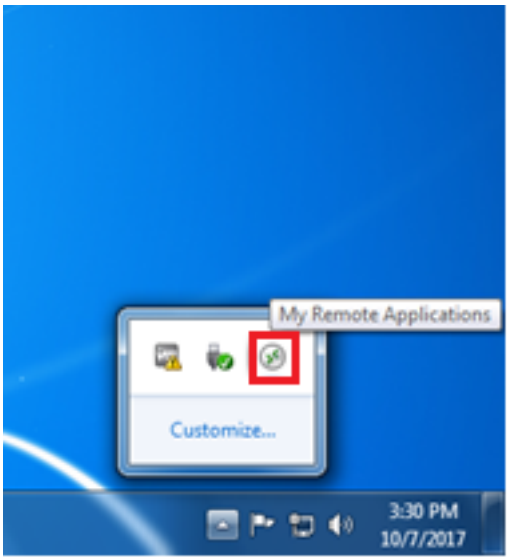
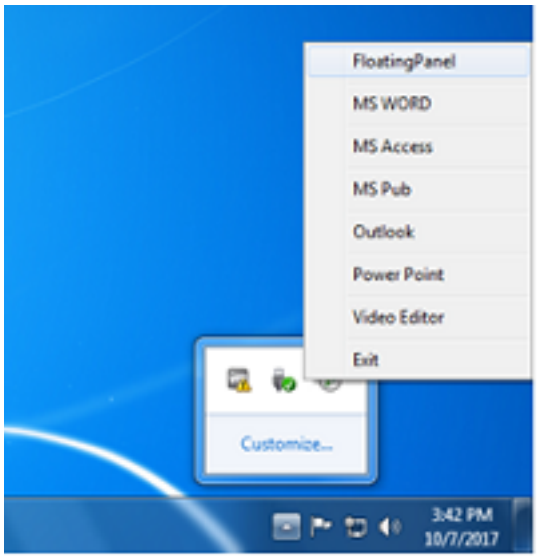
그러나 관리자는 그녀에게 TSplus 10.50 릴리스로 생성된 새로운 것을 제공했습니다. 그녀는 새로운 기능을 활용하기 위해 최소한 한 번 실행해야 합니다. **클라이언트의 RemoteApp 기능** 관리자가 사용자에게 애플리케이션을 추가하거나 제거할 때, 이러한 변경 사항은 다음 로그인 시 서버 측에 설정됩니다. 이는 현재 세션이 이러한 수정 사항을 반영하지 않음을 의미합니다. AdminTool의 고급 탭에는 기본적으로 활성화되어 있는 이 RemoteApp On Client 기능을 활성화하거나 비활성화하는 옵션이 있습니다.



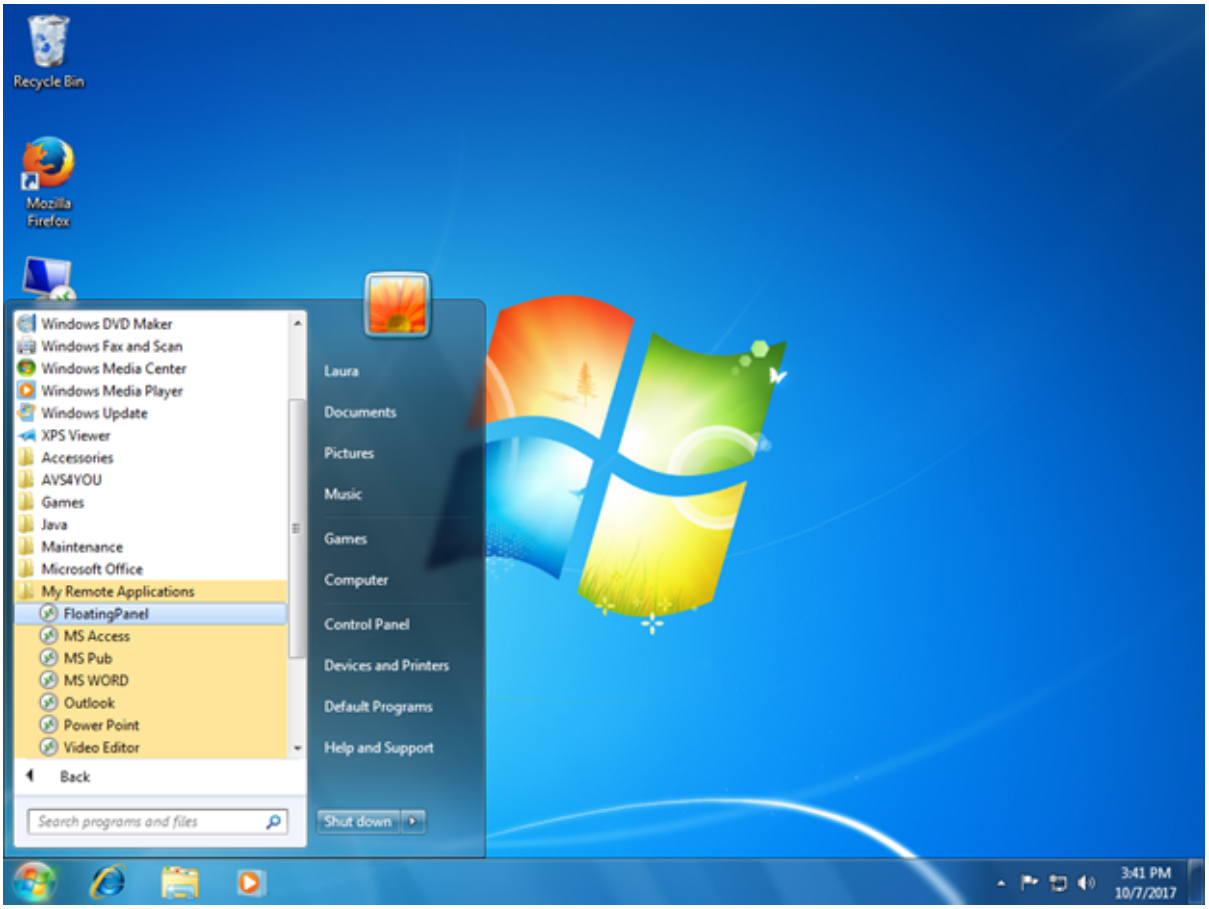
원하는 대로 메뉴 이름을 변경할 수 있습니다. 아래의 원격 애플리케이션 메뉴 제목을 클릭하고 값 상자에 추가하세요.



그녀가 새로 생성된 클라이언트를 한 번 실행할 때 그녀의 PC에서 어떤 일이 발생할까요: 그녀는 로컬 작업 표시줄의 알림 영역에 새로운 아이콘을 볼 것입니다.

내 원격 애플리케이션 새 아이콘	애플리케이션 목록 메뉴
	

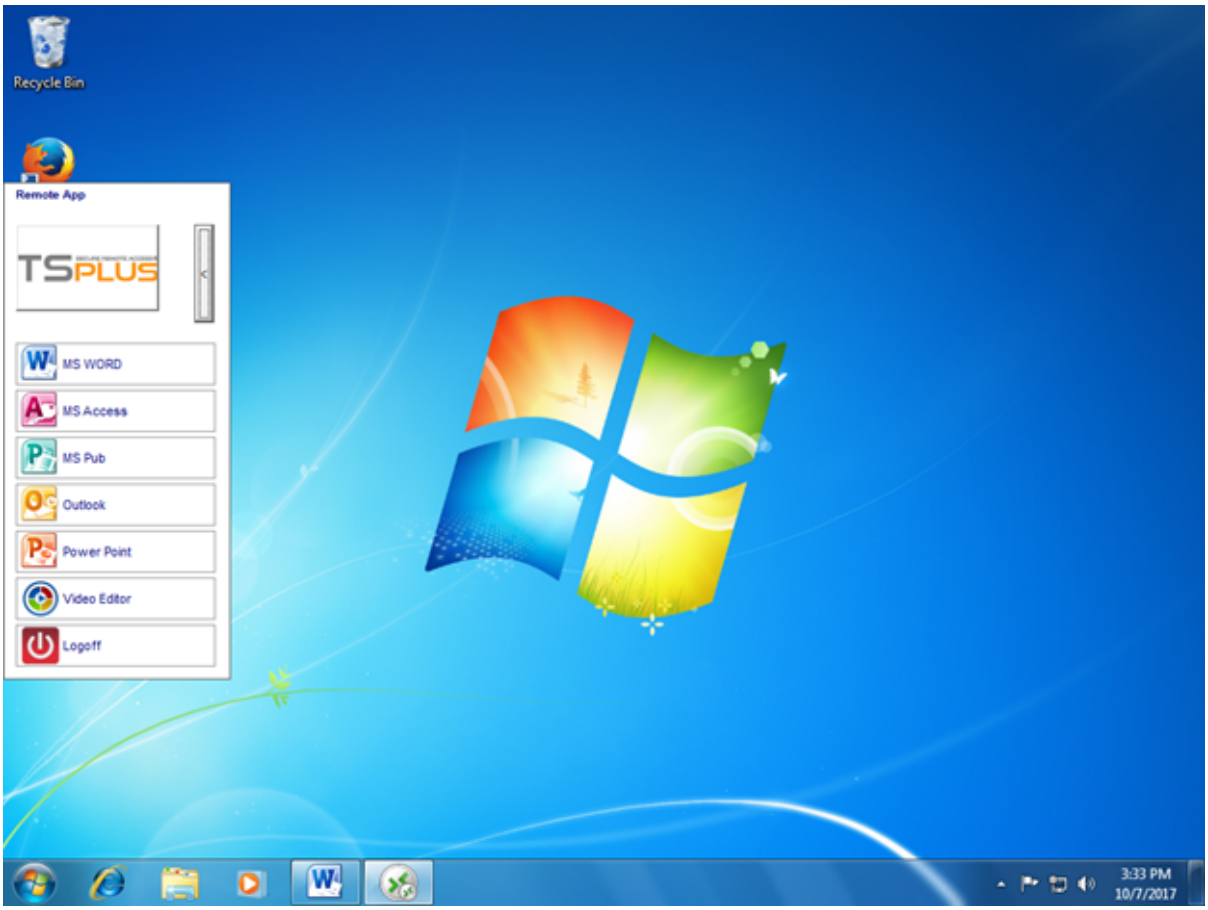
그녀는 또한 시작 메뉴 프로그램 목록에 새 항목이 추가된 것을 볼 것입니다. **내 원격 애플리케이션** :



이제 그녀는 나열된 애플리케이션 중 하나를 선택하고 RemoteApp으로 시작할 수 있습니다. 제공

된 LauraPortableClient.exe로 생성된 클라이언트를 사용할 필요가 없습니다.

예를 들어, 그녀가 플로팅 패널을 선택하면 이 결과를 얻습니다:

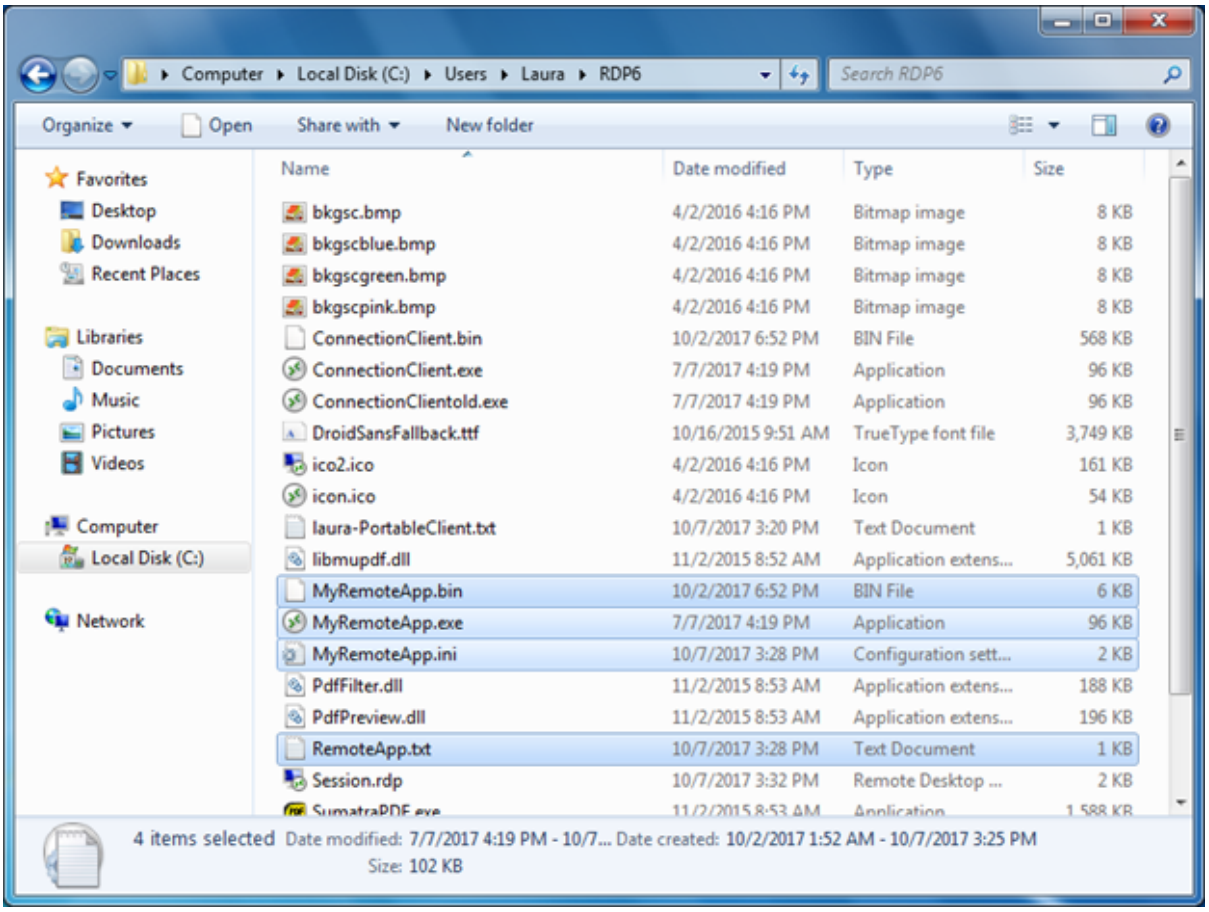


이 새로운 기술 뒤에 있는 기술적 배경.

10.50 릴리스의 새로 생성된 클라이언트는 로컬 PC의 사용자 프로필의 C:\Users%UserName%\RDP6 폴더 내에 여러 파일을 추가하고 있습니다.

MyRemoteApp.exe 그리고 MyRemoteApp.bin 알림 영역에 새 아이콘을 만들고 시작 버튼의 모든 프로그램 목록에 새 항목을 추가하기 위해 시작된 프로그램 코드입니다.

MyRemoteApp.ini 서버에서 수신된 파일입니다. 서버 측에서 이 사용자에게 할당된 각 애플리케이션의 세부 정보를 제공합니다. 서버에 대한 새로운 연결이 있을 때마다 업데이트됩니다. 일반적으로, 이 파일을 서버에서 수신하는 데는 각 로그온 후 30초가 소요됩니다. RemoteApp.txt는 이 PC에서 시작된 마지막 생성된 클라이언트의 이름을 제공합니다.



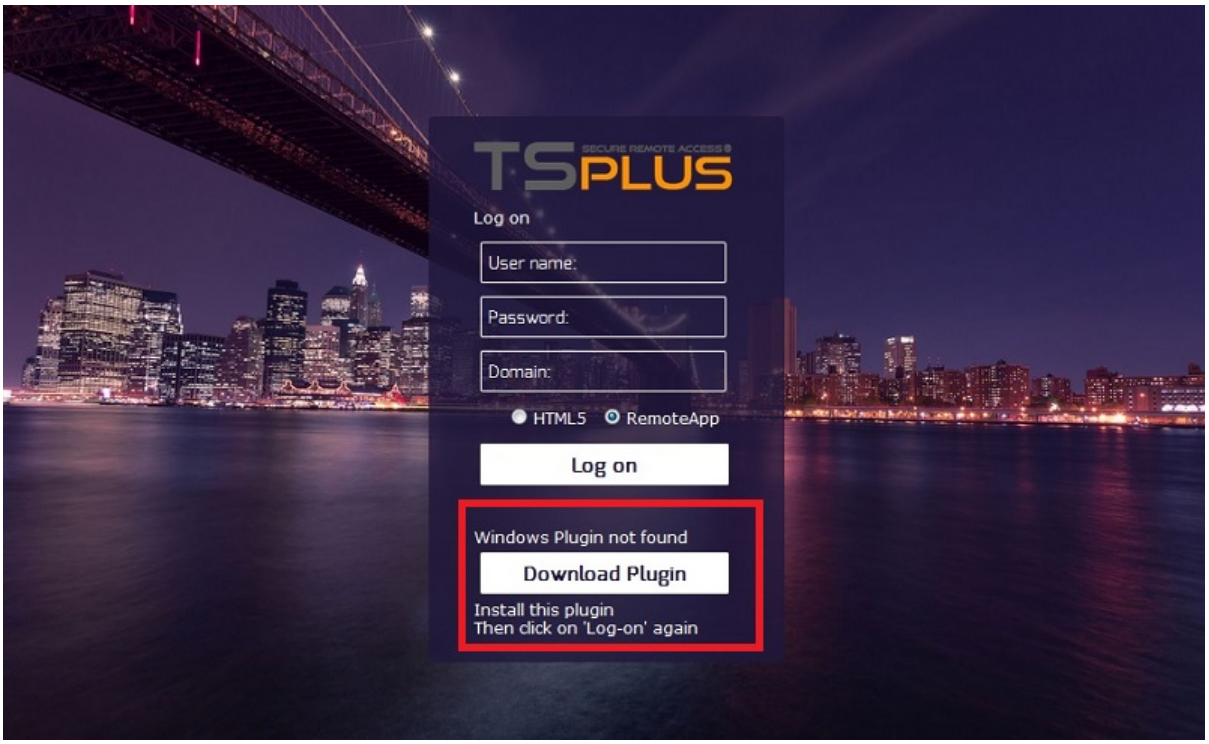
댓글:

사용자가 자신의 PC에서 관리자 권한을 가지고 있는 경우, **MyRemoteApp.exe** 각 재부팅 시 자동으로 시작되며 시작 버튼도 업데이트됩니다. 그렇지 않으면 관리자가 새로 생성된 클라이언트를 "관리자로" 한 번 실행하여 새로운 기능을 활성화해야 합니다. 이렇게 하면 HKLM에 적절한 레지스트리 항목이 생성됩니다. 사용자가 단일 서버에만 연결하는 경우 이 새로운 시스템은 완벽합니다. 그러나 여러 연결 클라이언트를 사용하여 다른 서버에서 세션을 열 경우 파일을 염두에 두어야 합니다. **MyRemoteApp.ini** 마지막 연결의 값으로 업데이트됩니다. 사용자가 혼란스러울 수 있으며, 이러한 배포 경우에는 이 새로운 기능을 사용하지 않는 것을 권장합니다.

원격 앱 플러그인

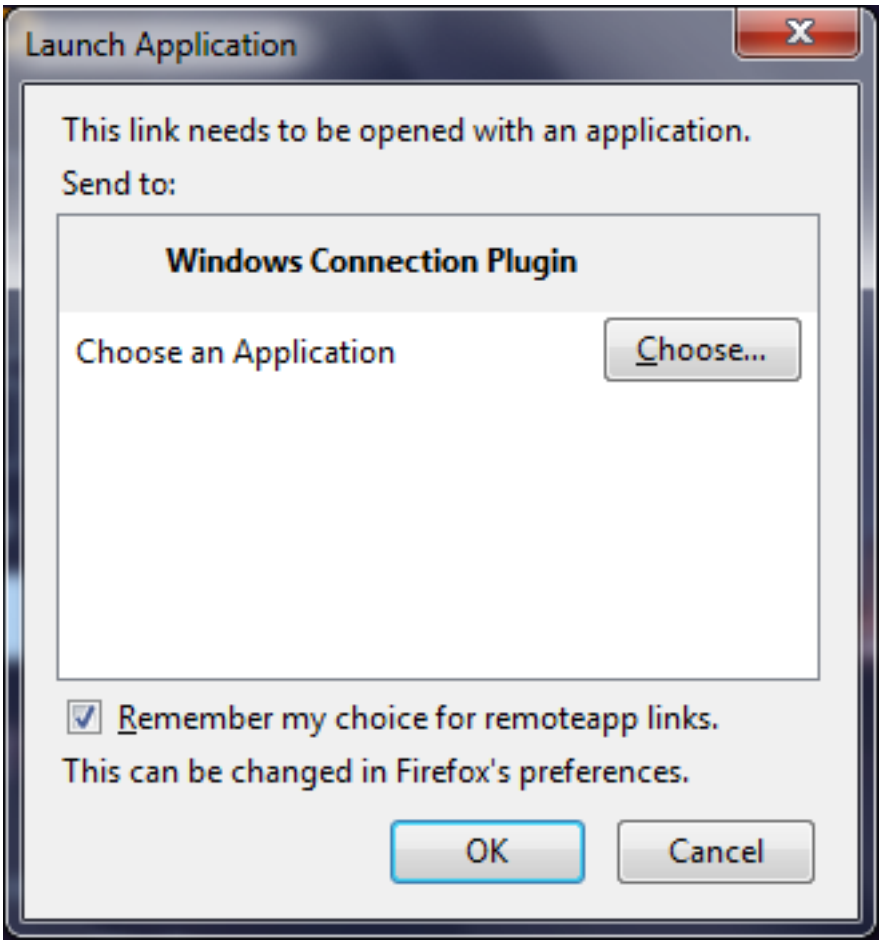
새로운 8.40 버전의 TSplus부터는 클라이언트 브라우저에 Java 플러그인을 설치할 필요가 없습니다.

이제 웹 포털을 통해 작은 Windows 플러그인을 다운로드하고 설치하여 Windows RemoteApp 클라이언트에 액세스할 수 있습니다. 이 작업은 빠르며 클라이언트당 한 번만 필요합니다.



C:\Program Files (x86)\TSplus\Clients\www\RemoteAppClient 폴더에 설치할 수도 있습니다.

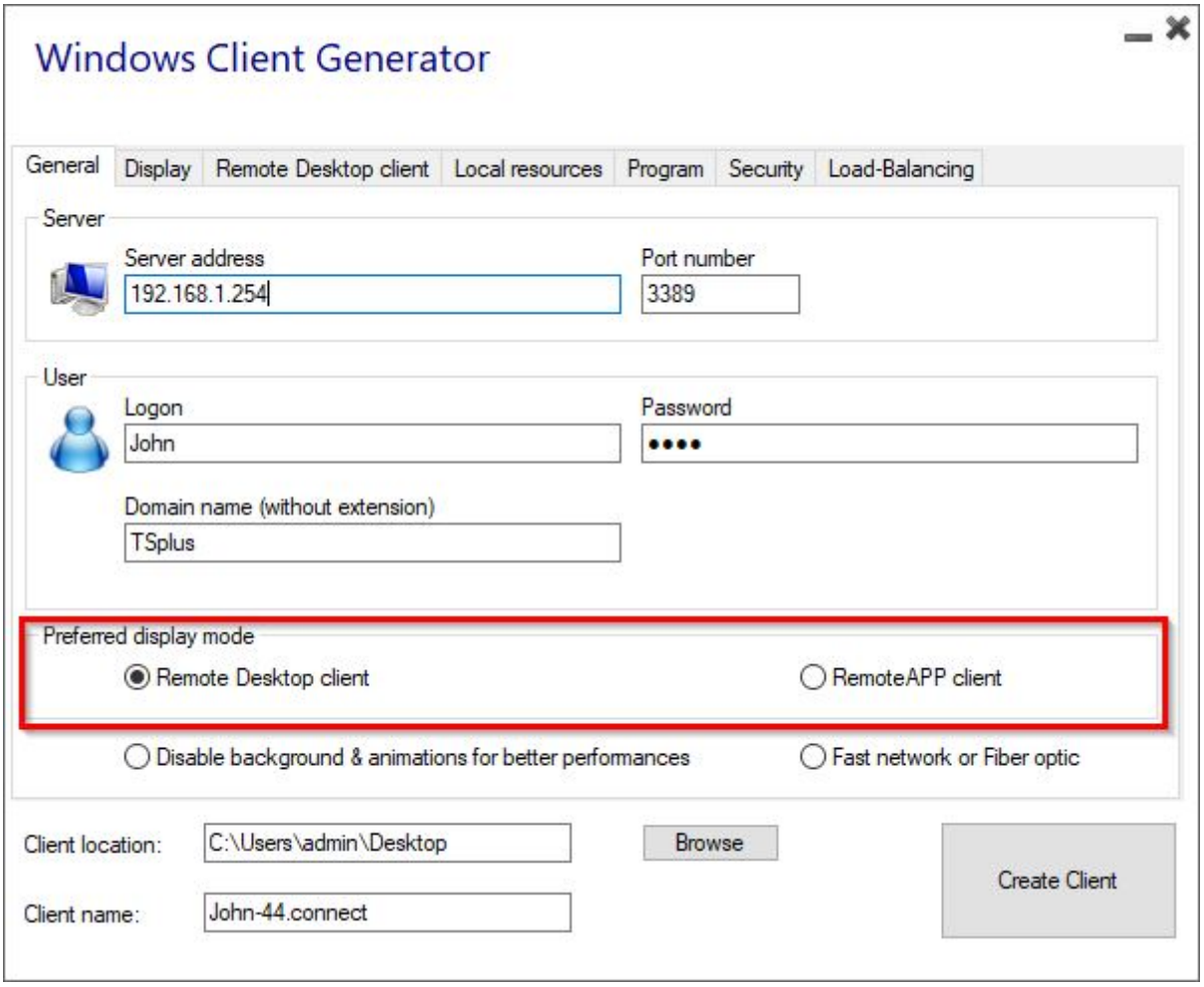
파이어폭스를 사용할 때, 이 메시지는 첫 연결 시 표시됩니다. '내 선택 기억하기' 옵션을 선택하면, 이후 연결 시 알림이 비활성화됩니다.



노트 TSplus 12.40부터 RemoteApp 클라이언트 설정 및 클라이언트 설정 프로그램 하나의 단일 설정으로 배포할 수 있도록 통합되었으므로 RemoteApp 클라이언트 설정을 다운로드하면 연결 클라이언트 설정을 다운로드할 필요가 없습니다.

원격 앱 연결 클라이언트

클라이언트 생성기의 일반 탭에서 2가지 표시 모드 중에서 선택할 수 있습니다:



###원격 앱 연결 클라이언트

원격 앱 연결 클라이언트는 투명도 색상 설정에 의존하지 않습니다.

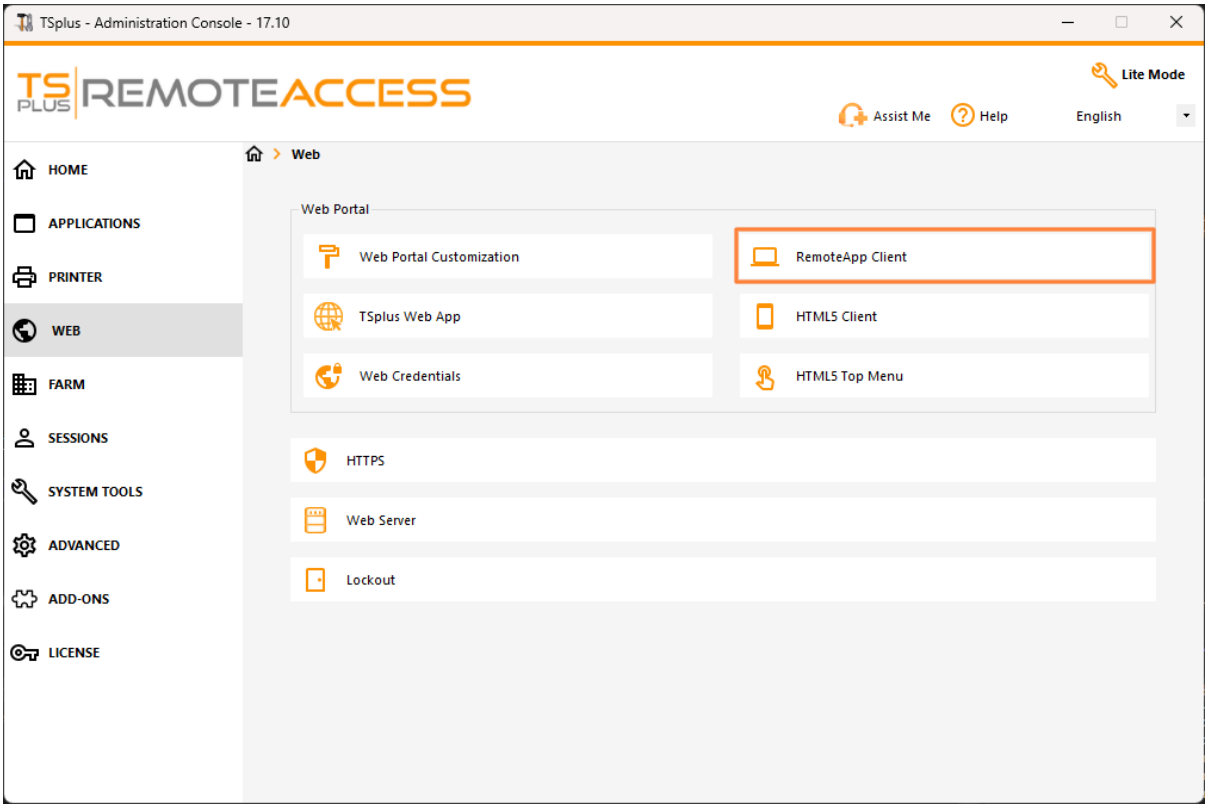
이것은 완벽한 애플리케이션 표시와 원래 Windows 동작을 가능하게 합니다.

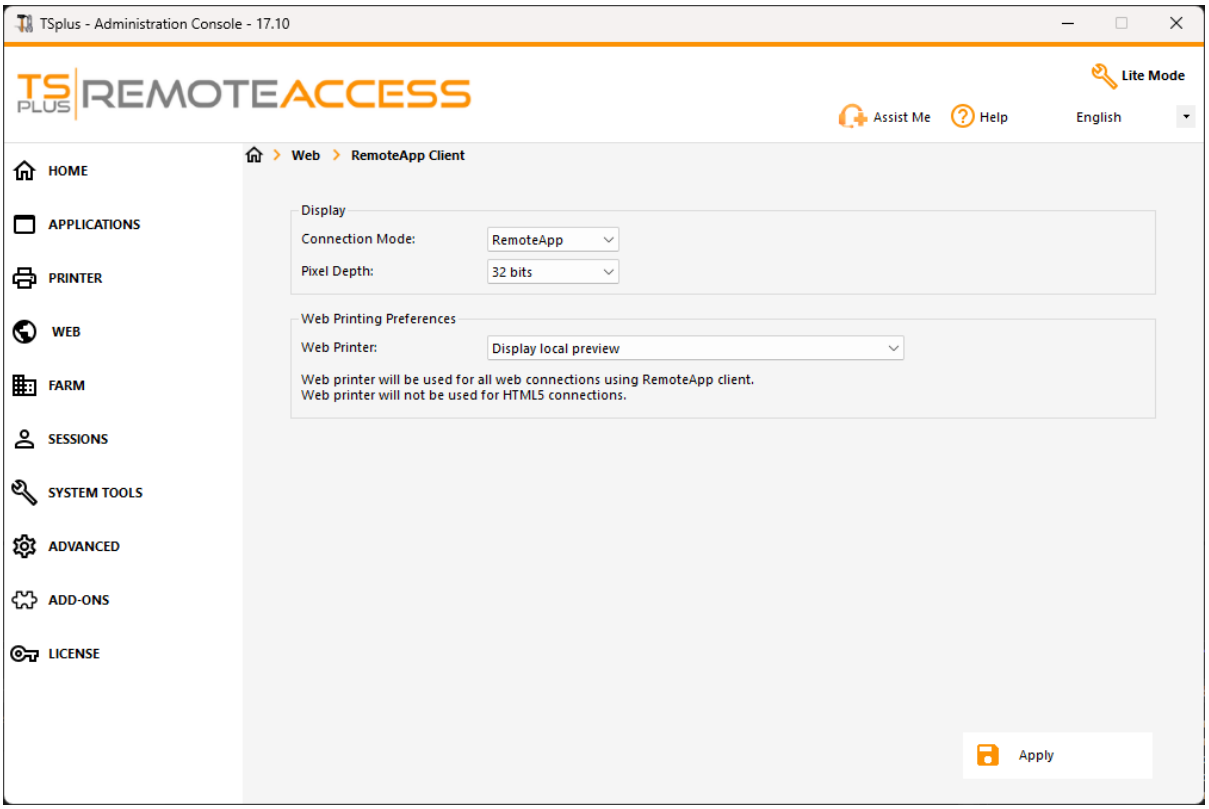
- 클라이언트 측에서는 RDP6 이상이 설치되어 있어야 합니다.

- 서버 측에서는 TSplus가 Windows 7에서 Windows Server 2019를 실행하는 머신에 설치되어야 합니다.

노트 RemoteApp는 Windows 10 1803 및 1809 Home Windows 2019 Essentials Editions에서 지원되지 않습니다.

원격 앱 클라이언트 디스플레이 및 인쇄 기본 설정을 Admintool의 웹 탭에서 변경할 수 있습니다.





최소화된 애플리케이션은 로컬 애플리케이션처럼 Windows 작업 표시줄 안에서 직접 찾을 수 있습니다.

이 예제에서는 Firefox와 Paint가 로컬에서 실행되고, Notepad, Word 및 Foxit가 원격으로 실행됩니다.



원격 앱 연결 클라이언트의 경우, 사용자가 로그인할 때 원활하게 시작될 하나의 고유한 애플리케이션을 게시하도록 선택할 수 있습니다. 응용 프로그램을 [당신은 또한 게시할 수 있습니다] TSplus 원격 작업 표시줄 , 플로팅 패널 또는 애플리케이션 패널 .

프록시 환경에서 Windows 클라이언트 실행

일반적으로 SSH 패키지는 HTTP(S) 프록시를 지원하며, 이는 대부분의 알려진 프록시를 극복하는 데 충분해야 합니다.

그러나 프록시 환경이 제대로 인식되지 않거나 제3자 소프트웨어에서 숨겨져 있거나 대상 서버가 리버스 프록시 뒤에 있는 매우 어려운 기존 사례가 있습니다.

이러한 어려운 경우를 위해 소프트웨어에는 "구조 모드"라는 비 SSH 솔루션이 포함되어 있습니다.

HTML5 연결을 설정할 수 있다면, 이 소프트웨어가 Websocket(FF, Chrome, Opera, IE10 등) 또는 XHR(IE6-IE9)를 통해 네이티브 소켓 연결을 설정하는 데 도움이 될 것임을 확신할 수 있습니다.

조심하세요, 일부 프록시는 허용합니다. 웹소켓/XHR 트래픽은 HTTPS 계층을 통해서만 이루어지므로 http 대신 https 주소를 사용하세요.

프록시가 프록시 인증을 요청하지 않고 브라우저를 통해 페이지에 접근할 수 있는 경우:

1. http(s)://yourserver.com__/software/html5/jwres/__ 열기
2. 성공적인 연결을 기다리세요 (요청 시 Java 실행을 승인하세요)
3. 빨간색 텍스트 “링크 열기”를 클릭하여 작업 웹 액세스 페이지를 엽니다.
4. Windows 클라이언트 액세스를 평소처럼 사용하세요.

프록시가 프록시 인증을 요청하고 브라우저를 통해 페이지에 접근할 수 있는 경우:

1. http(s)://yourserver.com__/software/html5/jwres/__ 열기
2. 프록시가 자바 애플릿에 대한 인증을 요청하면 "취소"를 누르십시오.
3. “Download LocalWebserver”를 클릭한 후 성공적으로 다운로드가 완료되면 실행하세요. 그러면 포트 18888에서 로컬 http 서버가 시작됩니다.
4. “Force Applet loading from”을 클릭하십시오. http://localhost:18888 ”, 이 작업은 로컬 http 서버에서 jar 파일을 로드하여 페이지를 새로 고칩니다.
5. 성공적인 연결을 기다리세요
6. 빨간색 텍스트 “링크 열기”를 클릭하여 작업 웹 액세스 페이지를 엽니다.
7. Windows 클라이언트 액세스를 평소처럼 사용하세요.

TSplus 서버 보안

개요

서버를 보호하는 것은 모든 전문가가 또 다른 장을 추가할 수 있는 끝나지 않는 이야기입니다.

TSplus는 회사의 기존 보안 인프라(Active Directory, GPO, HTTPS 서버, SSL 또는 SSL 통신 시스템, VPN, ID 카드 유무에 따른 접근 제어 등)에서 이점을 얻고 호환됩니다.

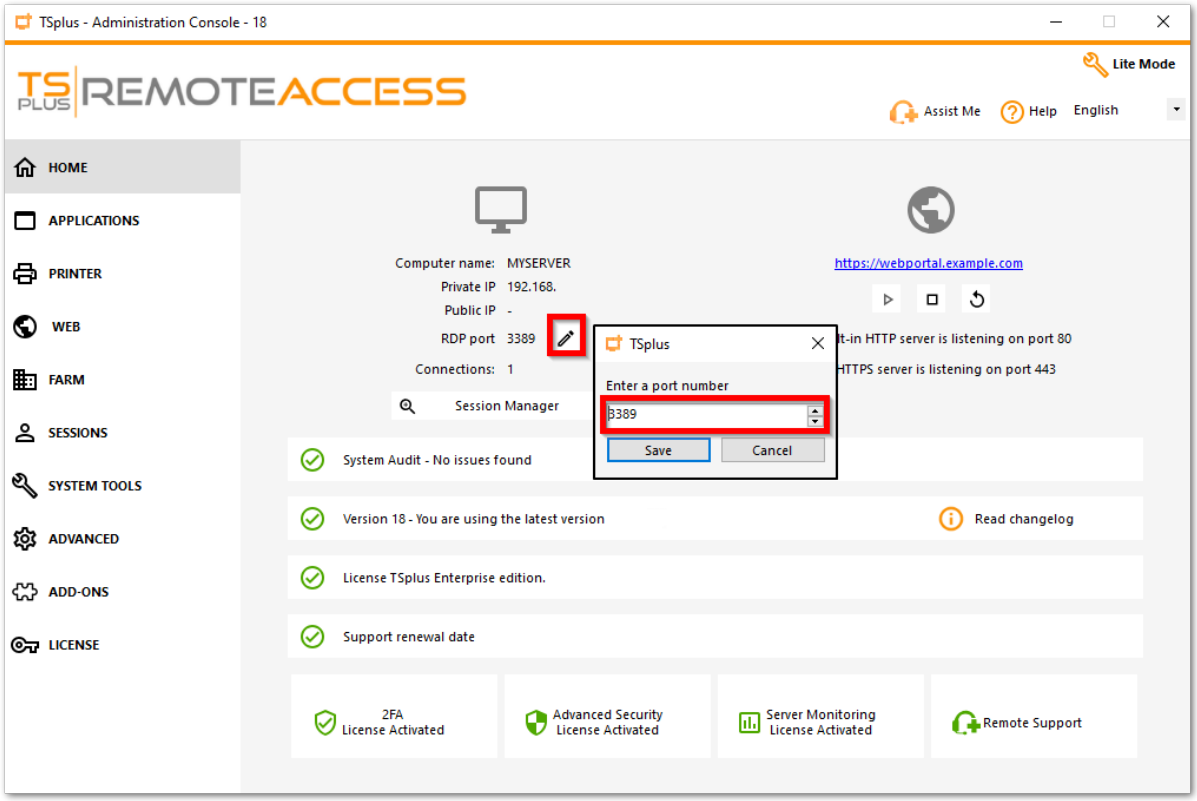
서버를 쉽게 보호하고자 하는 고객을 위해, TSplus는 높은 수준의 보안을 유지하기 위한 간단하고 효과적인 방법을 제공합니다.

AdminTool을 사용하면 RDP 서비스가 연결을 수락할 다른 TCP/IP 포트 번호를 선택할 수 있습니다. 기본 포트는 3389입니다.

임의의 포트를 선택할 수 있으며, 이는 네트워크에서 이미 사용되지 않고 방화벽과 각 TSplus 사용자 액세스 프로그램에서 동일한 포트 번호를 설정한다고 가정합니다.

TSplus는 고유한 포트 포워딩 및 터널링 기능을 포함합니다: 설정된 RDP 포트와 관계없이 RDP는 HTTP 및 HTTPS 포트 번호에서도 사용할 수 있습니다!

사용자가 네트워크 외부에서 TSplus 서버에 접근하려면 선택한 포트의 모든 수신 연결이 TSplus 서버로 전달되도록 해야 합니다. 홈 탭에서 "RDP 포트" 옆에 있는 연필 버튼을 클릭하세요.



RDP 포트를 변경하고 저장하십시오.

서버 측 보안 옵션

AdminTool은 관리자가 생성한 TSplus 연결 프로그램을 사용하지 않는 모든 사용자에 대한 접근을 거부할 수 있도록 합니다. 이 경우, TSplus 클라이언트 이외의 원격 데스크톱 클라이언트를 사용하여 세션을 열려고 시도하는 모든 사용자는 (올바른 서버 주소, 포트 번호, 유효한 로그인 및 유효한 비밀번호를 가지고 있다고 가정할 때) 자동으로 연결이 끊어집니다.

관리자는 Remote Desktop User 그룹의 구성원만 허용하도록 결정할 수 있습니다. 세션을 열 수 있습니다.

관리자는 세션을 열기 위해 비밀번호가 필수라고 결정할 수 있습니다.

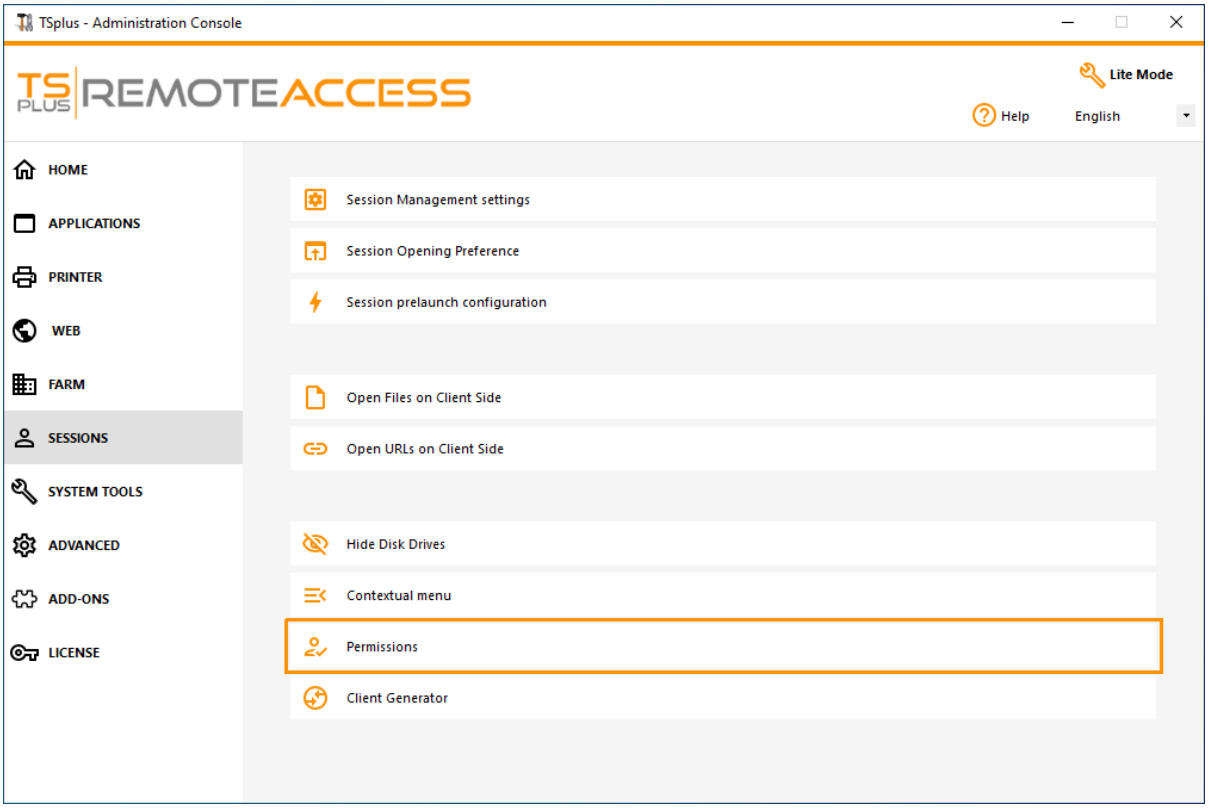
적용 가능한 로컬 그룹 정책을 설정함으로써, 관리자는 터미널 서비스 세션 중 클라이언트와 원격 컴퓨터 간에 전송되는 모든 데이터에 대한 암호화 수준을 강제할지 여부를 지정할 수 있습니다.

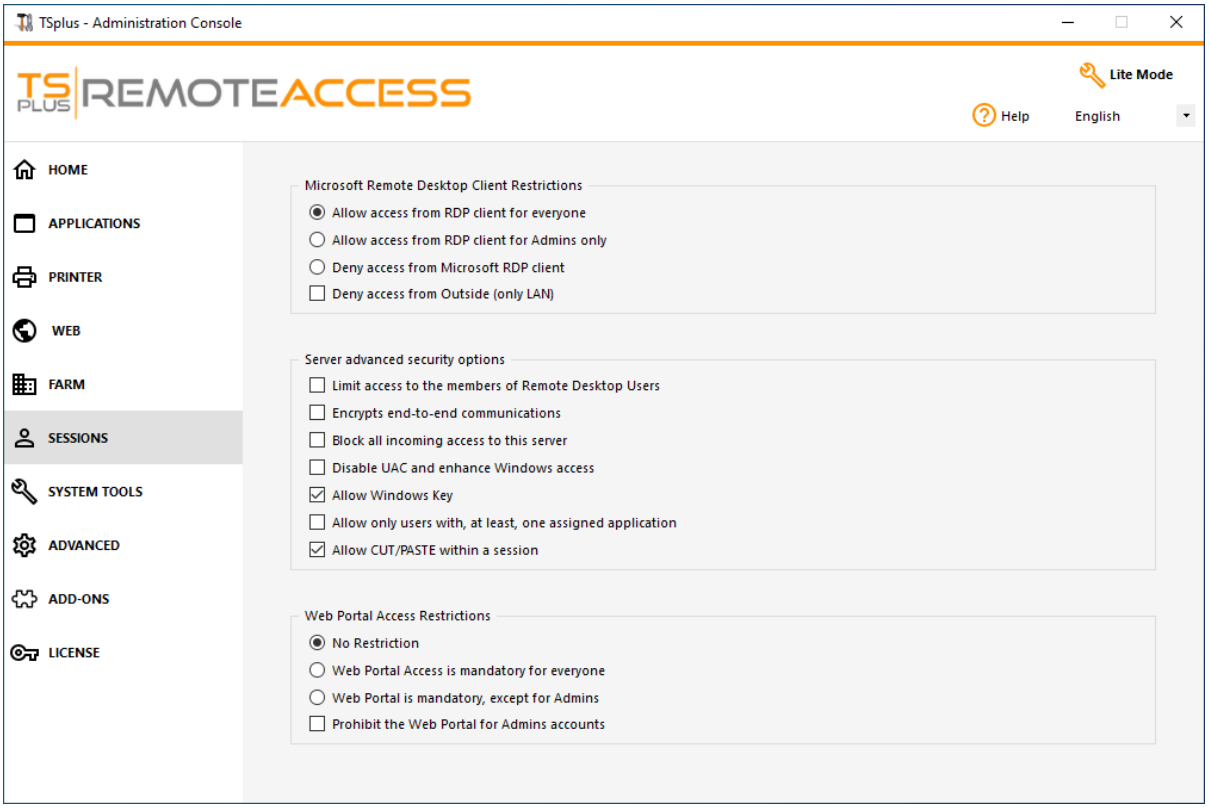
상태가 활성화로 설정되면 서버에 대한 모든 연결의 암호화는 관리자가 결정한 수준으로 설정됩니다. 기본적으로 암호화는 높음으로 설정됩니다.

관리자는 TSplus 연결 클라이언트를 가진 사용자만 세션을 열 수 있도록 규칙을 설정할 수도 있습니다.

표준 RDP 또는 웹 액세스를 통한 모든 수신 액세스는 자동으로 거부됩니다.

세션 - 권한 탭을 클릭하면 여러 가지 고급 보안 옵션을 찾을 수 있습니다.





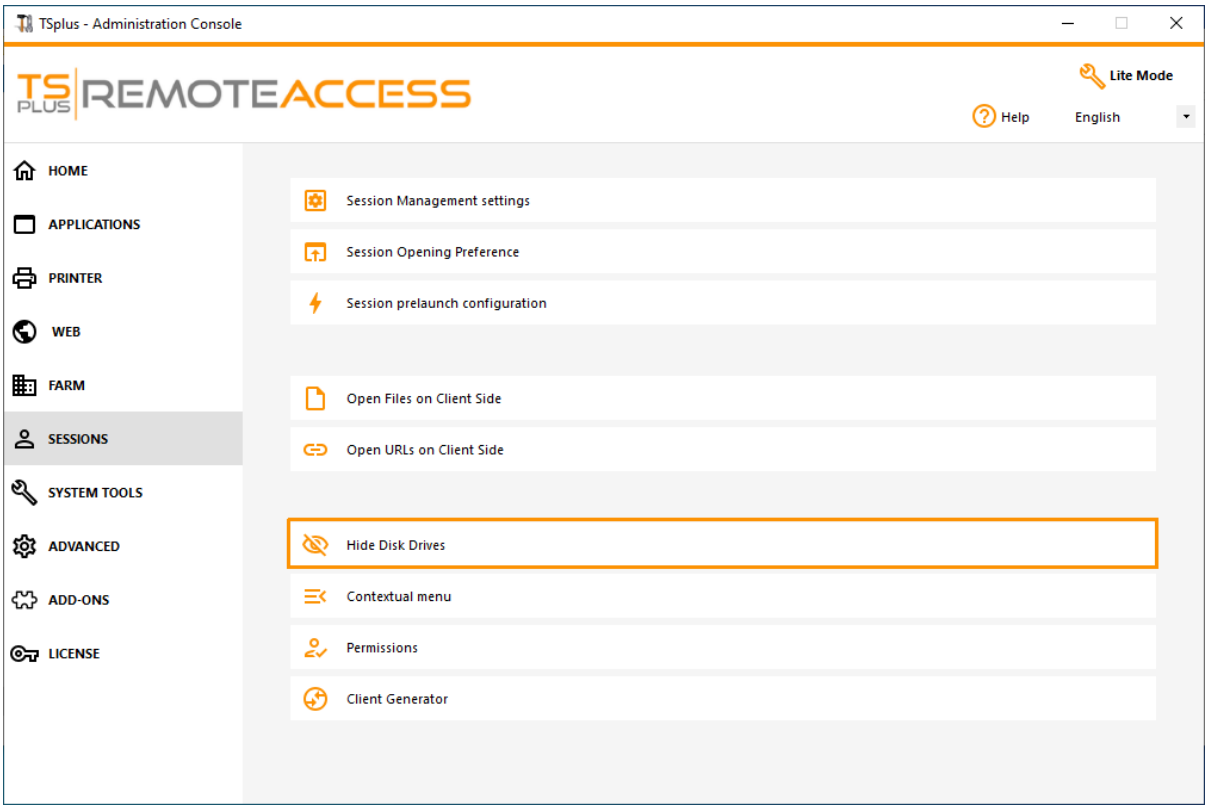
- **모든 사용자에게 Microsoft RDP 클라이언트에서 접근 허용:** 모든 사용자가 mstsc.exe를 사용하여 연결할 수 있도록 허용합니다.
- **관리자만을 위한 Microsoft RDP 클라이언트에서의 접근 허용:** 관리자만 mstsc.exe를 사용하여 연결할 수 있습니다.

- **Microsoft RDP 클라이언트에서 접근 거부:** mstsc.exe를 사용하여 연결할 수 없도록 방지합니다.
- **외부에서의 접근 거부:** 이는 LAN의 개인 IP만 세션을 열 수 있음을 의미합니다.
- **원격 데스크톱 사용자 회원에게만 접근 제한:** 이 제한은 이 로컬 사용자 그룹에만 적용됩니다 (클릭하여 확인할 수 있습니다). 사용자 및 그룹 타일 .
- **종단 간 통신을 암호화합니다:** 고급 암호화는 128비트 암호화를 사용하여 클라이언트/서버 통신을 암호화합니다. 터미널 서버에 접근하는 클라이언트가 128비트 암호화를 지원할 때 이 수준을 사용하십시오.
- **이 서버에 대한 모든 수신 접근을 차단하십시오:** 모든 활성 세션은 유지되며, 모든 들어오는 연결 시도는 차단됩니다. 이 상자를 선택하는 경우 서버의 콘솔에 물리적으로 접근할 수 있는지 확인하십시오. 서버가 클라우드 환경에 호스팅되는 경우 이 옵션을 사용하지 마십시오.
- **UAC를 비활성화하고 Windows 액세스를 향상시키십시오:** 사용자 계정 컨트롤을 비활성화하고 Windows에서 원치 않는 보안 팝업을 모두 제거합니다. 애플리케이션을 실행할 때 사용자 제한(메시지).
- **"Windows 키 허용" 상자** TSplus 세션 내에서 Windows 키와 조합의 사용을 허용합니다.
- **할당된 애플리케이션이 하나 이상 있는 사용자만 허용:** 하나 이상의 애플리케이션을 가진 사용자는 세션을 열 수 있습니다.
- **세션 내에서 CUT/PASTE 허용:** 이 상자를 선택 해제하면 CTRL C/CTRL V 명령이 비활성화됩니다.

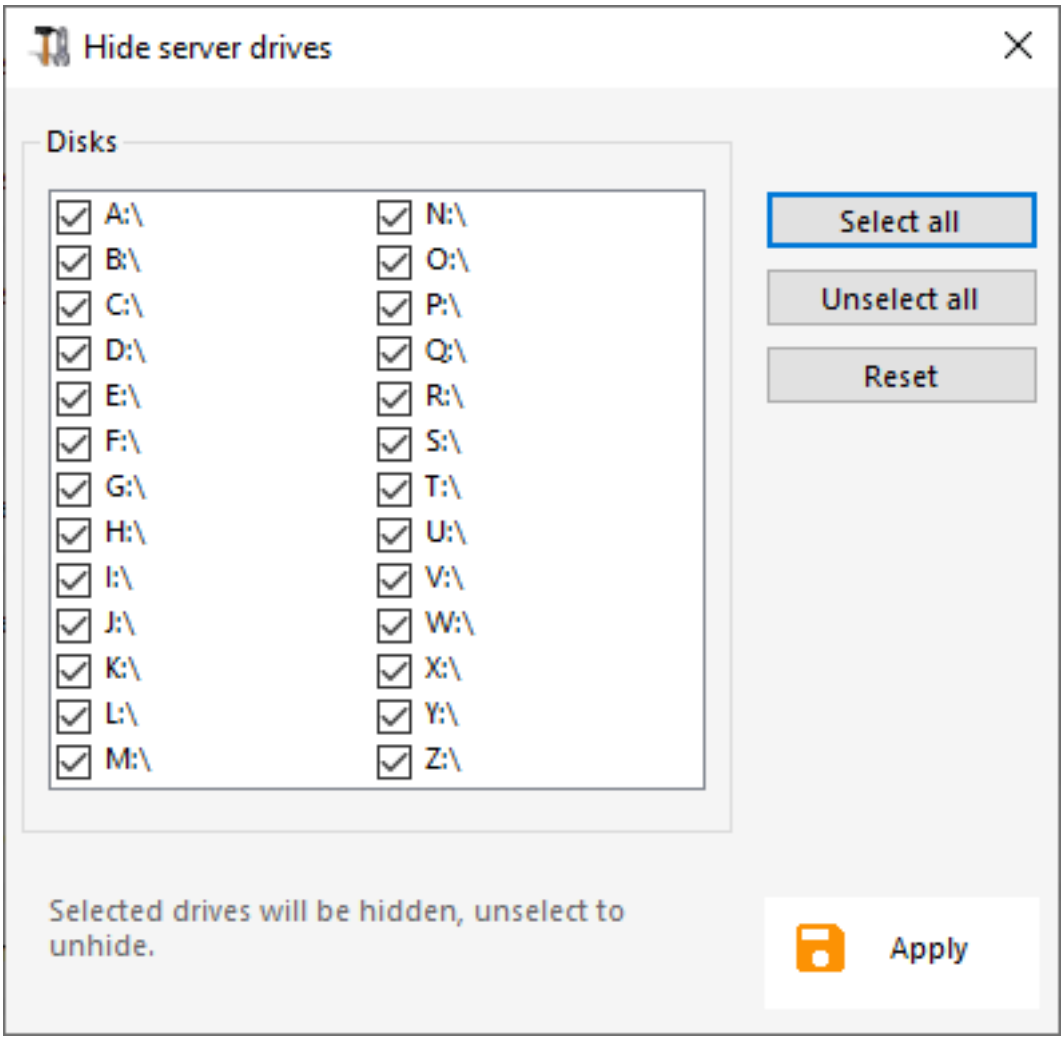
웹 포털 접근 제한

- 제한 없음
- 웹 포털은 모든 사용자에게 필수입니다: 사용자는 웹 포털을 통해서만 연결할 수 있습니다.
- 웹 포털은 필수이며, 관리자를 제외한 사용자들은 웹 포털을 통해서만 연결할 수 있습니다.
- 관리자 계정에 대한 웹 포털 사용 금지: 관리자는 웹 포털을 통해 연결할 수 없습니다.

AdminTool에는 사용자가 내 컴퓨터 또는 표준 Windows 대화 상자를 통해 폴더에 접근하지 못하도록 서버 디스크 드라이브를 숨기는 기능이 포함되어 있습니다. 세션 탭에서 "디스크 드라이브 숨기기"를 클릭하십시오.



이 도구는 전 세계적으로 작동합니다. 이는 설정이 적용된 후 관리자조차도 드라이브에 정상적으로 접근할 수 없음을 의미합니다. 아래 예시에서 모든 드라이버는 "모두 선택" 버튼으로 선택되었으며, 이는 모든 사용자가 숨겨질 드라이브에 해당하는 모든 상자를 체크합니다.



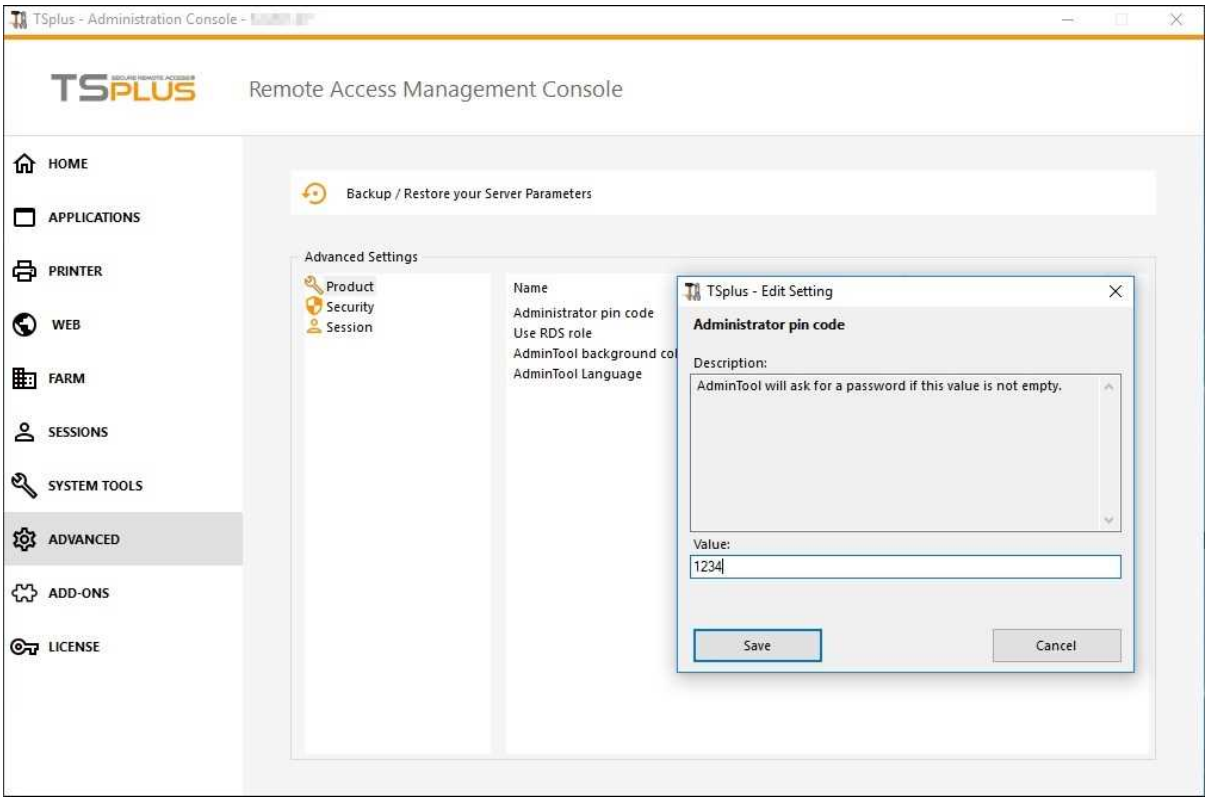
노트: 이 기능은 강력하며 디스크 드라이브에 대한 접근을 비활성화하지 않습니다. 단지 사용자가 이를 표시하지 못하도록 방지합니다.

이 도구는 디스크 드라이브를 숨김으로 표시하지만, 문서 및 설정의 전체 루트 폴더와 사용자 목록에도 HIDDEN 속성을 추가합니다.

관리자가 이러한 파일을 보려면 다음을 수행해야 합니다:

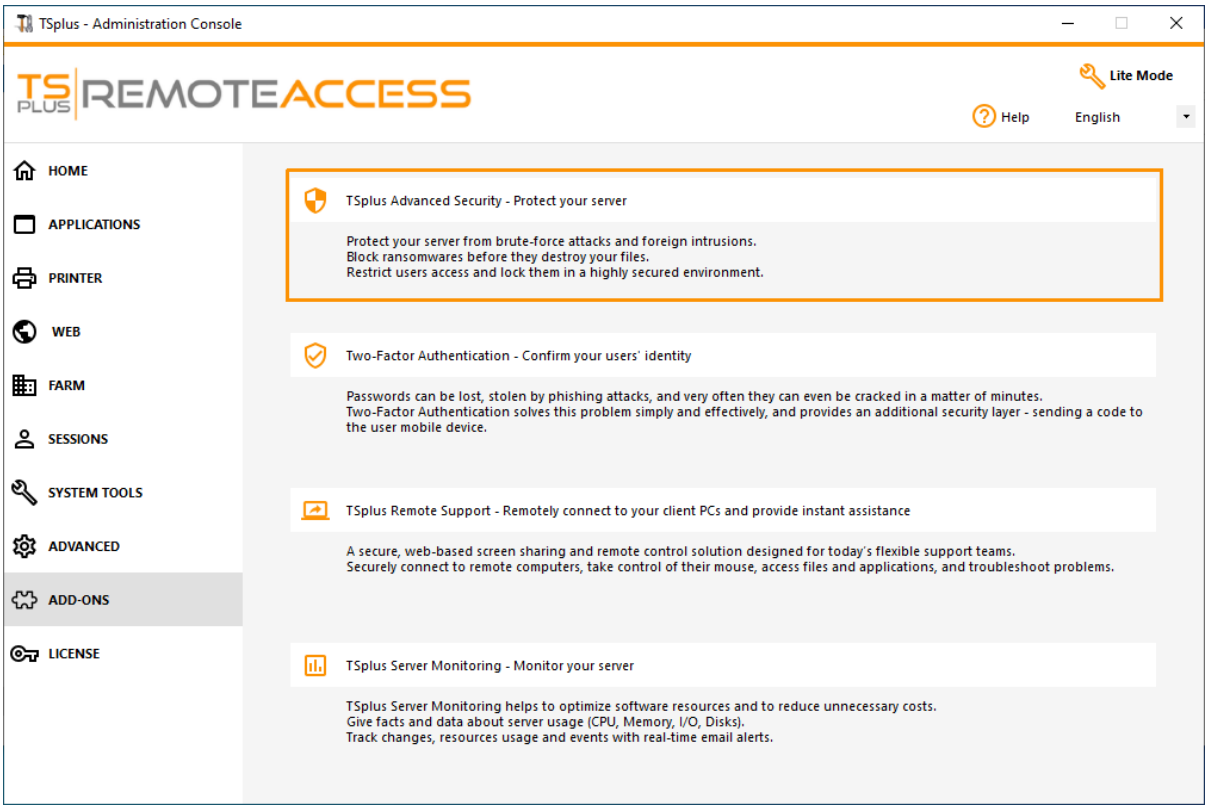
1. 디스크 드라이브 문자를 입력하세요. 예: **D:** D: 드라이브로 이동합니다.
2. 켜기 **숨겨진 파일 및 폴더 표시** 폴더 보기 속성에서.

관리자는 제품 설정의 AdminTool 고급 탭에서 매 시작 시 요청되는 PIN 코드를 설정하여 관리자 도구 접근을 보호할 수 있습니다.

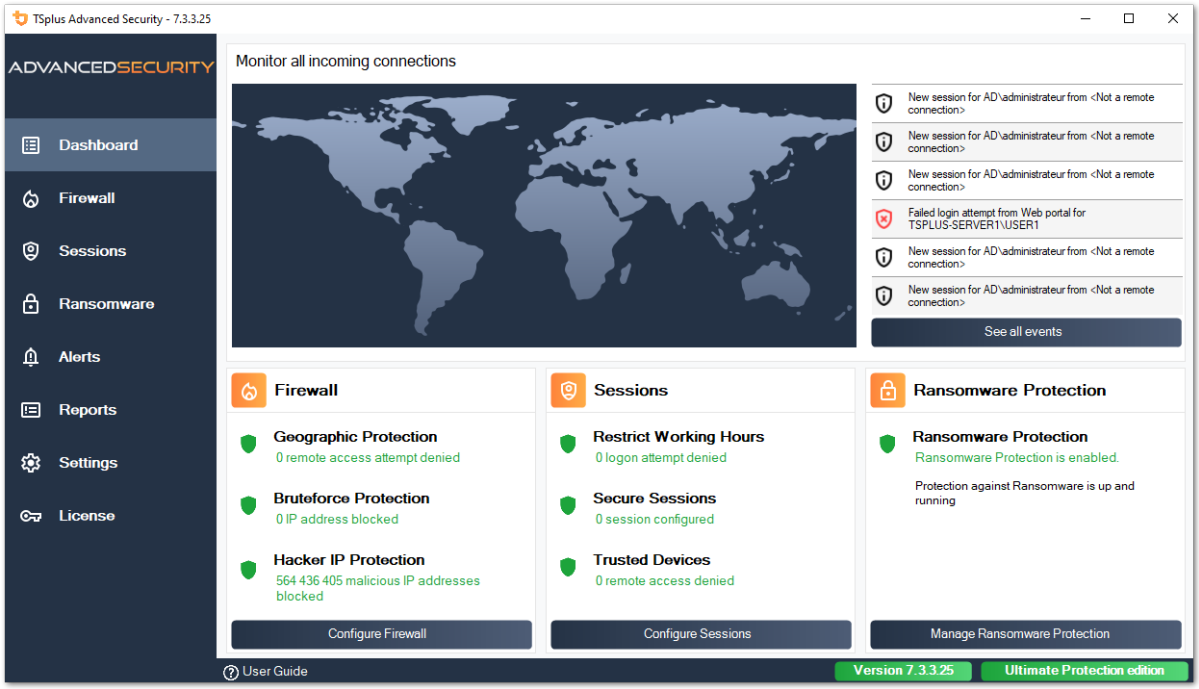


TSplus 고급 보안 궁극적

TSplus 11.40 버전 이후로, Add-Ons 탭에서 실행할 수 있는 독특한 보안 추가 도구를 찾을 수 있습니다.



강력한 기능을 제공하며, 문서화된 내용은 이 페이지 .



웹 포털의 브루트포스 보호 역할은 다음과 같이 설명됩니다. 이 페이지 .

이중 인증

TSplus 12 버전부터 TSplus 웹 포털에 대한 추가 기능으로 이중 인증을 활성화할 수 있습니다.



이 놀라운 새로운 기능에 대한 자세한 정보는 다음에서 확인할 수 있습니다. 이 페이지 .

SSL 인증서

SSL 인증서 프로세스는 이러한 페이지에 자세히 설명되어 있습니다:

- TSplus는 무료 및 유효한 SSL 인증서를 생성하는 사용하기 쉬운 도구를 제공합니다. 무료 및 설치가 쉬운 SSL 인증서
- HTTPS 및 SSL 제3자 인증서 .
-

당신의 선택 보안 강화를 위한 암호화 스위트 .

TSplus 액세스 프로그램 보안 옵션:

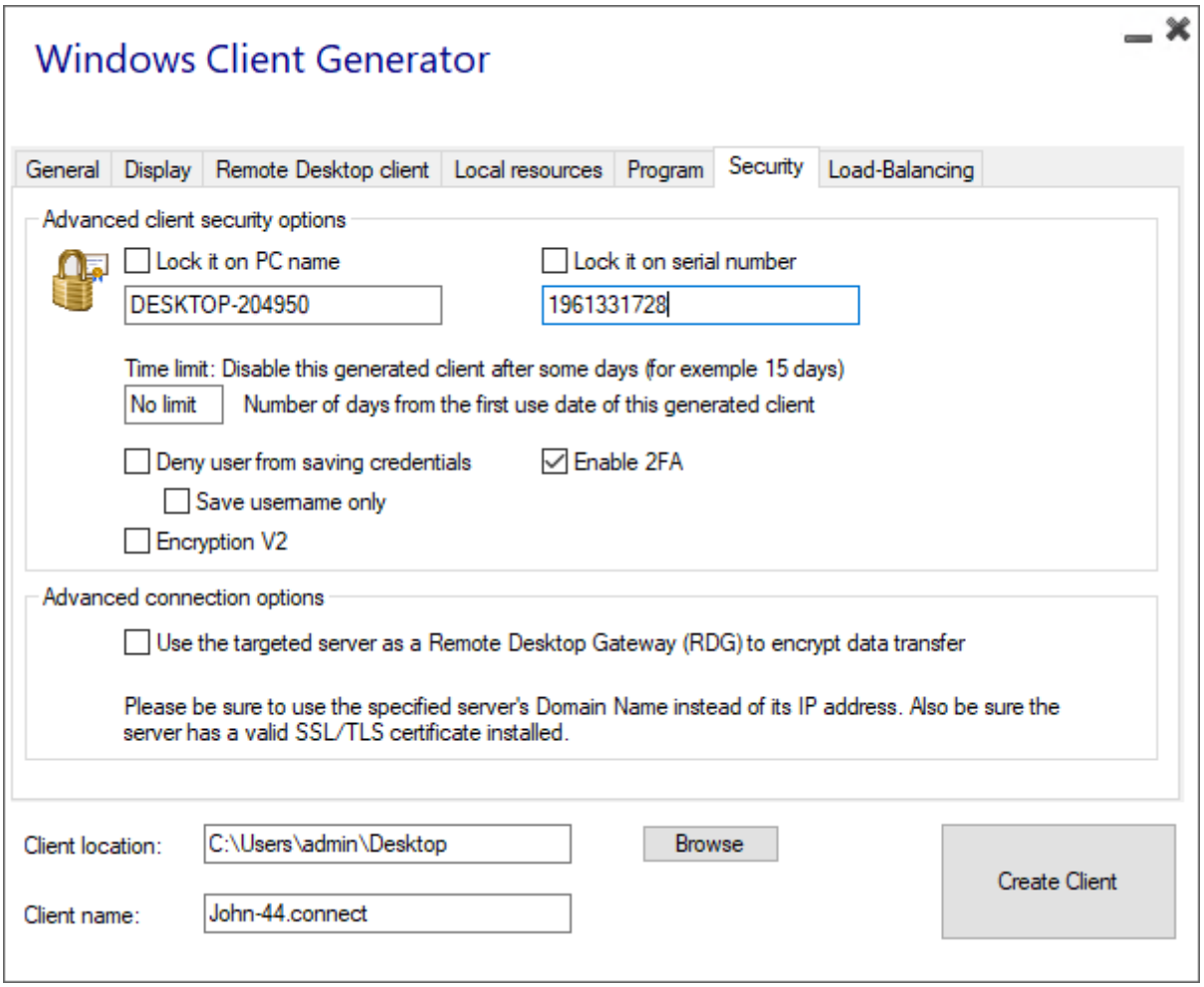
TSplus 클라이언트 생성기는 보안 탭에서 TSplus 클라이언트를 잠글 수 있는 기능을 제공합니다:

- 특정 PC 이름입니다. 이 프로그램은 다른 PC에서 시작할 수 없음을 의미합니다.
- 물리적 드라이브 일련 번호(PC HDD 또는 USB 스틱). 이는 높은 수준의 보안을 설정하는 매우 쉽고 강력한 방법입니다.

  연결하는 유일한 방법은 특정 클라이언트를 사용하는 것이며, 이 특정 클라이언트는 특정 USB 스틱이나 PC HDD에서만 시작할 수 있습니다.

  일부 고객은 각 사용자에게 지문 인식 USB 스틱을 제공하고 생성된 각 프로그램은 장치 일련 번호에 잠겨 있습니다.

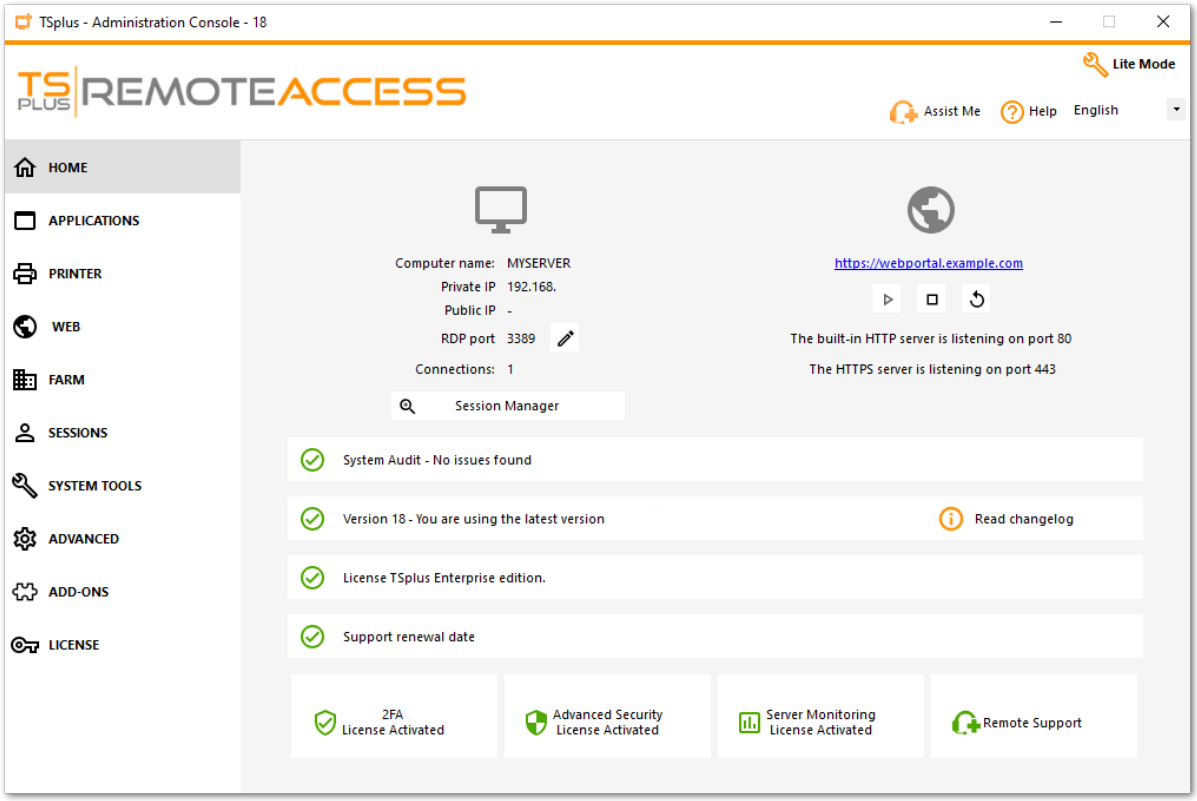
  이렇게 하면 클라이언트의 프로그램 자체에 대한 접근을 제한할 수 있을 뿐만 아니라 USB 메모리에서 복사되어 다른 곳에서 사용되지 않도록 보장할 수 있습니다.



더 많은 보안 기능 정보는 확인하세요. TSplus 휴대용 클라이언트 생성기 문서 그리고 우리의 FAQ.

서버 관리

관리 도구의 홈 탭에서 TSplus 서버에 대한 모든 필요한 정보를 볼 수 있습니다:

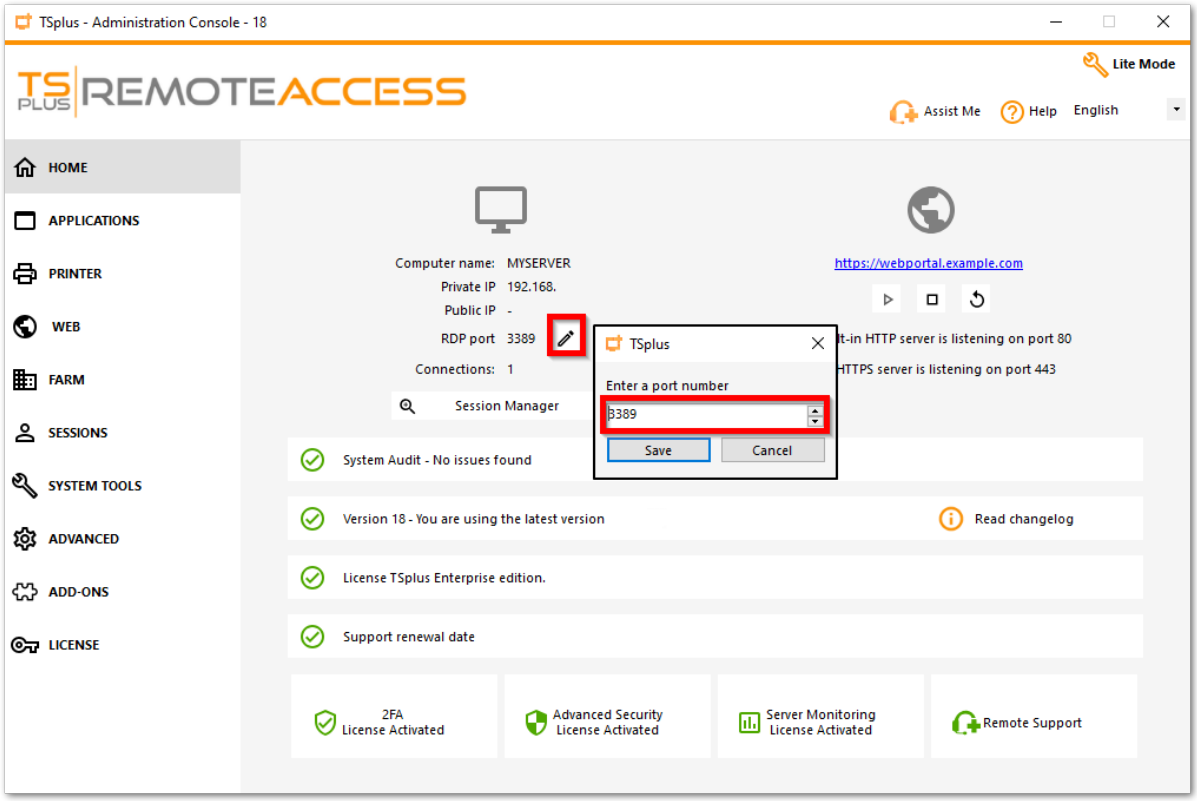


RDP 포트 번호 변경 및 방화벽 설정

AdminTool을 사용하면 RDP 서비스가 연결을 수락할 다른 TCP/IP 포트 번호를 선택할 수 있습니다. 기본 포트는 3389입니다. 네트워크에서 이미 사용되지 않는 임의의 포트를 선택할 수 있으며, 방화벽과 각 TSplus 사용자 액세스 프로그램에서 동일한 포트 번호를 설정해야 합니다.

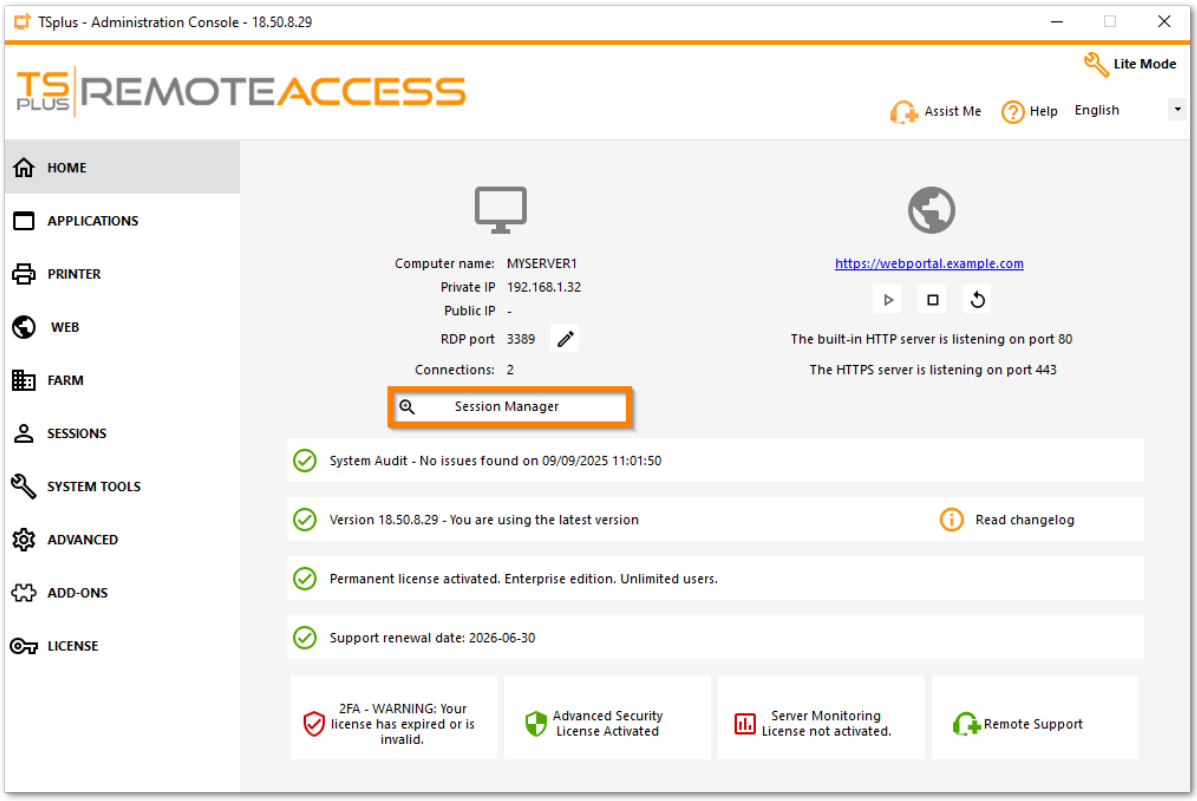
TSplus는 고유한 포트 포워딩 및 터널링 기능을 포함합니다: 설정된 RDP 포트와 관계없이 RDP는 HTTP 및 HTTPS 포트 번호에서도 사용할 수 있습니다!

사용자가 네트워크 외부에서 TSplus 서버에 접근하려면 선택한 포트의 모든 수신 연결이 TSplus 서버로 전달되도록 해야 합니다.

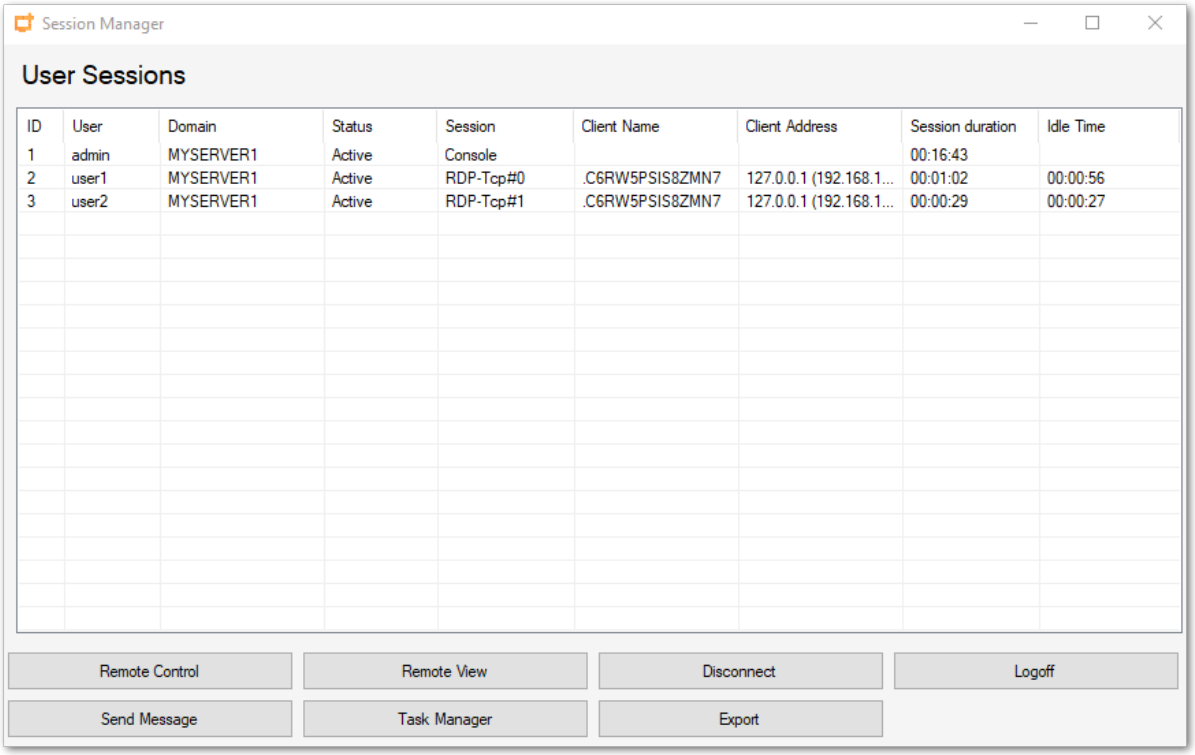


사용자 및 세션 관리

세션 관리자는 RDP 포트 바로 아래에 위치합니다:



서버의 작업 관리자를 표시할 수 있으며, 원격 제어를 활성화하거나, 연결을 끊거나, 로그오프하거나, 사용자에게 메시지를 보낼 수 있는 기능이 있습니다.



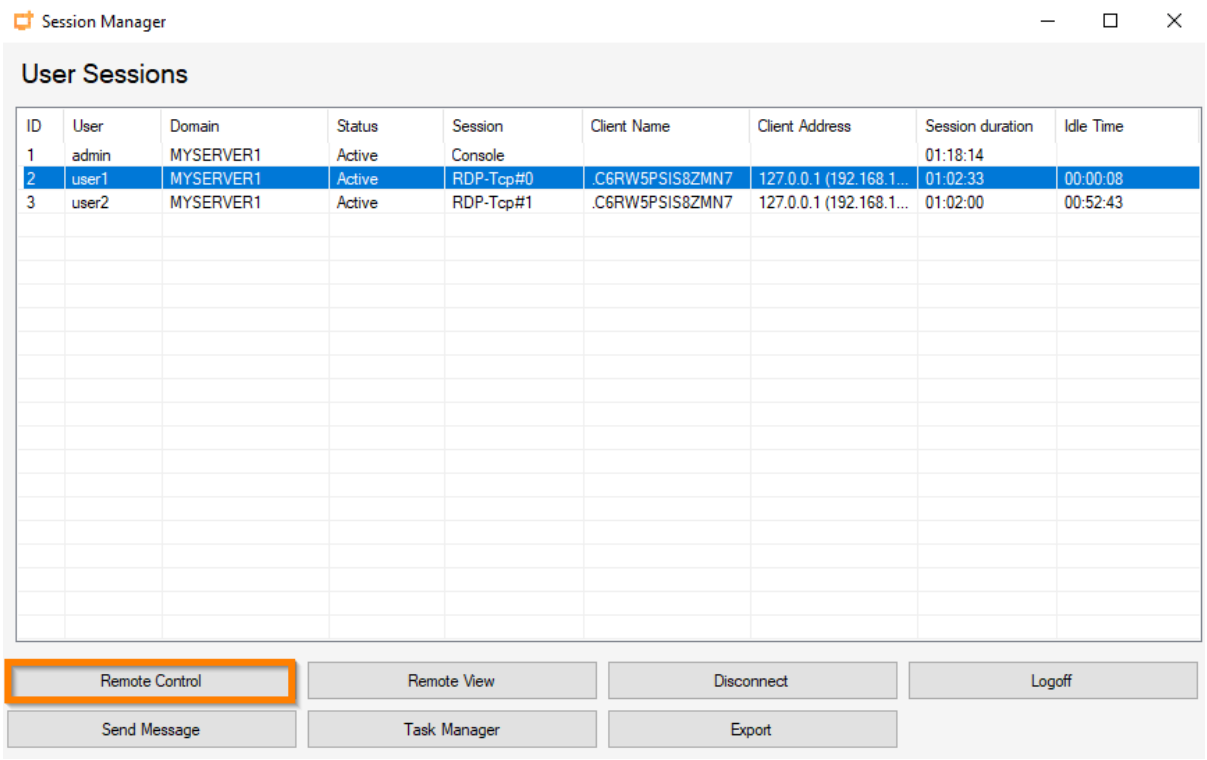
다음 운영 체제에서 관리자 계정을 사용하여 원격 세션을 통해 원격 제어를 활성화할 수 있습니다:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7
- Windows 8.1
- Windows 10 프로 이상

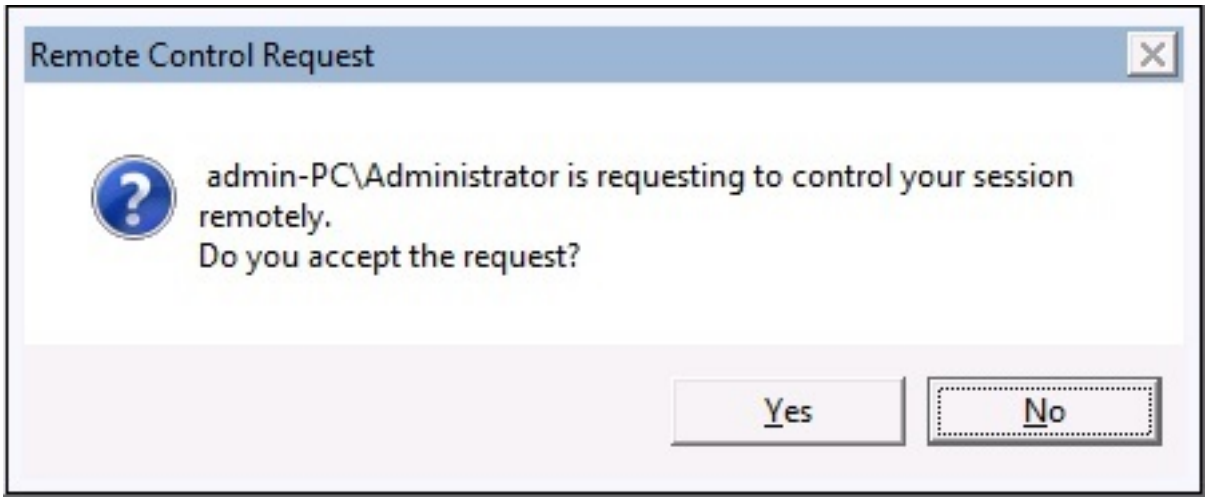
Windows XP, 2003, Vista 및 2008에서는 원격 제어 버튼이 없습니다.

Windows 2012 및 8에서는 2012 R2 또는 8.1로 업데이트하라는 메시지가 나타납니다.

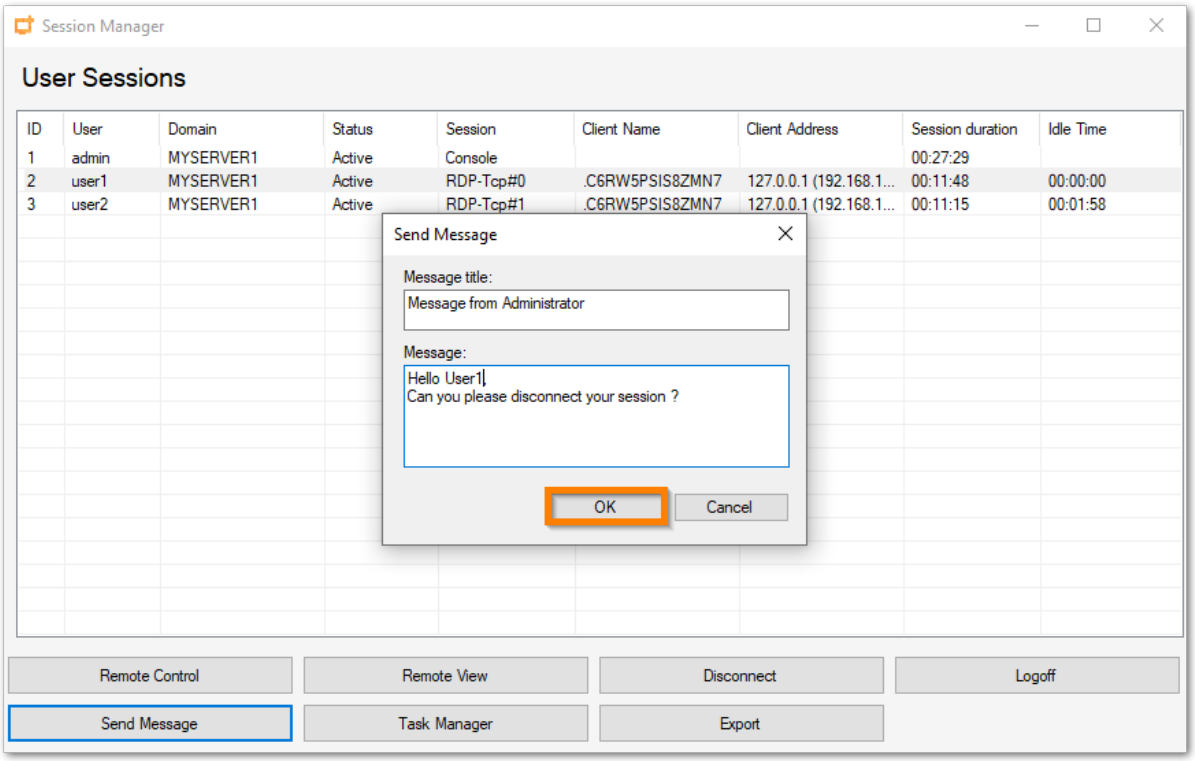
사용자의 세션에 대한 원격 제어를 활성화하면 세션을 종료하는 키보드 단축키를 나타내는 이 메시지가 나타납니다.



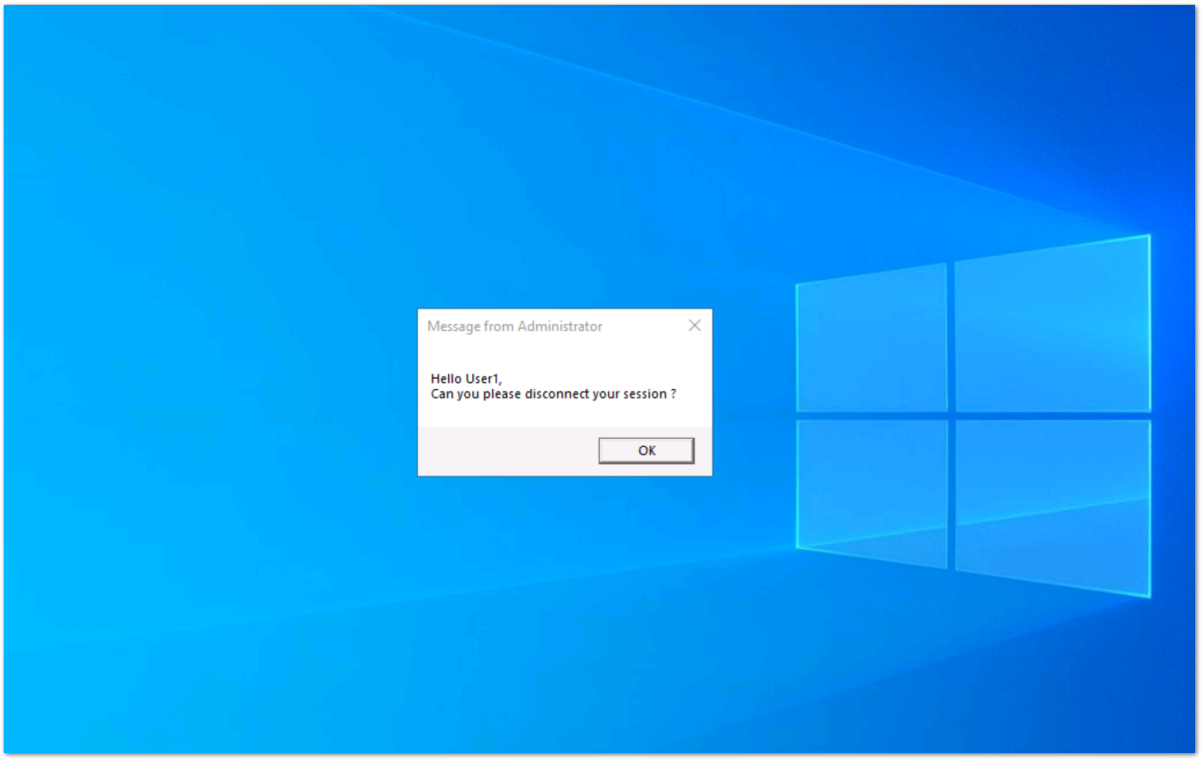
클라이언트 측에서 이 메시지는 원격 제어를 수락하는 것으로 나타납니다:



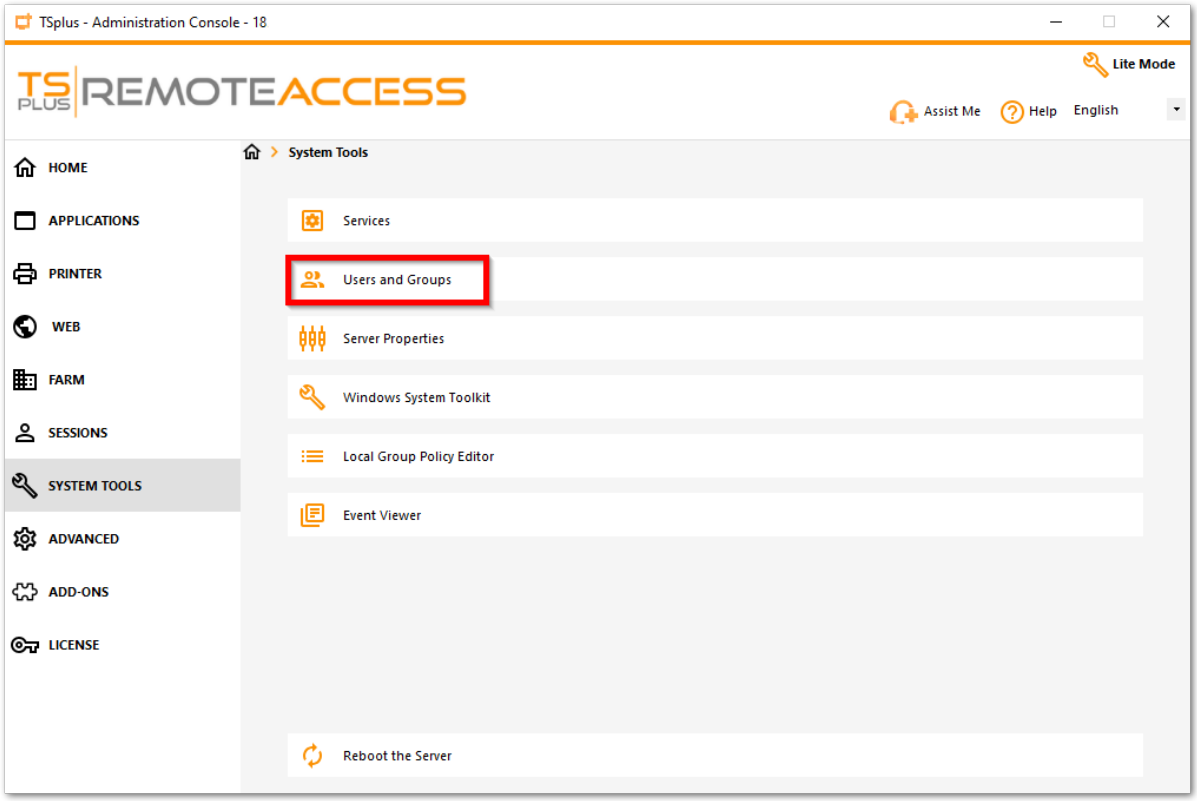
사용자에게 메시지를 보낼 수도 있습니다:



서버 측에서 전송된 메시지

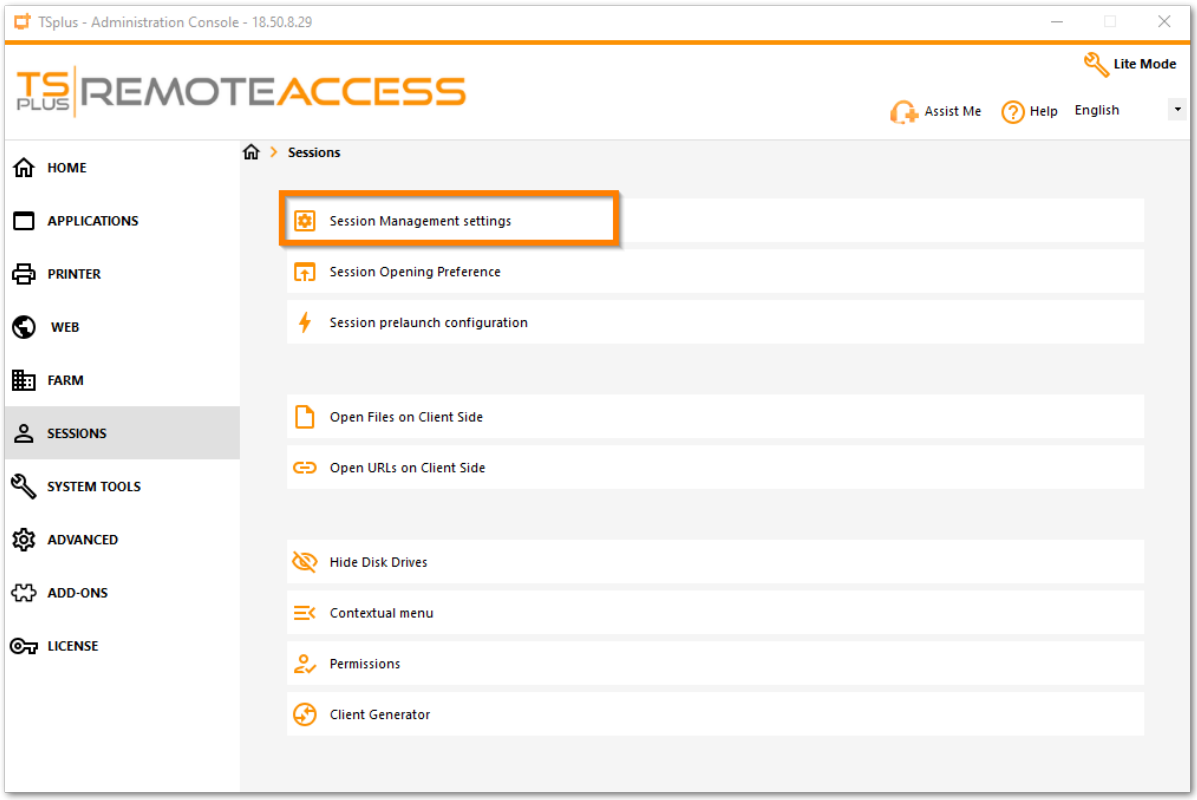


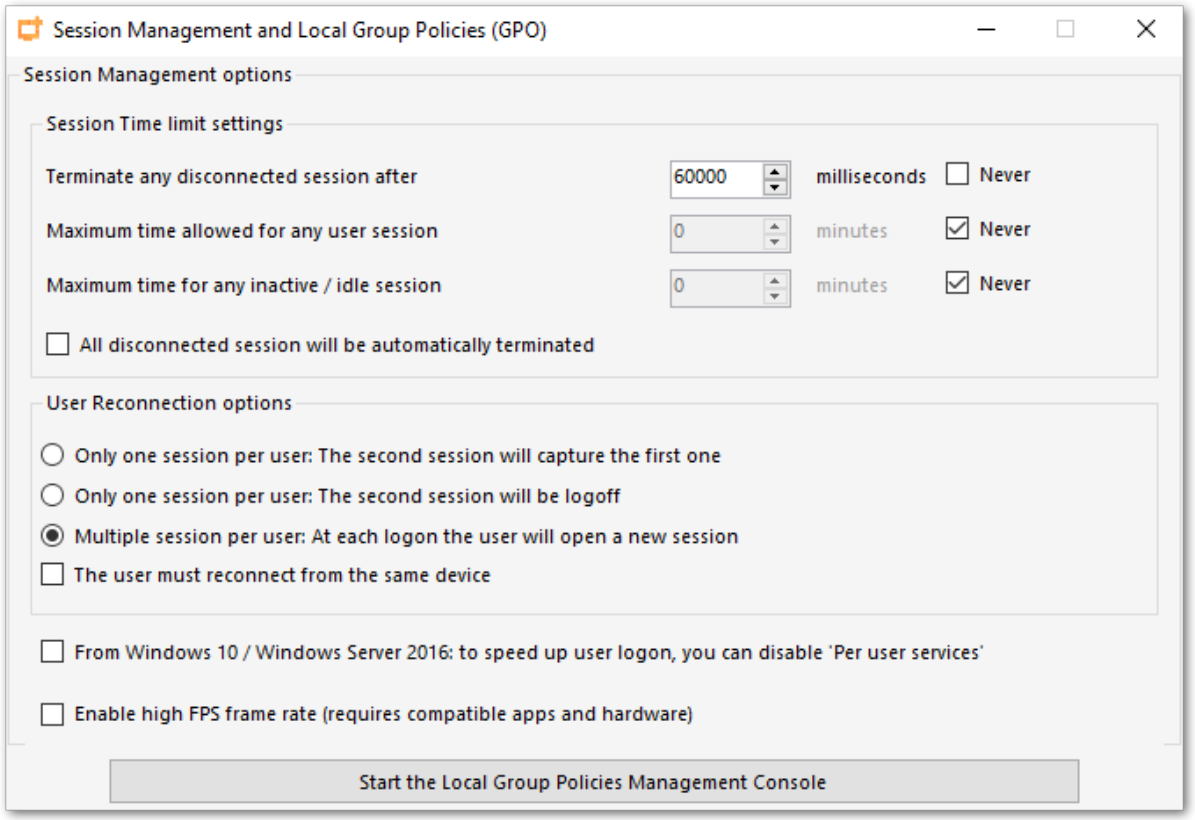
클라이언트 측에 나타나는 메시지



보세요 이 문서 자세한 정보는 다음과 같습니다.

- 세션 관리 설정(GPO) 탭을 사용하면 각 세션 및 사용자에 대한 다양한 연결 설정을 구성할 수 있습니다.

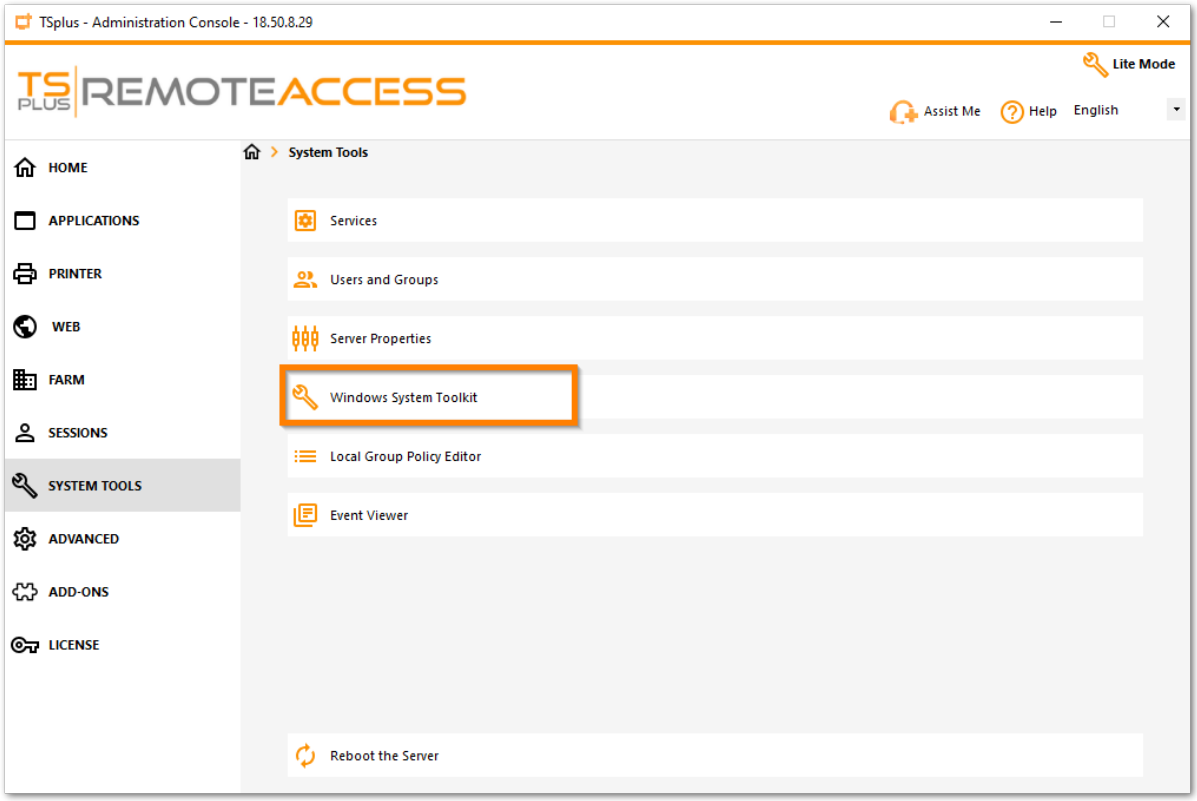


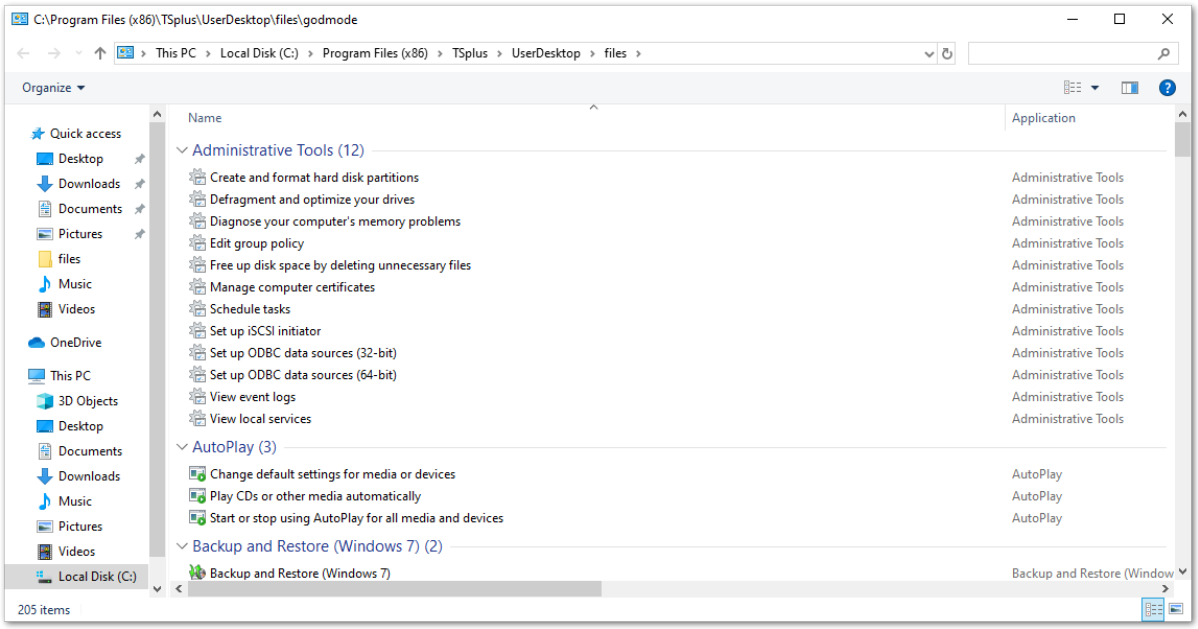


Windows Server 2016은 모든 프로세스를 사용자별로 시작하는 새로운 "사용자별 서비스"를 도입하여 사용자 로그인 시간을 느리게 만듭니다.

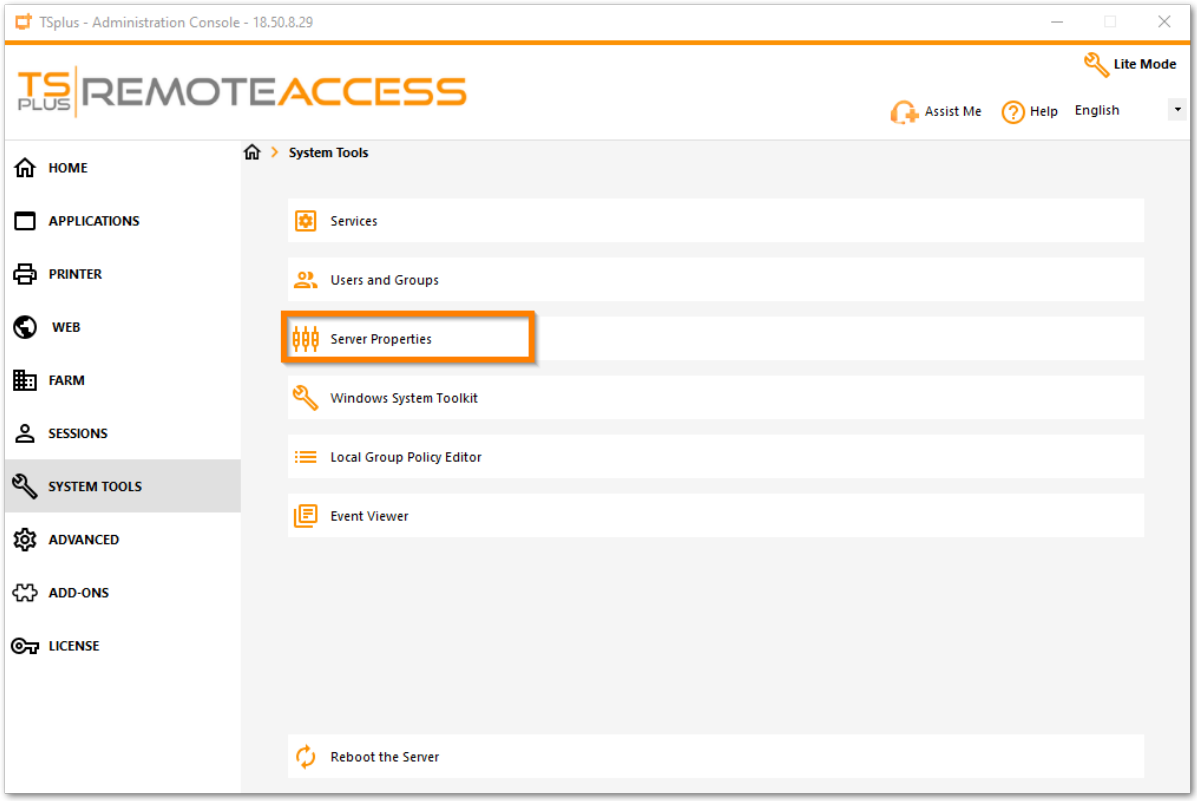
TSplus 11.70 버전 출시 이후, 당신은 **사용자 로그온 속도를 높이기 위해 사용자별 서비스 비활성화** .

- Windows 툴킷은 모든 Windows 관리 도구를 요약한 향상된 제어판입니다.

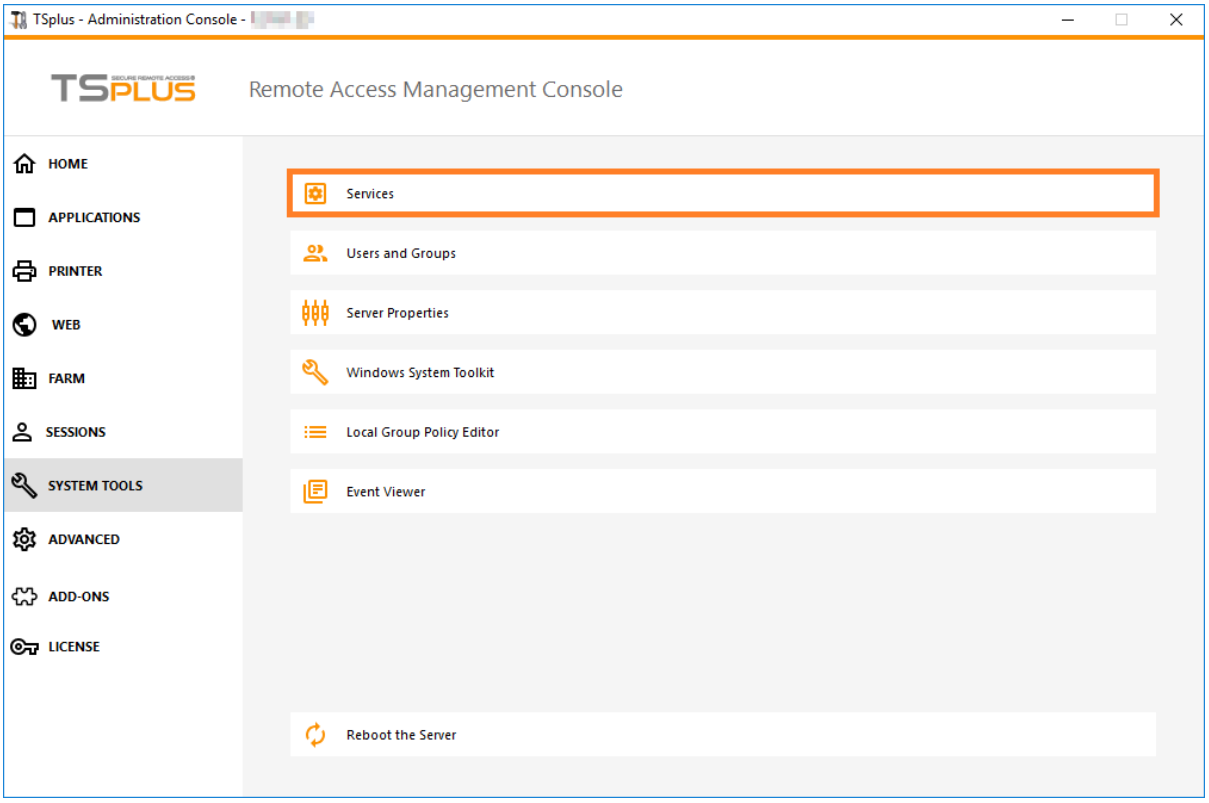




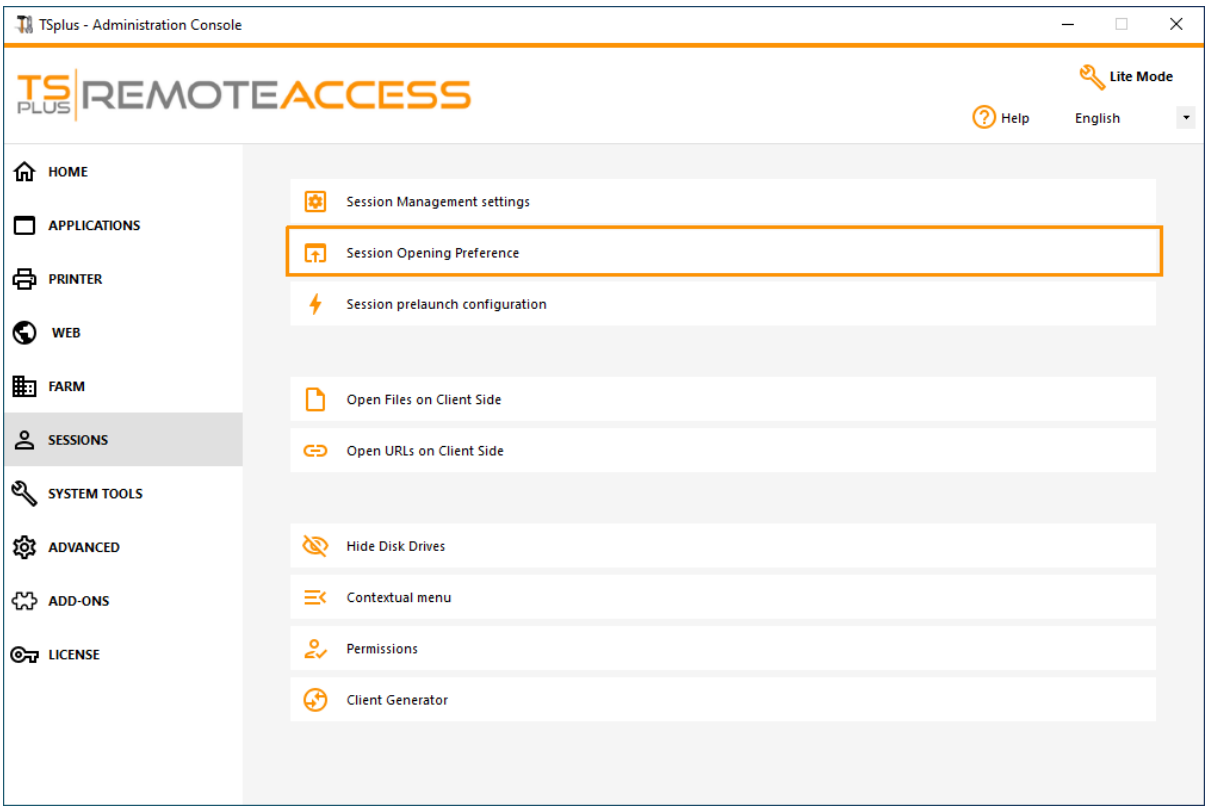
- 서버 속성 탭을 열어 제어판의 개요를 확인할 수도 있습니다.



- 서버의 모든 서비스와 그 상태를 서비스 타일에서 확인할 수 있습니다.

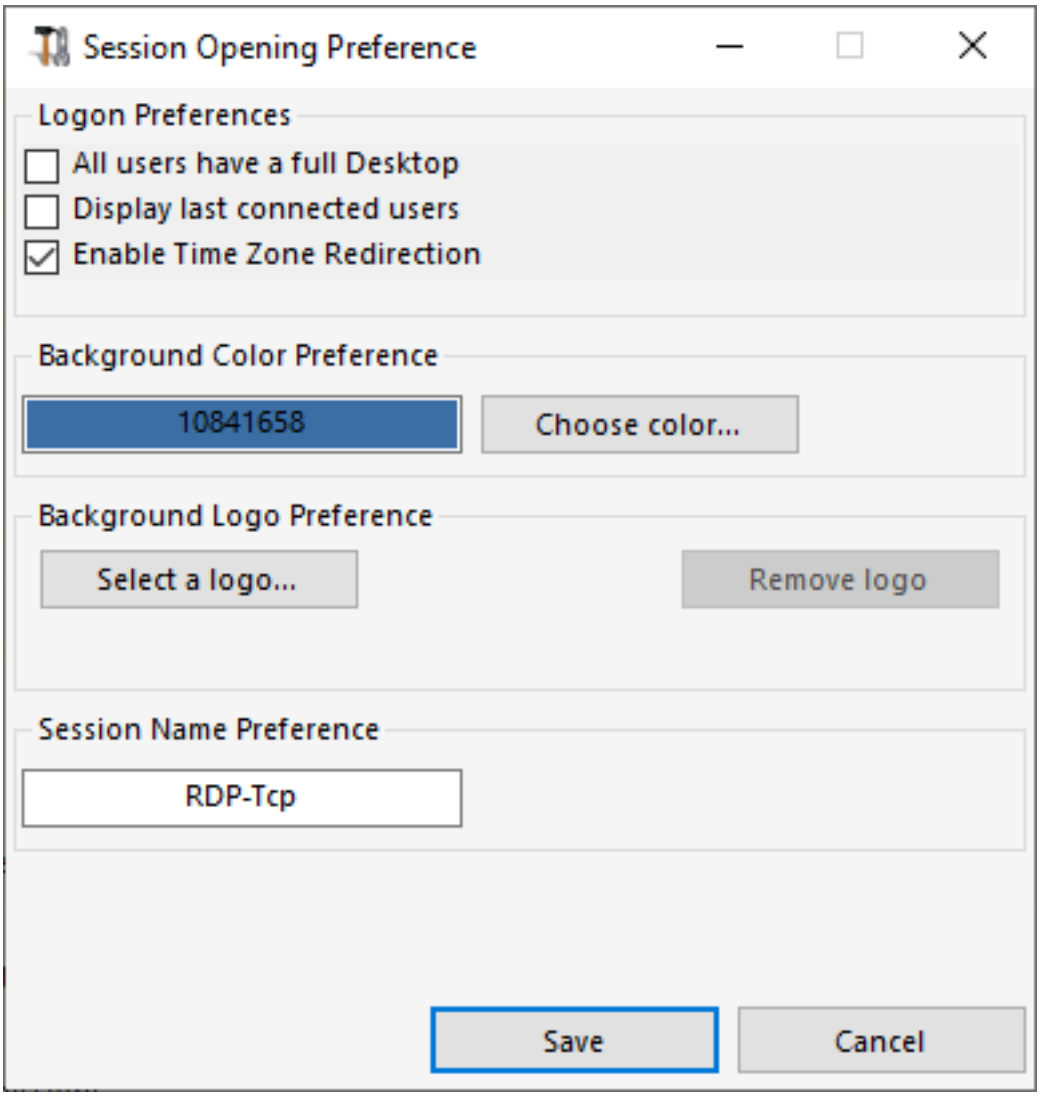


세션 열기 기본 설정을 통해 셸 세션 기본 설정, 로그인 기본 설정, 세션의 배경 색상, 자신의 로고 추가 및 원하는 대로 이름 변경을 선택할 수 있습니다.



기본적으로 이러한 로그인 기본 설정이 활성화되어 있습니다:

- “ **로그온 중 진행률 표시줄 표시** ”.
- “ **시간대 리디렉션 활성화** 클라이언트 컴퓨터가 원격 데스크톱 서비스 세션에 시간대 설정을 리디렉션할 수 있도록 하는 것입니다. 이 정책 설정을 활성화하면, 시간대 리디렉션이 가능한 클라이언트는 자신의 시간대 정보를 서버에 전송합니다.



당신은 또한 **전체 데스크탑 설정** 모든 사용자와 **마지막으로 연결된 사용자 표시 받기** 해당 상자를 선택하여 사용할 수 있습니다. **사용자 세션을 사용자 정의하세요** 새 배경 색상, 다른 로고 또는 없음 추가하고 원하는 세션 이름을 사용합니다.

- TSplus 11.70 버전 출시 이후, 사용하실 수 있습니다. **TSplus WinXshell** Windows 셸의 대안으로.

10월 10일 Windows 업데이트 이후, 원격 데스크톱을 시작할 수 있도록 사용자에게 허용한 관리자는 Windows 셸을 문제로 보았습니다.

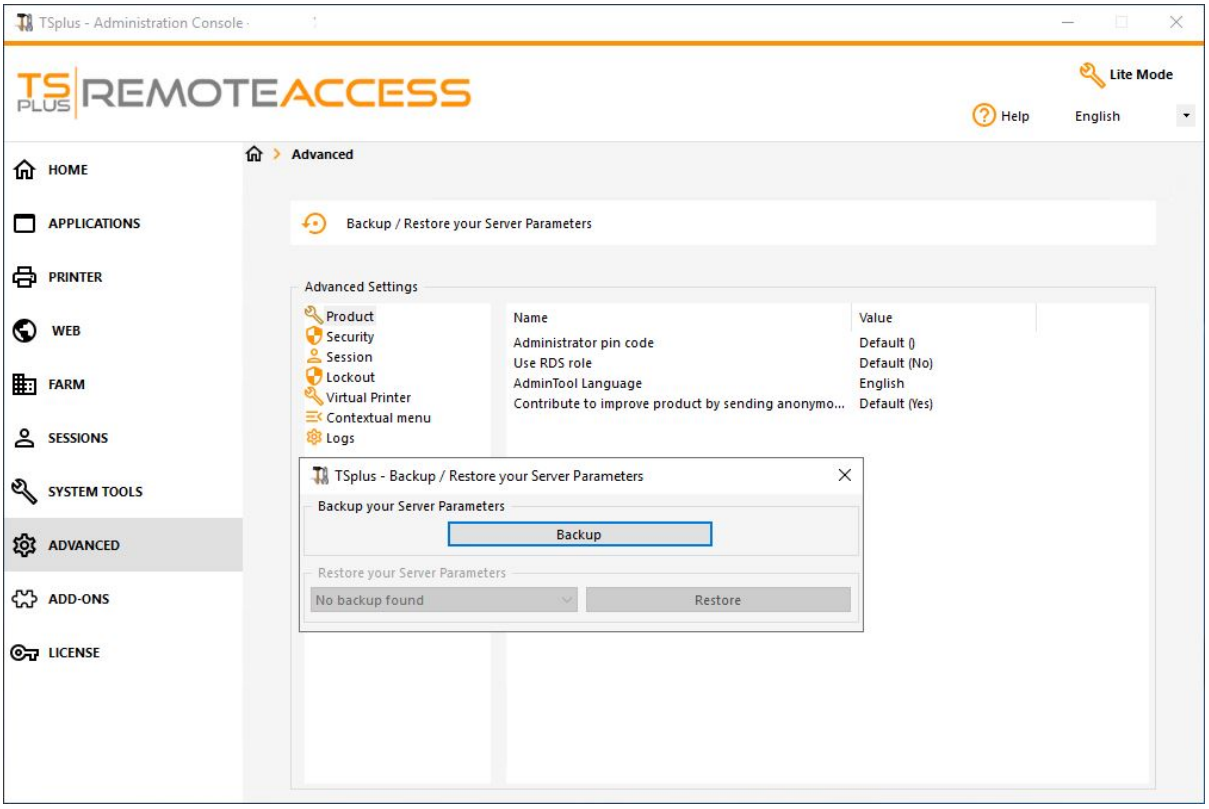
주요 문제는 Windows 10 및 Server 2016에서 전체 데스크톱이 여러 사용자에게 할당될 때 세션 열기/검은 화면 문제에 있습니다.

Windows 2016의 Windows 셸과 유사한 기능과 그래픽 경험을 제공하며, 2016 시작 버튼 및 작업 표시줄의 표시와 같은 기능을 포함합니다.

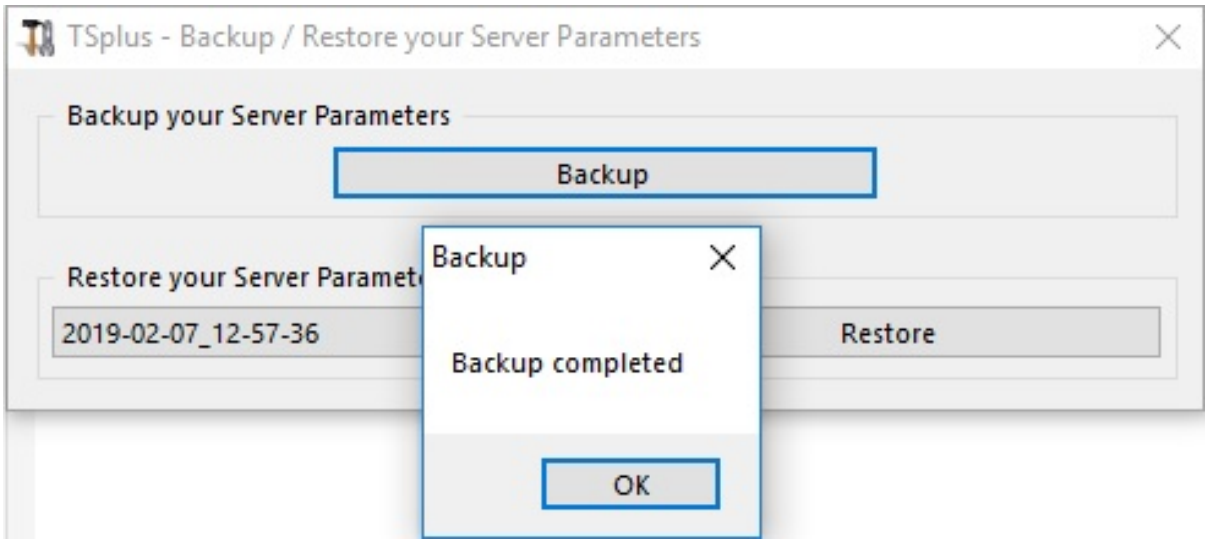
특히 유용합니다. **Windows 10 또는 Windows 16 운영 체제를 사용하십시오.** , **10명 이상의 사용자 관리** 그리고 **전체 데스크탑을 할당하고 싶습니다.** .

백업 매개변수

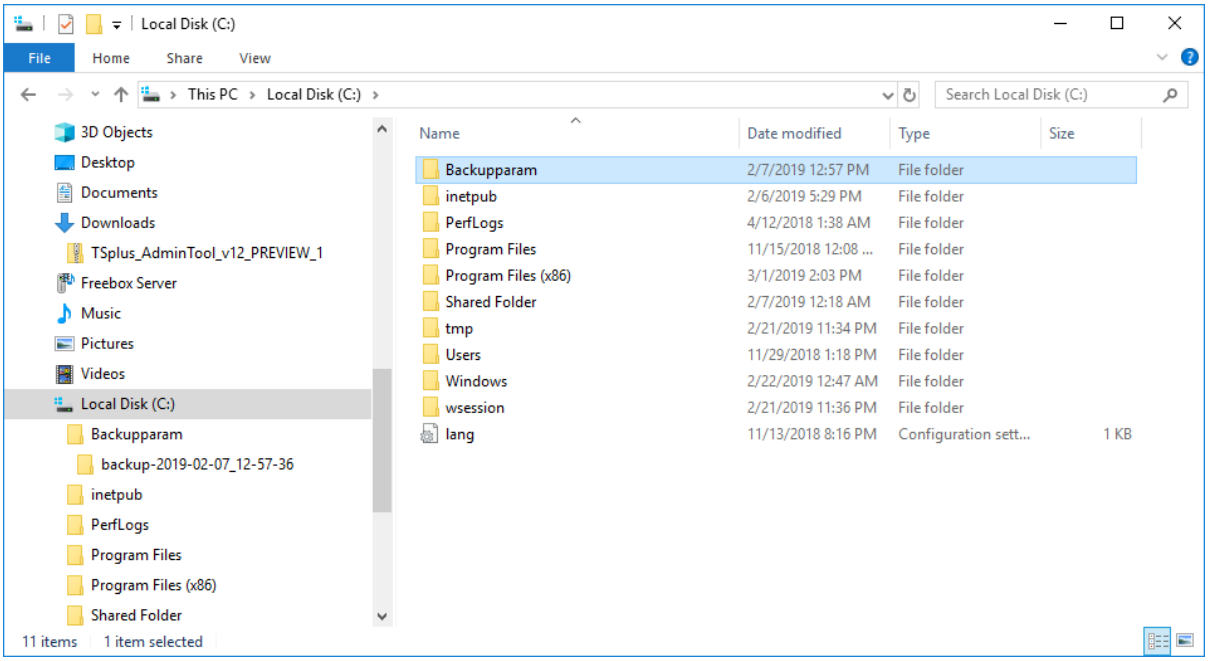
서버 매개변수를 백업하거나 복원하려면 고급 탭에서 동일한 이름의 타일을 클릭하세요.



백업 버튼을 클릭하여 백업을 생성하십시오. 이 백업은 날짜가 기록되어 복원 지점 목록에 추가됩니다.



백업 파일은 C:\Backupparam 폴더에서 찾을 수 있습니다.



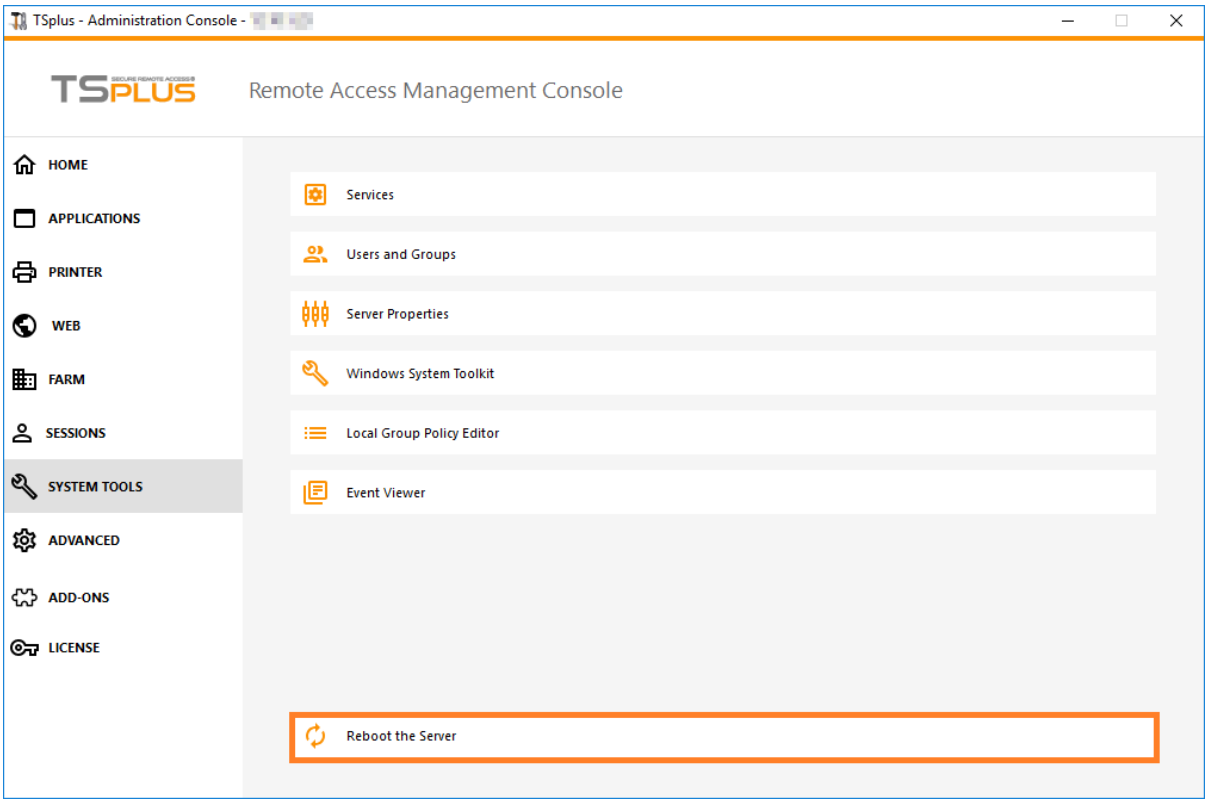
새 서버에 TSplus Remote Access를 설치한 후 폴더를 복사하고 백업을 복원하십시오.

15일 동안 시험판으로 계정 및 접근 기능이 올바른지 확인한 후 라이센스를 영구적으로 이전할 수 있습니다.

이것에 대한 더 많은 정보 문서화 .

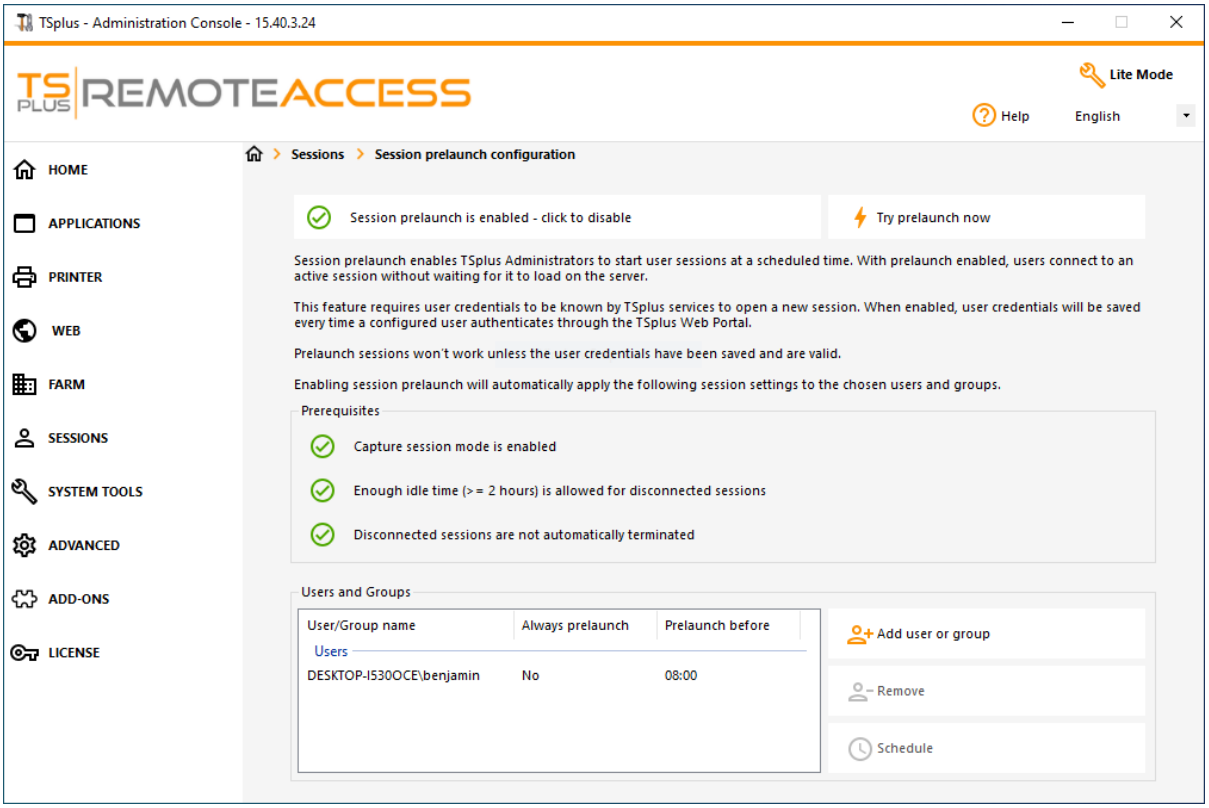
서버를 재부팅하세요

서버를 재부팅할 수 있는 "서버 재부팅 탭"을 제공합니다.


TSplus - Administration Console -
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Services
Users and Groups
Server Properties
Windows System Toolkit
Local Group Policy Editor
Event Viewer
Reboot the Server

세션 사전 시작

세션 > 설정 탭의 Admintool에서 “세션 사전 시작 구성” 타일을 클릭하여 세션 사전 시작 구성 메뉴에 접근합니다.

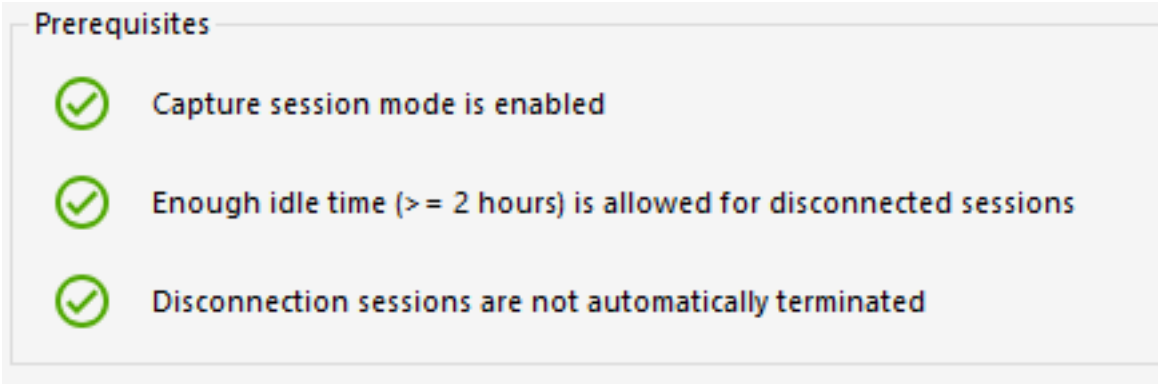


개요

세션 사전 시작 기능은 TSplus Remote Access 관리자가 사용자 세션을 예정된 시간 이전에 시작하도록 구성할 수 있게 해줍니다. 아이디어는 모든 구성된 사용자의 세션을 미리 준비하고 로드하여 사용자가 연결할 때 특정 세션을 캡처할 수 있도록 하는 것입니다. 이를 통해 연결 대기 시간을 몇 분에서 몇 초로 줄일 수 있습니다.

필수 조건

프리런칭을 위해 여러 가지 전제 조건이 충족되어야 합니다.



세션을 캡처하기 위해, **세션 캡처 모드를 활성화해야 합니다.** 이것은 다중 세션 구성이 사용자에게 필수인 경우 이 기능을 사용할 수 없음을 의미합니다.

2 - 사용자가 연결하고 세션을 캡처할 때 미리 준비된 세션이 존재해야 하므로 (로그아웃되지 않은 상태여야 함), **연결이 끊어진 세션에 대해 최소 2시간의 유휴 시간이 허용되어야 합니다.** 물론 연결이 끊어진 세션이 절대 로그오프되지 않도록 세션 설정을 조정할 수도 있습니다.

3 - 준비된 세션은 전체 리소스 사용량을 줄이기 위해 로드되면 연결이 끊깁니다. **세션 설정은 연결이 끊어진 세션을 자동으로 로그오프하지 않도록 구성되어야 합니다.**

중요한 참고 사항! 세션 사전 시작 기능이 활성화된 후 각 구성된 사용자는 TSplus 서비스가 구성된 사용자 세션을 열 수 있도록 TSplus 웹 포털을 통해 최소한 한 번 인증해야 합니다.

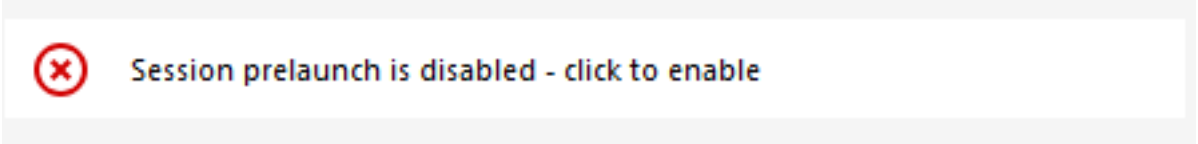
세션 사전 시작 호환성

세션 사전 시작은 HTML5 세션 및 생성된 클라이언트 또는 mstsc를 통해 열리는 일반 RDP 세션과 호환됩니다.

그러나 특정 프로그램을 열기 위해 만든 Remote App 연결 또는 사용자 지정 RDP 연결과는 호환되지 않습니다.
결과적으로, TSplus 웹 애플리케이션 포털에서 오는 연결은 지원되지 않습니다.

기능을 활성화하십시오

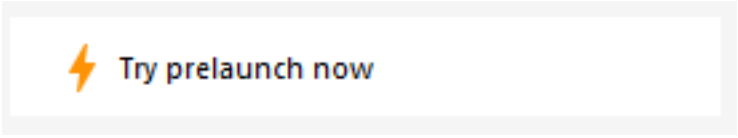
세션 사전 시작 기능을 활성화하려면, 창 상단 근처에 있는 "세션 사전 시작이 비활성화되었습니다 - 활성화하려면 클릭"이라는 타일을 클릭하면 됩니다.



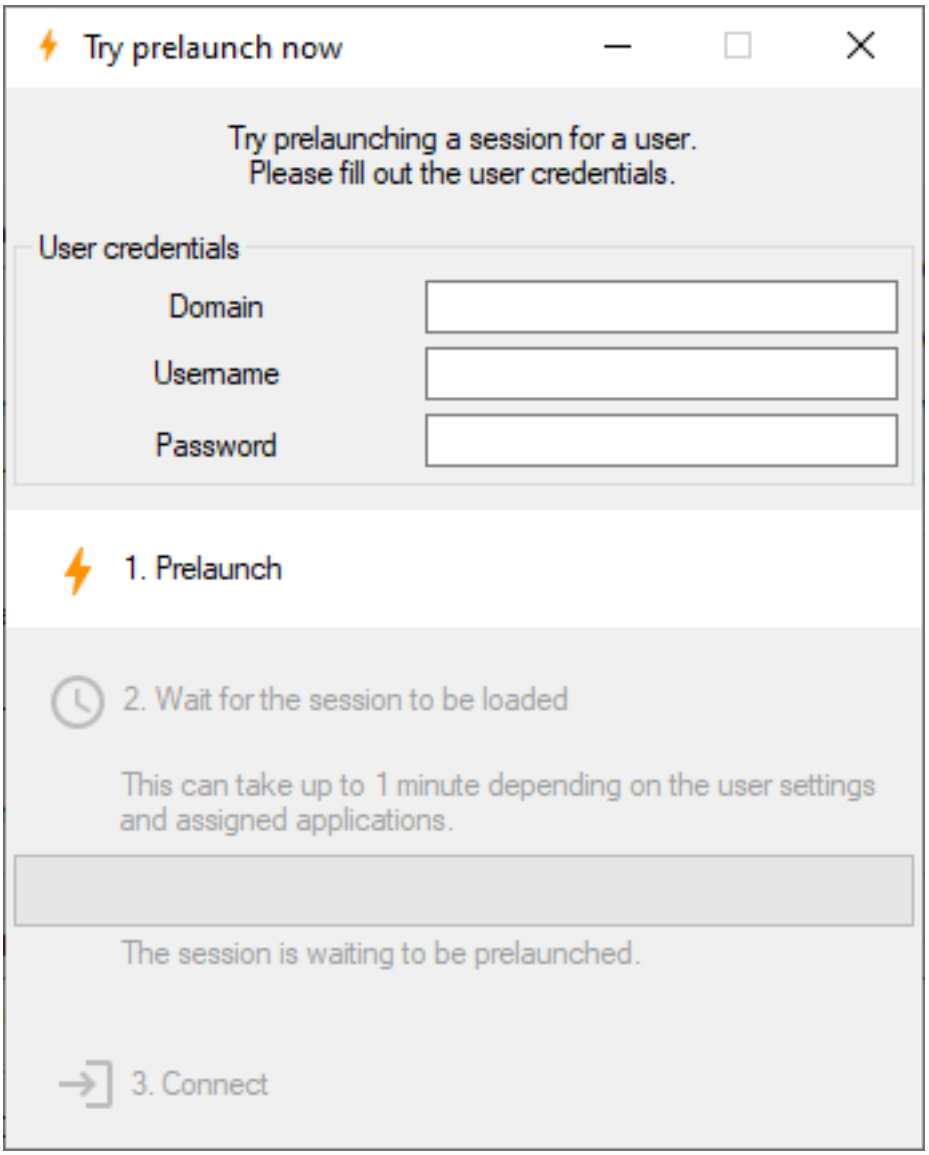
세션 사전 시작을 활성화할 때 필수 조건이 충족되지 않으면 필수 조건을 충족하고 기능을 사용하기 위해 세션 설정을 자동으로 구성할 것인지 묻는 메시지가 표시됩니다. 세션 설정을 변경하면 재부팅이 필요할 수 있습니다.

세션 사전 시작 테스트

기능을 활성화하면 상단의 “지금 사전 출시 시도” 버튼을 클릭하여 기능을 빠르게 테스트할 수 있습니다.



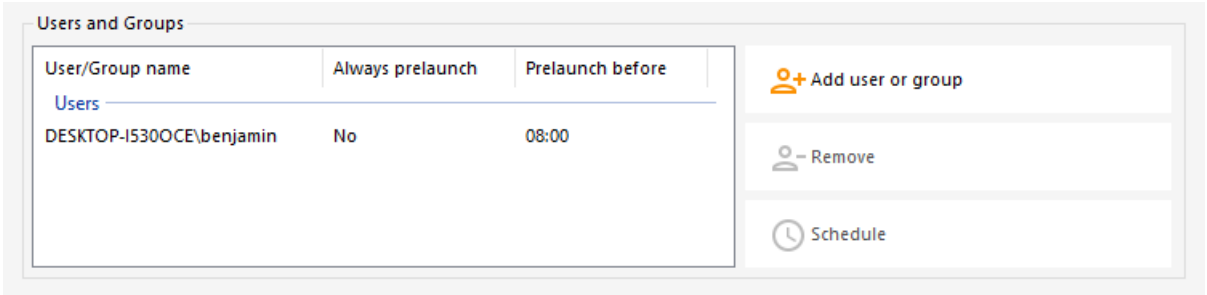
나타나는 창에서 TSplus 서비스가 이 특정 사용자의 세션을 미리 시작할 수 있도록 사용자 자격 증명을 입력하십시오.



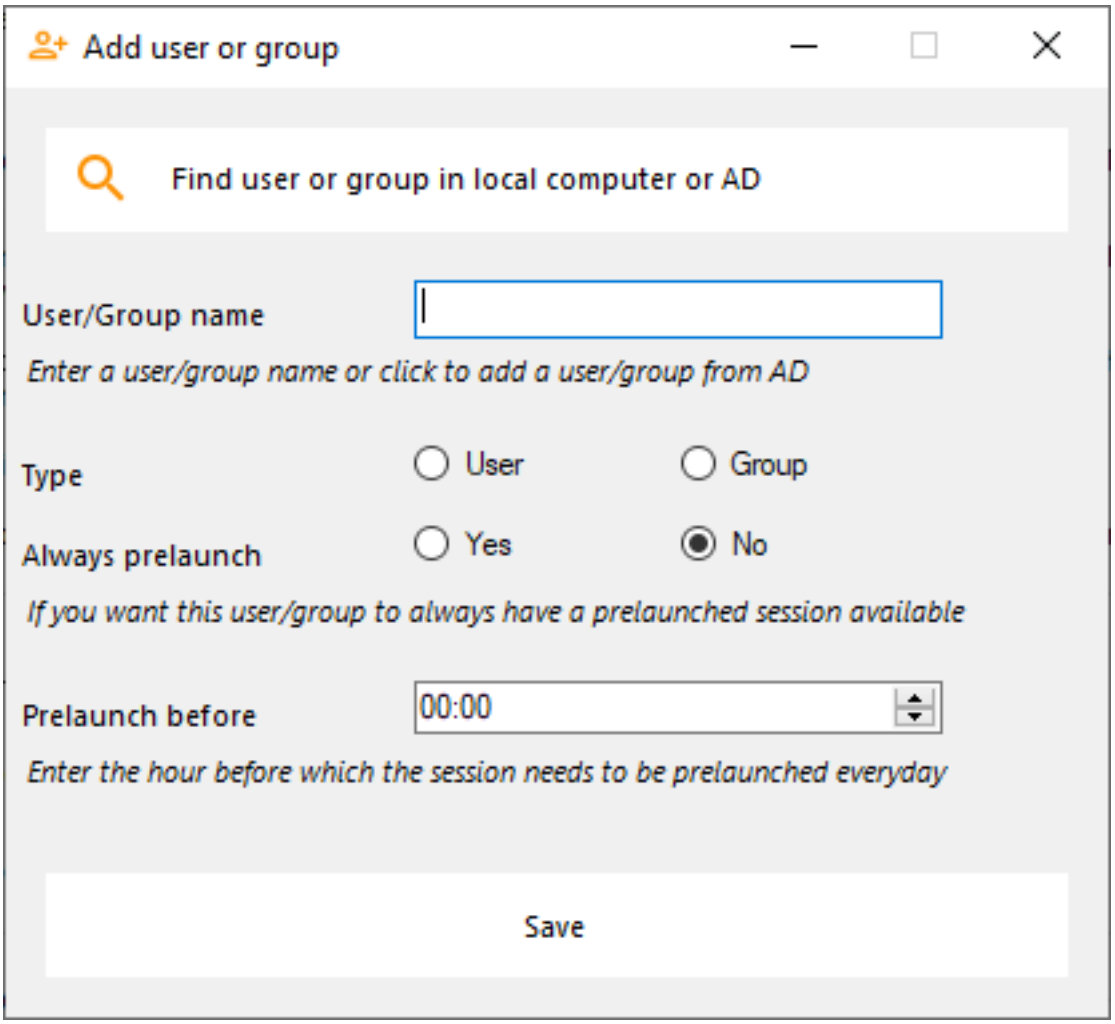
“Prelaunch”를 클릭하여 이 사용자의 새 세션을 시작하고 로드합니다.
완전히 로드될 때까지 기다린 후 "연결"을 클릭하여 새로 로드된 세션을 캡처하세요.

구성된 사용자 및 그룹 관리

세션 사전 시작 사용자 및 그룹을 추가하려면 “사용자 또는 그룹 추가”를 클릭하면 됩니다.
구성된 사용자/그룹 목록에서 일치하는 사용자/그룹을 선택한 다음, '사전 시작 전' 시간을 변경하려면 “일정”을 클릭하거나 사용자를 제거하려면 “제거” 버튼을 클릭하십시오.



“사용자 또는 그룹 추가”를 클릭한 후, 구성할 사용자/그룹 이름과 세션이 로드되어야 하는 시간을 요청받게 됩니다. 이 시간을 여기에서는 “사전 시작 전”이라고 합니다.
이 사용자/그룹이 연결할 때 항상 세션이 미리 시작되도록 구성할 수 있으며, "항상 미리 시작" 옵션에서 "예"를 선택하여 일정을 잡을 필요가 없습니다.



Apache 리버스 프록시의 Websockets 지원 설정 방법

1. 먼저 다음 변수를 false로 변경하십시오. www\software\html5\settings.js > W.xhrreverse = false; (이를 false로 변경하지 않으면 항상 웹소켓 대신 xhr을 시도하게 되며, 우리는 더 이상 원하지 않습니다.)

2. 프록시_wstunnel 지원으로 Apache 설치하기 (프록시_wstunnel이 없는 이전 Apache는 지원되지 않습니다!)

3. Apache 구성에서 허용 (httpd.conf 등) 다음 모듈들입니다. LoadModule proxy_module modules/mod_proxy.so LoadModule proxy_http_module modules/mod_proxy_http.so LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so

4. html5 메인 포털에 서브폴더 “/html5/”를 통해 접근하고자 한다고 가정해 보겠습니다. 예를 들어 http://your_ip_or_domain.net/html5/ 그리고 TSplus가 서버 “intranetxyz”의 인트라넷에 설치되어 있다면, 다음을 구성 파일(httpd.conf 등)에 추가하십시오.

   ProxyPass /html5 http://intranetxyz:80 ProxyPassReverse /html5 http://intranetxyz:80

   ProxyPass “ws://intranetxyz:80/socket.io/websocket_https”

   ProxyPass “ws://intranetxyz:80/socket.io/websocket”

   ProxyPass “ws://intranetxyz:80/socket.io/flashsocket_https”

   ProxyPass “ws://intranetxyz:80/socket.io/flashsocket”

5. Apache를 재시작하여 변경 사항을 적용하십시오.

이중 인증

이중 인증은 보안의 추가 계층을 추가합니다. **사용자의 세션에 대한 접근을 방지합니다. 비밀번호를 아는 사람이 있더라도.** .

두 가지 다른 요소의 조합이 더 높은 수준의 보안을 달성하는 데 사용됩니다:

1. 그들이 아는 무언가, **비밀번호** .

2. 그들이 가진 것, 하나 **인증 앱이 설치된 스마트폰과 같은 장치.** .

다음 인증기 앱 중 하나를 사용하여 진행할 수 있습니다. 이러한 앱은 다양한 플랫폼에서 사용할 수 있습니다.

- Authy
- 구글 인증기
- Microsoft Authenticator

사용자가 원격 세션에 로그인할 때마다 비밀번호와 모바일 전화에서 사용할 수 있는 인증 코드가 필요합니다. 설정이 완료되면 인증기 앱이 로그인할 수 있도록 인증 코드를 표시합니다. 장치가 오프라인 상태일 때도 작동합니다.

또는 인증 코드를 수신할 방법을 결정할 수 있습니다. **SMS** 이 경우, 무료 계정을 만들어야 합니다. 트윌리오 .

그 **2FA 코드 생성은 TOTP입니다.** (시간 기반 일회용 비밀번호), 따라서 단일 사용을 위한 것입니다.

따라서 이미 사용된 2FA 코드를 재사용할 수 없습니다. 이는 사용자가 코드를 입력하는 동안 관찰하여 2FA 코드를 도용하고 사용하는 것을 방지합니다.

요구 사항

이중 인증은 TSplus Remote Access를 요구합니다. **모바일 웹** 또는 **기업** 에디션.

이중 인증이 지원됩니다:

- TSplus Remote Access **웹 포털** HTML5 및 Remoteapp 연결 모두에 대해
- TSplus 연결 클라이언트, 버전 15.30.3.15 이후에 생성된 클라이언트를 위해, 2FA 지원이 명시적으로 활성화되었습니다. 확인하세요. 2단계 인증을 위한 휴대용 클라이언트 생성기 지원
- 2FA는 Windows 사용자와 관련이 있으며 웹 자격 증명과는 관련이 없습니다.

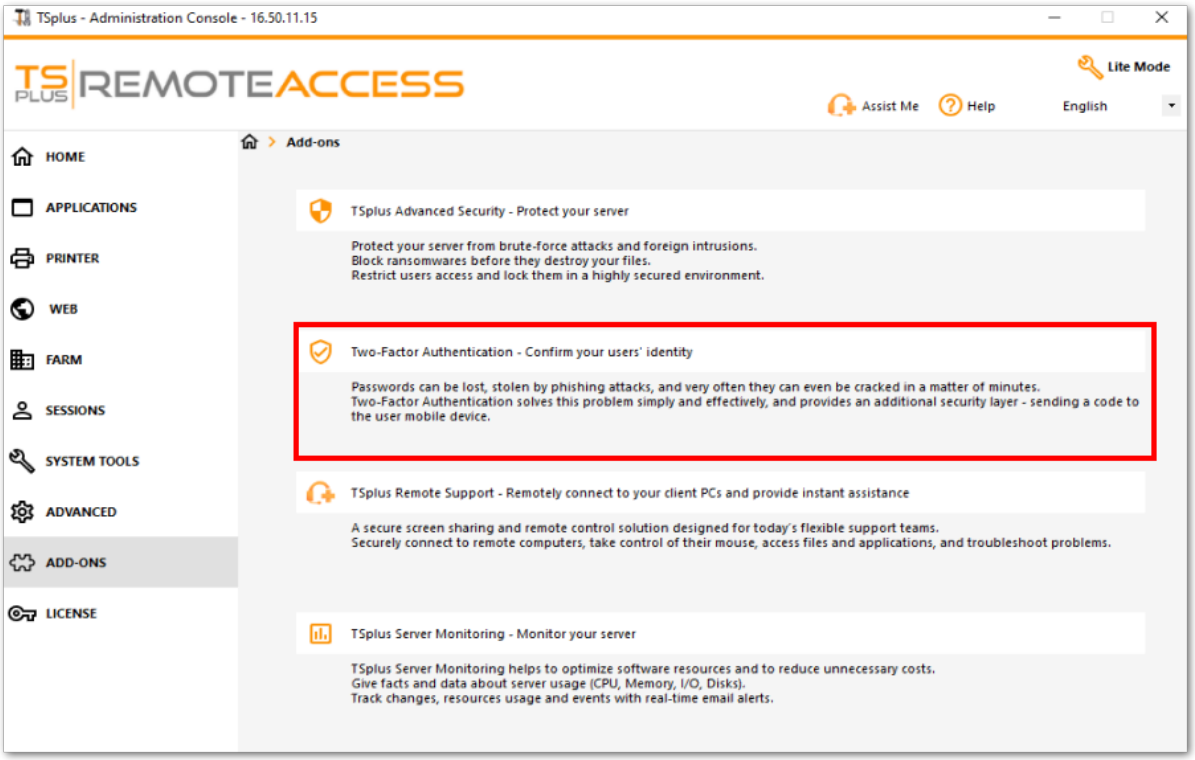
이 인증 모드는 표준 Microsoft Remote Desktop 클라이언트(mstsc.exe)를 통한 로그인을 지원하지 않습니다.

보다 안전한 솔루션을 제공하기 위해 2FA가 활성화된 사용자에 대한 RDP 연결이 거부됩니다.

사전 조건으로, TSplus 서버와 장치가 제시간에 있어야 합니다. 다음을 참조하십시오. 시간 동기화 그리고 설정 구성 정보에 대한 추가 섹션.

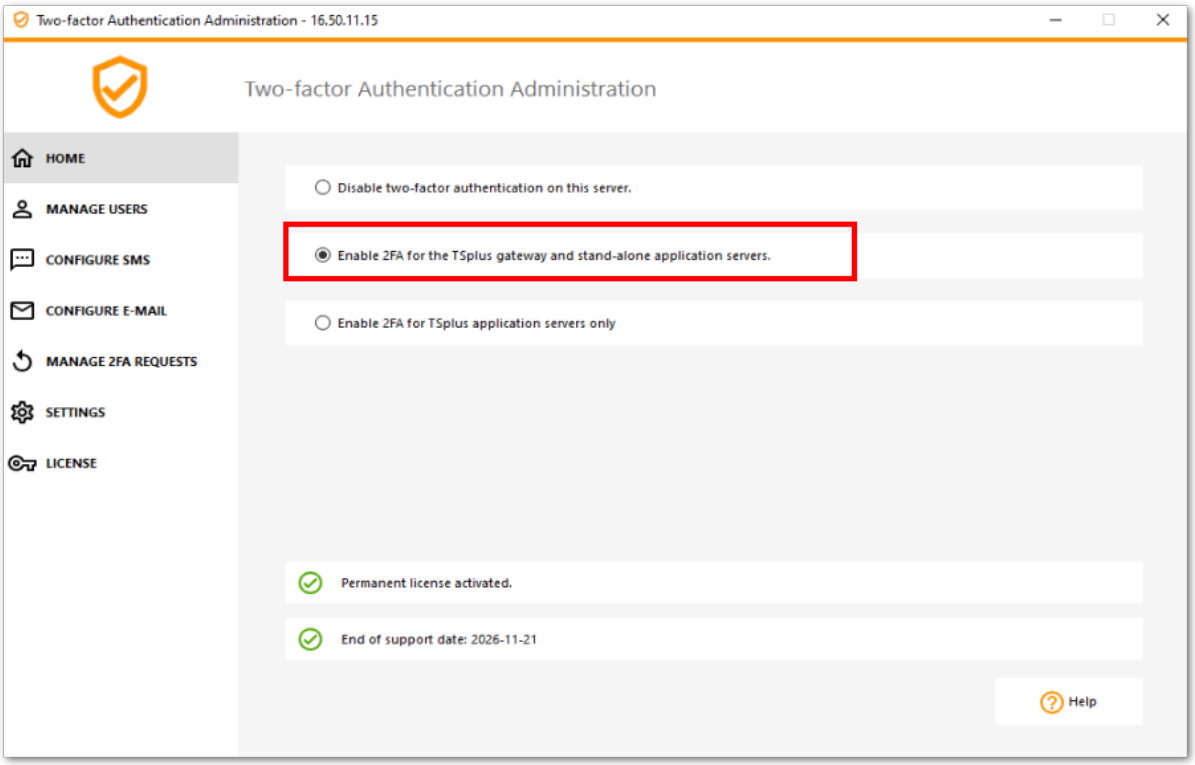
이중 인증 추가 기능 라이선스 활성화

Two-Factor Authentication 기능은 AdminTool의 Add-On 탭에서 찾을 수 있습니다.



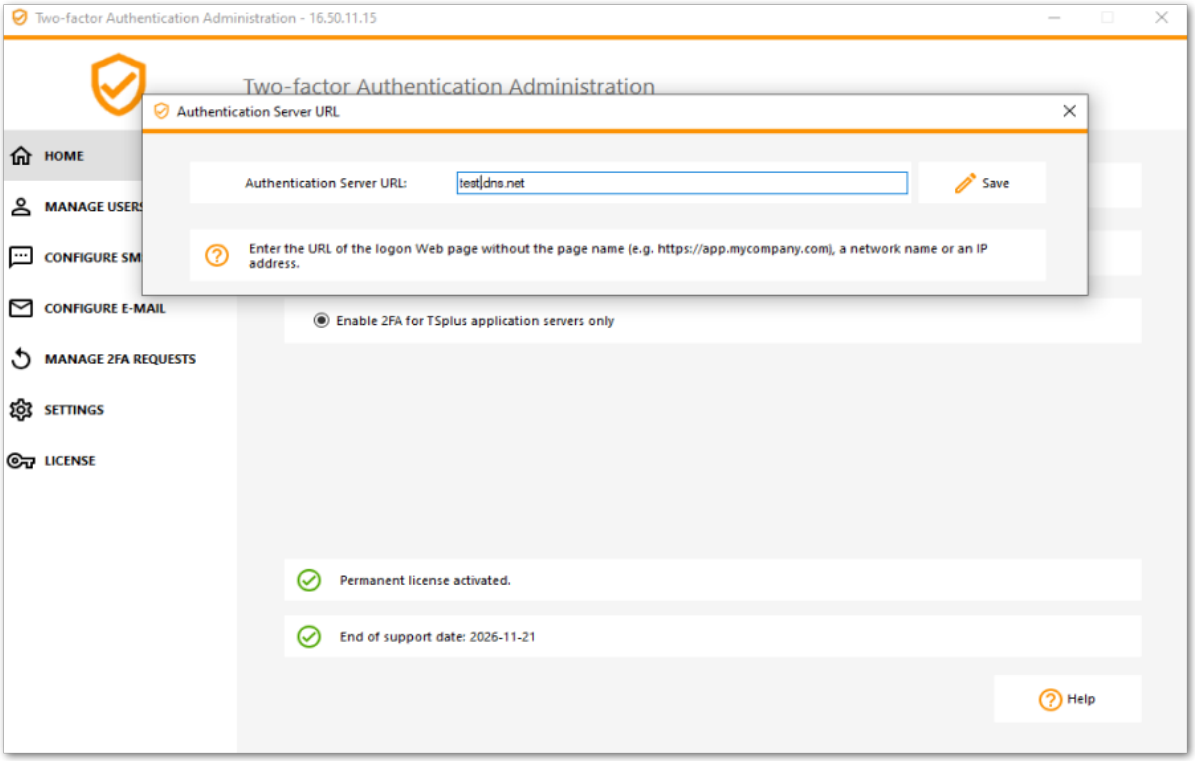
다음 단계를 수행하여 TSplus 서버 또는 배포에 대한 이중 인증을 활성화하십시오. TSplus 배포가 여러 서버를 사용하도록 구성된 경우, 사용자에 대한 단일 진입점으로 노출된 TSplus 서버 또는 리버스 프록시 역할을 하는 서버에서 이 작업을 수행하십시오.

1. 이중 인증 관리 애플리케이션을 엽니다. 이중 인증 상태와 라이센스 상태가 표시됩니다.

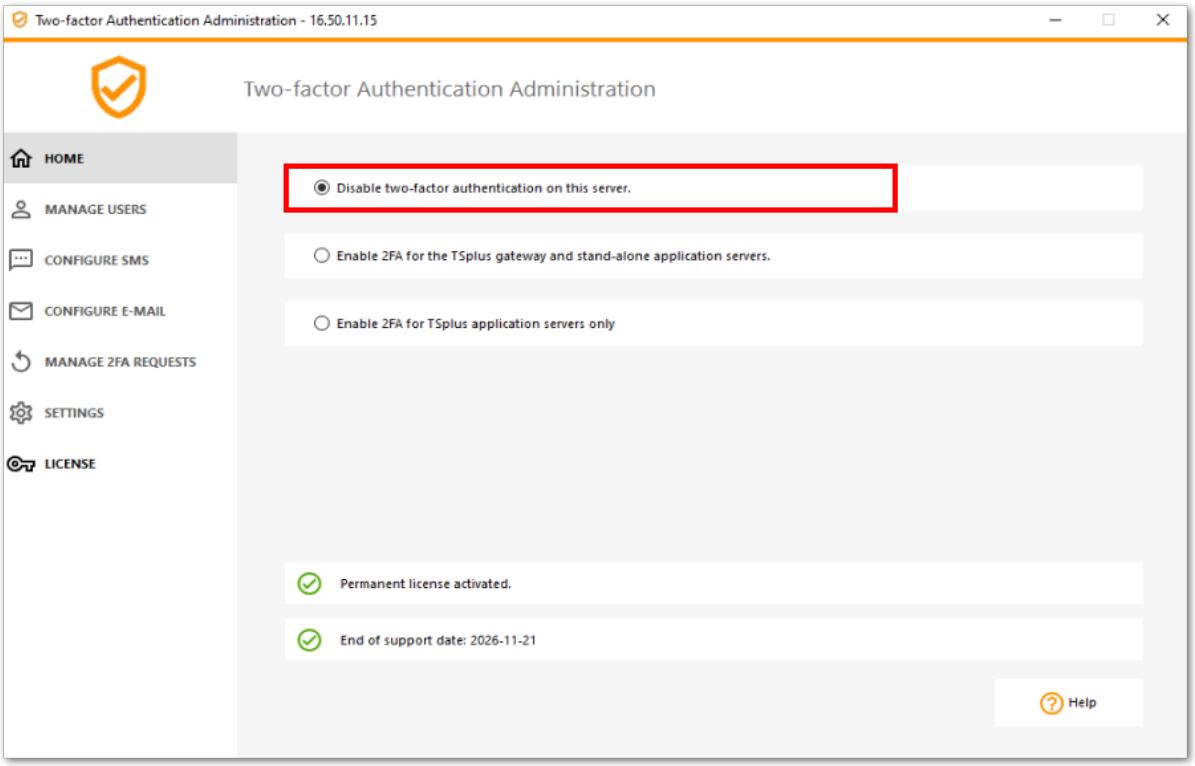


기본적으로, TSplus 게이트웨이 및 독립형 애플리케이션 서버에 대해 2FA가 활성화되어 있습니다.

TSplus 애플리케이션 서버에 대해서만 인증 서버 URL을 입력하여 활성화할 수 있습니다.



비활성화하거나:

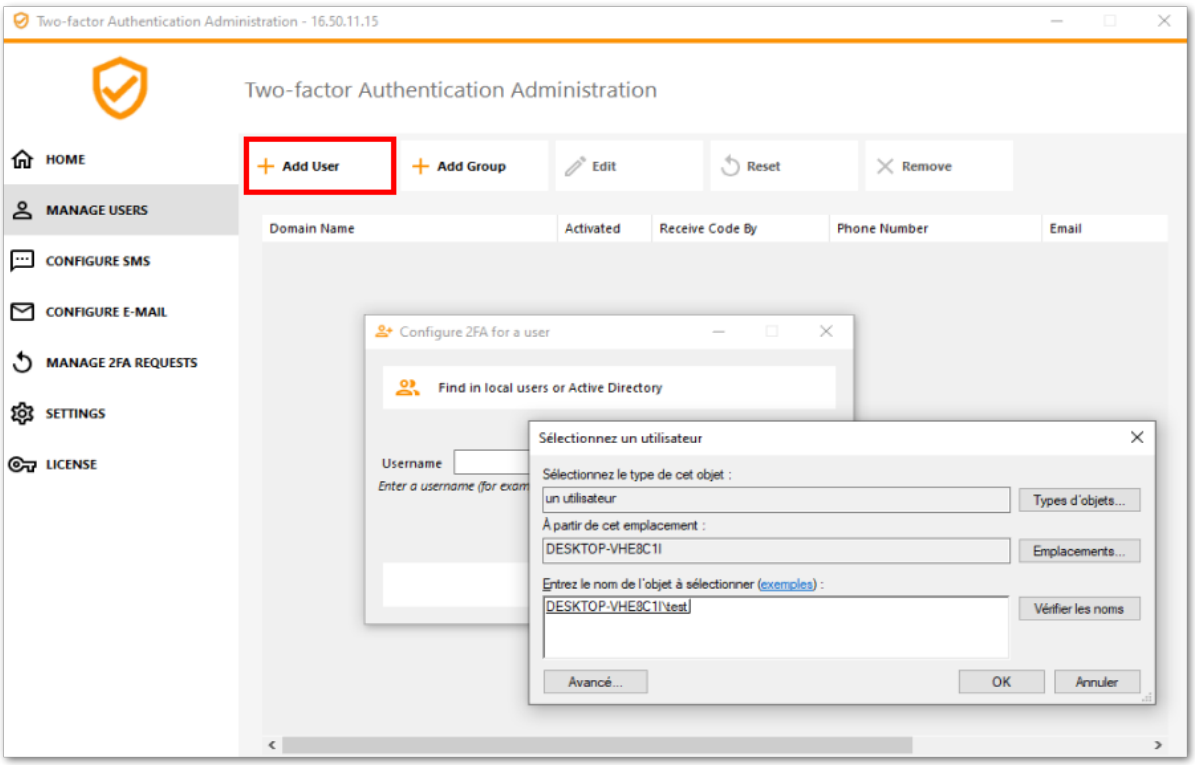


사용자 및 그룹 추가

이중 인증이 활성화되면 사용자를 이중 인증에 대해 구성할 수 있습니다.

1.
   이중 인증 관리 애플리케이션에서 클릭하십시오. 사용자 관리 탭.

2.
   그런 다음 클릭하십시오 추가 사용자 및/또는 사용자 그룹을 선택합니다. 사용자 또는 그룹 선택 상자가 열립니다.



3. 필요한 만큼 사용자와 그룹을 추가한 후 클릭하세요. 좋습니다. 사용자와 그룹이 목록에 추가되고 이중 인증이 활성화됩니다.

사용자/그룹을 추가하는 명령어는 다음과 같습니다.
가능한 인수의 3가지 유형:

도메인 이름만
TwoFactor.Admin.exe /addusers domainName1

- 기본값으로 사용자를 추가합니다(수신 방법 = 앱, 이메일 및 전화 필드가 입력되지 않음).

도메인 이름 및 수신 방법
TwoFactor.Admin.exe /addusers domainName1;SMS

- 원하는 수신 방법으로 사용자를 추가하지만 활성화하려고 시도하지 않습니다.

도메인 이름, 접수 방법, 전화 필드(비어 있어도), 이메일 필드(비어 있어도)
*TwoFactor.Admin.exe /addusers domainName1;SMS;+33606060606; username1@truc.net 도메인 이름2;이메일;; username2@truc.net 도메인이름3;SMS;+33606060607;도메인이름4

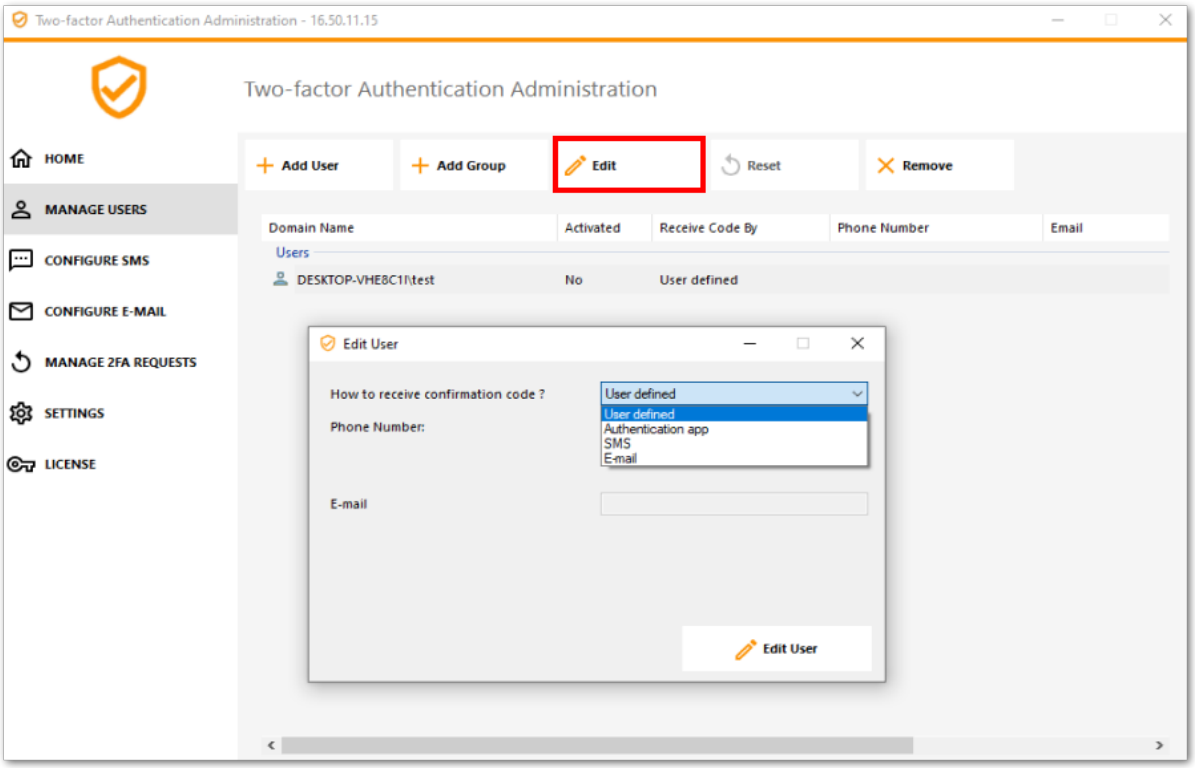
- HMI에서와 동일한 동작으로, 사용자를 추가한 후 올바른 정보로 편집할 때: 사용자를 활성화하려고 합니다.

마지막 예제에서 보여준 것처럼 여러 사용자를 표시할 수 있습니다(공백으로 구분). 사용자의 다양한 필드는 세미콜론으로 구분됩니다.

단일 그룹용:
TwoFactor.Admin.exe /addgroups group1 group2 group3

사용자 편집

같은 타일에서 사용자를 선택하고 “편집” 버튼을 클릭하여 사용자가 인증 코드를 받는 방식을 수정할 수 있습니다.

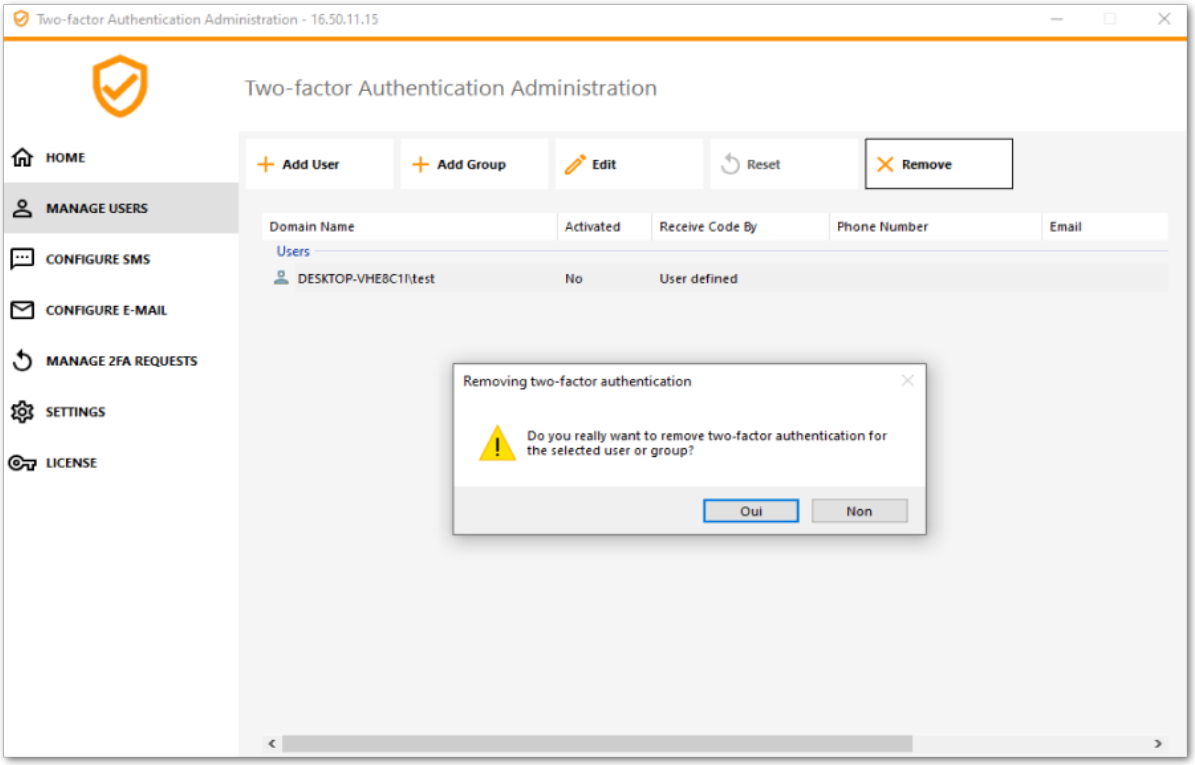


사용자는 기본적으로 인증 앱에서 인증 코드를 받습니다. 옵션을 선택하여 SMS 또는 이메일로 받을 수 있습니다.

선택한 SMS와 사용자의 전화번호를 필드에 추가하거나 선택한 EMAIL과 사용자의 이메일을 추가했습니다.

사용자 및 그룹 제거

사용자 또는 그룹을 제거하려면 사용자를 선택하거나 그룹을 선택한 다음 클릭하십시오. 제거하다 확인 메시지가 표시됩니다.



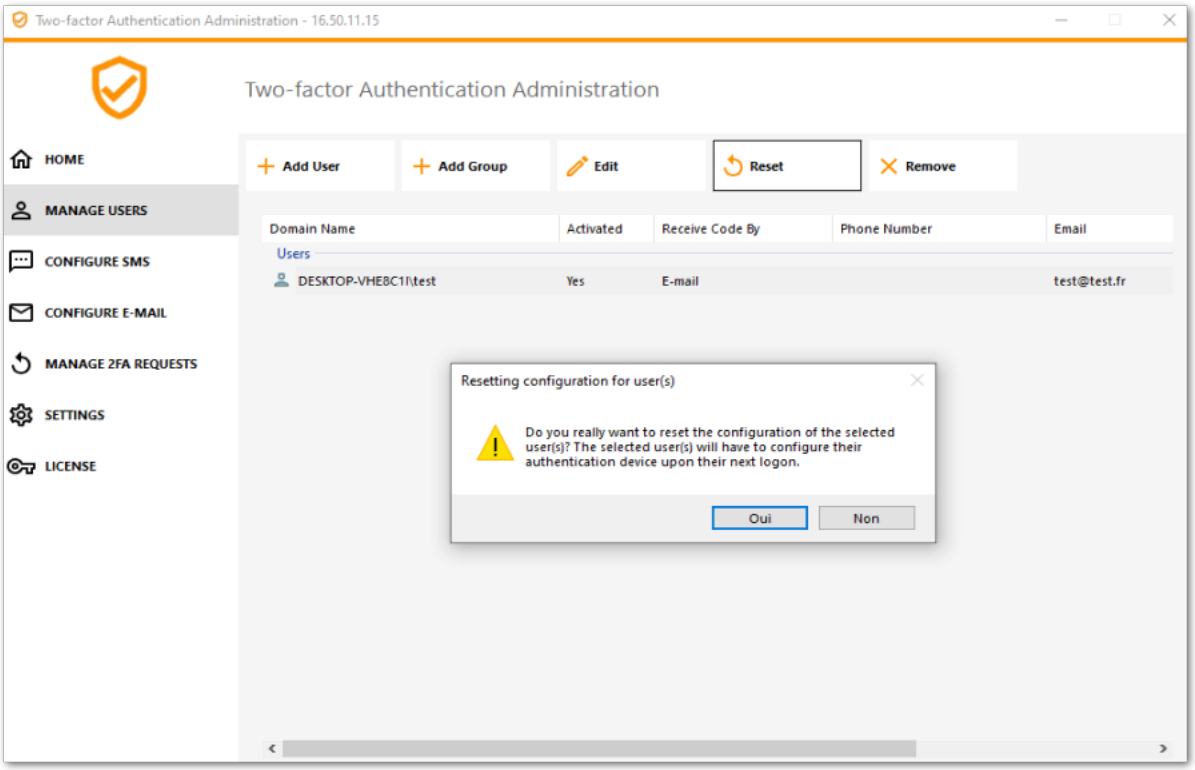
클릭 네 사용자 또는 그룹이 목록에서 제거되며 더 이상 이중 인증을 사용하여 연결되지 않습니다.

사용자 구성 재설정

사용자의 인증 장치를 분실한 경우 또는 사용자가 비밀 QR 코드를 다시 표시해야 하는 경우, 사용자 인증 설정을 재설정해야 합니다.

1. 이중 인증 관리 애플리케이션에서 클릭하십시오. 사용자 관리 탭.

2. 하나 이상의 활성화된 사용자를 선택한 다음 클릭하세요. 재설정 확인 메시지가 표시됩니다.



3. 클릭 네 선택된 사용자들은 다음 로그인 시 새로운 QR 코드를 제공받게 되며, 자신의 기기 인증 앱에서 이를 스캔해야 합니다.

사용자의 전화번호를 수정하여 새로운 장치에서 인증 코드를 받을 수 있습니다.

사용자를 이중 인증에 등록하기

사용자가 이중 인증을 사용하도록 활성화되면, TSplus 웹 포털에서 다음 성공적인 로그인 시 활성화 메시지가 표시됩니다.



필요한 단계를 완료하기 위해 두 가지 선택이 있습니다: 인증 앱을 통해 코드를 생성하거나, 사용자가 SMS로 코드를 받도록 할 수 있습니다.

인증자 애플리케이션으로 코드를 받으세요

사용자는 스마트폰과 같은 휴대용 장치에 인증기 앱을 설치해야 합니다.

다음 인증기 앱 중 하나를 사용하여 진행할 수 있습니다. 이러한 앱은 다양한 플랫폼에서 사용할 수 있습니다.

- Authy
- 구글 인증기
-

Microsoft Authenticator

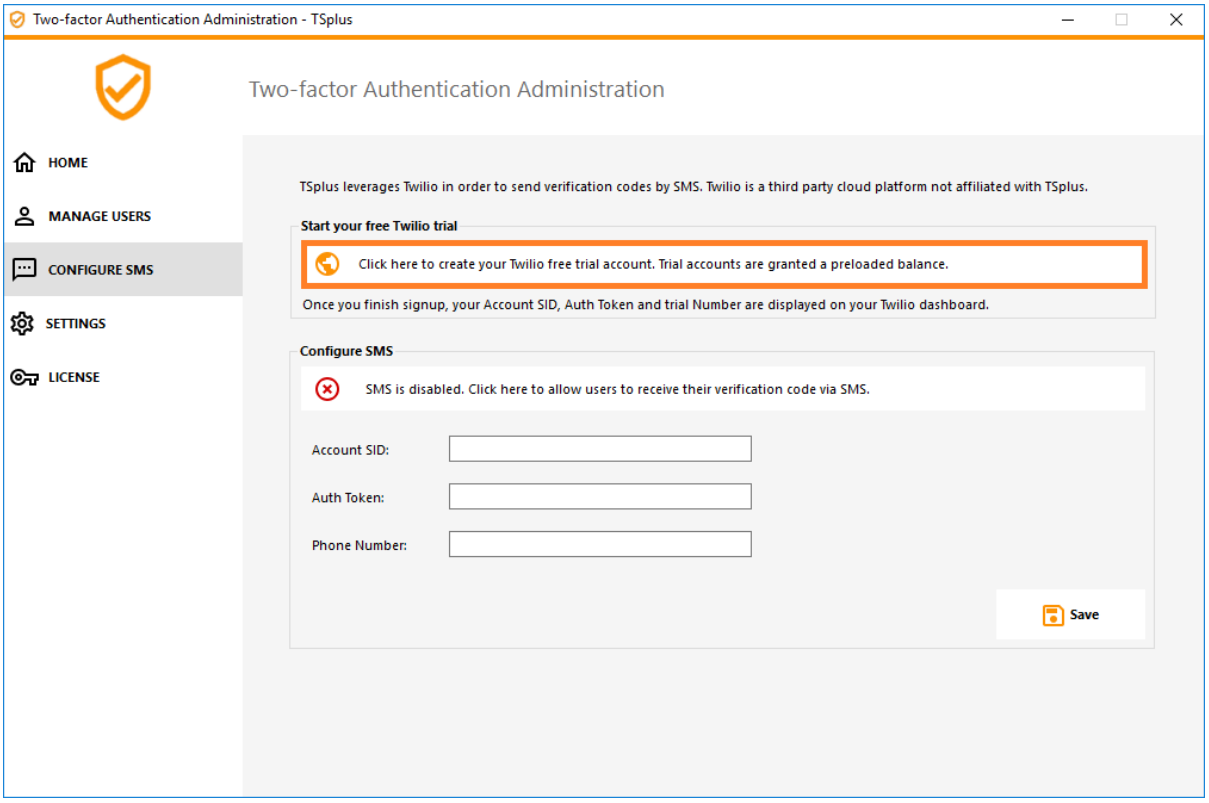
각 앱 문서를 참조하여 TSplus 계정을 추가하는 방법에 대한 자세한 내용을 확인하시기 바랍니다.

SMS 구성

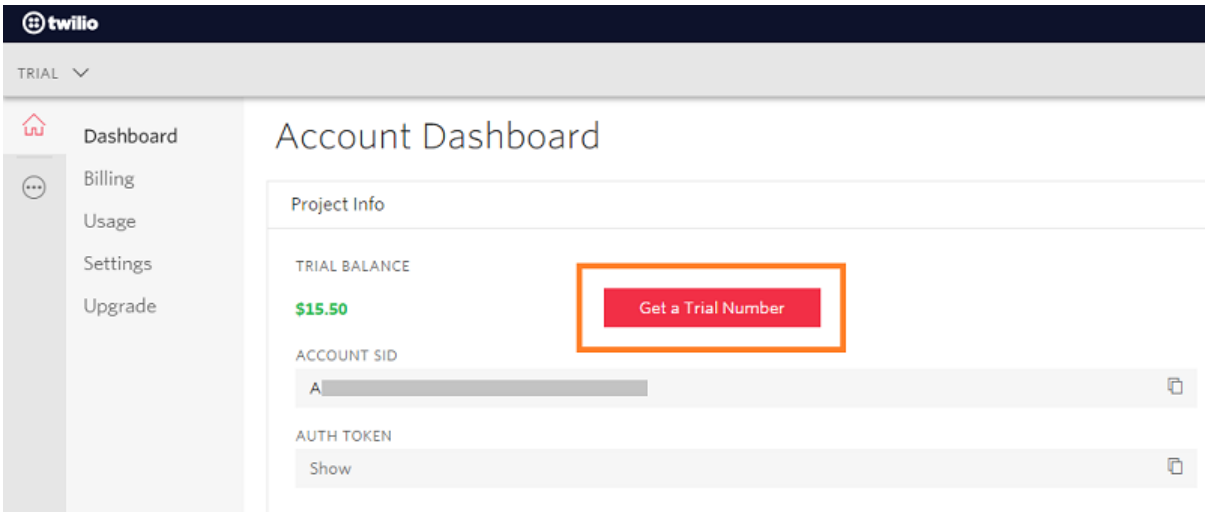
사용자가 SMS로 인증 코드를 받으려면 먼저 이를 활성화해야 합니다. 클릭하세요. SMS 구성 탭:

TSplus는 SMS로 인증 코드를 전송하기 위해 Twilio를 활용합니다. Twilio는 TSplus와 제휴하지 않은 제3자 클라우드 플랫폼입니다.

1. 무료 계정을 생성하세요. 트윌리오 아래의 “Twilio로 무료 체험 시작” 버튼을 클릭하여:

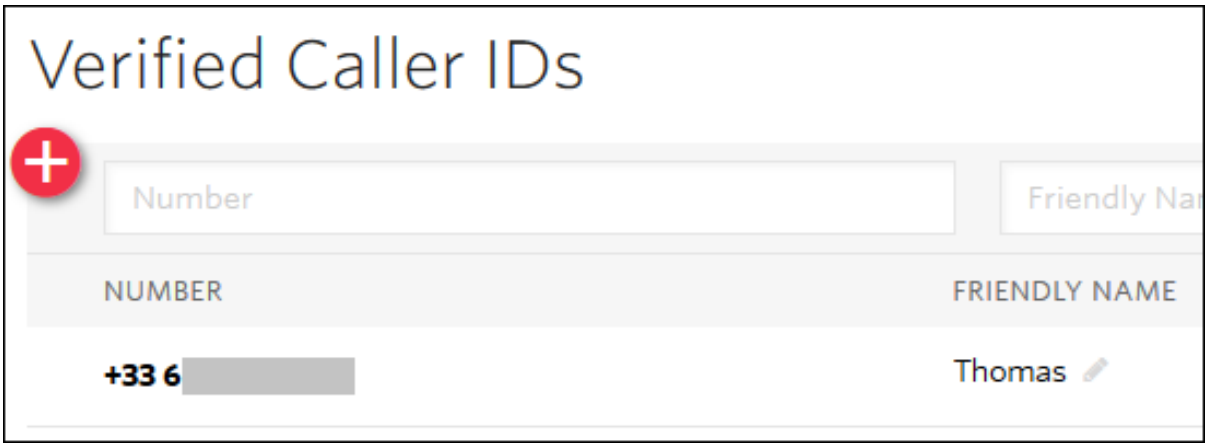


2. 당신의 트윌리오 계정 대시보드 귀하의 체험판 번호를 활성화해야 합니다.

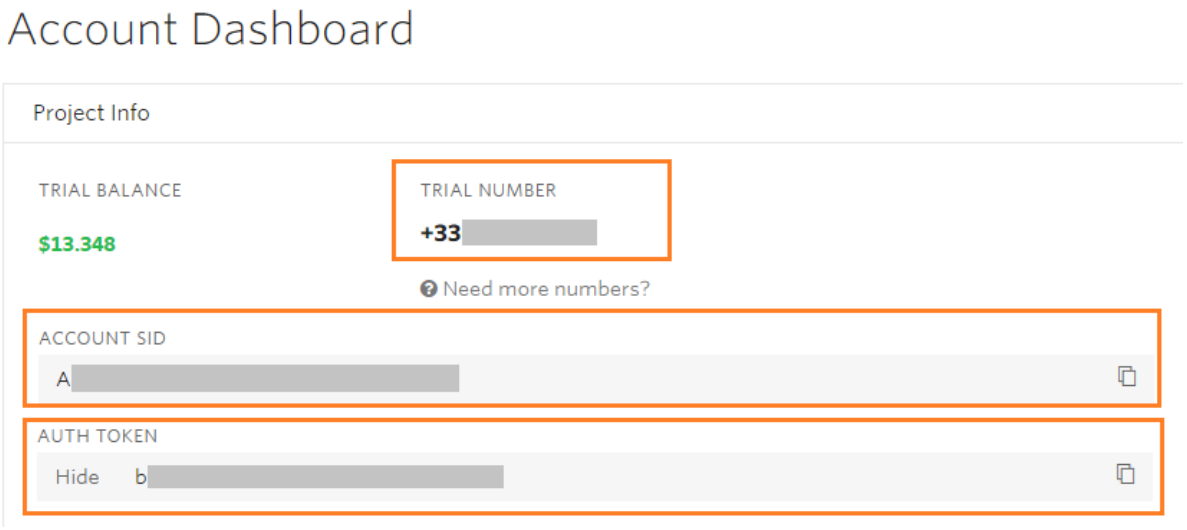


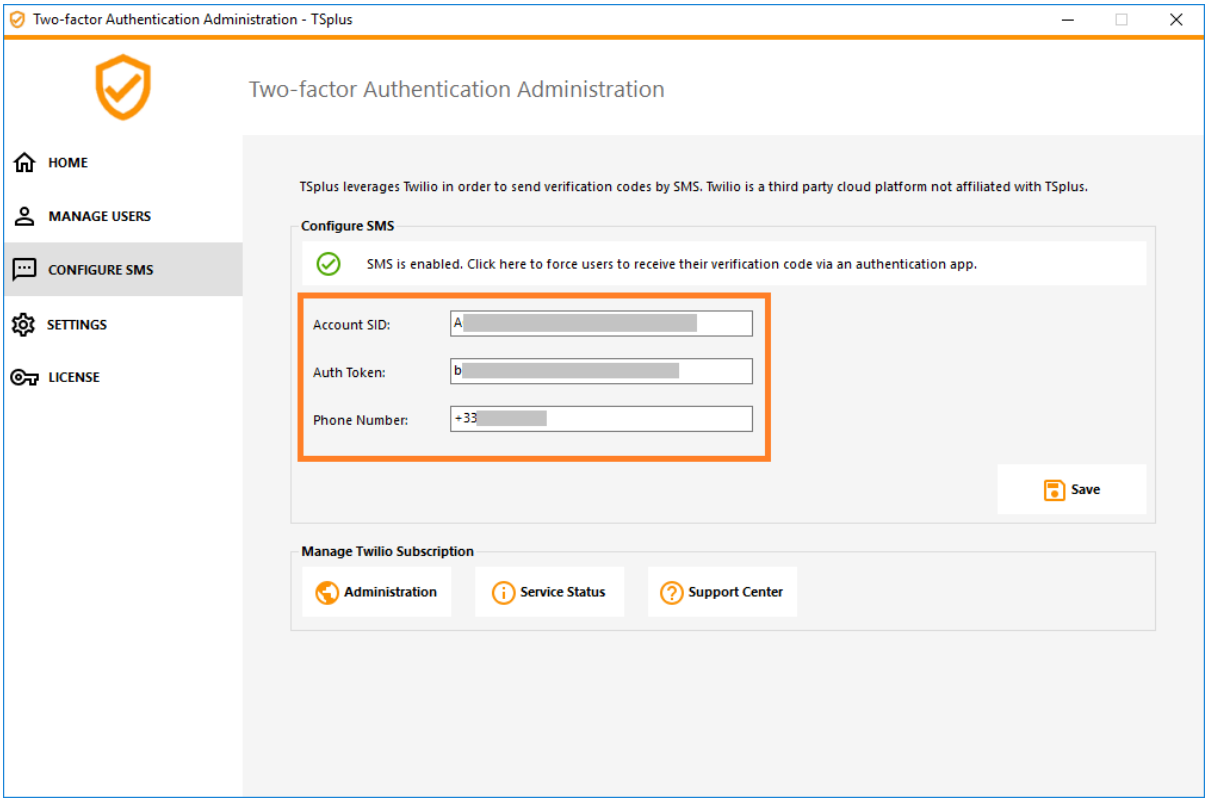
3. 다음 단계는 체험판 버전에서만 필요합니다. 이는 Twilio가 SMS가 전송될 실제 전화번호를 확인할 수 있도록 합니다.

이 번호를 아래에 입력하세요 "전화번호" 메뉴 - "확인된 발신자 ID" 탭 :

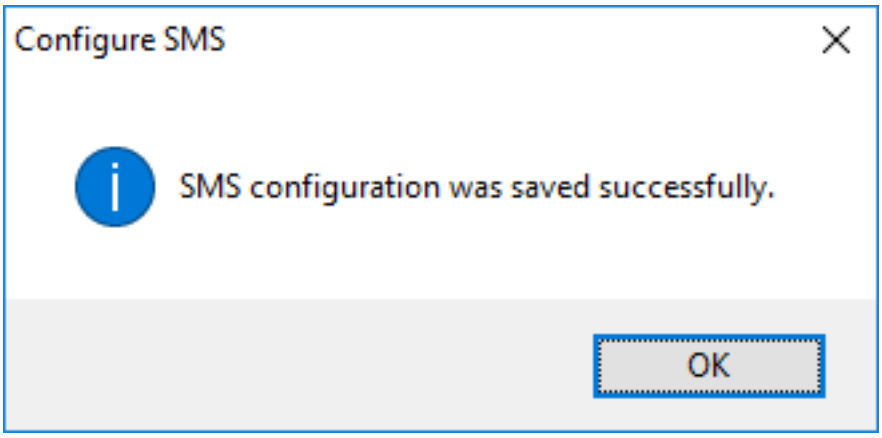


4. 그런 다음 계정 SID, 인증 토큰 및 입력할 수 있습니다. **시험 번호** 전화번호로서 SMS 구성 TSplus의 탭:





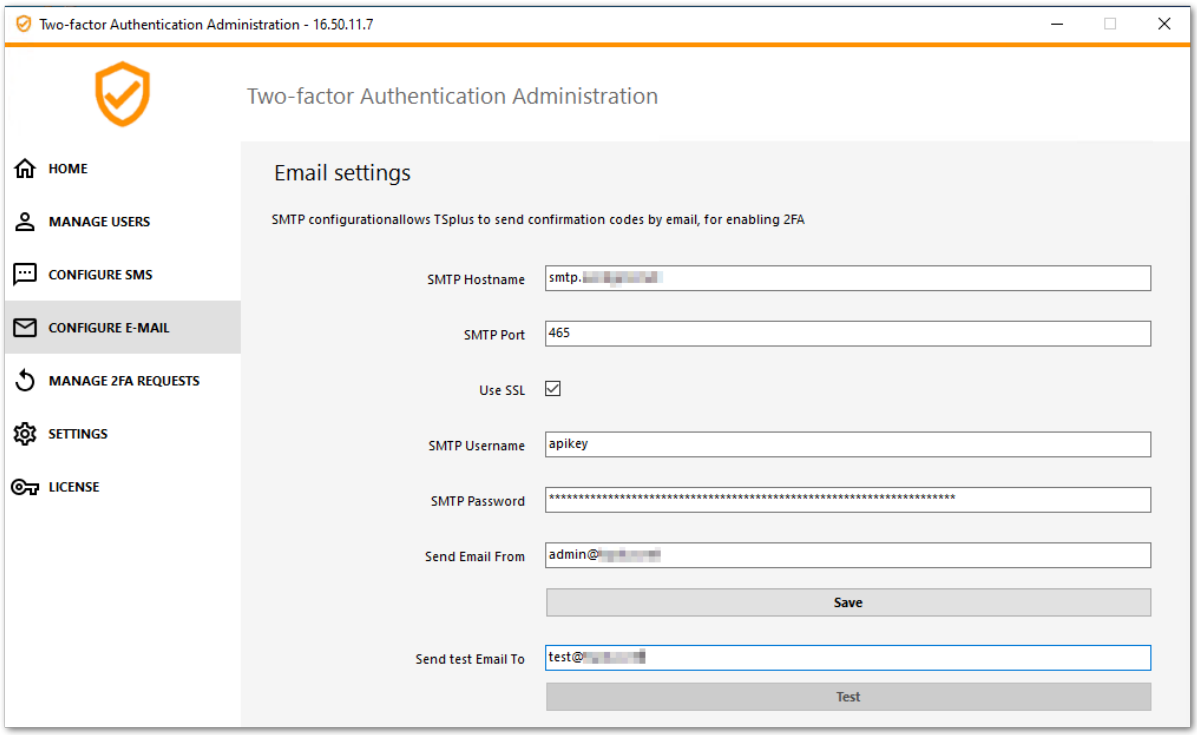
그런 다음 저장을 클릭하십시오. 다음 메시지가 표시됩니다:



당신은 Twilio 구독을 관리할 수 있습니다. 트윌리오 구독 관리 섹션, 하단의 SMS 구성 계정을 관리하고, 서비스 상태를 확인하거나 해당 버튼을 클릭하여 Twilio 지원 센터에 문의하세요.

이메일 구성

사용자가 이메일로 인증 코드를 받으려면 먼저 SMTP 이메일을 구성해야 합니다.



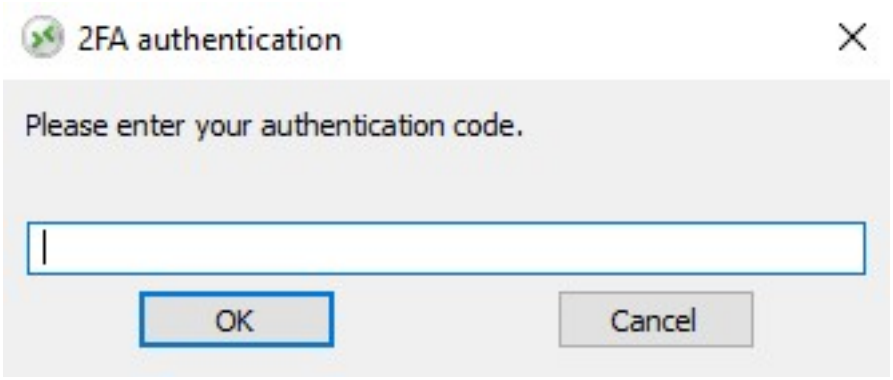
2단계 인증을 사용하여 로그인

사용자가 인증 앱에서 TSplus 계정을 설정하면, 비밀번호와 인증 앱에서 제공하는 코드, SMS 또는 이메일을 사용하여 연결할 수 있습니다.

TSplus Remote Access 웹 포털에서:



TSplus에서 생성된 클라이언트:



TSplus 애플리케이션 서버와 클라이언트 장치는 동일한 시간을 공유해야 합니다. 이는 서버의 시간과 날짜가 시간 서버와 동기화되어야 함을 의미합니다. 클라이언트 장치도 구성된 시간대와 관계없이 시간 동기화가 필요합니다.

인증 요청이 날짜와 시간이 동기화되지 않은 장치에서 오거나 서버의 날짜와 시간이 동기화되지 않은 경우, 이 요청은 거부될 수 있습니다.

장치와 서버 간의 정보 검증은 UTC 시간과 관련이 있습니다.

안에 **설정** 섹션, 불일치 매개변수는 코드의 유효 기간을 30초 간격으로 관리하는 데 사용됩니다.

유효성 검사 또는 유효한 인증의 예:

- 서버가 시간 서버와 동기화되어 있으며, 시간대는 UTC + 2이고, 현재 시간은 오후 2시 30분입니다.
- 장치가 시간 서버와 동기화되어 있으며, 시간대는 UTC + 1이고, 현재 시간은 오후 1시 30분입니다.
- 불일치 매개변수는 60으로 설정되어 있으며, 즉 코드 유효 기간은 30분입니다.
- UTC 시간에 따라 장치 시간과 서버 시간이 동일합니다.

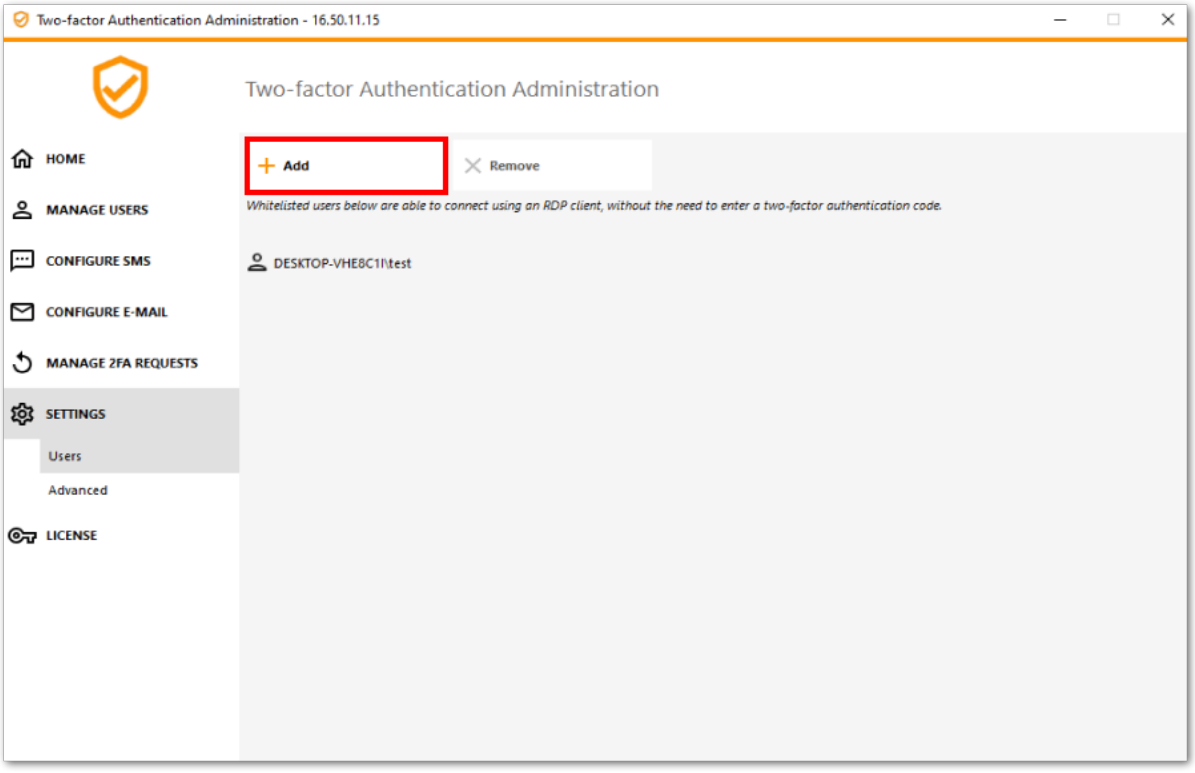
유효성 검사 또는 잘못된 인증의 예:

- 서버가 시간 서버와 동기화되어 있으며, 시간대는 UTC + 2이고, 현재 시간은 오후 2시 30분입니다.
- 장치가 시간 서버와 동기화되지 않았습니다. 시간대는 UTC-1이며, 시간은 수동으로 오후 1시 30분으로 설정되어 있습니다.
- 불일치 매개변수는 60으로 설정되어 있으며, 즉 코드 유효 기간은 30분입니다.
- 서버 시간이 UTC 시간으로 12:30 AM입니다.
- 장치에서 전달된 시간은 UTC 시간으로 오후 2시 30분입니다.
- 차이는 120분이며, 따라서 유효성 검사 코드는 거부됩니다.

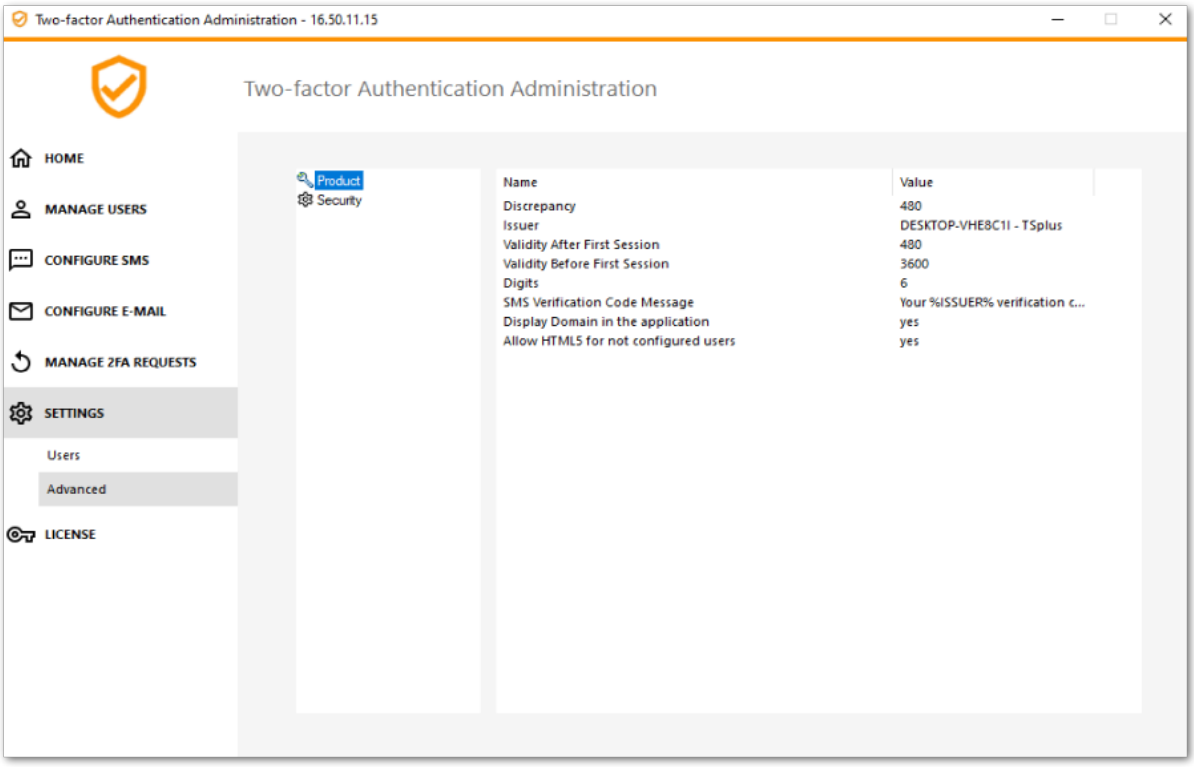
설정

설정 탭을 사용하면 **사용자가 RDP 클라이언트를 사용하여 두 번째 인증 코드를 입력할 필요 없이 연결할 수 있도록 허용합니다.**

“추가” 버튼을 클릭하여 사용자를 추가하고, 사용자를 선택한 후 “제거” 버튼을 클릭하여 사용자를 제거합니다.



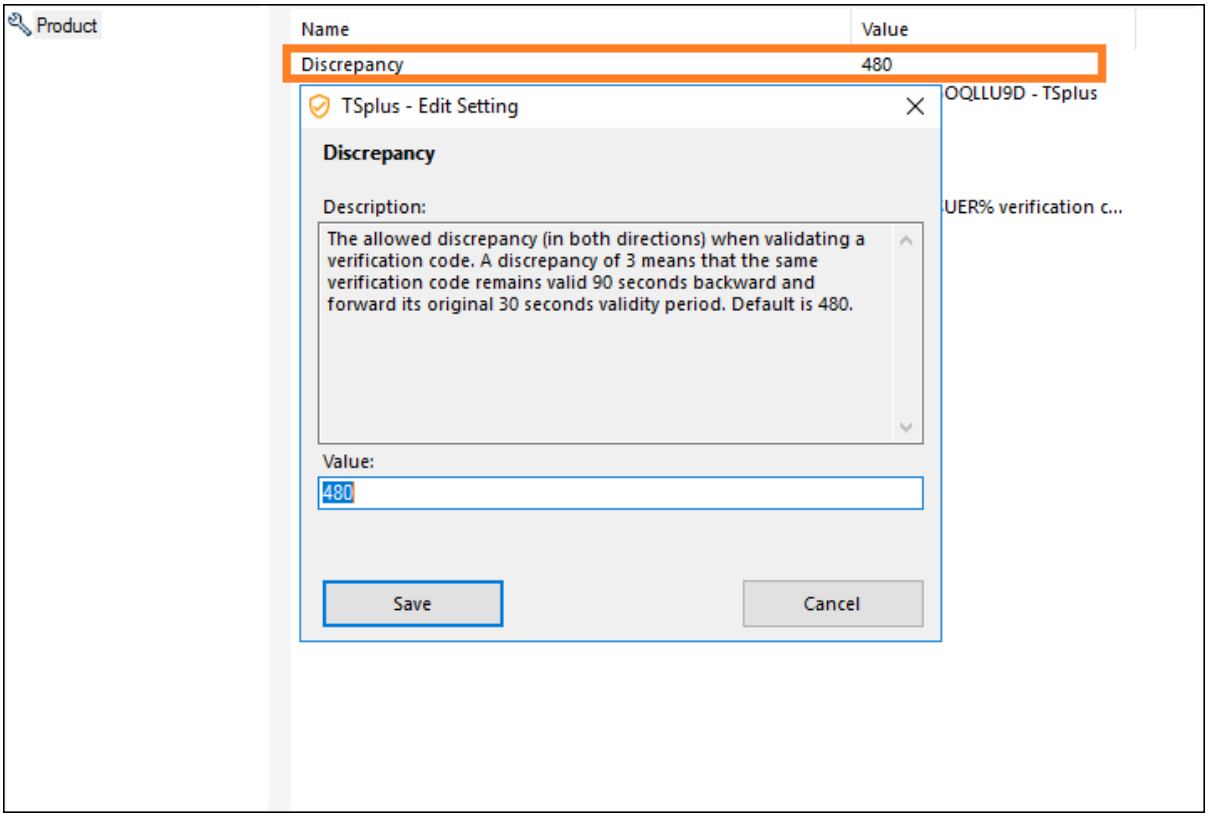
고급 탭을 사용하면 Two-Factor Authentication의 심층 설정을 구성할 수 있습니다.



불일치

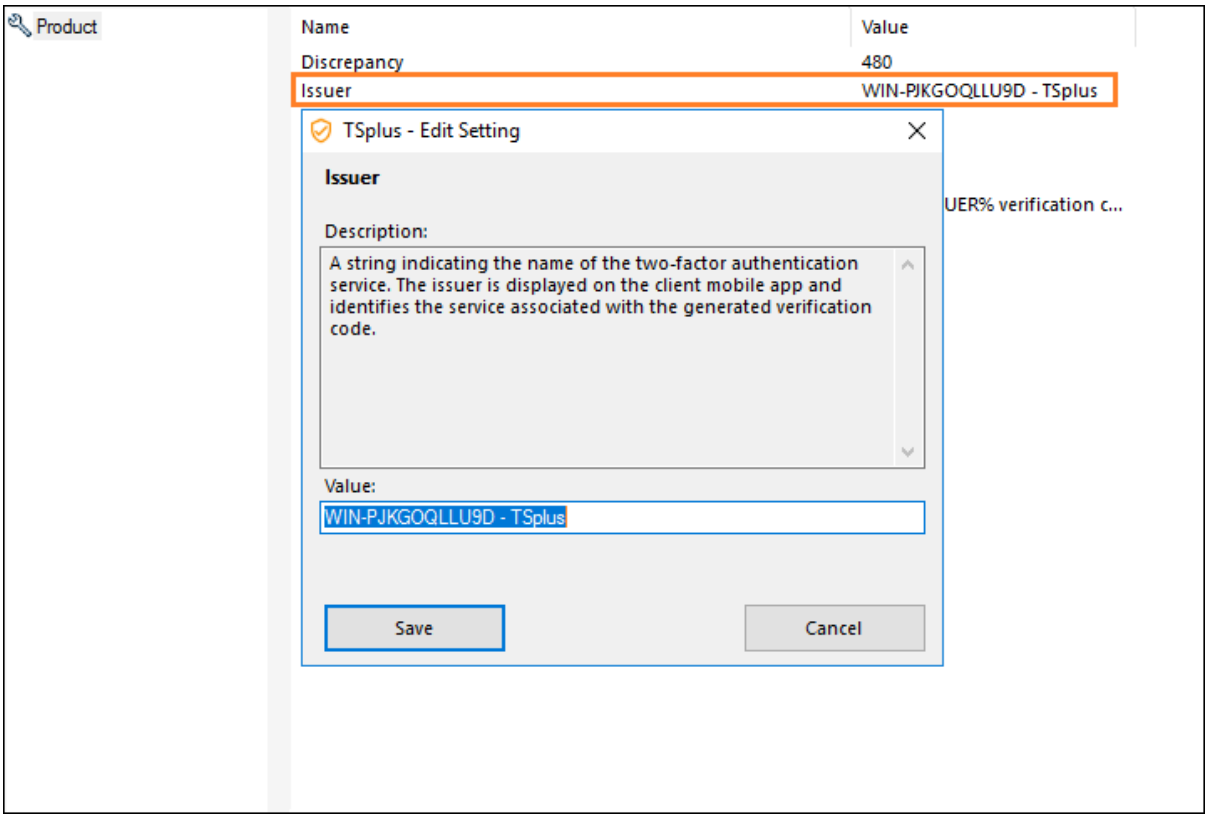
불일치 값을 수정할 수 있으며, 이를 통해 인증 코드의 유효성 검사 시간을 설정할 수 있습니다.

3의 불일치는 동일한 인증 코드가 원래 30초 유효 기간의 90초 전후로 유효하다는 것을 의미합니다. 기본값은 480으로, 이는 480 x 30초 = 4시간을 의미합니다.



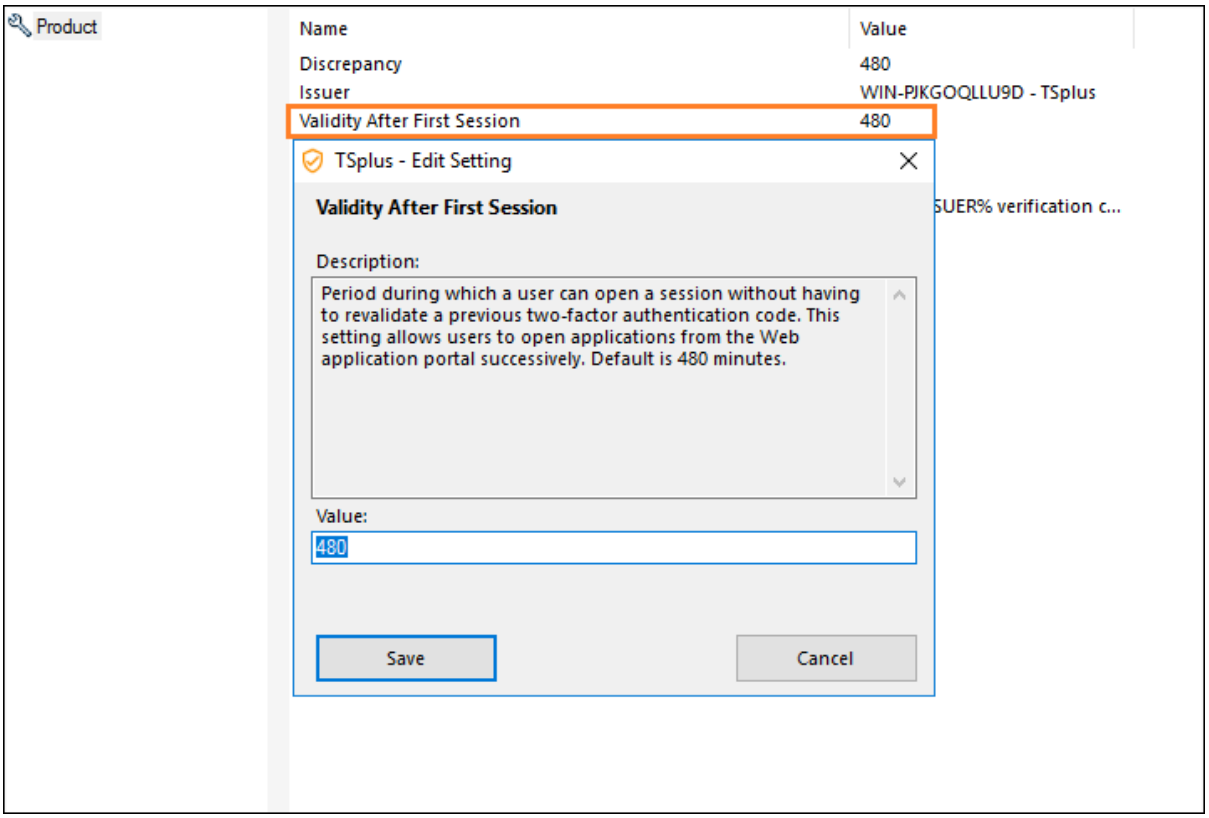
발급자

이 문자열은 이중 인증 서비스의 이름을 나타냅니다. 발급자는 클라이언트 모바일 앱에 표시되며 생성된 인증 코드와 연결된 서비스를 식별합니다. 기본적으로 TSplus와 함께 서버의 이름으로 구성됩니다.



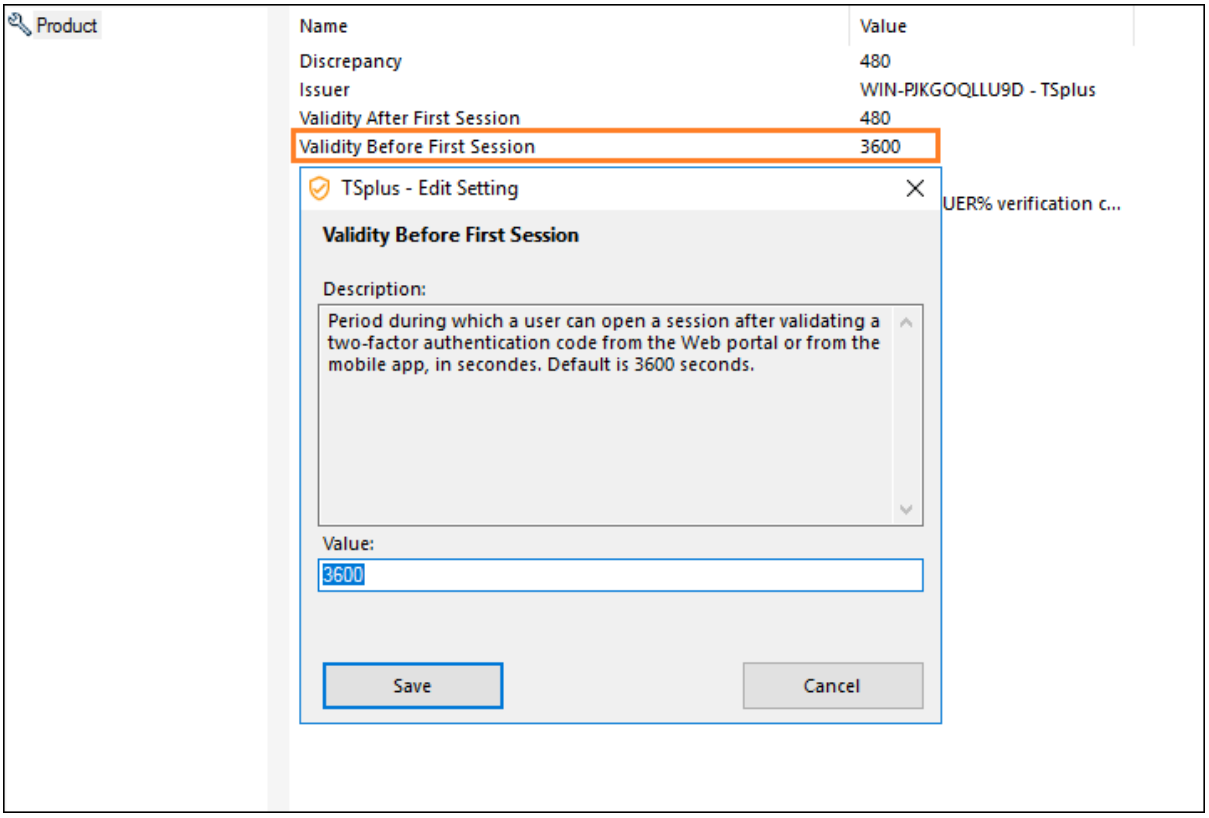
첫 세션 후 유효성

사용자가 이전의 이중 인증 코드를 재검증하지 않고 세션을 열 수 있는 기간입니다. 이 설정은 사용자가 웹 애플리케이션 포털에서 애플리케이션을 연속적으로 열 수 있도록 허용합니다. 기본값은 480분입니다.



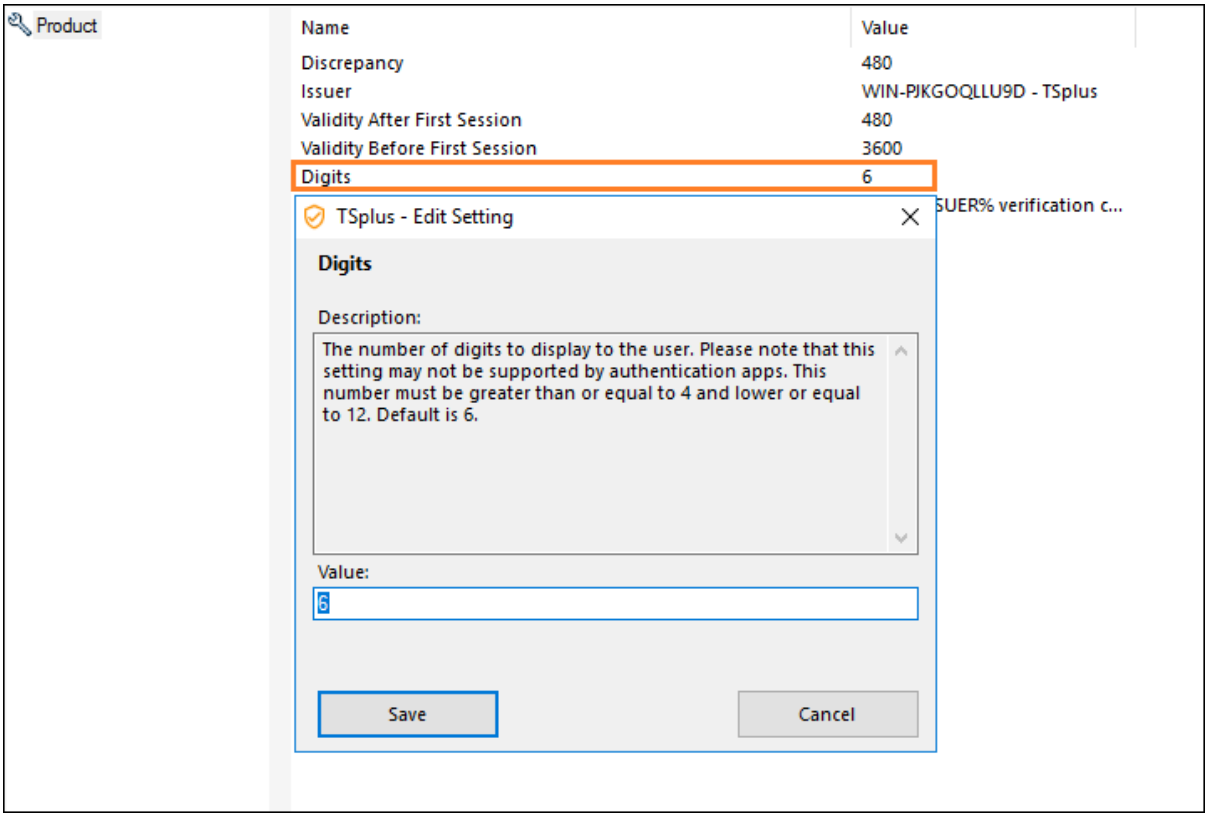
첫 세션 전 유효성

사용자가 웹 포털 또는 모바일 앱에서 이중 인증 코드를 확인한 후 세션을 열 수 있는 기간(초 단위). 기본값은 3600초입니다.



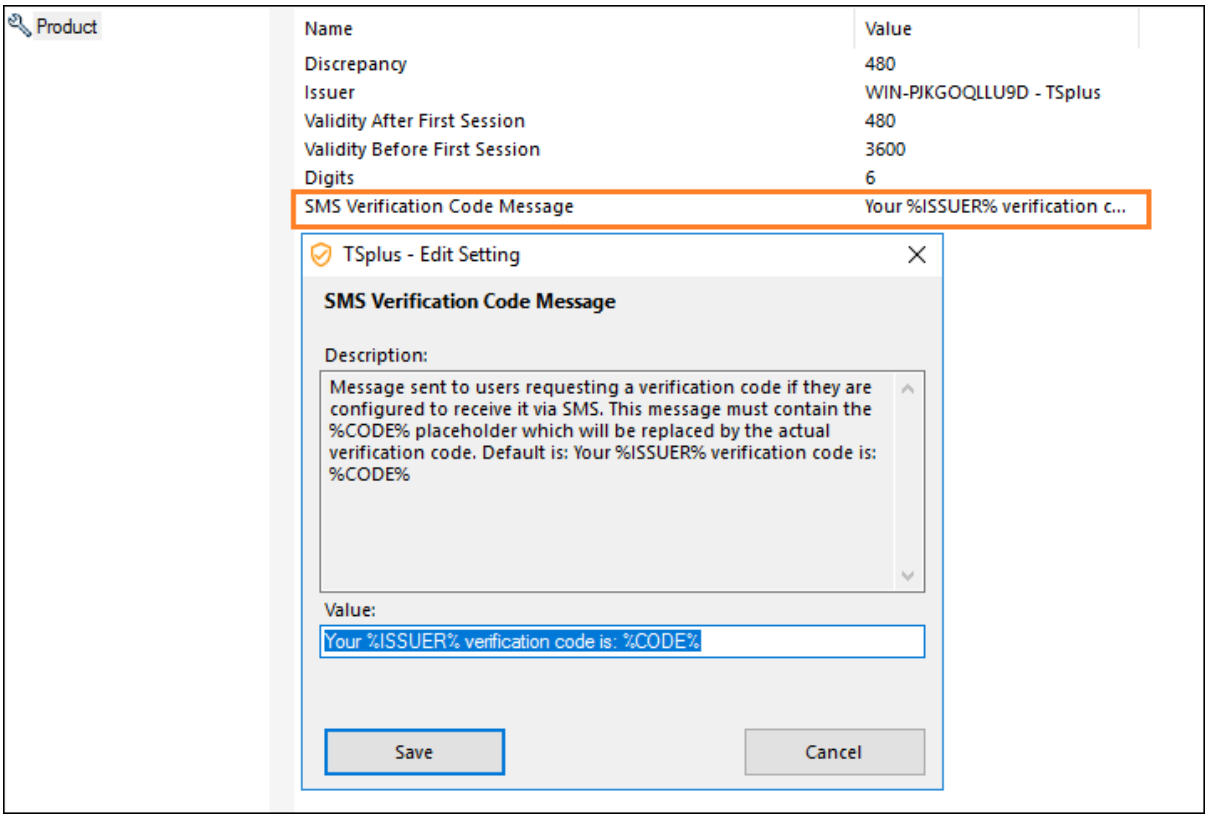
숫자

사용자에게 표시할 숫자의 개수입니다. 이 설정은 인증 앱에서 지원되지 않을 수 있습니다. 이 숫자는 4 이상 12 이하이어야 합니다. 기본값은 6입니다.



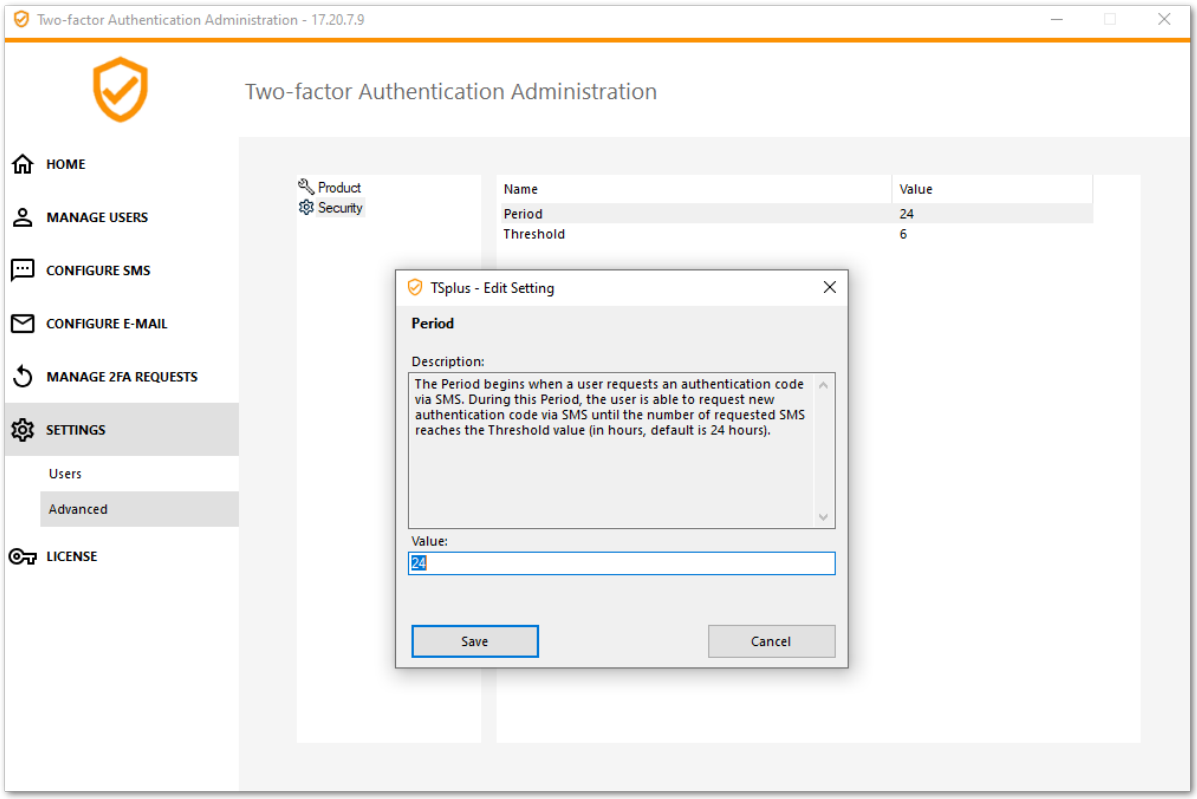
SMS 인증 코드 메시지

사용자가 SMS를 통해 수신하도록 설정된 경우 확인 코드를 요청하는 메시지가 전송됩니다. 이 메시지에는 실제 확인 코드로 대체될 %CODE% 자리 표시자가 포함되어야 합니다. 기본값은 다음과 같습니다: 귀하의 %ISSUER% 확인 코드는: %CODE%입니다.



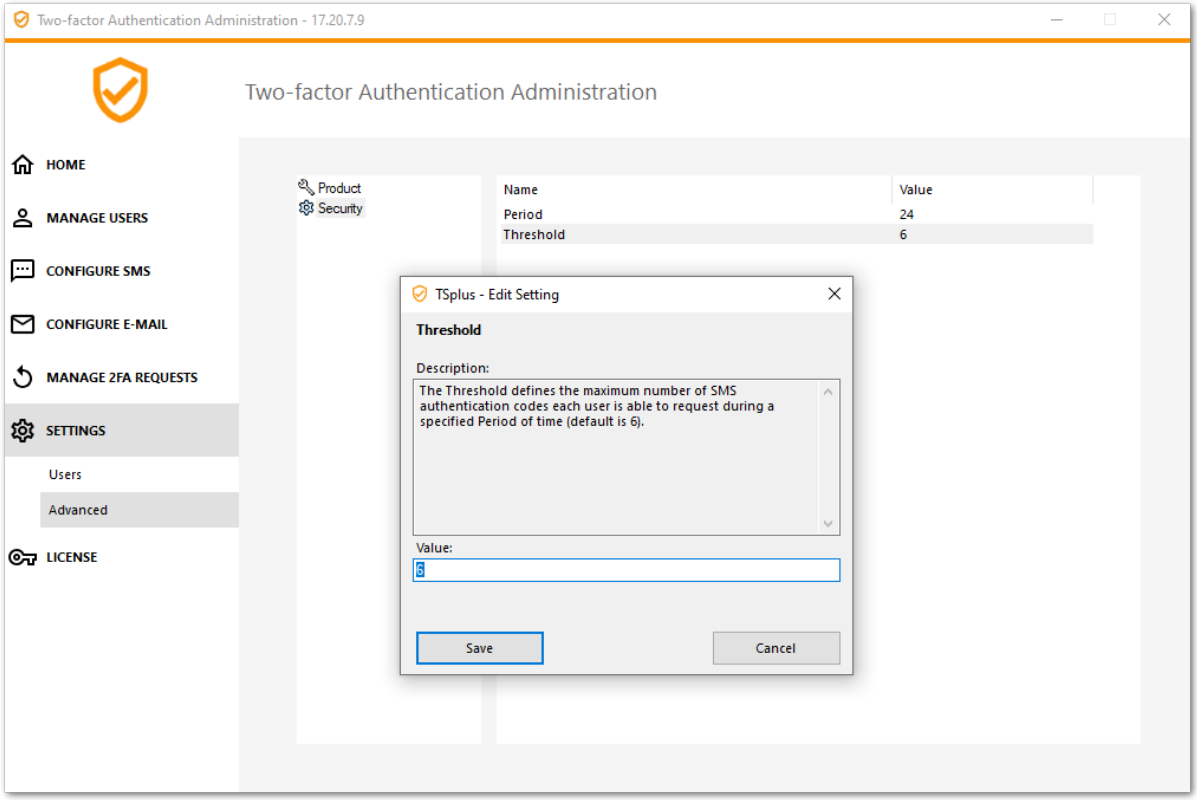
SMS 보안 기간

사용자가 SMS를 통해 인증 코드를 요청할 때 기간이 시작됩니다. 이 기간 동안 사용자는 요청한 SMS의 수가 임계값(시간 단위, 기본값은 24시간)에 도달할 때까지 SMS를 통해 새로운 인증 코드를 요청할 수 있습니다.



SMS 보안 임계값

임계값은 각 사용자가 지정된 기간 동안 요청할 수 있는 SMS 인증 코드의 최대 수를 정의합니다 (기본값은 6입니다).



유니버설 프린터 (novaPDF)

TSplus 유니버설 프린터를 사용하면 TSplus Remote Access에서 지원하는 모든 PC 또는 모바일 장치에서 문서를 미리 보기하거나 인쇄할 수 있습니다. 유니버설 프린터는 HTML5 세션에서 관련이 있으며 생성된 클라이언트를 사용하여 연결할 때 유효합니다. 표준 RDP 클라이언트 (mstsc.exe)를 사용할 때는 프린터가 서버와 클라이언트 간에 공유될 수 있기 때문에 유니버설 프린터는 관련이 없습니다.

원격 액세스 버전 17 시작, 유니버설 프린터는 novaPDF를 활용합니다. https://www.novapdf.com/ 원격 문서에서 100% 산업 표준 PDF(휴대용 문서 형식) 파일을 생성합니다. 생성된 PDF 문서는 원하는 로컬 프린터로 전송됩니다. 유니버설 프린터(novaPDF)는 더 이상 설치할 수 없는 유니버설 프린터(CustPDF) 및 유니버설 프린터(GhostScript)를 대체합니다.

원격 인쇄를 위해 두 개의 프린터가 제공됩니다: 유니버설 프린터와 가상 프린터. 가상 프린터가 더 나은 인쇄 성능을 제공하지만 HTML5 클라이언트와 호환되지 않으며 클라이언트 애플리케이션을 설치해야 합니다. 따라서 유니버설 프린터가 원격 액세스 설정에 따라 기본 프린터로 설정됩니다. 확인하세요. TSplus Virtual Printer .

요구 사항

NovaPDF11Service 서비스는 활성화된 방화벽이나 안티바이러스의 제외 목록에 있어야 합니다.

범용 프린터 구성

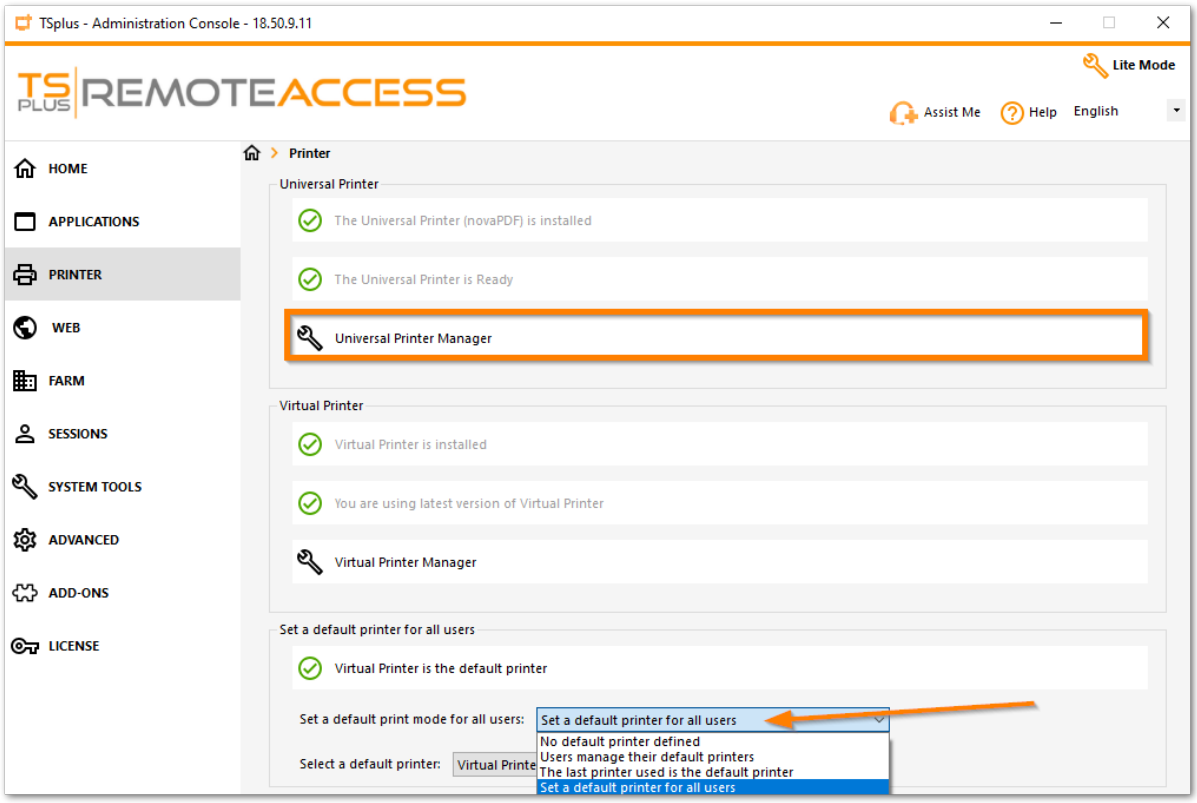
유니버설 프린터를 구성하려면 AdminTool을 열고 클릭하십시오. 프린터 메뉴.

Universal Printer 제어판에 접근하려면 AdminTool을 통해 다음 경로로 이동하십시오: 프린터 > Universal Printer 관리자

모든 사용자에 대한 기본 프린터 설정

- 기본 프린터가 정의되지 않았습니다: 사용자의 기본 프린터 구성에는 영향을 미치지 않습니다.
- 사용자가 기본 프린터를 관리합니다: "Windows가 내 기본 프린터를 관리하게 허용" 옵션이 비활성화되어 있으므로 사용자가 기본 프린터를 선택해야 합니다.
- 마지막으로 사용된 프린터는 기본 프린터입니다: "Windows가 내 기본 프린터를 관리하게 허용" 옵션이 활성화되어 있습니다.

- 모든 사용자를 위한 기본 프린터 설정: 관리자가 사용자의 기본 프린터를 강제합니다.



유니버설 프린터 섹션은 관리자가 다음을 가능하게 하는 네 개의 타일을 표시합니다:

- 유니버설 프린터 설정 상태를 확인하세요. 유니버설 프린터가 설치되어 있지 않으면 타일을 클릭하면 유니버설 프린터가 설치됩니다.

- 유니버설 프린터의 인쇄 상태를 확인하십시오. 유니버설 프린터가 인쇄 작업을 받을 준비가 되어 있지 않으면, 타일에 오류에 대한 추가 관련 정보가 표시될 수 있습니다.

- 유니버설 프린터가 기본 프린터로 설정되어 있는지 확인하십시오. 유니버설 프린터가 기본 프린터로 설정되어 있지 않으면 타일을 클릭하면 기본 프린터로 설정됩니다. 이 동작은 사용자가 그렇게 할 수 있는 경우 사용자가 재정의할 수 있음을 유의하십시오.

- 타일 이름 **유니버설 프린터 관리자** 더 자세한 화면으로 이어지며, 여기에는 유니버설 프린터 제거와 같은 추가 작업 및 속성이 제공됩니다.

유니버설 프린터 관리자

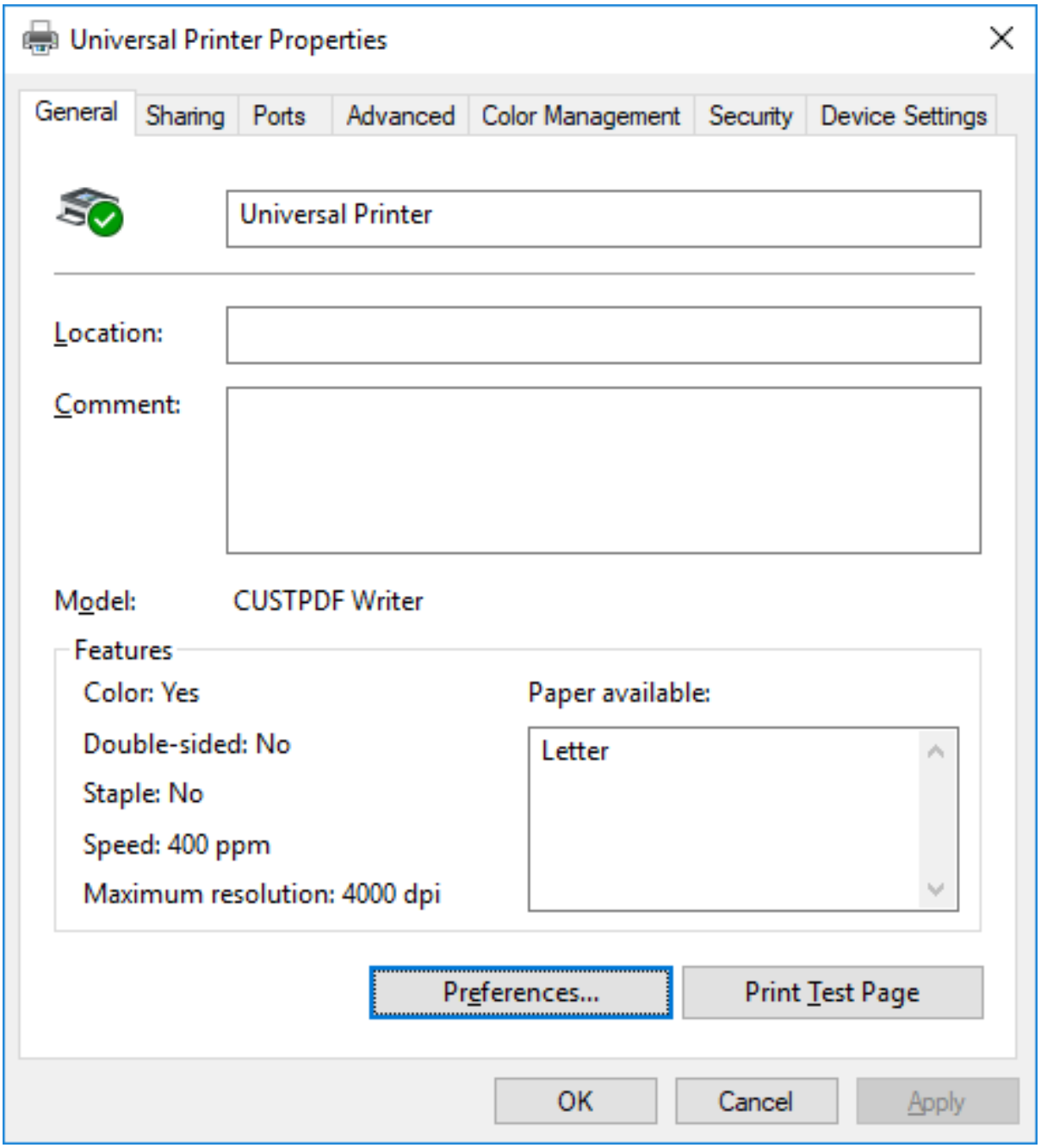
유니버설 프린터 관리자는 관리자가 유니버설 프린터 상태를 확인하고, 유니버설 프린터를 제거하며, 인쇄 대기열 및 프린터 속성에 접근할 수 있도록 합니다.

특히, 페이지 하단에 위치한 버튼은 관리자가 다음을 허용합니다:

- **유니버설 프린터 제거** 유니버설 프린터를 제거하십시오. 나중에 이 화면에서 다시 설치할 수 있습니다.

- **프린터 보기** 인쇄 문서의 상태를 확인하고, 일시 중지하거나, 재개하거나, 인쇄 작업을 취소할 수 있는 창을 엽니다. 또한 인쇄 기본 설정 및 속성을 설정할 수 있습니다.

- **유니버설 프린터 속성** 이 창을 열어 모든 인쇄 속성을 볼 수 있습니다. 일반 탭 다음에는 공유, 포트, 고급, 색상 관리, 보안 및 장치 설정을 위한 탭이 있습니다. 팝업 창의 하단에는 프린터가 있습니다. **속성** 관리자가 A4에서 모든 종류의 인쇄 형식으로 인쇄 페이지 크기를 설정할 수 있습니다. 또한 두 가지 인쇄 방향 중에서 선택할 수 있습니다: 세로 또는 가로.

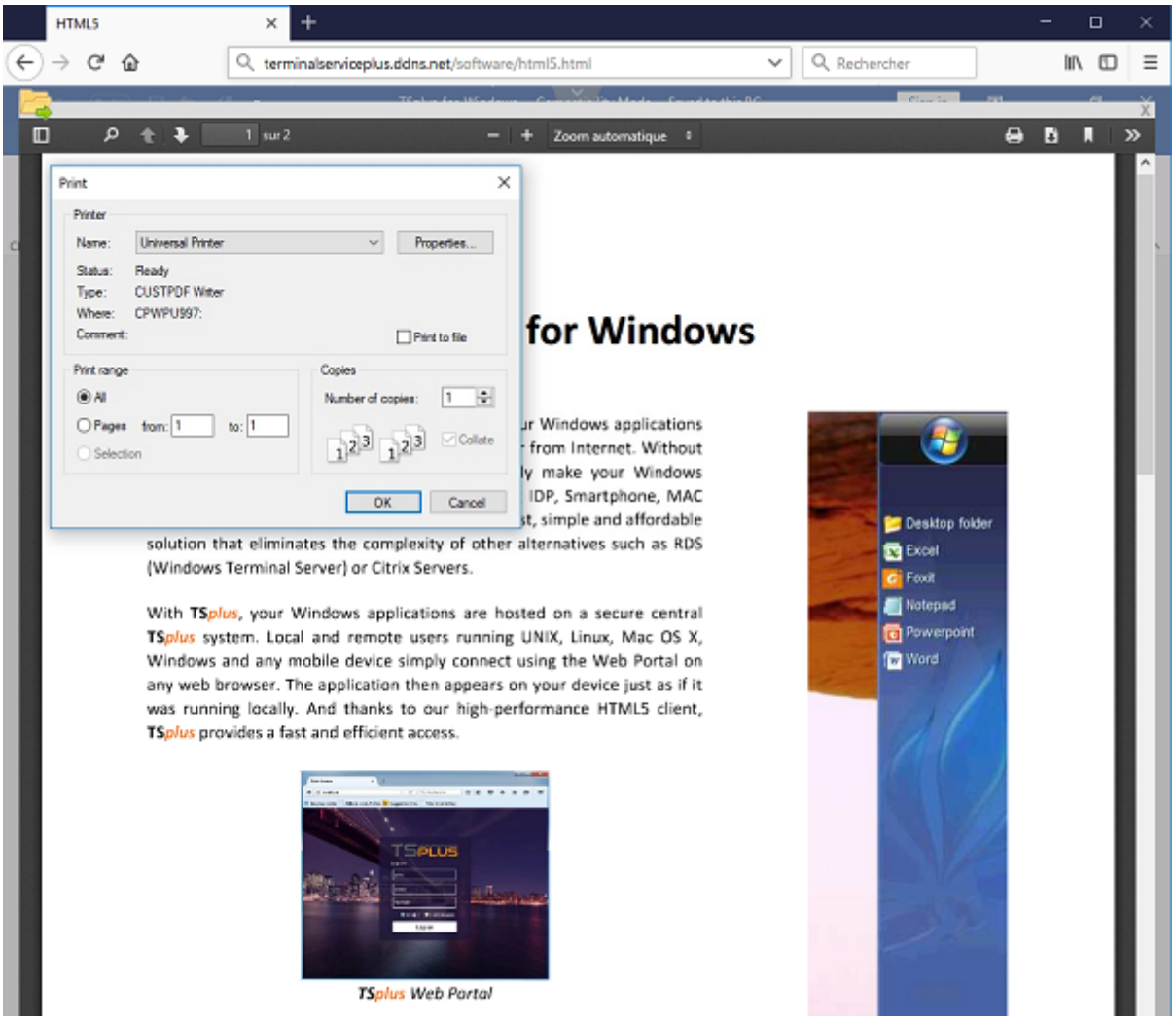


참고: 유니버설 프린터는 novaPDF를 활용하여 관리자가 글꼴, 그래픽, 워터마크, 오버레이 등을 정의하는 프로필을 생성할 수 있도록 합니다. **프로필 관리** 프린터 속성 팝업 창의 페이지 크기 및 방향 섹션 아래에 위치한 버튼. 기본적으로 프로필이 선택되어야 한다면, **인쇄하기 전에 선택 프로필 대화상자 표시** 사용자가 인쇄하기 전에 프로필을 선택할 수 있도록 확인할 수 있습니다. 프로필에 대한 자세한 내용은 novaPDF 문서를 참조하십시오. 프로필 관리자 .

유니버설 프린터로 인쇄하기

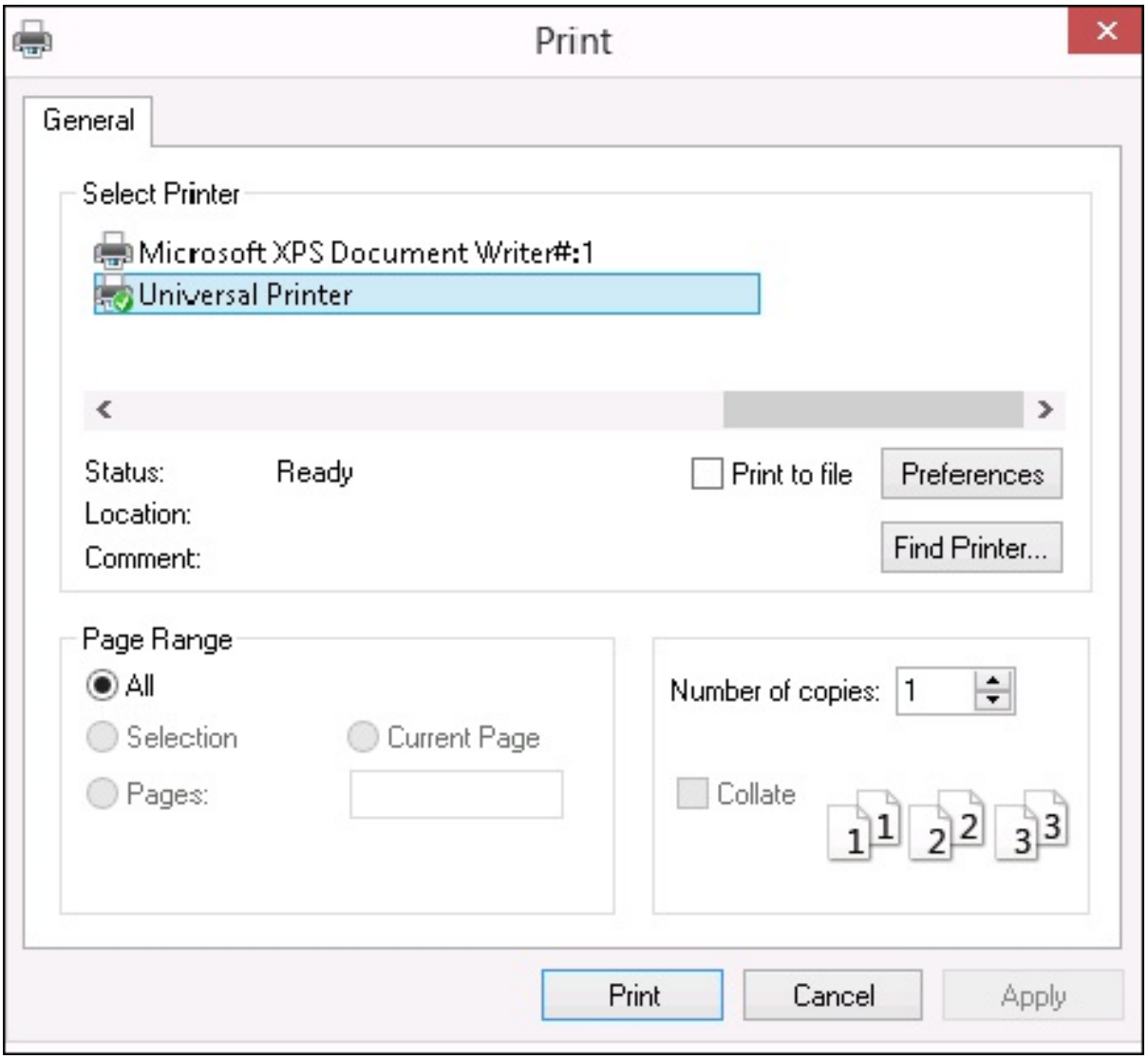
이 프린터를 사용하여 인쇄하는 동안 인쇄 대기열의 문서는 Universal Printer (novaPDF) 프린터에 의해 자동으로 PDF 파일로 변환됩니다.





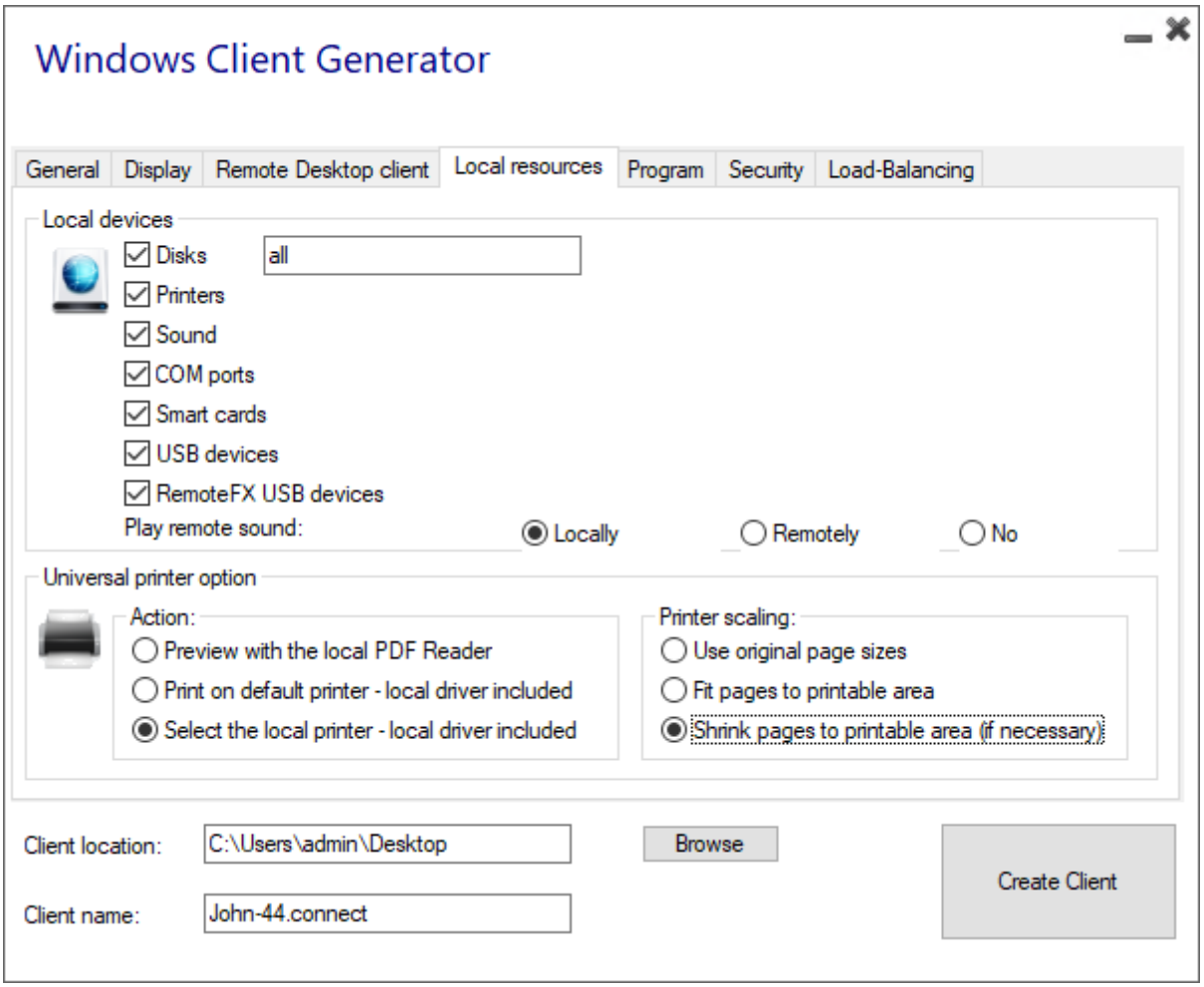
생성된 PDF 파일은 사용자의 워크스테이션의 로컬 PDF 리더로 전송됩니다.

각 인쇄 작업은 사용자의 로컬 디스크에서 준비가 완료되는 즉시 열립니다. PDF 파일이 클라이언트 측으로 전송되면 인쇄 프로세스가 시작되며, 이는 인쇄 작업이 지연 없이 시작됨을 보장합니다.



클라이언트 생성기를 사용한 인쇄 옵션 구성

로컬 리소스 탭에서 3가지 인쇄 옵션 중에서 선택할 수 있습니다. 휴대용 클라이언트 생성기 TSplus 연결 클라이언트를 사용할 때, 최소한 다음을 매핑해야 합니다. **C: 드라이브 또는 모든 디스크**



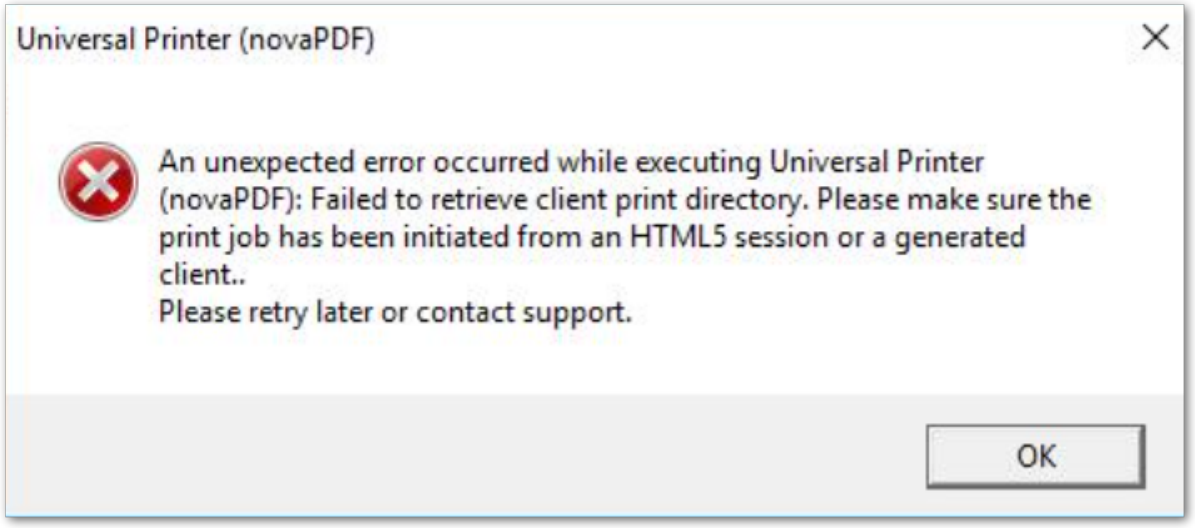
- **로컬 PDF 리더 미리보기** 문서는 클라이언트의 워크스테이션에 푸시되고 로컬 기본 PDF 리더가 수신된 PDF 파일을 엽니다. 사용자는 이를 인쇄하거나 로컬 디스크 드라이브에 복사본을 저장할 수 있습니다(이 동작은 HTML5 세션에서 인쇄할 때 예상됩니다).

- **사용자의 기본 프린터에 인쇄** 문서는 사용자의 기본 프린터에 의해 자동으로 인쇄됩니다(이 옵션은 TSplus 연결 클라이언트를 사용할 때만 사용할 수 있습니다). 이 옵션은 하루 동안 인쇄할 작업이 많은 사용자와 이 목적을 위해 동일한 프린터를 사용하는 사용자에게 권장됩니다.

- **로컬 프린터 선택** 사용자는 자신의 로컬 프린터 중 하나를 선택할 수 있습니다(이 옵션은 TSplus 연결 클라이언트를 사용할 때만 사용할 수 있습니다).

PDF 파일을 읽기 위해 요즘 많은 사람들이 외부 애플리케이션을 전혀 사용하지 않고도 지내고 있습니다. Firefox와 Chromium, 구글의 Chrome 브라우저의 오픈 소스 버전 모두 브라우저 내 PDF 리더가 포함되어 있어 대부분의 사용자에게 외부 플러그인이 더 이상 필요하지 않습니다.

귀하의 정보에 따라
C: 드라이브가 매핑되지 않은 경우, 사용자는 이 오류 메시지를 받게 됩니다.



novaPDF 프린터 구성

에서 **프린터 기본 설정 > 도구 > 비밀번호** , 당신은 할 수 있습니다:

- 기본 비밀번호 편집
- 프로필 관리자 인터페이스의 언어 변경
- 인쇄 작업의 진행 상황을 실시간으로 모니터링하십시오.
- 프린터 기록 확인

새 탭에서 인쇄 작업 열기

기본적으로 HTML5 세션에서 인쇄 작업은 이전 버전 17.10과 마찬가지로 팝업 안에 표시됩니다.

이 동작을 수정하고 다음 설정을 사용하여 새 브라우저 탭에서 인쇄 작업을 열 수 있습니다: **관리 도구 > 고급 > 세션 > 새 탭에서 인쇄 작업 열기**

프로필

프로필은 레이아웃, 워터마크, 압축 수준 등을 사용자 정의할 수 있게 해줍니다. 프로필 관리자는 프로필을 관리할 수 있게 해줍니다. 프로필은 유니버설 프린터를 사용하여 인쇄할 때 활용되는 구성으로 구성됩니다. 예를 들어, PDF 배포, 고품질 인쇄, 검토 목적 또는 문서를 기밀로 표시하는 등 특정 출력 요구 사항에 맞춘 다양한 인쇄 프로필을 설정할 수 있습니다.

프로필 관리자를 열려면 장치 및 프린터를 열고 유니버설 프린터를 마우스 오른쪽 버튼으로 클릭한 다음 인쇄 기본 설정을 선택합니다. 그런 다음 클릭하십시오. **프로필 관리** 버튼. 기본 비밀번호는: pass@word1

기본 프로필 이해하기

- **기본 프로필** 기본 프로필은 한 번에 하나 또는 여러 문서를 인쇄하는 데 사용됩니다. 대부분의 시나리오에 적합합니다.
- **열린 문서 인쇄 프로필** 이 프로필을 사용하여 PDF 뷰어로 열 때 문서를 자동으로 인쇄합니다. 이 프로필은 HTML5 세션에서 인쇄할 때 클릭을 얻는 데 유용합니다.

HTML5 세션을 열면 현재 사용자에 대해 인쇄된 문서 프로필이 자동으로 선택됩니다. 그러나 RDP 모드에서 동일한 사용자에 대해 다른 세션이 현재 열려 있는 경우 HTML5 세션에서 자동 인쇄가 비활성화됩니다. 이 경우 기본 프로필이 기본적으로 적용됩니다.

노트 UWP 애플리케이션인 Windows 11의 메모장과 같은 프로그램에 대해 Print Opened Documents 프로필을 자동으로 선택할 수 없습니다. 이러한 애플리케이션은 시스템과 완전히 격리된 상태에서 실행되도록 설계되었기 때문입니다. 그러나 사용자가 프로필을 수동으로 선택하고 다음 인쇄 작업에 대해 기본값으로 선택하는 것은 여전히 가능합니다. 현재로서는 우회 방법이 없습니다. 그러나 2024년 4분기에 예정된 다음 novaPDF 주요 릴리스에 대한 novaPDF 프린터의 재설계는 이 제한을 해제할 것입니다.

사용자가 선택할 수 있는 프로필은 무엇인가요?

기본적으로 사용자는 두 개의 기본 프로필 중에서 사용할 프로필을 선택할 수 있습니다. 사용자는 하나의 프로필을 활성 프로필로 선택할 수 있으며 다음 인쇄 작업에 대해 프로필 선택 대화 상자를 표시하지 않습니다. 관리자는 모든 사용자에게 사용할 수 있는 하나 이상의 프로필을 정의할 수 있습니다. 이 결정은 사용자의 선택을 무시합니다. 보세요 https://www.novapdf.com/printer-manager-profiles-help.html .

중요한 기존 프로필을 복사하여 보다 개인화된 프로필을 만드는 것이 권장됩니다. 기존 프로필에는 생성된 PDF 문서에 포함된 글꼴과 같은 대부분의 설치에 필요한 여러 기능이 포함되어 있습니다.

문제 해결

아래에서 Universal Printer (novaPDF) 문제를 해결하기 위한 문제 해결 팁을 확인하십시오.

최신 정보 유지

- 연결 클라이언트를 업데이트하면 클라이언트 측에서 발생하는 일부 문제를 해결할 수 있습니다.
- 변경 로그를 검토하여 최신 버전이 귀하의 문제를 해결하는지 확인하십시오. https://dl-files.com/TSplus-changelog.html
- 개발 팀은 최신 코드 베이스만 지원할 수 있다는 점을 기억하세요.

인쇄 프로세스의 어느 부분이 실패했는지 이해하기

- 인쇄 작업이 인쇄 대기열에 생성되었습니까? 상태는 무엇입니까?

인쇄 오류에 대한 로그 수집

- **세션 열기 로그** 특히 클라이언트 인쇄 디렉토리 검색 실패와 같은 문제에 유용하며, 위치는 **C:\wsession\trace** .
- **관리자 도구 애플리케이션 로그** 위치한 **C:\Program Files (x86)\TSplus\UserDesktop\files** .

- **유니버설 프린터 로그** 클라이언트 측에 위치한 인쇄 작업을 전송합니다. **C:\wsession\UniversalPrinter\logs** .
- **세션 이벤트 로그** 인쇄 사용자, 재연결 처리, 위치한 **%appdata%\UniversalPrinter\logs** .

프린터 설치 문제에 대한 로그 수집

- **설치 로그** 2024-02-XX #XX.txt는 다음에서 사용할 수 있습니다. **%temp%** 디렉토리.
- **유니버설 프린터 관리** _XX022024.txt 위치한 **C:\Program Files (x86)\TSplus\UserDesktop\files** .
- 모든 .txt 파일이 위치한 **C:\Program Files (x86)\TSplus\UserDesktop\files\UniversalPrinter** .

클라이언트 측 인쇄 오류에 대한 로그 수집, 연결 클라이언트를 사용할 때

- **version.dat** 파일. 항상 Connection Client를 최신 버전으로 업데이트하라고 권장합니다.
- **연결 클라이언트** 그리고 **유니버설 프린터 클라이언트** 로그. 이러한 로그는 레지스트리에서 다음 키 값을 생성하여 활성화할 수 있습니다. **HKEY_LOCAL_MACHINE\Software\Digital River\ConnectionClient\Debug" = "true"** 결과 로그는 여기 위치합니다: **C:\Users\RDP6\logs** .

TSplus 원격 액세스 업데이트

수정 사항 및 개선 사항을 확인하려면 클릭하세요. 변경 로그

우리 개발 팀은 Microsoft 운영 체제의 최신 버전과 최신 업데이트와의 안정성 및 호환성을 보장하기 위해 매일 작업하고 있습니다.

우리는 매주 새로운 기능과 개선 사항을 제공하게 되어 자랑스럽습니다.

서버를 최신 상태로 유지하는 것이 권장되는 이유입니다.

“서버당 2 세션” 문제가 발생할 때, 일반적으로 매달 두 번째 화요일에 Windows 업데이트 후, TSplus Remote Access (또는 TSplus LTS 18/17) 버전을 확인하십시오.

새로운 릴리스가 곧 발표되어 최신 Windows 업데이트와의 호환성을 복원할 것입니다.

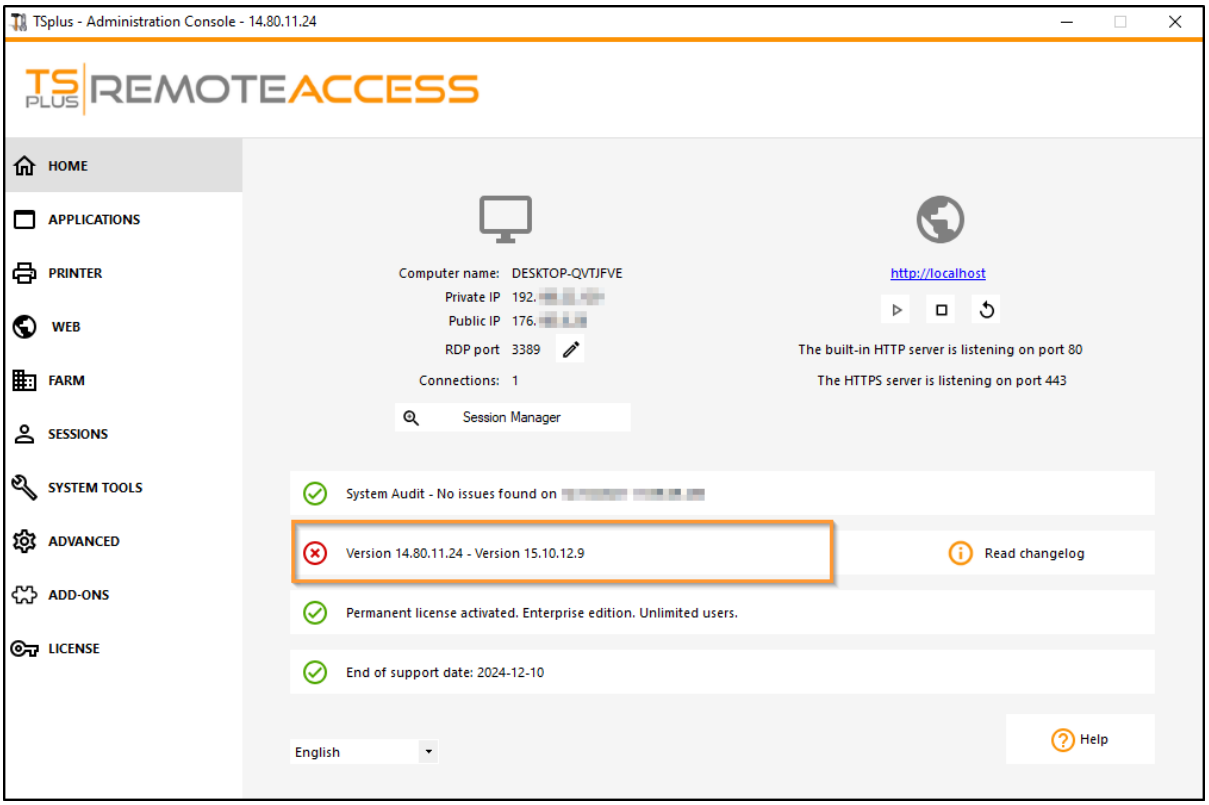
임시 해결책으로, 해당 날짜의 Windows 업데이트를 제거하고 재부팅할 수 있습니다.

중요: TSplus Remote Access를 제거하거나 이전 시스템 이미지를 복원하지 마십시오. 이러한 작업은 해결하기 훨씬 더 복잡한 라이센스 충돌을 유발할 수 있습니다. 대부분의 경우, 간단한 재부팅만으로 호환성 수정 사항을 자동으로 적용할 수 있습니다.

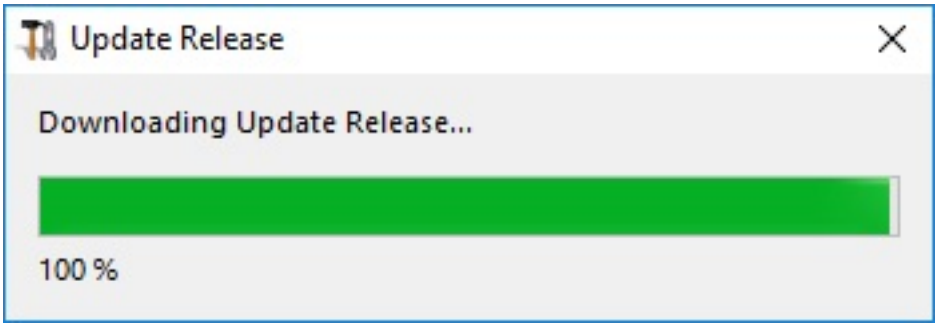
연간 지원 및 업데이트 서비스에 가입하면 최신 업데이트 및 버그 수정을 이용할 수 있습니다.

TSplus 버전을 확인하고 업데이트하려면:

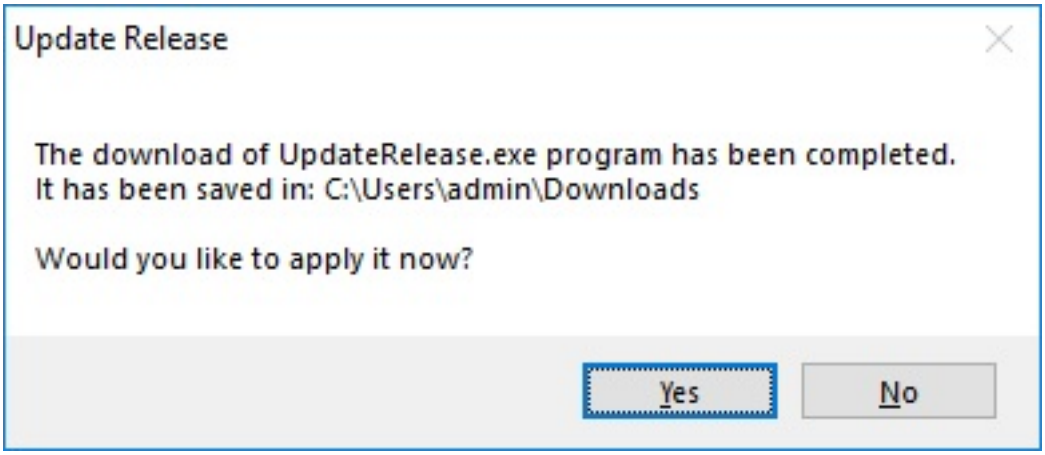
- 귀하의 AdminTool의 홈 탭에서 TSplus 릴리스 상태를 확인할 수 있습니다.



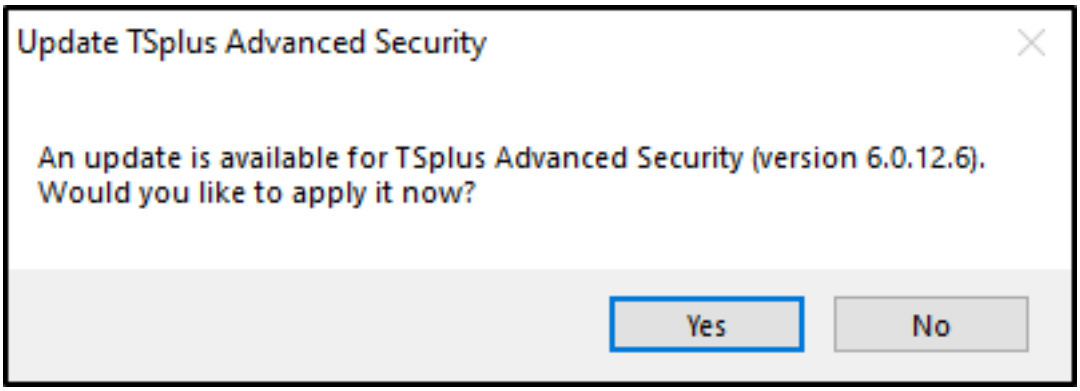
- 그것을 클릭할 수 있습니다. TSplus 11.50 버전부터 AdminTool이 자동으로 다운로드됩니다…



…그리고 요청 시 업데이트 릴리스 프로그램을 적용합니다:



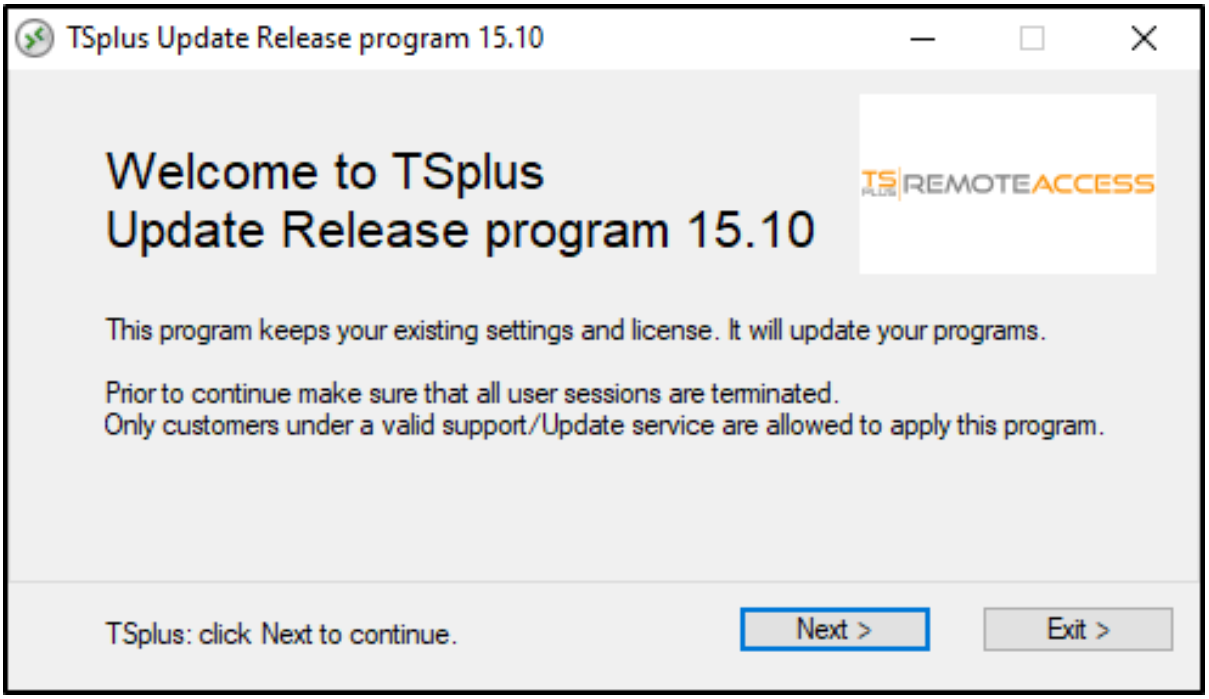
- TSplus 11.40 버전 이후로 설치할 선택권이 있습니다. TSplus 고급 보안 우리의 강력한 보안 추가 기능, 궁극적인 시험 버전(모든 보안 기능을 2주 동안 무료로 사용할 수 있음)을 귀하의 TSplus 시스템에:

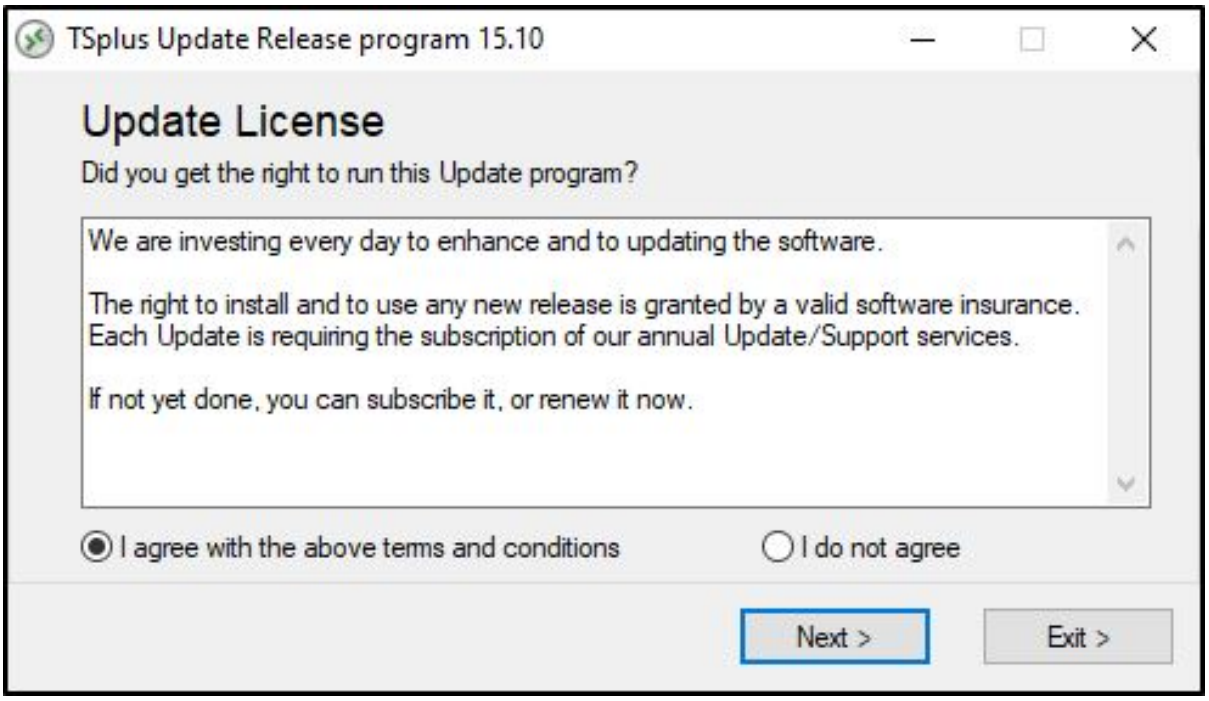


이 링크를 통해 여전히 다운로드할 수 있습니다: 업데이트 릴리스 수동으로 적용하세요.

업데이트 릴리스 프로그램은 현재 TSplus 설정을 안전하게 유지하도록 설계되었습니다.

TSplus 업데이트/지원 서비스에 아직 구독하지 않았거나 구독이 만료된 경우, 업데이트 릴리스 프로그램을 실행할 수 없습니다.

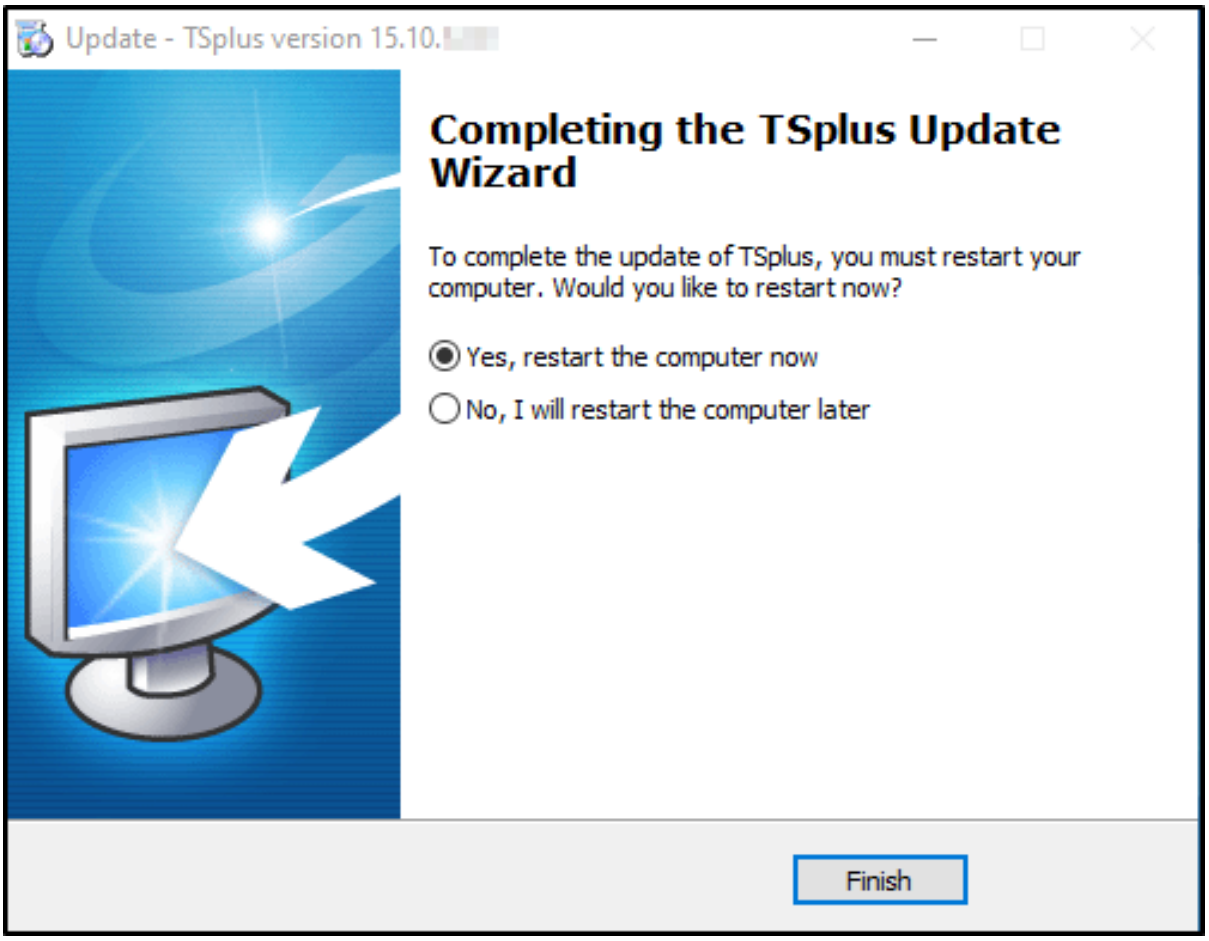




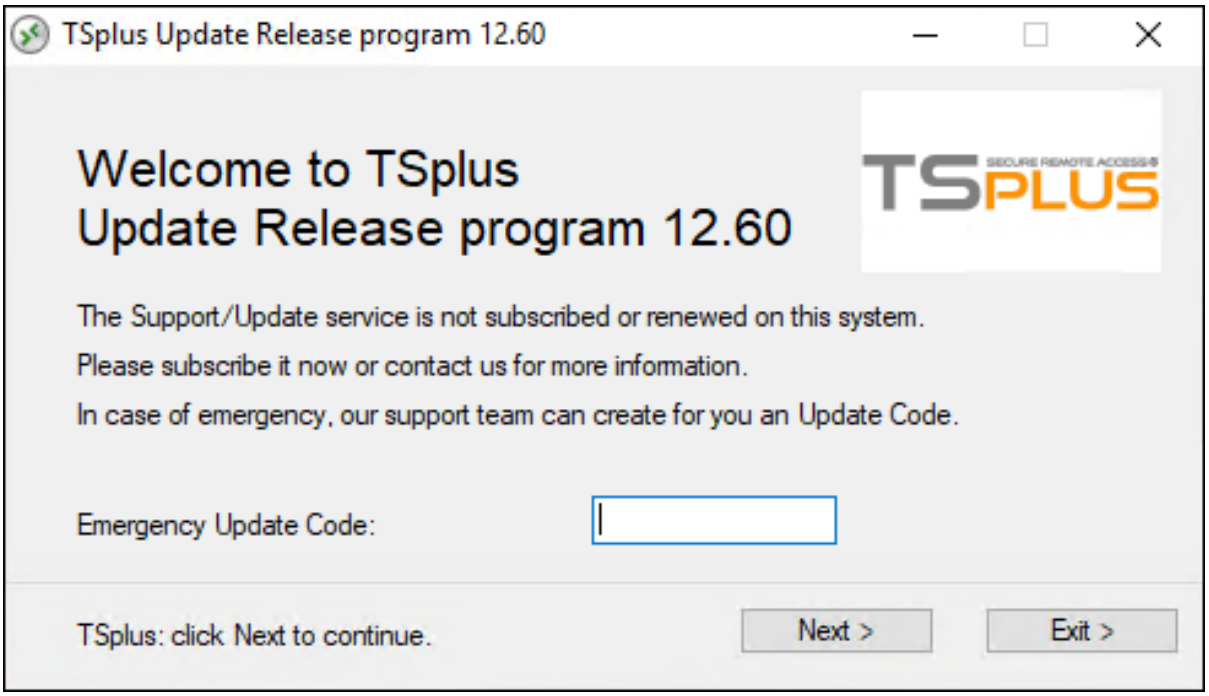
이 경우, 저희 Store Page에서 주문하시기를 권장합니다.

지원.lic 파일을 다운로드할 수 있는 적절한 정보를 받게 됩니다. 업데이트/지원 서비스를 활성화하는 것은 설명된 간단한 과정입니다. 여기 .

업데이트가 완료되면 재부팅이 필요합니다.



v14 이전 버전의 경우, 특정 요구 사항에 따라 TSplus 지원 팀이 업데이트 릴리스 프로그램을 잠금 해제하는 긴급 업데이트 코드를 제공할 수 있습니다.



업데이트 문제:

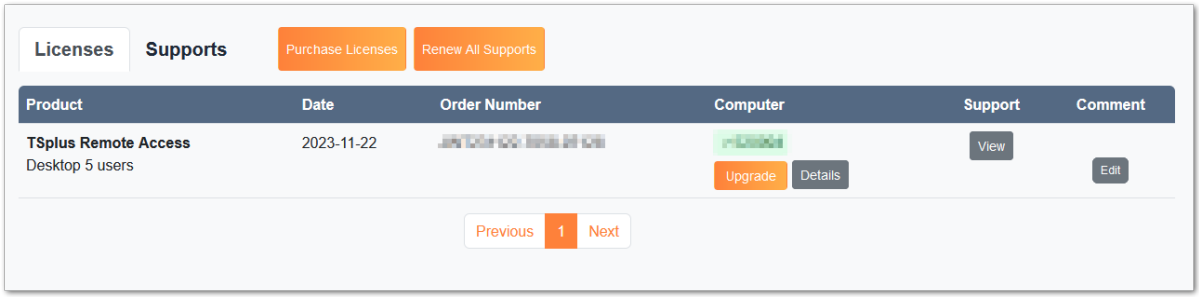
누락된 파일 확인

C:\Program Files (x86)\TSplus\reboot_required.dat

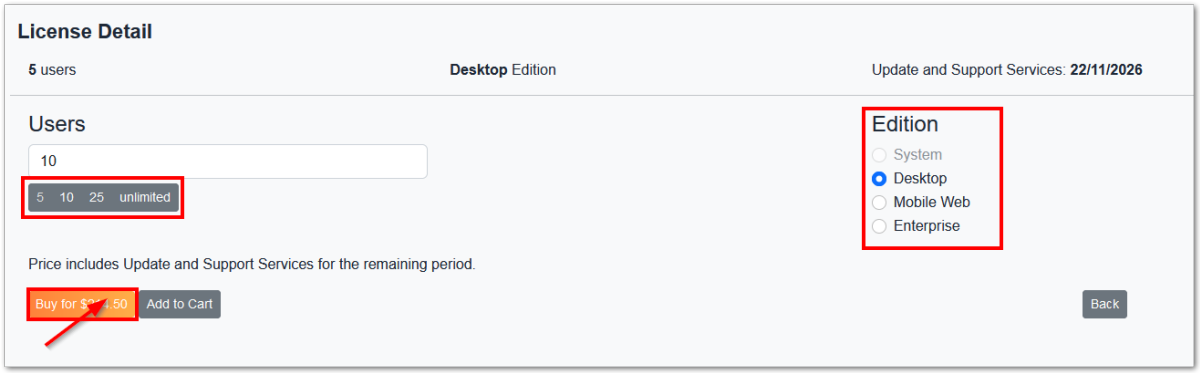
1. 이 파일이 존재하면 삭제하십시오.
2. 서버를 재시작하세요
3. 이 링크를 클릭하여 업데이트를 다시 실행하십시오: 업데이트 릴리스

TSplus 버전 업그레이드

현재 TSplus 버전을 업데이트하여 더 많은 사용자나 기능을 추가하고 싶다면, 귀하의 등록을 진행하십시오. 라이센스 포털.



업그레이드(사용자 및 버전)를 선택하고 클릭하세요. **구매하기** 우리 상점을 계속 이용해 주세요.



구매 후 업데이트는 즉시 적용되며 라이센스 포털에서 확인할 수 있습니다.
귀하의 장치에서도 동일한 절차를 따라 라이센스에 연결되도록 해야 합니다.

서버에서 클릭하십시오. **라이센스를 새로 고치세요** 관리 도구의 라이센스 탭에 있는 버튼.

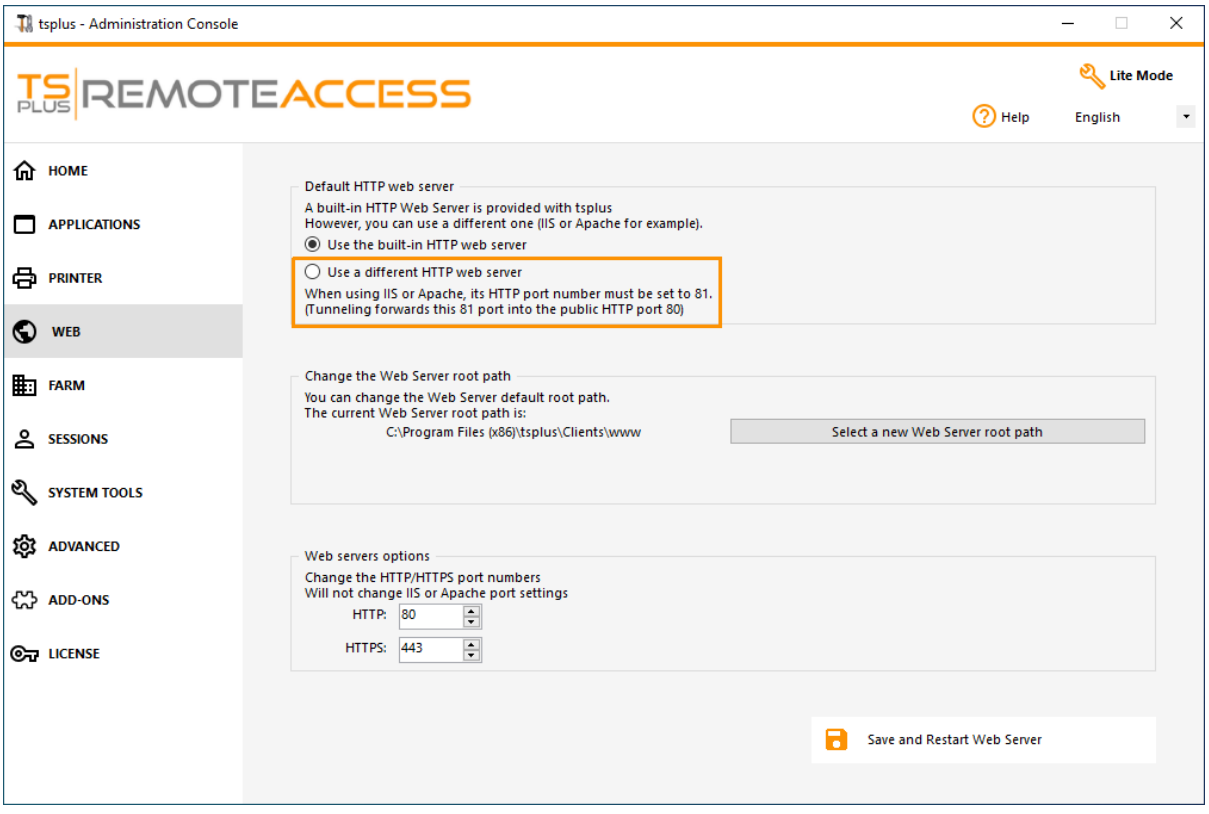
Apache를 Terminal Service Plus 기본 웹 서버 대신 사용하는 방법

사전 요구 사항

좋은 생각일 수 있습니다. 업데이트 터미널 서비스 플러스 최신 TSplus 프로그램을 받으려면 확실히 하세요.

1. AdminTool을 시작하고 웹 서버 탭으로 이동합니다.

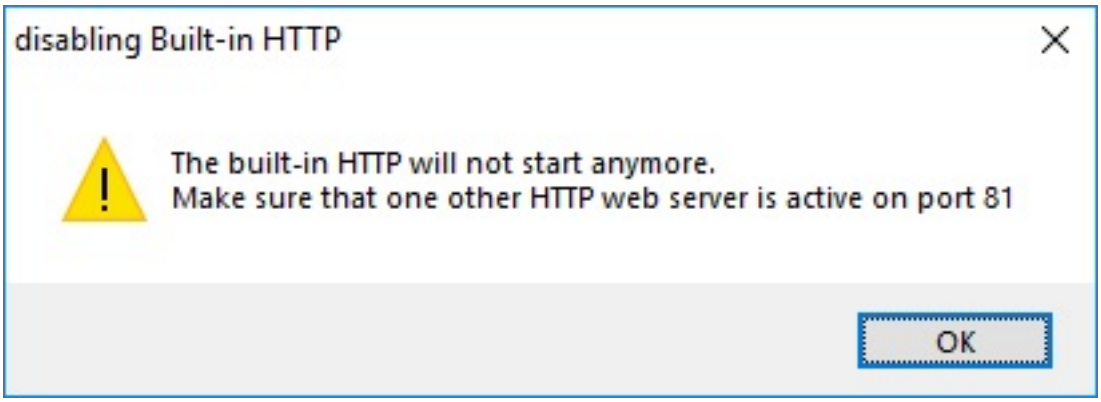
웹 서버 관리 타일을 클릭하고 확인하세요. **다른 HTTP 웹 서버 사용** 아파치를 사용하고 싶기 때문입니다.



그런 다음 버튼을 사용하십시오. **새로운 웹 서버 루트 경로 선택** TSplus에 새 웹 폴더 루트가 어

디에 있을지를 알려주기 위해.

TSplus는 요청된 파일/폴더를 이 새로운 루트 폴더로 복사하며, 이 시점에서 Apache에 대한 TSplus 설정이 거의 완료되었습니다. 팝업이 Apache HTTP 포트를 81로 변경할 것을 권장합니다.



이제 Apache를 설정할 시간입니다.

2. 아파치 설정하기

HTTP를 80에서 81로 변경하십시오.

이 작업을 수행하는 특정 방법은 귀하의 Apache 버전과 현재 Apache 설정에 따라 다릅니다.

Apache 설정 파일을 수정하기 전에 백업하는 것을 권장합니다. 필요할 경우 복원할 수 있는 방법이 있습니다.

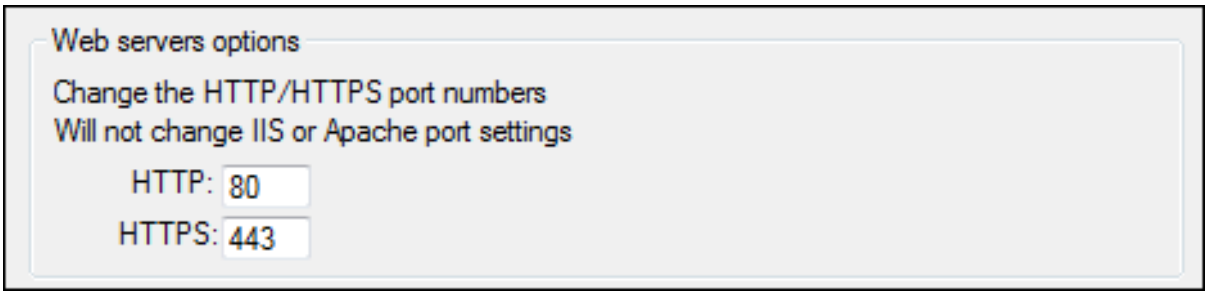
일반적으로 "Apache\conf" 디렉토리에 있는 httpd.conf 파일을 편집하여 Apache 수신 포트를 변경할 수 있습니다:

듣기 81

작업이 완료되면 Apache 서비스를 재시작하십시오.

3. TSplus 웹 서버 관리 도구로 돌아가기

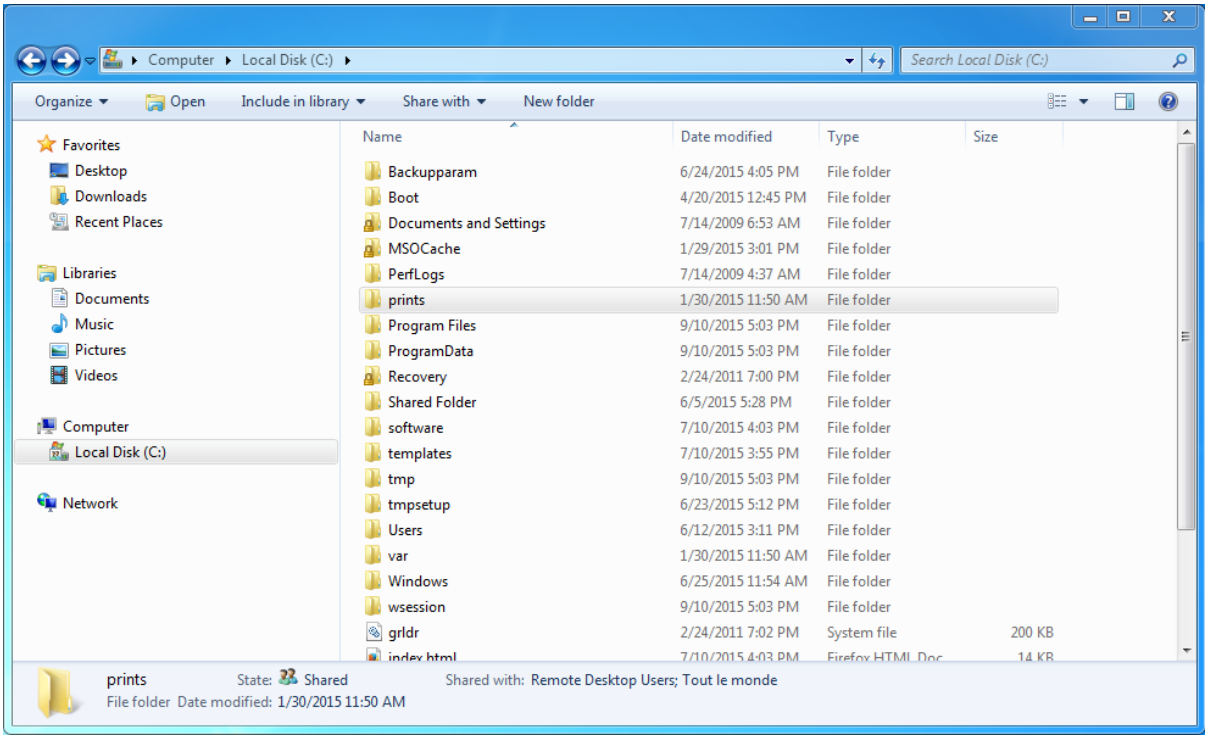
TSplus 웹 관리 도구에서 HTTP 및 HTTPS 포트를 설정할 수 있습니다. 표준 포트를 사용하는 것이 좋지만, 다른 프로세스와의 충돌을 피하려고 할 때 이 기능이 유용할 수 있습니다.

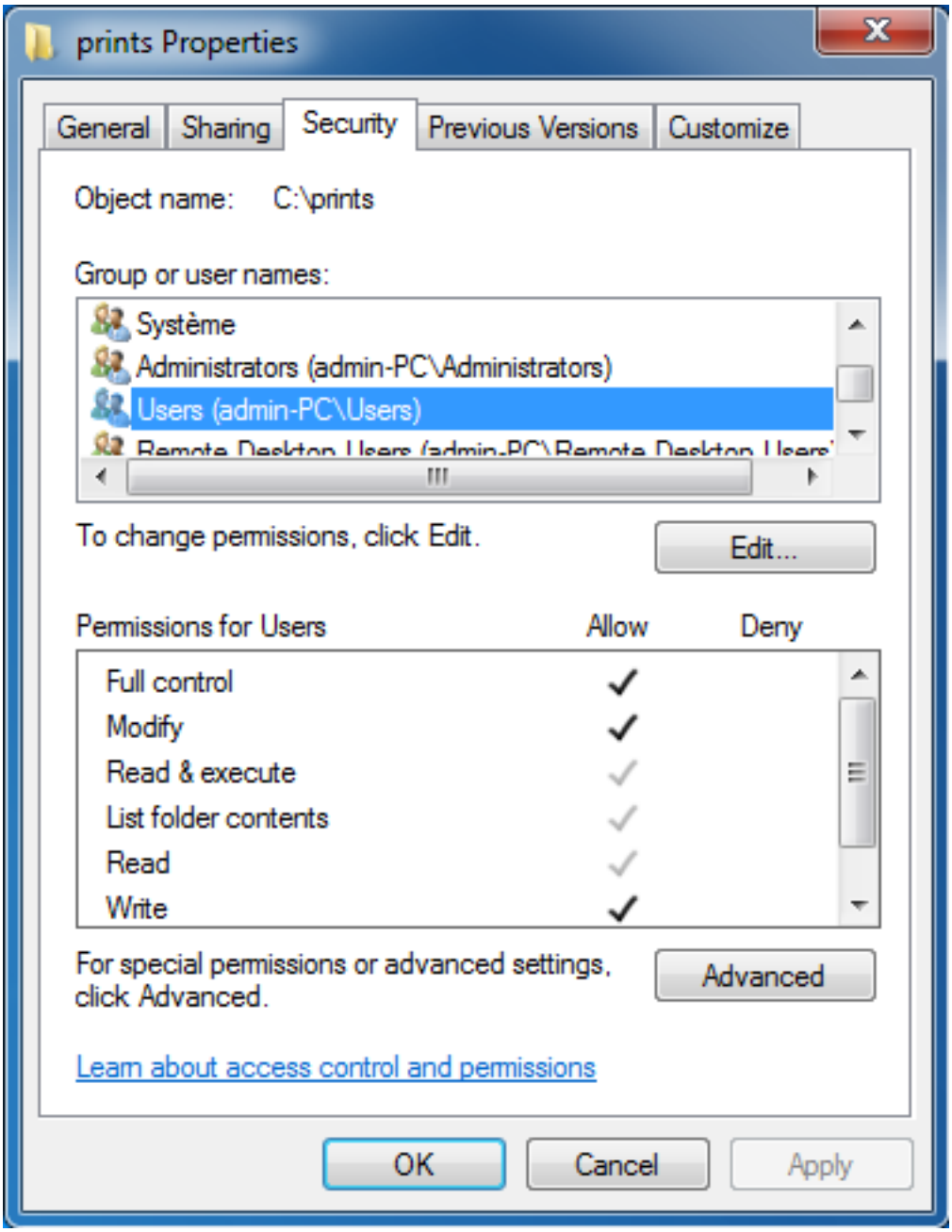


4. 마지막 단계

Universal Printer를 위해 PRINTS 폴더에 쓸 수 있어야 합니다.

모두/사용자...가 .../프린트 폴더에 대한 전체 권한을 가지고 있는지 확인하세요.





그런 다음 웹 액세스 페이지로 사용할 .html 파일을 선택하십시오:

C:\Program Files (x86)\TSplus\Clients\www

웹 루트 폴더에 index.html로 복사하세요. 일반적으로 이 폴더는 "Apache\htdocs" 디렉토리입니다.

5. TSplus Gateway Portal, 로드 밸런싱 및/또는 HTML5 파일 전송을 위한 특정 설정

이 Apache 기반 시스템을 TSplus Gateway Portal로 사용하거나 TSplus Gateway Portal Load Balancing 기능을 사용하거나 HTML5 파일 전송 기능을 사용하려면 Apache에서 TSplus GCI 스크립트의 실행을 허용해야 합니다.

먼저, Apache에서 CGI 모듈이 활성화되어 있어야 합니다.

httpd.conf 파일을 “Apache\conf” 디렉토리에서 편집하고 다음과 같은 줄을 찾으십시오:

;LoadModule cgi_module modules/mod_cgi.so

CGI 모듈을 활성화하려면 ”;”를 제거하십시오.

LoadModule cgi_module modules/mod_cgi.so

그런 다음, 다음으로 시작하는 줄을 찾으십시오:

AddHandler cgi-script

Apache가 .exe 파일을 CGI 프로그램으로 처리할 수 있도록 .exe 확장자를 추가하십시오:

AddHandler cgi-script .exe

마지막으로, Apache에 TSplus “cgi-bin” 폴더에 CGI 프로그램이 포함되어 있음을 알려야 합니다. 이를 위해 “Apache\conf” 디렉토리에 있는 httpd.conf 파일에 다음 줄을 추가해야 합니다:

ScriptAlias /cgi-bin/ “C:/Program Files (x86)/TSplus/Clients/www/cgi-bin/”

작업이 완료되면 Apache 서비스를 재시작하십시오.

Apache 서버에서 CGI를 설정하는 데 문제가 발생하면 다음을 참조하십시오. 공식 Apache 문서

설정 확인 중: 설정을 확인하려면 서버에서 웹 브라우저를 열고 이동하십시오. http://localhost/cgi-bin/hb.exe Apache 오류 페이지가 표시되면 Apache 구성에 문제가 있는 것입니다. 텍스트/숫자의 줄이 표시되면 모든 것이 정상입니다!

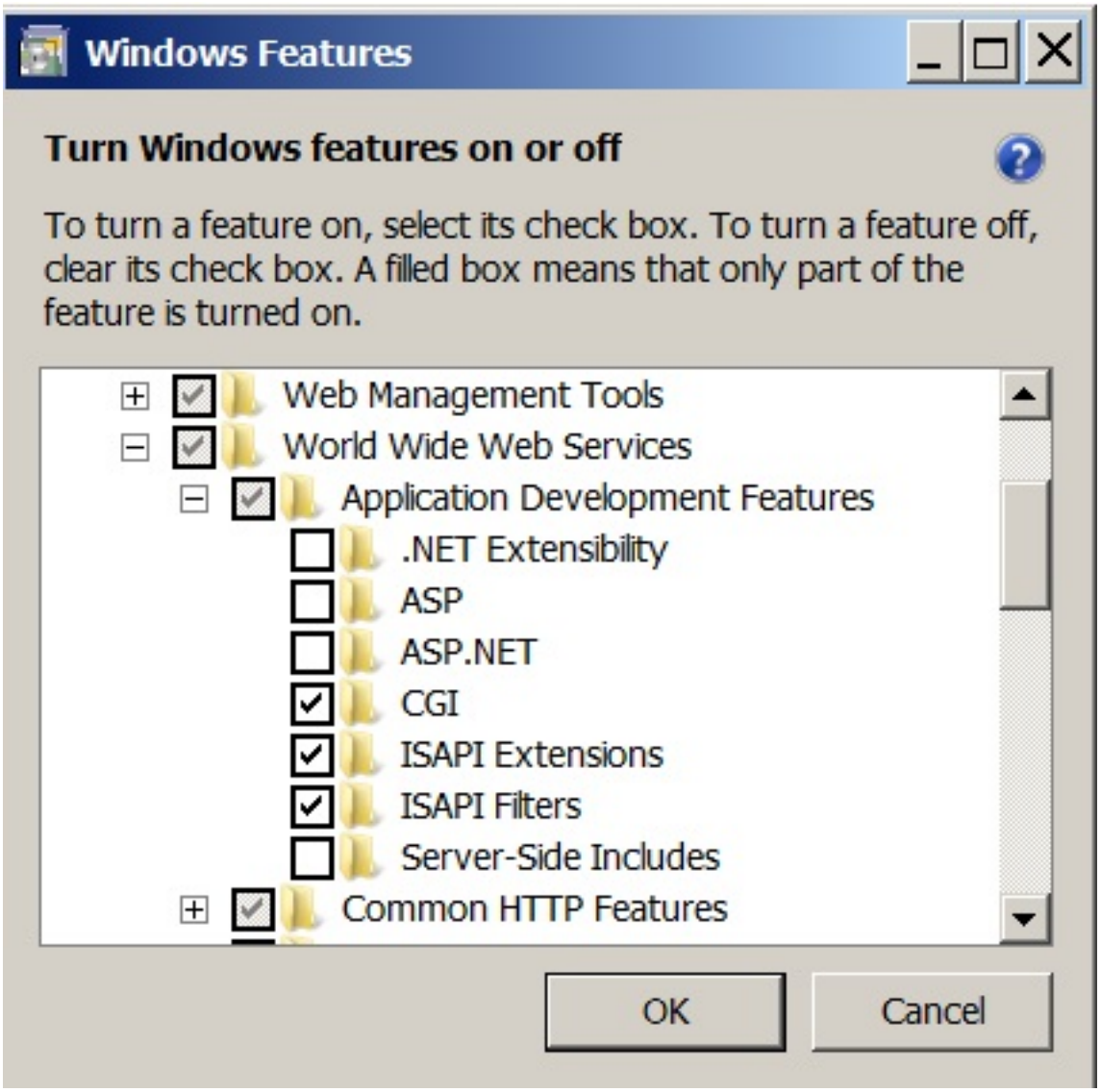
IIS를 Terminal Service Plus 기본 웹 서버 대신 사용하는 방법

사전 요구 사항

좋은 생각일 수 있습니다. 업데이트 터미널 서비스 플러스 최신 TSplus 프로그램을 받으려면 확실히 하세요.

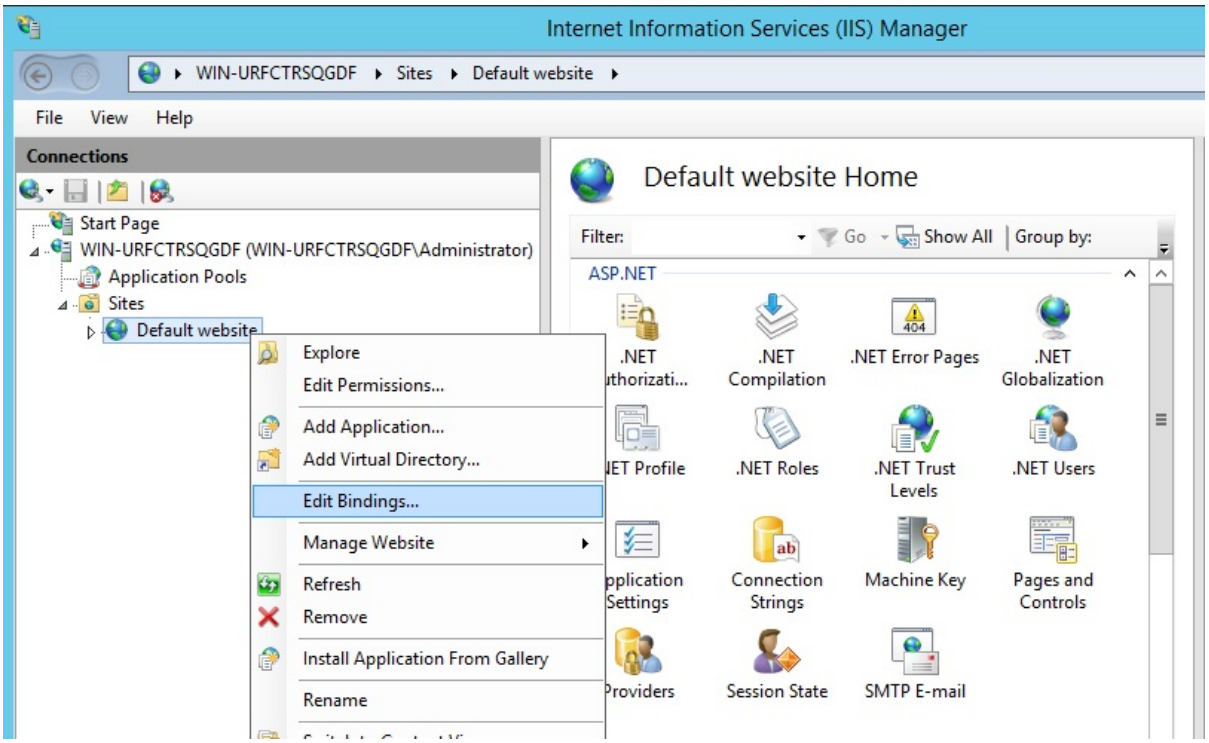
1. IIS 구성

- IIS를 다음 모듈과 함께 설치하십시오: CGI, ISAPI 확장 및 ISAPI 필터.

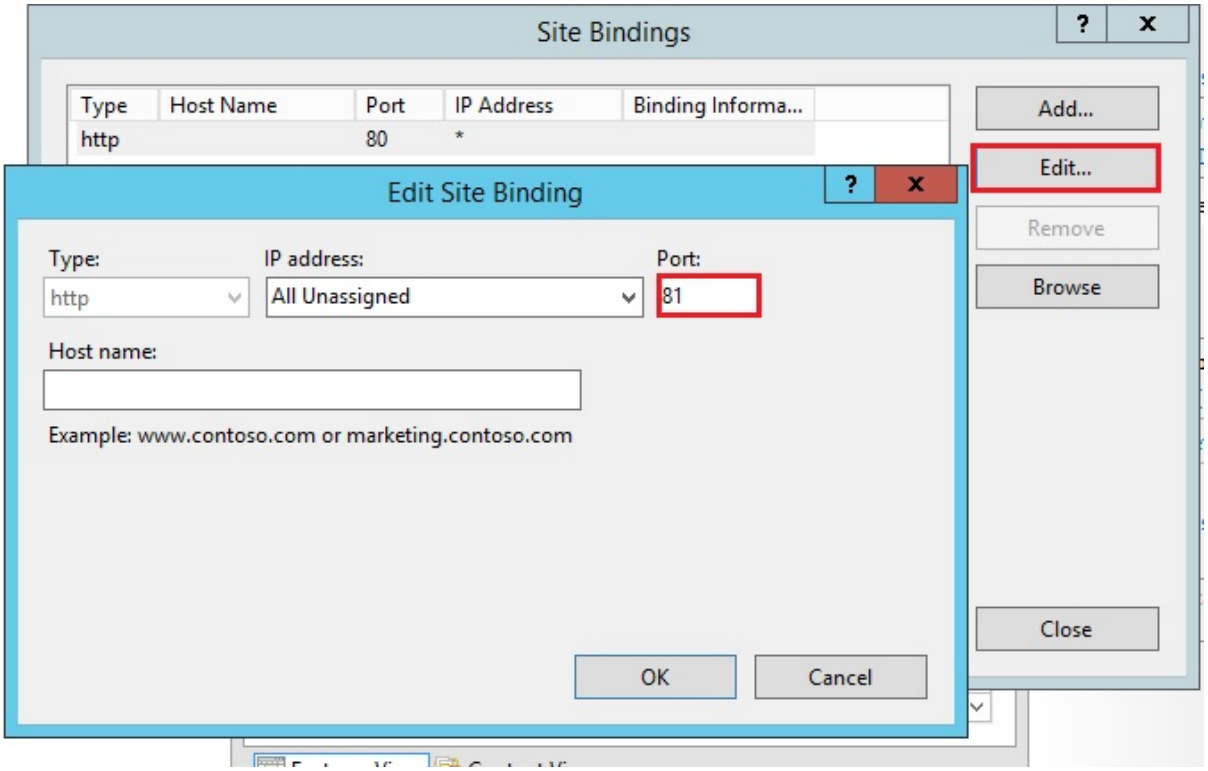


- IIS 포트 구성:

IIS 관리 콘솔에 접근하여 서버 이름 아래의 목록을 확장한 다음, “사이트” 메뉴를 확장하고 “기본 웹 사이트”를 마우스 오른쪽 버튼으로 클릭한 후 “바인딩 편집”을 클릭하십시오.



"http"를 클릭하고 "Edit"를 클릭하세요. 포트를 81로 변경한 후 Ok를 클릭하고, 그 다음 Close를 클릭하세요.



443 포트를 비활성화하거나 이 포트를 다른 무료 포트로 변경하십시오.

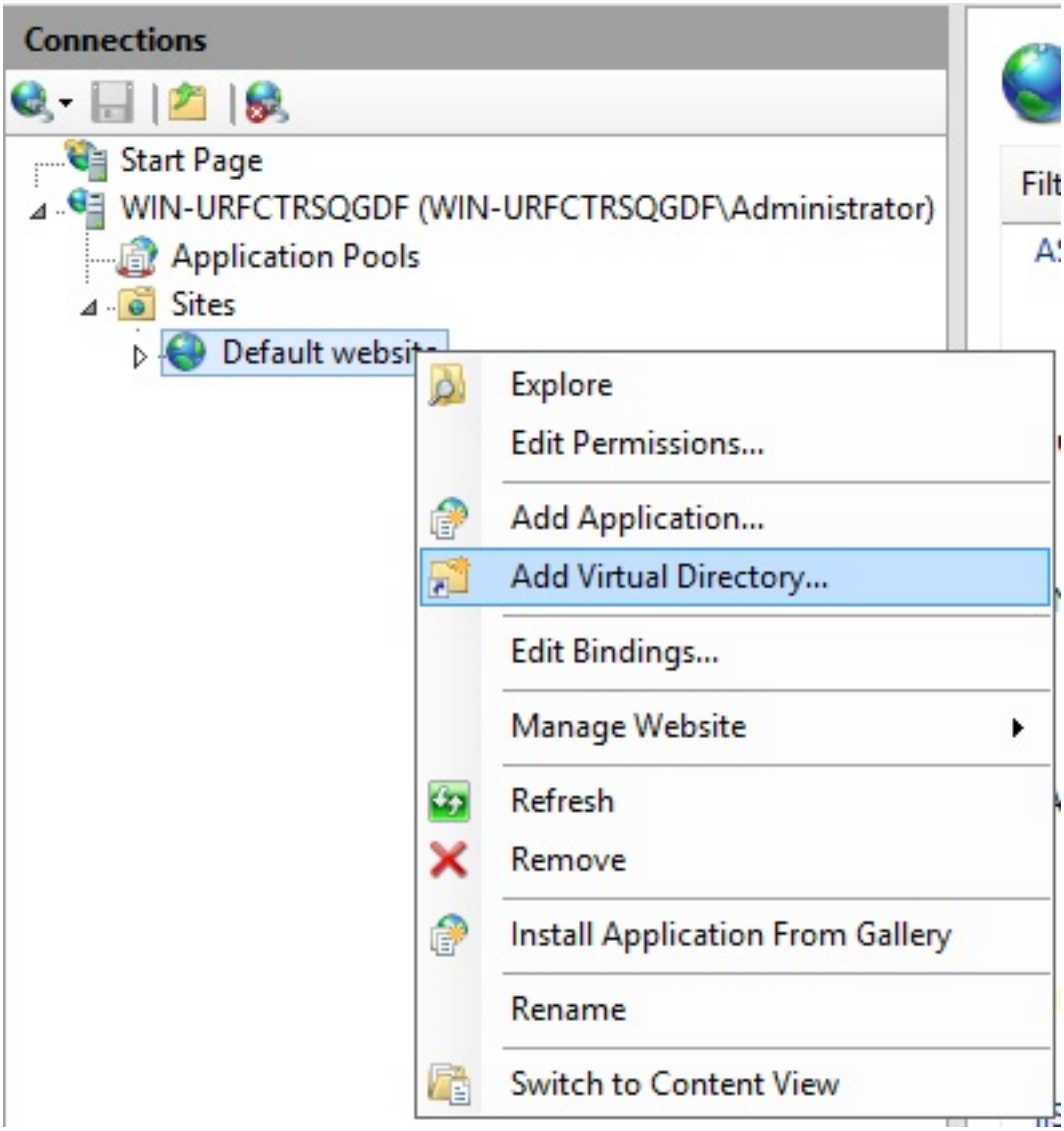
그런 다음 IIS 관리자를 다시 시작하십시오.

2. CGI를 위한 가상 디렉토리 생성

기본 웹 루트(C:\Program Files (x86)\TSplus\Clients\www)에서 모든 파일은 웹 루트 디렉토리가 수정될 때 복사되지 않습니다.

IIS 웹 서버로 마이그레이션할 때 수동으로 확인하고 복사해야 합니다.

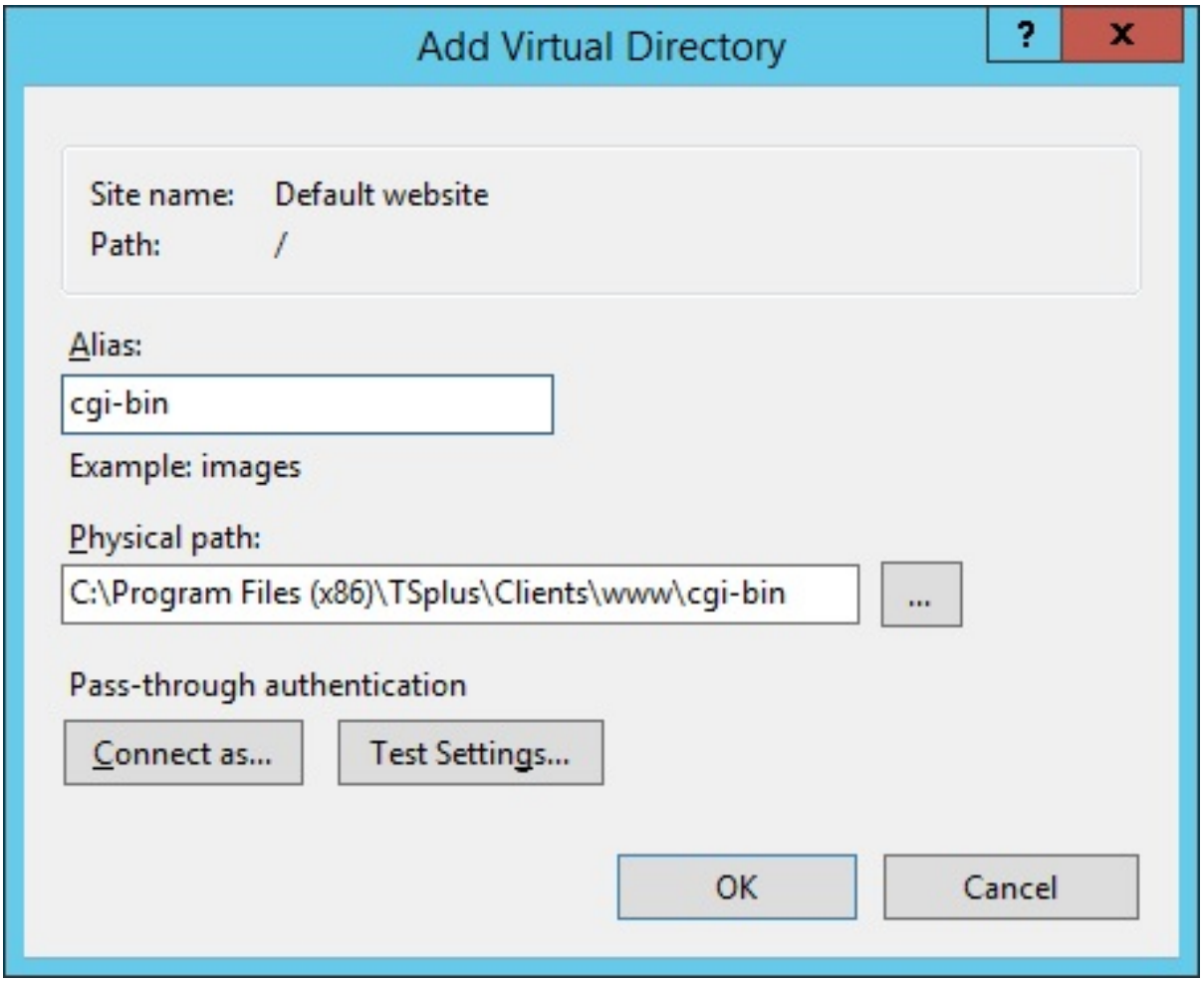
왼쪽 패널 메뉴에서 서버 아래의 메뉴를 확장한 다음 "사이트"를 선택하고, 아래 이미지에 표시된 대로 사이트를 마우스 오른쪽 버튼으로 클릭하여 새 "가상 디렉터리"를 추가합니다.



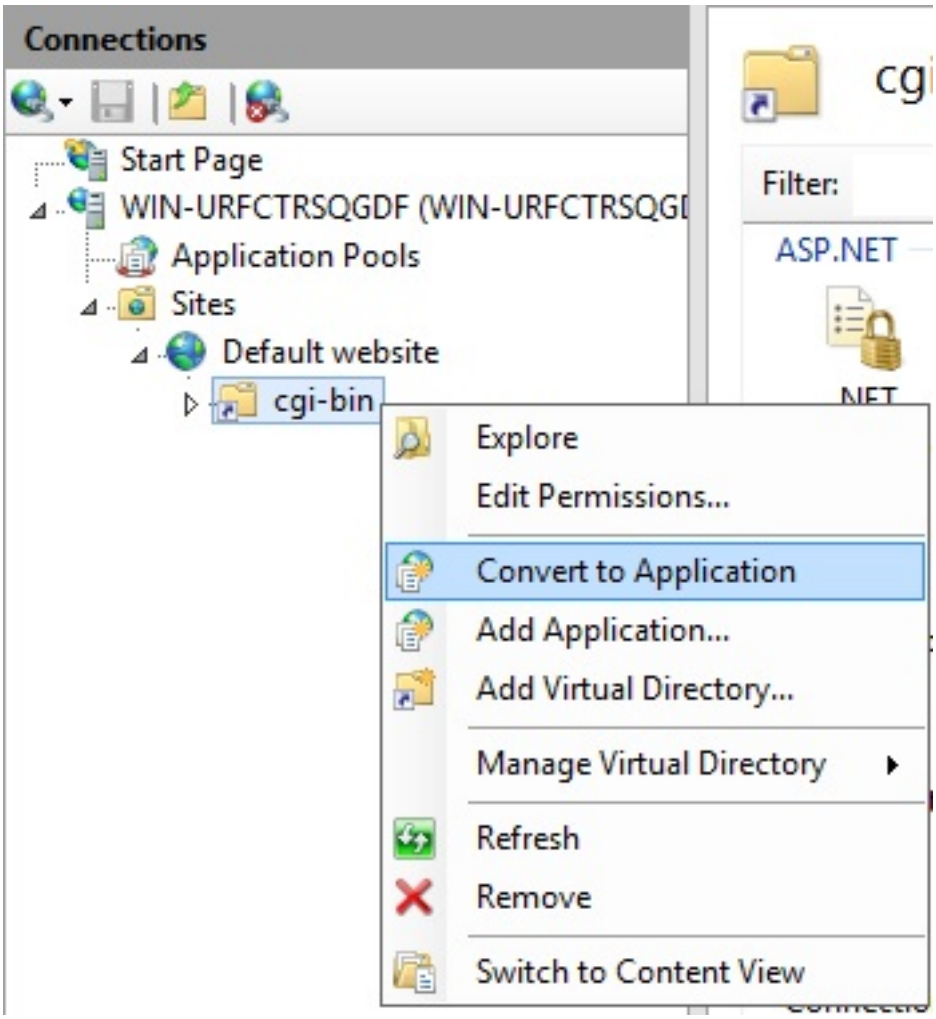
열리는 창에서 다음과 같이 입력하십시오:

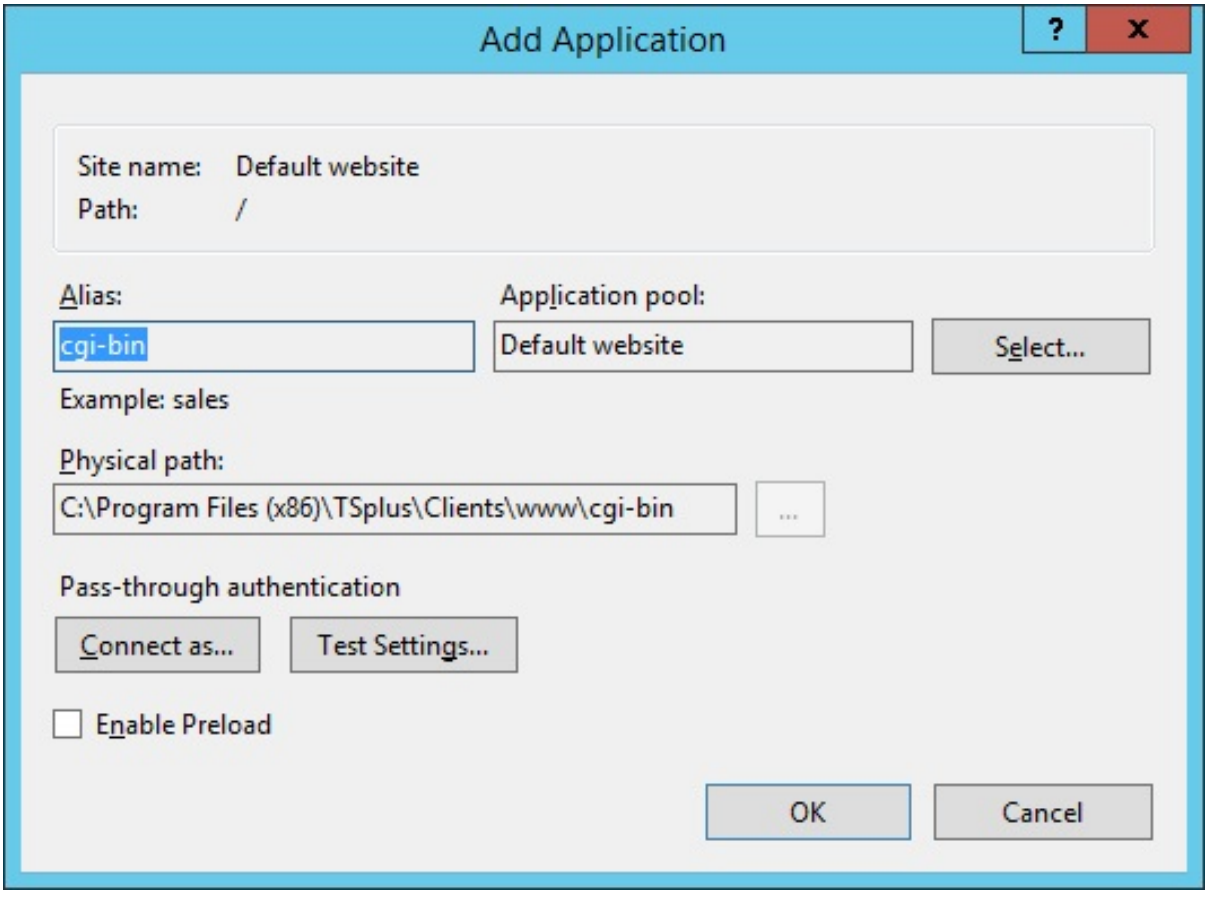
별칭: cgi-bin

물리적 경로: C:\Program Files(x86)\TSplus\Clients\www\cgi-bin

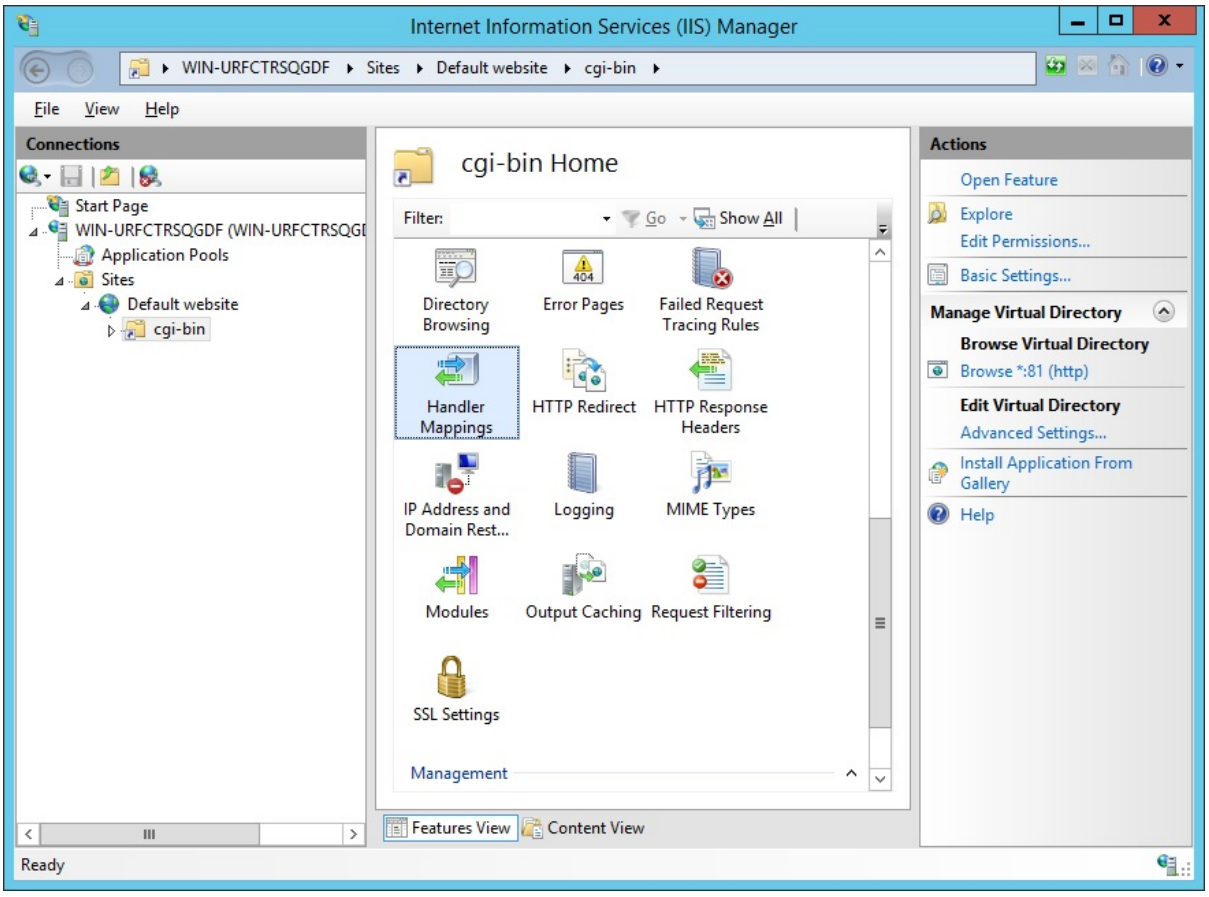


그런 다음 "확인"을 클릭하면 "cgi-bin" 가상 디렉터리가 IIS 웹 사이트에 추가된 것을 볼 수 있습니다. 이제 이 "cgi-bin" 가상 디렉터리를 마우스 오른쪽 버튼으로 클릭하고 "응용 프로그램으로 변환"을 클릭합니다. "확인"을 클릭하고 기본 설정을 수락합니다.


Connections
Start Page
WIN-URFCTRSQGDF (WIN-URFCTRSQGD
Application Pools
Sites
Default website
cgi-bin
Filter:
ASP.NET
Explore
Edit Permissions...
Convert to Application
Add Application...
Add Virtual Directory...
Manage Virtual Directory
Refresh
Remove
Switch to Content View

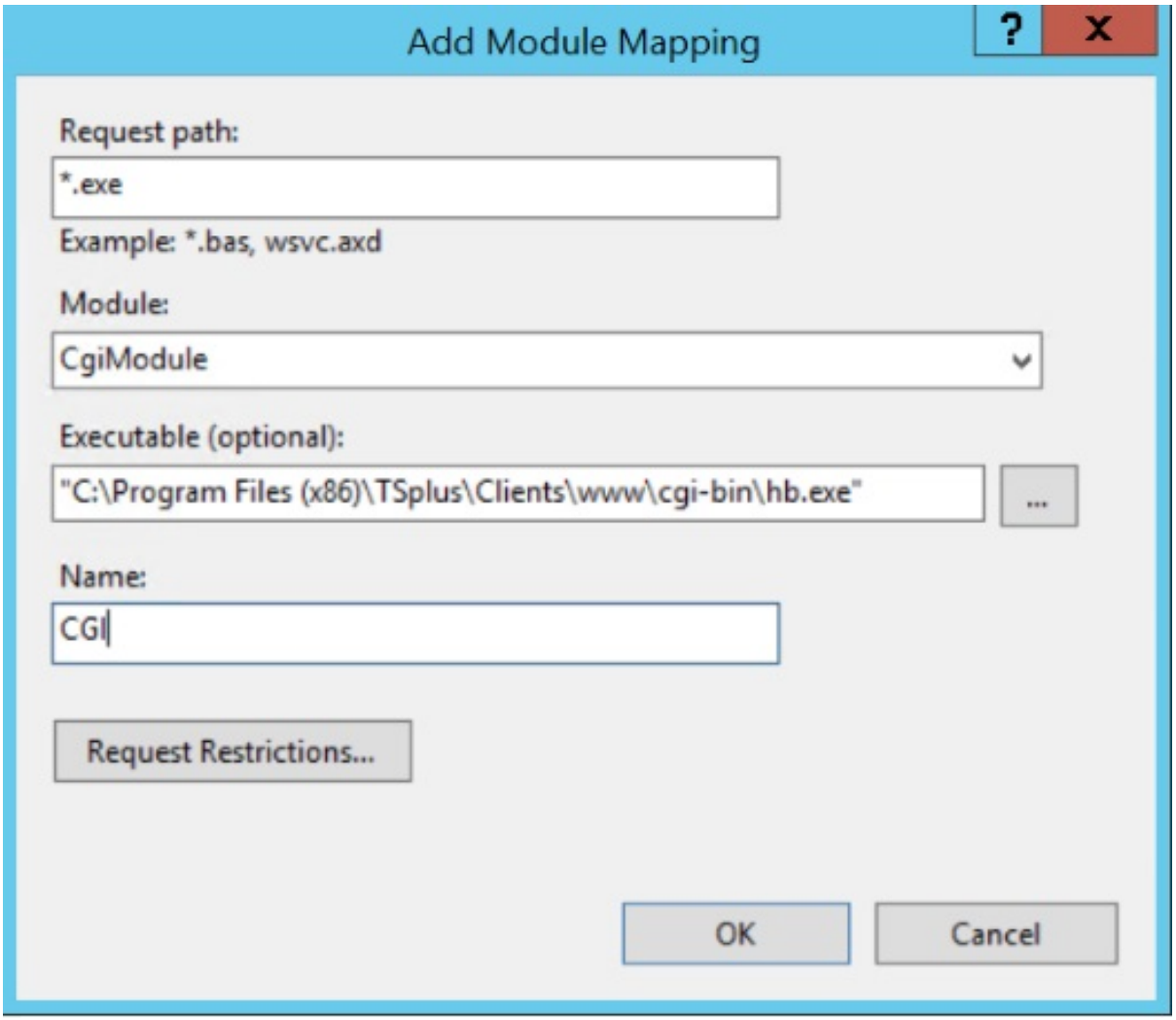

Add Application
Site name: Default website
Path: /
Alias:
cgi-bin
Example: sales
Application pool:
Default website
Select...
Physical path:
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin
...
Pass-through authentication
Connect as...
Test Settings...
Enable Preload
OK
Cancel

그런 다음 관리자 창의 오른쪽에서 이 폴더에 대한 "핸들러 매핑" 아이콘을 선택하십시오.

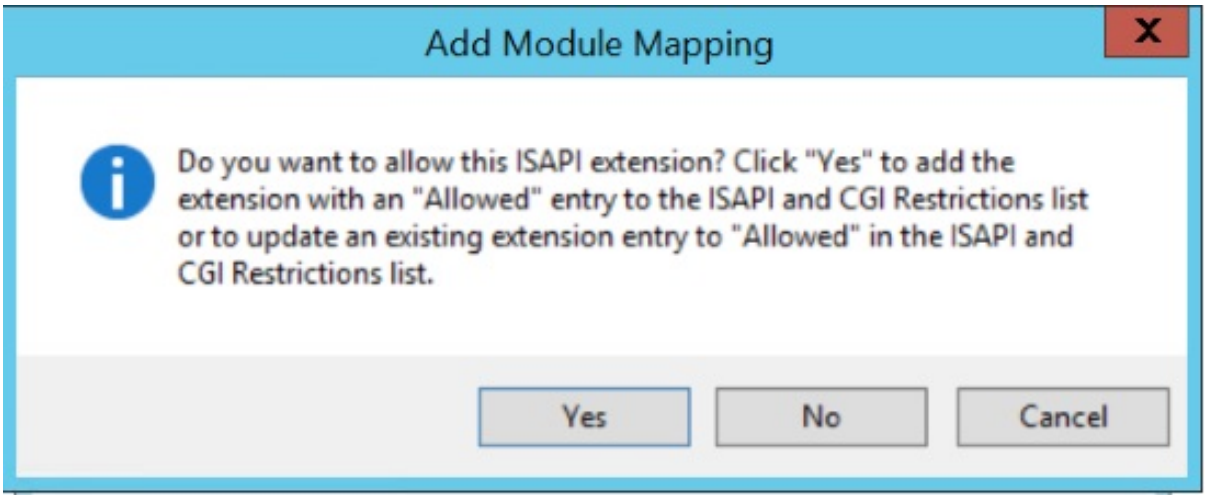


핸들러 매핑 목록에서 “CGI-exe”를 두 번 클릭합니다.

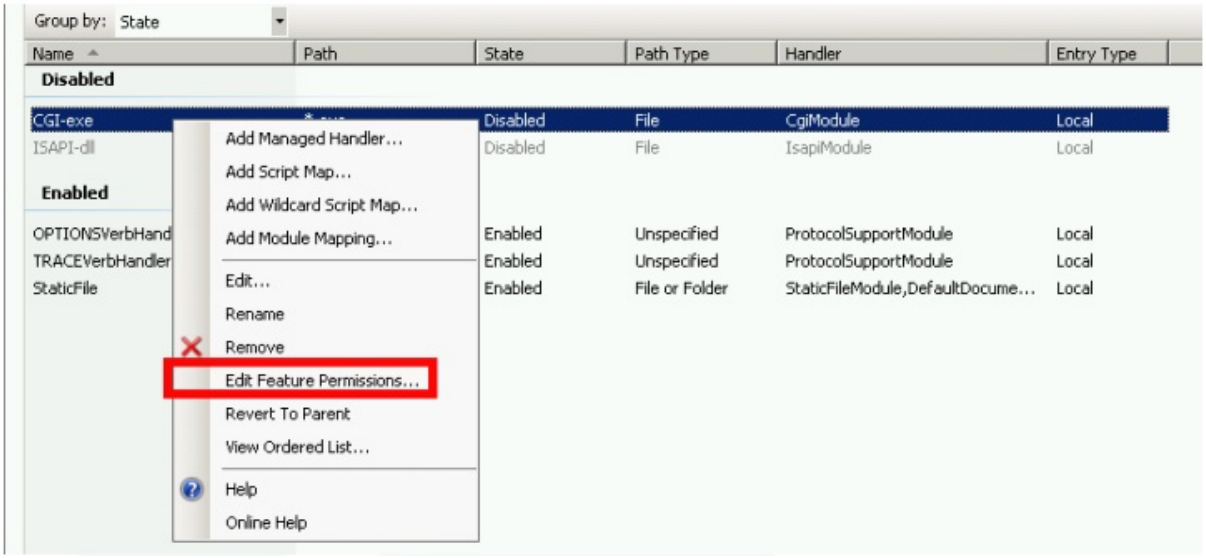
그런 다음 Executable 속성 상자에서 hb.exe 실행 파일을 검색하고 확인을 클릭합니다.



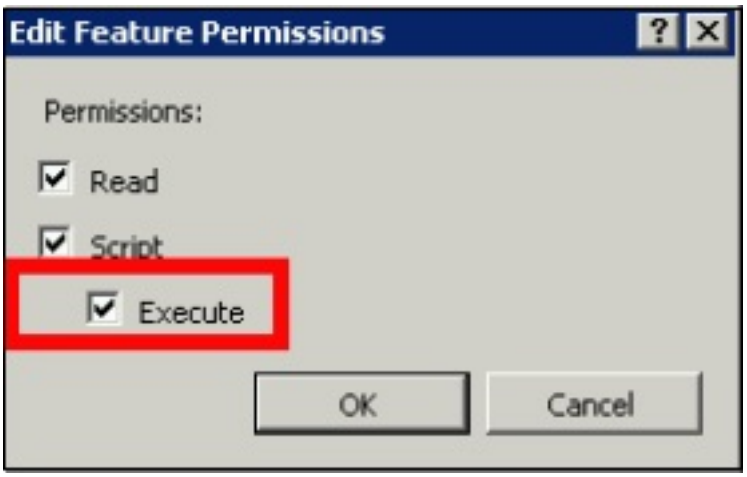
확인을 위한 프롬프트가 나타납니다. “확인”을 클릭하여 이 ISAPI 확장을 허용합니다.



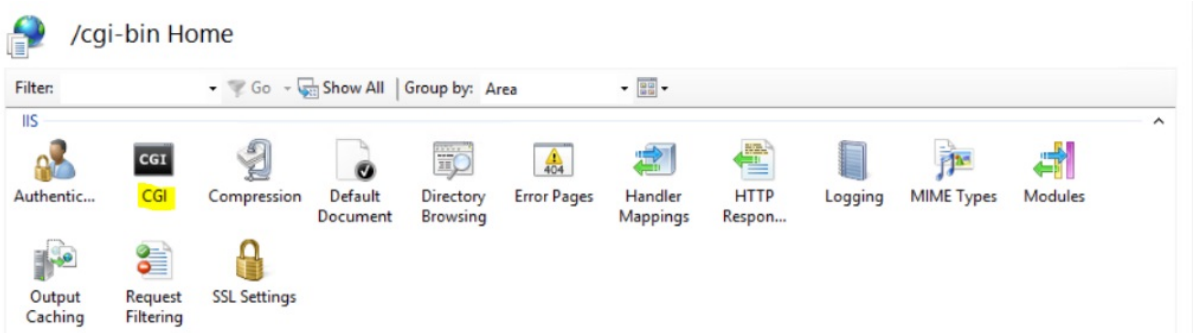
이제 “기능 권한 편집”을 클릭하세요:



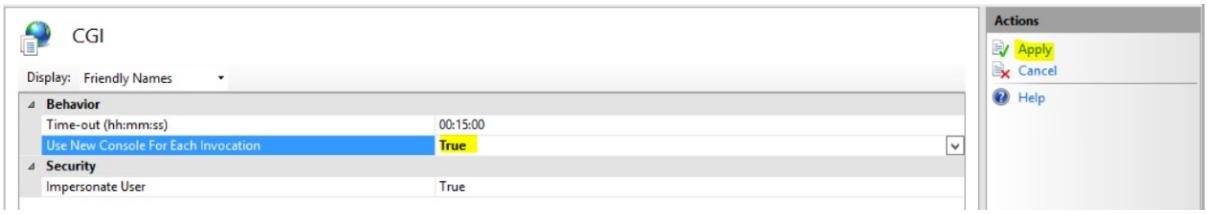
"실행" 체크박스를 선택하고 확인을 클릭하세요:



"CGI-bin" 홈으로 돌아가려면 "CGI"를 클릭하여 CGI 속성을 엽니다:



"각 호출에 대해 새 콘솔 사용"의 값을 "True"로 변경합니다. 그런 다음 "적용"을 클릭하여 변경 사항을 저장합니다.

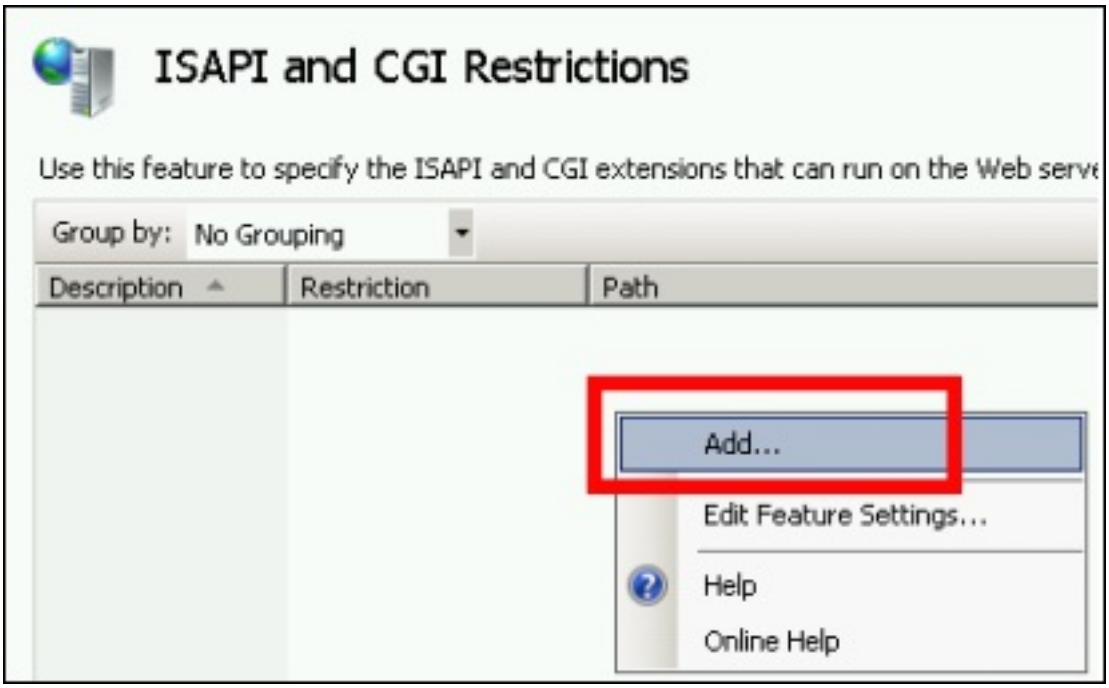


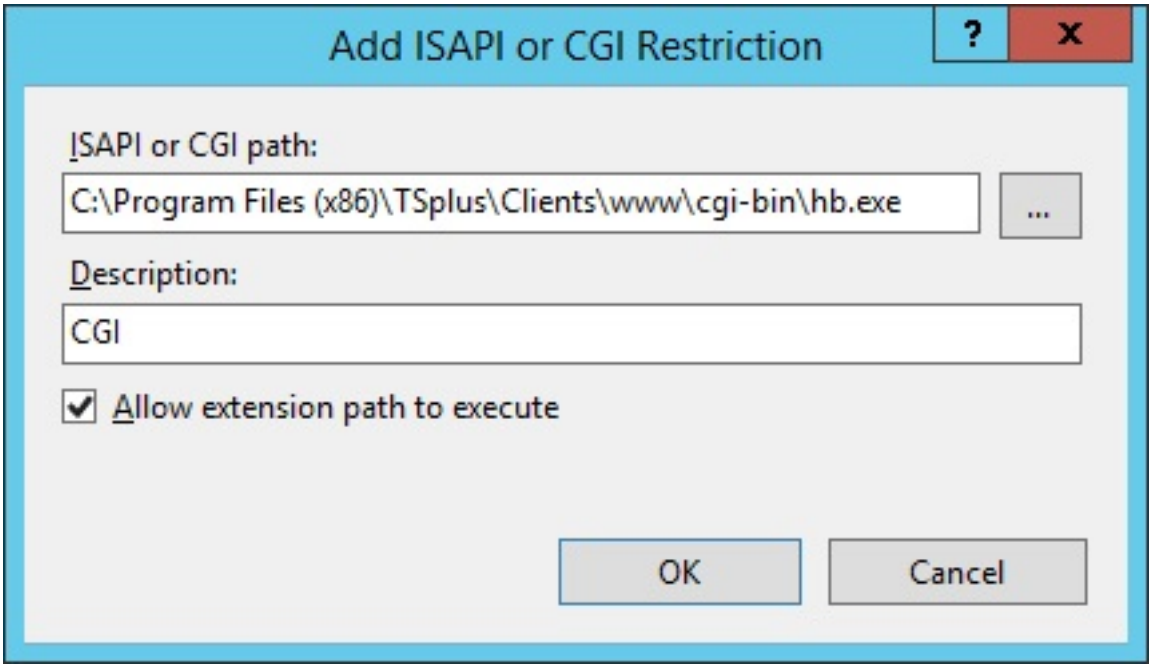
3. CGI 확장 권한 구성

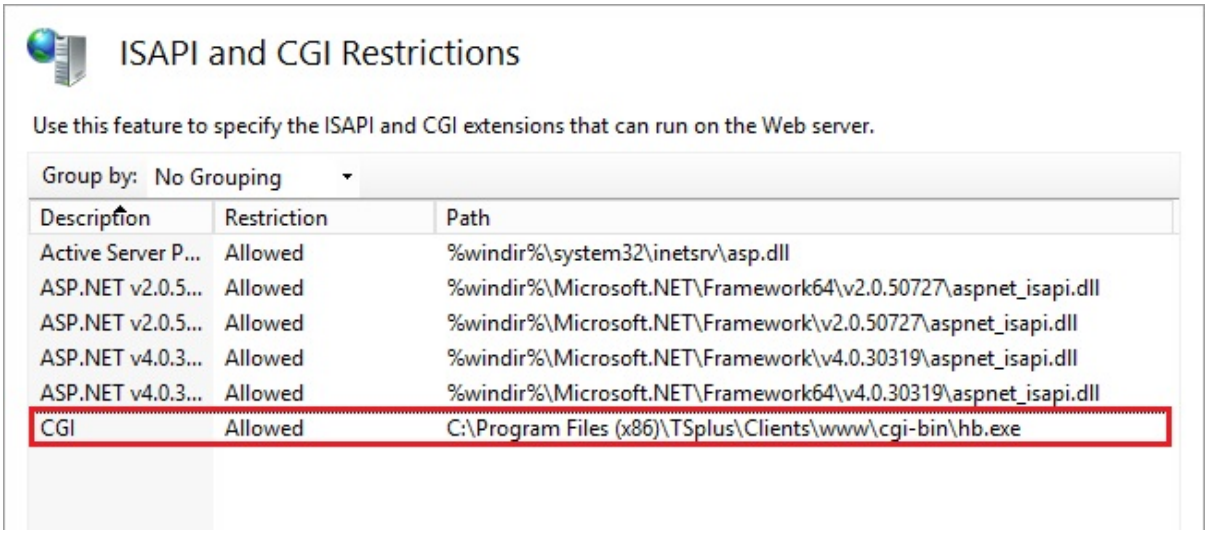
이제 마지막 단계는 서버에서 CGI 확장이 실행되도록 허용하는 것입니다. "ISAPI 및 CGI 제한" 아이콘을 클릭하십시오. 이 아이콘은 창 왼쪽 메뉴에서 머신 이름을 클릭하여 찾을 수 있습니다.



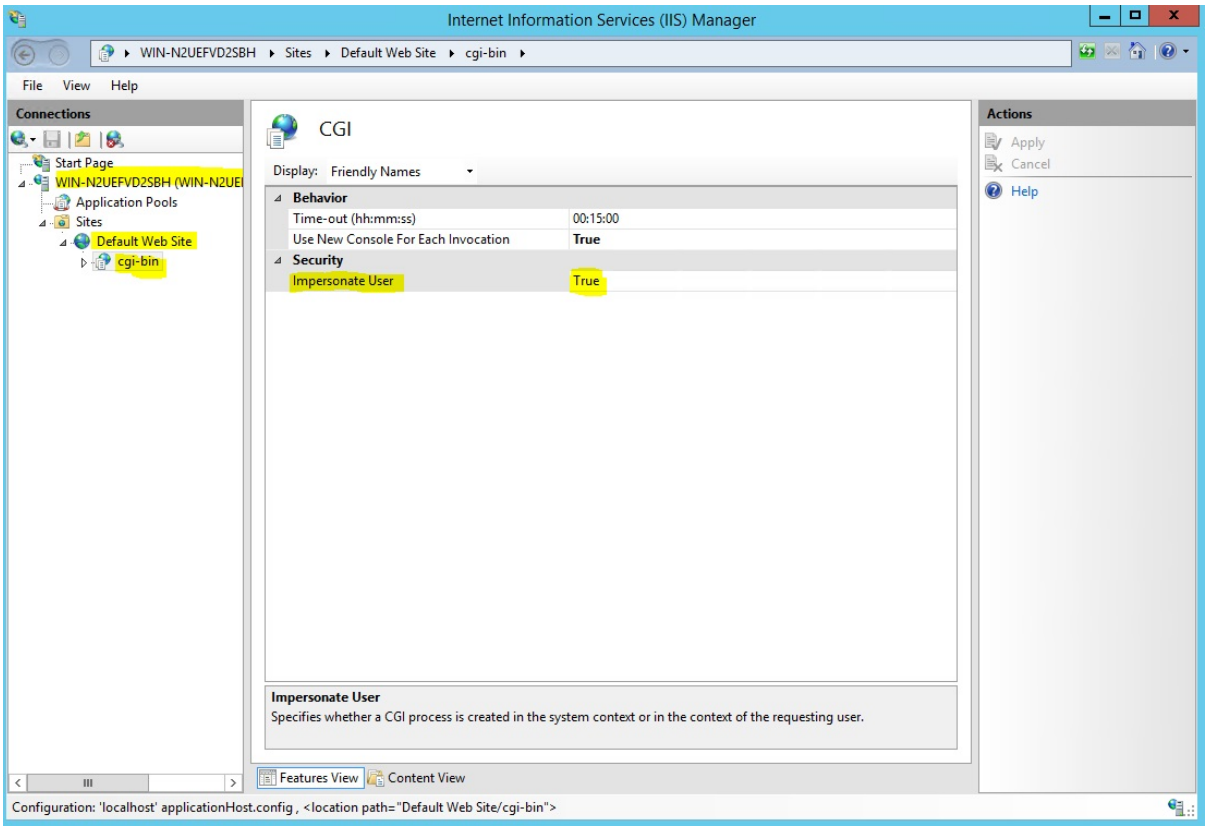
“ISAPI 및 CGI 제한” 페이지에서 창 오른쪽에 있는 “추가 ...”를 클릭합니다. 이제 TSplus 폴더에 호스팅된 “hb.exe” 파일의 전체 경로를 지정합니다. “확장 경로 실행 허용” 옵션을 반드시 선택하십시오. 다음 이미지를 설명합니다:







서버의 CGI 섹션에서 "기본 웹 사이트"와 "cgi-bin"의 "사용자 가장하기" 설정이 "참"으로 되어 있는지 확인하십시오.



- 사용자 "IUSR"에게 디렉터리에서 전체 권한 부여
  C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- IUSR 사용자가 디렉터리에 대한 전체 제어를 위해 구성될 때 권한 상속을 활성화해야 합니다.
  C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- 사용자 "IUSR"에게 디렉터리에서 전체 권한 부여
  C:\Program Files (x86)\TSplus\Clients\webserver\twofa

4. IIS에 Mime 유형 추가

관리자로 명령 프롬프트를 열고 다음 명령을 실행하십시오:

터미널 창

%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent

/+[fileExtension='.dat',mimeType='text/plain']

터미널 창

%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent
/+[fileExtension='.',mimeType='text/plain']

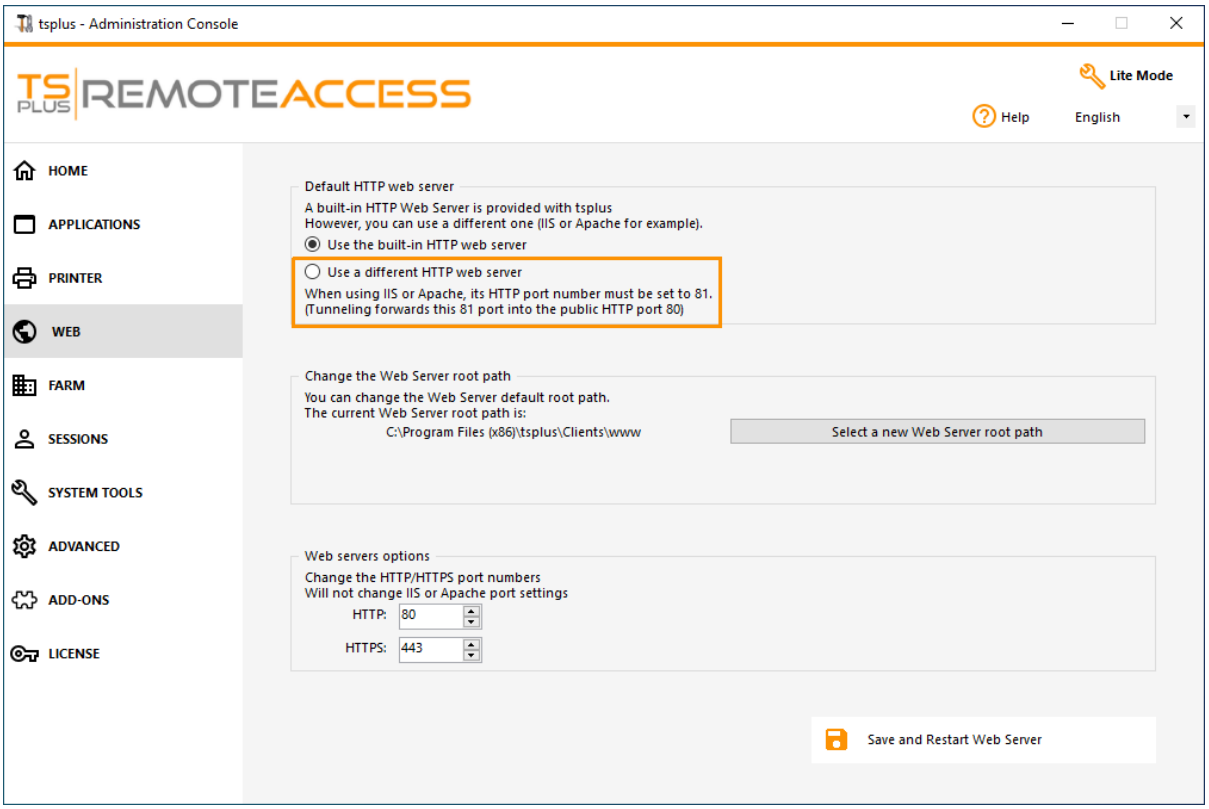
IIS를 재시작하십시오.

5. IIS 디렉터리 권한 구성

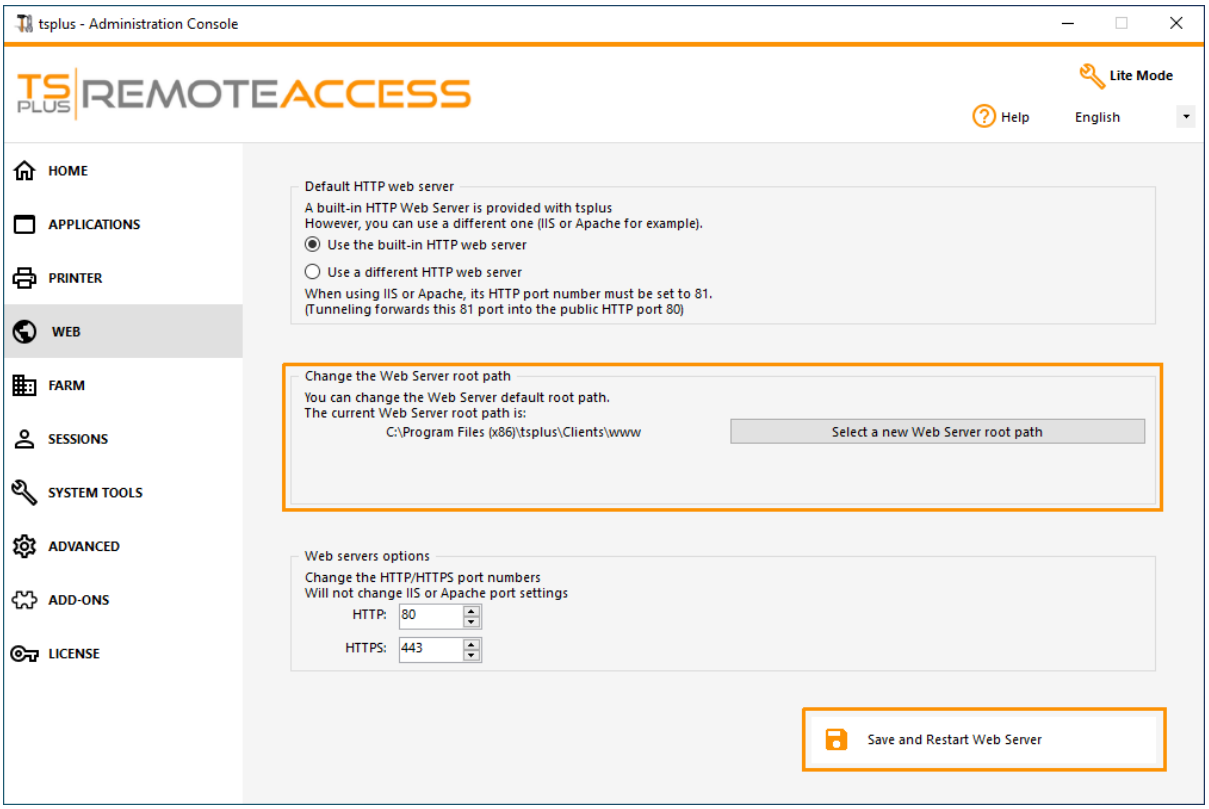
“C:\inetpub\wwwroot” 디렉토리에서 그룹 “Everyone”에 전체 권한 부여

6. TSplus 구성

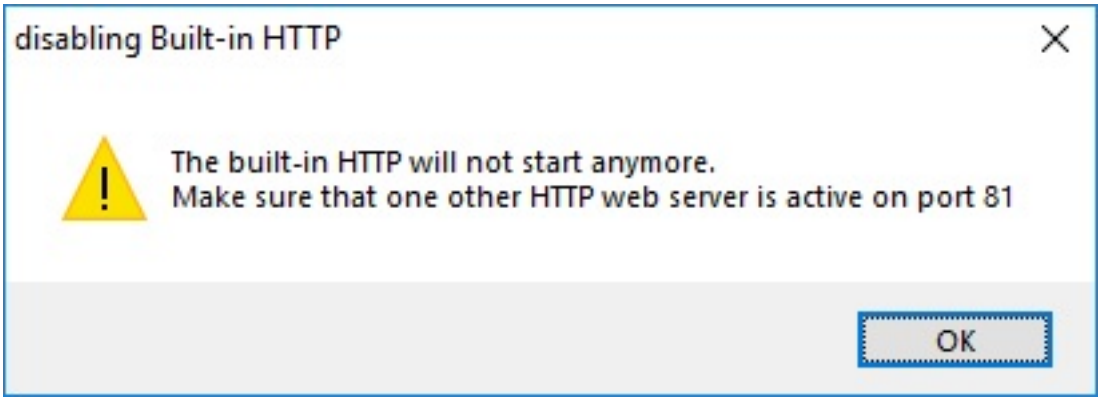
관리 도구의 웹 서버 탭으로 이동한 다음 "다른 HTTP 서버 사용" 옵션을 선택하십시오.

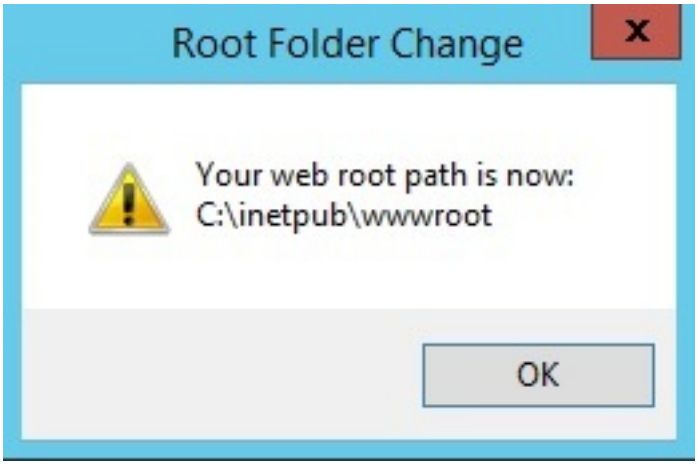


그런 다음 같은 창에서 "새 웹 서버 루트 경로 선택"을 클릭하고 IIS 디렉터리의 경로를 입력합니다. 경로는 "C: \ inetpub \ wwwroot"와 비슷해야 합니다. 이제 "AdminTool 저장 및 재시작"을 클릭합니다.



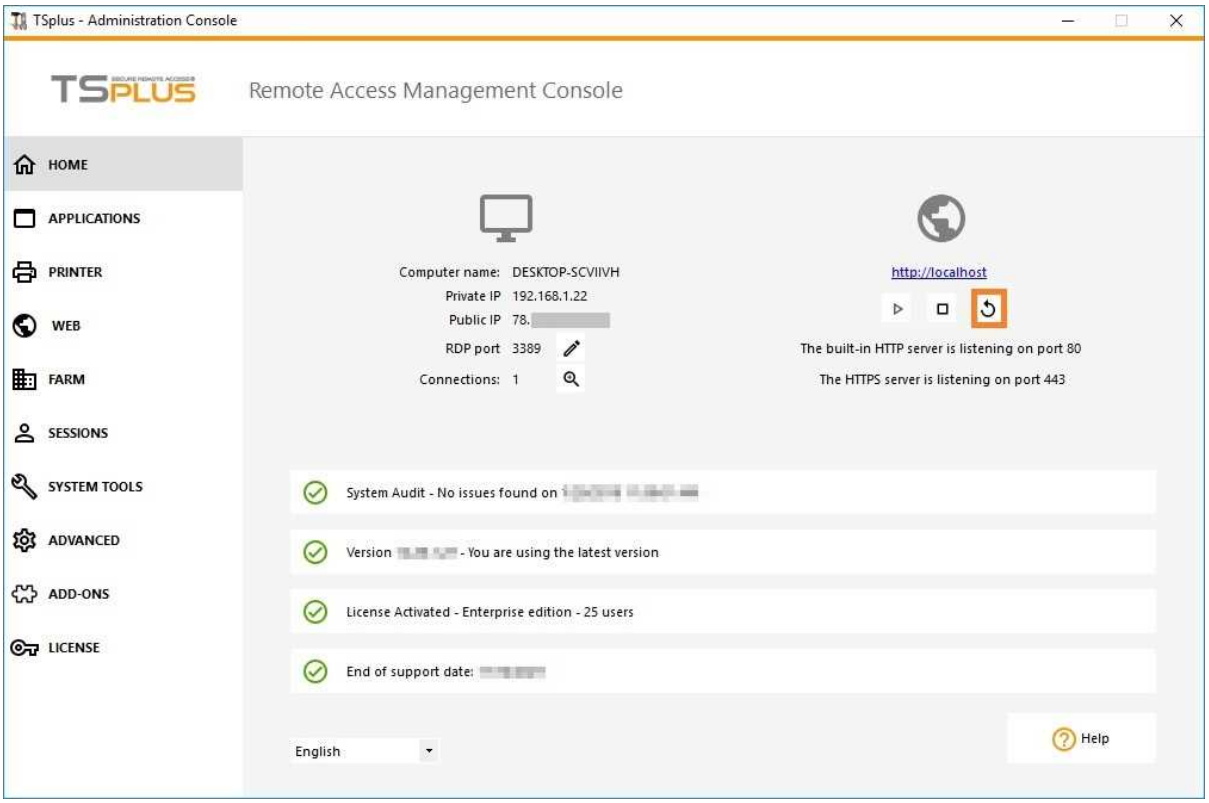
다음 메시지가 표시됩니다:





잠시만 기다려 주십시오. Admintool이 자동으로 닫힐 것입니다. 그런 다음 Admintool을 다시 열고 웹 타일을 클릭하십시오.

마지막으로, 웹 서버를 재시작하십시오:



7. 로컬 호스트로 테스트

경고 다른 사용자 계정을 사용하세요.

현재 사용자 계정으로 자신의 RDP 세션에서 서버에 접속을 시도하면 연결이 끊기고 다시 연결할 수 없습니다.



추가 작업:

원격 앱 구성

IIS 웹 루트(c:\inetpub\www\cgi-bin\remoteapp)의 "remoteapp" 폴더는 IUSR 사용자에게 전체 권한이 있어야 하며, 그렇지 않으면 RemoteApp을 사용하려고 할 때 704 오류가 발생합니다.

2FA 구성

2FA가 한 번도 활성화되지 않은 새 설치에서는 [이름이 지정된 폴더가 없습니다] C:\Program Files (x86)\TSplus\Clients\webserver\twofa, 또는 twofactorauth.ini 파일.

필요합니다:

- AdminTool에서 2FA를 활성화하여 이 폴더와 이 .ini 파일을 생성합니다.
- 그런 다음 2FA를 비활성화하십시오.
- 그런 다음 새로 생성된 twofa 폴더에 IUSR 사용자 권한을 적용합니다.

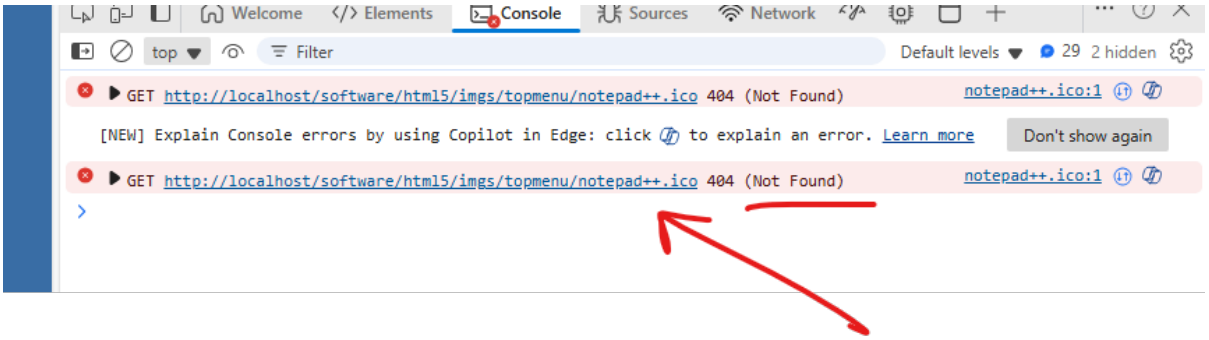
이 단계를 완료하지 않으면 (2FA를 사용할 의도가 없더라도) 사용자가 자격 증명이 유효하지 않다는 오류 메시지와 함께 로그인할 수 없습니다.

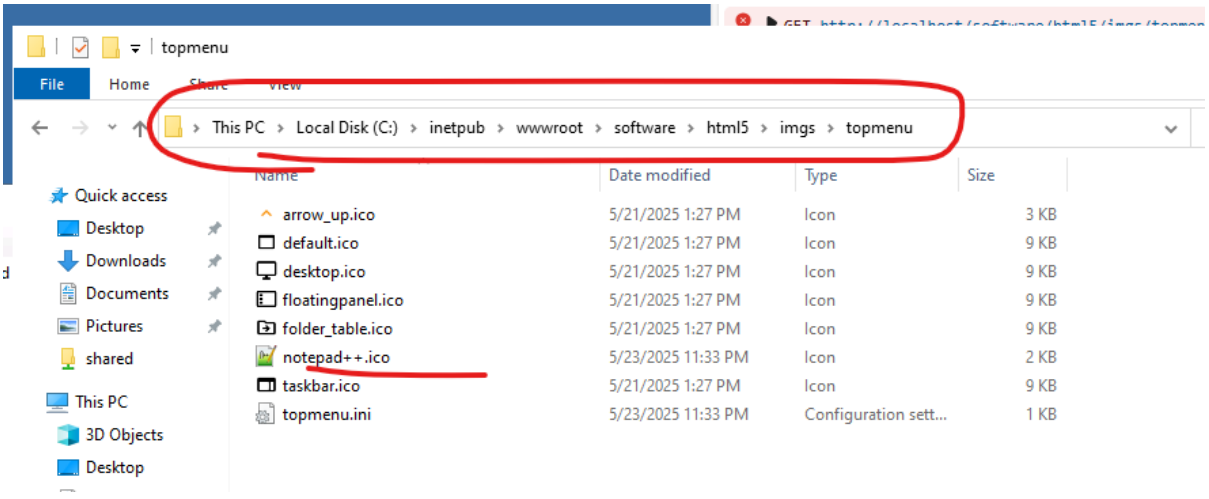
8. 이중 이스케이프 허용

다운로드를 허용하려면 IIS의 요청 필터링에서 "이중 이스케이프 허용"을 활성화해야 합니다. 이 변경 사항은 IIS가 파일 이름의 "+"와 같은 특수 문자를 올바르게 처리할 수 있도록 합니다. IIS에서 "이중 이스케이프 허용"을 활성화하는 방법은 다음과 같습니다:

1. IIS 관리자를 엽니다: 인터넷 정보 서비스(IIS) 관리자를 시작합니다.

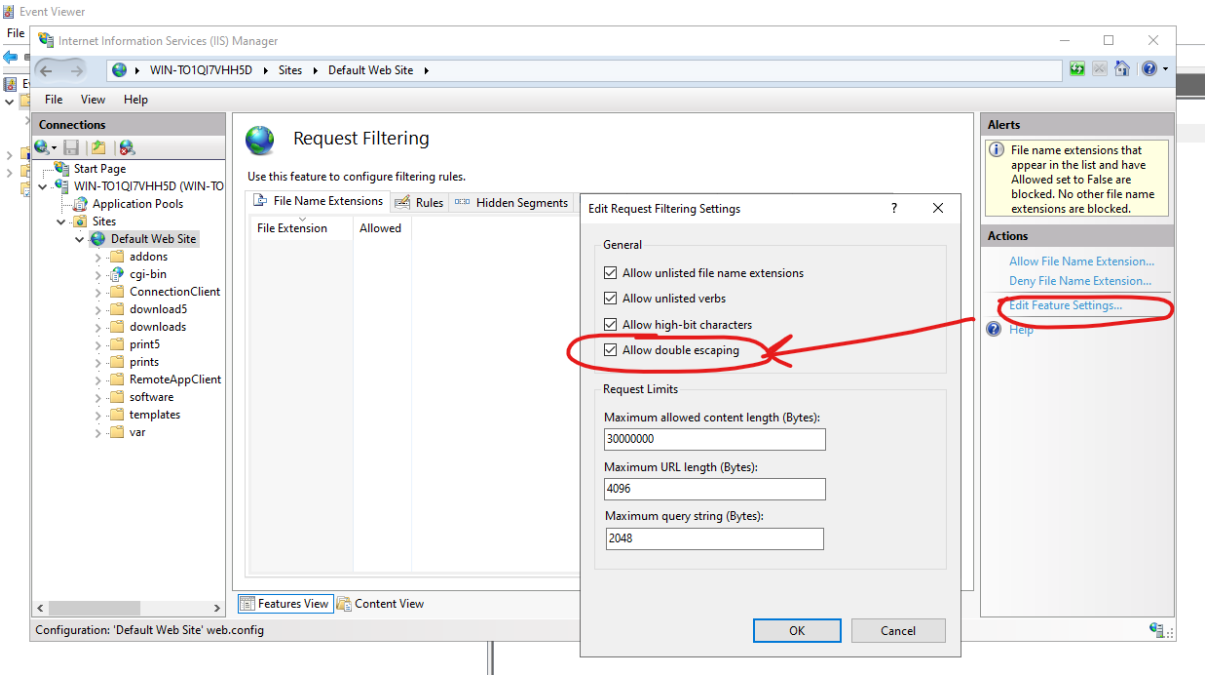
2. 요청 필터링으로 이동: IIS 관리자에서 "+" 문자가 포함된 파일이 있는 폴더나 웹사이트를 선택합니다. 그런 다음 기능 보기에서 "요청 필터링"을 두 번 클릭합니다.





3. 기능 설정 편집: 작업 창에서 "기능 설정 편집"을 클릭합니다.

4. 이중 이스케이프 허용 활성화: 요청 필터링 설정 편집 대화 상자에서 "이중 이스케이프 허용" 옵션을 선택합니다.



5. IIS 재시작(선택 사항): IIS를 재시작하면 변경 사항이 적용되는 데 도움이 될 수 있습니다.

리버스 프록시 뒤에 있는 서버 사용

서버를 역방향 프록시 뒤에서 xhr-polling을 통해 사용할 수 있지만, 몇 가지 제한 사항이 있습니다.

설명한 대로 웹소켓은 HTTP 프로토콜의 일부가 아닙니다. 첫 번째 HTTP 요청이 HTTP 요청처럼 보이더라도 실제로는 그렇지 않습니다. 따라서 대부분의 알려진 리버스 프록시는 웹소켓을 지원하지 않으며 첫 번째 웹소켓 요청의 많은 중요한 영역을 드롭합니다.

서버가 리버스 프록시 뒤에 있다는 것을 알고 있다면, Clients\www\software\html5\settings.js에서 이 옵션을 설정하여 Websockets를 비활성화하십시오.

disablewebsocket = true;

사용을 강제할 것입니다 XHR-폴링 연결할 때 시간 지연을 피하십시오.

“C:\Program Files (x86)\TSplus\Clients\www\software\html5” 폴더에 “settings.js”라는 파일이 없다면, 귀하의 TSplus 버전이 오래된 것이며 이 문서는 적용되지 않습니다. 먼저 시스템을 업데이트하거나 지원팀에 문의하시기 바랍니다.

XHR 폴링의 사용은 연결 특성으로 인해 웹소켓만큼 안정적이지 않다는 점에 유의하시기 바랍니다.

Xhr 폴링을 역방향 프록시를 통해 사용할 때의 또 다른 제한 사항은 파일 업로드에 대한 지원이 부족하다는 것입니다. Apache 역방향 프록시를 통해 직접 연결에서 XHR로 작업할 때, Apache가 파일 업로드를 우연히 중단할 수 있습니다.

TSplus Virtual Printer v2

새로운 버전의 Virtual Printer가 이제 사용 가능합니다!
이 버전은 Virtual Printer 구성 요소(v1.x -> v2.x)에 대한 중요한 업데이트를 포함합니다.

이유: Virtual Printer v2는 Fabulatech의 최신 플래그십으로, 많은 개선 사항을 가져오고 고객이 보고한 문제를 수정합니다.

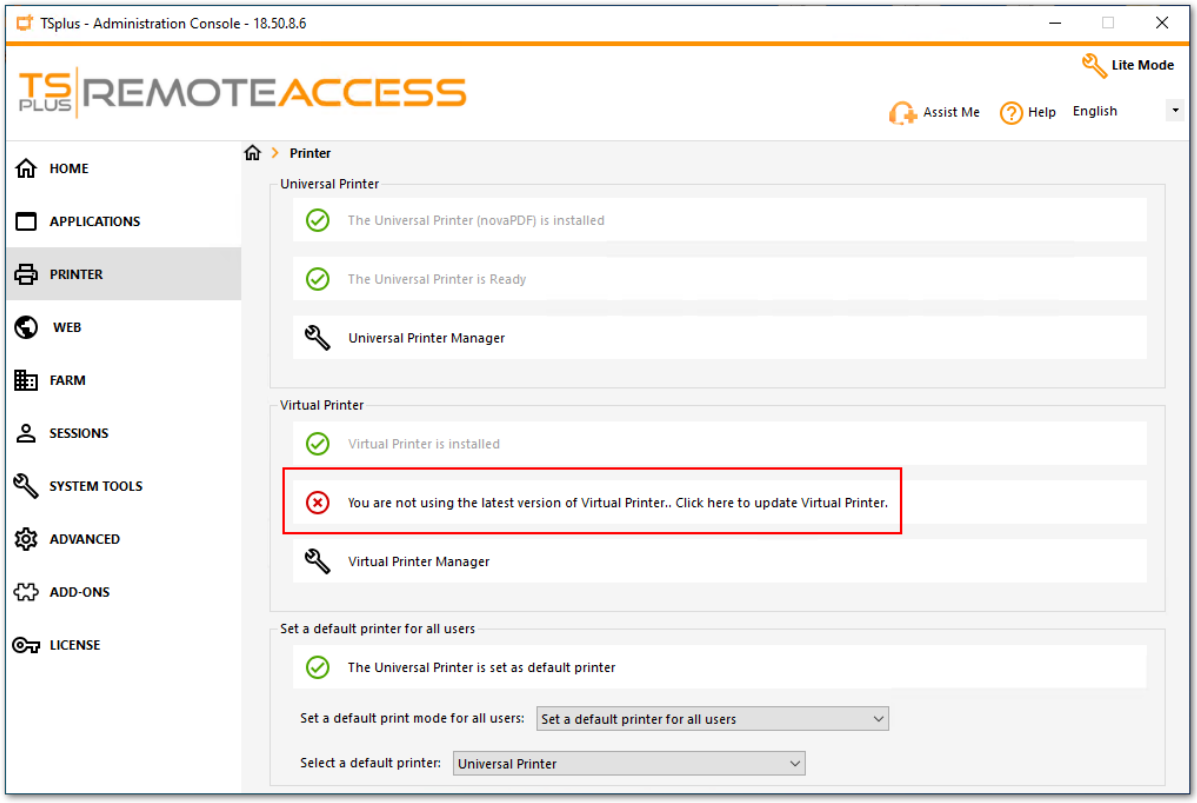
주의: Virtual Printer v1.x와 v2.x는 호환되지 않으며, 클라이언트와 서버 양쪽에서 동일한 주요 버전이 필요합니다.

당황하지 마세요: 업데이트 릴리스는 새로운 가상 프린터 설정 프로그램(클라이언트 및 서버)만 제공합니다.
그들은 위치해 있습니다 C:\Program Files (x86)\TSplus\UserDesktop\files\addons .
관리 도구에서 실제 가상 프린터 업데이트를 수동으로 트리거하는 것은 귀하에게 달려 있습니다.

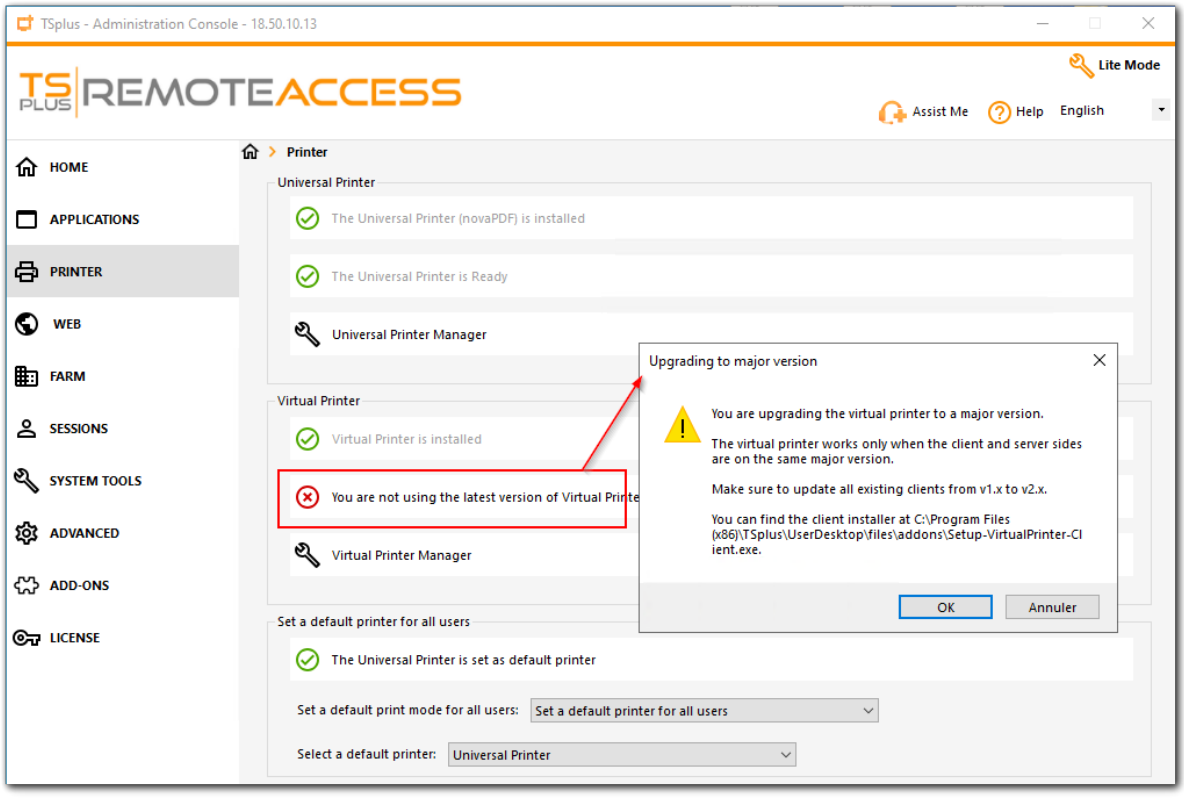
링크 : TSplus 설정 전체 TSplus 업데이트 릴리스 리브랜딩 업데이트 릴리스

업데이트 방법은?

업데이트 릴리스를 설치한 후, AdminTools는 새로운 가상 프린터 버전이 사용 가능하다는 것을 감지합니다.
“공지 업데이트” 버튼을 클릭할 때까지 현재 설치된 가상 프린터 버전은 변경되지 않으며, 모든 것이 이전과 같이 계속 작동합니다.

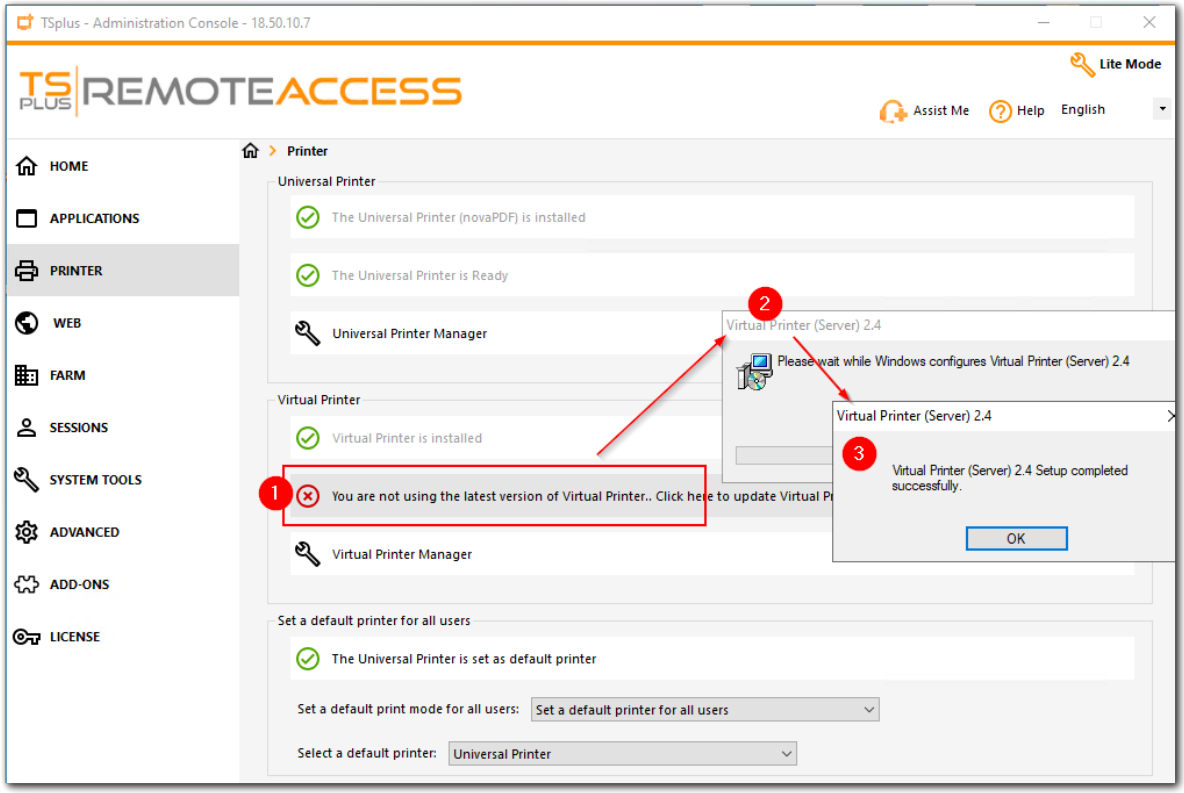


좋습니다, 하지만 우리는 새로운 VP 버전을 설치하기 위해 여기 있으므로 "공지 업데이트" 버튼을 클릭합시다.

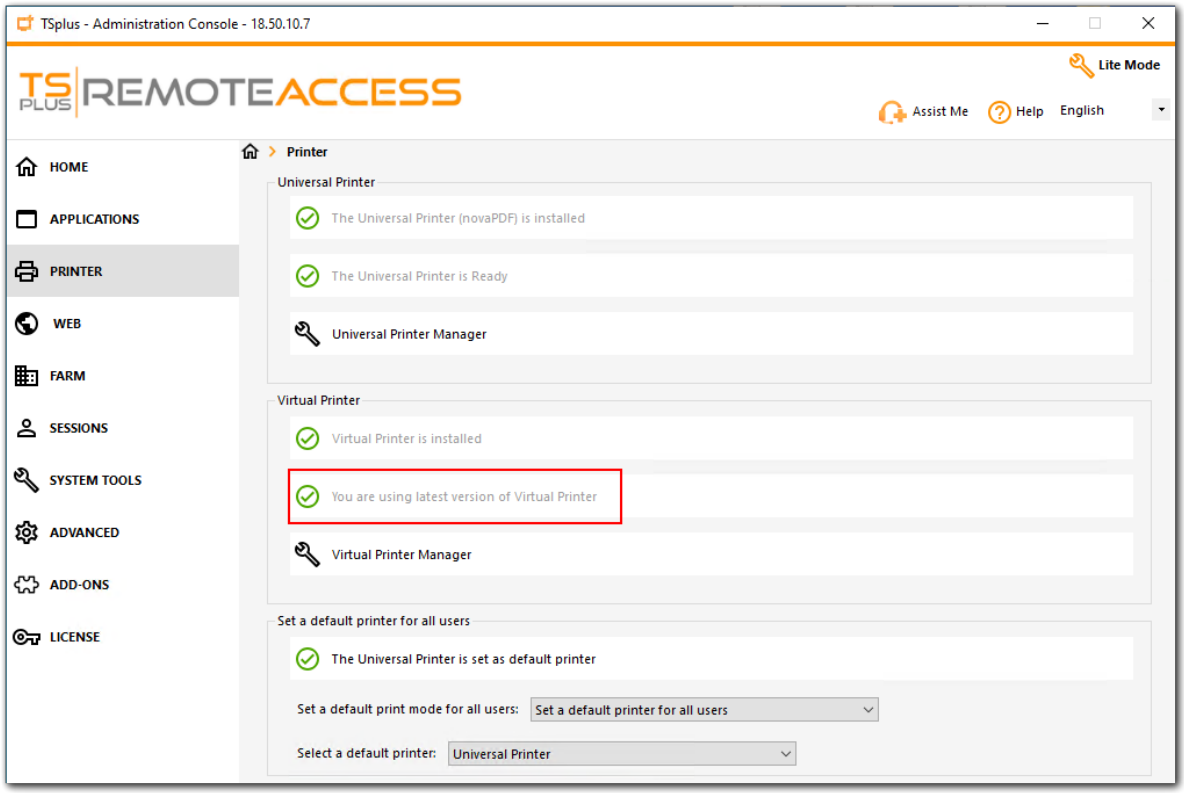


가상 프린터를 다음 주요 버전으로 업데이트하려고 정말로 하시겠습니까? 확인 대화 상자가 나타

납니다. “확인”을 클릭하세요.



설치가 완료되면 AdminTools가 최신 상태임을 감지합니다.



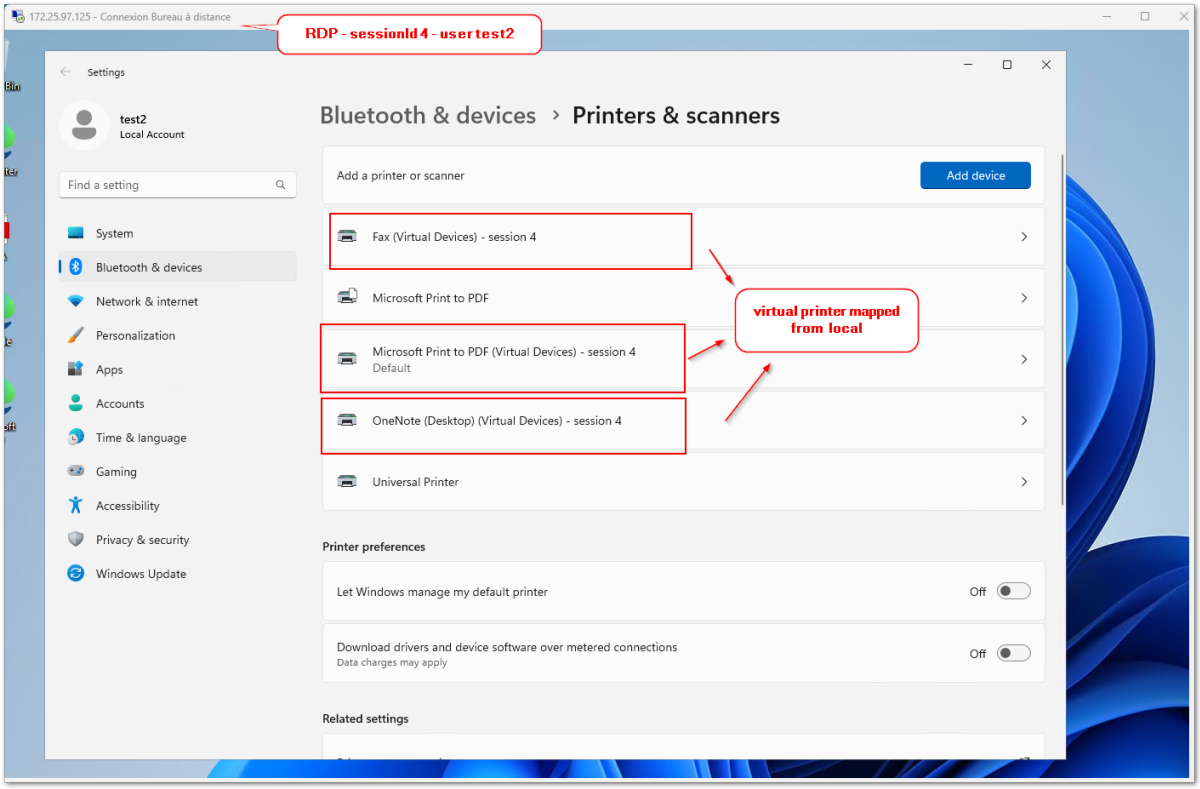
주의: 이 단계에서는 동일한 주요 버전(v2.x)을 실행하는 클라이언트만 이 서버에서 가상 프린터를 통해 인쇄할 수 있습니다. 서버와 클라이언트의 업데이트를 조정해야 합니다. 클라이언트 설치 프로그램은 “C:\Program Files (x86)\TSplus\UserDesktop\files\addons\Setup-VirtualPrinter-Client.exe”에 있습니다.

중대한 변경!

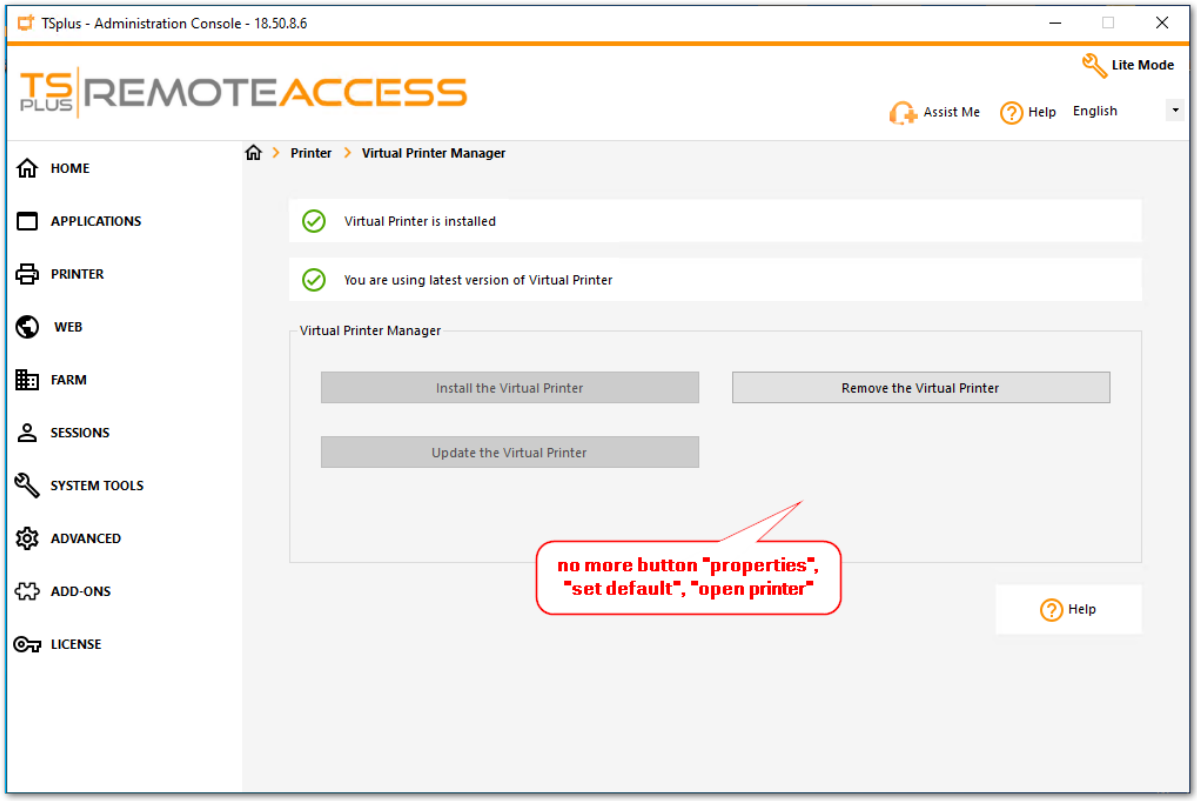
프린터 목록에 더 이상 단일 "Virtual Printer" 장치가 없습니다. 대신, 각 로컬 프린터는 이제 RDP 세션의 해당 가상 프린터에 매핑됩니다.

아래 스크린샷에서 사용자 “test2”가 RDP 세션 #4에 연결되어 있습니다. 프린터 패널을 열 때, 그는 로컬 프린터를 보고 사용할 수 있습니다. 각 프린터 이름은 다음 형식을 따릅니다: “$printerName (가상 장치) - 세션 $sessionId” .

사용자가 이제 각자의 로컬 프린터를 개별적으로 볼 수 있다는 것은 주요 UX 개선 사항이며, 그래서 Fabulatech는 이 새로운 버전을 추진하고 있습니다.

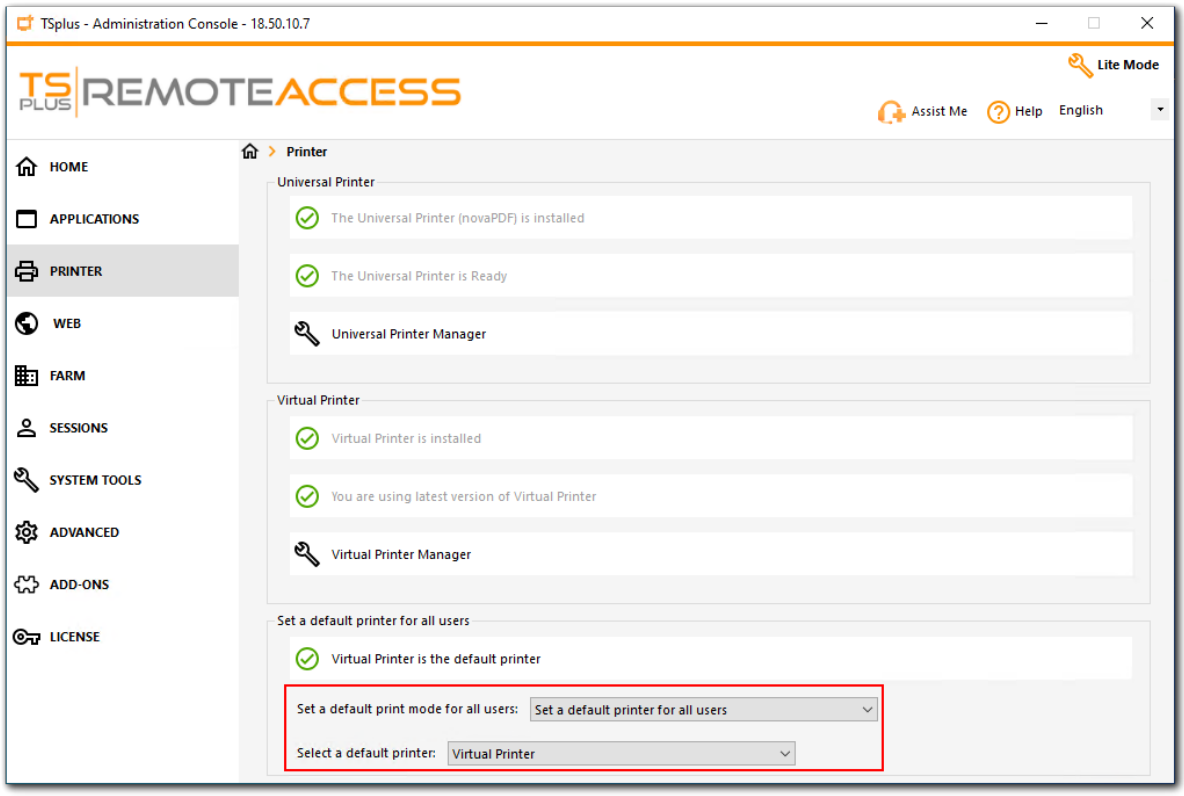


이로 인해 우리는 AdminTools UI의 일부를 조정했습니다. 예를 들어, Virtual Printer Manager에서 일부 버튼이 제거되었습니다.

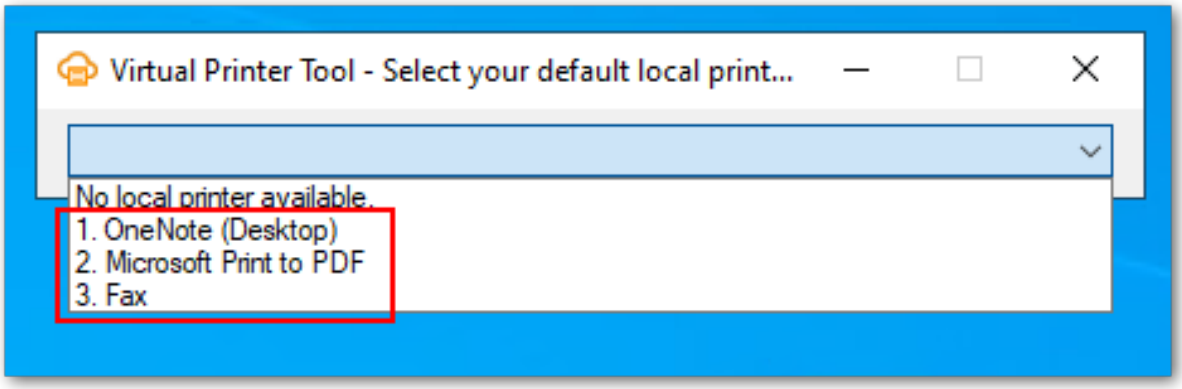


구성하는 방법?

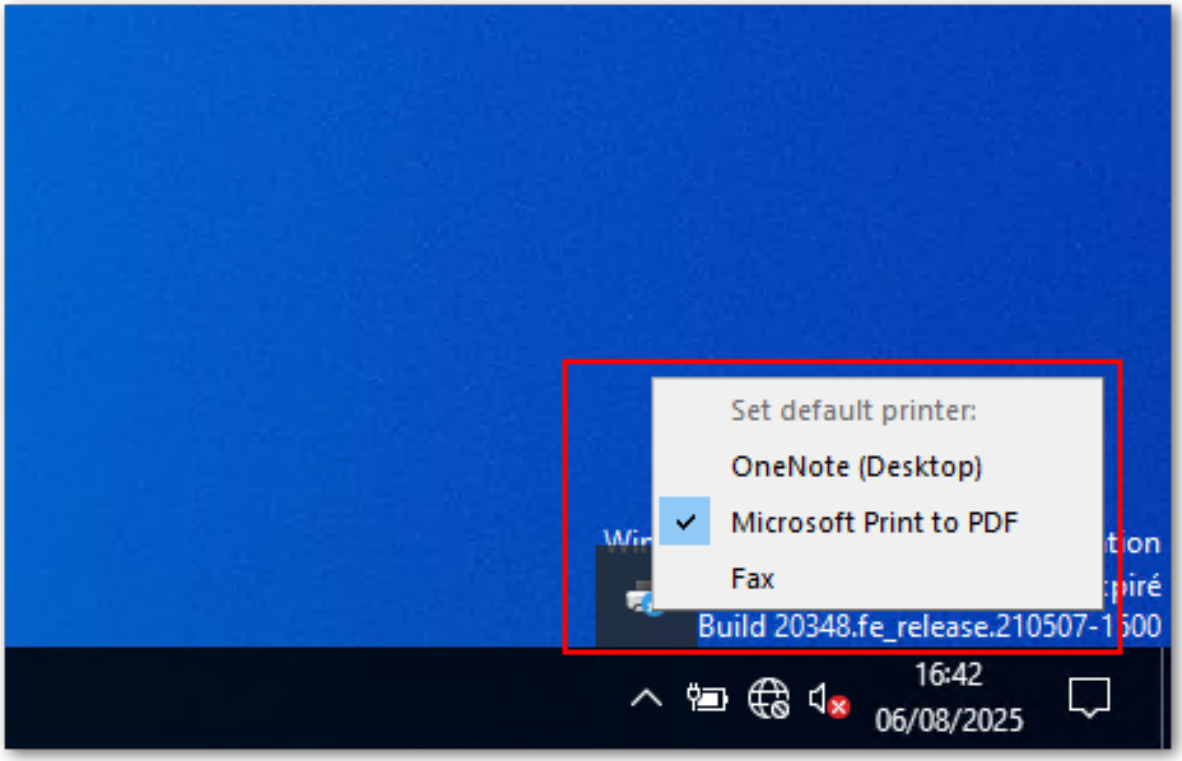
구성은 여전히 AdminTools에서 동일하게 유지되며 이전과 같이 작동해야 합니다.



가상 프린터 도구를 사용하면 아무것도 변경되지 않으며 이전과 같이 작동합니다.



툴바에서 선택기를 사용하면 아무것도 변경되지 않으며 이전과 같이 작동합니다.



가상 프린터 매핑 장치의 이름을 어떻게 사용자 정의하나요?

서버에서 첨부된 “customize-virtual-printer-name.reg”를 실행하십시오. 다운로드

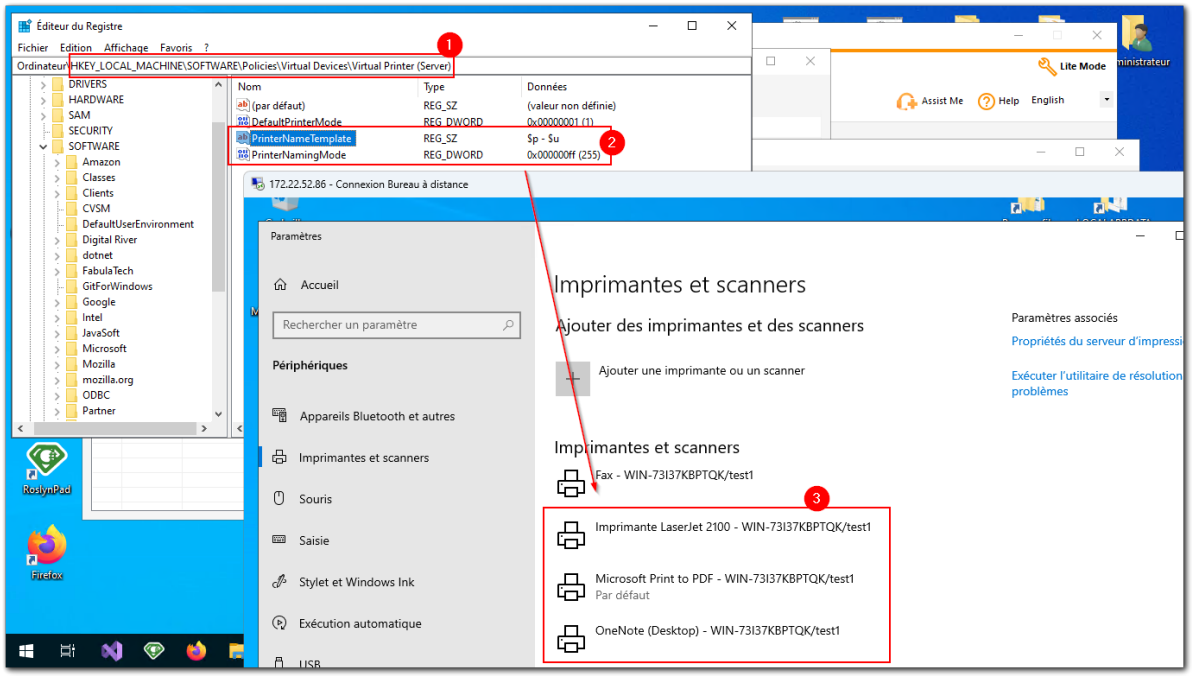
레지스트리에 2개의 키가 추가됩니다. HKEY_LOCAL_MACHINE\SOFTWARE\정책\가상 장치\가상 프린터(서버)

프린터 이름 템플릿은 템플릿 문자열이며, 사용 가능한 변수는 3개입니다:

- $p - 프린터 이름
- $u - 전체 사용자 이름 (도메인/사용자 또는 컴퓨터 이름/사용자)
- $s - 세션 번호

주어진 일부 Fabuletch 제약 조건: **$p와 $u 또는 $p와 $s를 지정하는 것은 필수입니다.**
프린터 이름은 서로 다른 사용자에 대해 서버에서 고유해야 하므로 필요합니다.

예: PrinterNameTemplate = “$p $u”, 아래 RDP 세션 스크린샷에서 결과를 확인할 수 있습니다.



고급 구성

가상 프린터 v2에 대한 고급 구성은 컴퓨터 구성 > 관리 템플릿 > 가상 장치 > 가상 프린터(서버) 아래의 그룹 또는 로컬 정책 개체를 통해 서버 측에서 관리할 수 있습니다.

다음 설정은 Remote Access 통합에 관련이 있습니다:

- 기본 프린터 선택 모드: 사용자가 원격 세션에 로그인할 때마다 기본 프린터가 어떻게 할당되는지를 정의합니다.
- 프린터 이름 템플릿: 사용자 세션에서 가상 프린터의 명명 형식을 지정합니다.
- 대형 인쇄를 위한 품질 제한: 지정된 크기를 초과하는 페이지의 인쇄 품질을 낮춰 대형 형식 인쇄 속도를 높이면서 작은 페이지의 최대 품질을 유지합니다.

전체 구성 세부정보는 Virtual Printer GPO 문서를 참조하십시오. https://www.fabulatech.com/printer-for-remote-desktop-server-help/gpo.html

TSplus Virtual Printer

TSplus 가상 프린터는 신뢰할 수 없고 하드웨어에 의존하며 관리하기 어려운 고전적인 원격 데스크톱 인쇄 솔루션에 대한 새로운 대안입니다. 가상 프린터의 독특한 압축 알고리즘은 이미지 품질을 유지하면서 데이터 전송을 최소화하여 원격 인쇄 작업의 전송 속도를 향상시킵니다.

노트 TSplus HTML5 클라이언트는 지원되지 않으며 필요합니다. TSplus 유니버설 프린터 .

이점

- 단일 사용자 및 다중 사용자 환경 지원.
- 제로 구성은 필요하지 않습니다.
- 모든 가상 머신과 호환됩니다.
- 혼합 32비트 및 64비트 환경.

사전 요구 사항

TSplus 가상 프린터 OS 호환성 목록:

- 윈도우 **7**
- 윈도우 **8/8.1**
- 윈도우 **10**
- 윈도우 **11**
- 윈도우 **서버 2008 R2**
- 윈도우 **서버 2012 R2**
- 윈도우 **서버 2016**
- 윈도우 **서버 2019**
- 윈도우 **서버 2022**
- 윈도우 **서버 2025**

TSplus Virtual Printer는 다음과 호환됩니다:

- TSplus에서 생성된 클라이언트
- TSplus RemoteApp 클라이언트
- TSplus RemoteApp 플러그인 웹 포털 사용 시
- 마이크로소프트 원격 데스크톱 클라이언트

호환되지 않습니다:

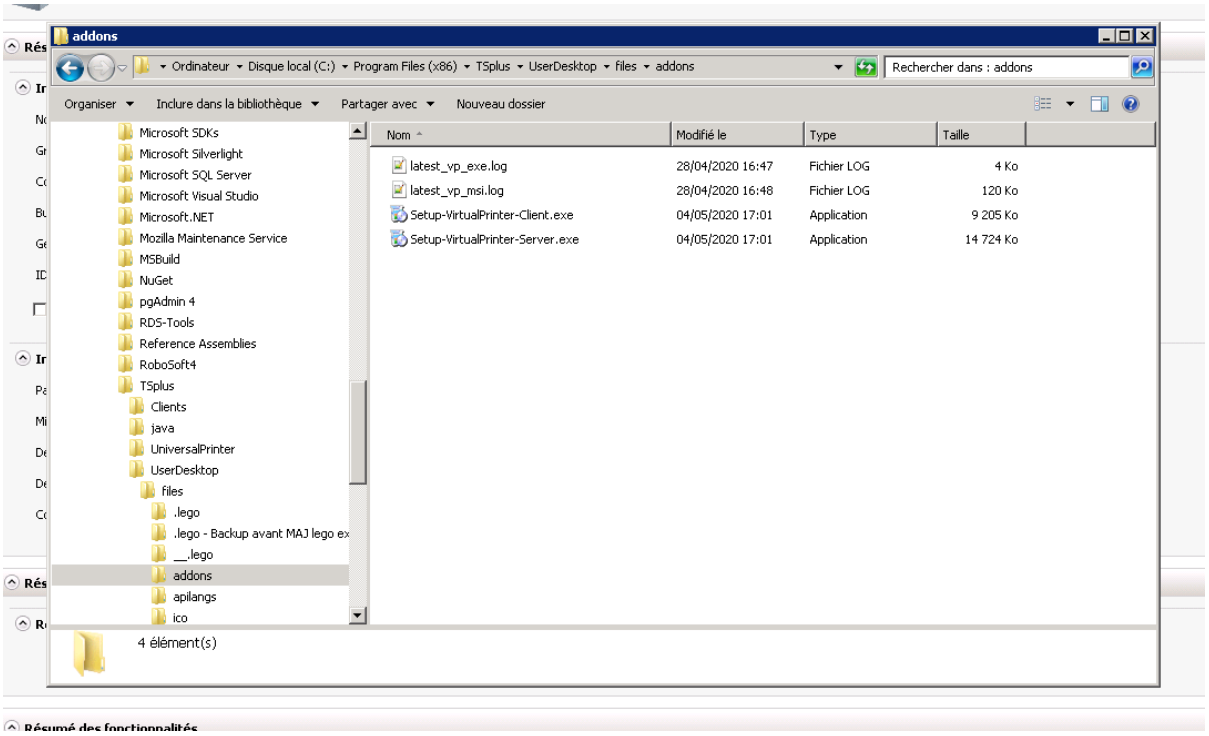
- TSplus HTML5 클라이언트
- 하드 코딩된 얇은 클라이언트 장치로 클라이언트 측 설정을 설치할 수 없습니다.

두 부분

TSplus Virtual Printer는 두 가지 구성 요소로 이루어져 있습니다:

- TSplus Remote Access에 설치되는 서버 측 구성 요소입니다.
- 최종 사용자의 Windows 워크스테이션에 설치되는 데스크톱 구성 요소입니다.

두 설정은 “C:\Program Files (x86)\TSplus\UserDesktop\files\addons” 폴더의 서버 측에서 직접 사용할 수 있으며, “Setup-VirtualPrinter-Server.exe” 및 “Setup-VirtualPrinter-Client.exe”라는 이름으로 되어 있습니다.



클라이언트 설정은 아래 링크를 사용하여 TSplus 웹 서버에서도 사용할 수 있습니다.

“yourtsplusserveriporpublicdomain”/addons/Setup-VirtualPrinter-Client.exe

클라이언트를 명령줄을 통해 조용히 설치할 수도 있으며, 다음 매개변수를 사용하여 설치 프로그램을 실행하면 됩니다.

/SUPPRESSMSGBOXES /VERYSILENT /SILENT /no_ui

시작하기

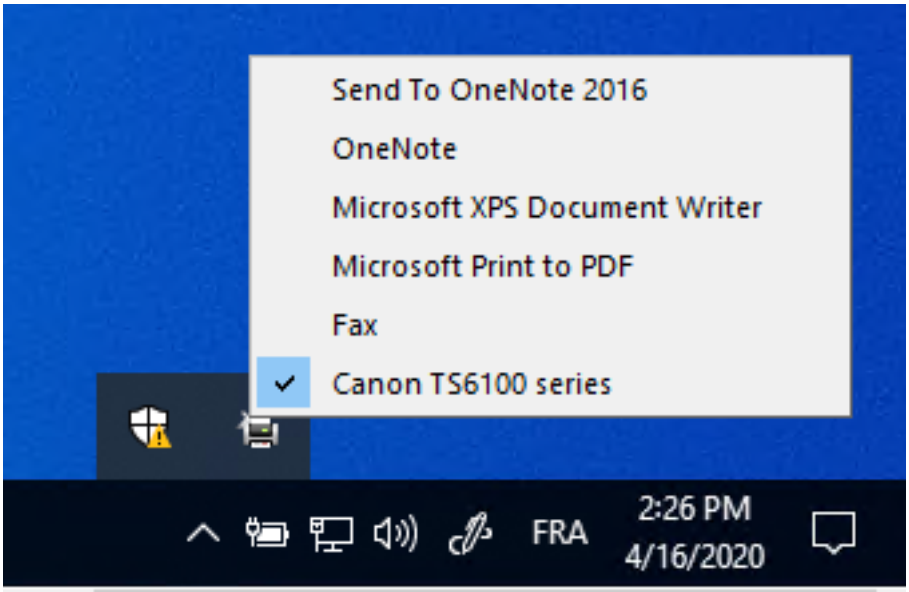
TSplus 가상 프린터는 첫 번째 TSplus 설치 중에 자동으로 설치되며, 평가 기간 동안 직접 사용할 수 있습니다.

TSplus가 설치되면 사용자의 컴퓨터에 "Virtual Printer Client"를 설치해야 합니다.

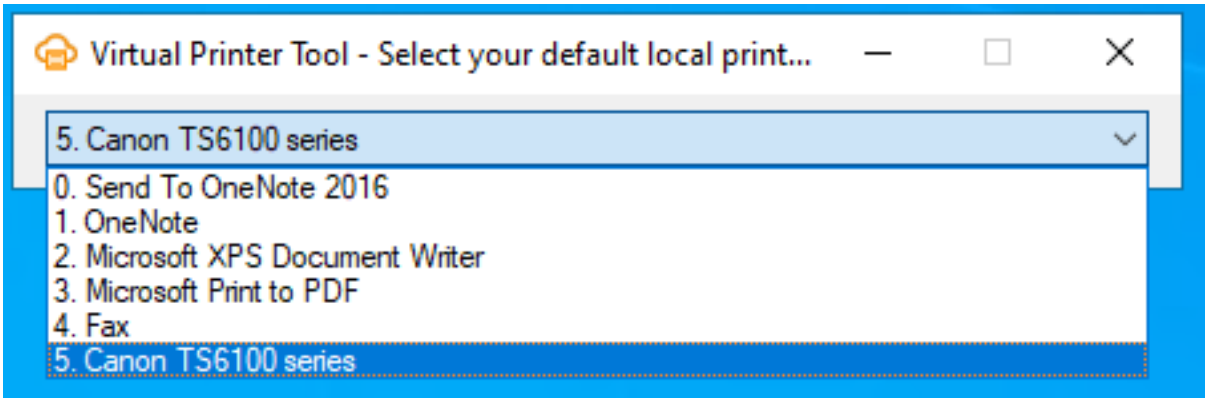
원격으로 TSPlus 서버에 연결할 때 사용하는 방법 중 하나는 **Microsoft RDP 클라이언트** (mstsc), **TSplus에서 생성된 클라이언트** 또는 **웹 포털 RemoteApp 플러그인** 원격 세션에서 "Virtual Printer" 프린터를 사용하여 로컬 프린터로 인쇄할 수 있습니다. 기본적으로 선택된 로컬 프린터는 로컬 기본 프린터입니다.

상황에 따라 "Virtual Printer" 프린터에 매핑된 로컬 프린터를 변경하는 방법은 2가지가 있습니다:

1. 전체 데스크톱을 사용하고 있다면, 시스템 트레이의 가상 프린터 아이콘을 사용하여 사용할 로컬 프린터를 선택할 수 있습니다.



2. 전체 데스크톱에 접근할 수 없는 경우, "C:\Program Files (x86)\TSplus\UserDesktop\files"에 위치한 "VirtualPrinterTool.exe"라는 이름의 "가상 프린터 도구"를 사용해야 합니다. 참고: 애플리케이션을 사용자에게 할당하거나 가상 프린터 고급 설정을 통해 로그온 시 자동으로 실행되도록 설정할 수 있습니다.

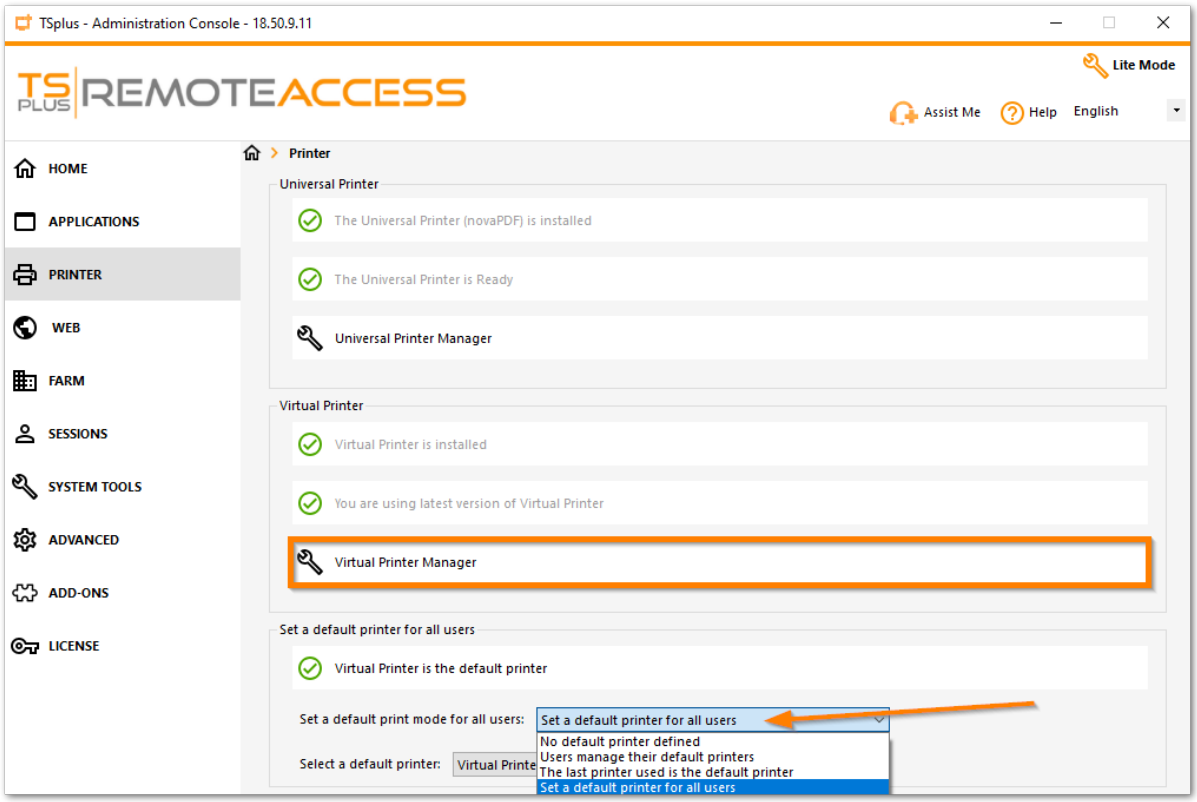


구성

TSplus Virtual Printer 제어판에 접근하려면 AdminTool을 통해 다음 경로로 이동하십시오: 프린터 > 가상 프린터 관리자

모든 사용자에 대한 기본 프린터 설정

- 기본 프린터가 정의되지 않았습니다: 사용자의 기본 프린터 구성에는 영향을 미치지 않습니다.
- 사용자가 기본 프린터를 관리합니다: "Windows가 내 기본 프린터를 관리하게 허용" 옵션이 비활성화되어 있으므로 사용자가 기본 프린터를 선택해야 합니다.
- 마지막으로 사용된 프린터는 기본 프린터입니다: "Windows가 내 기본 프린터를 관리하게 허용" 옵션이 활성화되어 있습니다.
- 모든 사용자를 위한 기본 프린터 설정: 관리자가 사용자의 기본 프린터를 강제합니다.



가상 프린터 문제 해결

가상 프린터가 작동하지 않는 경우 가장 일반적인 원인은 클라이언트 측 소프트웨어인 "Print Application"이 사용자의 로컬 컴퓨터의 작업 관리자에서 실행되고 있지 않거나, 가상 프린터(서버) 소프트웨어가 사용자의 로컬 컴퓨터에 설치되었고 가상 프린터(워크스테이션) 버전(Setup-VirtualPrinter-Client.exe)이 아닌 경우입니다. 아래는 클라이언트와 서버 측 모두에 대한 문제 해결 단계입니다.

가상 프린터는 HTML5 클라이언트와 호환되지 않음을 유의하시기 바랍니다. HTML5 클라이언트를 사용 중인 경우 대신 유니버설 프린터를 사용해 주십시오.

문제 해결 가이드

서버에서 설정 후 볼륨 라이센스를 활성화하는 방법은 무엇인가요?

제품을 명령줄 없이 설치한 경우, 시험 버전으로 설치됩니다.

활성화

볼륨 라이센스를 활성화하려면, 다음 명령줄을 관리자 권한으로 실행하십시오:

- **원격 액세스 및 이중 인증**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /사용자 1 (1에서 50 또는 무제한)
  /에디션 엔터프라이즈 (데스크탑, 모바일웹, 엔터프라이즈)
  /지원연도 1 (1,2,3만)

예시 : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 30 /edition Enterprise /supportyears 1

예시 : C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /supportyears 1

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  TSplus-Security.exe
  /에디션 궁극적 (필수 또는 궁극적)
  /지원연도 1 (1,2,3만)

예시 : C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /edition Ultimate /supportyears 1

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>
  ServerMonitoring.exe
  /사용자 1 (스타트업 1, 필수 5, 비즈니스 10)
  /지원연도 1 (스타트업 1, 필수 5, 비즈니스 10)

예시 : C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 5 /supportyears 1

- **다음 추가 매개변수를 추가할 수 있습니다:**
  — 당신의 의견 라이선스 포털에 라이선스에 첨부할 댓글을 지정하십시오.
  — /매우조용히 설치 프로그램을 조용히 실행합니다. 이렇게 하면 이 설치 프로그램을 자신의 초기화 또는 자동화 스크립트에 통합할 수 있습니다.

예시 : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users unlimited /edition Enterprise /supportyears 3 /comments "This is a comment"*

매개변수

이 명령은 다음 매개변수를 사용합니다:

명령줄을 사용하는 것을 좋아하고 다른 명령줄이 무엇인지 궁금하다면, 이곳으로 가십시오. 특정 문서)

업데이트 지원

업데이트/지원 구독을 연장하려면 연장 시간의 운영에서 1, 2 또는 3을 선택하십시오.
이 명령어를 사용하세요:

AdminTool.exe /vl /renewsupport YOUR-VOLUME-LICENSE-KEY /supportyears 1"

지원 추가하기

이 명령은 고객이 설치 중 지원을 활성화하는 것을 잊었거나 지원 기간의 특정 종료 날짜를 설정해야 할 경우 특히 유용합니다.

이 명령을 관리자 권한으로 실행하고, 세부 정보를 자신의 라이센스 정보와 선호하는 지원 종료 날짜로 교체하십시오.

AdminTool.exe /vl /activate-support YOUR-VOLUME-LICENSE-KEY /users [number] /edition [edition] /endofsupport [YYYY-MM-DD]

지원 활성화를 위해 2026년 7월 25일까지 프린터 에디션을 사용하는 Remote Access 5 사용자에 대해 입력하십시오:

AdminTool.exe /vl /activate-support YOUR-VOLUME-LICENSE-KEY /users 5 /edition Printer /endofsupport 2026-07-25

이 새로운 기능은 지원 기간을 관리하는 데 더 쉽게 만들어 주므로 고객은 항상 지원 기간이 시작

되고 끝나는 시점을 알 수 있습니다.

볼륨 라이센스 키의 남은 라이센스 크레딧을 어떻게 표시하나요?

볼륨 라이센스 키에 대한 남은 라이센스 크레딧을 표시하려면, 다음 명령줄을 관리자 권한으로 실행하십시오.

AdminTool.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE [/edition Essentials] [/silent]

매개변수

이 명령은 네 개의 매개변수를 받을 수 있습니다:

- 볼륨 라이센스 키를 사용하세요.
- /로그인 JOHNDOE : 볼륨 라이센스 키와 연결된 파트너의 로그인을 제공하십시오.
- /에디션 필수: 고급 보안 및 서버 모니터링 제품에 대한 선택적 에디션 매개변수를 제공합니다.
- /silent : 명령을 조용히 실행합니다

출력은 사용자 수준 환경 변수에 저장됩니다. 볼륨 라이선스 크레딧 값을 읽어야 할 수 있습니다. 볼륨 라이선스 크레딧 다른 프로세스에서 명령을 사용하여: 에코 %VOLUME_LICENSE_CREDITS%

아래에서 고급 보안 및 서버 모니터링 제품에 대한 예상 에디션을 확인하십시오:

- 고급 보안: “필수”, “궁극적”
- 서버 모니터링: “필수”, “스타트업”, “비즈니스”

다음 실행 파일을 사용하여 남은 크레딧 수를 확인해야 합니다:

- 원격 액세스: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- 고급 보안: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- 서버 모니터링: C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe
- 2FA: C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe
- RPA: C:\Program Files (x86)\TSplus-RPA\AdminTool.exe
- 원격 작업: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

제목: “볼륨 라이선스 키에 대한 남은 지원 크레딧을 표시하는 방법은?”

볼륨 라이센스 키에 대한 남은 지원 크레딧을 표시하려면, 다음 명령줄을 관리자 권한으로 실행하십시오.

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE [/edition Essentials] [/silent]

매개변수

이 명령은 네 개의 매개변수를 받을 수 있습니다:

- 볼륨 라이센스 키를 사용하세요.
- /로그인 JOHNDOE : 볼륨 라이센스 키와 연결된 파트너의 로그인을 제공하십시오.
- /에디션 필수: 고급 보안 및 서버 모니터링 제품에 대한 선택적 에디션 매개변수를 제공합니다.
- /silent : 명령을 조용히 실행합니다.

출력은 사용자 수준 환경 변수에 저장됩니다. 볼륨 라이선스 크레딧 값을 읽어야 할 수 있습니다. 볼륨 라이선스 크레딧 다른 프로세스에서 명령을 사용하여: 에코 %VOLUME_LICENSE_CREDITS%

아래에서 고급 보안 및 서버 모니터링 제품에 대한 예상 에디션을 확인하십시오:

- 고급 보안: “필수”, “궁극적”
- 서버 모니터링: “필수”, “스타트업”, “비즈니스”

다음 실행 파일을 사용하여 남은 크레딧 수를 확인해야 합니다:

- 원격 액세스: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- 고급 보안: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- 서버 모니터링: C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe
- 2FA: C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe
- RPA: C:\Program Files (x86)\TSplus-RPA\AdminTool.exe
- 원격 작업: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

서버에서 라이센스를 비활성화하는 방법은 무엇인가요?

볼륨 라이센스 키로 활성화된 서버를 비활성화하려면, 다음 명령줄을 관리자 권한으로 실행하십시오.

AdminTool.exe /vl /disable VOLU-MELI-CENS-EKEY

서버에서 라이센스를 활성화하는 방법은?

서버를 활성화할 수 있도록 하려면, 처음에 볼륨 라이센스 키로 활성화되었고 나중에 비활성화된 경우, 다음 명령줄을 관리자 권한으로 실행하십시오:

AdminTool.exe /vl /enable VOLU-MELI-CENS-EKEY

라이센스 포털에서 라이센스를 비활성화하는 방법은 무엇인가요?

먼저 라이센스 포털에서 라이센스를 비활성화한 다음, 관리 애플리케이션이나 명령줄에서 상태를 업데이트하여 새로운 상태가 서버에 적용되었는지 확인해야 합니다.

먼저, 라이선스 목록과 라이선스 세부 정보 페이지에서 선택한 라이선스를 비활성화하려면 "비활성화" 버튼을 클릭할 수 있습니다.

라이센스는 "활성화됨" 상태에서 "비활성화 중..." 상태로 이동하며, 이는 현재 서버가 스스로 비활성화되기를 기다리고 있음을 의미합니다.
그런 다음, 서버는 인터넷에 접속할 수 있는 경우 다음 날 자동으로 비활성화됩니다.

관리자 권한으로 다음 명령어를 실행하여 수동으로 이 작업을 수행할 수도 있습니다:

AdminTool.exe /license /refresh

모든 설치된 소프트웨어에 대해 새로 고침 명령어를 실행할 필요는 없습니다. 새로 고침은 2020 라이센스 시스템과 호환되는 모든 제품에서 지원됩니다.

라이센스는 서버가 라이센스 포털에 접속하여 비활성 상태를 확인할 때까지 라이센스 사용에 포함됩니다.

볼륨 라이센스 서버를 한 단계에서 설치하는 방법은?

볼륨 라이센스 서버를 한 번에 설치하려면 다음이 필요합니다:

- 제품 설치 프로그램 다운로드
- 볼륨 라이센스 키를 사용하세요
- 볼륨 라이센스 키를 매개변수로 사용하여 설치 프로그램을 실행하십시오.

귀하의 볼륨 라이센스 키는 모든 새로운 서버의 모든 설치에 대해 동일합니다. 기억나지 않으면 라이센스 포털에서 귀하의 계정에 연결하십시오. 귀하의 볼륨 라이센스 키는 홈페이지(라이센스) 상단에 표시됩니다.

볼륨 라이센스를 스크립트에서 설치하고 활성화하려면, 다음 명령줄을 관리자 권한으로 실행하십시오.

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments "This is a comment"

2020 볼륨 라이센스를 이용한 스크립트 활성화는 다음 제품 및 모든 리브랜딩된 버전에서 사용할 수 있습니다:

- Remote Access
- 고급 보안 (일명 RDS-Knight)
- 서버 모니터링 (구 서버 지니어스)
- 이중 인증

매개변수

이 명령은 다음 매개변수를 사용합니다:

- **원격 액세스 및 이중 인증**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /사용자 1 (1에서 50 또는 무제한)
  /에디션 엔터프라이즈 (데스크탑, 모바일웹, 엔터프라이즈)

/지원연도 1 (1,2,3만)

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  TSplus-Security.exe
  /에디션 궁극적 (필수 또는 궁극적)
  /지원연도 1 (1,2,3만)

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>
  ServerMonitoring.exe
  /사용자 1 (스타트업 1, 필수 5, 비즈니스 10)
  /지원연도 1 (스타트업 1, 필수 5, 비즈니스 10)

스크립팅 방법

설치-PRODUCT.exe를 올바른 명령줄로 시작하려면 3가지 방법을 사용할 수 있습니다:

1. 자신의 관리 스크립트 방법을 사용하세요

2. Setup-PRODUCT.exe의 바로 가기를 만들고 속성을 편집하여 경로 끝에 명령줄을 추가합니다.

3. 간단히 "명령 프롬프트"를 열려면 Windows 키와 "R" 키를 동시에 눌러 "cmd"를 입력한 후 "Enter" 키를 눌러 확인합니다. 이 키보드 단축키 방법은 이 문서 작성 시점에 존재하는 모든 Windows 버전에서 작동합니다.

4. 프롬프트가 나타나면 현재 디렉토리를 설치 프로그램이 있는 디렉토리로 변경하십시오(보통 다운로드 폴더입니다). 예를 들어, 입력하십시오:

   cd C:\Program Files (x86)\TSplus\UserDesktop\files

마지막으로 다음 매개변수를 사용하여 설정 프로그램을 실행하는 전체 명령을 입력하고 원하는 값을 제공하십시오:

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “This is a comment”

관련 관리 프로그램을 찾으십시오.

다음 프로그램은 볼륨 라이센스 명령을 지원합니다.
프로그램 이름과 위치는 제품 및 설정 폴더에 따라 다릅니다.

원격 액세스 및 이중 인증
C:\Program Files (x86)\TSplus\UserDesktop\files>
AdminTool.exe TwoFactor.Admin.exe

Advanced Security
C:\Program Files (x86)\TSplus-Security>
TSplus-Security.exe

Server Monitoring
C:\Program Files (x86)\TSplus-ServerMonitoring>
ServerMonitoring.exe

프로그램 실행은 조용합니다. 이를 통해 라이센스 활성화 프로세스를 자체 초기화 또는 자동화 스크립트에 통합할 수 있습니다.

제목: “문제 해결: 활성화, 사용, 비활성화 및 업데이트 명령”

문제를 조사하거나 스크립트를 프로토타입할 때 성공 및 오류 메시지를 보려면 다음을 확인할 수 있습니다. **VolumeLicensing.log** 프로그램의 루트에 파일이 발견되었습니다.

제목: “인터넷 액세스를 위한 프록시 서버 구성 방법”

설치 중에 정의된 프록시 설정은 기억되며 라이센스 작업을 수행하는 데 사용됩니다. 프록시 설정이 정의되지 않은 경우, 볼륨 라이센스 프로그램은 Internet Explorer 프록시 설정을 사용합니다(실

행 중인 세션 및/또는 Windows 서비스에 구성된 경우).

프록시 설정을 수동으로 구성하려면 다음 명령줄을 관리자 권한으로 실행하면 됩니다.

AdminTool.exe /proxy /set /host proxy.company.org /port 80 /username dummy /password pass@word1

매개변수

#	Parameter	Description
1	/set	Action to be performed on the proxy settings
2	/host (ie | none | custom)	The destination host can be a predefined value (e.g. "ie" or "none") or a user-defined value (ex. 127.0.0.1 or proxy.company.org). This parameter is mandatory.
3	/port 80	The port number used to connect to the proxy server. Required if the hostname value is a custom user-defined value.
4	/username dummy	The username to connect to the proxy server. This setting is optional.
5	/password pass@word1	The user's password must be supplied if a username has been defined. However, its value can be empty.

명령줄을 사용하는 것을 좋아하고 다른 명령줄이 무엇인지 궁금하다면, 이곳으로 가십시오. 특정 문서)

제목: "볼륨 라이선스 지원 받는 방법"

볼륨 라이선스 지원 및 서비스 팀은 서버에 볼륨 라이선스를 설치하고 실행할 때 문제가 발생하면 기꺼이 도와드릴 것입니다.

볼륨 라이선스 지원 및 서비스 팀에 연락하는 가장 쉬운 방법은 온라인 헬프 데스크에서 티켓을 여는 것입니다: https://support.tsplus.net

서버에서 볼륨 라이선스의 사용자를 업데이트하는 방법은 무엇인가요?

사용자 활성화 볼륨 라이센스와 연결된 사용자 수를 변경하려면, 다음 명령줄을 관리자 권한으로 실행하십시오.

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /users 10

매개변수

이 명령은 두 개의 매개변수를 사용합니다:

- 볼륨 라이센스 키를 사용하세요.
- 사용자 수 무제한: 1에서 50까지의 숫자 또는 "무제한"을 사용하세요.

다음 사항에 유의하시기 바랍니다:

- 이 명령은 Advanced Security 및 2FA add-on에 적용되지 않습니다.
- 서버 모니터링은 서버 모니터링의 세 가지 사용 가능한 에디션에 해당하는 숫자 1, 5 및 10만 허용합니다.
- TSplus Remote Work만 50명 이상의 사용자 수를 허용합니다.

서버에서 볼륨 라이센스의 에디션을 업데이트하는 방법?

활성화된 볼륨 라이선스와 연결된 에디션을 변경하려면, 다음 명령줄을 관리자 권한으로 실행하십시오.

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /edition Enterprise

매개변수

이 명령은 두 개의 매개변수를 사용합니다:

- 볼륨 라이센스 키를 사용하세요.
- 기업 에디션 : 에디션 이름 사용

다음 사항에 유의하시기 바랍니다:

- 이 매개변수는 원격 작업, 원격 지원, 서버 모니터링, 2FA 추가 기능 및 서버 지니어스에 적용되지 않습니다.
- 가능한 에디션은 Remote Access를 위한 “Desktop”, “MobileWeb” 또는 “Enterprise”입니다.
- 가능한 에디션은 Advanced Security를 위한 “Essentials” 또는 “Ultimate”입니다.

명령줄을 사용하는 것을 좋아하고 다른 명령줄이 무엇인지 궁금하다면, 이곳으로 가십시오. 특정 문서)

지원 업데이트

업데이트/지원 구독을 연장하려면 연장 시간의 운영에서 1, 2 또는 3을 선택하십시오.
이 명령어를 사용하세요: “AdminTool.exe /vl /renewsupport VOLU-MELI-CENS-EKEY /supportyears 1”

이 명령은 버전 15.60.11.8부터만 사용할 수 있습니다.

볼륨 라이선스

볼륨 라이선스는 TSplus의 솔루션을 위한 스크립팅 라이선스 솔루션입니다. 다음 제품은 2020 볼륨 라이선스를 사용한 활성화를 지원합니다: Remote Access, Remote Work, Advanced Security (일명 RDS-Knight), Remote Support 또는 Server Monitoring (이전의 Server Genius).

라이센스 관리 포털에서 볼륨 라이센스 계정이 생성되면, 볼륨 라이센스 팀이 제공할 것입니다:

1. 귀하의 볼륨 라이센스 키(이 정보를 비밀로 유지해 주십시오)
2. 라이센스 관리 포털에 연결하기 위한 자격 증명
3. 이 볼륨 라이선스 2020 관리자 가이드

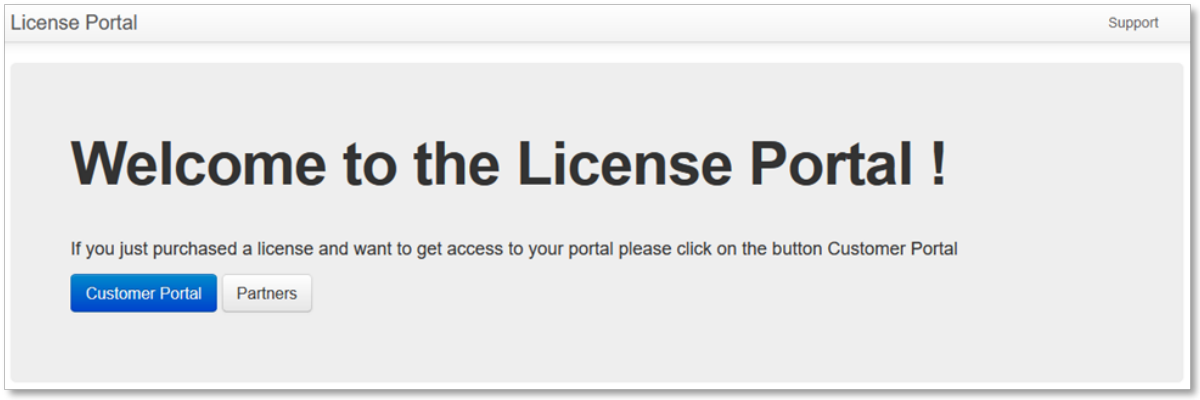
VIRTUAL PRINTER는 더 이상 라이센스가 없습니다.
2022년 3월 15일 이후 및 버전 15.40.3.14부터, Virtual Printer는 더 이상 라이센스가 없으며 TSplus Remote Access의 모든 에디션에 포함됩니다.

볼륨 라이센스를 어떻게 관리하나요?

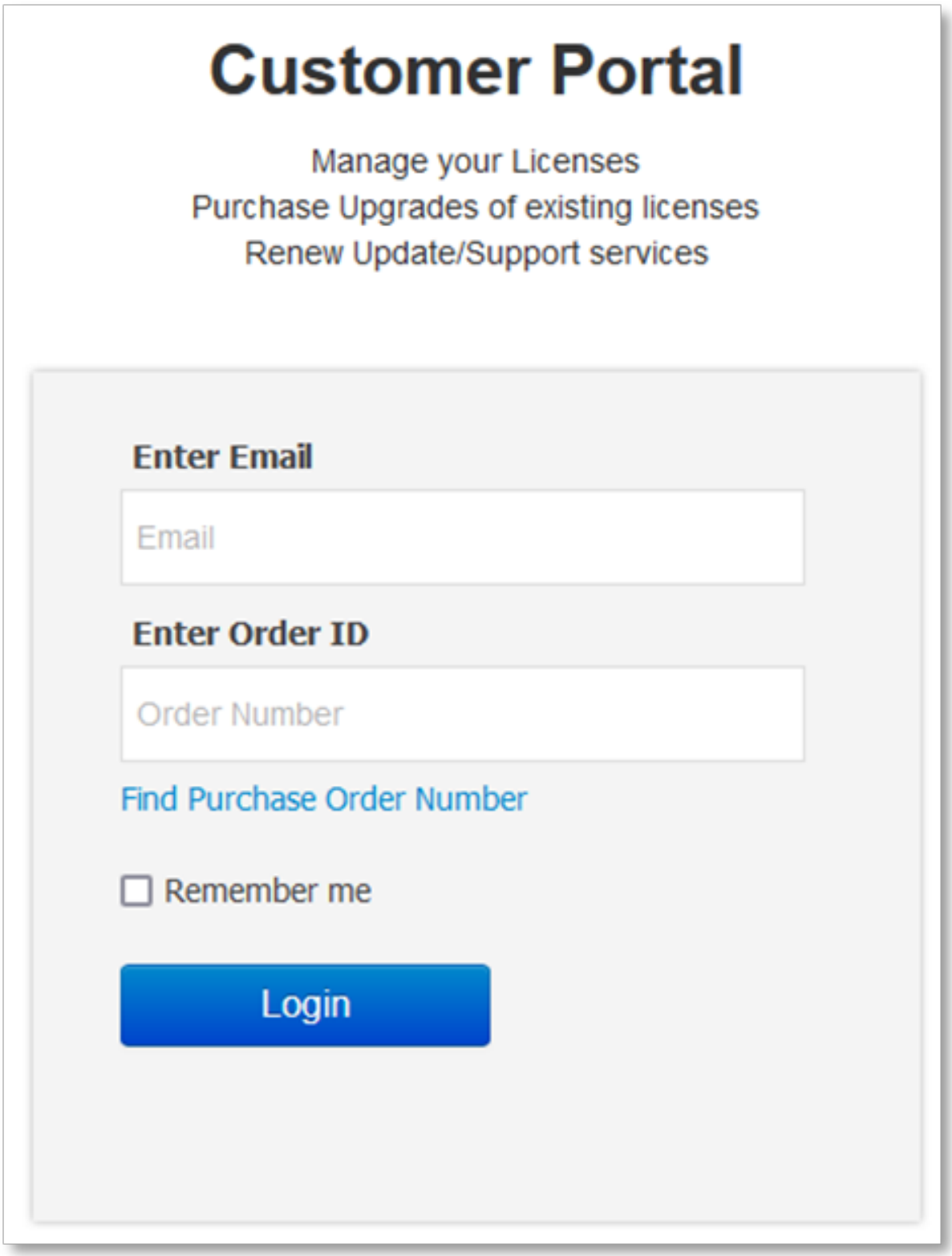
귀하의 볼륨 라이센스 및 크레딧 잔액은 TSplus 라이센스 포털에서 검토하고 관리할 수 있습니다.

TSplus 라이센스 포털은 다음 URL에서 이용할 수 있습니다: https://license.tsplus.net

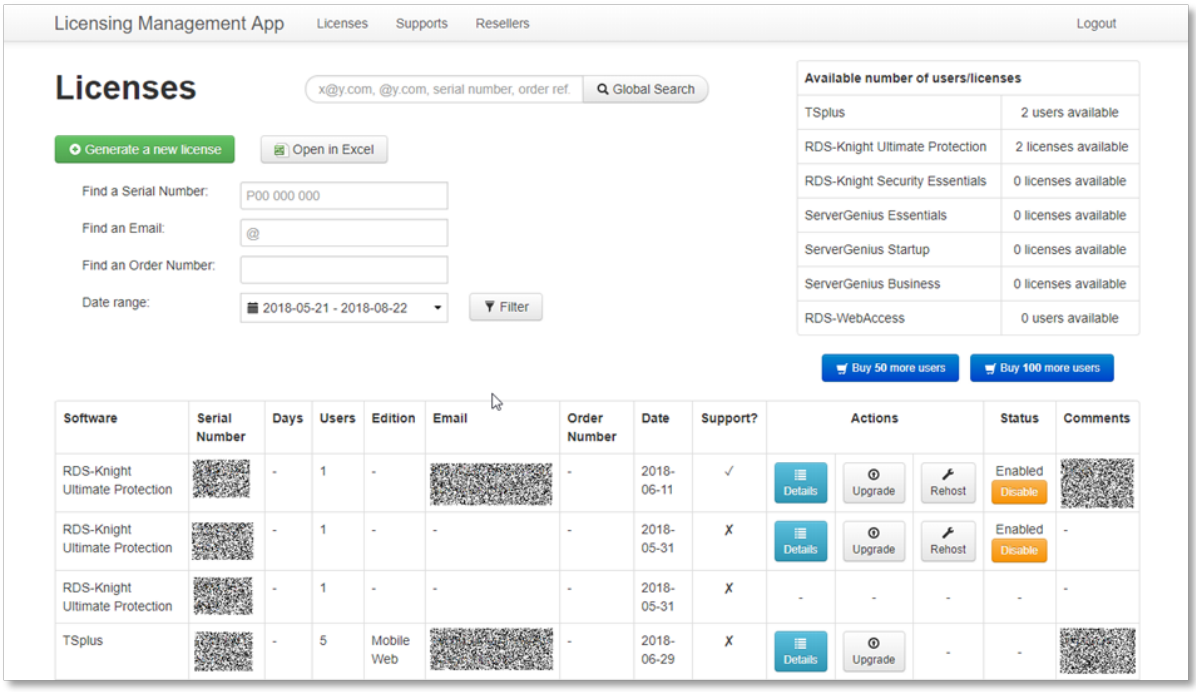
계정에 연결하고 접근하려면, 고객 섹션에 도달하기 위해 고객 포털을 클릭하여 시작하세요.



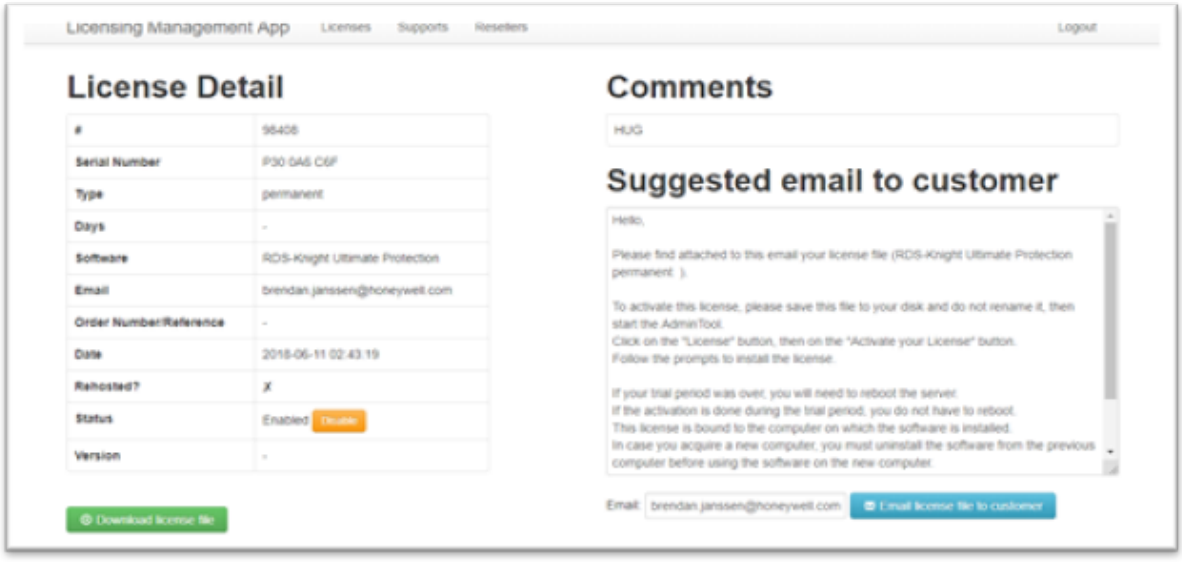
그런 다음 계정에 액세스하기 위해 자격 증명을 입력하십시오:



로그인하면 모든 라이센스가 나열된 다음 표를 볼 수 있습니다. 이 페이지는 모든 라이센스를 관리할 수 있는 주요 페이지입니다. 아직 볼륨 라이센스를 활성화하지 않았다면 이 페이지는 비어 있습니다.



라이선스 기록 세부정보를 검토하려면 연구하고자 하는 라이선스의 “세부정보” 버튼을 클릭하십시오. 아래 그림에 표시된 라이선스 세부정보 페이지를 확인할 수 있습니다.



TSplus 웹 앱

TSplus 웹 앱은 번거로운 소프트웨어 설치나 복잡한 연결 클라이언트 없이 원활한 원격 액세스 경험을 제공하기 위해 최신 브라우저 API를 활용하는 프로그레시브 웹 앱(PWA)입니다. 산업 표준 HTML5 디스플레이 및 통신 프로토콜을 활용하도록 설계된 TSplus 웹 앱은 사용하는 장치의 종류에 관계없이 네이티브 연결 솔루션처럼 보입니다.

이점

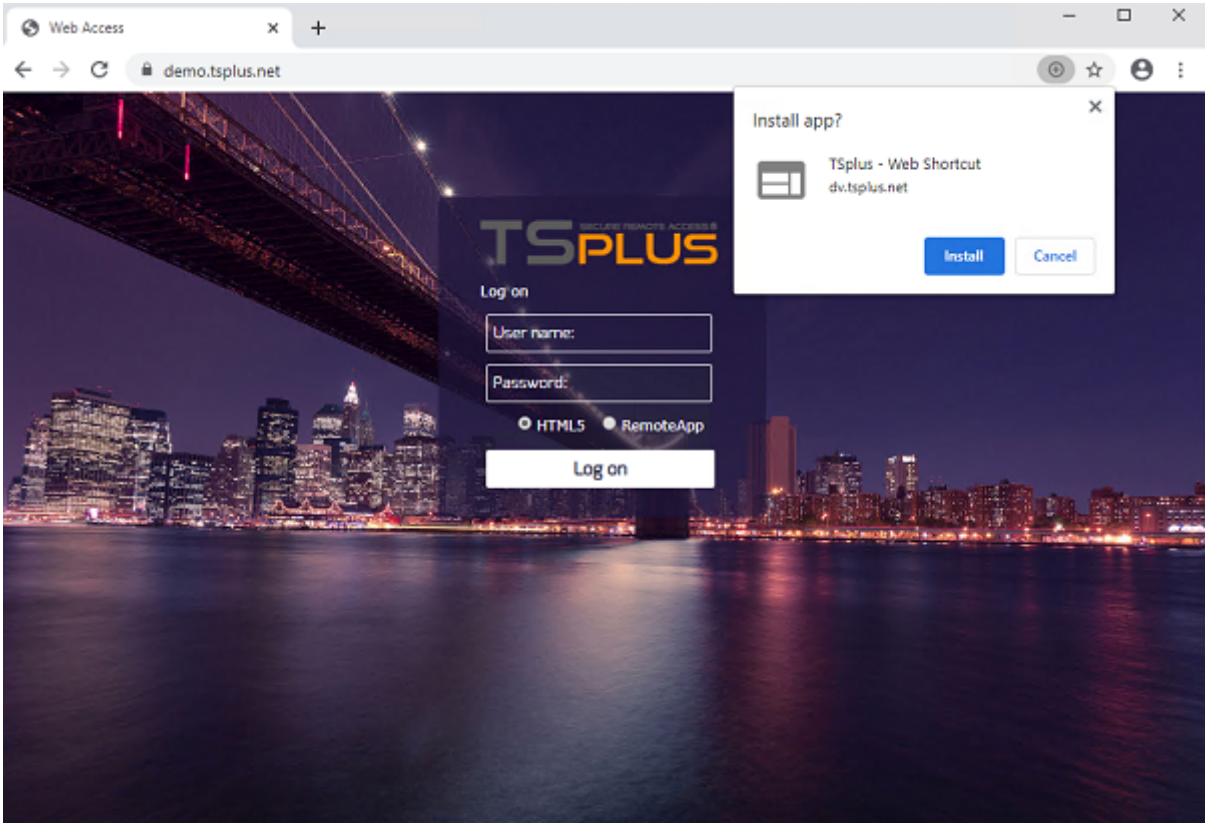
새로운 TSplus WebApp은 이전 애플리케이션 및 연결 클라이언트에 비해 다음과 같은 개선 사항을 통해 향상된 성능과 가치를 제공합니다:

- 작은 소프트웨어 발자국으로 인한 더 빠른 로드 시간.
- 데이터 사용량 감소 - TSplus Web App은 일반적인 브라우저 기반 트래픽 관리를 활용하여 데이터 사용량을 최소화합니다.
- 원활한 사용자 경험 - 로그인 화면에서 애플리케이션 렌더링까지, TSplus WebApp은 사용자에게 네이티브 애플리케이션 사용의 모습을 제공합니다.
- 더 이상 많은 브라우저 창으로 인해 브라우저 탭이나 세션을 잃어버리지 마세요. TSplus 웹 앱의 동작은 다른 최고 수준의 애플리케이션과 동일한 멀티태스킹 옵션을 제공합니다.

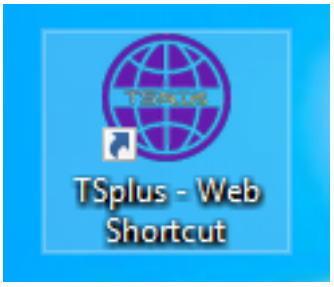
설치 - PC

귀하가 선호하는 일반 웹 브라우저를 사용하여 회사의 TSplus 웹 포털로 이동하십시오(HTTPS 구성 필요).
Firefox에서 사용하려면 설치해야 합니다. PWAS 추가 기능.

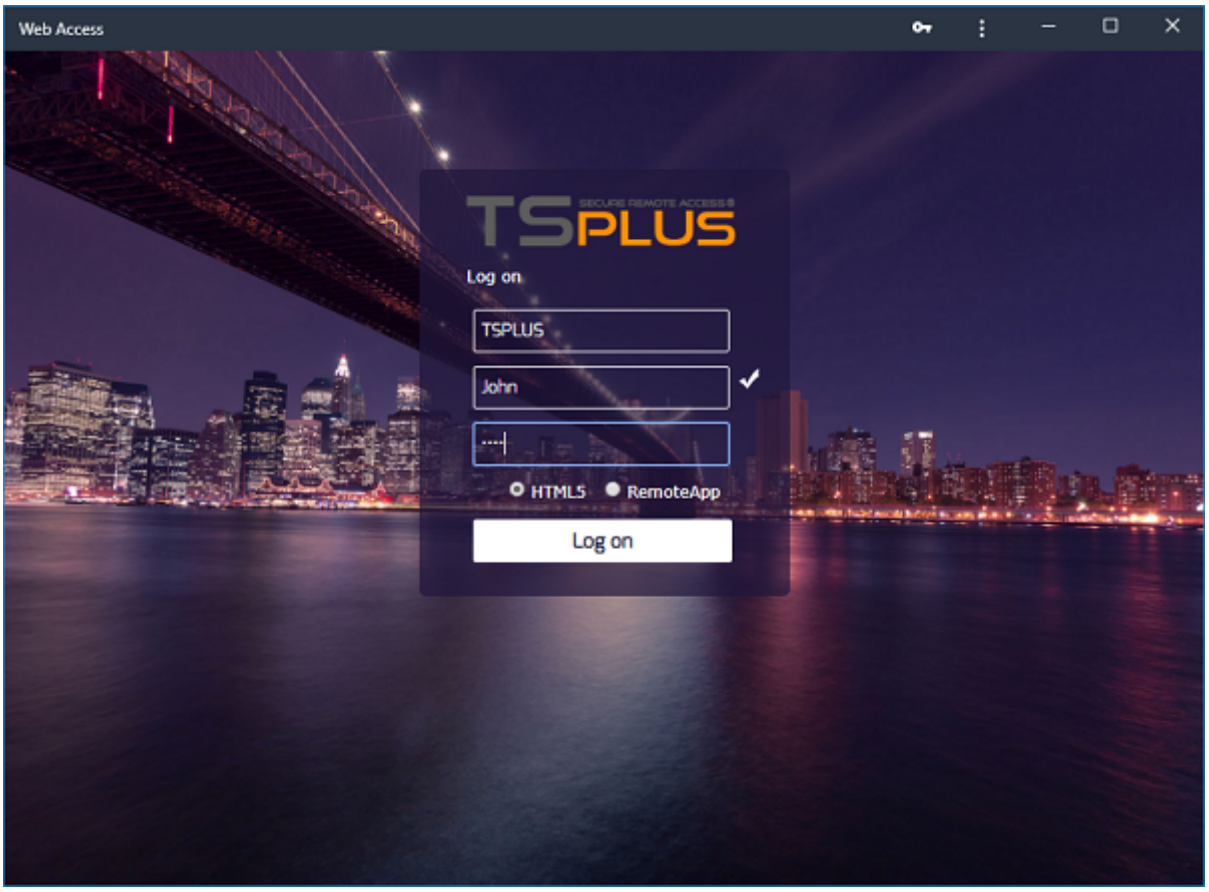
네비게이션 바 오른쪽에 위치한 + 버튼을 클릭하세요. 프롬프트가 나타나면 '설치'를 클릭하세요.



설치는 단 1초밖에 걸리지 않습니다. 바탕 화면에 아이콘이 생성됩니다:



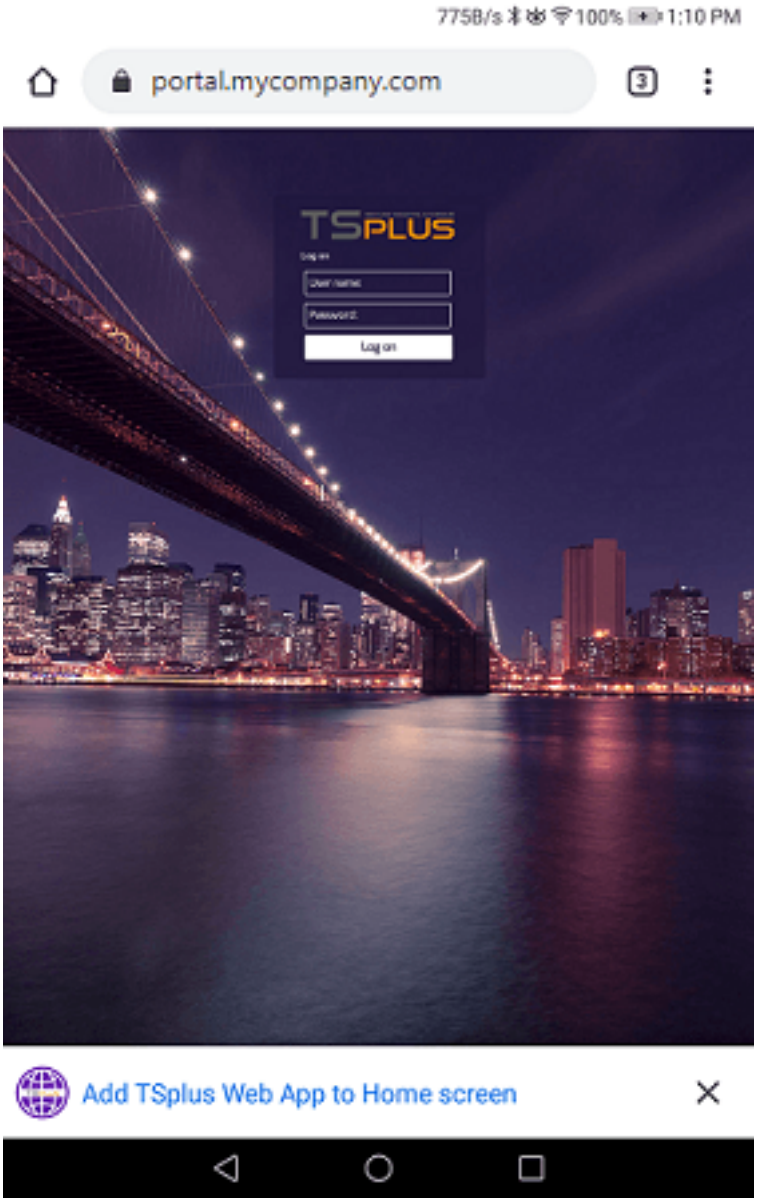
웹 앱은 완료되면 즉시 열립니다.



설치 - 안드로이드 모바일 장치

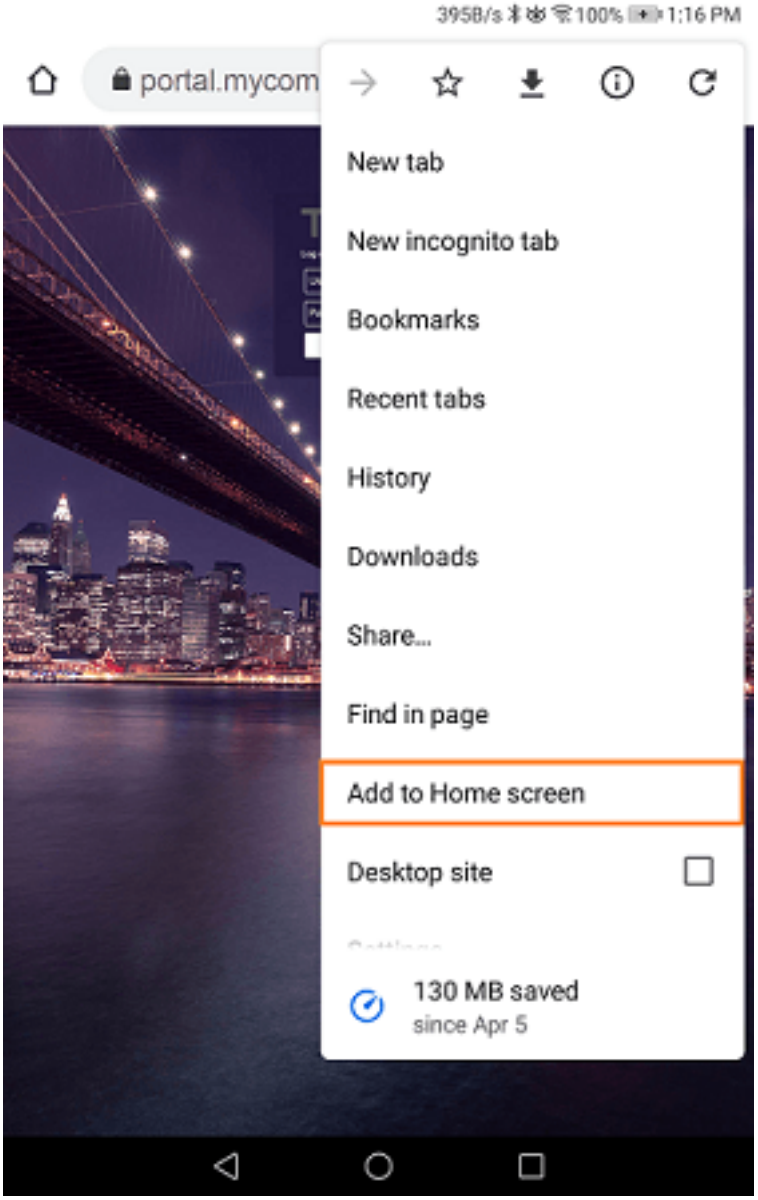
선호하는 일반 모바일 웹 브라우저를 사용하여 귀사의 TSplus 웹 포털로 이동하십시오. **TSplus 서버에서 HTTPS 프로토콜이 필요합니다.**

웹 포털은 창의 하단에 있는 "홈 화면에 TSplus 웹 앱 추가" 메시지를 클릭하여 TSplus 웹 앱을 홈 화면에 추가하는 옵션을 제공합니다.

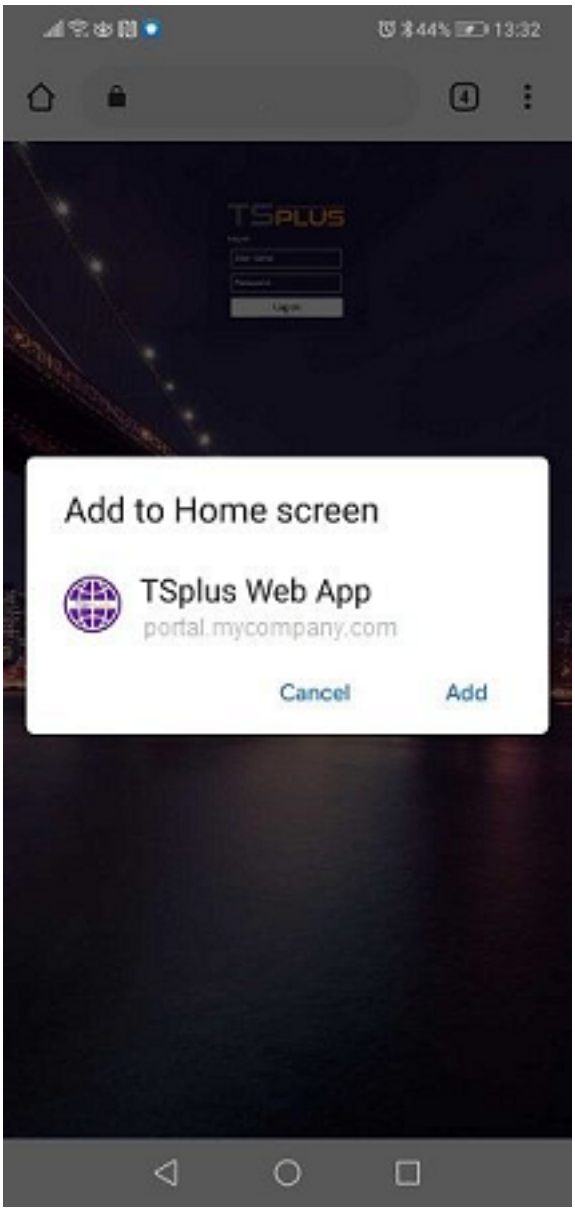


창의 오른쪽 상단에 있는 3점 메뉴를 클릭한 후 "추가"를 클릭하여

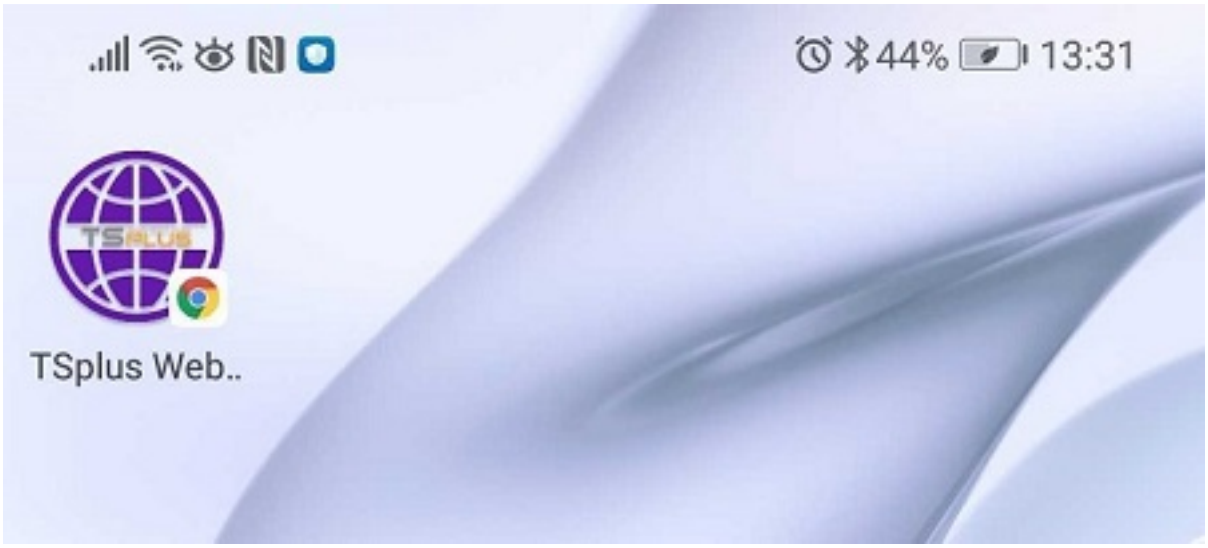
홈 화면에 추가 옵션을 수락한 후, 사용자는 다음 화면을 보게 됩니다:



‘추가’ 버튼을 클릭하면 프로세스가 완료됩니다.

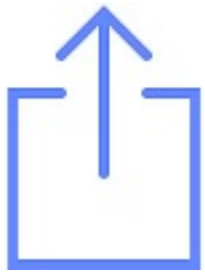


TSplus 웹 앱이 이제 모바일 기기의 홈 화면에서 직접 접근할 수 있습니다.



설치 - Apple iOS 모바일

iOS에서 웹 앱 설치 과정은 Android 과정과 유사합니다. Safari 웹 브라우저를 사용하여 TSplus 웹 포털로 이동하기만 하면 됩니다. 공유 버튼을 클릭하세요.

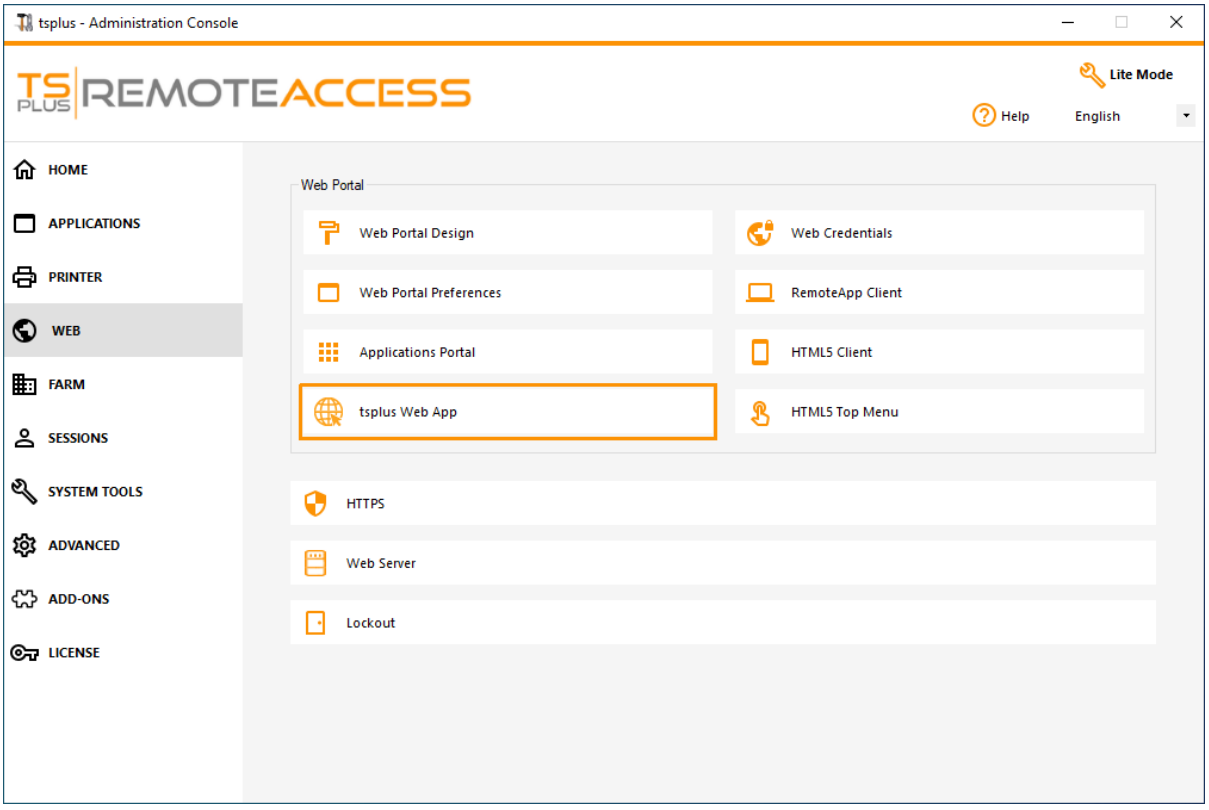


그런 다음 "홈 화면에 추가"를 클릭하십시오.

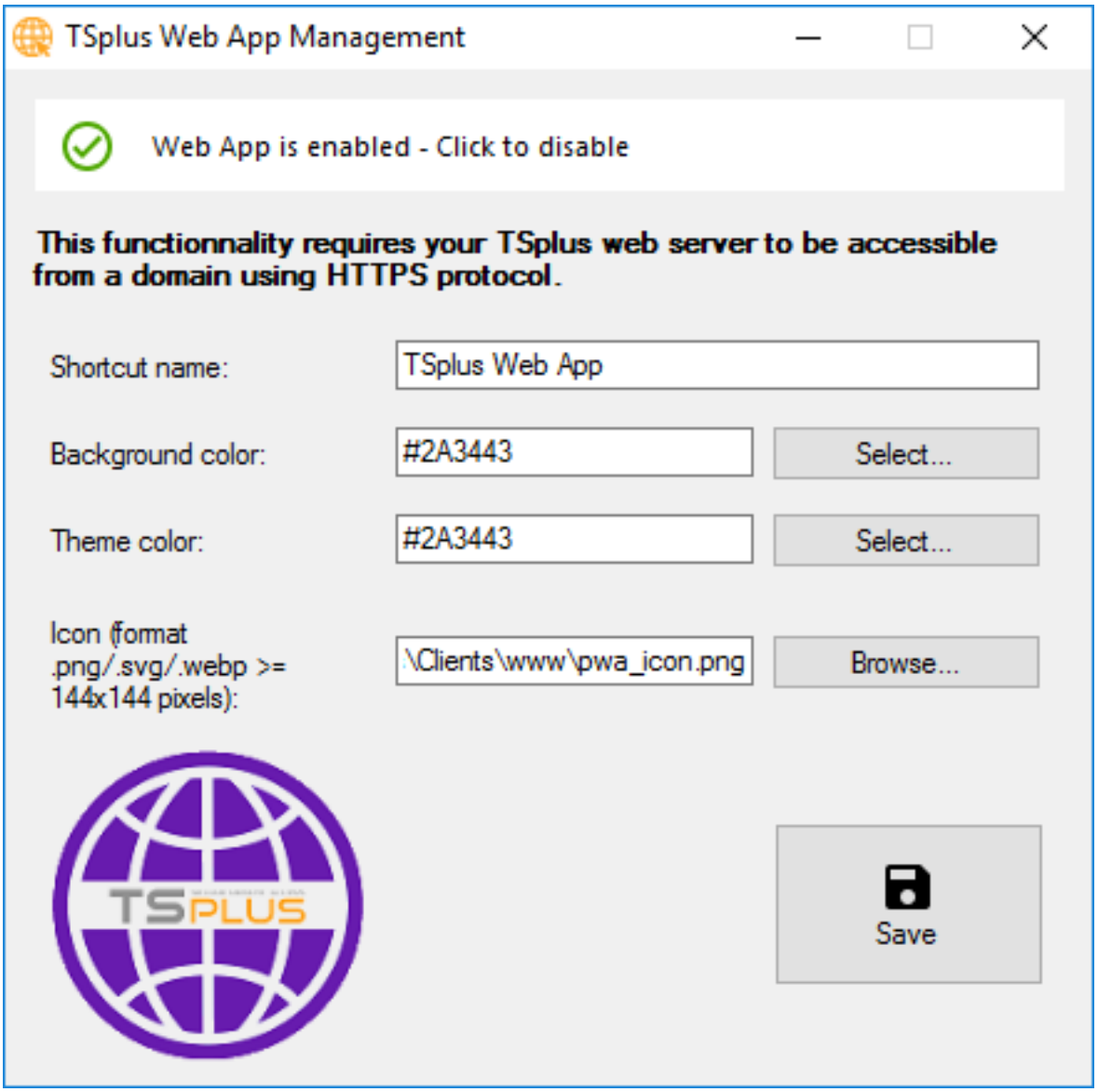
참고: Chrome 브라우저는 iOS에서 웹 앱 기능을 지원하지 않습니다.

관리

웹 앱을 관리하려면 TSplus 관리 도구 웹 - 웹 포털 섹션으로 이동하여 TSplus 웹 앱 타일을 클릭하세요.



웹 앱은 기본적으로 활성화되어 있지만 비활성화할 수 있습니다. TSplus 웹 앱의 바로 가기 이름, 배경 및 테마 색상, 아이콘을 수정할 수 있습니다.



“저장”을 클릭하여 수정 사항을 기록하세요.

웹 애플리케이션 포털: URL 주소의 매개변수

Terminal Service Plus 표준 로그인 웹 액세스 페이지를 우회하려면 사용하십시오. 웹 애플리케이션 포털 웹 애플리케이션 포털 페이지로 직접 이동하려면 URL 주소에 여러 매개변수를 지정해야 합니다.

- 사용자 로그인
- 사용자 비밀번호
- 사용자 도메인
- 서버
- 포트
- 클라이언트 유형 (HTML5 또는 Windows)

여기 HTML5 클라이언트를 사용하는 우리의 데모 서버에서 사용자 "demo"와 비밀번호 "demo"에 대한 전체 URL 주소의 예가 있습니다:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo&domain=&server=127.0.0.1&port=3389&type=html5

도메인, 서버, 포트 및 유형 매개변수가 선택 사항인 경우, 다음 URL 주소는 정확히 동일한 동작을 합니다:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo

Windows 클라이언트를 사용하려면 다음을 사용하십시오:

&type=원격액세스

해당 매개변수를 URL 주소에 사용하면 웹 애플리케이션 포털 페이지로 직접 이동할 수 있습니다.

모든 매개변수를 동시에 지정할 필요는 없습니다: 지정하지 않은 매개변수는 기본 설정 값이 적용됩니다.

HTML5 클라이언트를 사용할 때 Terminal Service Plus 표준 로그온을 우회하려면 확인하십시오. 이 페이지 .

웹 애플리케이션 포털

Terminal Service Plus 웹 애플리케이션 포털은 애플리케이션 및 데스크톱 배포와 생애 주기 관리를 간소화하여 IT 비용을 절감할 수 있는 단일 유연한 솔루션을 제공합니다. IT는 중앙 집중식으로 관리하고 웹을 통해 온디맨드 애플리케이션을 제공함으로써 역할 기반 관리, 애플리케이션 제어, 보안 및 사용자 지원을 제공하여 애플리케이션 배포의 성공률을 향상시킬 수 있습니다.

Terminal Service Plus 웹 애플리케이션 포털은 Windows 앱과 데스크톱을 안전한 온디맨드 서비스로 가상화하고 변환합니다.

웹 애플리케이션 포털을 사용하면 Microsoft Windows 애플리케이션(비즈니스 애플리케이션, Office 애플리케이션 등)을 웹에 게시할 수 있습니다.

Citrix와 마찬가지로, 사용자는 포털 웹 페이지의 애플리케이션 아이콘을 클릭하기만 하면 인터넷에서 직접 애플리케이션에 접근할 수 있습니다.

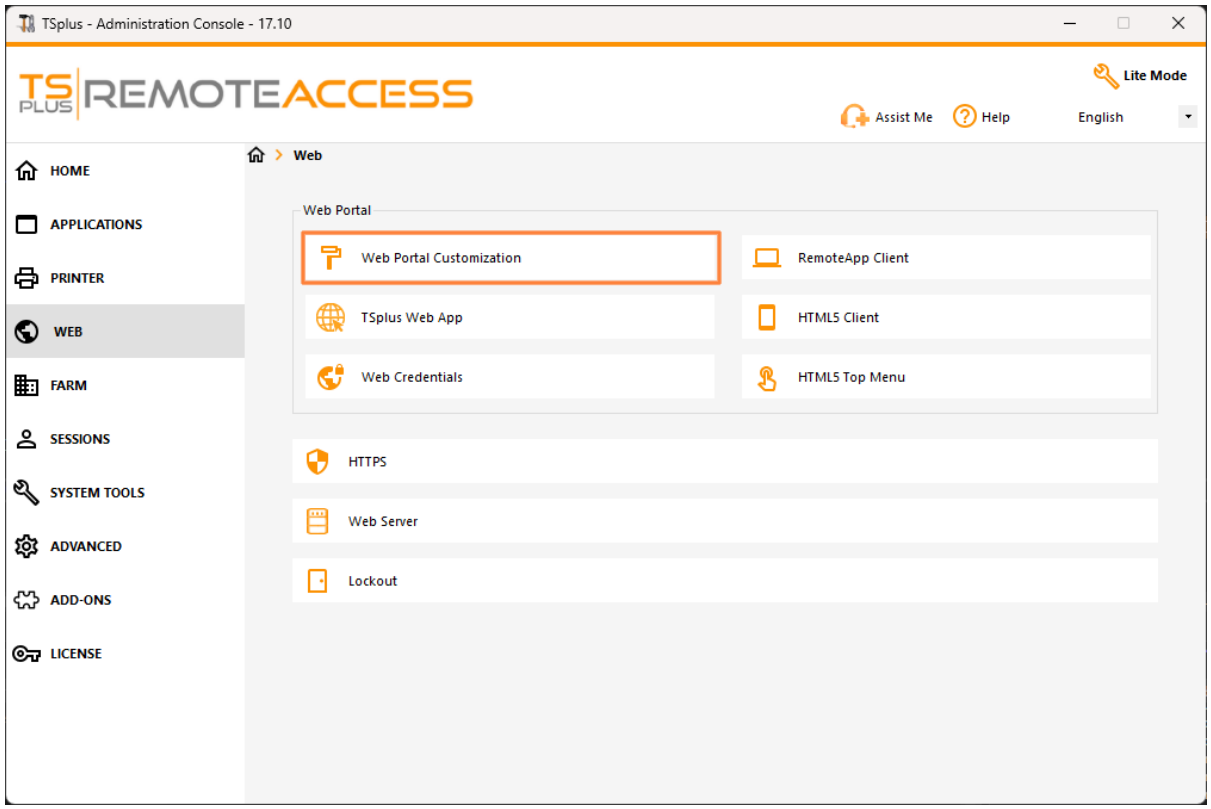
웹 애플리케이션 관리

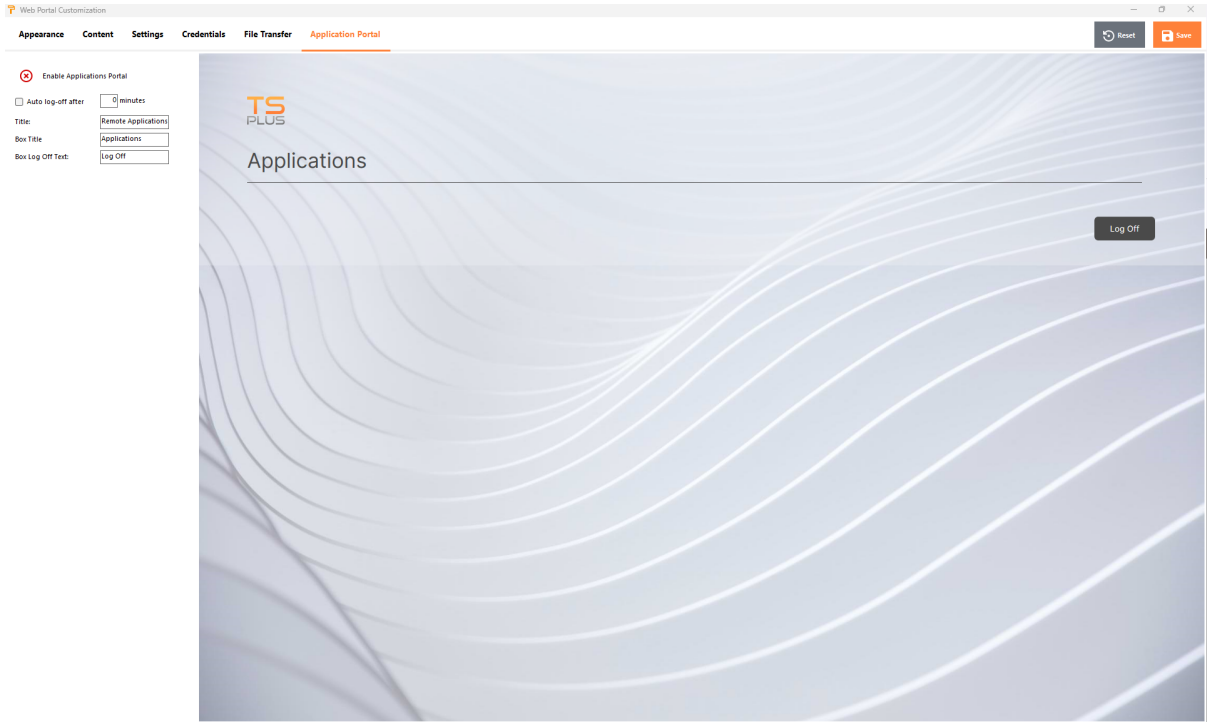
웹 애플리케이션 포털 기능은 **완전 통합** 터미널 서비스 플러스에서. 이는 터미널 서비스 플러스 애플리케이션 게시 기능에 의해 게시된 모든 애플리케이션이 웹 애플리케이션 포털에서 사용될 수 있음을 의미합니다.

이 출판 프로세스에 대해 더 알고 싶으시다면, 저희 문서에서 읽어보시기 바랍니다. 애플리케이션 퍼블리싱 그리고 사용자 또는 그룹에 애플리케이션 할당 .

웹 애플리케이션 포털 디자인

관리 도구에서 "웹" 탭을 열고 "웹 포털 사용자 정의" 타일을 클릭한 다음 "애플리케이션 포털" 타일로 이동합니다.





웹 애플리케이션 포털 기능이 활성화된 웹 액세스 페이지를 생성하려면, **"응용 프로그램 포털 사용" 체크박스를 선택하십시오.** 웹 액세스 페이지를 원하는 대로 사용자 정의한 후 "저장"을 클릭하여 이 새로운 웹 액세스 페이지를 게시할 수 있습니다.

참고: 클래식 테마에서만 상자와 상자 테두리 색상을 변경할 수 있습니다. 모양 탭 .

웹 애플리케이션 포털 사용

이 예제에서는 기본 이름 "index"로 새 웹 액세스 페이지를 게시했습니다.

접속하려면 웹 브라우저를 열고 http://your_server_name/로 이동하세요. (이 예제에서는 사용합니다. http://localhost 서버 자체에서 직접).

첫 번째 웹 페이지에 표시되는 것은 표준 Terminal Service Plus 웹 로그인 페이지입니다:

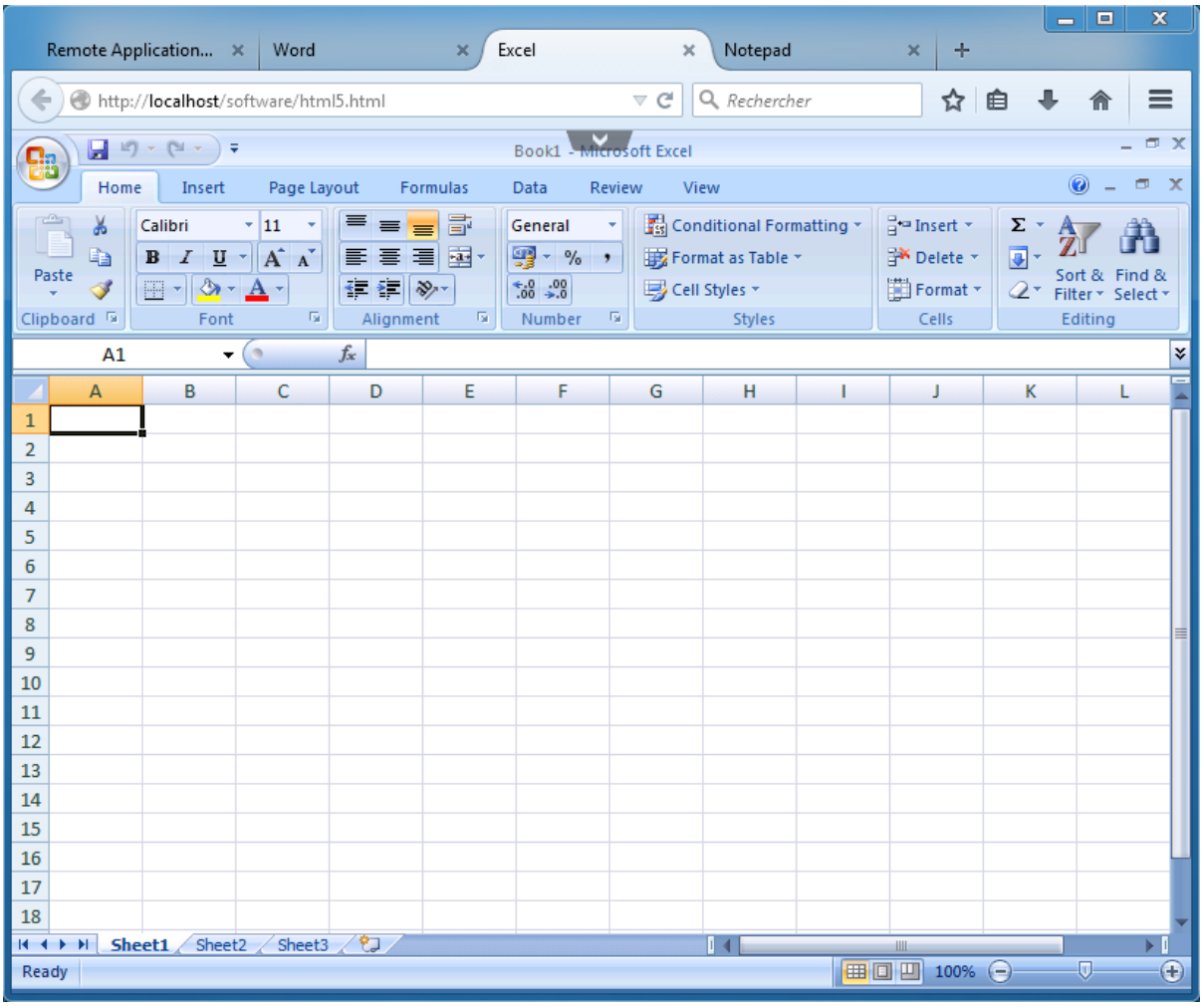


로그인하면 새로운 웹 페이지가 표시되며, 이것이 웹 애플리케이션 포털입니다:

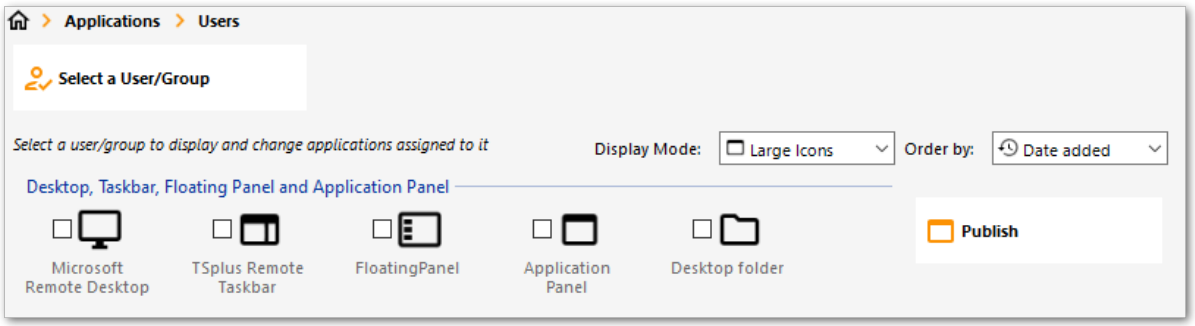


사용자가 접근할 수 있는 모든 게시된 애플리케이션에 대해 아이콘을 받는 것을 볼 수 있습니다.

사용자는 이제 하나 이상의 아이콘을 클릭하여 새 탭에서 일치하는 애플리케이션을 원격으로 열 수 있습니다.

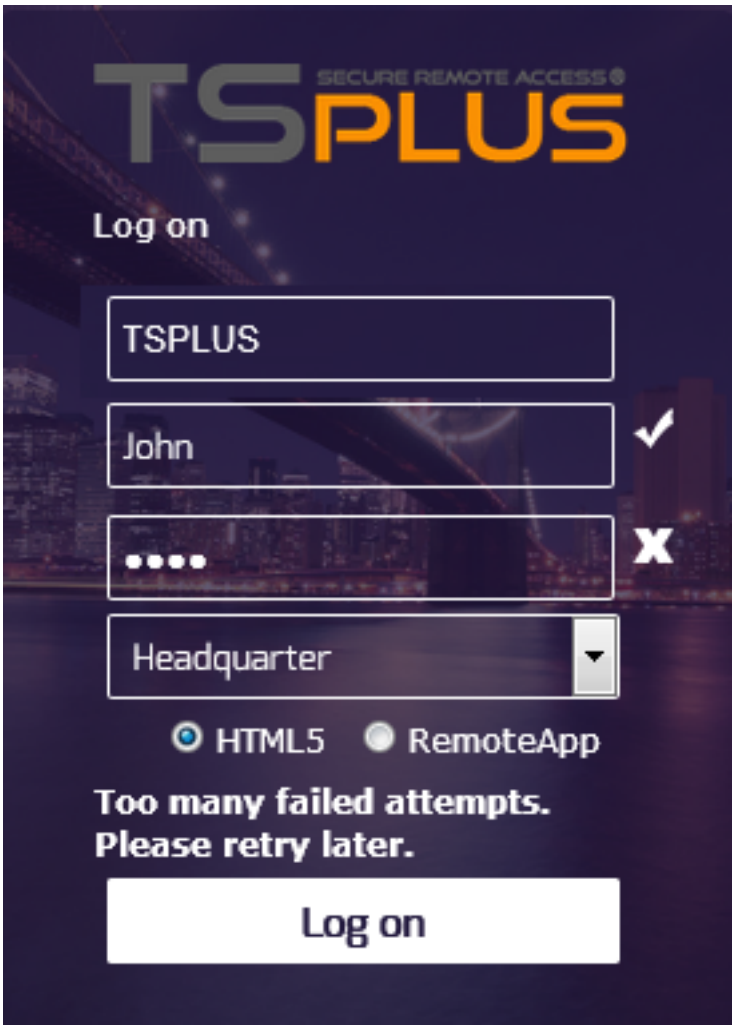


응용 프로그램 포털만 사용하고 Windows 세션, 원격 작업 표시줄, 플로팅 패널 등을 열지 않으려면 사용자 프로필과 관련된 모든 상자의 선택을 해제해야 합니다.



TSplus 11.40 버전 출시 이후, 사용자가 잘못된 자격 증명을 입력할 때 웹 포털에 대한 무차별 대입 공격이 차단됩니다.

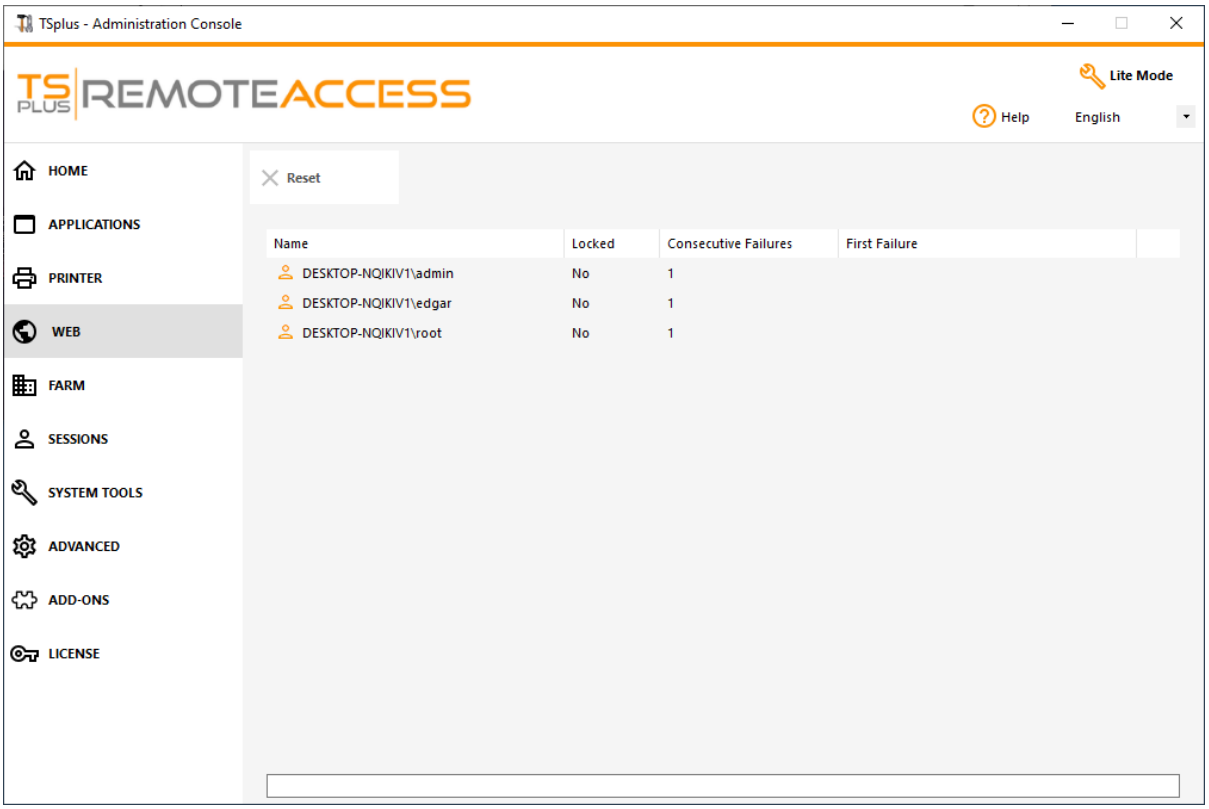
10회 시도 후 15분 동안, 웹 포털은 사용자가 30분 동안 로그인하는 것을 금지합니다 (사용자 정의 가능). 고급 - AdminTool의 잠금 탭) :]



이것은 TSplus 폴더에 위치한 hb.exe.config 파일에서 사용자 정의할 수 있는 기본 설정입니다.

TSplus\Clients\www\cgi-bin\hb.exe.config의 “appSettings” 단락에서.

TSplus의 잠금 기능에서 사용자가 차단된 모든 연결 및 로그를 확인할 수 있습니다.



이 기능 첫 번째 웹 포털 연결 후에 표시되고 활성화됩니다.

중요한 사항

- 웹 애플리케이션 포털 기능은 호환됩니다. 농장 / 게이트웨이 구성 그리고 또한 지원합니다 로드 밸런싱 .
- 농장 / 게이트웨이 구성에서 애플리케이션은 농장의 모든 서버에 게시되고 할당되어야 합니다.
- Terminal Service Plus 라이센스 측면에서 사용자는 1명의 사용자로 계산되지 않고 동시에 여러 애플리케이션을 열 수 있습니다.

웹 자동 로그인: 포털 없이 웹에서 연결

개요

Terminal Service Plus 웹 포털은 사용자가 Windows 자격 증명을 사용하여 모든 웹 브라우저에서 원격 서버에 연결할 수 있도록 합니다.

때때로 특정 URL 주소를 실행할 때 자동으로 연결하고 싶을 수 있습니다. 이 기능은 웹 자동 로그인이라고 합니다.

Web Autologon을 사용하면 특정 Terminal Service Plus 파일에 지정된 설정(로그인, 비밀번호, 포트 등)을 사용하여 연결됩니다.

주의

이 기능을 사용할 때, 귀하의 사용자 이름과 비밀번호가 페이지를 방문하는 누구에게나 노출될 수 있습니다.

또한 모든 사용자가 동일한 사용자 이름을 공유하는 경우, 사용자가 동일한 사용자 이름을 공유하는 다른 사용자로부터 민감한 정보를 볼 수 있을 가능성이 있습니다.

이 기능은 특정 사용 사례에만 적합하며 권장되지 않습니다.

HTML5 클라이언트를 이용한 웹 자동 로그인

직접 브라우징하여 연결할 수 있습니다. http://your-server/software/html5.html

연결 설정은 다음 파일을 메모장 또는 기타 텍스트 편집기(예: Notepad++ - MS Word는 사용하지 마십시오)로 편집하여 수정할 수 있습니다.

C:\Program Files (x86)\TSplus\Clients\www\software\html5\settings.js

웹 자동 로그인을 이용하려면 최소한 로그인과 비밀번호를 지정해야 합니다.

이 파일을 수정한 후 웹 브라우저에서 페이지를 새로 고쳐야 할 수 있습니다.

원격 앱 웹 클라이언트를 사용한 웹 자동 로그인

직접 브라우징하여 연결할 수 있습니다. http://your-server/software/remoteapp2.html

연결 설정은 다음 파일을 메모장 또는 기타 텍스트 편집기(예: Notepad++ - MS Word는 사용하지 마십시오)로 편집하여 수정할 수 있습니다.

C:\Program Files (x86)\TSplus\Clients\www\software\remoteapp2.js

웹 자동 로그인을 이용하려면 최소한 로그인과 비밀번호를 지정해야 합니다.

이 파일을 수정한 후 웹 브라우저에서 페이지를 새로 고쳐야 할 수 있습니다.

같은 자격 증명을 사용하여 여러 사용자 세션을 활성화합니다.

여러 사용자 세션을 동일한 자격 증명을 사용하여 활성화하려면 이 절차를 따르십시오.

index.html 파일이 위치한 곳에서 복사할 수 있습니다:

C:\Program Files (x86)\TSplus\Clients\www

사용자 수만큼 여러 번. 이름을 바꾼 후 URL로 접근할 수 있습니다. http://nameofyourserver.com/renamedindex.html

사용자 자격 증명에 해당하는 단락을 편집하십시오:

액세스 구성 ---------- var user = ""; // 원격 서버에 연결할 때 사용할 로그인 (이 페이지에 입력된 로그인 사용하려면 ""로 두세요) var pass = ""; // 원격 서버에 연결할 때 사용할 비밀번호 (이 페이지에 입력된 비밀번호 사용하려면 ""로 두세요) var domain = "";

원하는 만큼 index.html 파일을 복사할 수 있으며, 사용자 이름으로 이름을 바꾸면 개인 링크를 제공하는 데 더 쉬워집니다.

웹 자격 증명

개요

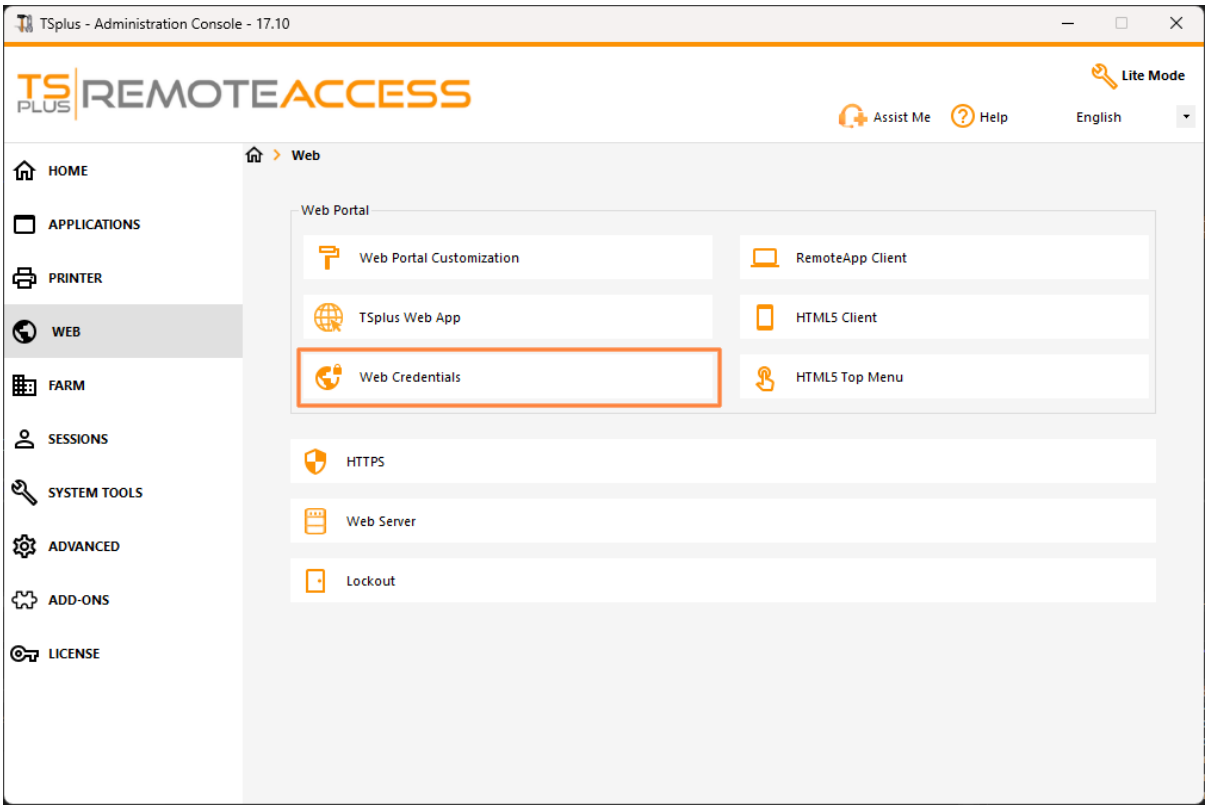
Terminal Service Plus Web Credentials는 사용자가 단순히 이메일 주소나 핀 코드를 사용하여 연결할 수 있도록 해주는 최첨단의 독특한 기능입니다.

웹 자격 증명을 사용하면 사용자의 이메일 주소 또는 비즈니스 애플리케이션에서 생성된 간단한 PIN 코드로 서버의 액세스를 보호할 수 있습니다. 이 기능의 큰 장점 중 하나는 이러한 자격 증명(이메일 또는 PIN 코드)이 순수한 웹 자격 증명이라는 것입니다: 사용자는 현재 사용 중인 Windows 사용자 계정을 알지 못하며, 애플리케이션에 연결하기 위해 실제 Windows 로그인/비밀번호를 알 필요가 없습니다.

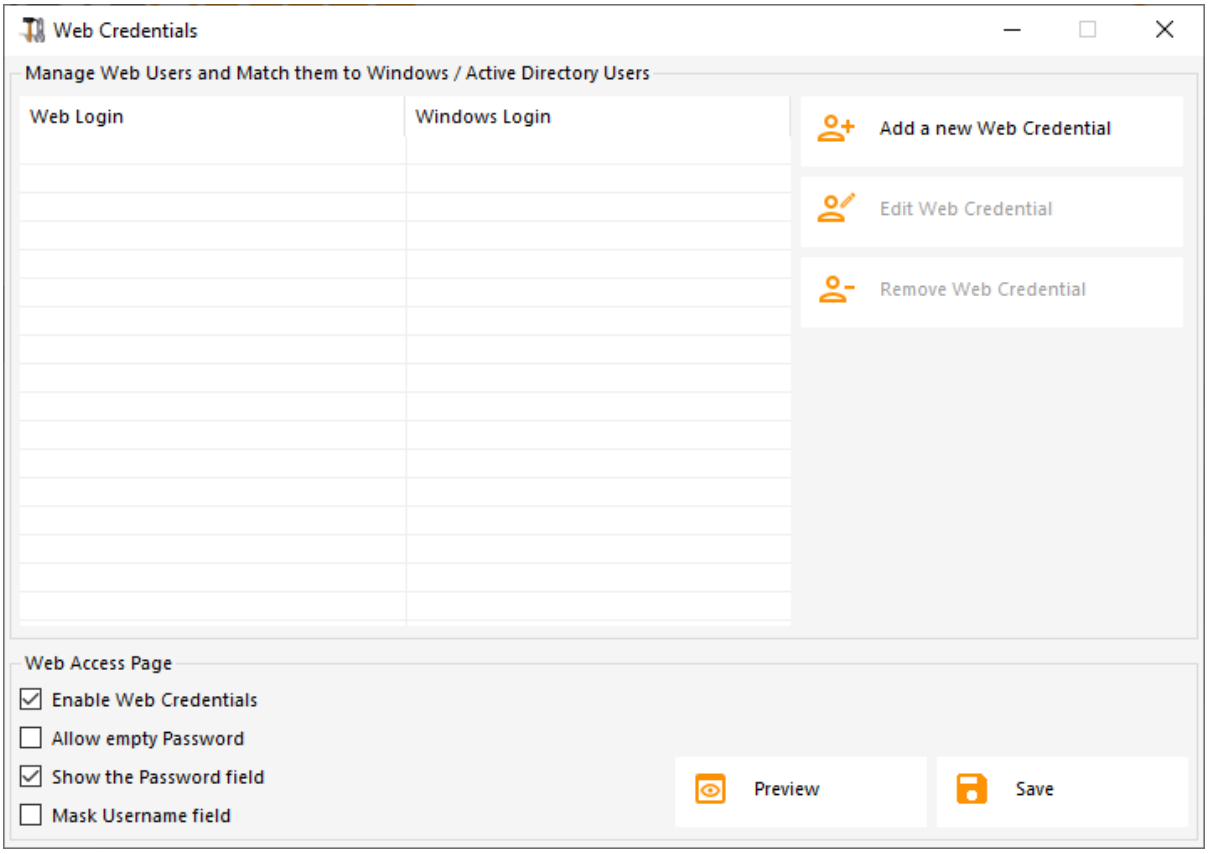
웹 자격 증명을 사용하면 사용자 정의 순수 웹 자격 증명을 정의하고 이를 기존 Windows / Active Directory 사용자 계정과 일치시킬 수 있습니다. 그런 다음 사용자는 Windows / Active Directory 자격 증명 대신 이러한 사용자 정의 자격 증명을 사용하여 연결할 수 있습니다.

웹 자격 증명 관리

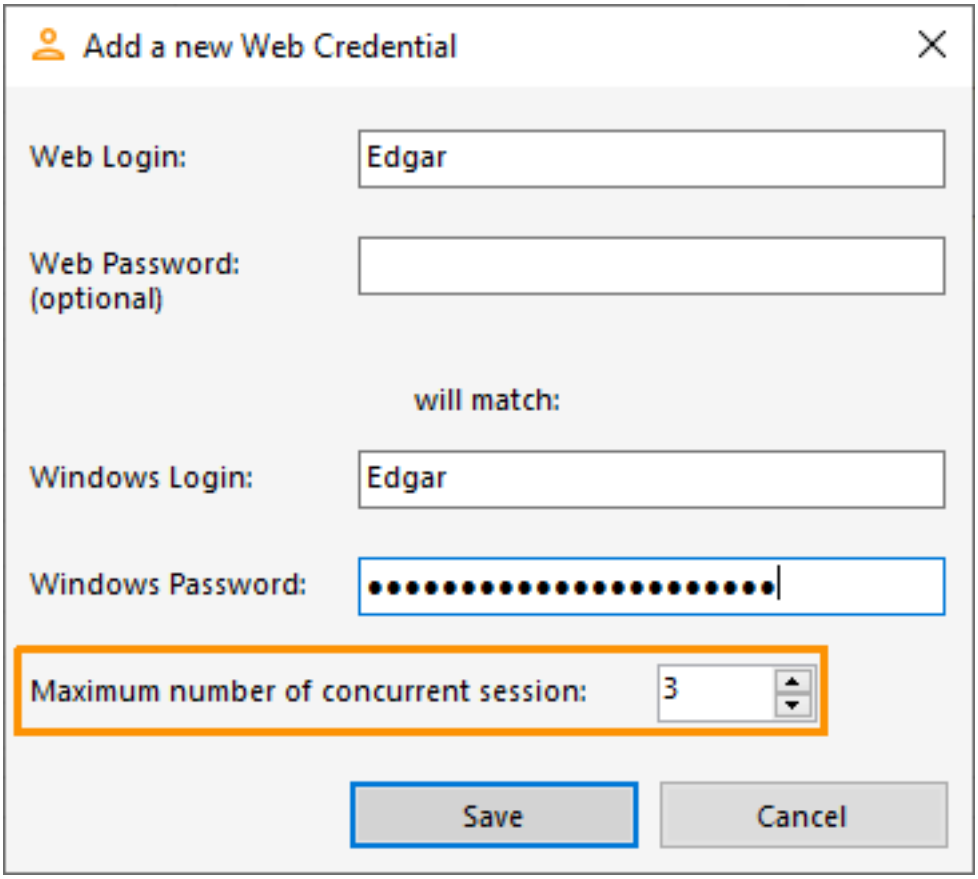
관리 도구에서 "웹" 탭을 열고 "웹 자격 증명" 타일을 클릭합니다.



웹 자격 증명 관리자가 열리고 이 창을 표시합니다:



이제 아래와 같이 기존 Windows / Active Directory 사용자 계정과 사용자 정의 로그인 및 (선택 사항) 비밀번호를 일치시켜 새로운 웹 자격 증명을 생성할 수 있습니다.



TSplus 9.50 버전 이후로, 사용자의 최대 동시 세션 수를 결정할 수 있습니다.

기존의 웹 자격 증명을 편집하거나 제거하여 구성한 사용자 지정 자격 증명을 변경하거나 비활성화할 수 있습니다.

대안으로, 명령줄을 통해 웹 자격 증명을 생성할 수 있습니다:

- Windows 시작 메뉴에서 실행 필드에 다음을 입력하세요: 'cmd.exe' (또는 프로그램/보조 프로그램 > 'Windows Power Shell')
- 그런 다음 올바른 폴더로 이동하기 위해 다음을 입력하십시오: cd “C:\Program Files (x86)\TSplus\UserDesktop\files”, 그런 다음 Enter 키를 눌러 확인합니다.
- 새로운 웹 자격 증명을 추가하려면 다음을 입력하십시오: AdminTool.exe /webcredentials-add your_web_login your_web_password your_windows_login your_windows_password maximum_concurrent_sessions
- 빈 자격 증명을 추가하려면 빈 텍스트를 나타내기 위해 두 개의 큰따옴표를 입력하십시오: ""
- 웹 자격 증명을 삭제하려면 다음을 입력하십시오: AdminTool.exe /webcredentials-remove your_web_login

명령줄을 사용하는 것을 좋아하고 다른 명령줄이 무엇인지 궁금하다면, 이곳으로 가십시오. 특정 문서)

중요한 사항

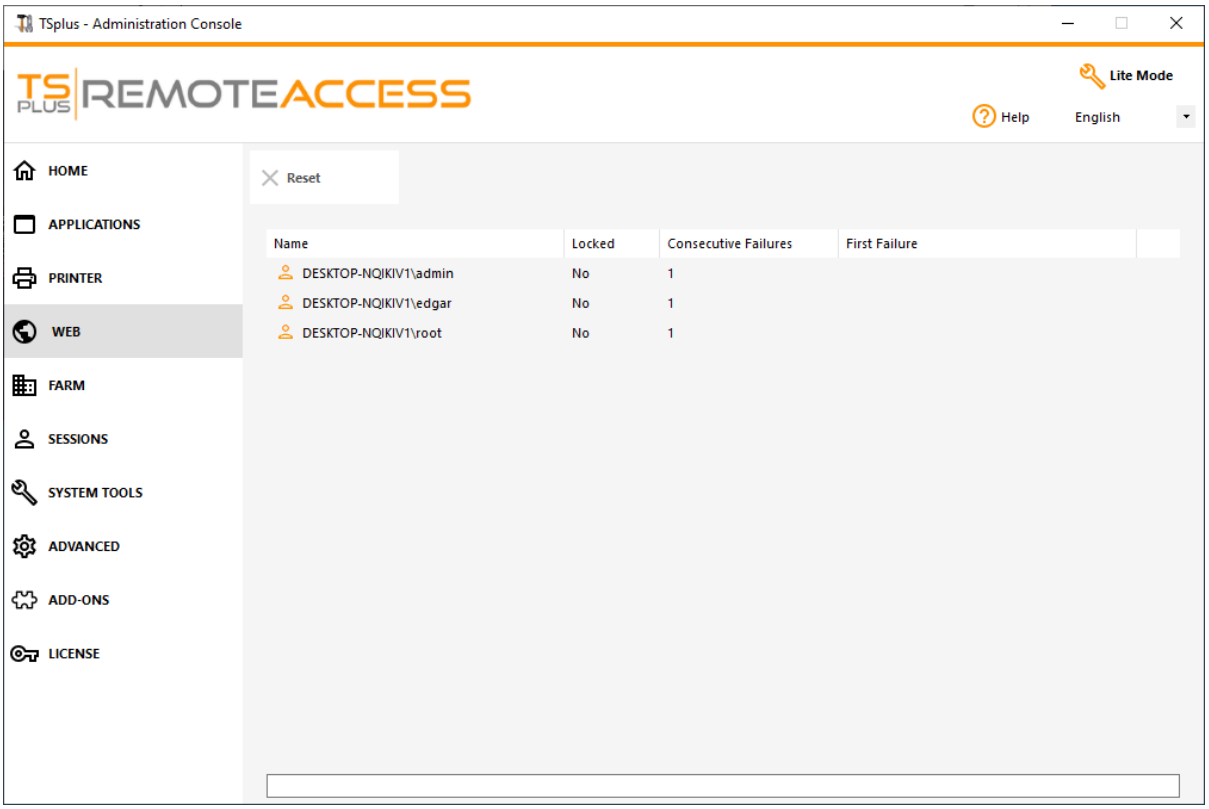
다음 제한 사항을 유의하시기 바랍니다:

- ’[’, ’]’ 및 ’°’ 문자는 비밀번호 필드에서 지원되지 않습니다.
- 안에 농장 / 게이트웨이 구성 웹 자격 증명은 다음만 지원합니다. 로드 밸런싱 모드 (서버 할당 모드에서는 작동하지 않습니다.)
- 로드 밸런싱 모드의 Farm / Gateway 구성에서는 웹 자격 증명이 농장의 모든 서버에서 정의되어야 합니다.
- 2FA는 웹 자격 증명 기능과 호환되지 않습니다.

웹 잠금

TSplus 웹 잠금 해제는 버전 12.40과 함께 도입된 웹 포털 잠금 해제 기능의 사용자 인터페이스로, 계정을 잠금 해제하고 고급 설정을 편집할 수 있습니다.

HTML5 웹 포털 잠금 기능 구성 방법에 대한 FAQ

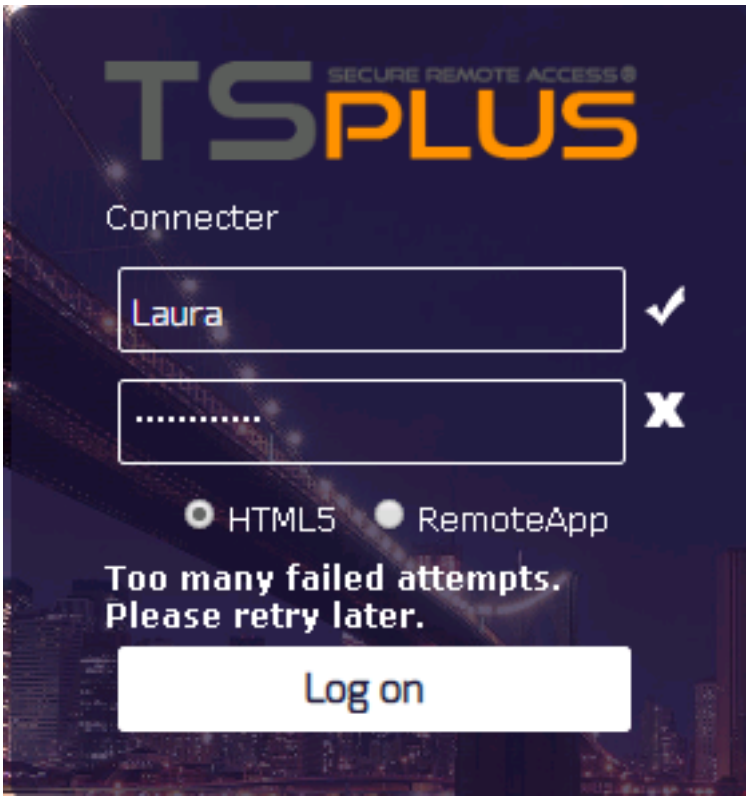


잠금 모니터는 TSplus 서버에서 웹 로그인 시도를 실패한 경우를 감시합니다. 시도를 기록하고 허용된 실패 시도 횟수에 도달한 후 해당 사용자를 자동으로 차단합니다.

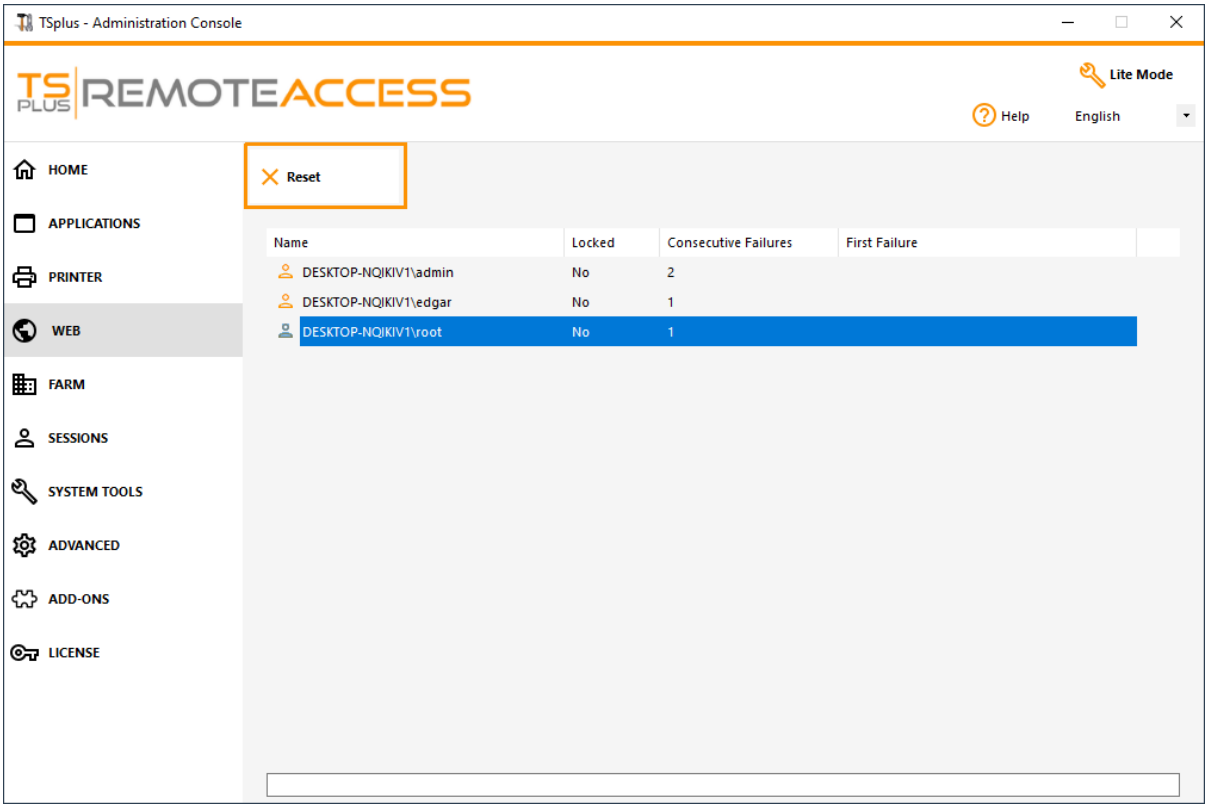
주소가 "잠금" 열 아래에 잠겨 있는지 쉽게 확인할 수 있습니다.

다음 열은 각 사용자에 대한 연속 실패 횟수를 나타냅니다.

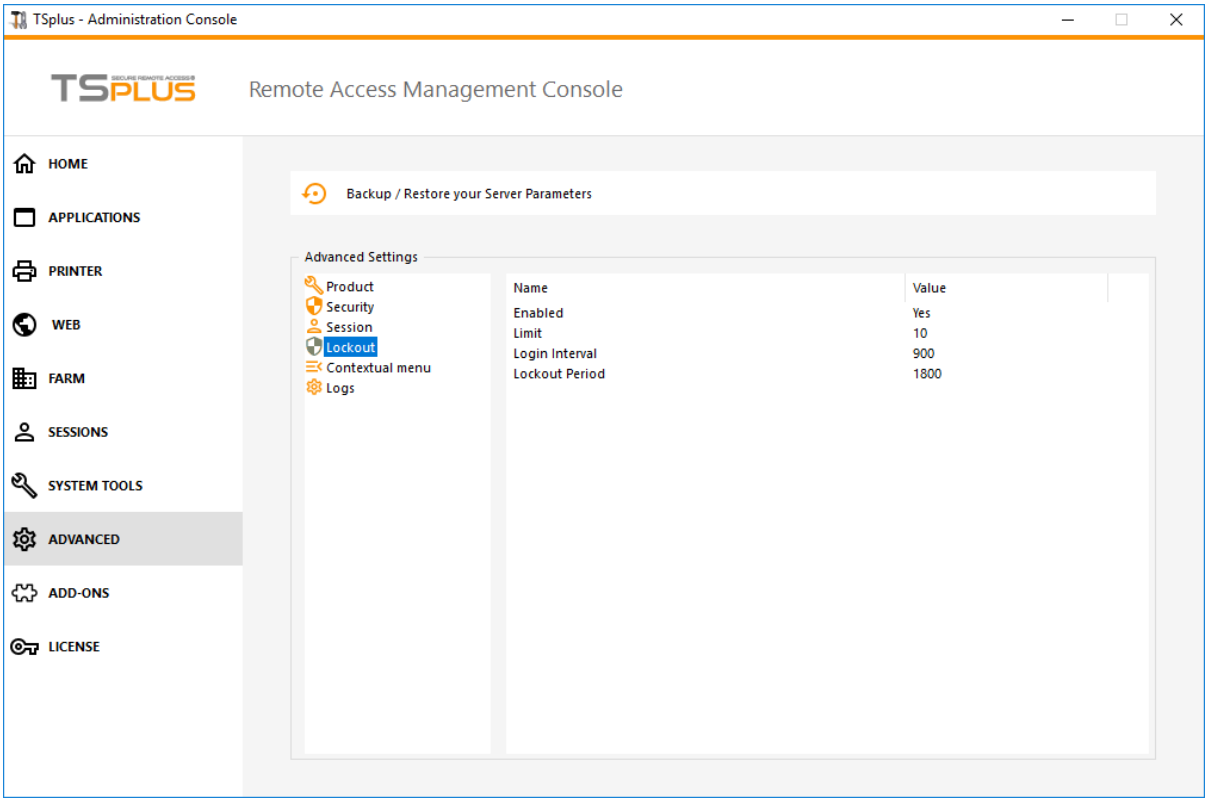
웹 포털에서 메시지가 사용자에게 너무 많은 실패한 시도가 있었음을 알립니다.



사용자는 AdminTool의 웹 탭에 있는 사용하기 쉬운 관리 콘솔에서 이 목록에서 신속하게 제거되고 차단 해제되며 화이트리스트에 추가될 수 있습니다. 재설정하거나 차단 해제하려는 사용자를 클릭한 다음 "재설정"을 클릭하기만 하면 됩니다.



사용자 차단 임계값은 관리자가 AdminTool의 고급 설정 탭에서 구성할 수 있습니다.



문서에서 잠금 설정을 구성하는 방법을 확인하세요.

TSplus 고급 보안 잠금 통합

웹 포털에서 로그인 실패 시도가 감지되면, TSplus Advanced Security가 이를 표시합니다. **"잠금 이벤트", 보안 이벤트 뷰어의 사용자 이름에 해당** :



“웹 포털에서 사용자 … 에 대한 로그인 실패 시도가 감지되었습니다. 이 사용자에 대해 1회의 로그인 실패 시도가 감지되었습니다…”

TSplus Advanced Security BruteForce Protection

TSplus Advanced Security Bruteforce Protection 포함합니다 **클라이언트 I.P. 주소 측면** 따라서 RDP 연결에도 작동합니다.

실패한 무차별 대입 연결 시도 TSplus Advanced Security 이벤트 로그에도 표시됩니다(프록시 차단을 피하기 위해 개인 IP 주소는 제외됨):



“IP 주소 … 에서 실패한 연결 시도가 감지되었습니다. 이 IP 주소는 화이트리스트에 없으며 여러 번의 연결 실패 후 차단됩니다. 제공된 사용자 이름: Harry.”

잠금 및 브루트포스 보호에 대한 자세한 정보는 확인하십시오. 이 문서 그리고 브루트포스 보호 문서

웹 로그인 페이지: 로그인 스플래시 화면 변경 방법

개요

원격 연결이 로딩 중일 때, HTML5 클라이언트는 아래 스크린샷과 같은 기본 스플래시 화면을 표시합니다.



이 콘텐츠는 JavaScript 구성 파일을 수정하여 사용자 정의할 수 있습니다.

HTML5 클라이언트

사용자 맞춤형 스플래시 스크린 콘텐츠 만들기

텍스트나 HTML의 모든 콘텐츠는 스플래시 스크린에 사용할 수 있습니다.

또한, 간단한 따옴표 (’) 또는 큰따옴표 (”)를 사용해야 하는 경우, 그냥 따옴표 대신 (’ 및 ”) 앞에 백슬래시를 써야 합니다.

마지막으로, 내용은 반드시 1줄로 작성되어야 합니다.

다음 예시는 스플래시 화면에 대한 유효한 콘텐츠입니다:

이것은 나의 맞춤형 스플래시 스크린입니다.

안녕하세요!
제목(“이것은 나의 맞춤형 스플래시 화면입니다.”), 텍스트(“안녕하세요!”) 및 표준 TSplus 스플래시 화면과 같은 애니메이션 링 그림이 표시됩니다.

자신의 콘텐츠를 사용하도록 스플래시 스크린 데이터를 수정하기

“C:\Program Files (x86)\TSplus\Clients\www\software\html5” 폴더에 “settings.js”라는 파일이 없다면, 귀하의 TSplus 버전이 오래된 것이며 이 문서는 적용되지 않습니다. 먼저 시스템을 업데이트하거나 지원팀에 문의하시기 바랍니다.

“C:\Program Files (x86)\TSplus\Clients\www\software\html5” 폴더에 위치한 “settings.js” 파일을 수정하십시오. Notepad 또는 Notepad++와 같은 텍스트 편집기를 사용하는 것이 좋습니다. 아니다 Word를 사용하세요.

이로 시작하는 줄을 검색하십시오:

W.splashscreencontent = ”

다음 줄로 완전히 교체하십시오:

W.splashscreencontent = “여기에 맞춤형 콘텐츠를 입력하세요”;

끝나는 큰따옴표와 세미콜론(”;)을 잊지 마세요.

HTML5에서 로그인 스플래시 화면의 지속 시간을 늘리고 싶다면, 밀리초 단위의 값을 수정하여 그렇게 할 수 있습니다.

W.splashscreentime = 5000; //스플래시 화면 재생 시간.

변경된 HTML 페이지를 저장한 후 브라우저의 캐시를 지우는 것을 권장합니다.

웹 로그인 페이지: 로그인 후 로그인 양식을 닫는 방법

개요

웹 로그인 페이지에서 사용자가 "로그온" 버튼을 클릭하면 선택한 클라이언트(HTML5 또는 Windows)가 새 브라우저 탭에서 열립니다.

때때로, 그리고 더 구체적으로는 Windows 클라이언트를 사용할 때, 사용자가 “로그온” 버튼을 다시 클릭하지 않도록 로그온 양식을 숨기고 싶을 수 있습니다.

사용하는 인터넷 브라우저에 따라 이 기본 동작을 변경하는 두 가지 선택이 있습니다. 두 솔루션 모두 JavaScript 파일을 수정해야 합니다.

솔루션 A: 로그온 탭 닫기 - 인터넷 익스플로러 전용

이 솔루션에서 사용자가 "로그온" 버튼을 클릭하면 선택한 클라이언트가 새 브라우저 탭에서 열리고 로그온 탭은 자동으로 닫힙니다. 인터넷 익스플로러 버전에 따라 사용자가 이 탭을 닫으려는 것을 확인하라는 작은 메시지 창이 표시될 수 있습니다.

“C:\Program Files (x86)\TSplus\Clients\www\software” 폴더에 저장된 “common.js” 파일을 수정하십시오. Notepad 또는 Notepad++와 같은 텍스트 편집기를 사용하는 것이 좋습니다. 아니다 Word를 사용하세요.

이 줄을 검색하세요:

```
 p = 'software/remoteapp.html';
 window.name = " " + window.opforfalse;
 if (cpwin != false) {
```

```
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
 } else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
 }
```

그리고 그것들을 다음 줄로 교체하십시오:

```
 p = 'software/remoteapp.html';
 window.name = " " + window.opforfalse;
 if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
 } else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
 }
 window.open('','_parent','');
 window.close();
```

변경된 JavaScript 파일을 저장한 후 브라우저의 캐시를 지우는 것을 권장합니다.

솔루션 B: 로그온 탭을 다른 웹 페이지로 리디렉션 - 모든 브라우저용

이 솔루션에서 사용자가 "로그온" 버튼을 클릭하면 선택한 클라이언트가 새 브라우저 탭에서 열리

고 로그온 탭이 자동으로 다른 웹 페이지로 이동합니다.

귀하가 “와 같은 기존 인터넷 주소(URL)를 자유롭게 사용할 수 있습니다. http://google.com ” 또는 “http://your_intranet/your/page.html” 또는 “thankyou.html”을 URL로 사용하여 자신의 웹 페이지를 만들고 “C:\Program Files (x86)\TSplus\Clients\www” 폴더에 “thankyou.html”이라는 파일을 생성하고 그 안에 HTML 콘텐츠를 넣을 수 있습니다.

“C:\Program Files (x86)\TSplus\Clients\www\software” 폴더에 저장된 “common.js” 파일을 수정하십시오. Notepad 또는 Notepad++와 같은 텍스트 편집기를 사용하는 것이 좋습니다. 아니다 Word를 사용하세요.

이 줄을 검색하세요:

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
```

그리고 그것들을 다음 줄로 교체하십시오:

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
```

```
}
window.location.href = "http://google.com";
```

변경된 JavaScript 파일을 저장한 후 브라우저의 캐시를 지우는 것을 권장합니다.

웹 로그인 페이지: HTML5 클라이언트를 동일한 탭에서 여는 방법

개요

웹 로그인 페이지에서 사용자가 "로그온" 버튼을 클릭하면 HTML5 클라이언트가 새 브라우저 탭에서 열립니다.

이 동작을 변경하고 HTML5 클라이언트가 웹 로그인 페이지와 동일한 브라우저 탭에서 열리도록 JavaScript 파일을 수정할 수 있습니다.

custom.js 파일 수정

“C:\Program Files (x86)\TSplus\Clients\www” 폴더에 저장된 “custom.js” 파일을 수정하십시오. Notepad 또는 Notepad++와 같은 텍스트 편집기를 사용하는 것이 좋습니다. 아니다 Word를 사용하세요.

이 줄을 추가하세요:

var openinsamewindow = true;

변경된 JavaScript 파일을 저장한 후 브라우저의 캐시를 지우는 것을 권장합니다.

common_applications.js 파일 수정

터미널 서비스 플러스 웹 애플리케이션 포털 기능을 사용하고 있다면, 두 번째 파일을 수정해야 합니다. “C:\Program Files (x86)\TSplus\Clients\www\software” 폴더에 저장된 “common_applications.js” 파일을 수정하세요. 메모장이나 Notepad++와 같은 텍스트 편집기를 사용하는 것을 권장합니다. 아니다 Word를 사용하세요.

이 줄을 검색하세요:

```
if (childurl != '') {
  window.name = childname;
  location.href = childurl + '#';
}
```

그리고 그것들을 다음 줄로 교체하십시오:

```
  if (childurl != '') {
    window.name = childname;
    location.href = childurl + '#';
  }
```

변경된 JavaScript 파일을 저장한 후 브라우저의 캐시를 지우는 것을 권장합니다.

SSO(베타) 웹 포털

주요 전제 조건 및 제한 사항

Web Portal 2026은 SSO를 위해 설계되었습니다. **창의적인** 테마와 사용은 AdminTool > 웹 > 웹 포털 사용자 정의에서 모든 사용자 지정을 사용합니다. 선택한 테마가 아닐 경우 **창의적인** 웹 포털은 표시되지 않습니다.

농장에서 활성화되면 모든 서버는 실행해야 합니다. **같은 Remote Access 버전** 및 활성화되도록 **웹 포털 2026과 SSO**

이 기능은 **베타** 그리고 해야 합니다 **아니다** 생산 서버에 배포됩니다.

새로운 웹 포털이 필요한 이유는 무엇인가요?

이전 웹 포털과 비교할 때, 이 구현은 더 높은 신뢰성과 더 나은 성능을 제공합니다. 또한, 다음을 허용합니다:

- **고급 SSO 기능**
  - Windows 통합 인증 (Negotiate / Kerberos / NTLM)
  - 타사 아이덴티티 공급자 통합 (현재 SAML)
- **더 강력한 보안 제어**
  - 내장된 위조 방지 보호 기능
  - 엔드포인트 속도 제한
  - 현대 인증 및 쿠키/세션 제어

그 구조는 우리가 잠재적인 보안 감사 피드백을 쉽게 처리할 수 있도록 해줄 것입니다.

또한 이것은 **더 접근 가능한 제품** 추천 및 향상된 대비를 통해.

웹 서버 유연성 (기본값: Kestrel)

애플리케이션은 하나의 프론트엔드 웹 서버에 묶여 있지 않습니다. 기본적으로, 그것은 실행됩니다. **케스트렐** (HTTP 포트 81). 앞에 있을 수 있습니다. **IIS** 또는 **아파치** 웹 서버 구성을 변경하여 리버스 프록시로.

예: 웹 포털 서비스에 대한 아파치 리버스 프록시

```
# Apache VirtualHost example
ProxyPreserveHost On
ProxyPass        /  http://127.0.0.1:81/
ProxyPassReverse /  http://127.0.0.1:81/

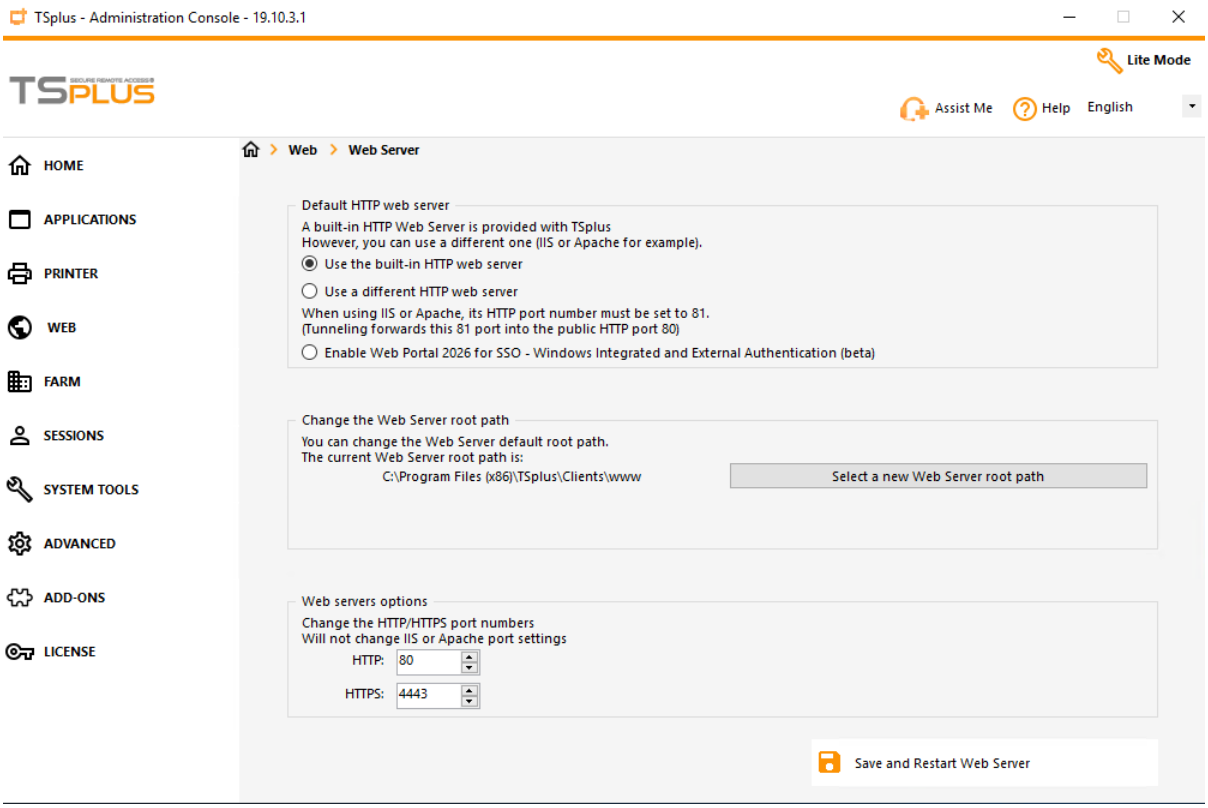
RequestHeader set X-Forwarded-Proto "https"
RequestHeader set X-Forwarded-For "%{REMOTE_ADDR}s"
```

이것은 Apache가 공용 HTTP/HTTPS 노출을 처리하는 동안 Web Portal 논리를 변경하지 않습니다.

개발 팀에 문의해 주시기 바랍니다. 이 시나리오는 아직 AdminTool 프로그램에서 접근할 수 없으며 수동으로 구성해야 합니다.

SSO로 2026년 웹 포털 활성화

1. 열기 **관리 도구**
2. 웹 > 웹 서버로 이동
3. 활성화: **SSO가 포함된 웹 포털 2026**



중요한 이 옵션은 베타입니다. 테스트 환경에서만 사용하십시오.

지원되는 로그인 모드

SSO를 지원하는 2026 웹 포털:

- Windows 자격 증명을 사용하는 전통적인 로그인 양식
- 웹 자격 증명. 참조: https://docs.tsplus.net/tsplus/web-credentials/
- Windows 통합 인증 (신뢰할 수 있는 / 로컬 시나리오에서 자동)
- 외부 아이덴티티 공급자를 통해 **SAML** 엔트라 ID(이전 Azure AD) 또는 옥타

외부 인증을 통한 지원에 대한 참고: **OIDC** 나중에 계획됨, 요청 시

2FA 동작

2FA는 다음을 포함한 표준 계정 흐름에 적용됩니다:

- Windows 자격 증명을 사용하는 로그인 양식
- 웹 자격 증명
- 윈도우 통합 인증

외부 인증 제공자는 종종 자체 MFA / 2FA를 적용합니다. 따라서 Remote Access 2FA 애드온에서

설정된 2FA 구성은 이 시나리오에 적용되지 않습니다.

로컬 네트워크 우회는 다음을 통해 가능합니다. CustomSettings:로컬 네트워크에 대한 2단계 인증 우회 파일에 위치한 매개변수: C:\Program Files (x86)\TSplus\Clients\webportal\appsettings.json 어디에 C:\Program Files (x86)\TSplus TSplus Remote Access 설정 폴더입니다. 활성화되면 클라이언트와 게이트웨이가 동일한 개인 서브넷에 있을 때만 우회가 발생합니다.

Windows 인증 흐름 구성

Windows 인증으로 로그인하는 사용자에게는 다음 중 하나가 필요합니다:

1. TSplus 명령어로 자격 증명 사전 등록: AdminTool.exe /windowscredential-addorupdate 문서를 참조하십시오. https://docs.tsplus.net/tsplus/commands-list/#add-or-update-credentials-to-the-windows-credentials-manager-windowscredential-addorupdate
2. 사용자가 Windows 자격 증명을 사용하여 웹 포털 로그인 양식을 통해 한 번 로그인하도록 허용합니다.

Windows 통합 인증을 구성하려면 다음을 참조하십시오: Active Directory 도메인에서 Windows 통합 인증 활성화. 이 인증 모드는 구성하기 어려운 경우가 많아 고객들은 종종 외부 신원 공급자를 설정하는 것을 선호합니다.

외부 인증 구성 (SAML)

외부 애플리케이션에 대한 필수 설정

외부 애플리케이션은 다음과 같이 구성되어야 합니다:

- 싱글 사인온 URL 웹 포털 SAML 소비자 서비스 엔드포인트로 설정해야 합니다. 예: https://mywebportal.company.com/Saml/acs
- 청중 URI (SP 엔티티 ID) 웹 포털 도메인 이름 또는 IP 주소로 설정해야 합니다. 예: https://mywebportal.company.com
- 이름 ID 형식 설정해야 합니다 **이메일 주소**
- 응용 프로그램 사용자 이름 설정해야 합니다 **이메일** , 왼쪽 부분은 Windows 계정 사용자 이름을 식별합니다.

필수 설정 사항 appsettings.json

파일 appsettings.json 위치해 있습니다 C:\Program Files (x86)\TSplus\Clients\webportal 어디에 C:\Program Files (x86)\TSplus TSplus Remote Access 설정 폴더입니다.

편집하다 Saml2 섹션:

- IdP메타데이터
- 발급자
- 싱글사인온대상 선택 사항(메타데이터가 제공하는 경우)
- 단일 로그아웃 대상 선택 사항(메타데이터가 제공하는 경우)
- 인증서 관련 필드

예를 들어, 제3자 신원 제공자 okta를 사용하여:


```
"Saml2": {
  "IdPMetadata": "https://mycompany.okta.com/app/abcdfegh12345678/sso/saml/metadata",
  "Issuer": "https://portal.mycompany.com",
  "SingleSignOnDestination": "https://mycompany.okta.com/app/mycompany_portalsaml_1/
abcdfegh12345678/sso/saml",
  "SingleLogoutDestination": "https://mycompany.okta.com",
  "SignatureAlgorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256",
  "SigningCertificateFile": "",
  "SigningCertificatePassword": "",
  "SignatureValidationCertificateFile": "okta.identity.saml2.portal.cert",
  "CertificateValidationMode": "ChainTrust",
  "RevocationMode": "Offline",
  "XmlCanonicalizationMethod": "http://www.w3.org/2001/10/xml-exc-c14n#"
}
```


발급자 설정은 외부 신원 공급자 측에서 정의된 대상을 URI로 설정합니다.

만약 서명 유효성 검사 인증서 파일 설정이 다른 값으로 설정되어 있습니다. **없음** 그런 다음 인증서가 애플리케이션 서버에서 유효한 것으로 간주되는지 확인하십시오. 이를 위해 인증서를 신뢰할 수 있는 인증서 목록에 추가해야 할 수 있습니다.

세션 시작을 위한 Windows 비밀번호 가용성

외부 SAML 인증의 경우, 세션을 시작하려면 여전히 사용 가능한 Windows 자격 증명이 필요합니다. 다음 중 하나를 사용하십시오:

1. Windows 자격 증명을 명령어로 등록: AdminTool.exe /windowscredential-addorupdate 문서를 참조하십시오. https://docs.tsplus.net/tsplus/commands-list/#add-or-update-credentials-to-the-windows-credentials-manager-windowscredential-addorupdate
2. IdP 클레임을 설정하여 비밀번호를 전달합니다. 사용자 정의 설정: SAML 비밀번호 클레임 사용 Windows 비밀번호가 포함된 청구 유형으로.

일반적으로 웹 포털은 사용자 이메일 주소의 '@' 이전 부분을 Windows 계정의 사용자 이름으로 사용합니다.

현재 외부 인증은 로컬 사용자와 함께 작동합니다.

비밀번호가 클레임 또는 자격 증명 저장소에서 사용할 수 없는 경우 사용자 검증이 실패합니다.

appsettings.json 구성 파일 참조 전체

파일 appsettings.json 위치해 있습니다 C:\Program Files (x86)\TSplus\Clients\webportal 어디에 C:\Program Files (x86)\TSplus TSplus Remote Access 설정 폴더입니다.

로그인

매개변수	목적	가능한 값	기본값
로깅:로그레벨:기본	전역 최소 로그 수준.	추적 , 디버그 , 정보 , 경고 , 오류 , 중요 , 없음	정보
로깅:로그레벨:Microsoft.AspNetCore	ASP.NET Core 프레임워크 로그 수준.	위와 동일함	경고
로깅:로그 수준:Microsoft.AspNetCore.Authentication	인증 하위 시스템 로그 수준.	위와 동일함	경고

글로벌 호스트 설정

매개변수	목적	가능한 값	기본값
허용된 호스트	ASP.NET Core 호스트 보호를 위한 호스트 헤더 필터링.	* (모든) 또는 세미콜론으로 구분된 호스트 목록	*

IP 속도 제한

매개변수	목적	가능한 값	기본값
IpRateLimiting:EnableEndpointRateLimiting	엔드포인트별 스로틀링 규칙을 활성화합니다.	참된 / 거짓	참된
IpRateLimiting:StackBlockedRequests	만약 참된 차단된 요청이 계속해서 카운터를 증가시키고 있습니다.	참된 / 거짓	거짓
IpRateLimiting:HttpStatusCode	요청이 차단될 때 반환되는 HTTP 상태.	정수 HTTP 코드 (일반적으로 429)	429
IpRateLimiting:RealIpHeader	프록시 뒤에 있는 클라이언트 IP를 해결하는 데 사용되는 헤더.	헤더 이름	X-Forwarded-For
IpRateLimiting:ClientIdHeader	사용자 정의 요금 제한을 위한 선택적 클라이언트 ID 헤더.	헤더 이름	X-ClientId

IpRateLimiting:일반규칙

각 규칙 객체에는 다음이 포함됩니다:

매개변수	목적	가능한 값	배송된 파일의 기본값
엔드포인트	경로/메서드 패턴 보호.	형식 VERB:/경로	여러 기본값(아래 참조)
기간	요금 창.	예: 1초 , 1m , 5분 , 1시간 , 1일	5분 모든 기본 규칙에 대해
한계	기간 내 최대 요청 수.	양의 정수	5 모든 기본 규칙에 대해

Saml2

매개변수	목적	가능한 값	기본값
Saml2:IdPMetadata	SAML 공급자 구성을 로드하는 데 사용되는 IdP 메타데이터 URL.	유효한 HTTPS URL	""
Saml2:발급자	SP 엔터티 ID	URI 문자열	""

	(이 웹 포털 ID).		
Saml2:SingleSignOnDestination	IdP SSO 엔드 포인트 URL(메타데이터에서 자동으로 해결될 수 있음).	HTTPS URL	""
Saml2:SingleLogoutDestination	IdP SLO 엔드 포인트 URL(메타데이터에서 자동으로 해결될 수 있음).	HTTPS URL	""
Saml2:서명알고리즘	XML 서명 알고리즘.	SAML 라이브러리에서 수락된 URI 값	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Saml2:서명인증서파일	로컬 SP 서명 인증서 파일(앱 기본 경로에 상대적).	파일 이름/경로	""
Saml2:서명인증서비밀번호	서명 인증서 파일의 비밀번호.	문자열	""
Saml2:서명유효성검증인증서파일	IdP 인증서 파일은 서명을 검증하는 데 사용됩니다(메타데이터가 인증서를 제공하는 경우 선택 사항).	파일 이름/경로	""
Saml2:인증서검증모드	인증서 체인 검증 모드.	없음 , 피어 트러스트 , 체인트러스트 , 피어 또는 체인 신뢰 , 사용자 정의 루트 신뢰	체인트러스트
Saml2:철회모드	인증서 폐기 동작.	노체크 , 온라인 , 오프라인	오프라인
Saml2:XmlCanonicalizationMethod	XML 정규화 알고리즘 URI.	XML-DSig 정규화 URI	http://www.w3.org/2001/10/xml-exc-c14n#

사용자 정의 설정

안에 appsettings.json 이 값들은 문자열로 저장됩니다. 참된 / 거짓) 및 .NET 구성 바인딩에 의해 부울로 매핑됩니다.

매개변수	목적	가능한 값	기본값
사용자 정의 설정: 애플리케이션 전체 경로 사용	애플리케이션 전체 경로가 할당된 앱을 나열하거나 실행할 때 사용되는지 여부를 제어합니다.	참된 / 거짓	거짓
CustomSettings:로컬호스트에서자동Windows인증사용가능	로컬호스트/루프백 시나리오에서 자동 Windows 인증을 허용합니다.	참된 / 거짓	거짓
사용자 정의 설정: 비밀번호 암호화 활성화	HTML5 시작 연결 문자열에서 RSA 매개변수를 사용하여 도메인/사용자 이름/비밀번호를 암호화합니다.	참된 / 거짓	참된
CustomSettings:로컬 네트워크에 대한 2단계 인증 우회	클라이언트가 서버와 동일한 개인 서브넷에 있을 때 웹 포털 2FA를 우회합니다.	참된 / 거짓	거짓
사용자 정의 설정: SAML 비밀번호 클레임 사용	세션 시작을 위한 전달된 Windows 비밀번호로 사용되는 SAML 클레임 유형.	청구 유형 URI/이름 또는 빈 문자열	""

문제 해결

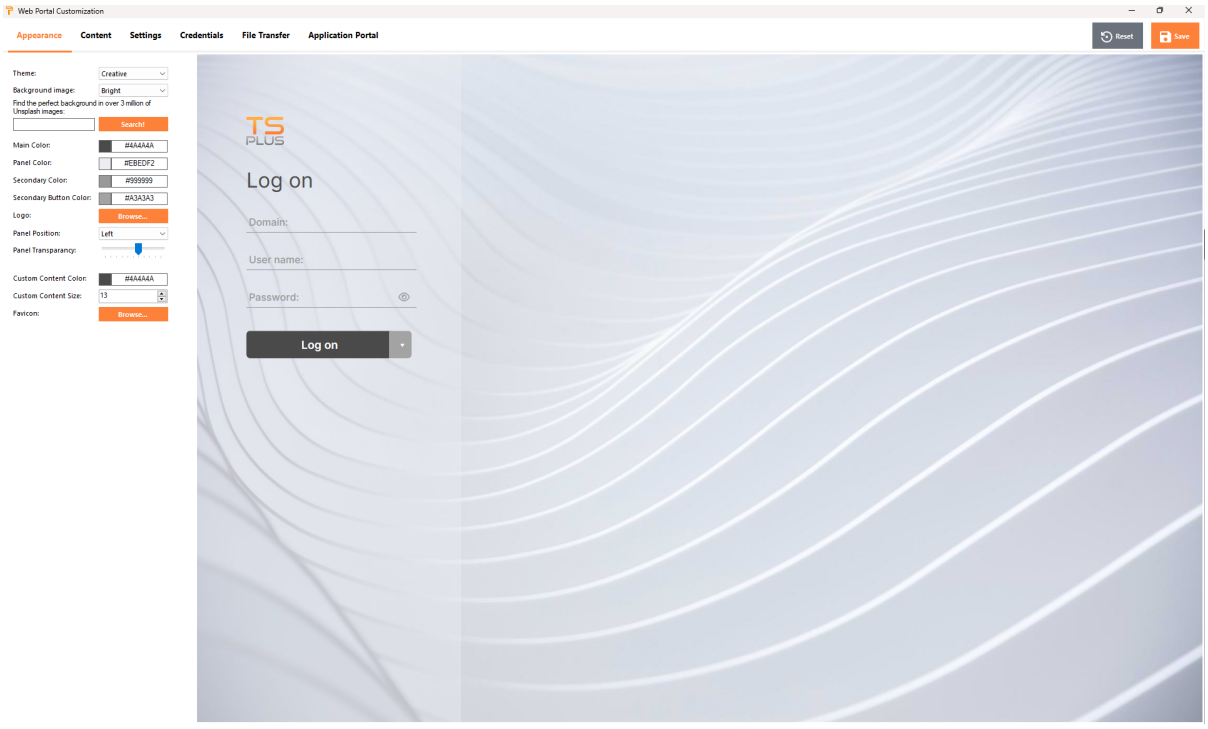
Web Portal 2026에서 SSO 로그는 AdminTool > 고급 > 로그 > 웹 포털 로그에서 활성화할 수 있습니다.

결과적으로 WebPortal.log 로그 파일은 다음 위치에 있습니다. C:\Program Files (x86)\TSplus\Clients\webportal 어디에 C:\Program Files (x86)\TSplus TSplus Remote Access 설정 폴더입니다.

웹 포털 사용자 지정을 사용하여 HTML 웹 액세스 페이지 만들기 및 사용자 지정

웹 포털 사용자 지정을 사용하면 자신만의 맞춤형 HTML 웹 액세스 페이지를 만들 수 있습니다 - 그리고 있습니다. 웹 개발자가 될 필요는 없습니다. !

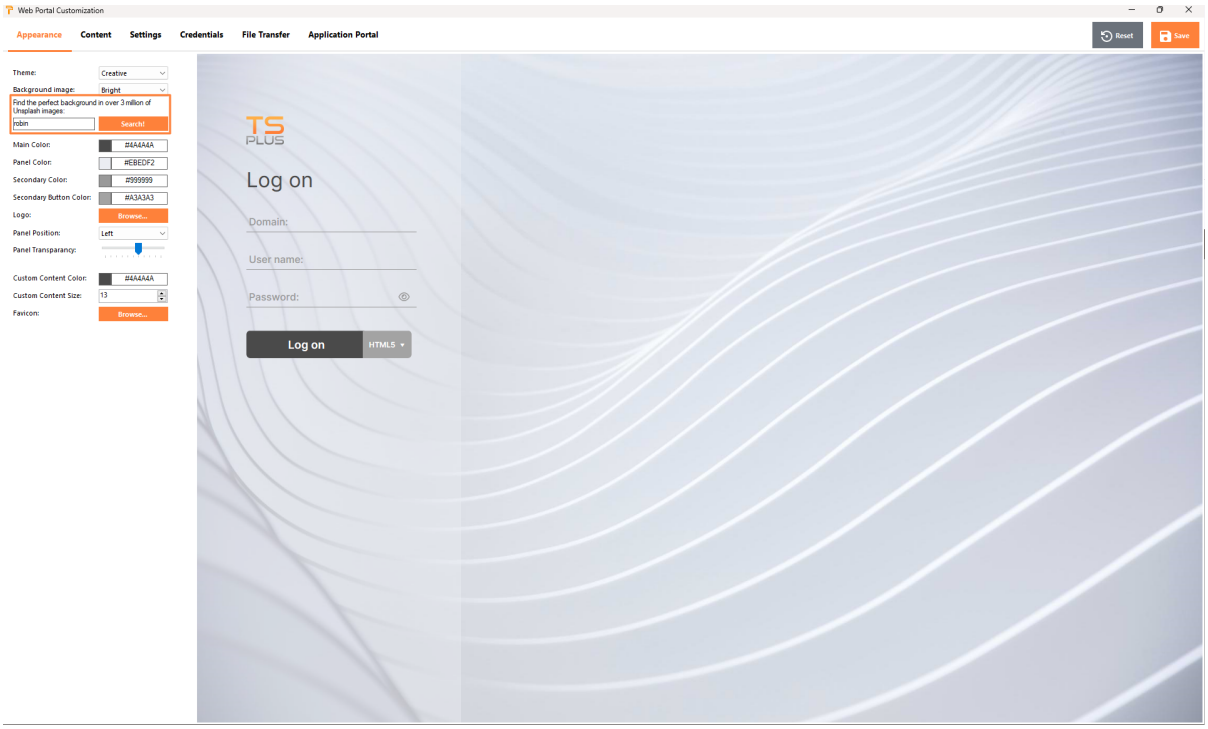
웹 포털 사용자 정의 - 외관



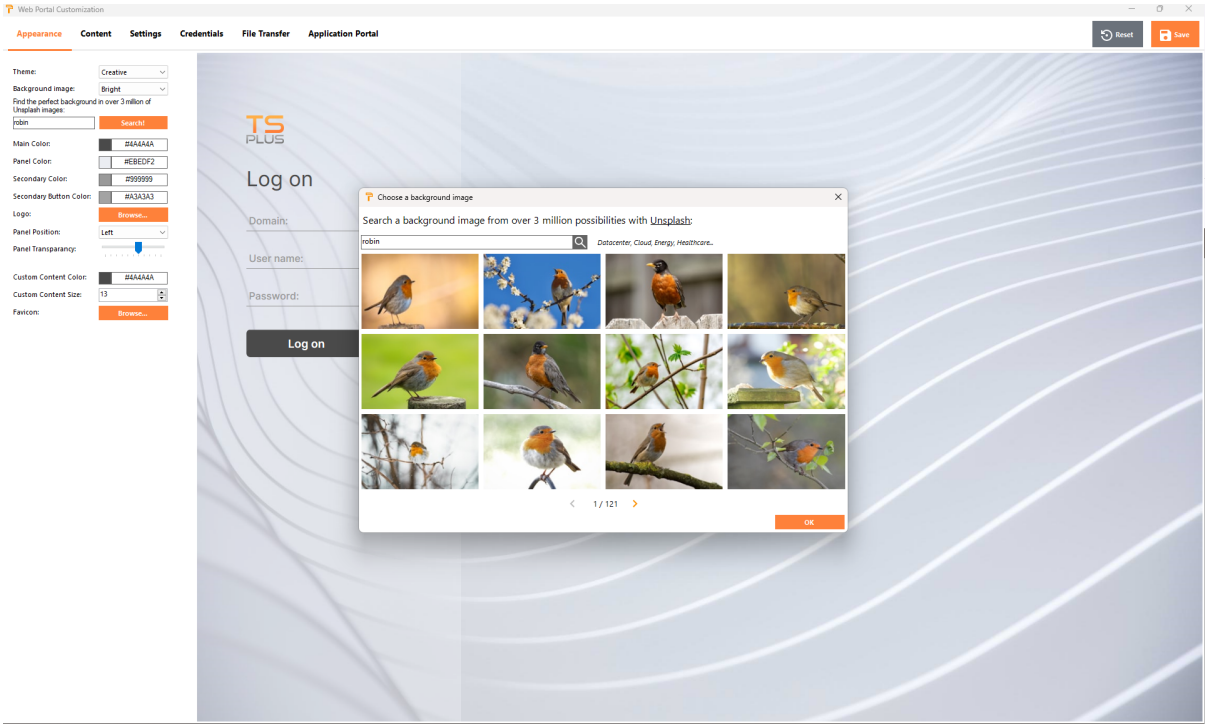
모양 탭을 사용하면 모든 그래픽 설정을 사용자 정의하고 자신의 로고를 추가할 수 있습니다.

사진 모음 중에서 선택하거나 직접 추가할 수 있습니다. 원하는 배경색으로 색상 테마를 설정하거나 클래식 테마 중 하나를 사용할 수도 있습니다.

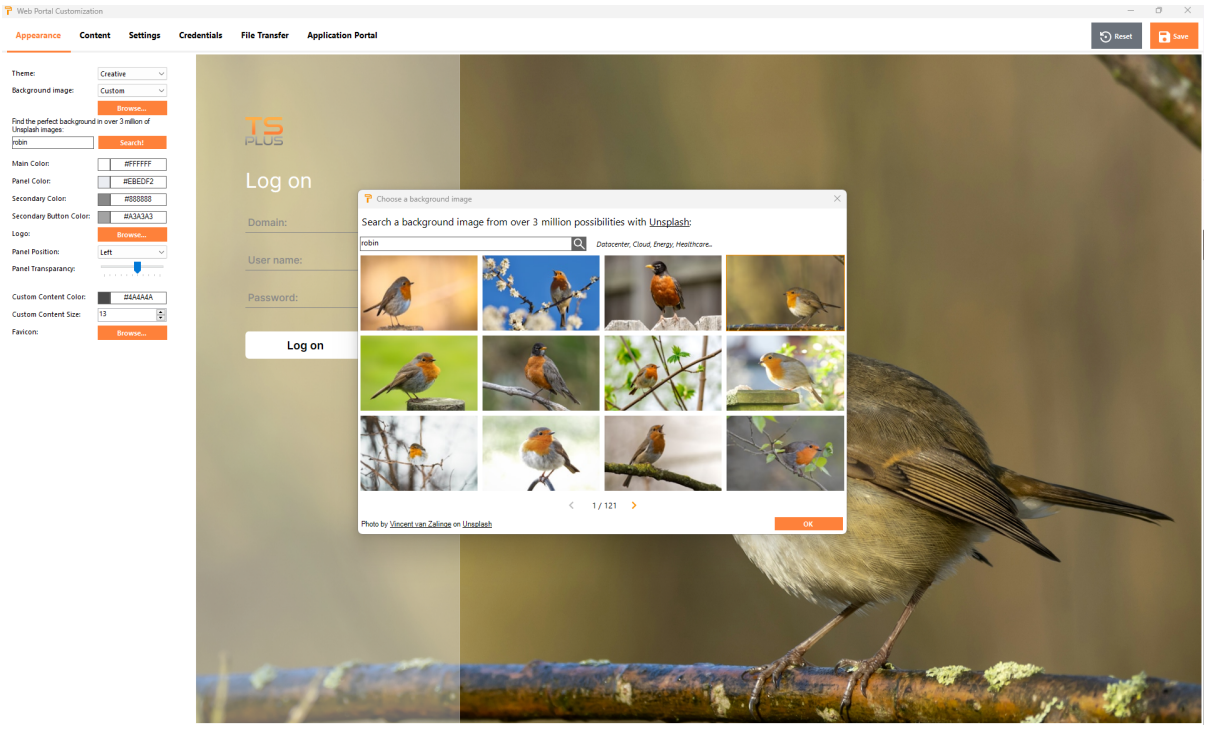
배경 이미지를 Unsplash 라이브러리에서 검색하려면 키워드를 입력할 수도 있습니다.



이미지 선택을 위한 모음을 표시하겠습니다.

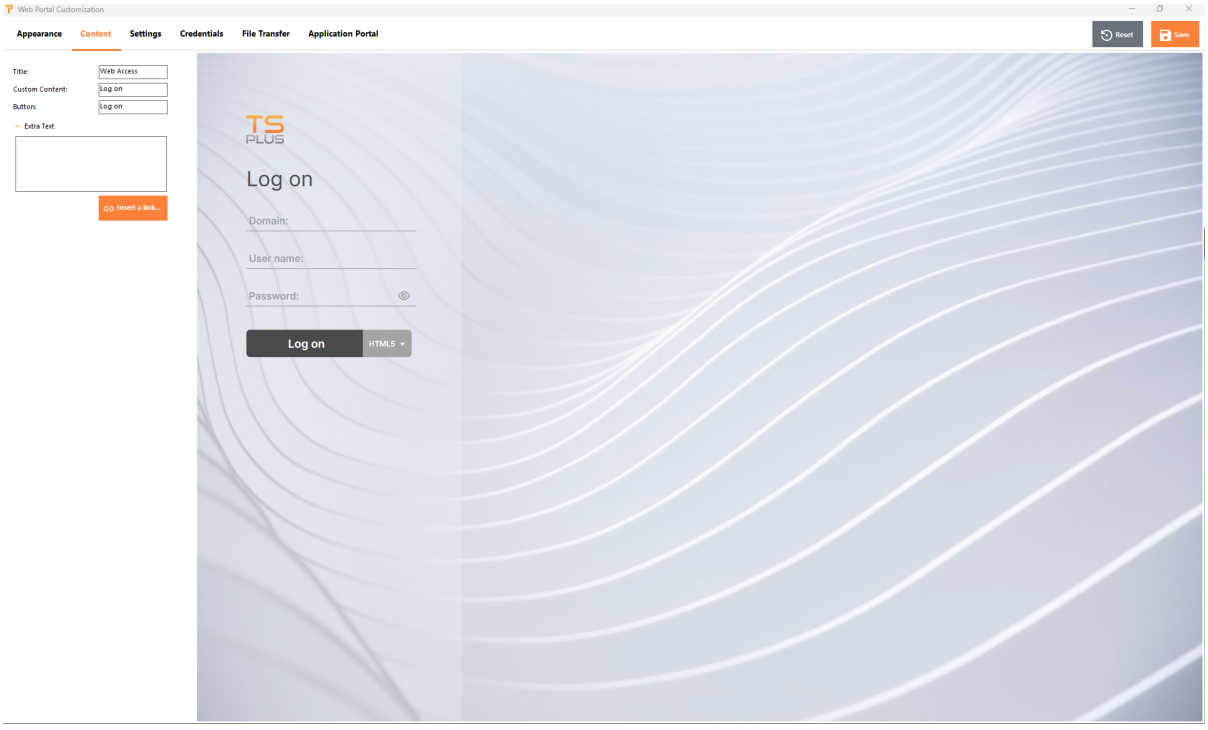


좋아하는 사진을 선택하여 웹 포털에서 결과를 확인하세요:

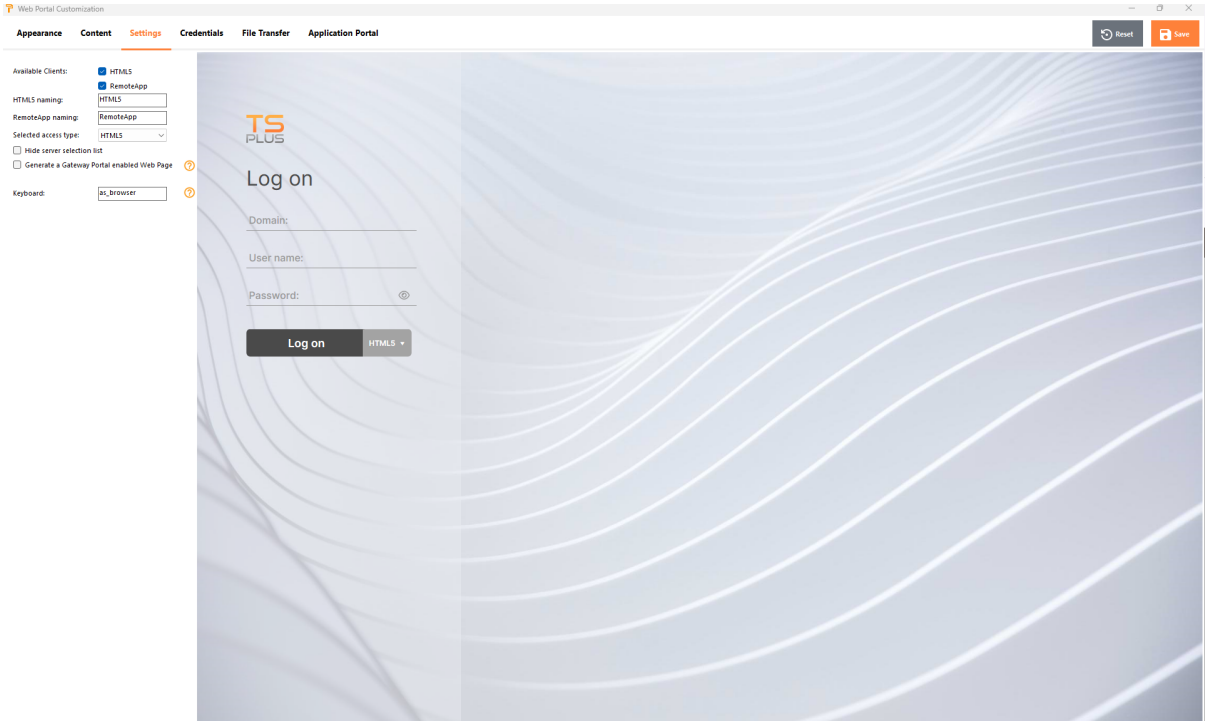


테마 색상은 "확인" 버튼으로 선택을 확인하면 선택한 그림에 자동으로 적응합니다. 물론 원하시는 대로 색상을 개인화할 수도 있습니다.

웹 포털 사용자 정의 - 콘텐츠

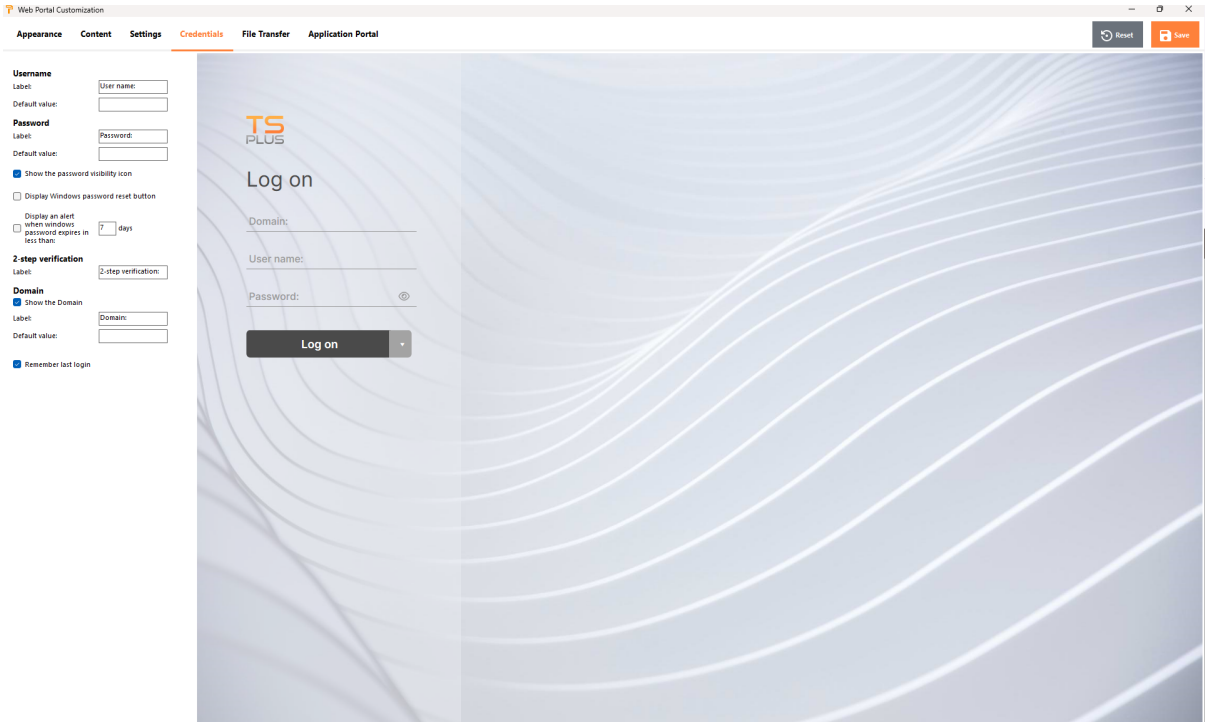


웹 포털 사용자 정의 - 설정

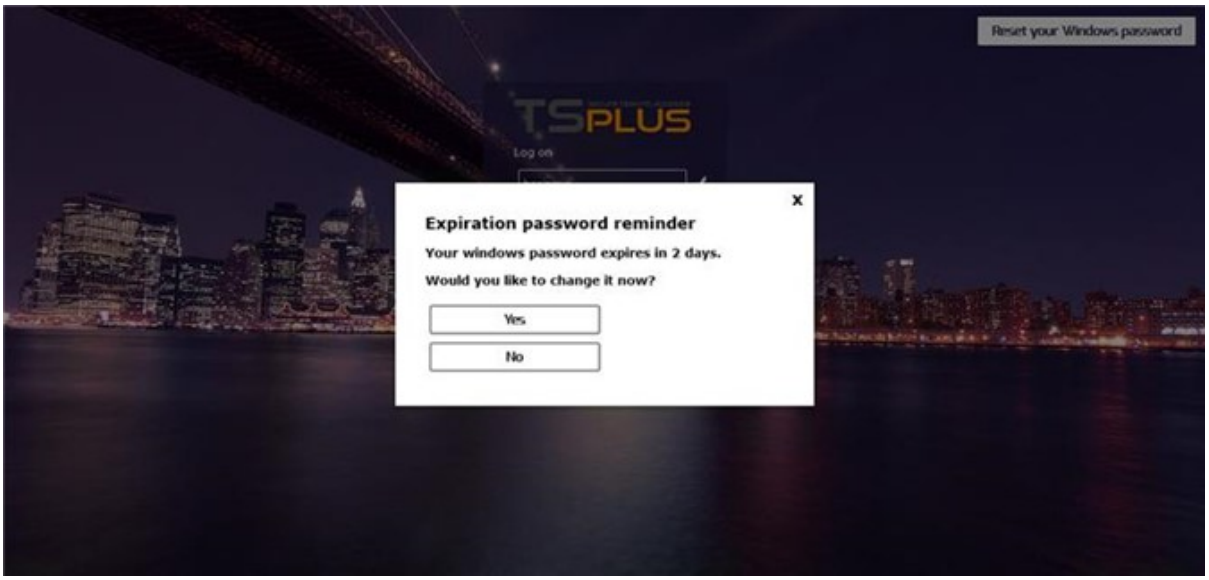


- “ **사용 가능한 클라이언트** 2종의 웹 연결 클라이언트 중에서 선택하세요. 두 가지 모두 선택하면 사용자가 선택할 수 있습니다. 이러한 옵션에 사용되는 이름은 웹 포털에서 변경할 수 있습니다. 두 옵션이 모두 사용 가능한 경우 기본적으로 선택할 옵션도 선택할 수 있습니다.
- “ **게이트웨이 포털** 게이트웨이 포털이 활성화된 페이지를 활성화하려면 확인하십시오. 이 기능은 서버를 사용자 또는 그룹에 할당할 때 추가 인증 단계를 추가합니다.
- “ **키보드** 고급 키보드 요구 사항이 있는 고급 관리자만을 위한 것입니다.

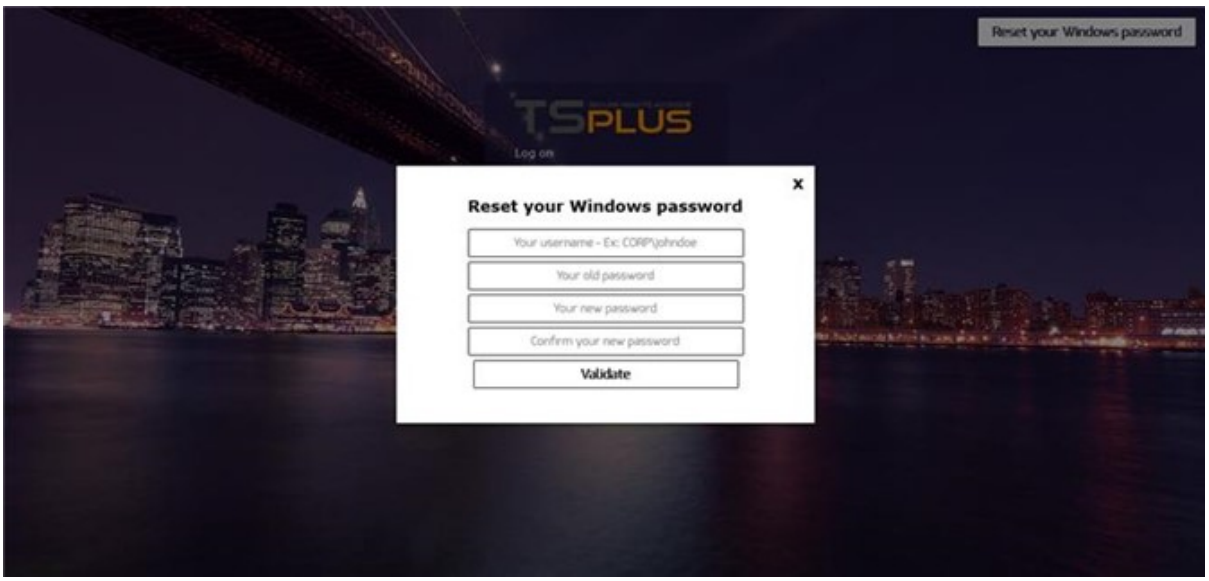
웹 포털 사용자 정의 - 자격 증명



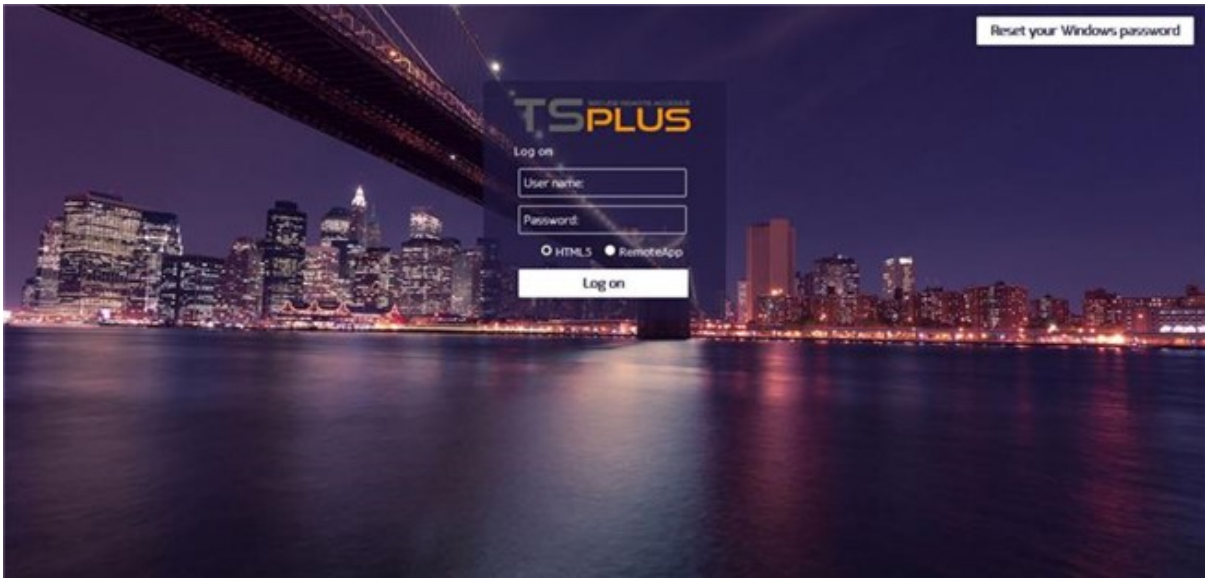
- “ **라벨** 사용자 이름, 비밀번호 등을 지정하는 데 사용되는 텍스트를 변경할 수 있습니다.
- “ **기본값** 기본 로그인, 비밀번호 및 도메인을 지정하여 로그인 필드를 자동으로 채울 수 있습니다. 여기 있는 모든 설정은 index.html 파일에 저장되며, 이 파일은 복사하여 원하는 대로 이름을 변경할 수 있습니다.
- “ **도메인 필드 표시** : 체크하면 도메인 필드가 로그인 정보 요청에 포함됩니다.
- “ **비밀번호** ”: 웹 포털을 통해 연결하는 동안 사용자에게 비밀번호 만료 날짜에 대한 정보를 제공하는 경고 메시지를 추가할 수 있습니다. 예를 들어, 사용자의 Windows 비밀번호가 3일 이내에 만료되면 다음과 같은 팝업이 표시됩니다.



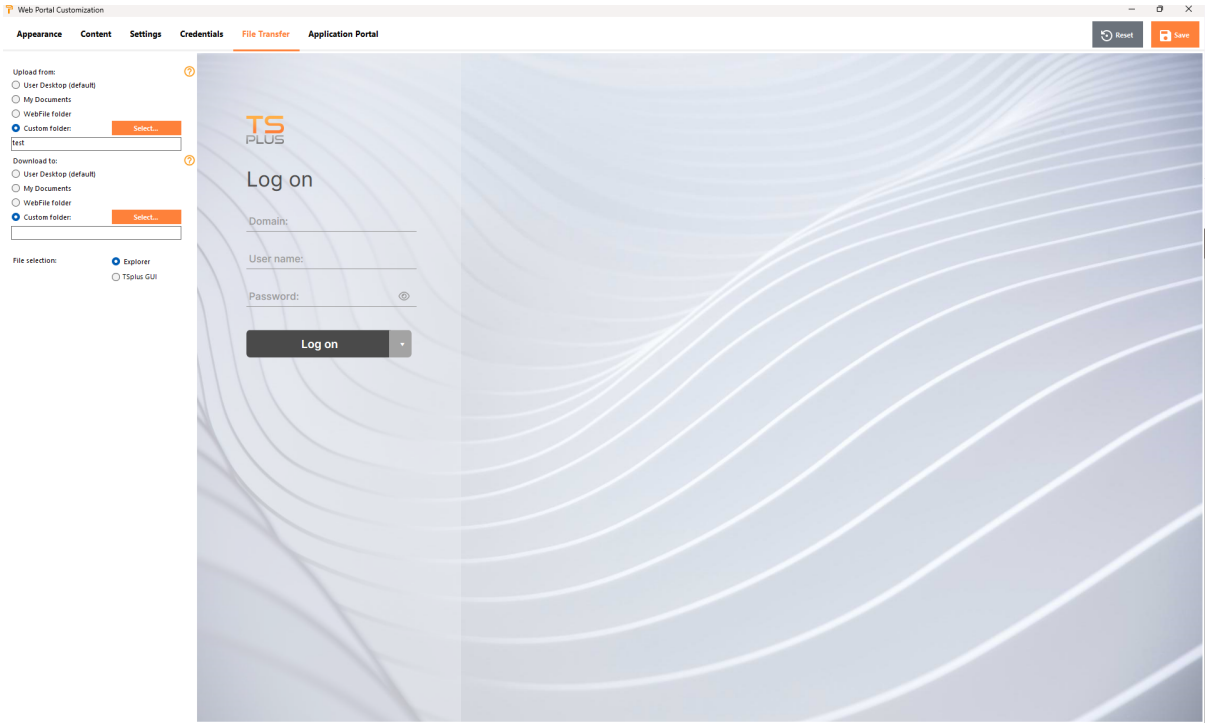
언급한 바와 같이, 그는 바로 아래에 표시된 팝업을 사용하여 웹 포털에서 직접 변경할 수 있는 가능성을 제공합니다.



사용자가 언제든지 자신의 Windows를 변경할 수 있도록 하려면 "Windows 비밀번호 재설정 버튼 표시" 옵션을 선택하면 됩니다.

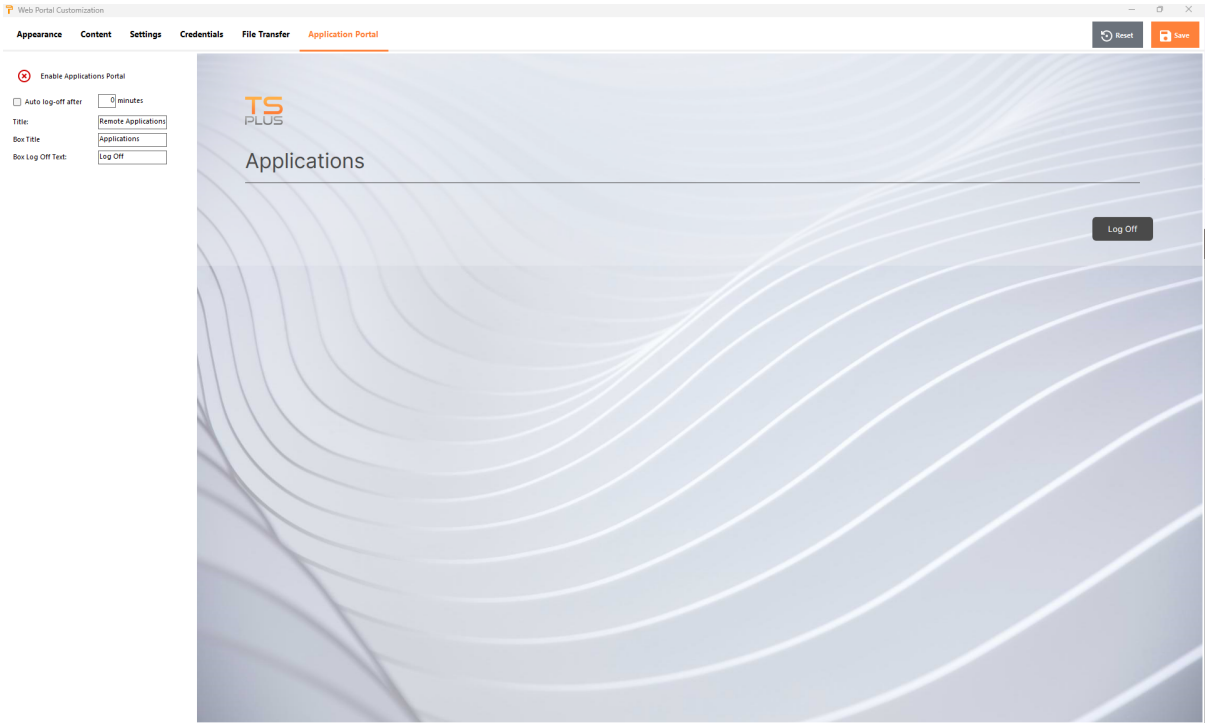


웹 포털 사용자 정의 - 파일 전송



- “ **업로드 - 다운로드** 소스 및 대상 경로를 선택하여 파일 업로드 및 다운로드를 수행합니다.

웹 포털 사용자 정의 - 애플리케이션 패널



애플리케이션 포털에 대한 추가 정보는 찾을 수 있습니다. 여기 .

입력한 값 저장 및 기본값으로 재설정

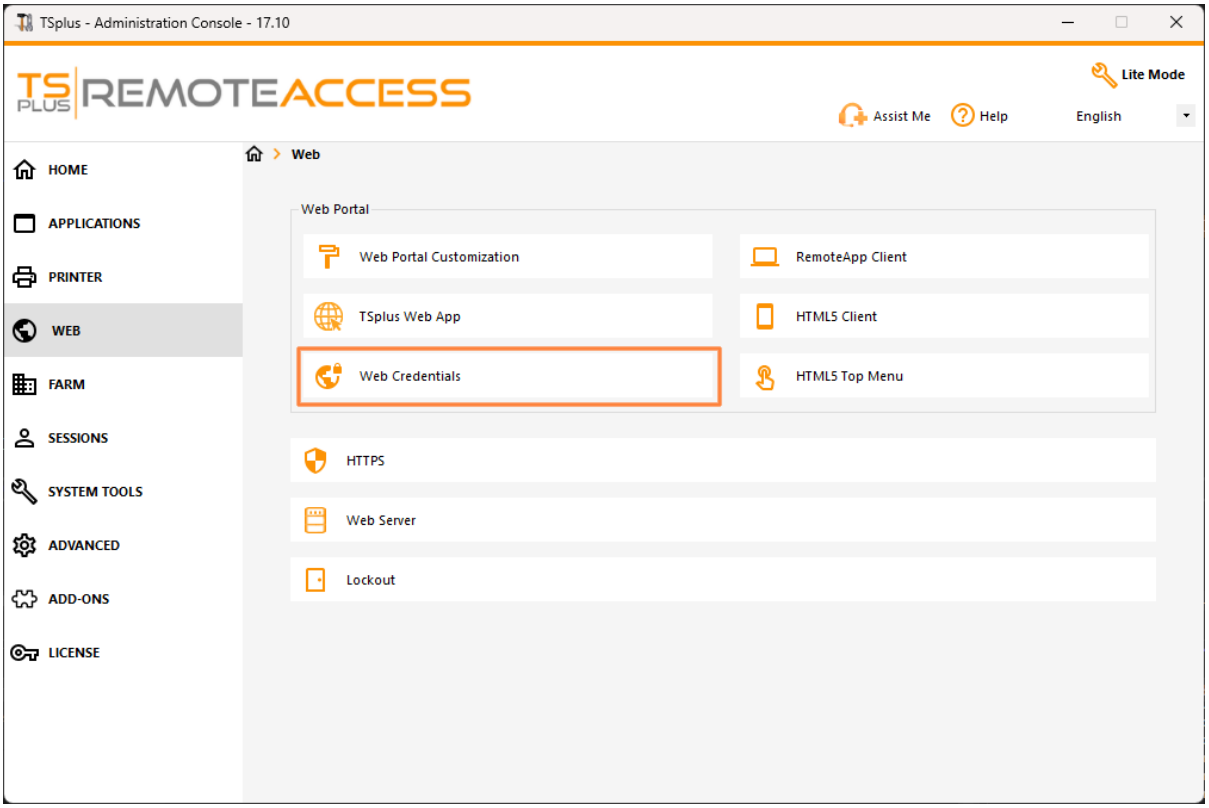
변경 사항을 모두 저장하려면 "저장" 버튼을 클릭하는 것을 잊지 마세요.

원래 값으로 이 값을 재설정하려면 "재설정" 버튼을 클릭하십시오.

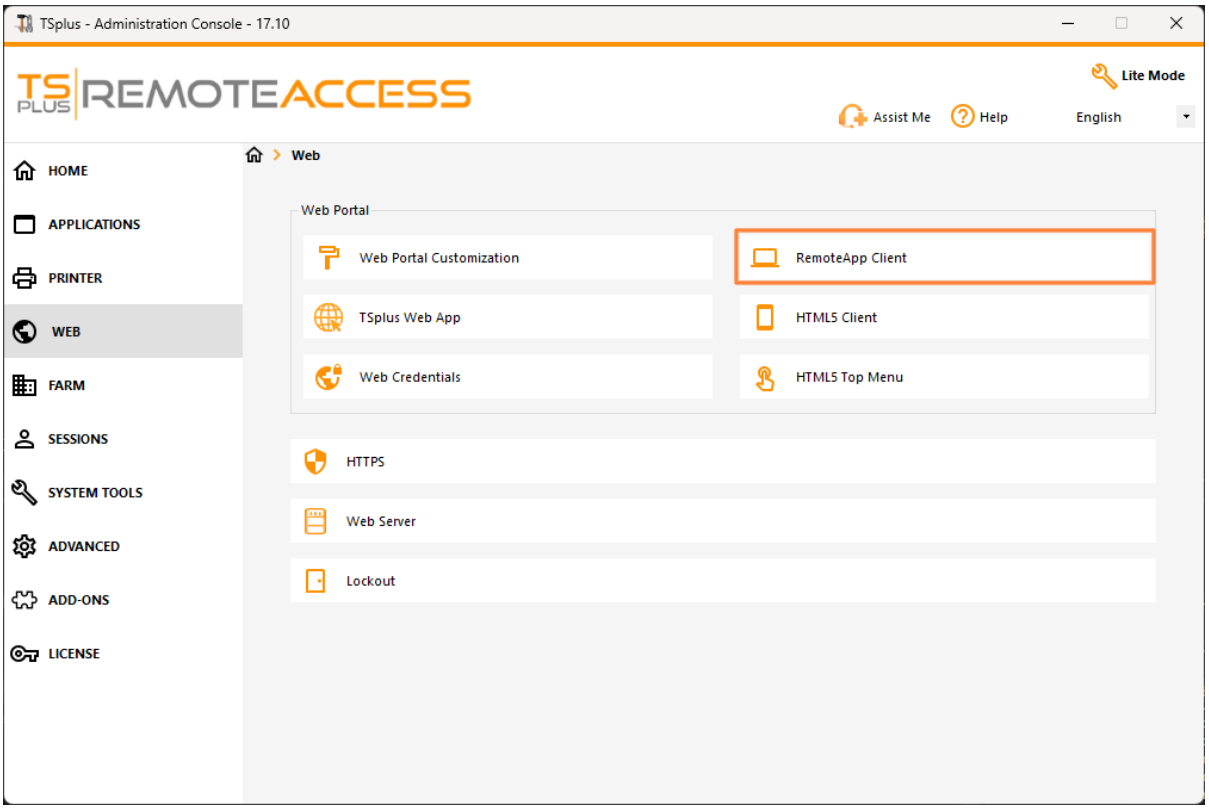
웹 자격 증명

“웹 자격 증명” 섹션에서는 사용자가 이를 활성화(또는 비활성화)할 수 있습니다. 웹 자격 증명 기능.

웹 자격 증명을 사용할 때 비밀번호를 비워둘 수 있도록 허용할 수 있습니다. 비밀번호가 비어 있는 웹 자격 증명만 있는 경우, 웹 로그인 페이지를 더욱 간소화하기 위해 "비밀번호 필드 표시" 옵션의 선택을 해제할 것을 권장합니다.

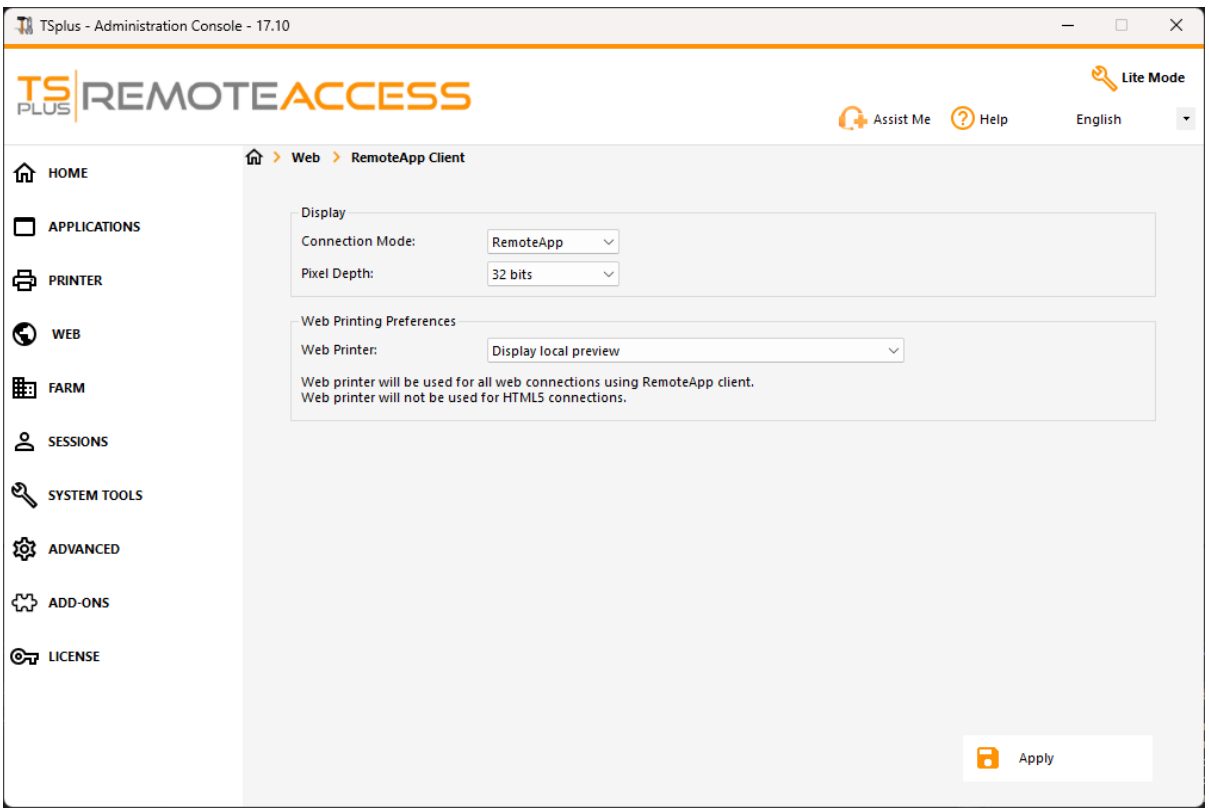


원격 앱 타일

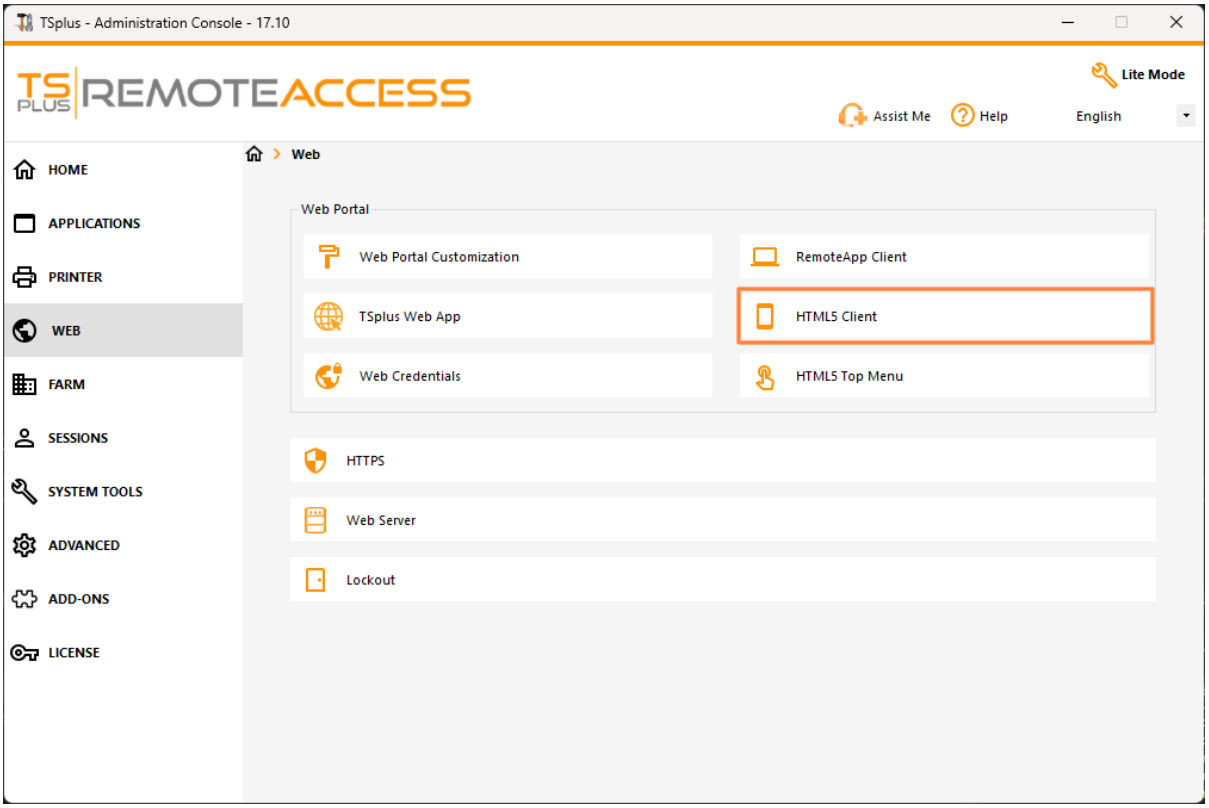


이 타일은 Windows 클라이언트 전용 설정을 위한 것입니다.

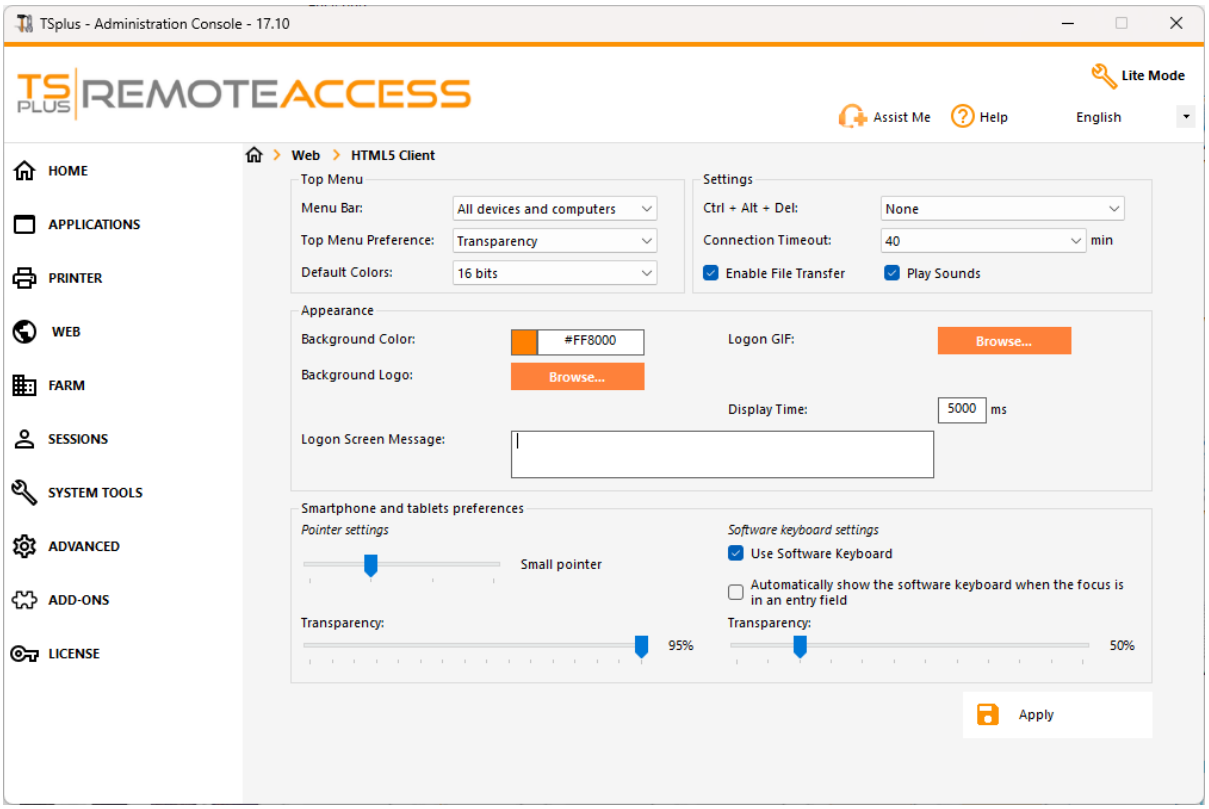
원격 앱(원격 데스크톱 없이 원격 연결) 또는 표준 RDP 중에서 디스플레이를 선택할 수 있습니다. 문서를 사용자 기본 프린터에 인쇄할지, 로컬 미리보기를 표시할지 또는 로컬 프린터 선택을 할지 결정할 수도 있습니다.



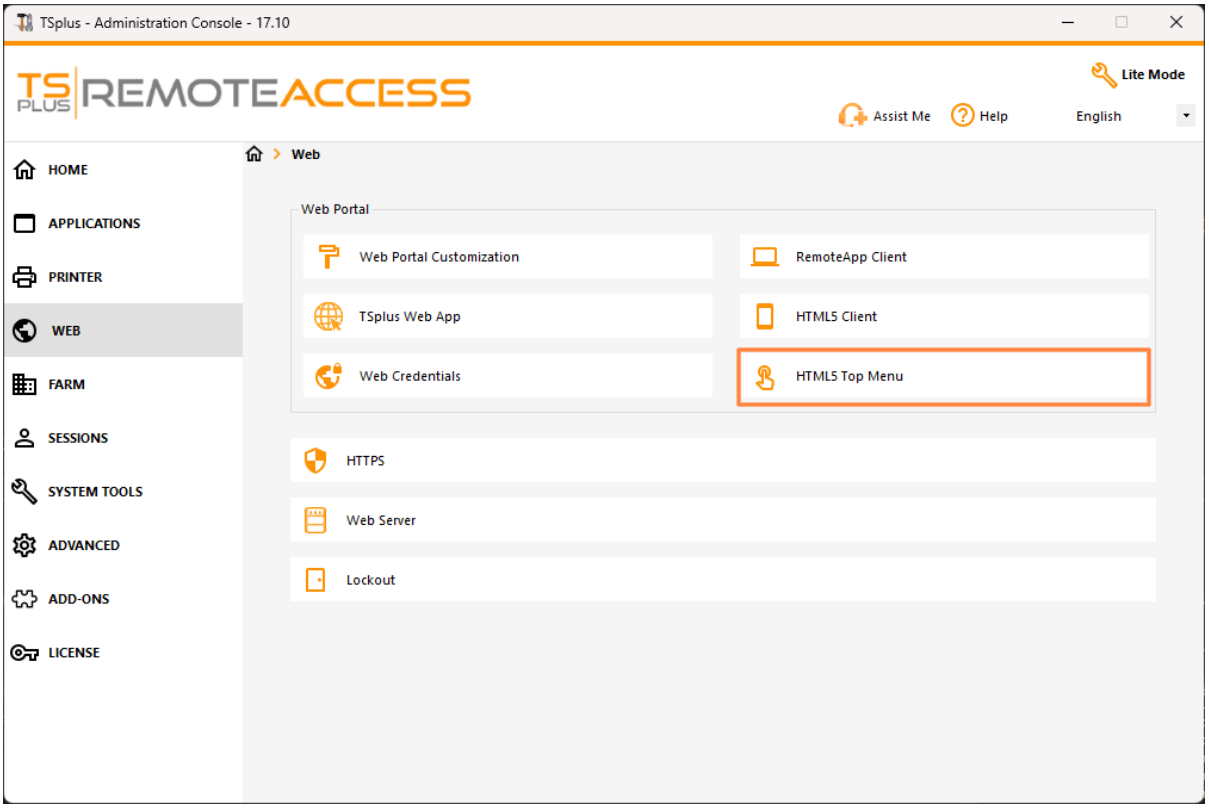
HTML5 클라이언트 타일



이 타일에서 HTML5 클라이언트 웹 디스플레이의 매개변수를 편집할 수 있습니다. 더 많은 정보는 이 페이지 .

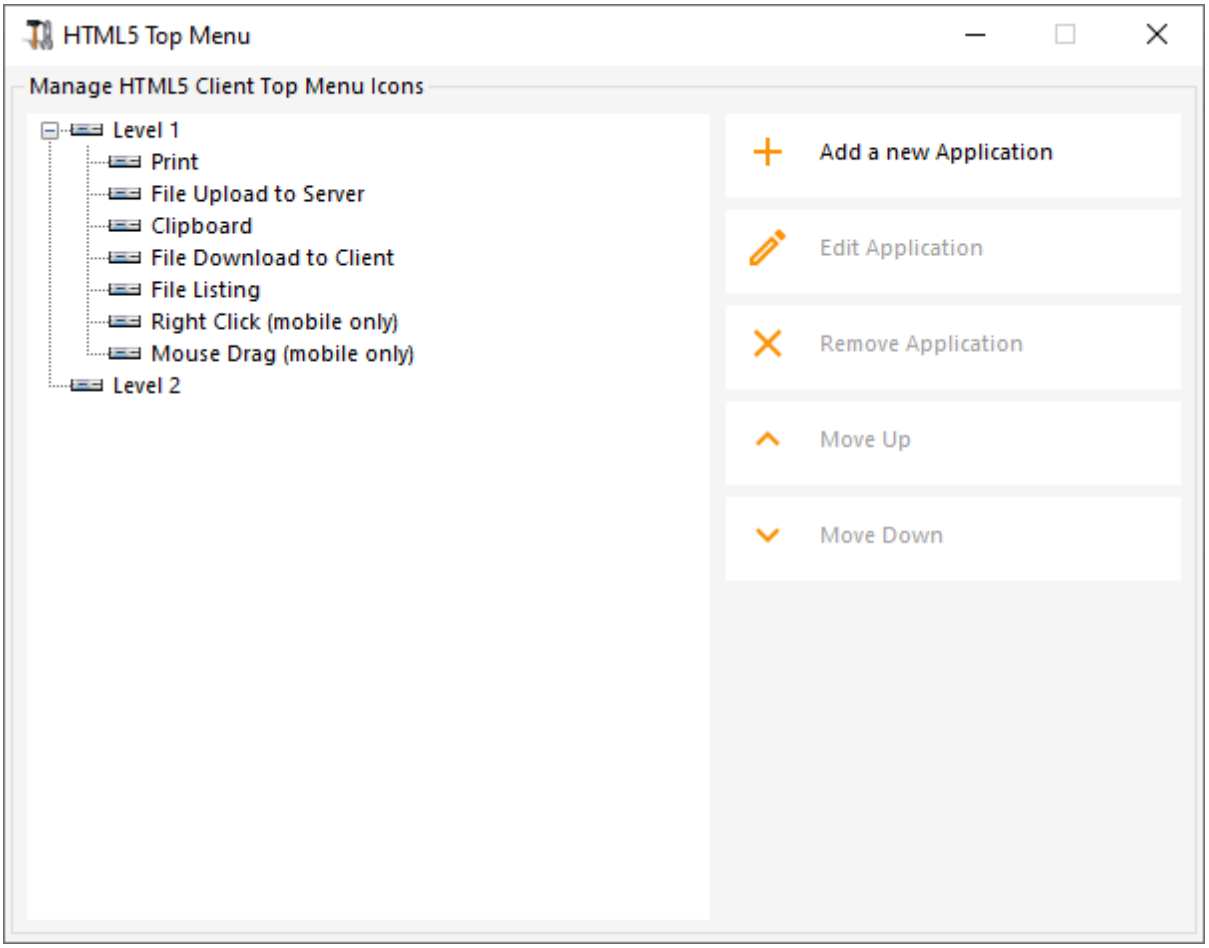


HTML5 상단 메뉴 타일



이 타일은 생성된 원격 웹 세션의 상단 메뉴에서 레벨 1 또는 2에 표시할 애플리케이션을 선택할 수 있게 해줍니다. 또한 이러한 애플리케이션을 특정 클라이언트 유형(pc, 모바일, ios 등)에 맞게

편집할 수 있습니다.


HTML5 Top Menu
Manage HTML5 Client Top Menu Icons
Level 1
Print
File Upload to Server
Clipboard
File Download to Client
File Listing
Right Click (mobile only)
Mouse Drag (mobile only)
Level 2
Add a new Application
Edit Application
Remove Application
Move Up
Move Down