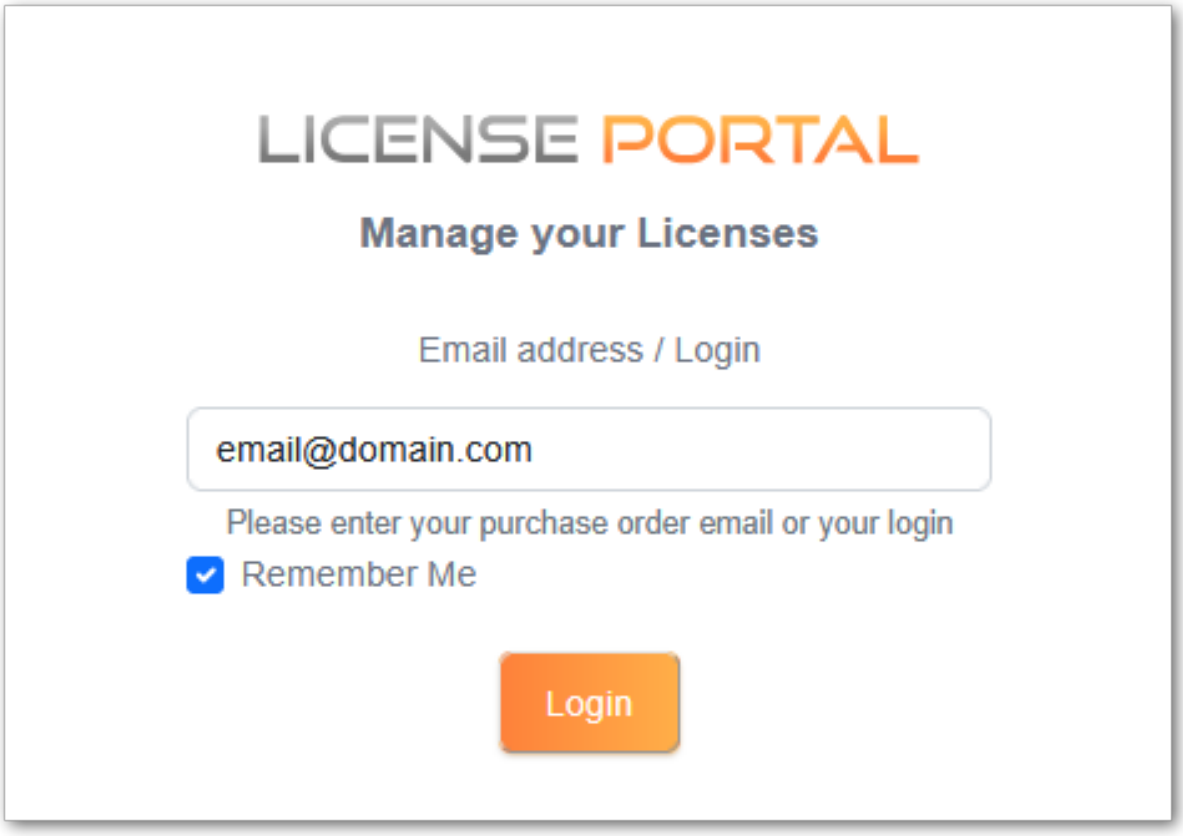
Aktivierung Ihrer TSplus Permanentlizenz (Offline)

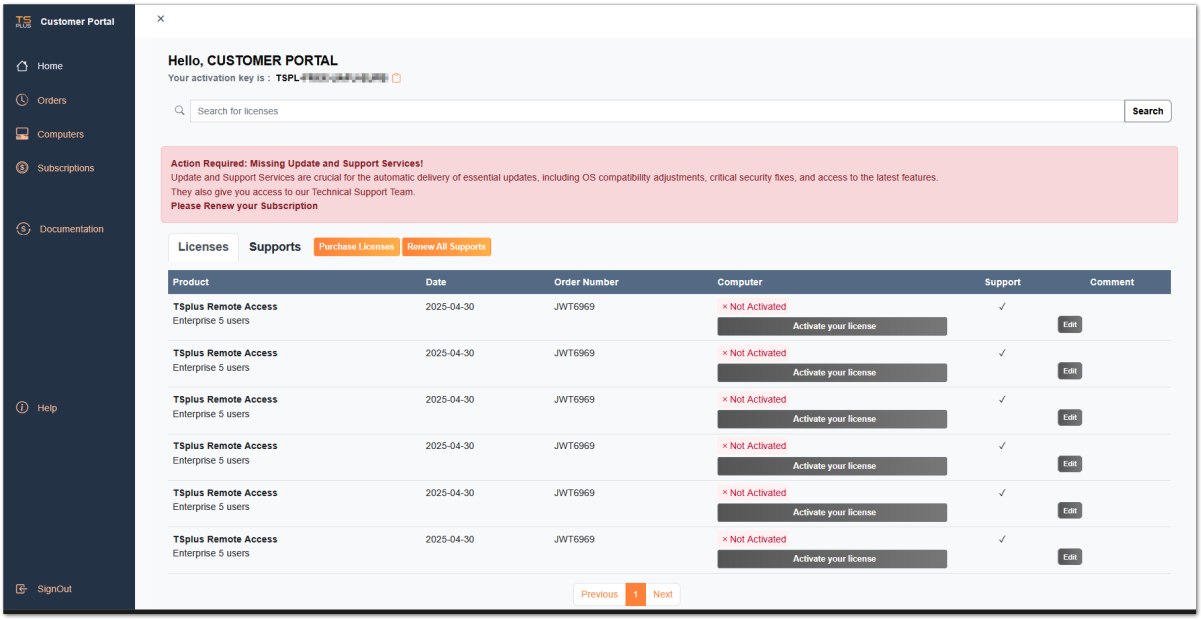
Aktivierungsschlüssel abrufen

Wenn Sie eine Lizenz bestellen, verbinden Sie sich mit unserem Lizenzportal und geben Sie Ihre E-Mail-Adresse und Ihre Bestellnummer ein.

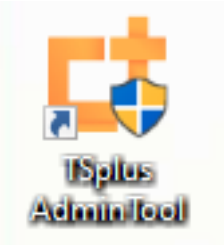


Laden Sie das Benutzerhandbuch für das Kundenportal herunter für weitere Informationen zur Verwendung.

Ihr Aktivierungsschlüssel wird oben im Dashboard angezeigt:



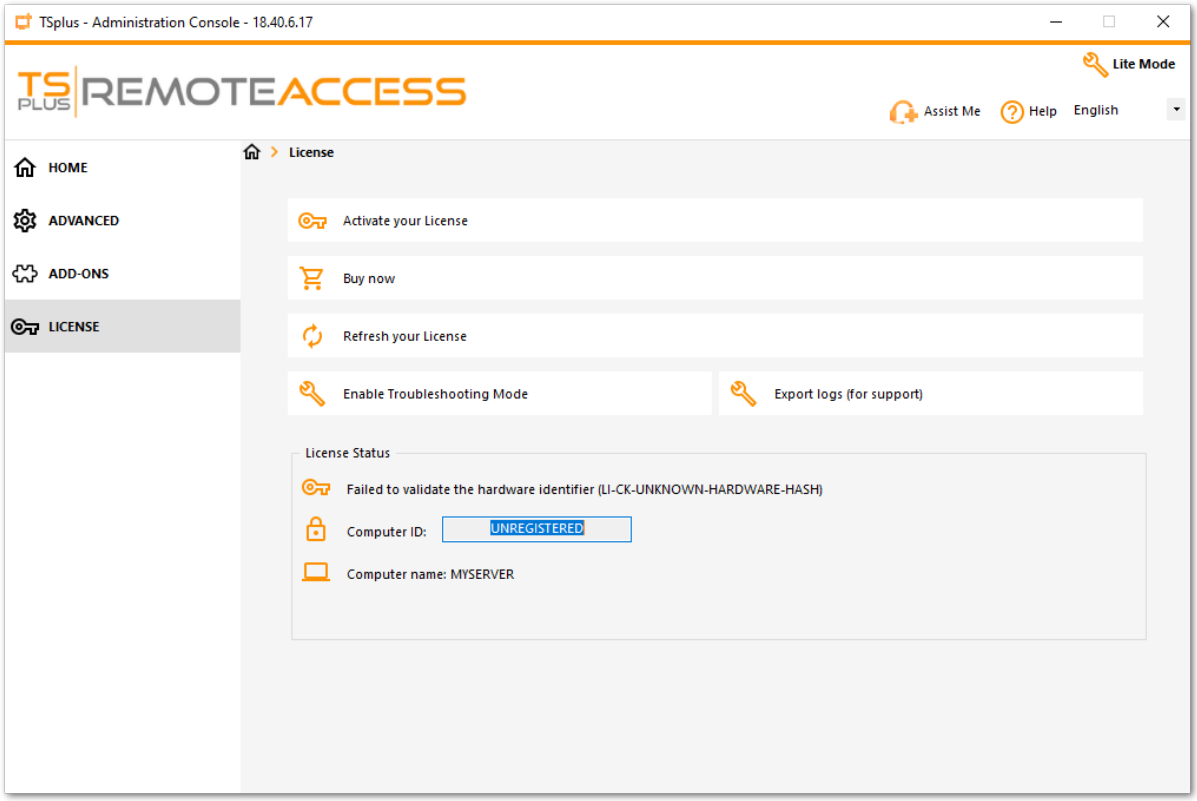
Finden Sie das Administrationswerkzeug auf Ihrem Desktop



Wenn Sie die Verknüpfung zum Administrationswerkzeug nicht finden können, sollte sie im Desktop-Ordner des Administratorkontos, das zum Herunterladen von TSplus verwendet wurde, zu finden sein. Sie können den TSplus-Ordner auch unter folgendem Pfad finden: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Doppelklicken Sie darauf und klicken Sie dann auf die Registerkarte Lizenz.

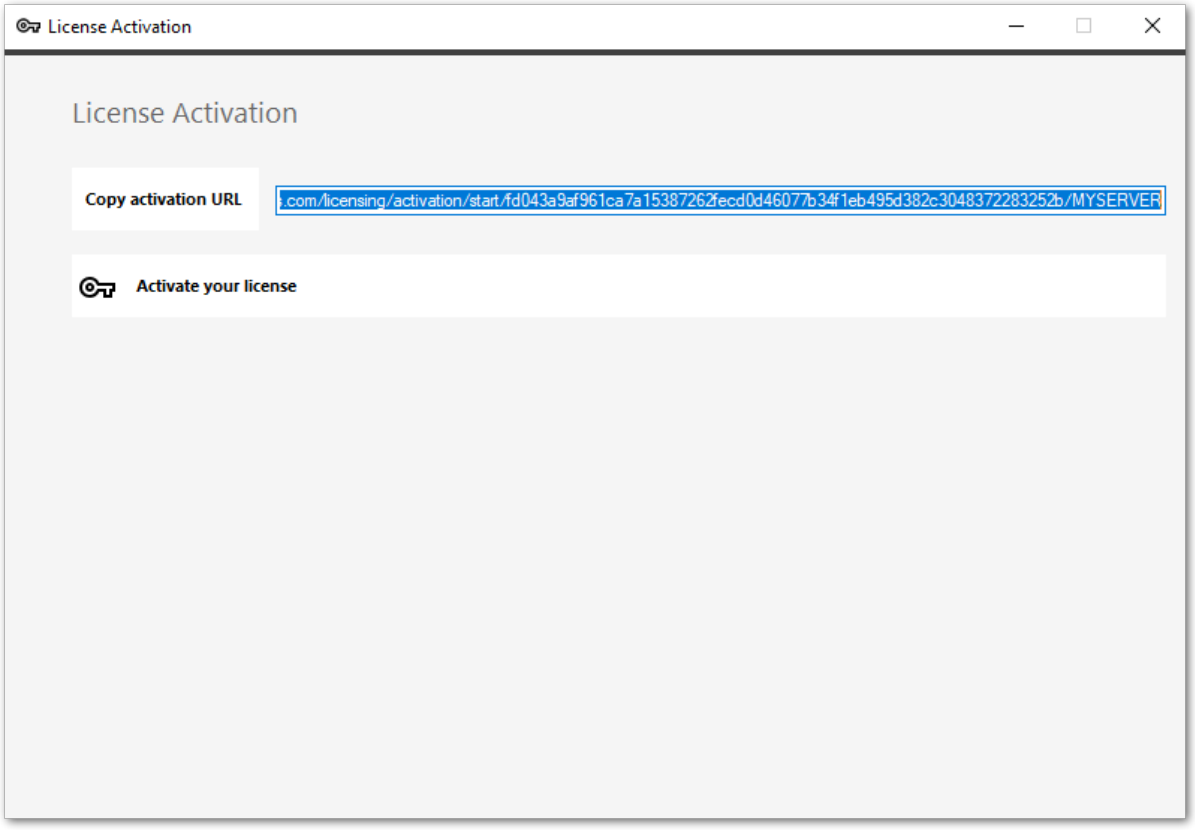
Hier können Sie den Status Ihrer TSplus-Lizenz sowie Ihre Computer-ID und den Computernamen „UNREGISTERED“ einsehen.



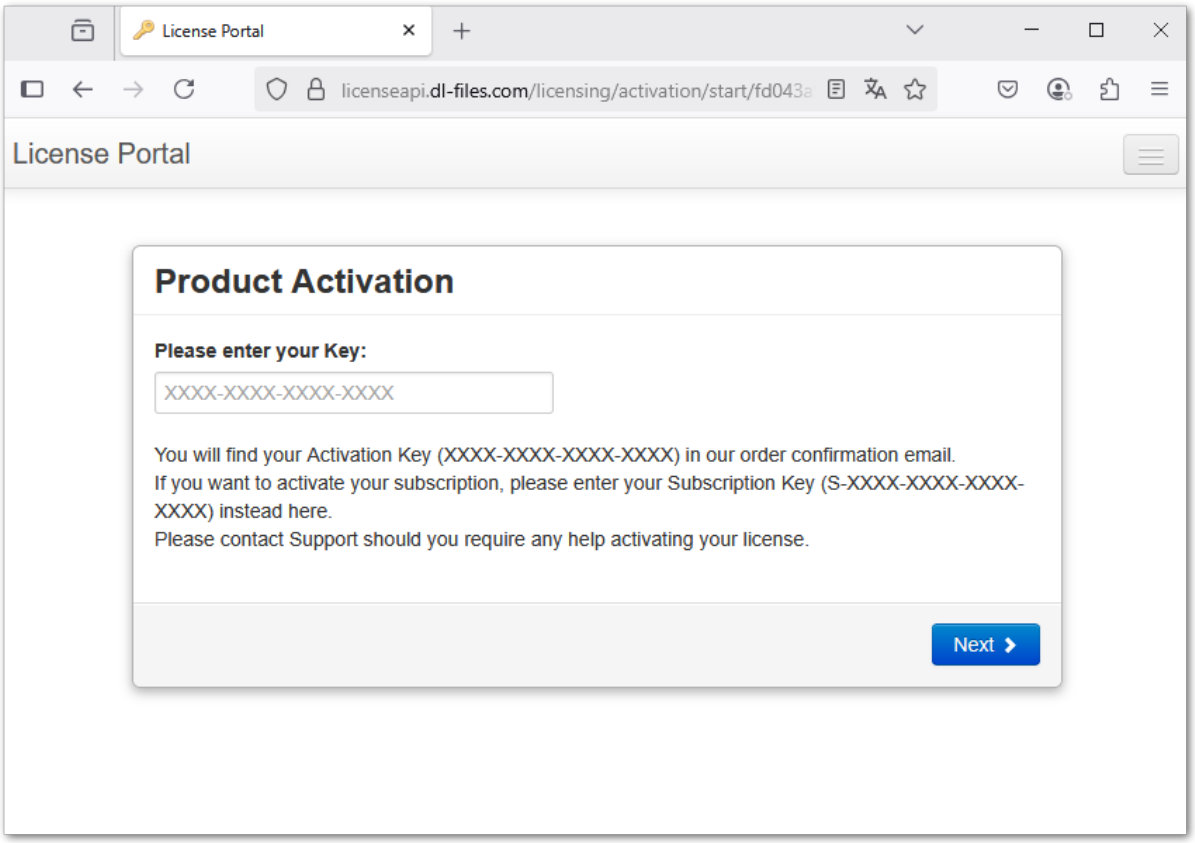
Aktivieren Sie Ihre Lizenzen auf einem Offline-TSplus-Server

Klicken Sie auf die Schaltfläche „Aktivieren Sie Ihre Lizenz“. Ein Popup erscheint und zeigt eine ziemlich lange URL-Adresse an.

Kopieren Sie diese URL in den Browser eines internetverbundenen Computers und greifen Sie darauf zu, um eine Lizenzdatei abzurufen:

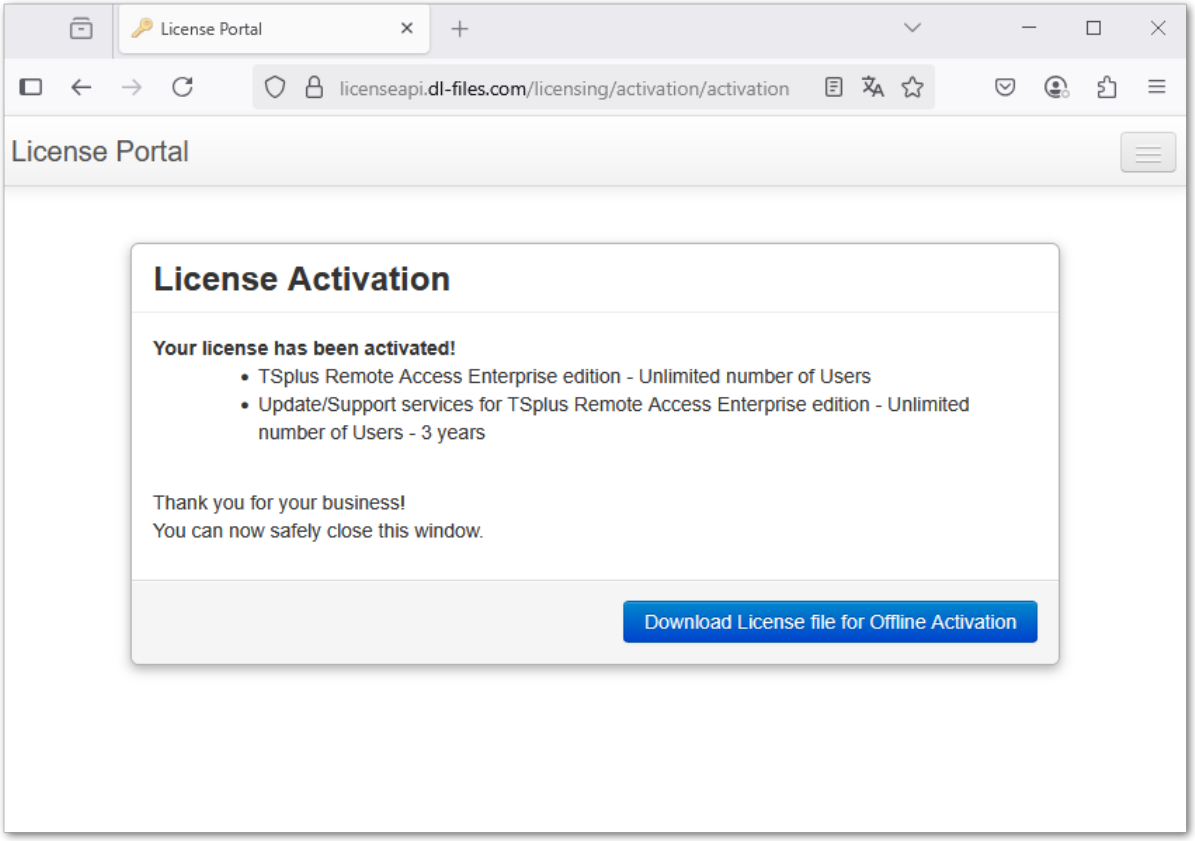


Geben Sie Ihren Aktivierungsschlüssel ein:

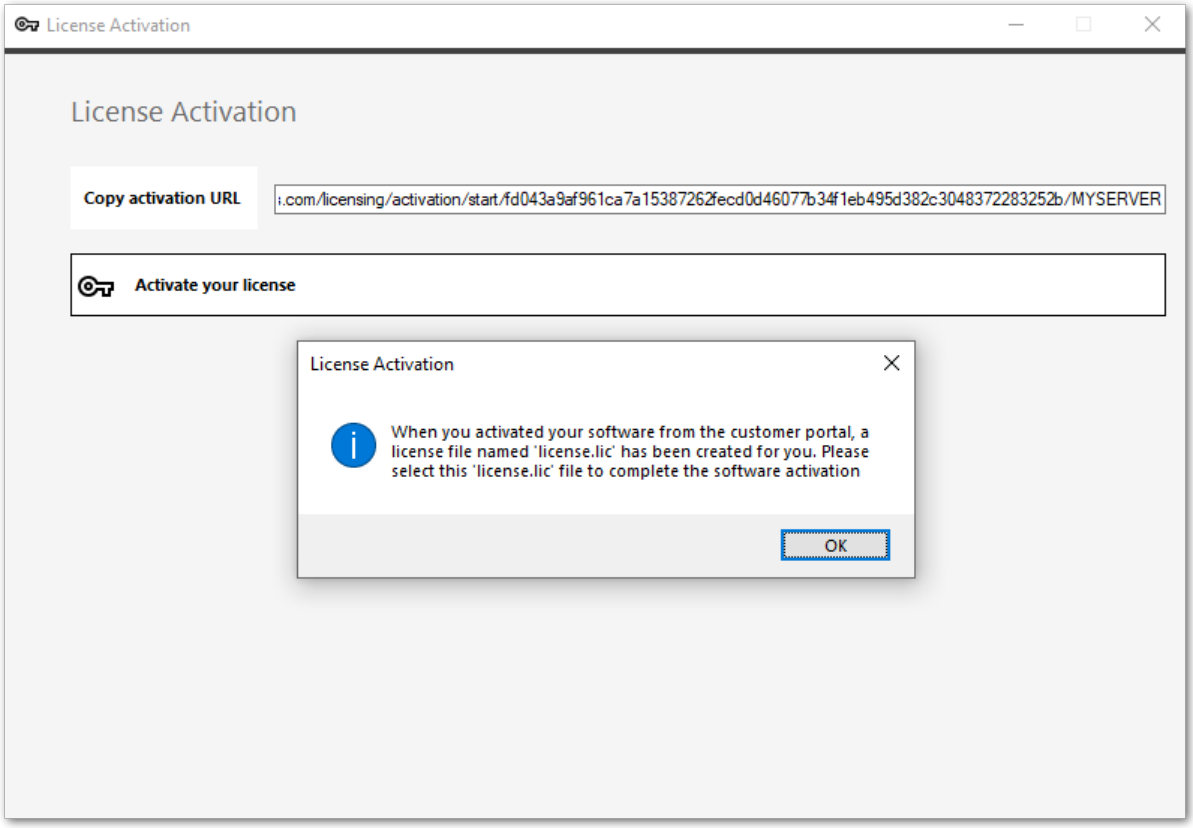


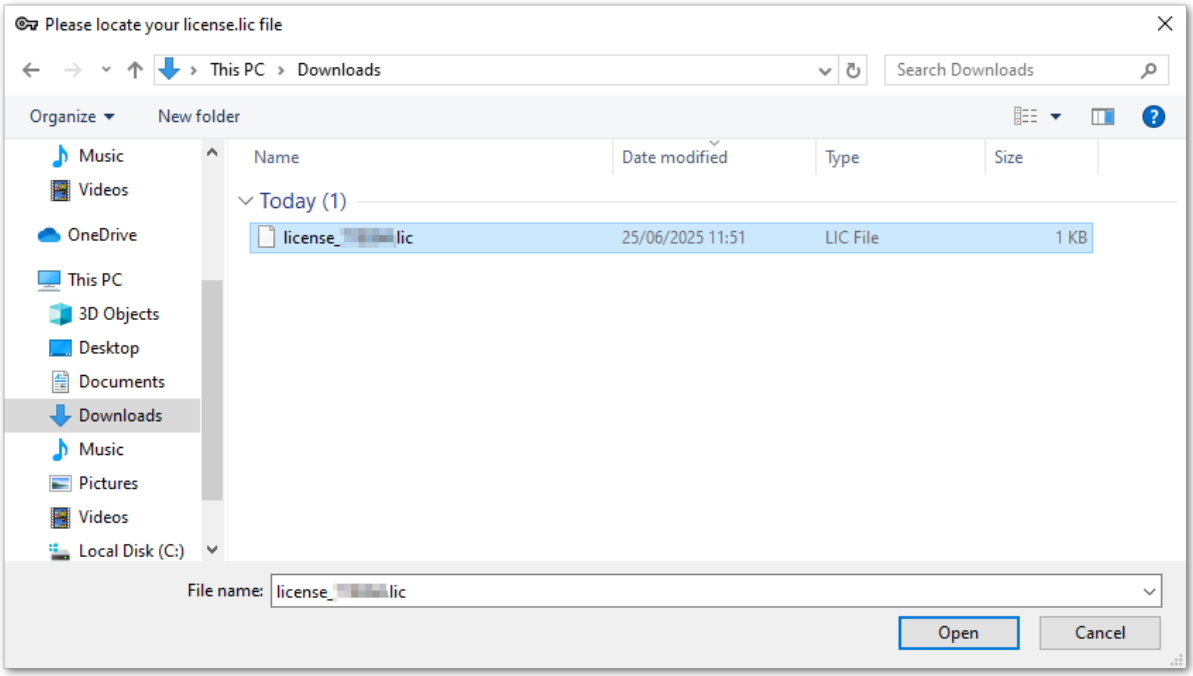
Ihre Lizenz wird dann validiert. Laden Sie die Lizenzdatei herunter, indem Sie auf die

entsprechende Schaltfläche klicken:

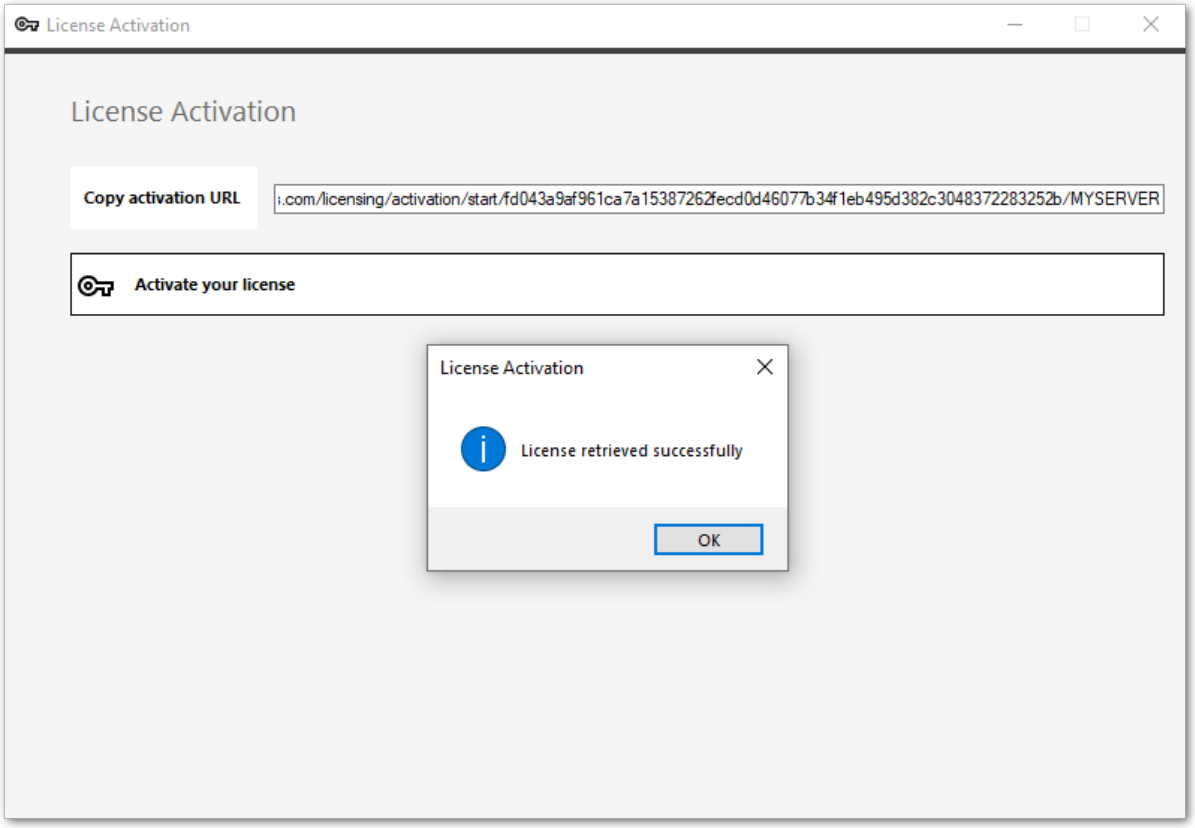


Diese Lizenzdatei muss dann zurück auf den Server kopiert werden, um den Offline-Aktivierungsprozess abzuschließen:





Eine Nachricht wird bestätigen, dass Ihre Lizenz erfolgreich abgerufen wurde:

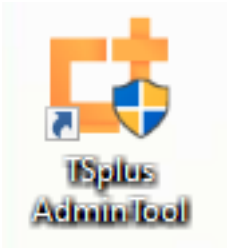


Sie müssen dann die entsprechenden Lizenzen / den Support auswählen, um zu aktivieren, und eine Nachricht erhalten, die bestätigt, dass alle Ihre Produkte / Ihr Support jetzt aktiviert sind.

Hinweis Sie können weiterhin license.lic-Dateien im Lizenzportal für TSplus Legacy-Versionen herunterladen. Laden Sie das Benutzerhandbuch für das Kundenportal herunter .

Aktivierung Ihrer TSplus-Lizenz (Online) Permanent oder Abonnement.

Finden Sie das Administrationswerkzeug auf Ihrem Desktop:

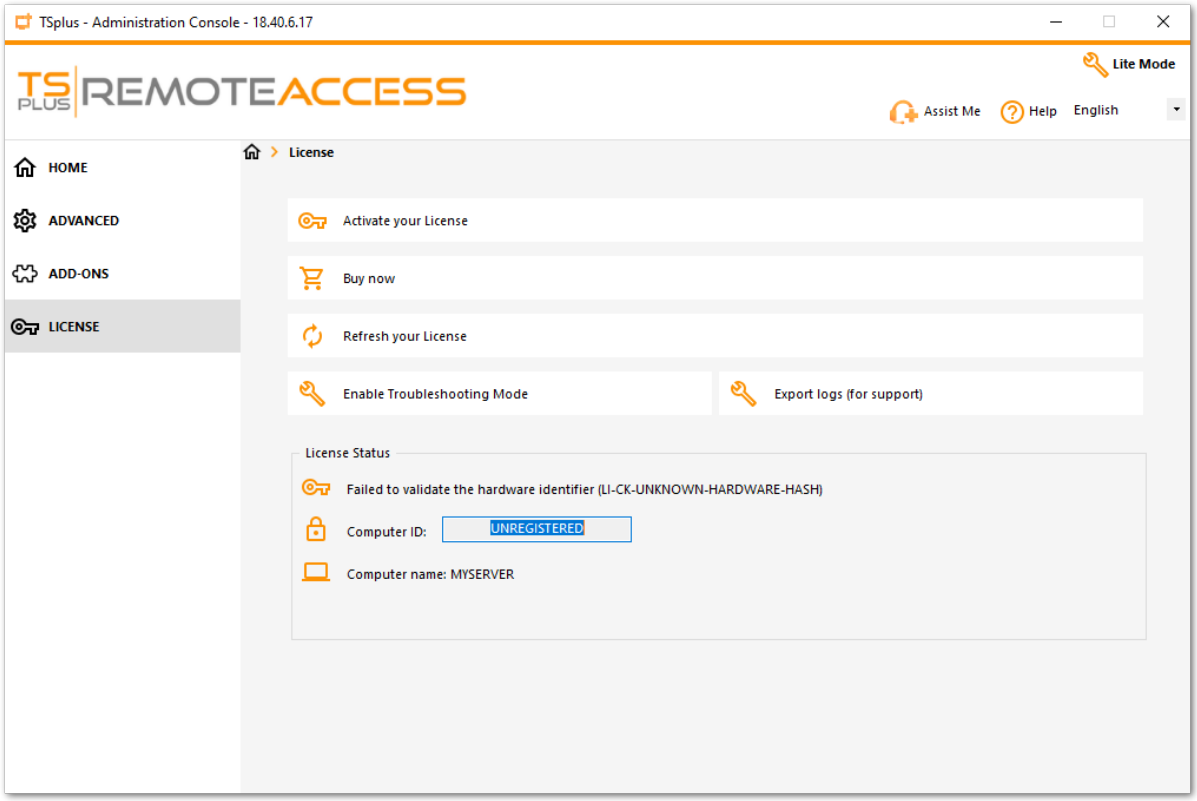


- Wenn Sie die Verknüpfung zum Administrationswerkzeug nicht finden können, sollte sie im Desktop-Ordner des Administratorkontos, das zum Herunterladen von TSplus verwendet wurde, zu finden sein. Sie können den TSplus-Ordner auch unter folgendem Pfad finden: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Doppelklicken Sie darauf und klicken Sie dann auf die Registerkarte Lizenz.

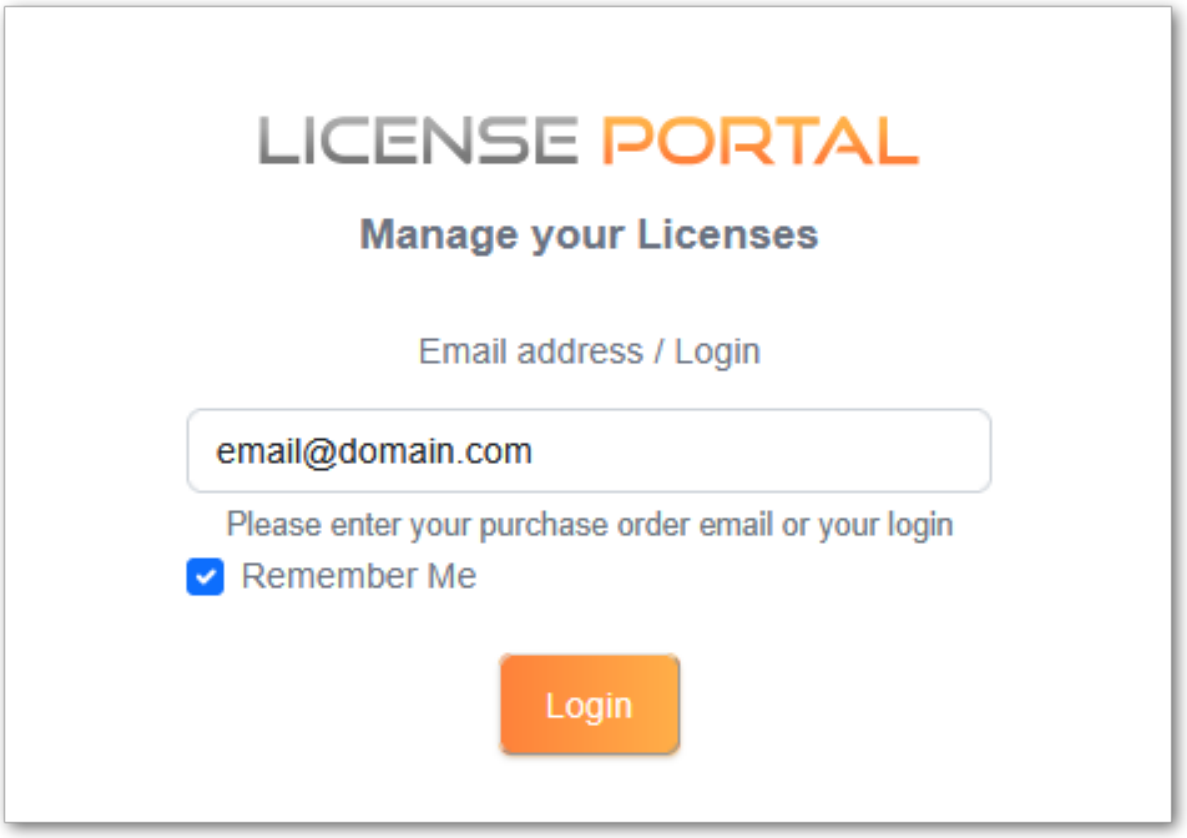
Hier können Sie den Status Ihrer TSplus-Lizenz sowie Ihre Computer-ID und Ihren Computernamen sehen:

wenn es "UNREGISTERED" anzeigt, bedeutet das, dass Ihr Server nicht mit dem Internet verbunden ist und Sie den Webzugang Ihres Servers überprüfen müssen, bevor Sie fortfahren.



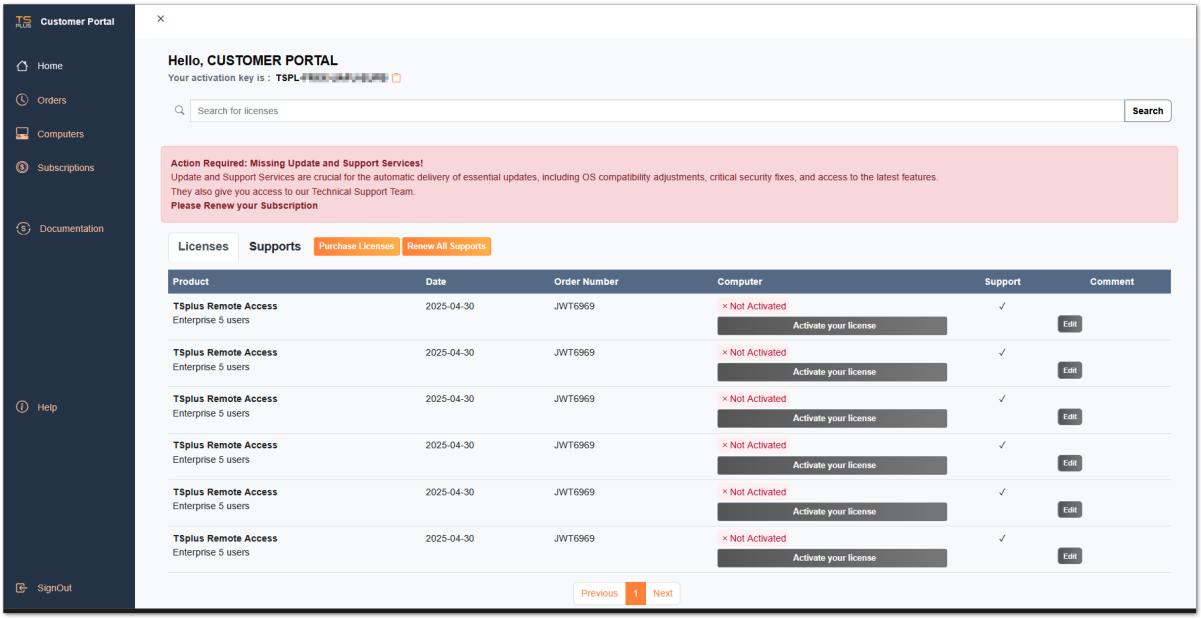
Aktivieren Sie Ihre Lizenzen auf einem Online-TSplus-Server

Wenn Sie eine Lizenz bestellen, verbinden Sie sich mit unserem Lizenzportal und geben Sie Ihre E-Mail-Adresse und Ihre Bestellnummer ein:



Laden Sie das Benutzerhandbuch für das Kundenportal herunter für weitere Informationen zur Verwendung.

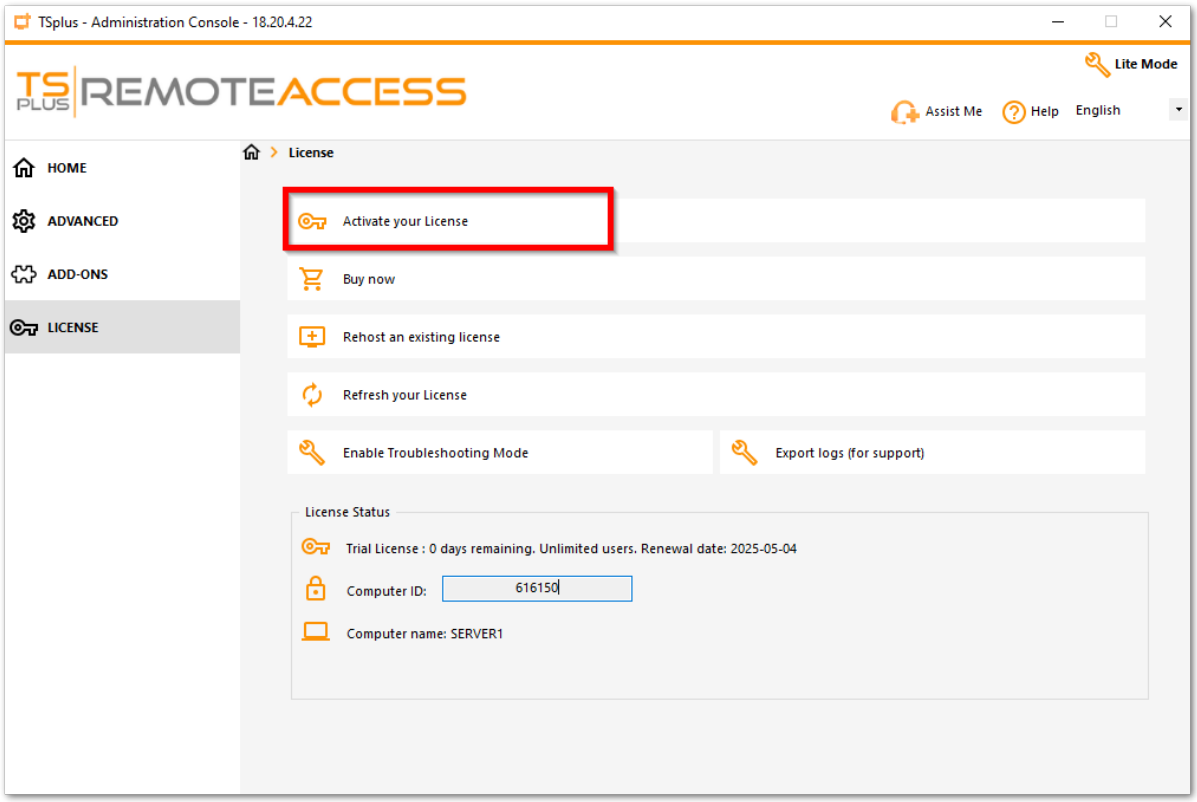
Ihr Aktivierungsschlüssel wird oben im Dashboard angezeigt:

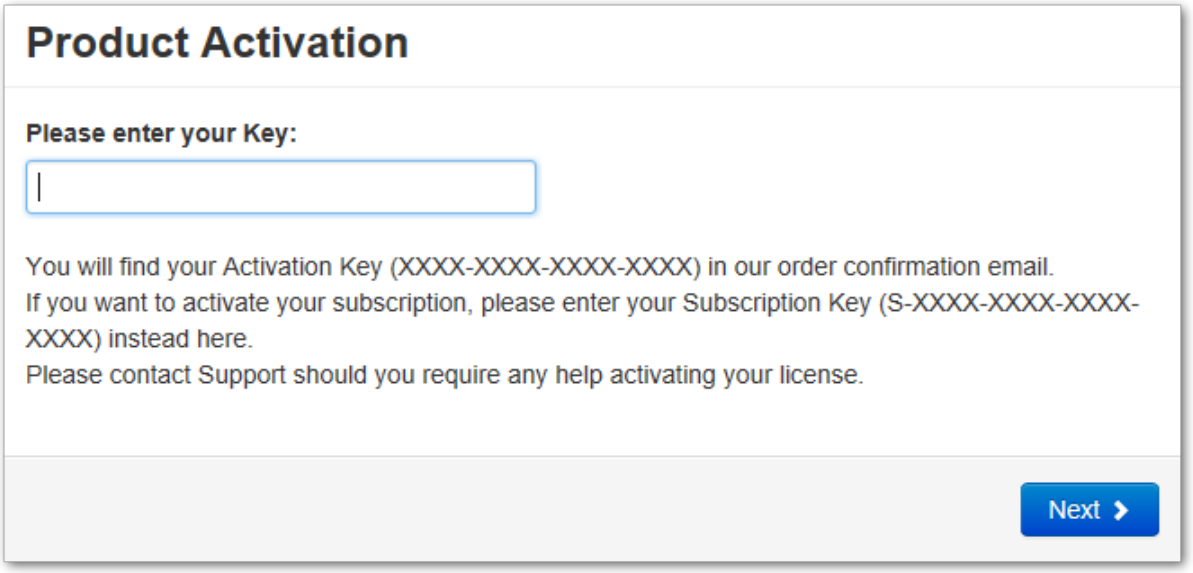


Sie können dann zur Lizenzkachel des AdminTools gehen, auf die Schaltfläche „Ihre Lizenz aktivieren“ klicken, diesen Aktivierungsschlüssel eingeben und auf „Weiter“ klicken.

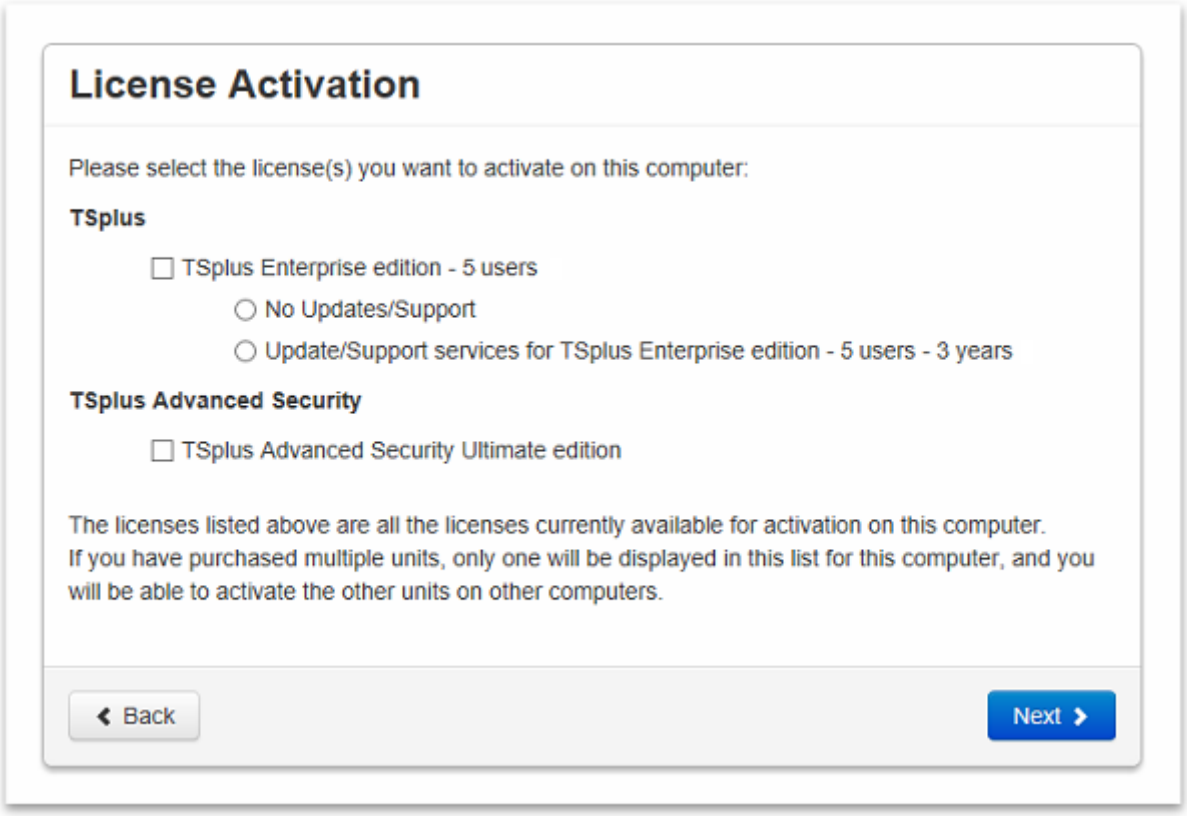
Sie finden Ihren permanenten Aktivierungsschlüssel. **(XXXX-XXXX-XXXX-XXXX)** in unserer Bestellbestätigungs-E-Mail.

Wenn Sie Ihr Abonnement aktivieren möchten, geben Sie bitte Ihren Abonnementschlüssel ein. **S-XXXX-XXXX-XXXX-XXXX** .

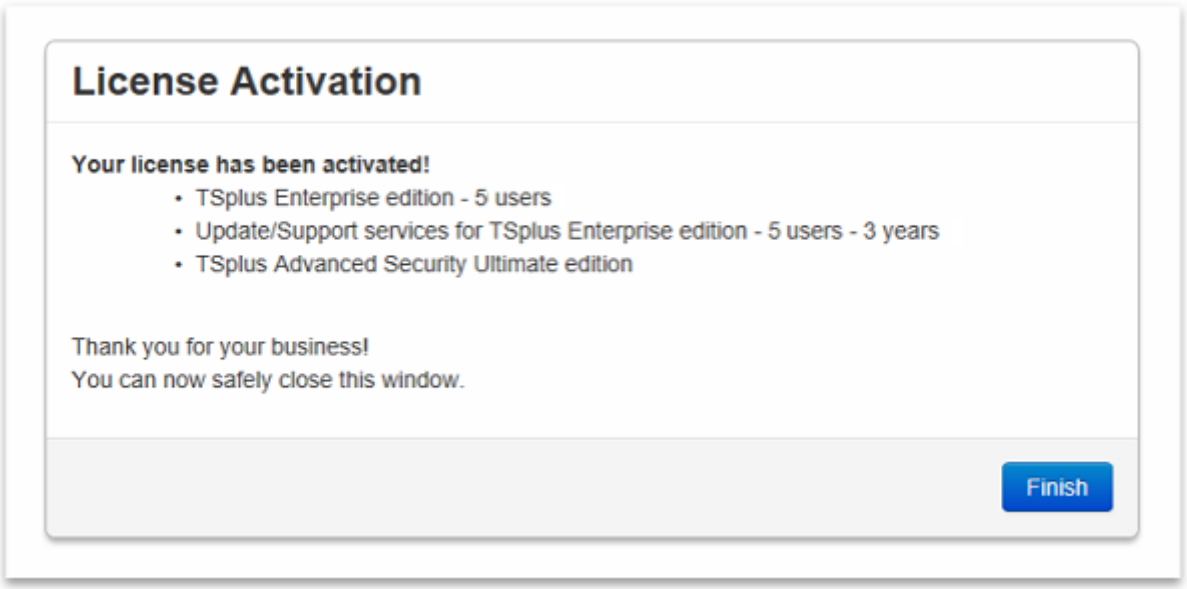




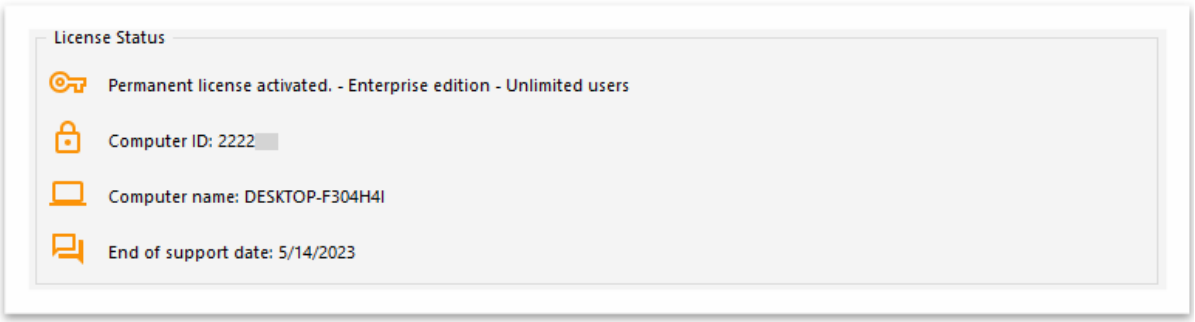
Sie erhalten eine Liste aller verfügbaren Lizenzen/Unterstützungen, die diesem Aktivierungsschlüssel zugewiesen sind, d.h. aller Lizenzen/Unterstützungen, die noch nicht aktiviert sind:



Überprüfen Sie ein oder mehrere Elemente und klicken Sie auf die Schaltfläche „Weiter“. Bitte beachten Sie, dass Sie mehrere Produkte gleichzeitig aktivieren können, indem Sie mehrere Produkte/Support auswählen!

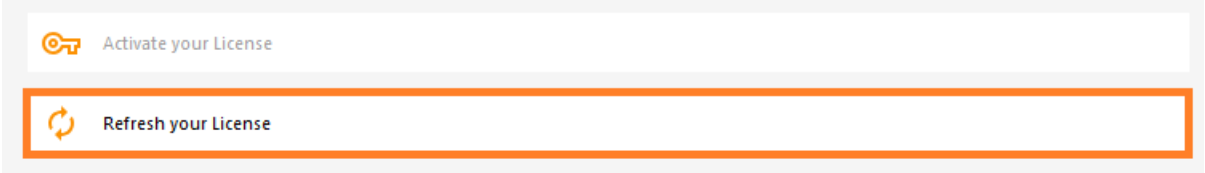


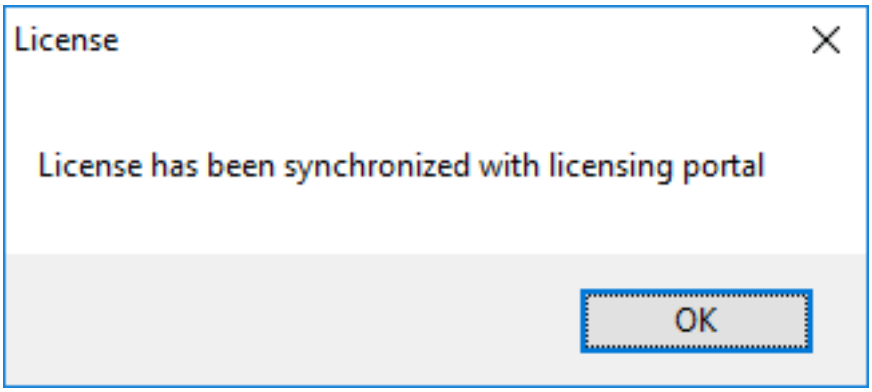
Alle Ihre Produkte/Support sind jetzt aktiviert (in diesem Beispiel wurden sowohl TSplus mit Support als auch TSplus Advanced Security gleichzeitig aktiviert).





Aktualisieren Sie Ihre Lizenzdaten, indem Sie auf die entsprechende Schaltfläche am Ende der Seite klicken. Dadurch werden die Informationen mit unserem Lizenzportal synchronisiert.





Hinweis Sie können weiterhin license.lic-Dateien im Lizenzportal für TSplus Legacy-Versionen herunterladen. Laden Sie das Benutzerhandbuch für das Kundenportal herunter .

Aktivierungsproblem:

Seitenfehler oder die Schaltfläche „NÄCHSTE“ funktioniert

nicht. Hier sind einige Lösungen.

Deaktivieren Sie Ihr Antivirenprogramm während der Lizenzaktivierung und überprüfen Sie Ihre Firewall- und Antiviren-Einstellungen.

Überprüfen Sie Ihren Browser auf die OK-Nachricht, indem Sie auf diesen Link klicken: https://licenseapi.dl-files.com/licensing/ping

Wenn Sie ein Problem mit einem Antivirenprogramm haben, besteht das Verfahren darin, die folgenden Verzeichnisse auszuschließen: C:\Program Files (x86)\TSplus und C:\wsession

URLs, die Sie in Ihrem Antivirenprogramm und Ihrer Firewall für Updates zulassen sollten: setup.dl-files.com dl-files.com secure-download-file.com

Lizenz / Telemetrie: 93.88.241.55 Updates: 51.254.22.117 TSplus-Kompatibilitätsupdates / Nach Updates suchen / Änderungsprotokoll anzeigen: 83.166.153.206

Ports zuzulassen: (Port 3389 für RDP von WAN, Port 80 für HTTP und 443 für HTTPS)

Überprüfen Sie Ihre Internetsicherheitseinstellungen
Systemsteuerung > Internetoptionen > Benutzerdefinierter Bereich Skripte > Aktive Skripte > Aktivieren

Fatal Alert Code 40 70

Wenn Sie während jeder Synchronisierung oder Aktualisierungsversuch fatale Alarmcodes 40/70 TLS im Ereignisprotokoll antreffen.

Einige TLS-Verschlüsselungssuiten können deaktiviert sein. Sie können Freeware wie **IIS Crypto 4.0** um sie zu überprüfen und zu aktivieren.

Aktivierung Ihrer Support-Lizenz

Die 15. Version von TSplus führte eine neue und einfache Möglichkeit ein, Ihren jährlichen Supportvertrag zu verwalten.

Support-Abonnements sind nur für unbefristete Lizenzen verfügbar. Abonnementlizenzen beinhalten Updates.

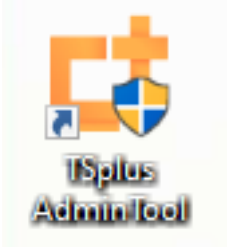
Die Supportdienste umfassen unseren weltweiten Ticket-/E-Mail-Support, den Zugang zum Forum, die Lizenzübertragung, FAQ und Unterstützung bei Tutorials.

Die Update-Dienste umfassen die Bereitstellung von Update-Codes, das Recht, jede neue Version, jeden Patch und alle Updates zu installieren und zu verwenden.

Wir investieren jeden Tag, um TSplus zu verbessern und alle bekannten Probleme zu beheben. Daher empfehlen wir allen unseren Kunden, ihre TSplus-Installation auf dem neuesten Stand zu halten. Die jährliche Gebühr ist nicht teuer und ist auf unserer Store-Seite verfügbar.

Schritt Eins

Finden Sie das Admin-Tool auf Ihrem Desktop:



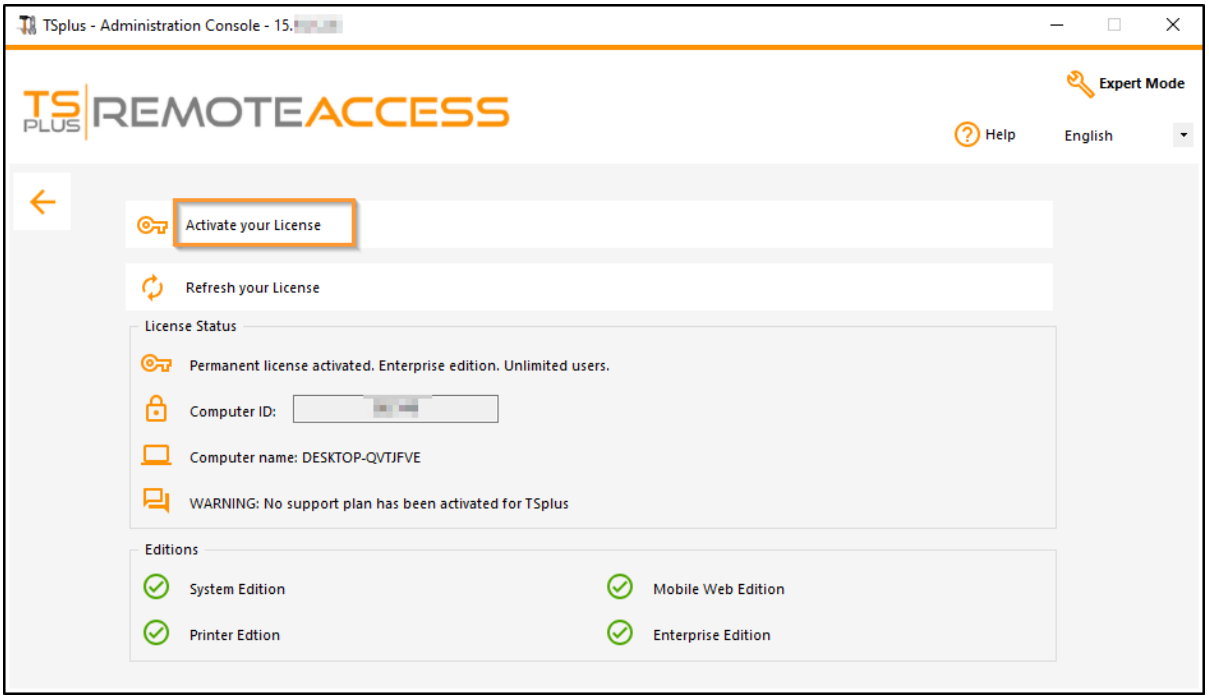
Doppelklicken Sie darauf und klicken Sie dann auf die Lizenzkachel.

- Wenn Sie die Verknüpfung zum Administrationswerkzeug nicht finden können, sollte sie im Desktop-Ordner des Administratorkontos, das zum Herunterladen von TSplus verwendet wurde, zu finden sein. Sie können den TSplus-Ordner auch unter folgendem Pfad finden: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Klicken Sie auf die Registerkarte Lizenz. Sie können jetzt die Seriennummer sehen.

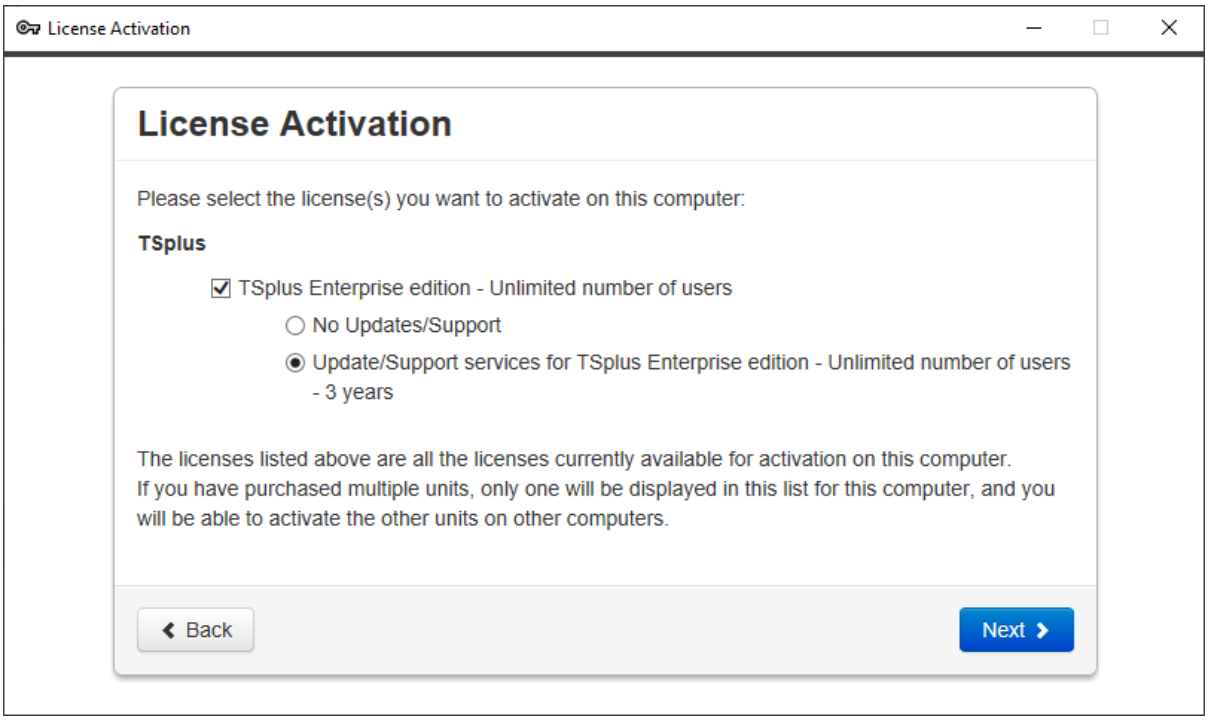
Schritt Zwei

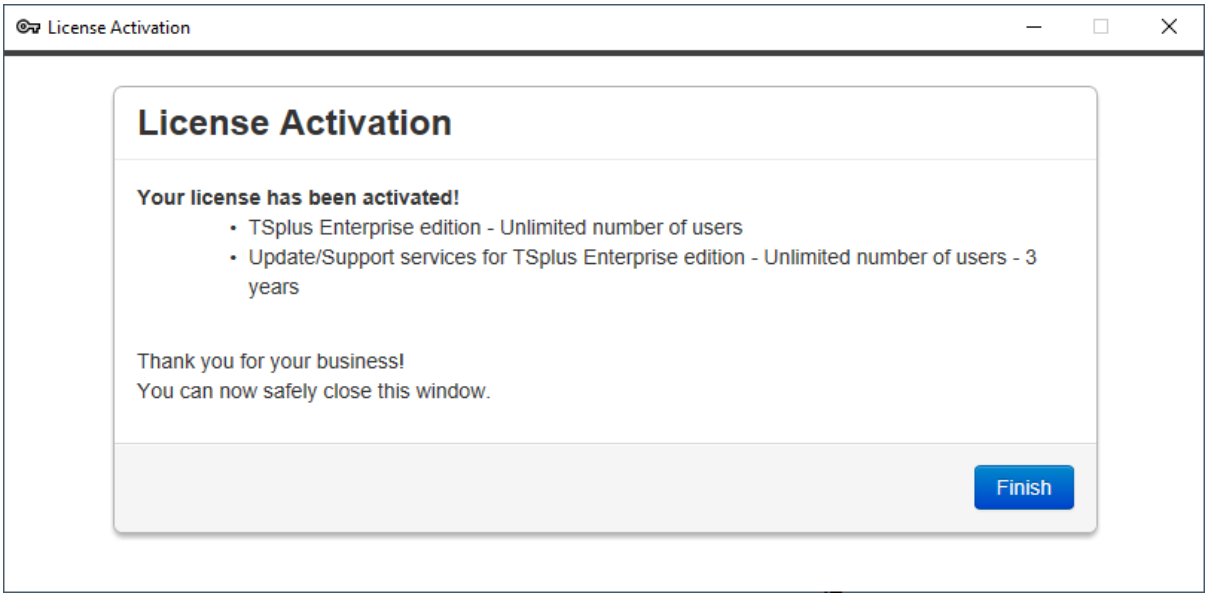
Klicken Sie auf das Feld „Aktivieren Sie Ihre Lizenz“ und geben Sie Ihren Aktivierungsschlüssel ein.



Schritt Drei

Dann wählen Sie „Supportzeitraum verlängern“ aus:



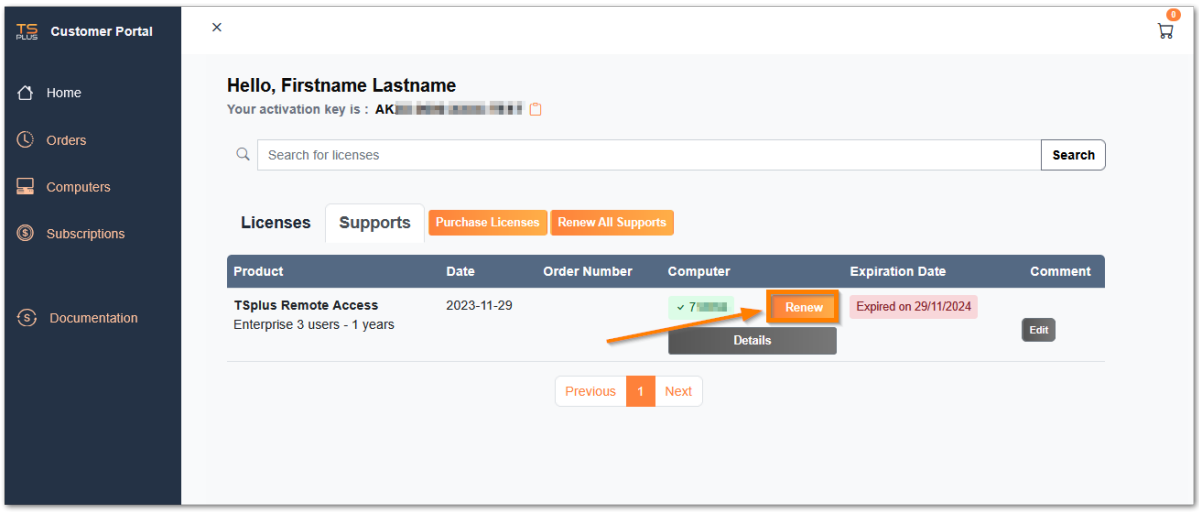


Ein Update-/Support-Abonnement verlängern

Zugriff auf Ihr Lizenzportal: https://license.tsplus.net/login
ID: „Kauf-E-Mail-Adresse“
Passwort: „Bestellnummer Ihrer Wahl“

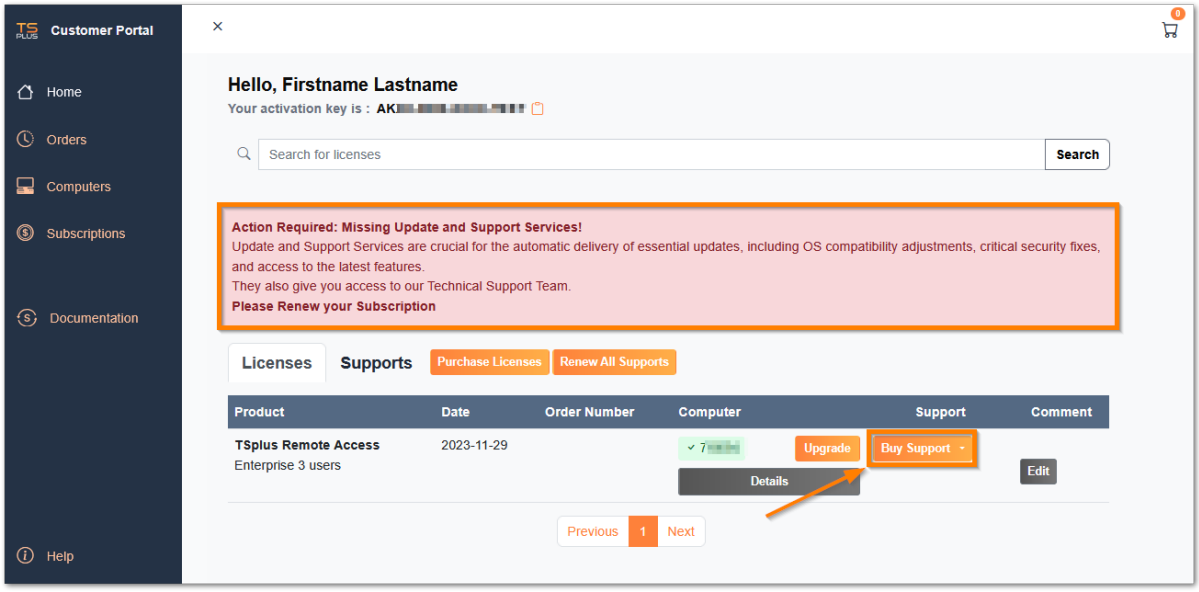
Dann gehen Sie zum Support-Tab und geben Sie Ihre Computer-ID ein (sichtbar im Lizenz-Tab des AdminTools).

Dann klicken Sie auf die Schaltfläche „Erneuern“, um die Unterstützungsdauer von 1, 2 oder 3 Jahren auszuwählen.



Wenn Sie kein Support-Abonnement für eine Lizenz haben, wird auf der Lizenzkarte eine Nachricht angezeigt.
Aktion erforderlich: Fehlende Update- und Supportdienste!

Sie können Ihr Support-Abonnement direkt erwerben, indem Sie auf die Schaltfläche „SUPPORT KAUFEN“ klicken.



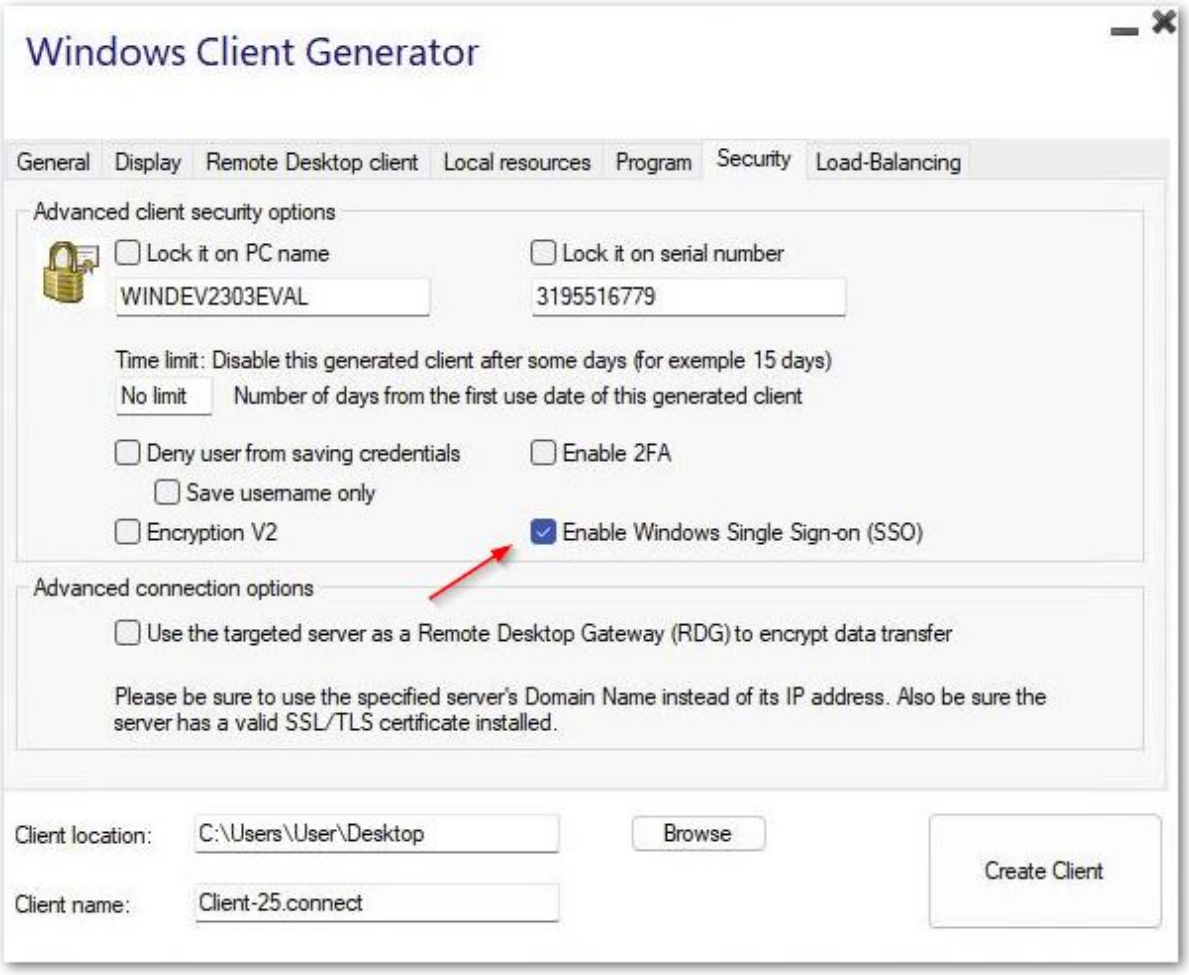
Active Directory Single Sign-On

Um die Windows SSO-Authentifizierung für generierte Clients zu aktivieren:

Aktualisieren Sie TSplus Remote Access auf die neueste Version auf einem Server, der der Domäne beigetreten ist.

Generieren Sie einen Client im Client-Generator, indem Sie das Kästchen „Single Sign-On (SSO) aktivieren“ im Tab „Sicherheit“ markieren.

Verbinden Sie sich von einem mit der Domäne verbundenen Computer aus mit dem generierten Client.



Konfigurieren der Gruppenrichtlinie für Windows Single Sign-On (SSO) über den Remote Desktop Client

Vom Domänencontroller:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.

2. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit (OU), auf die das Gruppenrichtlinienobjekt (GPO) angewendet werden soll, und wählen Sie „Erstellen Sie ein GPO in dieser Domäne und verlinken Sie es hier…“.

3. Benennen Sie die GPO (z. B. SSO_RDS_MEIN_SERVER) und klicken Sie auf „OK“.

4. Rechtsklicken Sie auf die erstellte Richtlinie und wählen Sie „Bearbeiten“.

5. Navigieren Sie zu folgendem Speicherort: „Computer Configuration / Policies / Administrative Templates / System / Credentials Delegation.“

6. Doppelklicken Sie auf „Standardanmeldeinformationen delegieren erlauben“, um die Einstellungen zu öffnen.

7. Aktivieren Sie die Einstellung und klicken Sie auf „Anzeigen…“

8. Im Feld Wert geben Sie den/die Server im Format TERMSRV/ server_fully_qualified_domain_name ein und klicken Sie auf „OK“.

9. Klicken Sie auf „Übernehmen“ und „OK“, um das Fenster zu schließen. Von der Client-Maschine:

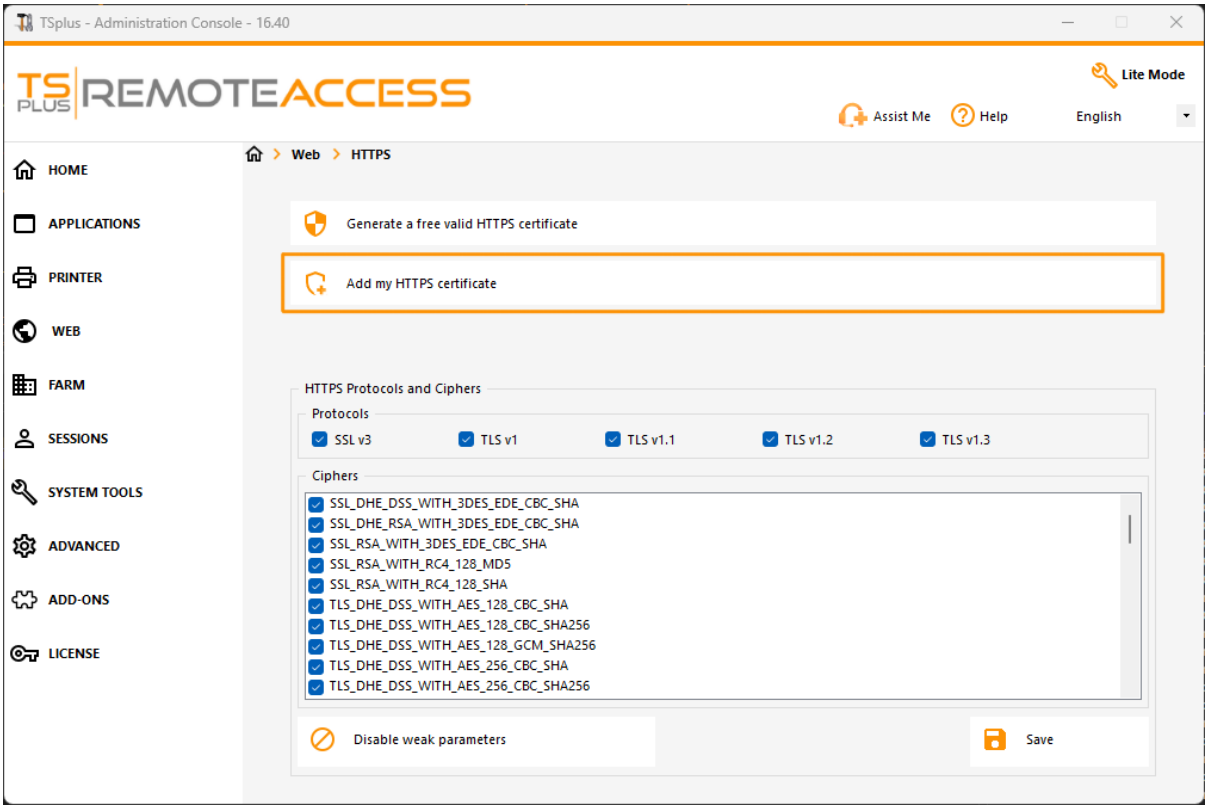
10. Aktualisieren Sie die Gruppenrichtlinien, indem Sie den folgenden Befehl als Administrator ausführen: gpupdate /force.

HTTPS & SSL-Drittanbieterzertifikate

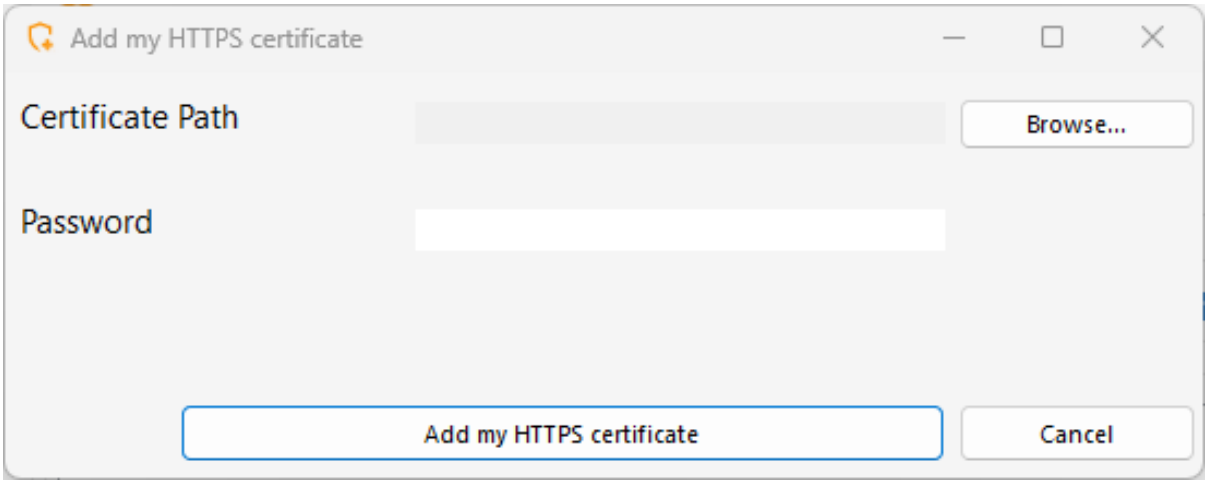
Eigenes Zertifikat hinzufügen

Wenn Sie bereits ein gültiges HTTPS-Zertifikat haben, können Sie es zu Ihrem Webserver hinzufügen.

Öffnen Sie das TSPlus AdminTool, klicken Sie auf die Registerkarte „Web“, gehen Sie zum Menü „HTTPS“ und klicken Sie dann auf „Mein HTTPS-Zertifikat hinzufügen“, wie im Screenshot unten gezeigt:



Ein Fenster öffnet sich, in dem Sie Ihr Zertifikat auswählen können:



Ihre Zertifikatdatei muss das Format ".pfx" verwenden.

Wenn Ihr Zertifikat durch ein Passwort geschützt ist, können Sie es im entsprechenden Feld eingeben.

Klicken Sie auf die Schaltfläche „Mein Zertifikat hinzufügen“, um Ihr Zertifikat hinzuzufügen.

Bitte beachten Sie, dass Sie Ihr Zertifikat manuell erneuern müssen.

Zusätzliche Links

Vertrauenswürdige SSL-Zertifikatanbieter:

- GoDaddy
- DigiCert

Sie können Ihre .pem in das pfx-Format mit Tools oder Online-Seiten konvertieren. Zum Beispiel auf dieser Seite: https://www.sslshopper.com/ssl-converter.html

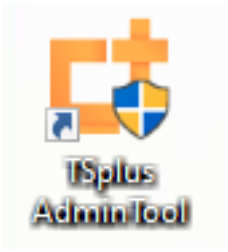
Sie können dies verwenden SSL-Server-Test-Tool um die gute Qualität eines Webportals in HTTPS zu validieren.

TSplus Administrationswerkzeug Übersicht

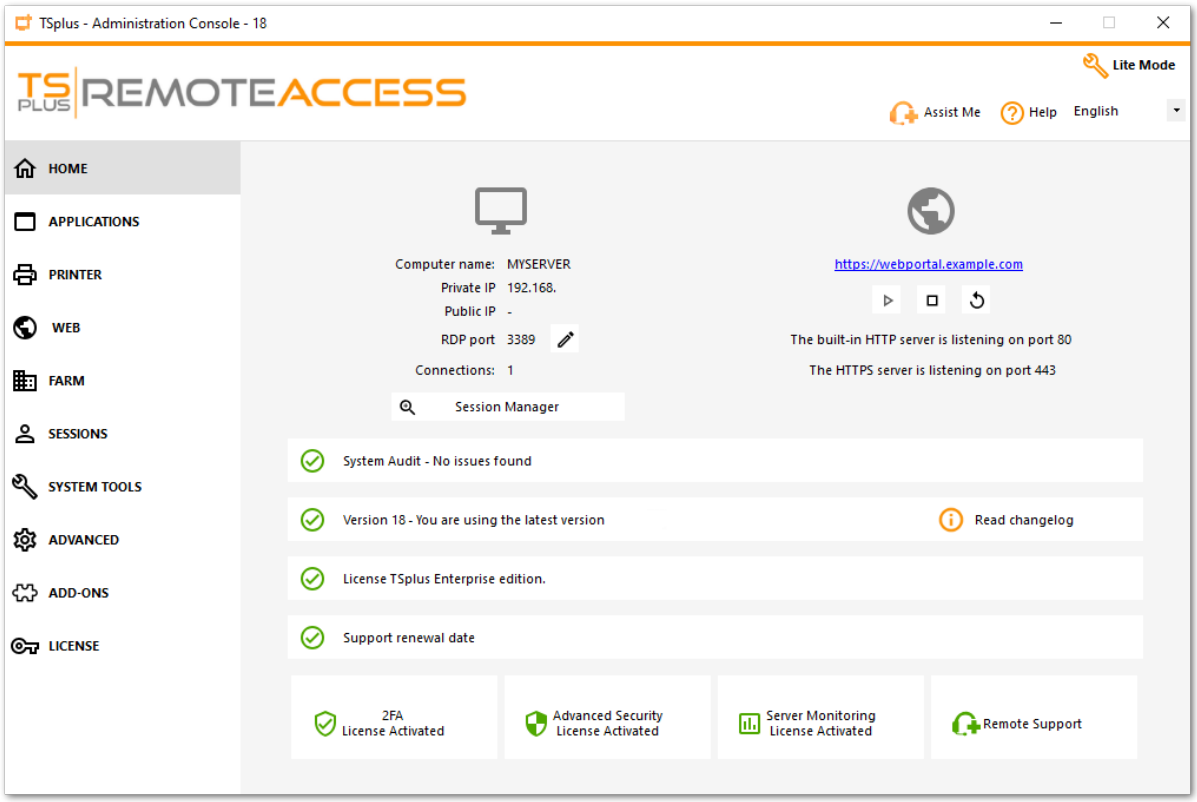
Nach installieren von TSplus Ihr Server ist sofort einsatzbereit.

Sie können jedoch **alle Systemparameter anpassen** mit einem leistungsstarken Administrationswerkzeug.

Um dies zu tun, klicken Sie auf das folgende Symbol, das auf Ihrem Desktop erstellt wurde:



Das Administrationswerkzeug wird dann angezeigt:

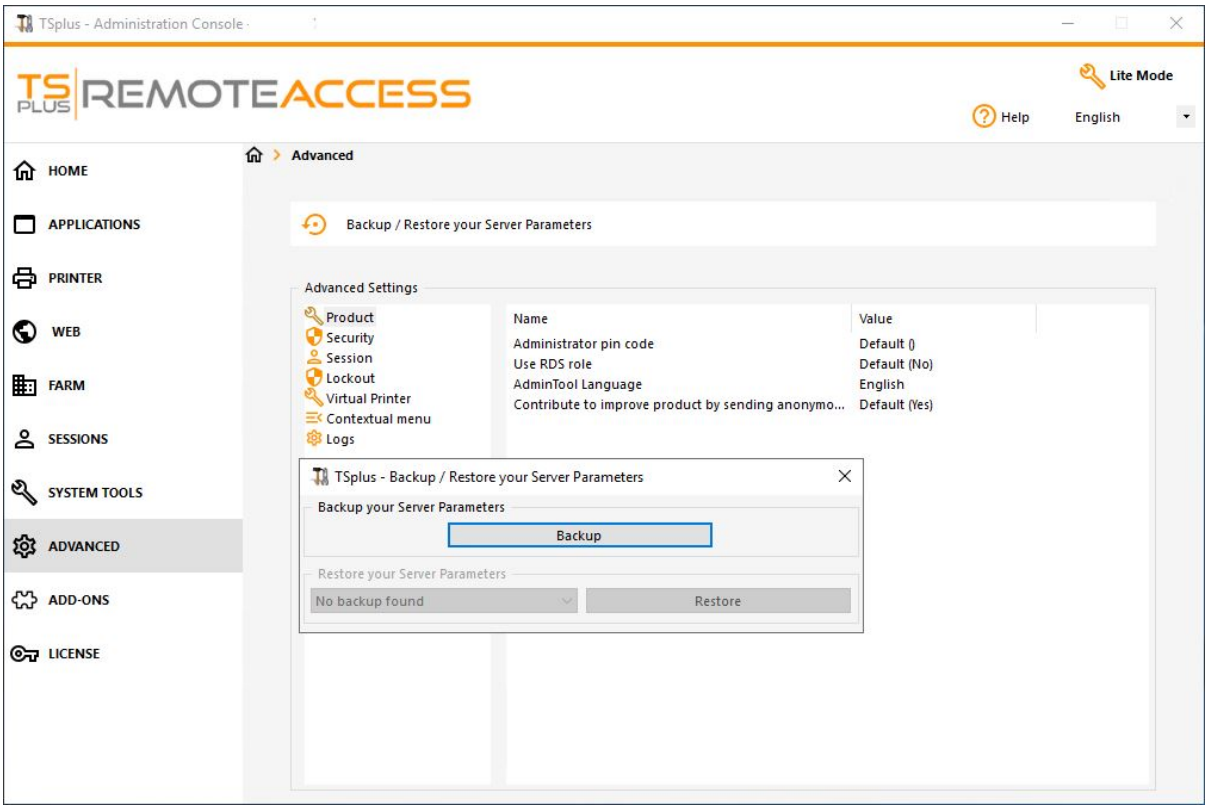


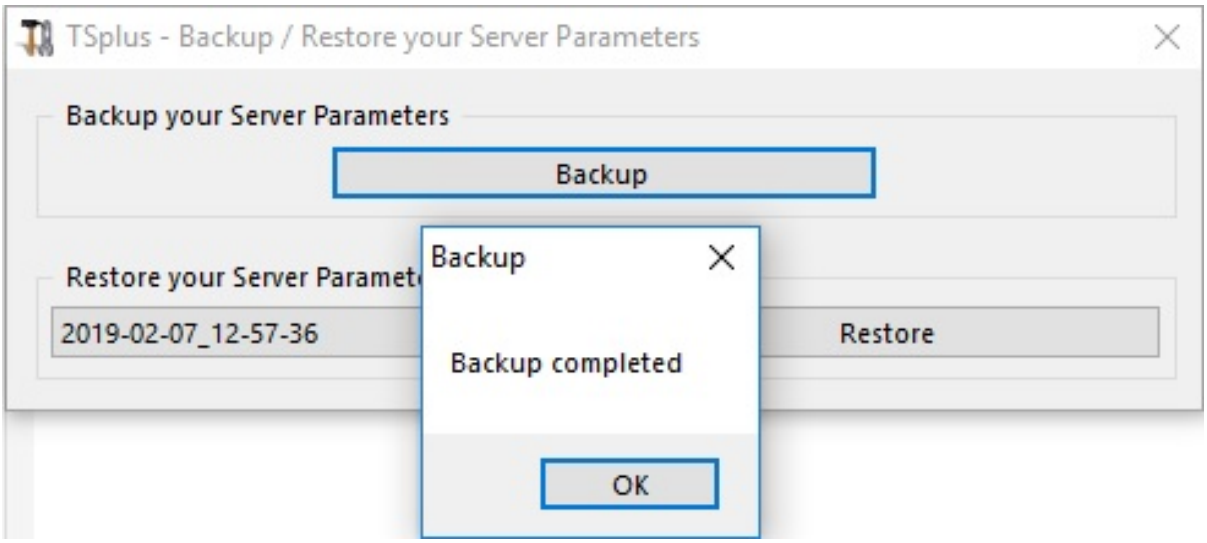
Möchten Sie schnell Hilfe zu einer Funktion des TSplus Admin Tools erhalten? Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!

Sicherung und Wiederherstellung

Seit Version 14 in der **Erweitert** Tab, Sie können die TSplus-Einstellungen konfigurieren.

Sie können TSplus-Daten und -Einstellungen sichern oder wiederherstellen, indem Sie auf die Schaltfläche „Backup/Wiederherstellen“ oben klicken:





Die Verwendung des Befehls wird unten beschrieben:

- **Sicherung** :

admintool.exe /backup [optional path to a directory]

Standardmäßig wird das Backup im Verzeichnis "archives" erstellt, das sich im TSplus TSplus Security-Setup-Ordner befindet. Das Backup kann jedoch in einem angegebenen Ordner gespeichert werden. Relative und absolute Pfade sind erlaubt.

- **Wiederherstellen** :

admintool.exe /restore [Pfad zu einem Sicherungsverzeichnis]

Das angegebene Backup-Verzeichnis muss einen Daten- und einen Einstellungsordner enthalten, die durch den Befehl /backup erstellt wurden.

wenn Sie gerne mit Befehlszeilen arbeiten und sich fragen, welche anderen Befehlszeilen verfügbar sind, besuchen Sie bitte diese spezifische Dokumentation)

Bitte folgen Sie den untenstehenden Schritten, um TSplus von Computer A auf Computer B zu migrieren:

1. Auf Computer A klicken Sie bitte auf die Schaltfläche Backup, um ein neues Backup zu erstellen. Einstellungen und Daten werden im Archivverzeichnis gespeichert, das sich im Ordner C:\Backupparam befindet.

2. Kopiere den neu erstellten Backup-Ordner (z. B. benannt backup-2021-01-29_15-01-29), einschließlich aller Inhalte, vom Archivverzeichnis auf Computer A in das Archivverzeichnis auf Computer B.

3. Auf Computer B, im Fenster Backup / Wiederherstellung, im Abschnitt „Wiederherstellen“, wählen Sie den entsprechenden Backup-Namen aus, der wiederhergestellt werden soll.

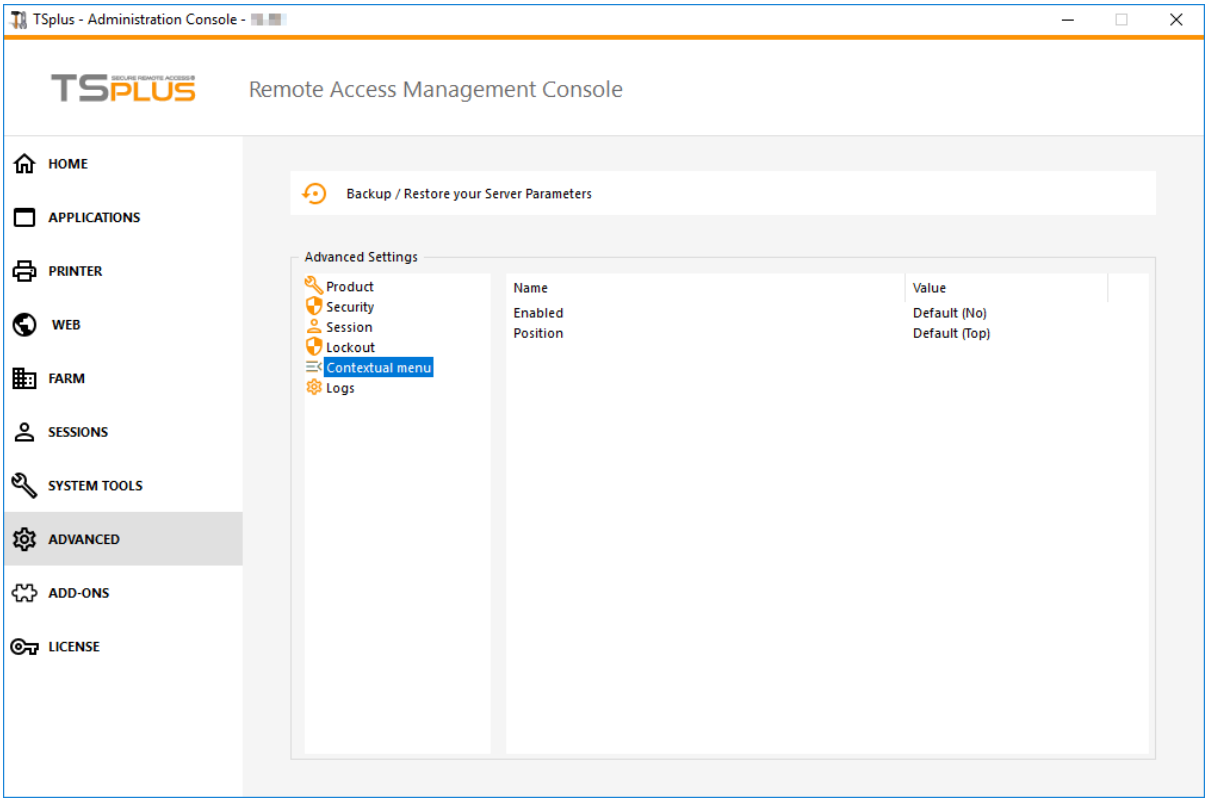
4. Dann klicken Sie auf Nur Einstellungen wiederherstellen, um die Einstellungen wiederherzustellen. Alternativ können Sie auf Wiederherstellen klicken, um alle Daten und Einstellungen wiederherzustellen, was für eine Migration nicht empfohlen wird, aber nützlich ist, um TSplus auf Computer A wiederherzustellen.

5. Bitte warten Sie maximal 2 Minuten, bis die Einstellungen von TSplus-Funktionen neu geladen werden.

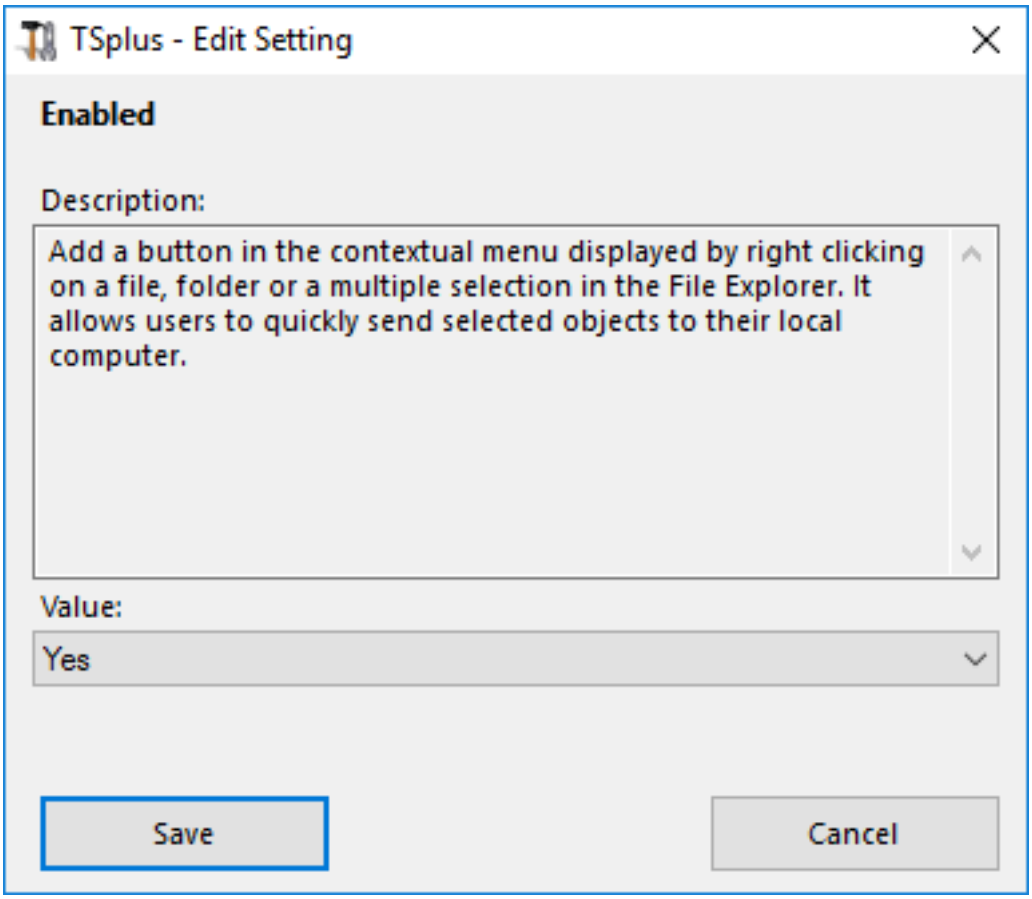
Erweiterte Funktionen - Kontextmenü

Übersicht

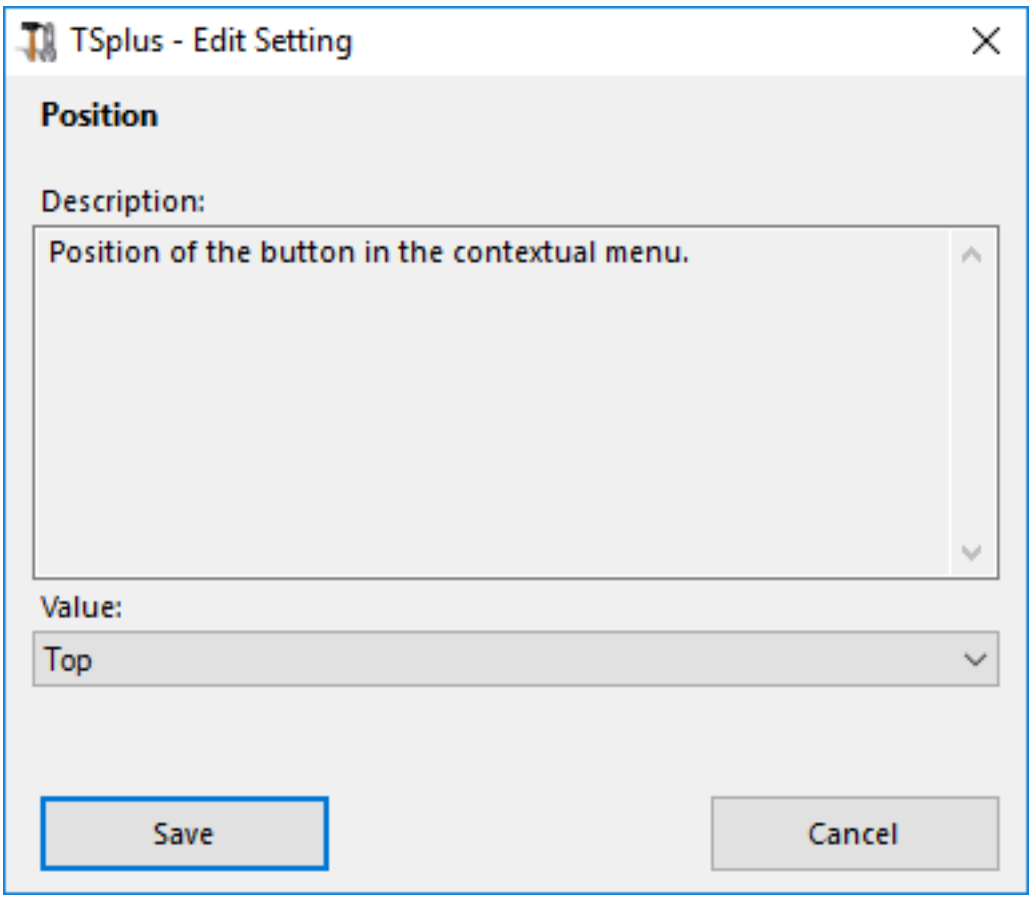
Seit der TSplus-Version 12.50 gibt es eine neue **“An Client senden” Menü** kann unter dem Tab Erweitert > Kontextmenü aktiviert werden, um Dateien einfach an die Arbeitsstation des Clients zu senden. Diese Funktion funktioniert mit allen Verbindungsarten.



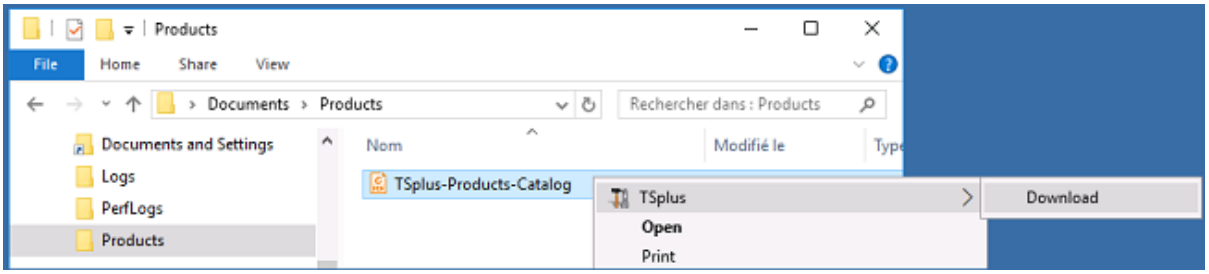
Standardmäßig ist diese Funktion deaktiviert. Wählen Sie den Wert „Ja“ und klicken Sie auf „Speichern“, um sie zu aktivieren.



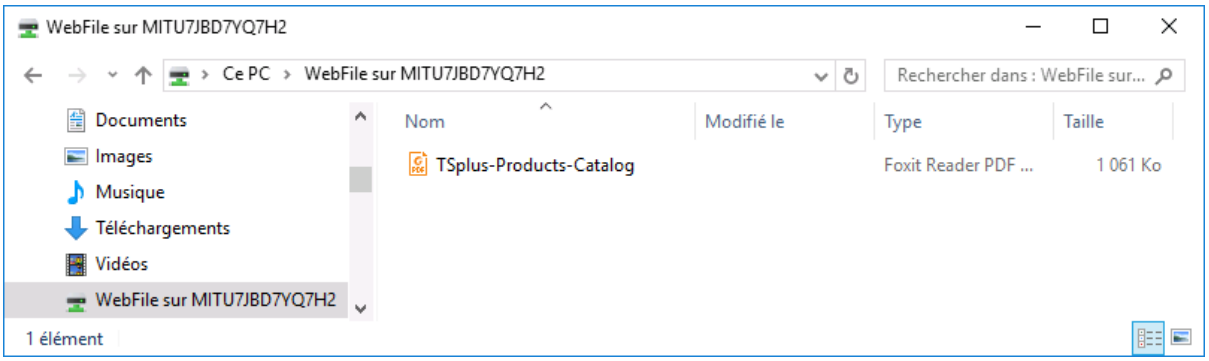
Sie können auch seine Position ändern. Standardmäßig wird es oben angezeigt:



Dies ist ein Kontextmenü für einen Rechtsklick. Wählen Sie einfach den gewünschten Ordner oder die Dateien aus, klicken Sie mit der rechten Maustaste darauf, wählen Sie die Registerkarte „TSplus“ und klicken Sie einfach auf „Herunterladen“.



Sie finden Ihren Download im Webfile-Ordner und im Ordner „Downloads“ Ihres Webbrowsers.

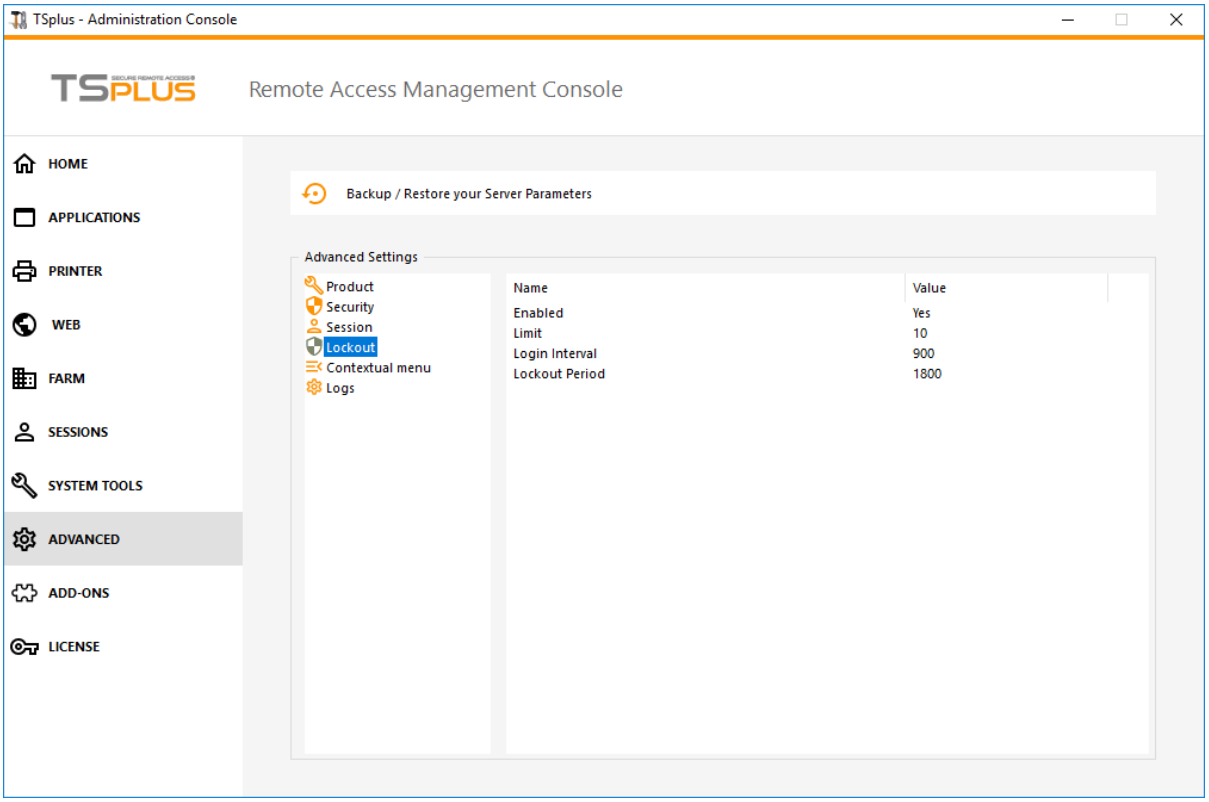


Jeder heruntergeladene Ordner wird automatisch in eine Zip-Datei komprimiert.

Erweiterte Funktionen - Sperrung

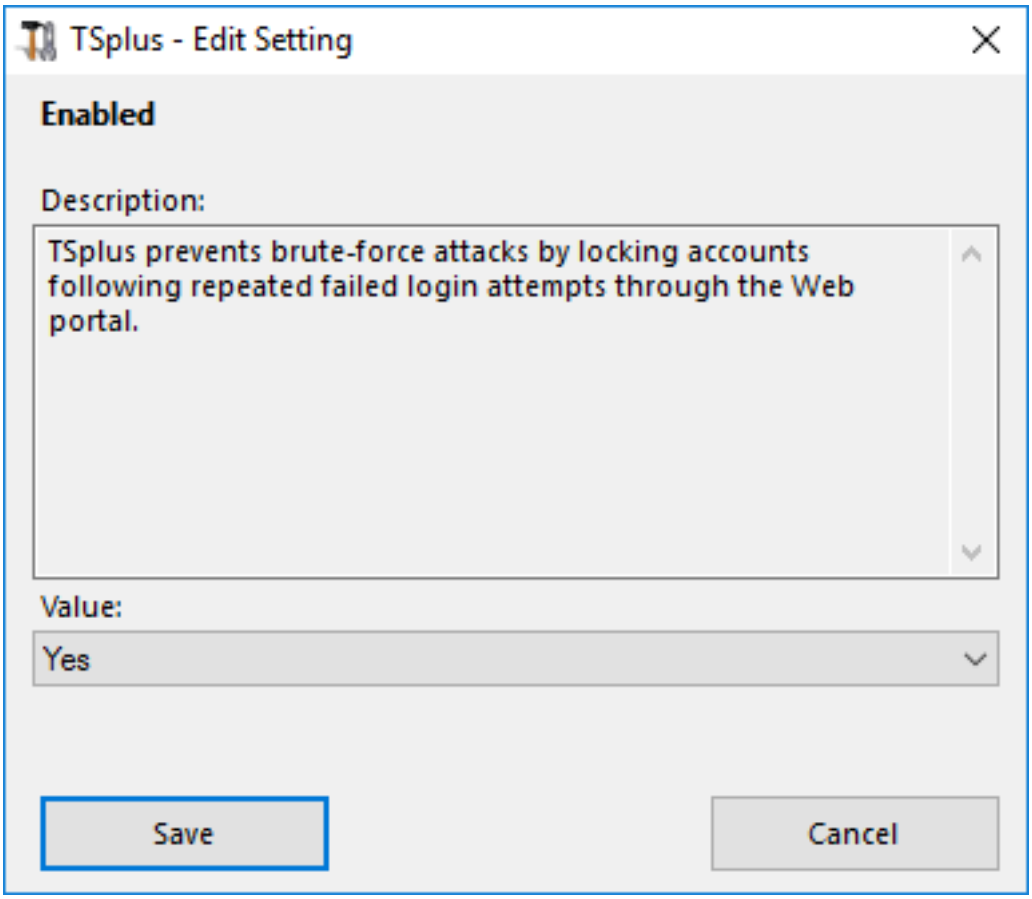
Übersicht

Auf diesem Tab können Sie aktivieren/deaktivieren und konfigurieren. TSplus Sperrung Einstellungen.



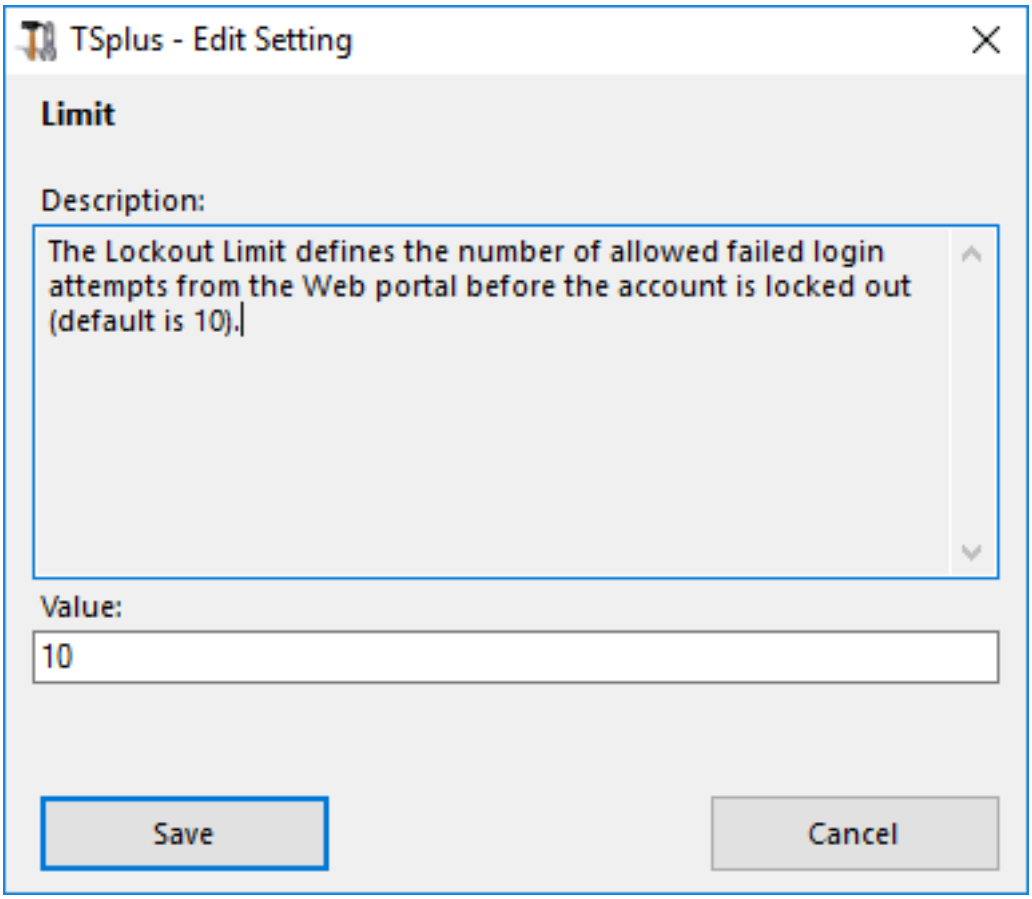
Sperren-Funktion aktivieren/deaktivieren

Die Sperrfunktion ist standardmäßig aktiviert. Sie können sie deaktivieren, indem Sie den Wert in diesem Fenster von „Ja“ auf „Nein“ ändern und dann auf Speichern klicken.



Limit

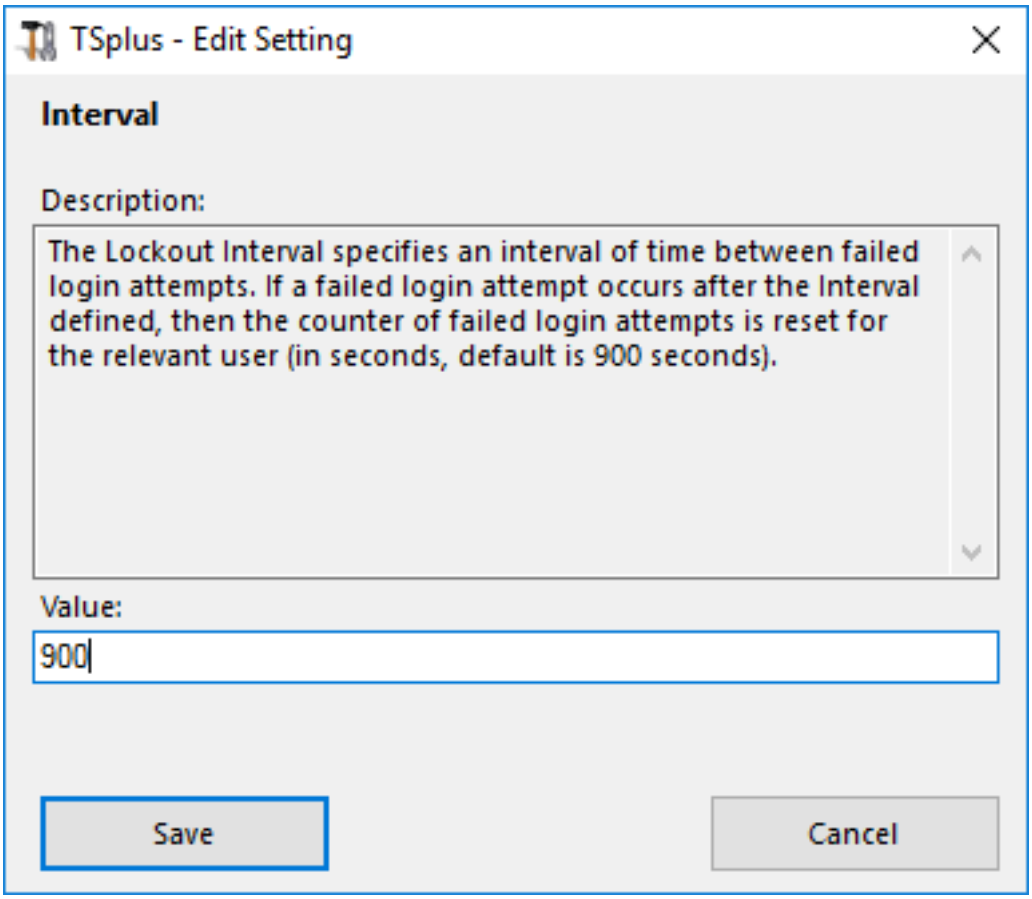
Die Sperrgrenze definiert die Anzahl der erlaubten fehlgeschlagenen Anmeldeversuche über das Webportal, bevor das Konto gesperrt wird (Standard ist 10). Sie können diesen Wert ändern, indem Sie den gewünschten Wert in das entsprechende Feld eingeben und auf Speichern klicken.



Intervall

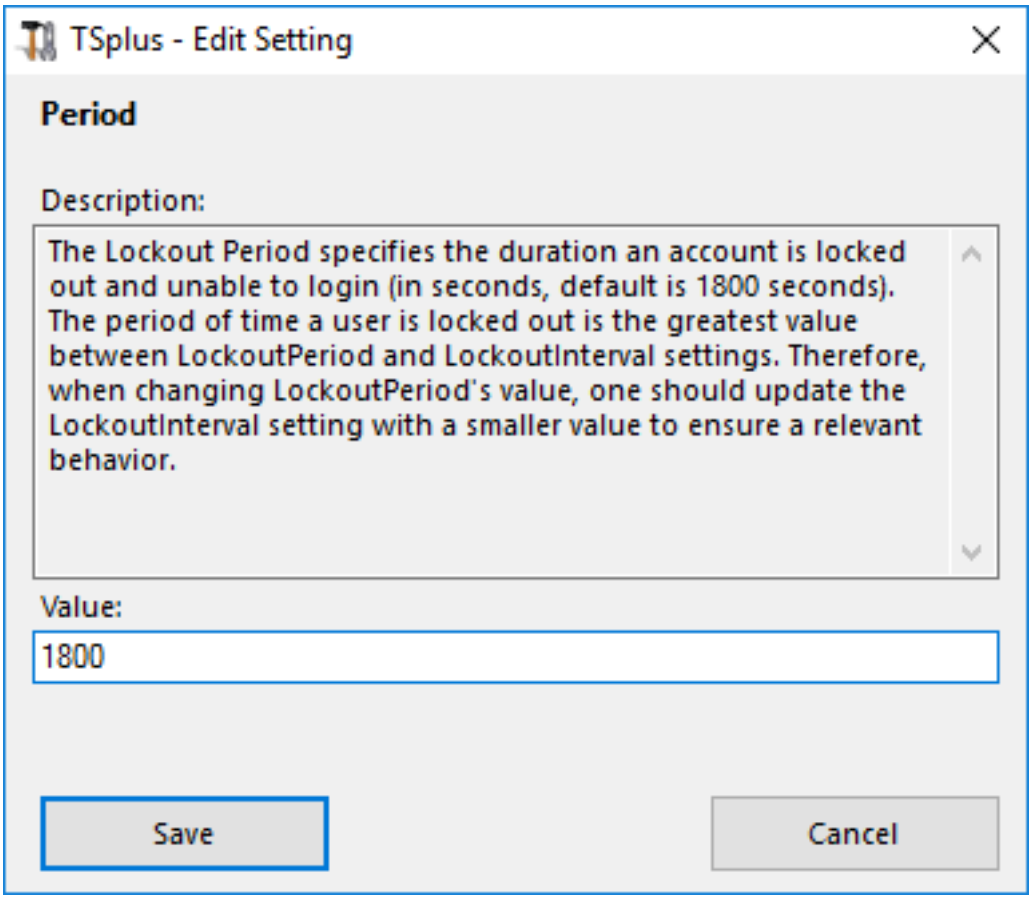
Der Sperrintervall gibt ein Zeitintervall zwischen fehlgeschlagenen Anmeldeversuchen an.

Wenn ein fehlgeschlagener Anmeldeversuch nach dem definierten Intervall auftritt, wird der Zähler für fehlgeschlagene Anmeldeversuche für den betreffenden Benutzer zurückgesetzt (in Sekunden, Standard ist 900 Sekunden). Sie können diesen Wert ändern, indem Sie den gewünschten Wert in das entsprechende Feld eingeben und auf Speichern klicken.



Periode

Der Sperrzeitraum gibt die Dauer an, in der ein Konto gesperrt ist und sich nicht anmelden kann (in Sekunden, Standard ist 1800 Sekunden). Der Zeitraum, in dem ein Benutzer gesperrt ist, ist der größte Wert zwischen den Einstellungen für Sperrzeitraum und Sperrintervall. Daher sollte man beim Ändern des Wertes des Sperrzeitraums auch die Einstellung des Sperrintervalls mit einem kleineren Wert aktualisieren, um ein relevantes Verhalten sicherzustellen. Sie können diesen Wert ändern, indem Sie den gewünschten Wert in das entsprechende Feld eingeben und auf Speichern klicken.


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

Erweiterte Funktionen - Protokolle

Übersicht

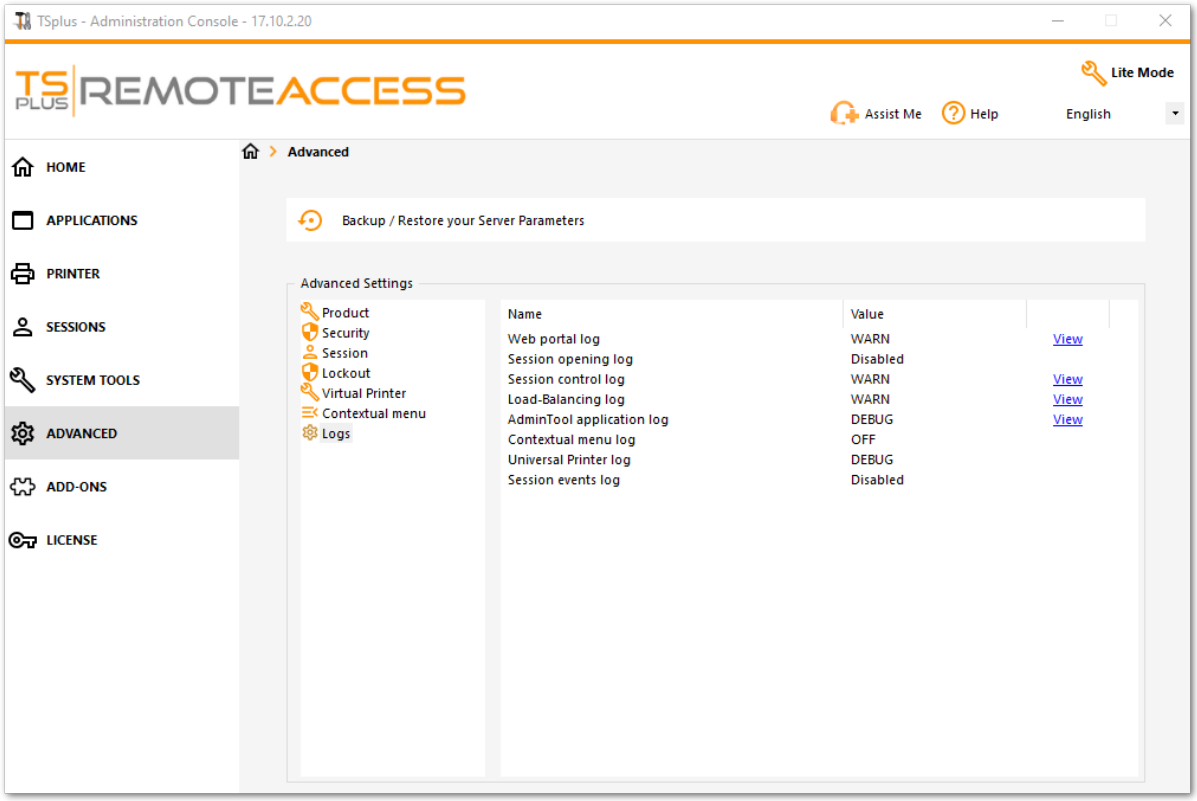
Auf diesem Tab können Sie die Einstellungen für TSplus-Protokolle konfigurieren.

Standardmäßig erstellt TSplus keine Protokolle, um Leistungsprobleme zu vermeiden.

Logs exist to find more easily the origin of the errors encountered on TSplus and you can enable them by doing so:

- gehe zu C:\wsession
- Erstellen Sie den Ordner 'Trace'. Pro Benutzer werden dort automatisch Protokolle erstellt.

Sie müssen die Protokollgenerierung im AdminTool > Erweitert > Protokolle aktivieren.



Es gibt 5 Arten von Protokollen:

- Das Webportal-Protokoll,
- Das Sitzungsöffnungsprotokoll,
- Das Sitzungsprotokoll
- Das Lastenausgleichsprotokoll und
- Die AdminTool-Anwendung (Schnittstelle) Protokoll.

Die Protokollebene entspricht verschiedenen Komponenten, unser Support-Team wird Ihnen sagen, welchen Wert Sie je nach aufgetretenem Problem eingeben sollen.

Hier sind die verschiedenen Protokolldateinamen und -standorte:

- Web-Portal-Protokoll: “C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\hb.log”

- Sitzungsöffnungsprotokoll: “C:\wsession\trace”
- Sitzungskontrollprotokoll: “C:\Program Files (x86)\TSplus\UserDesktop\files\APSC.log”
- Lastverteilung Protokoll: “C:\Program Files (x86)\TSplus\UserDesktop\files\svcenterprise.log”
- AdminTool-Anwendungsprotokoll: “C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.log”
- RDS-Knight / TSplus Advanced Security: “C:\Program Files (x86)\TSplus-Security\logs”

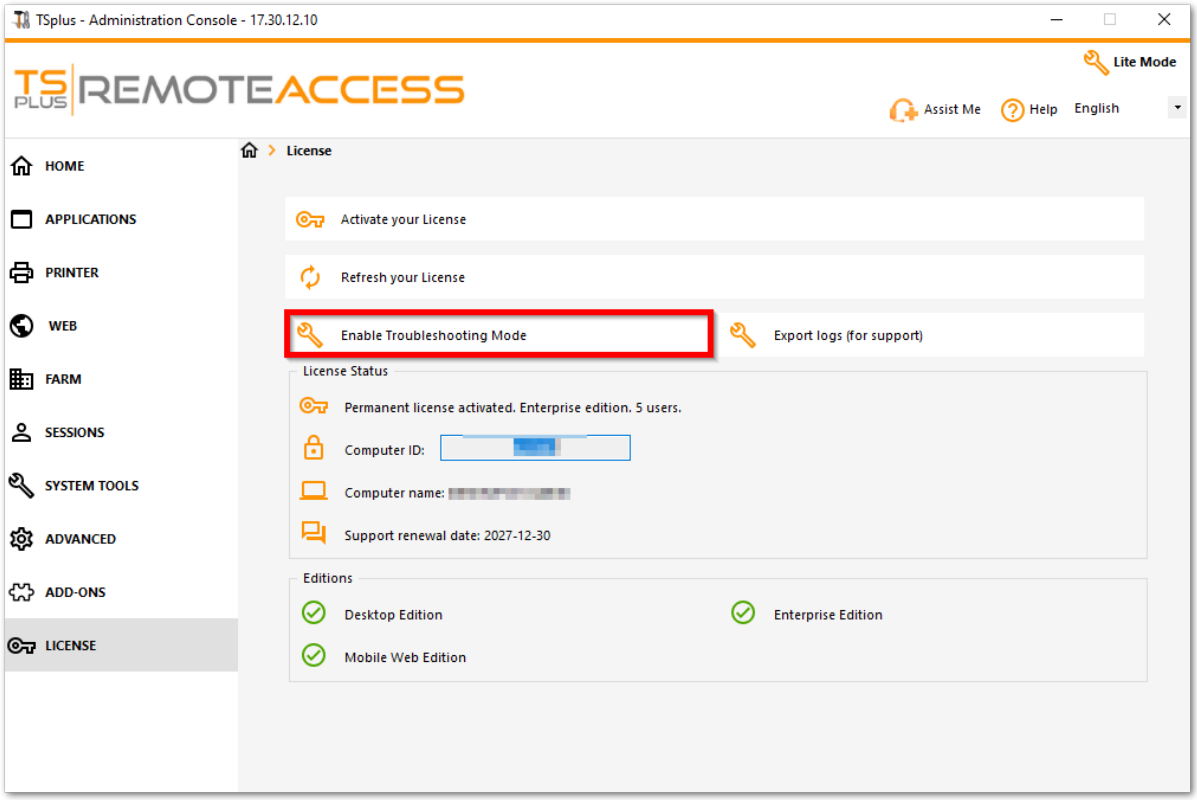
Sie können die Protokolle für den Verbindungsclient auf der Client-Seite aktivieren, indem Sie den folgenden Registrierungsschlüssel hinzufügen:

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

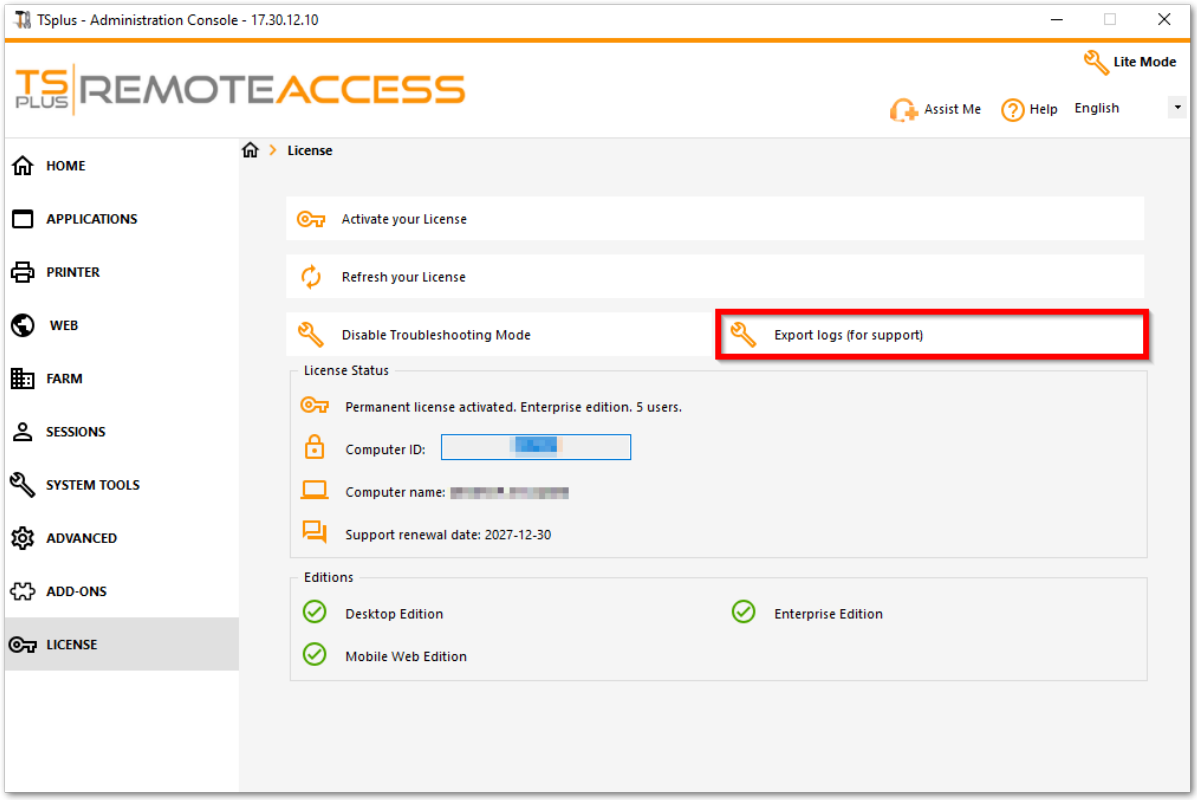
Die Protokolle befinden sich in C:\Users RDP6\logs-Verzeichnis, wenn die Installation benutzerspezifisch ist, oder im C:\Program Files (x86)\Connection Client\RDP6\logs-Verzeichnis, wenn die Installation für alle Benutzer erfolgt.

Fehlerbehebungsmodus aktivieren

Gehe zum Tab "Lizenz" Klicke auf die **“Fehlerbehebungsmodus aktivieren”** Taste.



Reproduzieren Sie Ihr Problem, klicken Sie dann auf die **Exportprotokolle (für den Support)** Taste, um die Protokolle per E-Mail an das Support-Team zu senden.



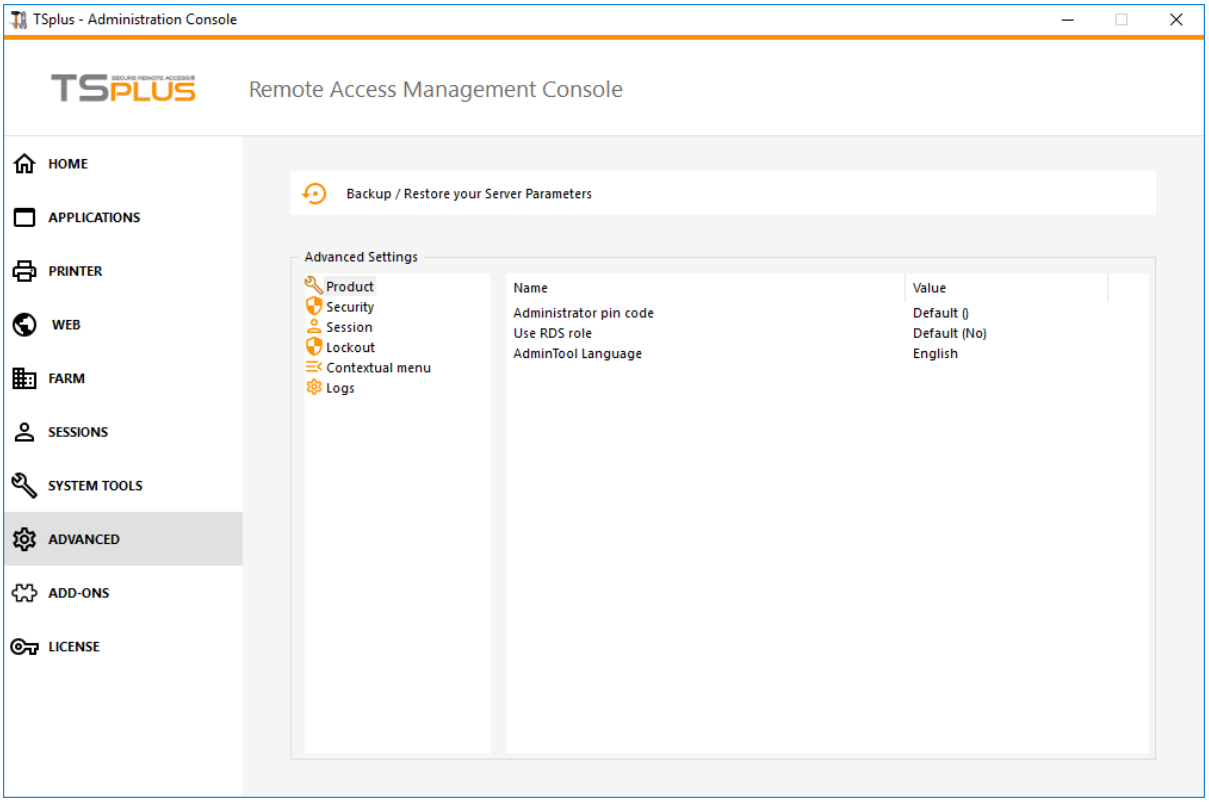


Das Format der zu sendenden Datei ist **.zip.Protokolle** Dateien und ist durch das Passwort geschützt **„Passwort“** .

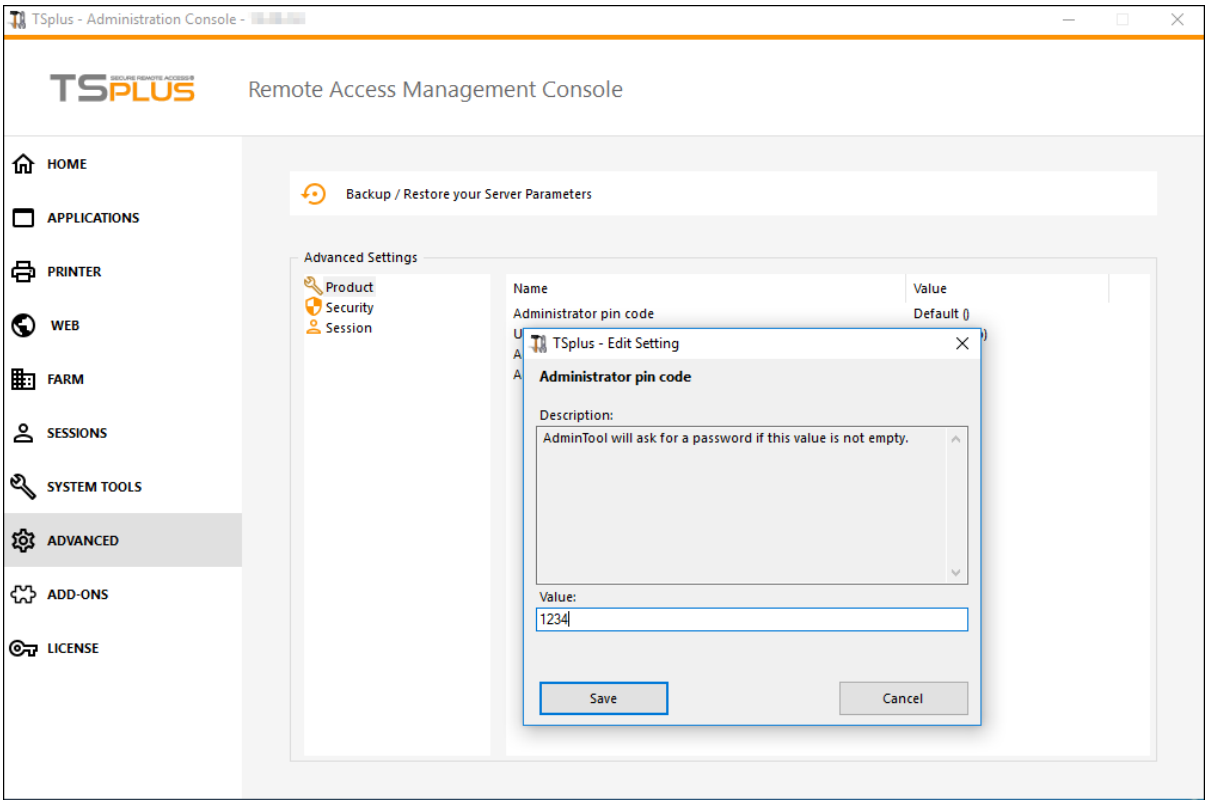
Erweiterte Funktionen - Produkt

Übersicht

Auf diesem Tab können Sie die TSplus-Einstellungen ändern, indem Sie einen AdminTool-Pincode hinzufügen, die Windows RDS-Rolle verwenden und die Hintergrundfarbe sowie die Sprache des AdminTools anpassen.



Der Administrator kann den Zugriff auf das Administrator-Tool sichern, indem er einen PIN-Code festlegt, der bei jedem Start abgefragt wird, im Reiter "Erweitert" des AdminTools, unter den Produkteinstellungen:

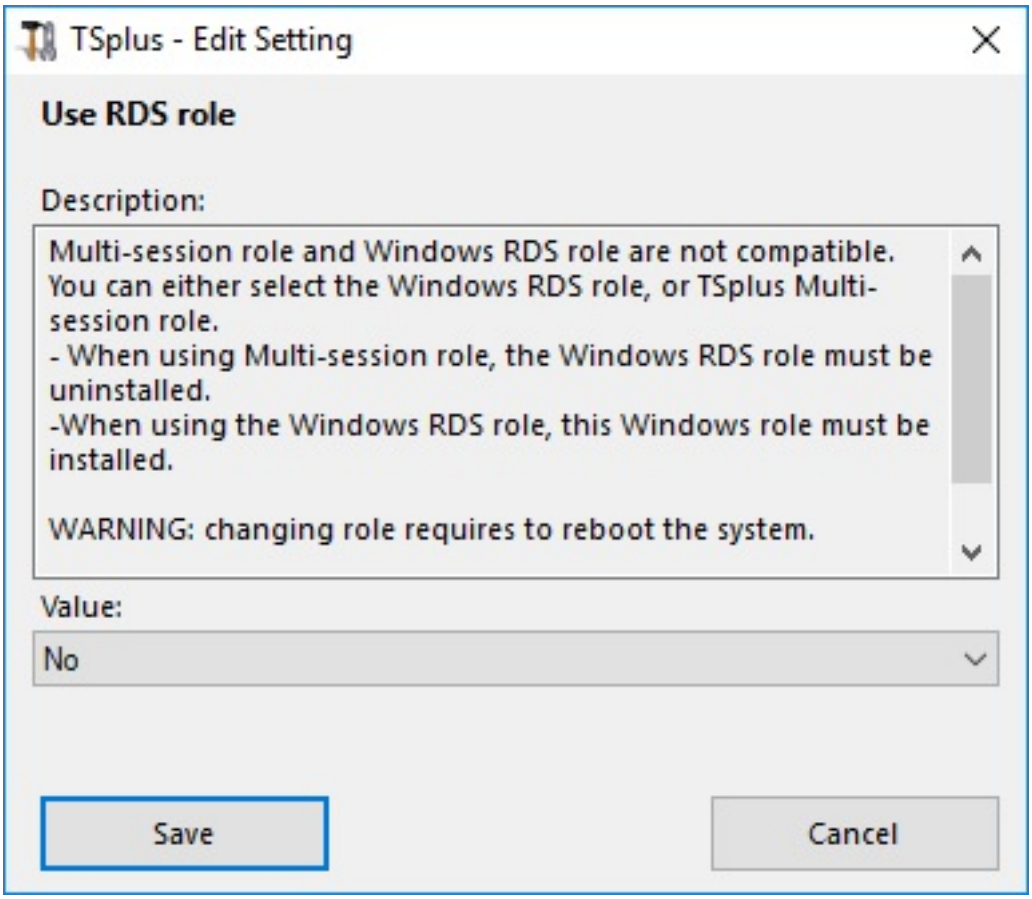


RDS-Rolle verwenden

Multi-Session-Rolle und Windows RDS-Rolle sind nicht kompatibel. Sie können entweder die Windows RDS-Rolle oder die TSplus Multi-Session-Rolle auswählen.

- Beim Verwenden der Multi-Session-Rolle muss die Windows RDS-Rolle deinstalliert werden.
- Beim Einsatz der Windows RDS-Rolle muss diese Windows-Rolle installiert sein.

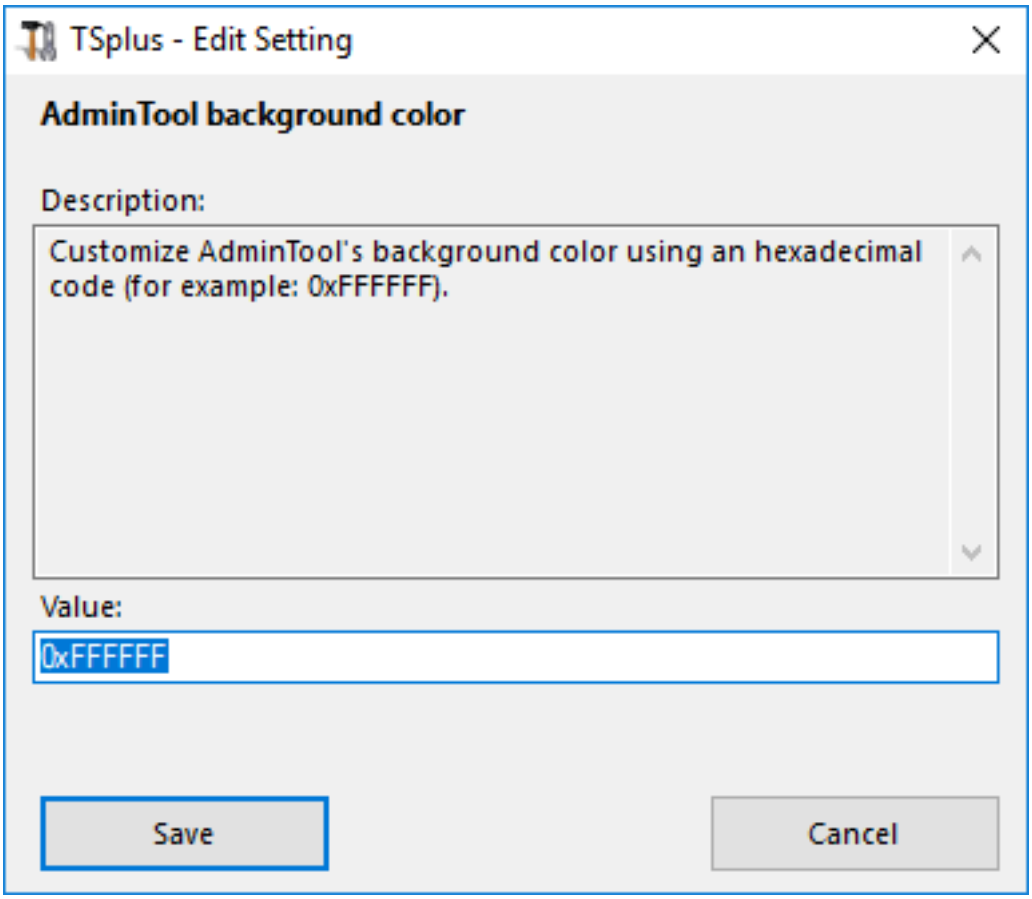
WARNUNG Ändern der Rolle erfordert einen Neustart des Systems. Bei der Auswahl des Windows Remote Desktop ist nur ein Benutzer gleichzeitig auf einem Arbeitsplatzsystem erlaubt.



Um die Windows RDS-Rolle zu verwenden, wählen Sie den Wert „Ja“ und speichern Sie.

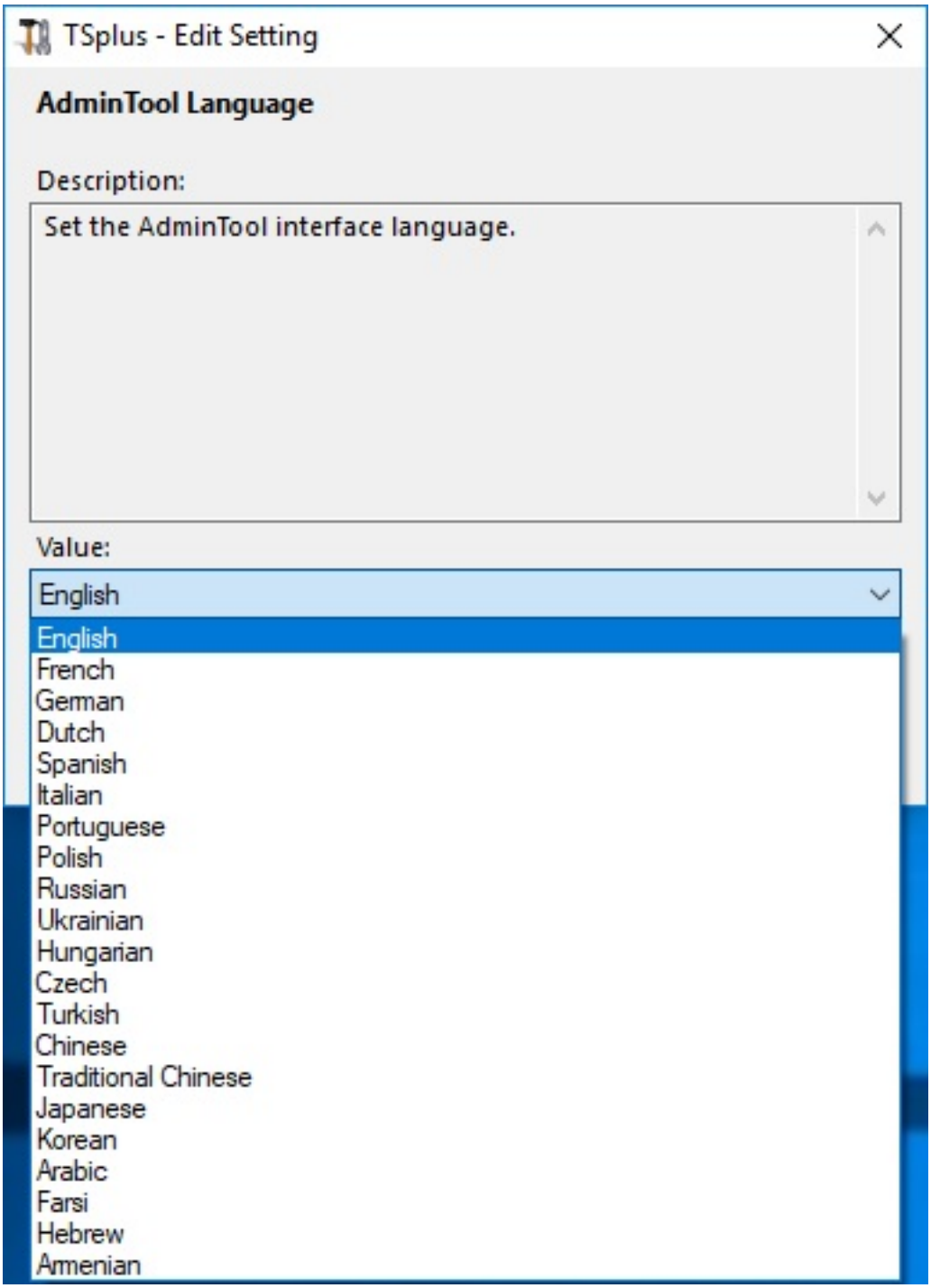
Ändern Sie die Hintergrundfarbe des AdminTools

Passen Sie die Hintergrundfarbe des AdminTools mit einem hexadezimalen Code an (zum Beispiel: 0xFFFFFF).



AdminTool-Sprache ändern

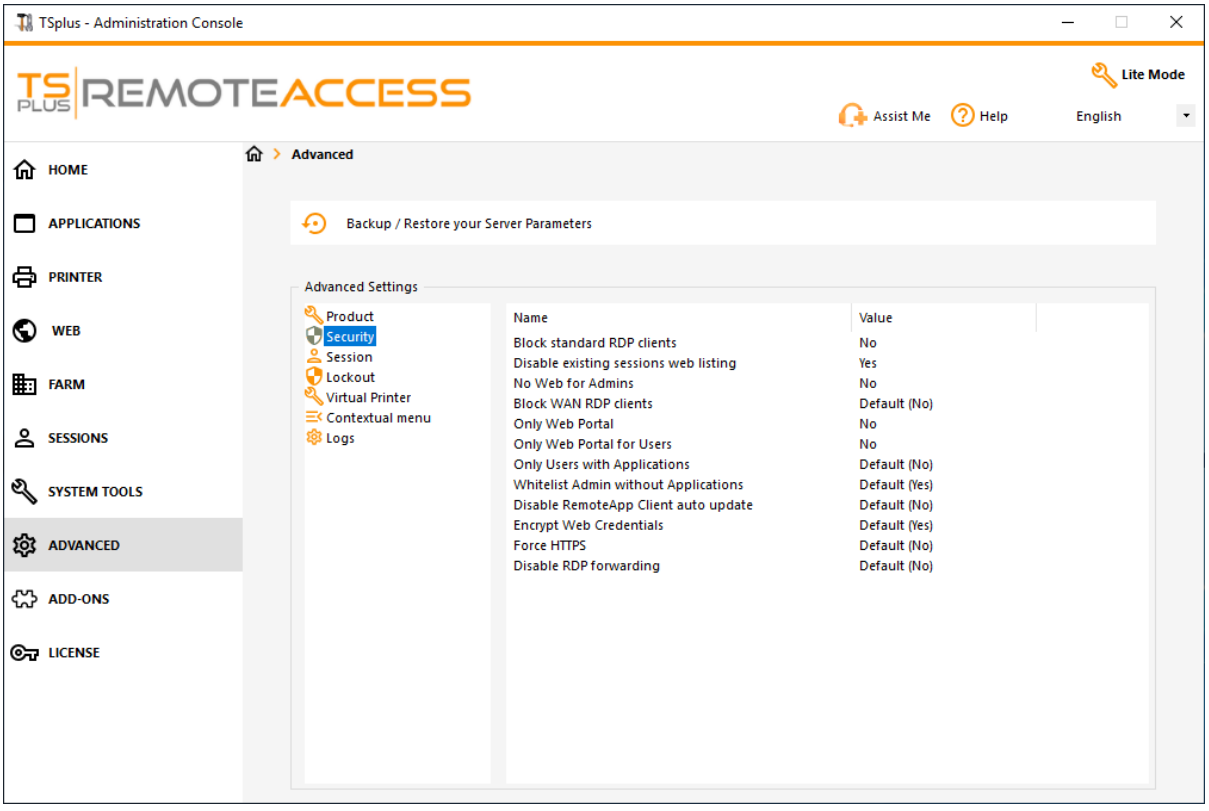
Wählen Sie Ihre bevorzugte Sprache für das AdminTool aus den 21 verfügbaren aus.


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

Erweiterte Funktionen - Sicherheit

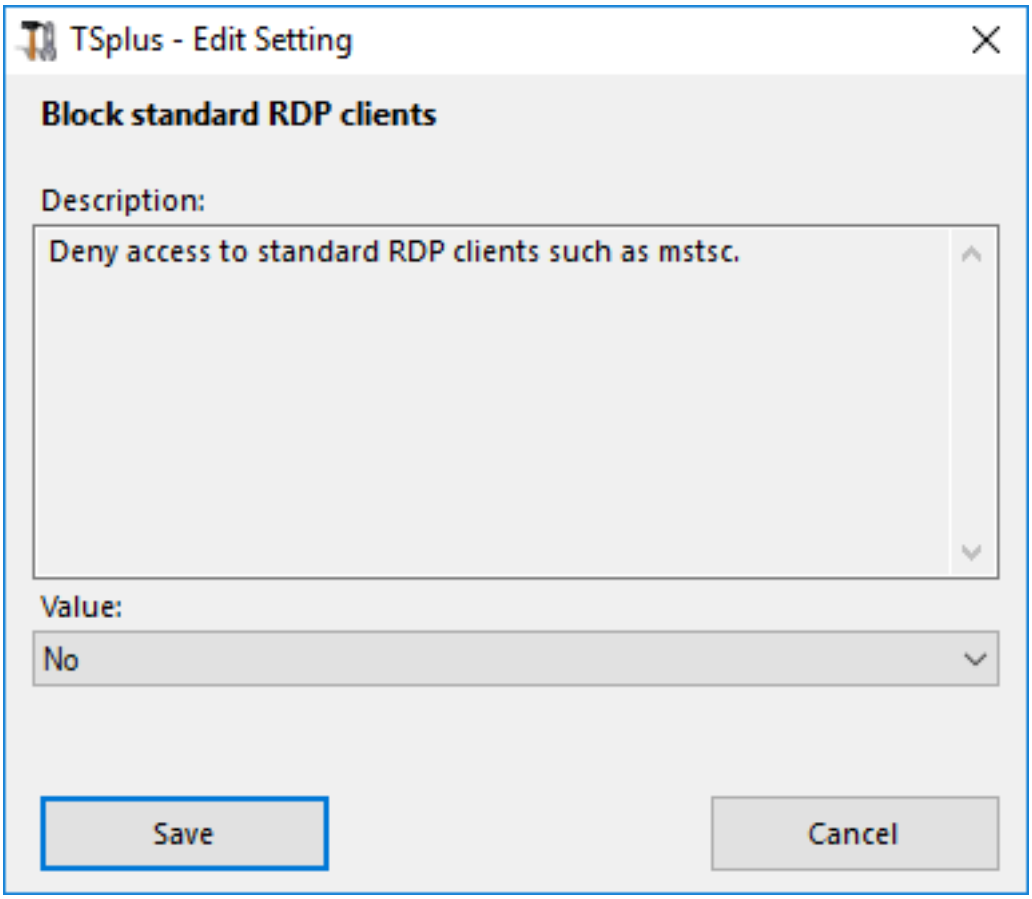
Übersicht

Im Abschnitt Sicherheit der erweiterten Funktionen können Sie Verbindungstypen für Benutzer blockieren, deaktivieren oder anpassen.



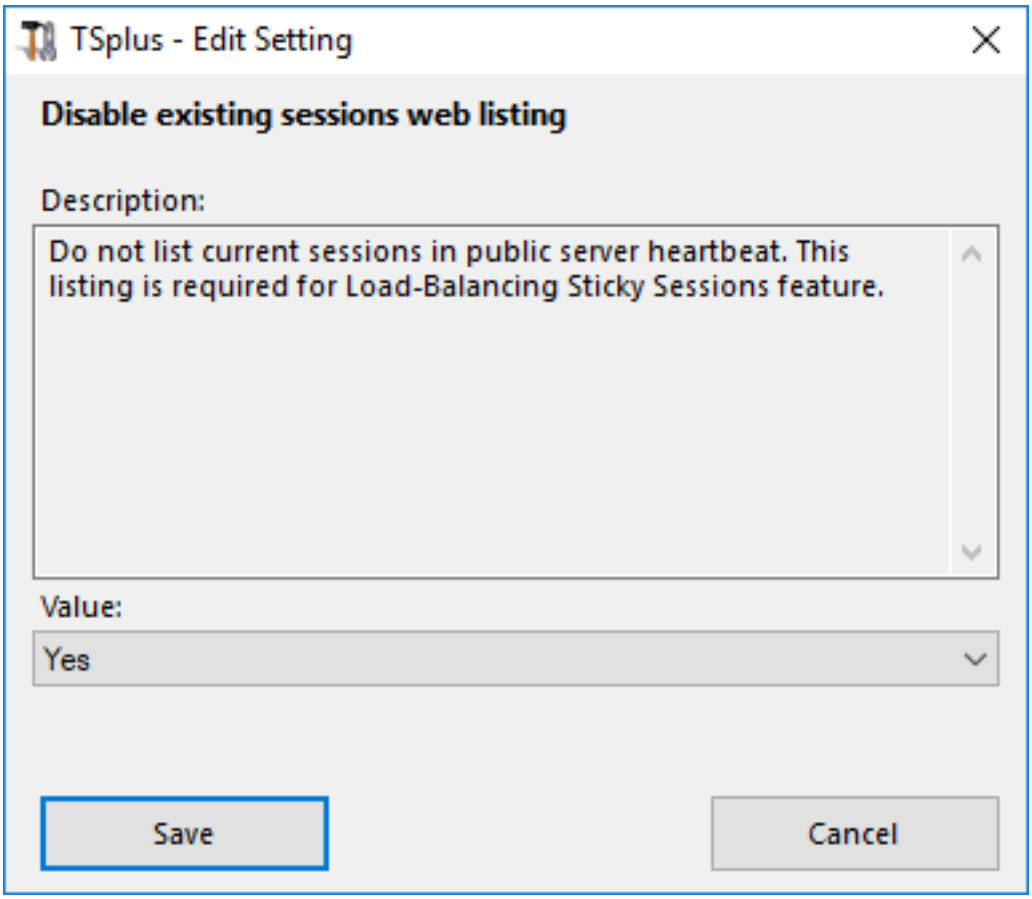
Block Standard RDP-Clients

Wählen Sie den Wert „Ja“, wenn Sie den Zugriff auf standardmäßige RDP-Clients wie mstsc für Ihre Benutzer verweigern möchten.



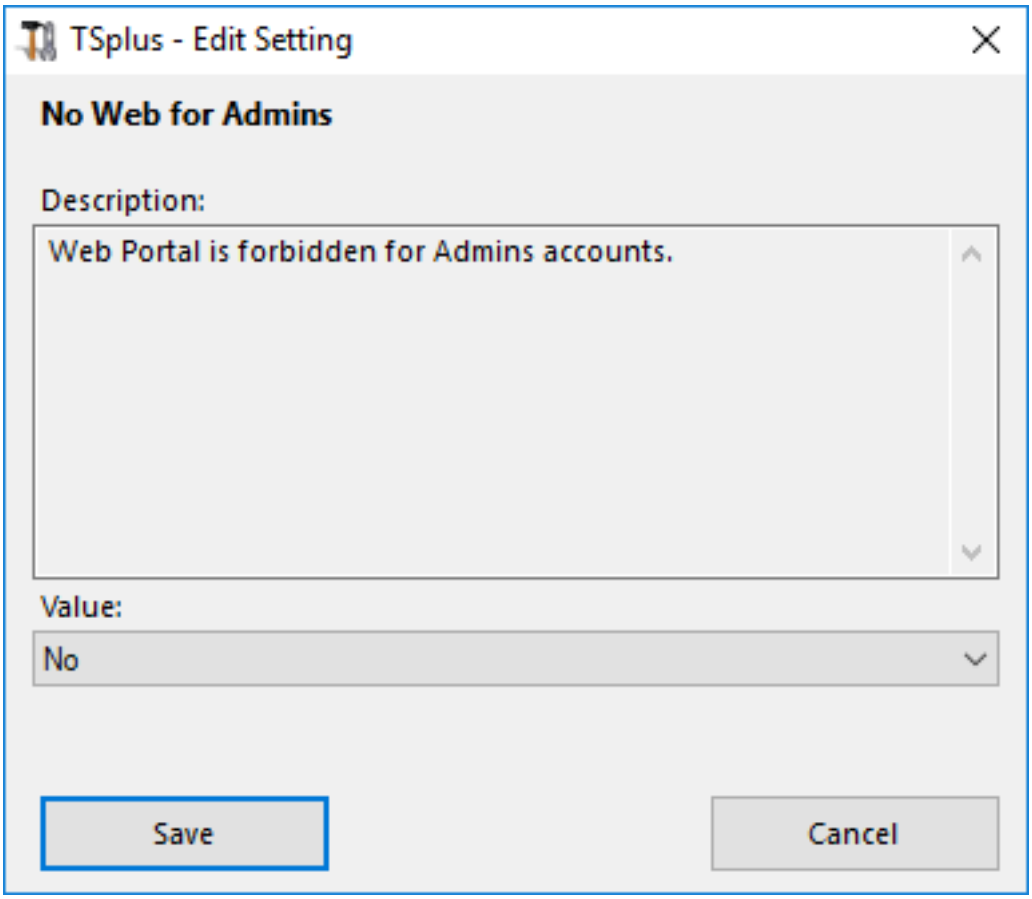
Deaktivieren Sie die vorhandenen Sitzungen in der Webauflistung

Diese Auflistung ist für die Funktion Load-Balancing Sticky Sessions erforderlich und standardmäßig aktiviert. Wenn Sie es deaktivieren möchten, wählen Sie den Wert „Nein“ in diesem Fenster aus und klicken Sie dann auf Speichern:



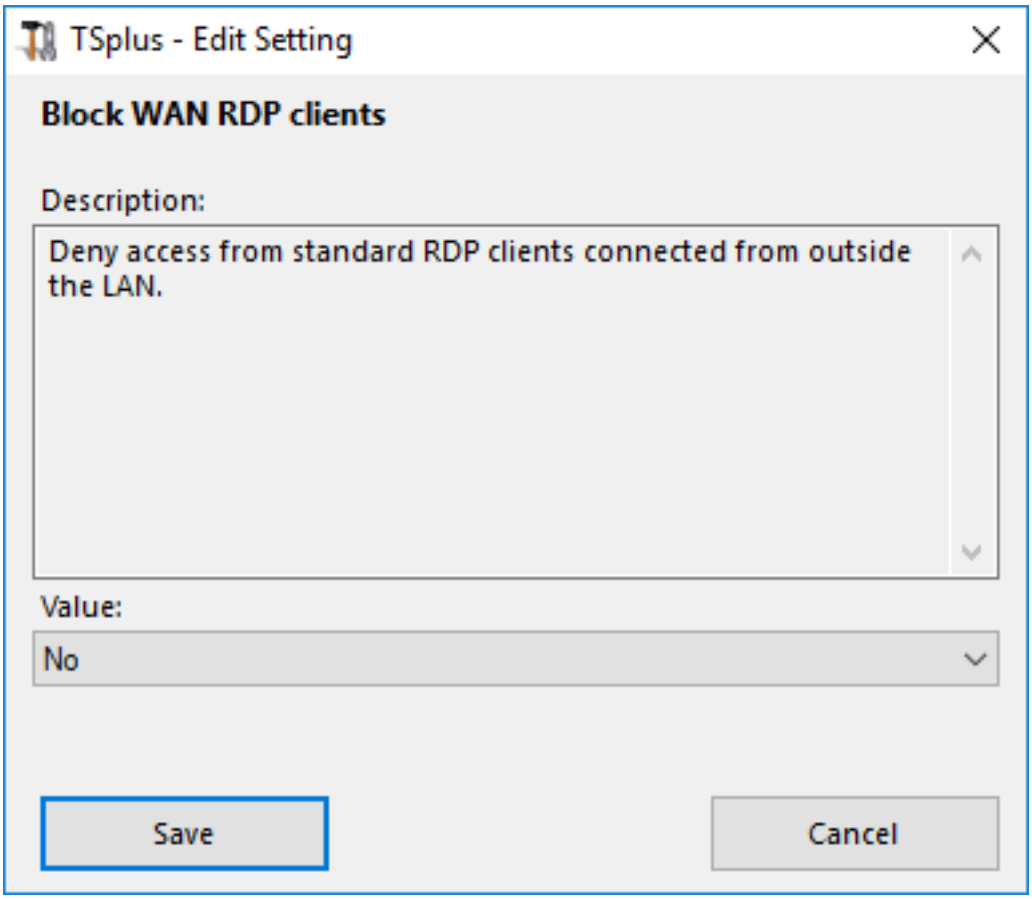
Kein Web für Administratoren

Deaktivieren Sie das Webportal für Administratoren, indem Sie den Wert „Ja“ auswählen:



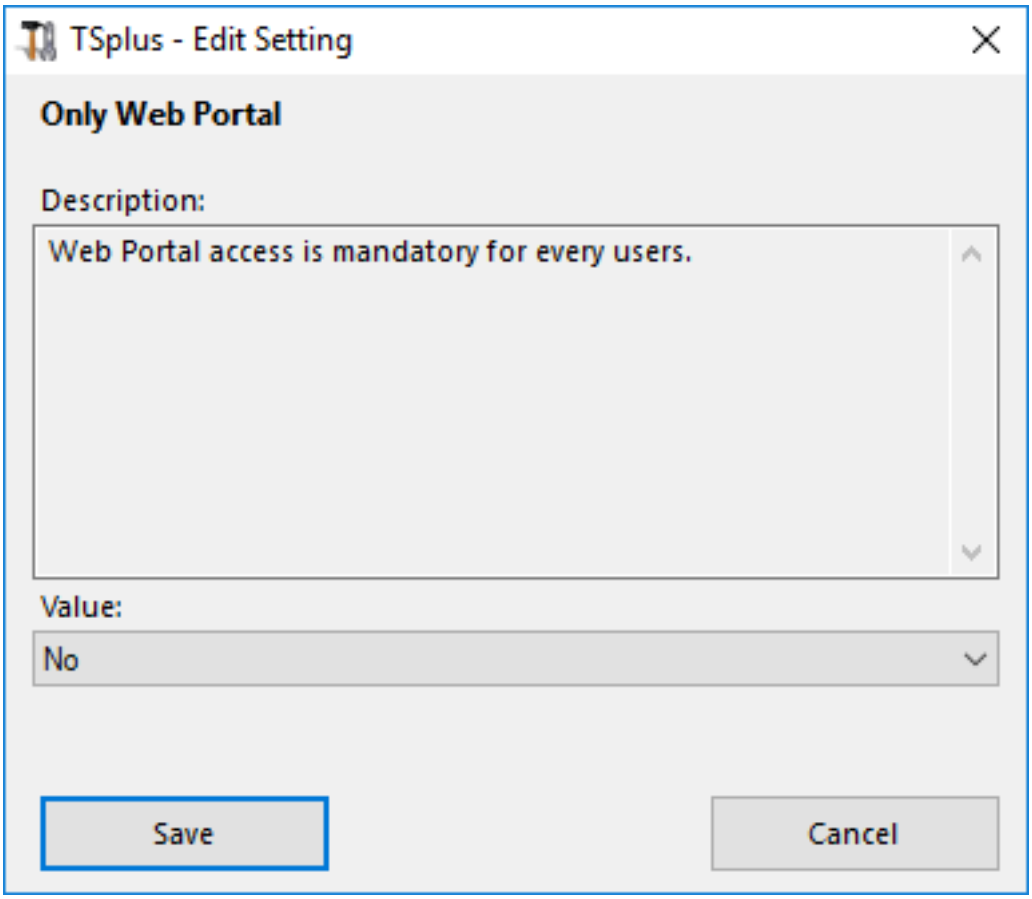
Block WAN RDP-Clients

Zugriff von standardmäßigen RDP-Clients, die von außerhalb des LANs verbunden sind, verweigern, indem Sie den Wert „Ja“ auswählen.



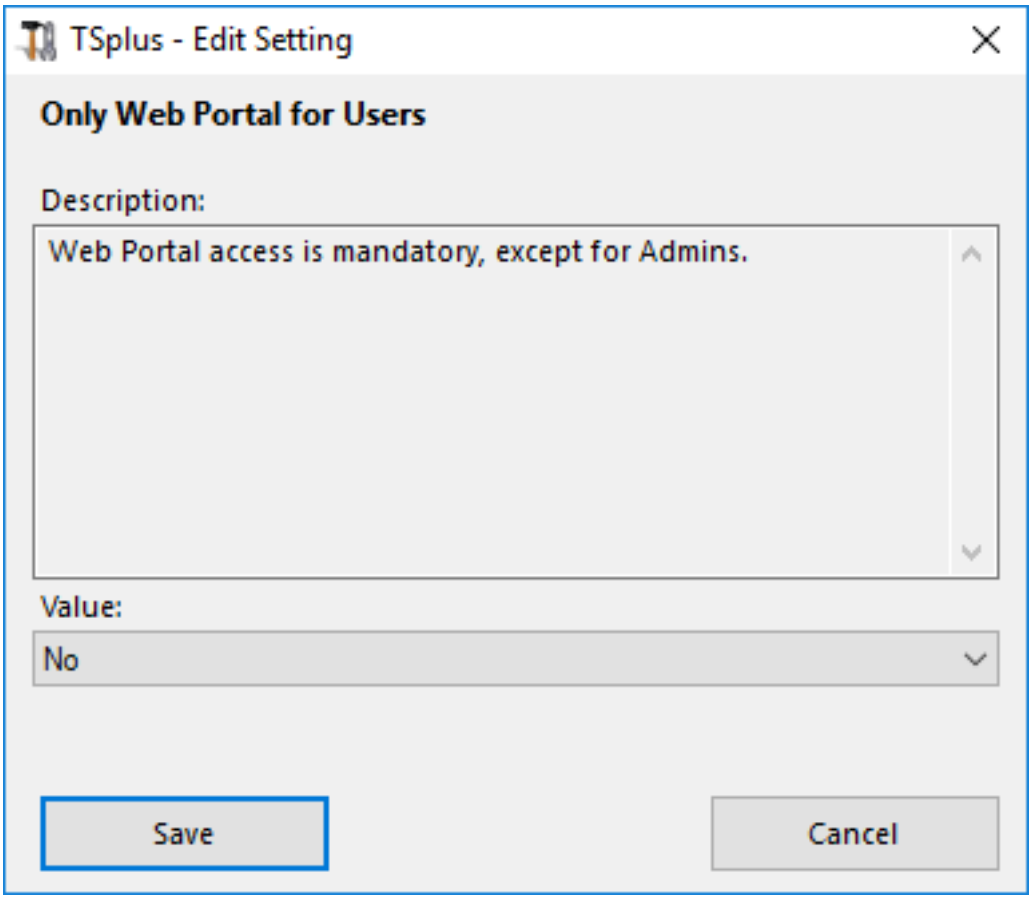
Nur Webportal

Webportal-Zugriff für jeden Benutzer verpflichtend machen, indem der Wert „ja“ ausgewählt wird.



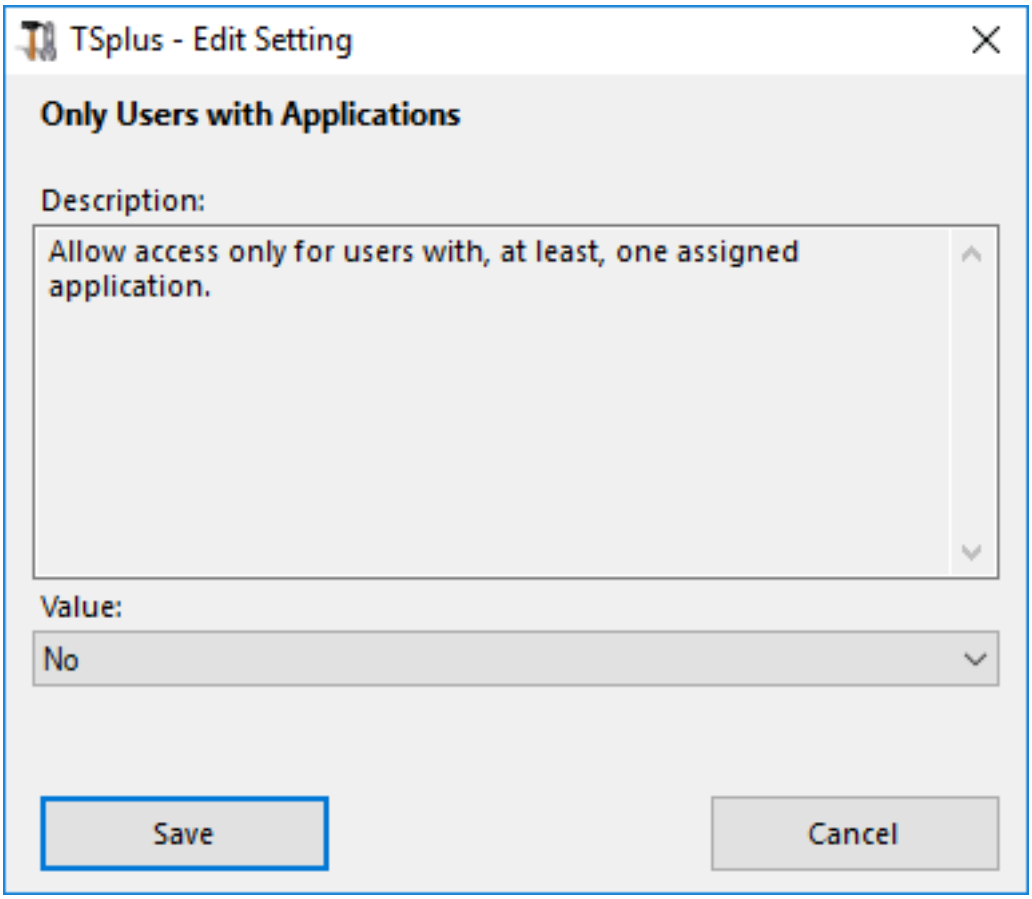
Nur Webportal für Benutzer

Webportalzugang für jeden Benutzer, außer für die Administratoren, durch Auswahl des Wertes „ja“ verpflichtend machen.



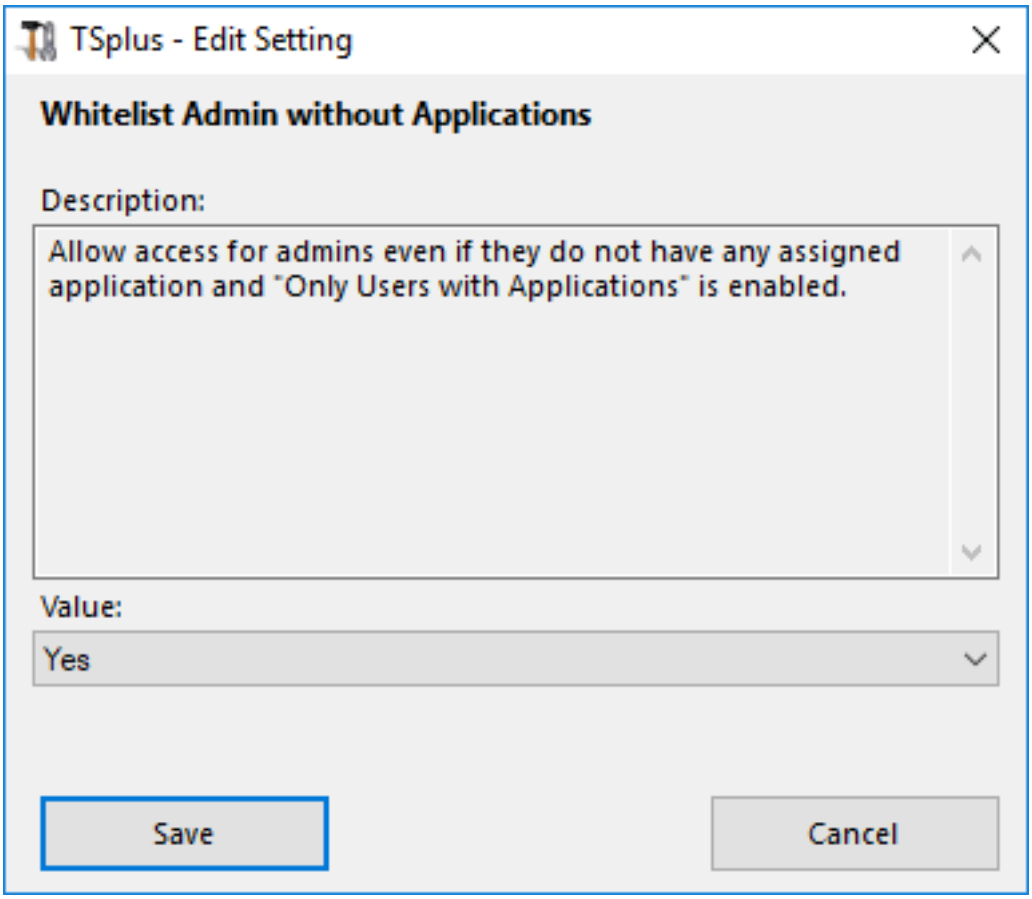
Nur Benutzer mit Anwendungen

Zugriff nur für Benutzer erlauben, die mindestens eine zugewiesene Anwendung haben, indem Sie den Wert "ja" auswählen.



Whitelist-Administratoren ohne Anwendungen

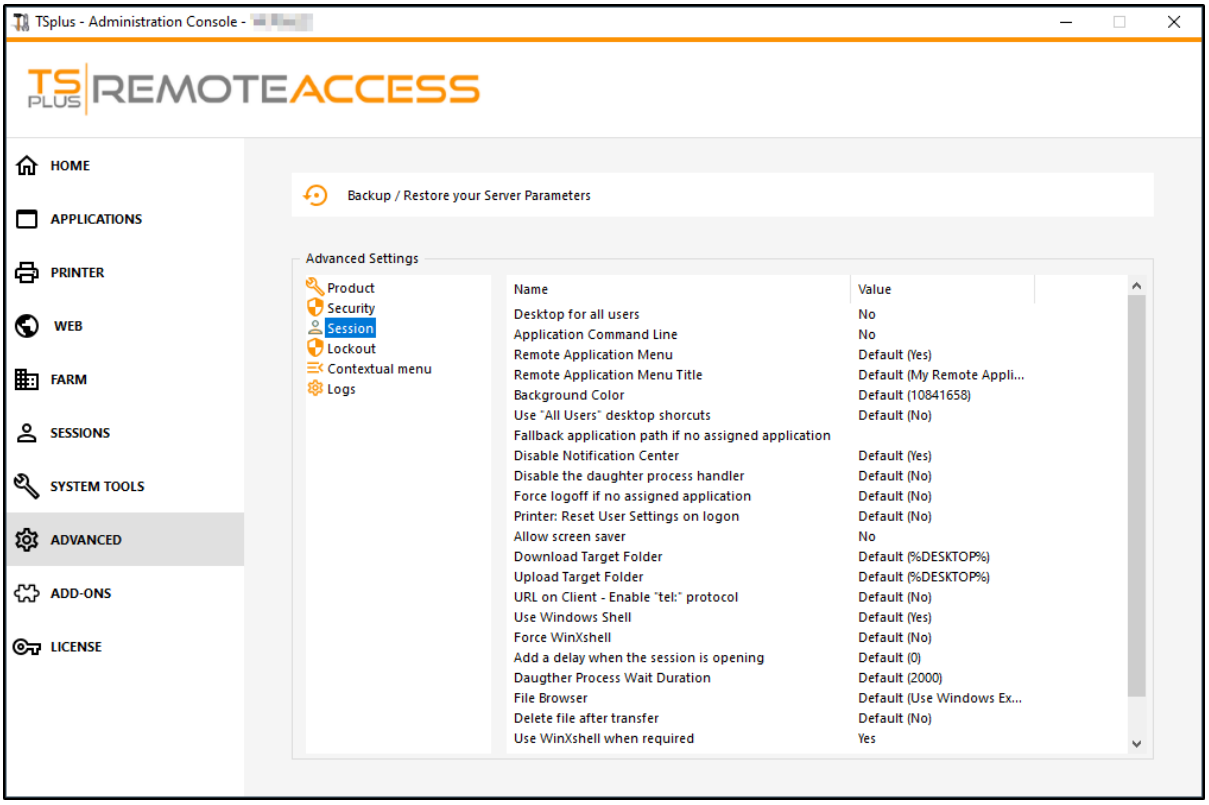
Zugriff für Administratoren erlauben, auch wenn sie keine zugewiesene Anwendung haben und „Nur Benutzer mit Anwendungen“ aktiviert ist. Diese Funktion ist standardmäßig aktiviert. Wenn Sie sie deaktivieren möchten, wählen Sie den Wert „Nein“ in diesem Fenster aus und klicken Sie dann auf Speichern:


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

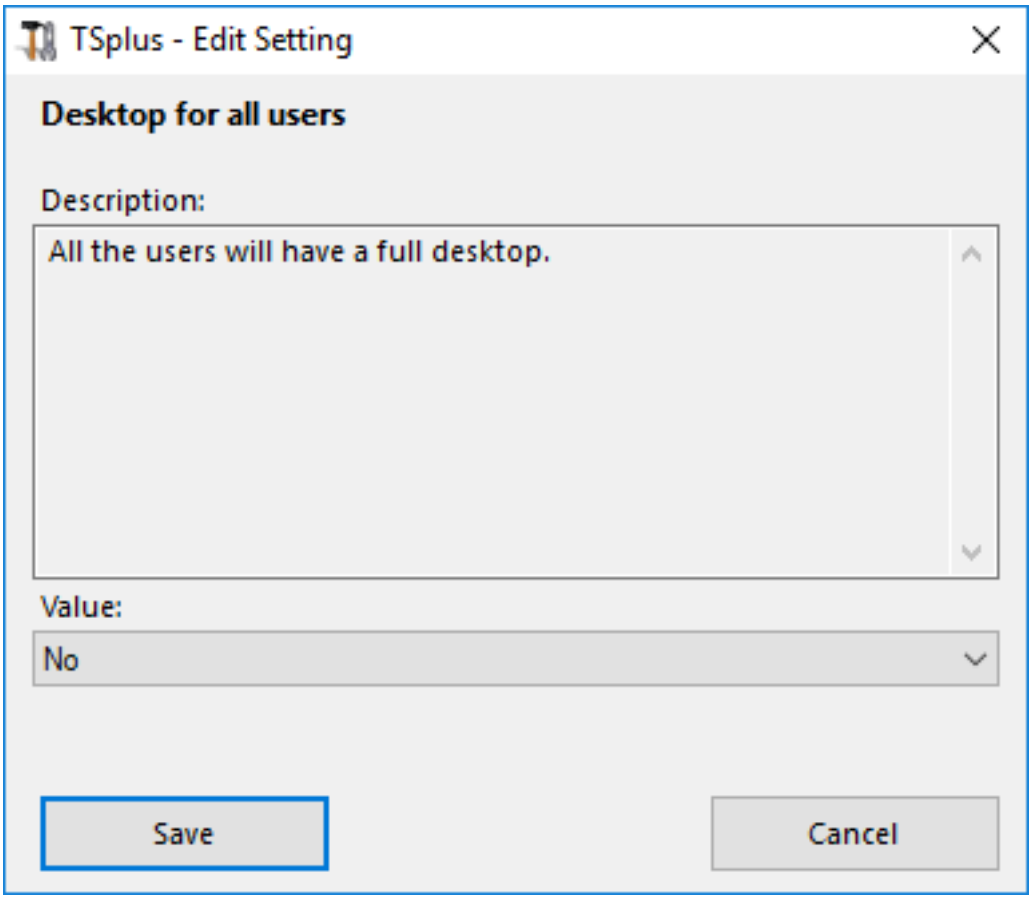
Erweiterte Funktionen - Sitzung

Übersicht

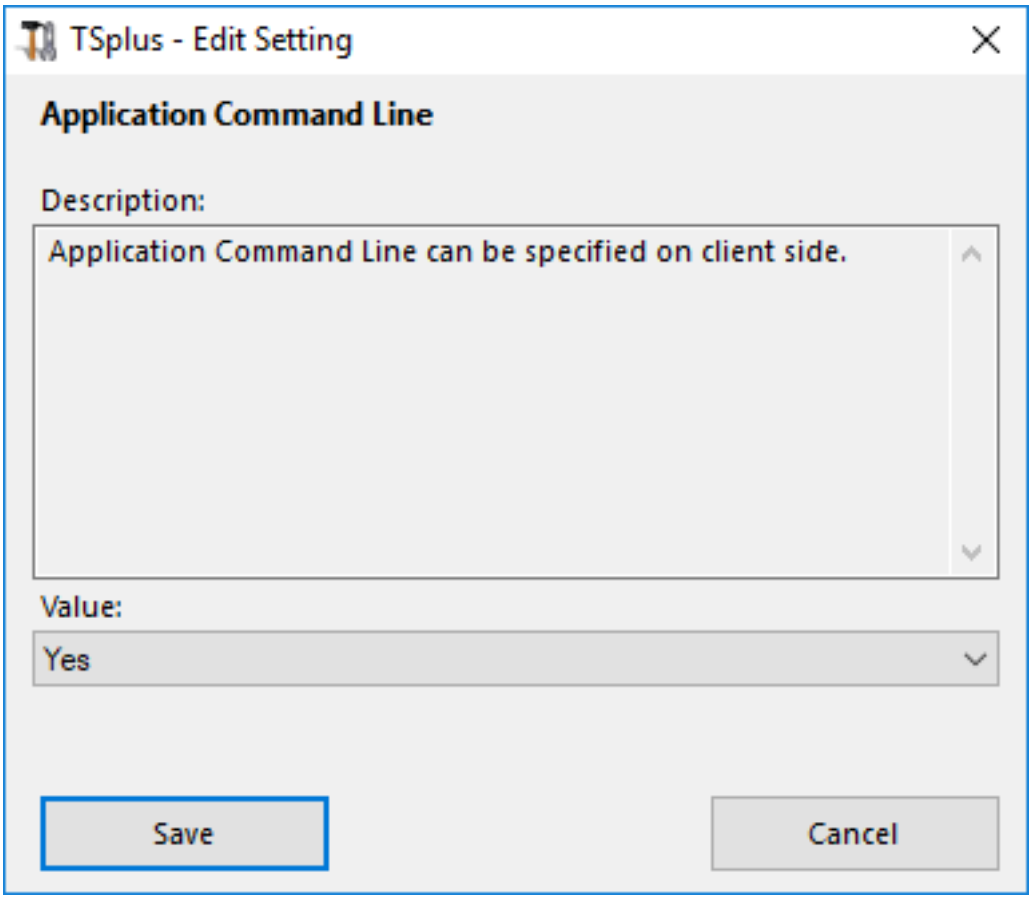
Dieser Abschnitt des erweiterten Tabs ermöglicht es Ihnen, Benutzerrechte und Aspekte ihrer Sitzungen zu konfigurieren.



Aktivieren Sie einen vollständigen Desktop für alle Benutzer, indem Sie den Wert „Ja“ in diesem Fenster auswählen, und klicken Sie dann auf Speichern:

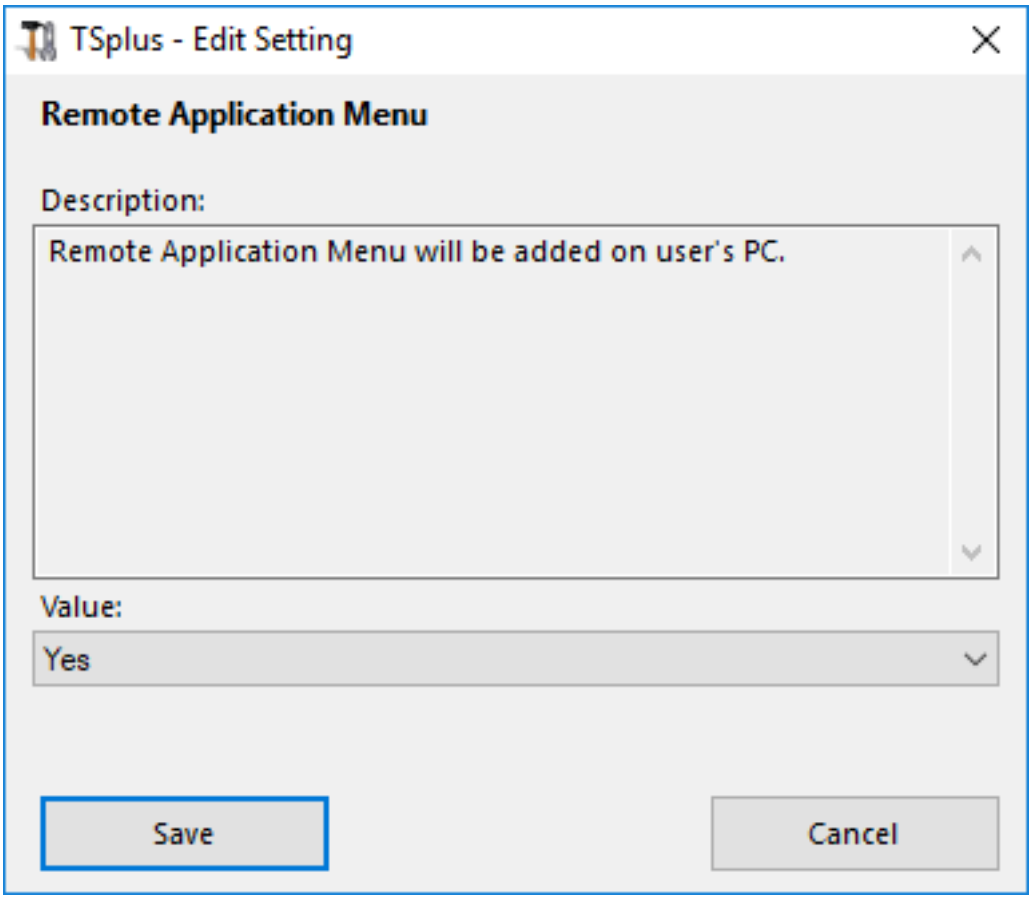


Anwendungsbefehlszeile kann auf der Client-Seite angegeben werden. Diese Funktion ist standardmäßig aktiviert. Wenn Sie sie deaktivieren möchten, wählen Sie den Wert „Nein“ in diesem Fenster aus und klicken Sie dann auf Speichern.



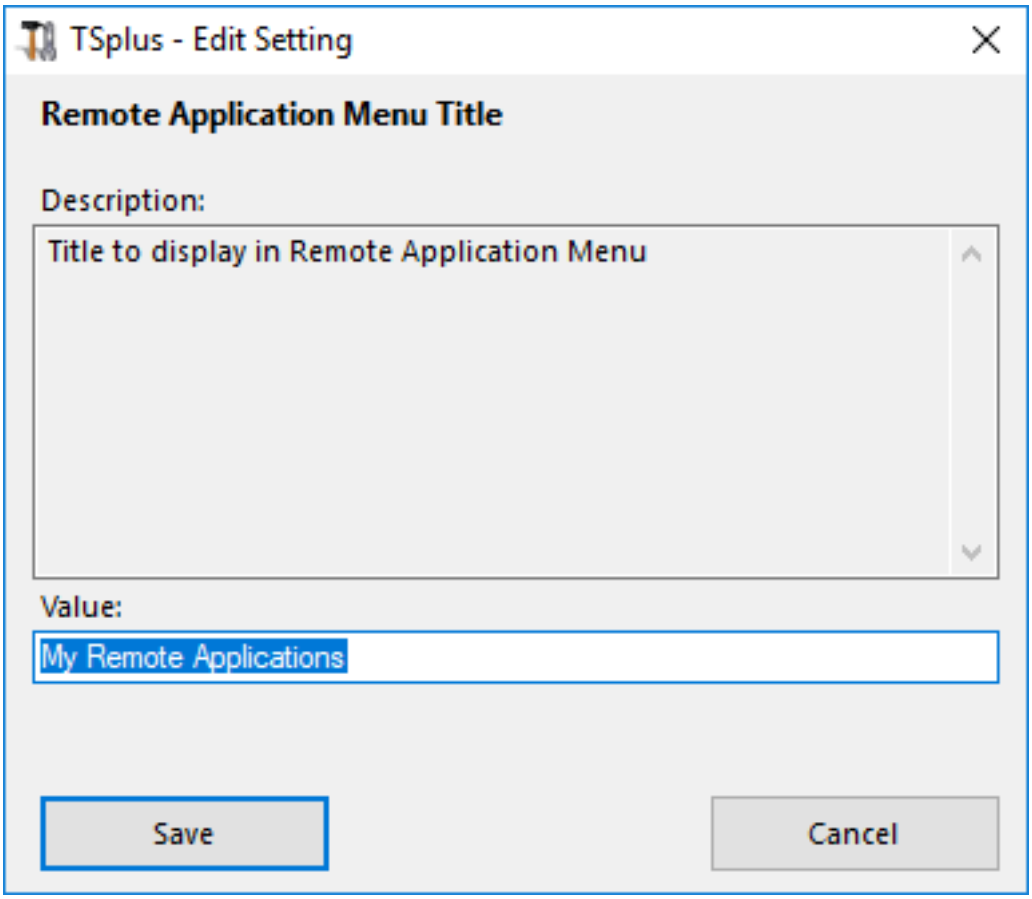
Remote-Anwendungsmenü

Das Remote-Anwendungsmenü wird auf dem PC des Benutzers hinzugefügt. Diese Funktion ist standardmäßig aktiviert. Wenn Sie sie deaktivieren möchten, wählen Sie den Wert "Nein" in diesem Fenster aus und klicken Sie dann auf Speichern.



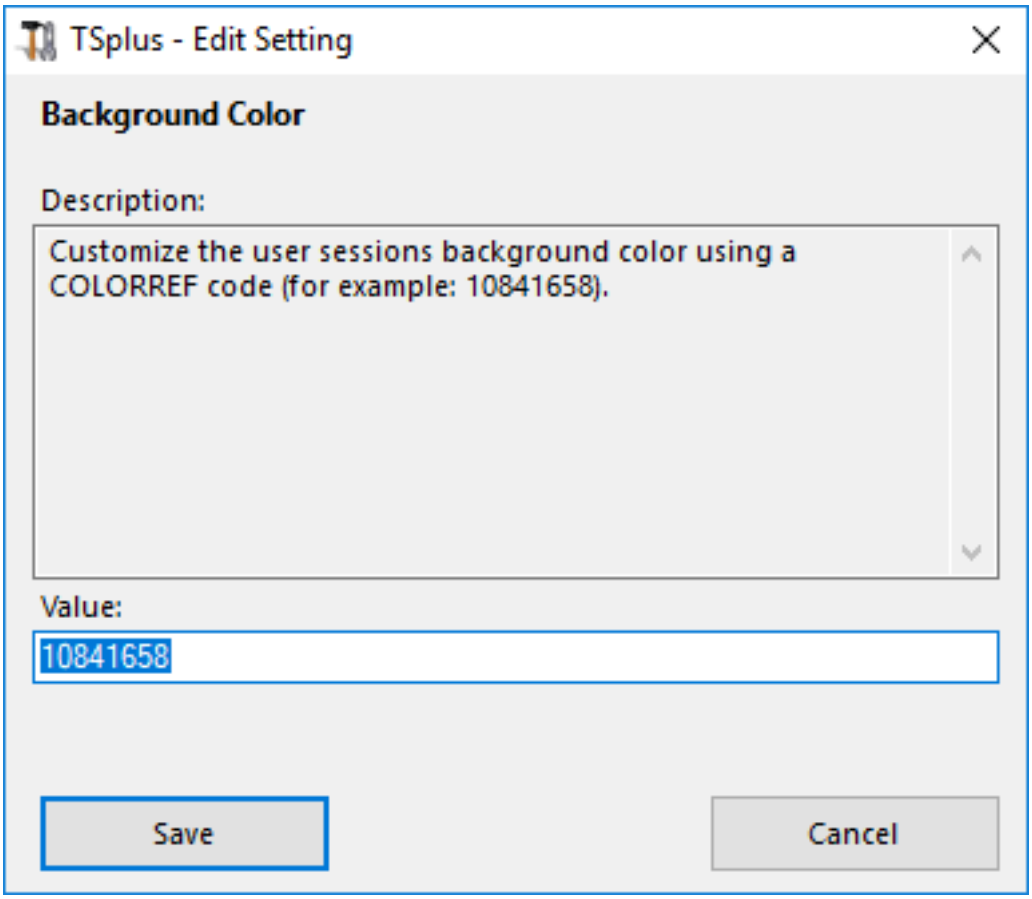
Remote-Anwendungsmenü-Titel

Sie können den Titel des Remote-Anwendungsmenüs ändern. Der Standardtitel lautet „Meine Remote-Anwendungen“. Wenn Sie ihn ändern möchten, geben Sie den gewünschten Titel ein und klicken Sie dann auf Speichern:



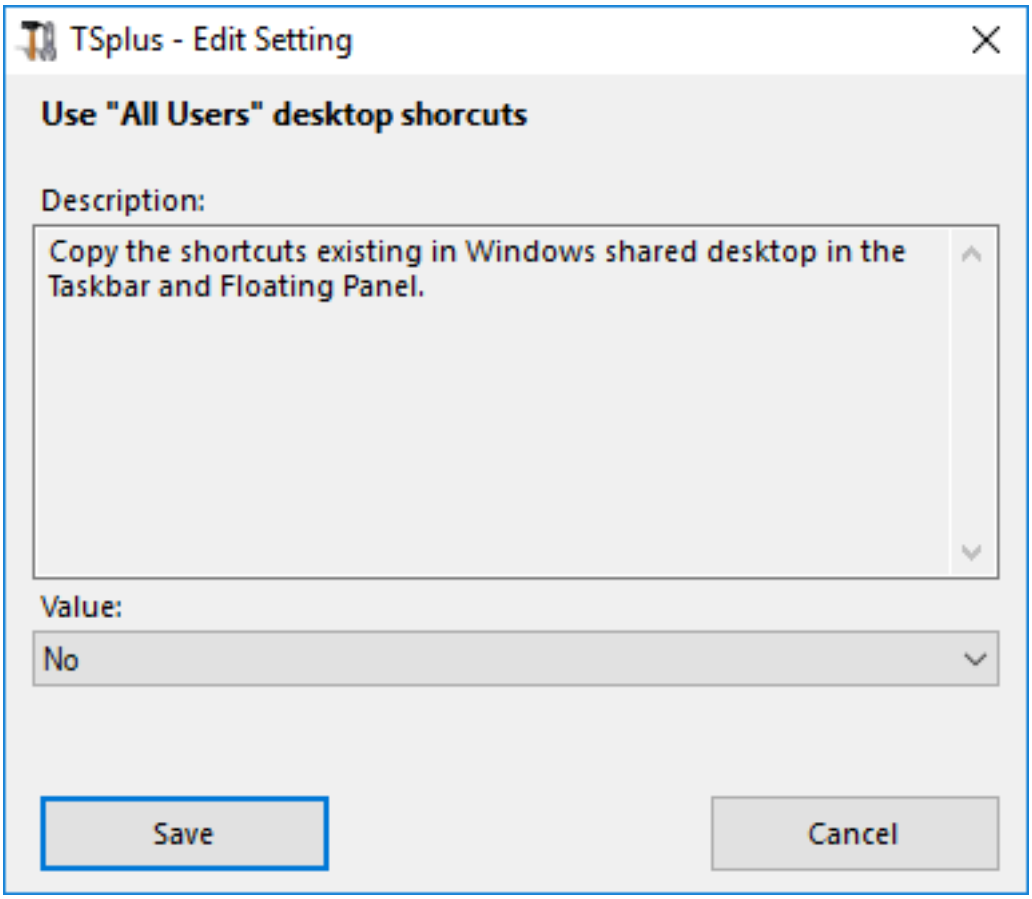
Hintergrundfarbe

Passen Sie die Hintergrundfarbe der Benutzersitzungen mit einem COLORREF-Code an (zum Beispiel ist der Standardwert: 10841658).



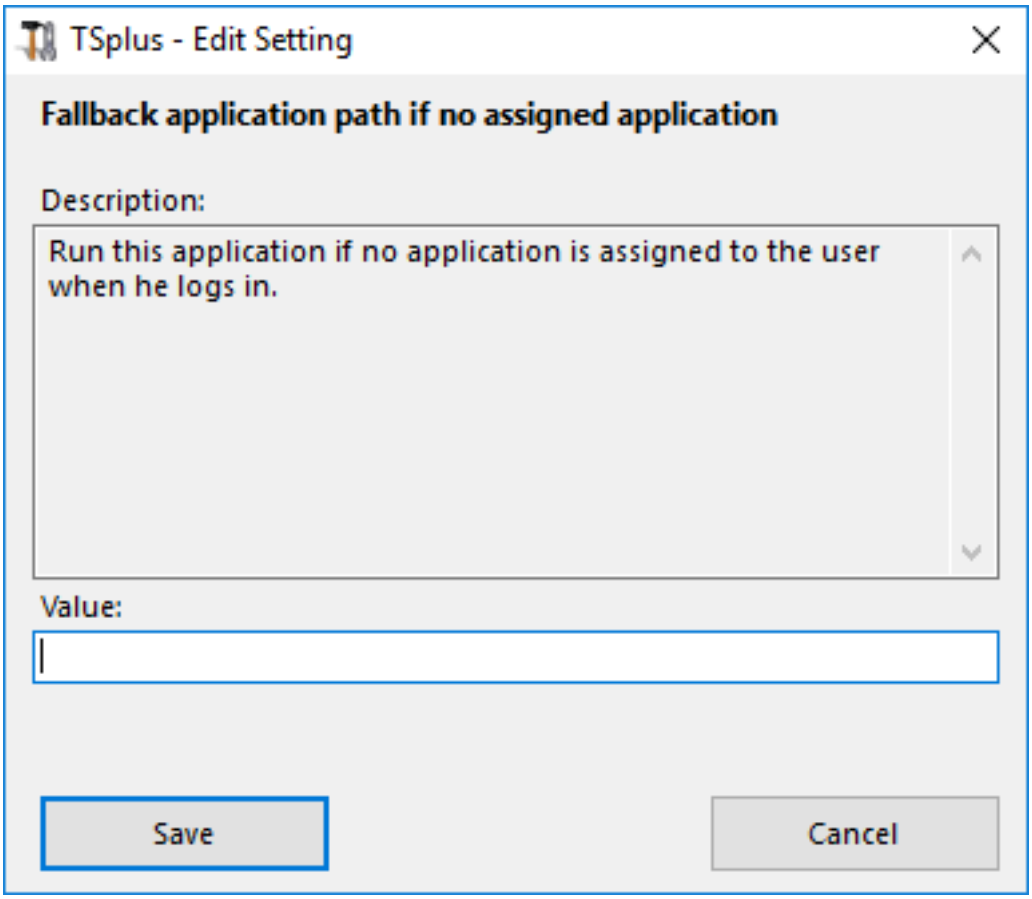
Verwenden Sie Desktop-Verknüpfungen für „Alle Benutzer“

Kopieren Sie die Verknüpfungen, die im freigegebenen Windows-Desktop in der Taskleiste und im schwebenden Panel vorhanden sind. Aktivieren Sie diese Funktion, indem Sie den Wert „Ja“ in diesem Fenster auswählen, und klicken Sie dann auf Speichern:



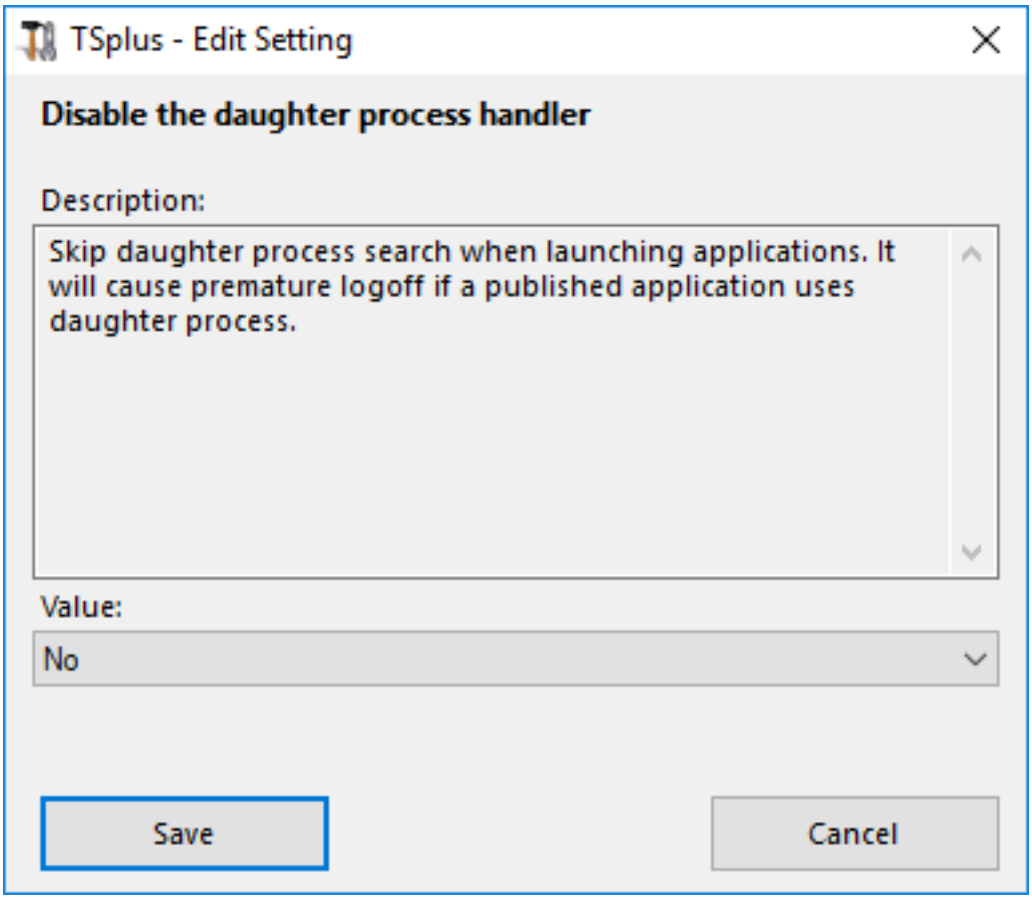
Fallback-Anwendungspfad, wenn keine zugewiesene Anwendung vorhanden ist

Führen Sie diese Anwendung aus, wenn dem Benutzer beim Anmelden keine Anwendung zugewiesen ist. Standardmäßig hat dies keinen Wert. Aktivieren Sie diese Funktion, indem Sie in diesem Fenster einen Wert von "Ja" eingeben, und klicken Sie dann auf Speichern.



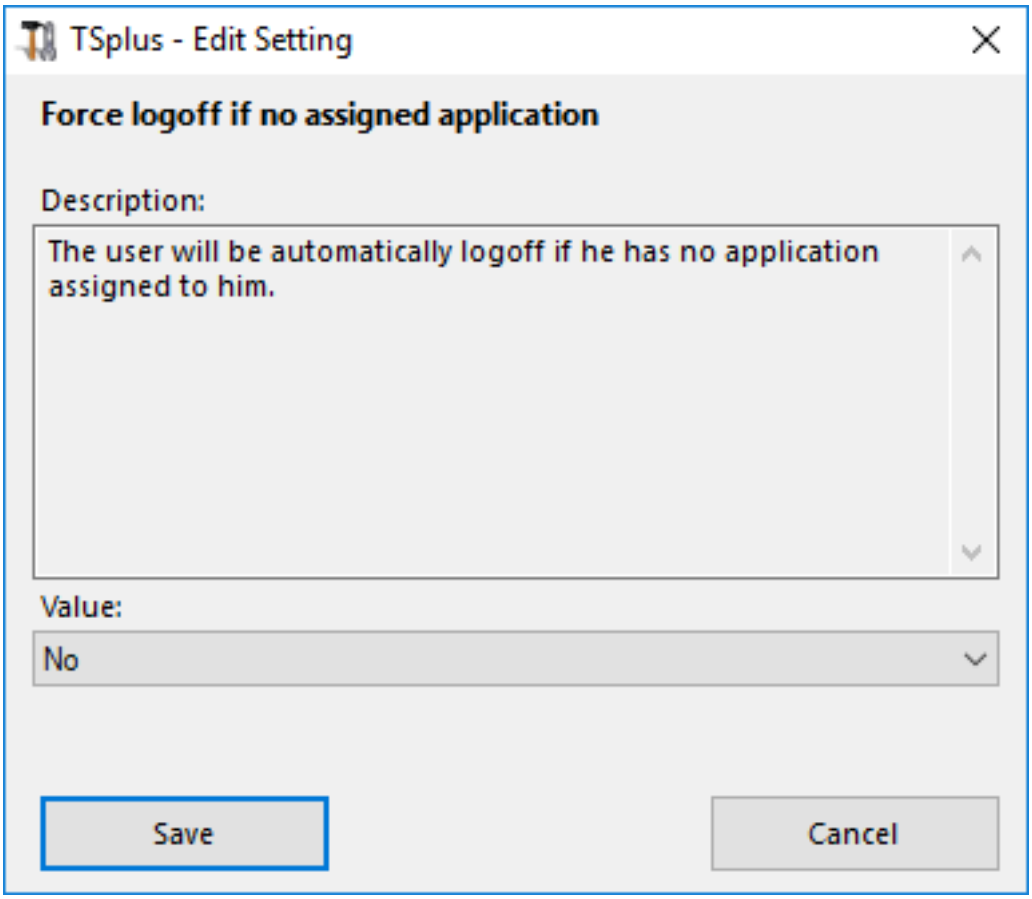
Deaktivieren Sie den Tochterprozess-Handler

Überspringen Sie die Suche nach Tochterprozessen beim Starten von Anwendungen. Dies führt zu einem vorzeitigen Abmelden, wenn eine veröffentlichte Anwendung Tochterprozesse verwendet. Diese Funktion ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion, indem Sie den Wert „Ja“ in diesem Fenster auswählen und dann auf Speichern klicken.



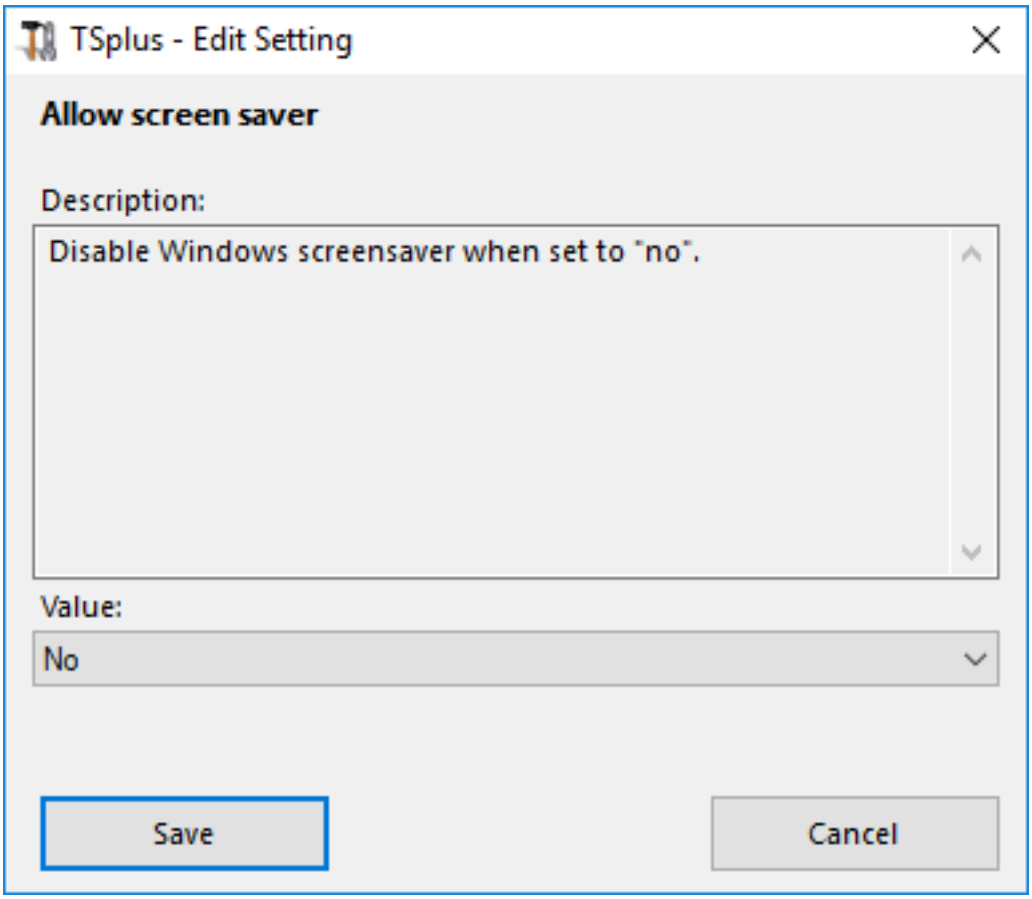
Zwangsabmeldung, wenn keine zugewiesene Anwendung vorhanden ist

Der Benutzer wird automatisch abgemeldet, wenn ihm keine Anwendung zugewiesen ist. Diese Funktion ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion, indem Sie den Wert „Ja“ in diesem Fenster auswählen und dann auf Speichern klicken.



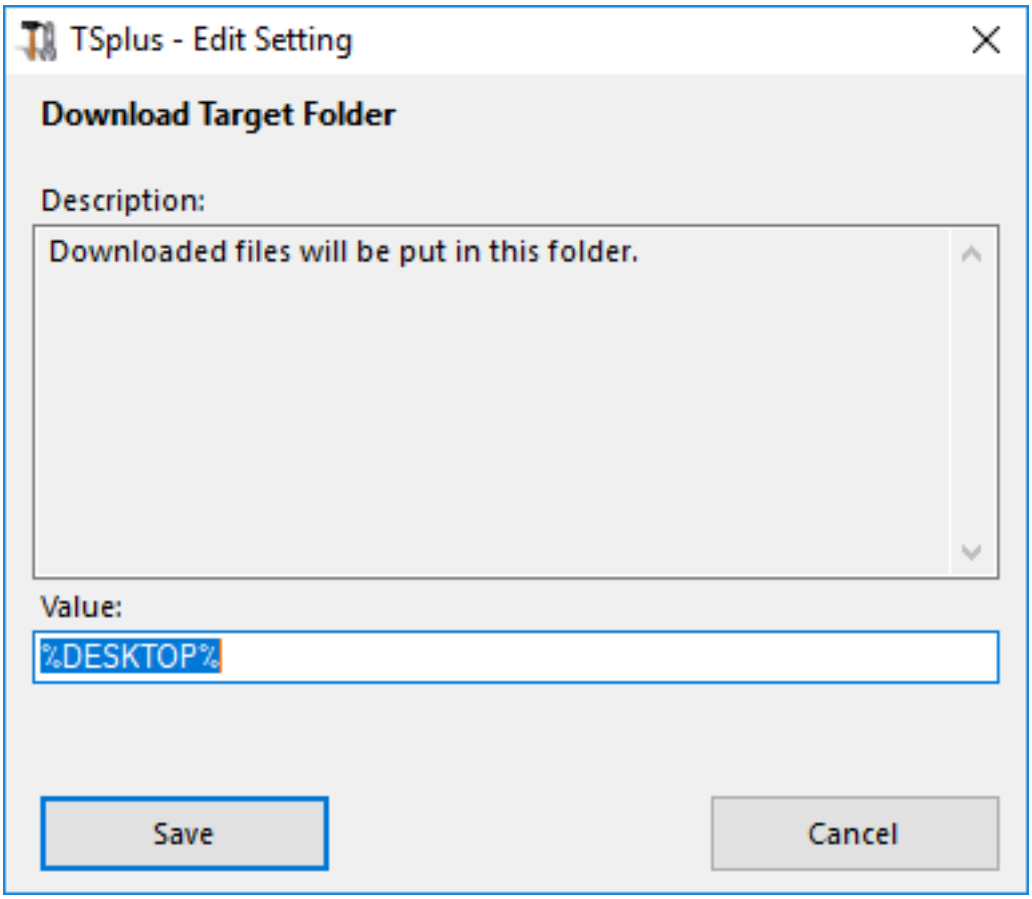
Bildschirmschoner erlauben

Diese Funktion ist standardmäßig deaktiviert. Aktivieren Sie den Windows-Bildschirmschoner, indem Sie den Wert „Ja“ in diesem Fenster auswählen, und klicken Sie dann auf Speichern:



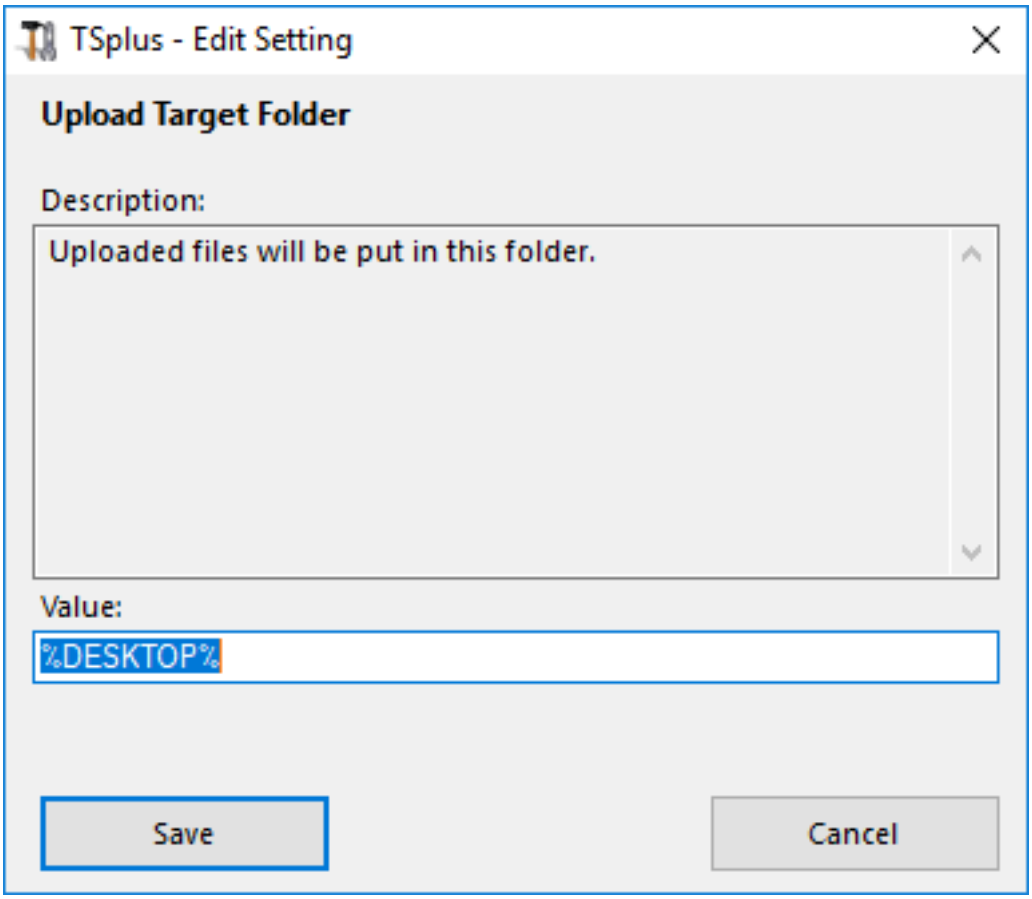
Zielordner herunterladen

Heruntergeladene Dateien werden standardmäßig auf dem Desktop abgelegt. Wenn Sie dies ändern möchten, geben Sie den gewünschten Pfad des Download-Ordners ein und klicken Sie dann auf Speichern:



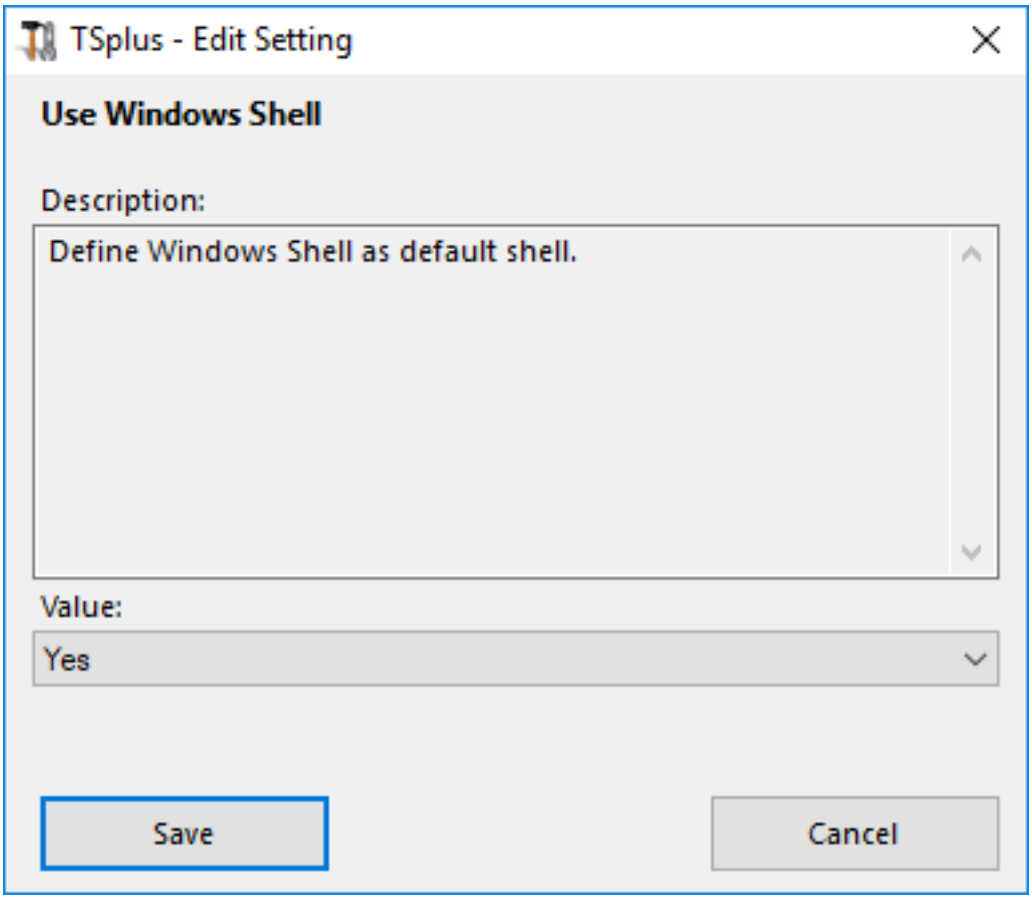
Zielordner hochladen

Hochgeladene Dateien werden in diesem Ordner abgelegt. Wenn Sie ihn ändern möchten, geben Sie den gewünschten Pfad des Upload-Ordners ein und klicken Sie dann auf Speichern:



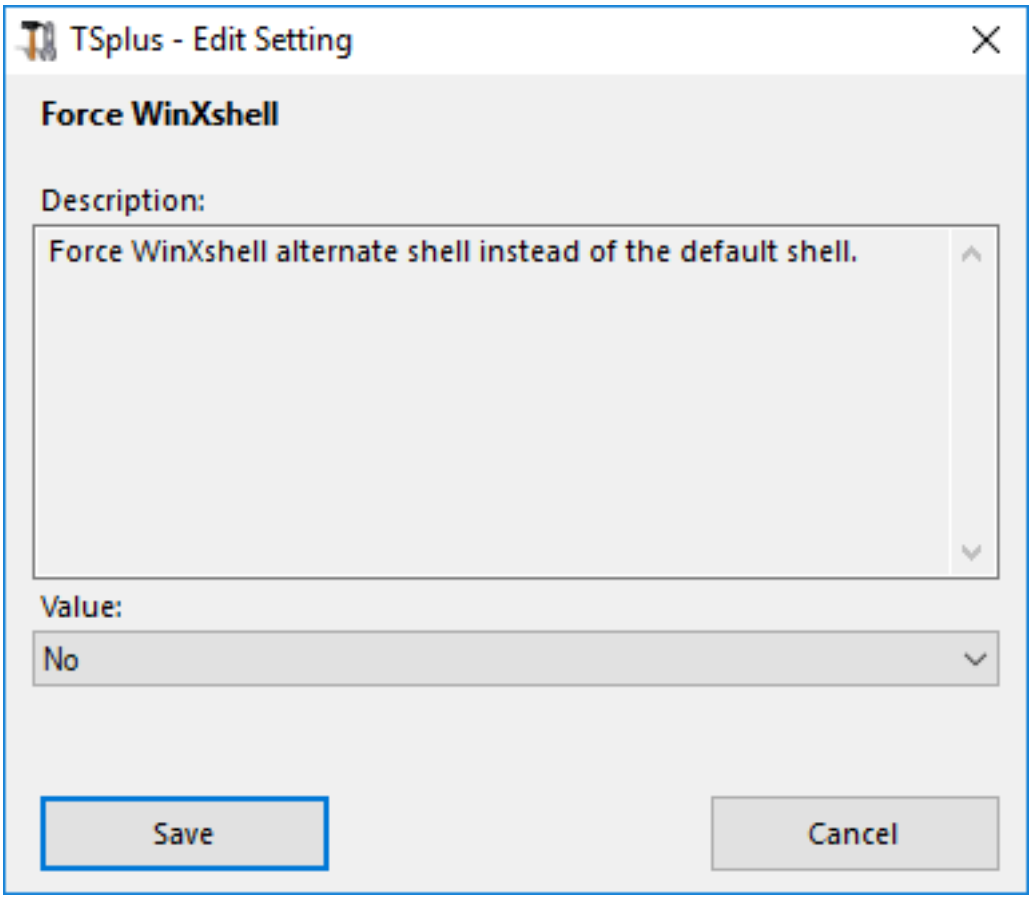
Verwenden Sie die Windows-Shell

Definieren Sie die Windows-Shell als Standardshell. Diese Funktion ist standardmäßig aktiviert. Wenn Sie sie deaktivieren möchten, wählen Sie den Wert „Nein“ in diesem Fenster aus und klicken Sie dann auf Speichern:



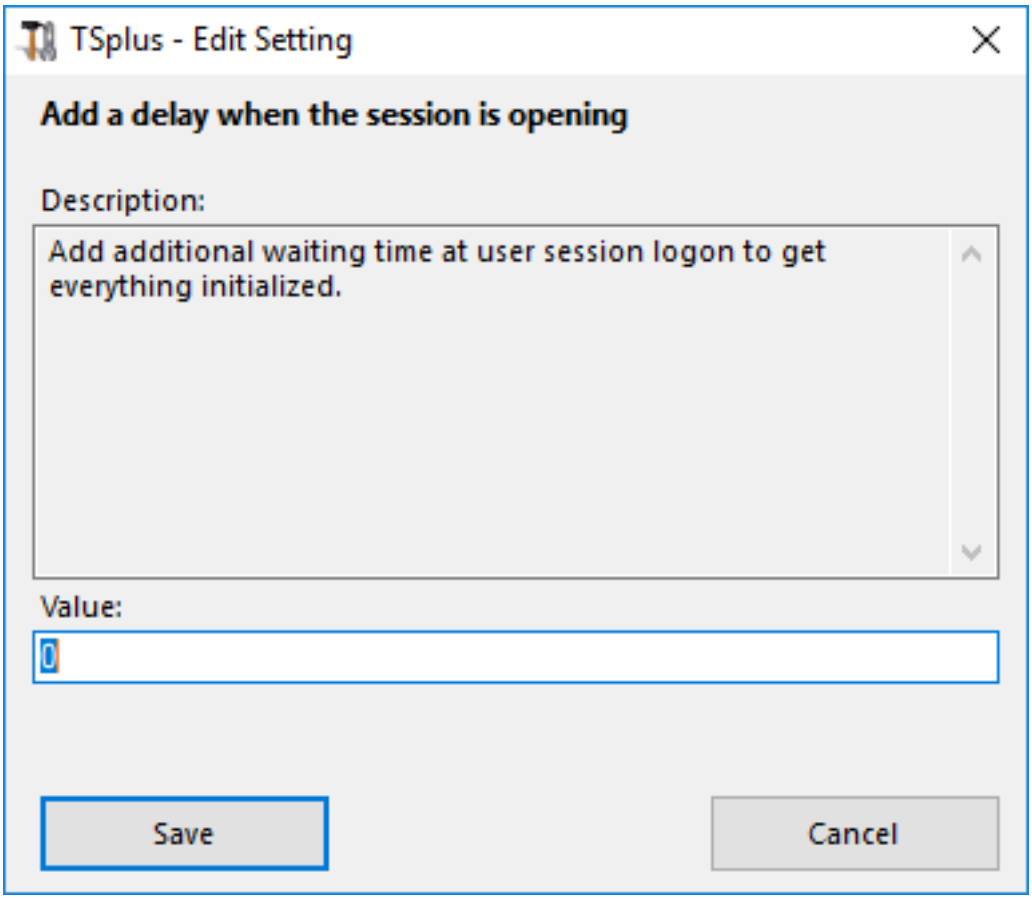
Force WinXshell

Diese Funktion ist standardmäßig deaktiviert. Erzwingen Sie die alternative Shell von WinXshell anstelle der Standard-Shell, indem Sie den Wert „Ja“ in diesem Fenster auswählen, und klicken Sie dann auf Speichern:



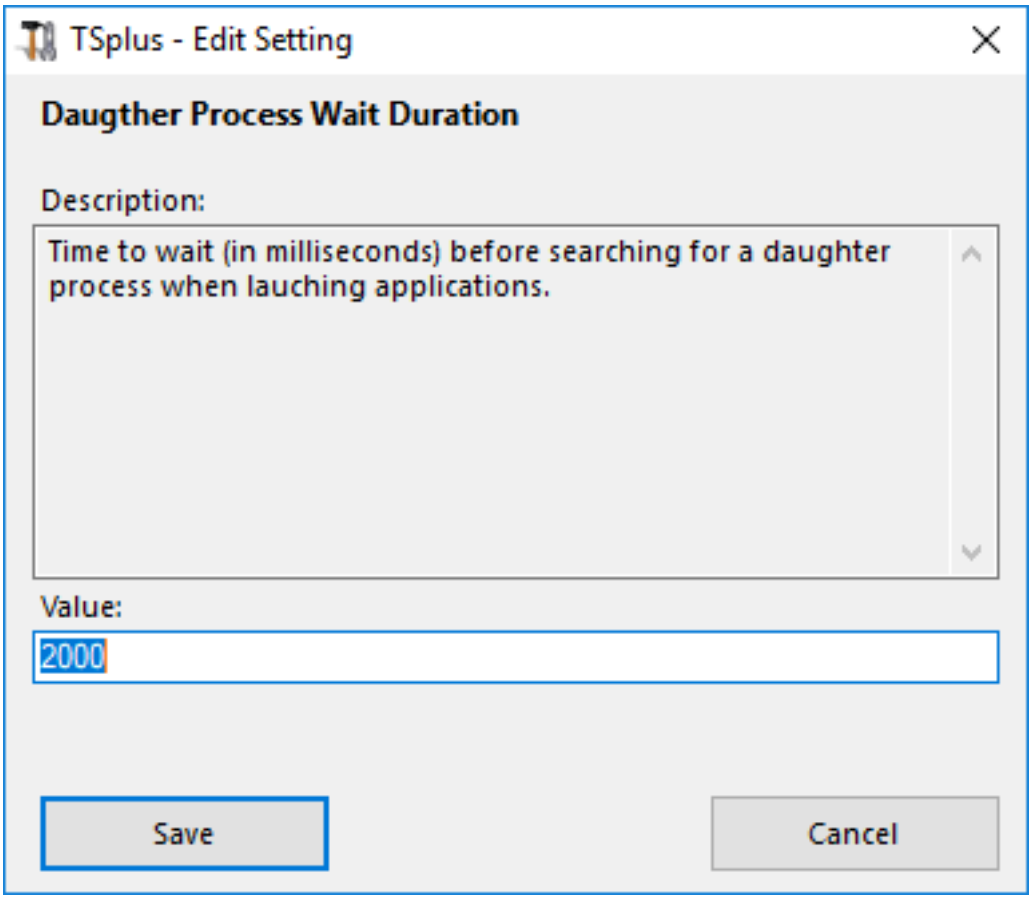
Fügen Sie eine Verzögerung hinzu, wenn die Sitzung geöffnet wird.

Zusätzliche Wartezeit beim Anmelden der Benutzersitzung hinzufügen, um alles zu initialisieren. Der Standardwert ist 0. Wenn Sie ihn ändern möchten, geben Sie den gewünschten Wert (in Sekunden) ein und klicken Sie dann auf Speichern:



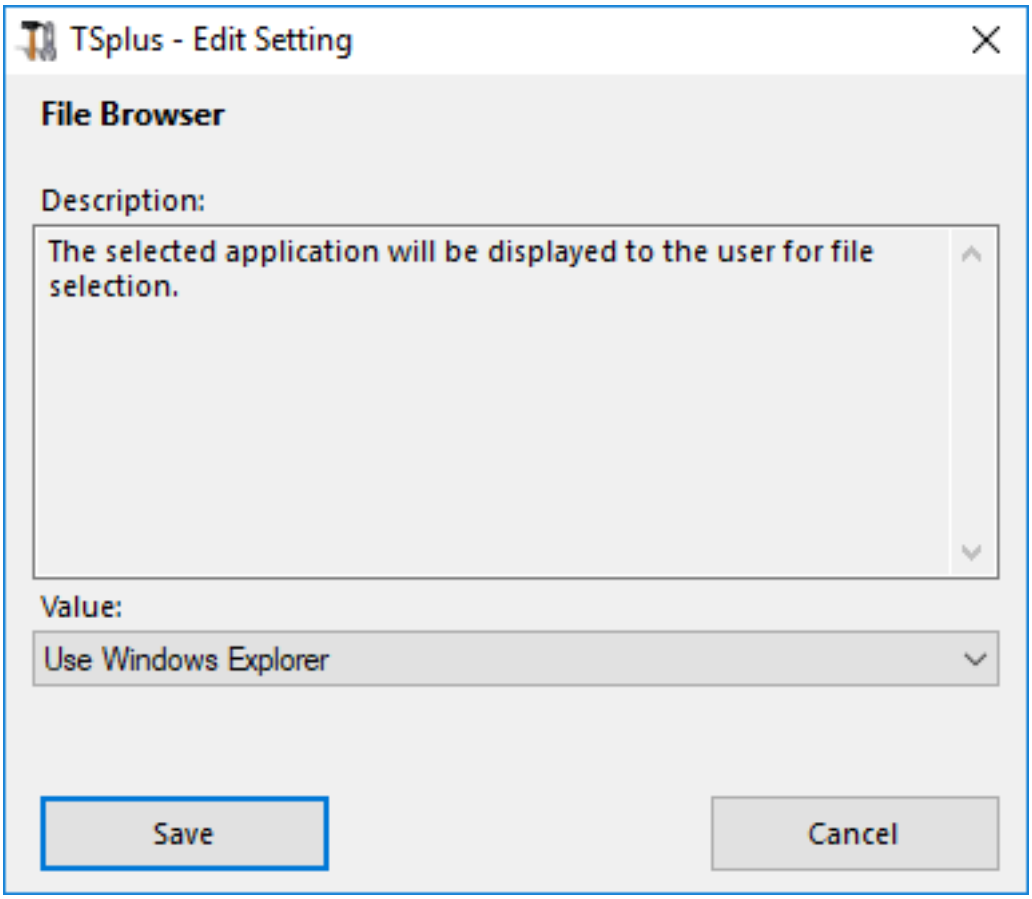
Dauer des Wartens auf den Tochterprozess

Zeit zum Warten (in Millisekunden), bevor nach einem Tochterprozess gesucht wird, wenn Anwendungen gestartet werden.



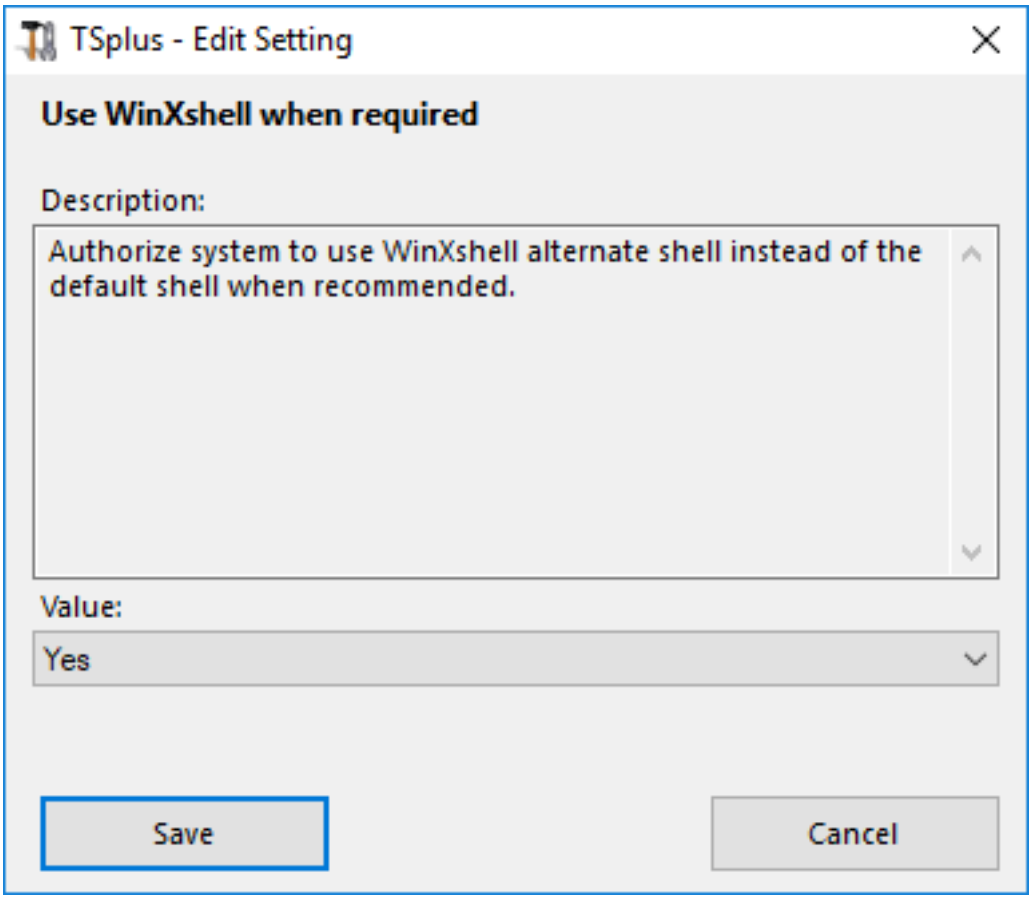
Dateibrowser

Die ausgewählte Anwendung wird dem Benutzer zur Dateiauswahl angezeigt. Der Standardbrowser ist der Windows-Explorer. Sie können den TSplus-Dateibrowser verwenden, indem Sie ihn auswählen und dann auf Speichern klicken:



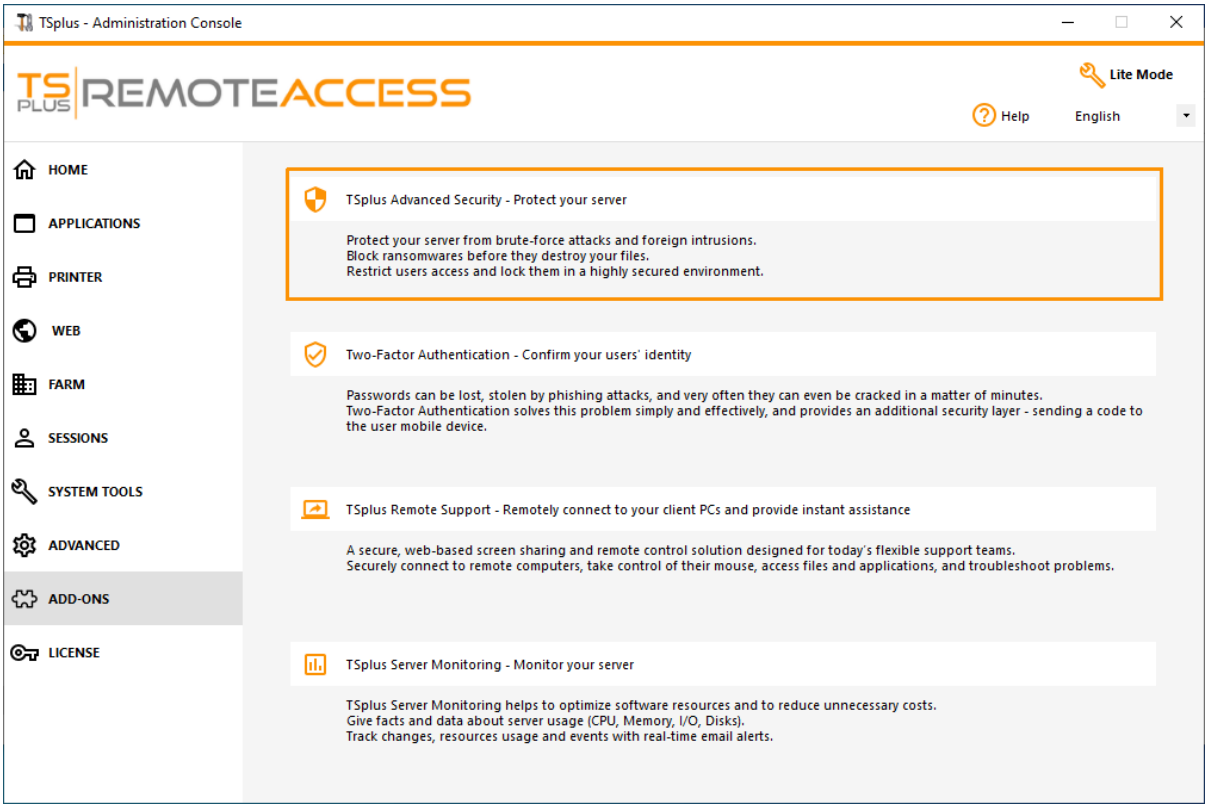
WinXshell verwenden, wenn erforderlich

System autorisieren, um die alternative Shell WinXshell anstelle der Standard-Shell zu verwenden, wenn dies empfohlen wird. Diese Funktion ist standardmäßig aktiviert. Wenn Sie sie deaktivieren möchten, wählen Sie den Wert "Nein" in diesem Fenster aus und klicken Sie dann auf Speichern.


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 Advanced Security

TSplus Advanced Security ist als Add-On im TSplus AdminTool verfügbar und ist im Tab Add-Ons verfügbar:

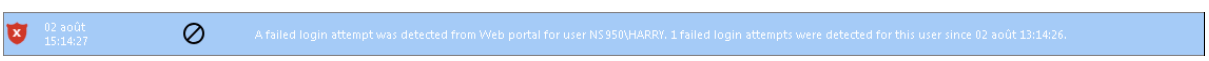


Sie können die vollständige Dokumentation finden. auf dieser Seite .

Sperreereignis

TSplus Sperrung überwacht fehlgeschlagene Web-Login-Versuche auf Ihrem TSplus-Server.

TSplus Advanced Security zeigt ein Sperrevent an, nach jedem fehlgeschlagenen Versuch im Webportal, wie im folgenden Beispiel:



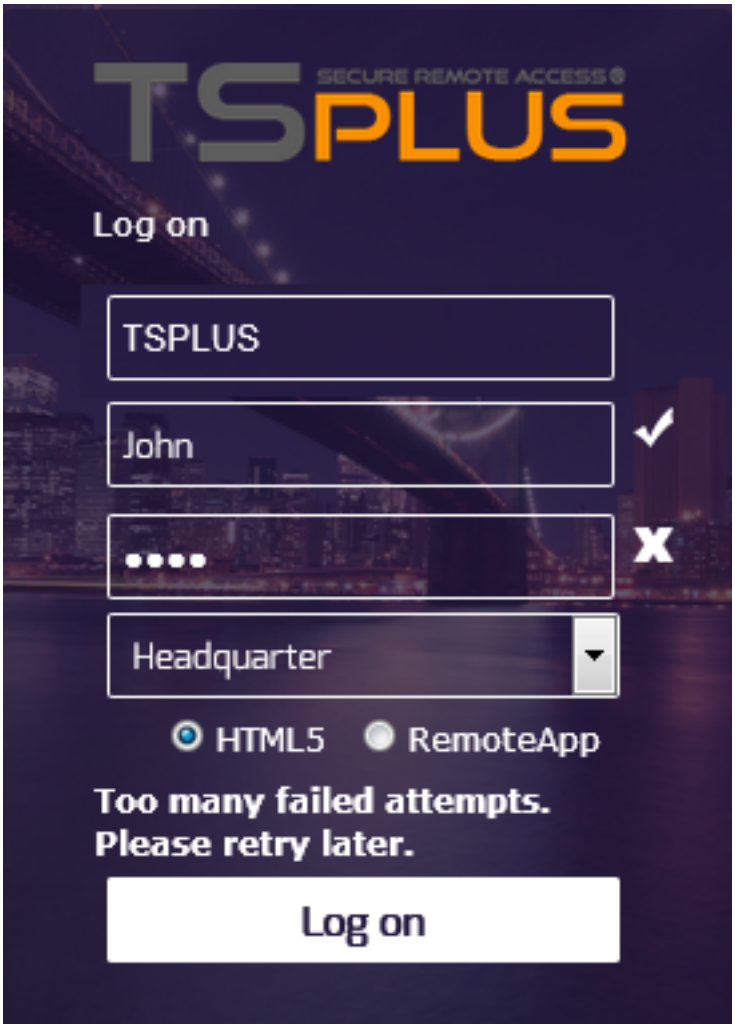
Ein fehlgeschlagener Anmeldeversuch wurde vom Webportal für den Benutzer … 1 fehlgeschlagener Anmeldeversuch wurde für diesen Benutzer seitdem erkannt…

Der Bruteforce-Schutz ermöglicht es Ihnen, Ihren öffentlichen Server vor Hackern, Netzwerkscannern und Brute-Force-Robotern zu schützen, die versuchen, Ihren Administrator-Login und Ihr Passwort zu erraten. Mit aktuellen Logins und Passwortwörterbüchern werden sie automatisch versuchen, sich Hunderte bis Tausende Male pro Minute in Ihren Server einzuloggen. Erfahren Sie mehr über diese Funktion auf diese Seite .

Im Webportal

Brute-Force-Angriffe auf das Webportal werden blockiert, wenn Benutzer falsche Anmeldeinformationen eingeben.

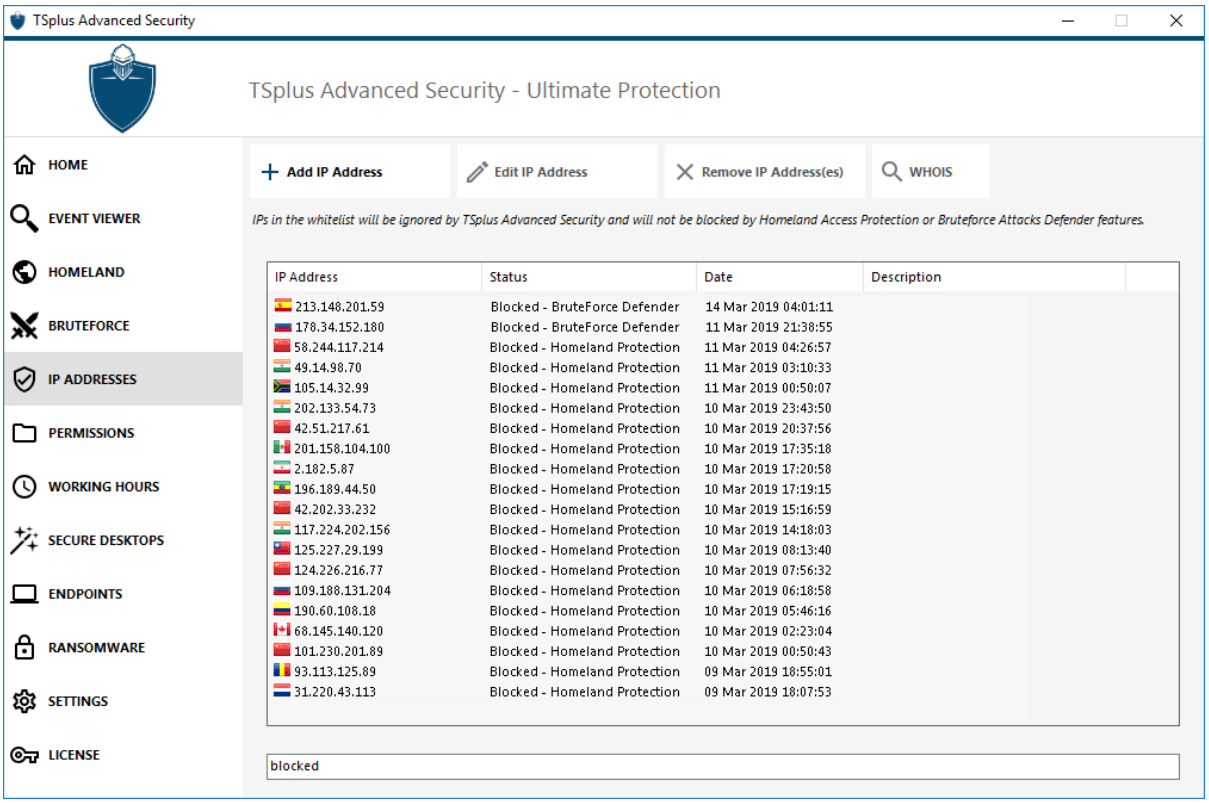
Nach 10 Versuchen innerhalb von 10 Minuten wird das Webportal dem Benutzer den Login für 20 Minuten verweigern.



Dies sind die Standard Einstellungen, die auf dem anpassbar sind. BruteForce Schutz-

Registerkarte von TSplus Advanced Security AdminTool.

Sie können alle blockierten Verbindungen und Protokolle auf der IP-Adressen-Kachel von TSplus Advanced Security Ultimate Protection überprüfen:



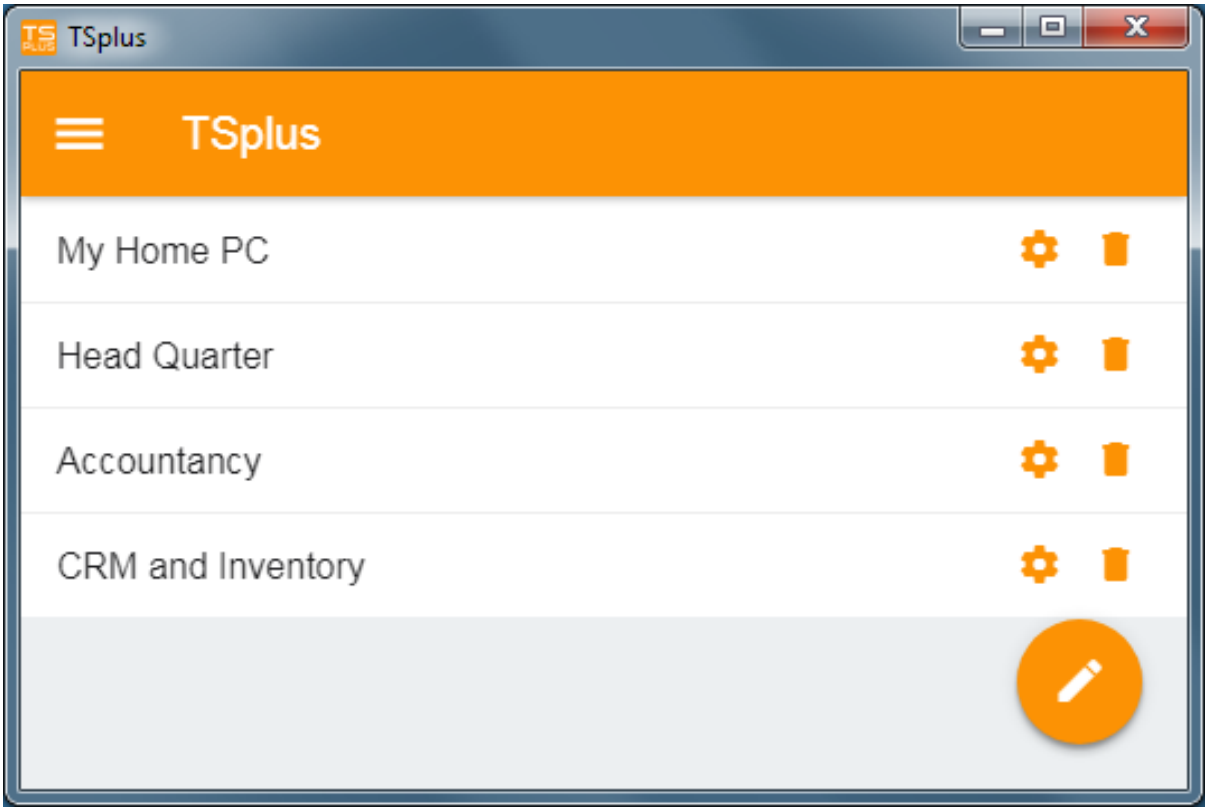
Diese Funktionalität ist sichtbar und aktiv nach der ersten Verbindung zum Webportal.

Die vollständige TSplus Advanced Security-Dokumentation ist verfügbar auf dieser Seite .

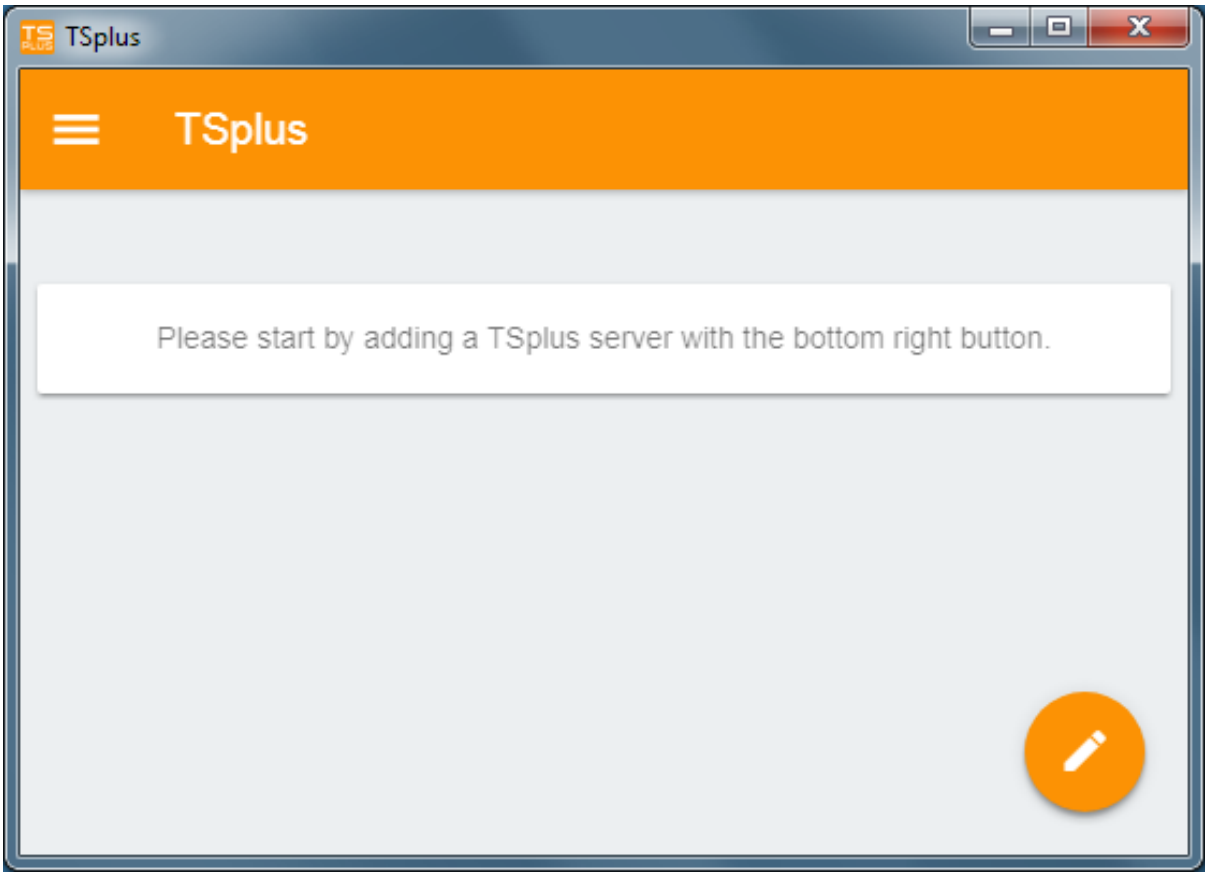
TSplus App-Konfiguration

Verwalten Sie Ihre Server

Die Benutzeroberfläche und die Konfiguration sind einfach und intuitiv.



Zuerst fügen Sie einen TSplus-Server hinzu, indem Sie auf die Schaltfläche unten rechts klicken:

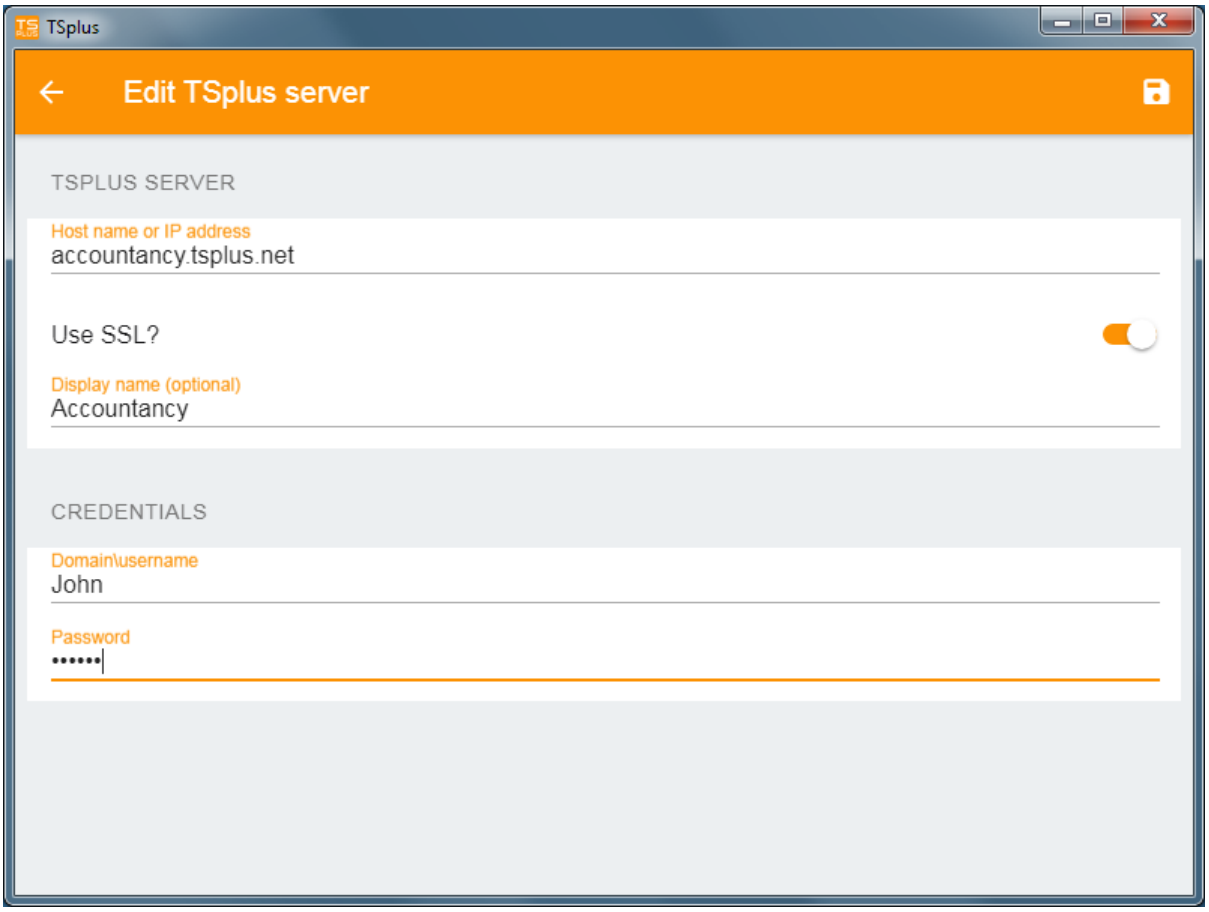


Dann fügen Sie Ihre Serverinformationen hinzu und konfigurieren Sie sie:

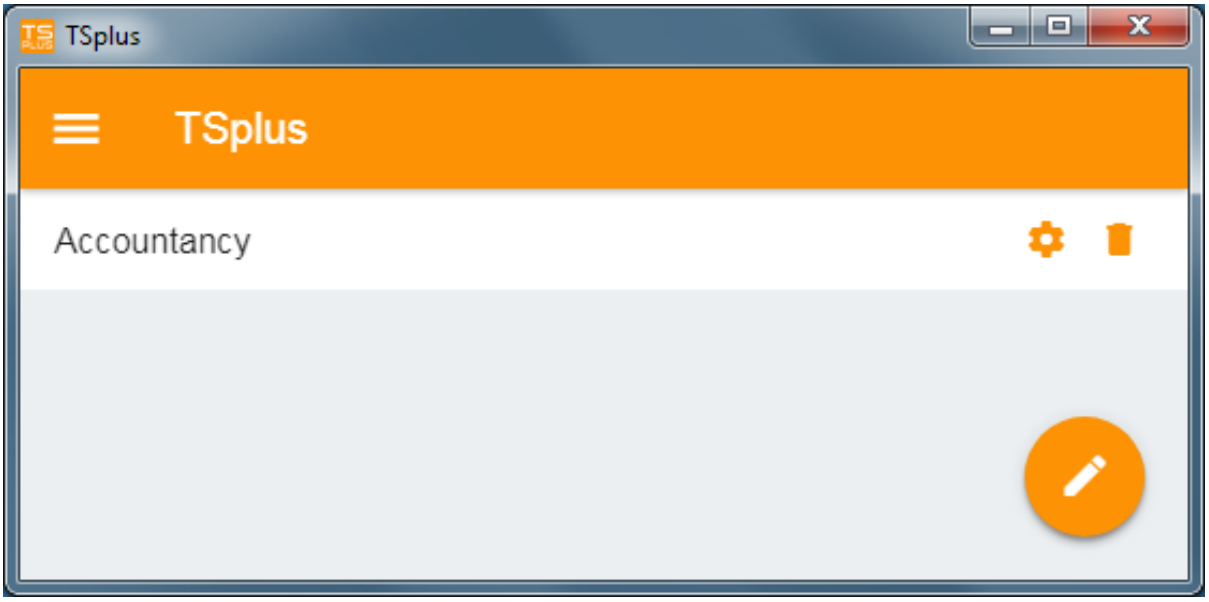
- Geben Sie den Hostnamen oder die IP-Adresse ein.
- SSL ist standardmäßig deaktiviert, aber Sie können sich entscheiden, es zu aktivieren.

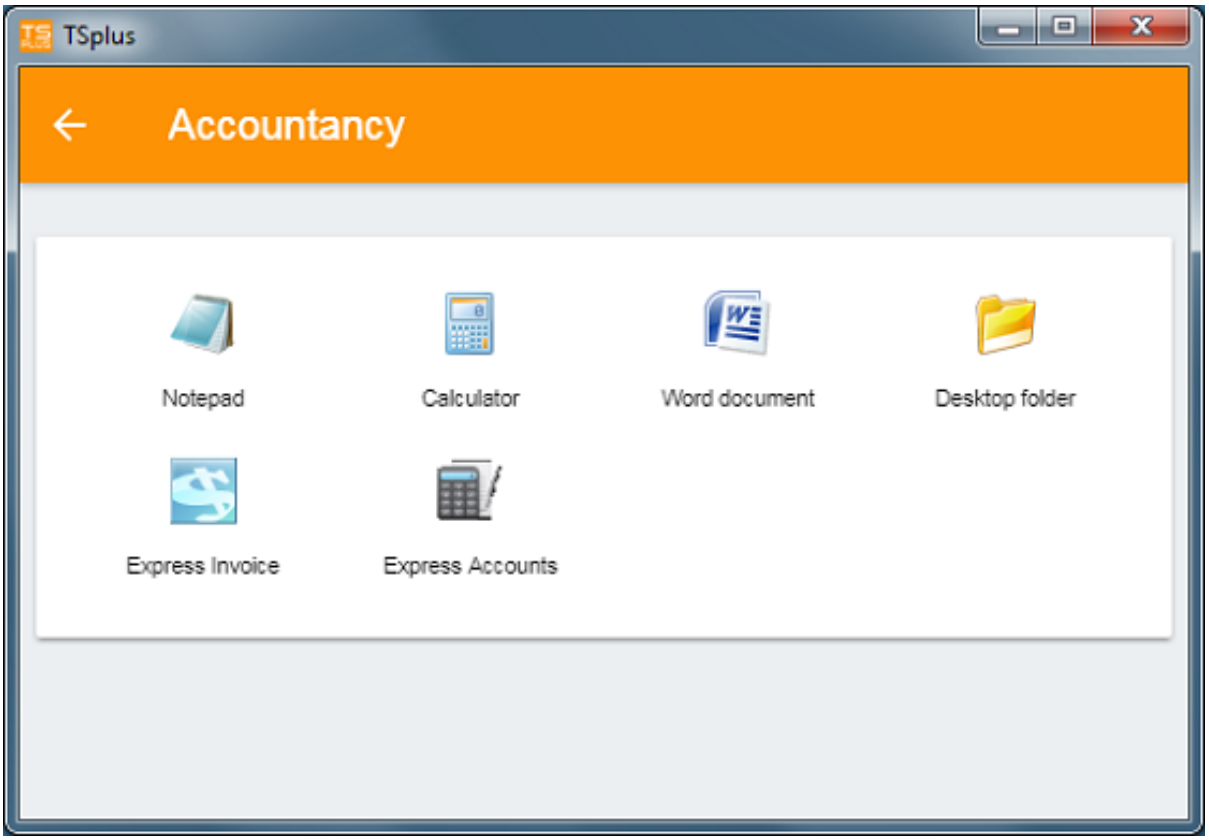
Warnung: SSL-Aktivierung funktioniert nur, wenn Sie ein gültiges SSL-Zertifikat auf Ihrem TSplus-Server installiert haben. Siehe diese Dokumentation für weitere Informationen.

- Geben Sie den Anzeigenamen ein, der optional ist.
- Geben Sie die Anmeldeinformationen Ihres Benutzers mit der Domäne oder dem Benutzernamen und dem Passwort ein.
- Wenn Sie das HTTPS-Protokoll verwenden, müssen Sie den Port in der konfigurierten Adresse eingeben. appportal.mydomain.com:443



Dann klicken Sie auf die Schaltfläche oben rechts, um zu speichern. Sie können jetzt auf Ihren Server klicken, um auf Ihre Anwendungen zuzugreifen.





Drucken

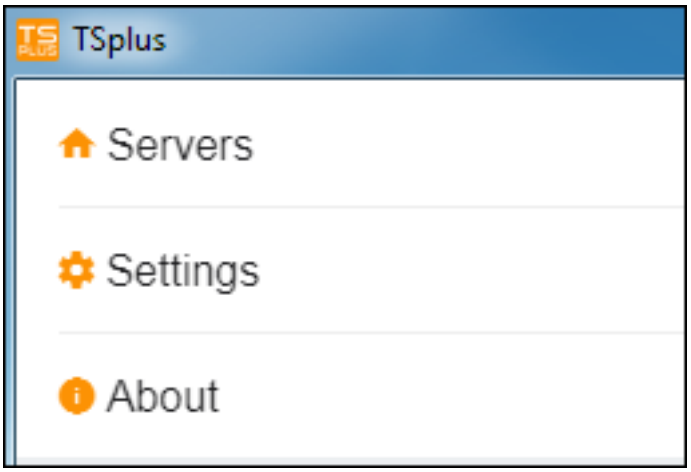
Drucken Sie ganz einfach auf Ihrem lokalen Drucker, indem Sie den Universaldrucker .

Seit der Version 11.40 der TSplus App öffnen sich gedruckte Dokumente mit der standardmäßigen PDF-Reader-App.

Einstellungen und Version

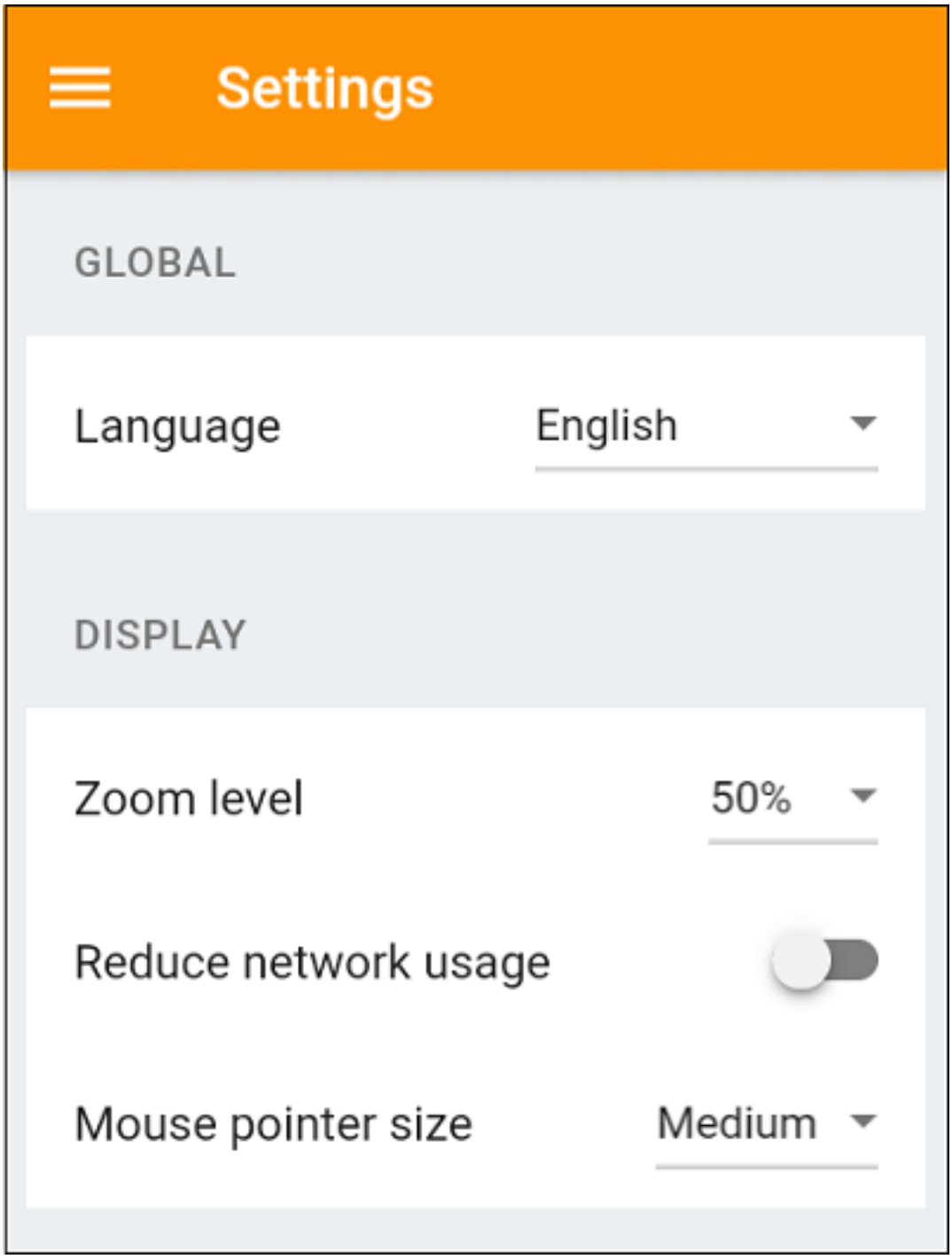
Unter dem oberen linken Menü können Sie:

- Verwalten Sie Ihre Server
- Verwalten Sie Ihre Einstellungen
- Siehe die rechtlichen Informationen im Abschnitt Über und Ihre TSplus App-Version.



Einstellungen

Es stehen verschiedene Einstellungen im Einstellungsfenster zur Verfügung:



- Sie können die Sprache ändern.
- Ändern Sie die Anzeigeeinstellungen, indem Sie den Zoomfaktor nach Belieben anpassen, den Netzwerkverbrauch reduzieren oder zwischen 3 Mauszeigergrößen wählen: klein, mittel oder groß.

2FA-Authentifizierung

Die Android-App ist mit 2FA kompatibel.

Die App fragt nach dem 2FA-Code, wenn das Benutzerkonto so konfiguriert wurde, dass es 2FA verwendet.

Die Aktivierung kann nicht über die mobile App erfolgen, Sie müssen zuerst 2FA über das Webportal konfigurieren.

Version

Auf der Registerkarte "Über" können Sie die rechtlichen Informationen sowie Ihre aktuelle TSplus App-Version sehen:



TSplus App

Die TSplus App ermöglicht es Ihnen, von jedem Gerät und überall eine Verbindung zu Ihrem TSplus-Server herzustellen!

Genau wie TSplus bietet es schnelle und stabile Remote-Verbindungen von Tablets und Smartphones zu Windows-Desktops und Geschäftsanwendungen.

Greifen Sie in Echtzeit auf Ihre Anwendungen und Geschäftsdaten zu und drucken Sie ganz einfach jedes Dokument und Foto, das Sie benötigen, auf dem nächstgelegenen lokalen Drucker.

Die TSplus App ist mit 2FA kompatibel.



Für weitere Informationen und Download-Links besuchen Sie die App-Seite auf unserer Website.

Hardwareanforderungen und Betriebssysteme

Die TSplus App ist auf Mobilgeräten und Tablets mit den folgenden Betriebssystemen verfügbar: iOS, Android ab Version 4.4 und Linux.

Android-Version

iOS-Version

Voraussetzungen

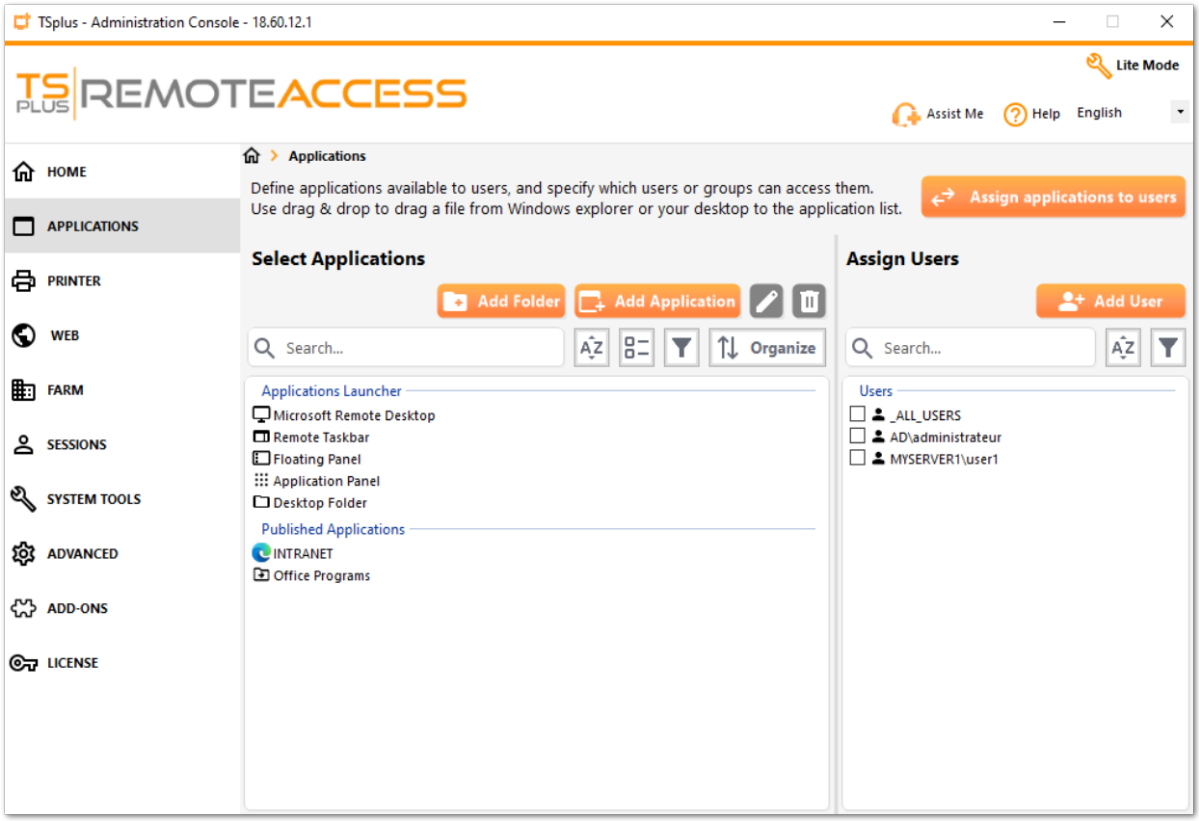
- Die Host-Website muss ein TSplus Mobile Web- oder Enterprise-System sein.
- Die Version 11.30 (und höher) muss auf diesem Host installiert werden.

Anwendungen Benutzern oder Gruppen zuweisen

Sobald Sie haben einige Anwendungen veröffentlicht , Sie können sie einem oder mehreren Benutzern und/oder Gruppen zuweisen.

Benutzer oder Gruppen Anwendungen zuweisen

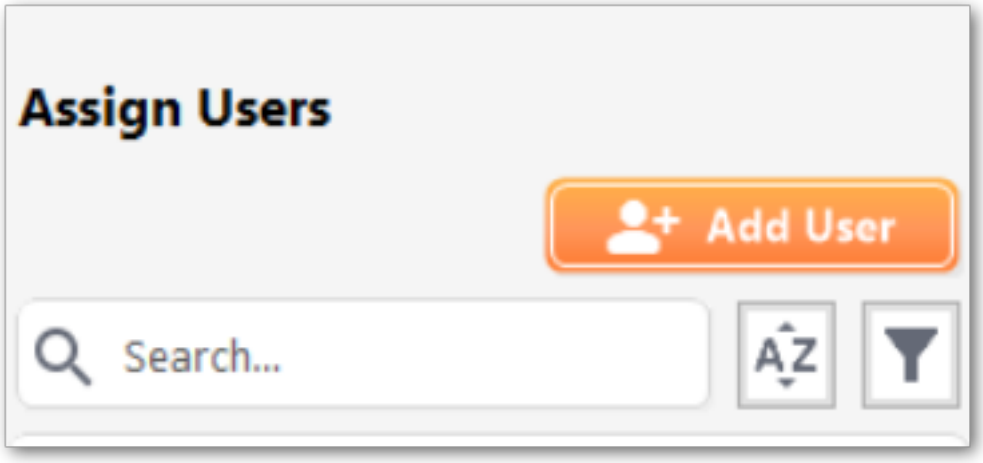
Jede Zuweisung muss im rechten Seitenbereich des Abschnitts „Anwendungen“ des AdminTools erfolgen. Dieser rechte Seitenbereich zeigt alle Benutzer und Gruppen an, die derzeit Anwendungen zugewiesen haben.



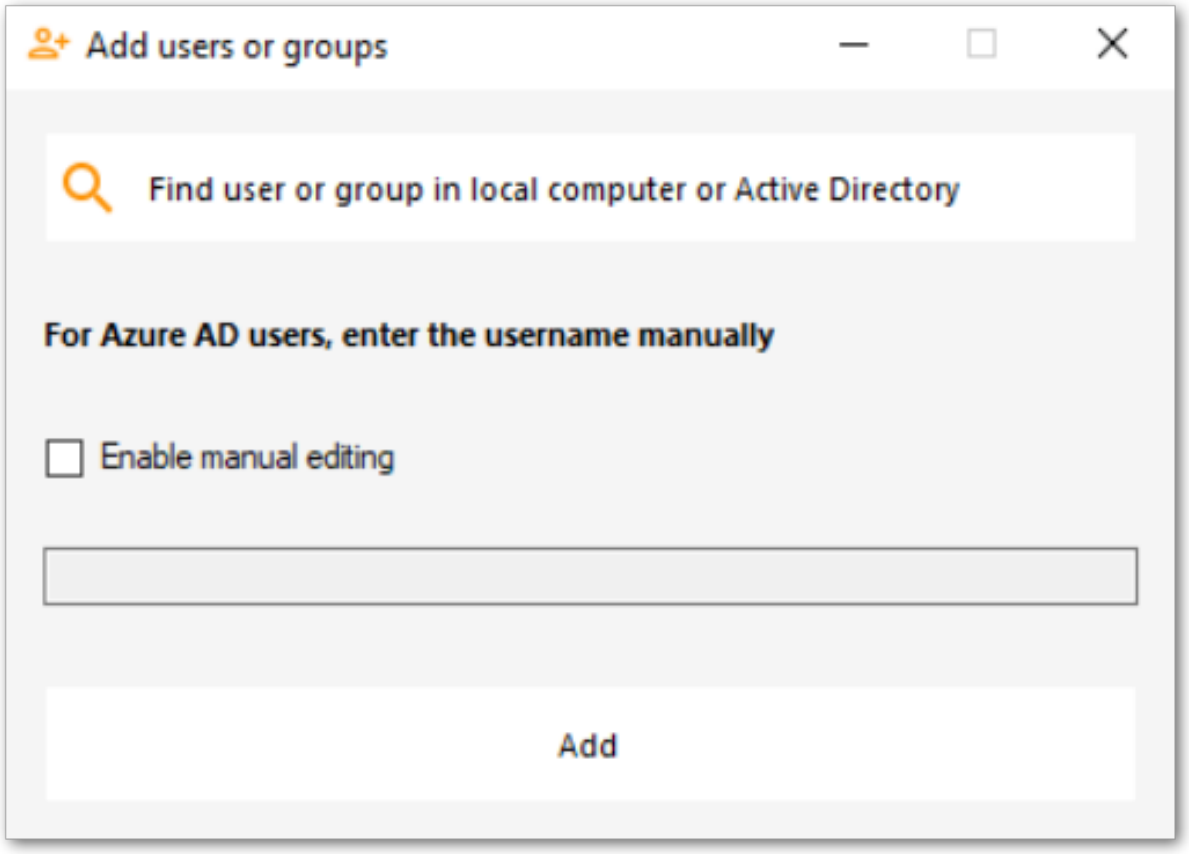
Um Benutzer oder Gruppen zuzuweisen, müssen Sie zuerst die Benutzer/Gruppen hinzufügen, für die Sie die Anwendung zuweisen möchten.

Benutzer oder Gruppen hinzufügen

Um Benutzer oder Gruppen hinzuzufügen, klicken Sie auf die Schaltfläche „Benutzer hinzufügen“.



Sie werden mit dieser Benutzeroberfläche begrüßt, die es Ihnen ermöglicht, entweder einen Benutzer oder eine Gruppe über den Benutzer-/Gruppenauswähler zu finden oder direkt den Namen des Benutzers/der Gruppe, die Sie hinzufügen möchten, einzugeben.
Lokale oder Active Directory-Benutzer müssen mit der Schaltfläche Lokale oder Active Directory-Benutzer oder -Gruppen suchen ausgewählt werden.
Nur externe Benutzer können direkt in das Textfeld eingegeben werden.



Der _ALL_USERS spezielle Benutzername

In der Benutzerliste finden Sie immer den verfügbaren Benutzer „_ALL_USERS“. Dieser Benutzer ist kein Windows-Benutzer, sondern ein virtueller Benutzer. Wenn Sie eine Anwendung auswählen und den Benutzernamen „_ALL_USERS“ aktivieren, wird die Anwendung allen Benutzern zur Verfügung stehen.

Benutzer oder Gruppen Anwendungen zuweisen

Sobald Benutzer hinzugefügt wurden, weisen Sie ihnen Anwendungen zu durch:

1. wählen Sie im linken Panel die Anwendungen aus, die Sie Ihrem Benutzer zuweisen möchten
2. Überprüfung im rechten Bereich das Kästchen neben seinem Benutzernamen anzukreuzen, um die ausgewählten Anwendungen diesem Benutzer zuzuweisen.

Wenn ich den Notepad dem Benutzer "benjamin" zuweisen möchte, wähle ich einfach die Anwendung "Notepad" links aus und aktiviere das Kästchen neben dem Benutzernamen "benjamin" rechts.

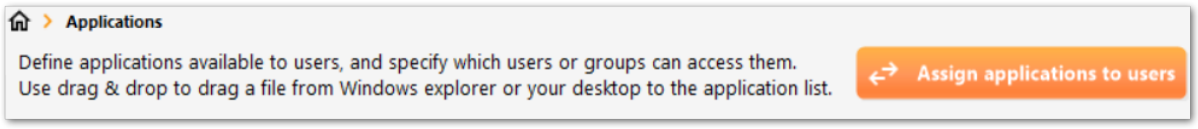
Um Benutzer zu entfernen, deaktivieren Sie einfach das Kontrollkästchen neben dem Benutzernamen.

Diese Aktion unterstützt die Mehrfachauswahl

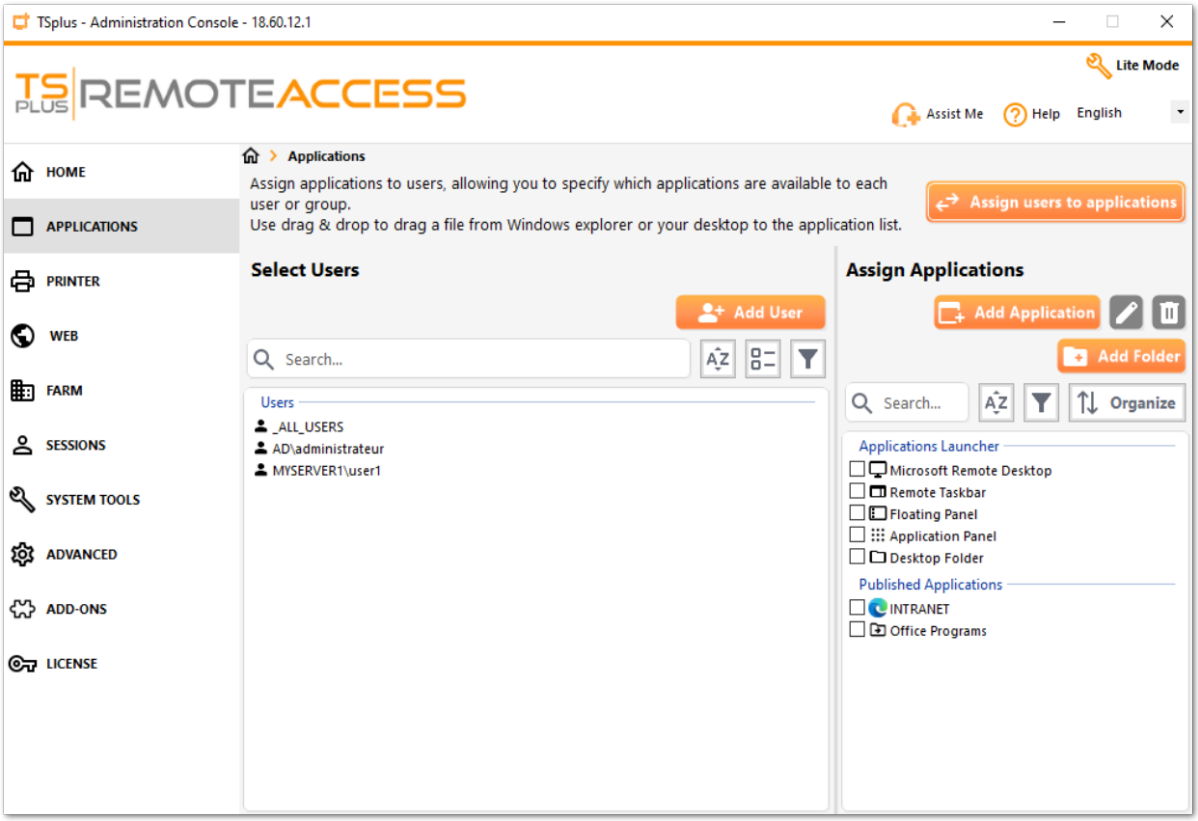
Das bedeutet, dass Sie mehrere Anwendungen auswählen können und nicht eine Anwendung nach der anderen zuweisen müssen.

Anwendungen Benutzern oder Gruppen zuweisen

Wenn Sie lieber Benutzer oder Gruppen auswählen und ihnen Anwendungen zuweisen möchten, können Sie dies tun, indem Sie auf „Anwendungen Benutzern zuweisen“ klicken.



Dies wird das linke und rechte Seitenpanel umdrehen.



Nachdem Sie auf die Schaltfläche geklickt haben, um Anwendungen Benutzern zuzuweisen:

1. Benutzer oder Gruppen auswählen, die Sie Ihrer Anwendung zuweisen möchten, indem Sie im linken Panel auswählen.
2. Überprüfen Sie im rechten Bereich das Kästchen neben dem Namen Ihrer Anwendung, um die ausgewählten Benutzer oder Gruppen dieser Anwendung zuzuweisen.

Wenn ich den Notepad dem Benutzer "benjamin" zuweisen möchte, wähle einfach den Benutzer

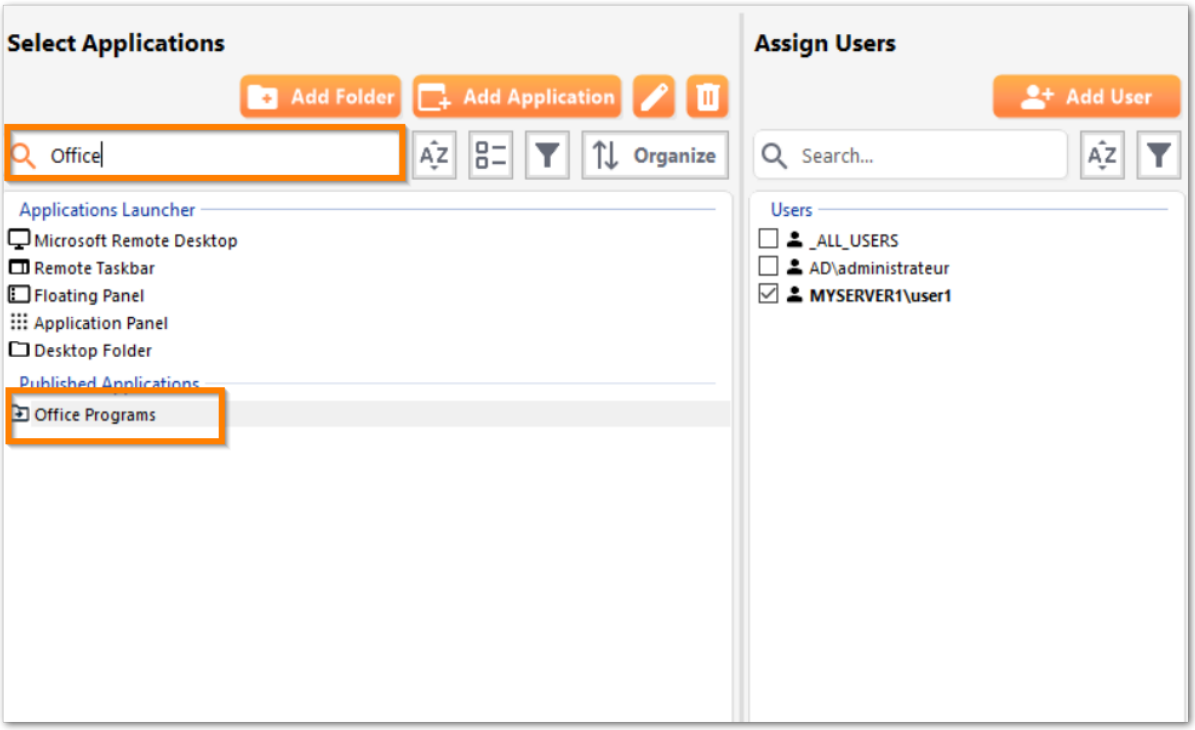
"benjamin" links aus und aktiviere das Kontrollkästchen neben dem Anwendungsnamen "notepad" rechts.

Um Anwendungen zu entfernen, deaktivieren Sie einfach das Kontrollkästchen neben dem Anwendungsnamen.

Diese Aktion unterstützt die Mehrfachauswahl
Das bedeutet, dass Sie mehrere Benutzer auswählen können und die Benutzer nicht einzeln zuweisen müssen.

Suchen und filtern

Um die Verwaltung der Benutzerzuweisungen zu erleichtern, steht eine Suchleiste sowie eine Filtertaste zur Verfügung, mit der Sie nur Benutzer oder nur Gruppen anzeigen können.

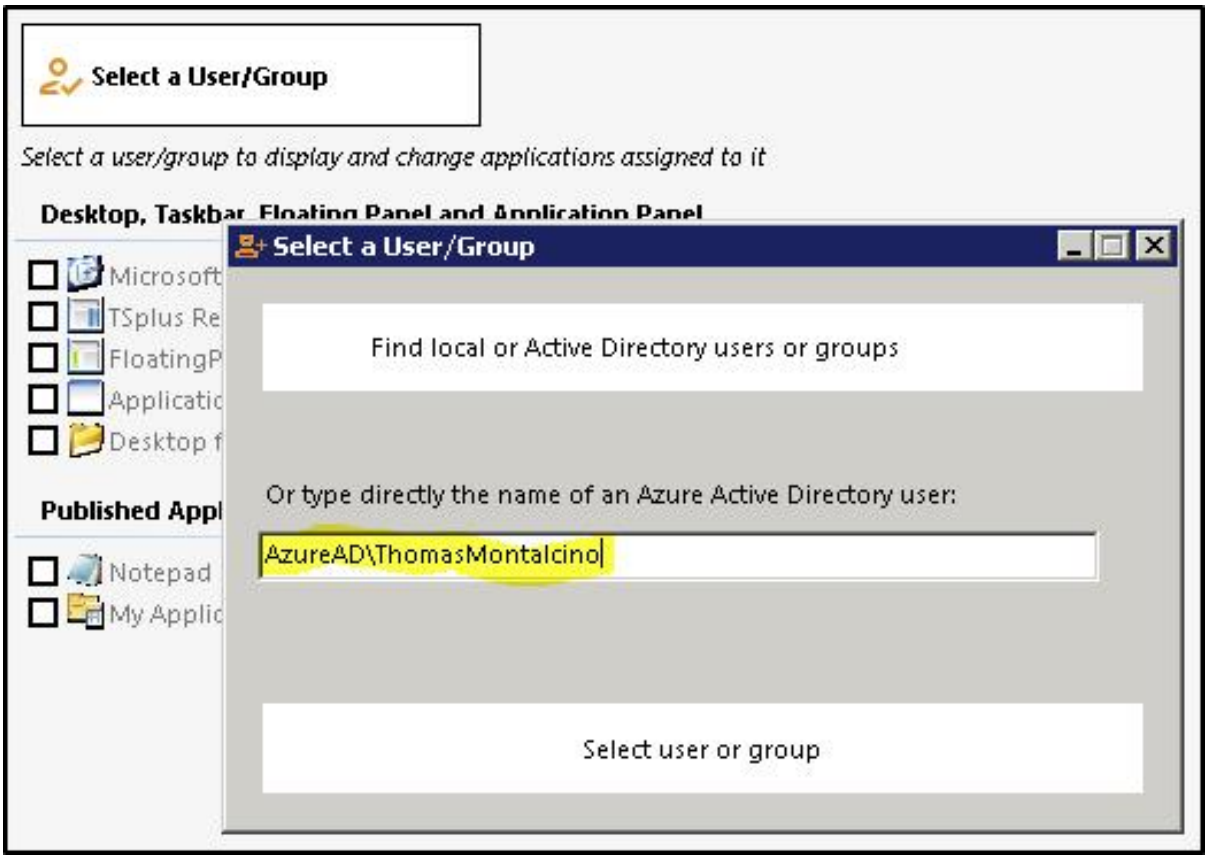


Sie können auch die Filtertaste verwenden, damit nur zugewiesene/nicht zugewiesene Anwendungen (oder zugewiesene/nicht zugewiesene Benutzer, wenn Sie die Ansicht wechseln) angezeigt werden.
Dies wird Ihnen helfen, Ihre Zuweisungen zu verwalten, falls Sie entweder viele Benutzer mit zugewiesenen Anwendungen haben oder einfach viele veröffentlichte Anwendungen.

Zuweisen von Anwendungen zu Benutzern mit Azure Active Directory

Übersicht

Um einen Azure Active Directory-Benutzer einer Anwendung im AdminTool > Anwendungen > Benutzer zuzuweisen:



Lokale oder Active Directory-Benutzer müssen mit der Schaltfläche Lokale oder Active Directory-Benutzer oder -Gruppen suchen ausgewählt werden. Nur externe Benutzer können direkt in das Textfeld eingegeben werden.

Integrierte Webserver-Verwaltung

Ihr Remote Desktop-Server muss verfügbar, leicht zugänglich und sicher sein. Deshalb nutzt TSplus einen integrierten Webserver, der Ihnen hilft, seinen Status und seine Funktionen einfach zu verwalten.

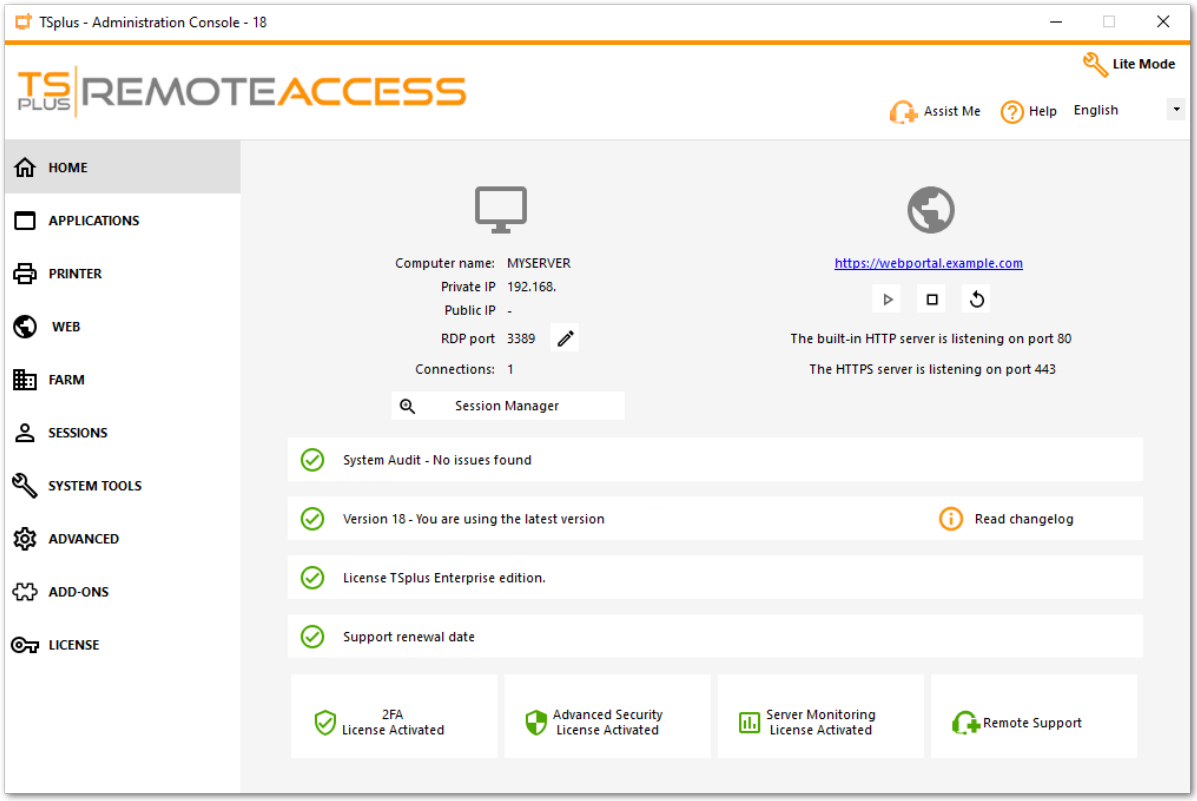
Eine Verwaltungs-Konsole ist im Administrations-Tool verfügbar. Diese Verwaltungs-Konsole ermöglicht es Ihnen, den Status des integrierten Webservers von Terminal Service Plus anzuzeigen und zu konfigurieren.

Wenn Sie install TSplus Webserver hören standardmäßig auf den Ports 80 und 443. Stellen Sie sicher, dass die definierten Ports verfügbar sind und dass Java auf dem Server installiert ist.

Siehe das Video über Webfunktionen.

Status der Webserverkomponenten

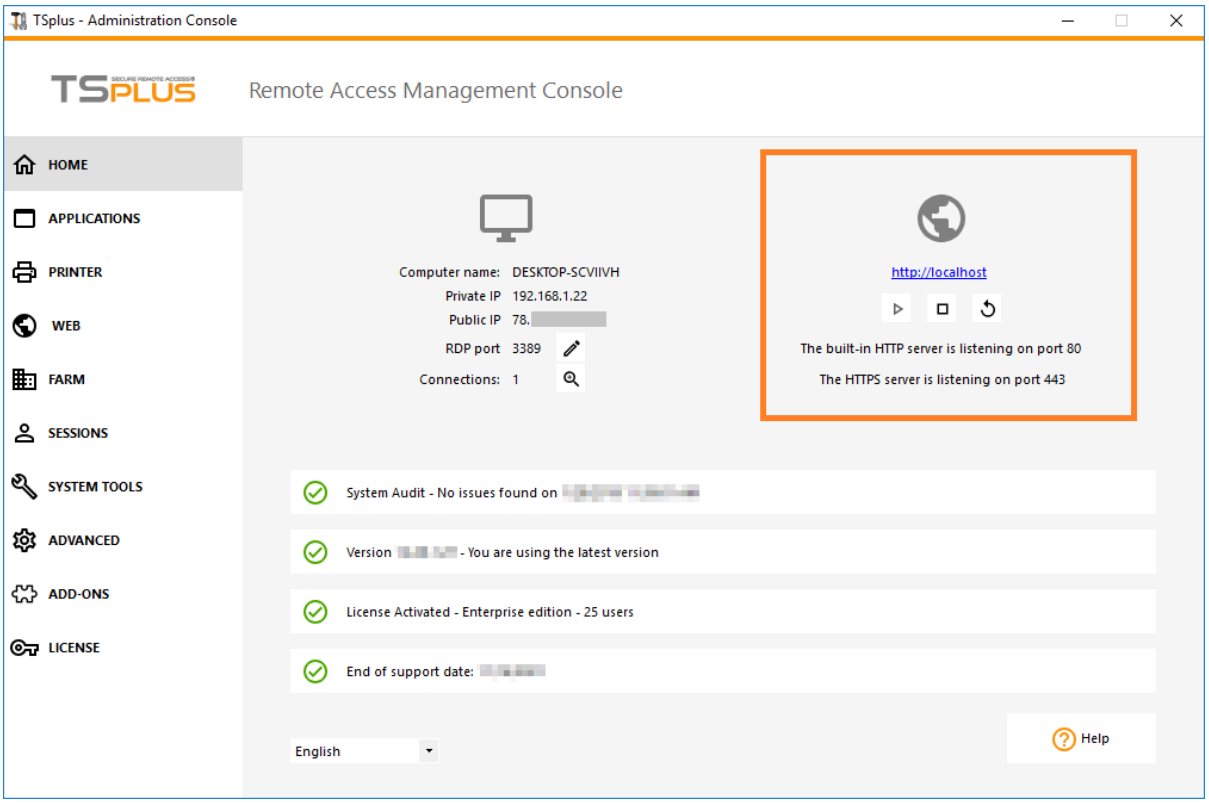
Der Status der Hauptkomponenten des Webservers wird auf dem Dashboard der AdminTool-Startseite angezeigt.



Ports Überlegungen (Lokale Maschine und Firewall / Router)

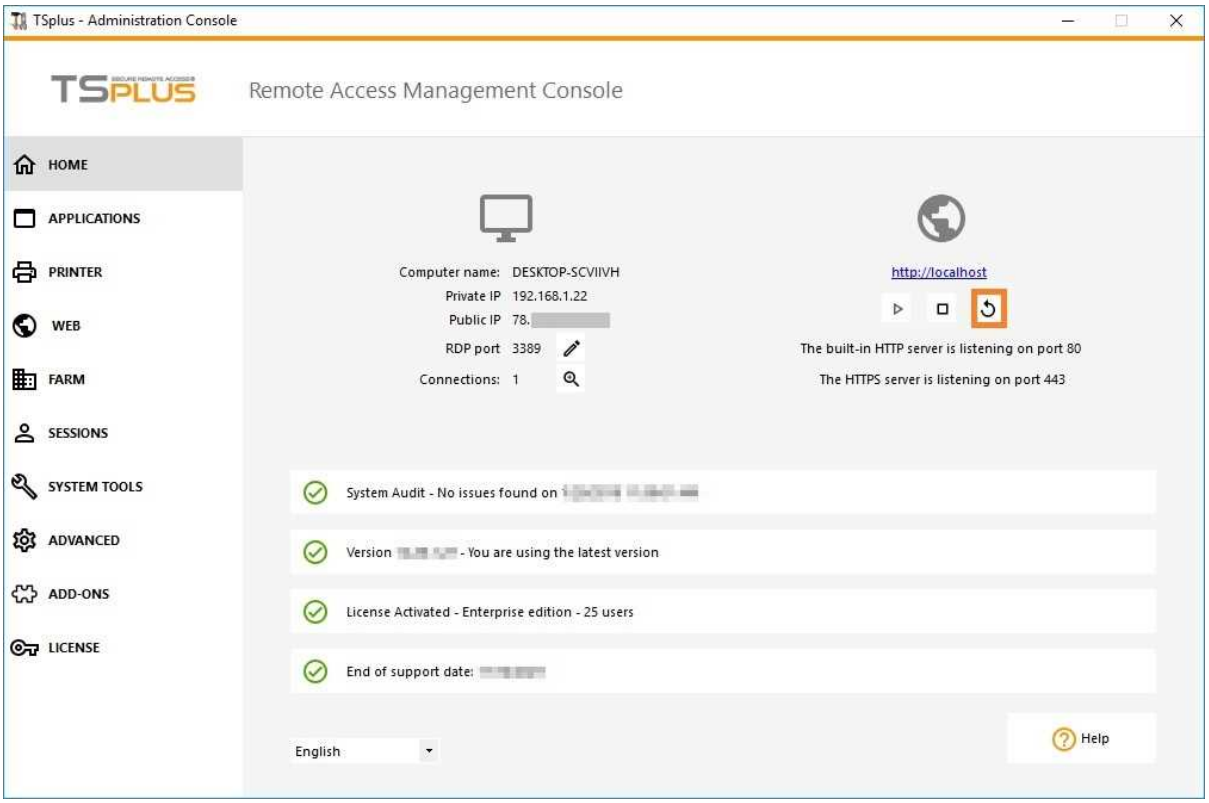
Terminal Service Plus benötigt nur entweder Port 80 oder Port 443, um geöffnet zu sein.

Port 3389 kann geschlossen bleiben.

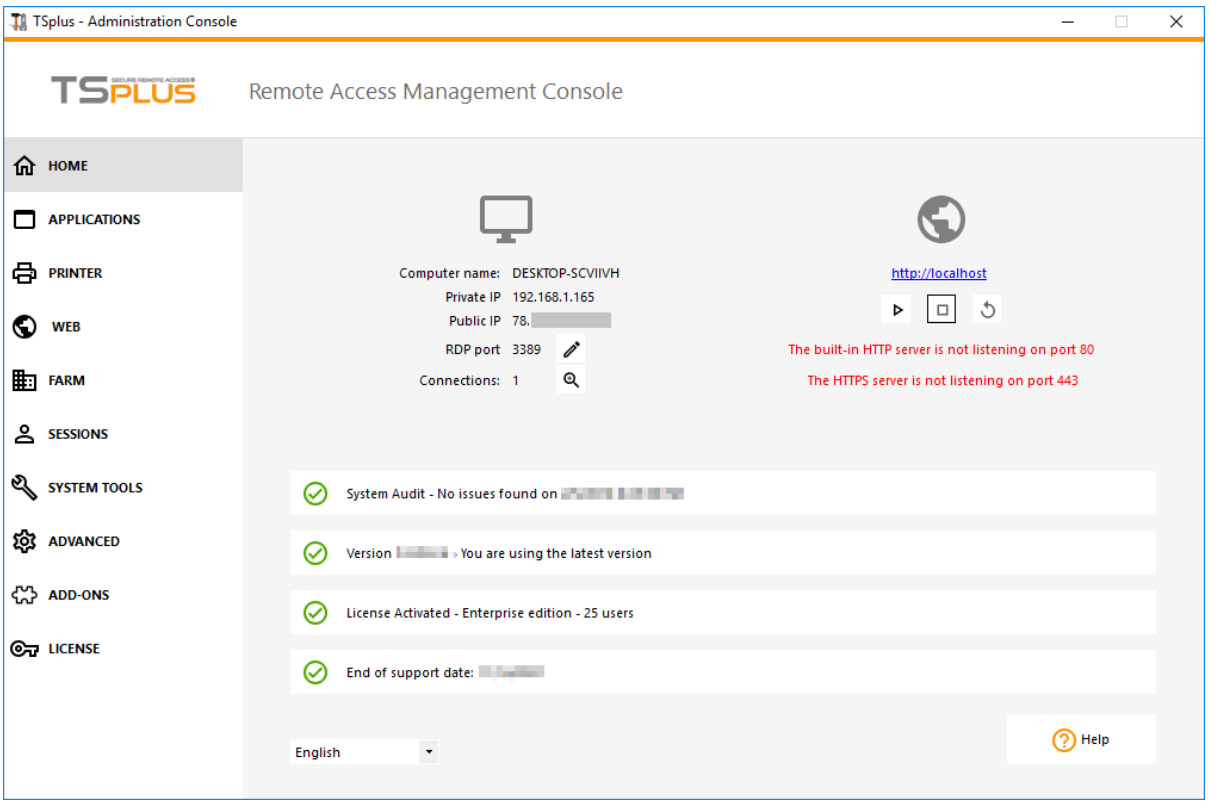


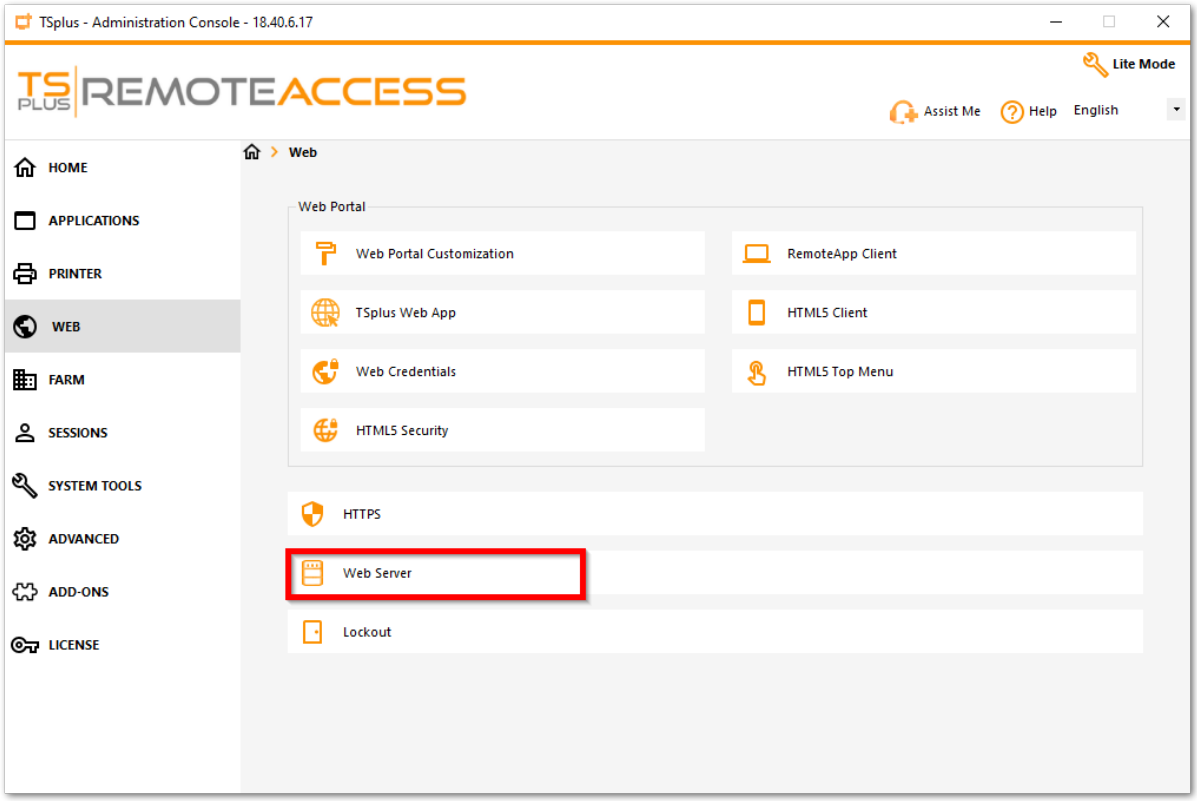
Webserverdienst neu starten / stoppen

Wenn Sie feststellen, dass ein Dienst nicht läuft, müssen Sie möglicherweise die Webserver neu starten, indem Sie auf die Schaltfläche „Webserver neu starten“ klicken, die durch einen Pfeil auf der rechten Seite dargestellt wird. Die Webserver werden neu gestartet und der Dienst sollte wieder laufen.



Wenn Sie auf die Schaltfläche „Webserver stoppen“ in der Mitte klicken, werden die Webserver gestoppt. Der Status des HTTP- und HTTPS-Servers wird jetzt rot angezeigt, was darauf hinweist, dass die HTTP-/HTTPS-Dienste gestoppt sind.





Sie können die Ports während der Installation oder jederzeit ändern, indem Sie auf die Registerkarte Web - Webserver klicken. Auf dieser Registerkarte können Sie einen anderen HTTP-Webserver auswählen, den Stammordner des Webservers ändern und die HTTP/HTTPS-Portnummern anpassen. Stellen Sie sicher, dass diese Ports verfügbar sind, bevor Sie sie ändern: Wenn ein Konflikt auftritt, funktioniert der TSplus-Webserver nicht. Hier ist eine nicht erschöpfende Liste von TCP-Ports, die von einer Anwendung auf Ihrem Server verwendet werden könnten. Sobald diese Änderungen vorgenommen wurden, klicken Sie auf Speichern und das AdminTool wird neu gestartet.

###HTTP nur oder HTTP auf HTTPS deaktivieren

Siehe diese Dokumentation für weitere Informationen zu diesem Thema.

Für detailliertere Informationen über **Serveranpassung** und **Einstellungen** , siehe diese Seiten:

Webportal-Anpassung , Webanwendungen-Portal , Web-Anmeldeinformationen .

Die Auswahl Ihrer Cipher-Suiten zur Verbesserung der Sicherheit

Übersicht

TLS/SSL, die Sicherheit hinter HTTPS, kann mehrere verschiedene Algorithmen verwenden, um eine Verbindung zu sichern, zu verschlüsseln und zu authentifizieren.

Die Wahl des zu verwendenden Algorithmus wird durch eine Vereinbarung zwischen dem Server und dem Client entschieden, abhängig davon, welche Algorithmen auf jeder Seite verfügbar sind.

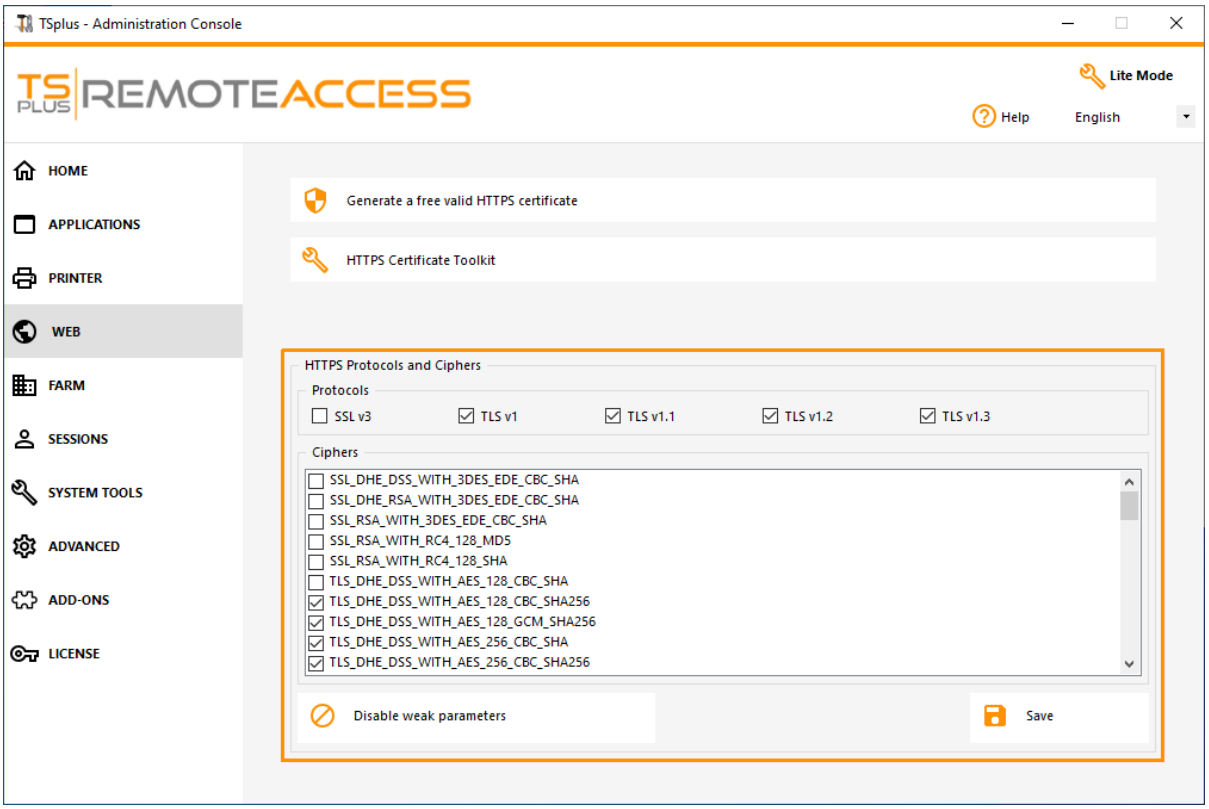
Ein Cipher-Suite ist eine benannte Kombination aus Authentifizierung, Verschlüsselung, Nachrichtenauthentifizierung und Schlüsselwechselalgorithmen.

Der Terminal Service Plus-Server kann viele verschiedene Cipher-Suiten verarbeiten. Einige von ihnen sind sicherer als andere, aber einige alte/legacy Browser benötigen möglicherweise relativ schwache Algorithmen, um eine Verbindung herzustellen.

Dies ist der Grund, warum Terminal Service Plus Ihnen die Auswahl der Verschlüsselungssuiten ermöglicht, die Sie aktivieren möchten. Natürlich verfügt Terminal Service Plus auch über eine einfache Einstellung, um die schwächsten Algorithmen zu deaktivieren, wodurch die Sicherheit Ihrer Verbindungen verbessert wird.

HTTPS-Protokolle und Cipher-Auswahl

Um die Auswahl der Terminal Service Plus-Verschlüsselungen anzuzeigen, öffnen Sie das Terminal Service Plus AdminTool, klicken Sie auf die Registerkarte „Web - HTTPS“, wo Sie die HTTPS-Protokolle und -Verschlüsselungen sehen werden:



Aktivieren/Deaktivieren einer Cipher Suite

Sie können eine Verschlüsselungssuite einfach aktivieren, indem Sie das Kontrollkästchen aktivieren, und eine Verschlüsselungssuite deaktivieren, indem Sie es deaktivieren.

Wenn Ihre Auswahl abgeschlossen ist, klicken Sie auf „Speichern“.

Dies wird Ihre Auswahl speichern und die neue Konfiguration im integrierten Webserver von Terminal Service Plus neu laden. Ihre neue Auswahl der Verschlüsselungssuiten wird sofort für jede neue Verbindung zu Ihrem Server angewendet.

Empfohlene Auswahl von Cipher-Suiten

Wir empfehlen den meisten Administratoren, unsere empfohlene Auswahl an Cipher-Suiten zu verwenden, indem sie einfach auf die Schaltfläche „Schwache Parameter deaktivieren“ und dann auf die Schaltfläche „Speichern“ klicken.

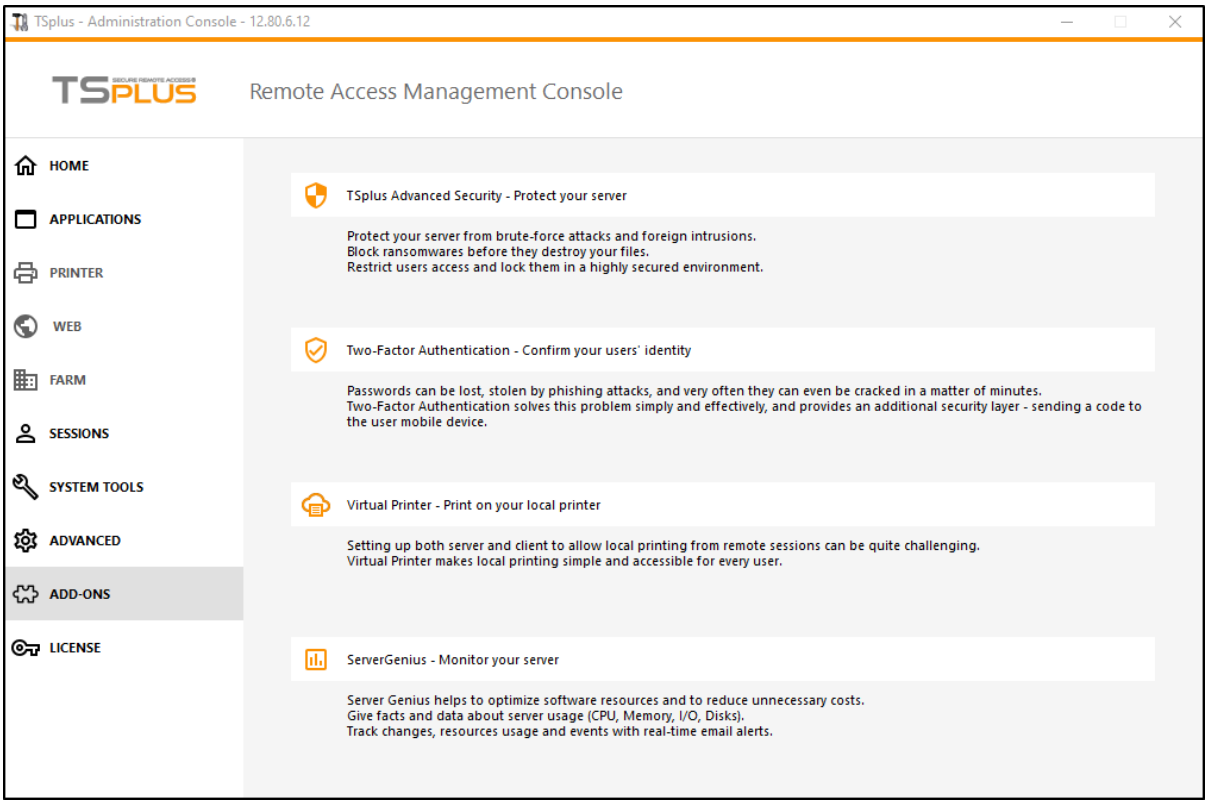
Diese Aktion deaktiviert alle Cipher-Suiten, die derzeit als schwach bekannt sind.

Sie können überprüfen mit SSL Labs Online Testing Tool ohne diese schwachen Cipher-Suiten sollten Sie die maximale Note: A! erhalten

Klicken-zum-Helfen - Administrationswerkzeug - Add-ons

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

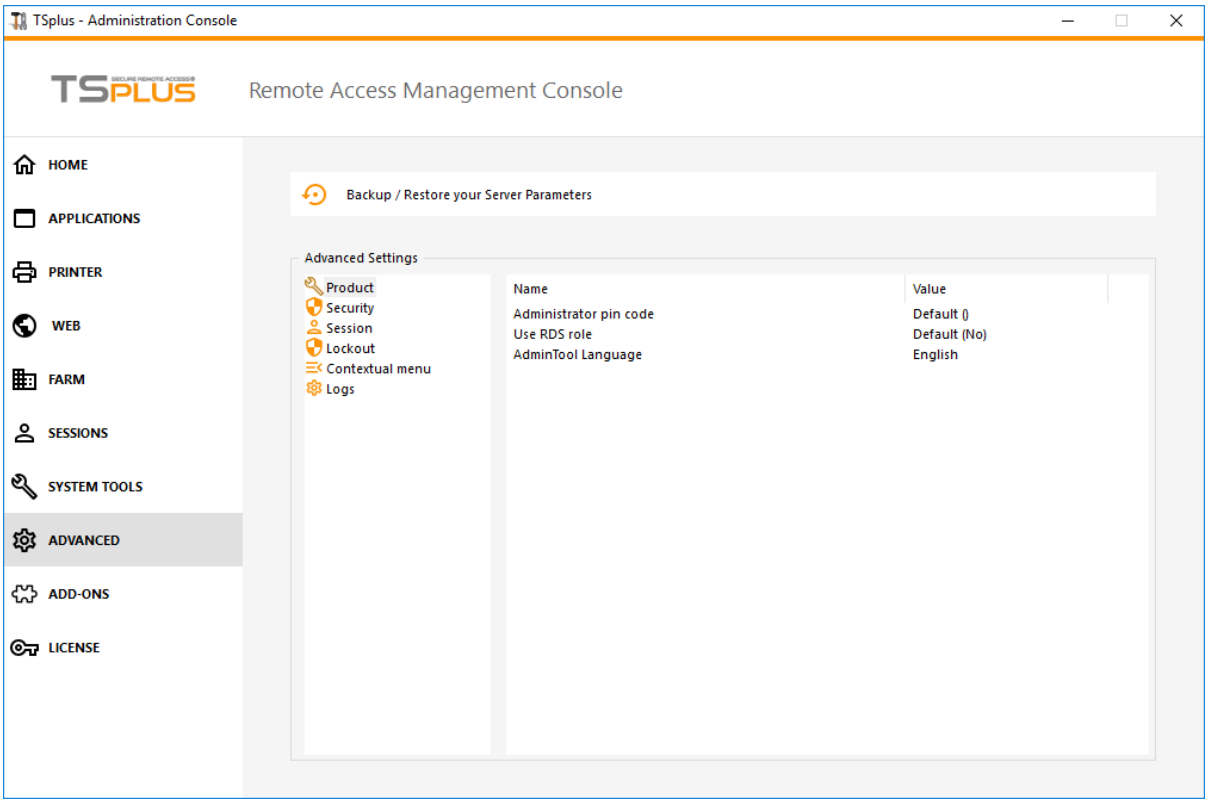
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Administrationswerkzeug - Erweitert

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

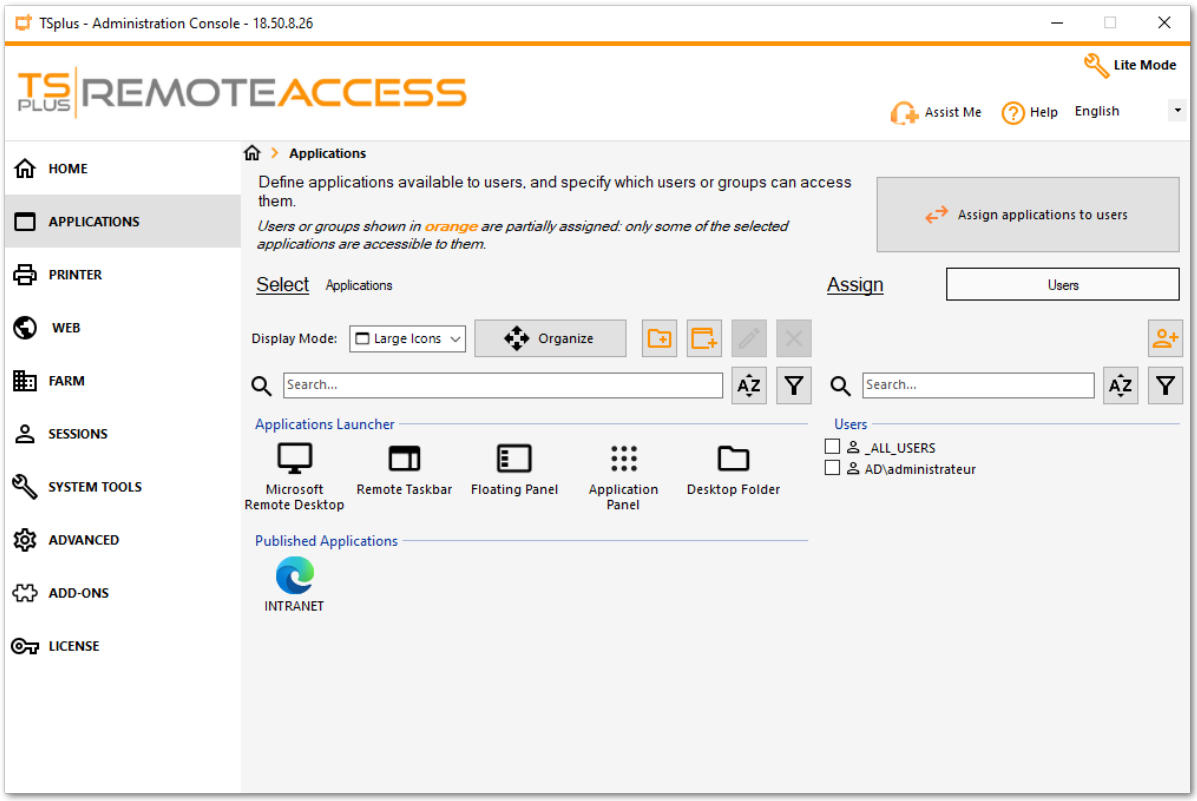
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Administrationswerkzeug - Anwendungen

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

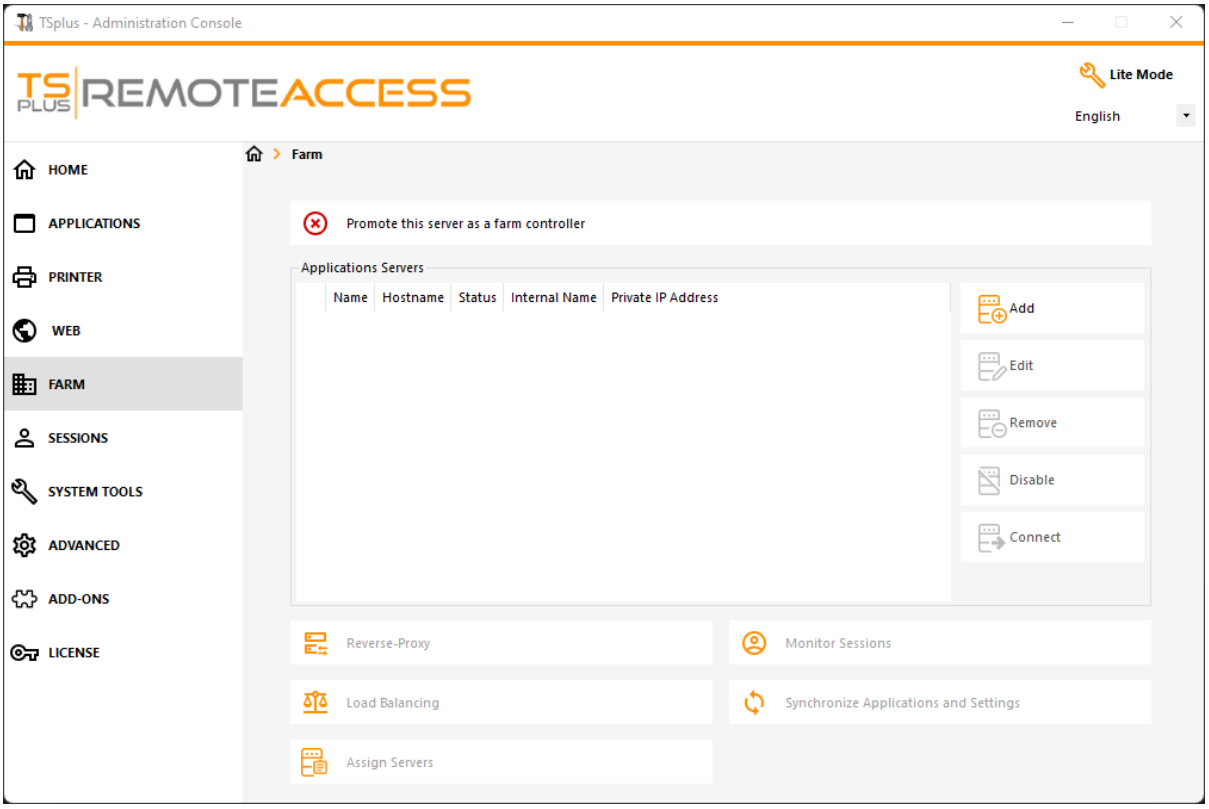
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Admin-Tool - Farm

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

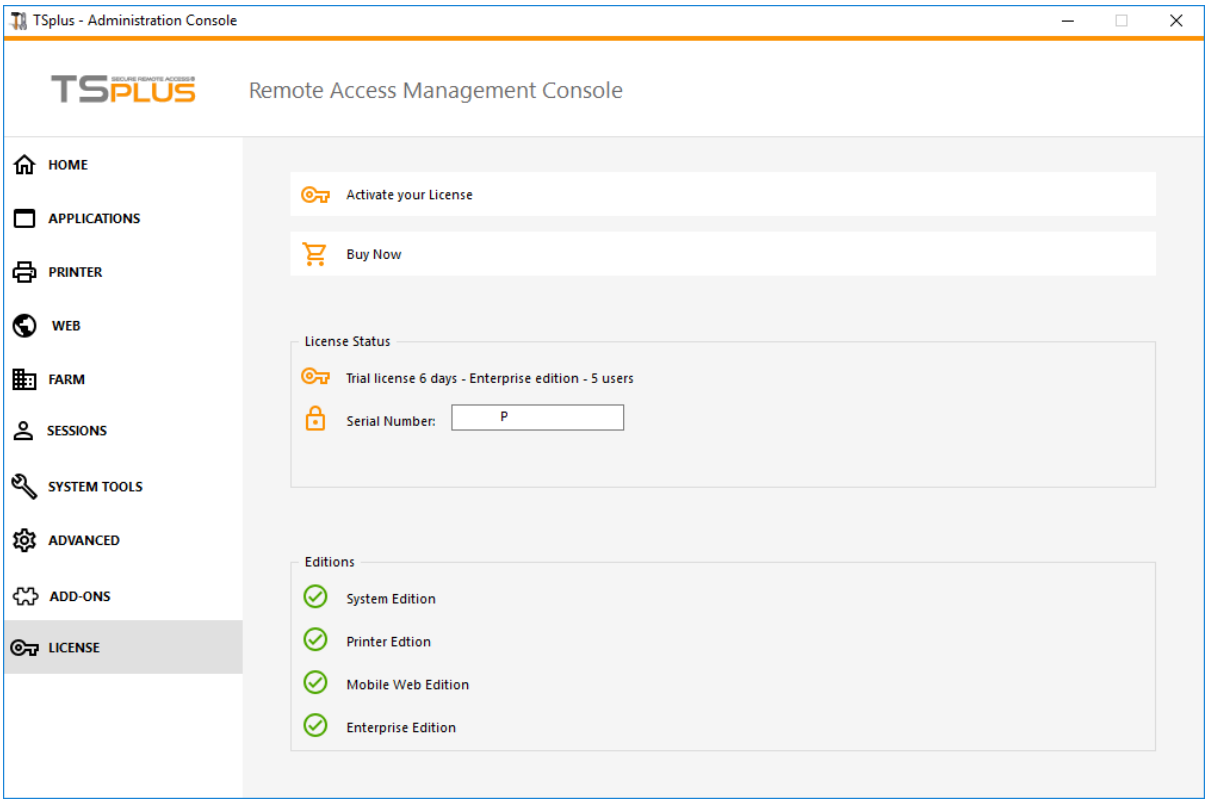
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Administrationswerkzeug - Lizenz

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

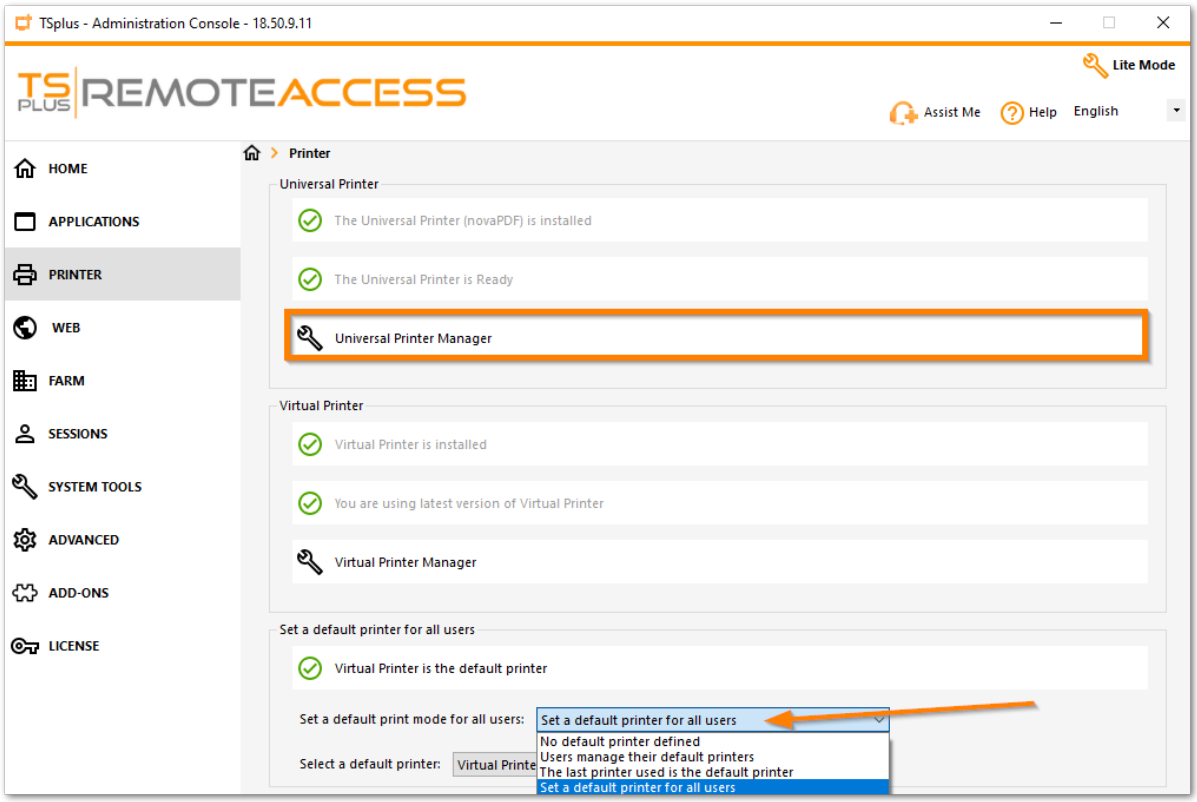
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Admin-Tool - Drucker

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Administrationswerkzeug - Sicherheit

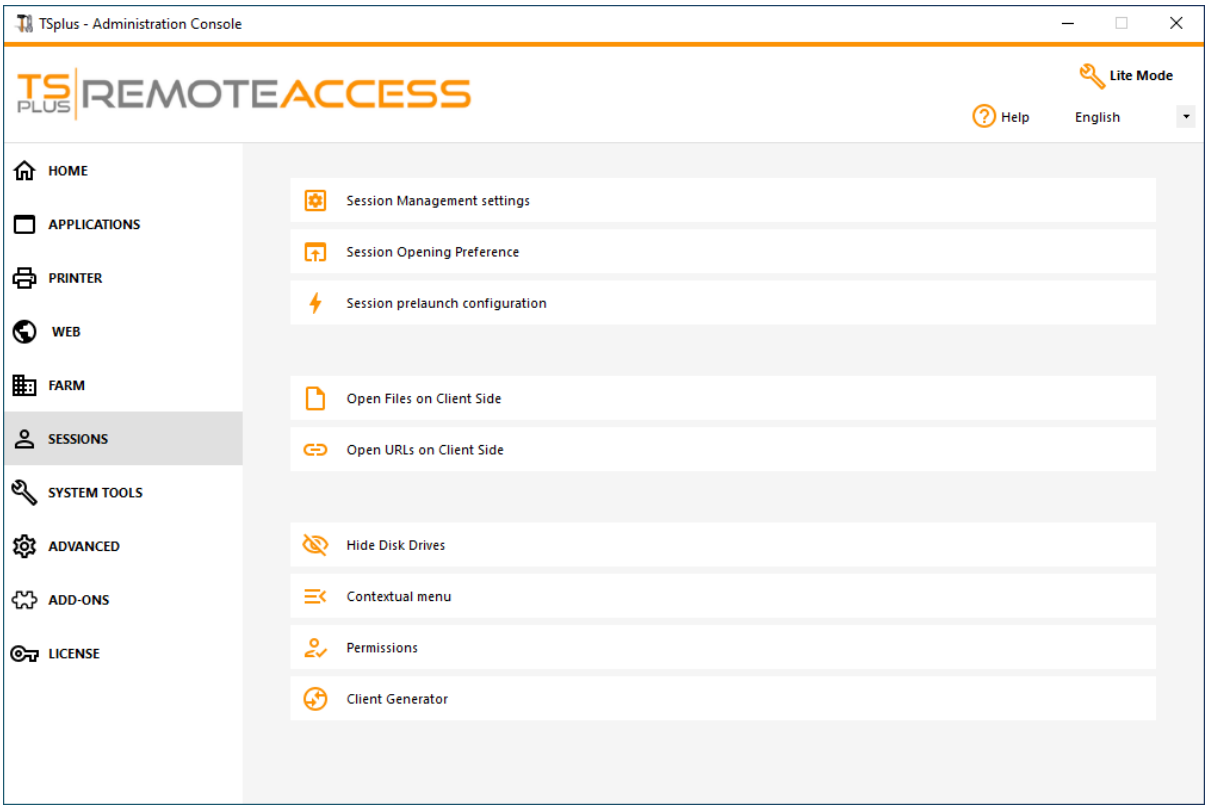
Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!

Klicken-zum-Helfen - Administrationswerkzeug - Sitzungen

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

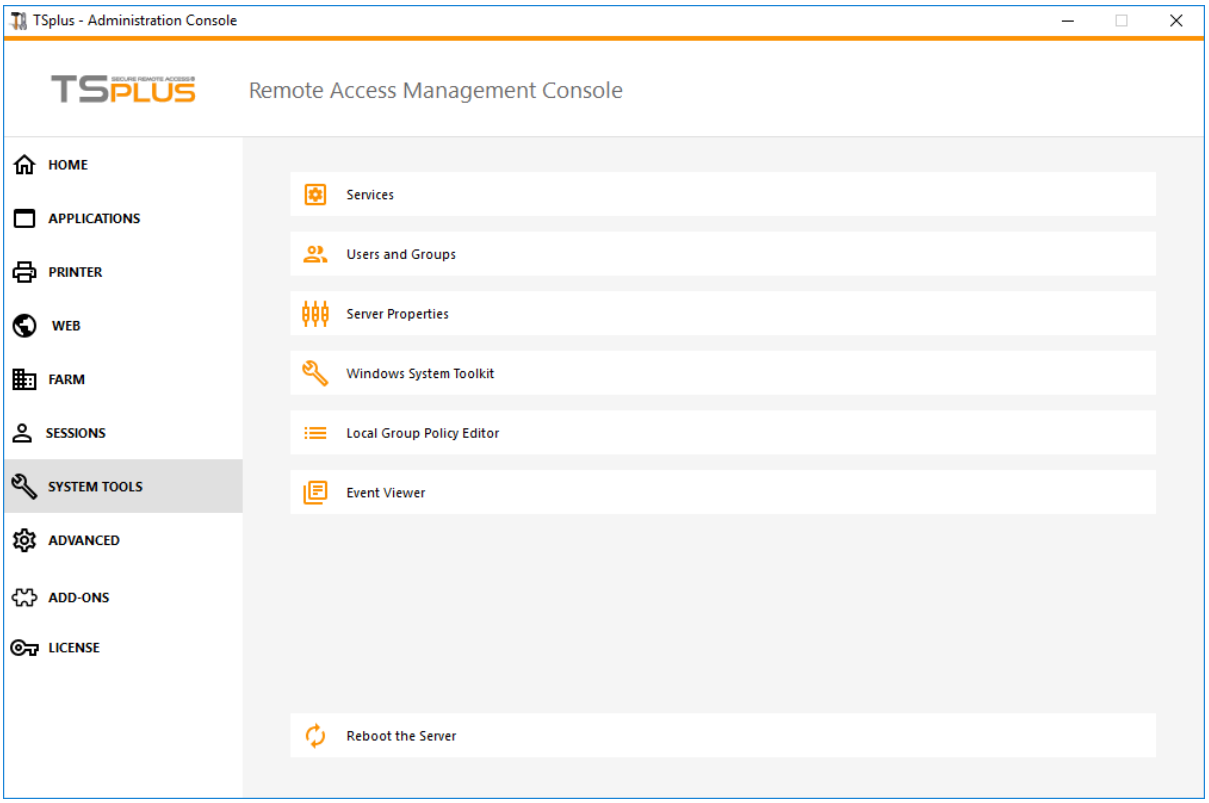
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Administrationswerkzeug - System

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

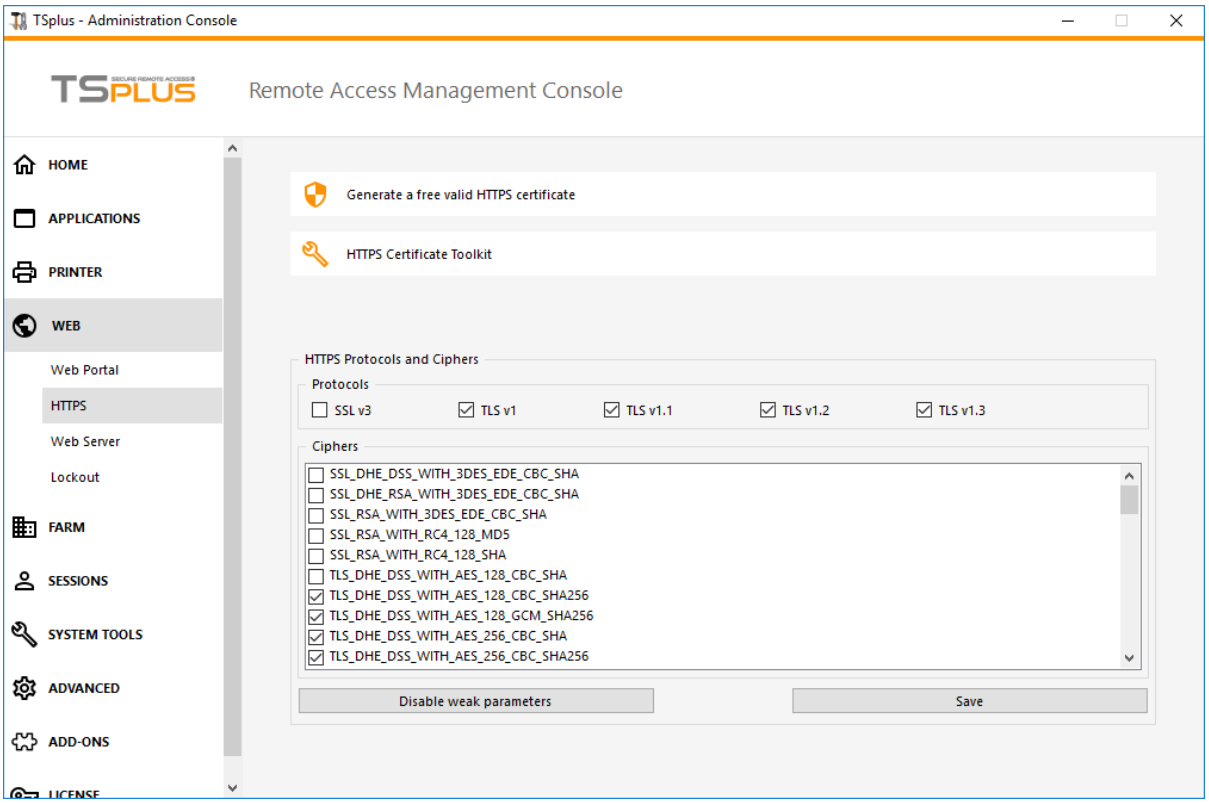
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Administrationswerkzeug - Web

Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

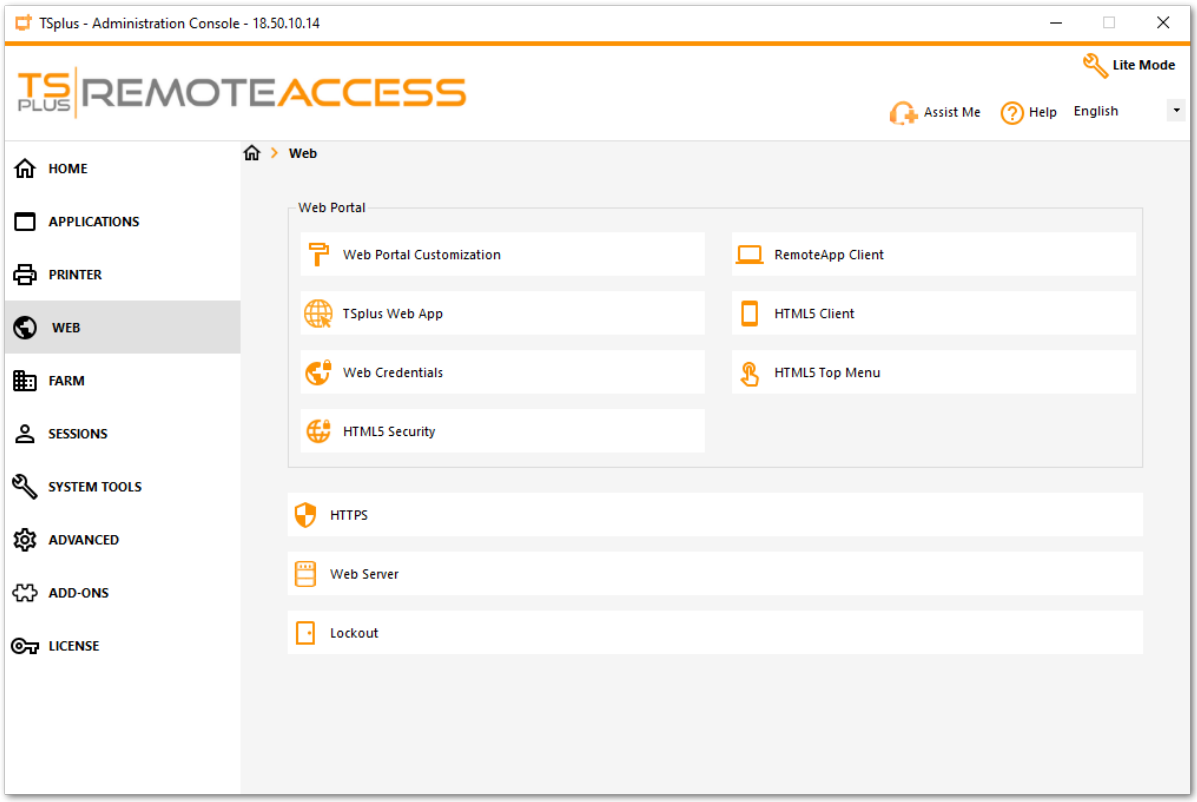
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!



Klicken-zum-Helfen - Administrationswerkzeug - Web

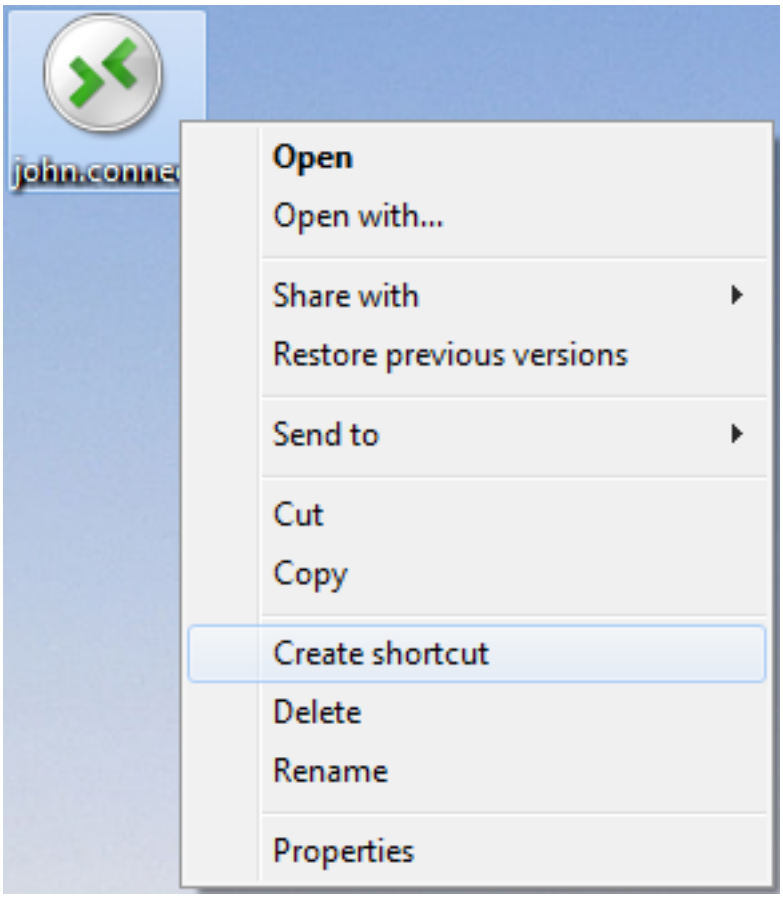
Möchten Sie schnell Hilfe zu einer Funktion des Terminal Service Plus Admin Tools erhalten?

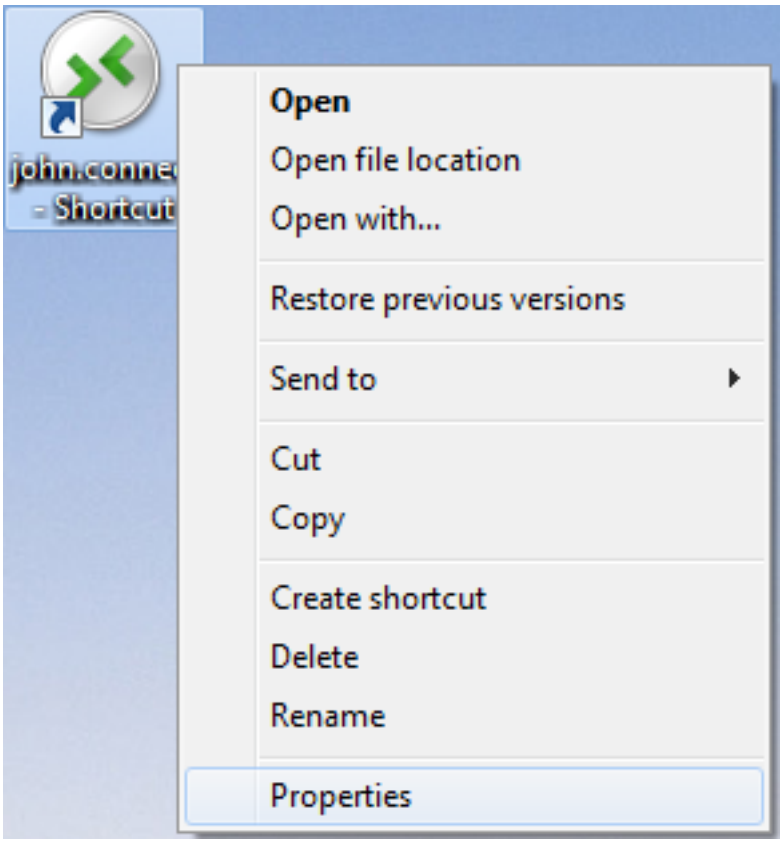
Nur **klicken Sie auf eine Kachel oder auf einen Tab** um zur passenden Hilfe zu gelangen!

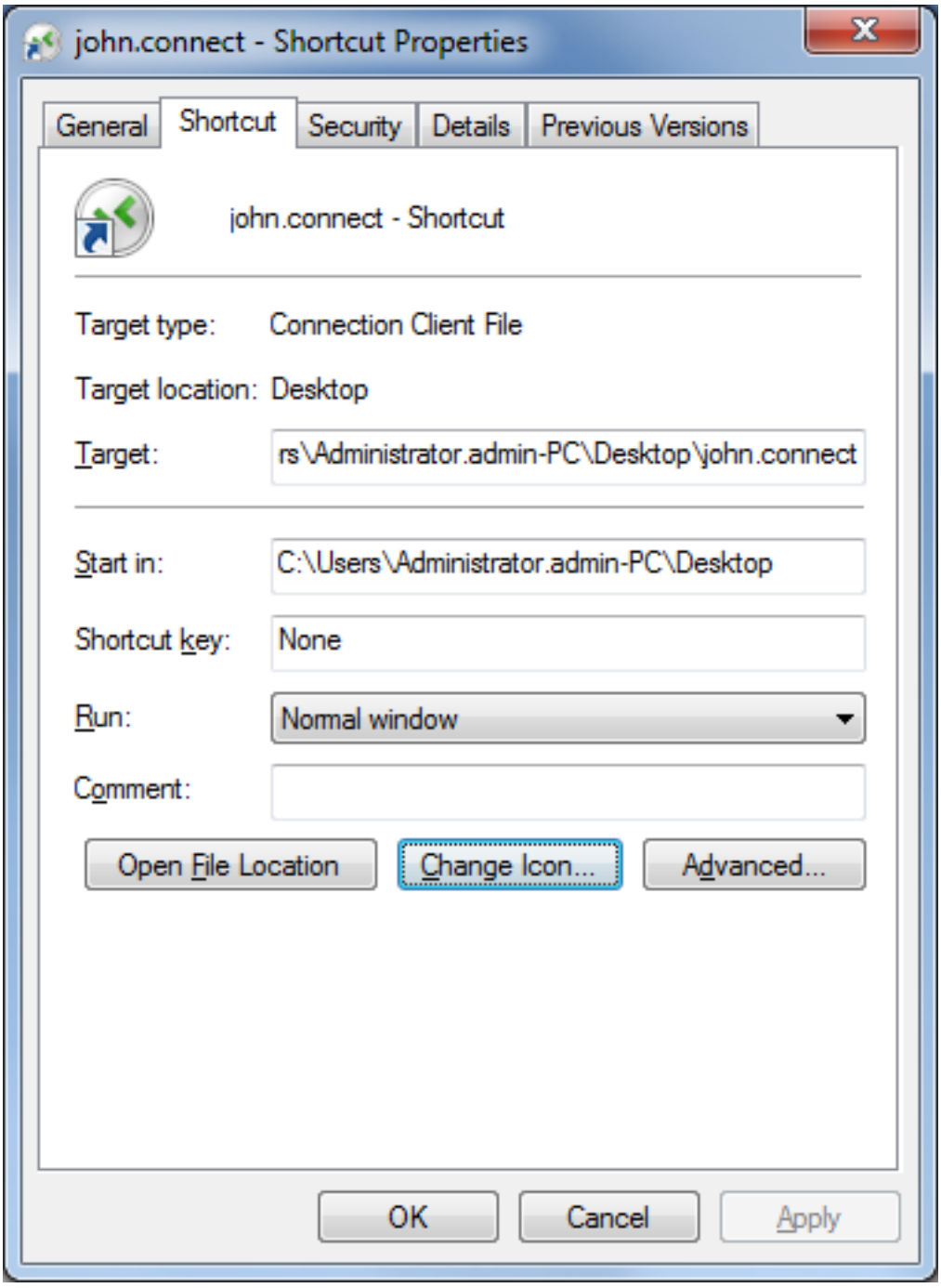


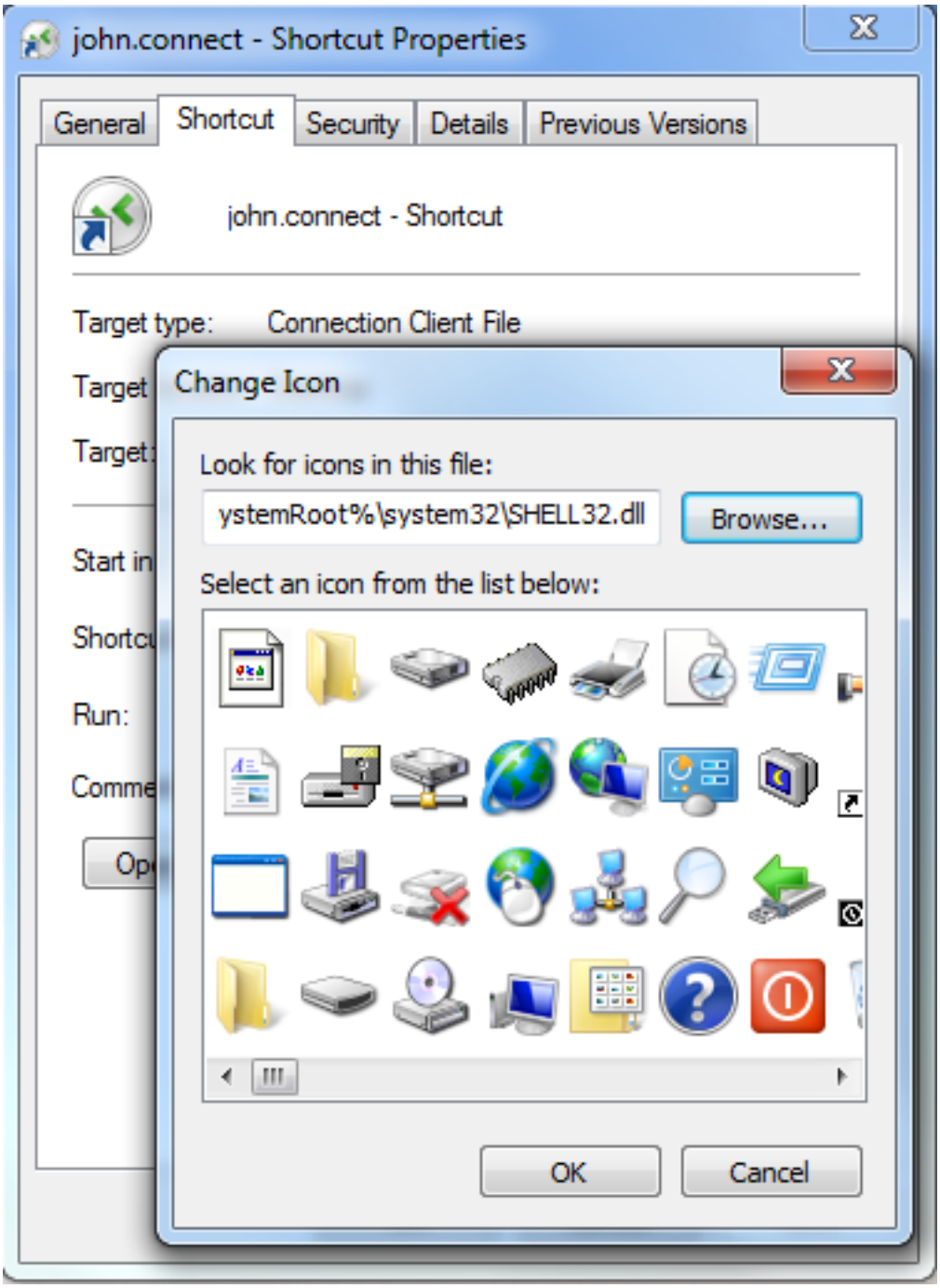
Wie man das Symbol des TSplus-Clients ändert

Um das generierte Symbol des Clients zu ändern, erstellen Sie einfach eine Verknüpfung des Clients und gehen Sie zu den Eigenschaften der Verknüpfung:




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

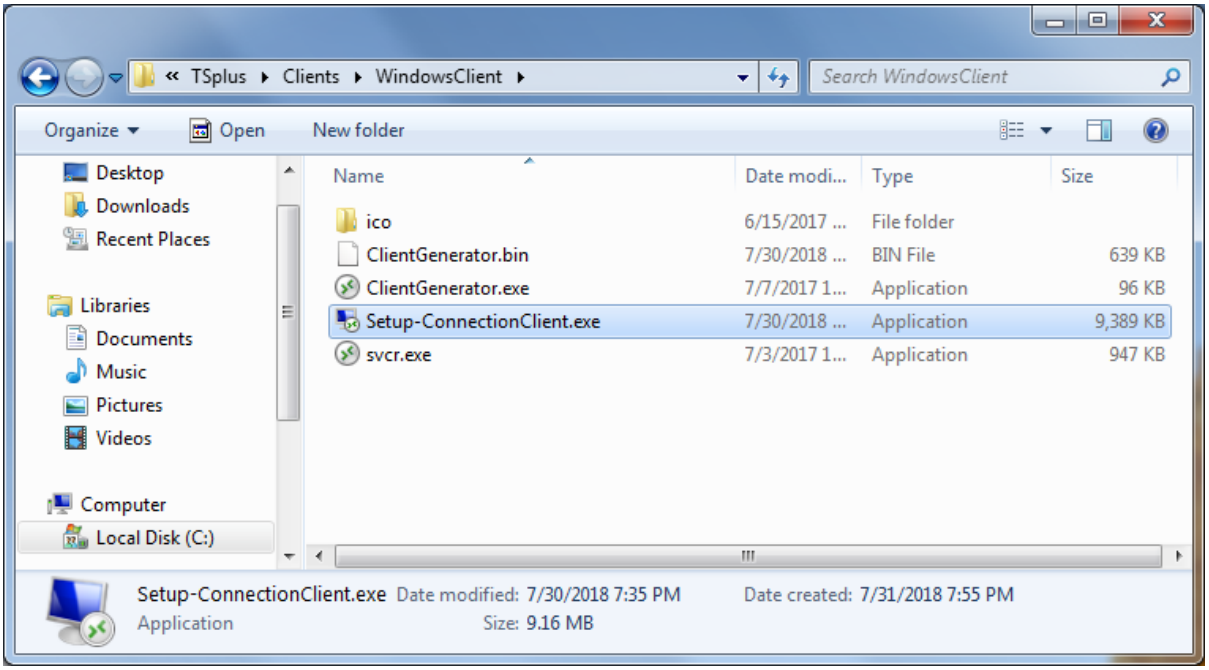

john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type:
Connection Client File
Target
Target:
Start in
Shortcu
Run:
Comme
Op
Change Icon
Look for icons in this file:
ystemRoot%\system32\SHELL32.dll
Browse...
Select an icon from the list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

TSplus Client Setup-Programm

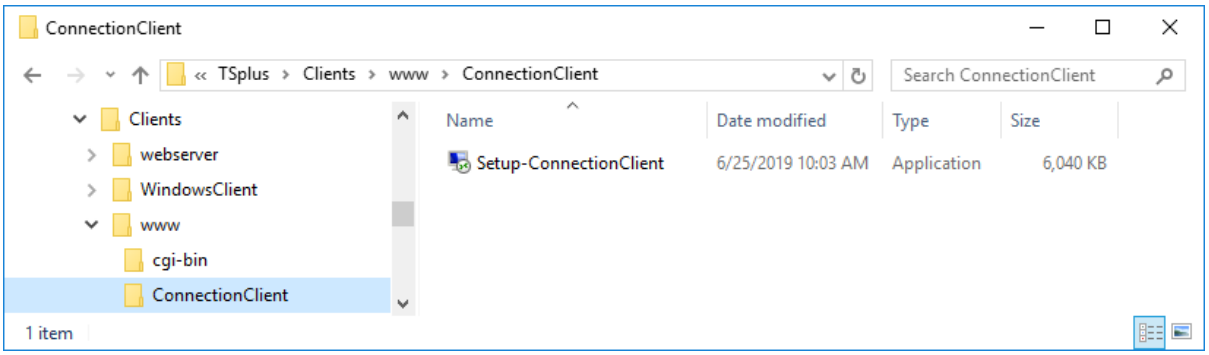
Installieren

Auf der Client-Seite, **Jeder Benutzer muss ein signiertes Programm mit dem Namen „Setup-ConnectionClient.exe“ als Voraussetzung ausführen.** .

Dieses Programm ist auf Ihrem Server im TSplus-Programmfolder verfügbar: C:\Program Files (x86)\TSplus\Clients\WindowsClient:



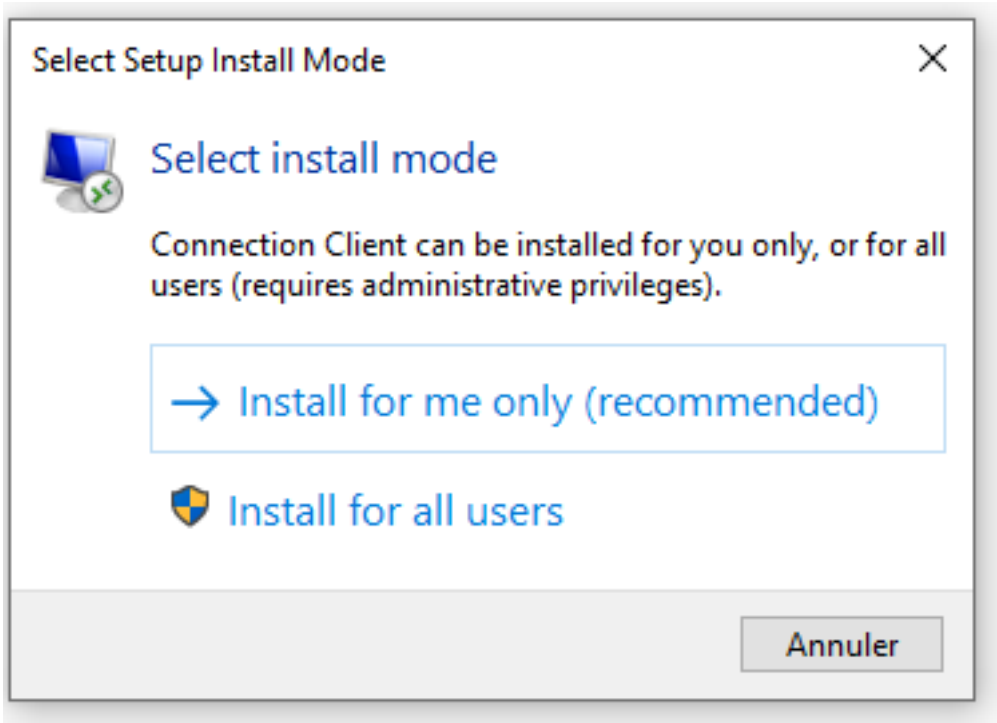
Es ist auch verfügbar in C:\Program Files (x86)\TSplus\Clients\www\ConnectionClient, sodass Ihre Benutzer das Programm einmal auf Ihrer Webserver-Adresse ausführen können: http://xxxxxxxxxx/ConnectionClient/Setup-ConnectionClient.exe



oder durch es herunterladen .

Für alle Benutzer installieren

Sie können jetzt den Verbindungsclient für alle Benutzer installieren. Das bedeutet, dass nach der Installation jeder Benutzer auf dem Computer davon profitieren und im RemoteApp-Modus über das Webportal sowie mit einer generierten .connect-Clientdatei eine Verbindung herstellen kann.



Hinweis: Damit dieses Pop-up angezeigt wird, müssen Sie den Connection Client nicht bereits installiert haben. Sie können auch während einer Installation über die Befehlszeile angeben, welchen Modus Sie mit dem Argument /ALLUSERS oder /CURRENTUSER verwenden möchten, um jeweils für alle Benutzer oder für den aktuellen Benutzer zu installieren.

Hinweis Seit TSplus 12.40, das Client-Setup-Programm und die RemoteApp-Client-Setup wurden zusammengeführt und können mit einem einzigen Setup bereitgestellt werden - wenn

Sie also das Setup des Verbindung Clients herunterladen, müssen Sie den RemoteApp Client nicht herunterladen.

Hardware-Identifikator & Klon-Server

1- Hardware-Identifikatoränderung.

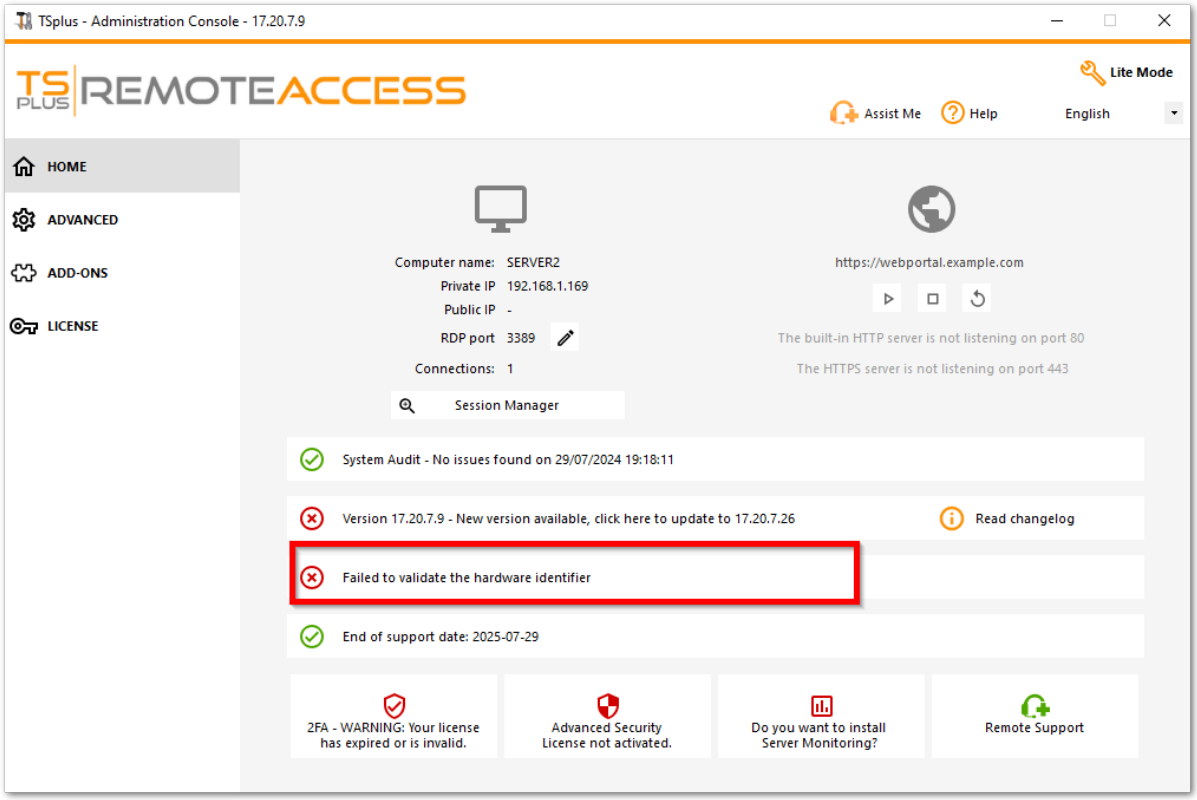
Reparatur des Hardware-Identifikators nach Klonen oder einem Update.

Warnung: Hardware-Identifikator konnte nicht validiert werden

Nach der Migration eines physischen Servers auf eine virtuelle Maschine oder ein Kernel-Update von Microsoft ändert sich der Lizenzstatus in "Hardware-Identifikator auf neuer Hardware konnte nicht validiert werden."

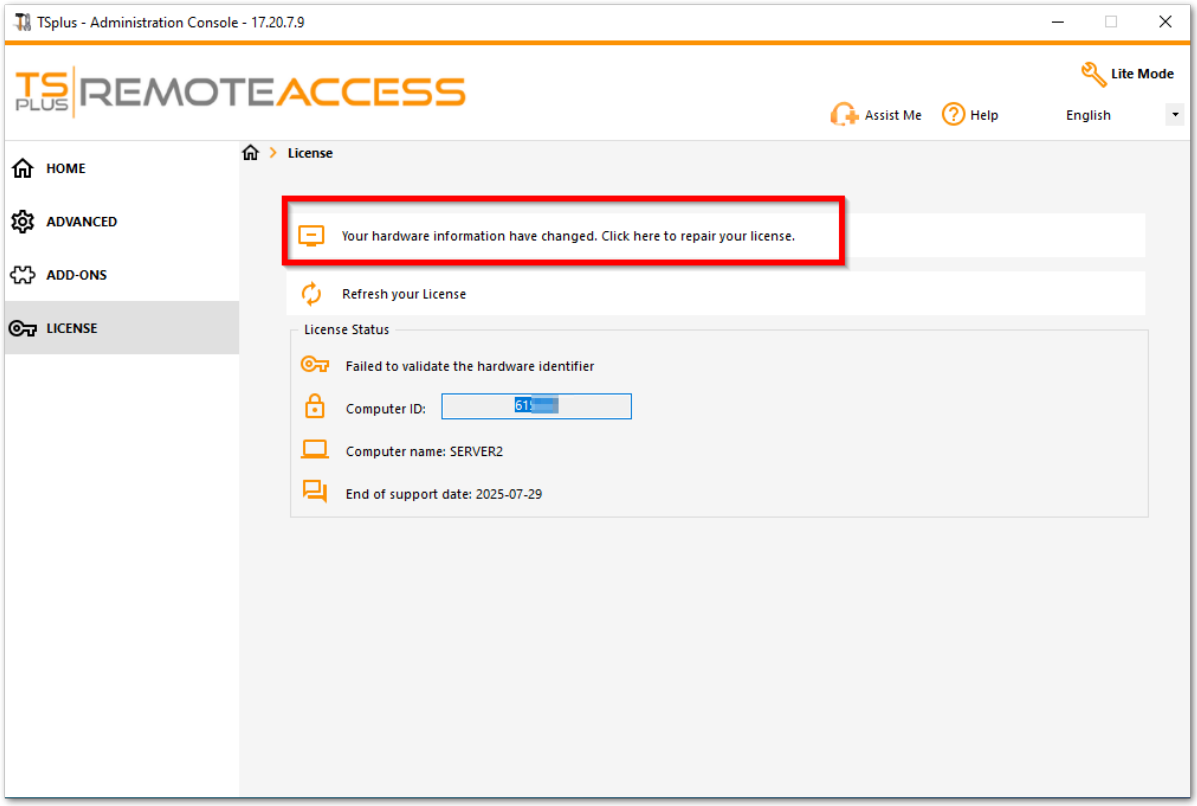
Diese Nachricht erscheint, weil TSplus einen Lizenzkonflikt festgestellt hat, der von einem Server auf einen anderen mit derselben Computer-ID und demselben Namen kopiert wurde.
Wir empfehlen bereits, Ihren neuen Server umzubenennen (Beispiel: SERVER1 > SERVER2)

- Starten Sie Ihren Server



Klicken Sie auf das Fenster, um zur Lizenzseite zu gelangen.

Dann klicken Sie auf die Registerkarte „Ihre Hardwareinformationen haben sich geändert. Klicken Sie hier, um Ihre Lizenz zu reparieren.“



Ein Popup zur "Lizenzübertragung" wird geöffnet, um Ihnen zu ermöglichen, Ihre Lizenz wiederherzustellen.

Fall 1: Sie haben keinen Support!
Rehosting wird daher nicht möglich sein, Sie müssen ein Support-Abonnement auf dem ursprünglichen Server abonnieren und die Migrationsaktion erneut starten.
Im Falle von Problemen, Kontaktieren Sie den Support und geben Sie Ihre Computer-ID und Ihren Aktivierungsschlüssel an.

Fall 2: Sie haben bereits seit 6 Monaten rehosted!
Die Nachricht: Sie haben diesen Computer in den letzten 6 Monaten bereits neu gehostet. Bitte kontaktieren Sie den Support, wenn Sie Hilfe beim Rehosting Ihrer Lizenz benötigen.

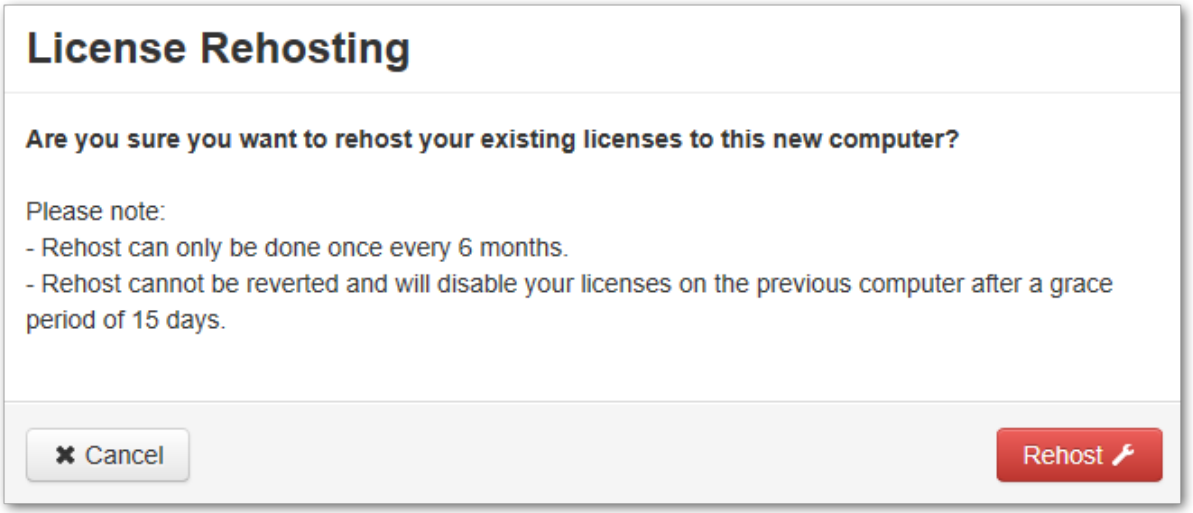
Die Neuhostung wird daher nicht möglich sein, Kontaktieren Sie den Support und geben Sie Ihre Computer-ID und Ihren Aktivierungsschlüssel an.

Fall 3: Sie haben Unterstützung!
Die folgende Nachricht erscheint: Sind Sie sicher, dass Sie Ihre bestehenden Lizenzen auf diesem neuen Computer neu hosten möchten?

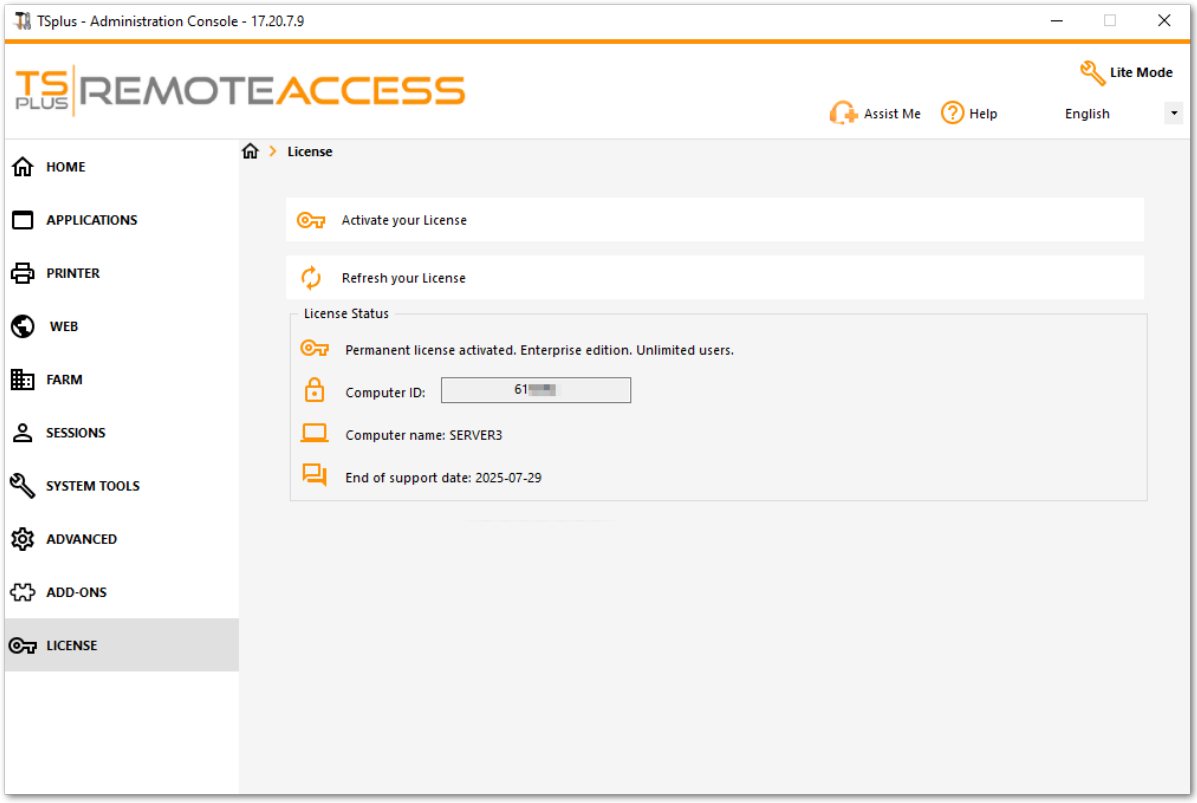
Bitte beachten Sie:

- Rehosting kann nur einmal alle 6 Monate durchgeführt werden.
- Rehosting kann nicht storniert werden und deaktiviert Ihre Lizenzen auf dem vorherigen Computer nach einer 15-tägigen Karenzzeit.

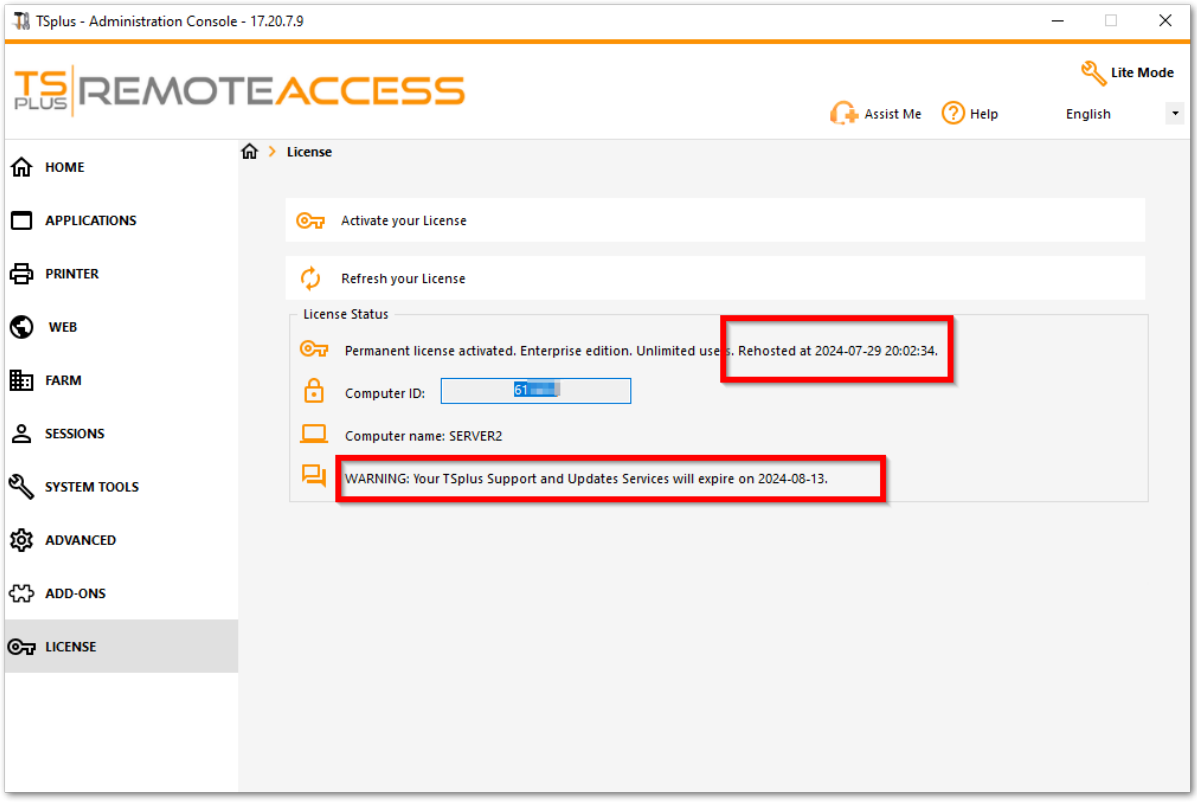
Klicken Sie auf den **„REHOST“** Taste



Ihre Lizenz ist rehosted!



Hinweis: Auf dem alten Server wird eine Nachricht mit dem Rehosting-Datum sowie dem Enddatum des Nutzungszeitraums des alten Servers (15 Tage) angezeigt.



Aktualisierungsfehler:

Führen Sie das Update-Release aus und überprüfen Sie, ob Ihr Problem nach dem Neustart Ihres Servers behoben wurde.

- Laden Sie die Aktualisierung veröffentlichen

2- Klonen Sie einen Server, während Sie den bestehenden Server beibehalten und eine neue Lizenz aktivieren.

Anforderungen

Beim Arbeiten mit geklonten virtuellen Maschinen ist es wichtig, den Computernamen und die Datenträger-ID zu ändern, um eine eindeutige TSplus Remote Access-Installation sicherzustellen und Lizenzprobleme zu vermeiden.

Computername Überlegungen

Der Computername wird im Windows-Registrierungseditor innerhalb des Images selbst gespeichert. Wenn er vor der Anwendung des Images geändert wird, wird er beim Booten von Windows von Sysprep überschrieben. Sie können jedoch einen Namen in einem vordefinieren. Unattended.xml Antwortdatei. Siehe Microsoft-Dokumentation für weitere Details.

Um den Computernamen festzulegen, fügen Sie den folgenden Abschnitt ein. Microsoft-Windows-Shell-Setup :

```
<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>
```

Volume-ID-Überlegungen

Die Volume-ID ist mit der Festplattenpartition verbunden, nicht mit dem Betriebssystem-Image. Sie kann vor der Anwendung des Images geändert werden und bleibt bestehen. Verwenden Sie volumeid.exe von Sysinternals, verfügbar unter Microsoft Sysinternals bevor Windows startet.

Bereitstellungsschritte

Beim Bereitstellen einer neuen virtuellen Maschine aus einem sysprepped Image wird Windows beim ersten Boot in die Out-Of-Box-Erfahrung (OOBE) eintreten und nach Konfigurationseinstellungen fragen.

Empfohlene Schritte für die Bereitstellung:

1. **Booten zu WinPE** – Bereiten Sie das System vor, ohne in Windows zu booten.
2. **Legen Sie die Volume-ID fest** – Ändern Sie es, bevor Sie das Bild anwenden, damit es erhalten bleibt.
3. **Das sysprepped Image bereitstellen** – Verwenden Sie DISM, um das Image anzuwenden auf C: .
4. **Setzen Sie den Computernamen offline** – Bearbeiten Sie die Registrierung im gemounteten Image.
5. **Kopiere ein Unattended.xml Datei** – Automatisieren Sie die OOBE-Konfiguration. Diese Datei kann vor der Bereitstellung dynamisch mit einem Skript geändert werden.
6. **Erstellen Sie ein Erststart-Skript** – Stellen Sie sicher, dass die endgültigen Konfigurationen mit nur einem Neustart vorgenommen werden.
7. **Neustart in Windows** – Windows finalisiert sich mit den angegebenen Konfigurationen.
8. **Remote Access-Lizenz zurücksetzen** – Führen Sie den folgenden Befehl aus:

Terminalfenster

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

Dies setzt die Lizenz zurück und wendet eine neue Lizenz an.

Bereitstellungsskript

Bitte finden Sie unten das zugehörige WinPE-Bereitstellungsskript.

Terminalfenster

```
<# 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
```

Lizenzaktivierung

Nach der Bereitstellung generiert die Aktivierung einer Lizenz eine neue Computer-ID für die virtuelle Maschine. Diese Computer-ID wird vom Lizenzportal erstellt, wenn eine Maschine eine Test- oder Lizenzaktivierung anfordert. Bei geklonten virtuellen Maschinen ist die Lizenzaktivierung obligatorisch. Verwenden Sie entweder einen Aktivierungsschlüssel oder einen Volumenlizenzschlüssel. **Offline-Setups sind nicht erlaubt** aufgrund von Sicherheitsbedenken. Für detaillierte Aktivierungsschritte siehe TSplus-Befehlsliste .

Schlussfolgerung

Dieser Leitfaden beschreibt wichtige Überlegungen zur Bereitstellung von geklonten virtuellen Maschinen mit TSplus Remote Access. Er bietet wesentliche Schritte zur korrekten Konfiguration und Lizenzierung des Systems und muss an Ihre Bedürfnisse und Anforderungen angepasst werden.

Server klonen mit sysprep

Anforderungen

Beim Arbeiten mit geklonten virtuellen Maschinen ist es wichtig, den Computernamen und die Datenträger-ID zu ändern, um eine eindeutige TSplus Remote Access-Installation sicherzustellen und Lizenzprobleme zu vermeiden.

Computername Überlegungen

Der Computername wird im Windows-Registrierungseditor innerhalb des Images selbst gespeichert. Wenn er vor der Anwendung des Images geändert wird, wird er beim Booten von Windows von Sysprep überschrieben. Sie können jedoch einen Namen in einem vordefinieren. Unattended.xml Antwortdatei. Siehe Microsoft-Dokumentation für weitere Details.

Um den Computernamen festzulegen, fügen Sie den folgenden Abschnitt ein. Microsoft-Windows-Shell-Setup :

```
    <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>
```

Volume-ID-Überlegungen

Die Volume-ID ist mit der Festplattenpartition verbunden, nicht mit dem Betriebssystem-Image. Sie kann vor der Anwendung des Images geändert werden und bleibt bestehen. Verwenden Sie volumeid.exe von Sysinternals, verfügbar unter Microsoft Sysinternals bevor Windows startet.

Bereitstellungsschritte

Beim Bereitstellen einer neuen virtuellen Maschine aus einem sysprepped Image wird Windows beim ersten Boot in die Out-Of-Box-Erfahrung (OOBE) eintreten und nach Konfigurationseinstellungen fragen.

Empfohlene Schritte für die Bereitstellung:

1. **Booten zu WinPE** – Bereiten Sie das System vor, ohne in Windows zu booten.
2. **Legen Sie die Volume-ID fest** – Ändern Sie es, bevor Sie das Bild anwenden, damit es erhalten bleibt.
3. **Das sysprepped Image bereitstellen** – Verwenden Sie DISM, um das Image anzuwenden auf C: .
4. **Setzen Sie den Computernamen offline** – Bearbeiten Sie die Registrierung im gemounteten Image.
5. **Kopiere ein Unattended.xml Datei** – Automatisieren Sie die OOBE-Konfiguration. Diese Datei kann vor der Bereitstellung dynamisch mit einem Skript geändert werden.
6. **Erstellen Sie ein Erststart-Skript** – Stellen Sie sicher, dass die endgültigen Konfigurationen mit nur einem Neustart vorgenommen werden.
7. **Neustart in Windows** – Windows finalisiert sich mit den angegebenen Konfigurationen.
8. **Remote Access-Lizenz zurücksetzen** – Führen Sie den folgenden Befehl aus:

Terminalfenster

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

Dies setzt die Lizenz zurück und wendet eine neue Lizenz an.

Bereitstellungsskript

Bitte finden Sie unten das zugehörige WinPE-Bereitstellungsskript.

Terminalfenster

```
<# 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
```

Lizenzaktivierung

Nach der Bereitstellung generiert die Aktivierung einer Lizenz eine neue Computer-ID für die virtuelle Maschine. Diese Computer-ID wird vom Lizenzportal erstellt, wenn eine Maschine eine Test- oder Lizenzaktivierung anfordert. Bei geklonten virtuellen Maschinen ist die Lizenzaktivierung obligatorisch. Verwenden Sie entweder einen Aktivierungsschlüssel oder einen Volumenlizenzschlüssel. **Offline-Setups sind nicht erlaubt** aufgrund von Sicherheitsbedenken. Für detaillierte Aktivierungsschritte siehe TSplus-Befehlsliste .

Schlussfolgerung

Dieser Leitfaden beschreibt wichtige Überlegungen zur Bereitstellung von geklonten virtuellen Maschinen mit TSplus Remote Access. Er bietet wesentliche Schritte zur korrekten Konfiguration und Lizenzierung des Systems und muss an Ihre Bedürfnisse und Anforderungen angepasst werden.

Befehlszeilen

Wir freuen uns, Ihnen ein umfassendes Set von Befehlszeilenwerkzeugen zur Verfügung zu stellen, die darauf ausgelegt sind, die Flexibilität und Effizienz unserer Software zu verbessern. Diese Werkzeuge ermöglichen es den Benutzern, verschiedene Funktionen zu skripten und zu automatisieren, um die Software an ihre spezifischen Bedürfnisse und Arbeitsabläufe anzupassen.

Entdecken Sie die Möglichkeiten und optimieren Sie Ihr Erlebnis mit unseren Befehlszeilenoptionen.

Sie müssen nur die folgenden Befehlszeilen als erweiterter Administrator ausführen. Zur Erinnerung, AdminTool.exe und TwoFactor.Admin.exe (2FA-Add-On) sollten sich hier befinden: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Sichern Sie Daten und Einstellungen: /backup

Syntax:

AdminTool.exe /backup [optionalPath] [parameters]

Beschreibung:

Befehl /backup wird verwendet, um TSplus-Daten und -Einstellungen zu sichern.

Standardmäßig wird das Backup im Verzeichnis "Archive" (C:\Backupparam) erstellt.

Parameter:

- optionalerPfad um in ein anderes Verzeichnis als das Standardverzeichnis zu sichern. Relative und absolute Pfade sind erlaubt.
- /silent wenn dieses Parameter erwähnt wird, erfolgt die Sicherung stillschweigend

Beispiele:

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

Für weitere Informationen besuchen Sie bitte TSplus - Backup-Einstellungen

---

Daten und Einstellungen wiederherstellen: / Wiederherstellen

Syntax:

AdminTool.exe /restore [backupPath] [parameters]

Beschreibung:

Befehl / Wiederherstellen wird verwendet, um TSplus-Daten und -Einstellungen wiederherzustellen.

Das angegebene Backup-Verzeichnis muss einen Daten- und einen Einstellungsordner enthalten, die durch den Befehl /backup erstellt wurden.

Parameter:

- SicherungsPfad der Pfad, wo sich der Sicherungsordner zum Wiederherstellen befindet.
- /silent Wenn dieser Parameter erwähnt wird, erfolgt die Wiederherstellung stillschweigend.

Beispiele:

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

Für weitere Informationen besuchen Sie bitte TSplus - Backup-Einstellungen

---

Webserver: /webstop , /webstart und / webrestart

Syntax:

AdminTool.exe /webstop

AdminTool.exe /webstart

AdminTool.exe /webrestart

Beschreibung:

Befehl /webstop wird verwendet, um den Webserver zu stoppen.

Befehl /webstart wird verwendet, um den Webserver zu starten.

Befehl /webrestart wird verwendet, um den Webserver neu zu starten.

Parameter:

None

Aktualisierung: /aktualisieren

Syntax:

AdminTool.exe /update [Optionen]

Beschreibung:

Befehl Aktualisierung wird verwendet, um TSplus Remote Access und potenziell Advanced Security zu aktualisieren.

Parameter:

- Optionen
  :
  - /zusätze Wenn diese Option verwendet wird, wird auch die Advanced Security aktualisiert, wenn eine neue Version verfügbar ist.

Beispiel:

AdminTool.exe /update /addons

Windows-Kompatibilitätsupdates anwenden: /updatekernel

Syntax:

svcac.exe /updatekernel [/silent]

svcac.exe sollte sich hier befinden: **C:\Program Files (x86)\TSplus**

Beschreibung:

Befehl /updatekernel wird verwendet, um Windows-Kompatibilitätsupdates anzuwenden.

Diese automatischen Updates stellen sicher, dass TSplus Remote Access mit neuen Windows-Updates kompatibel bleibt und die Notwendigkeit entfällt, eine neuere Version von TSplus Remote Access herunterzuladen und neu zu installieren.

Windows-Kompatibilitätsupdates können täglich erfolgen. TSplus Remote Access ermöglicht erzwungene Updates. Dies ist nützlich, wenn die Kompatibilität beschädigt zu sein scheint und Sie den neuesten TSplus Remote Access-Patch außerhalb des regulären Update-Zeitplans abrufen müssen.

Bitte beachten Sie, dass eine gültige Lizenz erforderlich ist, um Kompatibilitätsupdates abzurufen. Wenn Ihre Testlizenz abgelaufen ist oder Ihre Lizenz ungültig ist, wird ein Fehlermeldungsfenster angezeigt. Bitte kontaktieren Sie unser Support-Team mit einem Screenshot dieser Fehlermeldung, wenn das Problem unerwartet auftritt.

Parameter:

- /stumm Aktualisieren Sie stillschweigend, indem Sie diesen Parameter bereitstellen. Es wird kein Nachrichtenfeld angezeigt.

Installieren Sie den Universaldrucker: / InstallUniversalPrinter

Syntax:

universalprintermanagement.exe /InstallUniversalPrinter

universalprintermanagement.exe befindet sich hier: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Beschreibung:

Befehl /InstallUniversalPrinter wird verwendet, um den Universal Printer zu installieren.

Dies ist eine saubere Installation, da sie den vorhandenen Universal Printer entfernt, falls dieser zuvor installiert war.

Parameter:

None

Sie können diese Aktion auch manuell durchführen, bitte schauen Sie sich an Universaldrucker

---

Entfernen Sie UniversalPrinter: EntfernenSieUniversalDrucker

Syntax:

universalprintermanagement.exe /RemoveUniversalPrinter

universalprintermanagement.exe befindet sich hier: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Beschreibung:

Befehl EntfernenSieUniversalDrucker wird verwendet, um den Universal Printer zu deinstallieren.

Parameter:

None

Sie können diese Aktion auch manuell durchführen, bitte schauen Sie sich an Universaldrucker

---

Proxy-Server konfigurieren: /proxy /set

Syntax:

AdminTool.exe /proxy /set [Parameter]

Beschreibung:

Befehl /proxy /set wird verwendet, um einen Proxy-Server für den Internetzugang zu konfigurieren.

Parameter:

- /host der Zielhost kann ein vordefinierter Wert (“ie” oder “none”) oder ein benutzerdefinierter Wert (z.B.: 127.0.0.1 oder proxy.company.org) sein. Dieses Parameter ist obligatorisch
- /port die Portnummer, die verwendet wird, um eine Verbindung zum Proxy-Server herzustellen. Erforderlich, wenn der Hostname-Wert ein benutzerdefinierter Wert ist.
- /benutzername der Benutzername, um sich mit dem Proxy-Server zu verbinden. Diese Einstellung ist optional
- /Passwort Das Passwort des Benutzers muss angegeben werden, wenn ein Benutzername definiert wurde. Sein Wert kann jedoch leer sein.

Beispiele:

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

AdminTool.exe /proxy /set /host ie

Für weitere Informationen besuchen Sie bitte Wie konfiguriert man einen Proxy-Server für den Internetzugang?

Öffnen Sie das Webanmeldeformular: /webanmeldeinformationen

Syntax:

AdminTool.exe /webcredentials

Beschreibung:

Befehl /webanmeldeinformationen startet in einem einzigen Fenster die Web-Anmeldeinformationen-Oberfläche (wie Sie es in AdminTool > Web > Web-Anmeldeinformationen tun würden).

Parameter:

None

Webanmeldeinformationen erstellen: /webcredentials-hinzufügen

Syntax:

AdminTool.exe /webcredentials-add [webLogin] [webPassword] [windowsLogin]

[windowsPassword] [maximumConcurrentSessions]

Beschreibung:

Befehl /webcredentials-hinzufügen wird verwendet, um Webanmeldeinformationen zu erstellen (wie Sie es in AdminTool > Web > Webanmeldeinformationen tun würden).

Parameter:

- webLogin den Web-Login, den Sie erstellen möchten.
- webPasswort das zugehörige Web-Passwort. Es kann ein leeres Anmeldekennwort sein. Verwenden Sie dazu doppelte Anführungszeichen "" um ein leeres Passwort anzugeben.
- windowsLogin der Windows-Login des entsprechenden Benutzers.
- windowsPasswort das Windows-Passwort.
- maximale gleichzeitige Sitzungen (optional): die maximale Anzahl gleichzeitiger Sitzungen für diesen Benutzer.

Beispiel:

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

Für weitere Informationen besuchen Sie bitte Web-Anmeldeinformationen

---

Webanmeldeinformationen entfernen: /webcredentials-entfernen

Syntax:

AdminTool.exe /webcredentials-remove [webLogin]

Beschreibung:

Befehl /webcredentials-entfernen wird verwendet, um eine vorhandene Web-Anmeldeinformation zu entfernen (wie Sie es in AdminTool > Web > Web-Anmeldeinformationen tun würden).

Parameter:

- webLogin der Web-Login, den Sie entfernen möchten.

Beispiel:

AdminTool.exe /webcredentials-remove johndoe

Für weitere Informationen besuchen Sie bitte Web-Anmeldeinformationen

---

Sitzungsmanager öffnen: /sessionmanager

Syntax:

AdminTool.exe /sessionmanager

Beschreibung:

Befehl /sessionmanager startet in einem einzigen großen Fenster den Sitzungsmanager (wie Sie es in AdminTool > Startseite > Sitzungsmanager tun würden).

Parameter:

None

Offene Sitzungen überwachen: /farm-sessions-monitor

Syntax:

AdminTool.exe /farm-sessions-monitor

Beschreibung:

Befehl /farm-sessions-monitor startet in einem einzigen großen Fenster den Sitzungsmonitor des Farmmanagers (wie Sie es in AdminTool > Farm > Sitzungen überwachen würden).

Parameter:

None

Lastenverteilung-Manager öffnen: /farm-loadbalancing

Syntax:

AdminTool.exe /farm-loadbalancing

Beschreibung:

Befehl /farm-loadbalancing startet in einem einzigen großen Fenster den Lastenausgleichsmanager des Farmmanagers (wie Sie es in AdminTool > Farm > Lastenausgleich tun würden).

Parameter:

None

Systemaudit ausführen: /systemaudit

Syntax:

AdminTool.exe /systemaudit

Beschreibung:

Befehl /systemaudit führt eine Systemprüfung durch (wie Sie es manuell in AdminTool > Start >

Systemprüfung > Systemprüfung ausführen würden).

Parameter:

None

Lizenzaktivierung: /aktivieren

Syntax:

AdminTool.exe /aktivieren [licensePath]

Beschreibung:

Befehl aktivieren wird verwendet, um die Remote Access-Lizenz mit einer Lizenzdatei zu aktivieren.

Parameter:

- [Lizenzpfad] der Pfad der Lizenzdatei

Beispiel:

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

Lizenz zurücksetzen nach Klonen einer virtuellen Maschine: /Zurücksetzen

Syntax:

AdminTool.exe /license /reset

Beschreibung:

Beim Klonen eines Servers wird möglicherweise die Registerkarte „Lizenz“ im AdminTool nicht angezeigt oder zeigt die Fehlermeldung: „Ungültiger Hardware-Identifikator.“ Der Befehl / Zurücksetzen zielt darauf ab, die Lizenzierung auf dem Klonserver zu initialisieren, damit neue Lizenzen für die installierten TSplus-Produkte zugewiesen werden können.

Wichtige Hinweise:

1. Eine neue TSplus-Lizenz muss mit einem neuen Aktivierungsschlüssel aktiviert werden.
2. Verwenden Sie den Befehl /license /reset nicht auf einer nicht geklonten Maschine, da dies die Lizenzzuweisung dauerhaft verhindert. Bestätigen Sie immer den Status der Maschine, bevor Sie fortfahren.

Schritte zum Zurücksetzen der Lizenz auf einem geklonten Server:

1. Öffnen Sie eine Administrator-Sitzung auf dem geklonten Server.

2. Ändern Sie die HDD-Volumeseriennummer.

- Führen Sie die vol Befehl zur Anzeige der aktuellen Volume-Seriennummer (VSN). Das Ergebnis sollte ähnlich aussehen: 74F8-9C08 .

- Laden Sie das VolumeID-Dienstprogramm herunter und installieren Sie es, das verfügbar ist hier .

- Führen Sie den Befehl aus: volumeid C: 84F8-9C08 als Administrator den Laufwerks-VSN zu ändern. In diesem Beispiel haben wir den VSN der Festplatte C: geändert und ich habe nur ein Zeichen (das erste) des alten VSN geändert, um den neuen anzugeben.

- Hinweis: Dieser Schritt ist entscheidend, da bestimmte Windows Server-Versionen während des Klonens keine neue Volume-Seriennummer generieren, selbst wenn SysPrep verwendet wird.

3.
Benennen Sie den geklonten Server um und starten Sie ihn neu.

4.
Lizenzen im AdminTool zurücksetzen:

- Öffnen Sie eine Eingabeaufforderung mit Administratorrechten.
- Navigieren Sie zu dem Verzeichnis, das die AdminTool-executable enthält, indem Sie diesen Befehl verwenden: cd "C:\Program Files (x86)\TSplus\UserDesktop\files"
- Führen Sie den folgenden Befehl aus: AdminTool.exe /license /reset

5. Überprüfen Sie den Reset.

- Nach Ausführung des Befehls sollte die Registerkarte „Lizenz“ den folgenden Fehler anzeigen: Fehler beim Lesen der Lizenzdatei (unerwartetes Dateiformat).

6. Aktivieren Sie die neue Lizenz.

- Im Tab „Lizenz“ klicken Sie auf „Aktivieren Sie Ihre Lizenz“ und geben Sie den neuen Aktivierungsschlüssel ein, um die erforderlichen Lizenzen und Support zu aktivieren.

Beispiel:

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

---

Volumenlizenzaktivierung: /vr /aktivieren

Syntax:

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

Befehl vl /aktivieren wird verwendet, um eine Volumenlizenz zu aktivieren.

Parameter:

- Lizenzschlüssel Lizenzschlüssel zur Aktivierung, in diesem Format: AAAA-BBBB-CCCC-DDDD
- /benutzer : eine Zahl von 1 bis 50 oder „unbegrenzt“
- /ausgabe “Desktop”, “MobileWeb” oder “Enterprise”
- /supportjahre Jede Zahl von 0 bis 3.
- /Kommentare Gibt die Kommentare an, die dem Lizenz auf dem Lizenzportal angehängt werden sollen.

Beispiel:

AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “Dies ist ein Kommentar”

Für weitere Informationen besuchen Sie bitte Volumenlizenzdokumentation

---

Aktivieren und Deaktivieren der Volumenlizenz: /vr /aktivieren und /vr /deaktivieren

Syntax:

AdminTool.exe /vl /enable [licensekey]

AdminTool.exe /vl /disable [licensekey]

Beschreibung:

Befehl vl /aktivieren wird verwendet, um eine Volumenlizenz zu aktivieren.

Befehl vl /deaktivieren wird verwendet, um eine Volllizenz zu deaktivieren.

Parameter:

- Lizenzschlüssel Lizenzschlüssel zum Aktivieren/Deaktivieren, im folgenden Format: AAAA-BBBB-CCCC-DDDD

Beispiele:

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

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

Für weitere Informationen besuchen Sie bitte Wie man eine Lizenz vom Server aktiviert/ deaktiviert?

Volumenlizenzaktualisierung: /vl /aktualisieren

Syntax:

AdminTool.exe /vl /update [Lizenzschlüssel] [Parameter]

Beschreibung:

Befehl vl /update wird verwendet, um die Benutzer einer Volumenlizenz zu aktualisieren.

Parameter:

- Lizenzschlüssel Lizenzschlüssel zur Aktualisierung, in diesem Format: AAAA-BBBB-CCCC-DDDD
- /benutzer : eine Zahl von 1 bis 50 oder „unbegrenzt“

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Wie aktualisiere ich die Benutzer einer Volumenlizenz vom Server?

Verbleibende Lizenzguthaben für einen Volumenlizenzschlüssel anzeigen: /vl /credits-

lizenz

Syntax:

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

Beschreibung:

Befehl vl /credits-license wird verwendet, um die verbleibenden Lizenzguthaben, die mit einem Volumenlizenzschlüssel verbunden sind, anzuzeigen.

Parameter:

- Lizenzschlüssel Volumenlizenzschlüssel in diesem Format: AAAA-BBBB-CCCC-DDDD
- /anmelden geben Sie die Anmeldedaten des Partners an, der mit dem Volumenlizenzschlüssel verbunden ist
- /ausgabe bitte den optionalen Editionsparameter für Advanced Security und Server Monitoring Produkte angeben
- /silent : führt den Befehl stillschweigend aus

Die Ausgabe wird in der benutzerspezifischen Umgebungsvariable mit dem Namen gespeichert. VOLUMEN_LIZENZ_GUTHABEN Es kann erforderlich sein, den Wert von VOLUMEN_LIZENZ_GUTHABEN von einem anderen Prozess, unter Verwendung des Befehls echo %VOLUME_LICENSE_CREDITS% .

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Wie zeigt man die verbleibenden Lizenzguthaben für einen Volumenlizenzschlüssel an?

Verbleibende Supportguthaben für einen Volumenlizenzschlüssel anzeigen: /vl /credits-support

Syntax:

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

Beschreibung:

Befehl vl /credits-support wird verwendet, um die verbleibenden Supportguthaben, die mit einem Volumenlizenzschlüssel verbunden sind, anzuzeigen.

Parameter:

- Lizenzschlüssel Volumenlizenzschlüssel in diesem Format: AAAA-BBBB-CCCC-DDDD
- /anmelden geben Sie die Anmeldedaten des Partners an, der mit dem Volumenlizenzschlüssel verbunden ist
- /ausgabe bitte den optionalen Editionsparameter für Advanced Security und Server Monitoring Produkte angeben
- /silent : führt den Befehl stillschweigend aus

Die Ausgabe wird in der benutzerspezifischen Umgebungsvariable mit dem Namen gespeichert. VOLUMEN_LIZENZ_GUTHABEN Es kann erforderlich sein, den Wert von VOLUMEN_LIZENZ_GUTHABEN von einem anderen Prozess, unter Verwendung des Befehls echo %VOLUME_LICENSE_CREDITS% .

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Wie man die verbleibenden Supportguthaben für einen Volumenlizenzschlüssel anzeigt?

2FA - zurücksetzen: /resetuser

Syntax:

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

Beschreibung:

Befehl /resetuser wird verwendet, um 2FA-Benutzer zurückzusetzen, anstatt dies über die Benutzeroberfläche zu tun (dies kann hier in der Oberfläche durchgeführt werden: TwoFactor.Admin > Benutzer verwalten > Zurücksetzen)

Parameter:

- user1 user2 ... userN die Domainnamen der Benutzer, die Sie zurücksetzen möchten (durch einfaches Leerzeichen getrennt)

Beispiele:

TwoFactor.Admin.exe /resetuser johndoe jackrussell chuckbartowski

Für weitere Informationen besuchen Sie bitte Konfiguration für Benutzer zurücksetzen

---

2FA - Benutzer hinzufügen: /addusers

Syntax:

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

Beschreibung:

Befehl /addusers wird verwendet, um mehrere 2FA-Benutzer hinzuzufügen, anstatt dies über die Benutzeroberfläche, Benutzer für Benutzer, zu tun (dies kann hier in der Benutzeroberfläche erfolgen: TwoFactor.Admin > Benutzer verwalten > Benutzer hinzufügen)

Parameter:

- userInfos1 userInfos2 ... userInfosN
  die Benutzerinformationen der Benutzer, die Sie hinzufügen möchten. Diese Informationen bestehen aus den folgenden Feldern, die durch ein Semikolon getrennt sind.
  - domainName (obligatorisch): der Domainname des hinzuzufügenden Benutzers
  - empfangeneMethode (optional): die Methode zur Erhaltung von Bestätigungscodes. Muss

einer dieser Werte sein: SMS, App, E-Mail oder LassDenBenutzerWählen. App ist der Standardwert.
- Handy (optional): die Telefonnummer des Benutzers, die hinzugefügt werden soll
- E-Mail (optional): die E-Mail des Benutzers, die hinzugefügt werden soll

Beispiele:

TwoFactor.Admin.exe /addusers johndoe jackrussell;LassDenBenutzerWählen chuckbartowski;Telefon;+33101010101; abcd@efgh.com samanthacarter;E-Mail;;

Für weitere Informationen besuchen Sie bitte Benutzer und Gruppen hinzufügen

---

2FA - Gruppen hinzufügen: /addgroups

Syntax:

TwoFactor.Admin.exe /addgroups [Gruppe1] [Gruppe2] … [GruppeN]

Beschreibung:

Befehl /addgroups wird verwendet, um mehrere 2FA-Gruppen hinzuzufügen, anstatt dies über die Benutzeroberfläche, gruppenweise, zu tun (dies kann hier in der Benutzeroberfläche gemacht werden: TwoFactor.Admin > Benutzer verwalten > Gruppe hinzufügen)

Parameter:

- gruppe1 gruppe2 ... gruppeN die Namen der Gruppen, die Sie hinzufügen möchten.

Beispiele:

TwoFactor.Admin.exe /addgroups gruppe1 gruppe2 gruppe3

Für weitere Informationen besuchen Sie bitte Benutzer und Gruppen hinzufügen

---

2FA - Benutzer auflisten: /getusers

Syntax:

TwoFactor.Admin.exe /getusers

Beschreibung:

Befehl /getusers wird verwendet, um eine Liste aller Benutzer/Gruppen abzurufen, die in der 2FA-Verwaltungskonsole konfiguriert sind. Eine JSON-Darstellung dieser Liste von Benutzern/Gruppen wird zurückgegeben und kann beispielsweise in einem Powershell-Skript verwendet werden.

Diese Liste kann hier in der Benutzeroberfläche eingesehen werden: TwoFactor.Admin > Benutzer verwalten.

Parameter:

None

2FA - Gruppen hinzufügen: /löschenbenutzer

Syntax:

TwoFactor.Admin.exe /deleteuser [domainName] [userType]

Beschreibung:

Befehl /löschenbenutzer wird verwendet, um einen Benutzer aus der 2FA-Konfiguration zu entfernen (dies kann hier in der Benutzeroberfläche durchgeführt werden: TwoFactor.Admin > Benutzer verwalten > Entfernen)

Parameter:

- domainName der Name des Benutzers oder der Gruppe, die entfernt werden soll.
- Benutzertyp der Typ des zu löschenden Objekts. Der Wert muss "Benutzer" oder "Gruppe"

sein.

Beispiele:

TwoFactor.Admin.exe /deleteuser “Dies ist ein Gruppenname” Gruppe TwoFactor.Admin.exe / deleteuser Administrator Benutzer

Für weitere Informationen besuchen Sie bitte Benutzer und Gruppen entfernen

---

Anmeldeinformationen zum Windows-Anmeldeinformations-Manager hinzufügen oder aktualisieren: /windowscredential-hinzufügenoderaktualisieren

Syntax:

AdminTool.exe /windowscredential-addorupdate

oder

AdminTool.exe /windowscredential-addorupdate csvFilePath

Beschreibung:

Befehl /windowscredential-hinzufügenoderaktualisieren wird verwendet, um neue Windows-Anmeldeinformationen zum Windows-Anmeldeinformations-Manager hinzuzufügen oder vorhandene zu aktualisieren. Sie können Anmeldeinformationen einzeln angeben, indem Sie die Domain, den Benutzernamen und das Passwort angeben, oder mehrere Einträge aus einer CSV-Datei im Batch verarbeiten.

Dieser Befehl ist nützlich, um die externe Authentifizierung über SAML für das Webportal mit SSO zu konfigurieren.

Parameter:

- **Einzelanmeldemodus**

  - Domain (obligatorisch): der Domänenname des Benutzers, falls Teil eines Active Directory, oder der Maschinenname, wenn der Benutzer ein lokaler Benutzer ist
  - Benutzername (obligatorisch): der Windows-Benutzername
  - Passwort (obligatorisch): das Windows-Konto-Passwort

- **Bulk-Modus (CSV-Datei)**

  - csvDateipfad (obligatorisch): der Pfad zu einer CSV-Datei, die ein oder mehrere Anmeldeinformationen zum Hinzufügen oder Aktualisieren enthält

Beispiele

Für einen Active Directory-Benutzer:

AdminTool.exe /windowscredential-addorupdate COMPANY johndoe SecurePassword123

Für einen lokalen Benutzer:

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

Um Anmeldeinformationen aus einer CSV-Datei massenhaft hinzuzufügen oder zu aktualisieren:

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

---

Entfernen Sie Anmeldeinformationen aus dem Windows-Anmeldeinformations-Manager: /windowscredential-entfernen

Syntax:

AdminTool.exe /windowscredential-remove Benutzername

oder

AdminTool.exe /windowscredential-remove csvFilePath

Beschreibung:

Befehl /windowscredential-entfernen wird verwendet, um Windows-Anmeldeinformationen zu entfernen. Sie können eine einzelne Anmeldeinformation entfernen, indem Sie das Ziel angeben, oder mehrere Anmeldeinformationen im Bulk mithilfe einer CSV-Datei entfernen.

Parameter:

- **Einzelanmelde-Modus:**
- Ziel (obligatorisch): der Zielname für die Anmeldeinformationen, typischerweise ein Domänen- oder Servername
- **Bulk-Modus (CSV-Datei):**
  - csvDateipfad (obligatorisch): der Pfad zu einer CSV-Datei, die Benutzernamen enthält, die entfernt werden sollen. Die Datei muss vorhanden sein

Beispiele:

AdminTool.exe /windowscredential-remove UNTERNEHMEN

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

Wie kann die Webzugriffsseite vollständig über die Funktionen des Webportals hinaus angepasst werden?

Übersicht

Durch die Verwendung des Webportal Sie können die Webzugriffsseiten von Terminal Service Plus umfassend anpassen.

In einigen Fällen reicht dies jedoch nicht aus. In diesen Fällen können Sie die Webzugriffsseite vollständig anpassen, über die Möglichkeiten des Webportals hinaus, indem Sie die vom Webmaster Toolkit generierte Webzugriffsseite selbst ändern.

Warnung, diese Dokumentation ist nur für erfahrene Webentwickler gedacht.

Generierung der erforderlichen Einstellungen

Um die erforderlichen Einstellungen in Ihrer Webzugriffsseite einzuschließen, empfehlen wir Ihnen, zunächst Ihre Webzugriffsseite zu erstellen, indem Sie die Webportal .

Dateipfad

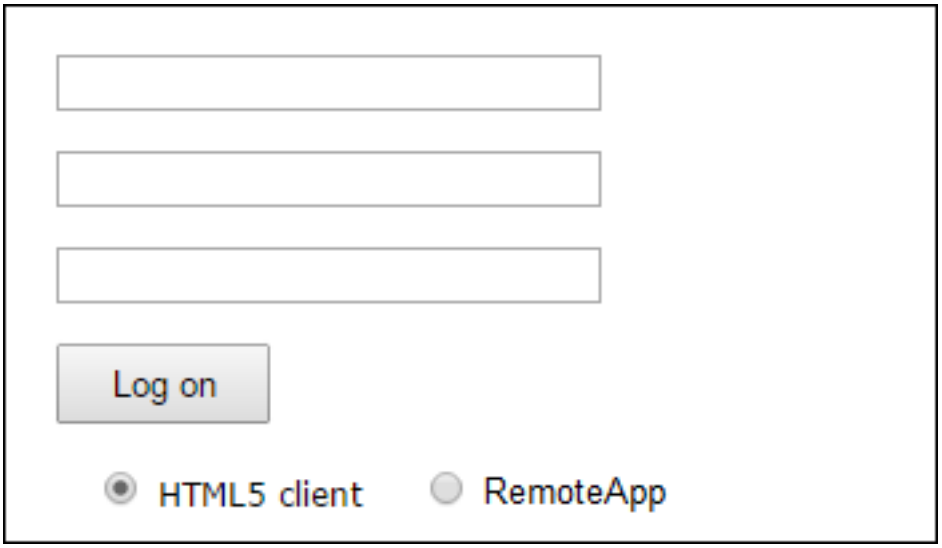
Die Webzugriffsseite wird im Ordner “C:\Program Files (x86)\TSplus\Clients\www” generiert. Wenn Sie beispielsweise “index” als Seitennamen wählen, wird es die Datei mit dem Namen “index.html” in diesem Ordner sein. Es handelt sich um eine Standard-HTML-Datei, sodass Sie Ihr gesamtes Wissen über die Programmiersprachen HTML, JavaScript und CSS nutzen können, um Ihre benutzerdefinierte Seite zu entwickeln.

Alle Dateiinclusions sind relativ zum Ordner „C:\Program Files (x86)\TSplus\Clients\www“ geschrieben. Zum Beispiel befindet sich die Haupt-CSS-Stildatei unter „C:\Program Files (x86)\TSplus\Clients\www\software\common.css“, sodass sie in die HTML-Webzugriffsseite durch die folgende Zeile eingebunden ist:

Minimale Webzugriffsseite

Starting from an HTML-Datei, die von den Webportal-Einstellungen generiert wurde, werden wir sie auf eine minimale Webzugriffsseite reduzieren. Wir empfehlen Ihnen, einen Texteditor wie Notepad oder Notepad++ zu verwenden. nicht verwenden Sie Word).

Nach unserer Arbeit wird es wie der Screenshot unten aussehen:



Zuerst müssen Sie alles, was zwischen den ist, behalten
und HTML-Tags:

- Meta-Tags, um Browser zu zwingen, ihren Cache zu leeren
- .js-Datei-Einschlüsse
- JavaScript-Einstellungenserklärungen

Dann können Sie den Inhalt zwischen den HTML-Tags 'body' und '/body' auf diese wenigen Zeilen reduzieren:

HTML5-Client RemoteApp

Aktualisieren Sie die Webseite in Ihrem Webbrowser, und Sie sollten die minimale Seite des obigen Screenshots erhalten.

Wir empfehlen Ihnen, den Cache Ihres Browsers zu leeren, nachdem Sie eine geänderte Datei gespeichert haben.

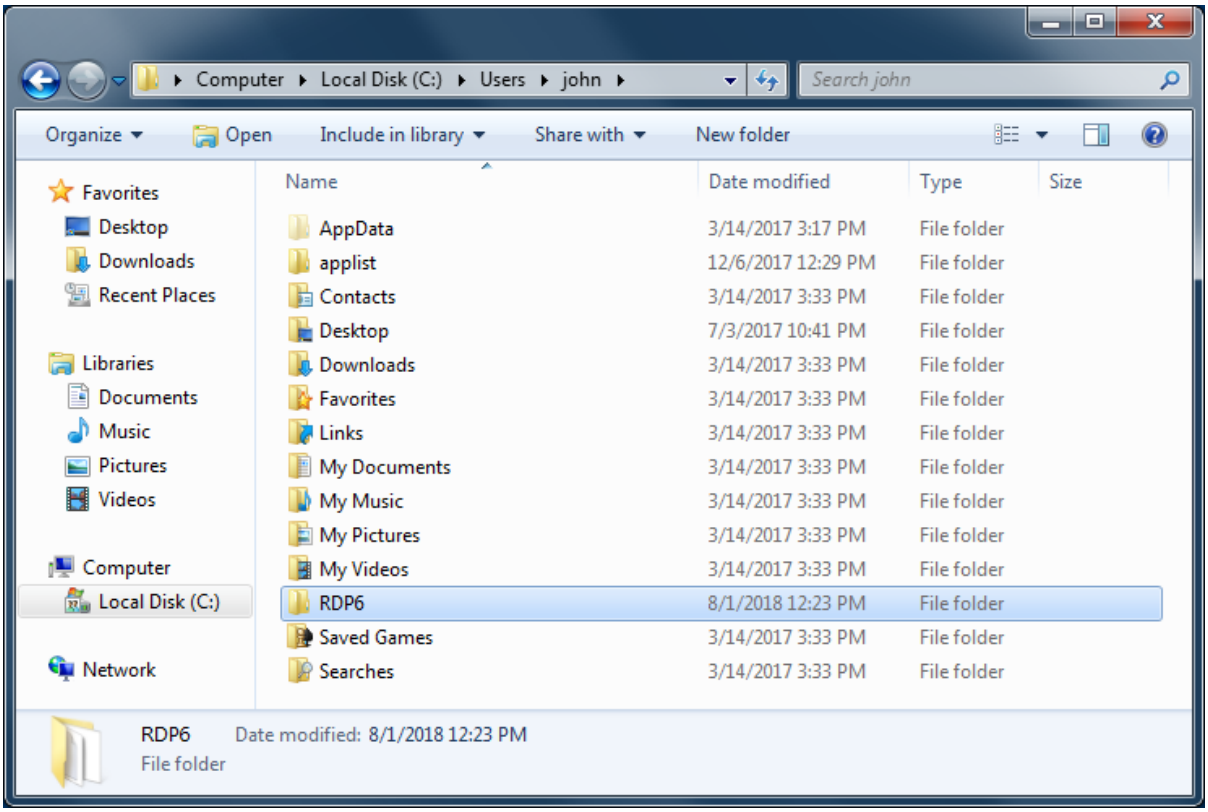
Schließlich liegt es jetzt an Ihnen!

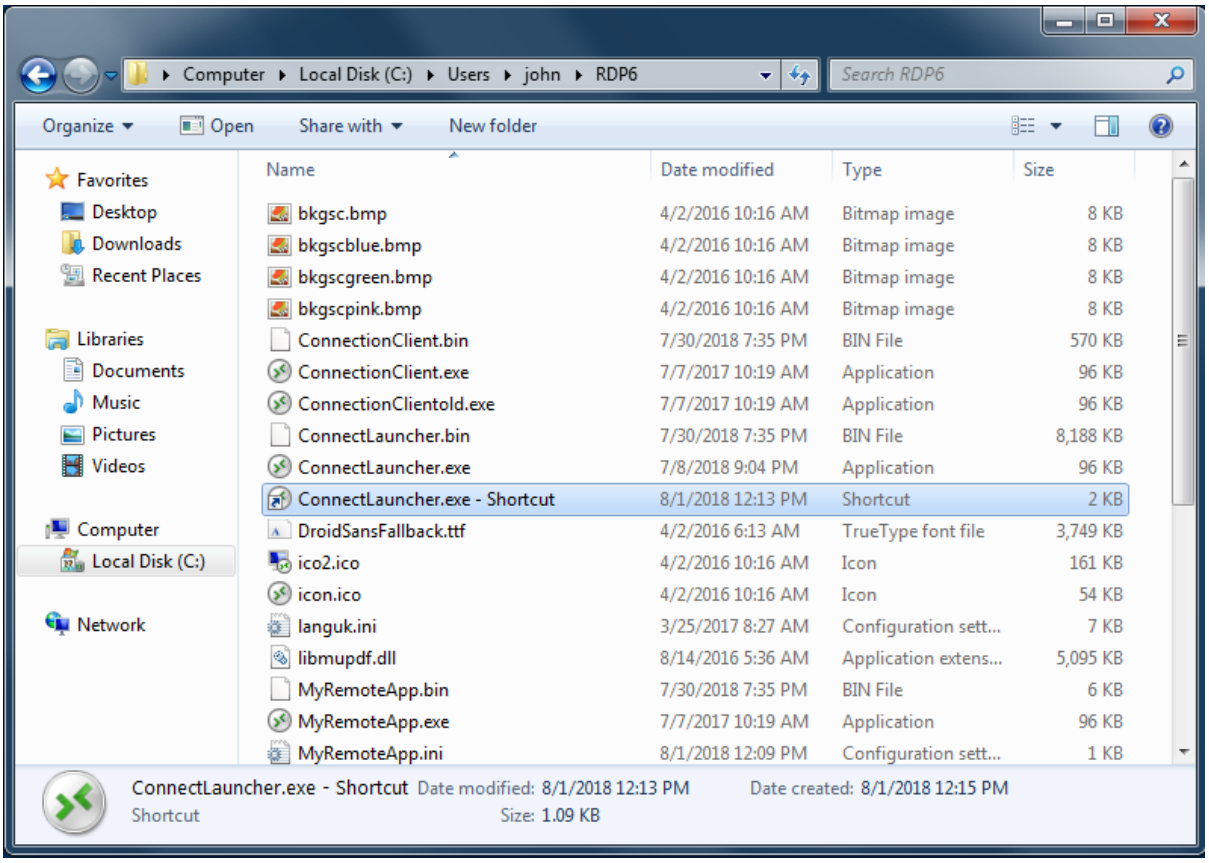
Solange Sie die Aufrufe von JavaScript-Funktionen bei bestimmten Ereignissen und die angegebenen Identifikatoren (id="…") beibehalten, wird Ihre vollständig angepasste Webzugriffsseite einwandfrei funktionieren!

Parameter eines generierten Clients bearbeiten oder löschen

Es gibt viele Gründe, warum Sie die Parameter Ihres Verbindungsclients ändern möchten: Ihre TSplus-Server-IP-Adresse hat sich geändert, Sie müssen die Druckerumleitung hinzufügen, die universellen Druckereinstellungen ändern oder so weiter…

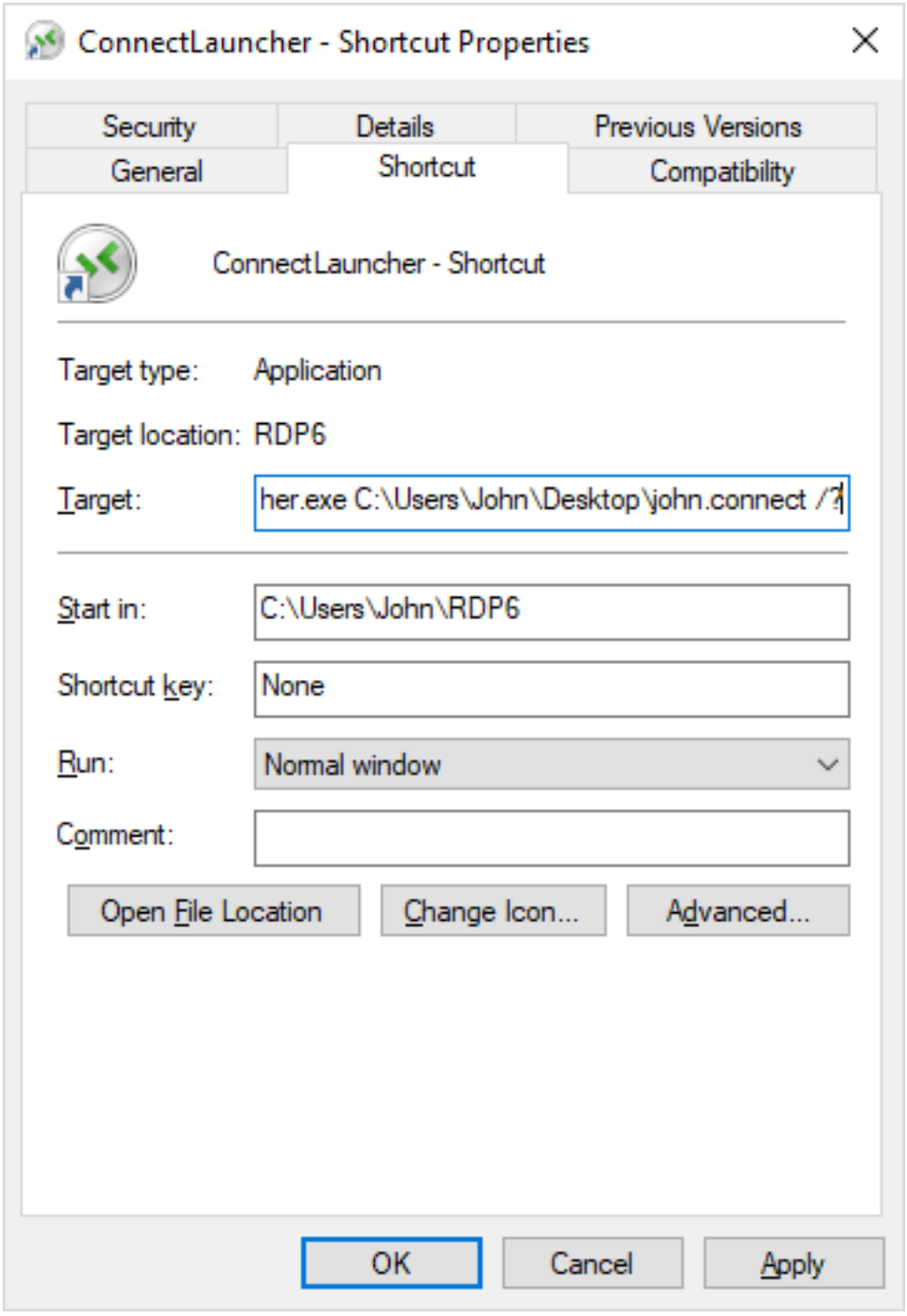
- Sie müssen zuerst eine Verknüpfung der Datei ConnectLauncher.exe erstellen, die sich im RDP6-Ordner des Benutzerprofils befindet.



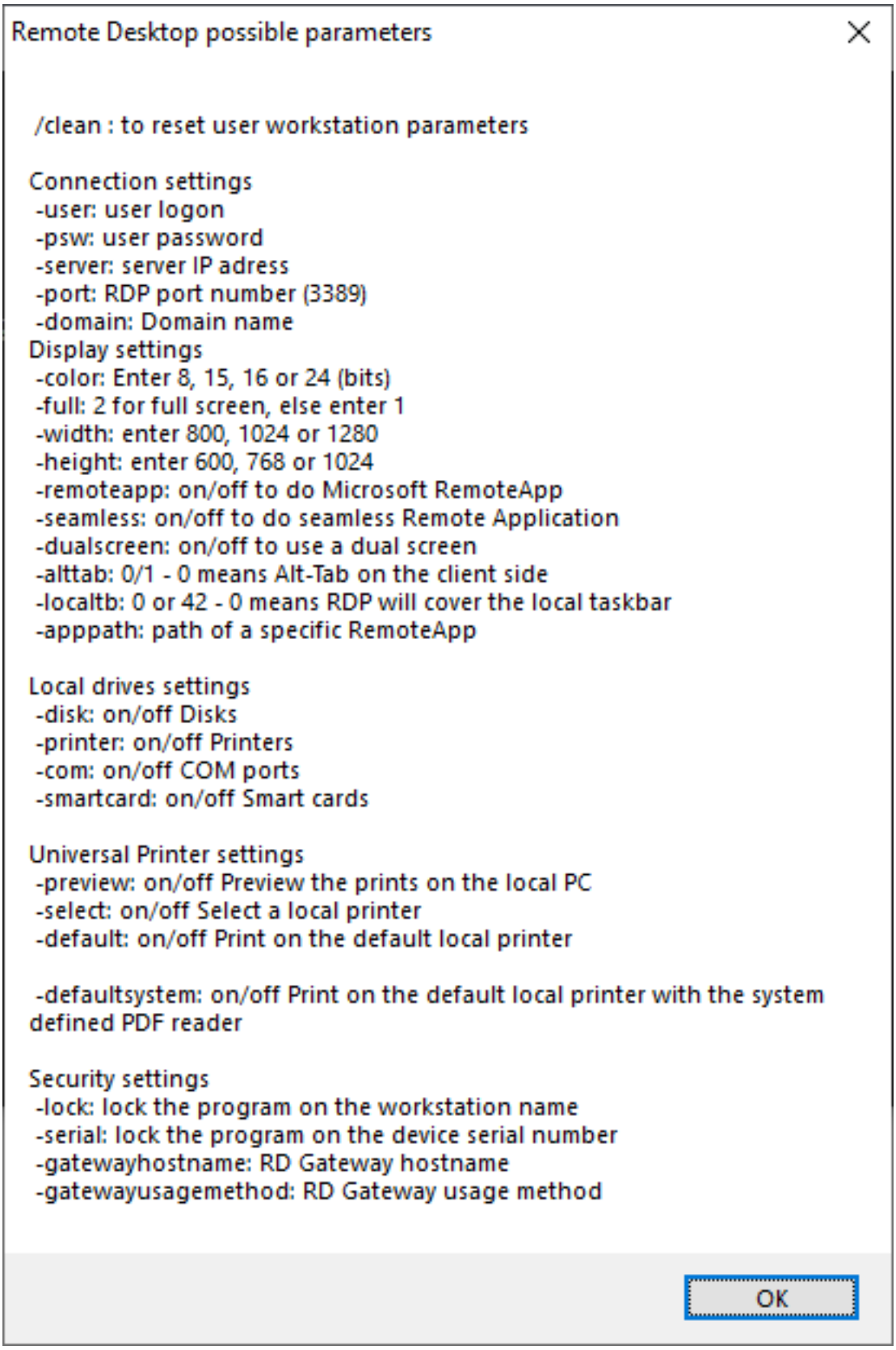


.

- Dann klicken Sie mit der rechten Maustaste darauf und wählen Sie Eigenschaften. Platzieren Sie Ihre Maus am Ende des Feldes „Ziel“ und geben Sie den Pfad des Clients gefolgt von „/?“ ein, zum Beispiel: „ C:\Users\John\Desktop\clientname.connect /?”:

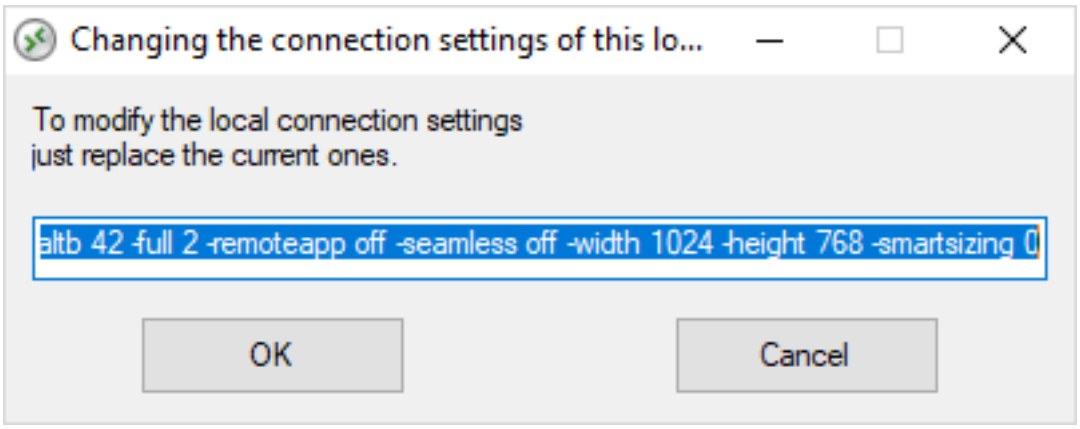


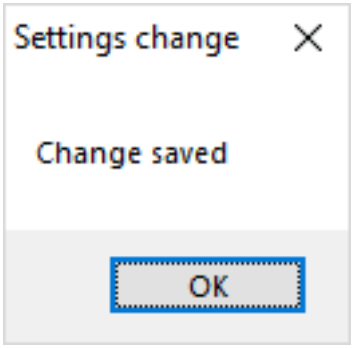
Jetzt klicken Sie auf OK und doppelklicken Sie auf die Verknüpfung. Eine Liste von Schaltern erscheint:



Klicken Sie auf OK, die Liste aller Parameter erscheint in einem kleinen Fenster.

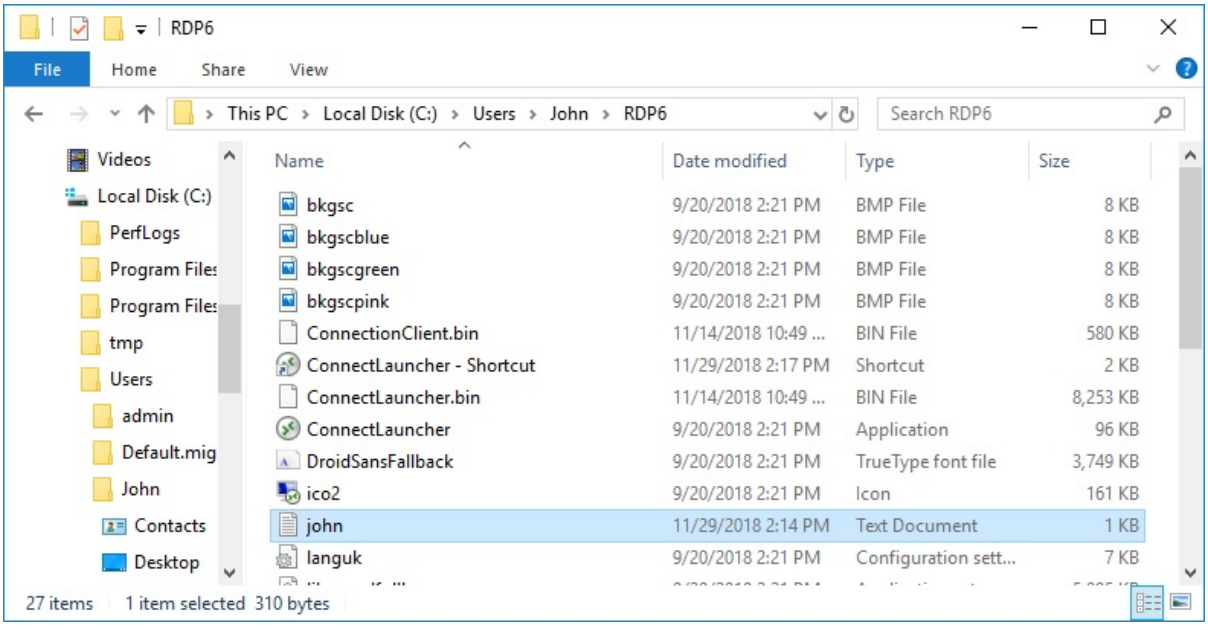
Sie können sie jetzt bearbeiten, um sie an Ihre Vorlieben anzupassen. Sie müssen sich abmelden und erneut anmelden, um die Änderungen anzuwenden.





Bereinigen Sie die Parameter eines generierten Clients

Nachdem Sie den Client mindestens einmal gestartet haben, können Sie die Parameter bereinigen, indem Sie die Datei client.txt im RDP6-Ordner löschen:



Aktivieren Sie die Windows-Integrationsauthentifizierung in einer Active Directory-Domäne

Dieser Leitfaden dient zur Konfiguration der Windows-Integrationsauthentifizierung (Kerberos/ NTLM) mit einem gruppenverwalteten Dienstkonto (gMSA) im Webportal.

Aufgrund der einzigartigen Natur des Netzwerks und der Architektur jedes Unternehmens können wir keinen Support für Probleme bieten, die aus der Befolgung dieser Dokumentation entstehen. Es erfüllt die technischen Anforderungen für das Webportal mit Windows-Integrationsauthentifizierung, aber die Implementierung liegt in Ihrer eigenen Verantwortung.

Domain-Konfiguration

Die Active Directory-Umgebung muss Kerberos- oder NTLM-Authentifizierung unterstützen.

Ein verwaltetes Dienstkonto (gMSA) einrichten

Installieren Sie den Webportal-Dienst und führen Sie ihn mit einem **Domänenverwaltetes Dienstkonto** anstatt eines Domänenadministrator-Kontos.

Voraussetzungen

- Active Directory-Schemaebene: **Windows Server 2012** oder später (erforderlich für gMSA)
- Mindestens ein Domänencontroller, der ausgeführt wird **Windows Server 2012** oder später
- KDS-Stamm-Schlüssel erstellt (einmalige Einrichtung)
- Mitgliedschaft in **Domänen-Administratoren** oder **Kontobetreiber** um das Konto zu erstellen

Erstellen Sie den KDS-Stamm-Schlüssel (falls noch nicht erstellt)

Führen Sie auf einem Domänencontroller in einer erhöhten PowerShell-Sitzung aus:

Terminalfenster

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

Dies macht den Stamm-Schlüssel sofort verfügbar.

Erstellen Sie das gMSA

Verwendung New-ADServiceAccount :

Terminalfenster

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

- Name gMSA-Kontoname
- DNS-Hostnamen FQDN für das Konto
- Berechtigte Personen zum Abrufen des verwalteten Passworts Computergruppe, die dieses

gMSA verwenden darf

Administrative Rechte gewähren (optional / nach Bedarf)

Standardmäßig hat ein gMSA keine besonderen Berechtigungen.

Um den Zugriff auf Domänenebene zu gewähren (optional):

Terminalfenster

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

Um lokale Administrator-/Anmelderechte zu gewähren (falls erforderlich):

Terminalfenster

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

Wichtig: das Nachgestellte $ ist erforderlich für gMSA-Konto-Referenzen in AD.

Neustart erforderlich

Ein Neustart ist erforderlich, bevor Sie fortfahren und das Dienstkonto installieren/verwenden.

Auch die Richtlinien aktualisieren.

Installieren Sie das gMSA auf Zielservern

Auf jedem Server ausführen, der das gMSA verwenden wird:

Terminalfenster

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

Testinstallation:

Terminalfenster

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

Dienste konfigurieren, um das gMSA zu verwenden

1. Gewähren **Als Dienst anmelden** zum Konto:

- Gruppenrichtlinien-Editor öffnen
- Gehe zu: Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment
- Öffnen Als Dienst anmelden

- Hinzufügen DOMAIN\WebPortalSvc$

2. Stellen Sie NTFS-Berechtigungen für Webportal-Dateien/-Ordner sicher:

   - Rechtsklick auf Anwendungsordner/executable > Eigenschaften > Sicherheit
   - Hinzufügen DOMAIN\WebPortalSvc$
   - Gewähren Sie mindestens **Lesen & Ausführen** oder **Vollständige Kontrolle** wenn erforderlich durch Ihre Bereitstellung

3. Dienstidentität konfigurieren:

   - Konto: DOMAIN\WebPortalSvc$
   - Passwort: **leave blank**

Konfigurieren Sie den Dienstprinzipalnamen (SPN)

Der Webdienst muss in Kerberos registriert werden.

Auf einem Domänencontroller ausführen:

Terminalfenster

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

Ersetzen Sie dies durch Ihren Server-FQDN und Ihr Konto.

Wenn der Hosting-Server des Webportals HTTP.sys verwendet, registrieren Sie SPN gegen das Maschinenkonto:

Terminalfenster

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

Netzwerk auf dem Client-Gerät konfigurieren

Um einen domänenverbundenen Client im richtigen Subnetz zu platzieren:

1. Identifizieren Sie die richtige Netzwerkoberfläche
2. Entfernen Sie die vorhandene statische IP (falls falsch)
3. Weisen Sie eine statische IP, Subnetzmaske und Standardgateway zu, die mit dem DNS/DC-Subnetz übereinstimmen.
4. DNS-Serveradressen festlegen

Wichtig: Weisen Sie statische IP-Adressen für den Domänencontroller und die Clients zu. Die Synchronisierung der Sicherheitsrichtlinie erfordert, dass sich die Maschinen in demselben Subnetz befinden.

Erforderliche Client-Verbindung zulassen

UDP/TCP 53 kann blockiert werden, was DNS-Abfragen verhindert.

Fehlerbehebungsschritte

Überprüfen Sie den Status des DNS-Servers

Auf dem Domänencontroller:

Terminalfenster

net start DNS

Überprüfen Sie, ob der DNS-Dienst ausgeführt wird.

DNS-Server-IP überprüfen

Auf dem Client:

Terminalfenster

```
ipconfig /all
```

Bestätigen Sie, dass die IP-Adresse des DNS-Servers mit der IP-Adresse des Domänencontrollers übereinstimmt.

Test der grundlegenden Konnektivität

Auf dem Client:

Terminalfenster

```
ping <DC_IP_Address>
```

Wenn der Ping fehlschlägt, beheben Sie die Netzwerk-/Firewall-Routing-Probleme.

Überprüfen Sie die Firewall-Regeln

Stellen Sie sicher, dass eingehender/ausgehender UDP/TCP 53 auf Client und Server erlaubt ist.

Test mit nslookup

Terminalfenster

nslookup domain.com <DC_IP_Address>

Wenn dies funktioniert, könnte der Standard-DNS-Server falsch konfiguriert oder nicht erreichbar sein.

Ereignisanzeige überprüfen

Überprüfen Sie auf dem Domänencontroller DNS-bezogene Fehler.

Mozilla Firefox für Windows integrierte Authentifizierung konfigurieren

Firefox verwendet standardmäßig kein WIA.

Schritt 1: vertrauenswürdige aushandeln URIs

1. Firefox öffnen

2. Gehe zu about:config
3. Warnung akzeptieren
4. Set
   network.negotiate-auth.trusted-uris
   zu Ihren Domains, zum Beispiel:
   - intranet.domain.com, domain.com

Schritt 2: vertrauenswürdige NTLM-URIs

Set netzwerk.automatische-ntlm-auth.vertraute-uris zur gleichen Domainliste.

Schritt 3: Kerberos-Delegierungs-URIs (falls erforderlich)

Set network.negotiate-auth.delegation-uris , zum Beispiel:

- domain.com

Schritt 4: Browser neu starten

Firefox neu starten, um die Änderungen anzuwenden.

Google Chrome für die integrierte Windows-Authentifizierung konfigurieren

Chrome verwendet die Windows/Systemauthentifizierungseinstellungen.

Über Gruppenrichtlinien (empfohlen)

1. Laden Sie Chrome ADMX-Vorlagen herunter:
   - https://chromeenterprise.google/policies/

2. Kopieren
   chrome.admx
   und
   chrome.adml
   zu:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\de-DE

3. Öffnen gpedit.msc
4. Gehe zu:

- Computer-Konfiguration > Administrative Vorlagen > Google > Google Chrome

5. Aktivieren Sie die integrierte Authentifizierung für Intranetsites und konfigurieren Sie vertrauenswürdige Sites:
   - intranet.domain.com, domain.com

6. Richtlinie anwenden:

Terminalfenster

```
gpupdate /force
```

Andere Methoden

Andere Methoden (Chrome-Befehlszeilenoptionen und -flags) waren in diesem Kontext nicht erfolgreich.

Microsoft Edge für die integrierte Windows-Authentifizierung konfigurieren

Edge verwendet Microsoft Edge-Richtlinien und Windows-Sicherheitszonen-Einstellungen.

Automatische Anmeldung in der Intranet-Zone aktivieren

1. Internetoptionen öffnen
2. Sicherheit Tab > Lokales Intranet > Benutzerdefinierte Stufe
3. Unter
   Benutzerauthentifizierung
   , setzen:
   - Automatische Anmeldung nur im Intranet-Bereich

Edge-Richtlinien über GPO konfigurieren

Schritt 1: Edge ADMX-Vorlagen installieren

1. Download:
   - https://www.microsoft.com/de-de/edge/business/download

2. Kopieren
   msedge.admx
   und
   msedge.adml
   zu:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\de-DE

Schritt 2: Richtlinieneinstellungen bearbeiten

1. Öffnen gpedit.msc
2. Gehe zu:
   - Computer Configuration > Administrative Templates > Microsoft Edge

3. Aktivieren:
   - Konfigurieren Sie die Liste der Server, an die Microsoft Edge Anmeldeinformationen delegieren kann.

4. Vertrauenswürdige Server konfigurieren:
   - intranet.domain.com, domain.com

Schritt 3: Richtlinien anwenden

Terminalfenster

gpupdate /force

Andere Methoden

Andere Methoden (Edge-Befehlszeilenoptionen und -flags) waren in diesem Kontext nicht erfolgreich.

Fehlerbehebung bei integrierter Authentifizierung

Überprüfen Sie Kerberos-Tickets

Auf Windows-Client:

Terminalfenster

klist

Sie sollten ein Ticket für sehen HTTP/webserver.domain.com .

Gespeicherte Anmeldeinformationen/Tickets löschen

Terminalfenster

klist purge

SPN-Registrierung überprüfen

Auf dem Domänencontroller:

Terminalfenster

```
setspn -L serviceaccount
```

Sicherstellen HTTP/webserver.domain.com ist aufgeführt.

Debug Kerberos in Firefox

Starten Sie Firefox mit Protokollierung:

Terminalfenster

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

Bewertung firefox.log bei Authentifizierungsfehlern.

Überprüfen Sie die Chrome-Richtlinien

In Chrome, öffnen Sie:

chrome://policy

Sicherstellen AuthServerWhitelist und AuthNegotiateDelegateWhitelist werden angewendet.

Edge-Richtlinien überprüfen

In Edge, öffnen Sie:

edge://policy

Sicherstellen AuthServerWhitelist und AuthNegotiateDelegateWhitelist werden angewendet.

Ende der Lebensdauer Version 1-12

Remote Access v12 (und alle älteren Versionen) wird auf allen Windows-Computern nicht mehr funktionieren.
Serviceunterbrechungen beginnen im Januar 2026 und werden schrittweise bis zur vollständigen Abschaltung im April verlängert.

Aktualisierung auf eine LTS-Version oder die neueste Version erfordert ein **aktive Support-Abonnement** für Ihre Lizenz. Wenn dies nicht der Fall ist, laden wir Sie ein, ein Support-Abonnement über Ihr Lizenzportal zu abonnieren und Ihre Lizenz über Ihr Admintool mit Ihrer .LIC-Datei zu aktualisieren, um von dem Update zu profitieren.

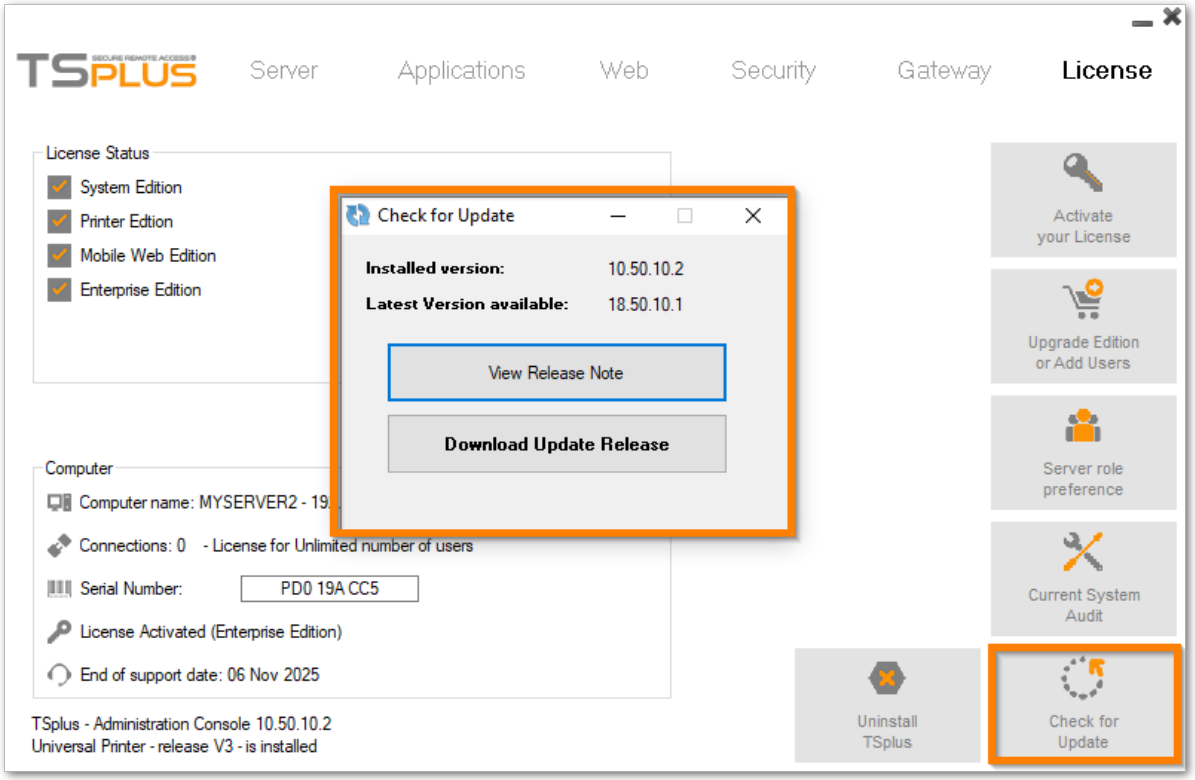
Wenn Sie ein Support-Abonnement nicht hinzufügen können oder eine Fehlermeldung erhalten, kontaktieren Sie uns über unsere Kontaktieren Sie den Support , bereitstellend:

- Ihre Lizenznummer im Format PXX XXX XXX (Sichtbar im Lizenz-Tab des Admintools)
- Ihre Lizenzkaufrechnung
- Ihre Support-Abonnementrechnung

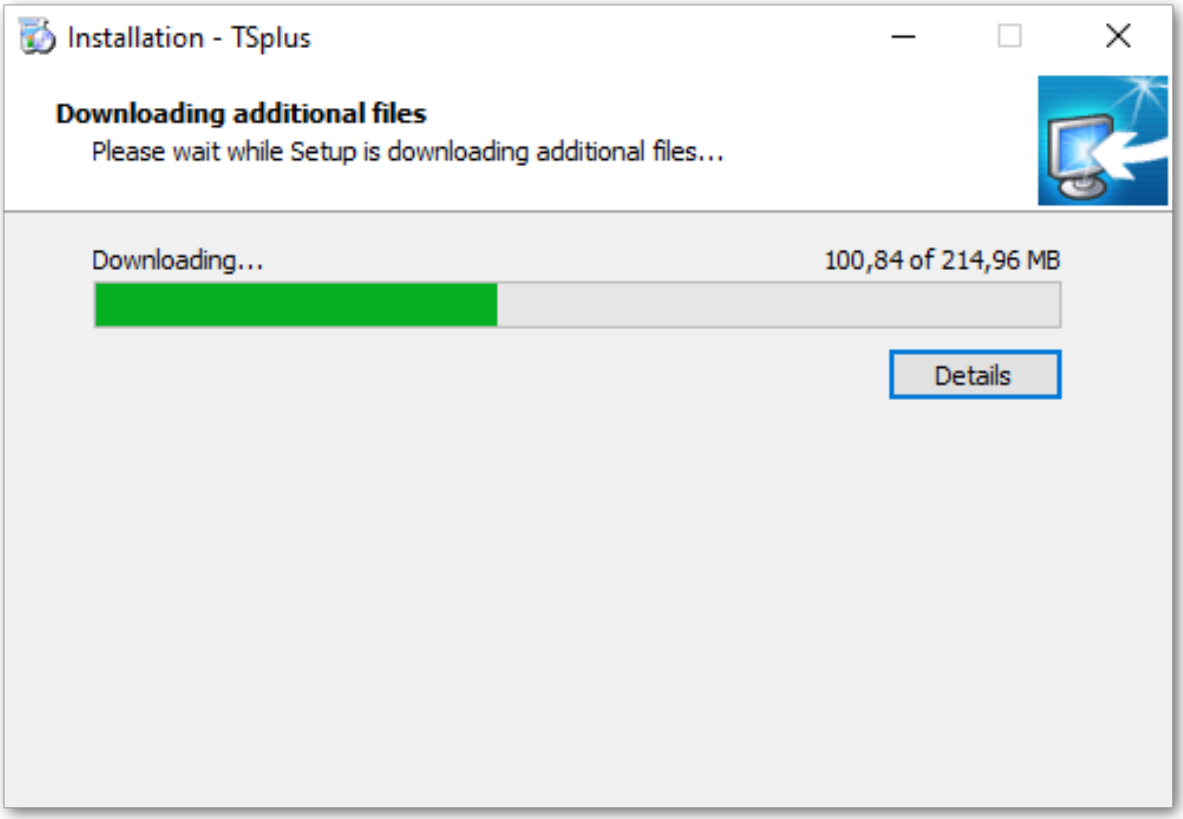
Aktualisierung Ihrer Version v10

Wenn Sie eine LTS anstelle der neuesten Version installieren möchten, gehen Sie zur Seite LTS)

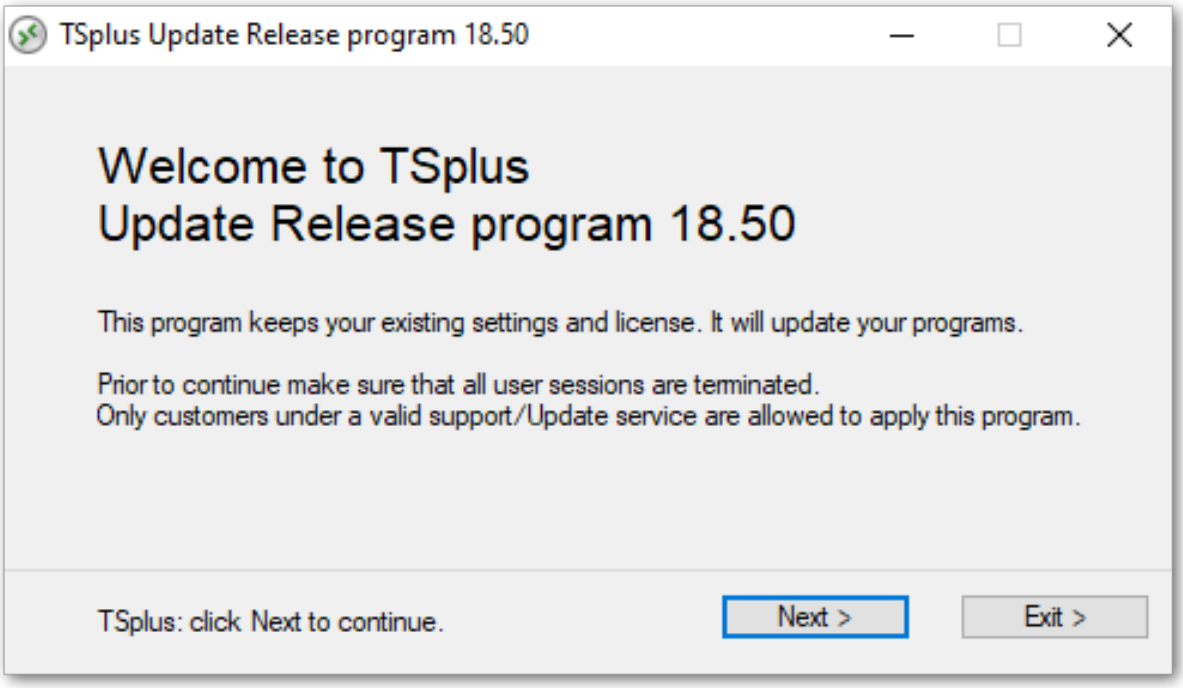
Von Ihrer Online-Version 10 klicken Sie auf das folgende Feld, um die herunterzuladen.
UpdateRelease.exe
Sie können auch die herunterladen UpdateRelease.exe um das Aktualisierungsverfahren zu starten.



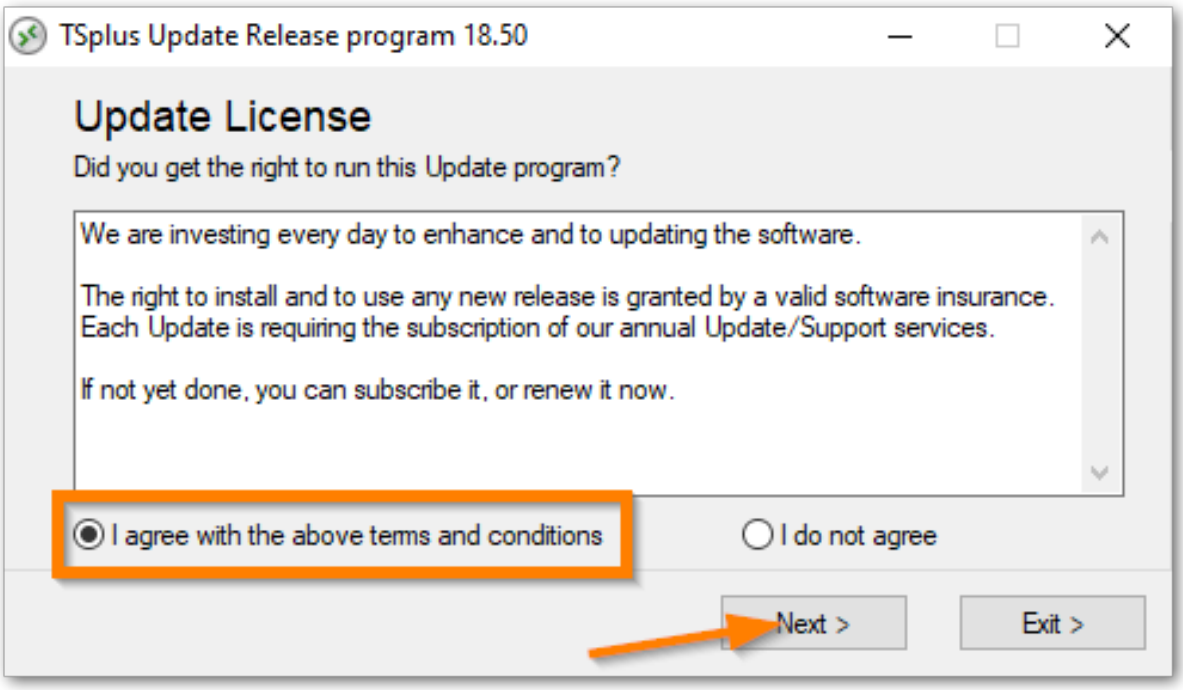
Laden Sie die updaterelease.exe herunter und führen Sie die ausführbare Datei aus.



Das Update-Programm wird angezeigt.



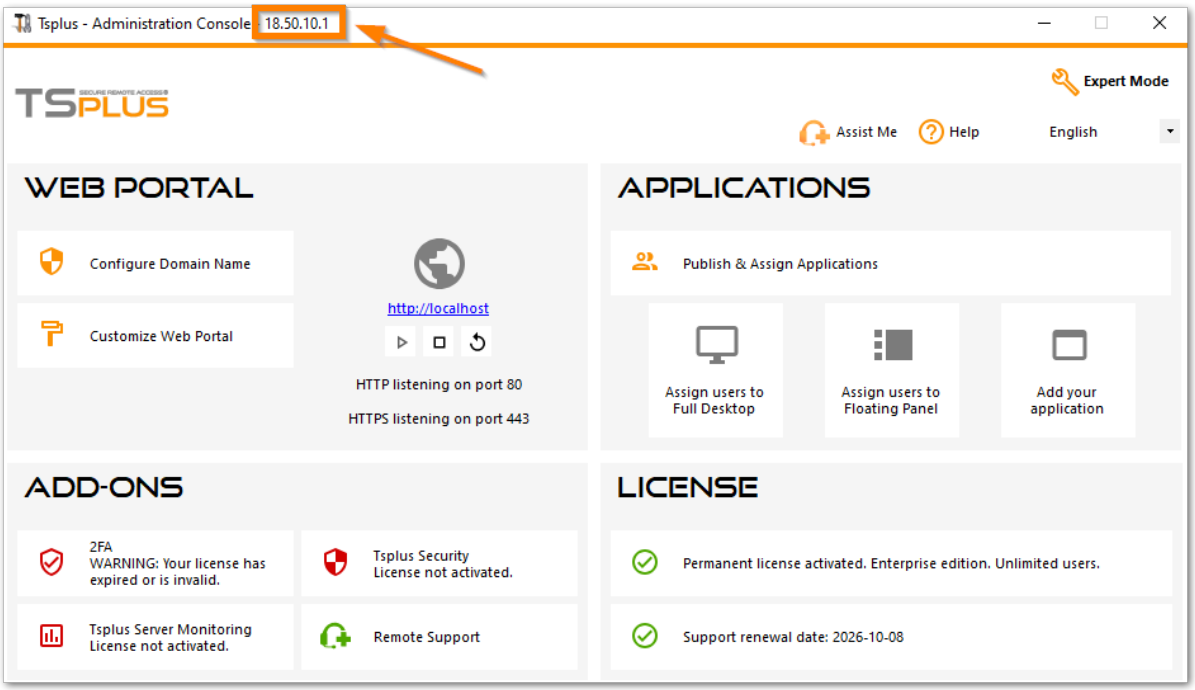
Akzeptieren Sie die Bedingungen und klicken Sie
NÄCHSTE



Befolgen Sie alle Schritte und starten Sie Ihren Server am Ende der Migration neu.

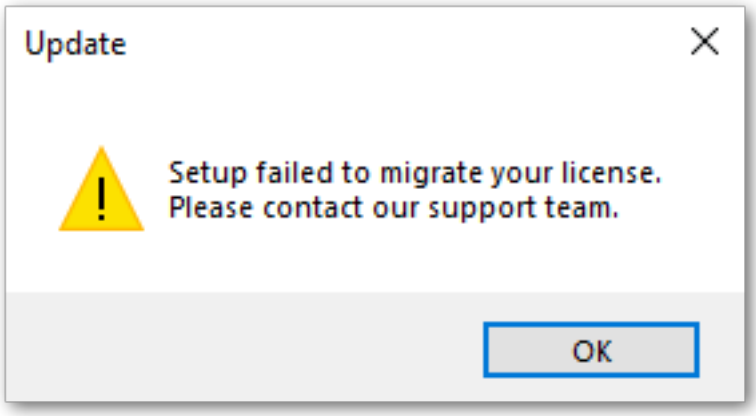
- Wenn Sie fertig sind, **Starten Sie Ihren Server** um das Update abzuschließen.

Starten Sie das AdminTool. Herzlichen Glückwunsch, Sie sind jetzt auf Version 19.



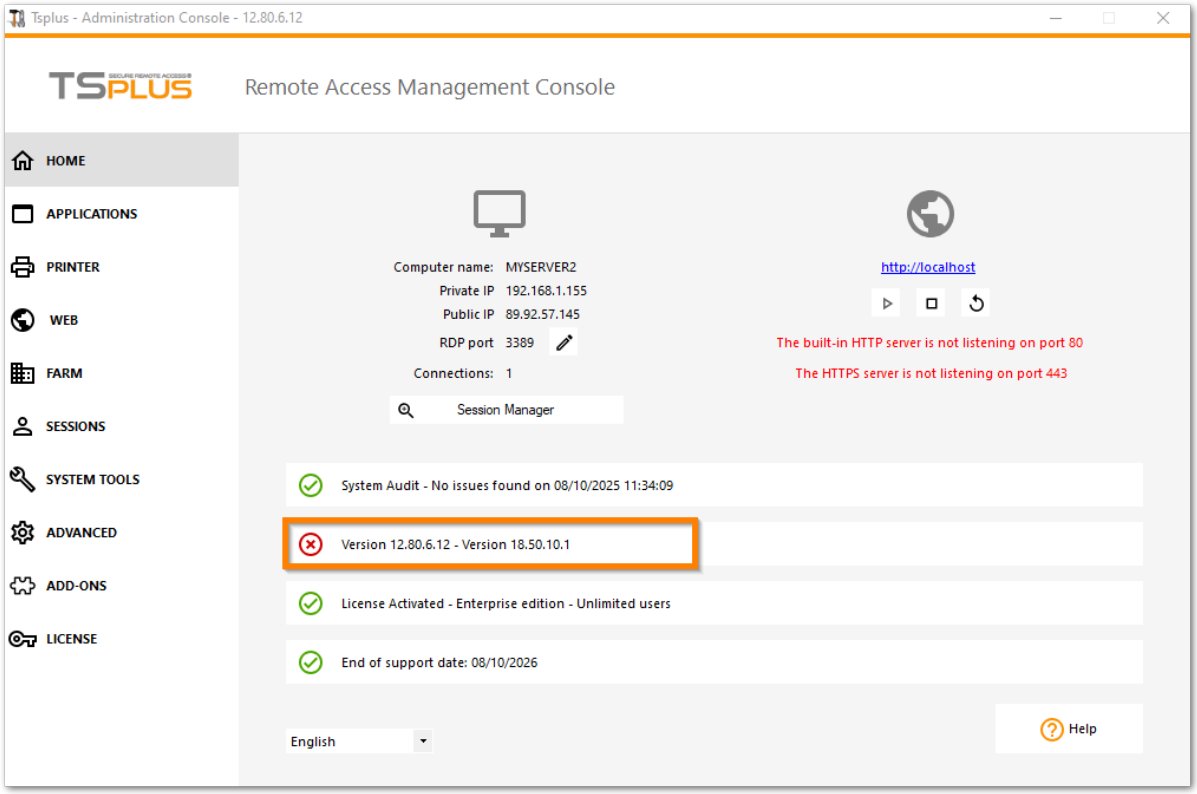
Fehlermeldung v10

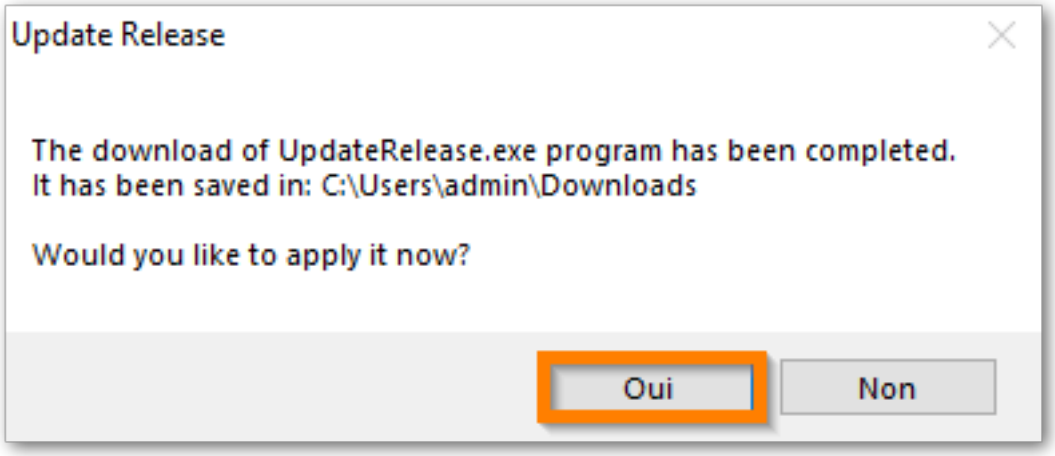
Wenn Sie diese Fehlermeldung erhalten,
Kontaktieren Sie den Support
um Remote Access zu deinstallieren. Bitte geben Sie die Lizenznummer im Format PXX XXX XXX an und auch den Nachweis der Rechnung für den Supportkauf.

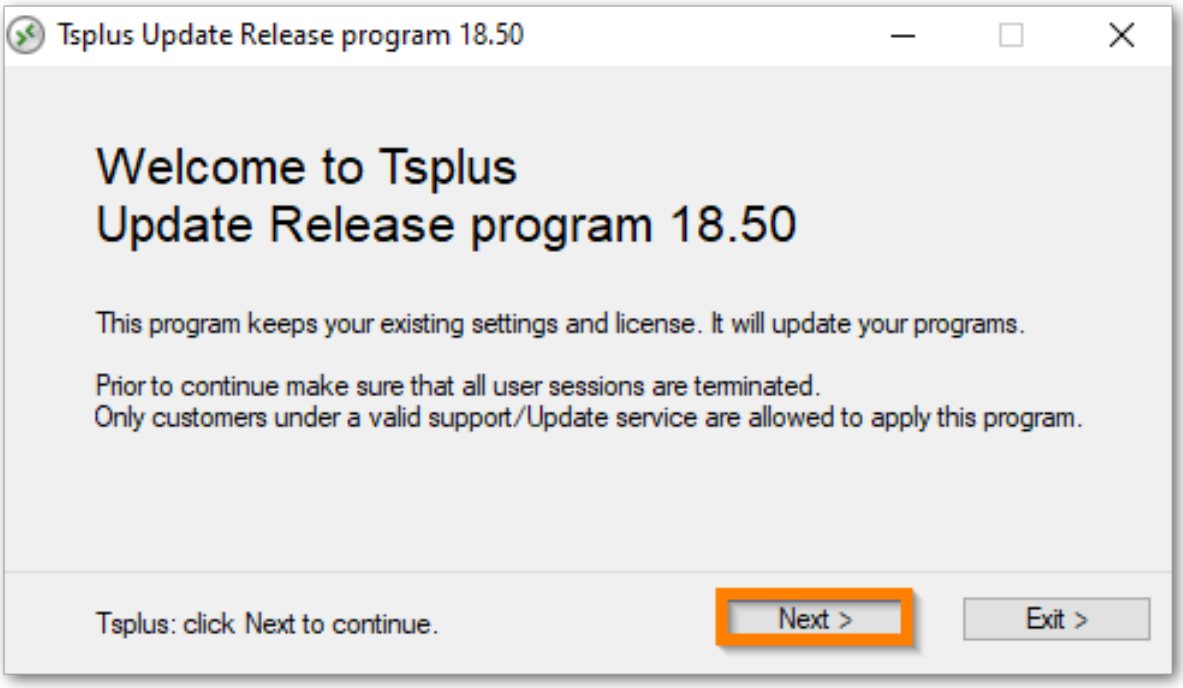


Aktualisierung Ihrer Version v12

Laden Sie die folgende Datei von Ihrer Online-Version 12 herunter. **UpdateRelease.exe**
Sie können auch die herunterladen UpdateRelease.exe um das Aktualisierungsverfahren zu starten.

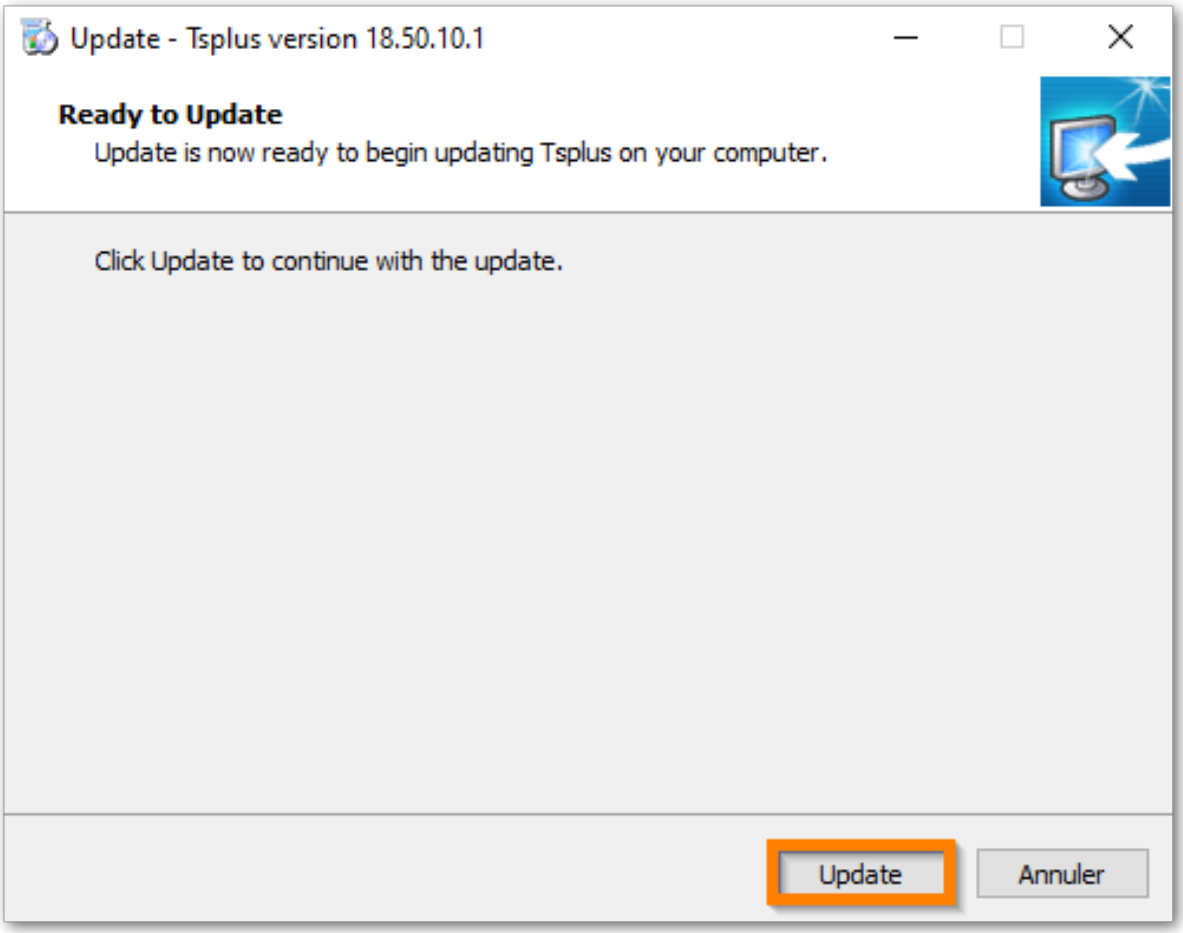

Tsplus - Administration Console - 12.80.6.12
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Computer name: MYSERVER2
Private IP 192.168.1.155
Public IP 89.92.57.145
RDP port 3389
Connections: 1
Session Manager
http://localhost
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

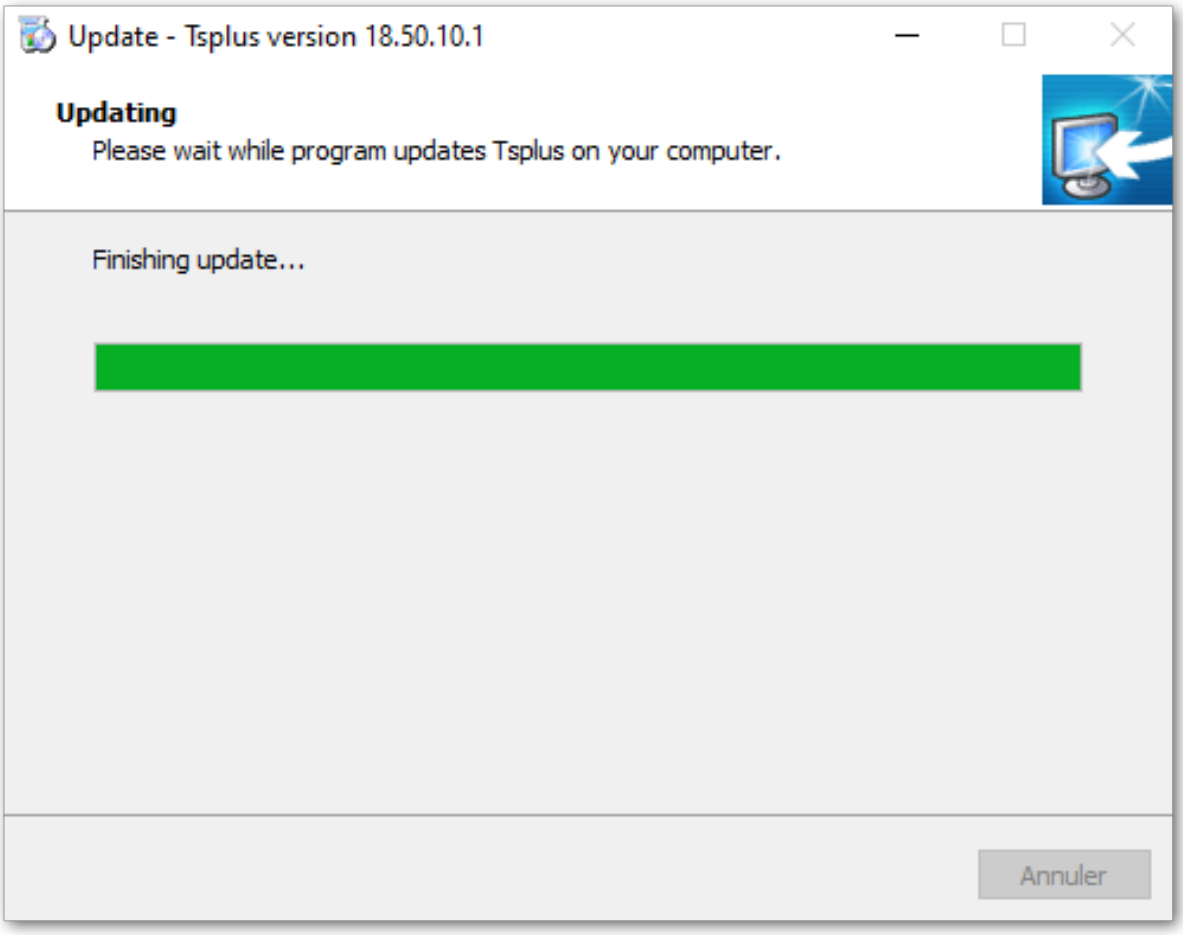

Update Release
The download of UpdateRelease.exe program has been completed.
It has been saved in: C:\Users\admin\Downloads
Would you like to apply it now?
Oui
Non



- Akzeptieren Sie die Bedingungen und klicken Sie auf WEITER

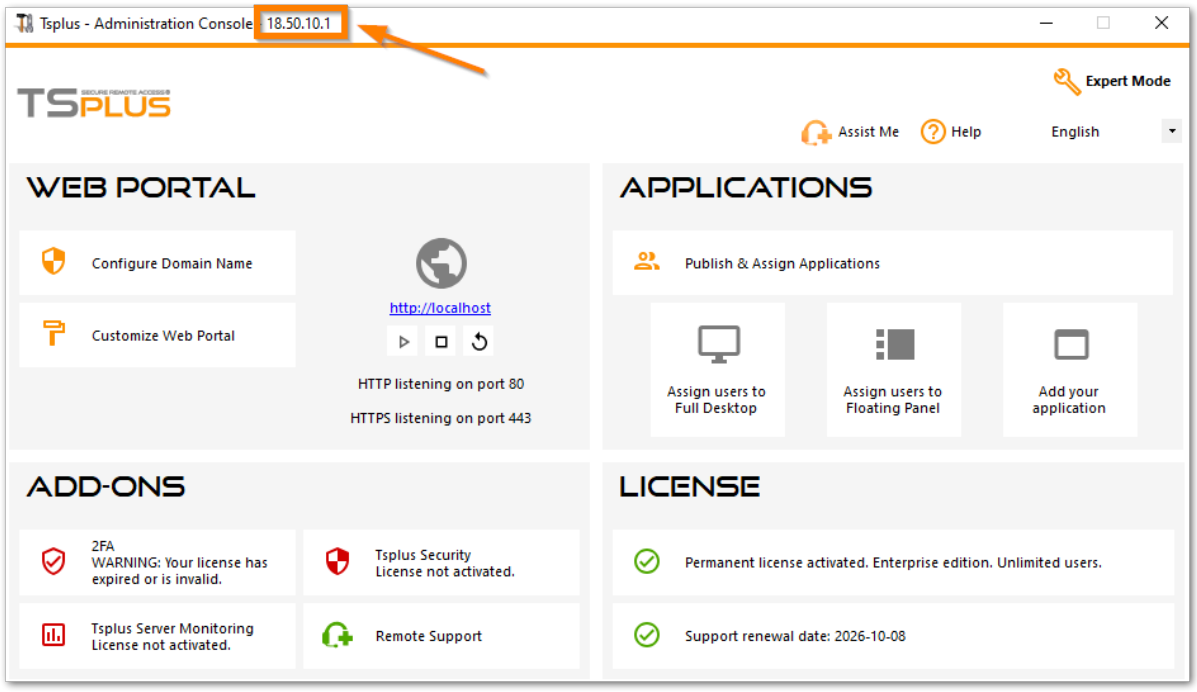
Sobald heruntergeladen, klicken Sie
Aktualisierung
um den Prozess zu starten.





- Wenn Sie fertig sind, **Starten Sie Ihren Server** um das Update abzuschließen.

Starten Sie das AdminTool. Herzlichen Glückwunsch, Sie sind jetzt auf Version 19.



Fehlermeldung v12

Wenn Sie diese Fehlermeldung erhalten, Kontaktieren Sie den Support um Remote Access zu deinstallieren.
Bitte geben Sie die Lizenznummer im Format PXX XXX XXX sowie einen Nachweis der Supportkaufrechnung an.

HTTPS-Protokoll erzwingen

Standardfall

Ab der Version 9.20 von Terminal Service Plus können Sie jede Webanfrage, die HTTP verwendet, auf das sichere Protokoll HTTPS umleiten.

Um diese Funktion auf einem Server zu aktivieren, bearbeiten Sie (oder erstellen Sie) die Datei „C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin“ und fügen Sie die folgende Zeile hinzu:

disable_http_only=true

Speichern Sie die Datei und starten Sie die Webserver von Terminal Service Plus neu (AdminTool > Web > Webserver neu starten oder Konfiguration durch Zugriff erneut lesen) http://127.0.0.1/w0j3?settings.bin).

Sobald diese Funktion aktiviert ist, können Sie versuchen, die unsichere Webseite unter folgender Adresse aufzurufen:

http://your-server

und es wird Ihre Anfrage automatisch zur sicheren Webportal-Seite umleiten:

https://your-server

Sonderfall: Benutzerdefinierte Web-Ports

Wenn Sie einen bestimmten Port verwenden, um HTTPS bereitzustellen, bearbeiten Sie die Datei „C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin“ und verwenden Sie die folgende Zeile anstelle der oben beschriebenen Zeile:

disable_http_only=“domain.com:4431”

wo domain.com Ihr eigener Server-Hostname ist und 4431 Ihr benutzerdefinierter HTTPS-Port ist.

Speichern Sie die Datei und starten Sie die Webserver von Terminal Service Plus neu (AdminTool > Web > Webserver neu starten).

Sobald diese Funktion aktiviert ist, können Sie versuchen, die unsichere Webseite unter folgender Adresse aufzurufen:

http://domain.com

und es wird Ihre Anfrage automatisch zur sicheren Webportal-Seite umleiten:

https://domain.com:4431

Kommentar: Auch wenn dies nicht sicher ist, aber Sie möchten SSL/HTTPS am HTTP-Port deaktivieren, dann bearbeiten Sie die settings.bin-Datei und fügen Sie hinzu: disable_ssl_on_http=true, speichern Sie und starten Sie die Server neu.

HTTP auf HTTPS deaktivieren

Standardmäßig ist der Zugriff erlaubt https://my-domain.com , https://my-domain.com:80 , http://my-domain.com:443 Es ermöglicht also http auf Port 443 oder erlaubt https auf Port 80, es hat keinen Einfluss auf die Sicherheit und erleichtert das Zurückfallen auf eine degradierte xhr-Verbindung, wenn keine Websocket-Unterstützung möglich ist. Wenn Sie es jedoch deaktivieren möchten, bearbeiten Sie die settings.bin-Datei und fügen Sie die folgende Zeile hinzu:

disable_http_on_https=true

Dann starten Sie die Terminal Service Plus-Webserver neu (AdminTool > Web > Webserver neu starten oder Konfiguration erneut einlesen). http://127.0.0.1/w0j3?settings.bin)

HTTPS-Durchsetzung und kostenlose SSL-Zertifikatvalidierung

Bitte beachten Sie, dass diese HTTPS-Durchsetzungsfunktion vollständig mit unserem Kostenloses SSL-Zertifikat Funktion.

Durchsetzung der Nutzung des Webportals zur Verbindung mit dem Server

Ab der Version 6.60 von Terminal Service Plus können Sie jeden Versuch, sich über den offenen/umgeleiteten Port (80 oder 443) mit mstsc.exe (oder anderen RDP-Clients) zu verbinden, blockieren/deaktivieren.

Diese Funktion erlaubt nur Zugriffe vom Terminal Service Plus Webportal und deaktiviert jede andere RDP-Verbindung über die Ports 80/443.

Um diese Funktion auf einem Server zu aktivieren, bearbeiten Sie die Datei C:\Program Files (x86)\TSplus\UserDesktop\files\AppControl.ini und fügen Sie die folgende Variable hinzu/ändern Sie sie:

Sicherheit Block_rdp_splitter=ja

Lastverteilung

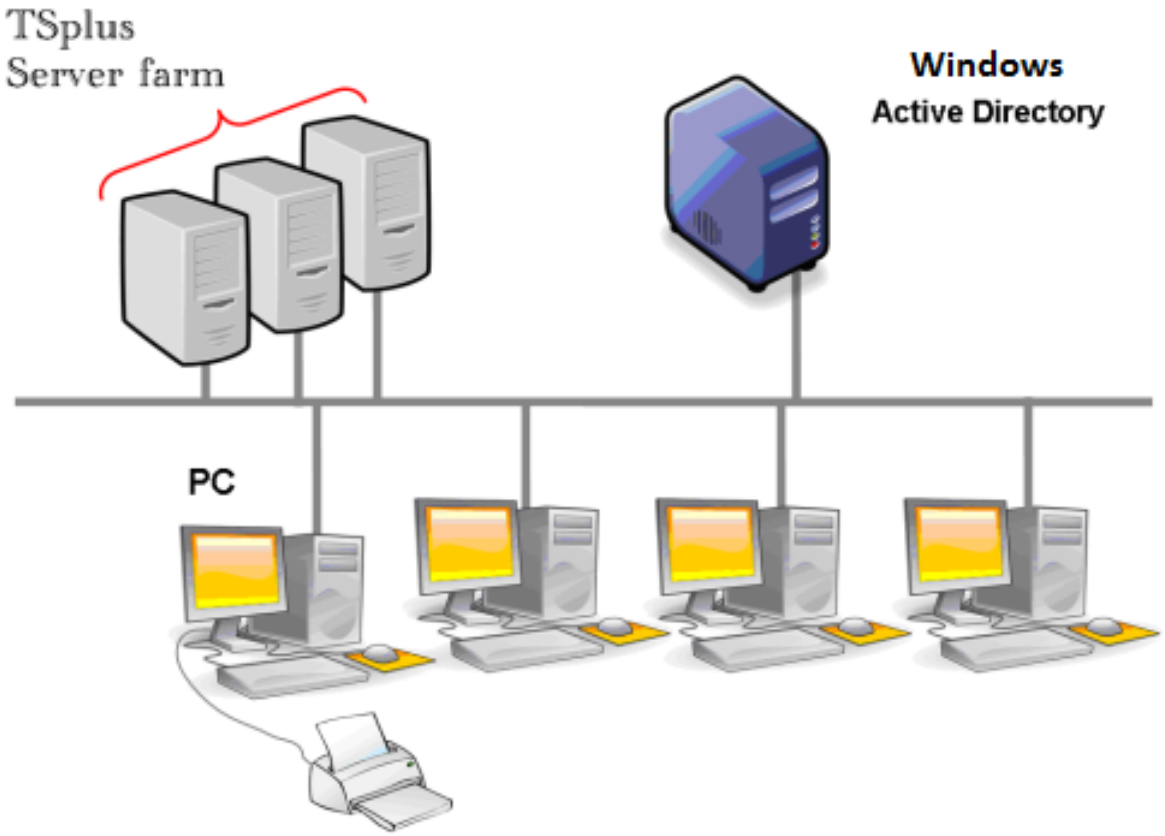
Voraussetzungen

Mit dieser Funktion können Sie eine Lastenausgleichs-Umgebung verwalten.

Es bedeutet, dass die Last aller Ihrer Benutzer zwischen Ihren Servern verteilt wird. Die Arbeitslast wird zwischen allen Servern Ihres Clusters geteilt.

Lastverteilung ermöglicht die Nutzung einer unbegrenzten Anzahl von Servern mit Lastverteilung und ist mit der Enterprise Edition verfügbar (eine gültige Lizenz pro Server). Diese sehr leistungsstarke und fortschrittliche Funktion sollte verwendet werden, wenn eine große Anzahl von Benutzern/Servern bereitgestellt werden muss.

Wichtig: Das einfache Aktivieren der Lastverteilung leitet Benutzer unabhängig von den für die Benutzer konfigurierten zugewiesenen Servern an den am wenigsten ausgelasteten Server des Clusters weiter. Wenn Sie die Lastverteilung UND die Serverzuweisung verwenden möchten, stellen Sie sicher, dass Sie das Kontrollkästchen „Lastverteilung auf zugewiesenen Servern“ aktivieren.



In der Regel empfehlen wir, einen Server für 50 gleichzeitige Benutzer zu verwenden.
Sie können mehr als 50 Benutzer überschreiten, abhängig von der Leistung Ihres Servers und dem Verbrauch der Anwendungsressourcen der Benutzer.

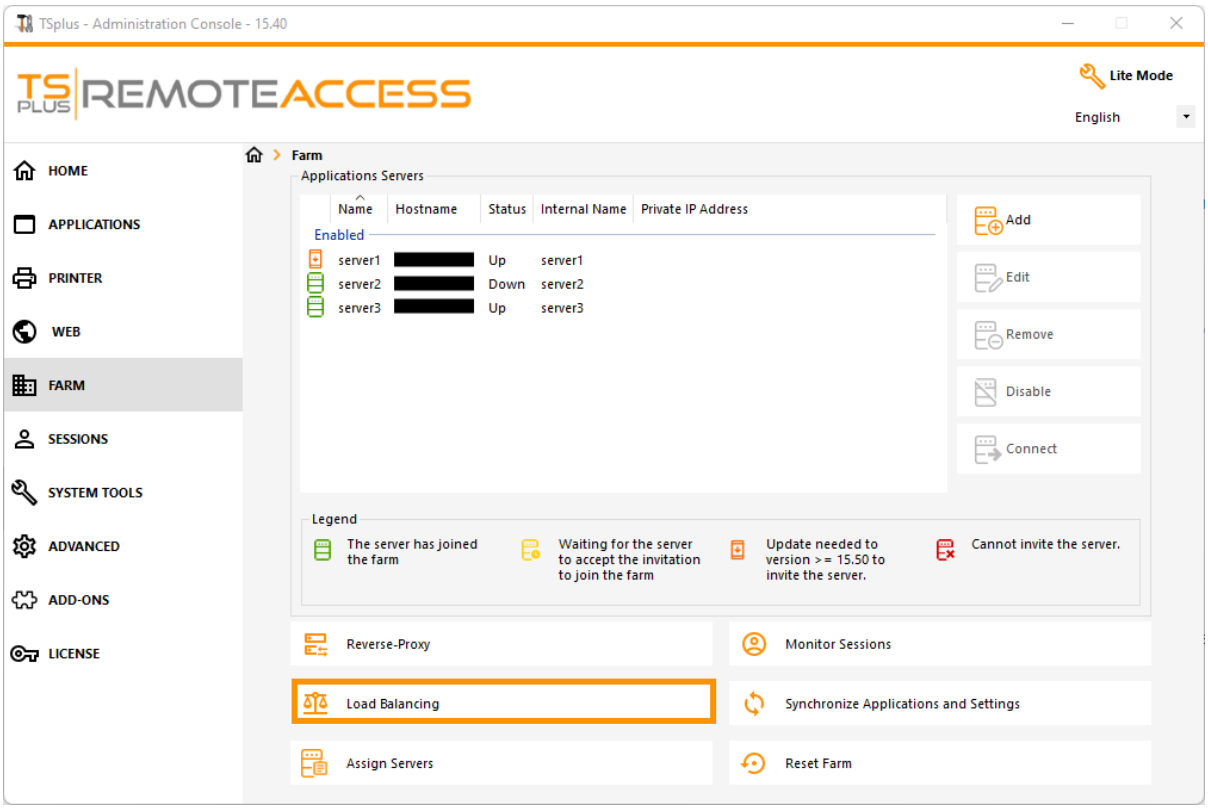
Generierte Clients und Webzugang

Es gibt drei Möglichkeiten, sich mit einem Lastenausgleichs-Cluster zu verbinden:

- Verwendung eines **Generierter Kunde** ausführbares Programm, erstellt von der Portabler Client-Generator)
- Verwendung eines **Webportalzugang** indem Sie es im Fenster "Webportal-Einstellungen" aktivieren.
- Mit dem TSplus App von Ihrem mobilen Gerät.

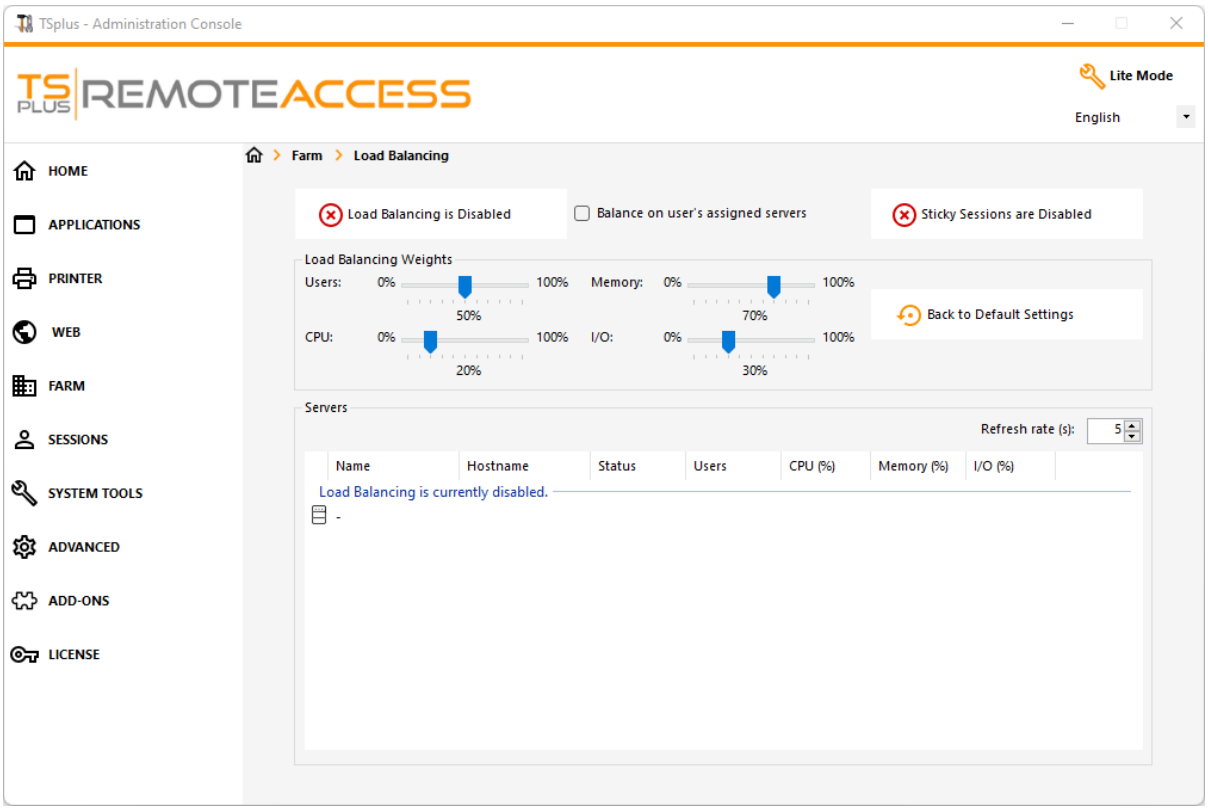
Lastenausgleich Hauptfenster

Der Lastenausgleichsmanager ist unter dem Farm-Tab des AdminTools zu finden:



Dieses Fenster ermöglicht es Ihnen, die Lastverteilung zu konfigurieren. Es listet alle Server in Ihrem Lastverteilten Serverfarm auf und ermöglicht es Ihnen, die Lastverteilung zu aktivieren, zu deaktivieren und zu konfigurieren (mehr dazu weiter unten).

Klicken Sie auf die Schaltflächen im Bild unten, um auf die entsprechenden Informationen zuzugreifen:



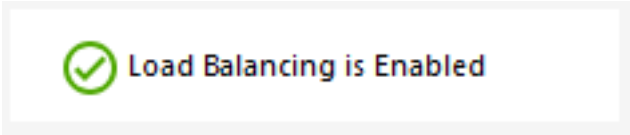
Oben im Load Balancing-Fenster sehen Sie einen großen Button:

- Dieser Button zeigt den aktuellen Zustand der Lastverteilung an.
- Wenn Sie darauf klicken, wird die Lastverteilung je nach aktuellem Zustand aktiviert oder deaktiviert.

Hier ist der Button, wenn die Lastverteilung aktiv ist. **Deaktiviert** Ein Klick darauf aktiviert es.



Hier ist der Button, wenn die Lastverteilung aktiv ist. **Aktiviert** Ein Klick darauf deaktiviert es.



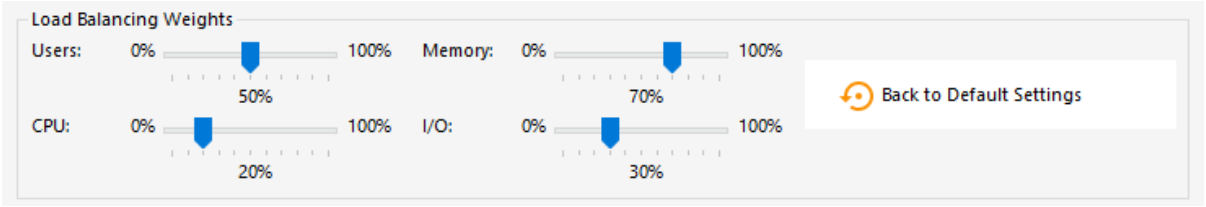
Wie wählt Load Balancing einen Server aus?

Wenn die Lastverteilung aktiviert ist, wird der Benutzer zum weniger ausgelasteten Server zum Zeitpunkt seiner Verbindung geleitet.

Um zu bestimmen, welcher Server am wenigsten ausgelastet ist, wird die Auslastung jedes Servers unter Verwendung eines gewichteten Durchschnitts mehrerer Leistungsindikatoren berechnet:

- Anzahl der verbundenen Benutzer
- Prozessorverbrauch
- Speicherverbrauch
- Festplattenspeicher

Sie können das Gewicht (die Wichtigkeit) dieser Indikatoren mithilfe der folgenden Schieberegler ändern:



Mit diesen Schiebereglern können Sie das Load Balancing feinabstimmen und es an Ihre eigenen Bedürfnisse anpassen. Wenn Ihre Benutzer beispielsweise eine Geschäftsanwendung mit hohen Speicheranforderungen starten, kann es eine gute Idee sein, den Einfluss des RAM in der Lastberechnung mit dem Schieberegler „Speicher“ zu erhöhen.

Sie können diese Werte auch zurücksetzen, indem Sie auf die Schaltfläche „Auf die Standardeinstellungen zurücksetzen“ klicken.

Wie wird die Last des Servers berechnet?

Die Last jedes Servers wird bei Bedarf berechnet, um zu entscheiden, auf welchen Server der Benutzer gesendet werden muss.

Für diese Berechnung verwenden wir ein **gewichteter Durchschnitt** zwischen 4 Hardware-Metriken.

Die 4 Schieberegler ermöglichen es Ihnen, jedem dieser Metriken mehr (oder weniger) Gewicht zu geben, die sind:

- Benutzer: Anzahl der verbundenen Benutzer
- CPU : Prozentsatz der nicht im Leerlauf befindlichen Prozessorzeit
- Speicher: Prozentsatz des verwendeten Speichers
- I/O : Prozentsatz der nicht-leeren Festplattenspeicherzeit

Wenn Sie beispielsweise den „Speicher“-Regler auf die rechte Seite und alle anderen Regler auf die linke Seite setzen, wird die Last jedes Servers fast ausschließlich anhand des Prozentsatzes des verwendeten Speichers berechnet - und Ihre Benutzer werden an den Server mit dem meisten verfügbaren Speicher gesendet.

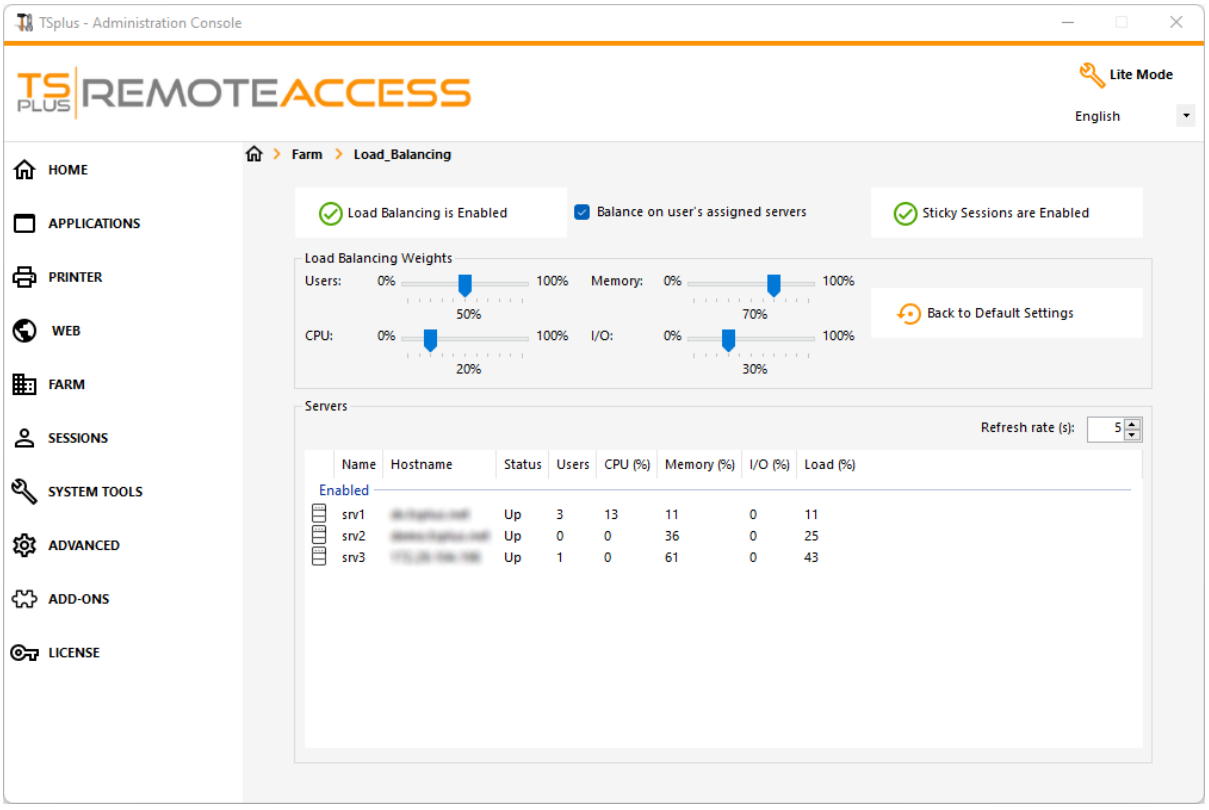
- Wenn ein Schieberegler ganz links ist, wird das Gewicht, das in der Lastberechnung verwendet wird, 1 sein.
- Wenn ein Schieberegler ganz links ist, wird das Gewicht, das in der Lastberechnung verwendet wird, 100 betragen.

Darüber hinaus hängt die Last eines bestimmten Servers vom Verhältnis [genutzte Ressourcen / Gesamte Ressourcen] ab; wenn also ein Server A doppelt so leistungsfähig ist wie ein Server B, sollten doppelt so viele Benutzer an Server A gesendet werden wie an Server B (vorausgesetzt, alle anderen Faktoren sind gleich).

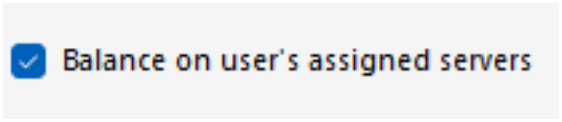
Sie können die Liste der Status von Lastverteilten Servern und Details zu den Leistungsindikatoren jedes Servers einsehen.

Die Server sind von den am wenigsten ausgelasteten bis zu den am stärksten ausgelasteten entsprechend Ihrer Konfiguration sortiert.

Die Liste der Status der Lastenausgleichsserver wird automatisch aktualisiert. Diese automatische Aktualisierung stoppt, wenn die Verbindung nicht mehr verfügbar ist. Sie können die Aktualisierungsrate in der oberen rechten Ecke des "Server"-Fensters ändern.



Lastverteilung kann auch direkt auf dem dem Benutzer zugewiesenen Server unter Verwendung des **Checkbox "Balance auf den zugewiesenen Servern des Benutzers"** .
Als Ergebnis werden Sie in der Lage sein, auf den Servern der Buchhaltungsabteilung nur für Buchhalterbenutzer Lastenausgleich durchzuführen, sobald diese spezifischen Server den Buchhalterbenutzern zugewiesen wurden.



Sie können die Funktion für sticky Sessions aktivieren, indem Sie auf die rechte Schaltfläche des Fensters für die Lastverteilung klicken:



Aktivierung **bestehende Sitzungen Webauflistung** ist erforderlich für die Funktion der Sticky Sessions bei der Lastenverteilung.

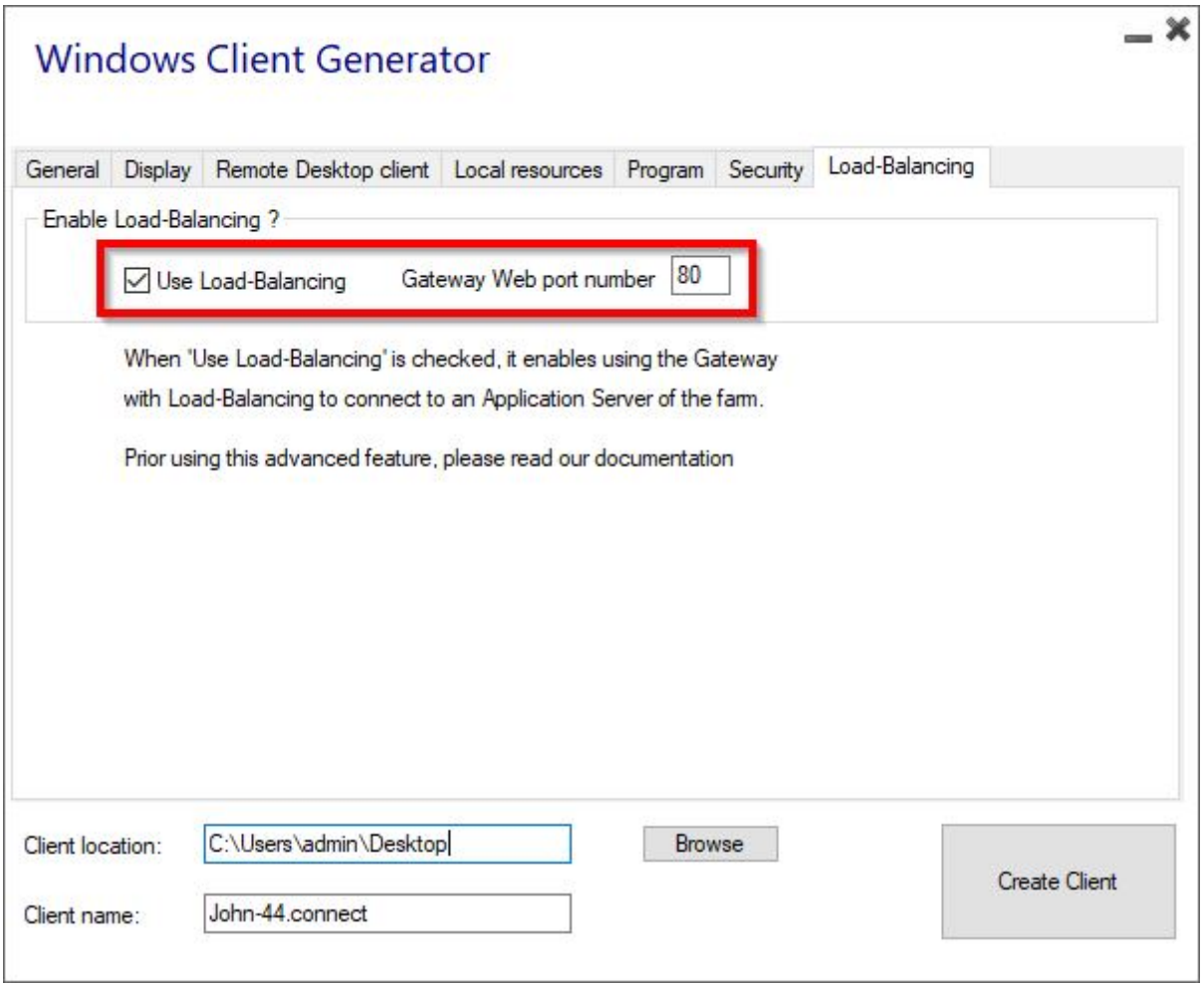
Es wird Ihnen ermöglichen, sich mit einer getrennten Sitzung erneut zu verbinden, anstatt eine neue Sitzung auf einem anderen Server zu öffnen.

Um zu aktivieren **bestehende Sitzungen Webauflistung** , stellen Sie Folgendes ein Einstellung zu "nein".

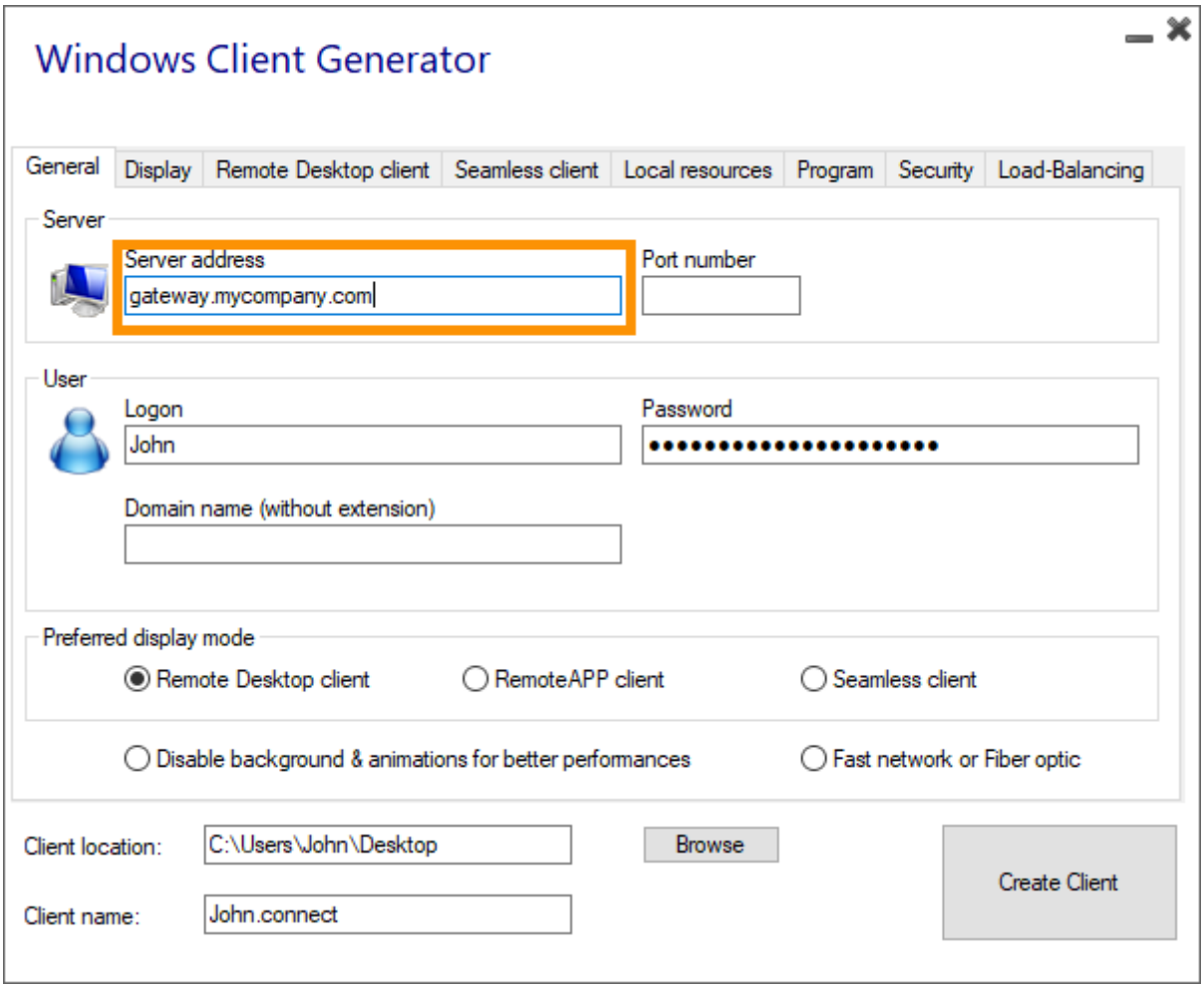
Lastverteilung mit einem Verbindungsclient

Wenn Sie eine erstellen möchten Verbindungsclient um sich mit dem weniger ausgelasteten Server zu verbinden , Sie benötigen von dem Client-Generator in der “ Lastverteilung ” Tab zu:

- Überprüfen Sie das Kontrollkästchen „Lastenausgleich verwenden“
- Füllen Sie das Feld „Gateway-Webportnummer“ mit dem HTTP- oder HTTPS-Port aus, der von Ihrem Gateway-Server verwendet wird.



- Verwenden Sie die öffentliche IP-Adresse oder den Hostnamen Ihres Gateway-Servers direkt im Feld „Server“.


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

Farm Manager API

Wir freuen uns, Ihnen eine leistungsstarke API anzubieten, die umfassende Verwaltungsfunktionen für Ihre Serverfarmen bereitstellt.

Diese API ermöglicht es Ihnen, unsere Software nahtlos in Ihre bestehende Infrastruktur zu integrieren, sodass Sie Serveroperationen mit Ihren eigenen benutzerdefinierten Skripten verwalten und automatisieren können.

Entdecken Sie das volle Potenzial unserer Software mit der robusten und vielseitigen API, die wir bereitstellen.

Anforderungen

Um die Farm-Manager-API abzufragen, muss Ihr Server Folgendes tun:

- haben Sie ein gültiges SSL/TLS-Zertifikat
- über Port 19956 geöffnet werden
- erreichbar sein, indem Sie die Domain verwenden, die Ihr Zertifikat abdeckt.

Beispiele für die Verwendung

Zum Beispiel können Administratoren die verwenden **Farm > Serverliste abrufen** Funktion zur Abrufung einer umfassenden Liste aller Server innerhalb ihres Farms, um das Inventarmanagement zu optimieren. Die **Farm > Farm initialisieren** Funktion ermöglicht die schnelle Einrichtung eines neuen Server-Pools und sorgt für einen reibungslosen Bereitstellungsprozess. Für die benutzerspezifische Serververwaltung, die **Farm > Liste der Server, die einem Benutzer zugewiesen sind** Funktion hilft bei der Verfolgung und Verwaltung von Serverzuweisungen.

In Lastenausgleichsszenarien, die **Lastverteilung > Server auswählen** und **Lastenausgleich > Neu laden** Funktionen ermöglichen die dynamische Serverauswahl und das Neuladen von Lastenausgleichs-Konfigurationen, um die Ressourcenverteilung und Leistung zu optimieren. Die **ReverseProxy > Neu laden** Die Funktion stellt sicher, dass Änderungen an den Proxy-Einstellungen ohne Ausfallzeiten angewendet werden. Darüber hinaus wird die **Server > Hinzufügen** und **Server > Bearbeiten** Funktionen erleichtern die nahtlose

Hinzufügung und Modifikation von Servern im Farm.

Administratoren können ihre Abläufe weiter verbessern, indem sie die nutzen **Einstellungen > Listeneinstellungen** und **Einstellungen > Einstellungen anwenden** Funktionen zum Abrufen und Anwenden von Konfigurationseinstellungen über die Serverfarm.

Für das Sitzungsmanagement, die **Sitzung > Trennen** und **Sitzung > Abmelden** Funktionen ermöglichen die kontrollierte Beendigung von Benutzersitzungen, während die **Sitzung > Benutzersitzungen auflisten** bietet eine detaillierte Ansicht aktiver Sitzungen zu Überwachungszwecken.

Durch die Nutzung dieser leistungsstarken API-Funktionen können Sie eine höhere Automatisierung, Effizienz und Kontrolle über Ihre Serververwaltungsprozesse erreichen, um die optimale Leistung und Zuverlässigkeit Ihrer Infrastruktur sicherzustellen.

Dokumentation

Die vollständige Dokumentation dieser API finden Sie hier : API-Dokumentation

Übersicht

Übersicht und Benennung

Das Ziel der TSplus Farm-Funktionen ist es, dem Administrator zu ermöglichen, alle seine TSPlus-Server von einem einzigen Server aus zu verwalten. Dieser Server kann als der bezeichnet werden **Farm Controller** .

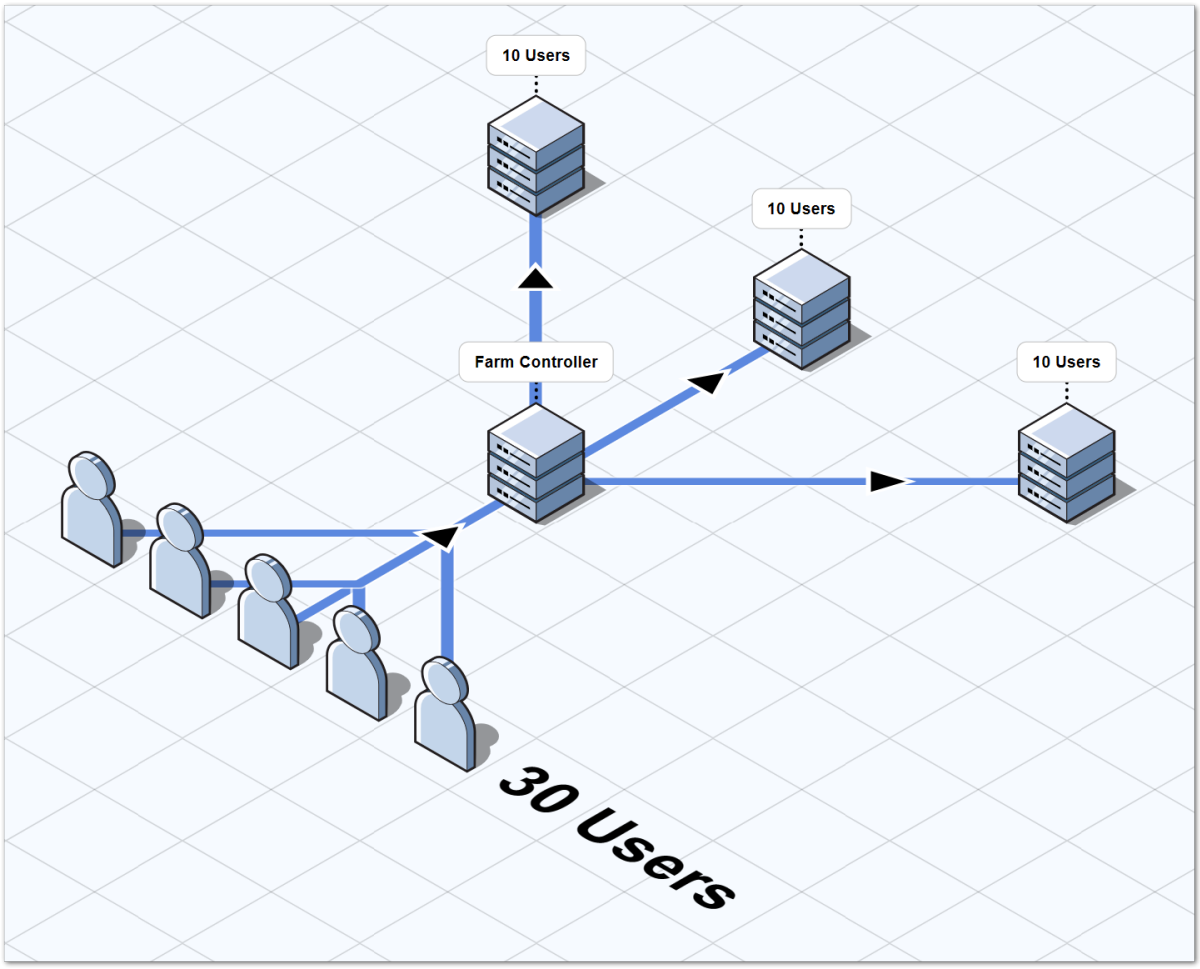
Die TSplus-Server im Farm werden genannt die **Anwendungsserver** oder einfach Server.

Dieser Farm-Controller, nachdem seine Farm mit Anwendungsservern bevölkert wurde, wird auch zu einem **Gateway-Server** sobald Sie eine der Farm-Funktionen wie aktiviert haben:

- Load balancing
- Reverse Proxy
- Server zuweisen

Dieser Gateway-Server wird im Grunde genommen der Hauptzugangspunkt für alle Ihre Benutzer, wenn entweder "Lastenausgleich" oder "Server zuweisen" aktiviert ist.

Schließlich ermöglicht Ihnen dieser Farm-Controller auch die Überwachung aller Anwendungsserver und das einfache Übertragen von TSplus-bezogenen Einstellungen wie Anwendungen und erweiterten Einstellungen von Ihrem Farm-Controller auf Ihre Anwendungsserver.



TSplus Farm of Servers Architektur

Es gibt 2 Optionen, um eine TSplus-Farm von Servern bereitzustellen:

Option 1 Alle Ihre Server haben öffentliche IP-Adressen und sind über das Internet erreichbar.

ODER

Option 2 Nur das Gateway-Portal kann über das Internet erreicht werden. Der Gateway-Server bietet eine „Reverse Proxy-Rolle“ an.

In beiden Optionen:

- Jeder Server hat die gleiche TSplus-Konfiguration.
- Jeder Server hat die gleichen HTTP/HTTPS-Ports.
- Um eine neue Anwendung zu veröffentlichen, fügen Sie sie einfach Ihren Benutzern/Gruppen von Benutzern im AdminTool hinzu.

Natürlich sollten Sie sicherstellen, dass diese Anwendung auf den angestrebten Anwendungsservern installiert ist.

Alle Webzugriffstypen sind ohne spezifische Konfiguration verfügbar: RemoteApp- und HTML5-Clients.

Option 1 - Alle Server haben ihre eigene öffentliche IP-Adresse und sind über das Internet erreichbar.

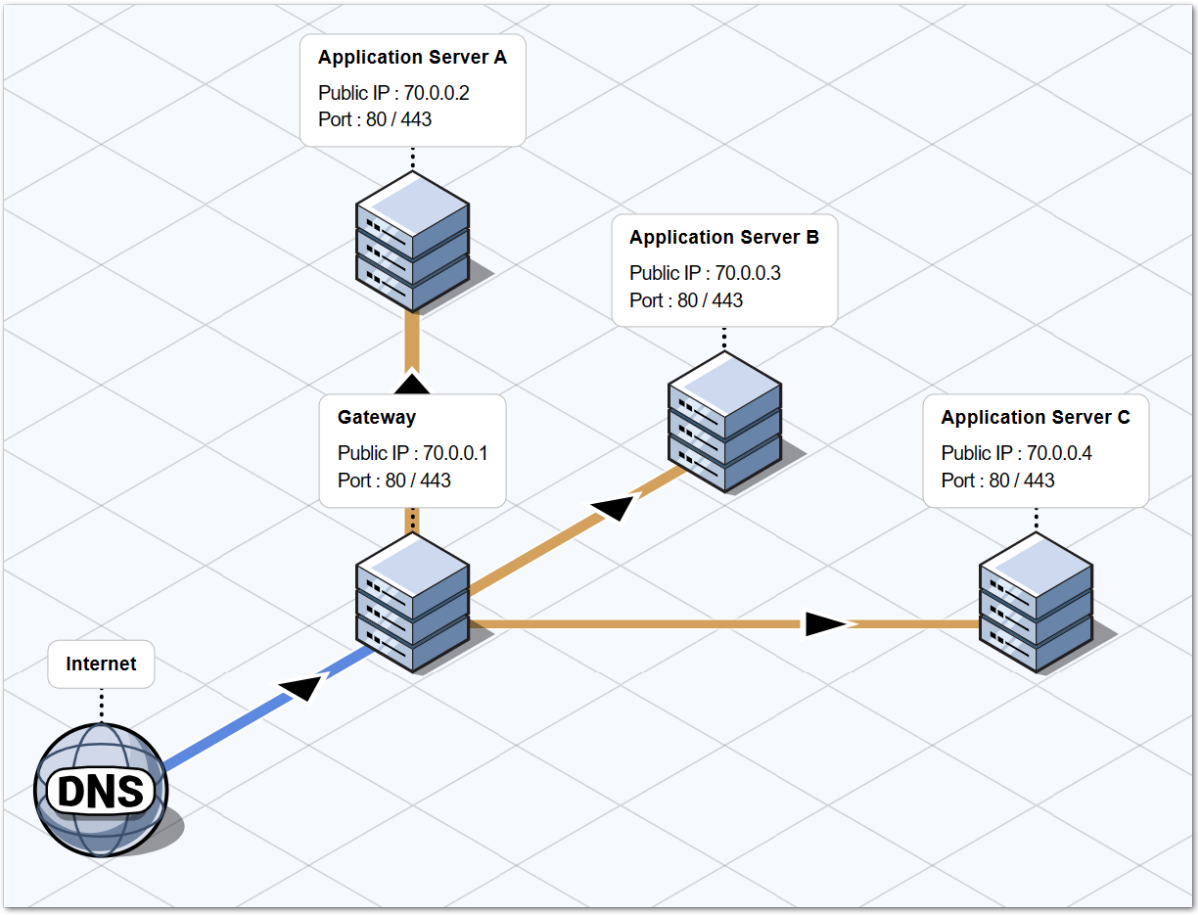
Dies ist die empfohlene Architektur zur Verwendung von Terminal Service Plus Gateway.

Diese Architektur folgt bewährten Praktiken und ermöglicht es dem IT-Administrator, seine Umgebung zu industrialisieren:

- Jeder Server hat die gleiche Terminal Service Plus-Konfiguration.
- Jeder Server hat die gleichen HTTP/HTTPS-Ports
- Die Bereitstellung eines neuen Anwendungsservers ist nur eine Frage von Minuten (fügen Sie einfach den Server im AdminTool auf dem Gateway-Server zur Farm hinzu).

Mit dieser Architektur sind alle Zugriffstypen ohne spezifische Konfiguration verfügbar: Remoteapp und HTML5-Clients.

Diese Architektur ist im folgenden Diagramm beschrieben:



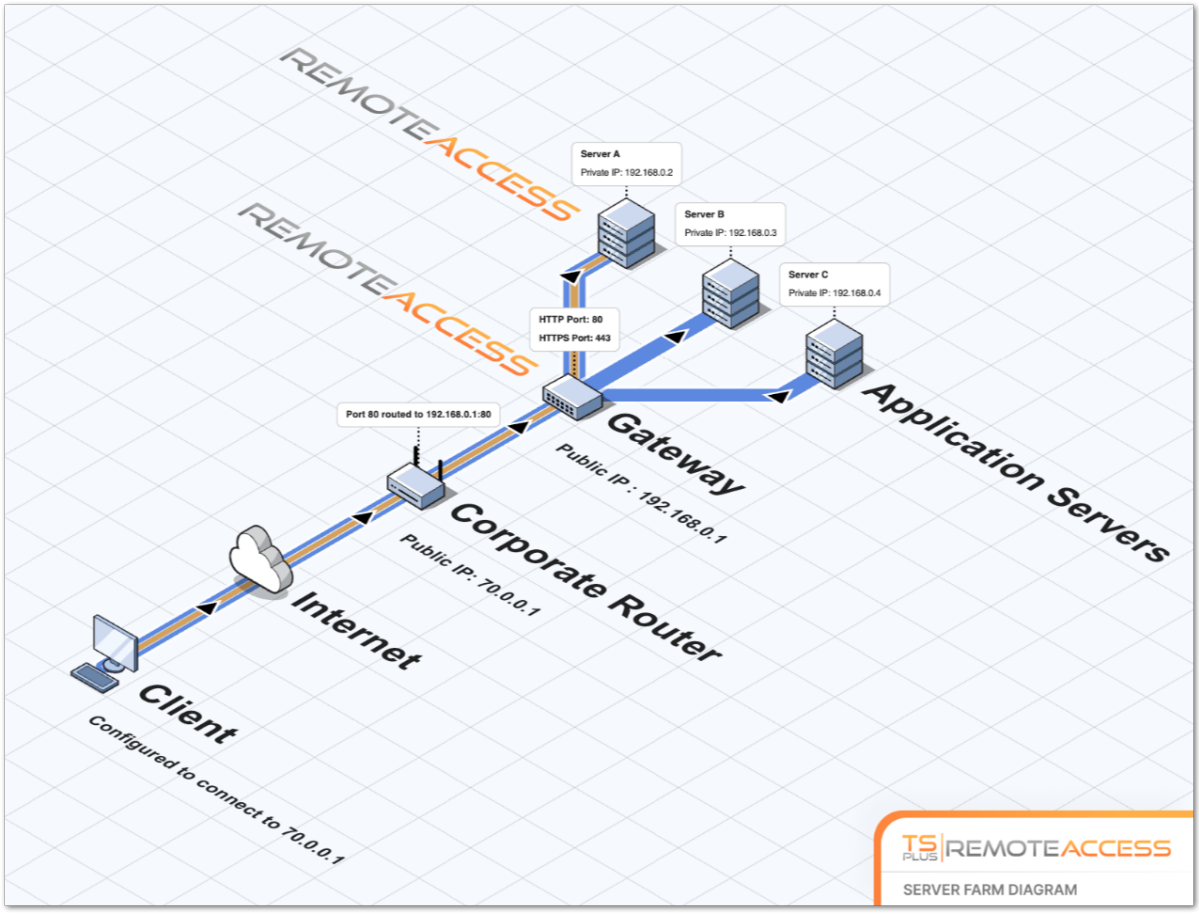
-
-
  -

Option 2: Nur das Gateway-Portal kann über das Internet erreicht werden und umfasst eine „Reverse Proxy-Rolle“.

Terminal Service Plus Gateway kann auch mit nur 1 öffentlicher IP-Adresse eingerichtet werden.

Das Gateway leitet jede externe Verbindungsanfrage an jeden verfügbaren Server weiter. Wenn Sie die Lastenausgleichsfunktion nicht verwenden, verbinden sich die Benutzer mit ihrem zugewiesenen Server(n).

Diese Architektur ist im folgenden Diagramm beschrieben:



Für weitere Informationen zur Reverse-Proxy-Rolle siehe die Reverse-Proxy-Funktion Dokumentation .

Versionsverlauf

- API 1.5 (veröffentlicht mit TSplus 15.50)
  - Integrierte Reverse-Proxy-, Lastenausgleichs- und Anwendungsserver-Zuweisungskonfiguration
  - Hinzugefügt wurde die Synchronisation zwischen Anwendungen/Einstellungen des Farmcontrollers und allen Anwendungsservern.

- API 1.4 (veröffentlicht mit TSplus 10.10)
  - Zentralisierte Überwachung der Lastverteilung
  - Server im TSplus Lastenausgleichsmanager aktivieren/deaktivieren
  - Übersetzungen in mehreren Sprachen (Die Sprache von TSplus wird verwendet)
  - Mehrere Einstellungen hinzugefügt + Anzeigeprobleme behoben

- API 1.3 (veröffentlicht mit TSplus 9.70)
  - Zentrale Überwachung und Verwaltung (Globale Einstellungen / Schwimmendes Panel / RemoteApp-Client / HTML5-Client)

- API 1.2 (veröffentlicht mit TSplus 9.60)
  - Farm Manager
  - Zentrale Verwaltung von Servern (hinzufügen/entfernen)
  - Zentralisierte Überwachung und Verwaltung von Sitzungen (Nachrichten/Trennen/Abmelden)

- API 1.1 (veröffentlicht mit TSplus 9.30)
  - Lastenverteilung internals
  - Lastenverteilung Sticky-Sitzungen

Voraussetzungen

Hardware-Anforderungen

Farm-Controller und Anwendungsserver haben den Standard Terminal Service Plus Anforderungen für Hardware.

Betriebssystemanforderungen

Farm-Controller und Anwendungsserver müssen eines der folgenden Betriebssysteme verwenden:

- Windows **7 Pro**
- Windows **8/8.1 Pro**
- Windows **10 Pro**
- Windows **11 Pro**
- Windows **Server 2008 SP2/Small Business Server SP2 oder 2008 R2 SP1**
- Windows **Server 2012 oder 2012 R2**
- Windows **Server 2016**
- Windows **Server 2019**
- Windows **Server 2022**
- Windows **Server 2025**

Sowohl 32- als auch 64-Bit-Architekturen werden unterstützt.

Netzwerkanforderungen

Jeder Anwendungsserver muss vom Farm-Controller aus zugänglich sein.

Genauer gesagt wird der Farm Controller Anfragen an jeden Anwendungsserver über seinen API-Port (standardmäßig 19955) senden, und dieser Port muss an jeder Firewall, die zwischen dem Farm Controller und den Anwendungsservern steht, geöffnet sein.

Die Netzwerkverzögerung zwischen dem Farm-Controller und den Anwendungsservern muss gering sein. Eine Verzögerung von unter 200 ms wird empfohlen, eine Verzögerung von unter 2.000 ms ist erforderlich.

Softwareanforderungen

.NET 2.0 oder höher ist erforderlich - das sollte kein Problem sein, da eine kompatible .NET-Version standardmäßig auf jedem unterstützten Betriebssystem für Terminal Service Plus Farm aktiviert ist.

Terminal Service Plus Lizenz- und Versionsanforderungen

Terminal Service Plus muss in der „Enterprise“ Edition auf dem Farm-Controller und auf allen Anwendungsservern sein.

Alle Server müssen auch die gleiche Version von Terminal Service Plus ausführen.

Konfigurationsanforderungen

Farm Controller und Anwendungsserver müssen die gleiche Datum/Uhrzeit konfiguriert haben. Es wird dringend empfohlen, die Windows-Uhr aller Server mit einem Internet-Zeitserver zu synchronisieren, falls dies noch nicht geschehen ist.

Benutzeranforderungen

Ein Active Directory ist **nicht** erforderlich, jedoch wenn Sie ein Active Directory haben, müssen Ihre Domänenadministratoren auch lokale Administratoren des Farm Controllers sein, um den Terminal Service Plus Farm Manager verwenden zu können.

Reverse Proxy

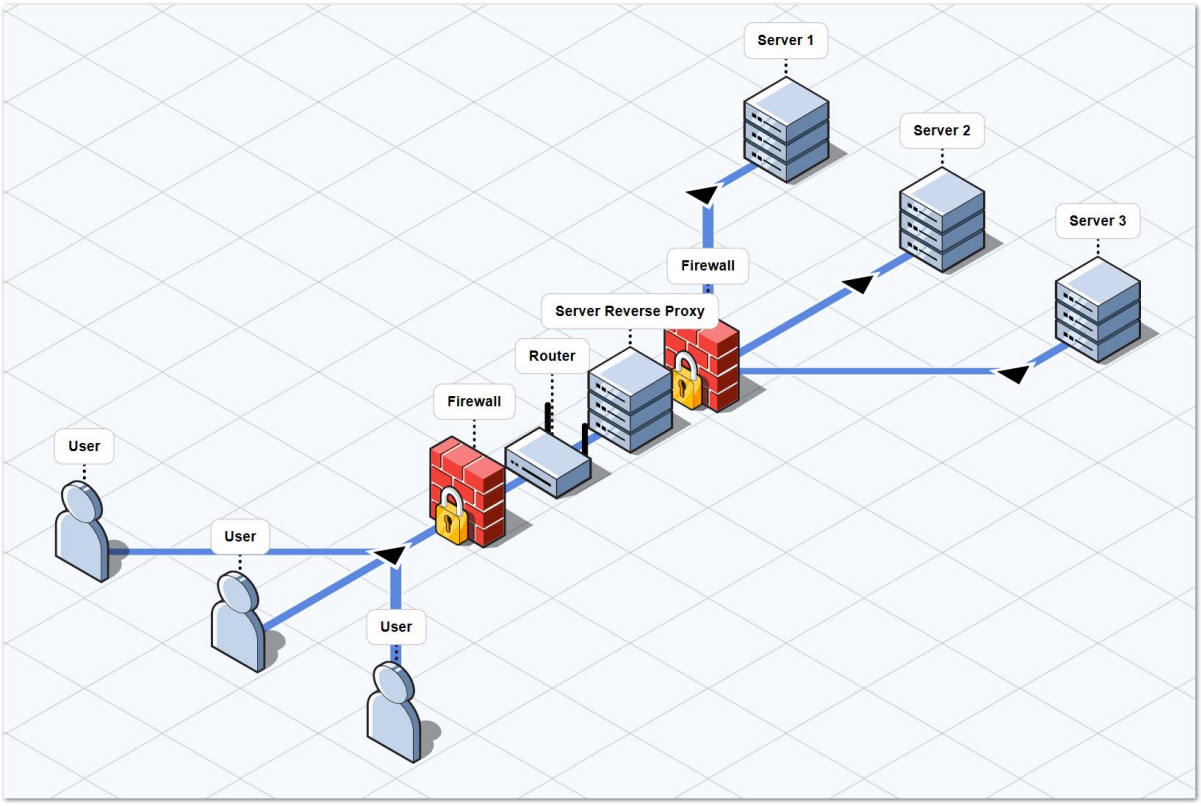
Übersicht

Diese Funktion ist in der TSplus Enterprise Edition verfügbar.

Das Reverse-Proxy-System fungiert als Vermittler, damit seine zugehörigen Server von jedem Client kontaktiert werden können.

Der Vorteil der Verwendung eines Reverse-Proxy ist einfach: Sie müssen nicht mehr so viele Portweiterleitungsregeln erstellen, wie Sie TSplus-Server haben.

Egal, ob Sie die Lastenausgleichsfunktion verwenden oder nicht, Sie müssen sie aktivieren, um sich über den Reverse-Proxy zu verbinden. In TSplus bietet es einen einzigartigen Zugangspunkt zu einem Farm von lastenausgeglichenen TSplus-Servern.

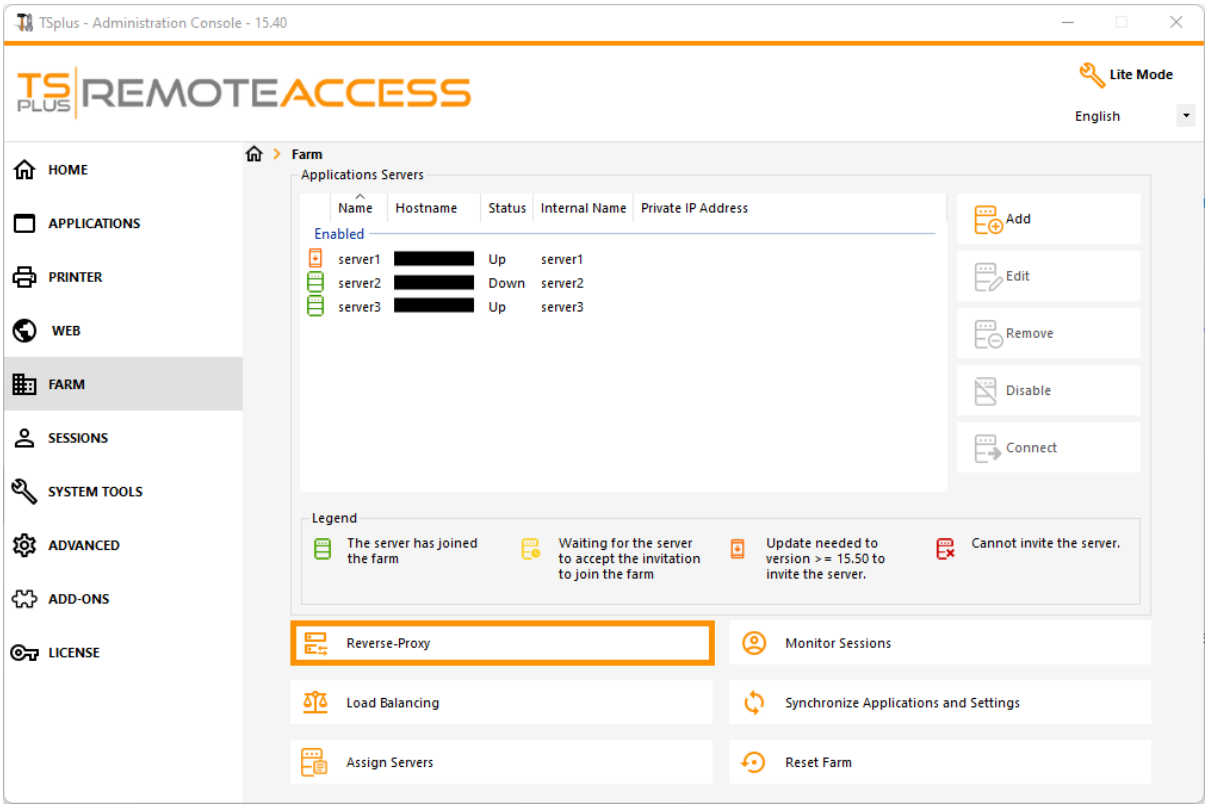


Dieser einzigartige Zugangspunkt wird Ihr Gateway-Server TSplus Webportal sein.

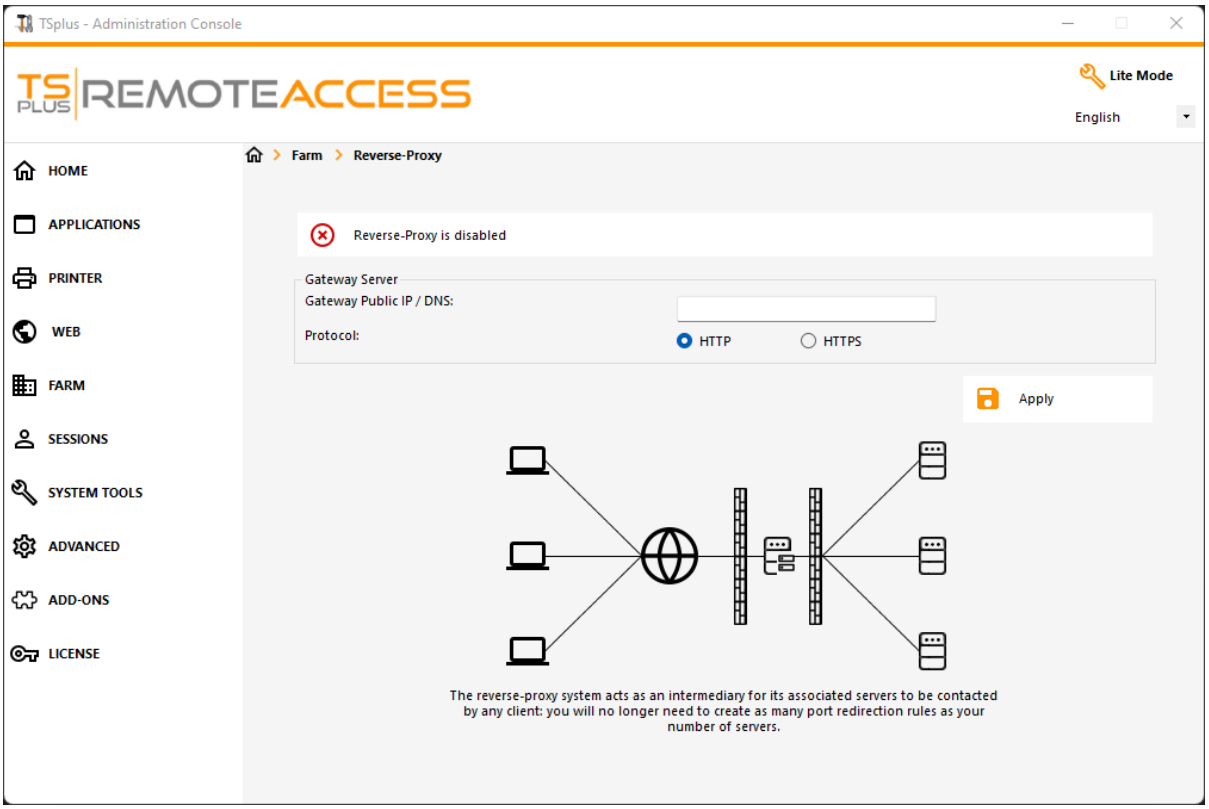
Da dieser Server remote zugegriffen werden soll, müssen Sie eine Portweiterleitungsregel auf Ihrem Router einrichten, einschließlich der http- oder https-Ports, je nach Ihrer Präferenz (80 ist der Standardport für http und 443 für https).

Konfiguration

Sie können auf die Konfigurationsoberfläche des Reverse Proxy über den FARM-Tab zugreifen:



Klicken Sie auf die Reverse-Proxy-Schaltfläche.



- Klicken Sie auf die Schaltfläche „Reverse-Proxy ist deaktiviert“, um sie zu aktivieren.
- Die öffentliche IP des Gateways muss mit einer festen gültigen IP-Adresse oder einem Domainnamen festgelegt werden.
- Wählen Sie HTTP oder HTTPS für Ihre bevorzugte Verbindungsart, die Server Ihrer Farm müssen in der Lage sein, über Port 80 oder 443 miteinander zu kommunizieren, je nachdem, welche Verbindungsart Sie verwenden. Es ist auch wichtig, dass Ihre Windows-Firewall diese Ports nicht blockiert.

Sobald Sie Ihre Konfiguration abgeschlossen haben, klicken Sie auf „Übernehmen“, um diese Reverse-Proxy-Einstellungen zu speichern.

Zugriff auf Anwendungsserver über Gateway-Server

Sobald die Reverse-Proxy-Funktion aktiviert und betriebsbereit ist, können Sie auf den Anwendungsserver über eine spezielle URL zugreifen, die wie folgt formatiert ist:
(1) :// **2** : **3** /~~ **4**
mit:

- (1): das konfigurierte Reverse Proxy-Protokoll

- die öffentliche IP-Adresse oder der Domainname des Gateway-Servers
- (3): der Webport des Gateway-Servers, der mit dem konfigurierten Reverse-Proxy-Protokoll verbunden ist
- (4): der interne Name des Anwendungsservers, der vom Reverse Proxy verwendet wird

Zum Beispiel, vorausgesetzt, dass:

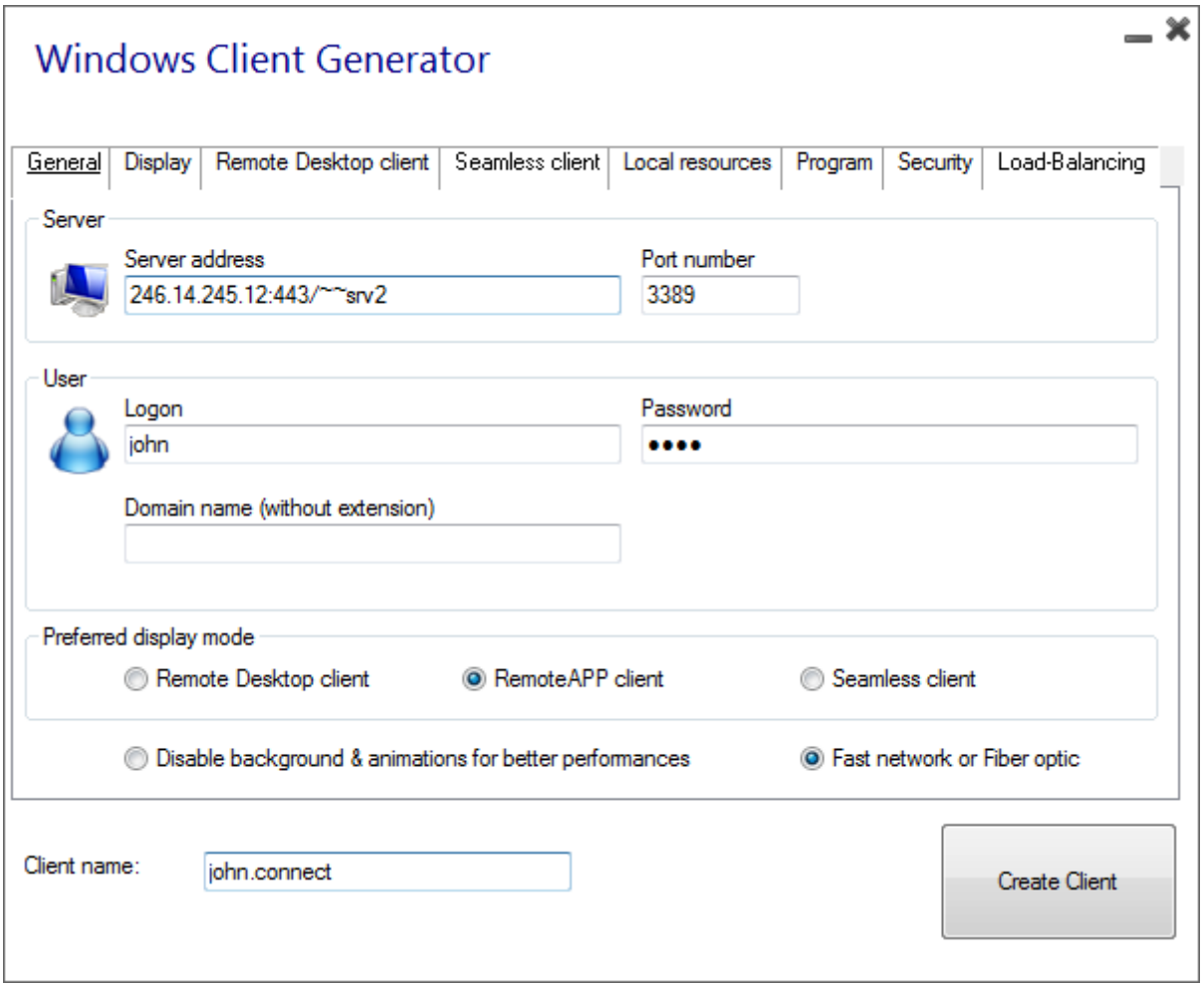
- das konfigurierte Reverse-Proxy-Protokoll ist HTTPS
- Ihr Gateway-Server hat die öffentliche IP 1.1.1.1
- Ihr Gateway-Server verwendet den HTTPS-Port 443
- der Zielanwendungsserver, mit dem Sie eine Verbindung herstellen möchten, verwendet den internen Namen „srv2“

Die spezielle URL, die verwendet werden muss, um den Zielanwendungsserver zu erreichen, wird sein 1.1.1.1:443/~~srv2

Als Ergebnis können Sie das Webportal dieses Anwendungsservers über diese spezielle URL aufrufen.

Sie können auch einen Verbindungsclient generieren, der über den Gateway-Server mit diesem spezifischen Anwendungsserver über dieselbe Methode verbunden wird. Verwenden Sie einfach die spezielle URL im Serveradressfeld des Verbindungsclient-Generators.

Zum Beispiel:


Windows Client Generator
General
Display
Remote Desktop client
Seamless client
Local resources
Program
Security
Load-Balancing
Server
Server address
246.14.245.12:443/~~srv2
Port number
3389
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 name:
john.connect
Create Client

Server-Zuweisung

Übersicht

Der Farm-Controller kann als Gateway-Server fungieren und Benutzer bei der Verbindung an bestimmte Anwendungsserver Ihrer Farm weiterleiten. Sie können einem Benutzer / einer lokalen Gruppe / einer Active Directory-Gruppe einen oder mehrere Server zuweisen.

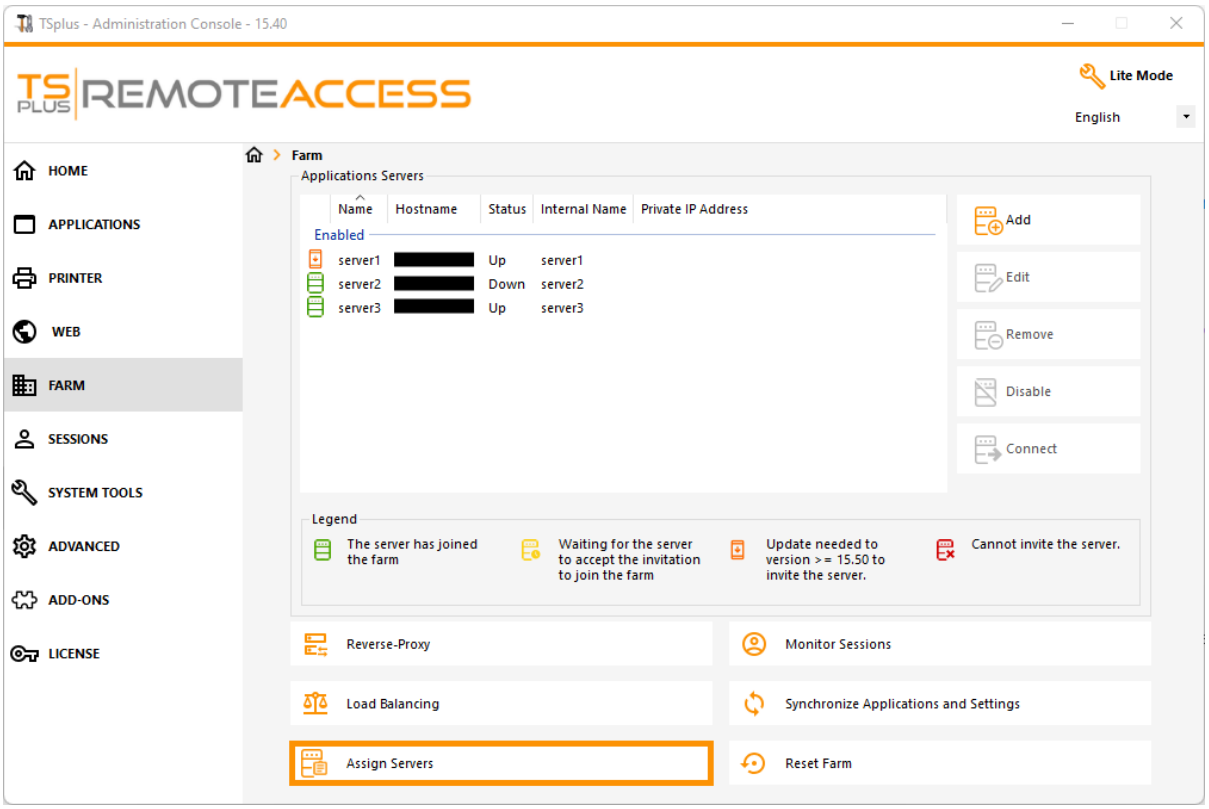
Wichtig: Die Zuweisung von Servern funktioniert nur über das TSplus Web Portal und nicht mit Verbindungsclients.

Wenn der Benutzer mehr als einen zugewiesenen Server hat, kann er in der Liste der ihm zugewiesenen Server auswählen, auf welchen Server er zugreifen möchte.

Wenn die Farm innerhalb einer Domäne ist, verwendet das Gateway seine AD-Anmeldeinformationen und der Benutzer verbindet sich mit Single Sign-On (SSO).

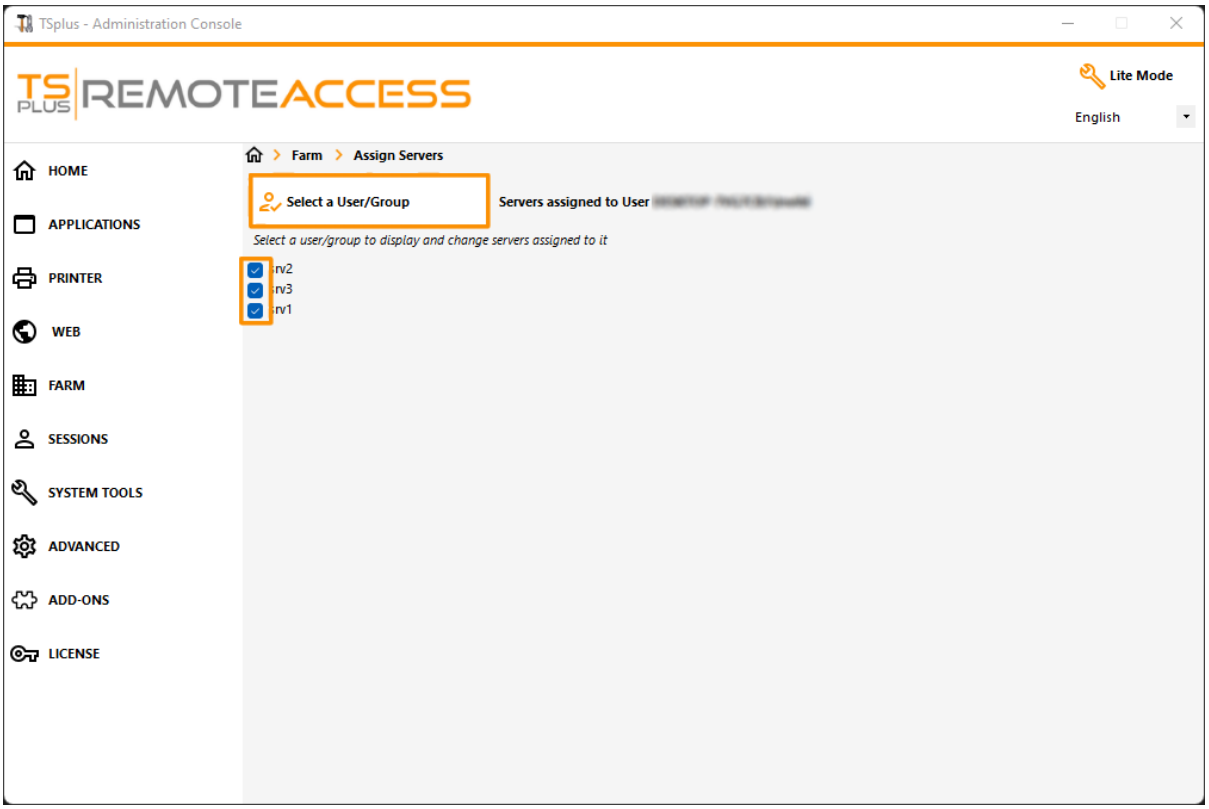
Andernfalls muss er über die gleichen lokalen Anmeldeinformationen auf jedem Server verfügen.

Um Server zuzuweisen, klicken Sie bitte auf die Schaltfläche „Server zuweisen“.



Um einen Server einem Benutzer zuzuweisen, wählen Sie ihn einfach mit der Schaltfläche „Benutzer/Gruppe auswählen“ aus und aktivieren Sie dann das Kontrollkästchen des Servers in der Liste „Server“.

Um einen einem Benutzer zugewiesenen Server zu entfernen, deaktivieren Sie einfach das Kontrollkästchen des Servers in der Liste „Server“.

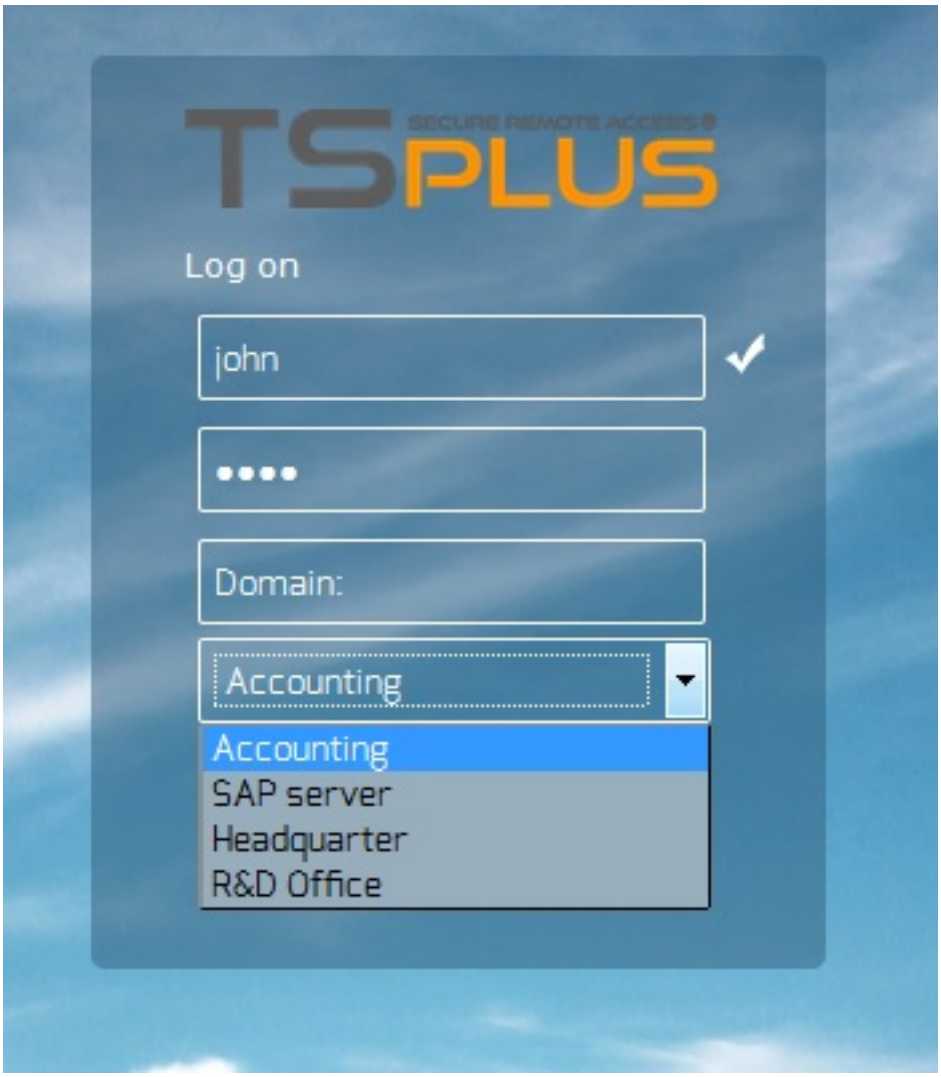


Wichtige Hinweise

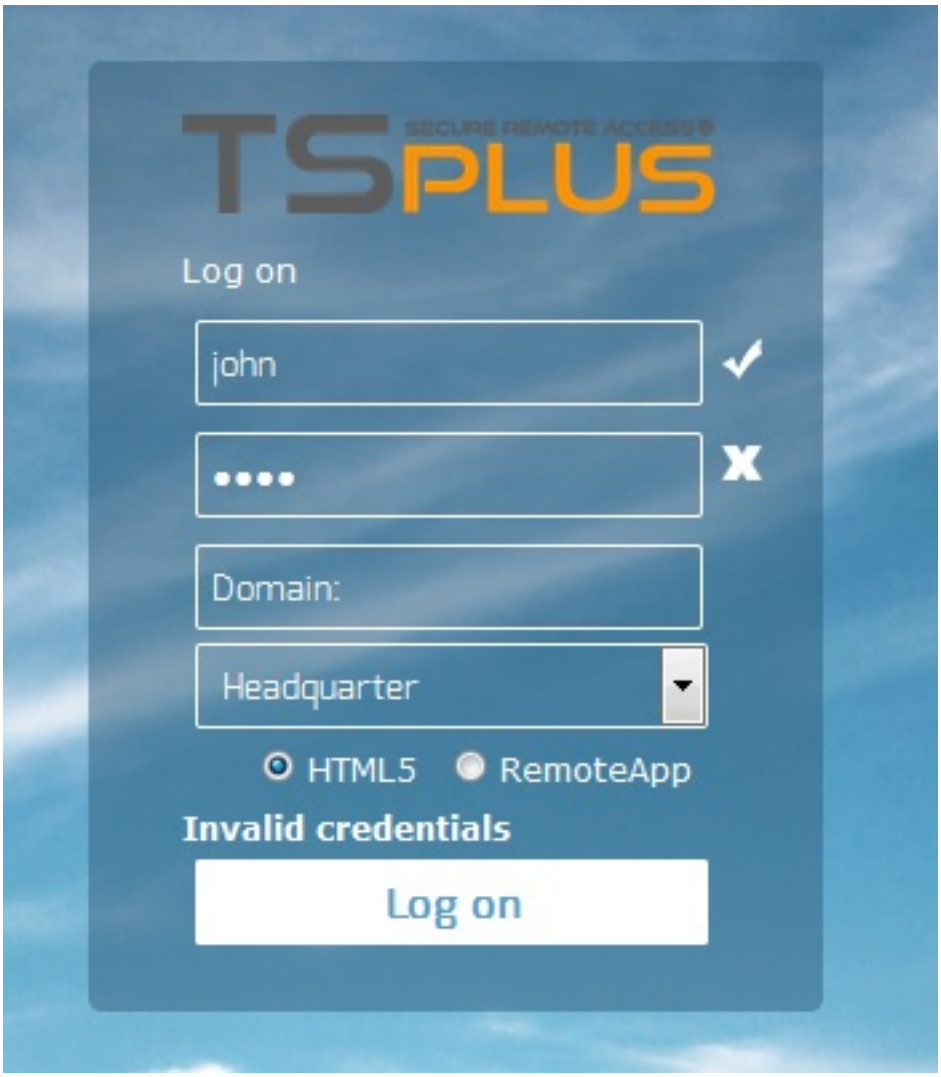
- Das obige Beispiel gilt für eine Domäne oder eine Arbeitsgruppe.
- Wenn Sie eine Arbeitsgruppe verwenden, müssen die Benutzeranmeldungen auf jedem Anwendungsserver, den Sie zuweisen, gleich sein.
- Diese Serverzuweisungsfunktion kann konfiguriert und gleichzeitig mit der Lastenausgleichsfunktion verwendet werden, sodass der Farmcontroller auf zugewiesenen Servern Lastenausgleich durchführen kann. Aktivieren Sie dazu den Lastenausgleich und aktivieren Sie die Option „Lastenausgleich auf zugewiesenen Servern“.
- Wenn die Funktion zur Serverzuweisung und das Lastenausgleich aktiviert sind, wird der Gateway-Server die Benutzer an den am wenigsten ausgelasteten Server weiterleiten, es sei denn, die Option „Lastenausgleich auf zugewiesenen Servern“ in der Konfiguration des Lastenausgleichs ist aktiviert.

Beispiel dafür, was Sie erhalten, wenn Benutzer sich mit dem Gateway verbinden.

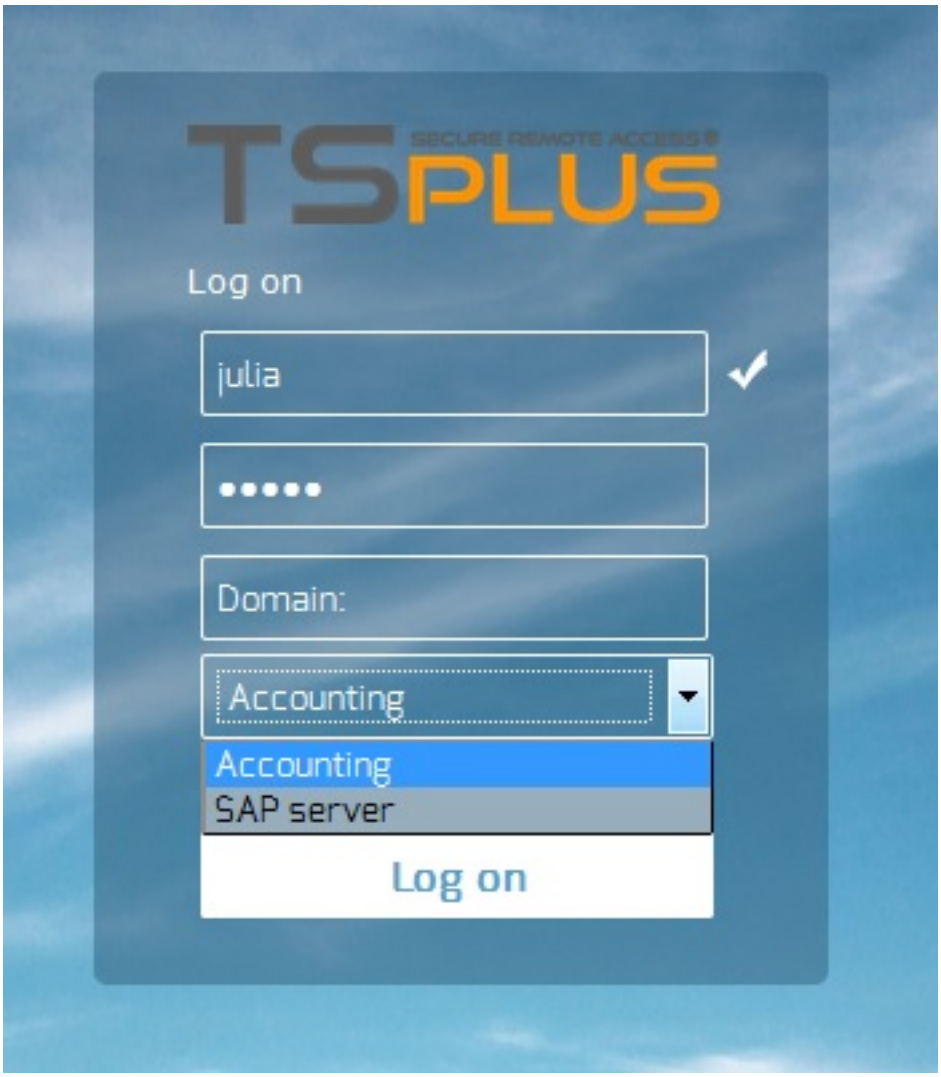
John kann den Server auswählen. Er möchte und er wird sich automatisch bei diesem Server anmelden:



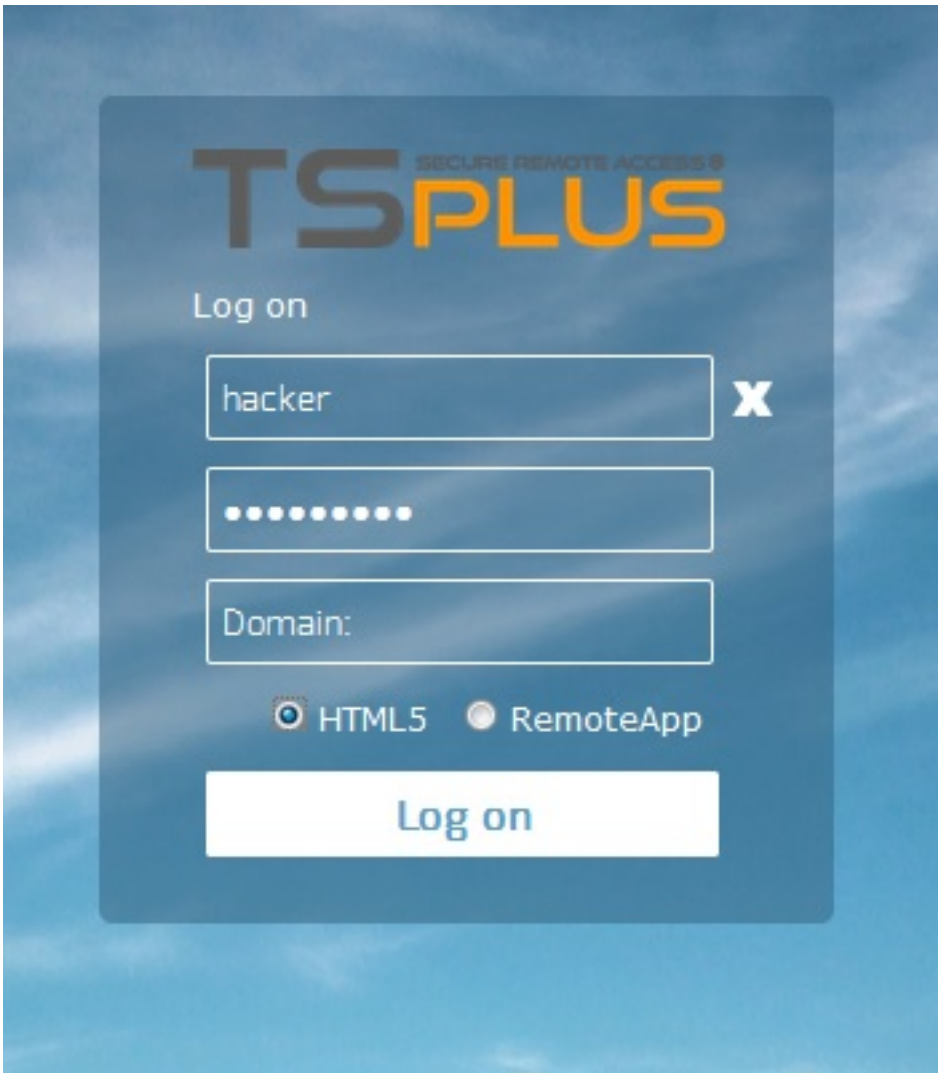
Wenn er ein falsches Passwort eingibt, muss John sein Passwort erneut eingeben:



Julia hat eine andere Liste möglicher Server:



Jemand versucht, das Gateway zu hacken. Er sieht keinen Server und das Gateway blockiert seinen Webzugang.

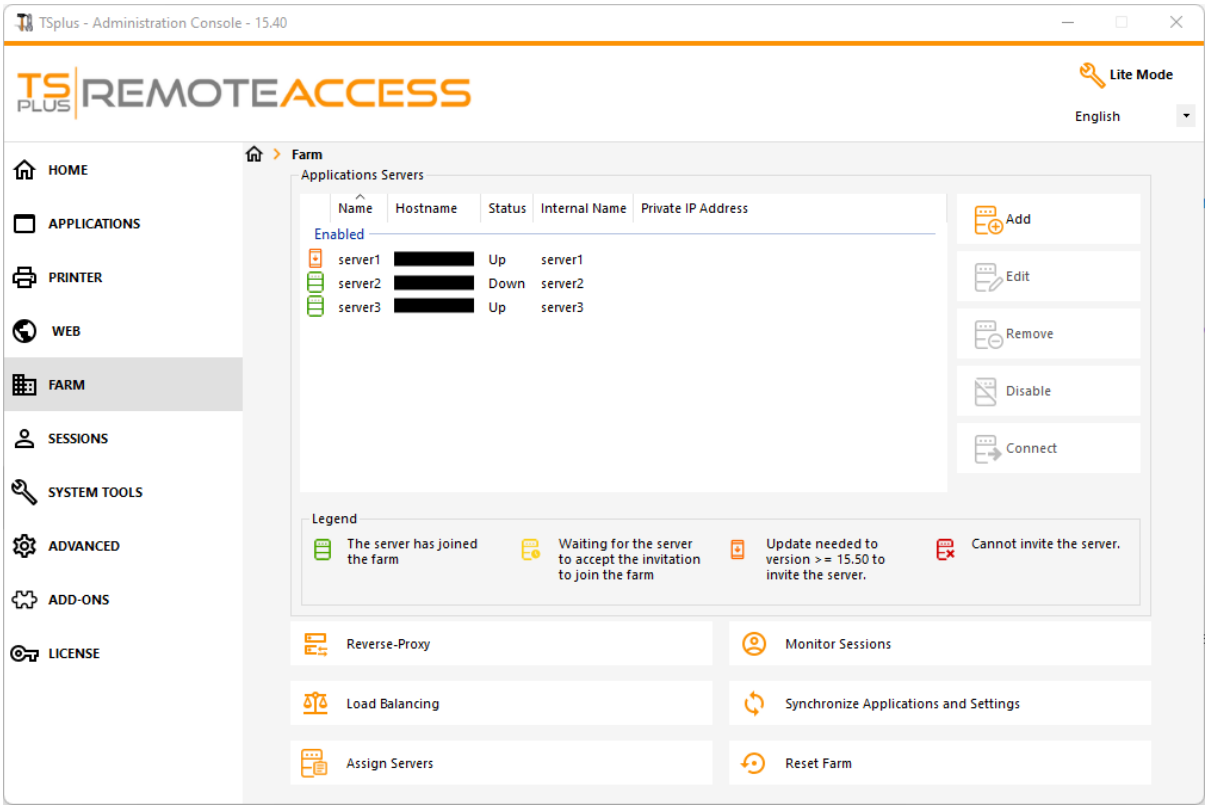

TSPLUS
SECURE REMOTE ACCESS
Log on
hacker
Domain:
HTML5
RemoteApp
Log on

Farm Einrichtung

Übersicht

Um eine Farm zu erstellen, müssen Sie einfach Anwendungsserver aus dem TSplus AdminTool hinzufügen.

Sie werden in der Sektion „Farm“ des AdminTools in der Lage sein, Anwendungsserver zu verwalten.



Von diesem Fenster aus können Sie mehrere Aktionen durchführen:

- “ Hinzufügen : eine neue Anwendungsserver hinzufügen
- “ Bearbeiten ”: Bearbeiten Sie den ausgewählten Server.
- “ Entfernen : den ausgewählten Server dauerhaft aus dem Farm entfernen (Sie können ihn später mit der Schaltfläche „Hinzufügen“ wieder hinzufügen).

- “ Deaktivieren/Aktivieren ”: Temporär den ausgewählten Server deaktivieren oder aktivieren (Benutzer können sich nicht mit diesem Server verbinden).
- “ Verbinden ”: Öffnen Sie den standardmäßigen RDP-Client und verbinden Sie sich automatisch mit dem ausgewählten Server. Wenn Ihre Anmeldeinformationen in MSTSC gespeichert sind, werden diese verwendet, andernfalls müssen Sie Ihre Anmeldeinformationen eingeben.

Sie können diese Aktionen auch über das Kontextmenü aufrufen, das mit einem Rechtsklick auf einen Server angezeigt wird.

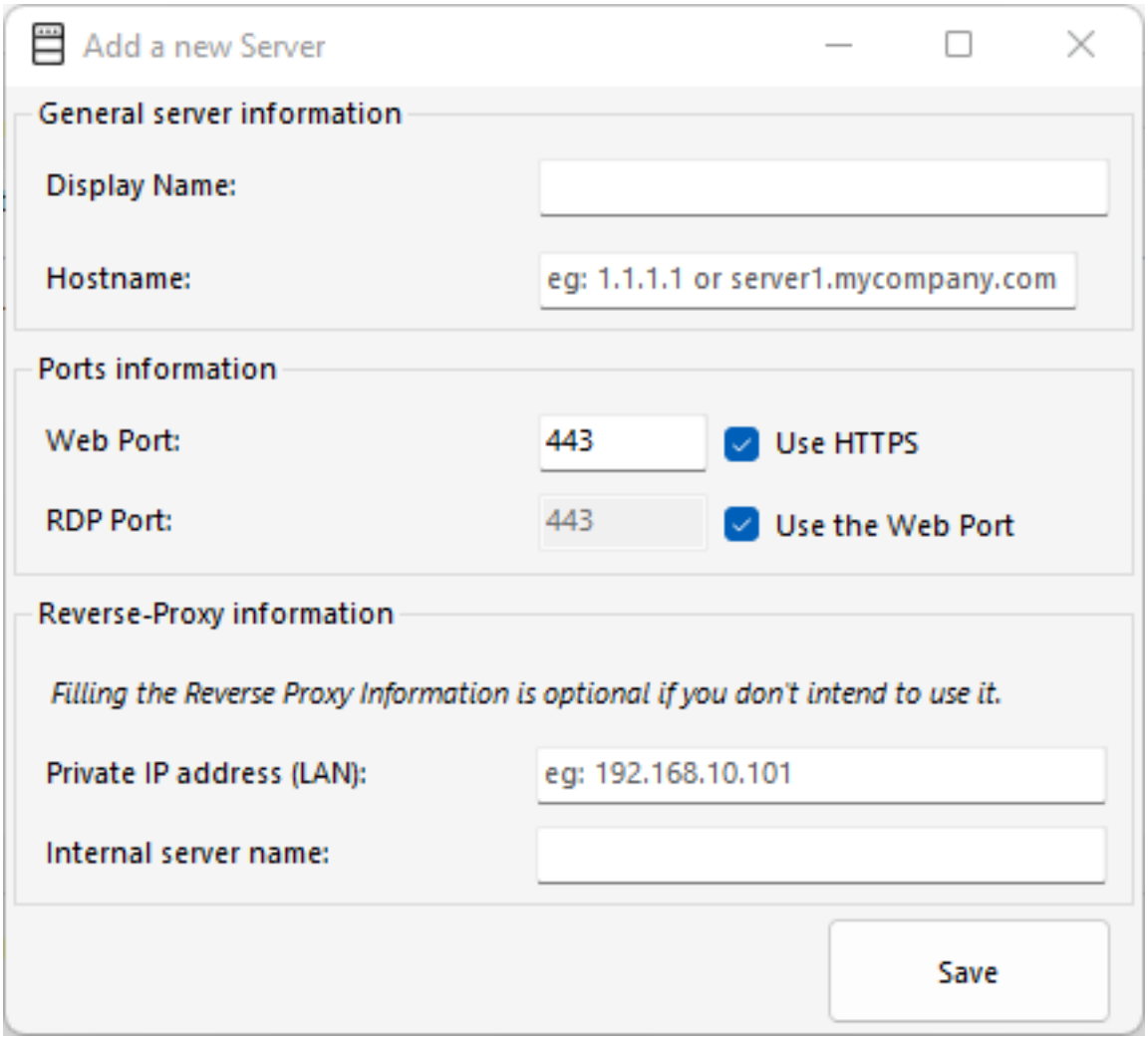
Im unteren Bereich finden Sie einen schnellen Zugriff auf die Hauptfunktionen der Farm, die verfügbar sind, sobald Anwendungserver hinzugefügt wurden:

- „Lastenausgleich“: ermöglicht es Ihnen, Benutzer, die sich vom Gateway-Server verbinden, zum am wenigsten ausgelasteten Server des Clusters umzuleiten.
- „Reverse Proxy“: ermöglicht es Ihnen, nur den Gateway-Server freizugeben und macht Anwendungsserver über URLs wie zugänglich https://gateway-server-domain-or-ip-address/~~anwendungsserver-internal-name
- “Server zuweisen”: ermöglicht es Ihnen, die verfügbaren Anwendungsserver für Benutzer und Gruppen einzuschränken, wenn sie sich vom Gateway-Server aus verbinden, sodass sie den Server auswählen können, mit dem sie sich verbinden möchten, wenn mehrere Server zugewiesen sind.
- “Sitzungen überwachen” * ermöglicht es Ihnen, die aktuellen Sitzungen zu überwachen und schnell Aktionen wie Trennen, Abmelden, Nachricht senden, Sitzung anzeigen oder Sitzung steuern auszuführen.
- Synchronisieren Sie Anwendungen und Einstellungen * ermöglicht es Ihnen, alle erweiterten Einstellungen und veröffentlichten Anwendungen auf die ausgewählten Anwendungsserver zu übertragen
- „Farm zurücksetzen“: ermöglicht es Ihnen, die Farm zurückzusetzen, wodurch alle Server entfernt und alle Farmfunktionskonfigurationen zurückgesetzt werden, z. B. die Konfigurationen „Reverse Proxy“, „Lastenverteilung“ und „Server zuweisen“.

* Diese Funktionen sind nur für Anwendungsserver zugänglich, die aus Sicherheitsgründen vollständig dem Farm beigetreten sind, was bedeutet, dass Sie zunächst die Einladung akzeptieren müssen, die von Ihrem Farm-Controller an den Anwendungsserver gesendet wurde.

Fügen Sie einen Anwendungsserver zum Farm hinzu

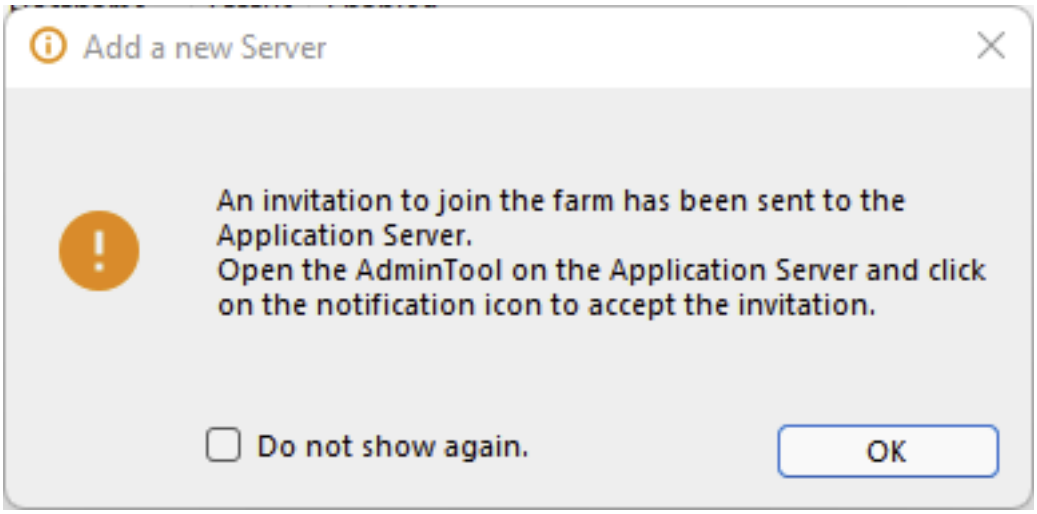
Um einen Anwendungsserver hinzuzufügen, klicken Sie auf die Schaltfläche „Hinzufügen“. Das folgende Fenster wird angezeigt:



Sie müssen den Anzeigenamen und den Hostnamen angeben (Sie können eine IP oder einen Domainnamen ohne Portnummer eingeben).
Das Ausfüllen der Informationen zu den Reverse-Proxy-Feldern ist nur optional, wenn Sie die Reverse-Proxy-Funktion derzeit nicht verwenden.
Der interne Name wird automatisch mit einem verfügbaren Anzeigenamen ausgefüllt, wenn er leer ist, um die gesamte Serverkonfiguration zu erleichtern.

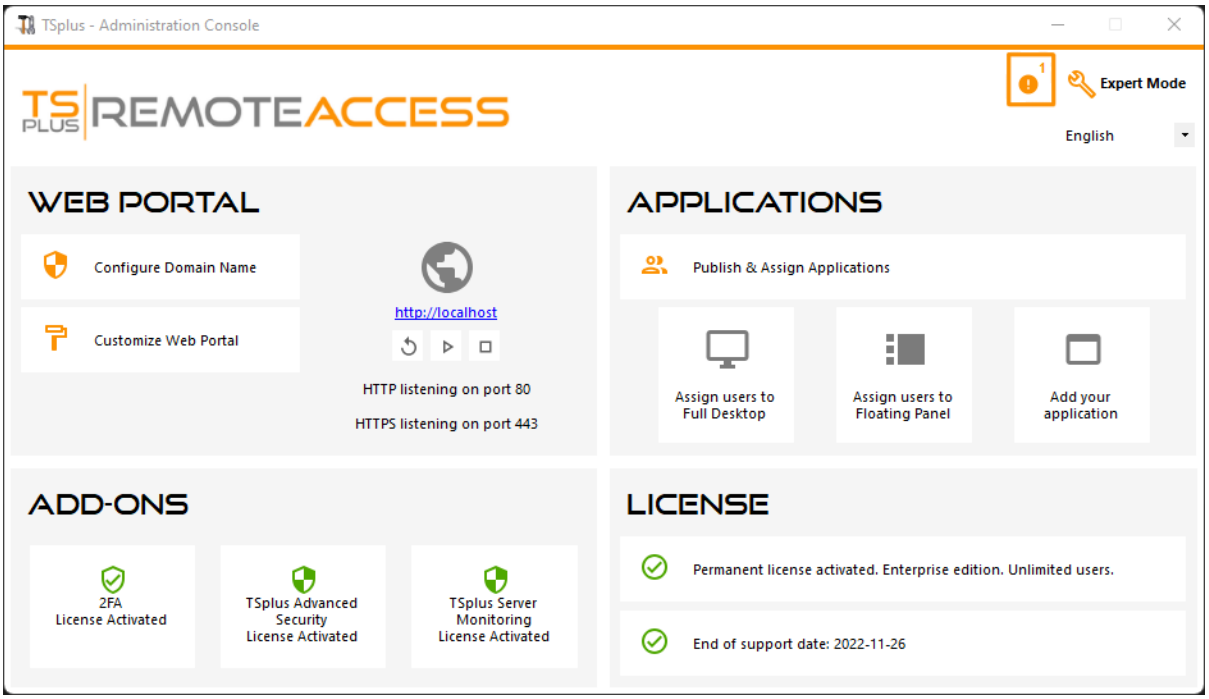
WICHTIG: Die RDP-Port-Option „Webport verwenden“ gibt an, dass Sie die RDP-Port-Weiterleitungsfunktion (standardmäßig aktiviert), die vom Webserver des Anwendungsservers angeboten wird, nutzen möchten.
Als Ergebnis, wenn Sie die Option „Webport verwenden“ nutzen möchten, stellen Sie bitte sicher, dass auf dem hinzugefügten Anwendungsserver die Option „RDP-Weiterleitung deaktivieren“ im AdminTool > Erweitert > Sicherheit auf „Nein“ gesetzt ist.

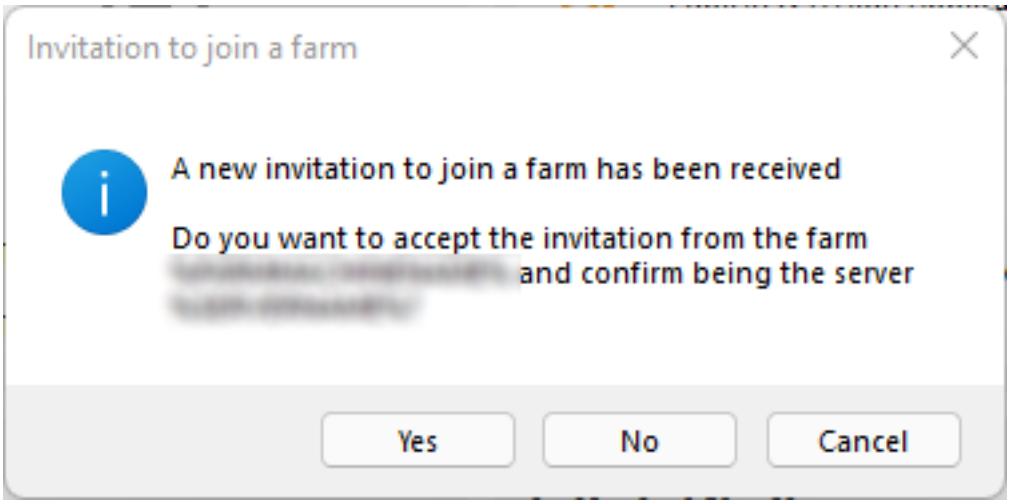
Geben Sie die Details des Anwendungsservers ein und klicken Sie dann auf die Schaltfläche „Speichern“. Eine Einladung zum Beitritt zur Farm wird an den hinzugefügten Anwendungsserver gesendet.



Das Akzeptieren dieser Einladung auf der Anwendungsserver-Seite ist erforderlich, wenn Sie die Funktionen „Sitzungen überwachen“ und „Anwendungen und Einstellungen synchronisieren“ aus Sicherheitsgründen nutzen möchten.
Es ist jedoch nicht erforderlich, wenn Sie nur die Funktionen „Reverse Proxy“, „Loadbalancing“ und „Server zuweisen“ verwenden müssen.

Um die Einladung anzunehmen, öffnen Sie eine Administrator-Sitzung. **auf dem Anwendungsserver** Sie haben zur Farm hinzugefügt. Klicken Sie auf die Alarmtaste in der oberen rechten Ecke des TSplus AdminTool und klicken Sie dann auf „Ja“:





Auf der Seite des Farm Controllers können Sie die Liste der Anwendungsserver in der Farm sehen. Sie können drei Zustände haben, die durch farbige Symbole dargestellt werden:

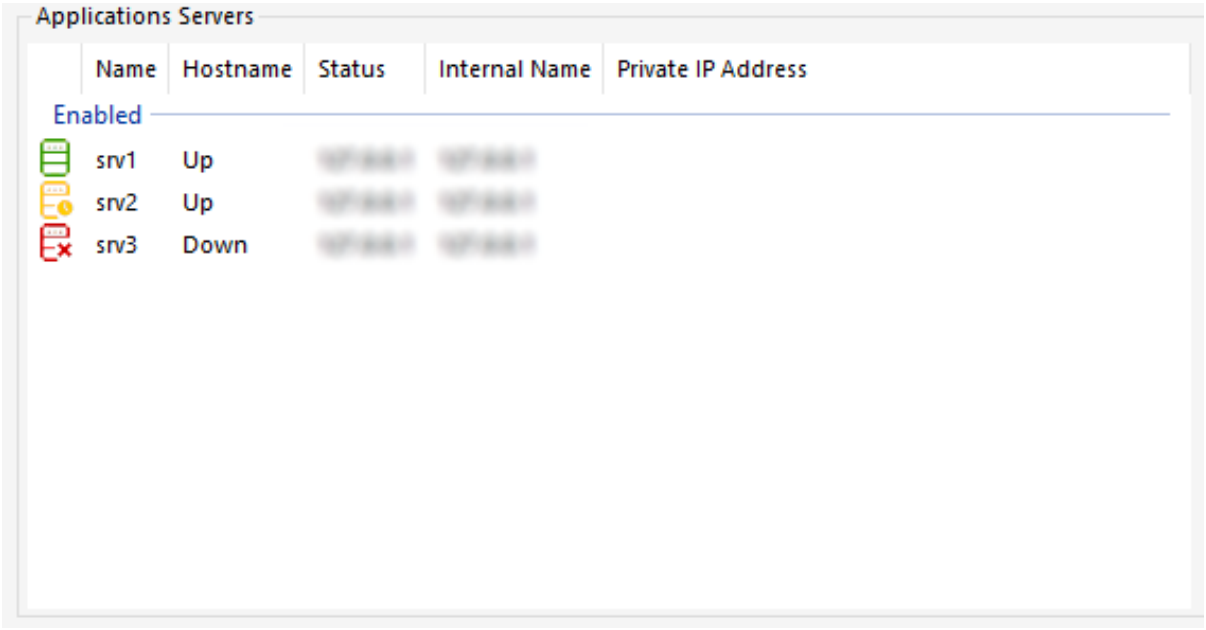
- Beigetreten Der Anwendungsserver hat die Farm vollständig beigetreten, indem er die Einladung angenommen hat.

- Ausstehend Der Anwendungsserver hat sich teilweise dem Farm angeschlossen und wartet darauf, dass der Anwendungsserver die Einladung annimmt.

- Aktualisierung erforderlich Der Anwendungsserver hat sich teilweise dem Farm angeschlossen, aber die Einladung kann nicht gesendet werden, da der Server eine TSplus Remote Access-Version < 15.50 verwendet.

- Unerreichbar Der Anwendungsserver hat sich teilweise dem Farm angeschlossen, aber die

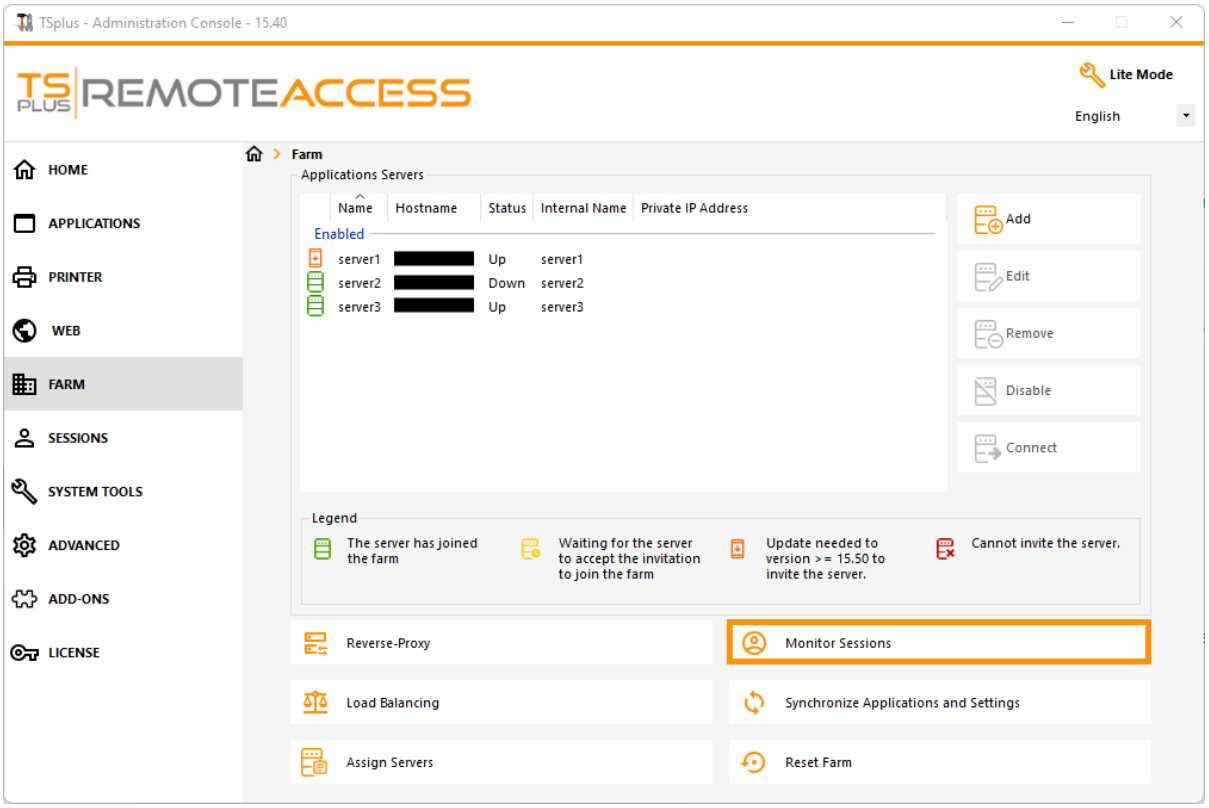
Einladung kann nicht gesendet werden, da der Server nicht erreichbar ist.



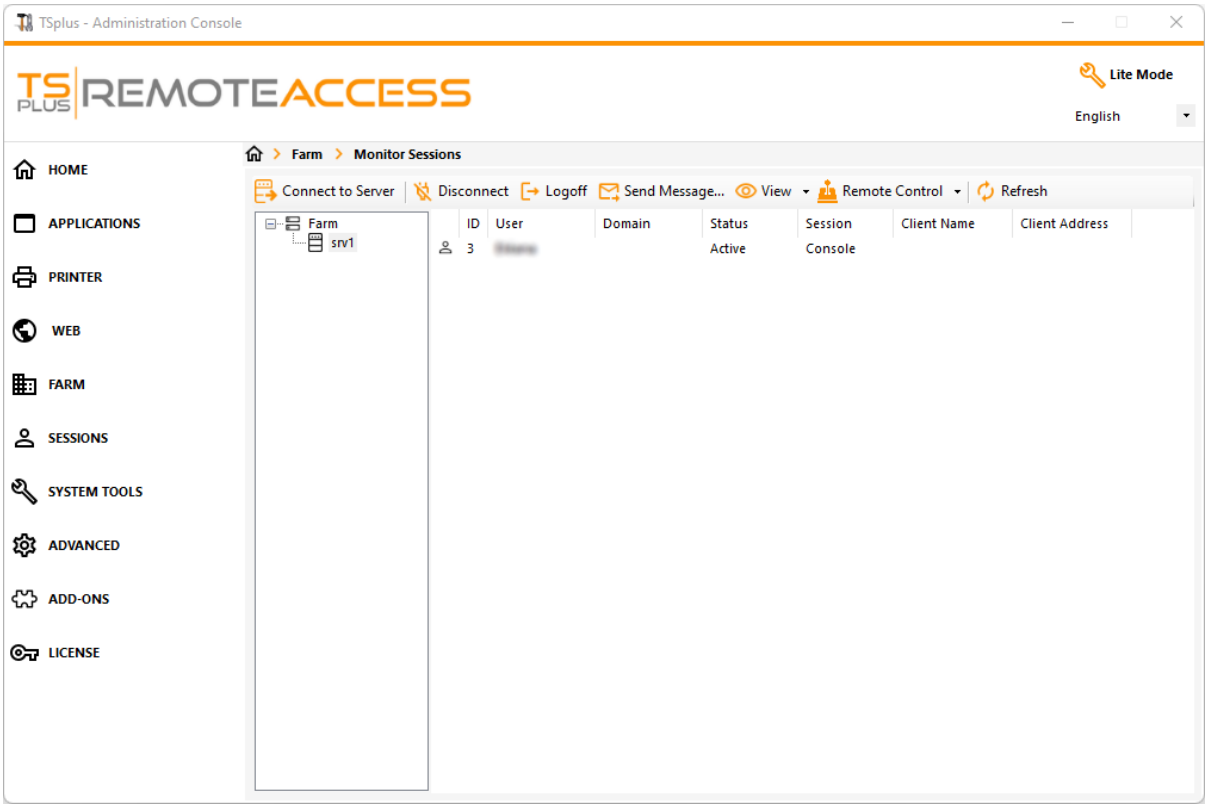
Sitzungen überwachen

Übersicht

Sie können auf die Überwachungs-Sitzungsoberfläche über den FARM-Tab zugreifen:



Klicken Sie auf die Schaltfläche „Sitzungen überwachen“, um den folgenden Tab anzuzeigen:



In diesem Tab können Sie die Liste der Benutzersitzungen auf jedem Anwendungsserver der Farm einsehen.
Klicken Sie auf einen Anwendungsserver im linken Bereich, um ihn auszuwählen und die aktuellen aktiven Benutzersitzungen anzuzeigen. Sobald sie angezeigt werden, können Sie eine oder mehrere Sitzungen auswählen und mehrere Aktionen durchführen, indem Sie auf eine der folgenden Schaltflächen klicken.

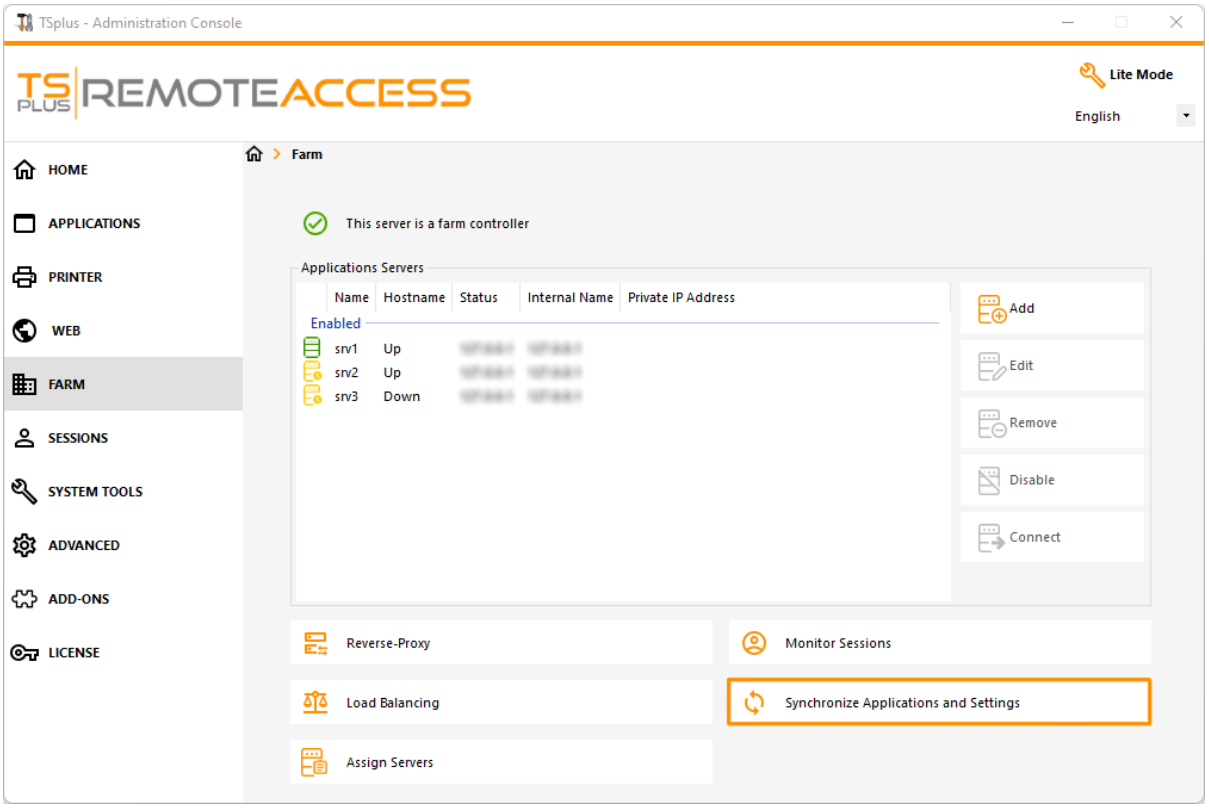
- “Disconnect”: die ausgewählte Benutzer-Sitzung(en) trennen (der Benutzer kann weiterhin auf seine Sitzung zurückverbinden).
- „Abmelden“: die ausgewählte Benutzersitzung(en) abmelden (alle nicht gespeicherten Änderungen gehen verloren, Anwendungen werden abrupt geschlossen).
- „Nachricht senden“: ein Fenster anzeigen, um einen Titel und einen Text einzugeben, und dann diese Nachricht an die ausgewählte(n) Benutzersitzung(en) senden.
- “Ansicht”: Ansicht einer ausgewählten Benutzersitzung mit/ohne***** Berechtigungen.
- „Fernsteuerung“: Steuern Sie eine ausgewählte Benutzersitzung mit/ohne***** Berechtigungen.
- “Aktualisieren”: Führen Sie eine vollständige Aktualisierung der Liste der Benutzersitzungen für den/die ausgewählten Server aus.

* Um eine Sitzung anzuzeigen oder zu steuern **ohne Berechtigungen** , Sie müssen **Ändern Sie die folgende GPO auf dem Anwendungsserver, dessen Sitzungen Sie anzeigen und/ oder steuern möchten.** .
GPO-Standort: Computer Configuration> Administrative Templates> Windows Components> Remote Desktop Services> Remote Desktop Session Host > Connections .
GPO-Schlüssel: Regeln für die Fernsteuerung von Benutzer-Sitzungen der Remote Desktop Services festlegen

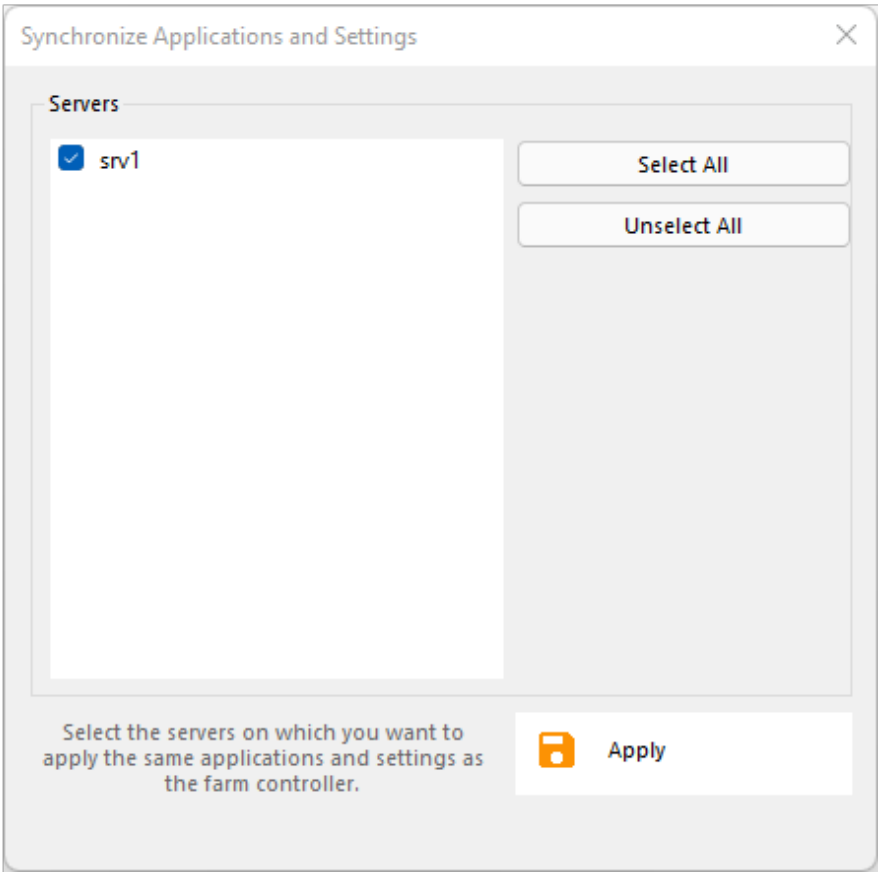
Die Liste der Benutzersitzungen wird alle 5 Sekunden automatisch aktualisiert. Diese automatische Aktualisierung stoppt, wenn der ausgewählte Server nicht mehr verfügbar ist. Ein Klick auf die Schaltfläche „Aktualisieren“ setzt die automatische Aktualisierung fort.

Anwendungen und Einstellungen Synchronisierung

Übersicht

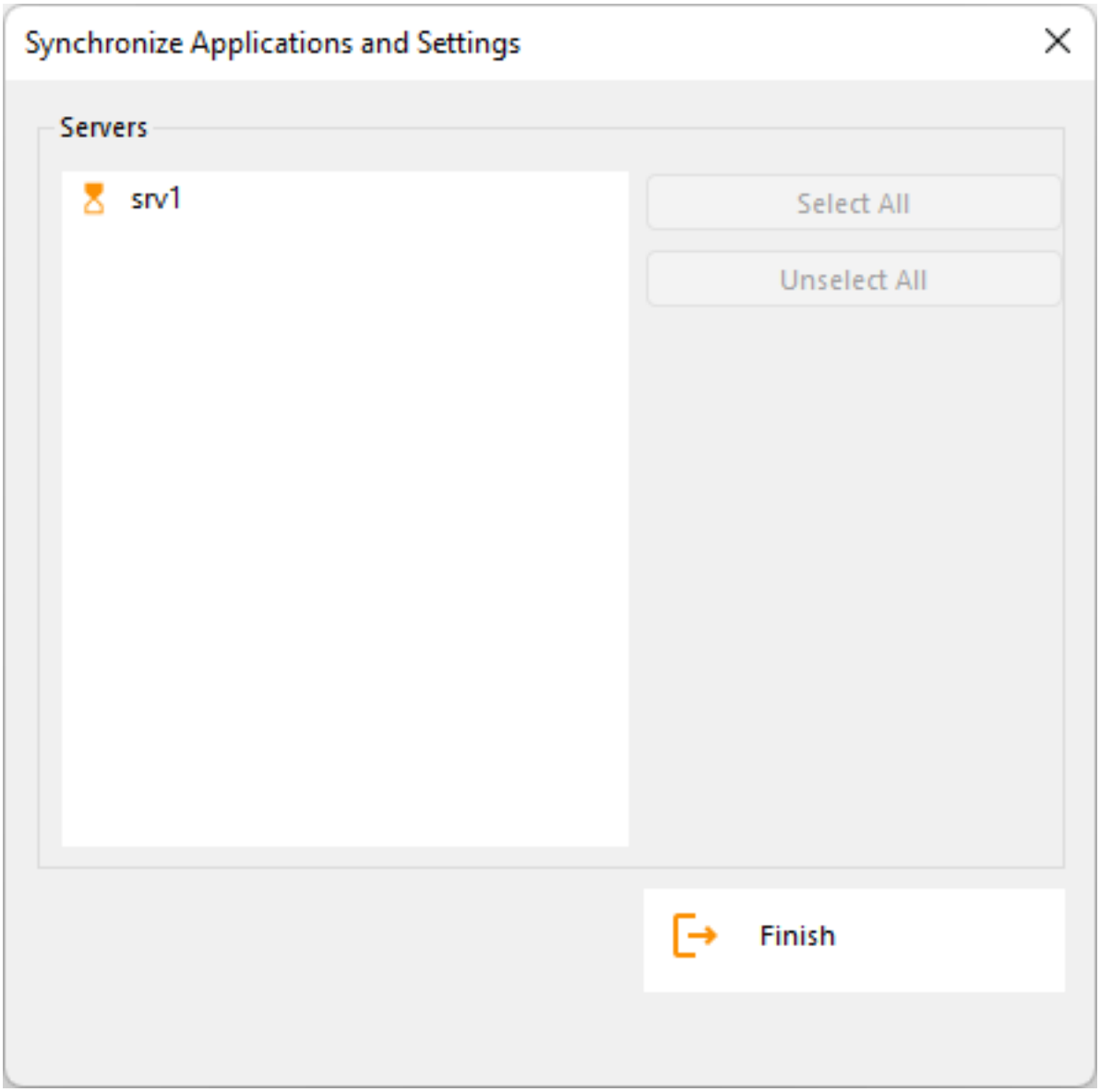


Klicken Sie auf die Schaltfläche „Anwendungen und Einstellungen synchronisieren“, um das folgende Fenster anzuzeigen:



Überprüfen Sie alle Server, auf denen Sie die gleichen Einstellungen anwenden und die gleichen Anwendungen wie die des Farm Controllers veröffentlichen möchten, und klicken Sie dann auf „Übernehmen“.

Das folgende Fenster wird angezeigt, das es Ihnen ermöglicht, den Fortschritt der Aufgabe zu überwachen:


Synchronize Applications and Settings
Servers
srv1
Select All
Unselect All
Finish

Schnelle und einfache Dateiübertragung zwischen dem Benutzer und dem Server

Übersicht

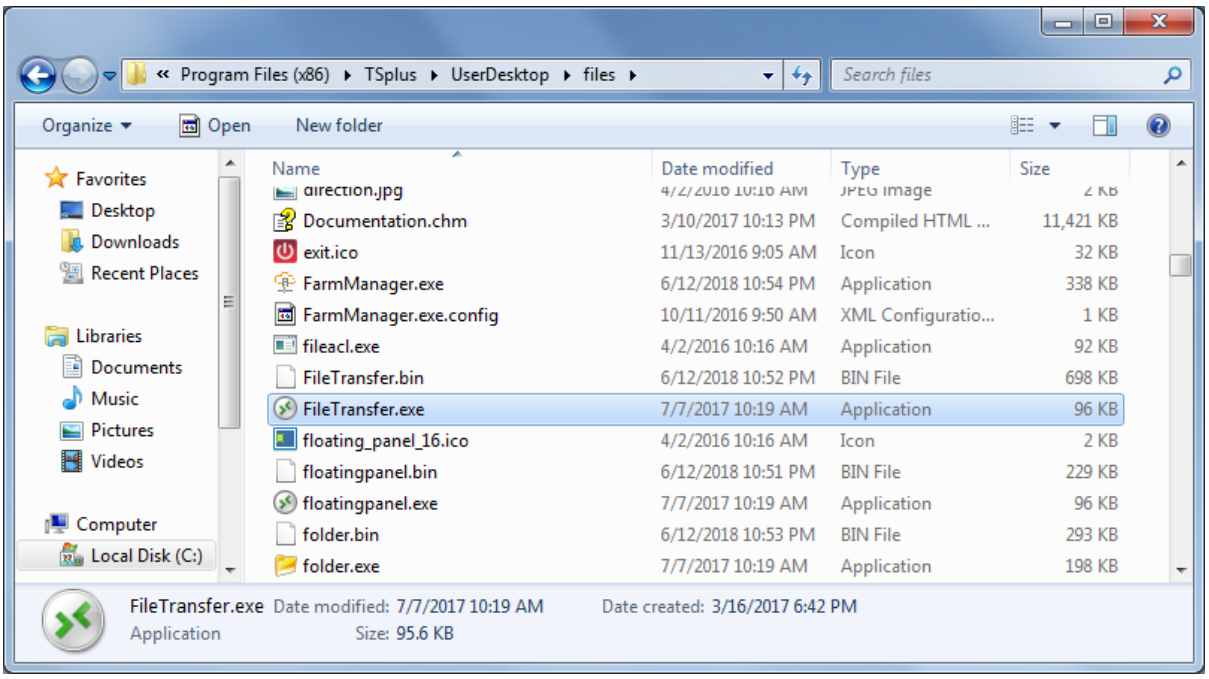
TSplus bietet eine einzigartige Methode zum Übertragen von Dateien:

- von der lokalen Benutzerarbeitsstation => zum Benutzer Remote Desktop
- vom TSplus-Server zum lokalen Benutzer-Desktop

Weil die Dateiübertragungen auf einem virtuellen Kanal basieren, ist es viel schneller als eine Datei kopieren, und es kann durchgeführt werden. **auch wenn die lokalen Benutzerlaufwerke nicht zugeordnet sind** .

Dateiübertragungsprogramm und generierte Clients

Das Programm zur Dateiübertragung befindet sich in Ihrem TSplus-Programmfolder unter dem Namen „FileTransfer.exe“ im folgenden Pfad: „UserDesktop\files“



Dateien übertragen

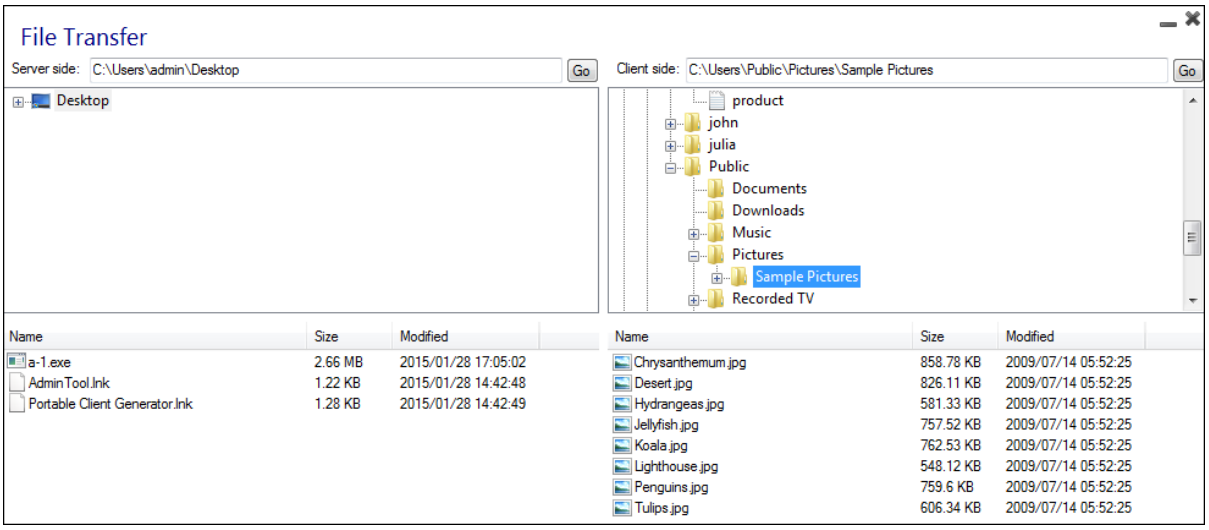
Dateien zu übertragen ist sehr einfach.

Zuerst starten Sie die Dateiübertragung (zum Beispiel über das TSplus Floating Panel):

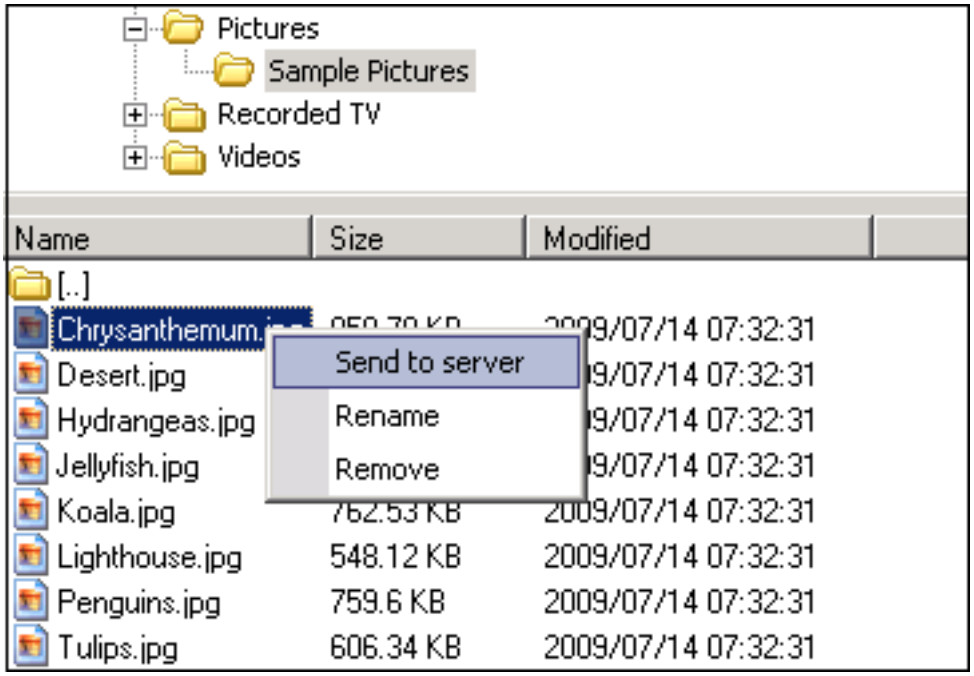


Dann navigieren Sie zu Ihrer Datei über den Ordnerbaum:

- Serverordner und -dateien befinden sich auf dem **linke Fensterseite (Serverseite)**
- Die Ordner und Dateien des lokalen Arbeitsplatzes befinden sich auf dem **rechter Teil des Fensters (Client-Seite)**



Schließlich klicken Sie mit der rechten Maustaste auf die Datei, die Sie auf die andere Seite übertragen möchten, und klicken Sie auf „An Server senden“ (oder „An Client senden“):



Dateiübertragung funktioniert von der lokalen Arbeitsstation zum Server sowie umgekehrt (vom Server zur lokalen Arbeitsstation).

Hinweis Wenn Sie das Dateiübertragungsprogramm aus einer HTML5-Sitzung verwenden, können Sie Ihre Dateien nur vom Server zum Client übertragen. Bitte bevorzugen Sie die HTML5 Top-Menü-Methode , wo Sie Dateien auf den Server hochladen, auf den Client herunterladen und Ihre Dateiübertragungsauflistung verwalten können.

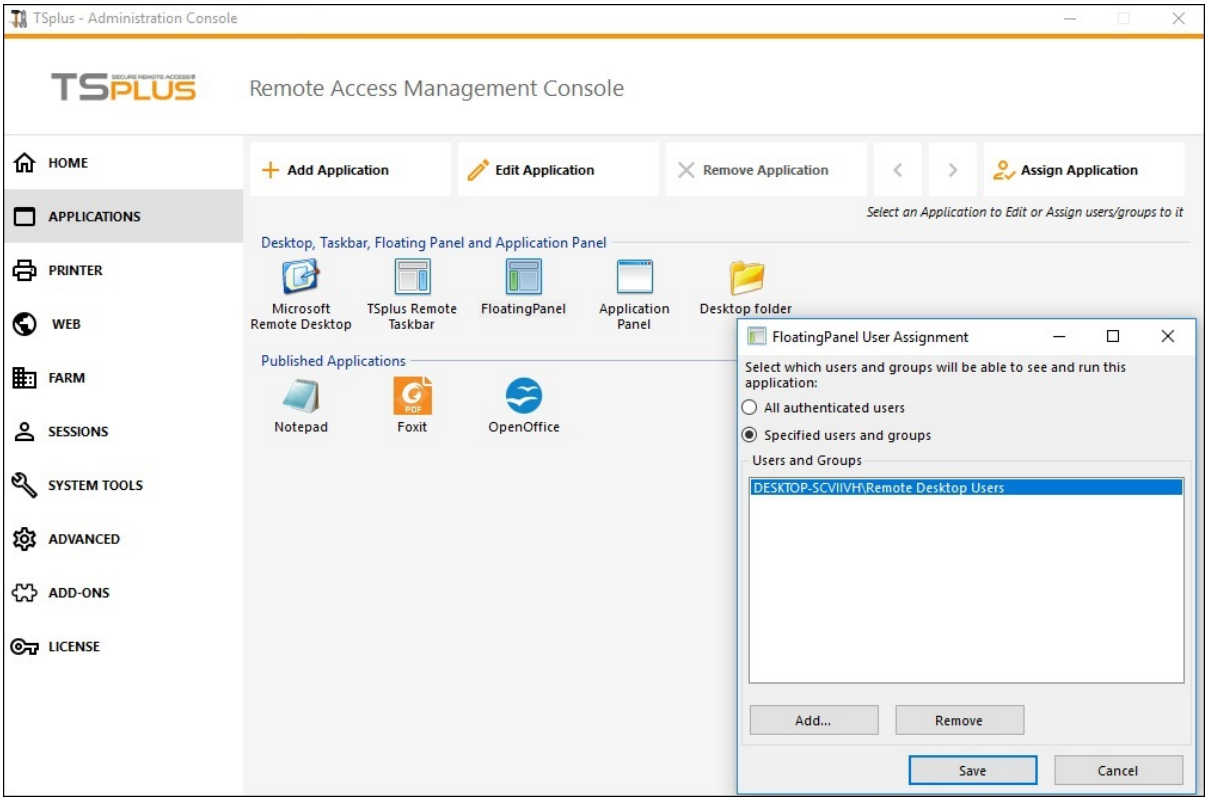
Schwebendes Panel und Anwendungsfenster

Sie können wählen, ob Sie das Floating- oder das Anwendungsfenster für Ihre Benutzer oder Gruppen aktivieren möchten.

Diese beiden Möglichkeiten zur Veröffentlichung von Anwendungen sind für jede Verbindungsart verfügbar.

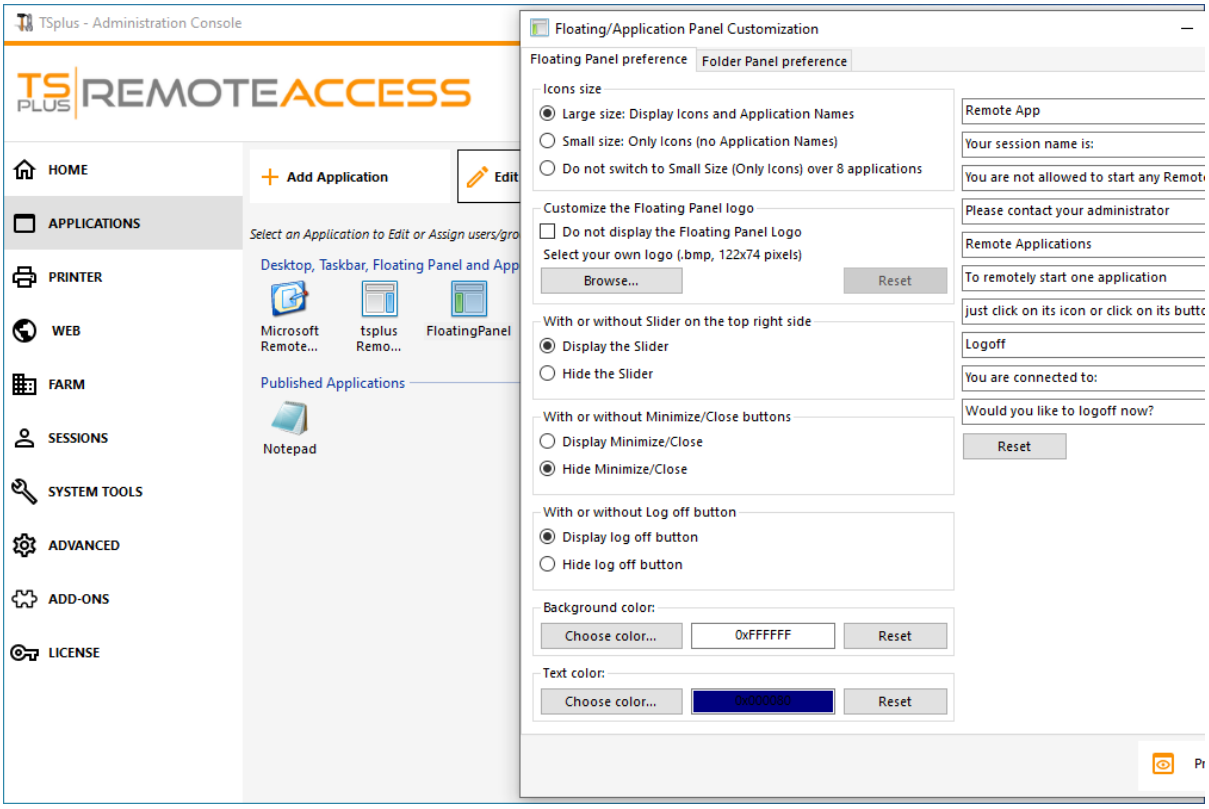
Wenn aktiviert mit den zugewiesenen Anwendungen, können Sie in der Mitte links des Benutzerscreens die Mini-Dropdown-Liste der Anwendungen oder das schwebende Panel sehen (sehr geschätzt von TSplus-Nutzern):

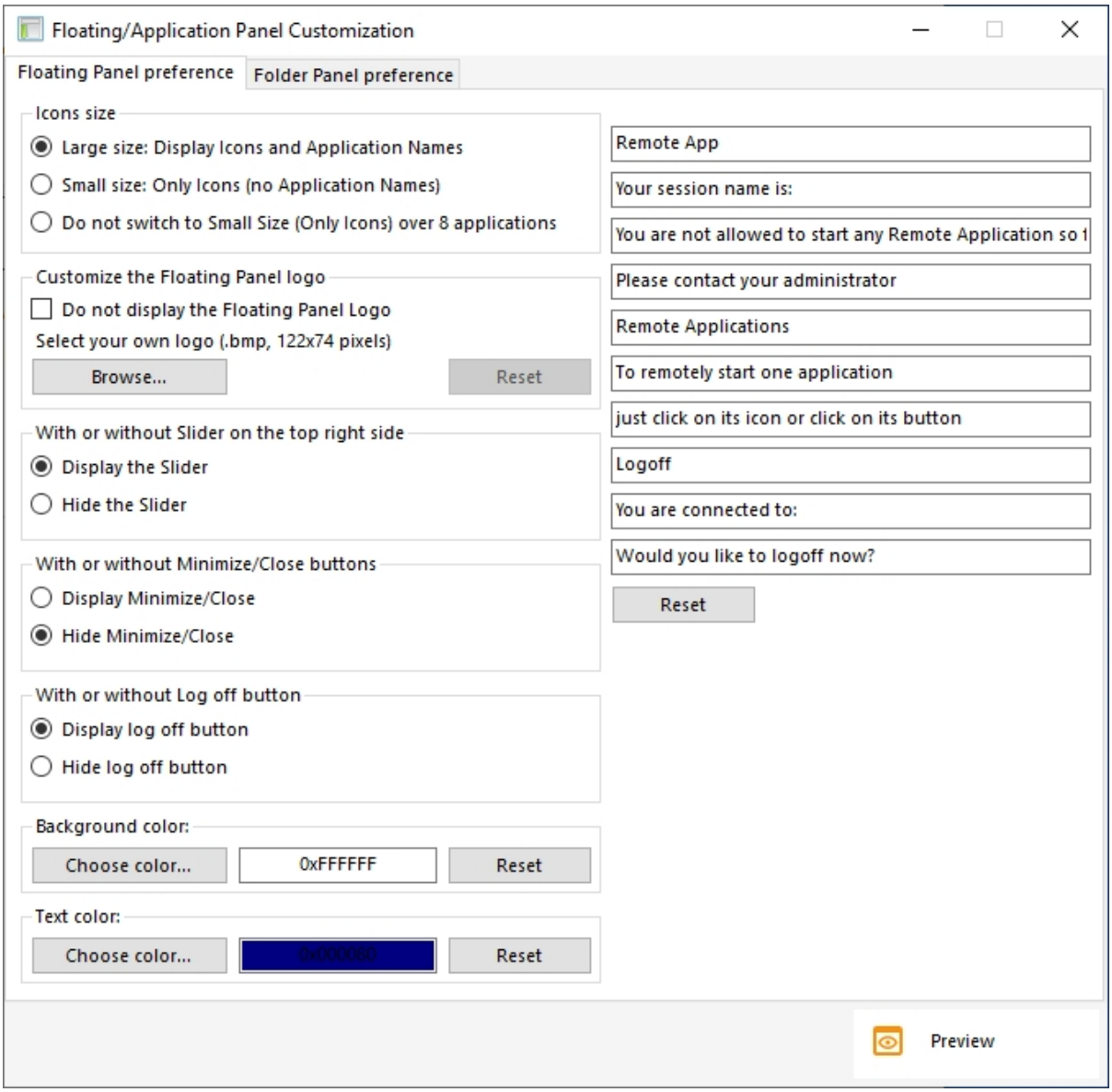
Weisen Sie es als Anwendung zu:



Wählen Sie das schwebende Panel aus und klicken Sie dann auf die Kachel „Anwendung

bearbeiten“, um das schwebende Panel nach Ihren Wünschen anzupassen.





Diese verschiedenen Optionen ermöglichen es Ihnen, die Erfahrung des Endbenutzers anzupassen.

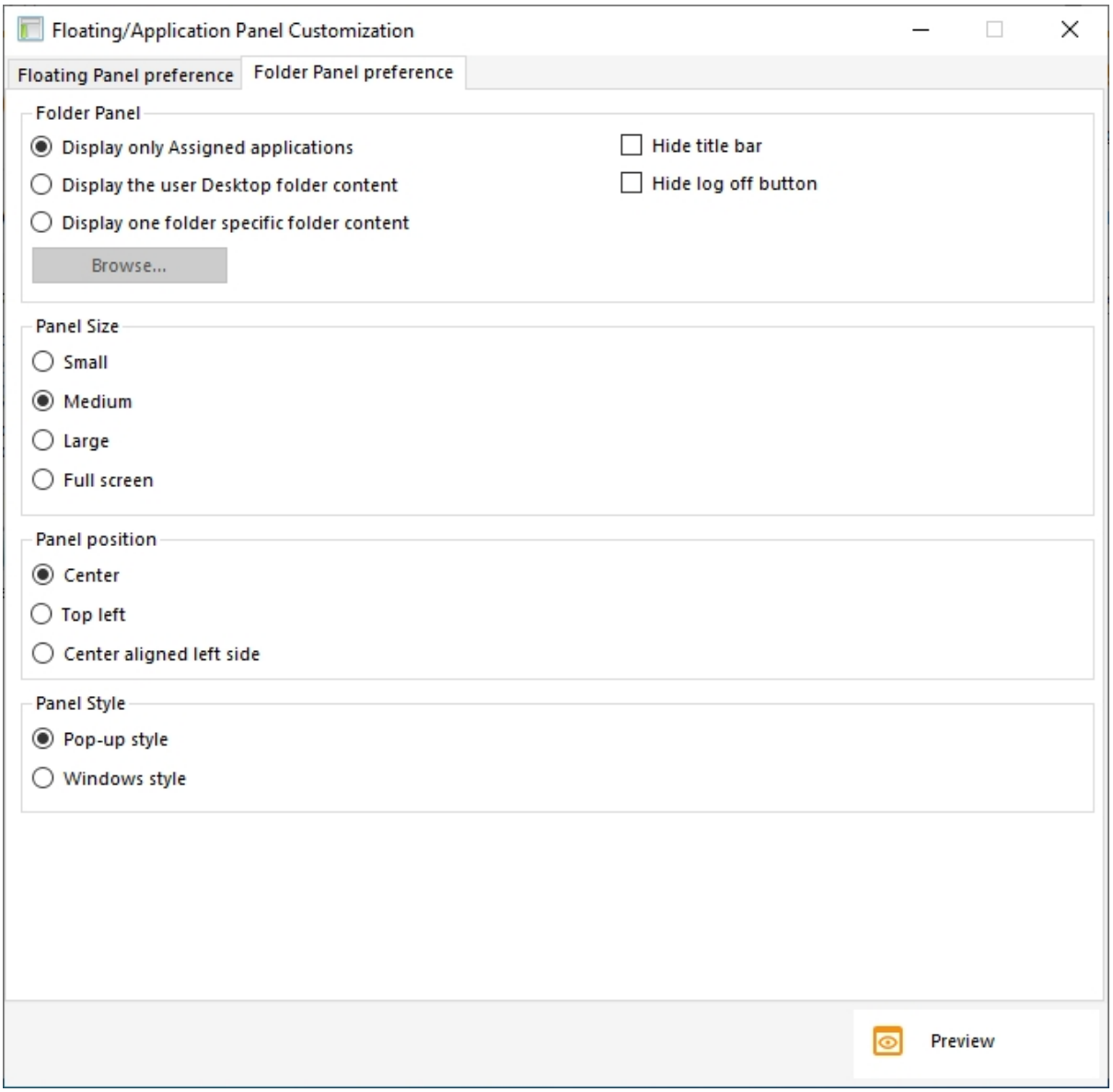
Hier sind die verschiedenen Anzeigeoptionen für das Floating Panel, wo Sie einstellen können,

- Ändern Sie den angezeigten Text,
- Wählen Sie Ihre bevorzugte Größe, zwischen Groß und Klein, in der Sie nur Symbole anzeigen können,
- Fügen Sie Ihr eigenes Logo hinzu,
- Farbe für den Hintergrund und für den Text anpassen,
- Den Schieberegler anzeigen oder nicht,
- Minimieren/Schließen-Schaltflächen anzeigen oder nicht,
- Das Logoff-Symbol anzeigen oder nicht…

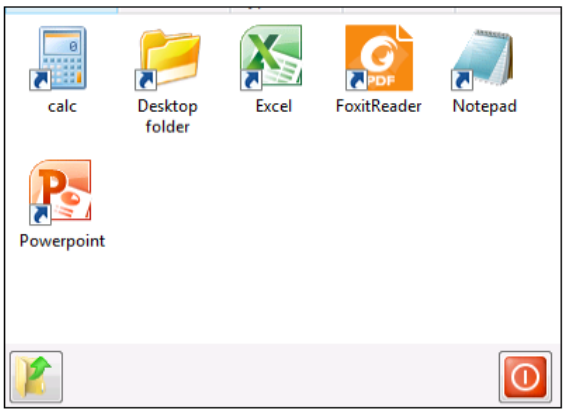


Bitte beachten Sie dass bei über 8 Anwendungen das Floating Panel automatisch auf kleine Größe wechselt. Wenn Sie dennoch möchten, dass die Anwendungsnamen angezeigt werden, wählen Sie „Nicht auf kleine Größe wechseln (nur Symbole) bei über 8 Anwendungen.

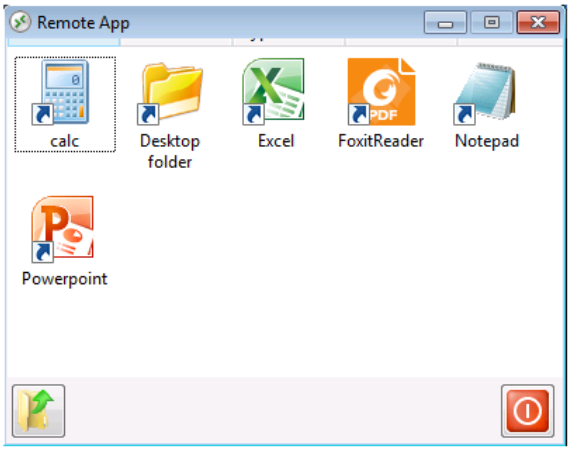
Die **Ordnerpanel** ist ebenfalls anpassbar und ermöglicht die Anzeige der zugewiesenen Anwendungen, des Benutzer-Desktop-Ordners oder des Inhalts eines bestimmten Ordners in Ihrer Sitzung mit vielen Anzeigeoptionen:



Sie können die Größe, Position und den Stil des Ordnerfensters (Popup oder Fenster) nach Belieben ändern:

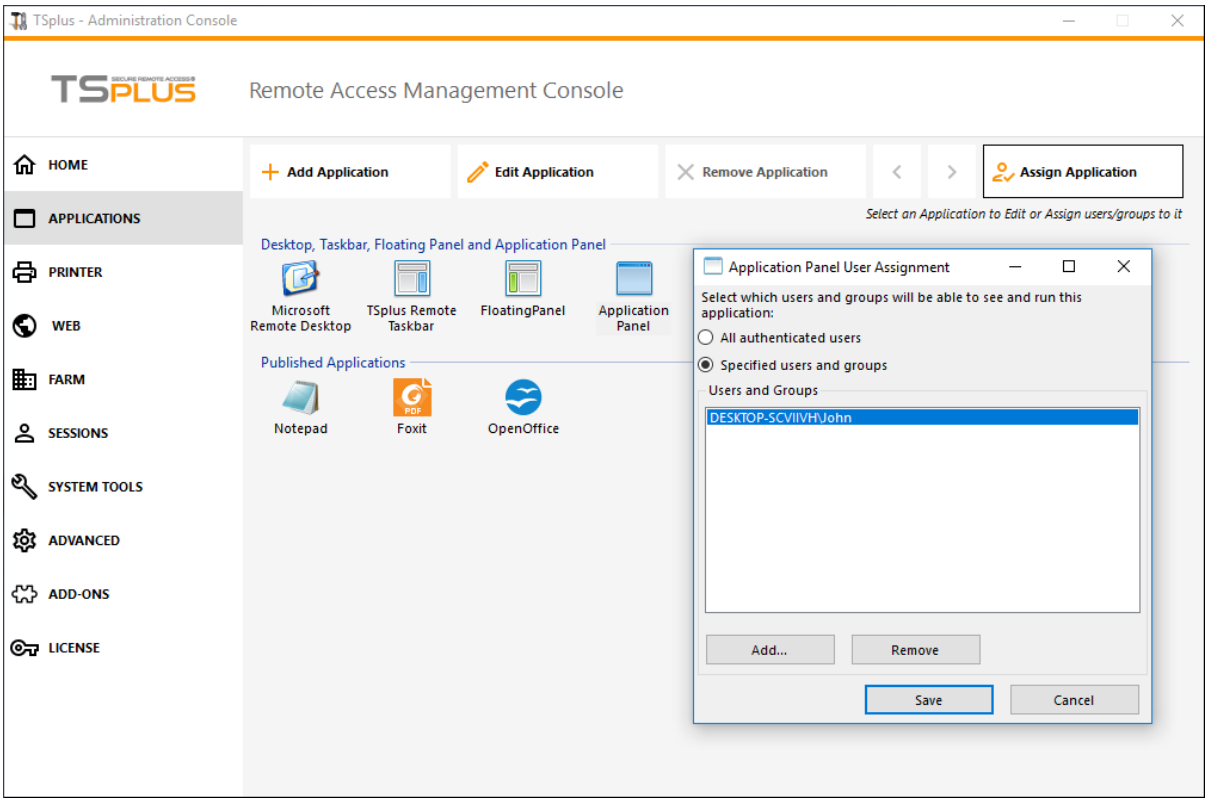


Pop-up style

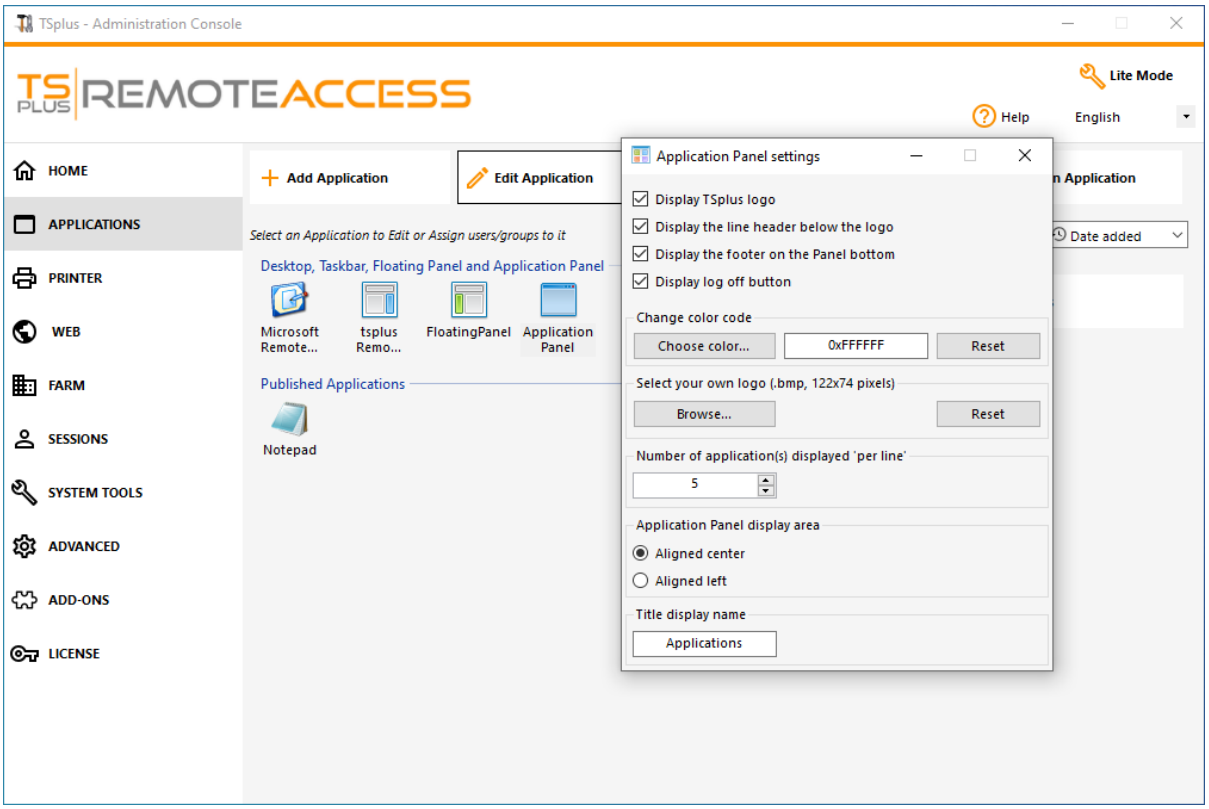


Windows style

Das Anwendungsfeld gibt Ihnen die Möglichkeit, die angezeigten Anwendungen zu organisieren, genau wie im Webanwendungsportal, indem Sie es einfach einem Benutzer oder einer Gruppe zuweisen:



Der Administrator kann es anpassen, indem er wählt, ob das TSplus-Logo oder sein eigenes Logo angezeigt werden soll, die Linienüberschrift unter dem Logo und die Fußzeile anzeigt, die Farbe ändert oder entscheidet, ob er überhaupt etwas davon anzeigen möchte, indem er die entsprechenden Kästchen abwählt. Er kann auch die Anzahl der angezeigten Anwendungen nach Zeilen und Spalten anpassen, indem er die Anzahl der pro Zeile angezeigten Anwendungen eingibt, sowie die Ausrichtung und den Namen des Anwendungsbereichs.



Zum Beispiel, zeigen Sie sechs Apps in einer Spalte ohne Logo an; oder angezeigt in 2 Spalten und 3 Zeilen mit dem TSplus-Logo:


Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

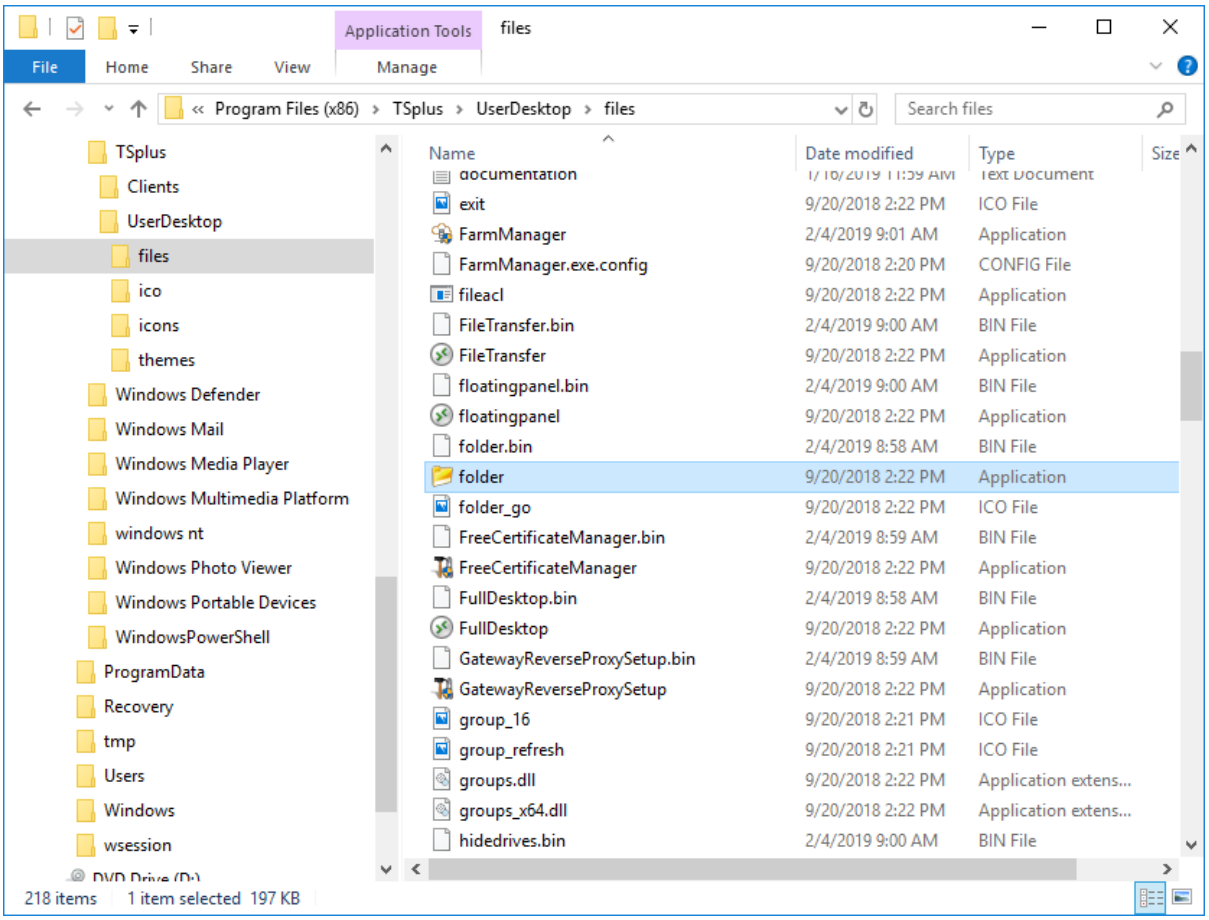

TSPLUS
Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

Sichere Ordnerfreigabe - Folder.exe

Die Ordneranwendung wird den Inhalt eines Ordners sicher anzeigen, den Sie Ihren Benutzern zur Verfügung stellen.

Zuerst erstellen Sie einen Ordner auf Ihrem Server mit Anwendungen oder Dokumenten, die Sie teilen möchten.

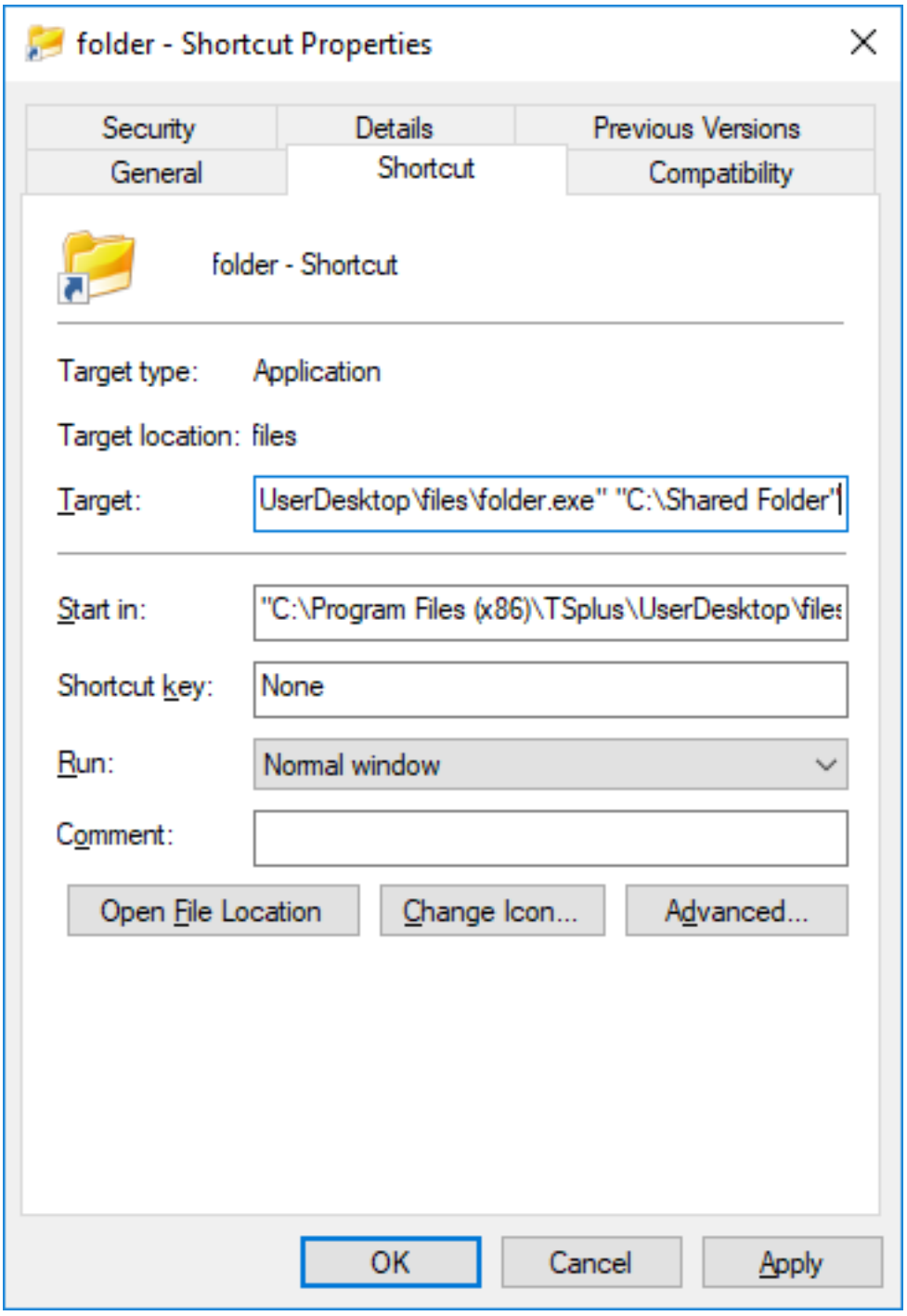
Öffnen Sie eine explorer.exe und suchen Sie die Anwendung folder.exe im Verzeichnis C:\Program Files\tsplus\UserDesktop\files:



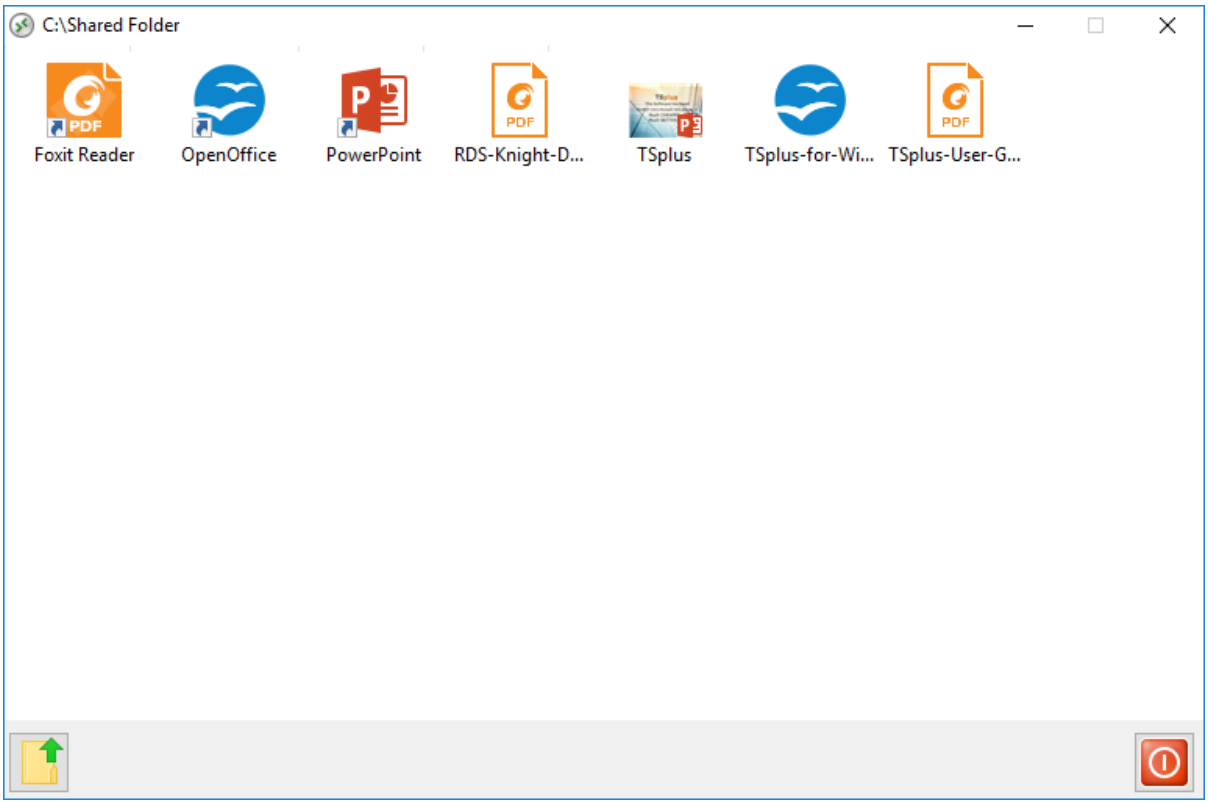
Erstellen Sie eine Verknüpfung zu dieser Datei. Bearbeiten Sie die Eigenschaften dieser Verknüpfung, indem Sie mit der rechten Maustaste darauf klicken.

Dann ändern Sie den Zielpfad der Verknüpfung, indem Sie den Pfad Ihres Anwendungsordners in die Zeile „Ziel“ eingeben, nach dem ursprünglichen Zielpfad, zum Beispiel:

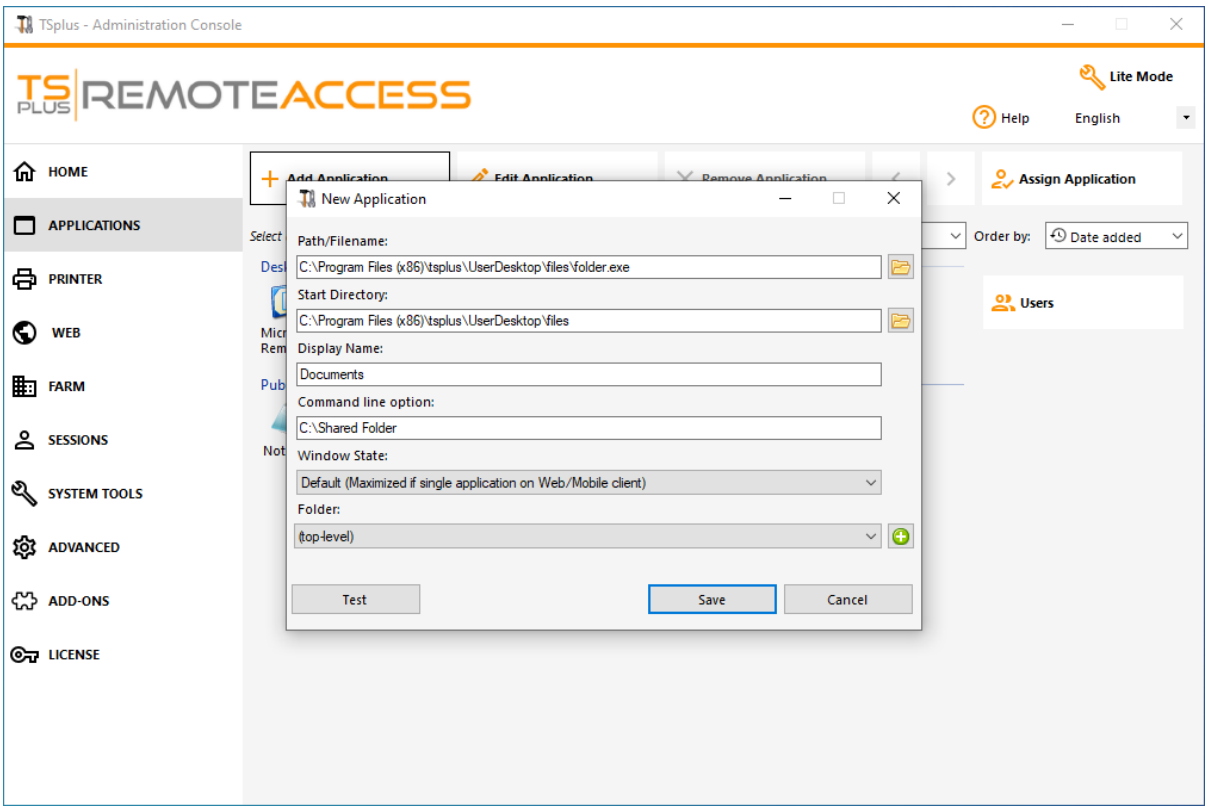
“C:\Program Files\tsplus\UserDesktop\files\folder.exe” “C:\Shared Folder”



Wenn Sie die Verknüpfung zum Ordner.exe öffnen, sollte es so aussehen (mit Ihren eigenen Dokumenten und Anwendungen):



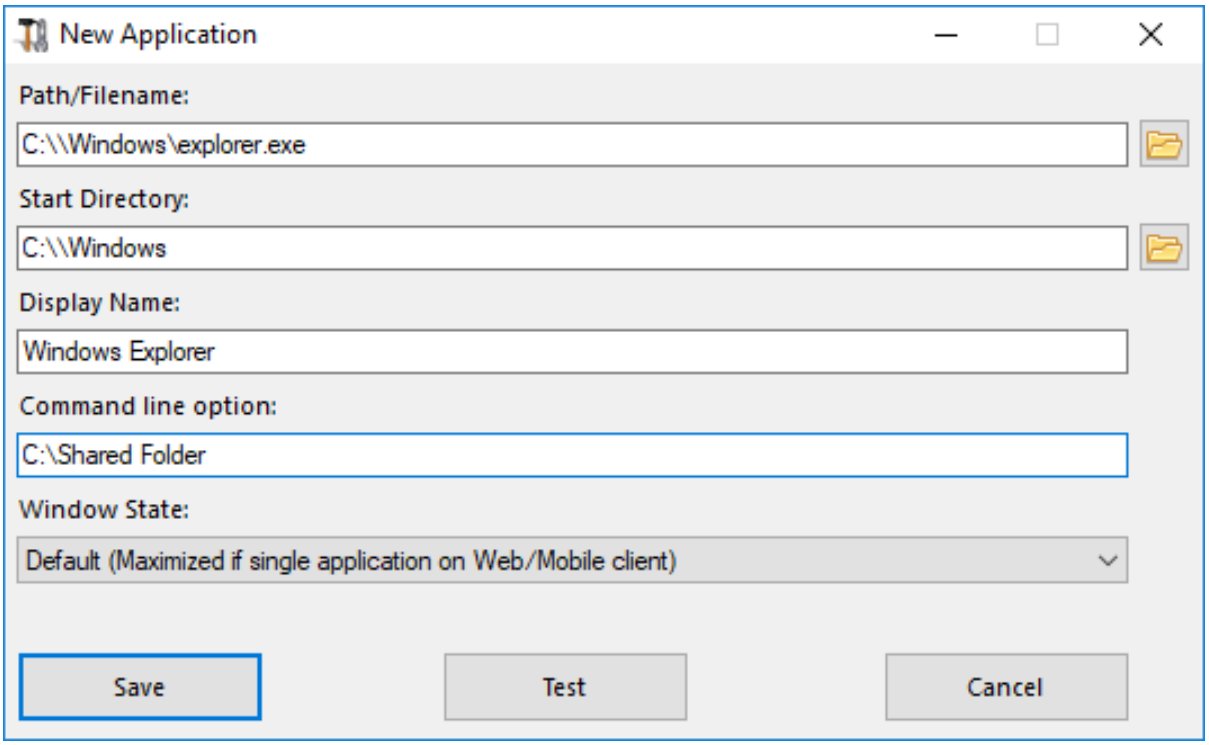
Diese Verknüpfung kann in den Desktop-Ordner des Benutzers kopiert werden, oder Sie können die folder.exe für einen Benutzer als Anwendung veröffentlichen. Wenn Sie Letzteres tun, müssen Sie den Pfad Ihres Ordners im Abschnitt Befehlszeilenoption angeben.



Es gibt eine alternative Möglichkeit, einen Ordner mit Dokumenten zu teilen.

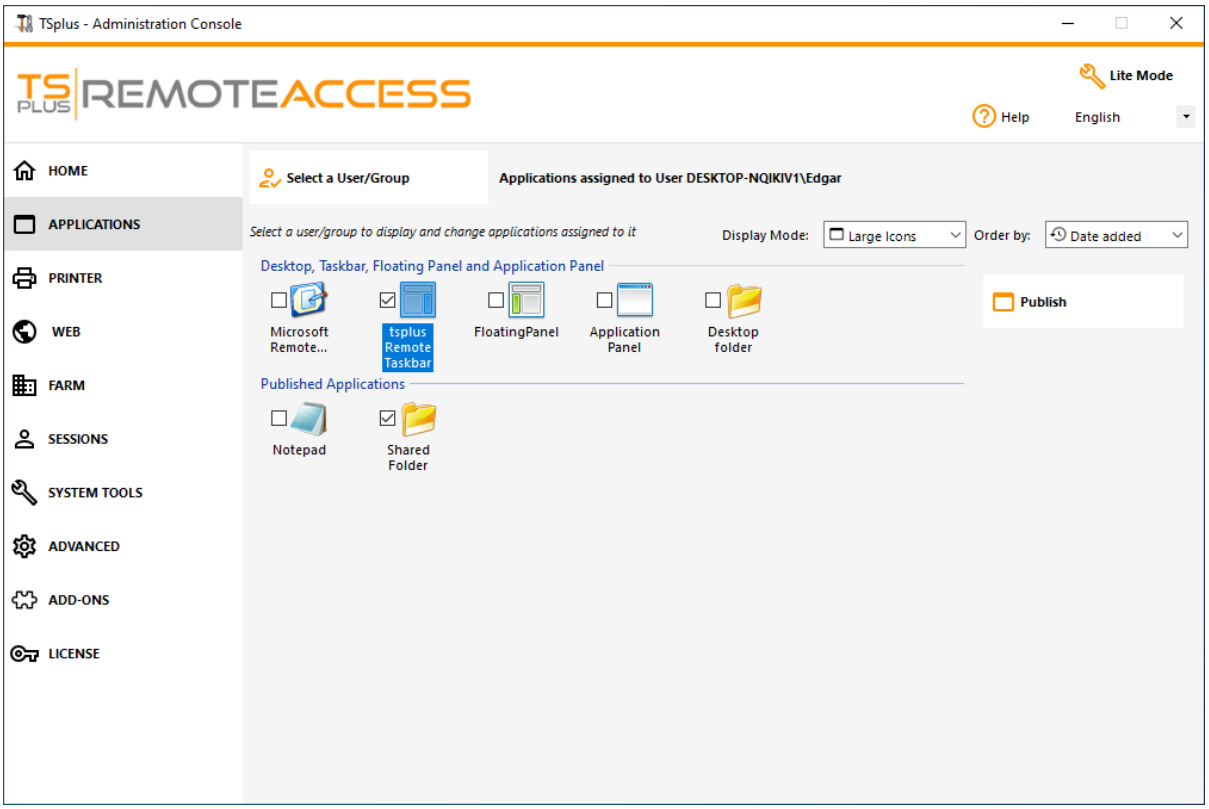
Einen freigegebenen Ordner als einzigartige Anwendung veröffentlichen :

Fügen Sie eine neue Anwendung hinzu. Geben Sie im Anzeigenamen den Namen des freigegebenen Ordners oder einen beliebigen Namen ein, den Sie möchten. Klicken Sie auf die Schaltfläche Durchsuchen, die sich rechts im Feld „Pfad/Dateiname“ befindet, und suchen Sie C:\Windows\explorer.exe. Das Startverzeichnis wird automatisch mit dem Pfad von explorer.exe ausgefüllt. Geben Sie im Feld für die Befehlszeilenoption den Pfad des freigegebenen Ordners ein, es kann sich um einen lokalen Ordner oder einen im Netzwerk freigegebenen Ordner mit einem UNC-Pfad handeln (Beispiel: \data\shared folder). Füllen Sie das Feld unten mit Ihren Informationen zum freigegebenen Ordner aus.

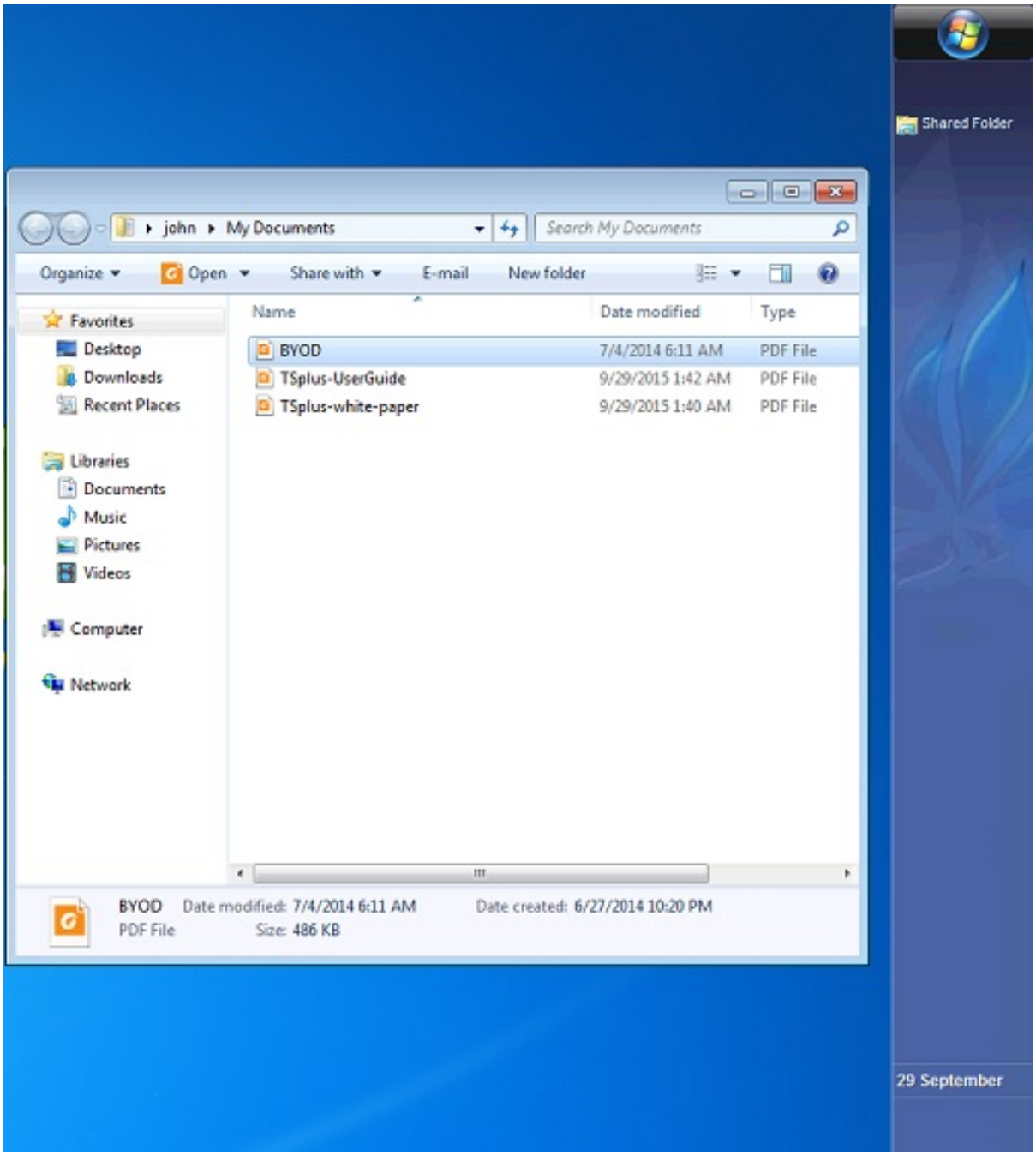


Dann klicken Sie auf „Speichern“.

Klicken Sie auf die Registerkarte „Benutzer“. Wählen Sie Ihren Benutzer aus und aktivieren Sie die Kästchen für die TSplus Remote Taskleiste und den gemeinsamen Ordner.

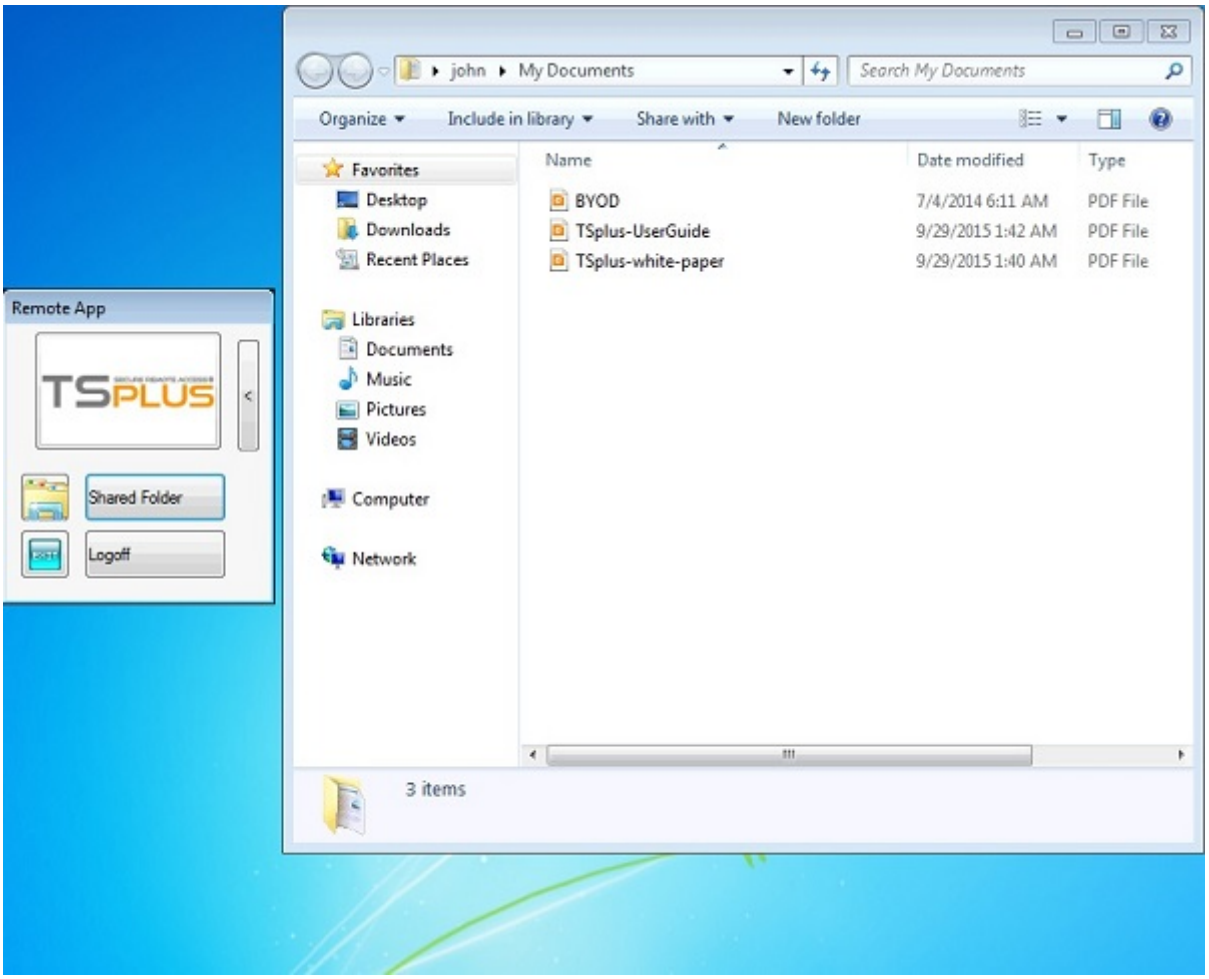


Hier ist das Ergebnis: Wenn Sie eine Sitzung mit einem RDP-Client öffnen, sehen Sie die TSplus-Taskleiste mit der Anwendung für den freigegebenen Ordner.



Sie können dies auch mit dem schwebenden Panel tun. Öffnen Sie ein Administrationswerkzeug und klicken Sie auf die Registerkarte „Anwendung zuweisen“. Aktivieren Sie die Kästchen für das schwebende Panel und den freigegebenen Ordner.

Hier ist das Ergebnis:


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

Kostenloses und einfach zu installierendes HTTPS-Zertifikat

Übersicht

Ab Version 9.20 bietet TSplus eine benutzerfreundliche Funktion zur Erstellung eines kostenlosen und gültigen HTTPS-Zertifikats.

In 3 Mausklicks erhalten Sie ein sicheres, gültiges Zertifikat, das automatisch erneuert und automatisch in den integrierten Webserver von TSplus konfiguriert wird.

Diese Funktion verwendet Let's Encrypt um ein kostenloses und sicheres HTTPS-Zertifikat für Ihre HTTPS-Verbindungen bereitzustellen.

Voraussetzungen

Bitte stellen Sie sicher, dass Ihr TSplus-Server diese Anforderungen erfüllt, bevor Sie den kostenlosen Zertifikatsmanager verwenden:

- Du musst **verwenden Sie den integrierten Webserver von TSplus, der auf Port 80 für HTTP hört** Dies ist erforderlich für den Validierungsprozess des Domainbesitzes von Let's Encrypt.

- Ihr **Der Domainname des Servers muss zugänglich sein.** aus dem öffentlichen Internet. Dies ist auch erforderlich, um zu bestätigen, dass Sie der tatsächliche Eigentümer der Domain sind.

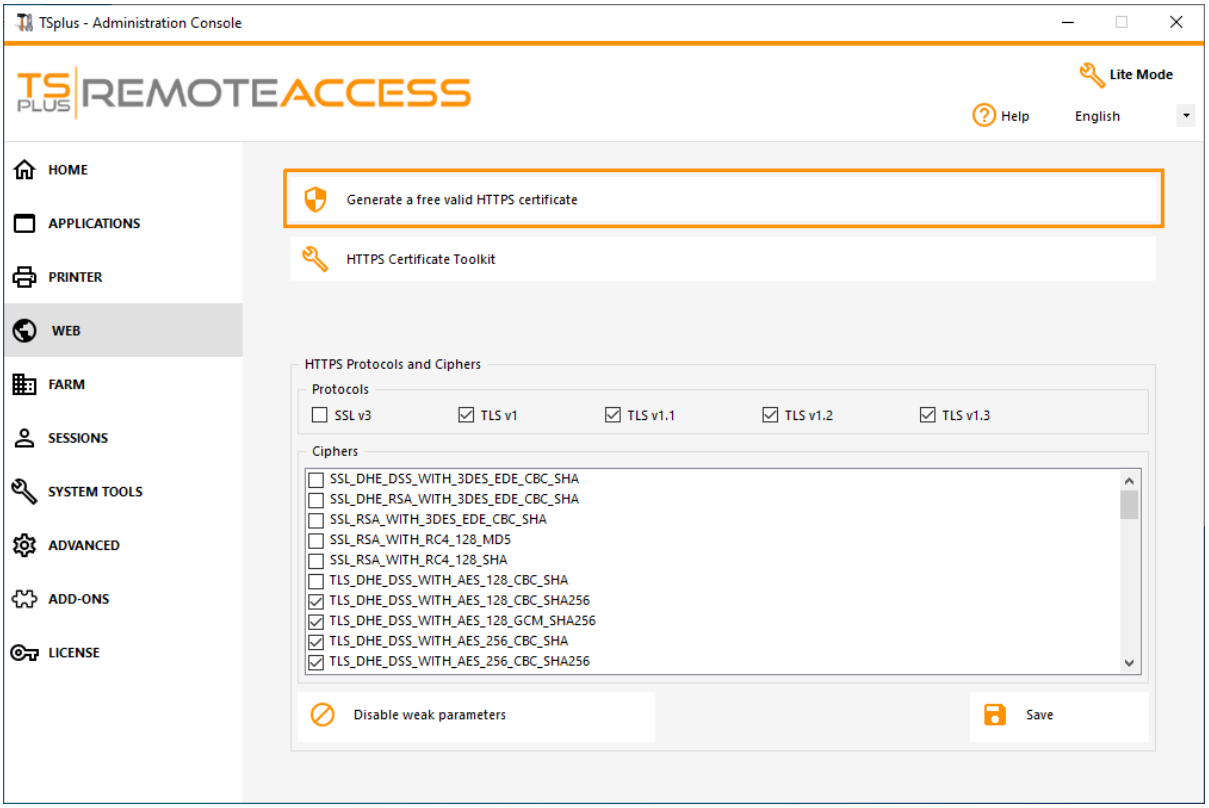
- Du musst **Führen Sie dieses Programm auf dem Gateway-Server oder einem Standalone-Server aus, nicht auf einem Anwendungsserver.** (außer wenn Ihr Anwendungsserver über das öffentliche Internet zugänglich ist und einen öffentlichen Domainnamen hat).

Es ist nicht möglich, ein Zertifikat für eine IP-Adresse zu erhalten, sei sie öffentlich oder privat.

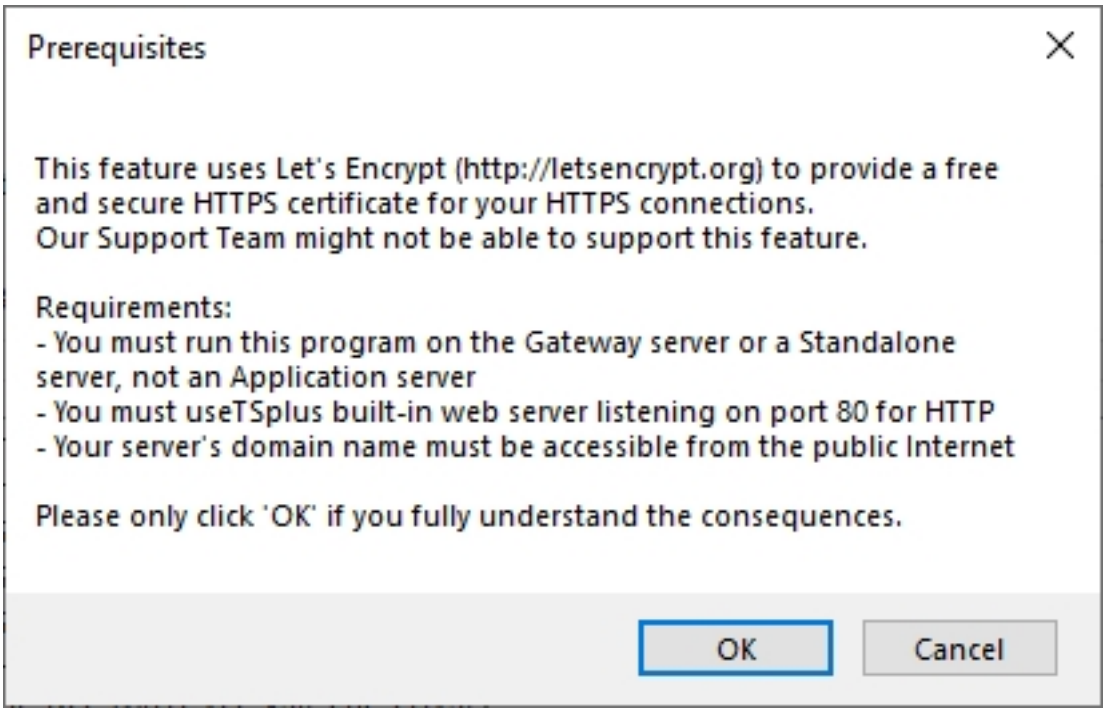
Es ist nicht möglich, ein Zertifikat für einen internen Domainnamen (d.h. eine Domain, die nur innerhalb Ihres privaten Netzwerks aufgelöst wird) zu erhalten.

Kostenloser Zertifikat-Manager GUI

Um die TSplus Free Certificate Manager GUI zu öffnen, öffnen Sie das TSplus AdminTool, klicken Sie auf die Registerkarte „Web - HTTPS“ und klicken Sie dann auf „Ein kostenloses gültiges HTTPS-Zertifikat generieren“, wie im Screenshot unten gezeigt:



Die kostenlose Zertifikatsmanager-GUI wird geöffnet und erinnert Sie an die Voraussetzungen, wie im Screenshot unten gezeigt.



Bitte lesen Sie sorgfältig und überprüfen Sie, ob Ihr Server alle Anforderungen erfüllt, und klicken Sie dann auf die Schaltfläche „Ok“.

Schritt 1: Geben Sie Ihre E-Mail ein

Diese E-Mail wird nicht verwendet, um Sie mit Spam zu belästigen. Tatsächlich wird sie nicht einmal an TSplus oder Dritte gesendet, außer an die Zertifizierungsstelle: Let’s Encrypt.

Sie werden Sie nur kontaktieren, wenn es notwendig ist, gemäß ihren Nutzungsbedingungen.

Schritt 2: Geben Sie den Domänennamen des Servers ein

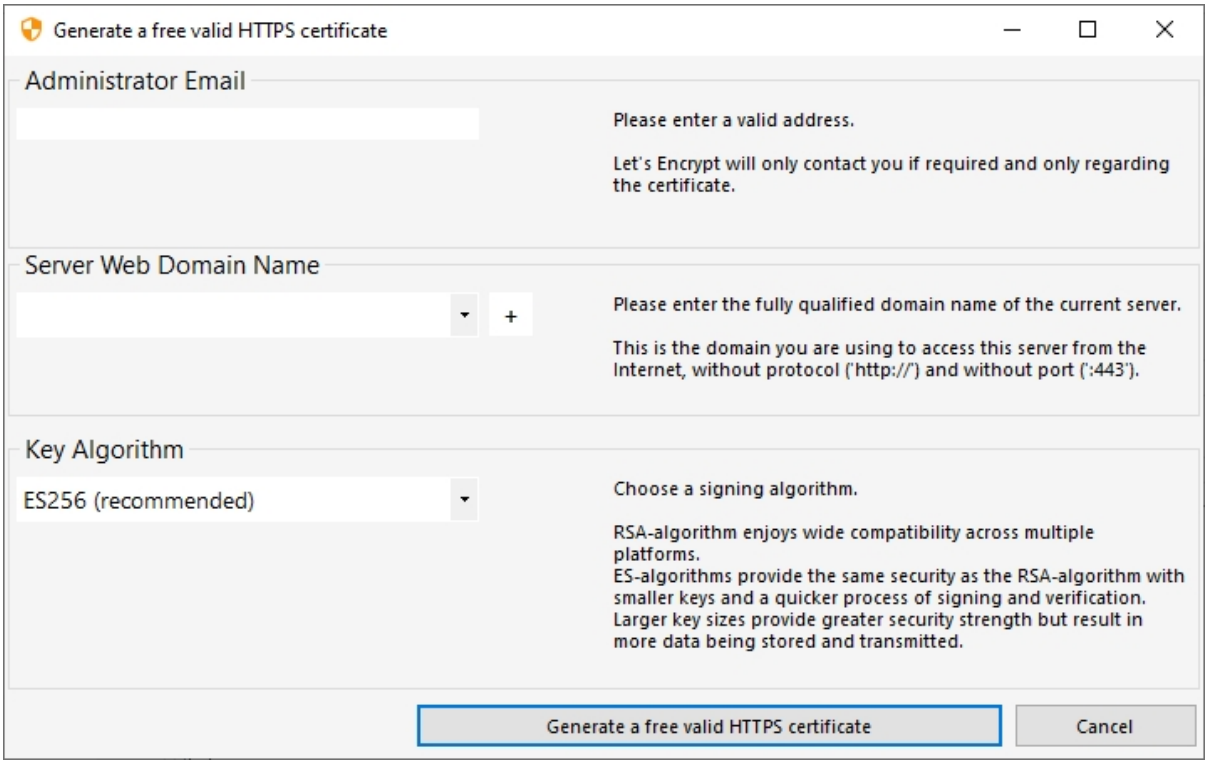
Dies ist der öffentlich zugängliche Domainname im Internet, etwas wie gateway.ihre-firma.com. Sie können auch einen weiteren Domainnamen oder einen Subdomainnamen hinzufügen, nachdem Sie auf die Schaltfläche „+“ geklickt haben.

Wie im GUI erklärt, fügen Sie kein Protokollpräfix und/oder einen Portsuffix hinzu, geben Sie einfach den sauberen Domainnamen/die sauberen Domainnamen ein.

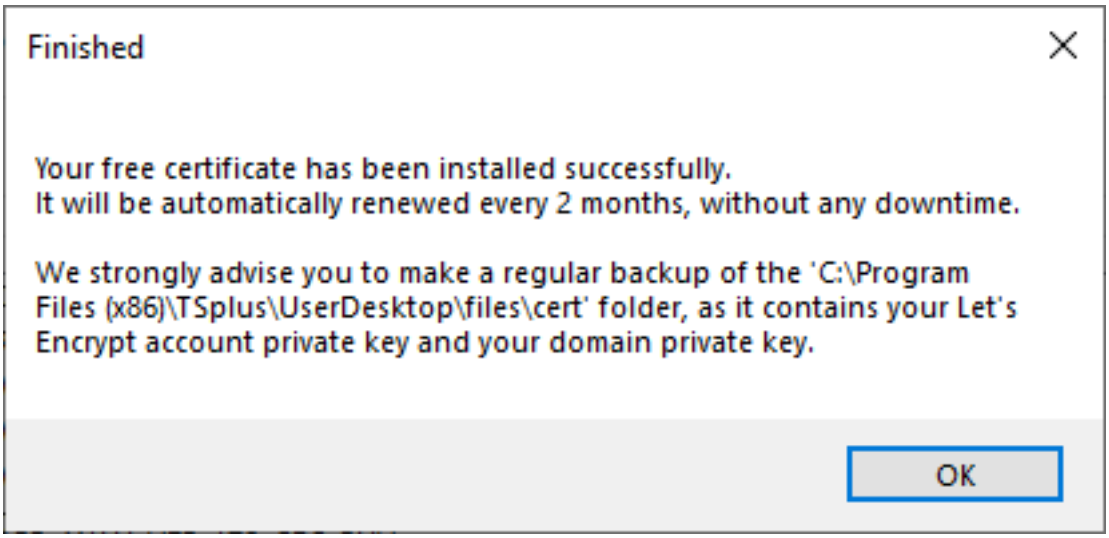
Das Zertifikat wird für diesen Domainnamen generiert und ist nur auf einer Webseite gültig, die unter diesem Domainnamen gehostet wird. Wenn Ihre Benutzer sich über Ihr Webportal verbinden, verwenden Sie https://server1.example.com:1234 Dann müssen Sie "server1.example.com" eingeben.

Schritt 3: Wählen Sie einen Schlüsselalgorithmus

Es wird verwendet, um Schlüsselpaaren zu erstellen und digitale Signaturoperationen durchzuführen.



Genießen Sie Ihr Zertifikat!



TSplus Free Certificate Manager wird nun alle Daten verwenden, um sich mit Let’s Encrypt zu verbinden, zu validieren, dass Sie wirklich den Domainnamen besitzen, den Sie eingegeben

haben, und das passende gültige Zertifikat zu erhalten.

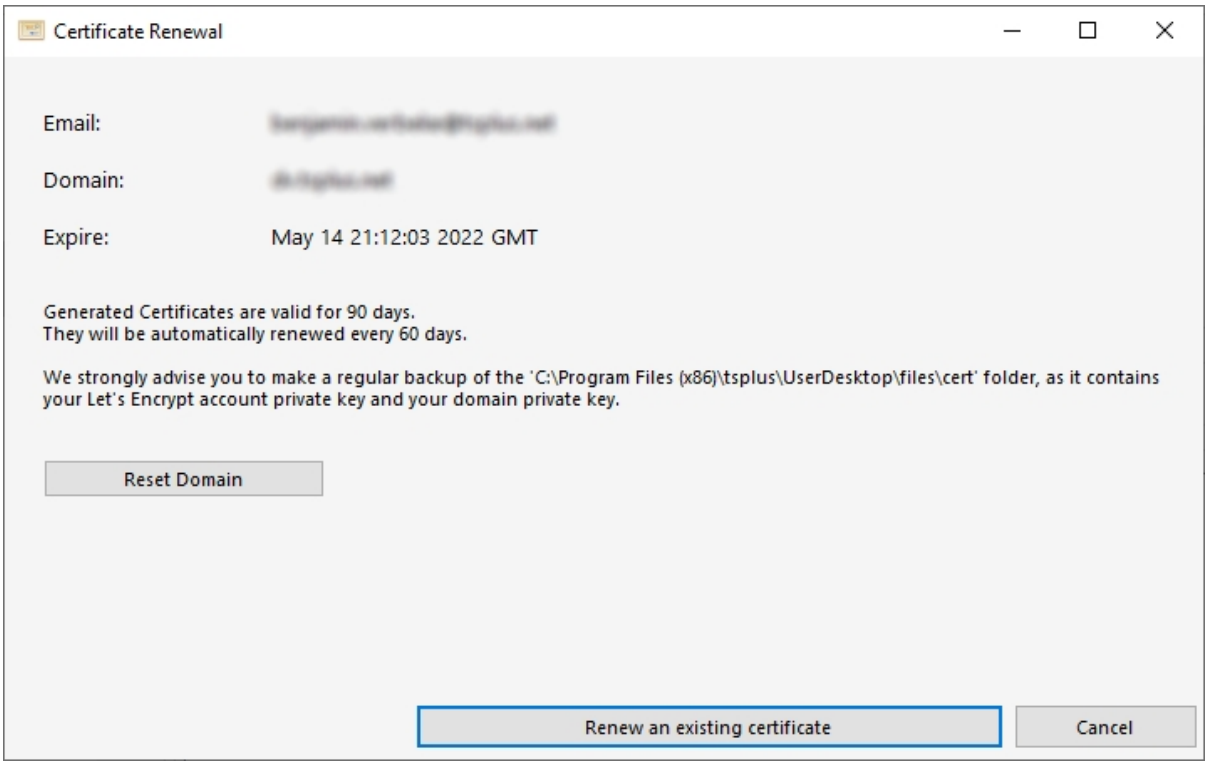
Sobald das Programm das Zertifikat erhält, wird es automatisch alle erforderlichen Dateiformatkonvertierungen durchführen und den integrierten Webserver von TSplus sanft neu laden, um das neue Zertifikat auf jede neue Verbindung anzuwenden. Der Webserver ist **nicht** neugestartet und keine Verbindung ist gestoppt.

Zertifikatserneuerung

Let’s Encrypt-Zertifikate sind 90 Tage lang gültig. Die Gültigkeitsdauer wird bis 2028 auf 45 Tage halbiert, ebenso wie der Rest der Branche.

TSplus wird das Zertifikat alle 15 Tage automatisch erneuern, um die Sicherheit zu gewährleisten. Bei jedem Neustart des Windows-Servers wird eine Überprüfung durchgeführt, und dann alle 24 Stunden.

Sie können Ihr Zertifikat manuell erneuern, indem Sie das Tool "Free Certificate Manager" öffnen. Es zeigt den Domainnamen des Zertifikats und das Ablaufdatum an, wie im Screenshot unten dargestellt.



Um Ihr Zertifikat manuell zu erneuern, klicken Sie einfach auf die Schaltfläche „Weiter“.

Der Button „Domain zurücksetzen“ in diesem Fenster löscht das SSL-Zertifikat und konfiguriert den Webserver in seinen ursprünglichen Zustand zurück, bevor der Zertifikatsmanager verwendet wird.

Beste Praktiken

Wenn kein Fehler auftritt, wird TSplus das Zertifikat automatisch alle 15 Tage erneuern. Wir empfehlen, dass Sie **alle 45 Tage überprüfen** dass Ihr Zertifikat automatisch erneuert wurde. Let's Encrypt stellt derzeit Zertifikate aus, die 90 Tage gültig sind, was bis 2028 auf 45 Tage halbiert wird.

Wir empfehlen auch, dass Sie **mindestens einmal im Monat sichern** den folgenden Ordner und seine Unterordner:

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

Dies ist ein interner Ordner, der Ihren privaten Schlüssel für das Let's Encrypt-Konto sowie das Schlüsselpaar Ihres Zertifikats enthält.

Fehlerbehebung

Im Falle eines Fehlers Bitte kontaktieren Sie den Support und senden Sie ihnen die folgende Protokolldatei.

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

Diese Protokolldatei (und möglicherweise die anderen Protokolldateien im selben Ordner) sollte unserem Support-Team helfen, das Problem zu untersuchen und besser zu verstehen.

Wenn Sie ein zuvor verwendetes Zertifikat wiederherstellen möchten gehe zum Ordner:

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

Es werden alle verwendeten „cert.jks"-Dateien enthalten sein. Dies sind die „Key Store"-Dateien, und wir löschen sie niemals, wir benennen sie nur mit dem Datum und der Uhrzeit ihrer Deaktivierung um.

Fehlercodes

- Fehler 801: Der kostenlose Zertifikatsmanager konnte Ihr Let's Encrypt-Konto nicht registrieren. Überprüfen Sie Ihre Internetverbindung. Stellen Sie sicher, dass Ihre E-Mail-Adresse nicht bereits bei Let's Encrypt registriert ist. Versuchen Sie es erneut mit einer anderen E-Mail.
- Fehler 802 & Fehler 803: Der kostenlose Zertifikatsmanager konnte die URL-Adresse der

Let’s Encrypt-Nutzungsbedingungen nicht abrufen. Dies ist ein nicht blockierender Fehler: Sie können weiterhin fortfahren und die Let’s Encrypt-Nutzungsbedingungen akzeptieren - lesen Sie sie natürlich zuerst in Ihrem Browser.

- Fehler 804: Der kostenlose Zertifikatsmanager konnte Ihre Zustimmung zu den Nutzungsbedingungen von Let’s Encrypt bei den Let’s Encrypt-Servern nicht validieren. Überprüfen Sie Ihre Internetverbindung. Versuchen Sie es erneut.

- Fehler 805 & Fehler 806: Der kostenlose Zertifikatsmanager konnte nicht bestätigen, dass Sie die Domain besitzen, die Sie während der Zertifikatserstellung (Fehler 805) oder der Zertifikatserneuerung (Fehler 806) eingegeben haben. Überprüfen Sie erneut alle Voraussetzungen. Überprüfen Sie Ihre Internetverbindung. Stellen Sie sicher, dass Ihr Webserver auf Port 80 lauscht. Stellen Sie sicher, dass Sie keinen Drittanbieter-Webserver wie IIS oder Apache verwenden. Überprüfen Sie, ob Ihr Domainname aus dem öffentlichen Internet zugänglich ist.

HTTPS-Zertifikat-Befehlszeile

Zubereitung der Zertifikat-Konfigurationsdatei

Innerhalb des Ordners “C:\Program Files (x86)\TSplus\UserDesktop\files\cert” erstellen Sie eine Datei mit dem Namen “FreeCertificateManager.ini”, falls sie noch nicht existiert. Stellen Sie sicher, dass Ihr Texteditor und/oder der Windows-Datei-Explorer keine Endung “.txt” hinzufügt.

Bearbeiten Sie die Datei und schreiben oder aktualisieren Sie sie, damit sie das folgende Format hat, und speichern Sie sie dann:

Einstellungen

E-Mail = your.email@company.com

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

Zertifikat erstellen

Als Serveradministrator führen Sie den folgenden Befehl aus:

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

Damit dieser Befehl erfolgreich ist:

- Die Datei „FreeCertificateManager.ini“ muss vorhanden sein und das erwartete Format verwenden.
- Ihr TSplus Remote Access-Server muss betriebsbereit sein.
- Ihr TSplus Remote Access Webportal muss mit dem Protokoll verfügbar sein

HTTP über Port 80 aus dem öffentlichen Internetnetzwerk, da der TSplus HTTPS-Zertifikatanbieter dies verwenden wird, um den Server-Domainnamen zu validieren.

Zertifikat erneuern

Sobald das Zertifikat konfiguriert und erstellt ist, wird TSplus Remote Access es alle zwei Monate automatisch erneuern, um sicherzustellen, dass es niemals abläuft.

Hinzufügen eines Drittanbieterzertifikats

Innerhalb des Ordners “C:\Program Files (x86)\TSplus\UserDesktop\files\cert” erstellen Sie eine Datei mit dem Namen “certpassword.txt”, die nur das Zertifikatspasswort enthält. Als Serveradministrator führen Sie den folgenden Befehl aus:

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

Wenn Sie TSplus Advanced Security verwenden, müssen Sie möglicherweise die Funktion zur geografischen Schutz vorübergehend deaktivieren, damit sie funktioniert. Sie können Ihre Passwortdatei nach dem Ausführen des Befehls löschen.

Verhindern Sie den RDP-Zugriff und erlauben Sie HTTP auf dem Gateway-Server

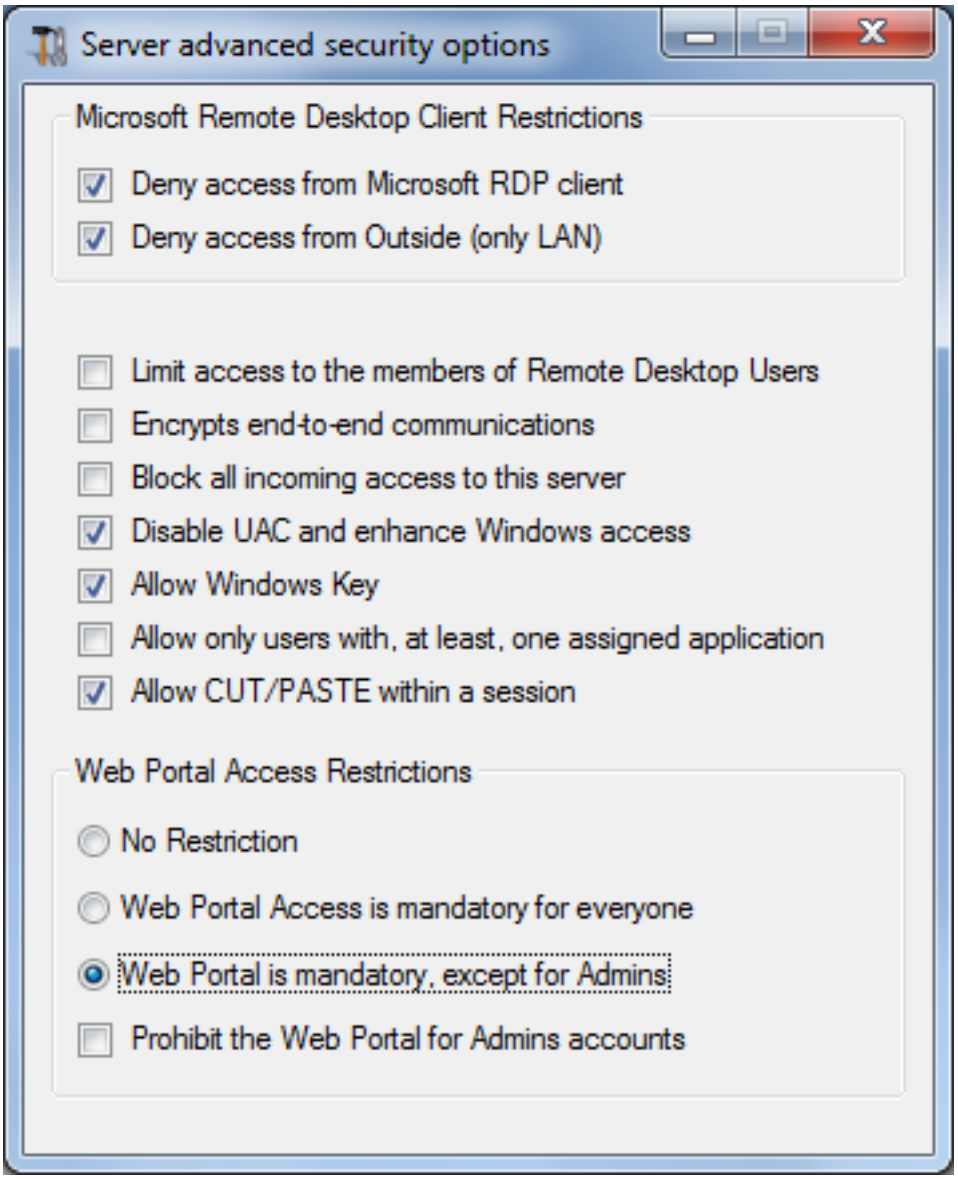
Es gibt 2 Möglichkeiten, auf den Gateway-Server zuzugreifen:

- HTML5 / HTML
- RDP-Sitzung (über die Gateway-IP/DNS – Portnummer)

Wie man HTML/HTML5 ABSCHLIEßT

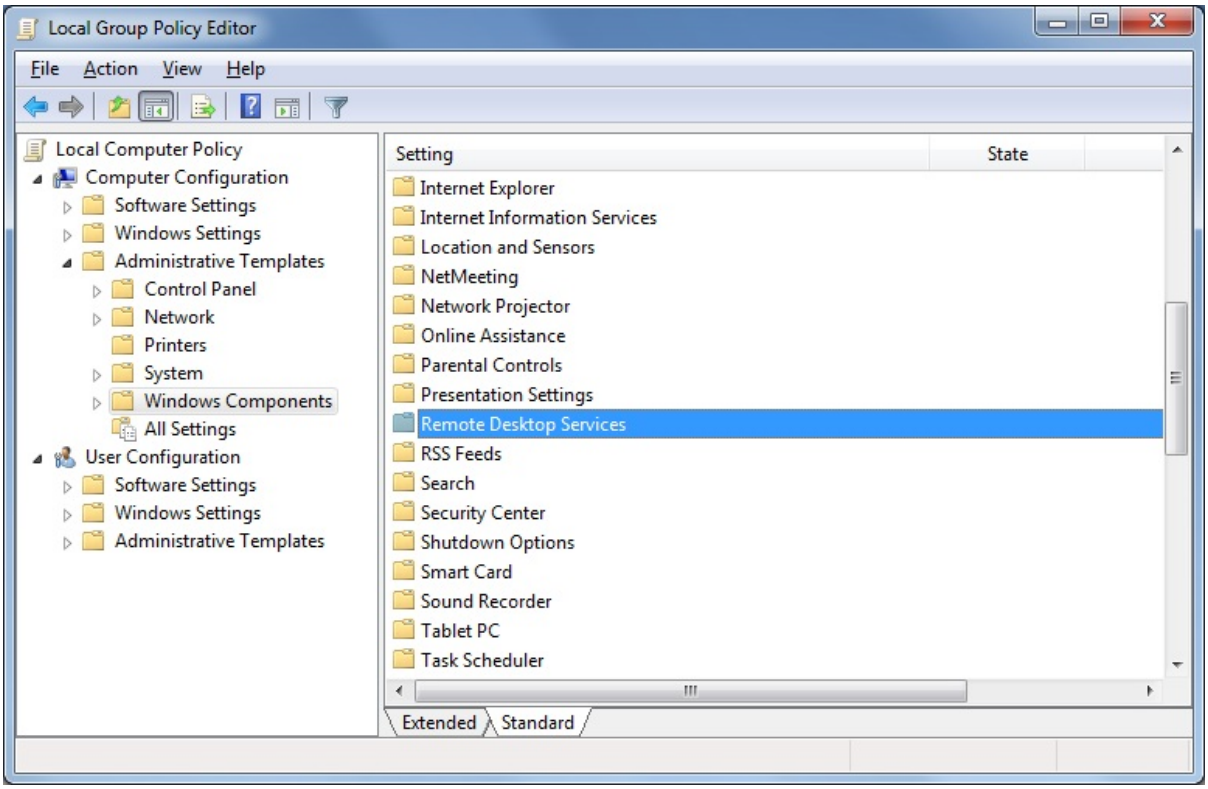
Wir können mstsc mit einer PORT-Nummer verwenden und uns in einen TSplus-Anwendungs-/ Gateway-Server einloggen.

Wenn wir jedoch diese fortschrittlichen Sicherheitswerkzeuge verwenden, die sich in der TSplus Admin-Konsole auf dem Gateway-Server befinden, indem wir auf die Sicherheitskachel/den Tab klicken und dann auf die Kachel mit den Optionen für die erweiterte Sicherheit klicken…

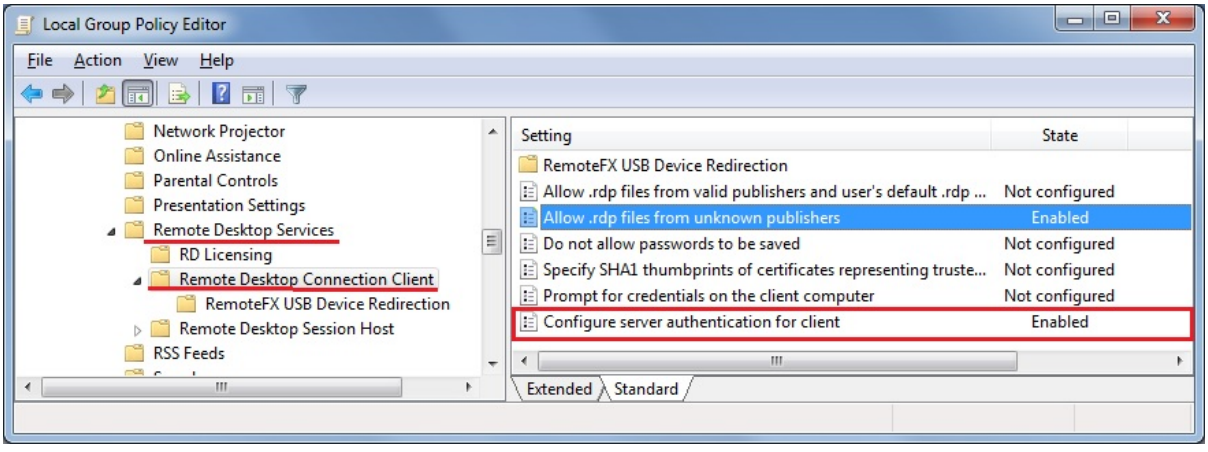


…der Zugriff wird verweigert, wenn Sie versuchen, sich mit RDP zu verbinden. Um dieses Verhalten zu vermeiden, müssen Sie auf dem Gateway-Server Folgendes tun:

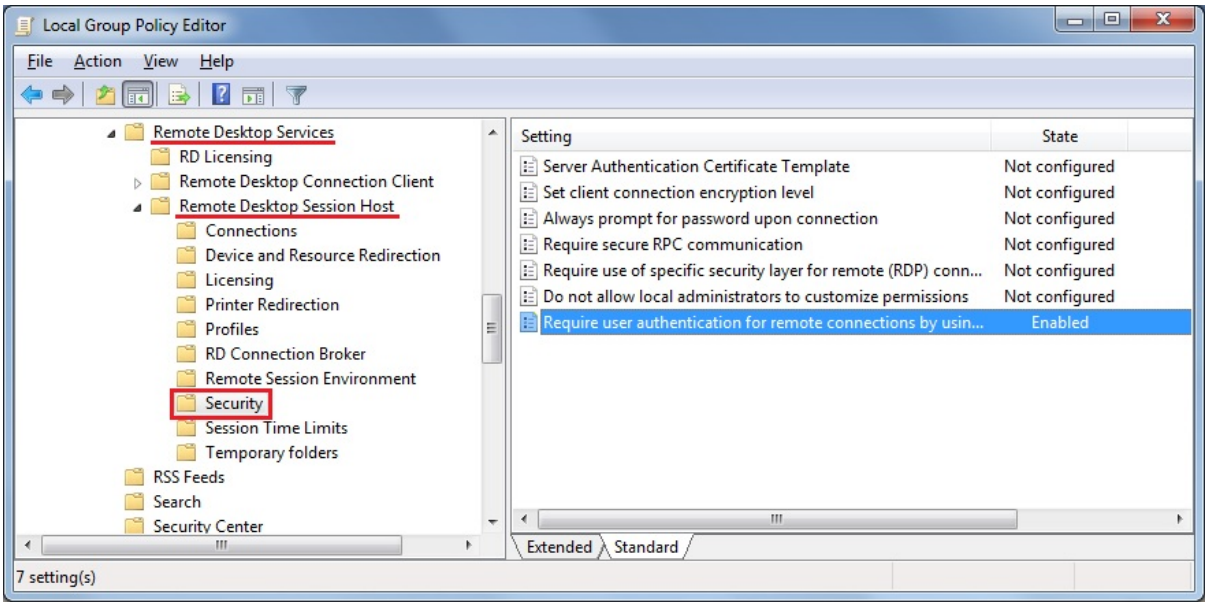
- Gehe zu Gpedit.msc, klicke dann unter Computerkonfiguration auf den Ordner Administrative Vorlagen, auf den Ordner Windows-Komponenten und auf Terminaldienste:



- Dann klicken Sie auf den Ordner Remote Desktop Connection Client, doppelklicken Sie auf die Einstellung „.rdp-Dateien von unbekannten Herausgebern zulassen“ und aktivieren Sie sie sowie die „Serverauthentifizierung für den Client konfigurieren“:



- Unter dem Menü des Remote Desktop Clients klicken Sie auf den Ordner Remote Desktop Session Host und dann auf den Ordner Sicherheit. Aktivieren Sie die Einstellung „Benutzerauthentifizierung für Remoteverbindungen mit Netzwerkebene-Authentifizierung erforderlich“.

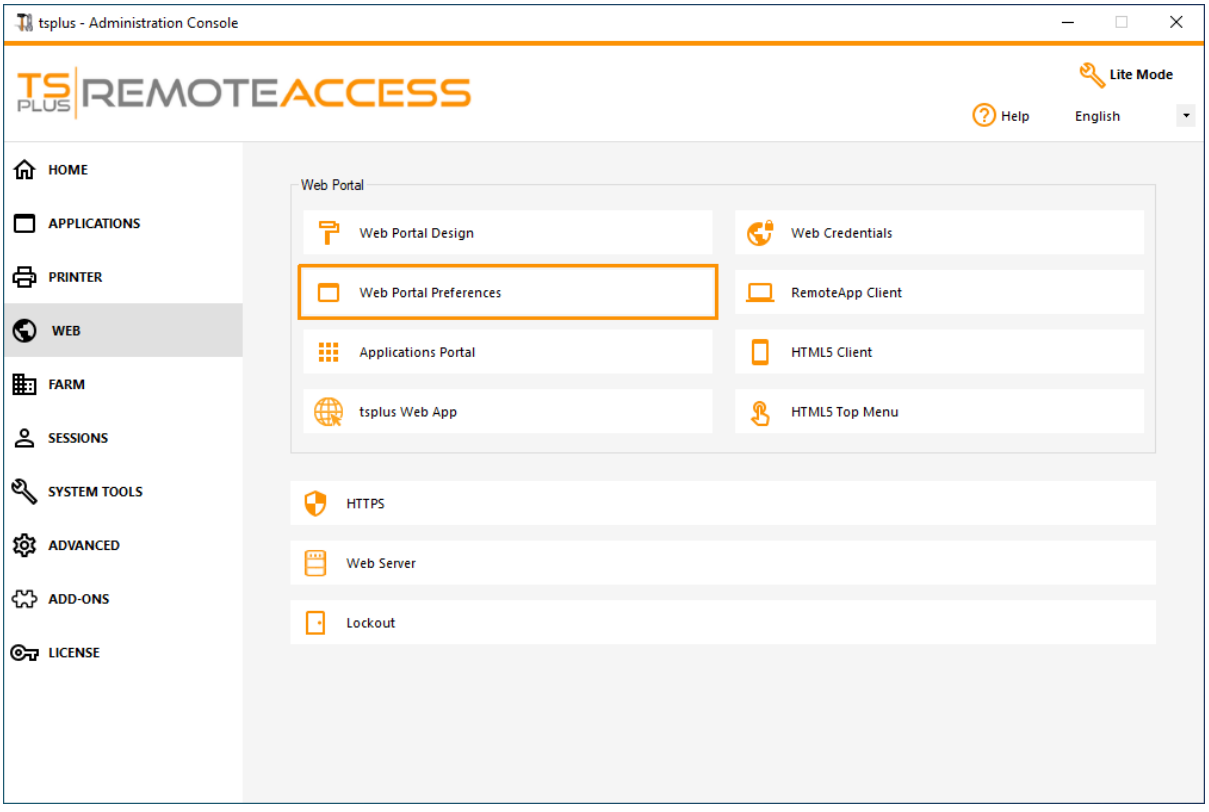

Local Group Policy Editor
File Action View Help
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment
Security
Session Time Limits
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)

Gateway-Server manuell aktivieren/ deaktivieren

Übersicht

Basierend auf Ihrer Farmkonfiguration wird der Farmcontroller automatisch seine eigenen Webportal-Einstellungen ändern, um ein Gateway-Server zu werden. , sodass Benutzer, die sich über das TSplus Webportal des Farm Controllers verbinden, nicht direkt mit dem Farm Controller selbst, sondern mit einem der Anwendungsserver der Farm verbinden können.

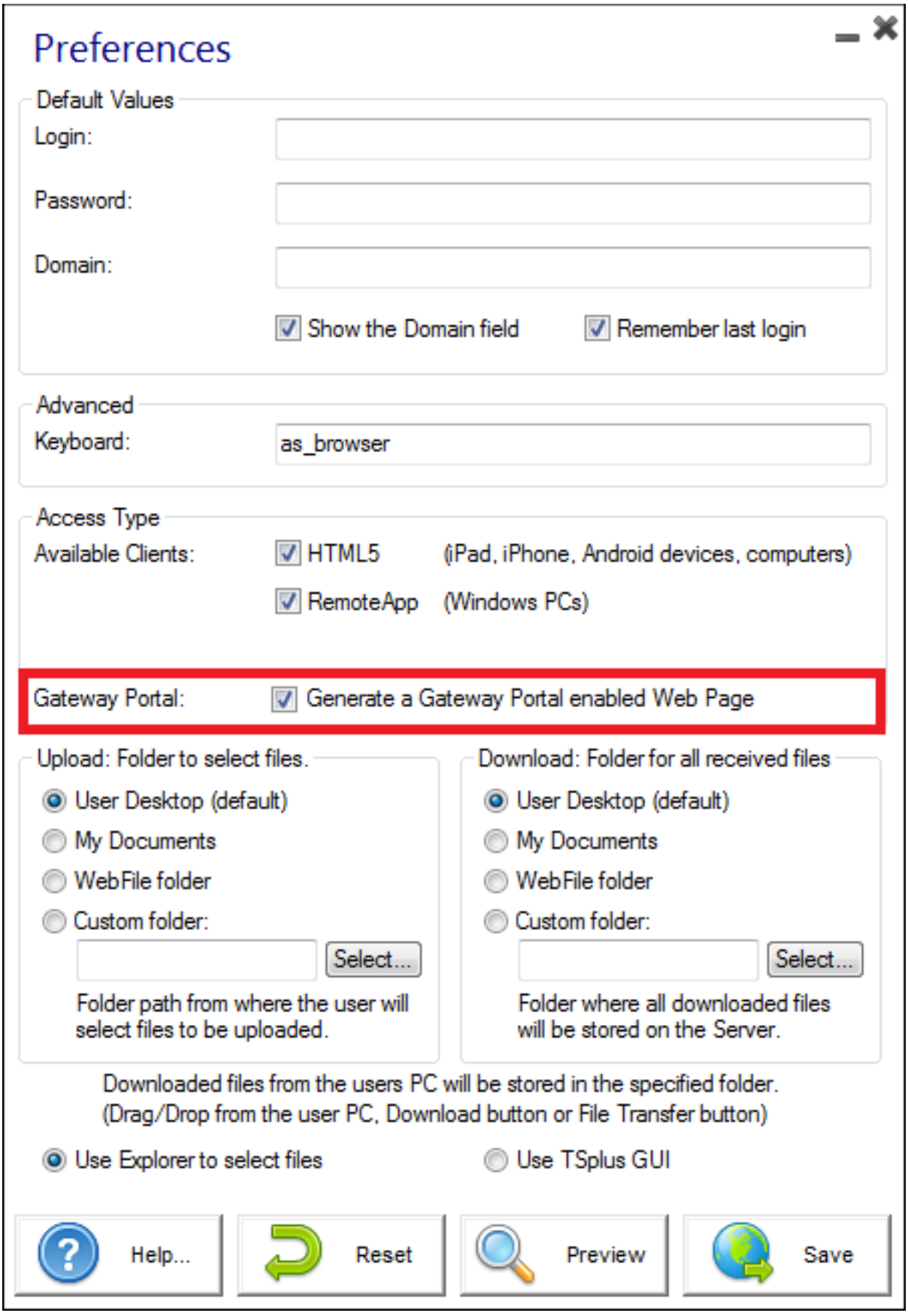
Wenn Sie dieses Verhalten jedoch manuell ändern möchten, können Sie dies tun, indem Sie auf das „WEB“-Kachel klicken und dann auf die Schaltfläche Webportal-Einstellungen.



- Aktivieren Sie das Kontrollkästchen „Eine Gateway-Portal-fähige Webseite generieren“, wenn

Sie möchten, dass das Gateway-Portal des Farm Controllers (des aktuellen Servers, den Sie gerade konfigurieren) zu einem Gateway-Server wird und Benutzer zu den Anwendungsservern der Farm umleitet.

- Deaktivieren Sie das Kontrollkästchen „Eine Gateway-Portal-fähige Webseite generieren“, wenn Sie möchten, dass das Gateway-Portal des Farm Controllers auf den Farm Controller selbst umgeleitet wird, wodurch jede Farmkonfiguration umgangen wird.



Klicken Sie auf „Speichern“, um diese Einstellung zu speichern.

Hardware-Identifikator & Klon-Server

1- Hardware-Identifikatoränderung.

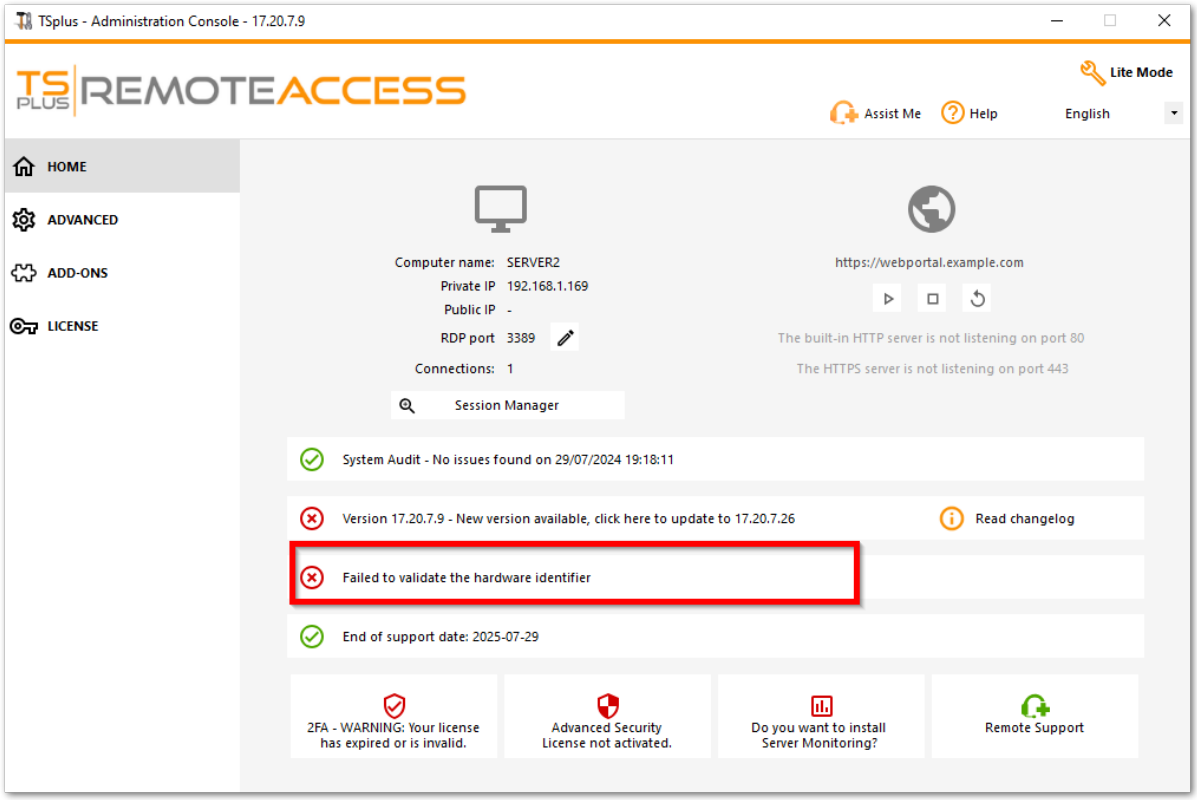
Reparatur des Hardware-Identifikators nach Klonen oder einem Update.

Warnung: Hardware-Identifikator konnte nicht validiert werden

Nach der Migration eines physischen Servers auf eine virtuelle Maschine oder ein Kernel-Update von Microsoft ändert sich der Lizenzstatus in "Hardware-Identifikator auf neuer Hardware konnte nicht validiert werden."

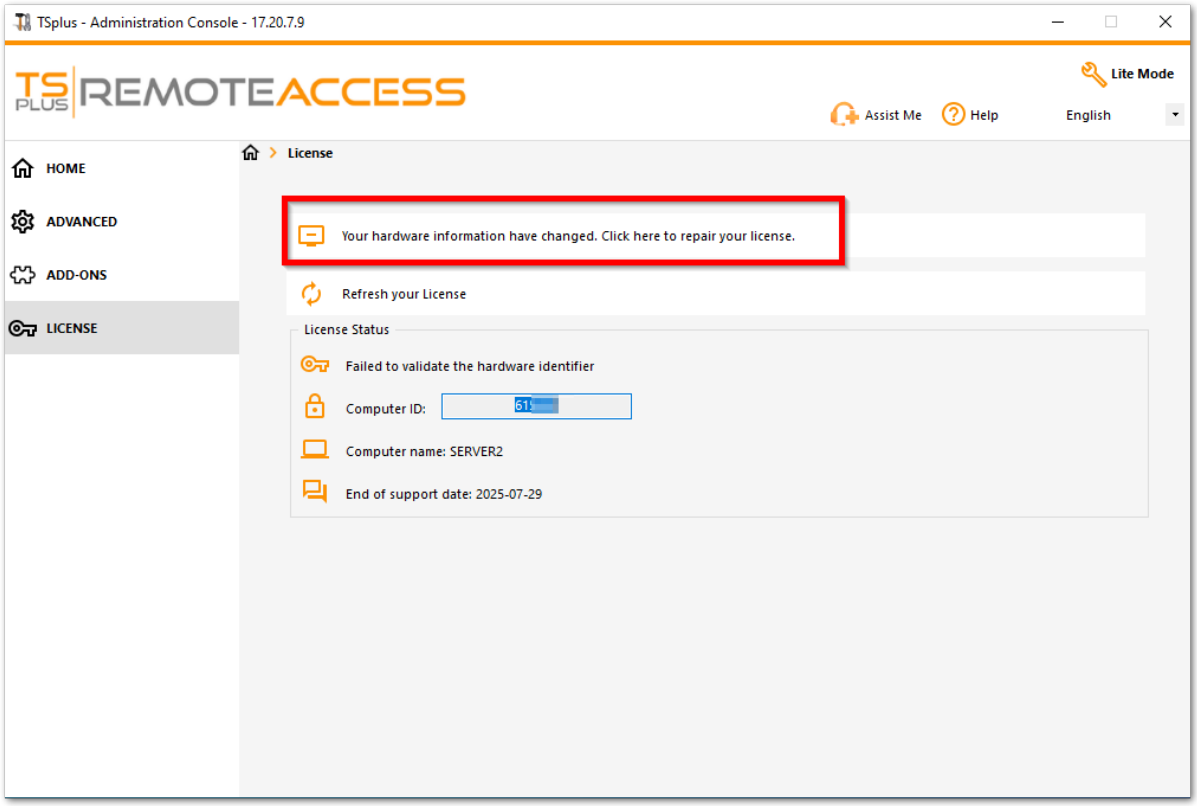
Diese Nachricht erscheint, weil TSplus einen Lizenzkonflikt festgestellt hat, der von einem Server auf einen anderen mit derselben Computer-ID und demselben Namen kopiert wurde.
Wir empfehlen bereits, Ihren neuen Server umzubenennen (Beispiel: SERVER1 > SERVER2)

- Starten Sie Ihren Server



Klicken Sie auf das Fenster, um zur Lizenzseite zu gelangen.

Dann klicken Sie auf die Registerkarte „Ihre Hardwareinformationen haben sich geändert. Klicken Sie hier, um Ihre Lizenz zu reparieren.“



Ein Popup zur "Lizenzübertragung" wird geöffnet, um Ihnen zu ermöglichen, Ihre Lizenz wiederherzustellen.

Fall 1: Sie haben keinen Support!
Rehosting wird daher nicht möglich sein, Sie müssen ein Support-Abonnement auf dem ursprünglichen Server abonnieren und die Migrationsaktion erneut starten.
Im Falle von Problemen, Kontaktieren Sie den Support und geben Sie Ihre Computer-ID und Ihren Aktivierungsschlüssel an.

Fall 2: Sie haben bereits seit 6 Monaten rehosted!
Die Nachricht: Sie haben diesen Computer in den letzten 6 Monaten bereits neu gehostet. Bitte kontaktieren Sie den Support, wenn Sie Hilfe beim Rehosting Ihrer Lizenz benötigen.

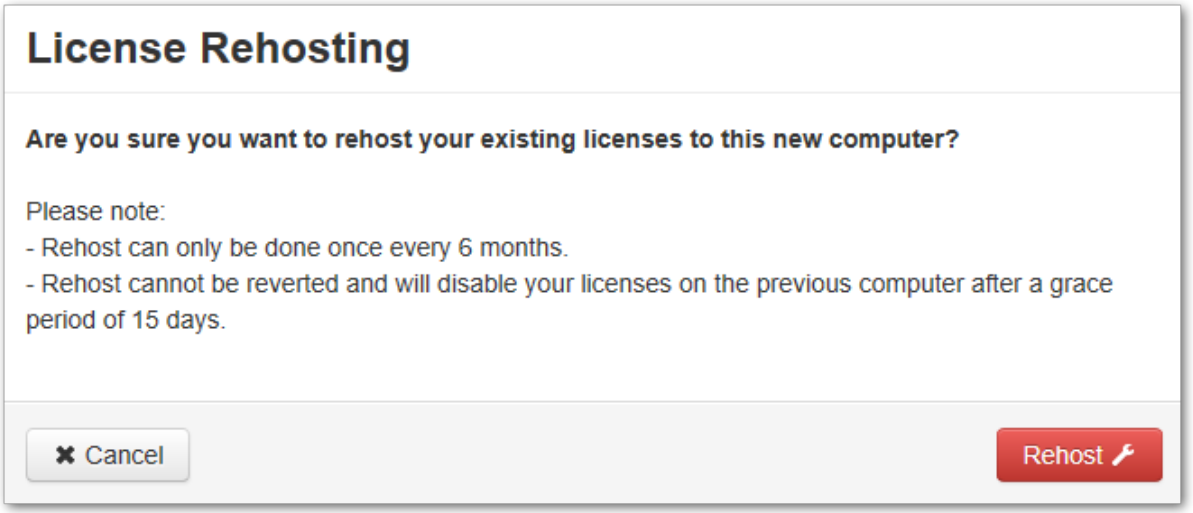
Die Neuhostung wird daher nicht möglich sein, Kontaktieren Sie den Support und geben Sie Ihre Computer-ID und Ihren Aktivierungsschlüssel an.

Fall 3: Sie haben Unterstützung!
Die folgende Nachricht erscheint: Sind Sie sicher, dass Sie Ihre bestehenden Lizenzen auf diesem neuen Computer neu hosten möchten?

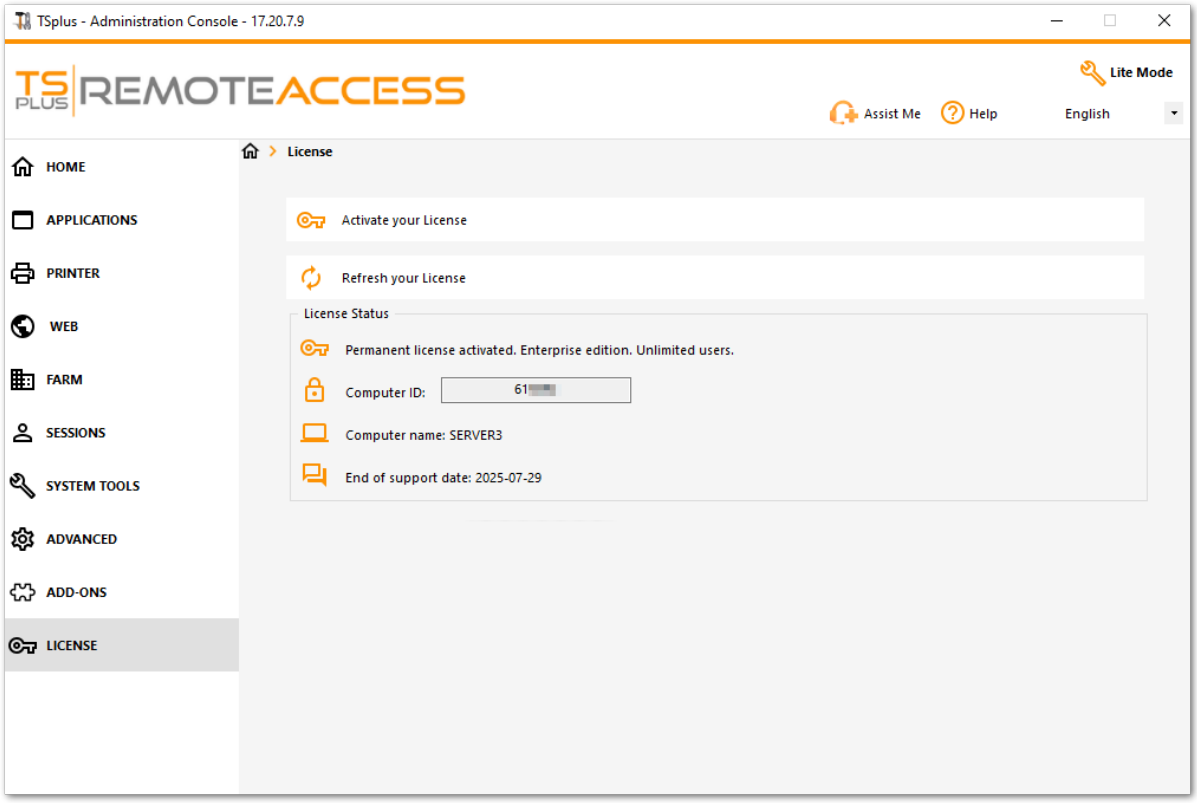
Bitte beachten Sie:

- Rehosting kann nur einmal alle 6 Monate durchgeführt werden.
- Rehosting kann nicht storniert werden und deaktiviert Ihre Lizenzen auf dem vorherigen Computer nach einer 15-tägigen Karenzzeit.

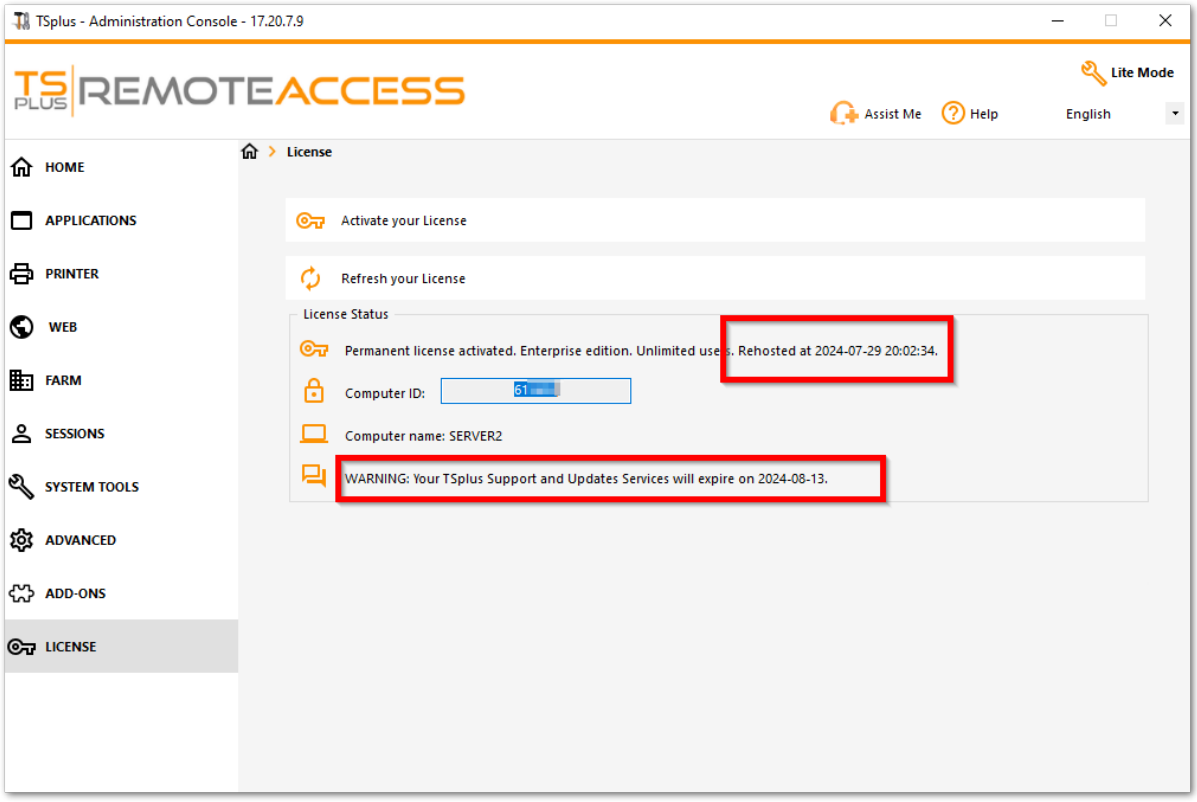
Klicken Sie auf den **„REHOST“** Taste



Ihre Lizenz ist rehosted!



Hinweis: Auf dem alten Server wird eine Nachricht mit dem Rehosting-Datum sowie dem Enddatum des Nutzungszeitraums des alten Servers (15 Tage) angezeigt.



Aktualisierungsfehler:

Führen Sie das Update-Release aus und überprüfen Sie, ob Ihr Problem nach dem Neustart Ihres Servers behoben wurde.

- Laden Sie die Aktualisierung veröffentlichen

2- Klonen Sie einen Server, während Sie den bestehenden Server beibehalten und eine neue Lizenz aktivieren.

Anforderungen

Beim Arbeiten mit geklonten virtuellen Maschinen ist es wichtig, den Computernamen und die Datenträger-ID zu ändern, um eine eindeutige TSplus Remote Access-Installation sicherzustellen und Lizenzprobleme zu vermeiden.

Computername Überlegungen

Der Computername wird im Windows-Registrierungseditor innerhalb des Images selbst gespeichert. Wenn er vor der Anwendung des Images geändert wird, wird er beim Booten von Windows von Sysprep überschrieben. Sie können jedoch einen Namen in einem vordefinieren. Unattended.xml Antwortdatei. Siehe Microsoft-Dokumentation für weitere Details.

Um den Computernamen festzulegen, fügen Sie den folgenden Abschnitt ein. Microsoft-Windows-Shell-Setup :

```
<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>
```

Volume-ID-Überlegungen

Die Volume-ID ist mit der Festplattenpartition verbunden, nicht mit dem Betriebssystem-Image. Sie kann vor der Anwendung des Images geändert werden und bleibt bestehen. Verwenden Sie volumeid.exe von Sysinternals, verfügbar unter Microsoft Sysinternals bevor Windows startet.

Bereitstellungsschritte

Beim Bereitstellen einer neuen virtuellen Maschine aus einem sysprepped Image wird Windows beim ersten Boot in die Out-Of-Box-Erfahrung (OOBE) eintreten und nach Konfigurationseinstellungen fragen.

Empfohlene Schritte für die Bereitstellung:

1. **Booten zu WinPE** – Bereiten Sie das System vor, ohne in Windows zu booten.
2. **Legen Sie die Volume-ID fest** – Ändern Sie es, bevor Sie das Bild anwenden, damit es erhalten bleibt.
3. **Das sysprepped Image bereitstellen** – Verwenden Sie DISM, um das Image anzuwenden auf C: .
4. **Setzen Sie den Computernamen offline** – Bearbeiten Sie die Registrierung im gemounteten Image.
5. **Kopiere ein Unattended.xml Datei** – Automatisieren Sie die OOBE-Konfiguration. Diese Datei kann vor der Bereitstellung dynamisch mit einem Skript geändert werden.
6. **Erstellen Sie ein Erststart-Skript** – Stellen Sie sicher, dass die endgültigen Konfigurationen mit nur einem Neustart vorgenommen werden.
7. **Neustart in Windows** – Windows finalisiert sich mit den angegebenen Konfigurationen.
8. **Remote Access-Lizenz zurücksetzen** – Führen Sie den folgenden Befehl aus:

Terminalfenster

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

Dies setzt die Lizenz zurück und wendet eine neue Lizenz an.

Bereitstellungsskript

Bitte finden Sie unten das zugehörige WinPE-Bereitstellungsskript.

Terminalfenster

```
<# 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
```

Lizenzaktivierung

Nach der Bereitstellung generiert die Aktivierung einer Lizenz eine neue Computer-ID für die virtuelle Maschine. Diese Computer-ID wird vom Lizenzportal erstellt, wenn eine Maschine eine Test- oder Lizenzaktivierung anfordert. Bei geklonten virtuellen Maschinen ist die Lizenzaktivierung obligatorisch. Verwenden Sie entweder einen Aktivierungsschlüssel oder einen Volumenlizenzschlüssel. **Offline-Setups sind nicht erlaubt** aufgrund von Sicherheitsbedenken. Für detaillierte Aktivierungsschritte siehe TSplus-Befehlsliste .

Schlussfolgerung

Dieser Leitfaden beschreibt wichtige Überlegungen zur Bereitstellung von geklonten virtuellen Maschinen mit TSplus Remote Access. Er bietet wesentliche Schritte zur korrekten Konfiguration und Lizenzierung des Systems und muss an Ihre Bedürfnisse und Anforderungen angepasst werden.

Wie man: Webserver an mehrere Netzwerkkarten bindet

Übersicht

Einige Anwendungsfälle könnten erfordern, dass der Terminal Service Plus-Webserver auf mehr als einer Netzwerkkarte lauscht, zum Beispiel, wenn der Server zu mehreren verschiedenen Netzwerken gehört.

Diese Funktion erfüllt dieses spezifische Bedürfnis.

Binding des Webservers an mehrere Netzwerkkarten

Um den Terminal Service Plus-Webserver an mehrere Netzwerkkarten zu binden, müssen Sie:

- Erstellen Sie die Datei „settings.bin“ im Ordner „C:\Program Files (x86)\TSplus\Clients\webserver“
- Fügen Sie die folgende Zeile mit allen lokalen IP-Adressen für alle Netzwerkadapter hinzu, die Sie binden möchten, zum Beispiel:

  bind_nic=“127.0.0.3”,“127.0.0.4”
- Webserver neu starten (AdminTool > Web > Webserver neu starten), um Änderungen anzuwenden

Der Terminal Service Plus-Webserver wird nun alle Anfragen von allen gebundenen Netzwerkkarten empfangen (in unserem Beispiel würde die Bindung automatisch an 127.0.0.3, 127.0.0.4 und 127.0.0.1 erfolgen).

Wie man: Einen benutzerdefinierten HTTP-Header hinzufügen

Voraussetzungen

Diese Funktion ist sehr technisch und diese Dokumentation ist nur für technische Experten.

Sie sollten mit dem HTTP-Protokoll sowie mit HTTP-Headern vertraut sein.

Übersicht

Einige Anwendungsfälle könnten erfordern, dass der Terminal Service Plus-Webserver zusätzlich zu den Standard-HTTP-Headern einen oder mehrere benutzerdefinierte HTTP-Header zurückgibt.

Diese Funktion erfüllt dieses spezifische Bedürfnis.

Einrichten eines benutzerdefinierten HTTP-Headers

Um Ihren eigenen benutzerdefinierten HTTP-Header hinzuzufügen, müssen Sie:

- Erstellen Sie die Datei „headers.bin“ im Ordner „C:\Program Files (x86)\TSplus\Clients\webserver“
- Fügen Sie die benutzerdefinierten Header hinzu, getrennt durch eine neue Zeile, zum Beispiel: header1=X-Frame-Options
- Webserver neu starten (AdminTool > Web > Webserver neu starten), um Änderungen anzuwenden

Der Terminal Service Plus-Server wird jetzt auf alle Anfragen mit diesem benutzerdefinierten HTTP-Header zusätzlich zu den Standard-Headern reagieren.

HTML-Seiten und Anpassung

Sie können die bereitgestellten HTML-Seiten mit Notepad oder Notepad++ bearbeiten, um die Benutzeroberfläche anzupassen.

index.html-Seite

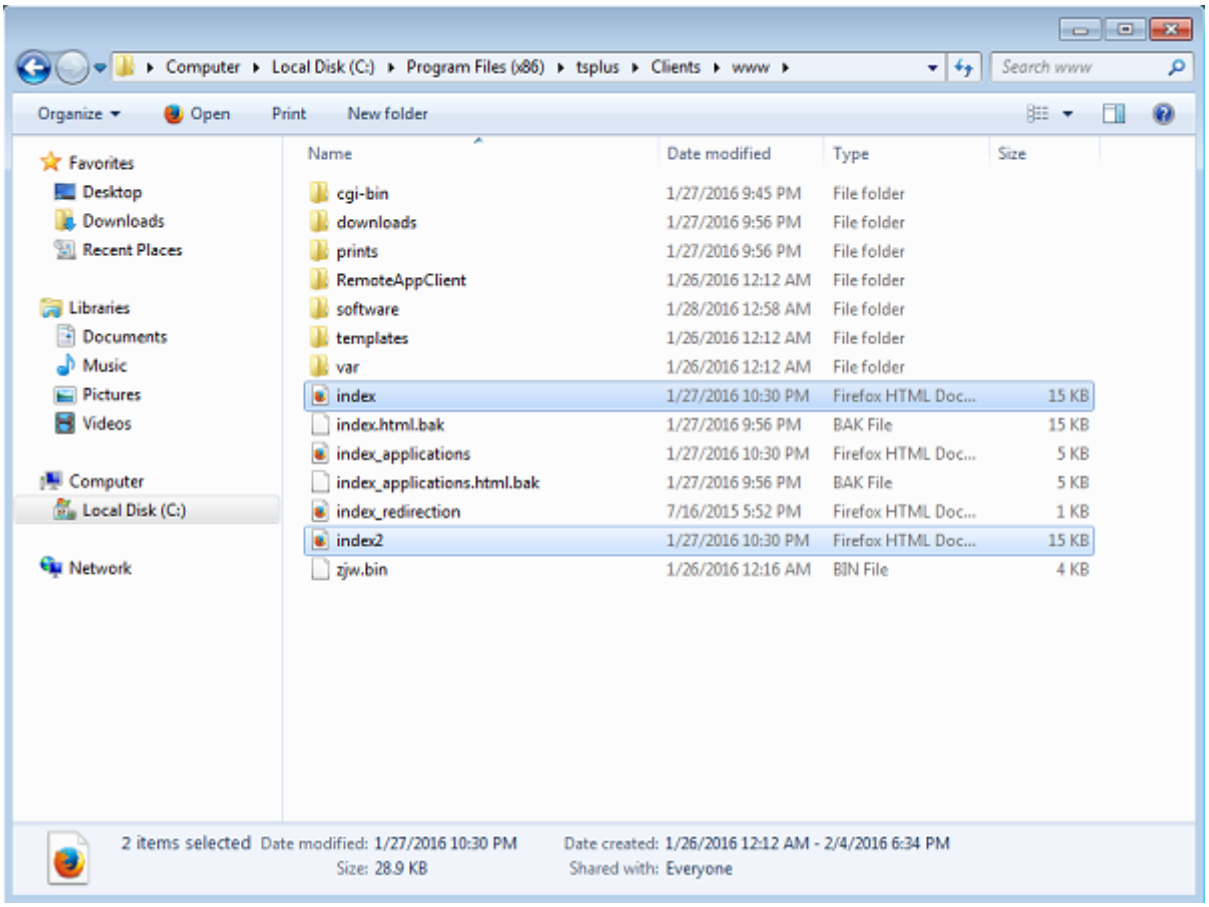
Die index.html befindet sich im Stammordner des Webservers.

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

Index.html-Seite ist die Standard-Webseite. Sie ist wie eine Front-End-Portal-Seite mit Links zu den Verbindungsseiten, die im \www\-Ordner gespeichert sind.

Diese Webseite kann kopiert und umbenannt werden, um mehrere Konfigurationen und / oder Anmeldeinformationen zu ermöglichen.

Zum Beispiel lassen Sie uns index.html kopieren und in index2.html umbenennen, diese Seite wird unter dieser URL verfügbar sein. http://localhost/index2.html



Achten Sie darauf, dass wenn Sie den Dateinamen „index.html“ in „index2.html“ ändern und das Web Applications Portal verwenden, Sie die folgende Variable in dieser Datei ändern müssen: „page_configuration[„applications_portal“] = „index_applications.html“ in „index2_applications.html“ ändern und die Datei „index_applications.html“ in „index_2applications.html“ umbenennen.

Die Standard index.html enthält alle möglichen Optionen:

- RemoteApp-Zugriff auf Anwendungen, Verbindung außerhalb des Webbrowsers
- Verbindung über HTML5 von jedem Gerät
- Lokale Druckeinstellungen

Sie können Kopf- und Fußzeile im Design der Webportal-Funktion auf der Kachel der Webportal-Einstellungen im Web-Tab ändern.

Durch das Bearbeiten der index.html-Webseite haben Sie Zugriff auf verschiedene Einstellungen.

// ---------- Zugriffsconfiguration ----------

var user = ""; // Anmeldename, der verwendet wird, um sich mit dem Remote-Server zu verbinden ("" lassen, um den auf dieser Seite eingegebenen Anmeldename zu verwenden)

var pass = ""; // Passwort, das beim Verbinden mit dem Remote-Server verwendet wird (lassen Sie "" leer, um das auf dieser Seite eingegebene Passwort zu verwenden)

var domain = ""; // Domäne, die beim Verbinden mit dem Remote-Server verwendet werden soll ("" lassen, um die auf dieser Seite eingegebene Domäne zu verwenden)

var server = "127.0.0.1"; // Server, mit dem verbunden werden soll ("" lassen, um localhost und/oder den auf dieser Seite gewählten Server zu verwenden)

var port = ""; // Port zum Verbinden ("" lassen, um localhost und/oder den auf dieser Seite gewählten Port des Servers zu verwenden)

var lang = "as_browser"; // Sprache zu verwenden

var serverhtml5 = “127.0.0.1”; // Server, mit dem verbunden werden soll, wenn der HTML5-Client verwendet wird

var porthtml5 = "3389"; // Port zum Verbinden, wenn der HTML5-Client verwendet wird

var cmdline = ""; // Optionaler Text, der in die Zwischenablage des Servers eingefügt wird, sobald die Verbindung hergestellt ist

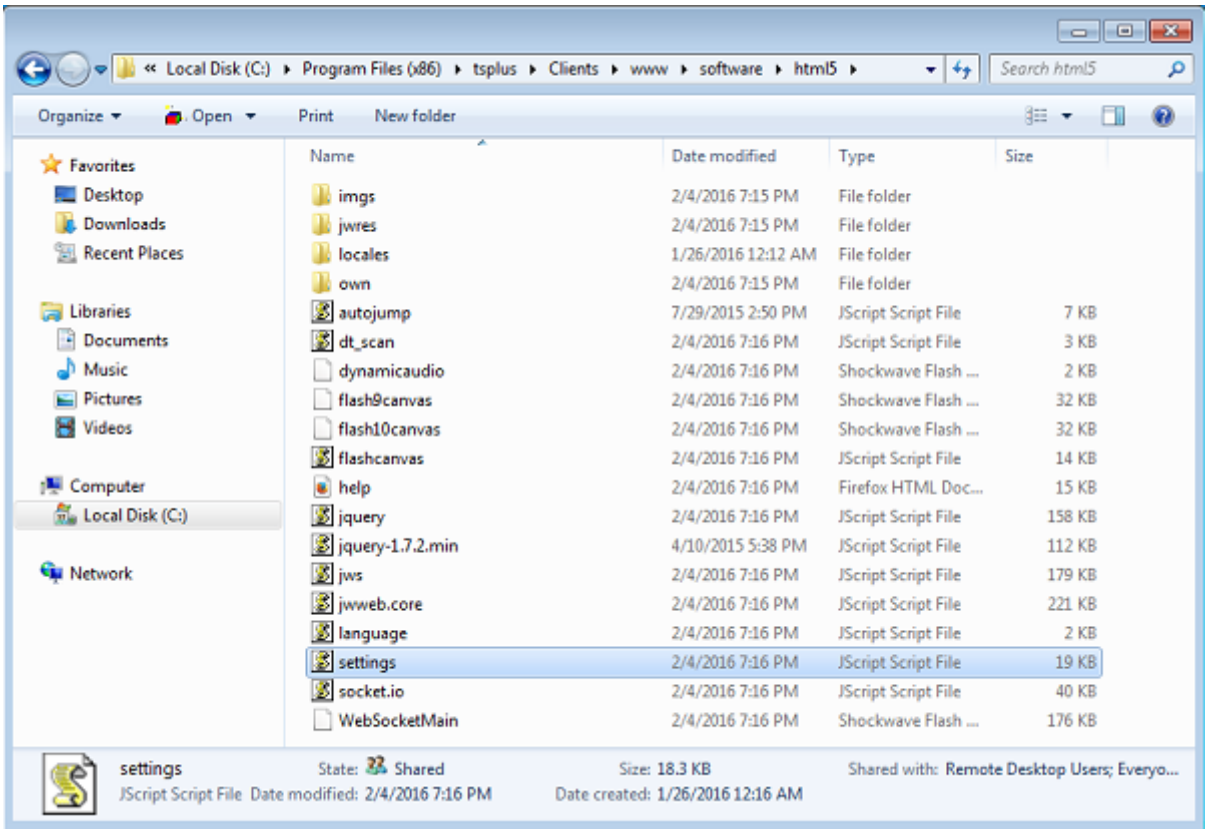
// ---------- Ende der Zugriffs-Konfiguration ----------

Zum Beispiel werde ich demo/Psw als Benutzername/Passwort festlegen, indem ich bearbeite:

var user = "Demo"; var pass = "Psw";

Durch dies werden die vorausgefüllten Anmeldeinformationen bei jedem Besuch des Portals sichtbar.

Eine weitere sehr wichtige Konfigurationsdatei ist **Einstellungen.js** , befindet sich in C:\Program Files (x86)\TSplus\Clients\www\software\html5:



Diese Datei enthält verschiedene Einstellungen für den HTML5-Webclient, wie das Deaktivieren von Sound, die Zwischenablage oder das Erlauben der Sitzungswiederverbindung, wenn der Browser-Tab geschlossen ist.

- Zwischenablage deaktivieren:

W.clipboard = "ja"; //oder "nein"

- Das Deaktivieren des Sounds erfolgt mit dieser Einstellung:

W.playsound = false;

- Ändern der Standardauflösung für mobile Geräte:

W.viewportwidth = "1024" - Die Höhe wird vom Browser berechnet.

- HTTPS für die Remote-Verbindung erzwingen

W.forcealways_ssl = true;

- Sitzungswiederverbindung zulassen, wenn der Browser-Tab geschlossen ist:

W.send_logoff = false;

- Eine Warnmeldung hinzufügen, um das Schließen des Browser-Tabs zu verhindern:

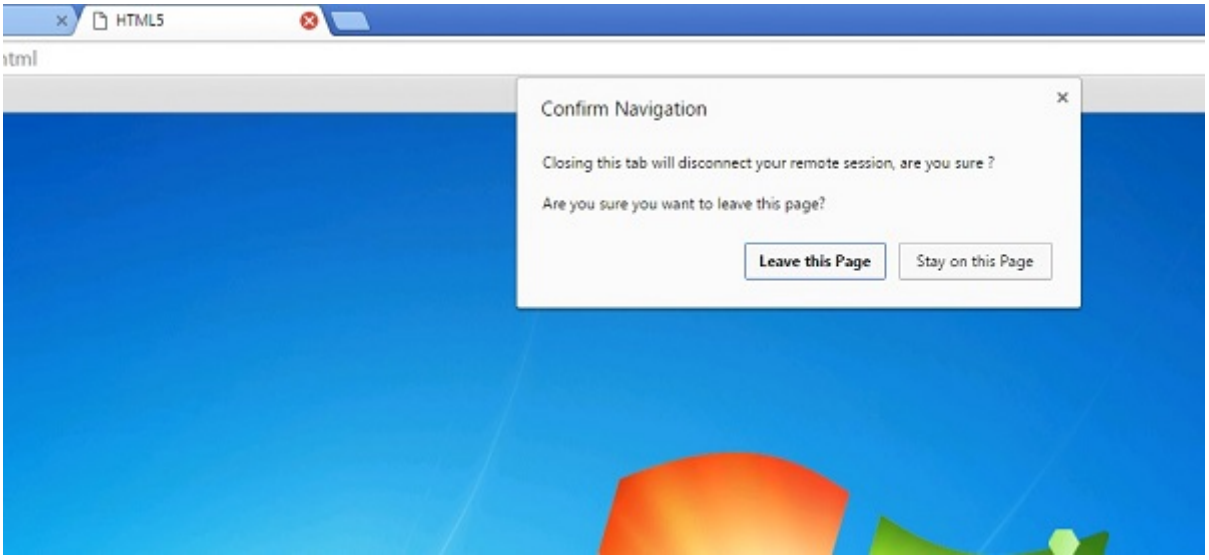
suche den Parameter “W.pageUnloadMessage = "" ”.

Ich habe ein Beispiel für eine Nachricht festgelegt, die unten verwendet werden kann:

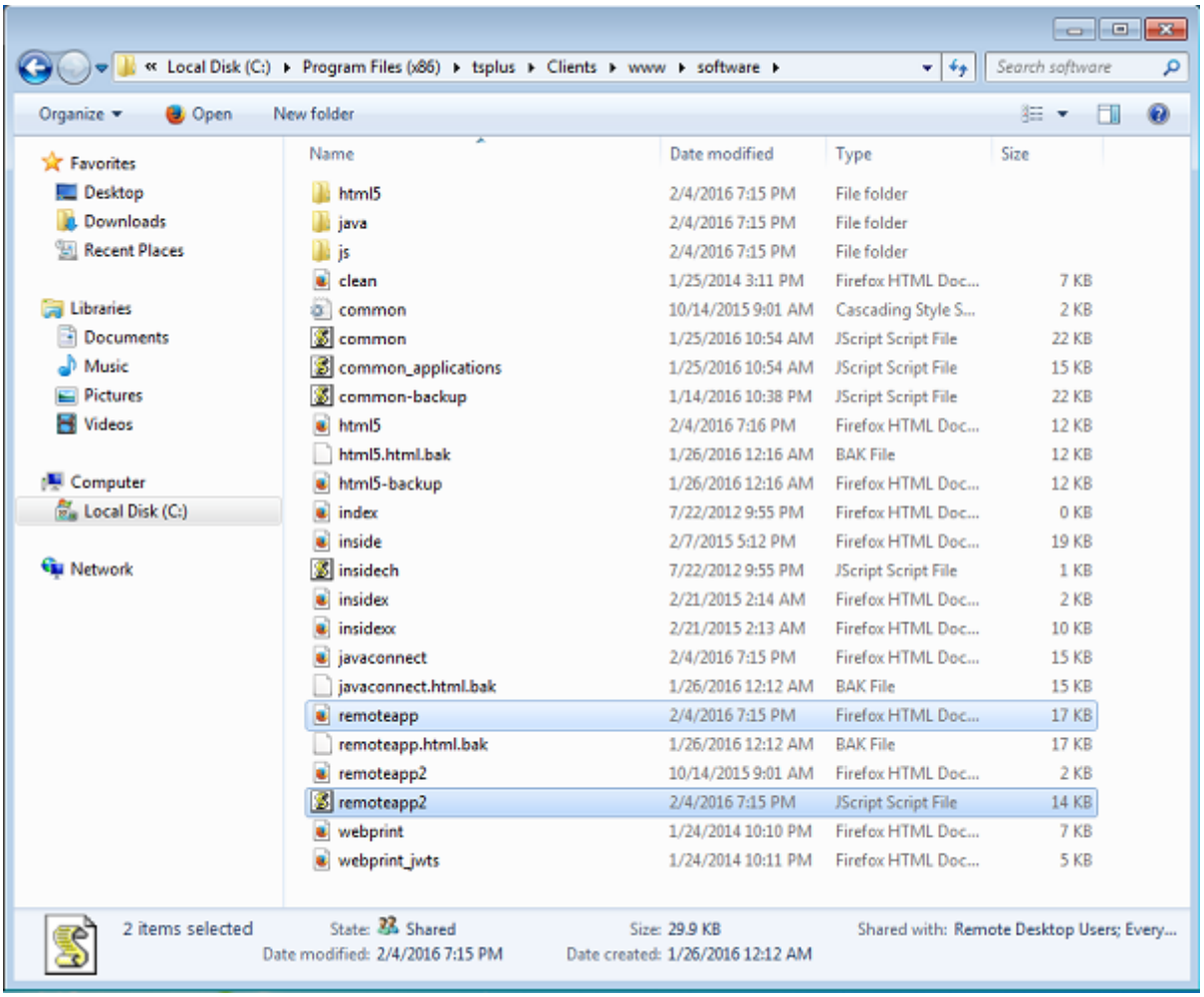
W.pageUnloadMessage = "Das Schließen dieses Tabs trennt Ihre Remote-Sitzung. Sind Sie sicher?"; //Dialog, der zurückgegeben wird, wenn die Seite entladen wird.

Wichtiger Hinweis: Eigene Dialoge werden nicht in allen Browsern unterstützt.

//2. Der HTML-Standard unterscheidet nicht zwischen der Aktion Seitenaktualisierung und Seiten schließen, das Dialogfeld wird auch bei der Seitenaktualisierung angezeigt.



Die allgemeinen Einstellungen für die RemoteApp-Webseite werden im Software-Ordner in zwei verschiedenen Dateien gespeichert: **remoteapp.html** und **remoteapp2.js** .



Beispiel für verfügbare Einstellungen, die in **remoteapp2.js** :

// Remote Desktop Server

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

Windows-Authentifizierung

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

// Optionale Befehlszeilenparameter

var remoteapp2_apppath = ”;

// RemoteApp-Modus

var remoteapp2_wallp = 'grün'; var remoteapp2_remoteapp = 'ein';

// Bildschirm

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 = 'aus';

var remoteapp2_span = 'aus';

// Laufwerkszuordnung (erforderlich für das Drucken)

var remoteapp2_disk = '1';

// Drucken

var remoteapp2_printer = 'aus';

var remoteapp2_preview = 'aus';

var remoteapp2_default = 'on';

var remoteapp2_select = 'aus';

// Hardware

var remoteapp2_com = '0';

var remoteapp2_smartcard = '0';

var remoteapp2_serial = 'aus';

var remoteapp2_usb = 'aus';

var remoteapp2_sound = 'ein';

var remoteapp2_directx = 'aus';

// Verschiedenes

var remoteapp2_alttab = '0';

var remoteapp2_firewall = '1';
```

```
var remoteapp2_localtb = '32';

var remoteapp2_lock = 'aus';

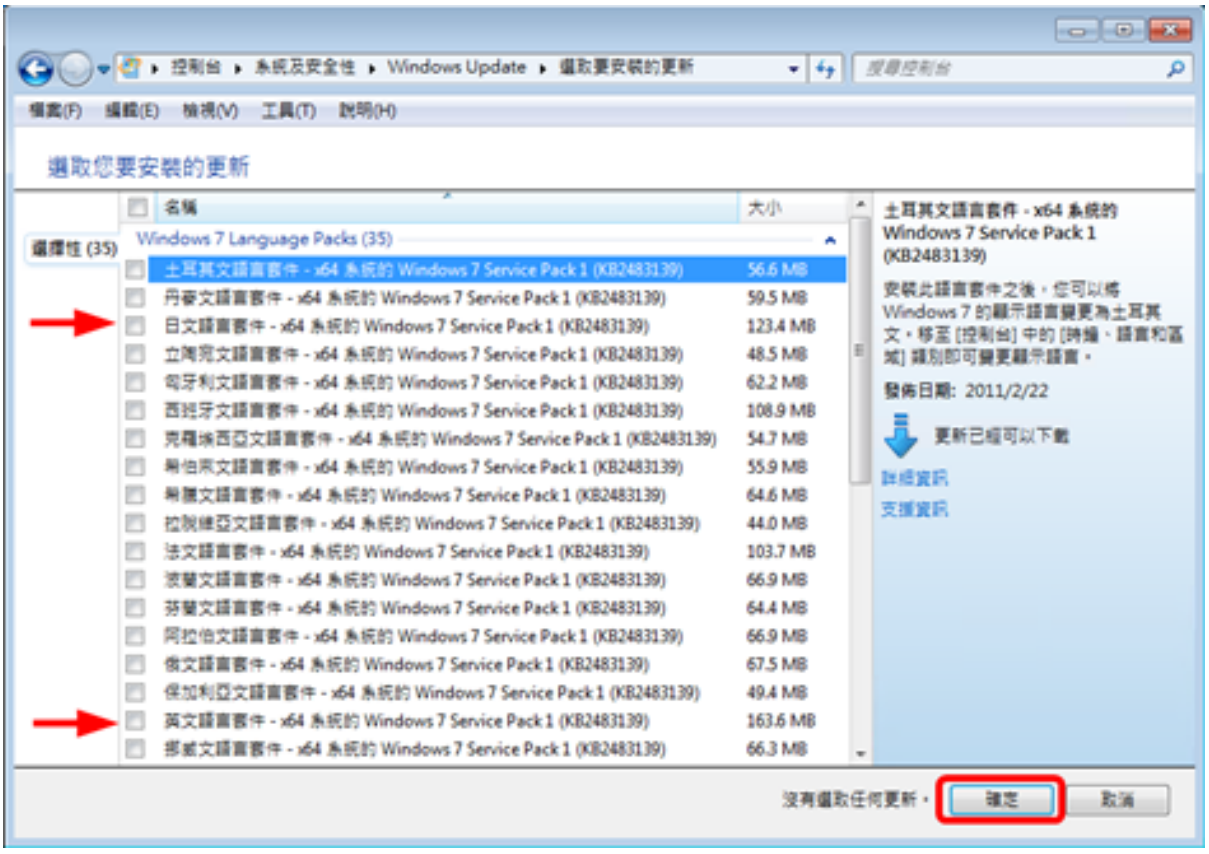
var remoteapp2_rdp5 = 'aus';

var remoteapp2_reset = 'aus';
```

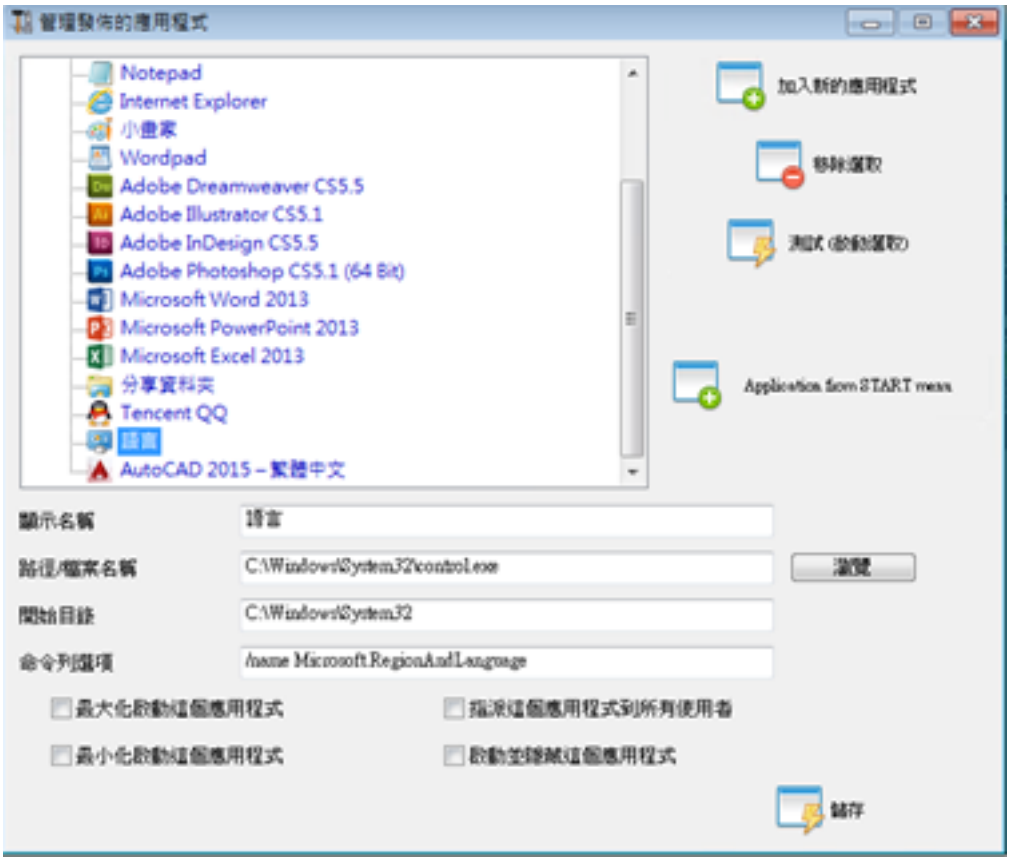
HTML5 : Sprache auf Chinesisch ändern

Sie benötigen Windows 7 Enterprise oder Ultimate / Windows 8 Enterprise oder Professional, um Mehrsprachigkeit auf einem System zu nutzen.

Sie können jede Sprache auf dem System installieren, wenn Sie dies benötigen.



Sie könnten ein Sprach-Applet veröffentlichen, damit Benutzer ihre eigene O/S-Sprache der Benutzeroberfläche ändern und IME (Input Method Editor) hinzufügen können.

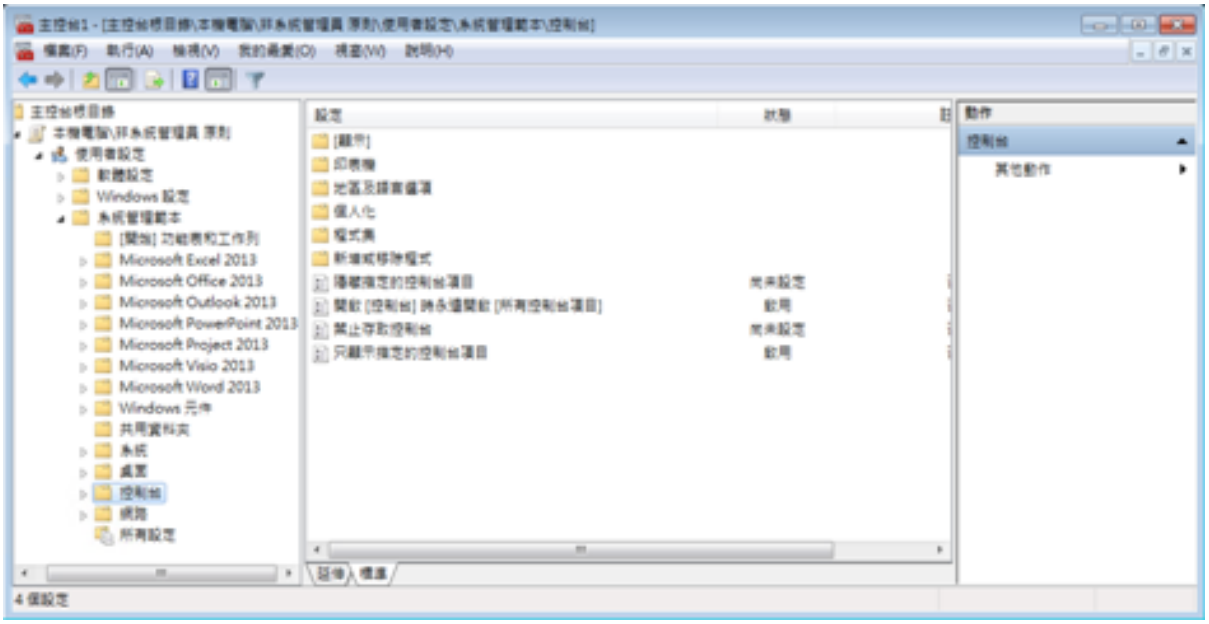


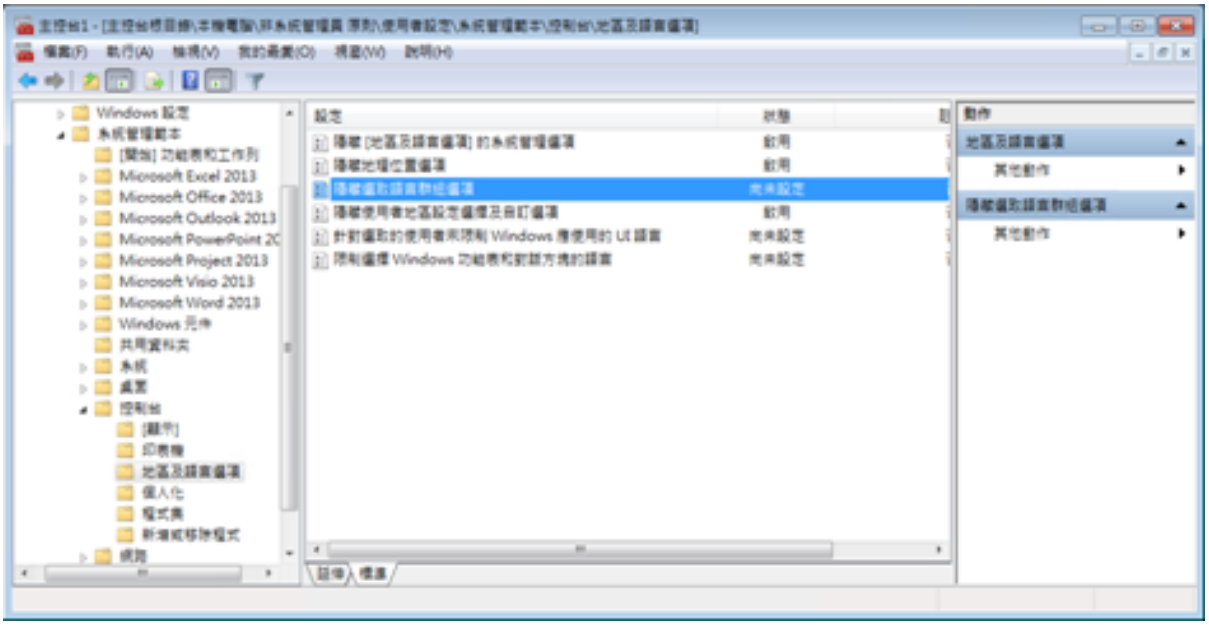
Für Windows 7: control /name Microsoft.RegionAndLanguage

Für Windows 8: Steuerung /name Microsoft.Language

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

Optional: so können Sie das Verhalten der Systemsteuerung für Benutzer über GPO einschränken:

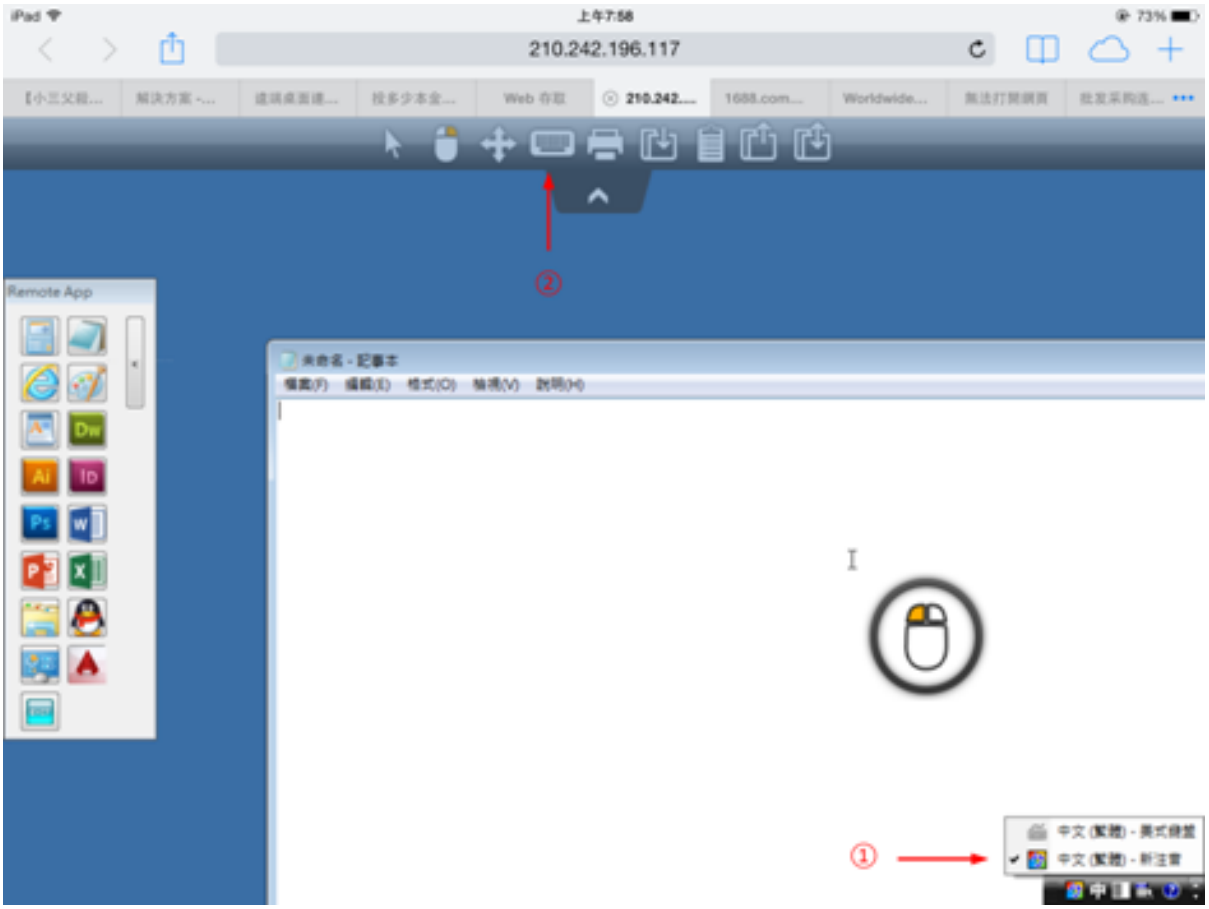




Benutzer können die O/S-Sprache der Benutzeroberfläche nach dem Anmelden am System ändern. (Benutzer müssen sich abmelden und erneut anmelden, damit diese Einstellung wirksam wird.)



Der Benutzer muss zuerst die chinesische IME auswählen, um chinesische Zeichen einzugeben.


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 肉
.?123
上一個
確認
下一個
換行


210.242.196.117
確認
.?123
一聲
.?123

HTML5-Client: Was ist der Unterschied zwischen Websockets und XHR?

Websockets ist die persistente Verbindung, die verwendet werden kann, um Daten ohne sequentielle Reihenfolge und ohne HTTP-Header zu empfangen/zu senden.

Xhr-Polling erstellt eine neue Anfrage mit dem HTTP-Header und wartet auf die Antwort mit dem HTTP-Header, ebenfalls in sequenzieller Reihenfolge.

Wenn Sie dies tun, sieht der XHR-Datenfluss immer so aus:

HTTP_HEADER_ANTWORT

auch bevor die Daten heruntergeladen werden können, müssen sie mit HTTP_HEADER angefordert werden, daher sein Name: xhr-polling.

Websockets-Datenfluss kann so aussehen:

FRAME_DATA_SEND FRAME_DATA_SEND FRAME_DATA_RECEIVE FRAME_DATA_SEND FRAME_DATA_RECEIVE FRAME_DATA_RECEIVE

Es handelt sich auch um zufällige Datenübertragung/-empfang ohne spezielle Reihenfolge und ohne HTTP-Headerdaten.

Das macht die Nutzung mit Reverse-Proxys aufgrund des Fehlens von Websockets-Unterstützung durch die meisten bekannten Reverse-Proxys unmöglich; aber die Hälfte des xhr-Transports könnte mit dem Apache-Reverse-Proxy funktionieren.

Auch ansehen: HTML5-Client: Unterstützte Browser

HTML5-Client: RDP-Sitzungsauflösung auf mobilen Geräten

Die gängige Bildschirmauflösung der meisten Geräte, insbesondere von Mobiltelefonen, beträgt 320x480, aber das ist offensichtlich nicht ausreichend, um die RDP-Sitzung zu erstellen.

Daher wurde die Auflösung auf 800 in der Breite voreingestellt. Die Höhe der Auflösung wird durch die native Logik versteckter Browser neu berechnet. Je höher die Breite, desto größer die Höhe.

- Als Beispiel beträgt die Standardauflösung 320x480. Wenn Sie nun die Ansicht auf 800 einstellen, berechnet der Browser den Wert für die Höhe beispielsweise auf 800x904. Wenn Sie die Breite auf 1280 einstellen, beträgt sie dann 1280x1160 usw.

Die Höhe und Breite hängen von der Landschafts-/Hochformatansicht Ihres Geräts ab, wie 800x904 oder 904x800 usw. Jeder Browser kann dies mit seiner eigenen Logik neu berechnen, um den RDP-Bildschirm in den Ansichtsbereich Ihres Geräts einzupassen, und kann je nach Browser unterschiedlich sein, selbst wenn er auf demselben Gerät verwendet wird.

Wenn Sie die Höhe manuell einstellen, brechen Sie das Seitenverhältnis Ihres Geräts, und die endgültige RDP-Sitzung wird außerhalb Ihrer Portansicht liegen. Um diese Bereiche zu erreichen, müssen Sie zu den gewünschten Positionen scrollen.

- Daher wird empfohlen, die Höhe nicht manuell festzulegen, sondern das Gerät die Höhe automatisch wählen zu lassen.

Wenn Sie mehr Höhe benötigen, erhöhen Sie die Breite!

Durch Tests auf Mobiltelefonen war der gute Wert für die Breite 800. Sie müssen jedoch darauf achten: Die CPUs der meisten Mobiltelefone sind normalerweise langsam, daher wird die CPU-Auslastung steigen, wenn Sie die Höhe erhöhen. Auf Tablet-Geräten sind die CPUs schneller, daher wird empfohlen, die Breite auf einen höheren Wert wie 1280 einzustellen und dem Gerät zu erlauben, den Wert für die Höhe neu zu berechnen.

Weil einige Browser wie FireFox Mobile das Festlegen des Viewports nach dem Laden der Seite nicht erlauben, wurde dieser Wert fest in die Datei Clients\www\software\html5.html gesetzt.

Zum Beispiel ändern Sie es zu:

um die Breite zu erhöhen und gleichzeitig die Höhe, die von der nativen internen Logik der Browser neu berechnet wird.

Als zweites Beispiel, es zu ändern in:

würde den Ansichtsbereich brechen und die RDP-Sitzung würde nicht auf den Bildschirm passen.

HTML5-Client: Parameter in der URL-Adresse

Wenn Sie den HTML5-Client von Terminal Service Plus verwenden, um eine Verbindung zu einem Remote-Server herzustellen, können Sie mehrere Parameter in der URL-Adresse angeben, um die Standardparameter zu überschreiben, wie zum Beispiel:

- Benutzeranmeldung
- Benutzerpasswort
- Programm zum Ausführen
- Startverzeichnis für das Programm zum Ausführen
- Befehlszeile für das auszuführende Programm

Führen Sie eine bestimmte Anwendung aus

Hier ist ein Beispiel für eine vollständige URL-Adresse, um eine Remote-Sitzung für den Benutzer „demo“ mit dem Passwort „demo“ zu öffnen und den Standard-Notepad beim Öffnen der Sitzung zu starten:

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

Bitte beachten Sie, dass in der URL-Adresse alle Schrägstrichzeichen wiederholt werden müssen. **4 mal** .

Sie müssen nicht alle diese Parameter gleichzeitig angeben: Die nicht angegebenen Parameter haben ihren standardmäßig konfigurierten Wert.

Mit Webanmeldeinformationen verbinden

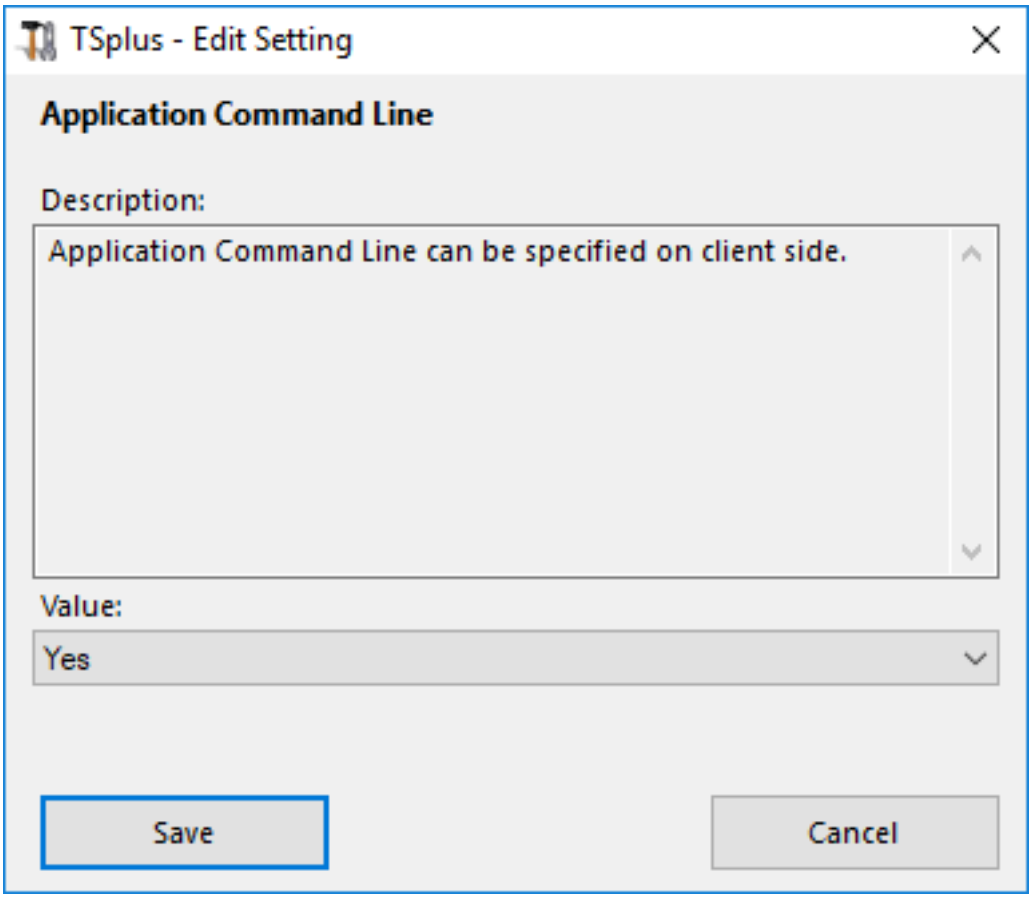
Wenn Sie eine verwenden möchten Web-Anmeldeinformationen Um sich zu verbinden, können Sie es in einer URL über das Hinzufügen eines "@" vor dem Web-Login übergeben.

Hier ist ein Beispiel für eine URL-Adresse, um eine Remote-Sitzung mit dem Anwendungsbereich für Web-Anmeldeinformationen „1234“ mit dem Passwort „demo“ zu öffnen:

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

Diese Nutzung auf die Standardanwendungen der Benutzer beschränken

Sie können die Anwendungsbefehlszeile für Benutzer deaktivieren, indem Sie auf die **Erweiterte —> Sitzungsregister** der AdminTool, indem Sie auf die Einstellung „Anwendungsbefehlszeile“ doppelklicken und den Wert auf „Nein“ setzen.



HTML5-Client: Unterstützte Browser

Wenn Ihr Browser beim Start mit dem HTML5-Client eine rote Warnung anzeigt

Es bedeutet, dass Ihr Browser keine Websockets unterstützt oder Ihr Browser kein Canvas unterstützt.

Solche Browser, die diese Technologien nicht unterstützen, sind IE6, IE7, IE8, IE9 und benötigen FLASH, um diese Funktionen zu emulieren.

Browser, die Websocket und Canvas unterstützen

Browser	Leinwand	Websocket
FireFox	Vollständig	Vollständig ab Version 4
Chrome	Vollständig	Voll in den bekanntesten Versionen auf PCs
Opera	Vollständig	Vollständig in den neuesten Versionen
IE6	Blitz	Flash (emuliert und ohne Proxy-Unterstützung)
	Blitz	XHR (mit Proxy-Unterstützung)
IE7	Blitz	Flash (emuliert und ohne Proxy-Unterstützung)
	Blitz	XHR (mit Proxy-Unterstützung)
IE8	Blitz	Flash (emuliert und ohne Proxy-Unterstützung)
	Blitz	XHR (mit Proxy-Unterstützung)
IE9	Blitz	Flash (emuliert und ohne Proxy-Unterstützung)
	Blitz	XHR (mit Proxy-Unterstützung)
IE10	Vollständig	Vollständig
Android-nativ	Vollständig	XHR
Opera mobil	Vollständig	Vollständig in den neuesten Versionen
Firefox mobil	Vollständig	Vollständig
Safari mobil	Vollständig	Voll in den neuesten Versionen ab iOS4, sonst emuliert über XHR

Auch ansehen: Was ist der Unterschied zwischen Websockets und XHR?

Wenn Ihr Browser die Seiten automatisch auf die HTTPS-Adresse neu lädt

Es bedeutet, dass der Websockets-Transport nicht unterstützt wird. Dies ist bei mehreren nativen Android-Mobilbrowsern der Fall.

Es liegt daran, dass der Browser automatisch auf den XHR-Transport umschaltet.

Aber da diese Transportebenen über lange Distanzen mit dem HTTP-Protokoll arbeiten, erstellt jede Anfrage eine neue Verbindung. Es ist sehr langsam und instabil, neue Verbindungen zu erstellen (bis zu 20 neue Verbindungen pro Sekunde), daher wurde das Programm so konzipiert, dass die Seite automatisch auf die HTTPS-Adresse neu geladen wird, um die HTTPS-Verbindung durchzusetzen.

Physisch erhalten Sie auch größtenteils eine persistente, gesicherte Verbindung, die auf langen Strecken viel stabiler ist. Die Logik des Browsers nutzt bereits etablierte SSL-Verbindungen wieder, anstatt eine neue Verbindung wie bei der Verwendung des HTTP-Protokolls zu erstellen.

Dieses Verhalten kann durch die folgende Option in der Datei setting.js geändert werden, die sich im TSplus-Programmfolder unter folgendem Pfad befindet: Clients\www\software\html5\settings.js:

forcesslforxhr = false;

Es wird jedoch absolut nicht empfohlen, die Verwendung von SSL im XHR-Modus zu deaktivieren.

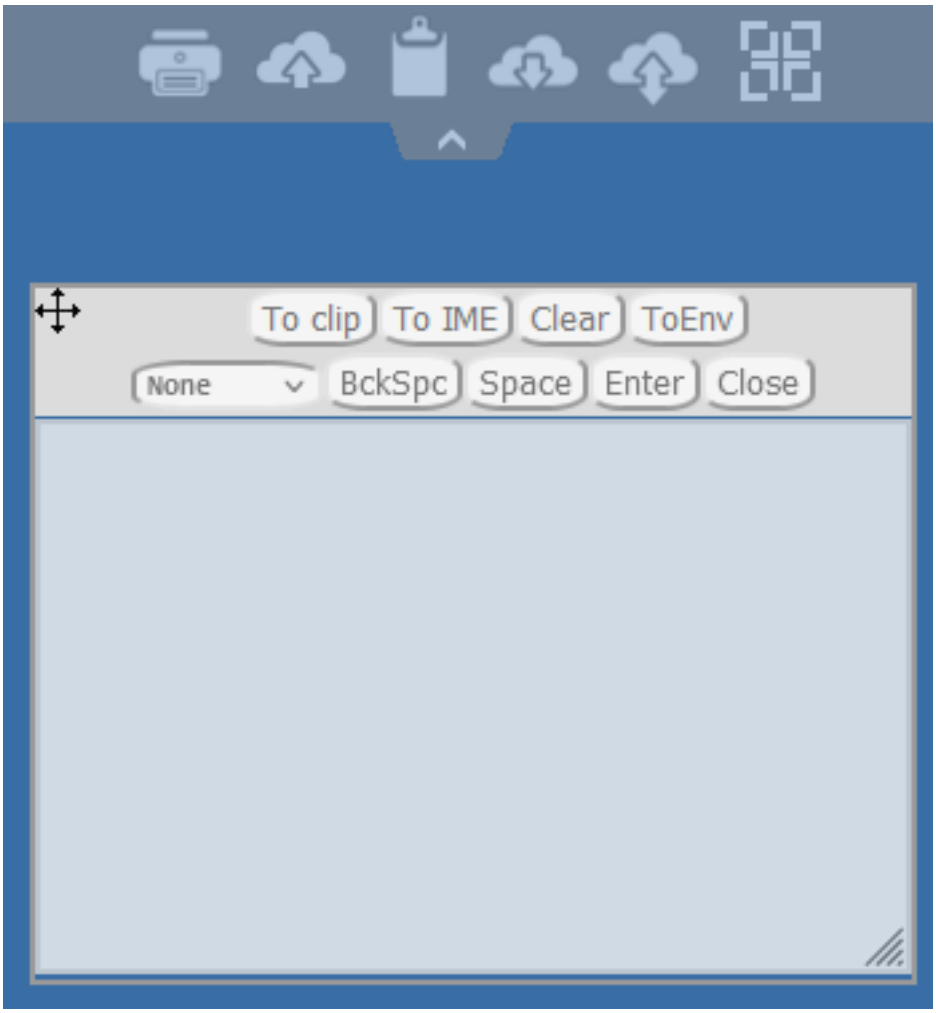
Wenn Sie keine Datei mit dem Namen „settings.js“ im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software\html5“ haben, dann ist Ihre TSplus-Version älter und diese Dokumentation gilt nicht. Bitte aktualisieren Sie zuerst Ihr System oder kontaktieren Sie den Support.

HTML5-Client: Verwendung der Zwischenablage

Die Zwischenablage finden Sie im HTML5-Hauptmenü, mit diesem Symbol:



Die meisten Browser, mit Ausnahme älterer MSIE-Browser, unterstützen aus Sicherheitsgründen nicht das direkte Lesen und Schreiben der Zwischenablage.



Hier sind die verschiedenen Aktionen:

- **Zu Clip** sendet den Inhalt des TEXTBEREICHS an die RDP-SITZUNG und erzeugt am Ende Ctrl+V, um den Text IN DER RDP-SITZUNG einzufügen (Ihre EIGENE UMGEBUNG wird nicht berührt!!!)

- **Um IME** : konvertiert Zeichen aus dem TEXTBEREICH in Tasteneingaben und sendet sie, als ob Sie die Tastatur verwendet hätten. (Dieser Button ist notwendig, wenn Sie den Text dort eingeben möchten, wo die Eingabe von Text aus der Zwischenablage in der RDP-Sitzungsanwendung nicht unterstützt wird.)

- **Umgebung** TRIES, um Text aus dem TEXTBEREICH in Ihre eigene Zwischenablage außerhalb Ihres Browsers (nicht in die RDP-Sitzung, sondern in Ihre eigene UMGEBUNG!!!!) zu kopieren. Da das Hinzufügen von Text zur eigenen Zwischenablage eine privilegierte Aktion ist, muss es durch einen Klick ausgeführt werden.

- **Zu Clip** wie erwähnt, behandelt das Einfügen von Text in rdp-clip+ctrl/v-Aktionen, ohne Text

außerhalb des eigenen Browsers hinzuzufügen, aus Sicherheitsgründen, da es ziemlich dumm wäre, Text in die eigene Zwischenablage zu legen, wenn dies nicht wirklich gewünscht ist. Verwenden Sie dafür "ToEnv", dieses Verhalten bleibt so und wird nicht geändert, da es so angefordert wurde.

- **Rücktaste** sendet den Befehl der RDP-Sitzung für die BACKSPACE-Taste (Ihre App muss fokussiert sein und die Aktion der Backspace-Taste unterstützen)

- **Raum** sendet den Befehl für die RDP-Sitzung mit der Leertaste (Ihre App muss fokussiert sein und die Aktion der Leertaste unterstützen)

- **Eingeben** : sendet den Befehl für die Eingabetaste an die RDP-Sitzung (Ihre App muss fokussiert sein und die Aktion der Eingabetaste unterstützen)

Um den Text aus der Sitzung in die Zwischenablage zu kopieren, verwenden Sie Strg+C, und um den Text aus der Zwischenablage einzufügen, verwenden Sie Strg+V.

Achten Sie jedoch darauf, den Text mit Strg+C zu kopieren, warten Sie einige Zeit, bevor Sie die gedrückten Strg+C-Tasten loslassen, da der angeforderte Text aus der Zwischenablage nicht zu Ihrer Umgebungszwischenablage hinzugefügt wird, wenn der Text ankommt, nachdem Sie diese Tastenkombination losgelassen haben. Auf diese Weise wird eine native Unterstützung zum Kopieren in die Zwischenablage des Browsers verwendet, die durch Strg+C initiiert wird.

Alternativ können Sie **verwenden Sie das Zwischenablage-Menü** Um Text aus der RDP-Sitzungszwischenablage zu kopieren und einzufügen.

Dort können Sie den Text einfach in die RDP-Sitzungszwischenablage einfügen oder ihn in die Zwischenablage hinzufügen und automatisch Ctrl+C in der RDP-Sitzung auslösen, um den Text einzufügen. Das Zwischenablagenmenü kann über das Aktionsmenü oder Shift + F11 geöffnet werden.

- Wenn Sie die Zwischenablage mit der Maus innerhalb einer RDP-Sitzung kopieren, wird der Text an den Browser gesendet, und sobald Sie den Fokus des Browsers verlassen, erscheint das Zwischenablagenmenü automatisch, um Sie darüber zu informieren, dass es einen Zwischenablagetext gab und dass Sie ihn nicht zu Ihrer Zwischenablage hinzugefügt haben.

Um dieses Verhalten zu vermeiden, setzen Sie die folgende Zeile im Clients-Ordner. Der Standardpfad ist: C:\Program Files(x86)\tsplus\Clients\www\software\html5\settings.js :

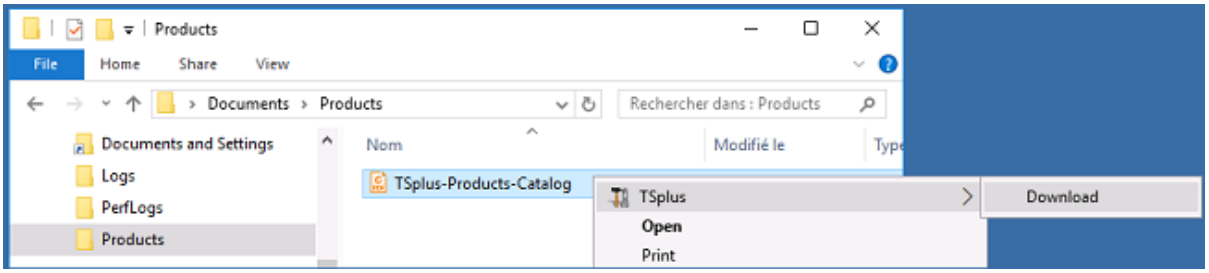
openonclipblur = false;

Wenn Sie keine Datei mit dem Namen „settings.js“ im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software\html5“ haben, dann ist Ihre TSplus-Version älter und diese

Dokumentation gilt nicht. Bitte aktualisieren Sie zuerst Ihr System oder kontaktieren Sie den Support.

HTML5-Client: Dateiübertragung verwenden

Dateiübertragungen können auf verschiedene Weise mit TSplus durchgeführt werden: seit Version 12.50, **Ein kontextuelles Menü steht zur Verfügung, um Dateien vom Server auf den lokalen PC herunterzuladen.** :



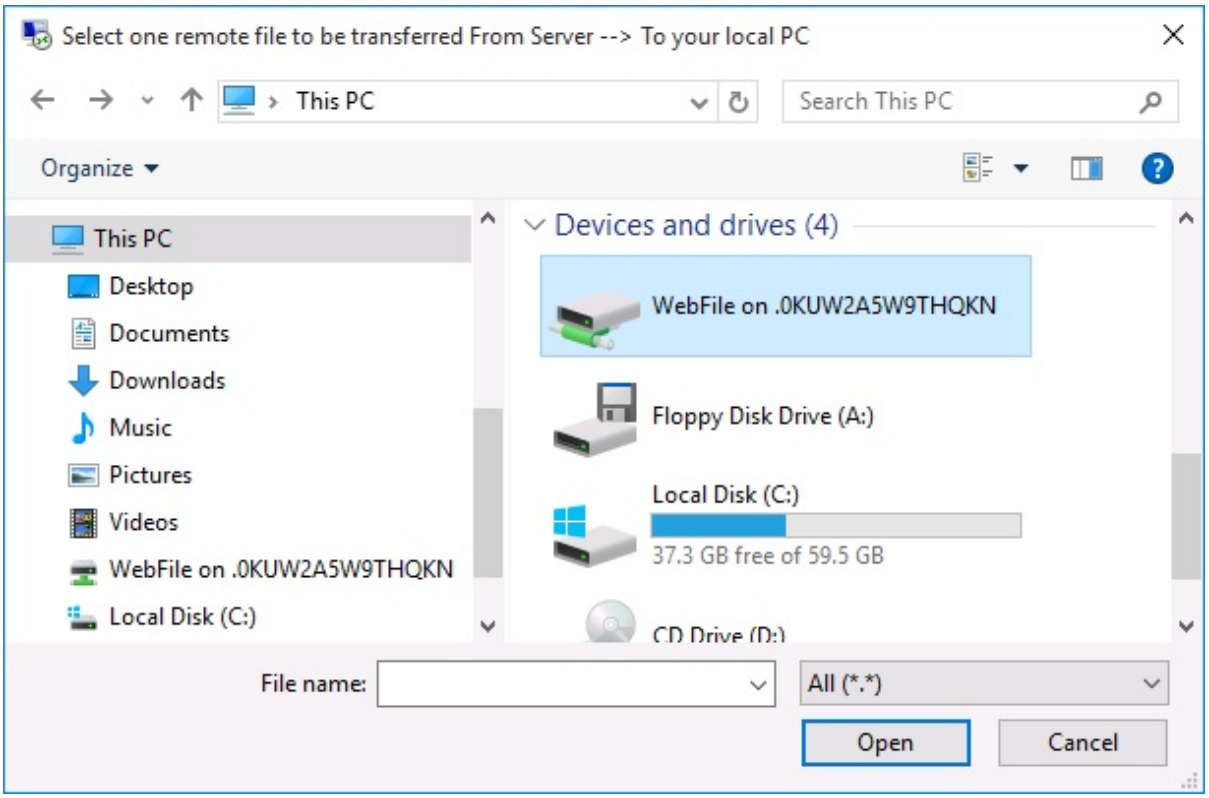
Weitere Informationen finden Sie unter diese Dokumentation .

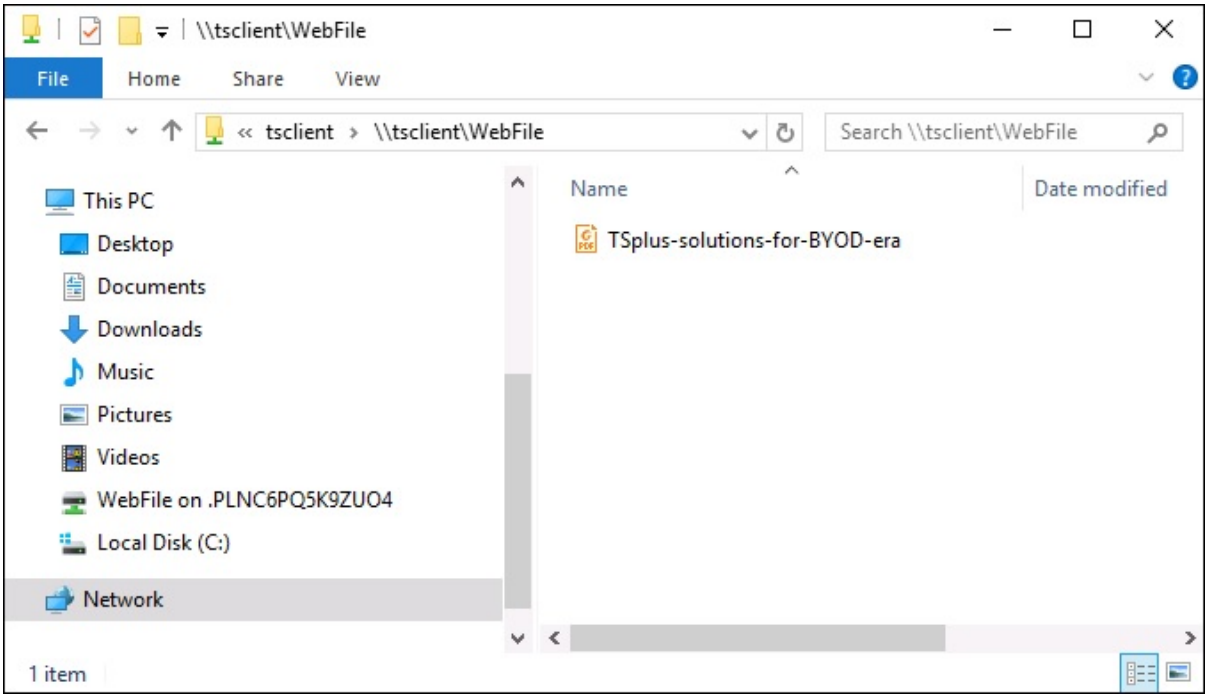
Verwendung des oberen Menüs für den Dateitransfer:



Im Gegensatz zu einer echten RDP-Sitzung erlauben die Browser keinen direkten Zugriff auf die Festplatten, der Dateitransfer wird emuliert.

Der Unterordner des Gateways wird als WebFile-Gerät in Ihre RDP-Sitzung eingebunden. Innerhalb der RDP-Sitzung können Sie darauf über den Explorer zugreifen, indem Sie auf „WebFile“ klicken oder direkt „\\tsclient\WebFile“ aufrufen.

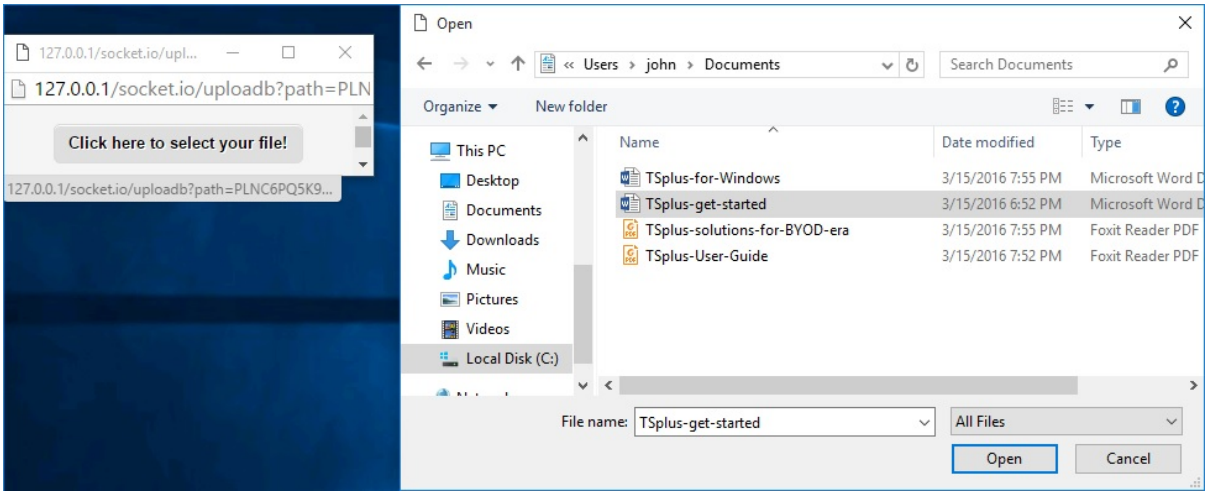




Es gibt 3 verschiedene Möglichkeiten, eine Datei zu übertragen:

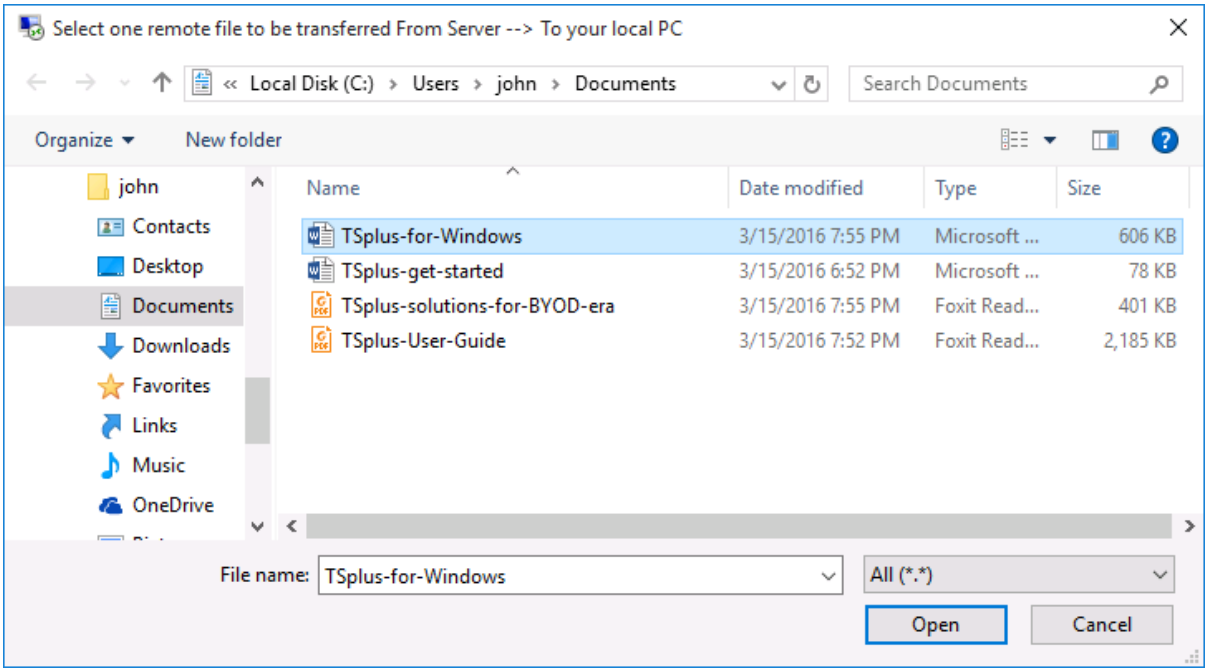
- Vom lokalen Computer zum Server:



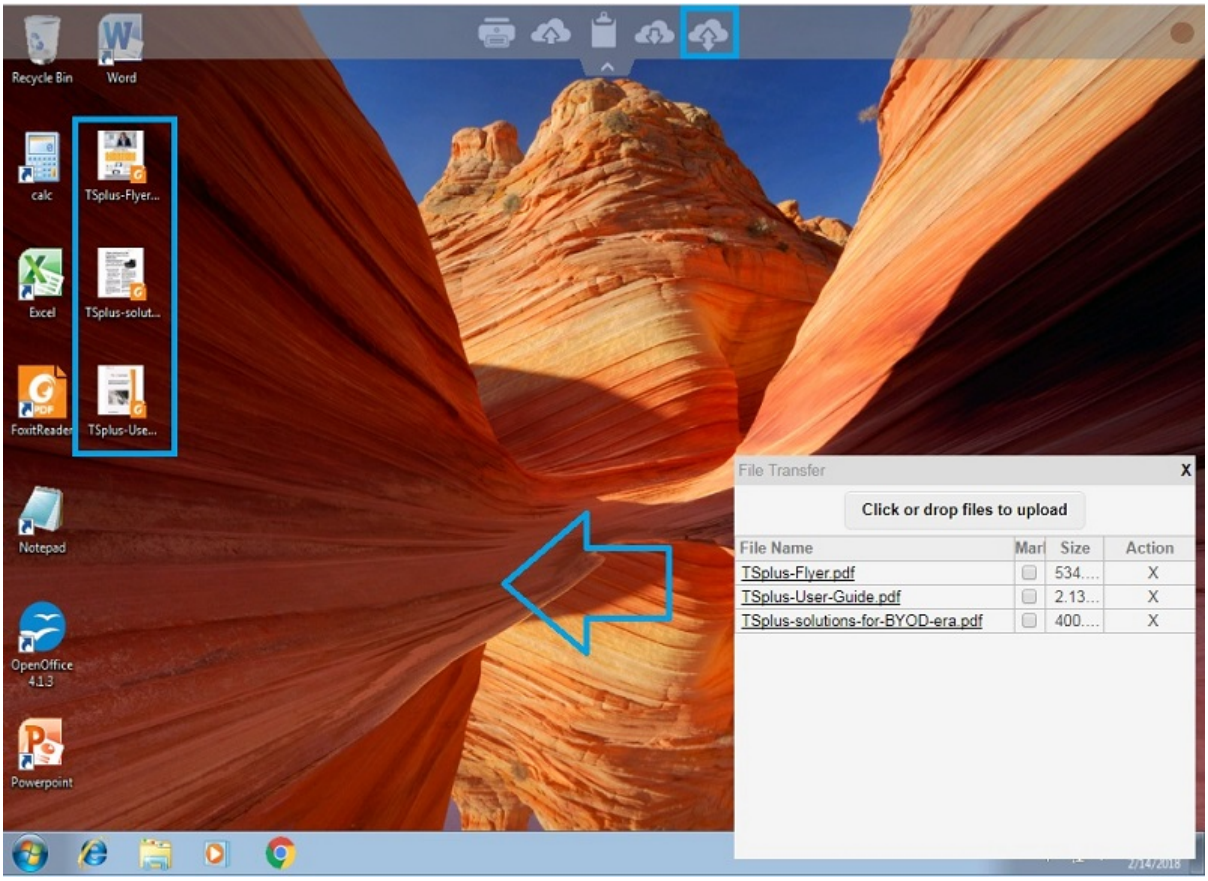


- Vom Server zum lokalen Computer:



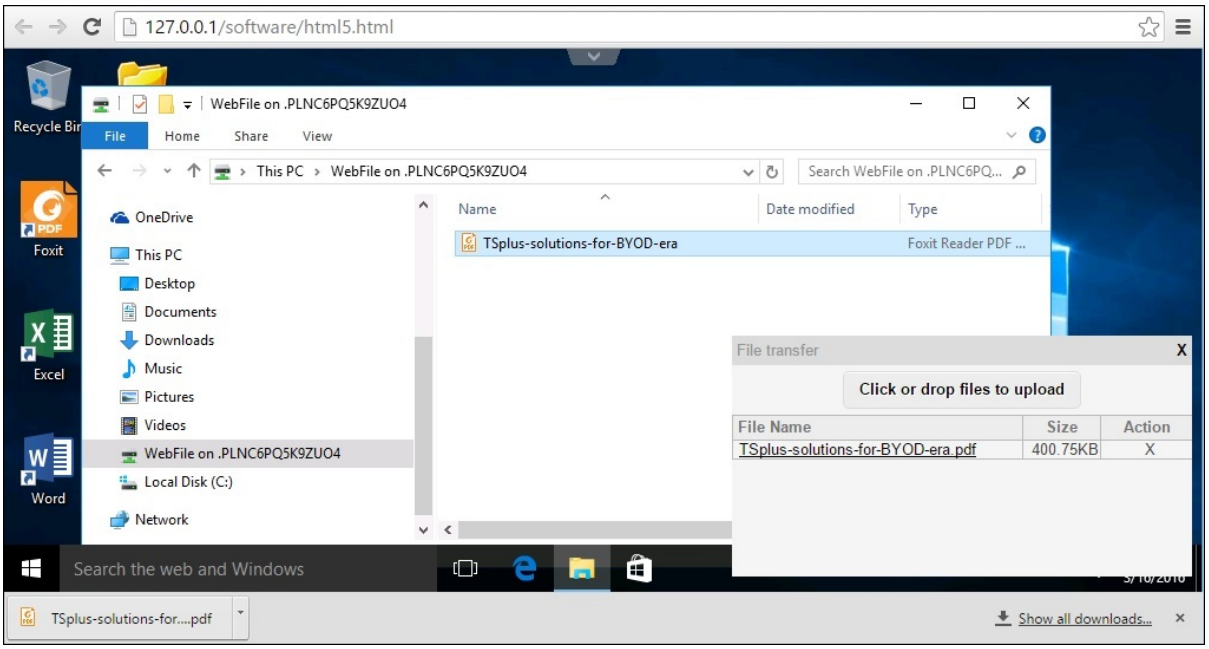


- Der Dateimanager, der es Ihnen ermöglicht, Dateien vom lokalen Computer auf den Server zu übertragen, mit einer Historie der übertragenen Dateien:

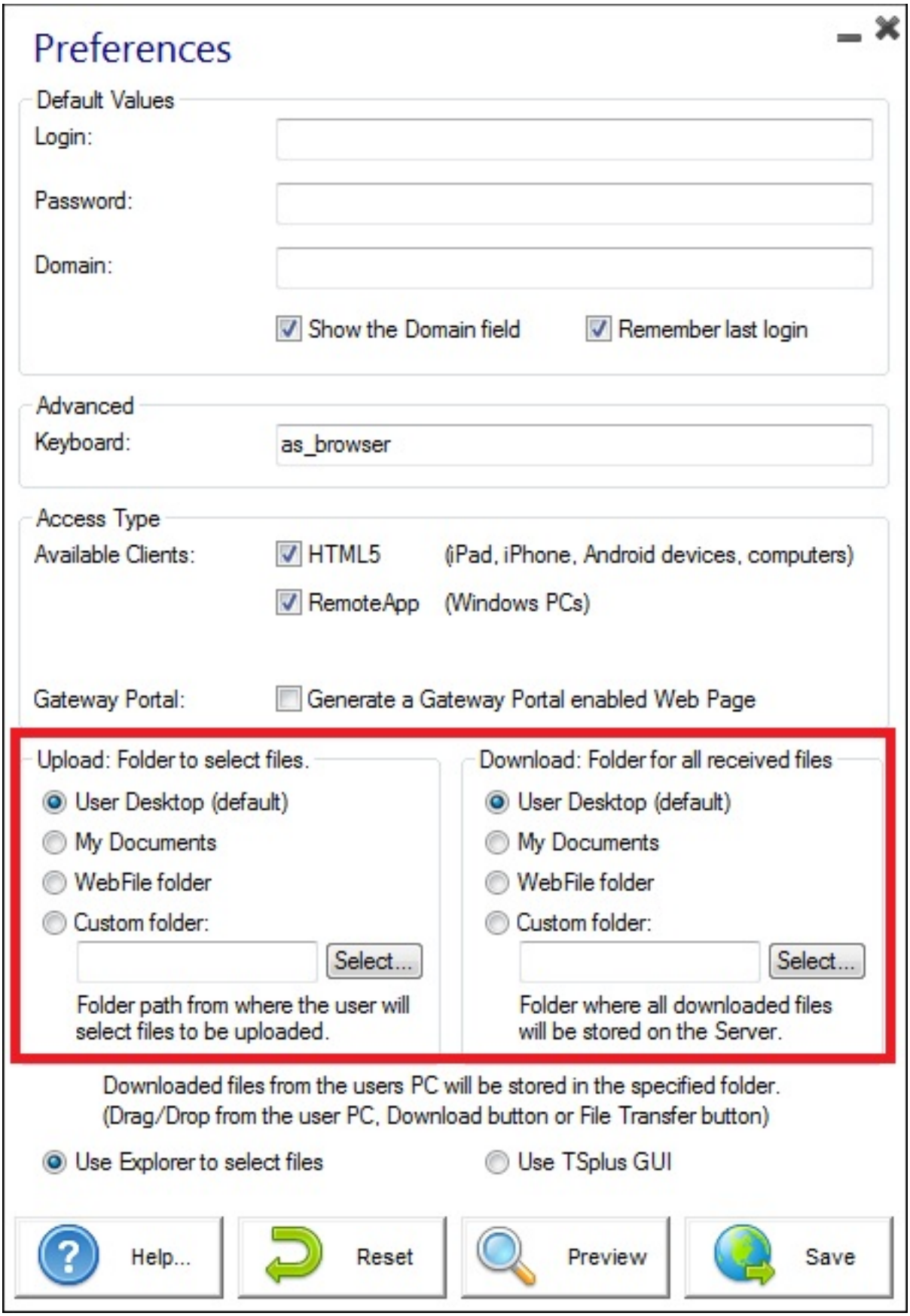


Im Browser werden die Dateien im Menü der Liste angezeigt. Sie können über das Aktionsmenü oder mit Shift + F12 geöffnet werden.

- Wenn Sie Dateien mit dem Explorer in den WebFile-Ordner kopieren, wird automatisch das Ereignis über die Erstellung einer neuen Datei im WebFile-Ordner ausgelöst, und das Browser-Menü öffnet sich/aktualisiert sich automatisch, um die neue Datei anzuzeigen.



Wenn Sie einen benutzerdefinierten Ordner verwenden, stellen Sie sicher, dass dieser Ordner sowohl auf der Client- als auch auf der Serverseite vorhanden ist. Sie können den Zielordner für den Upload/Download im Bereich der Webportal-Einstellungen auf der Web-Registerkarte des Admin-Tools festlegen.



Wenn Sie dieses Verhalten vermeiden möchten, setzen Sie die folgende Zeile in der Datei settings.js, deren Pfad standardmäßig ist: C:\Program Files (x86)\tsplus\Clients\www\software\html5\settings.js :

dropboxonnewfile = 0;

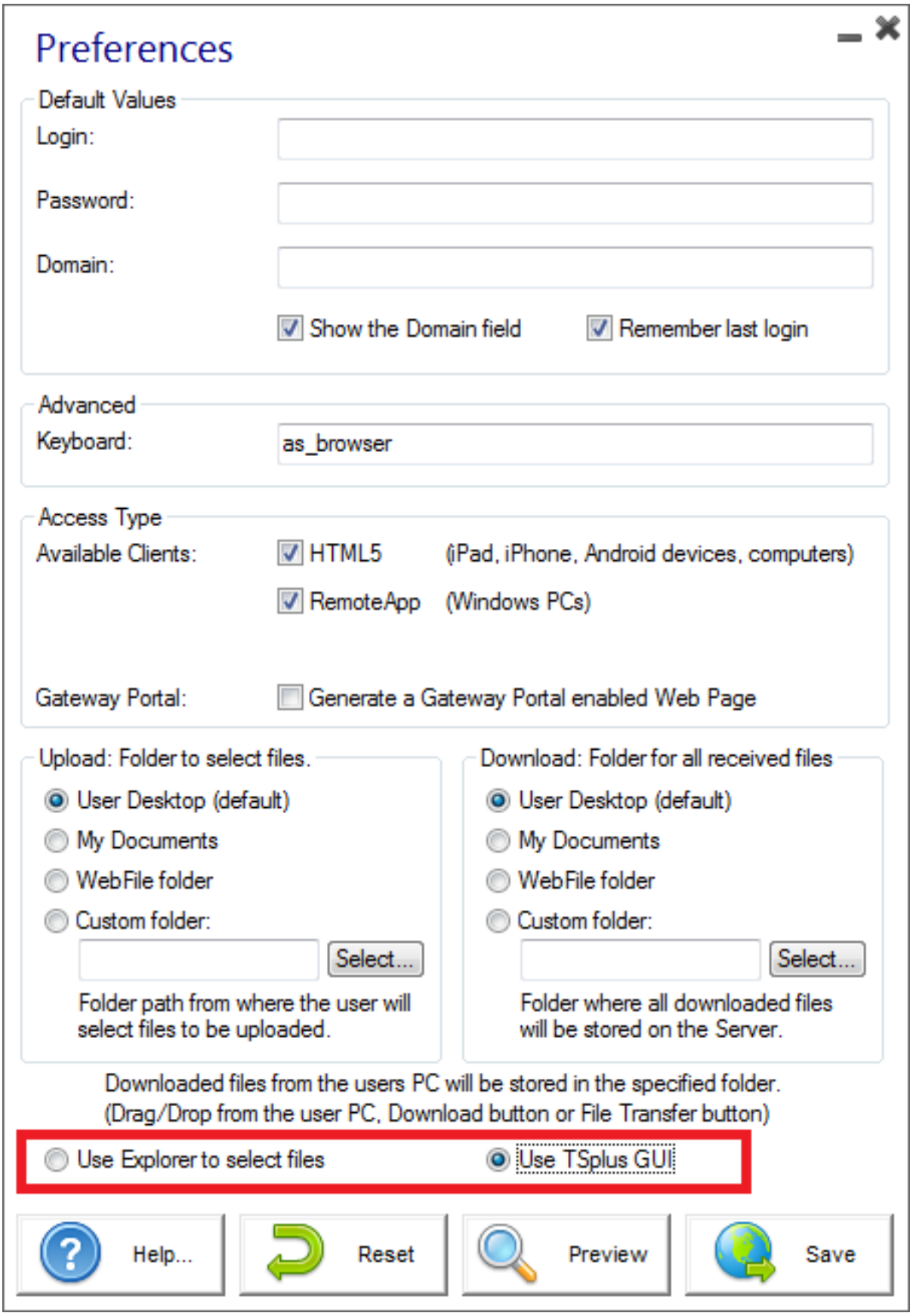
Zusätzlich können Sie einstellen:

sharedfolder = "ja";

um freigegebene Ordner anzuzeigen und Ihre Dateien mit anderen Benutzern zu teilen (standardmäßig deaktiviert).

Wenn Sie keine Datei mit dem Namen „settings.js“ im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software\html5“ haben, dann ist Ihre TSplus-Version älter und diese Dokumentation gilt nicht. Bitte aktualisieren Sie zuerst Ihr System oder kontaktieren Sie den Support.

- Standardmäßig wird der Explorer verwendet, um Dateien zu übertragen. Sie können Ihre Dateien auch direkt vom Server zum Client herunterladen, indem Sie "TSplus GUI verwenden" aktivieren, und beliebige Dateien in den Webfile-Ordner kopieren.


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-Client: Gesten auf mobilen Geräten (Touch) verwenden

Verwendeter Bildschirmbereich:

1. Einfache Berührung auf dem Bildschirm = Mausbewegung zur berührten Position und linker Mausklick
2. Schnelles Doppeltippen auf dem Bildschirm = Mausbewegung zur berührten Position und linke Maustaste Doppelklick
3. Berühren und halten Sie den Bildschirm eine Sekunde lang = Mausbewegung zur berührten Position und rechter Mausklick
4. Berühren und außerhalb des Cursorbereichs bewegen = Scrollen des sichtbaren Sitzungsrahmens (dies ist das native Verhalten von Browsern zum Scrollen, insbesondere nach dem Pinch-Zoom)
5. Berühren Sie den Cursorbereich und bewegen Sie = Mauszeiger bewegt sich nur
6. Doppeltippen Sie im Cursorbereich und bewegen Sie = linke Maustaste gedrückt halten und Maus bewegen. Nützlich zum Verschieben von Fenstern, Verschieben von Elementen, Ändern der Größe.
7. Doppeltippen Sie auf den Bildschirm (außerhalb des Cursorbereichs) und bewegen Sie den Finger nach unten/oben = mittlere Maustaste scrollen. Nützlich zum Scrollen von Seiten oder zum Anzeigen von PDFs.
8. Pinch zoom mit zwei Fingern = zoomen des RDP-Sitzungsrahmens (dies ist das native Verhalten von Browsern)

Verwendung des Mauspadbereichs - zusätzliche Funktionen im Mittelpunkt des Mauspads:

1. Einfache Berührung in der Mitte = linker Mausklick
2. Doppeltippen in der Mitte = Doppelklick mit der linken Maustaste
3. Berühren und bewegen in der Mitte = Mausbewegung und Mauspadbewegung
4. Berühren und halten Sie eine Sekunde lang = rechter Mausklick

Tastaturmodus aktiviert:

1. Einfache Berührung auf dem Bildschirm = Fokus verloren, Tastatur deaktiviert (dies ist das Verhalten nativer Browser), aber dies wird Mausbewegungen und einen linken Mausklick auslösen.
2. Schnelles Doppeltippen = Mausbewegung und linker Mausklick (ohne Tastaturdeaktivierung)

Nützlich, um den Cursor neu zu positionieren, den Fokus auf ein anderes Zeichen zu setzen und gleichzeitig im Tastaturmodus zu bleiben.

3. +Funktionen des oben beschriebenen Mauspad

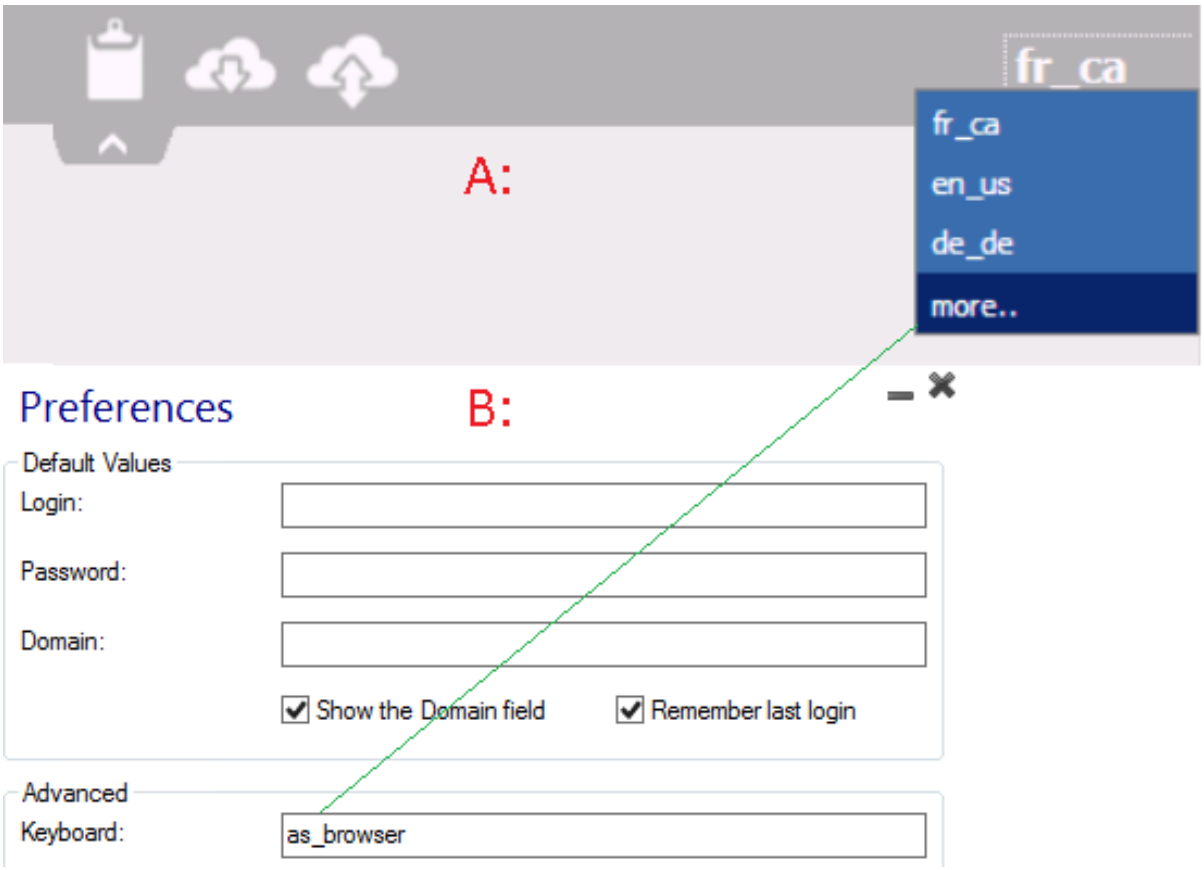
HTML5-Client: Verwendung von zwei Sprachen

Standardmäßig versucht der HTML5-Client, die Standardsprache des Browsers zu erkennen und verwendet diese dann innerhalb der RDP-Sitzung. Dieses Verhalten wird durch das Tag „as_browser“ gesteuert. Sie finden jedoch die vollständige Liste der verfügbaren Sprach-Tags unter http:// dein_server /software/sprache.html unter “Locale”

Sie haben die Wahl, eine feste Sprache festzulegen. **A:** pro client direkt über das HTML5-Hauptmenü.

	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: oder vom Portal, indem es in der AdminTool-GUI eingestellt wird, was für alle wirksam sein wird.



Sie sollten die Sitzung neu starten, wenn Sie eine andere Sprache als Hauptsprache festlegen.

Denken Sie daran: beim Verwenden **HTML5-Client** In einem Szenario mit mehreren Sprachen stellen Sie sicher, dass die Sprache, die innerhalb der Web-HTML5-RDP-Sitzung verwendet wird, mit der Sprache synchronisiert ist, die tatsächlich auf Ihrem PC/Laptop/Mac usw. eingestellt ist. Andernfalls können einige Zeichen, die in jeder Sprachzuordnung dargestellt werden, falsche Zeichen erzeugen, indem der Scan-Code für eine andere Sprache gesendet wird. Das bedeutet auch, dass, wenn Sie die Sprache von Englisch auf Deutsch innerhalb der Web-Sitzung geändert haben, Sie sie auch auf Deutsch auf dem PC/Laptop/Mac ändern sollten.

HTML5-Client: So maximieren Sie das Browserfenster

Übersicht

Das RDP-Protokoll erlaubt es nicht, während der Verbindung ohne eine erneute Verbindung die Größe zu ändern.

Bitte beachten Sie, dass Sie die bestmögliche Erfahrung mit dem HTML5-Client von Terminal Service Plus erhalten, indem Sie sich mit einem verbinden. maximierter Browser **.**

Wenn Sie jedoch möchten, dass das Browserfenster so groß wie möglich ist, können Sie versuchen, das HTML5-Fenster mit der maximalen Größe zu öffnen (aber nicht als "maximiertes" Fenster, aufgrund von Sicherheitsbeschränkungen der Internetbrowser).

Das Browserfenster maximieren

Sie müssen die Datei „Clients\www\software\common.js“ in Ihrem Terminal Service Plus-Verzeichnis ändern. Wir empfehlen Ihnen, einen Texteditor wie Notepad++ zu verwenden (do nicht verwenden Sie Word).

Um ein Browserfenster zu haben, das den gesamten Bildschirm nutzt, müssen Sie die Zeile(n) mit „window.open“ darin ändern und den folgenden Text hinzufügen:

Terminalfenster

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

Dies ermöglicht es IE/Chrome/Firefox/Safari, das Fenster mit einer Bildschirmgröße (minus Windows-Leiste) zu öffnen. Leider ist es nicht möglich, einen Webbrowser zu zwingen, das Fenster im „Vollbild“-Windows-Typ zu „maximieren“.

Öffnen Sie die Datei und suchen Sie nach „window.open(“

Dann fügen Sie das Neue am Ende hinzu.

Terminalfenster

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

wird werden:

Terminalfenster

```
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)));
```

Und wieder:

Terminalfenster

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

wird werden:

Terminalfenster

```
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
```

Und wieder:

Terminalfenster

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

wird werden:

Terminalfenster

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

Und schließlich :

Terminalfenster

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

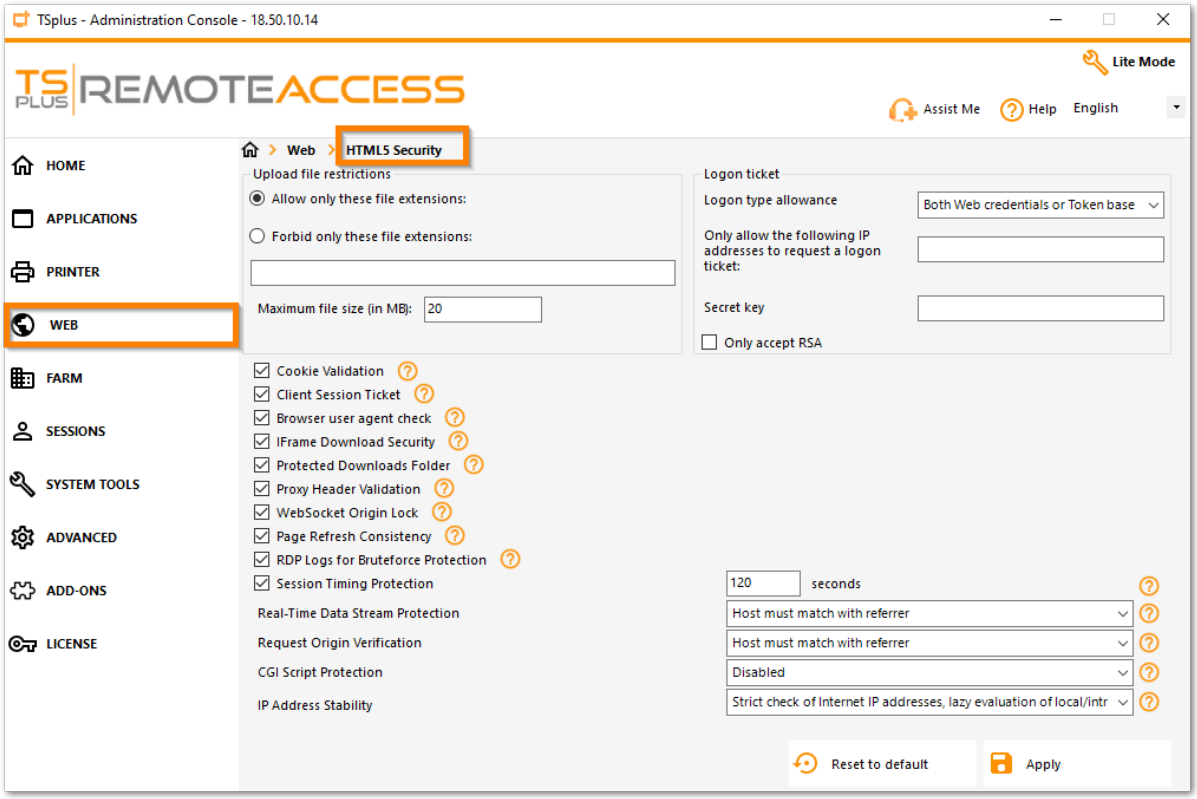
wird werden:

Terminalfenster

```
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-Sicherheit

Im HTML5-Sicherheitstab können Sie die Webeinstellungen verwalten.



Wenn Sie zusätzliche Sicherheit benötigen, können Sie unsere einsehen und herunterladen. Advanced Security .

HTML5 Server-Speicherverbrauch

Terminal Service Plus HTML5 Server läuft auf JAVA. Das Verständnis, wie JAVA mit Speicher umgeht, hilft, die Speichernutzung des Terminal Service Plus HTML5 Servers zu verstehen.

Zugewiesener Speicher

Wenn Java ausgeführt wird, versucht es, 25 % des physischen Speichers des Computers zuzuweisen. Dieser Speicher ist "zugewiesen", wird jedoch nicht direkt verwendet - es ist nicht die tatsächliche Speichernutzung, die man im Windows-Task-Manager sehen kann.

JAVA-Plattform: 32-Bit vs 64-Bit

Es gibt einen großen Unterschied zwischen diesen beiden Plattformen:

- JAVA 32-Bit kann per Definition nicht mehr als 4 GB RAM verarbeiten. Da es 25 % des gesamten verfügbaren Speichers zuweist, wird es höchstens 1 GB zuweisen, vorausgesetzt, es sind 4 GB physischer Speicher vorhanden. Wenn nur 2 GB physischer Speicher vorhanden sind, wird es nur 500 MB zuweisen, usw.
- JAVA 64-Bit kann theoretisch bis zu 16 GB verarbeiten. exa Bytes), sodass der zugewiesene Speicher nur von dem physischen Speicher abhängt.

JAVA-Speicherverwaltung

JAVA ist eine „virtuelle Maschine“. Das bedeutet, dass JAVA das Speichermanagement eigenständig übernimmt. Sobald JAVA einen Teil des Speichers zugewiesen hat, wird es diesen, auch wenn er nicht mehr benötigt wird, nicht automatisch an das System zurückgeben. Dies geschieht aus Leistungsgründen, da das Zuweisen und Freigeben von Speicher CPU-intensive Aufgaben sind.

JAVA wartet normalerweise, bis es einen großen Block ungenutzten Speichers hat, bevor es ihn an das System zurückgibt. Die Größe dieses großen Blocks hängt direkt von der Größe des physischen Speichers des Computers ab. Je mehr physischer Speicher auf einem Computer vorhanden ist, desto mehr Speicher wird von JAVA zugewiesen.

Terminal Service Plus HTML5 Server-Speicherverbrauch

All diese technischen Details sind der Grund, warum man den Windows Task-Manager öffnen und denken kann, dass Terminal Service Plus HTML5 Server viel Speicher verwendet oder dass JAVA 32 Bit weniger Speicher als JAVA 64 Bit verwendet.

Tatsächlich hängt der tatsächlich von Terminal Service Plus HTML5 Server verwendete Speicher direkt von der Anzahl der geöffneten HTML5-Sitzungen ab. Je mehr verfügbarer Speicher auf dem Computer vorhanden ist, desto mehr HTML5-Sitzungen können Sie öffnen.

HTML5-Sitzungsspeicherverbrauch

Der Speicher, der von einer HTML5-Sitzung verwendet wird, hängt von den Benutzeraktivitäten (verwendete Anwendungen und Programme, Word/Excel im Vergleich zu grafikintensiven Programmen) und der Verbindungsart ab, die zwischen dem Terminal Service Plus HTML5-Server und dem Client-Computer hergestellt wird.

Im allgemeinen Anwendungsfall benötigt eine HTML5-Sitzung 30 MB Speicher (Standardnutzung, binäre Websocket-Konnektivität). Im schlimmsten Fall benötigt eine Sitzung bis zu 100 MB Speicher (intensive Nutzung, „XHR“-Fallback-Konnektivität für ältere Browser).

Verlust des HTTP- und HTTPS-Serverhörens

Jeder Java-Fehlerprotokoll zeigt ausreichend nativen Speicher für den Betrieb an.

Das Problem ist eigentlich ganz einfach.
Wenn die HTML5-Sitzung startet, ist genügend Speicher gemäß den gemeldeten Werten vorhanden.
Dann startet es innerhalb der RDP-Sitzung ein unbekanntes Programm und stiehlt den gesamten nativen Speicher für sich.

Wenn Java es erneut anfordert, ist es plötzlich nicht mehr verfügbar, was diesen Speicherfehler verursacht.

- Es gibt nicht genügend Speicher für die Java-Laufzeitumgebung, um fortzufahren.
- Native-Speicherzuweisung (mmap) konnte 234881024 Bytes nicht zuordnen. Fehlermeldung: virtueller Speicher G1# Mögliche Gründe:
- Das System hat keinen physischen RAM oder Swap-Speicher mehr# Dieser Prozess läuft mit aktivierten komprimierten Oops, und der Java-Heap könnte das Wachstum des nativen Heaps blockieren.

Mögliche Lösungen:

- Reduzieren Sie die Speicherauslastung des Systems

- Erhöhen Sie den physischen Speicher oder den Swap-Speicher# Überprüfen Sie, ob der Swap-Support-Speicher voll ist
- Verringern Sie die Java-Heap-Größe (-Xmx/-Xms)
- Verringern Sie die Anzahl der Java-Threads # Verringern Sie die Java-Thread-Stackgröße (-Xss)
- Setzen Sie einen größeren Code-Cache mit -XX:ReservedCodeCacheSize=

Die JVM läuft im Zero Based Compressed Oops-Modus, in dem der Java-Heap im ersten 32-GB-Adressraum platziert ist. Die Basisadresse des Java-Heaps ist die maximale Grenze für das Wachstum des nativen Heaps.
Bitte verwenden Sie **-XX:HeapBaseMinAddress**

Möglicherweise könnten Sie von Anfang an mehr nativen Speicher für Java zuweisen und es zwingen, den Speicher nicht an das System zurückzugeben, sondern ihn sich selbst zuzuweisen.
In diesem Fall werden Sie jedoch auf folgendes Problem stoßen: Programme, die in einer RDP-Sitzung ausgeführt werden, können Speicherplatz erschöpfen, und das gesamte System könnte abstürzen.

Aber du kannst es trotzdem versuchen.

1. Öffnen und bearbeiten Sie die folgende Datei mit Notepad:
   *\Clients\webserver\runwebserver.ini

2. Dort finden Sie die folgenden Befehlszeilen-Einstellungen, wie diese:

Terminalfenster

-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. Entfernen Sie die gesamte Zeile aus runwebserver.ini und fügen Sie Folgendes an ihrer Stelle hinzu:

Terminalfenster

-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. Starten Sie den HTML5-Server über die AdminTool-GUI neu, um die Änderungen anzuwenden.
   (Aber stellen Sie vorher sicher, dass die Datei webserver\runwebserver.bat in ihren Eigenschaften kein schreibgeschütztes Attribut hat. Andernfalls kann die AdminTool-GUI runwebserver.bat nach einem Neustart nicht anpassen.)

In den meisten Fällen sollte dies ausreichend sein. Sobald Java Speicher verwendet, wird es ihn für andere Zwecke zuweisen, anstatt ihn an das System zurückzugeben. Daher könnte die Speichernutzung von html5service.exe potenziell 70 % des verfügbaren Speichers des Systems erreichen. In diesem Fall sollte Java potenziell aufhören abzustürzen. Wenn jedoch ein anderes Programm eine große Menge Speicher verbraucht, könnte es stattdessen abstürzen. In diesem Fall sind wir machtlos; Sie müssen sicherstellen, dass genügend Speicher vorhanden ist, um einen Java HTML-Server sowie andere Programme auszuführen.

Es gibt eine Option in Java namens -XX:+AggressiveHeap, die die Speicherzuweisung für die Java Virtual Machine selbst verbessern könnte, und damit den endgültigen Inhalt von *\webserver\runwebserver.ini.

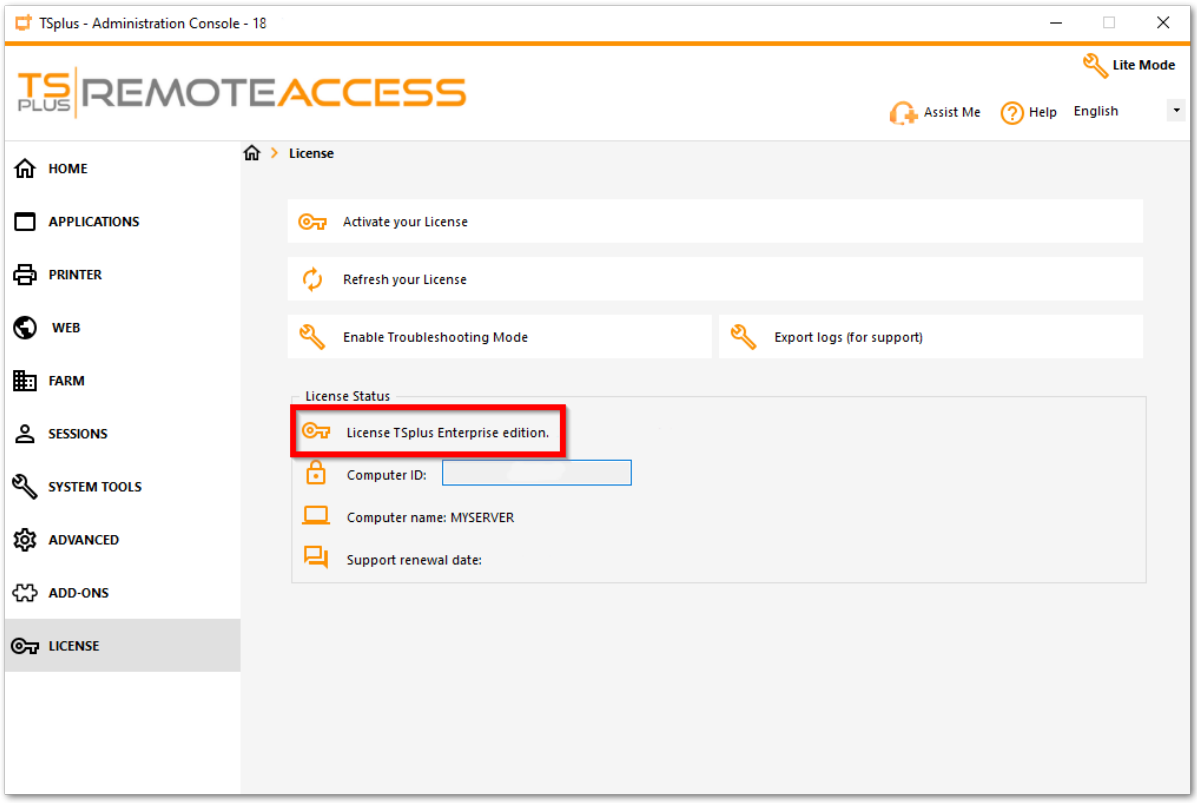
Es könnte ungefähr so aussehen:

Terminalfenster

-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

Wie man seine TSplus Edition identifiziert

Auf der Lizenzkarte unter der Seriennummer können Sie den Typ der Lizenz, die Sie gekauft haben, sowie Ihre Anzahl an Benutzern neben der Anzahl der Verbindungen sehen.



TSplus hat alte Lizenzen zu einer zusammengeführt, um mehr Klarheit zu gewinnen. System- und Drucker-Editionen wurden migriert zu **Desktop Edition** .

Desktop Edition

Grundlegende Funktionen:

- TSplus Administrator Tool (AdminTool),

- Unterstützung für gleichzeitige Verbindungen,
- Anwendungssteuerung pro Benutzer und/oder pro Gruppen,
- TSplus Remote Taskbar und/oder TSplus Floating Panel,
- Remote Desktop-Zugriff,
- TSplus Portable Client Generator,
- RemoteApp-Verbindungsclient,
- Vollständig konform mit dem RDP-Protokoll,
- Dual-Screen-Unterstützung, bidirektionaler Sound, RemoteFX, wenn mit der Windows-Version kompatibel,
- Lokale und Remote-Verbindungsunterstützung,
- Unterstützung für Arbeitsgruppen- und Active Directory-Benutzer,
- Geräte-/Festplattenumleitung.
- Virtual Printer, ermöglicht es Ihnen, von jedem Standort aus zu drucken, ohne einen speziellen Treiber installieren zu müssen, und erlaubt die Druckerumleitung.

Mobile Web Edition

Ermöglicht Ihnen (neben allen Funktionen der System- und Druckereditionen) zu:

-

Verbinden Sie sich von jedem Webbrowser mit dem TSplus HTTP-Webserver,

- Vollständig gesicherte Verbindung von jedem Webbrowser mit dem TSplus HTTPS-Webserver und SSH-Server,
- HTML-Seiten enthalten Windows- und HTML5-Webzugriffsclients,
- Einfach von iPhone/iPad und Android-Geräten verbinden, auch mit dem TSplus Mobile App ,
- Passen Sie die Anmeldeseite mit dem benutzerfreundlichen Webmaster-Toolkit von TSplus an,
- Mit dem TSplus Web Applications Portal können Benutzer auf ihre Anwendungsliste in ihrem Webbrowser zugreifen,
- Statt Windows-Anmeldeinformationen ermöglicht TSplus Web-Anmeldeinformationen den Benutzern, sich nur mit einer E-Mail oder einer PIN zu verbinden.
- Universal Printer ermöglicht es Ihnen, von jedem Standort aus zu drucken, ohne einen speziellen Druckertreiber installieren zu müssen,

Enterprise Edition

Enthält alle vorherigen Funktionen sowie diese hier:

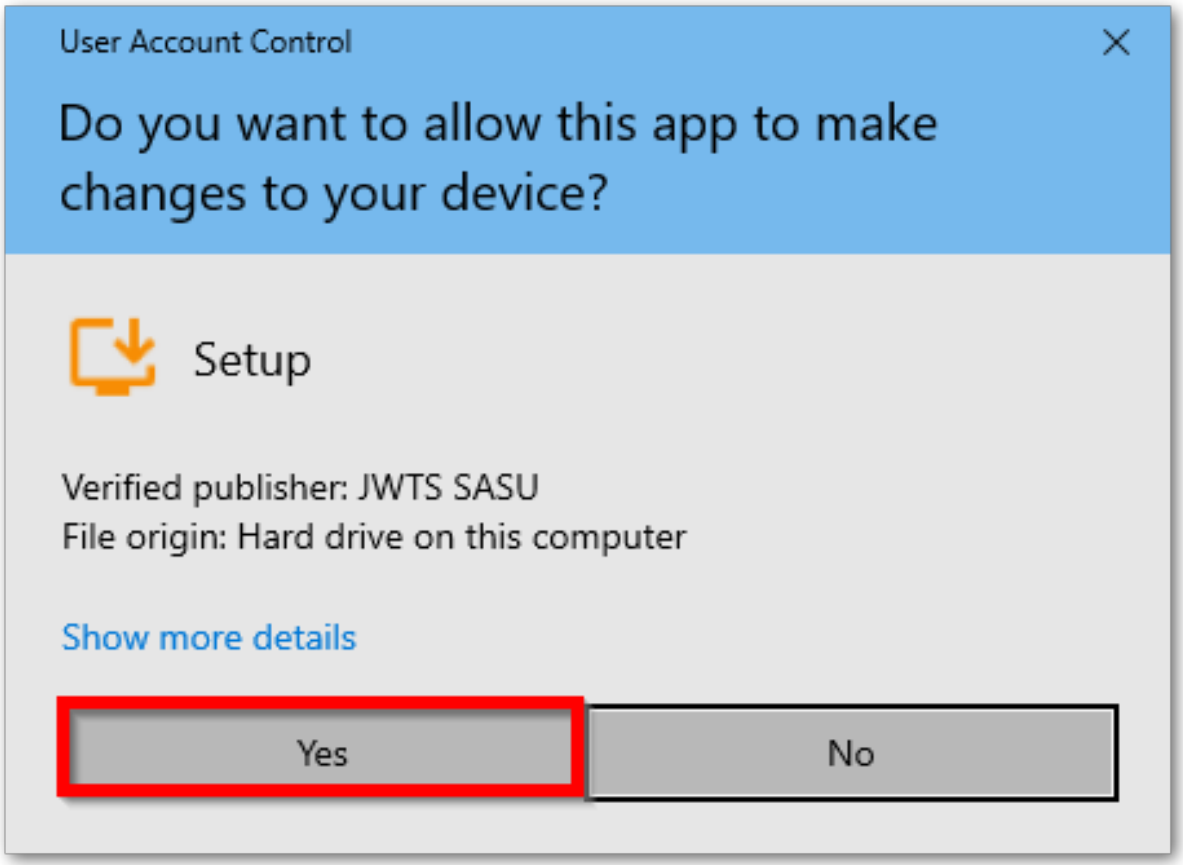
- Supportieren Sie eine unbegrenzte Anzahl von Servern innerhalb jeder TSplus Farm (erfordert eine Lizenz pro Server),
- Tausende von Benutzern, die gleichzeitig an einer skalierbaren Lastenausgleichsarchitektur arbeiten,
- Einzelnes Unternehmensportal zum Zugriff auf alle Ihre TSplus-Server,
-

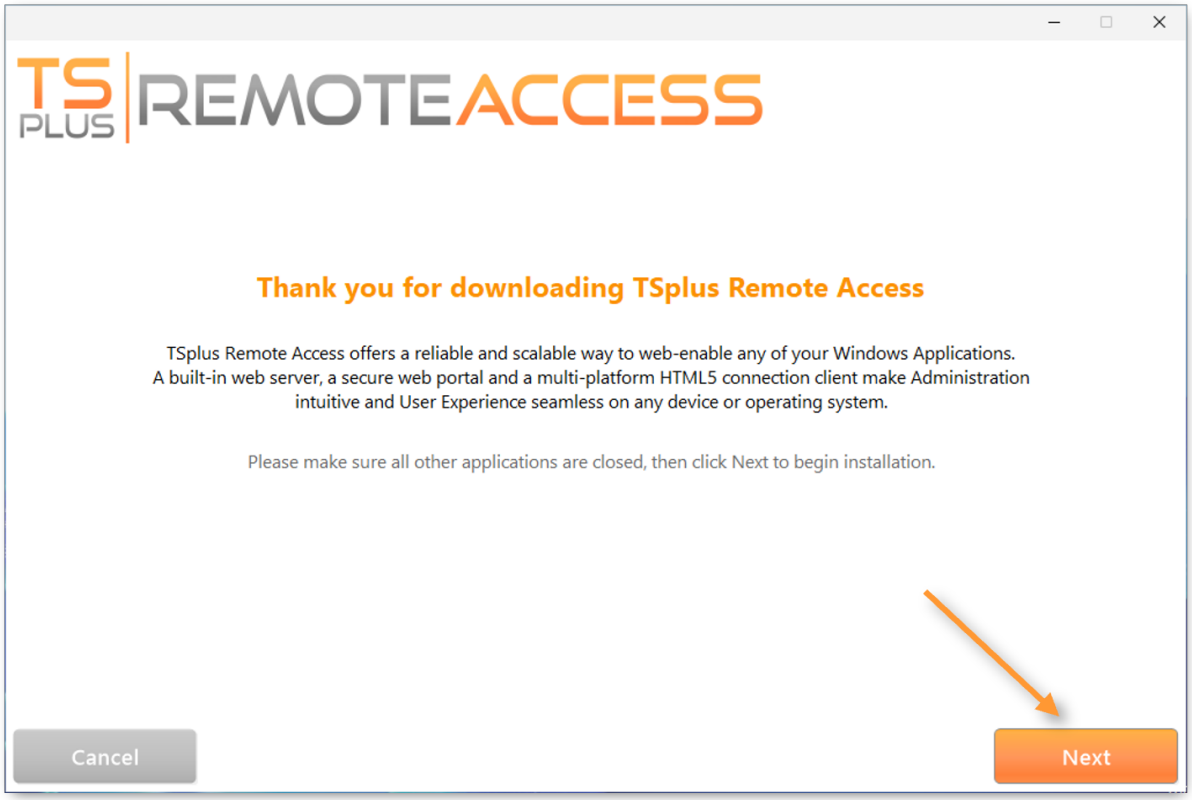
Fähigkeit, einen oder mehrere Anwendungsserver Benutzern oder Benutzergruppen zuzuweisen,

- Lastverteilung und Failover-Unterstützung enthalten.
- Die Möglichkeit, eine zusätzliche Sicherheitsebene mit dem hinzuzufügen TSplus 2FA Add-On .

TSplus Remote Access v19 Installation

Ausführen TSplus Remote Access Setup-Programm und dann **folge den Installationsschritten** .
Ihr lokales Administratorkennwort ist nach dem ersten Neustart von TSplus Remote Access erforderlich.





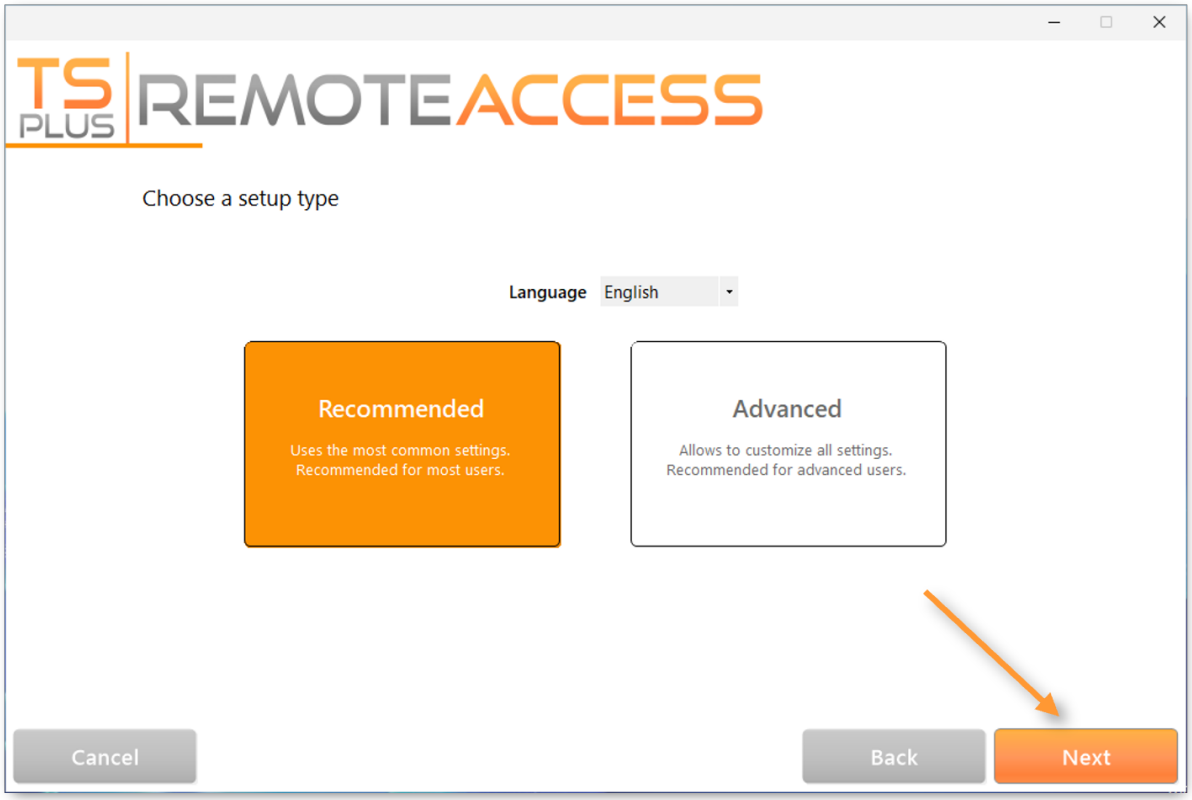
Sie können dann Ihre Sprache auswählen (später änderbar).

Sie können dann zwei benutzerdefinierte Optionen auswählen, indem Sie die entsprechenden Kästchen ankreuzen: **Empfohlen** oder **Erweitert**

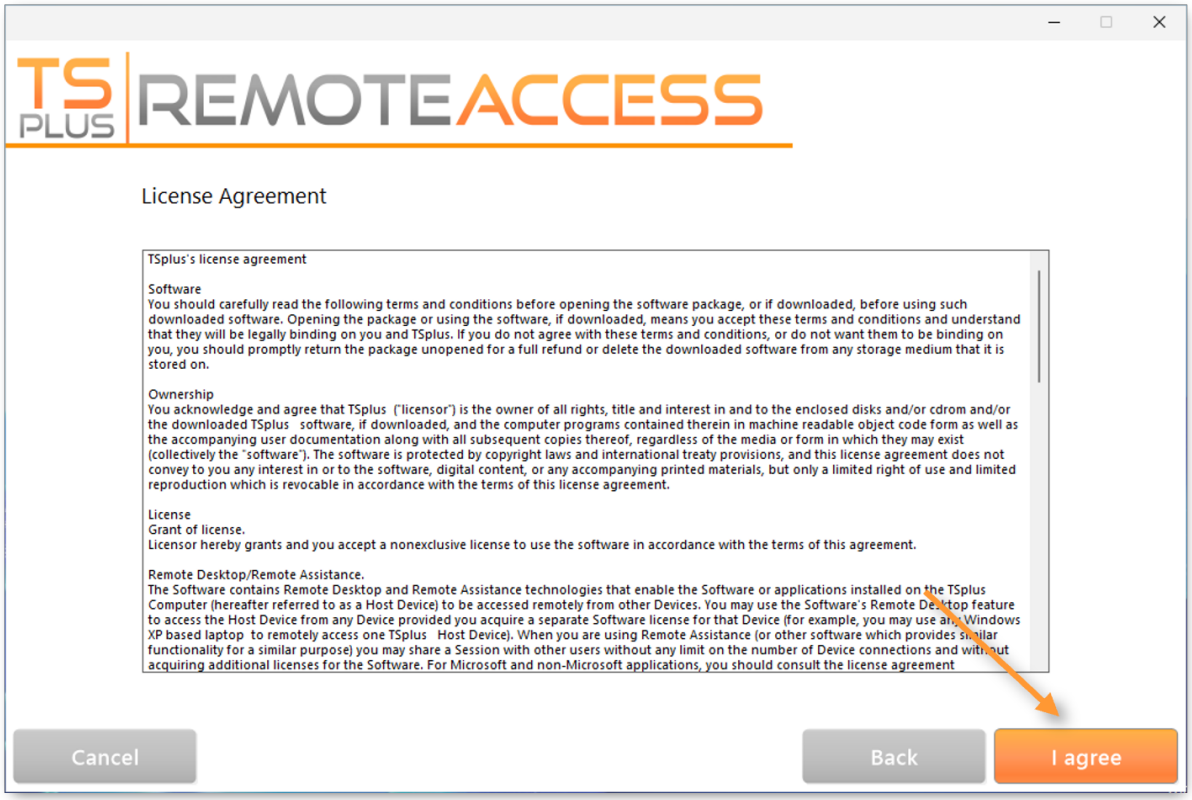
Die erweiterte Option ermöglicht es Ihnen, zu:

- Nicht installieren TSplus Advanced Security.
- Benutzen Sie benutzerdefinierte Proxy-Einstellungen.
- Laden Sie nur den Installer herunter, der TSplus nicht installiert.
- Ändern Sie die Standardports (nicht empfohlen).

Klicken Sie auf Weiter.



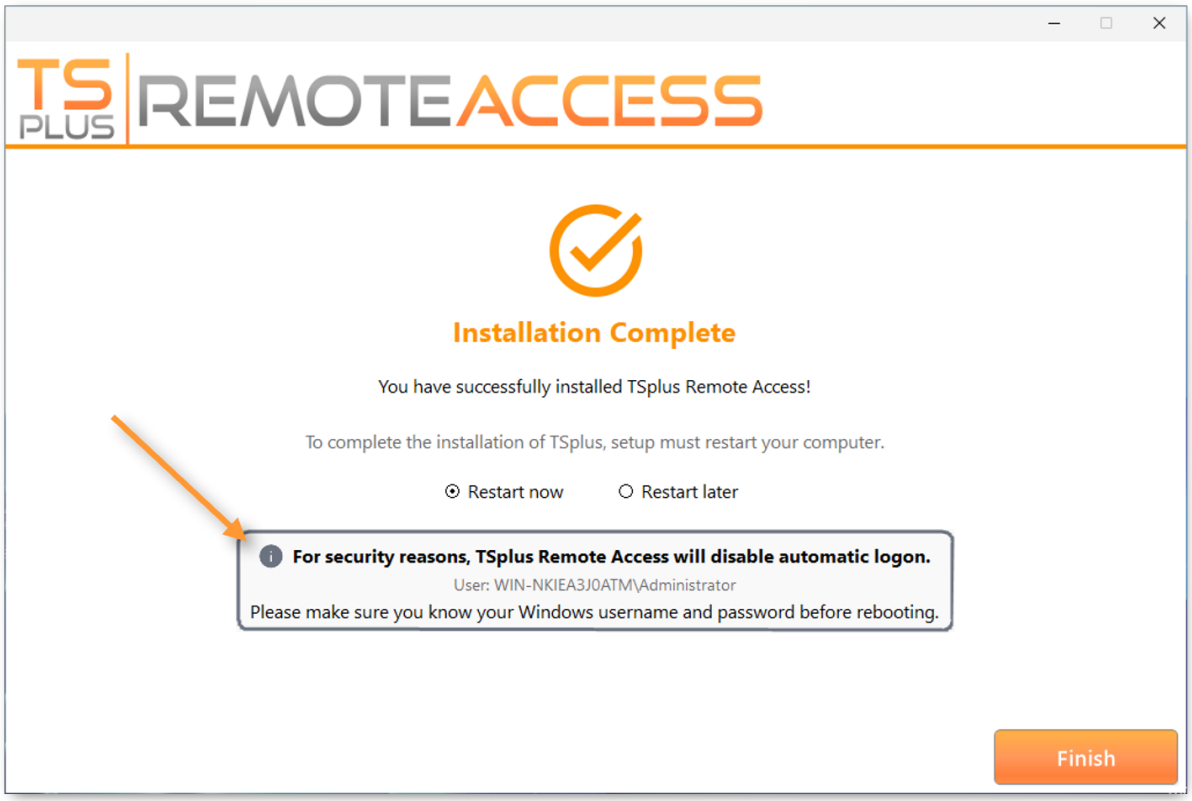
Klicken Sie auf „Ich akzeptiere die Vereinbarung.“



Bitte warten, das Programm wird heruntergeladen und installiert.



Dann erscheint das TSplus-Logo und ein Fenster informiert Sie über den Abschluss der Installation.

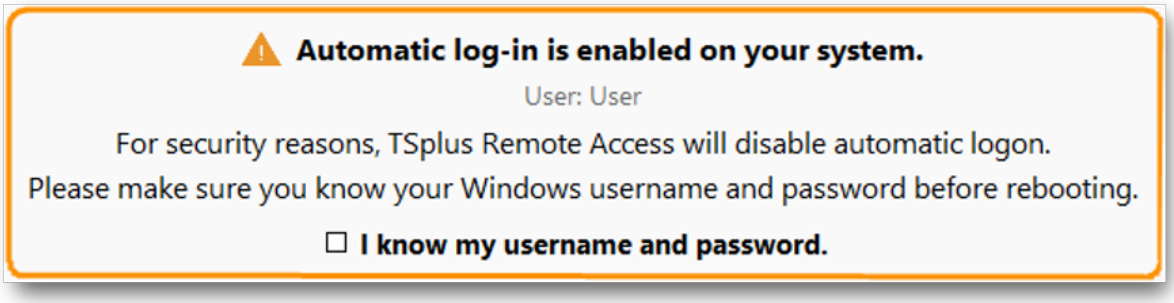


☐ **Wichtige Mitteilung**

Aus Sicherheitsgründen, **TSPlus Remote Access** Sie müssen bei jedem Login Ihren Benutzernamen und Ihr Passwort manuell eingeben.

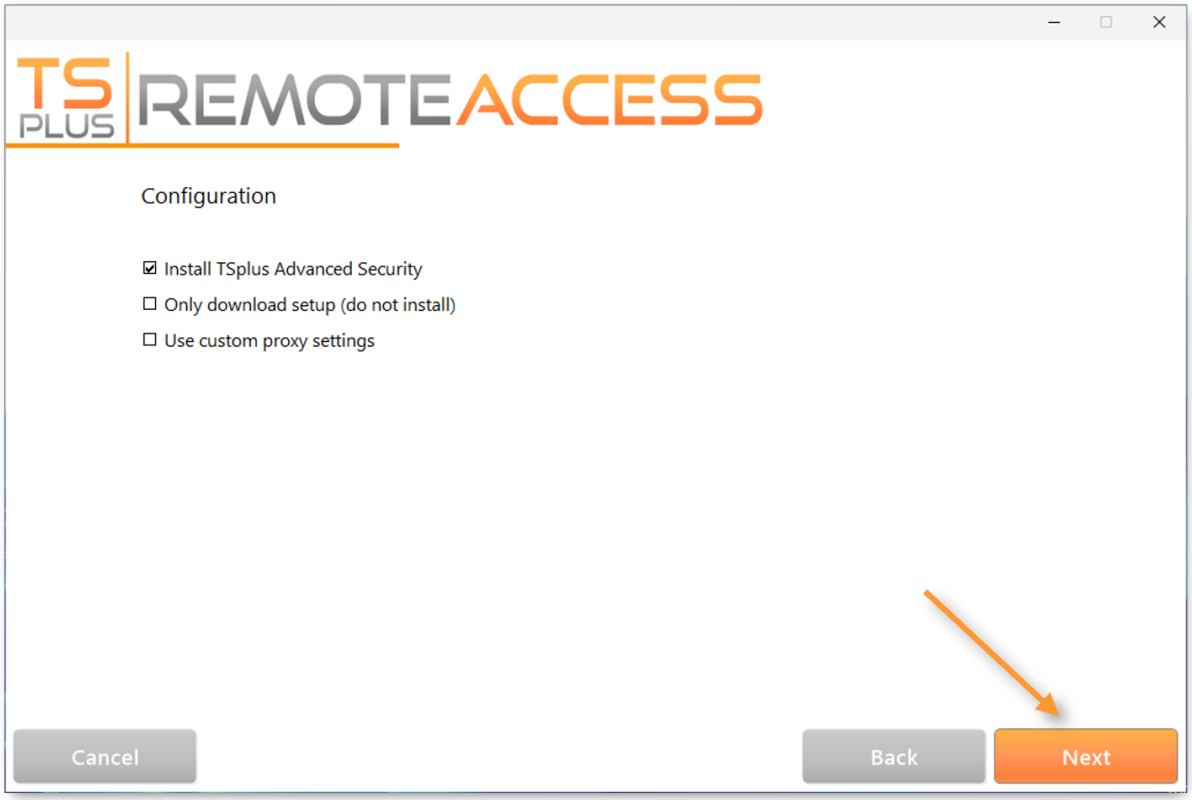
Stellen Sie sicher, dass Sie Ihre Anmeldeinformationen kennen, bevor Sie das System neu starten, um zu vermeiden, dass Sie ausgesperrt werden.

Wenn
Autologon
ist auf dem System aktiviert, der Installer zeigt ein Warn-Popup an, das Sie auffordert zu bestätigen, dass Sie Ihren Benutzernamen und Ihr Passwort kennen.



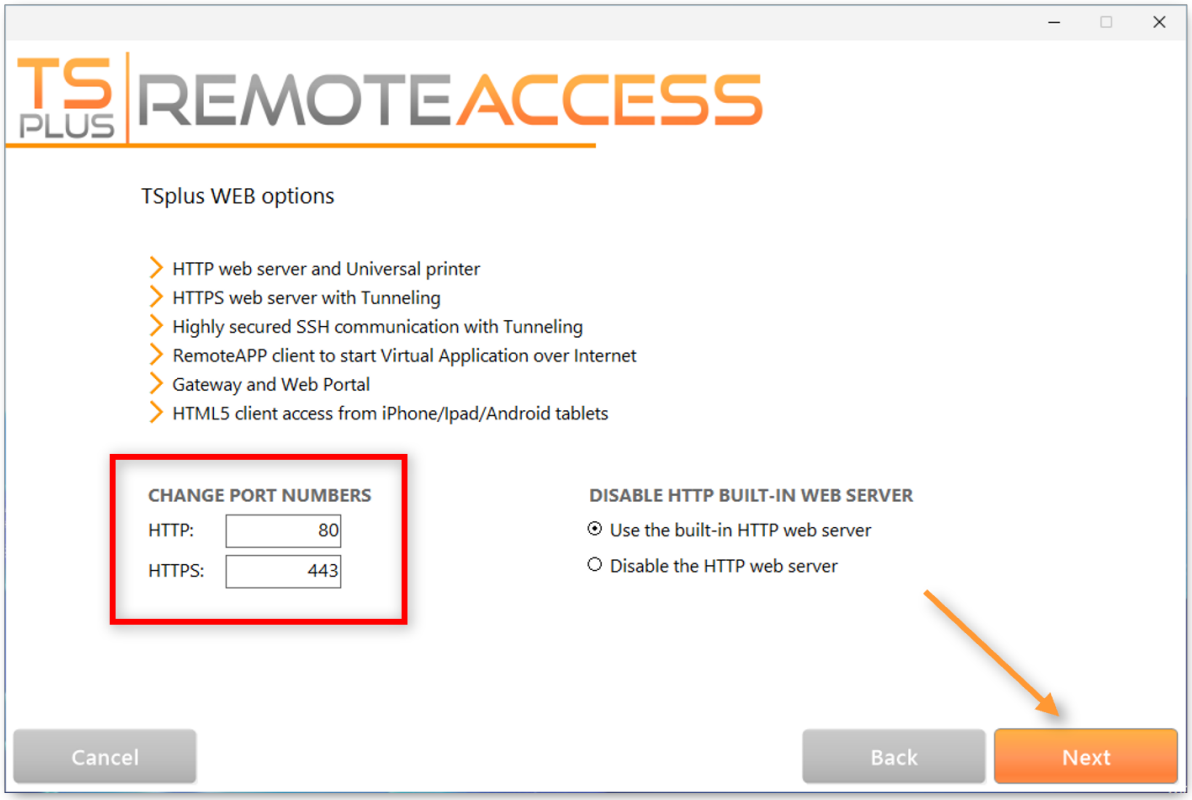
Um TSplus zu verwenden, müssen Sie Ihr System neu starten. Die Testphase bietet ein vollständiges Produkt für 15 Tage und 5 gleichzeitige Benutzer.

Die folgenden Schritte nur, wenn Sie TSplus Remote Access in installieren. **Erweiterter Modus** .

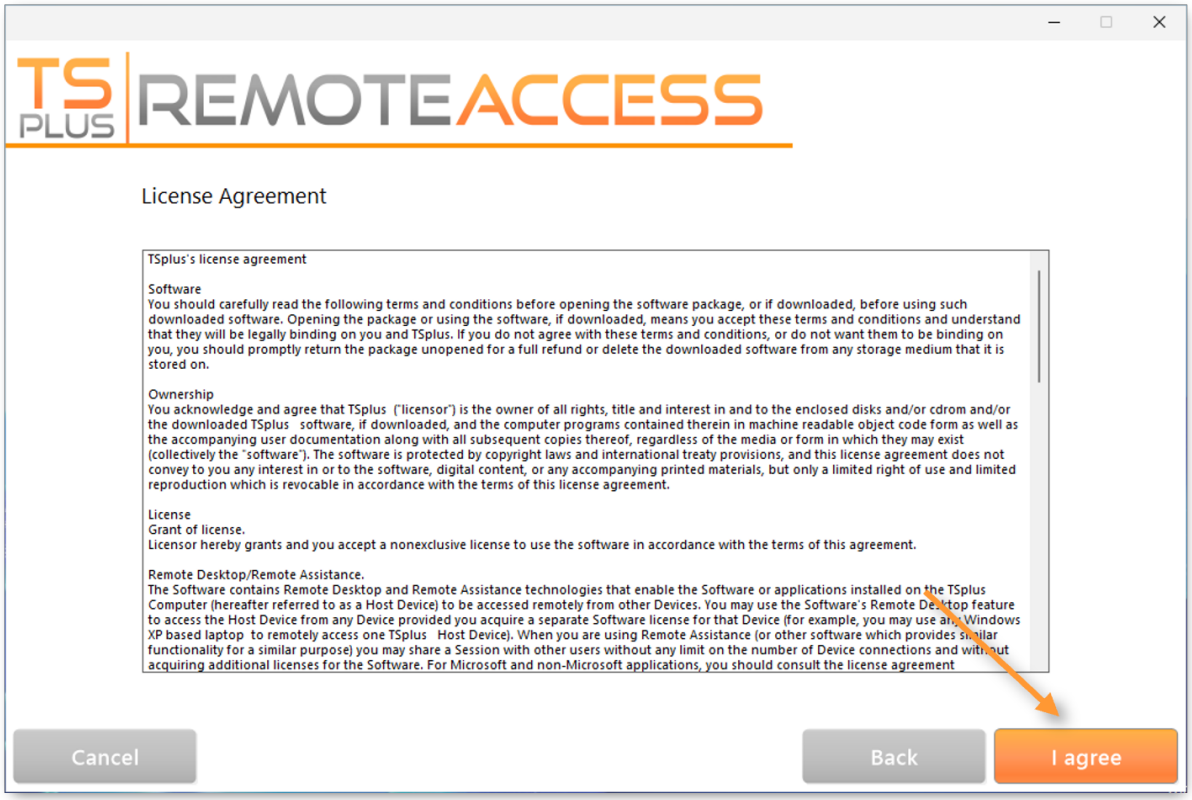


Webserver hören standardmäßig auf den Ports 80 und 443. Wir empfehlen Ihnen, unsere standardmäßigen TSplus-Installations Einstellungen zu akzeptieren. Nach unserer Erfahrung sind die meisten Produktionsprobleme auf die Sicherheitsfunktionen von Windows zurückzuführen.

Sie können diese Ports während der Installation oder jederzeit auf dem noch ändern, wenn Sie möchten. Integrierte Webserver-Verwaltung des AdminTools Stellen Sie nur sicher, dass die definierten Ports verfügbar sind und dass Java auf dem Server installiert ist.



Klicken Sie auf „Ich akzeptiere die Vereinbarung.“



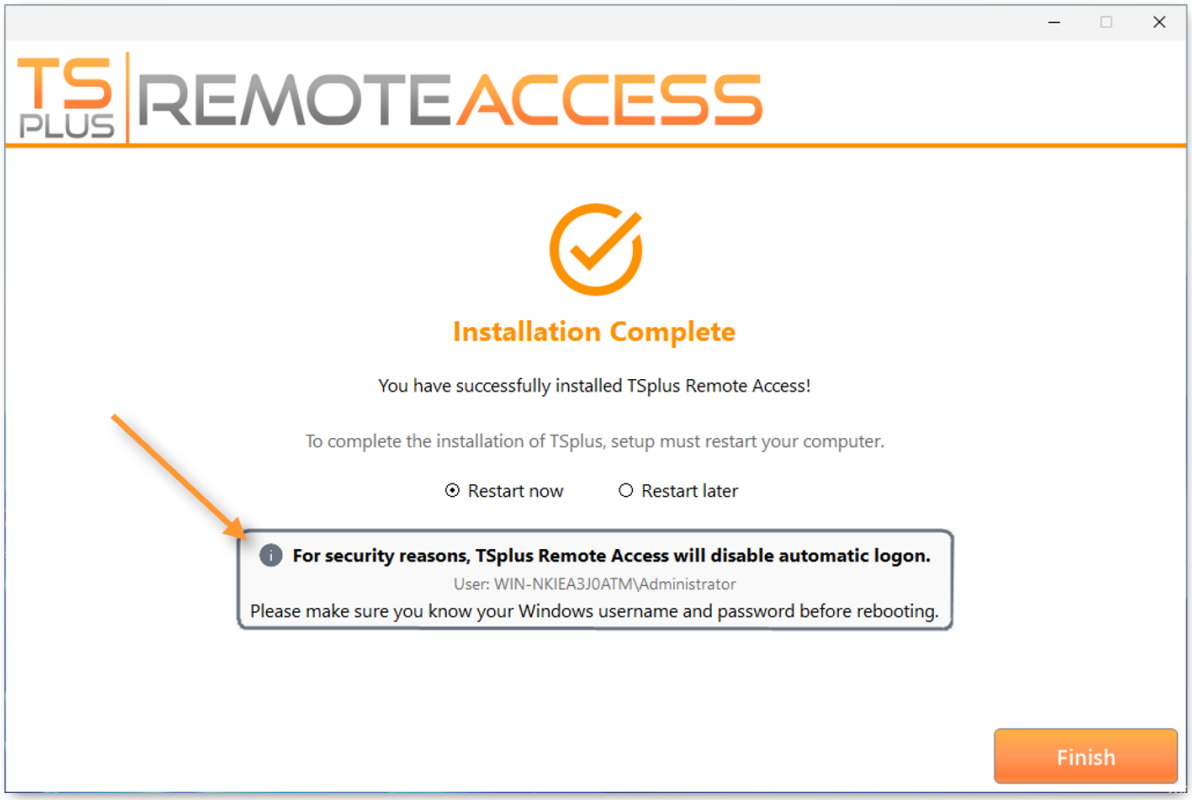
Die Fortschrittsanzeige erscheint und ermöglicht es Ihnen, den Fortschritt des Prozesses zu verfolgen:



- Seit der Version TSplus 11.40 haben Sie die Wahl, zu installieren TSplus Advanced Security unser leistungsstarkes Sicherheits-Add-On in seiner ultimativen Testversion (Alle Sicherheitsfunktionen 2 Wochen lang kostenlos nutzbar) zu Ihrem TSplus-System:

Für weitere Informationen zu diesem Produkt siehe Seiten über TSplus Advanced Security Dokumentation .

Dann erscheint das TSplus-Logo und ein Fenster informiert Sie über den Abschluss der Installation.

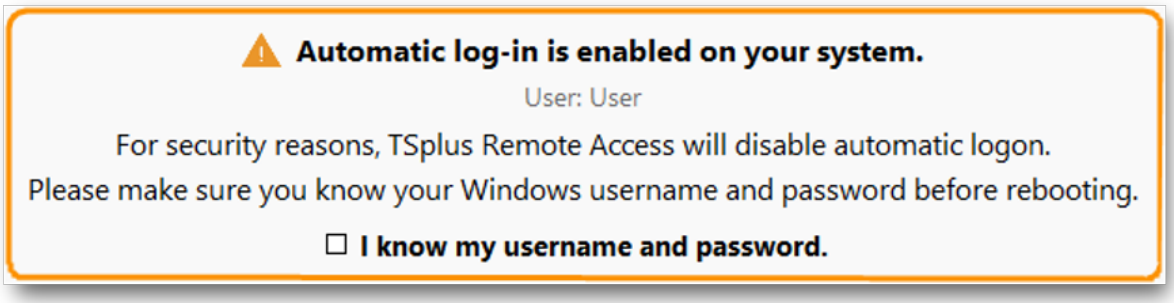


☐ **Wichtige Mitteilung**

Aus Sicherheitsgründen, **TSPlus Remote Access** Sie müssen bei jedem Login Ihren Benutzernamen und Ihr Passwort manuell eingeben.

Stellen Sie sicher, dass Sie Ihre Anmeldeinformationen kennen, bevor Sie das System neu starten, um zu vermeiden, dass Sie ausgesperrt werden.

Wenn
Autologon
ist auf dem System aktiviert, der Installer zeigt ein Warn-Popup an, das Sie auffordert zu bestätigen, dass Sie Ihren Benutzernamen und Ihr Passwort kennen.



Um TSplus zu verwenden, müssen Sie Ihr System neu starten. Die Testphase bietet ein vollständiges Produkt für 15 Tage und 5 gleichzeitige Benutzer.

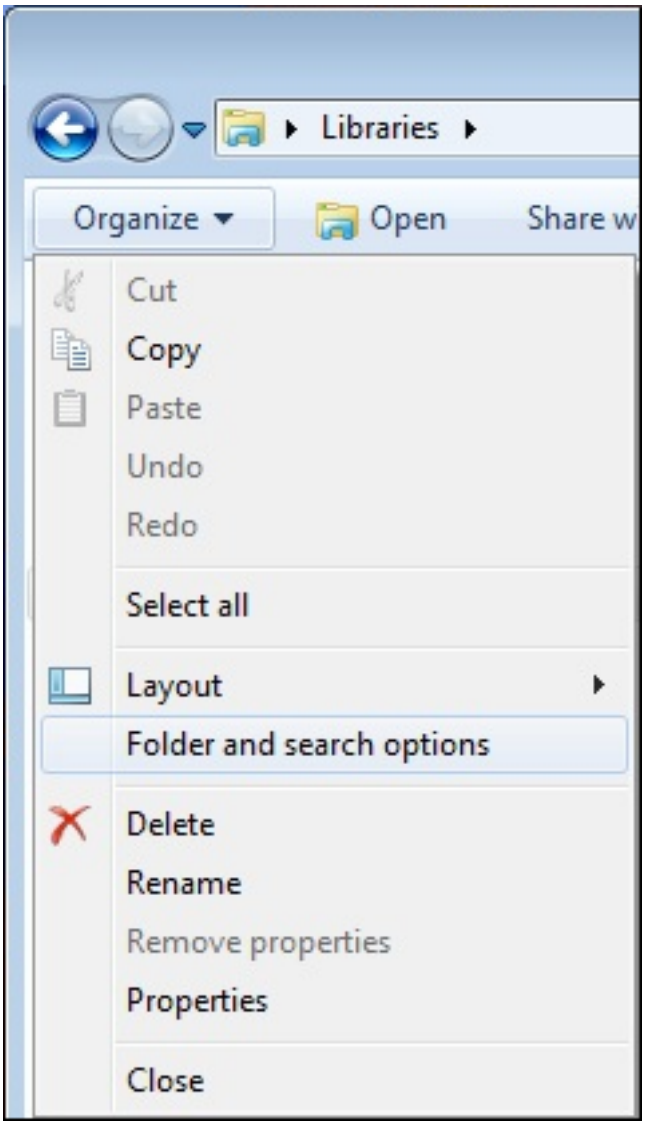
Wie man ein logisches Laufwerk innerhalb einer TSplus-Sitzung einbindet

Dieses Tutorial behandelt die folgenden Aspekte:

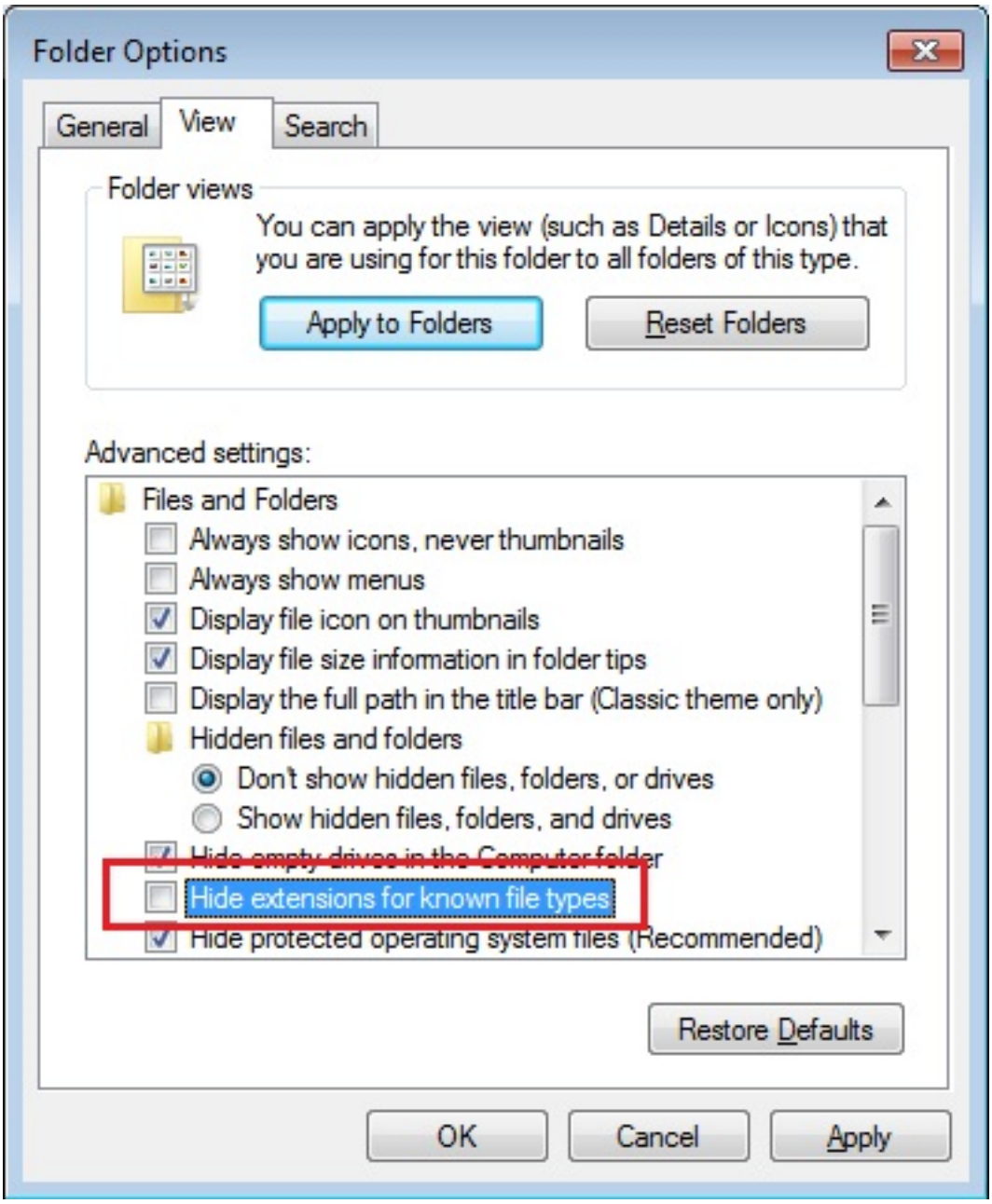
- Wie man ein Anmeldeskript bereitstellt und mehrere Anmeldeskript-Szenarien hat.
- Ein bestimmter Ordner innerhalb einer Sitzung vom Client- oder Server-Seite einbinden.

Wenn Sie einen Ordner auf einem logischen virtuellen Laufwerk für Ihre Benutzer veröffentlichen möchten, befolgen Sie einfach dieses Verfahren:

Vor dem Erstellen des Skripts öffnen Sie den Windows-Explorer und klicken Sie auf „Ordner- und Suchoptionen“.



Dann klicken Sie auf die Registerkarte Ansicht und deaktivieren Sie das Kontrollkästchen „Erweiterungen bei bekannten Dateitypen ausblenden“:

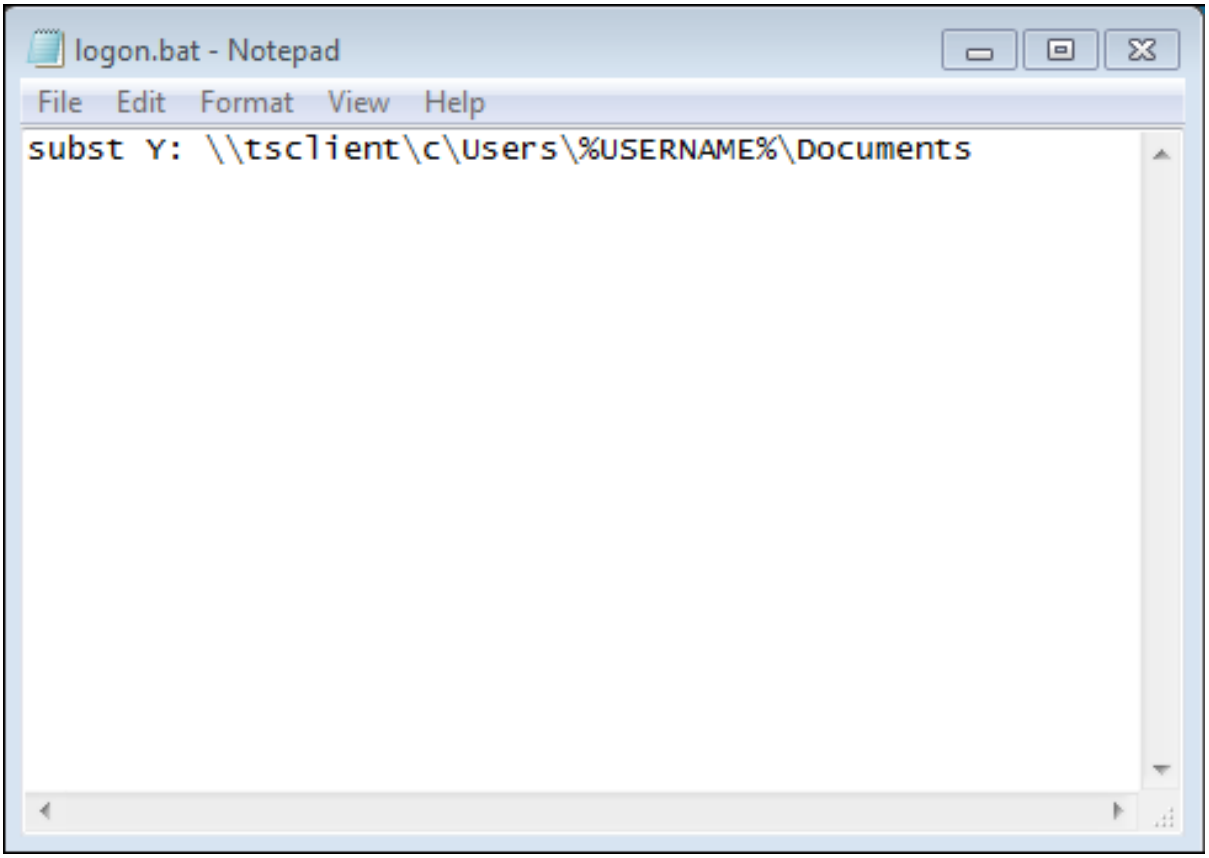


Erstellen Sie ein Textdokument und ändern Sie die Erweiterung, indem Sie es „logon.bat“ nennen.



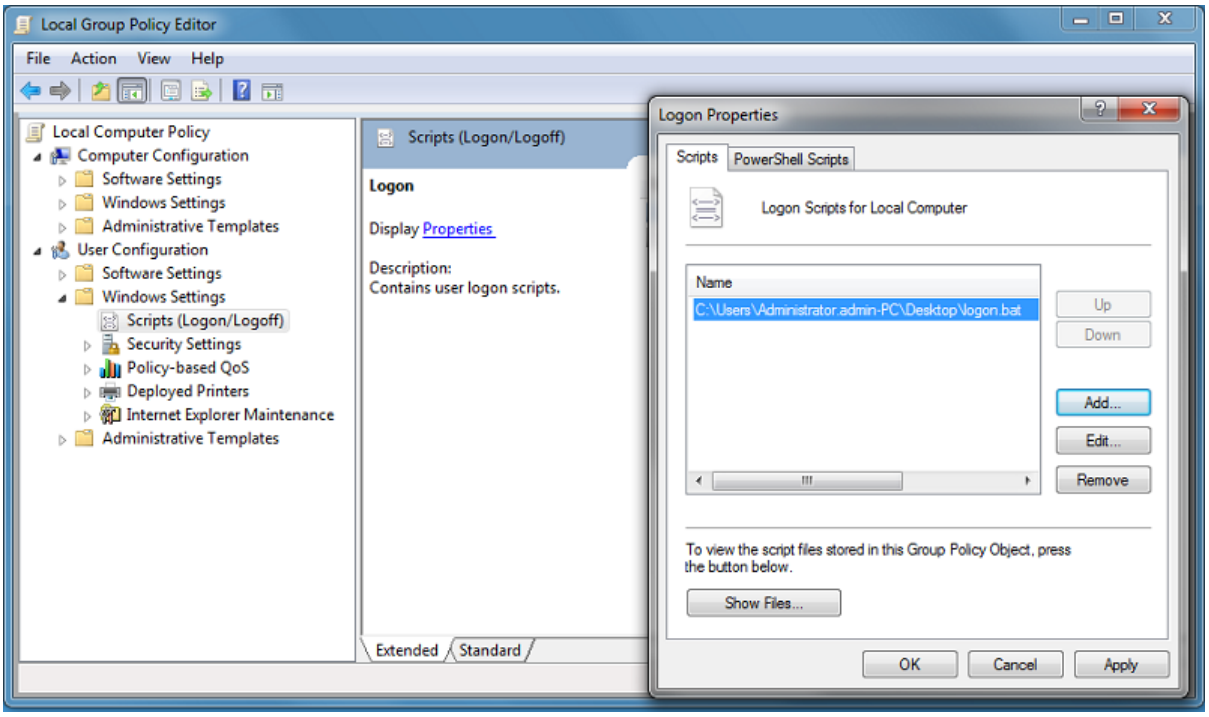
Innerhalb der Datei geben Sie beispielsweise diesen Befehl ein, um den Ordner Folder.exe zu veröffentlichen:

subst Y: \tsclient\C\Users%USERNAME%\Documents

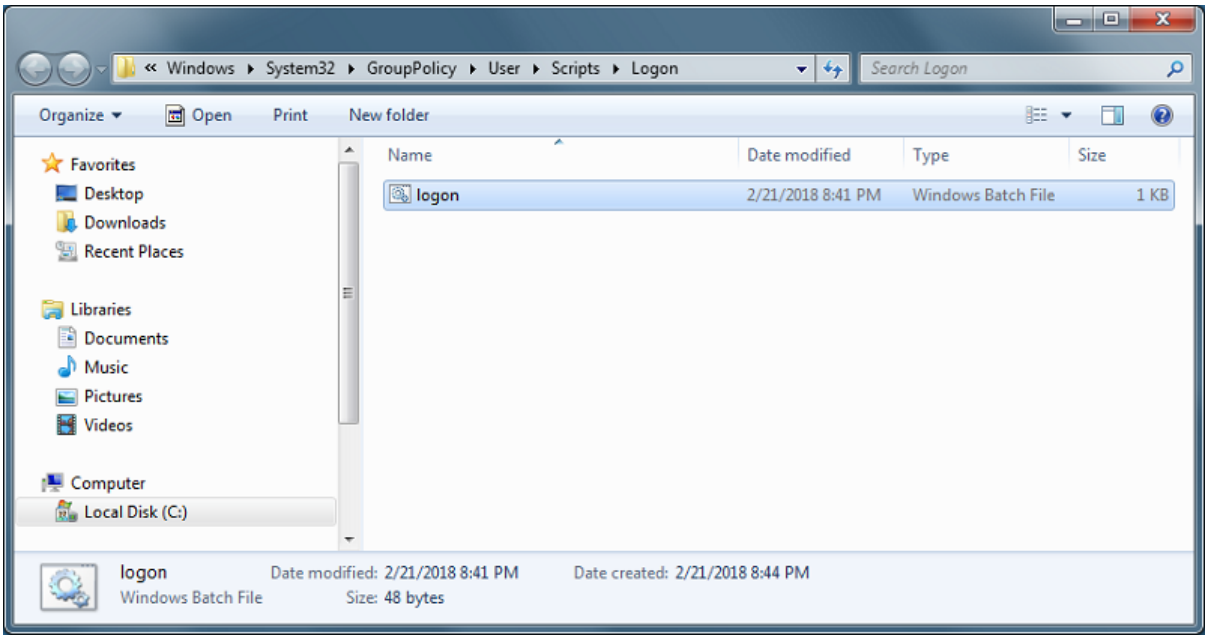


Dann geben Sie im Startmenü gpedit.msc in die Suchleiste ein. Wir werden die lokale Richtlinie verwenden, damit jeder Benutzer, der sich mit diesem Server verbindet, das Skript startet.

Gehen Sie in das Konfigurationsmenü des Benutzers, dann in die Windows-Einstellungen und schließlich in Skripte (Anmeldung/Abmeldung). Doppelklicken Sie auf das Anmeldeskript, klicken Sie dann auf „Hinzufügen“ und anschließend auf „Durchsuchen“.



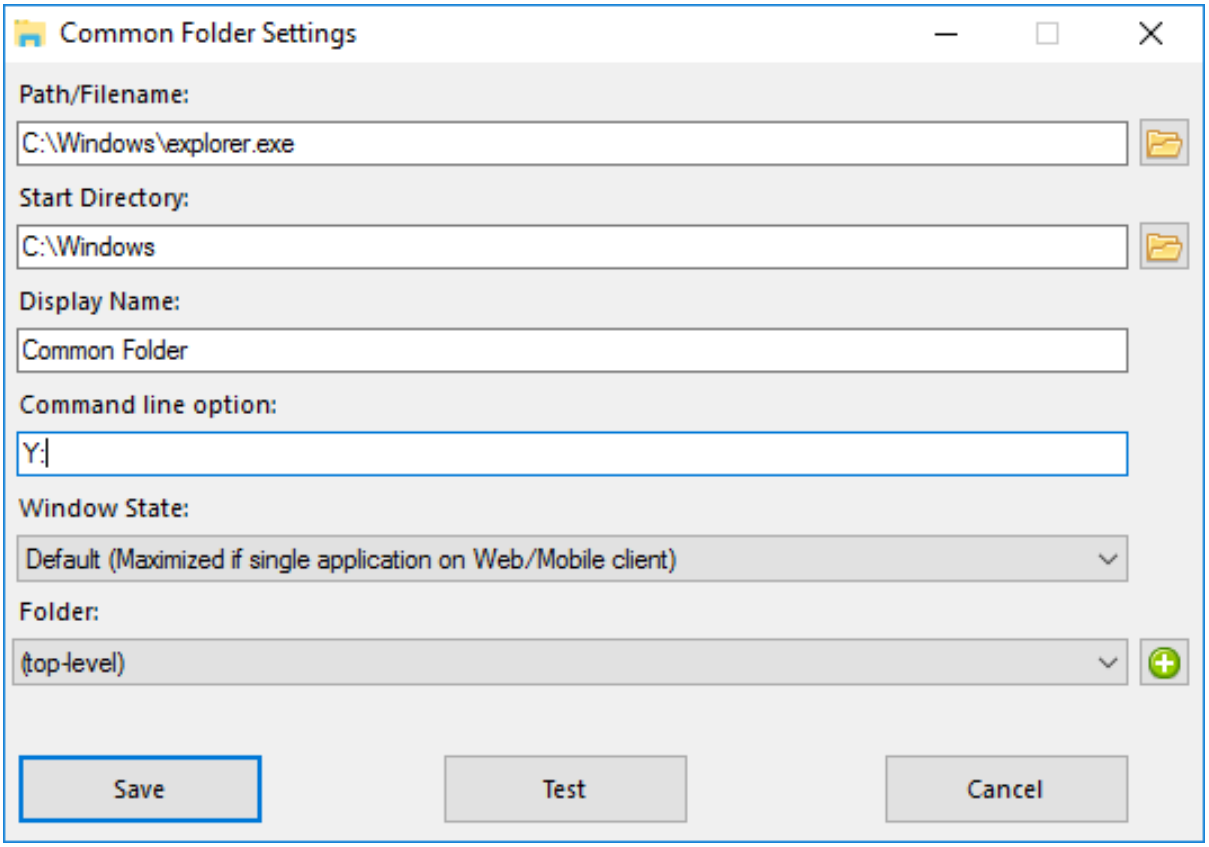
Dann klicken Sie auf die Schaltfläche „Dateien anzeigen“ im Fenster der Anmeldeeigenschaften und kopieren Sie Ihr logon.bat-Skript in den vom Gruppenrichtlinien-Editor angegebenen Pfad, d.h.: „C:\Windows\System32\GroupPolicy\User\Scripts\Logon“



- Sie können diese logon.bat-Datei in C:\ProgramData kopieren, wenn Sie möchten, dass dieses Skript für alle Ihre Benutzer ausgeführt wird.
- Wenn Sie ein spezifisches Anmeldeskript für jeden Benutzer benötigen, kopieren Sie das Skript in C:\Users\Username\AppData\Roaming

Jetzt, wie bringen wir dieses Y-Laufwerk in der Benutzersitzung zum erscheinen? Es gibt viele Möglichkeiten, dies zu erreichen. Sie können eine neue Anwendung im Administrationswerkzeug

erstellen und sie Ihren Benutzern zuweisen, dadurch wird die Verknüpfung in der Sitzung angezeigt.




CommonFolder

Wenn Sie sich mit mstsc.exe mit einer Sitzung verbinden, vergessen Sie nicht, zum Menü Optionen zu gehen, und im Tab Lokale Ressourcen, unter Lokale Geräte und Ressourcen, klicken Sie auf „Mehr“, und aktivieren Sie das Kontrollkästchen „Laufwerke“.

Wenn Sie dieses Skript nur für Nicht-Admin-Benutzer zuweisen möchten, folgen Sie diesem. Anleitung .

Wenn Sie den Zugriff auf einen Ordner sichern möchten, sehen Sie sich unsere Dokumentation zum Veröffentlichen an. gesicherter Ordner .

Anmeldeticket und Lastenausgleich

Logon Ticket-Erstellung auf dem Gateway-Server

Sie können ein Anmeldeticket im Gateway erstellen mit:

/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

Aber es wird Ihnen nur erlauben, sich mit dem Gateway-Server selbst zu verbinden.

Logon Ticket-Erstellung auf einem Anwendungsserver

Sie können auch ein Anmeldeticket auf einem umgekehrten Proxy-Anwendungsserver mit erstellen:

/srv4/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

(angenommen, ~~srv4 ist der interne Name des Anwendungsservers, wie im TSplus-Reverse-Proxy konfiguriert)

Aber es wird Ihnen nur erlauben, sich mit diesem spezifischen Anwendungsserver zu verbinden.

Anmeldeticket und Lastenausgleich

Wenn Sie also Anmeldetickets und Lastenausgleich verwenden möchten, sollten Sie zuerst eine zusätzliche HTTP-Anfrage durchführen:

https://your-gateway-server.com/cgi-bin/hb.exe?action=lb&l=ANMELDUNG&d=DOMAIN&t=ZEITSTEMPEL

Dies wird eine Antwort wie diese zurückgeben:

loadbalancing-on|APP SERVER 4|your-gateway-server.com/~~srv4|https|443|

Sie können diese Antwort analysieren, um den Anwendungsserver abzurufen, mit dem TSplus Load-Balancer Ihnen empfehlen würde, sich mit diesem bestimmten Benutzer zu verbinden.

es wird den weniger ausgelasteten Server in Ihrer TSplus-Farm empfehlen. Wenn sticky Sessions auf Ihrem TSplus-Gateway aktiviert sind, werden bestehende aktive Sitzungen berücksichtigt usw.

Sie können dann ein Anmeldeticket auf diesem speziellen Anwendungsserver erstellen und sich mit dem Benutzer verbinden.

Dies ist genau die http-Anfrage, die auf der Anmeldeseite des TSplus Web Portals durchgeführt wird.

Ein Logon-Ticket verwenden, um eine Benutzersitzung zu öffnen

Jetzt, da Sie ein gültiges Anmeldeticket haben, können Sie eine Benutzersitzung mit diesem Ticket öffnen, indem Sie ein Browserfenster zu dieser URL öffnen:

https://your-gateway-server.com/~~srv4/software/html5.html?user=*xxxxxxxx

wo “xxxxxxxx” das Anmeldeticket ist.

Langzeitunterstützungs-Versionen

Kunden, die sich für die TSplus Support- und Update-Dienste angemeldet haben und an den neuesten Funktionen und Verbesserungen von TSplus nicht interessiert sind, können eine TSplus LTS (Long Term Support) Version installieren.

TSplus LTS (Langzeitunterstützung) Version verlängert den Zeitraum der Softwarewartung; sie reduziert auch die Häufigkeit von Softwareupdates, um das Risiko, die Kosten und die Störungen bei der Softwarebereitstellung zu verringern, während die Zuverlässigkeit der Software gefördert wird.

Darüber hinaus erhält TSplus LTS (Long Term Support) keine neuen Funktionen.

TSplus Lebenszyklus

TSplus Standardversionen werden recht häufig veröffentlicht, und die neueste Version ist immer die beste Lösung, die unseren Kunden zur Verfügung steht: Alle bekannten Fehler werden behoben und neue Funktionen sind sehr oft verfügbar.

Eine neue Hauptversion von TSplus wird zu Beginn jedes Jahres veröffentlicht.

Ab Januar 2019 ist TSplus auch in einer Long Term Support-Version erhältlich, die „LTS“ genannt wird. Mit jeder neuen Hauptversion wird TSplus eine stabile LTS-Version der vorherigen Version veröffentlichen, die 2 Jahre lang unterstützt wird.

Vorteile und Einschränkungen von TSplus LTS

TSplus LTS hat mehrere Vorteile:

- Keine Updates außer Sicherheitskorrekturen und Kompatibilität mit Windows-Updates
- Keine Änderungen im Verhalten und keine Änderungen an den Funktionen, wenn Sie aktualisieren.
- Weniger Risiko beim Aktualisieren zwischen zwei Minor-Versionen eines bestimmten LTS
- Unterstützt für mindestens 2 Jahre

TSplus LTS hat auch Einschränkungen und Begrenzungen:

- Kunde muss Support- und Update-Dienste erwerben (eine Lizenz kann ohne aktive Support- und Update-Dienste nicht aktiviert werden)
- Keine neuen Funktionen (im Vergleich zur TSplus Standardversion, die ständig viele Updates und neue Funktionen erhält)

Wir empfehlen unseren Kunden, die Standardversion von TSplus zu verwenden, um von unserer hochmodernen Lösung zu profitieren.

TSplus LTS-Links

TSplus LTS 18 unterstützt von 2026-01 bis 2028-01:

- Änderungsprotokoll
- Einrichtung TSplus auf einem neuen Server installieren
- Aktualisierung Veröffentlichung um eine vorhandene TSplus-Installation zu aktualisieren
- LTS18 Dokumentation

TSplus LTS 17 unterstützt von 2025-01 bis 2027-01:

- Änderungsprotokoll
- Einrichtung TSplus auf einem neuen Server installieren
- Aktualisierung Veröffentlichung um eine vorhandene TSplus-Installation zu aktualisieren
- LTS17 Dokumentation

TSplus LTS 16 (unterstützt von 2024-01 bis 2026-01): **Ende des Supports**

TSplus LTS 15 (unterstützt von 2023-01 bis 2025-01): **Ende des Supports**

TSplus LTS 14 (unterstützt von 2021-12 bis 2023-12): **Ende des Supports**

TSplus LTS 12 (unterstützt von 2019-12 bis 2022-12): **Ende des Supports**

TSplus LTS 11 (unterstützt von 2018-12 bis 2021-12): **Ende des Supports**

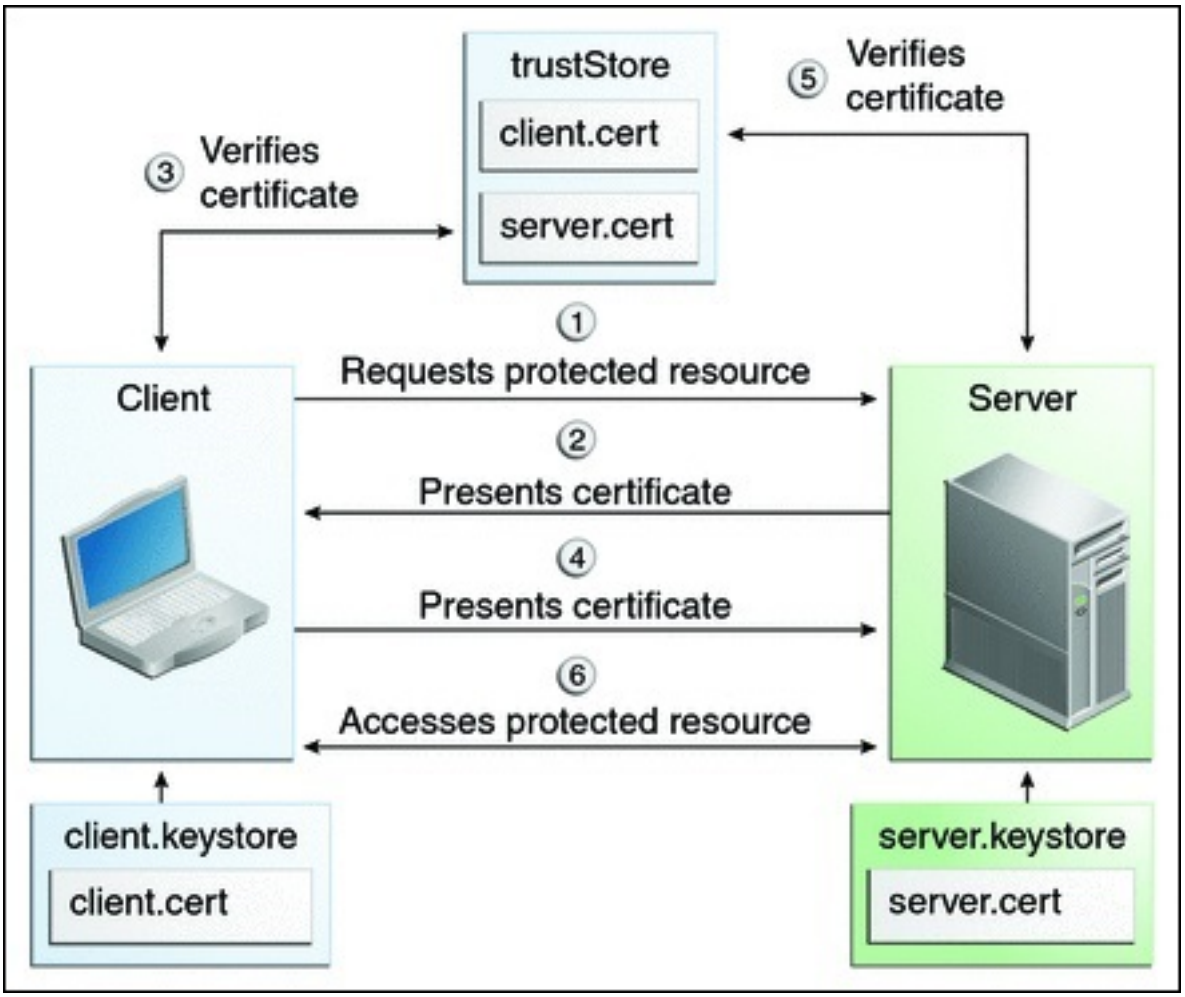
Aktivierung der gegenseitigen SSL-Authentifizierung

Was ist gegenseitige Authentifizierung?

Viele Menschen erwarten zusätzliche Sicherheit, und die gegenseitige Authentifizierung wird bereits in Terminal Service Plus unterstützt. Sie wird normalerweise von Banken oder Regierungsbehörden implementiert.

Um zu verstehen, was das ist, können wir es mit einem standardmäßigen SSL-Prozess vergleichen, bei dem Sie eine zusätzliche Überprüfung hinzufügen, um zu verifizieren, ob der Webbrowser des Benutzers eine SSL-Verbindung zulässt. Sie wissen, was Ihr serverseitiges SSL-Zertifikat ist. Stellen Sie sich vor, das Zertifikat wird in den Webbrowser importiert, um sicherzustellen, dass dieser spezielle Webbrowser als vertrauenswürdig gilt, um eine Verbindung herzustellen. Im ersten Schritt der Kommunikation fungiert der Webbrowser als Client und im zweiten Schritt ist es umgekehrt. Am Ende haben beide Seiten, der Client-Webbrowser und der Webserver, die Autorität akzeptiert und die Verbindung kann beginnen.

Eine vollständigere Definition: Die gegenseitige SSL-Authentifizierung oder zertifikatsbasierte gegenseitige Authentifizierung bezieht sich auf zwei Parteien, die sich gegenseitig authentifizieren, indem sie das bereitgestellte digitale Zertifikat überprüfen, sodass beide Parteien sich der Identität des jeweils anderen sicher sind. In technologischen Begriffen bezieht es sich auf einen Client (Webbrowser oder Client-Anwendung), der sich gegenüber einem Server (Website oder Serveranwendung) authentifiziert, und dieser Server authentifiziert sich ebenfalls gegenüber dem Client, indem er das öffentliche Schlüsselzertifikat/das digitale Zertifikat überprüft, das von den vertrauenswürdigen Zertifizierungsstellen (CAs) ausgestellt wurde. Da die Authentifizierung auf digitalen Zertifikaten basiert, sind Zertifizierungsstellen wie Verisign oder Microsoft Certificate Server ein wichtiger Bestandteil des Prozesses der gegenseitigen Authentifizierung.



Aktivierung auf TSplus

TSplus integrierter Webserver ermöglicht die Einrichtung einer gegenseitigen Authentifizierung.

Um die gegenseitige Authentifizierung zu aktivieren, folgen Sie diesem Prozess:

Sie müssen das neueste Java Development Kit (JDK) installieren, das verfügbar ist von http://java.com > Downloads > JDK.

1. Erstellen und bearbeiten Sie mit Notepad die folgende Datei: C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin

Fügen Sie diese 3 Zeilen hinzu:

disable_http_only=true disable_print_polling=true force_mutual_auth_on_https=true

2. Entfernen Sie cert.jks

In “C:\Program Files (x86)\TSplus\Clients\webserver” sehen Sie die Datei cert.jks. Kopieren Sie sie nach “C:\Program Files (x86)\TSplus\Clients”. Entfernen Sie “C:\Program Files

(x86)\TSplus\Clients\webserver\cert.jks”.

3. Erstellen Sie die Batch-Datei

In ‘C:\Program Files (x86)\TSplus\Clients’ erstellen Sie eine Batch-Datei, zum Beispiel “createcertuser.bat” mit diesen Einstellungen:

@rem Kommentiere die nächste Zeile aus, wenn du ein neues selbstsigniertes cert.jks generieren möchtest @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

Dies wird automatisch das Zertifikatsschlüsselpaar aus dem Webbrowser in „cert.jks“ importieren, nachdem das Schlüsselpaar des Browsers erstellt wurde.

4. Stellen Sie das neu erstellte, modifizierte „cert.jks“ wieder her.

Kopiere “C:\Program Files (x86)\TSplus\Clients\cert.jks” nach “C:\Program Files (x86)\TSplus\Clients\webserver” und starte die Webserver neu.

5. Zertifikatimport und Testen

Die bereitgestellte Batch-Beispiel sollte eine Testdatei „BrowserUser1.p12“ generiert haben. Wenn Sie die HTTPS-Adresse öffnen, erhalten Sie eine Sicherheitsnachricht und können nicht auf die Seiten des Webservers zugreifen. Mit Chrome oder IE können Sie auf diese Datei „BrowserUser1.p12“ klicken, um das Zertifikat in den standardmäßigen Windows-Schlüsselbund zu importieren. Mit FireFox müssen Sie zu den Einstellungen gehen und diese Datei „BrowserUser1.p12“ in Ihren Zertifikatsordner importieren.

Sobald Sie es ordnungsgemäß importiert haben, können Sie auf die HTTPS-Adresse zugreifen.

Der Administrator kann für jeden Benutzer eine separate Schlüsselpaardatei erstellen.

Zum Beispiel:

forBrowserUser1.p12 forBrowserUser2.p12 forBrowserUser3.p12

Und er kann diese Zertifikate in cert.jks exportieren. Wenn er den Zugriff für einen Benutzer deaktivieren möchte, muss er diesen Benutzer einfach aus "cert.jks" löschen. Dadurch verliert der Benutzer seine Berechtigung und kann nicht mehr auf den Webserver zugreifen.

Diese gegenseitige Authentifizierung betrifft nur die HTTPS-Verbindungen, und die HTTP-

Verbindung wird mit der Befehlszeile verboten: settings.bin>disable_http_only=true

Dateien auf der Client-Seite öffnen

Übersicht

Diese Funktion ist eine leistungsstarke. Sie ermöglicht das Öffnen von Dokumenten, die sich auf dem Server befinden, auf der Client-Seite, abhängig von der Dateierweiterung.

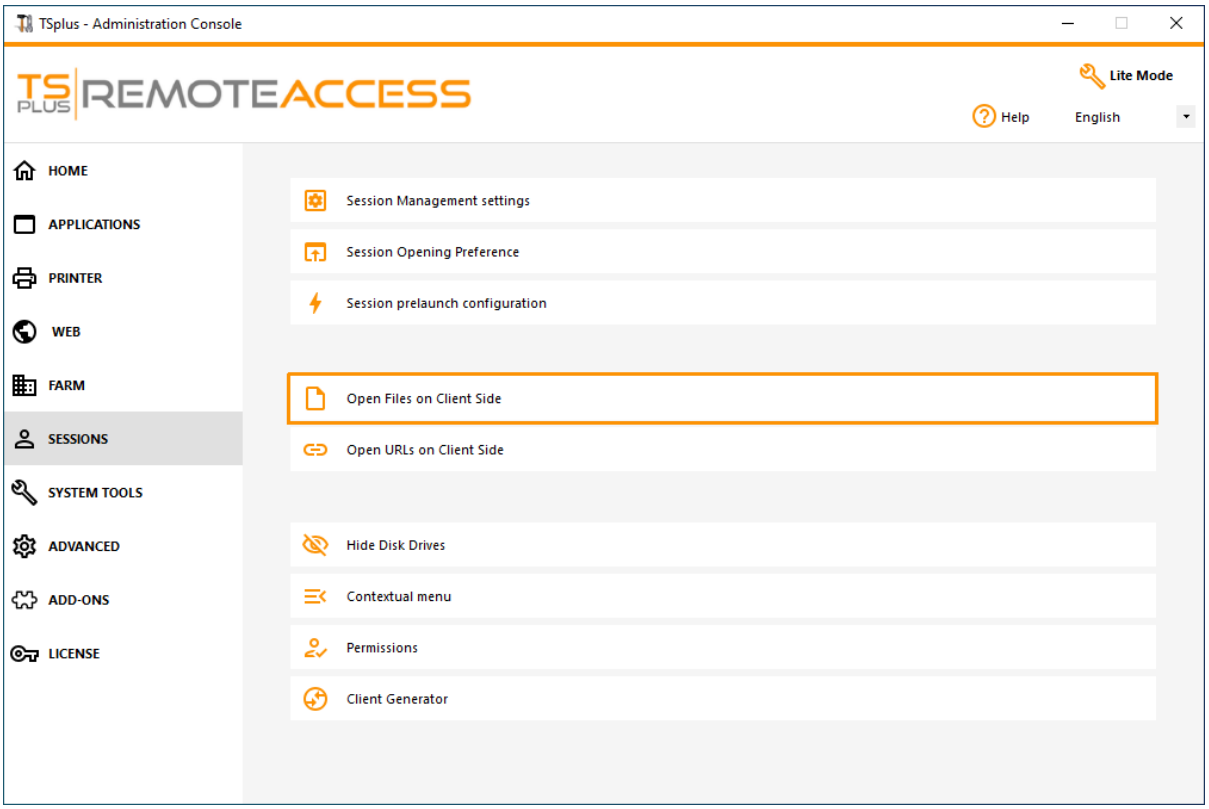
Zum Beispiel können Sie ein Microsoft Office Word-Dokument öffnen, ohne Office auf Ihrem Server installiert zu haben.

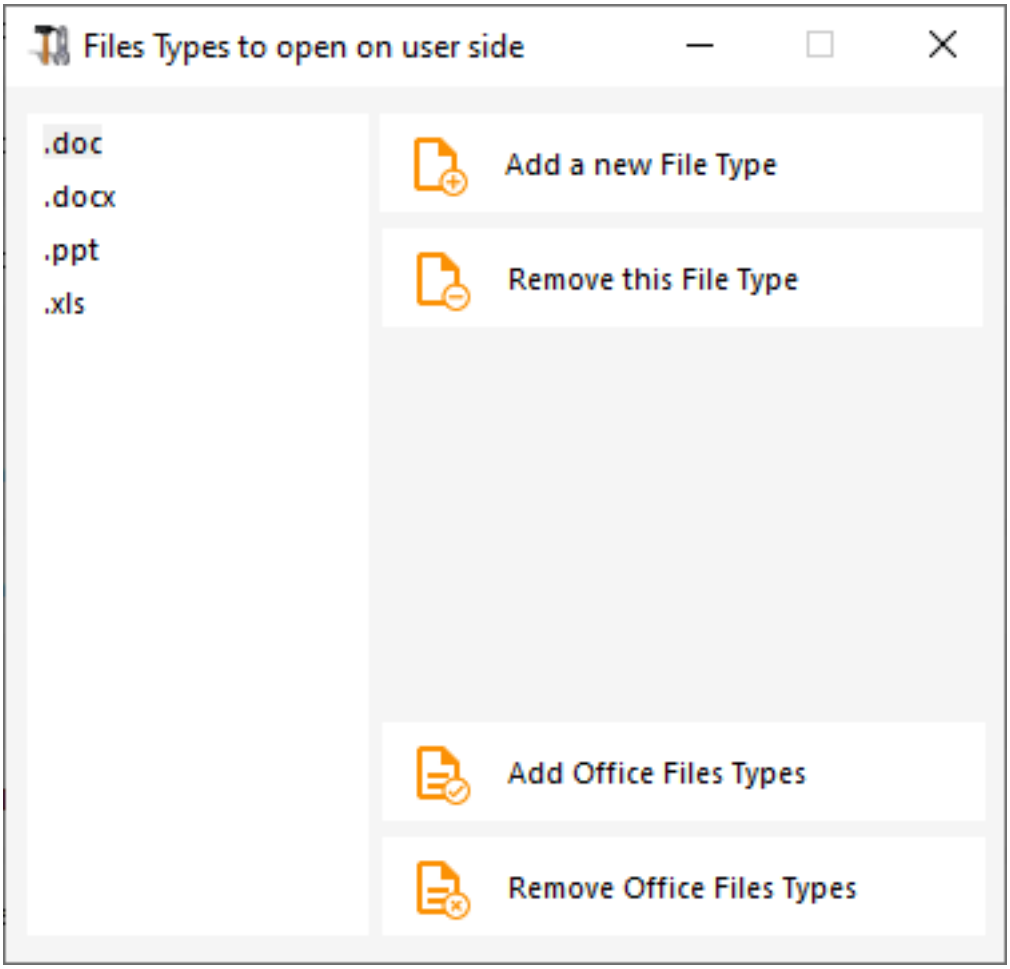
Das .docx (oder .xlsx) Dokument wird automatisch auf der Benutzerseite hochgeladen, wo das lokale Office verwendet wird, um es zu öffnen.

Wenn Sie Ihre Anwendung auf einem Cloud-Server hosten und Ihre Anwendung ein Excel-, Access- oder Word-Dokument generiert, verhindert diese Funktion, dass Sie sich um Office-Lizenzen auf dem Server kümmern müssen.

Konfigurieren eines Dateityps, der auf der Client-Seite geöffnet werden soll

Die Registerkarte „Dateien auf der Client-Seite öffnen“ befindet sich im Tab „Sitzungen - Einstellungen“ des AdminTools. Klicken Sie darauf, um das Konfigurationsfenster anzuzeigen.





Der Button „Neuen Dateityp hinzufügen“ ermöglicht es Ihnen, eine Erweiterung (wie „.docx“ für

Microsoft Office Word 2007-2010) zur Liste hinzuzufügen.

Alle Dateien mit einer Erweiterung in dieser Liste werden dann auf der Client-Seite geöffnet. , vorausgesetzt, dass Sie einen der Terminal Service Plus-Verbindungsclients verwenden:

- Jeder generierte Terminal Service Plus Client (RemoteApp oder RDP)
- Jede Windows-Verbindung vom Terminal Service Plus Web Portal
- Jede HTML5-Verbindung vom Terminal Service Plus Webportal

Warnung: Diese Funktion wird nicht unterstützt für:

- Jeder RDP-Client (mstsc zum Beispiel)

Fehlerbehebung

Wenn Sie einen Dateityp so konfiguriert haben, dass er auf der Client-Seite geöffnet wird, und es nicht funktioniert (d.h. die Datei wird weiterhin auf dem eigenen Computer geöffnet), empfehlen wir Ihnen, die Liste „Öffnen mit“ im Windows-Kontextmenü zu überprüfen:

- Rechtsklick auf die Datei.
- Klicken Sie auf den Menüpunkt „Öffnen mit“.
- Wenn mehr als eine Anwendung in dieser Liste vorhanden ist, klicken Sie auf „Standardprogramm auswählen“ und wählen Sie „OpenOnClient.exe“ aus.

Dieses Terminal Service Plus großartiges Tool wendet seine Konfiguration auf alle Benutzer an, die den Computer verwenden. Bitte beachten Sie jedoch die folgenden Regeln:

- Windows ermöglicht es jedem Benutzer, dieses standardmäßige Öffnungsprogramm durch ein anderes Programm seiner Wahl zu ändern.
- Mit dem HTML5-Verbindungsclient wird die Datei heruntergeladen und vom lokalen Browser verwaltet. Einige Browser behandeln bestimmte Dateitypen auf spezifische Weise, daher sollten die Einstellungen des Browsers ebenfalls zweimal überprüft werden.

Diese Regeln erklären die meisten Probleme bei der Verwendung der Funktion Open On Client, weshalb wir Ihnen raten, zunächst das Standardprogramm zu überprüfen:

- für den angemeldeten Benutzer auf dem Server
- für den Benutzer auf dem Client
- für den Browser auf dem Client (bei Verwendung von HTML5)

URLs auf der Client-Seite öffnen

Übersicht

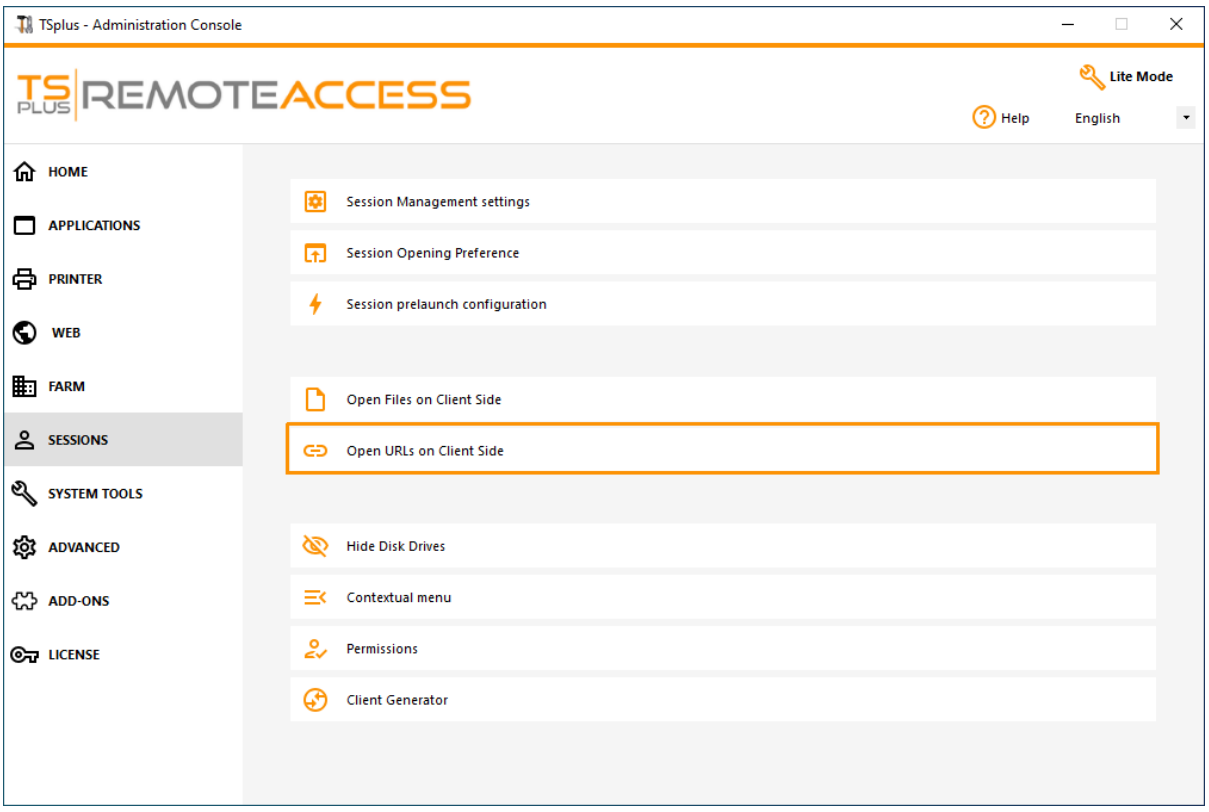
Diese Funktion ist eine leistungsstarke. Sie ermöglicht das Öffnen aller Webseitenlinks und Webseitenverknüpfungen, die sich auf dem Server befinden, auf der Client-Seite.

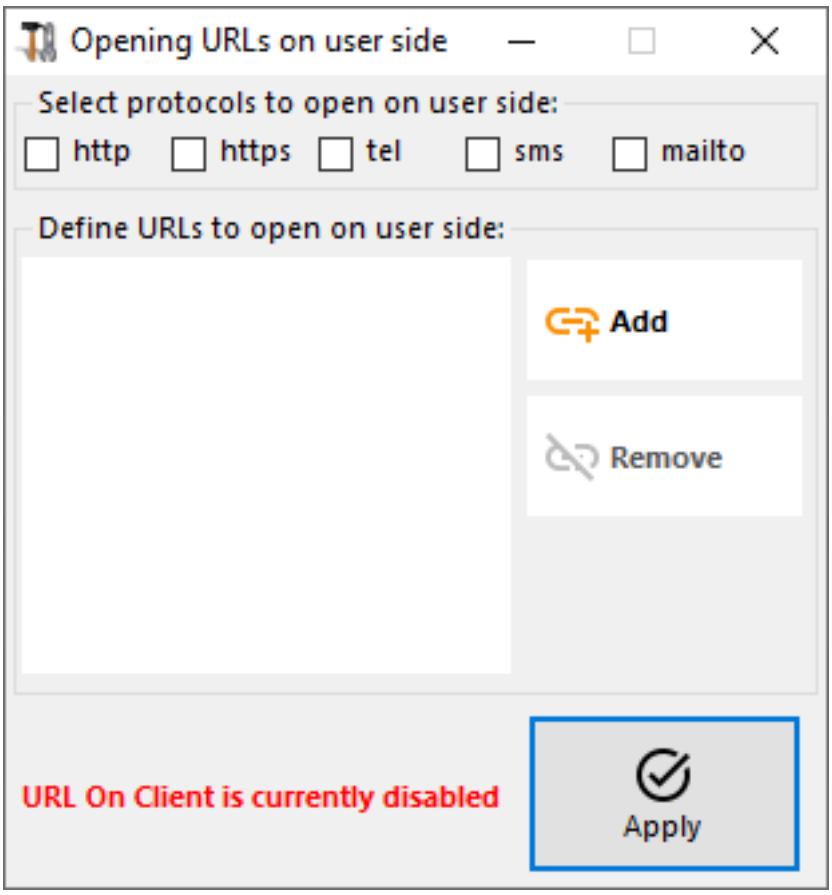
Zum Beispiel können Sie YouTube-Videos direkt auf dem Client öffnen, wodurch viel Bandbreite und CPU-Leistung auf Ihrem Server gespart wird.

Die Webadresse (URL) wird automatisch auf der Benutzerseite übertragen, wo der lokale Standardbrowser verwendet wird, um sie zu öffnen.

Diese Funktion auf einem Server aktivieren

Die Kachel „URLs auf der Client-Seite öffnen“ befindet sich im Tab „Sitzungen - Einstellungen“ des AdminTools. Klicken Sie darauf, um das Konfigurationsfenster anzuzeigen.





Http- und https-Protokollkästchen sind standardmäßig nicht aktiviert.
Sie können auch die Protokolle tel, sms und mailto aktivieren, indem Sie die entsprechenden Kästchen ankreuzen.

Dann klicken Sie auf die Schaltfläche „Übernehmen“, mit der Sie diese Funktion für alle Benutzer auf dem Server aktivieren können.

Um diese Funktion vollständig zu aktivieren, muss jeder Benutzer seine Sitzung neu starten (abmelden und dann anmelden), bevor er diese Funktion nutzen kann.

Alle Weblinks und Verknüpfungen werden dann auf der Client-Seite geöffnet. ,
vorausgesetzt, dass Sie einen der Terminal Service Plus-Verbindungsclients verwenden:

- Jeder generierte Terminal Service Plus Client (RemoteApp oder RDP)
- Jede Windows-Verbindung vom Terminal Service Plus Web Portal
- Jede HTML5-Verbindung vom Terminal Service Plus Web Portal.

Warnung: diese Funktion wird nicht unterstützt für:

- Jeder RDP-Client (mstsc zum Beispiel).

Webbrowser-Verhalten (Webportal):

Einige Webbrowser – insbesondere auf iOS-Geräten – erlauben es nicht, Links automatisch aus

unserer Anwendung zu öffnen. In diesen Fällen wird ein klickbarer Link angezeigt, damit die Benutzer manuell auf das beabsichtigte Ziel zugreifen können.



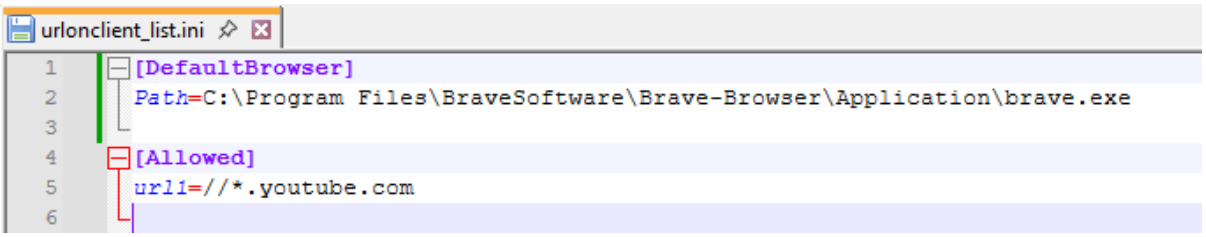
Ändern des Standard-Webbrowsers des Servers

Alle URLs, die nicht definiert sind, um auf der Client-Seite geöffnet zu werden, werden weiterhin auf der Server-Seite geöffnet, unter Verwendung von Microsoft Edge oder Internet Explorer. Wenn Sie den Standard-Webbrowser, der auf der Server-Seite verwendet wird, ändern möchten, müssen Sie die Konfigurationsdatei bearbeiten. **urlonclient_list.ini** im TSPlus-Installationsordner.

Der genaue Speicherort (abhängig von Ihrem genauen Installationspfad) sollte sein: C:\Program Files (x86)\TSplus\UserDesktop\files\urlonclient_list.ini .

Sie müssen einen neuen Abschnitt „DefaultBrowser“ in die Datei hinzufügen und einen Eintrag „Path“ mit dem Wert des Pfades des gewünschten Webbrowsers. So:

[DefaultBrowser]
Path=C:\Path\To\Your\Favorite\WebBrowser.exe



Standardbrowser auf Brave einstellen

☐ **Wenn Sie firefox.exe durch c:\wsession\URLonClient.exe ersetzt haben**

und Sie möchten, dass Firefox Ihr Standard-Webbrowser auf der Serverseite ist :

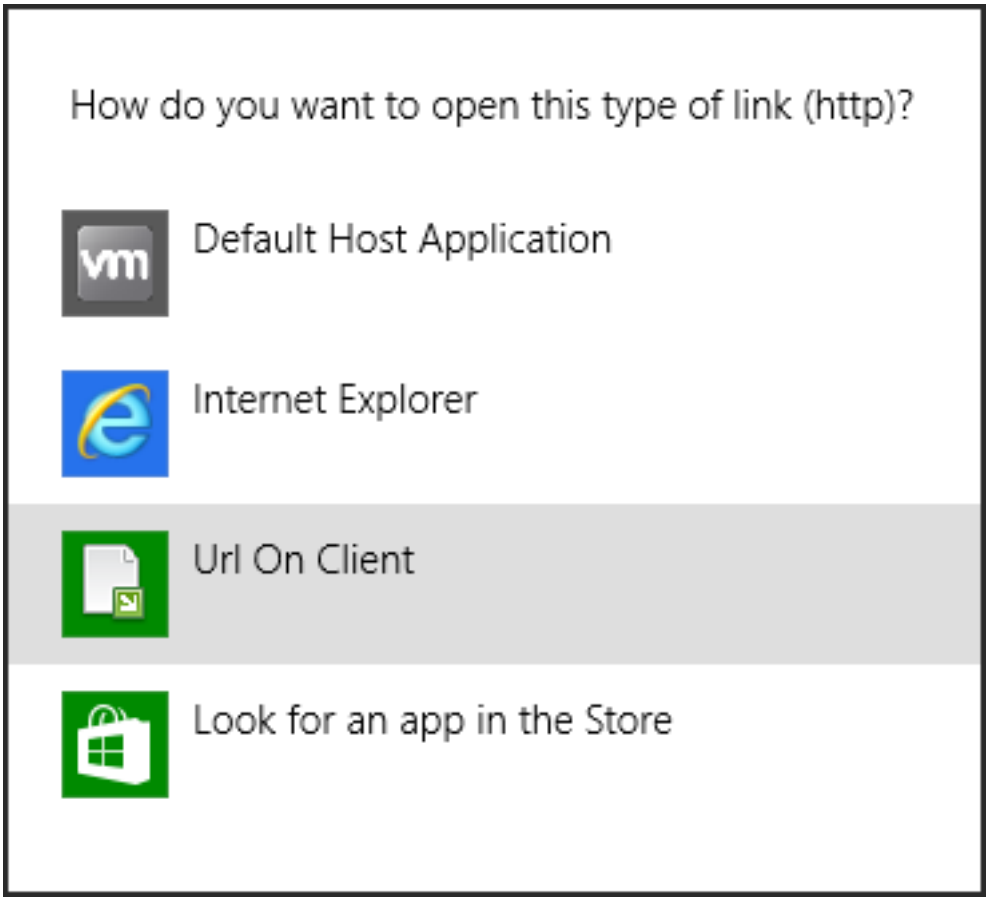
- Benennen Sie die alte firefox.exe-Datei in firefox-real.exe um.
- verwenden Sie den neuen ausführbaren Namen in der **urlonclient_list.ini** Datei :

[DefaultBrowser]
Path=C:\Program Files\Mozilla Firefox\firefox-real.exe

Windows 8 und 8.1

Ab Windows 8 hat Microsoft die automatische Änderung des Standardbrowsers des Benutzers verboten.

Deshalb muss jeder Benutzer, sobald die Funktion auf dem Server aktiviert ist, 'Url On Client' auswählen, wenn er nach einem Standardbrowser gefragt wird.



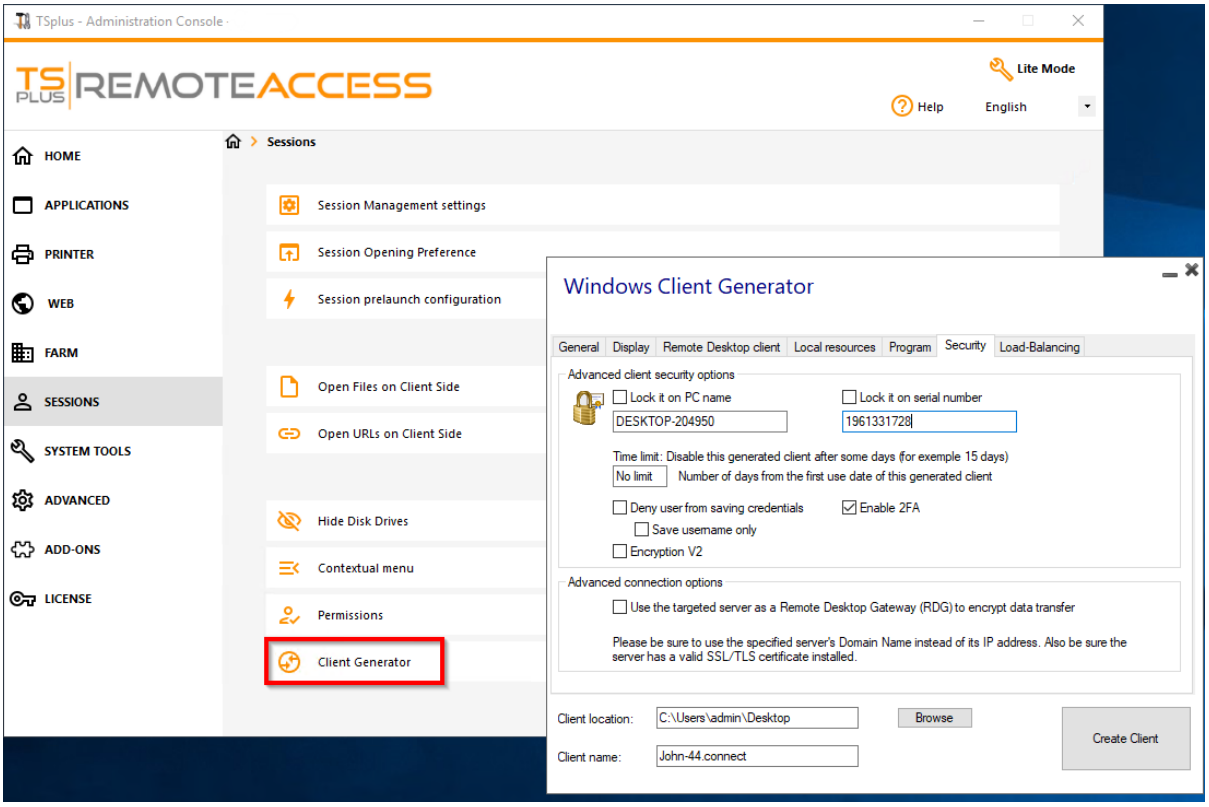
Dieses Fenster wird nur beim ersten Öffnen eines Weblinks durch einen Benutzer angezeigt. Leider ist dies die Richtlinie von Microsoft Windows, und wir sind uns keiner Umgehungslösung bewusst.

Portabler Client-Generator

TSplus erstellt standardmäßig ein Symbol für den Portable Client Generator:



Es kann auch im Reiter Sitzungen des AdminTools zugegriffen werden.



Es ermöglicht Ihnen, 2 Arten von Verbindungsclients zu erstellen, die auf den Desktop der

Benutzer oder auf einen USB-Stick für den portablen Gebrauch kopiert werden können.

Hinweis Connection Clients sind nicht mit Mac-Computern kompatibel.

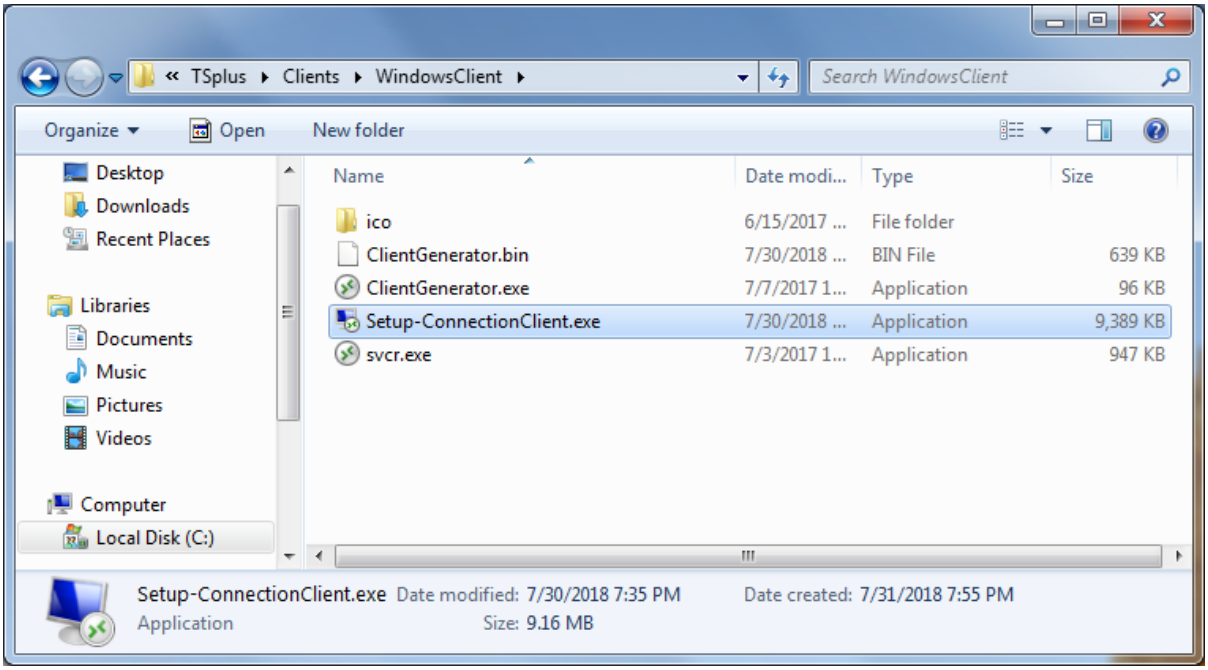
Seit der Veröffentlichung von TSplus 11.40 wurde der Client-Generator neu gestaltet, um numerisch signiert zu sein und um falsche/positive Reaktionen von Antivirenprogrammen zu vermeiden.

Statt eines „.exe“-Programms erstellt der neue Client-Generator eine flache verschlüsselte Datei mit der Erweiterung „.connect“.

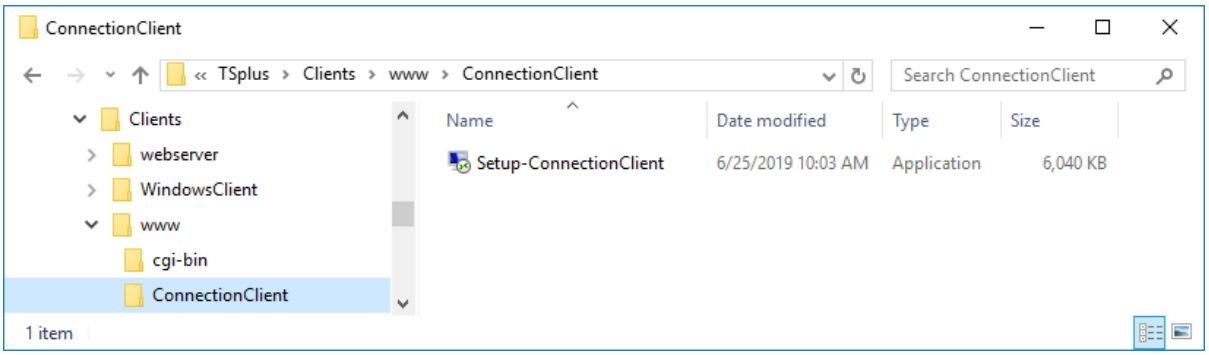


Voraussetzung auf der Client-Seite

Auf der Client-Seite muss jeder Benutzer ein signiertes Programm namens „Setup-ConnectionClient.exe“ als Voraussetzung ausführen. Dieses Programm ist auf Ihrem Server im TSplus-Programmfolder verfügbar: TSplus\Clients\WindowsClient:



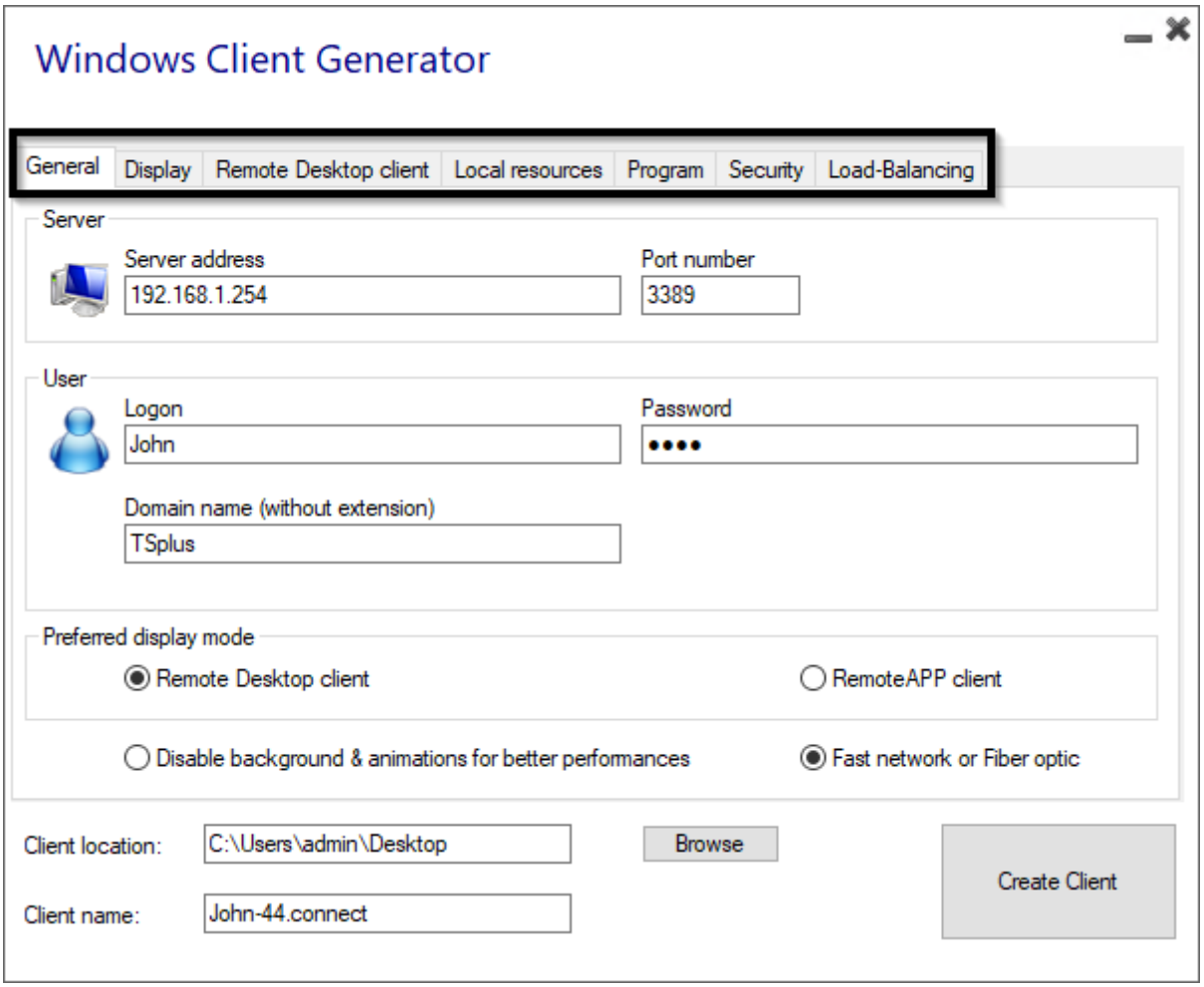
oder im TSplus\Clients\www-Ordner:



oder durch es herunterladen .

Detaillierte Übersicht

Klicken Sie auf **ein Tabulator** um zu den entsprechenden Informationen zu gelangen:



Wenn Sie den Client-Generator starten, wird die erste angezeigte Registerkarte die allgemeine Registerkarte sein. Hier finden Sie alle wesentlichen Verbindungseinstellungen, die Sie

benötigen, um loszulegen.

- **Serveradresse:** Geben Sie die IP-Adresse des Servers ein, mit dem der Client eine Verbindung herstellen soll.
- **Portnummer:** Geben Sie die Serverportnummer ein. Der Standardwert ist 3389.
- **Benutzername und Passwort:** Wenn Sie einen Benutzernamen und ein Passwort eingeben, wird das Client-Programm den Benutzer nicht auffordern, es bei jeder Sitzung erneut einzugeben.

Um diese Anmelde-/Passwortspeicherung zurückzusetzen, müssen Sie eine Verknüpfung des Remote Desktop Clients erstellen und bearbeiten und die hinzufügen -reset aktivieren Schalter am Ende des Zielbereichs.

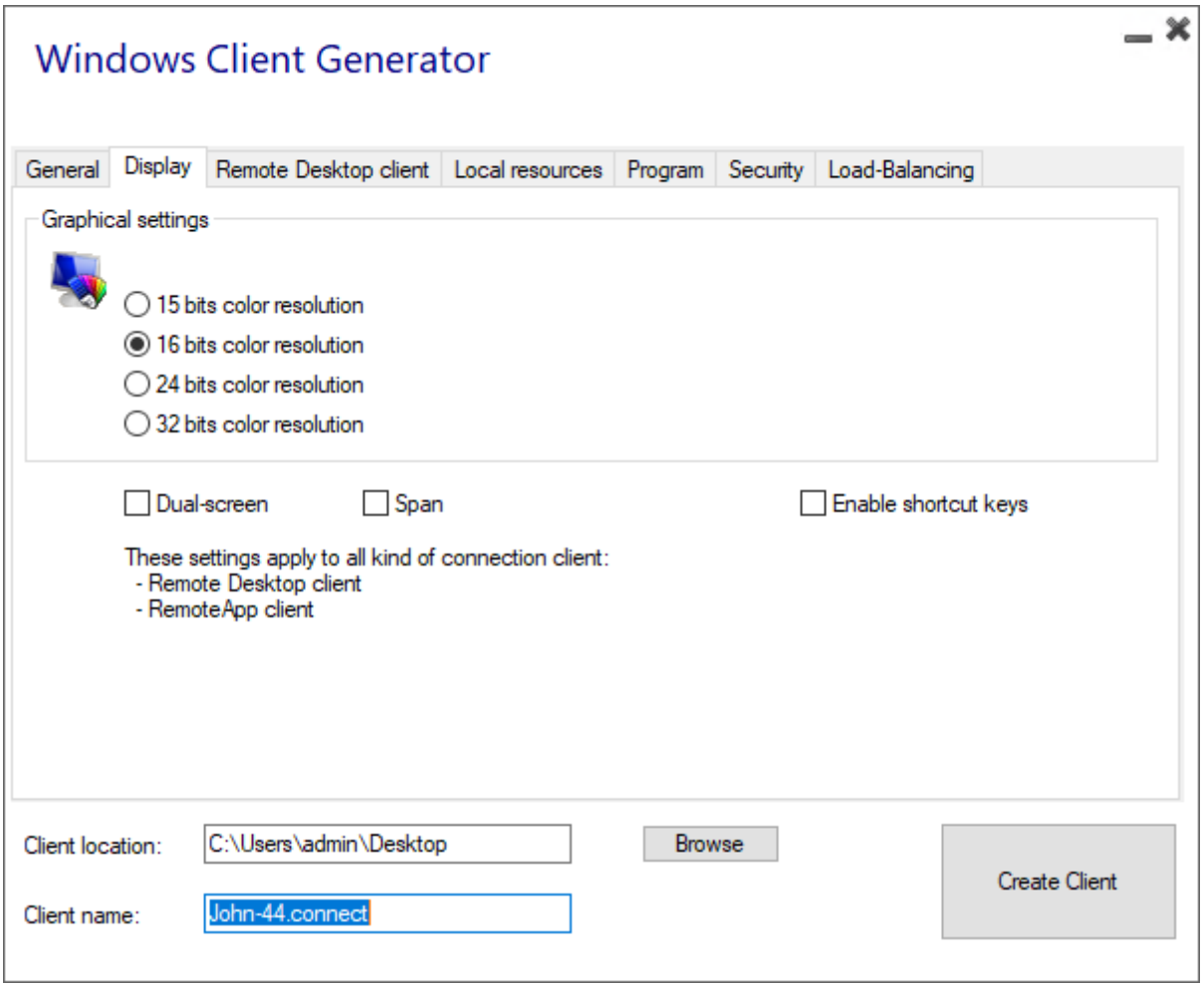
Anmeldeinformationen

- Wenn Sie keine Anmeldeinformationen speichern möchten, geben Sie „nosavecredential“ in das Anmeldefeld des Portable Client Generators ein.
- Wenn Sie das Anmeldefenster mit dem Benutzernamen, Passwort und Domänennamen nicht anzeigen möchten, geben Sie einfach „nopassword“ im Passwortfeld ein.
- Wenn Sie die automatische Anmeldung aktivieren möchten, geben Sie *SSO im Benutzernamenfeld ein. Das Client-Programm wird beim allerersten Verbindungsaufbau nur nach Benutzername und Passwort fragen. Es speichert diese Informationen auf der Arbeitsstation des Benutzers, sodass sich der Benutzer nie wieder identifizieren muss.
- Wenn Sie den aktuellen lokalen Benutzernamen als Anmeldedaten für die Sitzung anzeigen lassen möchten, geben Sie ** oder %USERNAME% im Anmeldefeld ein.

- **Domainname:** Geben Sie einen Domainnamen ein, falls vorhanden.
- **Bevorzugter Anzeigemodus:** Sie können Ihren bevorzugten Anzeigemodus aus den folgenden Optionen wählen:
  - Die Klassisches Remote-Desktop , die Ihre Remote-Sitzungsumgebung anzeigt.

- Die Microsoft RemoteApp-Verbindungsclient , um Ihre Remote-Anwendungen so anzuzeigen, als wären sie lokal installiert. Es bietet eine bessere grafische Leistung bei minimierten Anwendungen.

- **Netzwerkgeschwindigkeit** Sie können je nach Ihrer Netzwerkgeschwindigkeit zwischen zwei Optionen wählen:
  - Hintergrundanzeige und grafische Animationen für langsame Netzwerke deaktivieren.
  - Hintergrundanzeige und grafische Animationen für Glasfaser- oder schnelle Netzwerke aktivieren.
- **Kundenstandort:** Definieren Sie den Speicherort Ihres generierten Clients.
- **Kundenname:** Sie können Ihren Kunden nach Belieben benennen.

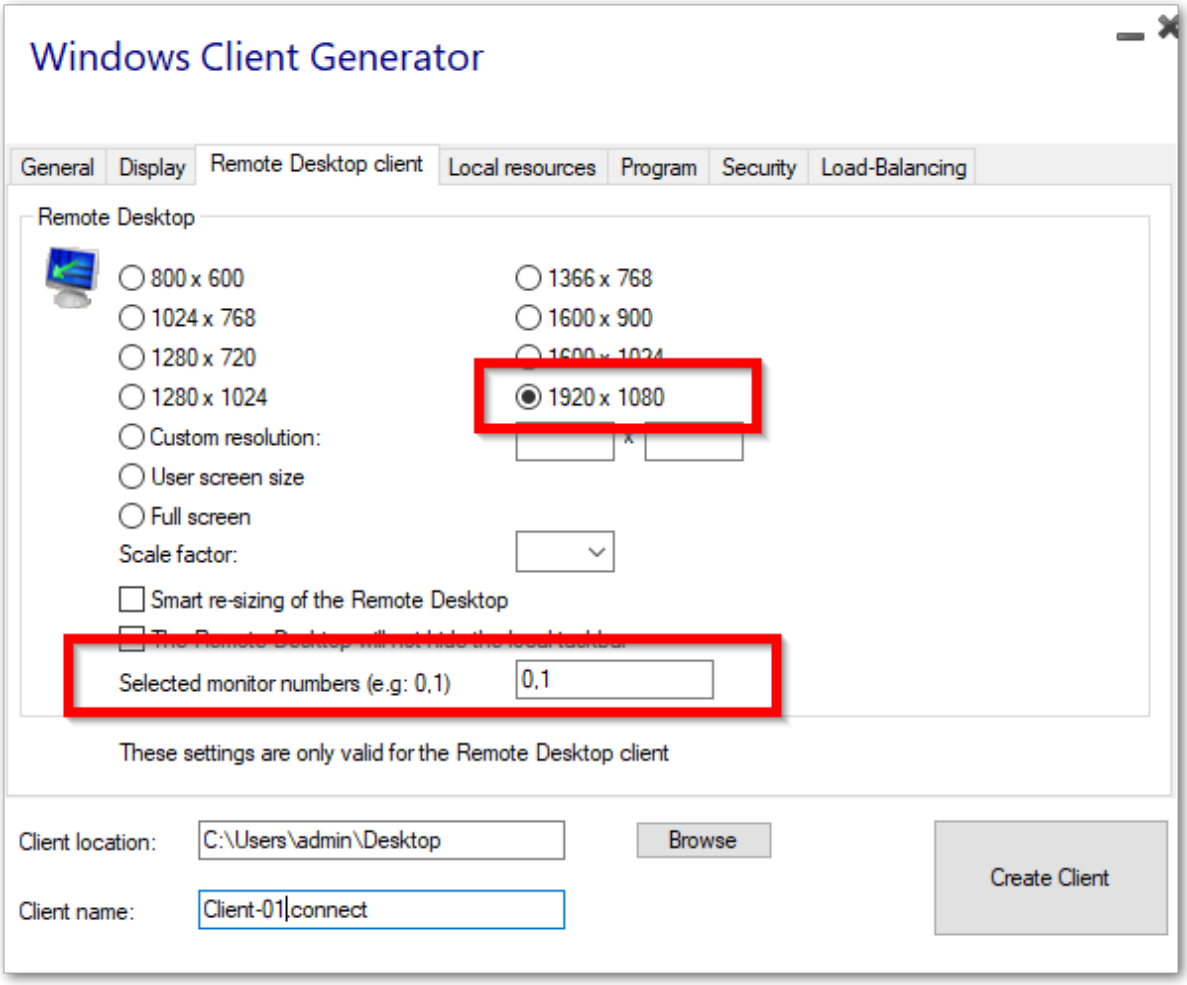


Auf diesem Tab können Sie die Farbe und die Bildschirmauflösung der Sitzung ändern.

Sie können Ihre Sitzung auch für Dual-Screens anpassen, mit oder ohne Überlappung. Die Überlappungsoption ermöglicht es Ihnen, Ihre Sitzung über beide Bildschirme zu strecken.

Sie können die Verwendung der TAB-Taste in der Sitzung erlauben.

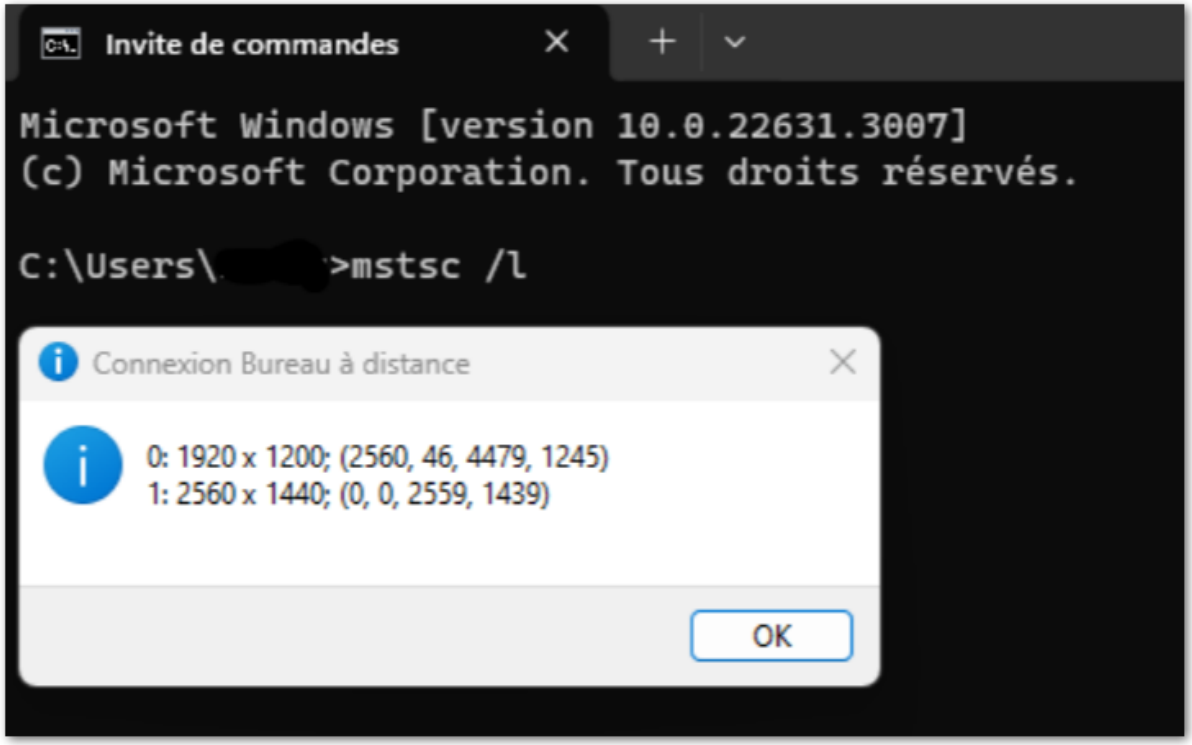
Auf diesem Tab können Sie auswählen, welche Auflösung Sie für den Benutzer aktivieren möchten:



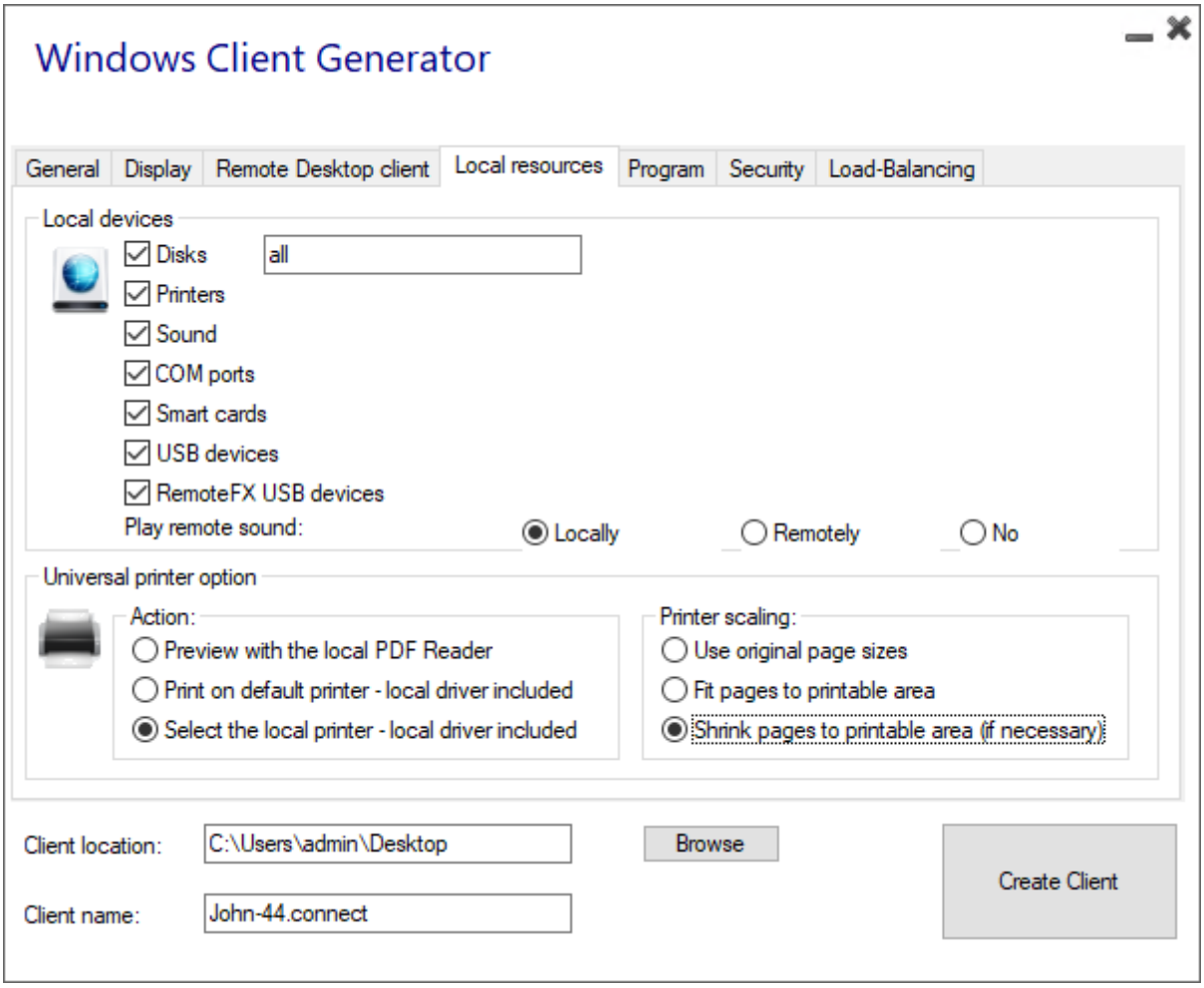
Sie können die Kästchen aktivieren, um das intelligente Anpassen des Remote Desktop zu ermöglichen, und wenn Sie möchten, dass der Remote Desktop die lokale Taskleiste nicht versteckt oder überlappt.

Bildschirmauswahloption

Dies ermöglicht es Ihnen, die Monitore anzugeben, die Sie für die RDP-Sitzung verwenden möchten. Das Feld muss mit der Liste der zu verwendenden Bildschirmnummern gefüllt werden (getrennt durch ein Komma, ein Leerzeichen oder ein Semikolon).



Um die Bildschirmnummern zu identifizieren, führen Sie einfach den Befehl aus. **mstsc /l**



Die Registerkarte für lokale Ressourcen sammelt alle Geräte, die Sie in Ihrer Remote-Sitzung umleiten können.

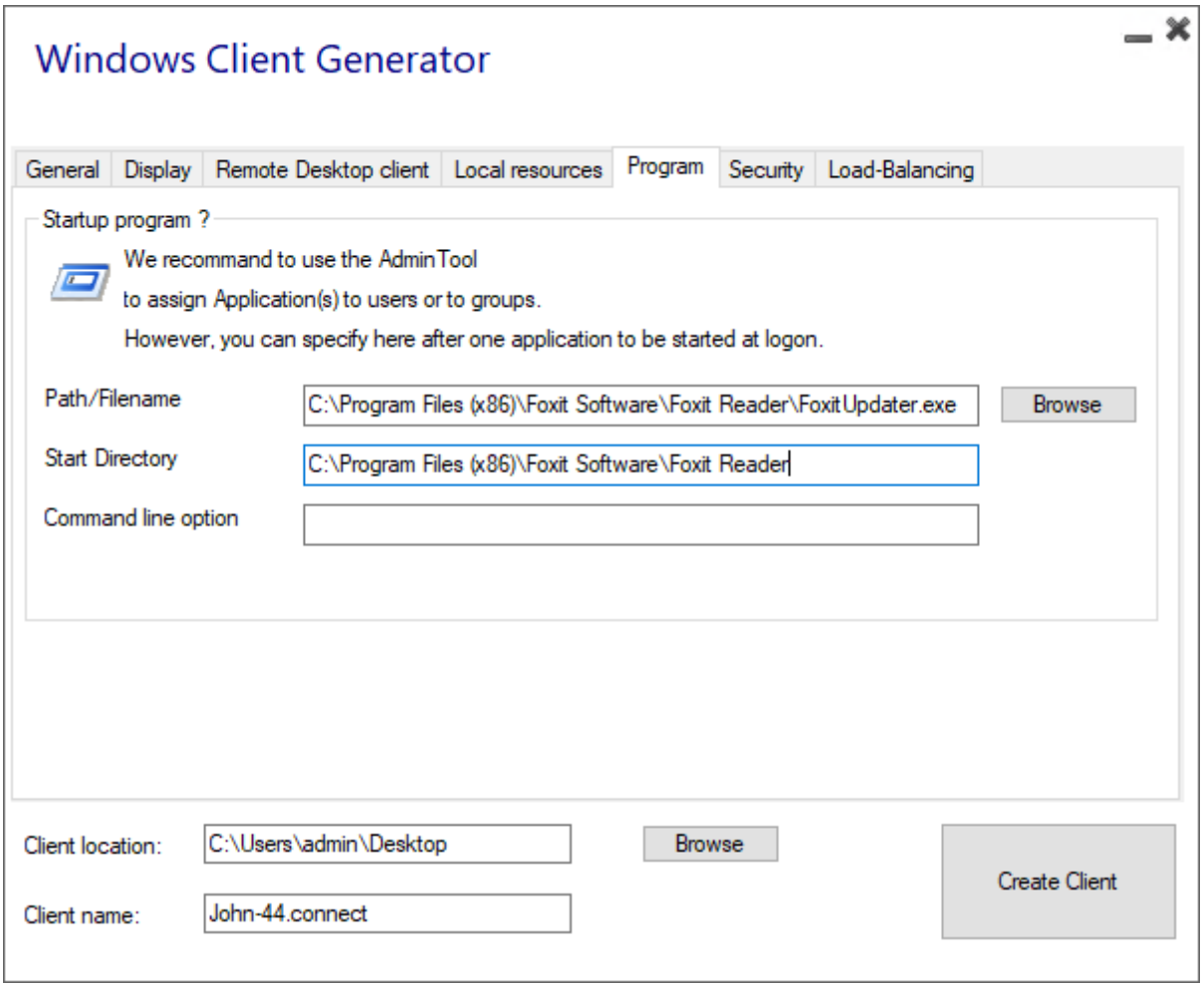
Das bearbeitbare Feld neben dem **Festplatten** Das Feld ermöglicht es, welche Laufwerke in der Remotesitzung verfügbar sind, anzugeben. Sie müssen nur jeden Buchstaben des Laufwerks (C :, E: …) durch ein Komma trennen. Wenn das Laufwerksfeld aktiviert ist und kein Laufwerk angegeben ist, sind alle Laufwerke in der Remotesitzung enthalten.

Drucker Entsprechen LPT-Ports, und COM-Ports entsprechen seriellen Ports. Seit der Version 11.50 von TSplus werden diese lokalen Geräte standardmäßig ausgewählt.

Unten können Sie Ihre Option zum Drucken mit dem universellen Drucker auswählen:

- **Lokale PDF-Reader-Vorschau:** Das Dokument wird als PDF gerendert und der lokale Acrobat Reader öffnet die Datei. Der Benutzer kann es drucken oder eine Kopie auf seinem lokalen Datenträger speichern.
- **Drucken auf dem Standarddrucker des Benutzers:** Das Dokument wird automatisch an den Standarddrucker des Benutzers gesendet (der lokale Druckertreiber ist im TSplus-Verbindungsclient enthalten).
- **Wählen Sie einen lokalen Drucker:** Der Benutzer kann einen seiner lokalen Drucker auswählen (der lokale Druckertreiber ist im TSplus-Verbindungsclient enthalten).

Wenn Sie keinen PDF-Reader auf Ihrem Computer installiert haben, empfehlen wir die Verwendung von Foxit Reader.



Sie können eine Startanwendung über den Portable Client Generator festlegen und ihren Pfad, das Verzeichnis und die Parameter angeben, seit der Version 11.30.

Wir empfehlen Ihnen jedoch, das AdminTool zu verwenden, um die gewünschten Anwendungen zuzuweisen.

TSplus bietet zwei zusätzliche Schichten physischer Sicherheit, um die Verbindungen Ihrer Benutzer zu schützen.

Die Verbindung kann an die ID eines USB-Schlüssels, an einen Computernamen gebunden oder Sie können beide Sicherheitsebenen gleichzeitig verwenden.

Erweiterte Sicherheitsoption für Clients

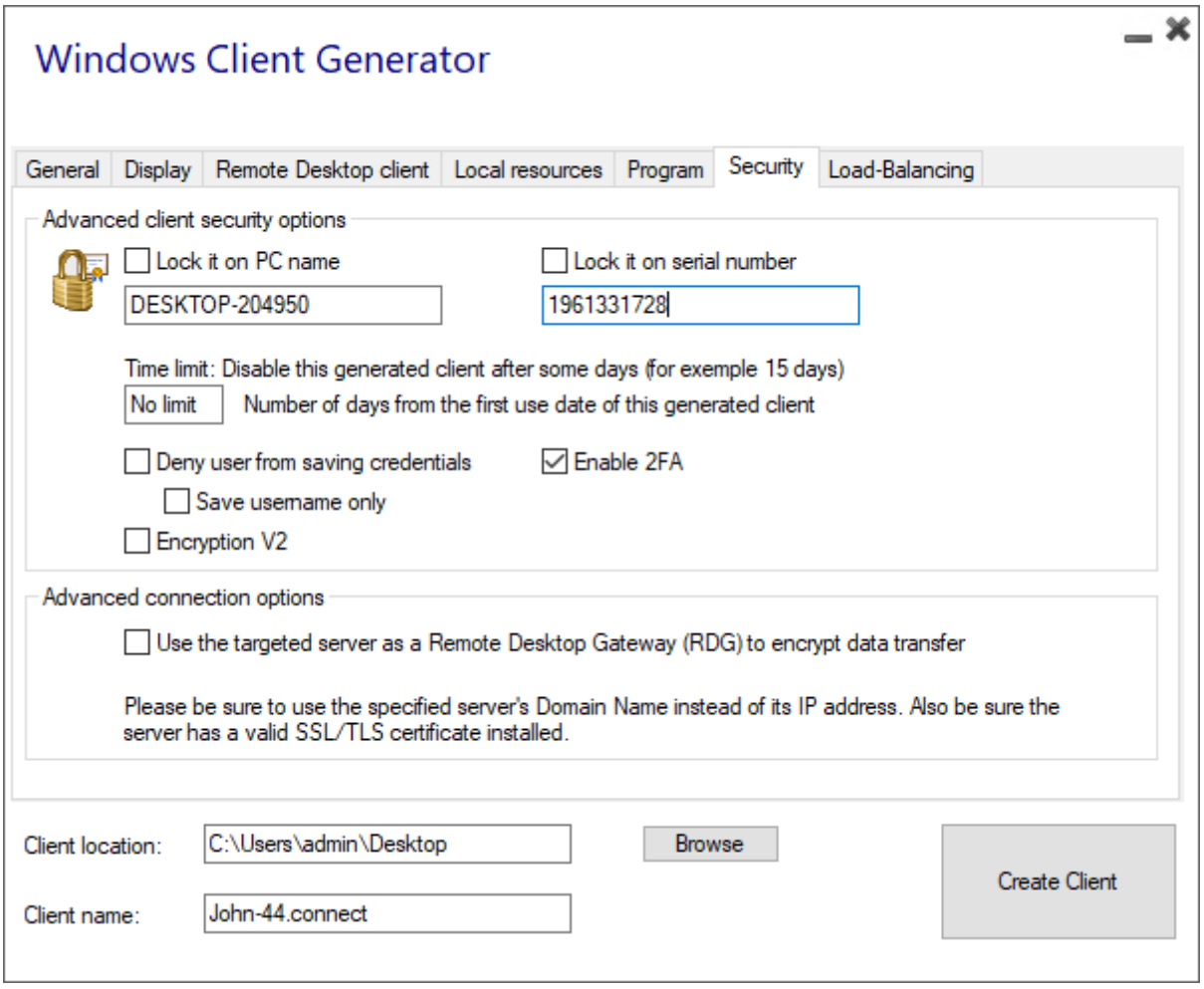
- **Wenn an einen USB-Schlüssel gebunden** Der Benutzer kann eine Verbindung von jedem qualifizierten Windows-Computer herstellen, indem er den USB-Schlüssel einfügt und das dort vom Administrator platzierte Verbindungsprogramm verwendet.
- **Wenn an einen Computernamen gebunden** Der Benutzer kann nur erfolgreich von dem Computer aus eine Verbindung herstellen, dessen Name beim Server für die tragbare Clientverbindung dieses Benutzers registriert wurde. Wenn beide Sicherheitsoptionen verwendet werden, ist der Benutzer darauf beschränkt, sich nur von seinem spezifischen

Gerät aus zu verbinden und nur, wenn der richtige vorkonfigurierte USB-Schlüssel vorhanden ist.

Um einen Verbindungsclient an einen USB-Stick zu binden, können Sie dies tun, indem Sie den Client-Generator kopieren, der sich befindet in: C:\Program Files (x86)\TSplus\Clients\WindowsClient

Jetzt doppelklicken Sie auf den Client-Generator und überprüfen Sie das Schloss im Feld für die Seriennummer, das sich auf der Registerkarte Sicherheit befindet. Sobald dies erledigt ist, können Sie den Client-Generator vom USB-Stick löschen.

Der neu generierte Verbindungsclient wird auf dem Desktop platziert, vergessen Sie nicht, ihn zurück auf den USB-Stick zu kopieren! Sie können den Client-Generator, den Sie anschließend auf den USB-Stick kopiert haben, löschen.



- Sie können die **Zeitlimit** von dem ersten Nutzungsdatum eines generierten Clients, indem der Wert im Zeitlimitfeld eingegeben wird. (das standardmäßig auf "kein Limit" eingestellt ist).

- Die Kästchen unten ermöglichen es Ihnen, zu:

- Nicht die Möglichkeit anzeigen, Anmeldeinformationen für einen generierten Client zu speichern.
  - Benutzername nur speichern.
  - Verwenden Sie Verschlüsselung V2.

Unterstützung für die Zwei-Faktor-Authentifizierung

Der Client-Generator unterstützt **Zwei-Faktor-Authentifizierung** seit Version 15.30.3.15. Die Unterstützung der Zwei-Faktor-Authentifizierung erfordert ebenfalls eine **Mobile Web Edition oder höher** .

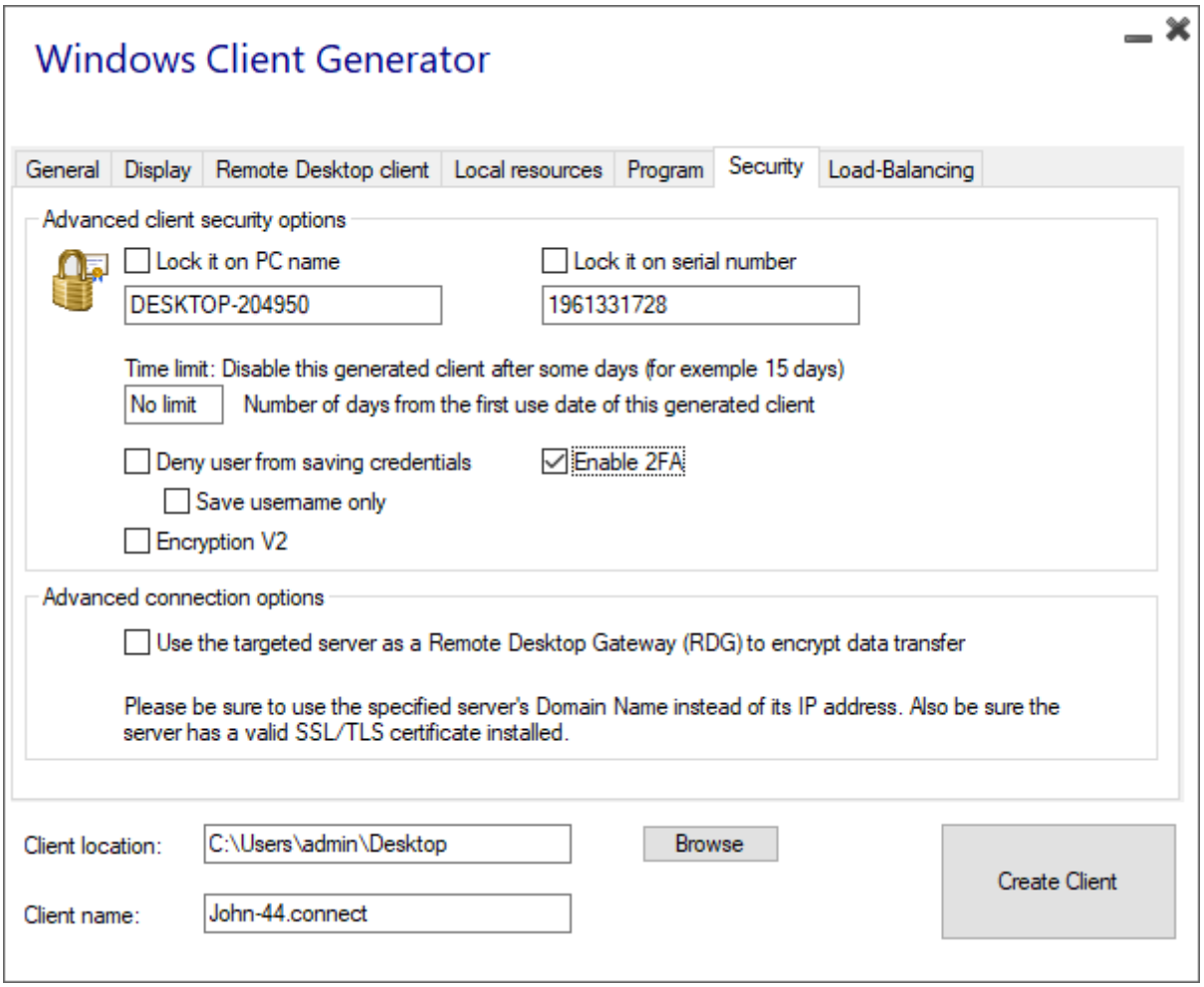
Bitte beziehen Sie sich auf Zwei-Faktor-Authentifizierung Dokumentationsseite für weitere Informationen zur Konfiguration und Aktivierung der Zwei-Faktor-Authentifizierung für Benutzer und Gruppen in Ihrer TSplus Remote Access-Installation.

Bitte beachten Sie die folgenden zusätzlichen Anforderungen, um die Zwei-Faktor-Authentifizierung für einen generierten Client zu aktivieren:

- Der Connection Client validiert den Authentifizierungscode gegen das Webportal über den HTTPS-Port. Daher, **Webportal muss betriebsbereit sein** und über seinen HTTPS-Port von der Clientmaschine aus erreichbar.
- Wenn der HTTPS-Port des Webportals geändert wird, müssen die generierten Clients, die für die Zwei-Faktor-Authentifizierung aktiviert sind, erneut generiert werden. Zuvor generierte Clients werden bei der Validierung der Zwei-Faktor-Authentifizierung fehlschlagen.

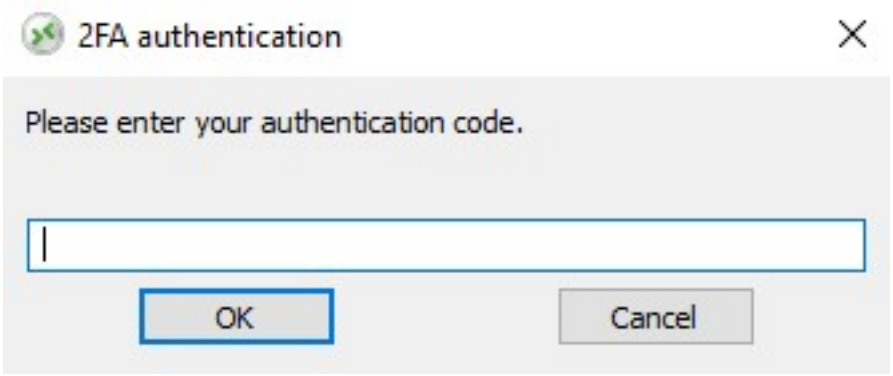
Seit Version 15.30.3.15 verhalten sich alle zuvor generierten Clients und alle neuen Clients, die ohne aktivierte 2FA-Unterstützung generiert werden, wie zuvor. **Wenn ein Benutzer, der für die Zwei-Faktor-Authentifizierung aktiviert ist, versucht, sich mit einem Client anzumelden, der ohne explizite 2FA-Unterstützung generiert wurde, wird der Login verweigert.** da die Zwei-Faktor-Authentifizierung nicht möglich ist und daher fehlschlagen wird.

Um Unterstützung für die Zwei-Faktor-Authentifizierung hinzuzufügen, überprüfen Sie die **Aktivieren Sie 2FA** Aktivieren Sie das Kontrollkästchen, bevor Sie Ihre Client-Datei generieren. Infolgedessen wird die Zwei-Faktor-Authentifizierung validiert, wenn Sie sich mit dem Remote Access-Anwendungsserver verbinden. Wenn die Zwei-Faktor-Authentifizierung auf dem Anwendungsserver aktiviert ist und der sich verbindende Benutzer nicht konfiguriert ist, wird die Verbindung verweigert.



Seien Sie sich bewusst, dass die spätere Hinzufügung von 2FA-Unterstützung zu einem generierten Client nicht unterstützt wird. Zum Beispiel wird die Hinzufügung von 2FA-Unterstützung über die Befehlszeile gegen die generierte .connect-Datei nicht unterstützt.

Sobald ein Benutzer sein Konto in einer Authentifizierungs-App konfiguriert hat, kann er sich mit seinem Passwort und dem von seiner Authentifizierungs-App oder per SMS bereitgestellten Code verbinden.



Erweiterte Verbindungsoption

Wenn der Zielserver über einen spezifischen und zugänglichen Domainnamen sowie ein gültiges SSL/TLS-Zertifikat verfügt, können Sie die Option „Den Zielserver als Remote Desktop Gateway (RDG) verwenden, um die Datenübertragung zu verschlüsseln“ aktivieren.

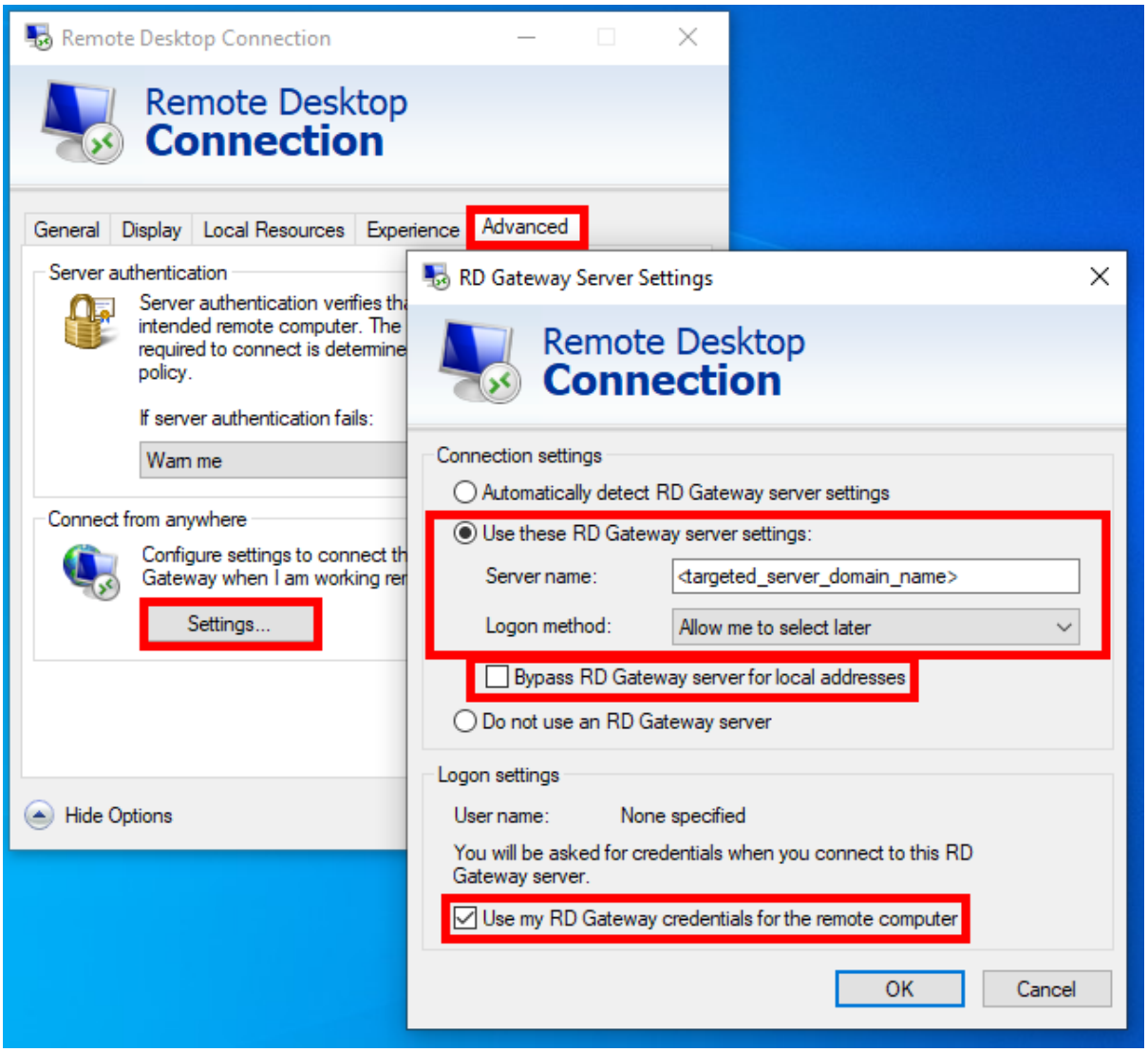
Diese Option verschlüsselt die RDP-Datenübertragung während der Verbindung mithilfe von TLS-Kapselung, wodurch sie eine geeignete Alternative zu jedem VPN in Bezug auf die Datenverschlüsselung darstellt.

Verwenden Sie stattdessen mstsc, um eine Verbindung zum RD-Gateway herzustellen.

Sie können diese Funktion auch über die mstsc-Konfiguration nutzen, ohne einen generierten Client zu verwenden, wenn die oben genannten Voraussetzungen erfüllt sind.

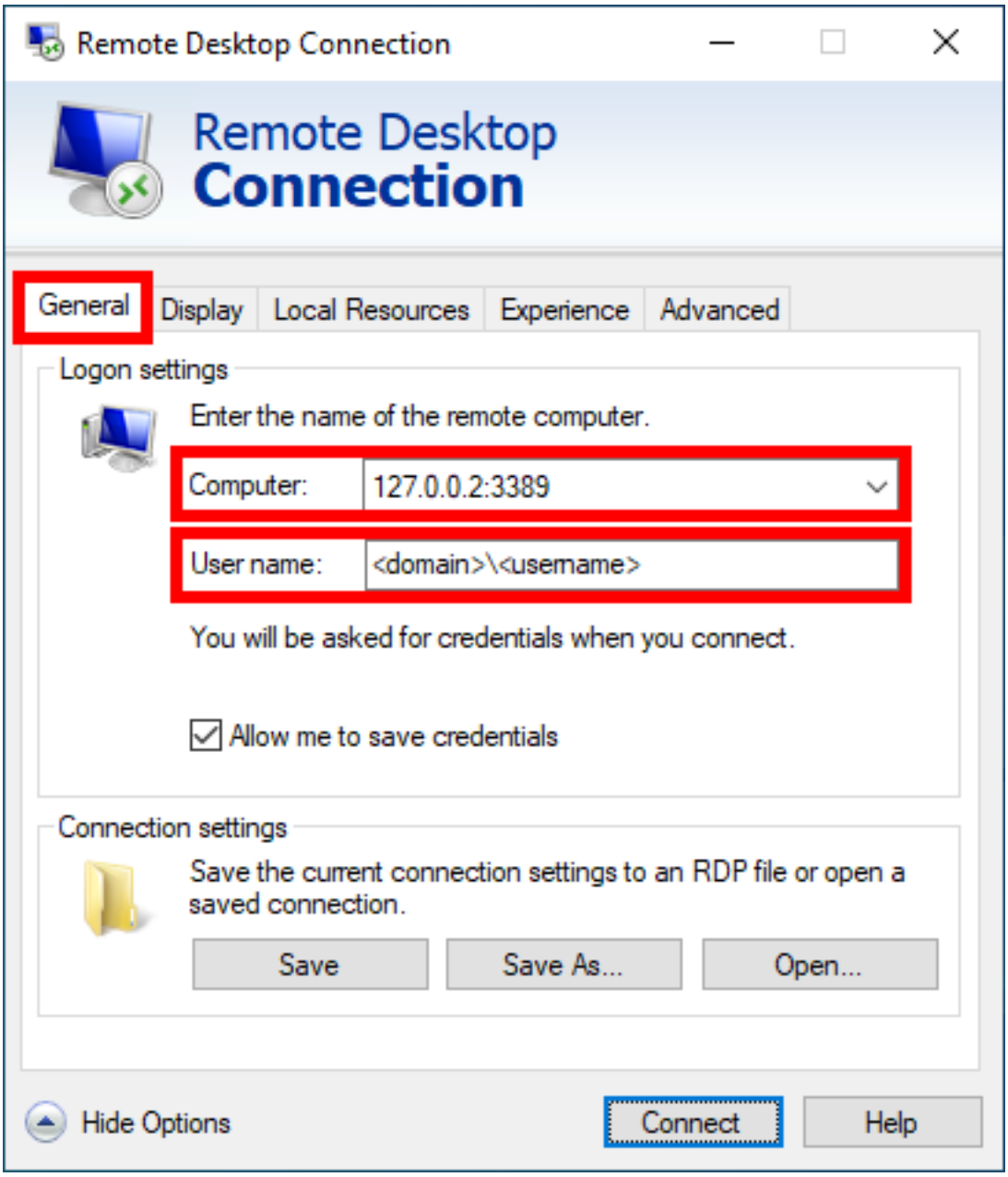
Um dies zu tun, gehen Sie zuerst zum erweiterten Tab, klicken Sie dann im Abschnitt „Von überall verbinden“ auf „Einstellungen“ und konfigurieren Sie das Remote Desktop Gateway mit:

- Das Aktivieren der Option „Diese RD-Gateway-Servereinstellungen verwenden“
- Ersetzen des Servernamens durch den Zielserver-Domainnamen (ohne https://)
- Auswahl der Anmeldemethode „Lass mich später auswählen“
- Das Deaktivieren der Option „RD-Gateway-Server für lokale Adressen umgehen“
- Das Aktivieren der Option „Meine RD Gateway-Anmeldeinformationen für den Remote-Computer verwenden“
- Klicken Sie auf „OK“, um diese Einstellungen zu speichern



Dann gehen Sie zum Tab "Allgemein" und :

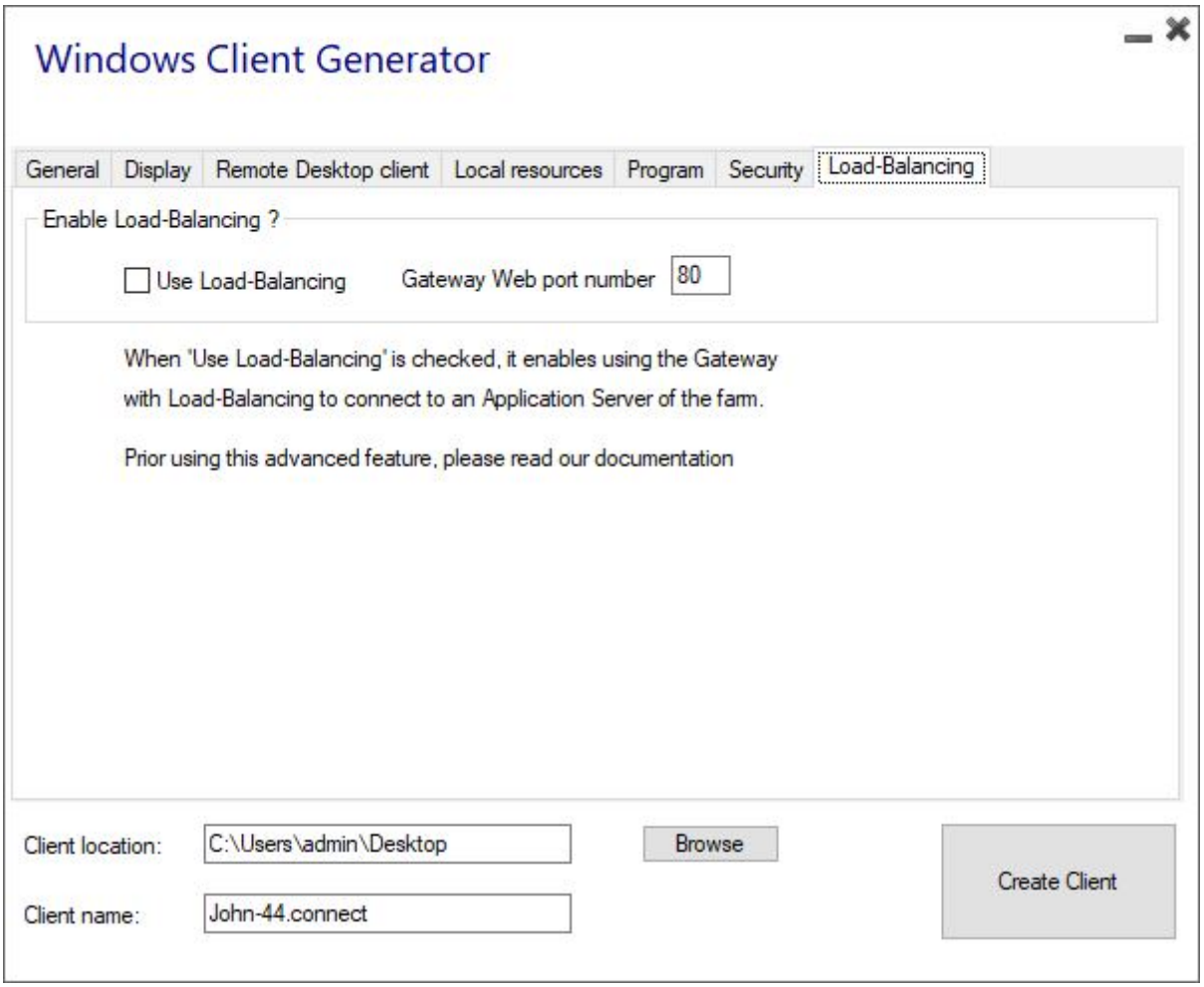
- Ersetzen Sie den Computernamen durch „127.0.0.2:3389“ und ändern Sie den Port „3389“, wenn Sie einen anderen verwenden.
- Ersetzen Sie den Benutzernamen durch den Benutzernamen, mit dem Sie sich verbinden möchten (**wichtig: die Angabe der Domain ist obligatorisch**)
- Klicken Sie auf „Verbinden“

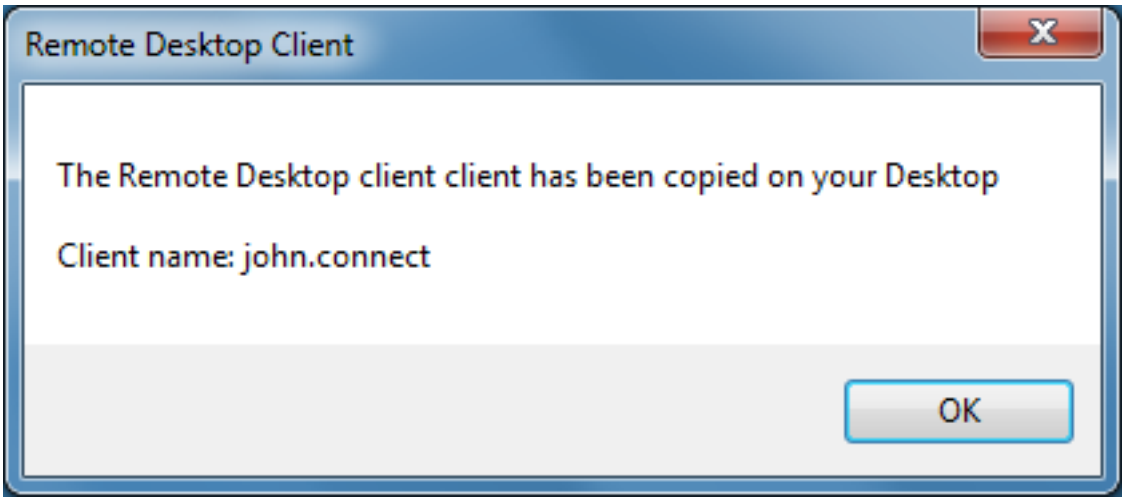


Sie können auch die Lastverteilung aktivieren, um eine Verbindung zu einem Server Ihres Clusters herzustellen.

Aktivieren Sie das Kontrollkästchen „Lastenausgleich verwenden“ nicht, wenn Sie die Lastenausgleichsfunktion auf Ihrem Server nicht aktiviert haben.

Sie müssen den Gateway-Webport eingeben, der derselbe sein sollte wie der Standard-Webport, der auf allen Servern Ihrer Farm verwendet wird.





Client-Anpassung ist möglich. Siehe die entsprechende Dokumentation zu wie man das Symbol des Clients ändert und Parameteren bearbeiten oder löschen .

Sie können die Protokolle für den Verbindungsclient auf der Client-Seite aktivieren, indem Sie den folgenden Registrierungsschlüssel hinzufügen:

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

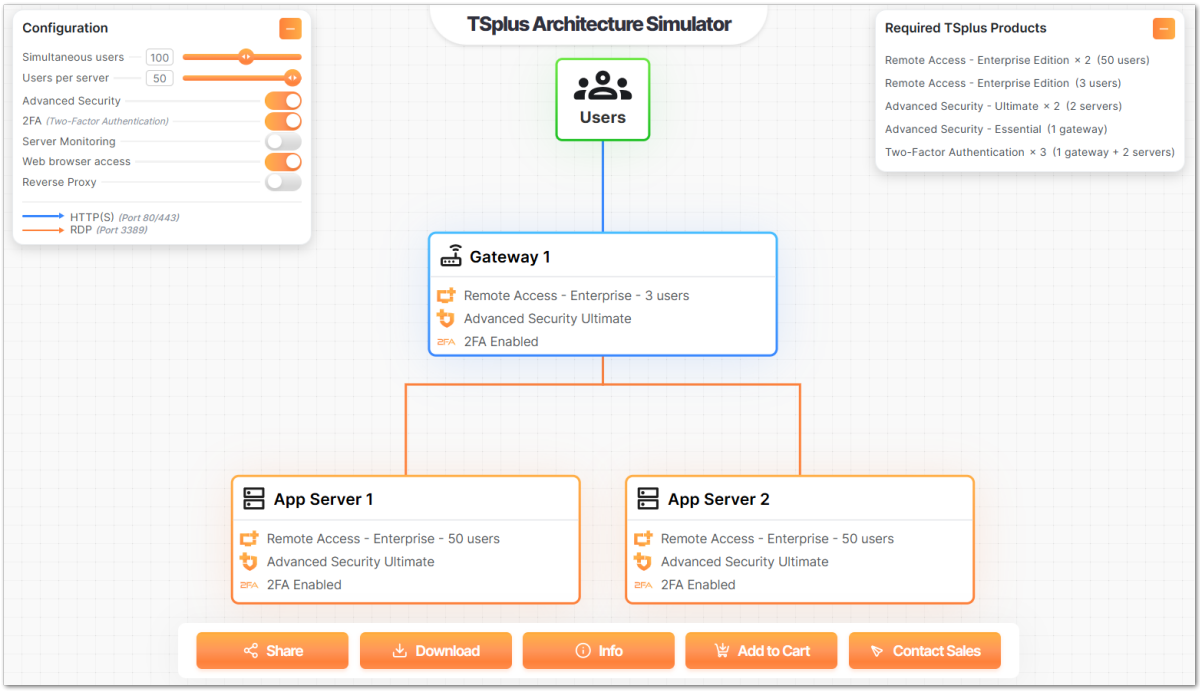
Die Protokolle befinden sich in C:\Users RDP6\logs-Verzeichnis, wenn die Installation benutzerspezifisch ist, oder im C:\Program Files (x86)\Connection Client\RDP6\logs-Verzeichnis, wenn die Installation für alle Benutzer erfolgt.

TSplus Remote Access Voraussetzungen

Architektursimulator

Konfigurieren Sie Ihre Architektur online, um Ihnen bei der Auswahl unserer Software und Add-Ons zu helfen.

TSplus Architektur-Simulator



1. Hardware

TSplus Remote Access Server Mindestanforderungen:

Anzahl der Benutzer	Windows 2008 bis 2025 oder 7 bis 11 Pro
3 - 5	I5 oder höher One CPU 2 GHZ Minimum : 4 GB RAM

	Empfohlen: 8 GB RAM
10	I5 oder höher One CPU 2 GHZ Minimum : 8 GB RAM Empfohlen: 16 GB RAM
25	Eine CPU I7 oder Xeon Minimum : 16 GB RAM Empfohlen: 32 GB RAM
50 und mehr	32 GB Dual-CPU - SSD-Disk, die dem System gewidmet ist Minimum: 32 GB RAM Empfohlen: 64 GB RAM

Wir empfehlen die Verwendung einer CPU, die weniger als zehn Jahre alt ist.

Bezüglich der RAM-Nutzung hängt es vom installierten Betriebssystem, der Anzahl der gleichzeitigen Benutzer und den Anwendungen ab, die ihnen zugewiesen sind.

Jeder Server (physisch oder virtuell) kann potenziell bis zu 50 gleichzeitige Benutzer verwalten. Für über 50 gleichzeitige Sitzungen empfehlen wir die Verwendung eines Server-Pools mit der Lastenausgleichsfunktion, die in TSplus Remote Access Enterprise Edition verfügbar ist.

Hinweis: Die genauen Spezifikationen Ihrer Hardware hängen davon ab, welche Art von Ressourcen (CPU/RAM/Disk) Ihre Anwendungen verbrauchen.

Nur **x86 und x64** Architekturen werden unterstützt.
ARM32 und ARM64 Architekturen werden nicht unterstützt.

2. Betriebssystem

Ihre Hardware muss eines der folgenden Betriebssysteme verwenden:

- Windows **7 Pro**
- Windows **8/8.1 Pro**
- Windows **10 Pro**
- Windows **11 Pro**
- Windows **Server 2008 SP2/Small Business Server SP2 oder 2008 R2 SP1**
- Windows **Server 2012 oder 2012 R2**
- Windows **Server 2016**
- Windows **Server 2019**
- Windows **Server 2022**
- Windows **Server 2025**

Sowohl 32- als auch 64-Bit-Architekturen werden unterstützt.

Der erforderliche Rahmen ist **.NET-Version 4.7.2** für alle unterstützten Windows-Versionen.

Remote Access-Version	Minimale Windows-Version
19, LTS 18, LTS 17, LTS 16, LTS 15	Windows 7 Service Pack 1 Windows Server 2008 R2 Service Pack 1
LTS 14	Windows Vista Windows Server 2008

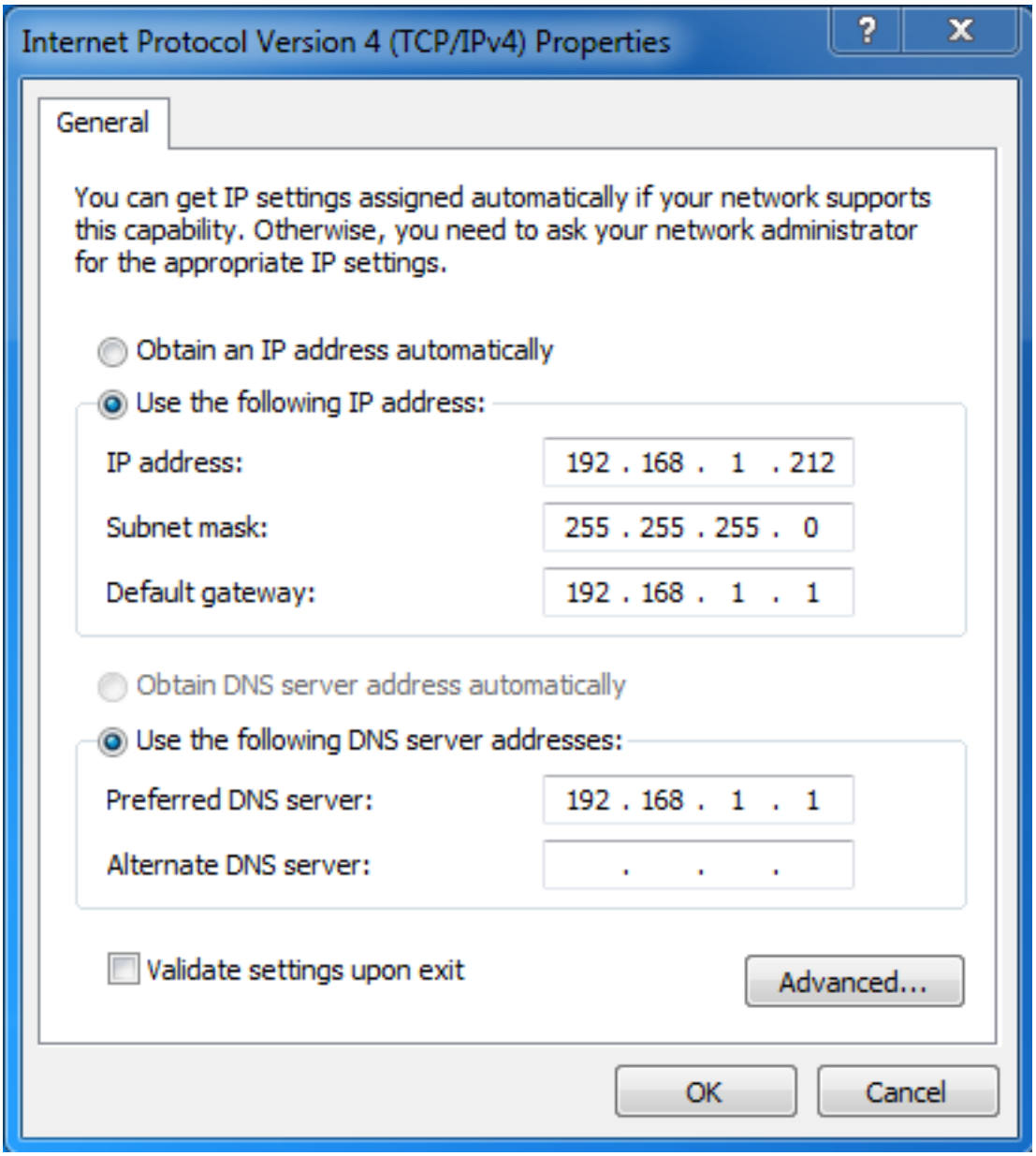
- Wenn Sie Remote Access auf einem Windows Server-Betriebssystem installieren, stellen Sie sicher, dass die RDS/Terminaldienste und die RDS/Terminaldienste-Lizenzierungsrollen nicht installiert sind, bevor Sie TSplus Remote Access installieren.

Wenn diese Rollen derzeit installiert sind, entfernen Sie sie und starten Sie neu.

- Windows Home Editionen werden nicht unterstützt.
- Auf Windows Server 2016 sind maximal 15 Sitzungen für den Remote Desktop-Zugriff erlaubt.
- Windows Server 2016, 2019, 2022 Essentials Edition wird nicht unterstützt und ist nicht für die Verwendung mit TSplus Remote Access empfohlen.
- TSplus Remote Access integrierter Webserver benötigt **Java OpenJDK 17 oder höher.** .

3. Netzwerkkonfiguration

Der Remote Access Server muss eine statische private IP-Adresse haben:



Remote-Zugriff (von Wide Area Network - WAN)

- Eine Breitband-Internetverbindung wird empfohlen, ebenso wie eine statische öffentliche IP-Adresse. Wenn Sie keine statische IP-Adresse haben, ziehen Sie in Betracht, einen dynamischen DNS-Dienst wie
- Der TCP RDP-Port (standardmäßig 3389) muss in beide Richtungen in Ihrer Firewall geöffnet werden.

3. Sicherheit

Seit Anfang 2024,
TSplus hat seinen automatischen Mechanismus zur Generierung von SSL/TLS-Zertifikaten aktualisiert, um sich an die Änderung der Vertrauenskette von Let’s Encrypt anzupassen: den **DST Root CA X3** root wurde ersetzt durch **ISRG Root X1** .

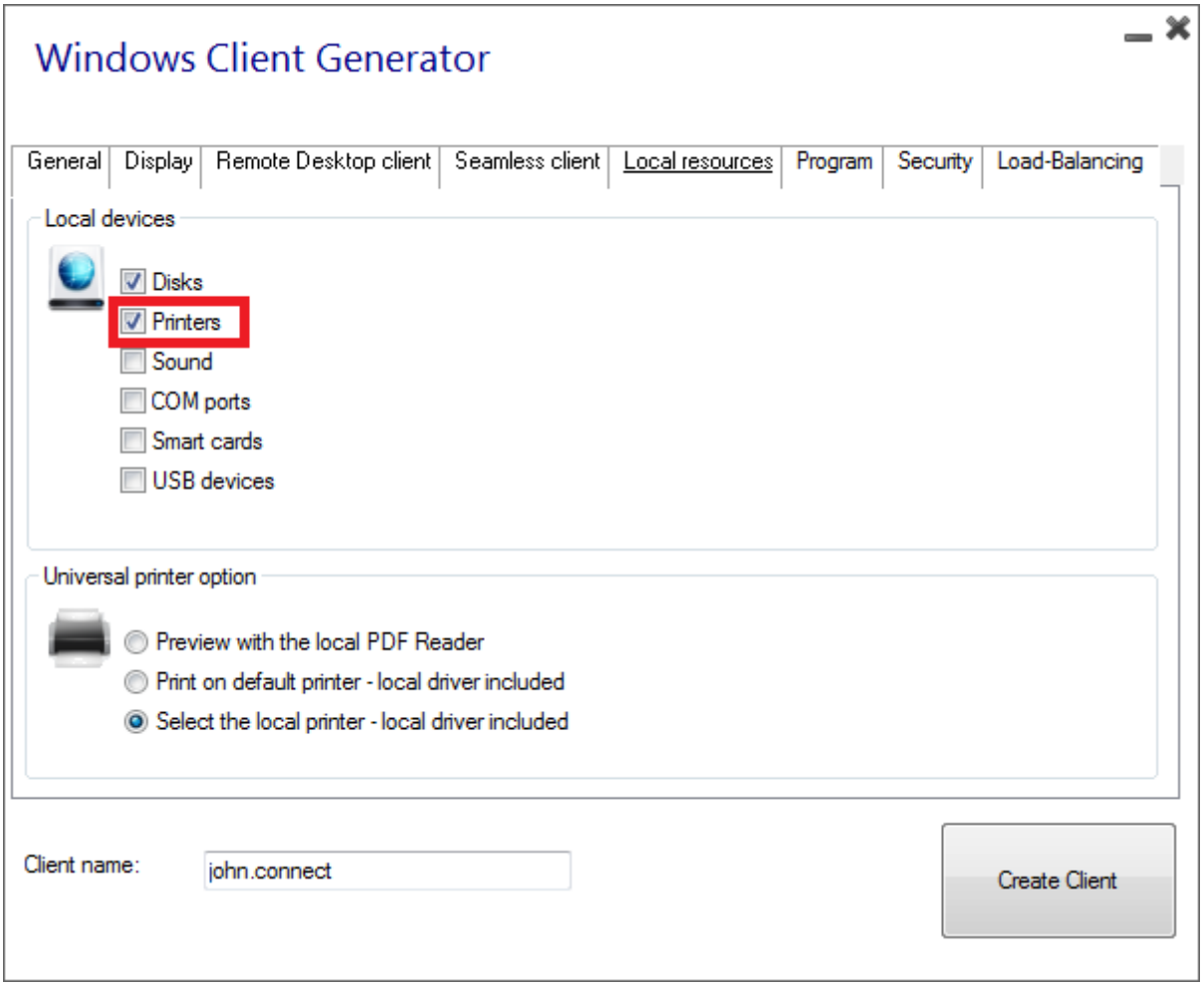
Wenn ein Client oder Arbeitsplatz das neue Zertifikat nicht erkennt, kann es notwendig sein, hinzuzufügen **ISRG Root X1** zum Windows-Vertrauenszertifikatspeicher.

TSplus arbeitet mit Wildcard-Zertifikaten und unterstützt das TLS-Protokoll für sichere Remote-Verbindungen.

Drucken mit der Standard-RDP-Druckerzuordnungsfunktion

Dies wird häufig von Remote Desktop-Benutzern verwendet und entspricht dem, was Sie mit Microsoft Terminal Services hätten.

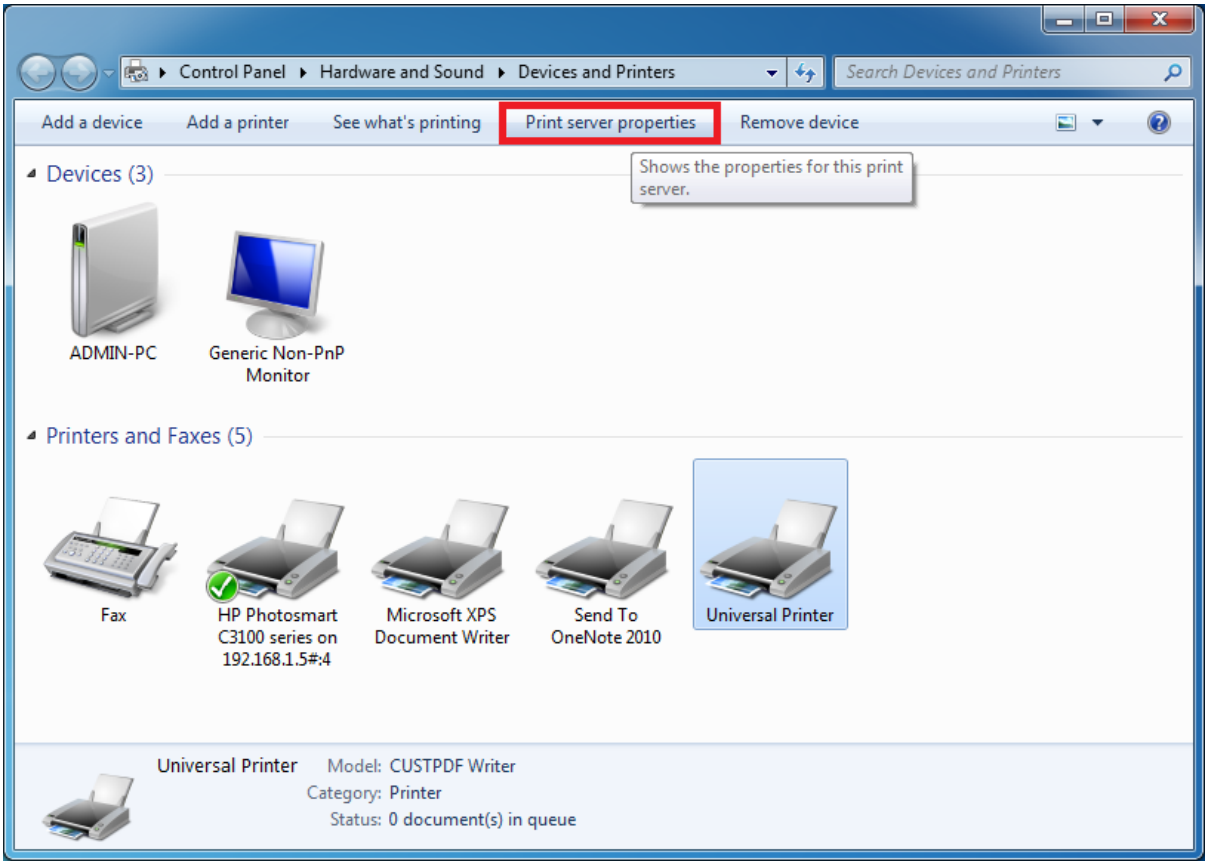
Wenn Sie planen, exotische Drucker zu verwenden, stellen Sie sicher, dass Sie das Kästchen für Drucker im Tab "Lokale Ressourcen" des Client-Generators aktivieren.



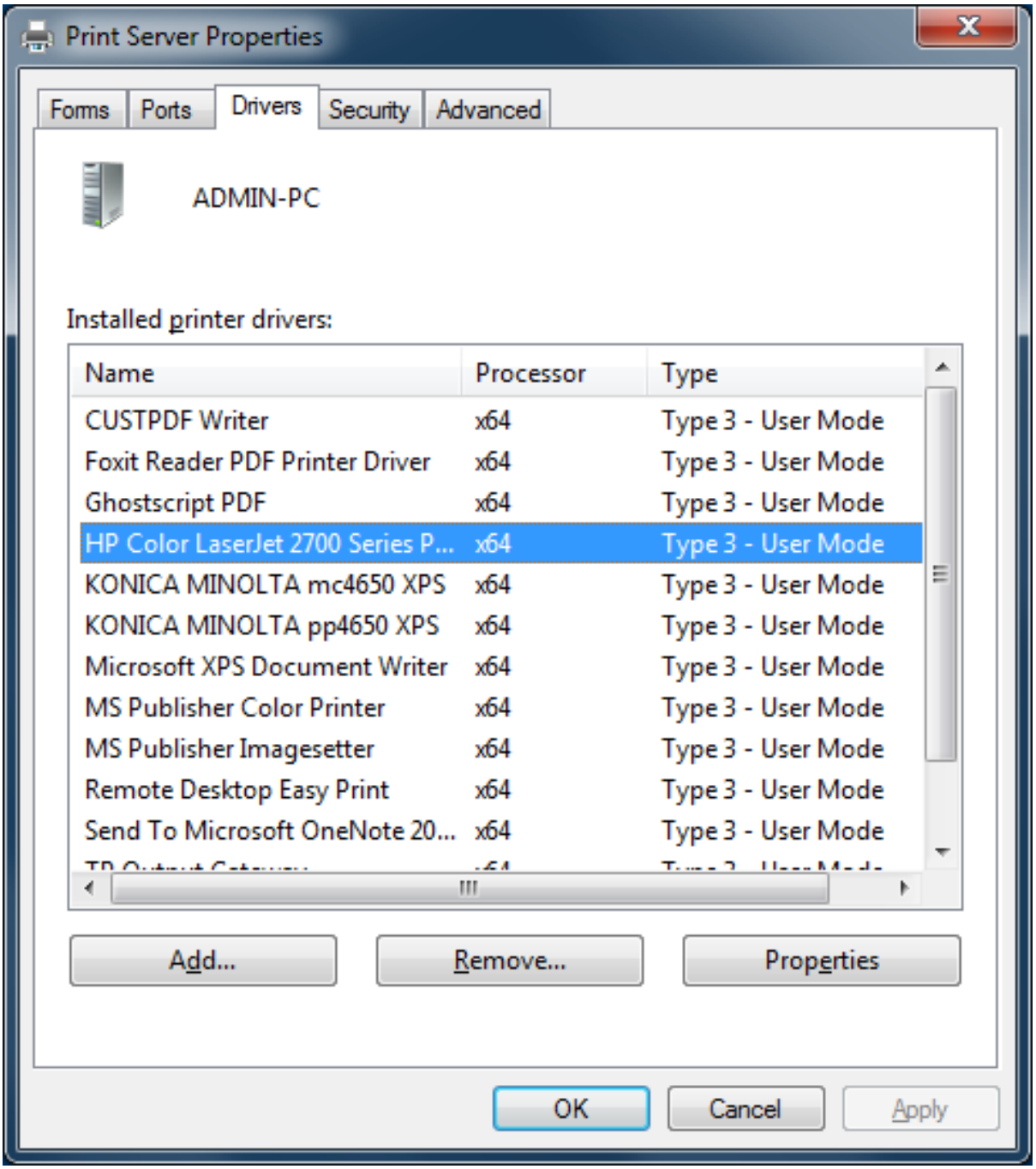
Die meiste Zeit müssen Sie die gleiche Version der Druckertreiber sowohl auf dem Client als auch auf dem Server installieren, damit sie ordnungsgemäß funktionieren.

Das bedeutet, dass wenn Ihr Server Windows 2008 64 Bit ist und Ihre Client-Computer Windows XP 32 Bit ausführen, Sie die 32-Bit-XP-Druckertreiber auf dem Server installieren müssen.

Klicken Sie auf das Startmenü und dann auf Geräte und Drucker. Klicken Sie auf einen beliebigen Drucker, um die Schaltfläche Druckservereigenschaften oben im Fenster anzuzeigen.



Sobald Sie sich in den Eigenschaften des Druckservers befinden, klicken Sie auf die Registerkarte Treiber, um Ihren Clienttreiber manuell hinzuzufügen. (In diesem Fall installieren wir den Windows XP 32-Bit-Treiber.)



Sie können auch direkt Ihre Druckertreiber mit Informationen und Treibern von der Website des Druckerherstellers installieren.

- Es wird empfohlen, Ihr Hardware-Handbuch auf ein Installationsverfahren in einer Terminalserver-Umgebung zu überprüfen.
- Wenn Sie USB-Drucker verwenden, stellen Sie sicher, dass Sie das RDP-Protokoll Ihres Client-Computers auf RDP-Version 6 oder höher aktualisiert haben, um maximale Kompatibilität mit umgeleiteten Druckern zu gewährleisten.

Für die besten Ergebnisse wird empfohlen, keine USB-Drucker zu verwenden. Die Kompatibilität und Zuverlässigkeit werden verbessert, wenn COM- oder LPT-Drucker verwendet werden.

Einige exotische Drucker, wie z. B. Etiketten- oder Quittungsdrucker, sind möglicherweise nicht

geeignet, um in einer TSplus-Sitzung umgeleitet zu werden. Sie sollten immer mit Ihrem Hardwarehersteller die Kompatibilität und Installationsverfahren in einer RDS- oder Terminalserver-Umgebung überprüfen, die in diesem Fall sehr nah an TSplus ist.

TSplus Remote Access v19: Schnellstartanleitung

Voraussetzungen :

Auf dem Server :

- **Betriebssystem:** Microsoft Windows Versionen 7 bis 11 oder Windows Server 2008R2 bis 2025 mit mindestens 2 GB RAM.
- TSplus unterstützt die Installation von Remote Access auf Windows Home Editionen nicht.
- Das Betriebssystem **muss** auf dem C: Laufwerk.
- Java Runtime Environment. Wenn Java noch nicht installiert ist, wird Remote Access OpenJDK während der Einrichtung installieren.
- Wenn Sie Remote Access auf einem Windows Server-Betriebssystem installieren, stellen Sie sicher, dass die RDS/Terminaldienste und die RDS/Terminaldienste-Lizenzierungsrollen aktiviert sind. **nicht installiert** vor der Installation von TSplus Remote Access.
- Ihr Remote Access-Server muss eine statische private IP-Adresse haben.
- Für den externen Zugriff muss Ihr Server über eine statische öffentliche IP-Adresse oder einen dynamischen DNS-Anbieter verfügen.
- TSplus Remote Access integrierter Webserver benötigt **Java OpenJDK 17 oder höher.** .

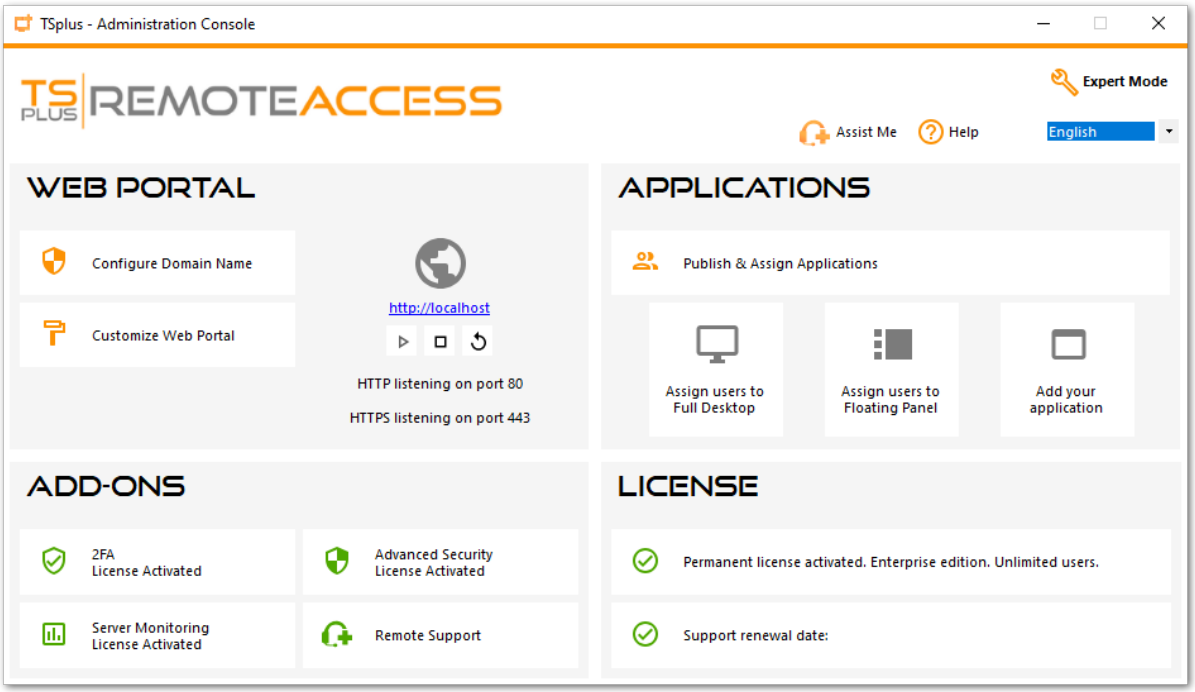
Am Client :

- **Betriebssystem:** Microsoft Windows Versionen 7 bis 11 werden vollständig unterstützt.
- Für MacOS können Sie jeden Mac RDP-Client oder den TSplus HTML5-Client verwenden.
- Für Linux können Sie Rdesktop oder den TSplus HTML5-Client verwenden.
- Java Runtime Environment.
- Ein PDF-Reader (Beispiel: Foxit Reader oder Acrobat DC)

Für detailliertere Voraussetzungen siehe die Dokumentation

Hinweis:

Starting with Remote Access Version 15, die Administrationskonsole hat ihr Aussehen geändert. A **Lite-Modus** und ein **Expertenmodus** wurden eingeführt. Administratoren können zwischen den beiden Benutzeroberflächenstilen umschalten, indem sie auf die Schaltfläche in der oberen rechten Ecke der Admin-Konsole klicken.



Schritt 1: Installation.

Hinweis:

Die Testversion von Remote Access ist die voll ausgestattete Enterprise Edition. Sie ist lizenziert für bis zu 5 gleichzeitige Benutzer für einen Zeitraum von 15 Tagen.

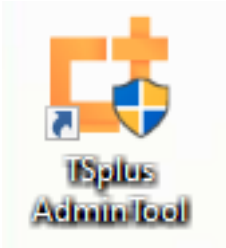
Die Installation von TSplus Remote Access ist ein einfacher Prozess. Laden Sie es einfach von unserer Website herunter und führen Sie das Programm Setup-TSplus.exe aus.

Dateien werden entpackt und kopiert in:

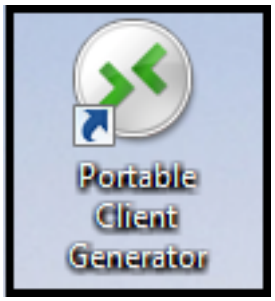
- C:\Program Files\TSplus (32-Bit-Systeme)
- C:\Program Files(x86)\TSplus (64-Bit-Systeme).

Sobald die Installation abgeschlossen ist, wird der Installer Sie auffordern, neu zu starten.

Nach dem Neustart sehen Sie 2 neue Symbole auf Ihrem Desktop:



Das AdminTool ist das, was Sie für den Remote Access benötigen.

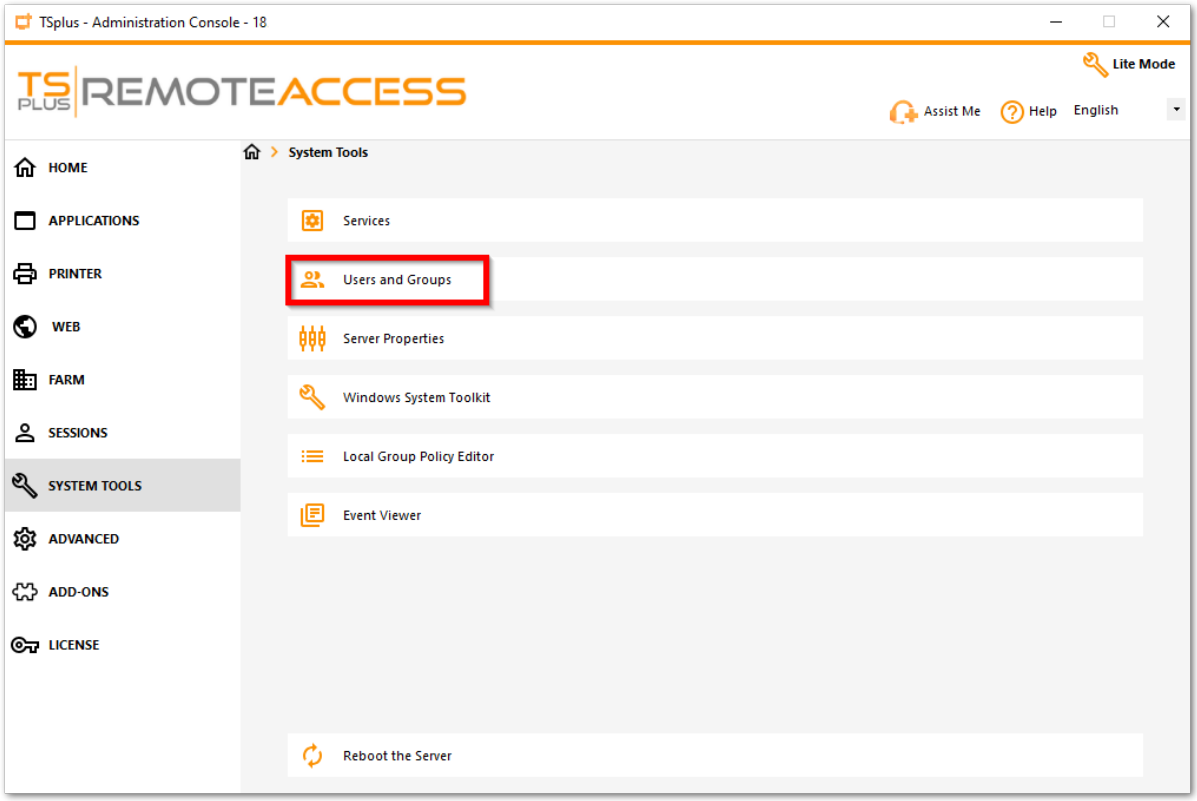


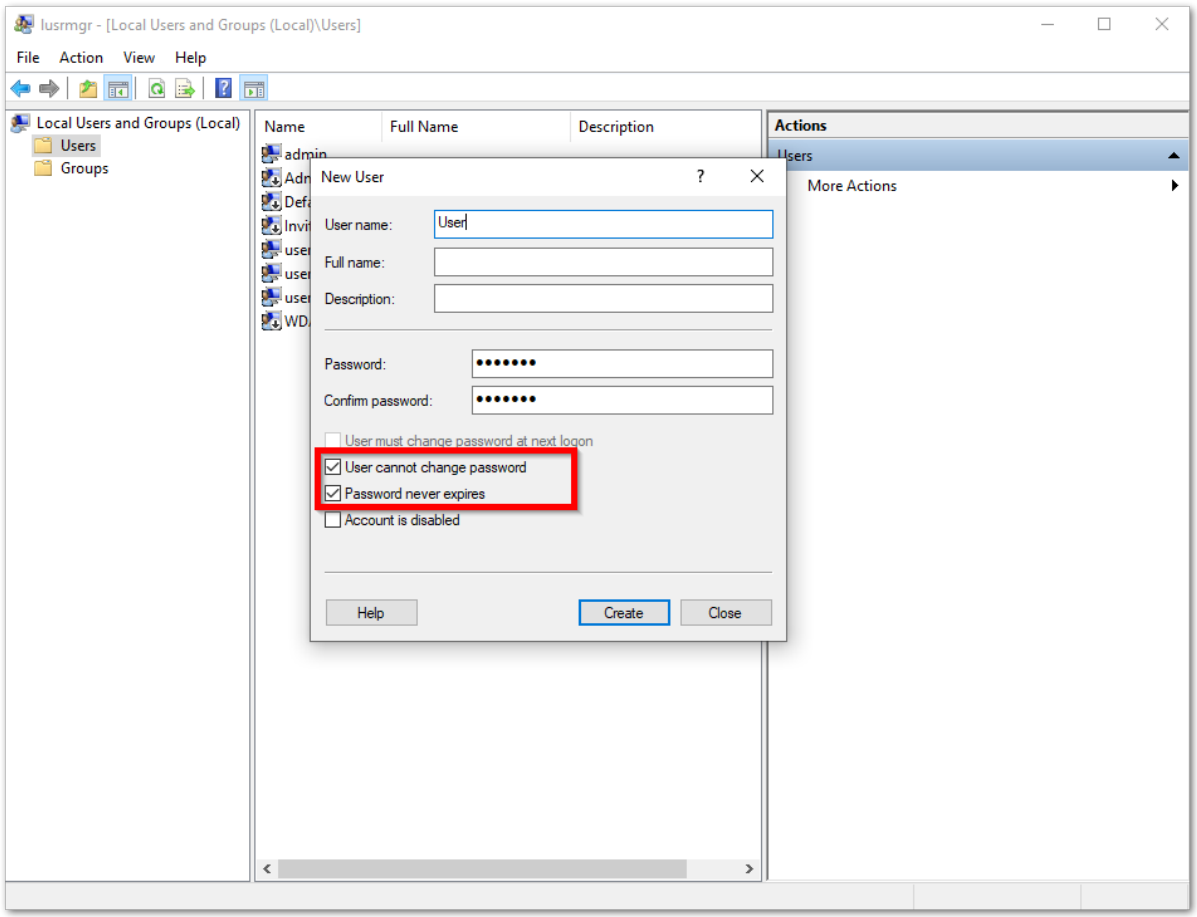
Der Portable Client Generator wird verwendet, um Remote Access-Verbindungsclients für Ihre Benutzer zu erstellen.

Siehe die Dokumentation für vollständige Installationsanweisungen.

Schritt 2: Benutzer erstellen.

Nach dem Neustart ist der Remote Access Server fast bereit. Jetzt erstellen wir Benutzer. Öffnen Sie das AdminTool, um zu beginnen. Gehen Sie dann zum Tab Systemtools und klicken Sie auf „Benutzer und Gruppen“. Dies bringt Sie zum Fenster Lokale Benutzer und Gruppen.





Jeder Benutzer muss einen Benutzernamen UND ein Passwort haben. Beim Erstellen von Benutzern sollten Sie auf das Feld mit der Bezeichnung „Benutzer muss das Passwort beim

nächsten Anmelden ändern“ achten. Wenn Sie nicht möchten, dass Ihre Benutzer ihr Passwort beim ersten Anmelden ändern, deaktivieren Sie dieses Feld und aktivieren Sie „Passwort läuft niemals ab“ oder „Benutzer kann Passwort nicht ändern“.

Schritt 3: Wählen Sie den am besten geeigneten Client für Ihre Bedürfnisse aus.

Remote Access ist mit dem Windows Remote Desktop Protocol kompatibel. Jeder Benutzer kann sich lokal oder remote mit einem standardmäßigen Remote Desktop Connection-Client (mstsc.exe) oder einem beliebigen RDP-kompatiblen Client verbinden. Um vollständig von den erweiterten Funktionen in Remote Access (RemoteApp, Universal Printer…) zu profitieren, können Sie einen generierten Client oder das Remote Access Web Portal verwenden.

Remote Access ist eine sehr flexible Lösung und bietet mehrere Möglichkeiten, eine Sitzung zu öffnen:

- **Klassische Remotedesktopverbindung** MSTSC.EXE.
- **Portabler TSplus RDP-Client** das ein fensterbasiertes Umfeld für Ihre Remote-Verbindung anzeigt, das Sie in der Windows-Taskleiste minimieren können.
- **MS RemoteAPP-Client** die Anwendung, die die native MS RemoteApp verwendet, anzeigen.
- **Windows-Client** über das TSplus Webportal.
- **HTML5-Client** über das TSplus Webportal.

Diese Kunden bieten dem Benutzer folgende Erfahrung:

Mit der Remotedesktopverbindung (mstsc.exe)

- **Verbindung** Die Verbindung ist eine sehr standardmäßige. Der Universal Printer wird mit dieser Art von Verbindung nicht unterstützt.

- **Anzeige** Benutzer sehen ihre Sitzung in einem Remote Desktop-Fenster. Dieser Desktop zeigt den Inhalt des Desktop-Ordners des Benutzers an.

  Wenn der Administrator bestimmte Anwendungen mit dem AdminTool zugewiesen hat, werden nur diese Anwendungen angezeigt (keine Taskleiste, kein Desktop).

TSplus RDP generierter Client .

Dies ist eine einzigartige TSplus-Lösung, die es lokalen und entfernten Benutzern ermöglicht, sich mit einem einzigen dedizierten Programm zu verbinden.

Es umfasst das Verbindungsprogramm, die erweiterte Funktion Universelles Drucken, Portabilität mit hohem Sicherheitsniveau und bleibt dabei sehr einfach für die Benutzer.

Für weitere Informationen zur Verwendung des TSplus Client Generators siehe diese Dokumentation

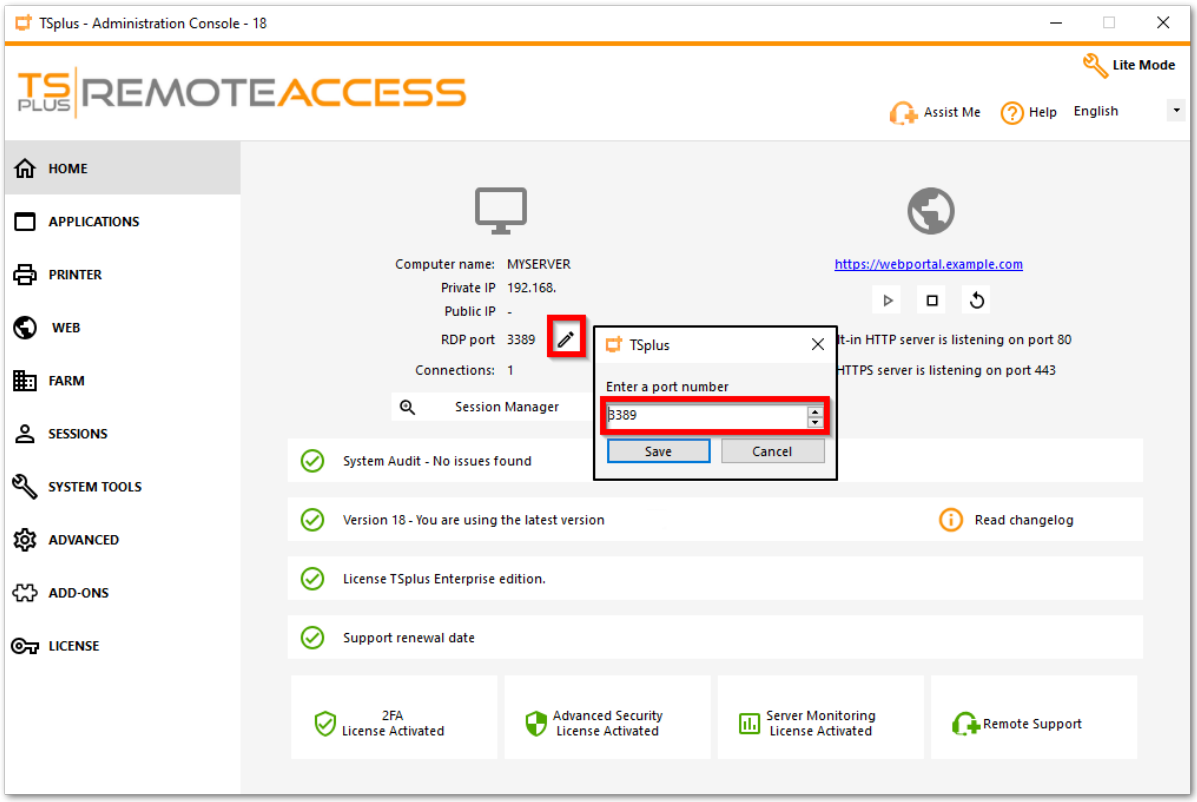
Der TSplus RemoteApp generierte Client .

Remote-Anwendungen sehen aus und verhalten sich wie eine lokale Anwendung. Anstelle eines klassischen Remote Desktop-Fensters können Sie zwischen Ihren lokalen und Remote-Anwendungen wechseln, ohne ein Remote Desktop-Fenster minimieren zu müssen.

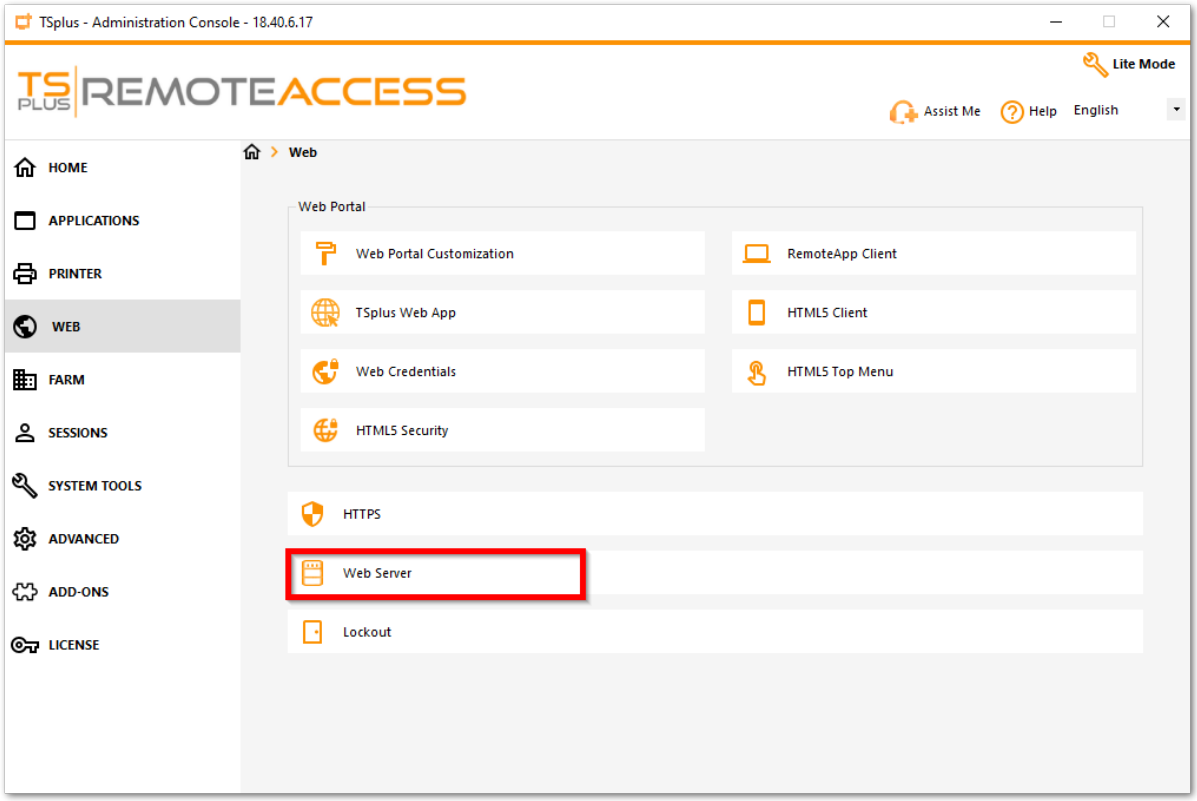
Für weitere Informationen zu diesen Clients, siehe diese Dokumentation .

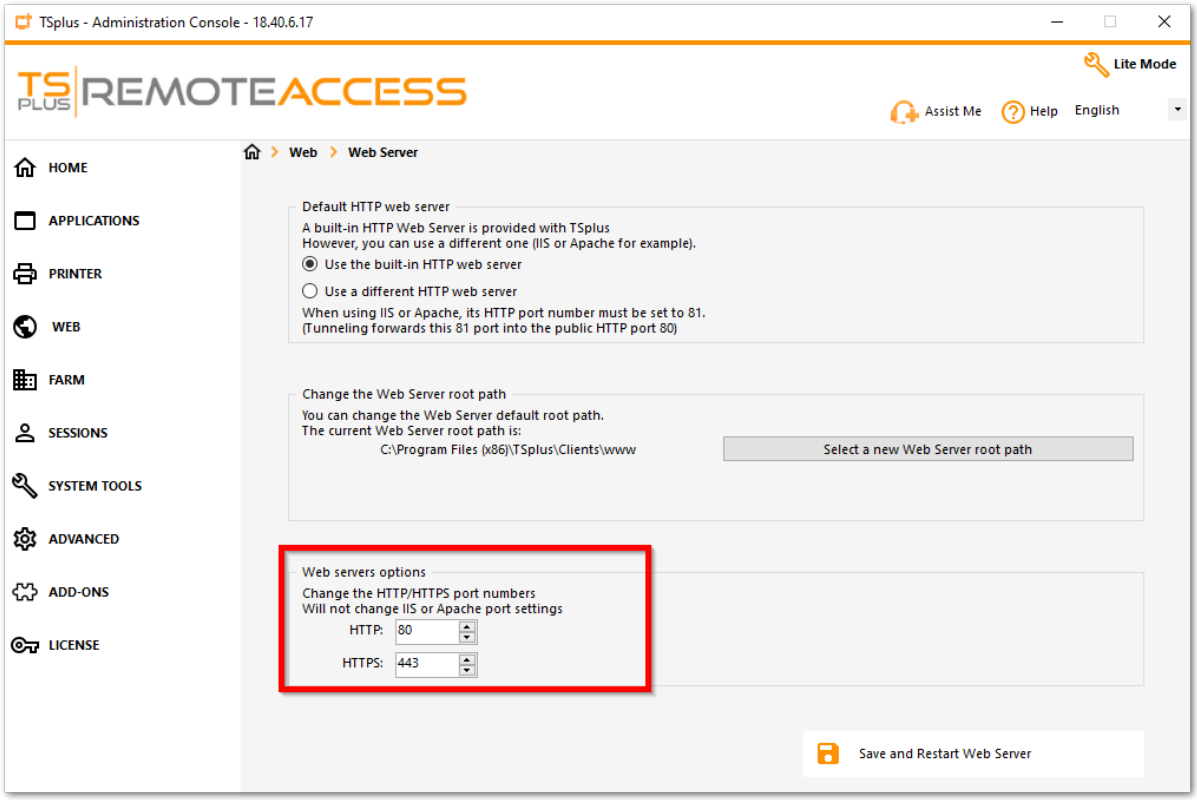
Zugriff auf Ihren TSplus Remote Access-Server von einem entfernten Standort

Um von außerhalb Ihres lokalen Netzwerks auf Ihren Remote Access-Server zuzugreifen, müssen Sie eine Portweiterleitungs- oder Portumleitungsregel für die Ports 3389/80/443 erstellen, je nach Ihrer bevorzugten Verbindungsart. Sie können den RDP-Port im Tab "Start" ändern.



Die Ports 80/443 können im Tab Webserver geändert werden:



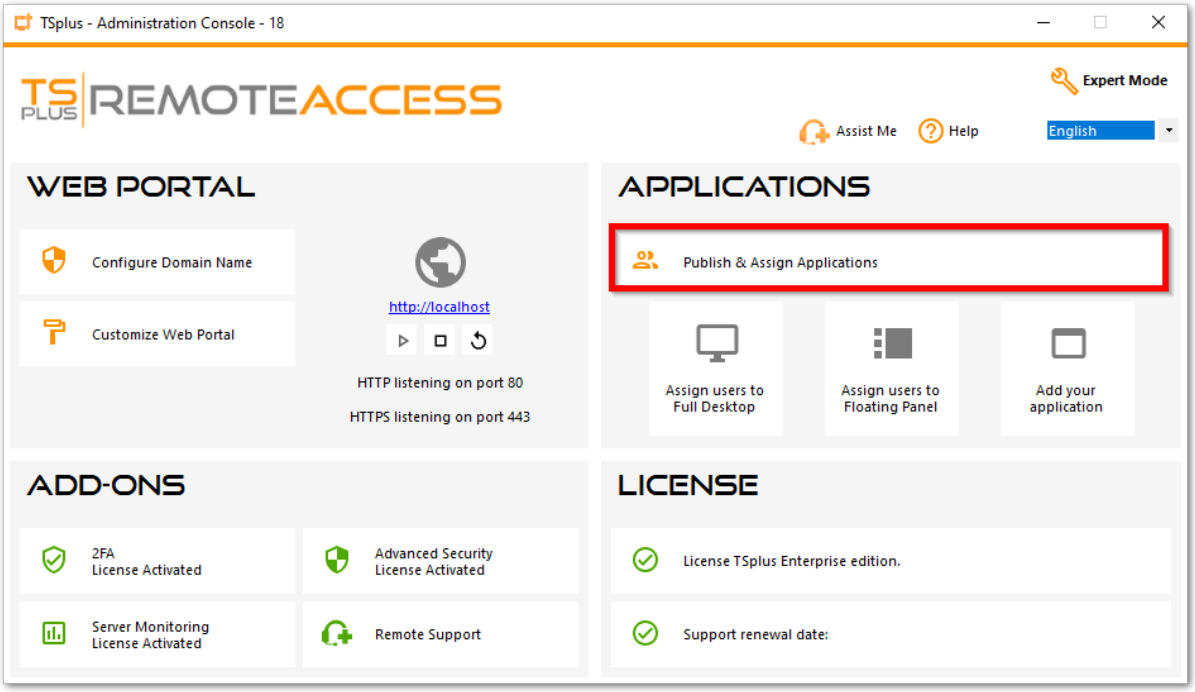


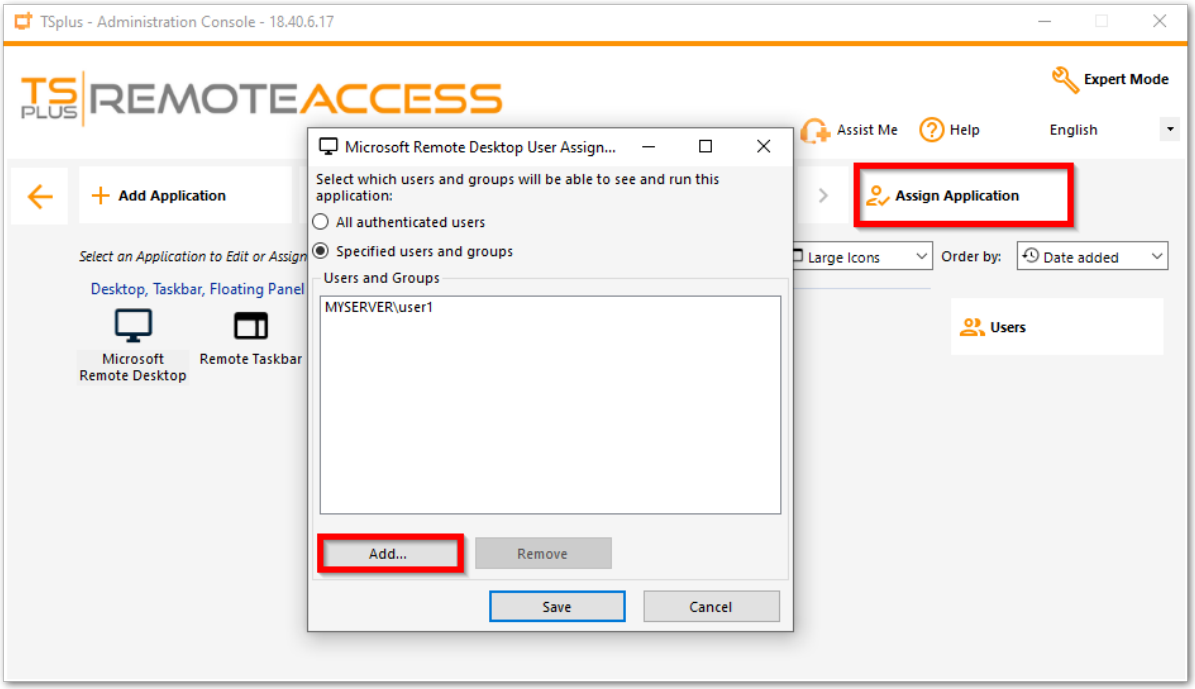
Schritt 4: Anwendungsbereitstellung und Anwendungssteuerung.

Im Remote Access AdminTool können Sie Anwendungen Benutzern oder Gruppen zuweisen.

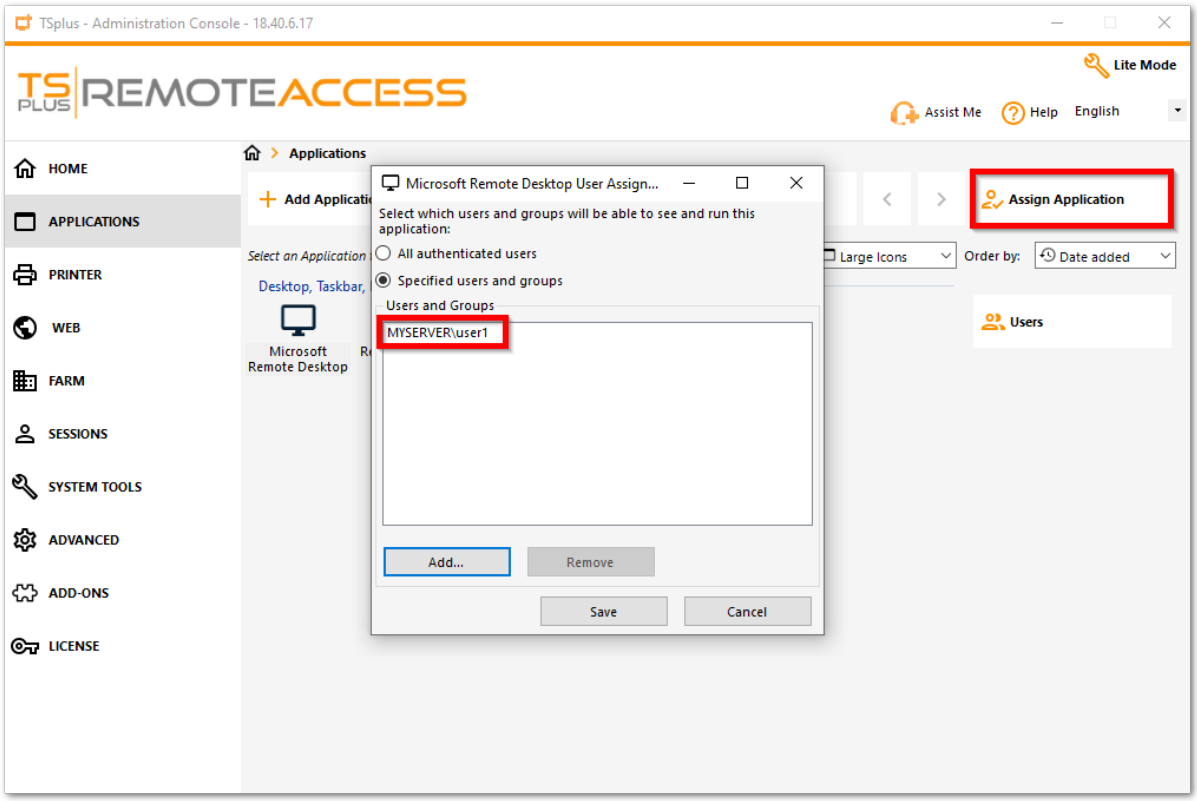
- Wenn Sie eine Anwendung einem Benutzer zuweisen, sieht dieser nur diese Anwendung.
- Sie können ihnen auch die TSplus-Taskleiste, das schwebende Panel oder das Anwendungs-Panel zuweisen, um mehrere Anwendungen anzuzeigen.
- Sie können auch einen vollständigen Remote Desktop veröffentlichen.

Jetzt verfügbar in
Lite-Modus
von der Startseite.





Oder gehen Sie zu **Expertenmodus** Apps-Register, um Apps hinzuzufügen, zu bearbeiten, zu löschen und zuzuweisen.



In diesem Beispiel hat der Administrator entschieden, dass der Benutzer 'John' die TSplus Taskleiste erhält. Siehe diese Dokumentation für weitere Informationen.

Vielen Dank, dass Sie TSplus Remote Access verwenden!

Rehosting Ihrer TSplus-Lizenz

Online-Rehosting

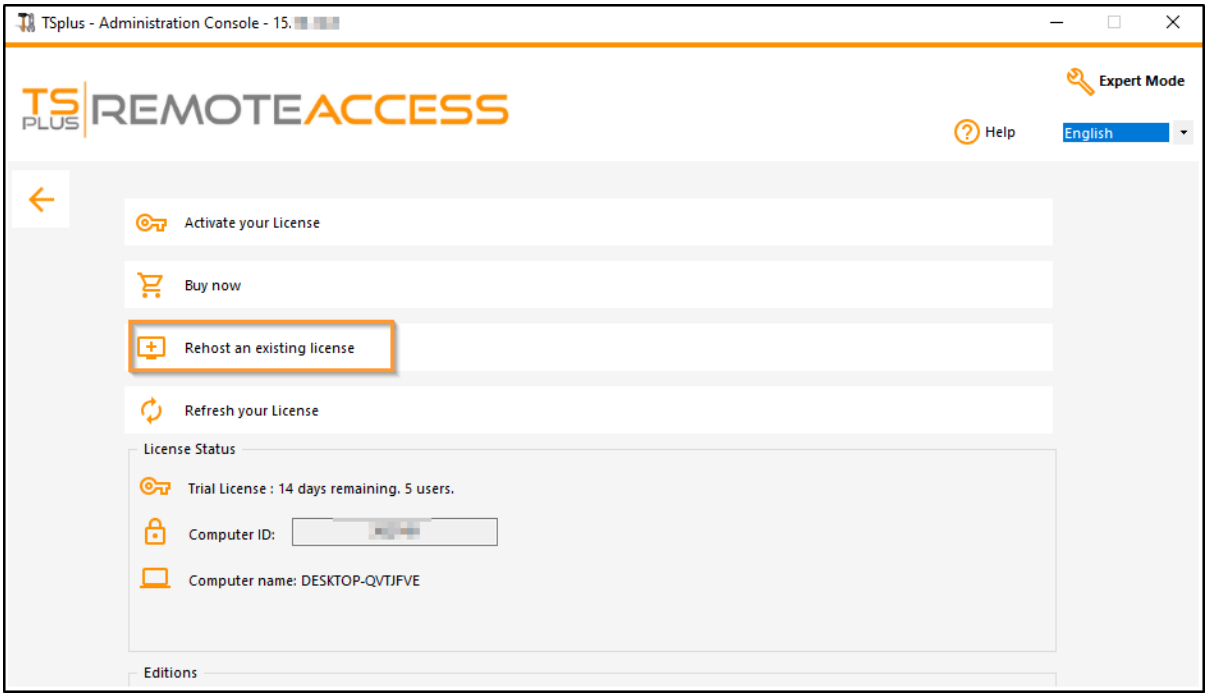
Online-Aktivierung ist einmal im Monat autorisiert.

Voraussetzungen: Es ist erforderlich, ein aktives Support-Abonnement zu haben, um Ihre Lizenz neu zu hosten.

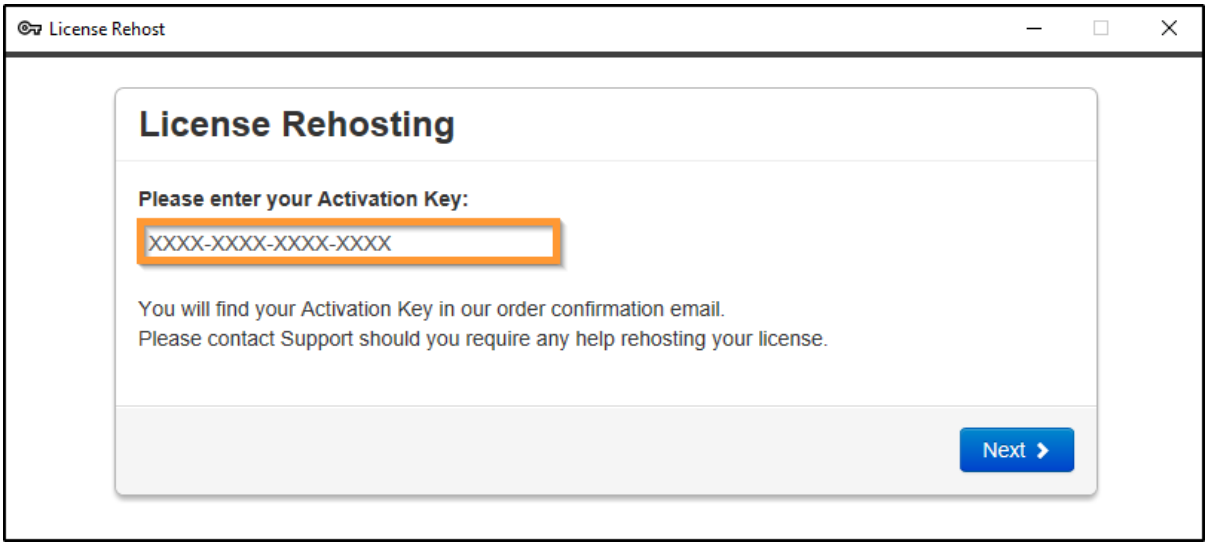
Es ist notwendig, eine neue Version des nicht-klonierten Remote Access zu installieren, um eine neue Computer-ID zu generieren.

Wenn Sie Ihren Server dupliziert und den Remote Access geklont haben, gehen Sie bitte zu der folgenden Seite: Klonen Sie Ihren Server

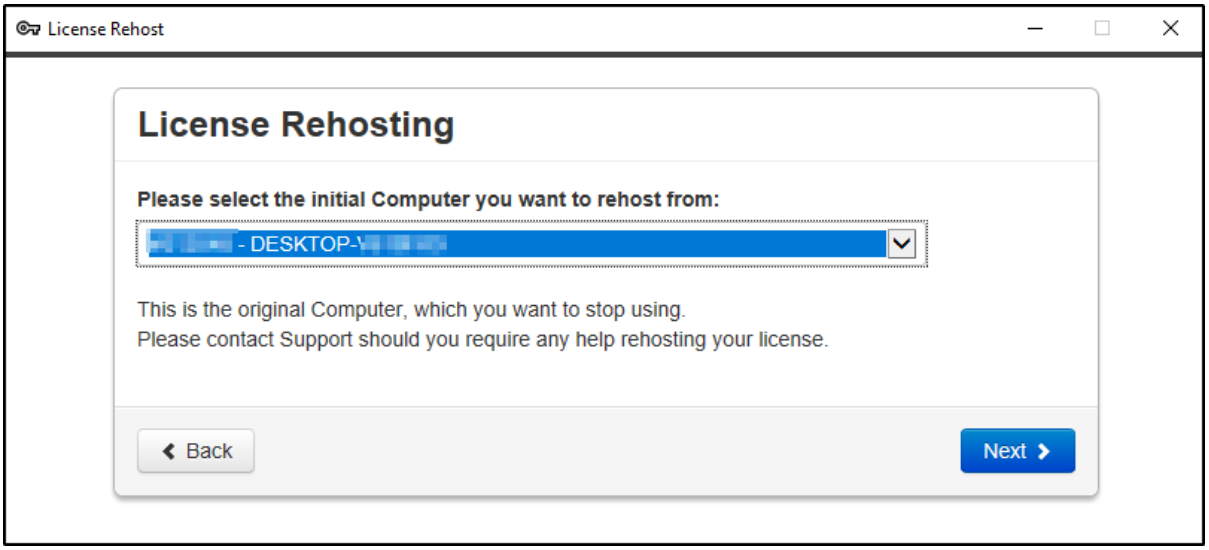
Auf dem neuen Server Gehe zum Tab „Lizenz“ Klicke auf „Eine vorhandene Lizenz neu hosten“



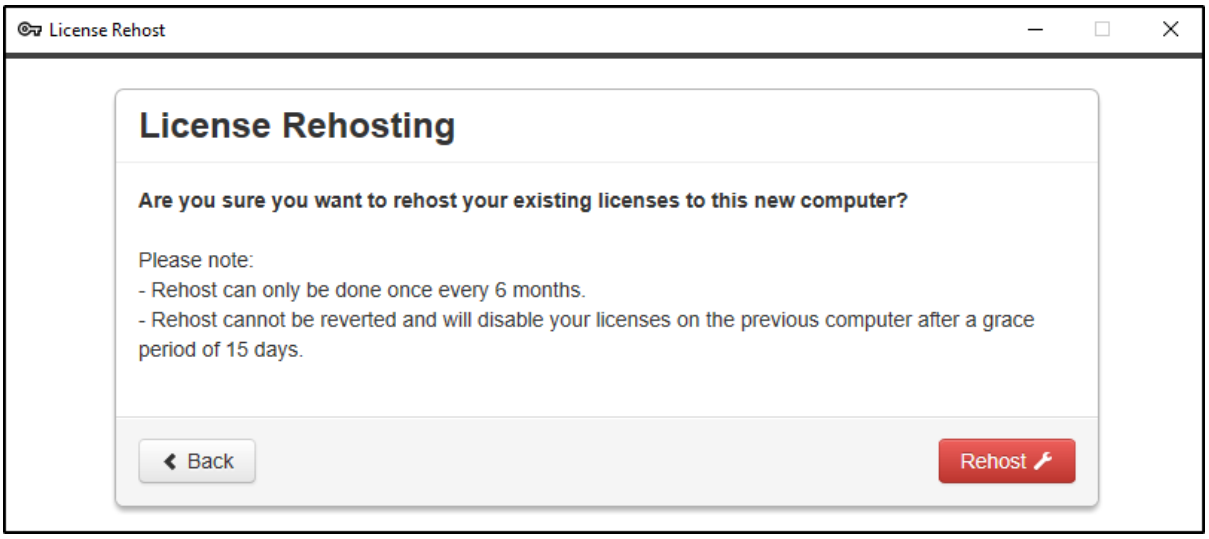
Geben Sie Ihren Aktivierungsschlüssel ein:



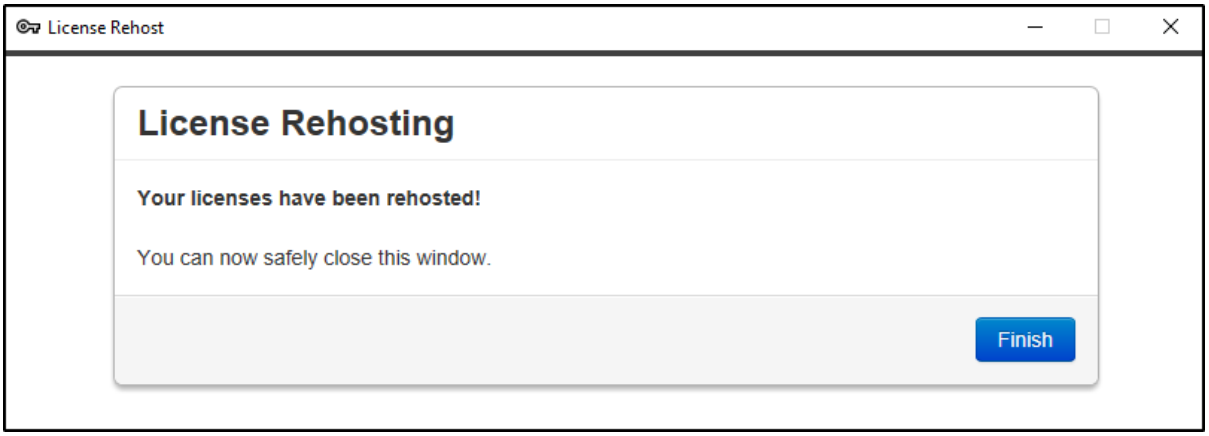
Wählen Sie den ursprünglichen Computer aus, den Sie rehosten möchten.



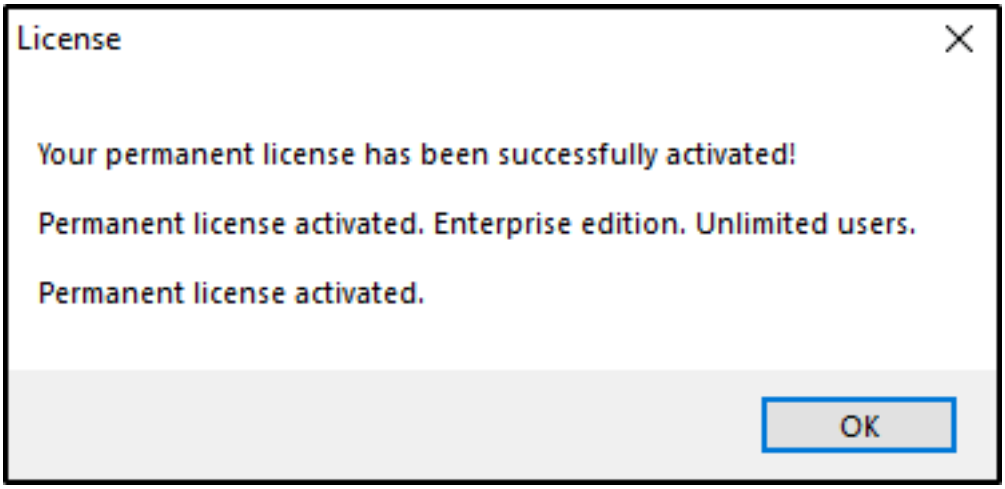
Bestätigen Sie das Rehosting



Ihre Lizenz-Rehosting ist abgeschlossen.

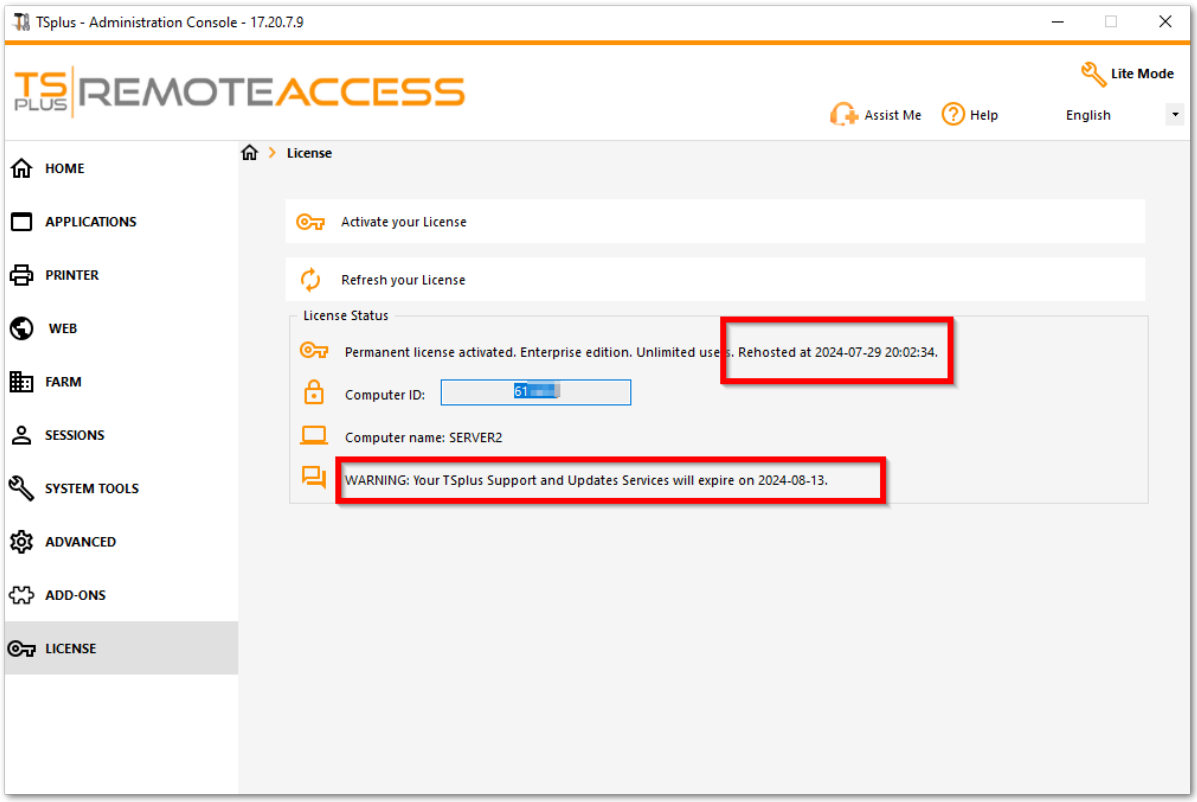


Warten Sie einen Moment, bis Ihr AdminTool synchronisiert ist, bis das Fenster erscheint.



Herzlichen Glückwunsch, Ihre Lizenz wurde erfolgreich aktiviert!

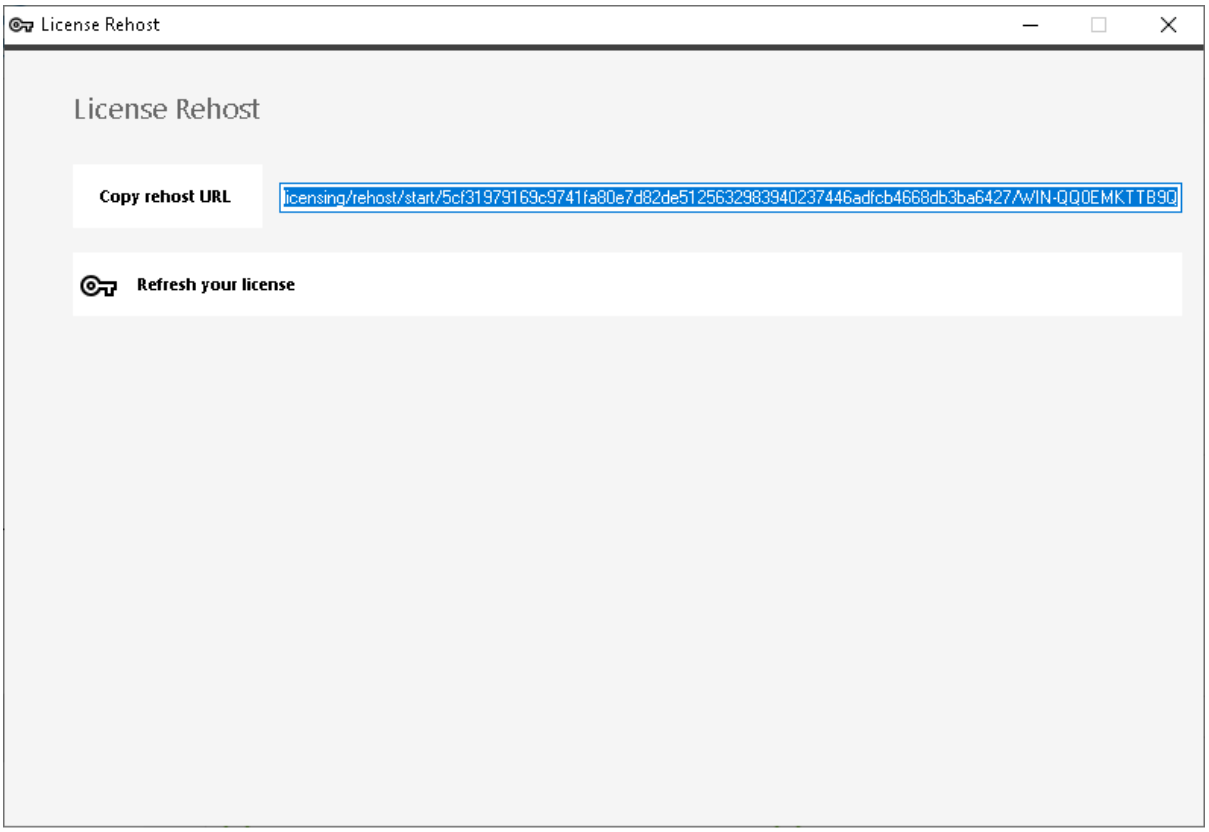
Hinweis: Auf dem alten Server wird eine Nachricht mit dem Rehosting-Datum sowie dem Enddatum der Nutzung angezeigt.
Nach einem Rehosting wird der alte Server weiterhin für funktionieren **15 Tage** um Ihnen bei der Umstellung zu helfen.



Offline Rehosting

Offline-Aktivierung kann auch für Rehosting-Lizenzen durchgeführt werden.

Wenn der Server keinen Internetzugang hat, wird die Schaltfläche „eine vorhandene Lizenz neu hosten“ die Offline-Neu-Hosting-Seite anzeigen:



Der Prozess ist derselbe wie bei der Offline-Aktivierung.

Remote-Verbindung von einem iPhone / iPad / Android-Gerät

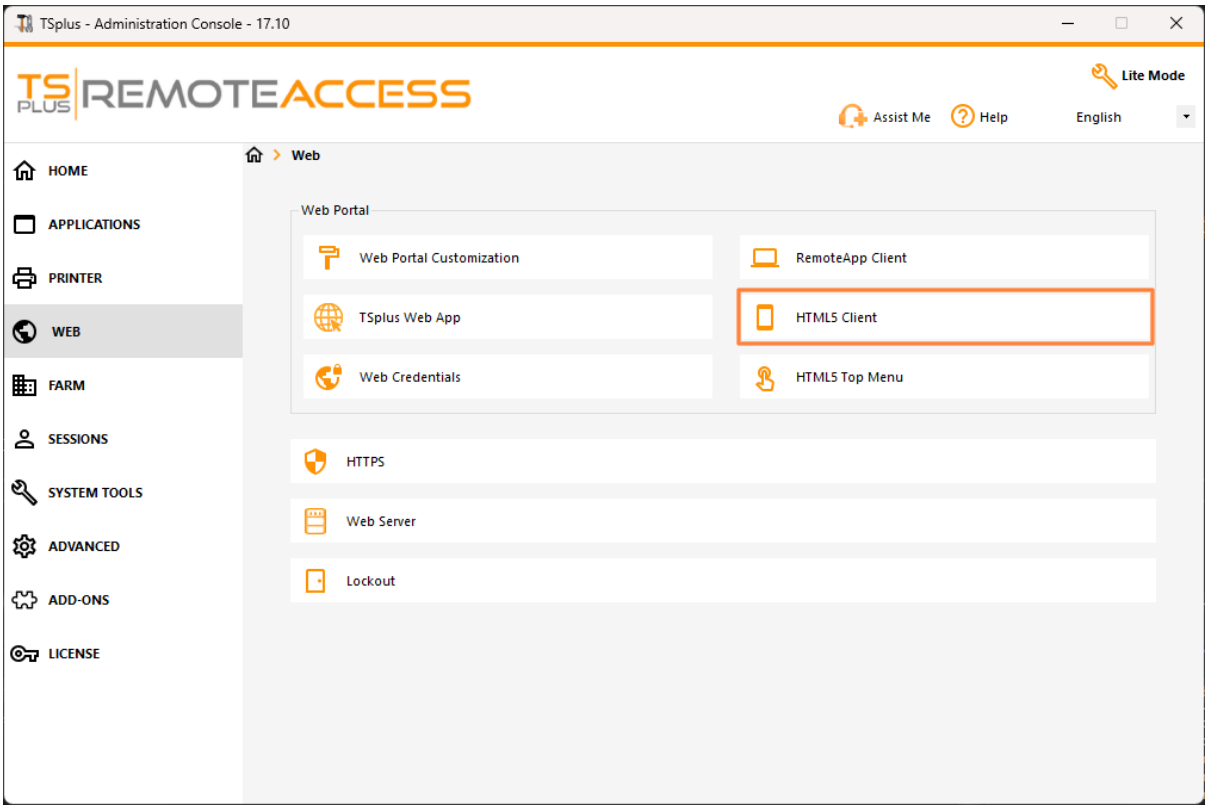
Sie können von jedem mobilen Gerät, das die HTML5-Technologie unterstützt, über jeden Browser eine Verbindung zu Ihrem Terminal Service Plus-Server herstellen, wie zum Beispiel:

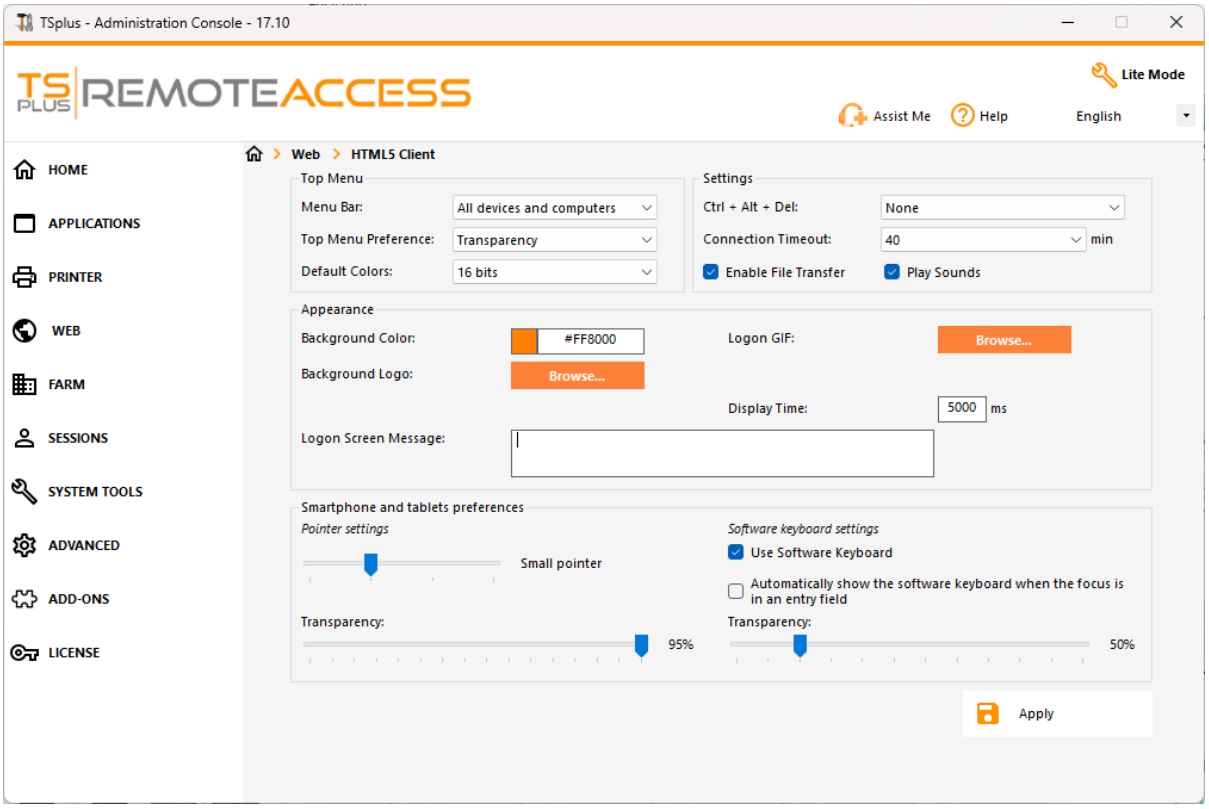
- ein iPhone
- ein iPad
- ein Android-Smartphone
- ein Android-Tablet

Bearbeiten Sie die Einstellungen für mobile Geräte

Seit der Version 11.20 wurde der TSplus HTML5-Client erheblich verbessert, um das bestmögliche Benutzererlebnis selbst von Smartphones oder Tablets zu bieten. Die Tastatur wurde neu gestaltet, um automatisch aufzuklappen, wenn der Fokus auf ein Eingabefeld gerichtet ist. Der Mauszeiger wurde neu gestaltet, um die Auswahl von Schaltflächen und Feldern zu erleichtern, selbst wenn sie sich an den linken oder unteren Rändern eines Smartphones befinden.

Sie können verschiedene HTML5-Einstellungen für mobile Geräte oder Computer auf der HTML5-Client-Kachel des Web-Tabs einrichten:





- Zeigen Sie die Menüleiste für alle Geräte und Computer oder nur für mobile Geräte an.
- Dateiübertragung aktivieren oder deaktivieren.
- Erlauben Sie die Ctrl + Alt + Del-Tastenkombination auf einem bestimmten Gerätetyp.
- Wählen Sie Ihre bevorzugte Anzeige des oberen Menüs zwischen Transparenz und Solid.
- Die Anzahl der grafischen Farbbits.

- Die Verbindungszeitüberschreitung, die maximale Dauer (in Sekunden), die eine Sitzung aktiv bleibt, während sie auf eine erneute Verbindung des Clients wartet. 0 zum Deaktivieren der Zeitüberschreitung.
- Warnmeldungen anzeigen oder ausblenden.
- Geräusche aktivieren oder deaktivieren.
- Wählen Sie Ihre Lieblingshintergrundfarbe.
- Fügen Sie ein Logo zum Hintergrund hinzu.
- Ändern Sie die Anmeldemeldung und das animierte GIF sowie die Anzeigezeit in Millisekunden.

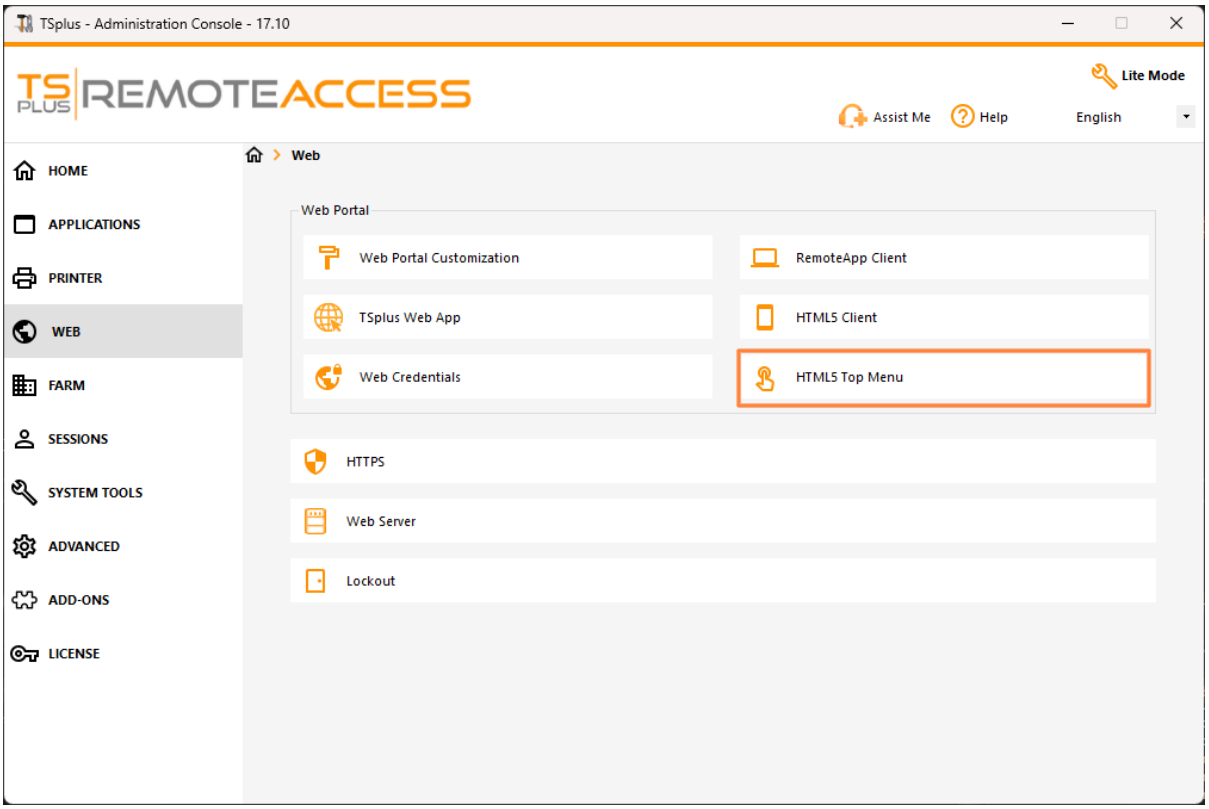
Smartphone- und Tablet-Einstellungen :

- Wenn der Administrator die Software-Tastatur verwendet, wird beim Ausblenden eines Eingabefelds die Anwendung nach oben verschoben, und der Benutzer kann weiterhin sehen, was er eingibt.

- Der Administrator kann eine kleine, eine mittlere oder eine große Größe für den Mauszeiger oder überhaupt keinen Mauszeiger auswählen. Es macht es dem Benutzer intuitiv, innerhalb seiner Anwendung zu navigieren.

- Er kann auch die Transparenzstufe für Maus und Tastatur auswählen.

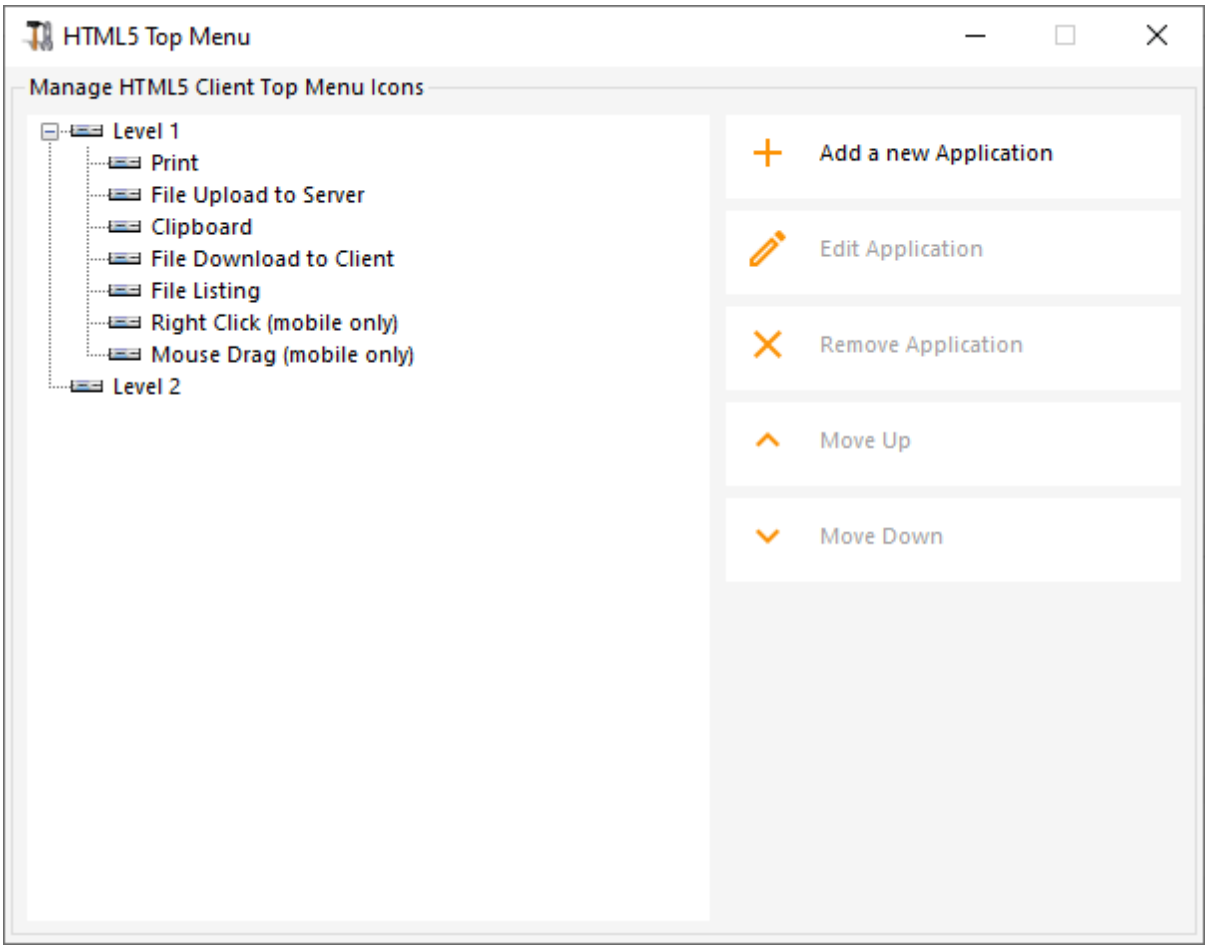
Im Tab "HTML5 Top Menu" können Sie Anwendungen hinzufügen, die auf der ersten oder zweiten Ebene des Top Menüs in HTML5 angezeigt werden.



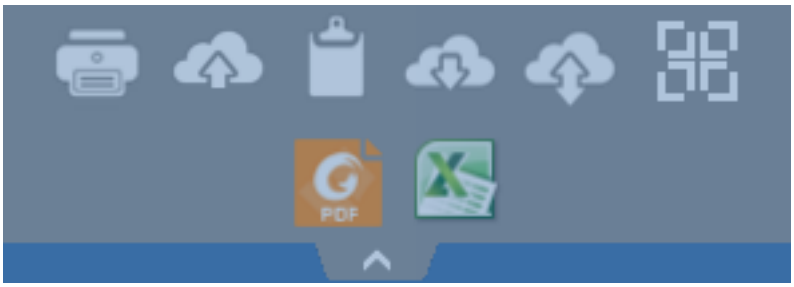
Auf Ebene eins finden Sie die integrierten HTML5-Funktionen: Drucken, Dateiübertragung und eine Zwischenablage. (Für weitere Informationen zu diesen Funktionen besuchen Sie bitte diese Seiten:

Universaldrucker für HTML5 , Dateiübertragung verwenden und Verwendung der Zwischenablage .)

In diesem Beispiel sind Foxit und Excel auf Stufe 2 veröffentlicht:

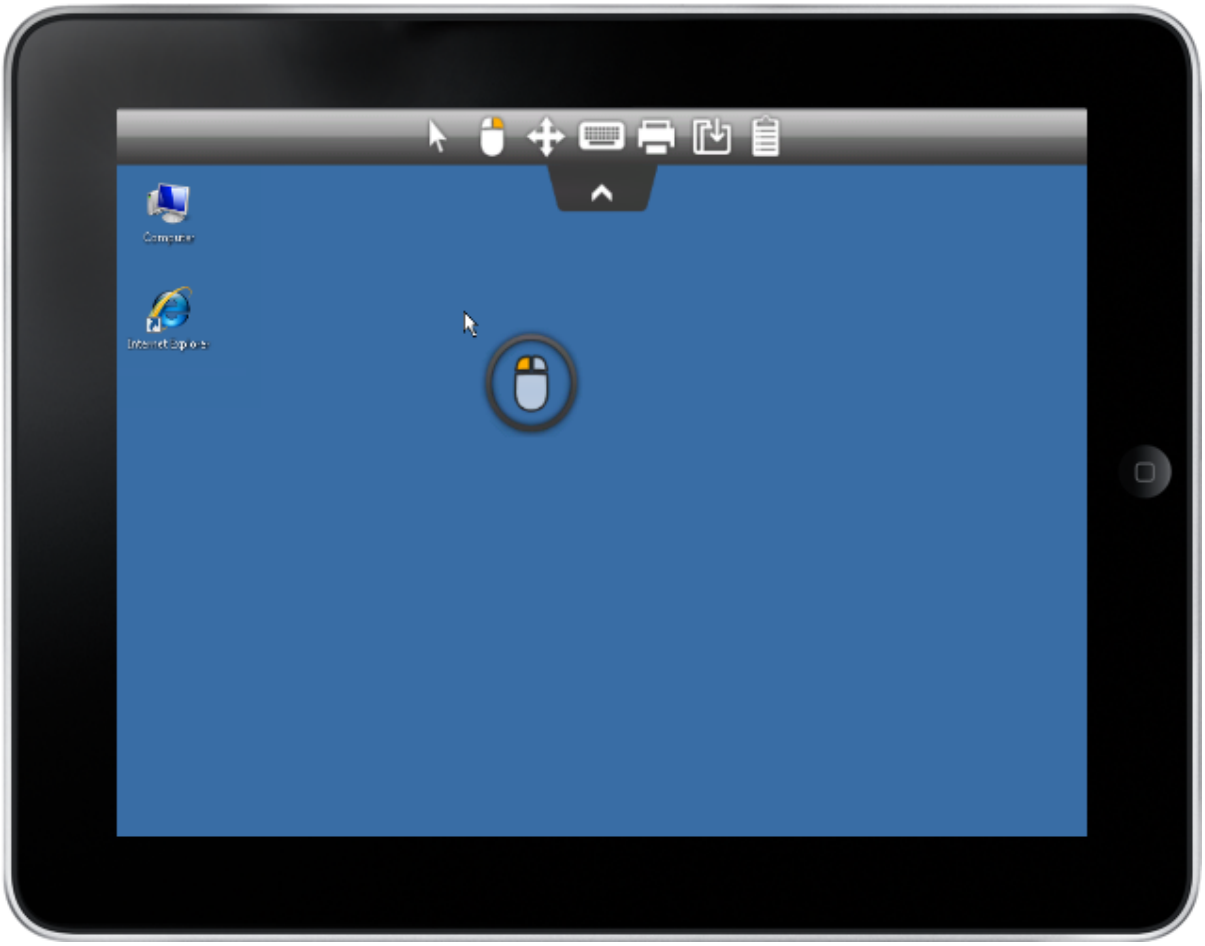


Und kann unter den integrierten Funktionen im oberen Menü der HTML5-Sitzung gefunden werden:



Darüber hinaus ermöglicht das Symbol oben rechts, Ihre Sitzung im Vollbildmodus zu wechseln.

Terminal Service Plus integrierter HTML5-Client bietet dem Benutzer ein völlig neues Menü auf Tablets und mobilen Geräten. Mit diesem neuen Menü erhält der Benutzer einfachen Zugriff auf die mobile Tastatur und das Rechtsklicken, aber auch auf die Dateifreigabe und unser einzigartiges Universal Printing-Feature!



Bitte beziehen Sie sich auf diese Dokumentation für die Verwendung der Mini-Maus und der Tastatur.

Sprachauswahl

Sie können jetzt die Sprache mit der Sprachschaltfläche rechts im oberen Menü ändern:



Sie können die Sprache für das spezifische Land, das Sie in diesem Menü wünschen, auswählen:

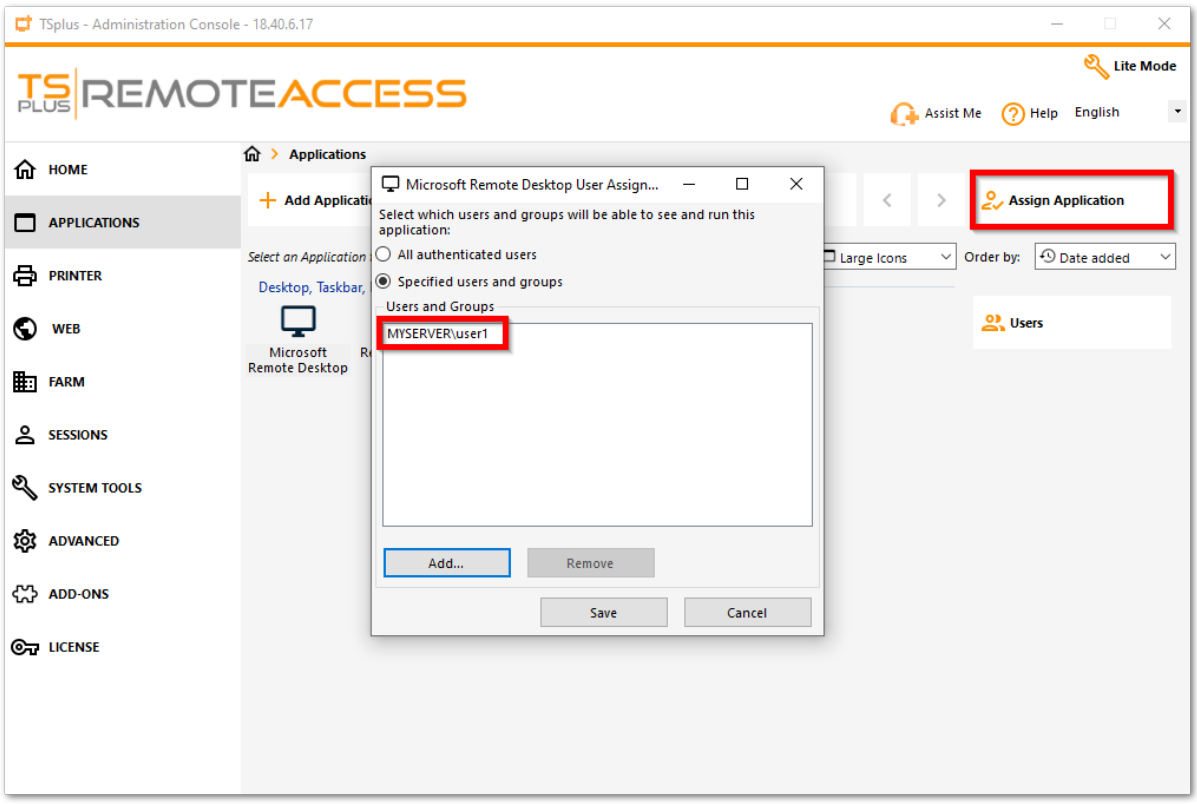
	Language	Locale	Value
◯	Portal	as_portal	
◯	Browser	as_browser	
◯	Gateway	as_gateway	
◯	Arabic	ar_ar	1025
◯	Belarusian	be_be	1059
◯	Bulgarian	bg_bg	1026
◯	Bengali	bn_bn	1093
◯	Bosnian (Cyrillic)	bs_cyrl_ba	8218
◯	Bosnian (Latin)	bs_latn_ba	5146
◯	Catalan	ca_ca	1027
◯	Czech	cs_cs	1029
◯		cs_cz	1029
◯	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

Remote-Taskleiste und Desktop-Themen

Administrator-Tools auf dem Server

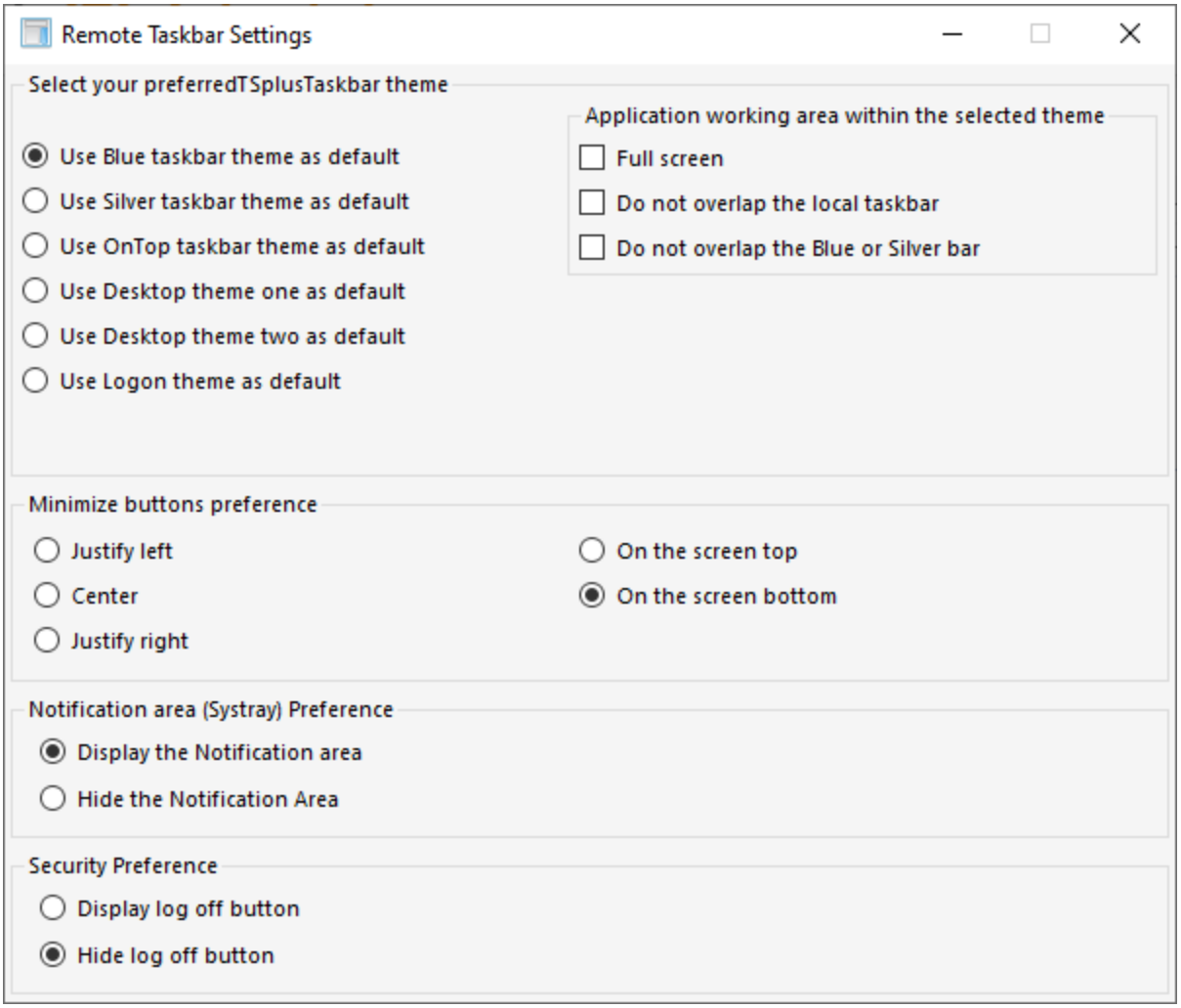
Mit dem AdminTool kann der Administrator zwischen 4 Anzeige Modi wählen, wenn er Anwendungen zuweist: Der Microsoft Remote Desktop , Die Remote-Taskleiste , Das schwebende Panel oder Das Anwendungsfeld Die Remote-Taskleiste, schwebenden und Anwendungsfenster sind für jede Verbindungsart verfügbar.

Wenn Sie Anwendungen einem Benutzer zuweisen, können Sie die TSplus Remote-Taskleiste aktivieren. Der Benutzer kann Remote-Anwendungen mit einem Klick auf die TSplus-Taskleiste starten und hat weiterhin den vollständigen lokalen Desktop zur Verfügung. Sie können die Remote-Taskleiste Ihren Benutzern oder Gruppen zuweisen, indem Sie darauf doppelklicken oder sie auswählen und dann auf das Feld „Anwendung zuweisen“ klicken.



Der Administrator kann leicht entscheiden, welches das Standard-Remote-Desktop-Design ist,

das der Benutzer beim Öffnen einer Sitzung sieht. Wählen Sie die TSplus Remote Taskleiste aus und klicken Sie dann auf „Anwendung bearbeiten“:



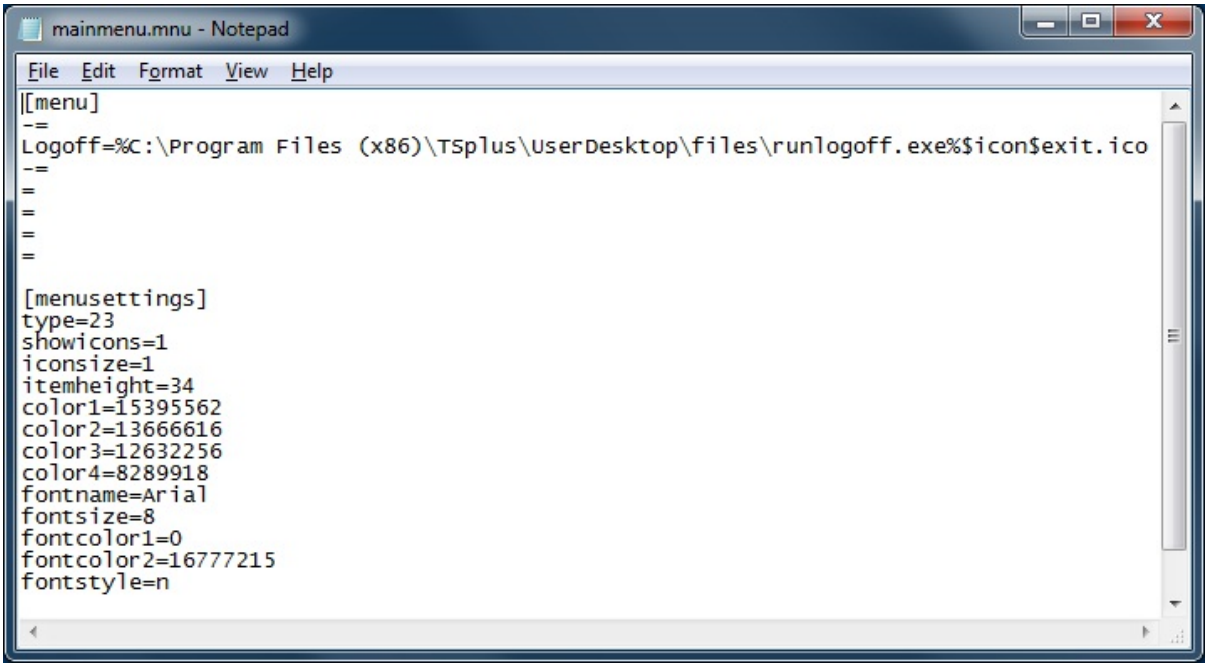
- Nur der Administrator kann die Themen für seine Benutzer auswählen.
- Er kann wählen, ob er die maximierten Anwendungen im Vollbildmodus anzeigen möchte oder ob die TSplus-Taskleiste sowie die Silber- oder Blaustreifen nicht überlappt werden sollen.
- Die Position der minimierten Schaltflächen in der Taskleiste kann geändert werden (oben auf dem Bildschirm, unten, rechts, links oder in der Mitte).

  Der Administrator kann sogar entscheiden, es oben auf dem Bildschirm des Benutzers anzuzeigen, anstatt an der standardmäßigen unteren Seite.
- Systray-Symbole können durch Aktivieren des Kreises „Benachrichtigungsbereich ausblenden“ ausgeblendet werden.

- Seit der Version TSplus 12.60 kann die Abmeldetaste jetzt ausgeblendet werden.

Durch die Bearbeitung des Benutzermenüs kann der Administrator Anwendungen und Funktionen hinzufügen oder entfernen. Die Anpassung des Benutzermenüs ist einfach.

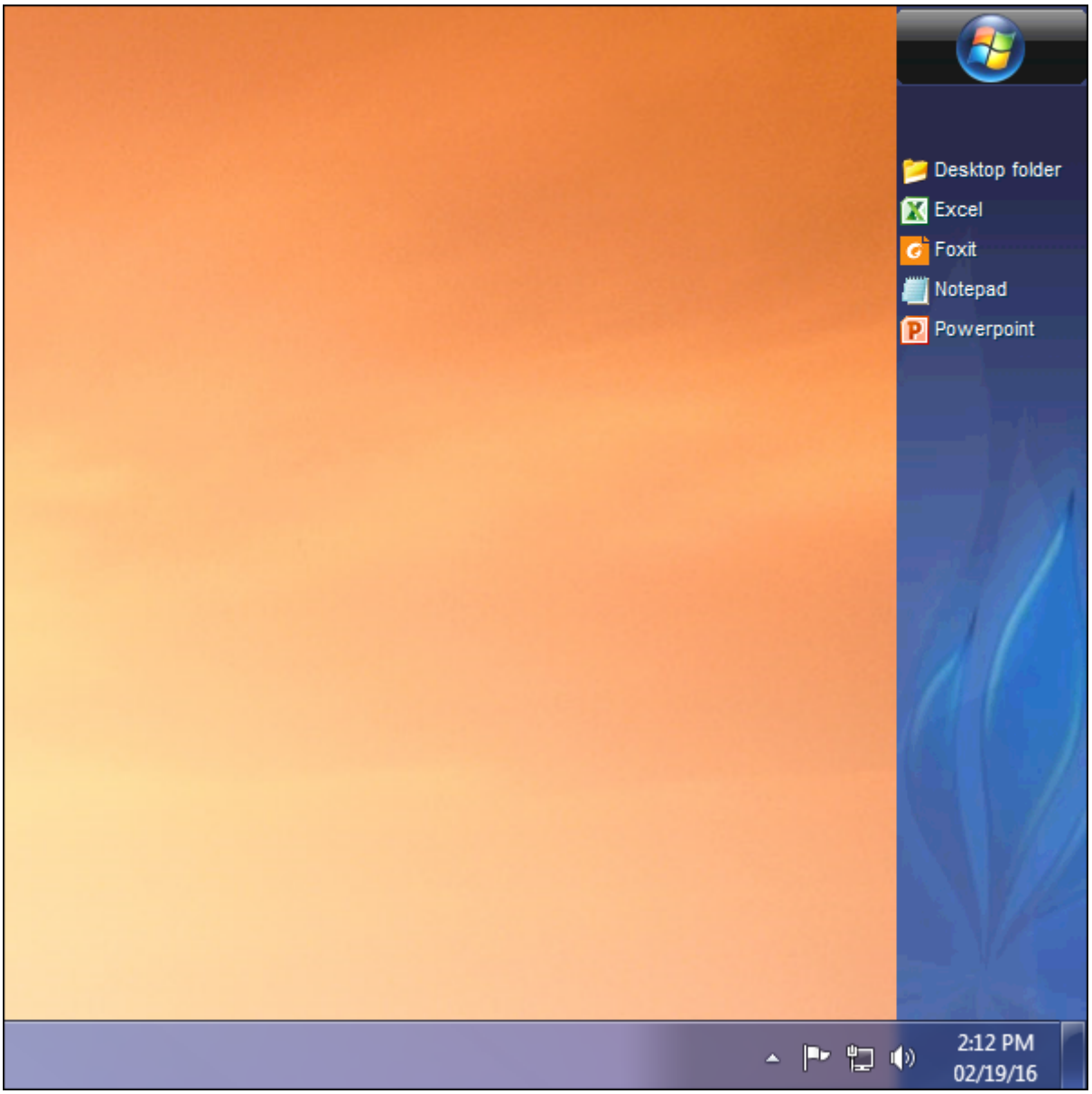
Der Inhalt des Benutzermenüs (zu finden in Program Files/TSplus/UserDesktop/mainmenu.mnu) kann vom Administrator mit Notepad geändert werden:



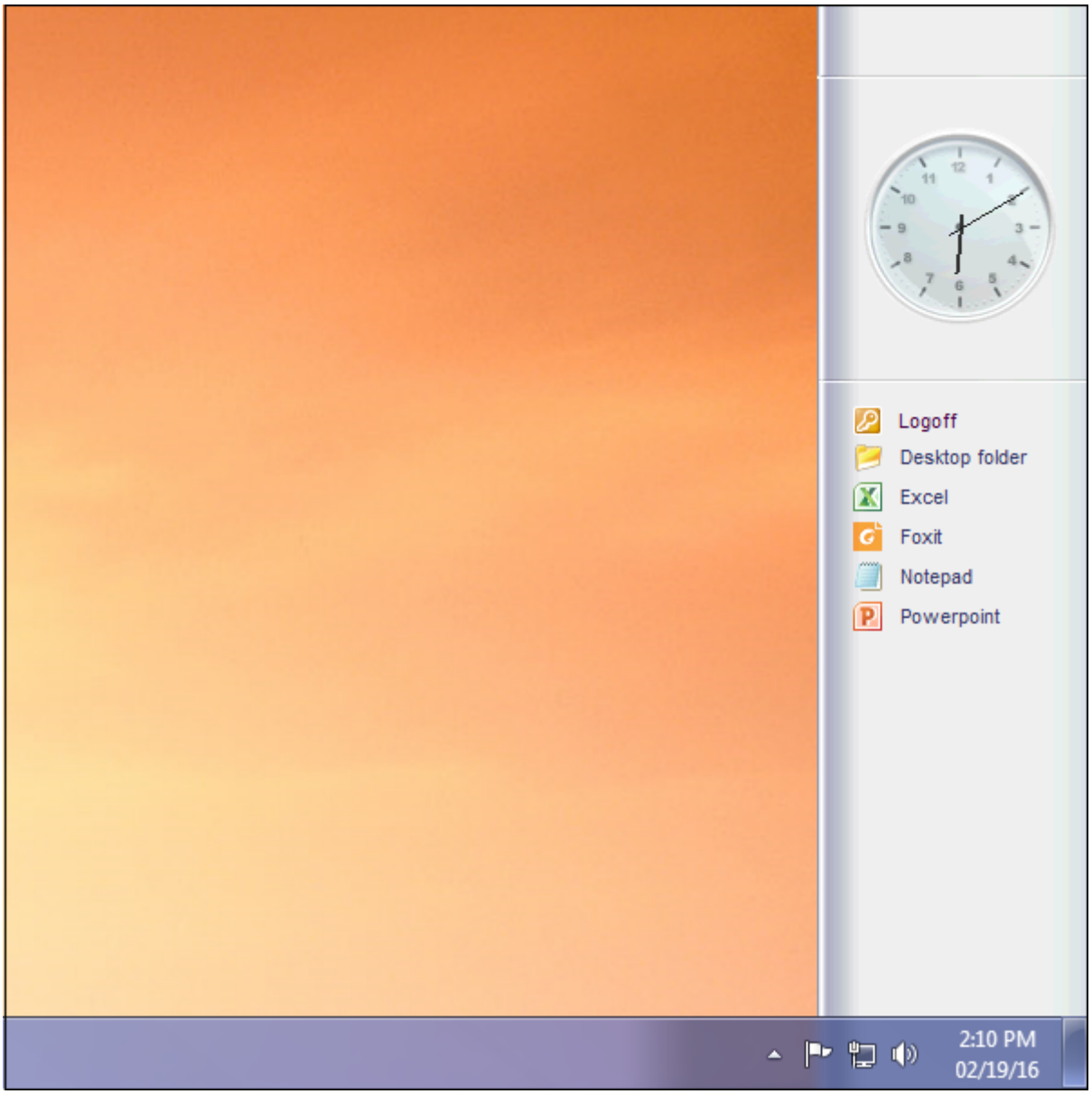
Auf der Anwendungskachel des AdminTools kann der Administrator 3 verschiedene Stile der Remote Desktop TSplus Taskleiste auswählen.

Der Benutzer kann Remote-Anwendungen mit einem Klick auf die TSplus-Taskleiste starten und hat weiterhin den vollständigen lokalen Desktop zur Verfügung.

Rechtsseitige blaue Themen-Taskleiste



Rechtsseitige Silber-Themen-Taskleiste



Auf der oberen Taskleiste



Zurück nach oben

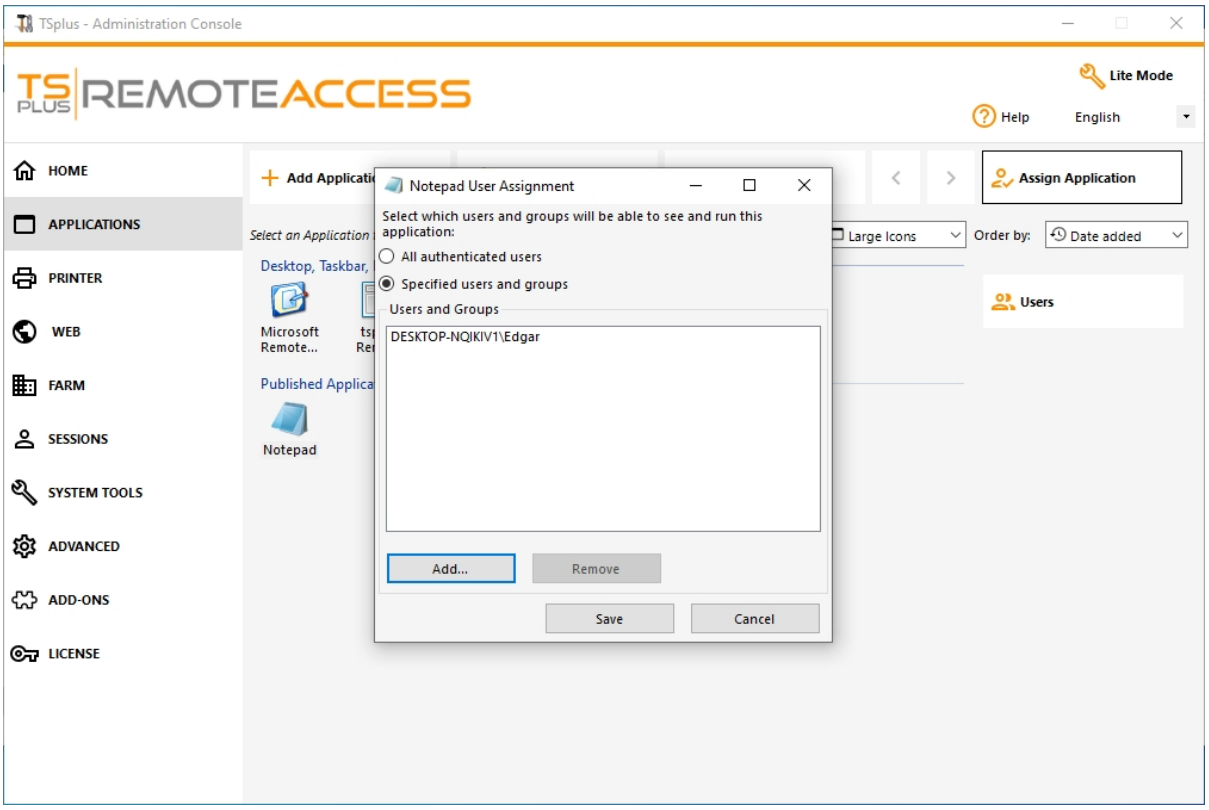
Mit dem AdminTool kann der Administrator leicht entscheiden, welches das Standard-Remote-

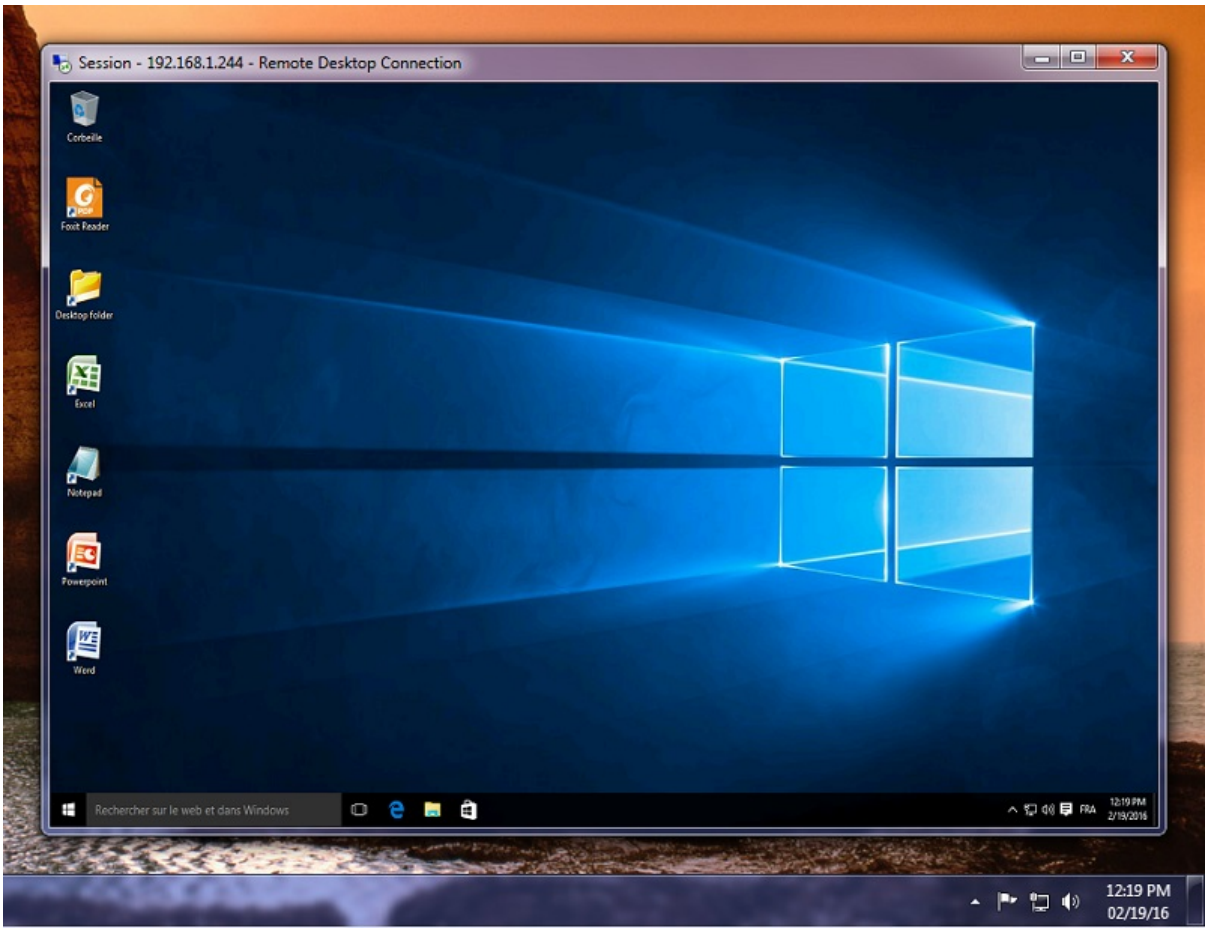
Desktop-Thema ist, das der Benutzer beim Öffnen einer Sitzung sieht. Er hat die Wahl zwischen 4 verschiedenen Stilen des Vollbild-Remote-Desktops. Das standardmäßige Microsoft Remote Desktop kann ebenfalls verwendet werden, wenn gewünscht.

Weil diese TSplus Desktops Vollbild-Desktops sind, wird der Bildschirm des Benutzers vollständig ausgefüllt, wenn eine Sitzung von dedizierten Thin Clients, einem RDP-basierten Client oder von einer Webseite oder TSplus Remote Desktop-Clients aus geöffnet wird.

Es gibt Vorteile gegenüber einem standardmäßigen Remote Desktop. Es verbessert die Serversicherheit (kein START-Button und keine vollständige Kontrolle über den Desktop).

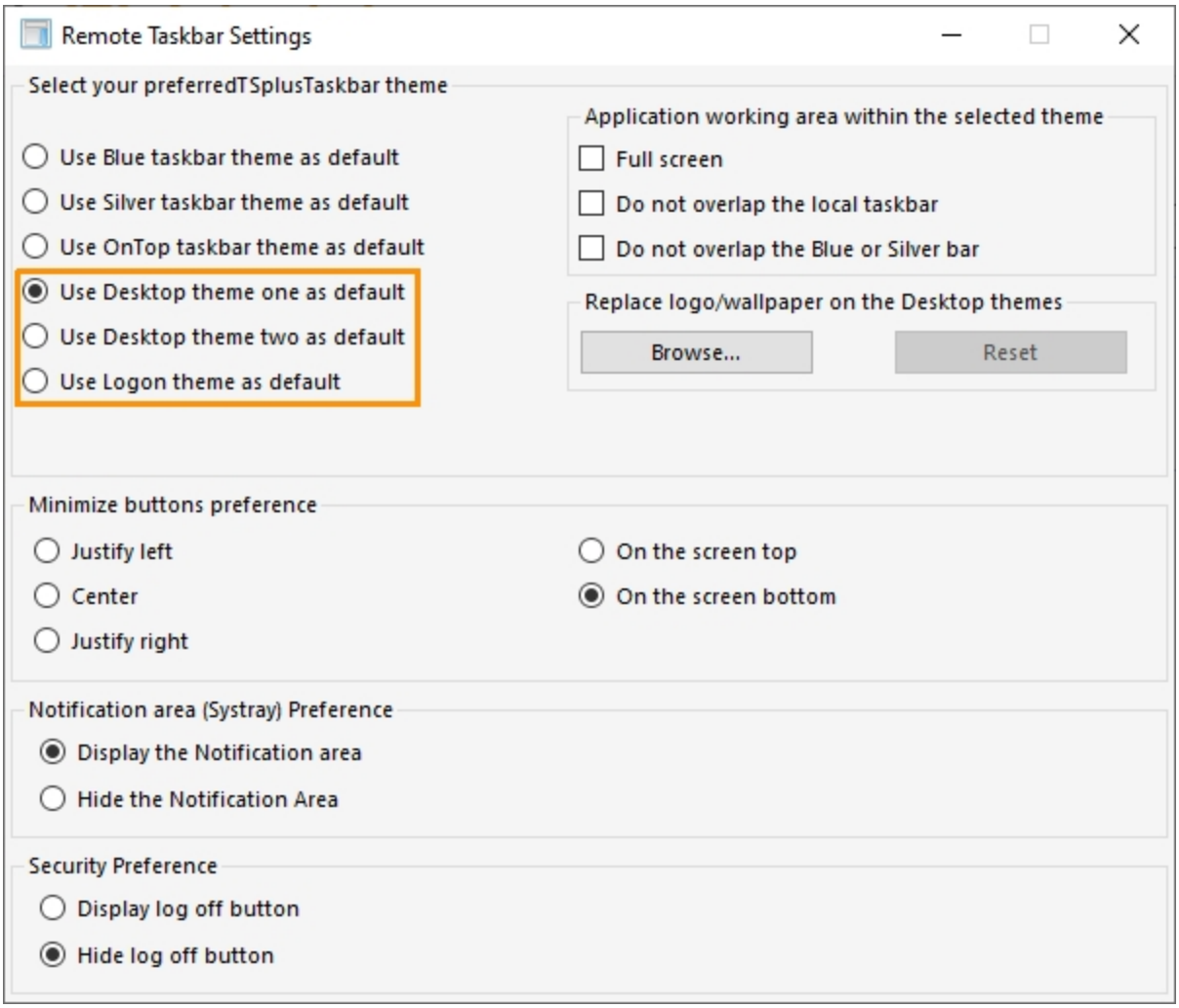
Standard Microsoft Remote Desktop





- Der Benutzer hat einen vollständigen Desktop, einschließlich der Startschaltfläche und vollständiger Kontrolle über den Desktop.
- Um das vollständige Desktop zuzuweisen, weisen Sie einfach die Microsoft Remote Desktop-Anwendung zu.

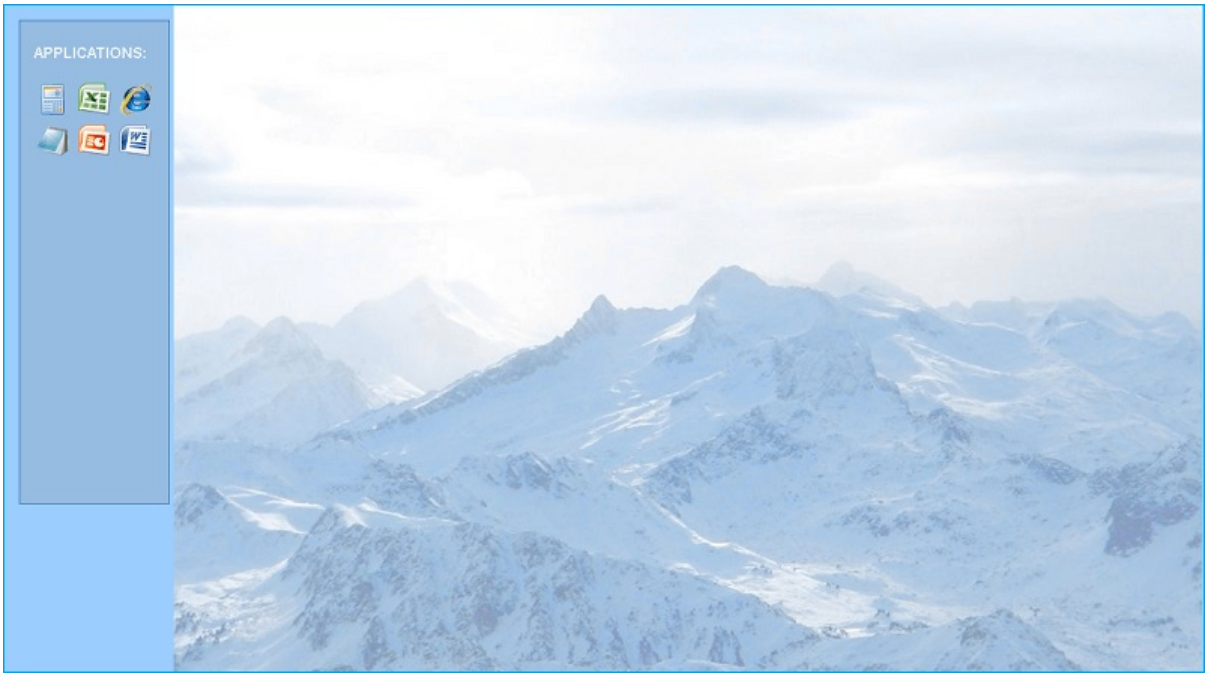
Um die Desktop-Themen zu ändern, müssen Sie die TSplus Remote Taskleiste zuweisen und zwischen den 3 vorgeschlagenen Themen wählen:



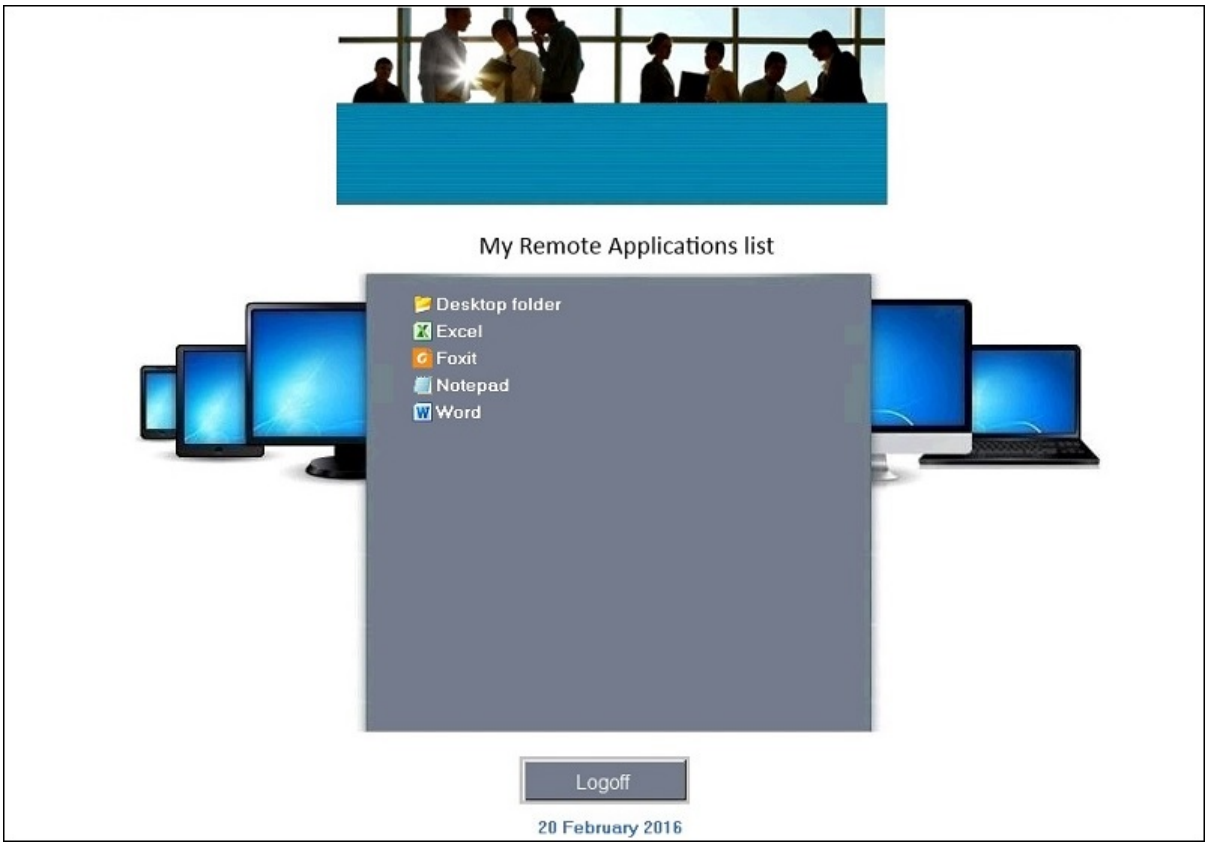
TSplus Desktop-Thema eins



TSplus Desktop-Thema zwei



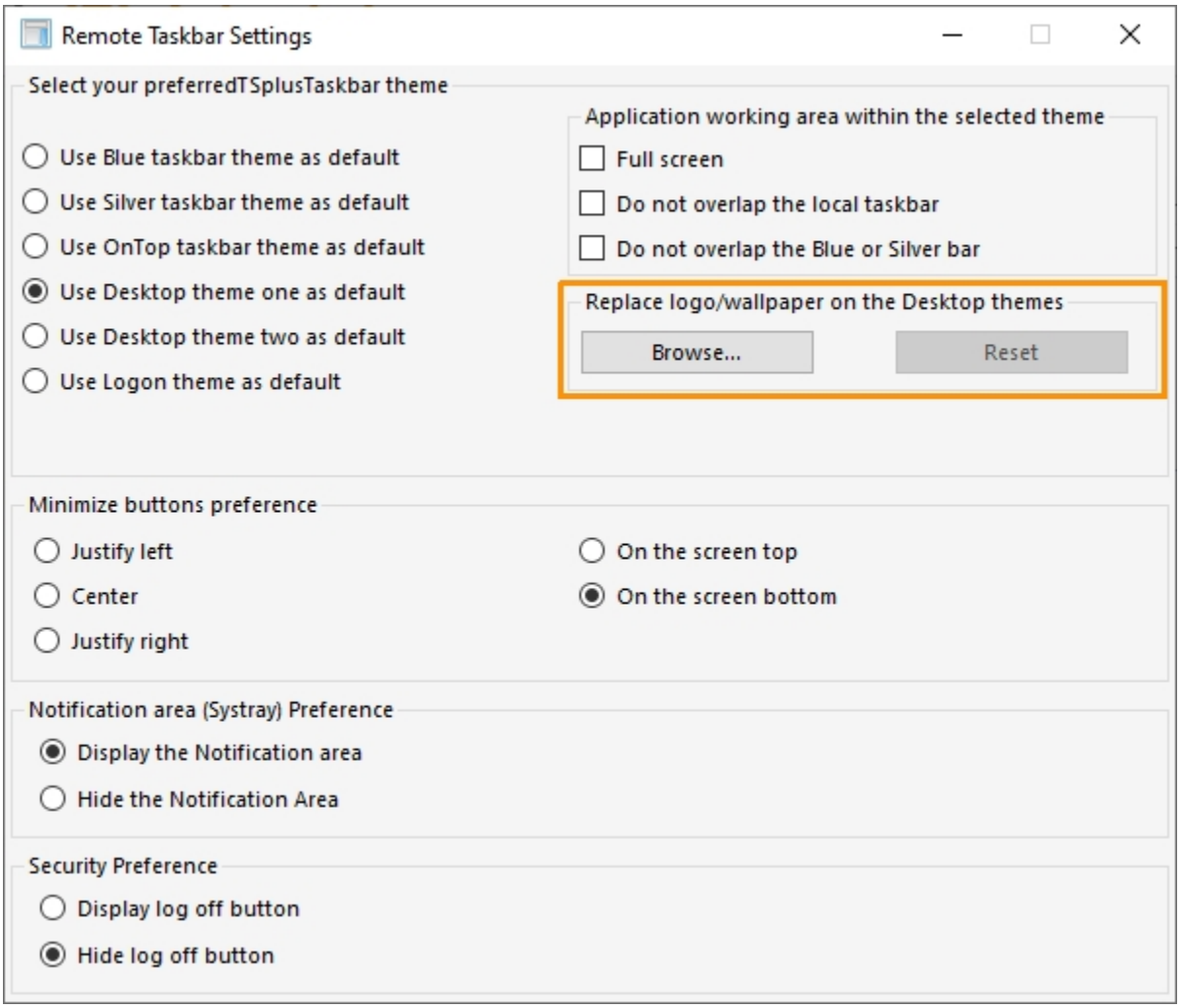
TSplus Anmeldethema



Angepasstes Thema

Für jedes Thema kann der Administrator es anpassen und beispielsweise das

Unternehmenslogo anzeigen. Er kann auch sein eigenes Desktop-Hintergrundbild hinzufügen, indem er eines der Desktop-Themen auswählt und auf die Schaltfläche Logo/Hintergrundbild ersetzen klickt, um beispielsweise seine .jpg-Datei auszuwählen.



- Sie können Ihren eigenen Desktop-Hintergrund hinzufügen, indem Sie eines der Desktop-Themen auswählen und auf die Schaltfläche Logo/Hintergrund ersetzen klicken, um Ihre .jpg-Datei auszuwählen, zum Beispiel:


APPLICATIONS:
15 June 17

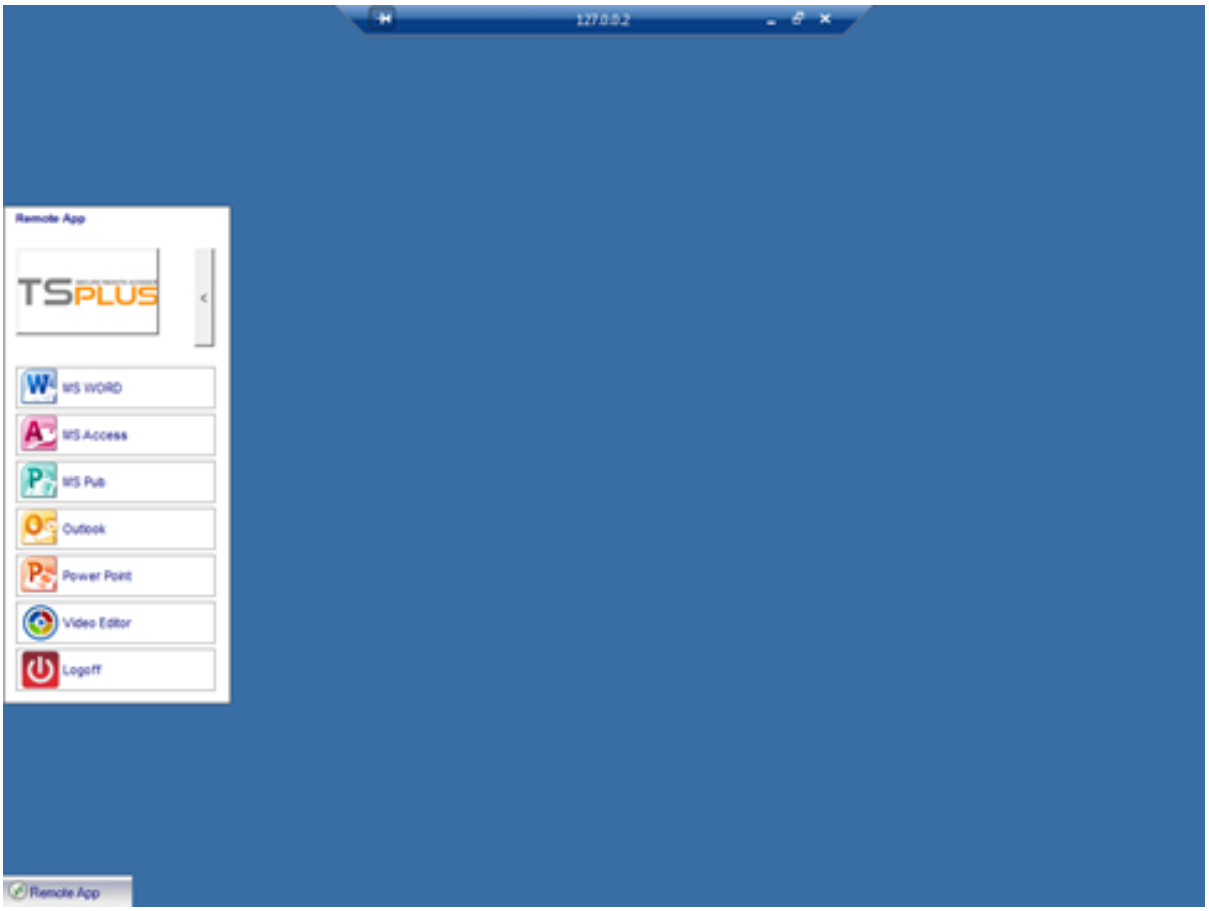
RemoteApp-Funktion auf dem Client

In der Vergangenheit war der generierte TSplus Portable-Client die übliche Methode für einen Benutzer, um Anwendungen zu starten. Die Version 10.50 führt ein. **ein Symbol im Benachrichtigungsbereich** welches jedem Benutzer die Liste aller seiner Remote-Anwendungen gibt. Innerhalb dieser Anwendungsübersicht kann der Benutzer diejenige auswählen, die er starten möchte.

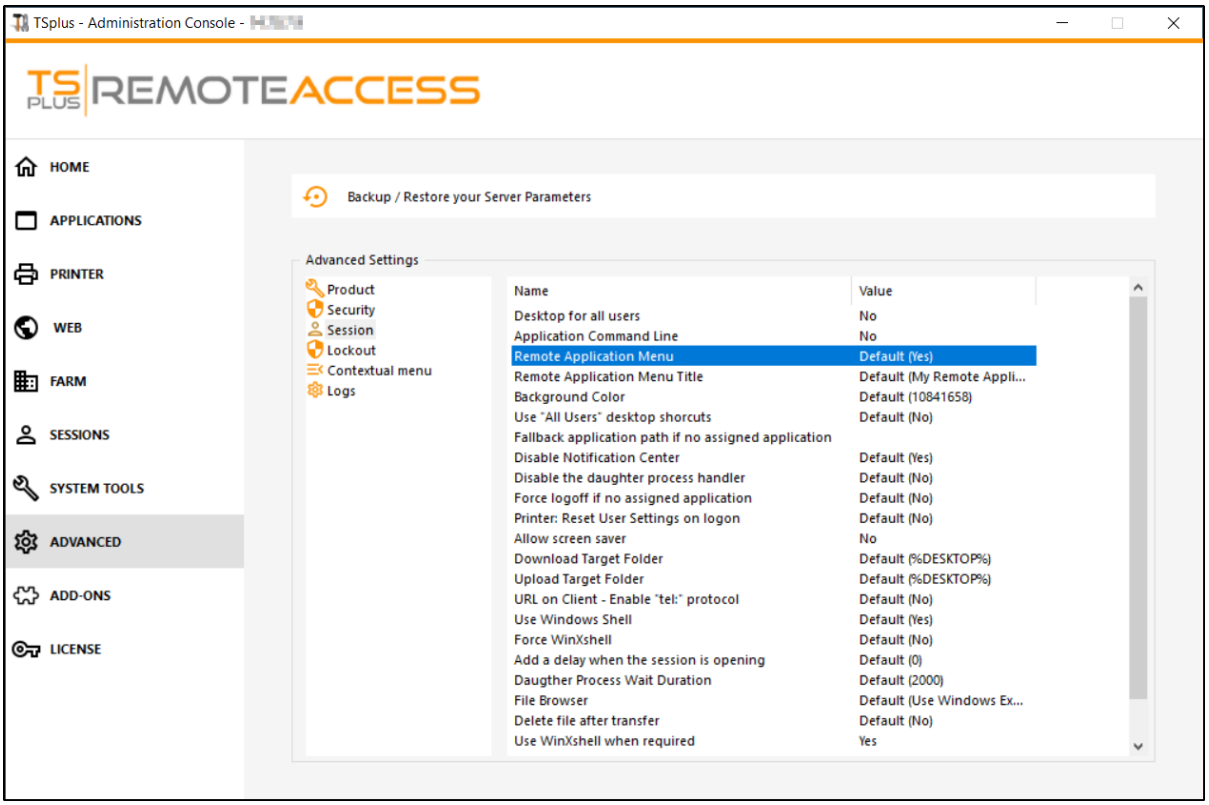
Dies ist eine neue Möglichkeit für Administratoren, Remote-Anwendungen (die als „RemoteApps“ bezeichnet werden) an ihre Benutzer bereitzustellen. Insbesondere ermöglicht RemoteApp On Client einen einfachen Veröffentlichungsprozess, der es ermöglicht, Anwendungen, die direkt auf dem Server installiert sind, den Benutzern zur Verfügung zu stellen, RemoteApp-Programme neben lokalen Programmen auszuführen und eine Integration mit einer benutzerdefinierten „Launcher“-Anwendung anzubieten, um es den Benutzern zu erleichtern, RemoteApp-Programme zu finden und zu starten.

Die Benutzeranwendungsliste wird ebenfalls im erscheinen. **Startmenü** unter **Alle Programme** in einem Ordner namens **Meine Remote-Anwendungen** Um diese neue erstaunliche TSplus-Funktion bereitzustellen, ist es einfach: Der Administrator hat neue Verbindungsclients generiert und sie mit dem AdminTool aktiviert. Dieser Leitfaden erklärt Schritt für Schritt, was passieren wird, wenn der Administrator diese neue Funktion aktiviert und seinen Benutzern einen neu generierten Verbindungsclient bereitstellt.

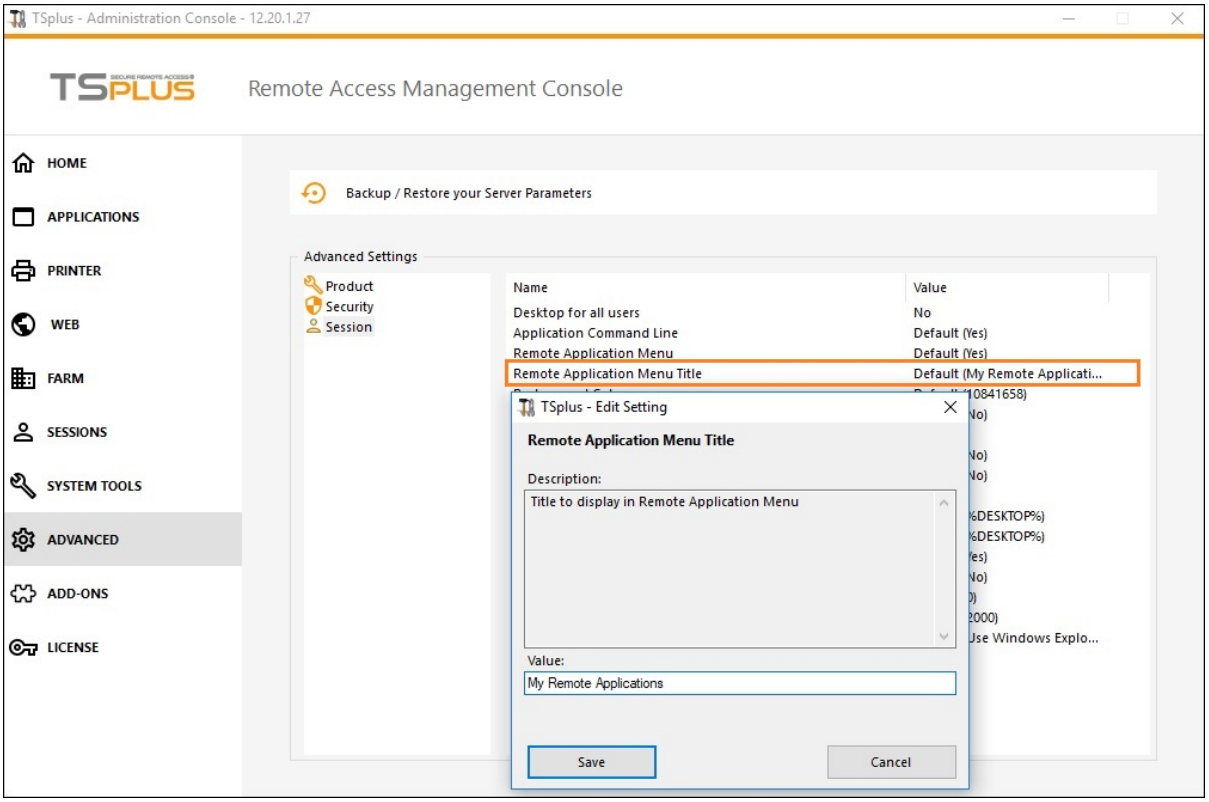
Beispiel: Die Benutzerin „Laura“ verwendet TSplus, um auf ihre Remote-Anwendung zuzugreifen. Dazu nutzt sie einen generierten Client namens **LauraPortableClient.exe** Wenn sie es auf ihrem PC ausführt, erhält sie folgendes Ergebnis:



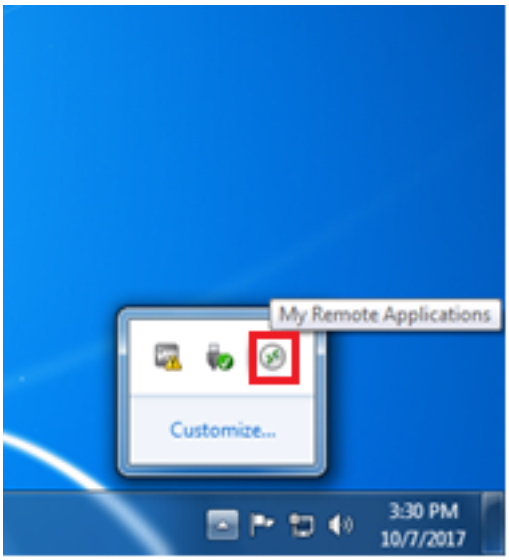
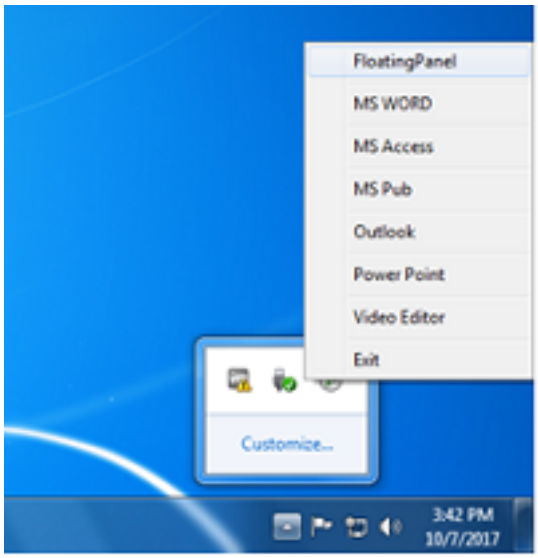
Allerdings stellte der Administrator ihr eine neue zur Verfügung, die mit der TSplus 10.50-Version erstellt wurde. Sie muss sie mindestens einmal ausführen, um von dem neuen zu profitieren. **RemoteApp-Funktion auf dem Client** Wenn der Administrator eine Anwendung zu einem Benutzer hinzufügt oder entfernt, wird diese Änderung beim nächsten Anmelden auf der Serverseite vorgenommen. Das bedeutet, dass die aktuelle Sitzung diese Änderung nicht widerspiegelt. Die erweiterte Registerkarte des AdminTools bietet eine Option, um diese RemoteApp On Client-Funktion zu aktivieren oder zu deaktivieren; standardmäßig ist sie aktiviert.



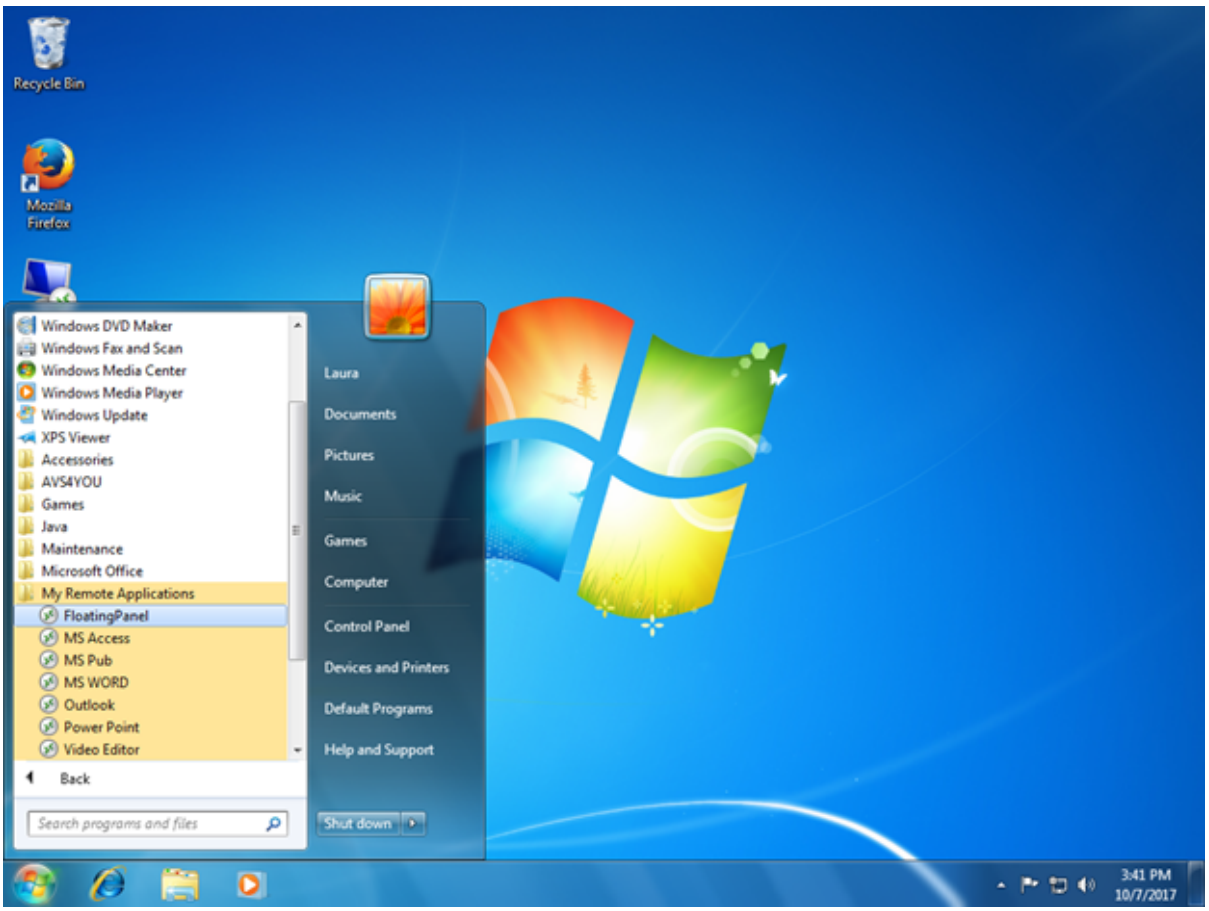
Sie können den Menünamen nach Belieben ändern, indem Sie auf den Titel des Remote-Anwendungsmenüs unten klicken und ihn im Wertfeld hinzufügen.



Was auf ihrem PC passieren wird, wenn sie einmal ihren neu generierten Client ausführt: Sie wird ein neues Symbol im Benachrichtigungsbereich ihrer lokalen Taskleiste sehen.

Mein neues Symbol für Remote-Anwendungen	Anwendungslistenmenü
	

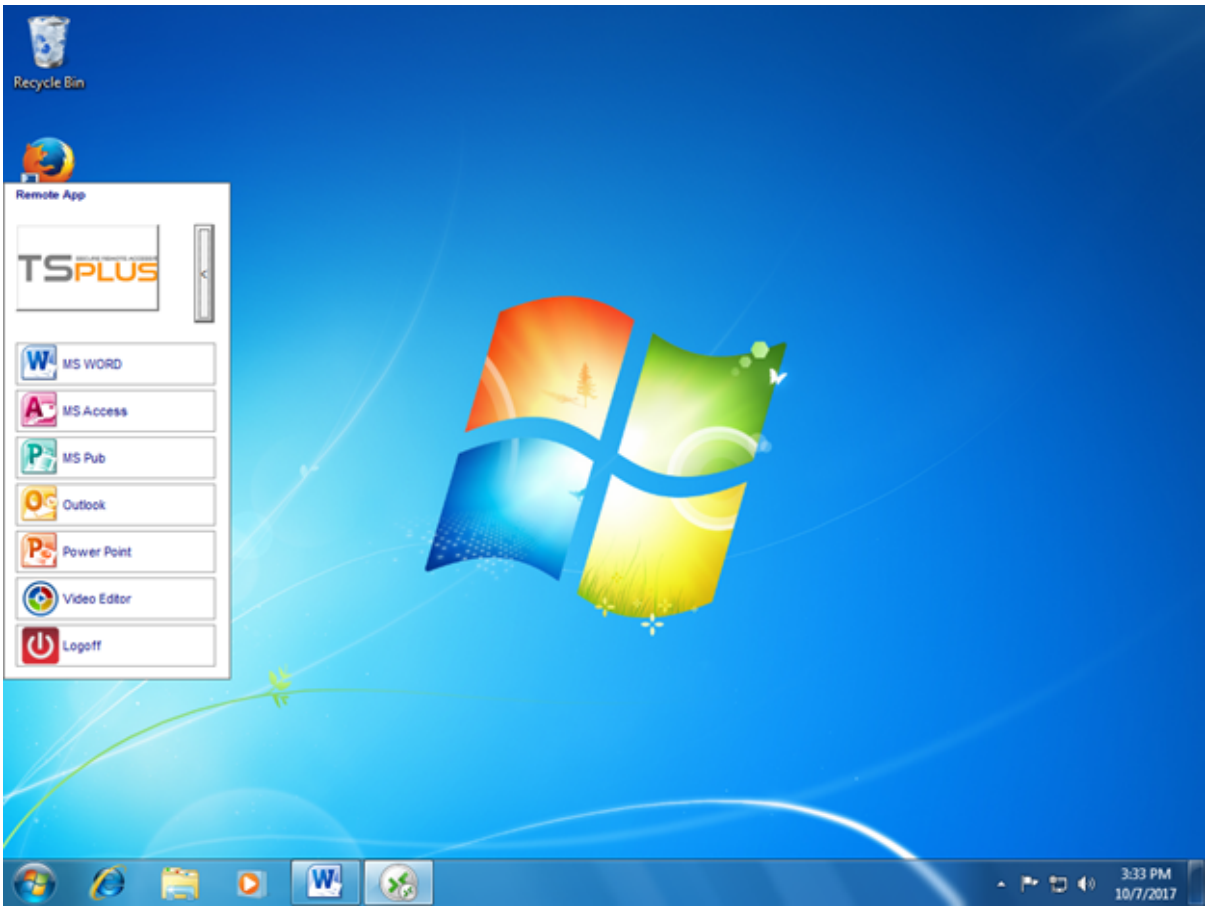
Sie wird auch einen neuen Eintrag in ihrer Startmenü-Programmliste mit dem Namen sehen. **„Meine Remote-Anwendungen“** :



Sie wird jetzt in der Lage sein, eine dieser aufgeführten Anwendungen auszuwählen und sie als

RemoteApp zu starten. Sie muss den bereitgestellten LauraPortableClient.exe generierten Client nicht verwenden.

Wenn sie beispielsweise das schwebende Panel auswählt, erhält sie dieses Ergebnis:

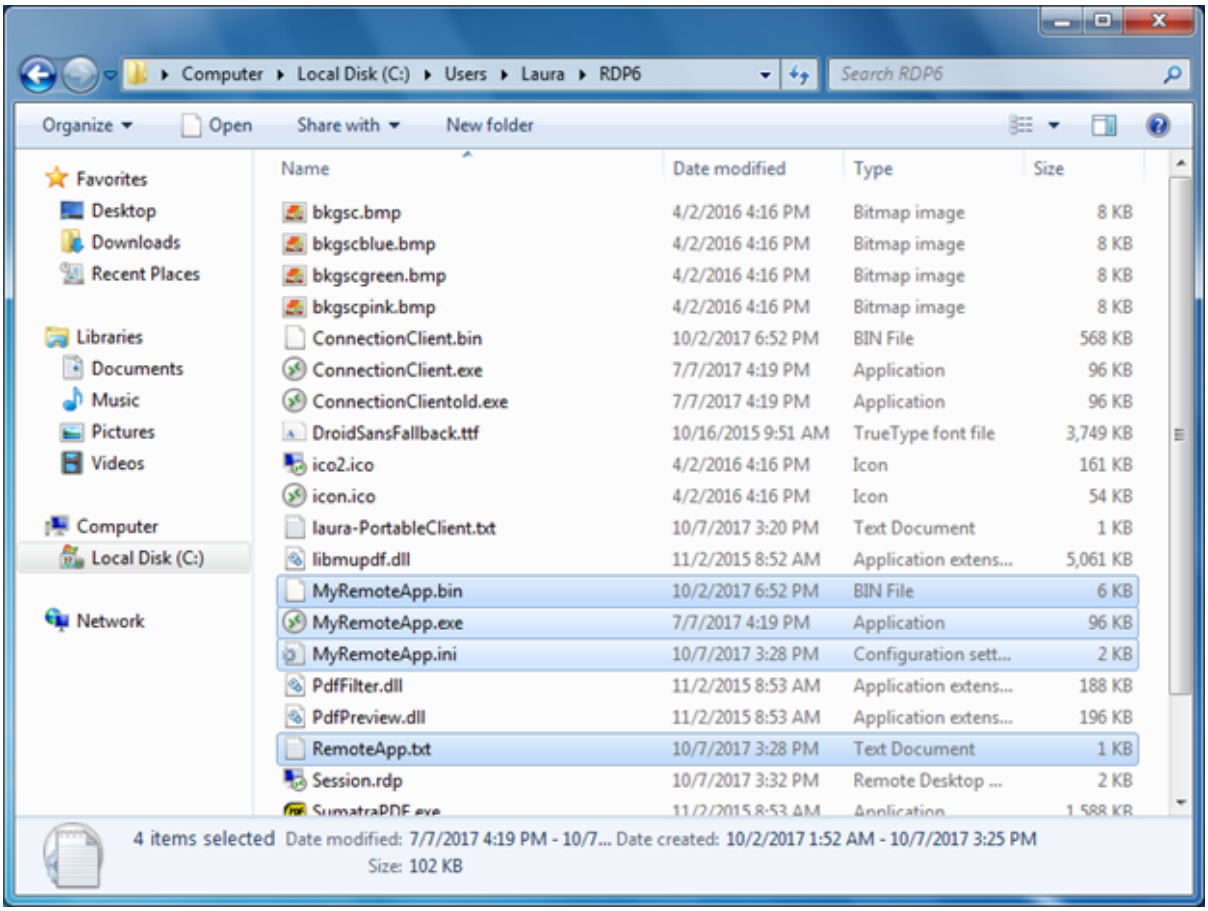


Technischer Hintergrund dieser neuen Technologie.

Die neu generierte Client-Version des Releases 10.50 fügt mehrere Dateien im C:\Users%UserName%\RDP6-Ordner des Benutzerprofils des lokalen PCs hinzu.

MyRemoteApp.exe und MyRemoteApp.bin sind die Programmcodes, die gestartet werden, um das neue Symbol im Benachrichtigungsbereich und den neuen Eintrag in der Liste Alle Programme des Startknopfs zu erstellen.

MyRemoteApp.ini ist eine Datei, die vom Server empfangen wird. Sie enthält die Details jeder Anwendung, die diesem Benutzer auf der Serverseite zugewiesen ist. Sie wird bei jeder neuen Verbindung zum Server aktualisiert. Normalerweise dauert es 30 Sekunden nach jedem Anmelden, um diese Datei vom Server zu erhalten. RemoteApp.txt gibt den Namen des zuletzt generierten Clients an, der auf diesem PC gestartet wurde.



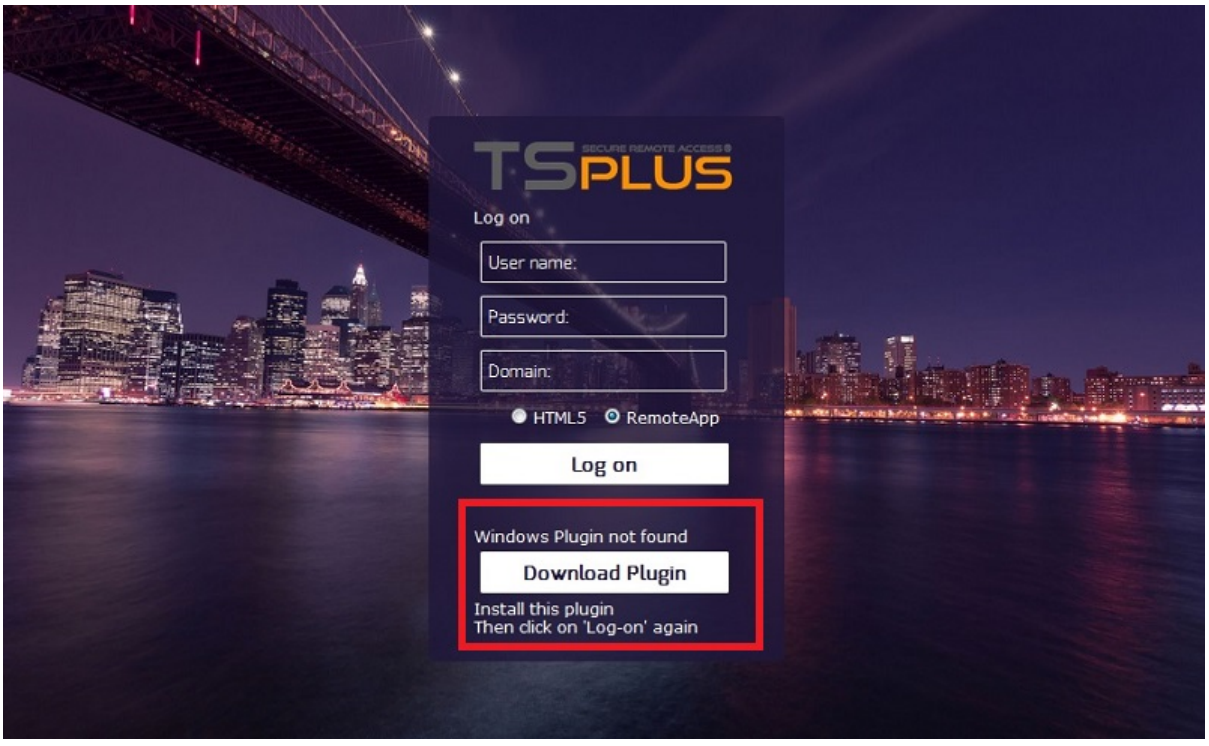
Kommentare:

Wenn der Benutzer Administratorrechte auf seinem eigenen PC hat, **MyRemoteApp.exe** wird bei jedem Neustart automatisch gestartet und die Schaltfläche "Start" wird ebenfalls aktualisiert. Andernfalls muss der Administrator den neu generierten Client einmal "Als Administrator" ausführen, um die neue Funktion zu aktivieren. Dadurch werden die entsprechenden Registrierungseinträge in HKLM erstellt. Wenn ein Benutzer sich nur mit einem Server verbindet, ist dieses neue System perfekt. Wenn er jedoch mehrere Verbindungsclients verwendet, um Sitzungen auf verschiedenen Servern zu öffnen, sollten Sie beachten, dass die Datei **MyRemoteApp.ini** wird mit den Werten der letzten Verbindung aktualisiert. Es kann für den Benutzer verwirrend sein, und in einem solchen Bereitstellungsfall empfehlen wir, diese neue Funktion nicht zu verwenden.

Remote App Plugin

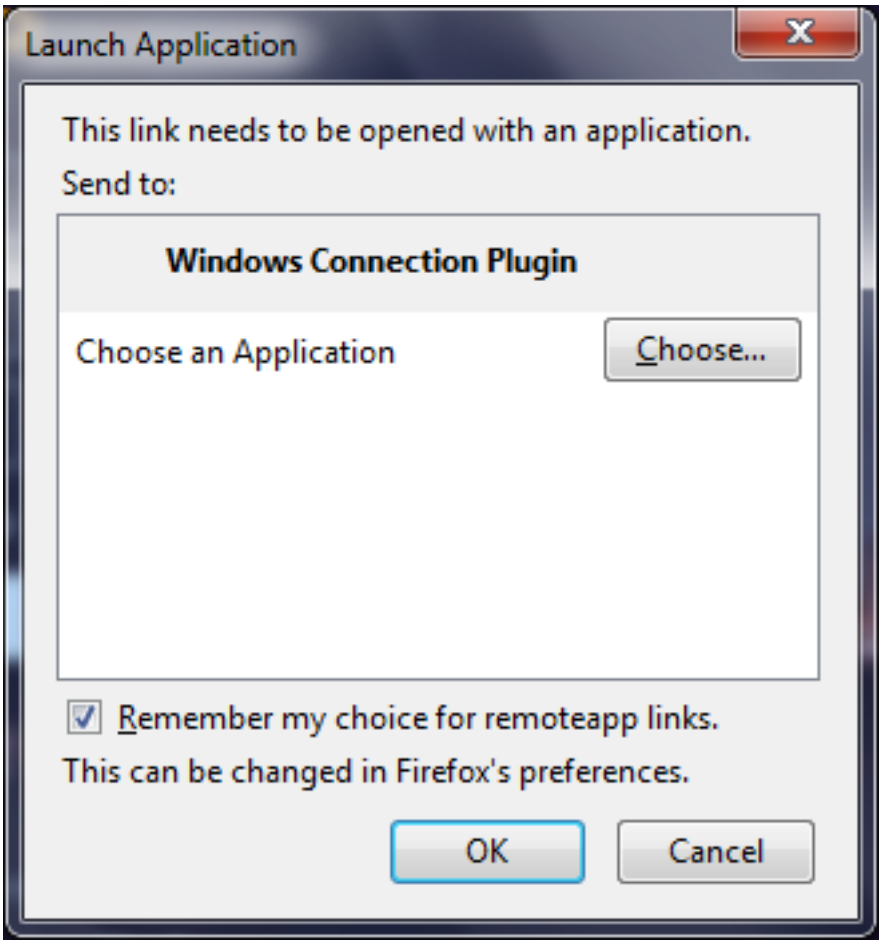
Seit der neuen Version 8.40 von TSplus ist es nicht mehr erforderlich, ein Java-Plugin im Client-Browser zu installieren.

Sie können jetzt auf den Windows RemoteApp-Client zugreifen, indem Sie ein kleines Windows-Plugin über das Webportal herunterladen und installieren. Dieser Vorgang ist schnell und muss nur einmal pro Client durchgeführt werden.



Sie können es auch im C:\Program Files (x86)\TSplus\Clients\www\RemoteAppClient-Ordner installieren.

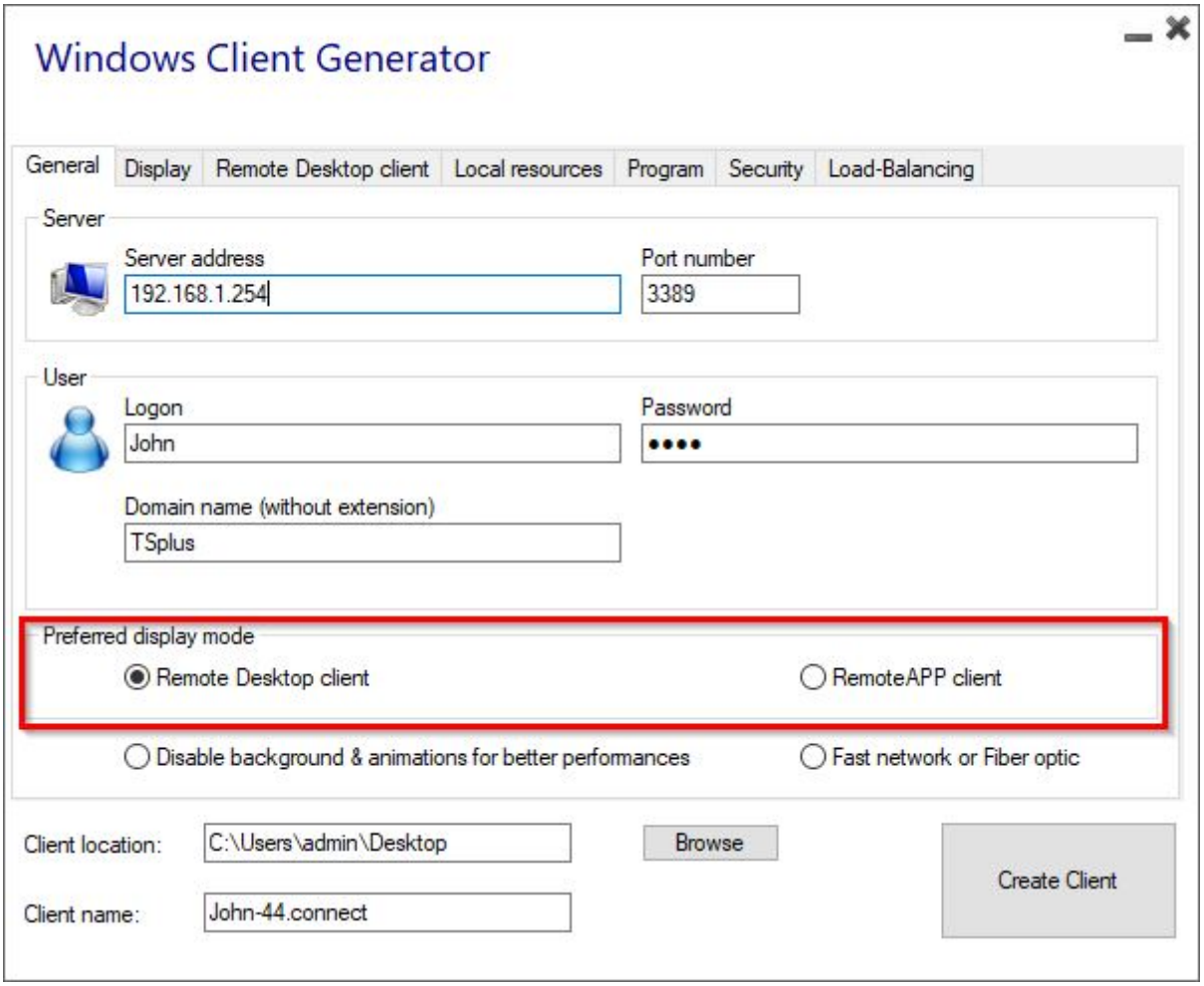
Wenn Sie Firefox verwenden, wird diese Nachricht bei Ihrer ersten Verbindung angezeigt. Wenn Sie die Option „meine Entscheidungen merken“ wählen, wird die Benachrichtigung bei zukünftigen Verbindungen deaktiviert.



Hinweis Seit TSplus 12.40, die RemoteApp-Client-Konfiguration und die Das Client-Setup-Programm wurden zusammengeführt und können mit einem einzigen Setup bereitgestellt werden - wenn Sie also das RemoteApp-Client-Setup herunterladen, ist es nicht erforderlich, das Connection-Client-Setup herunterzuladen.

RemoteApp-Verbindungsclient

Sie können zwischen 2 Anzeige Modi im allgemeinen Tab des Client-Generators wählen:



###RemoteApp-Verbindungsclient

Der RemoteApp-Verbindungsclient hängt nicht von den Einstellungen der Transparenzfarbe ab.

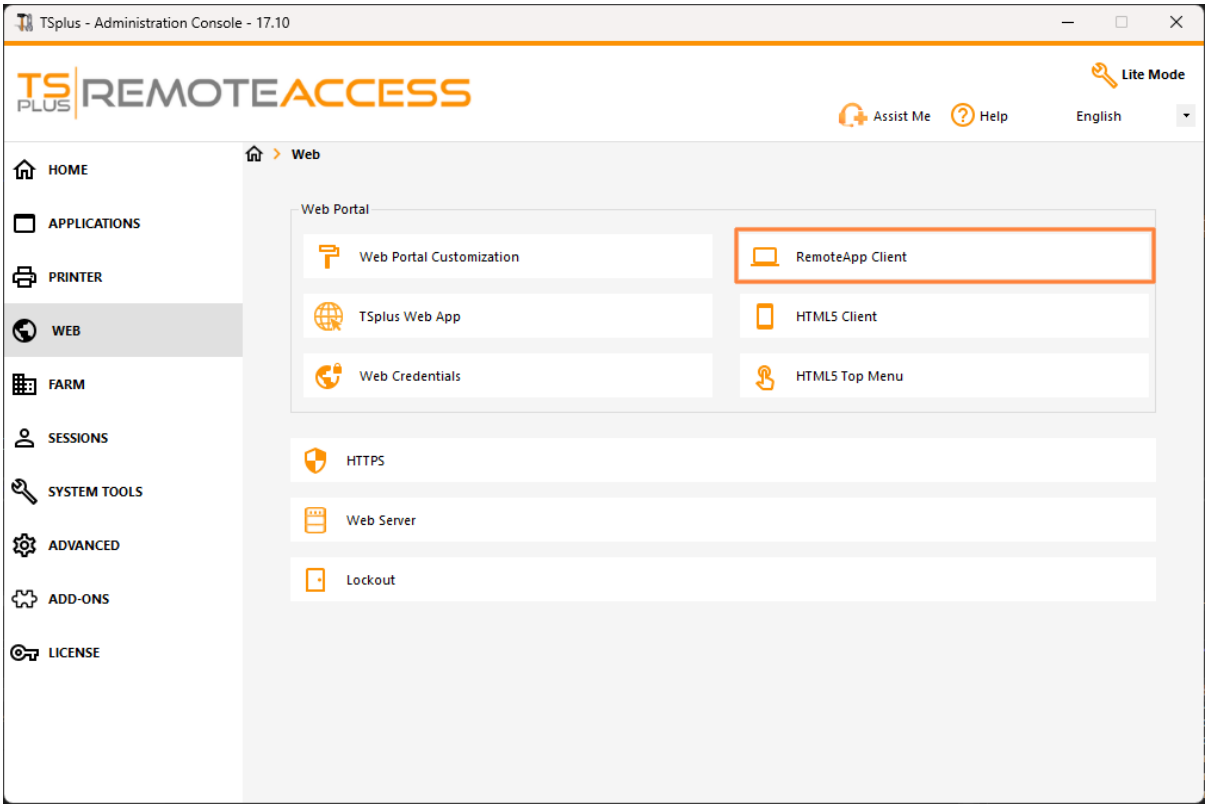
Dies ermöglicht eine perfekte Anwendungsanzeige sowie ein natives Windows-Verhalten.

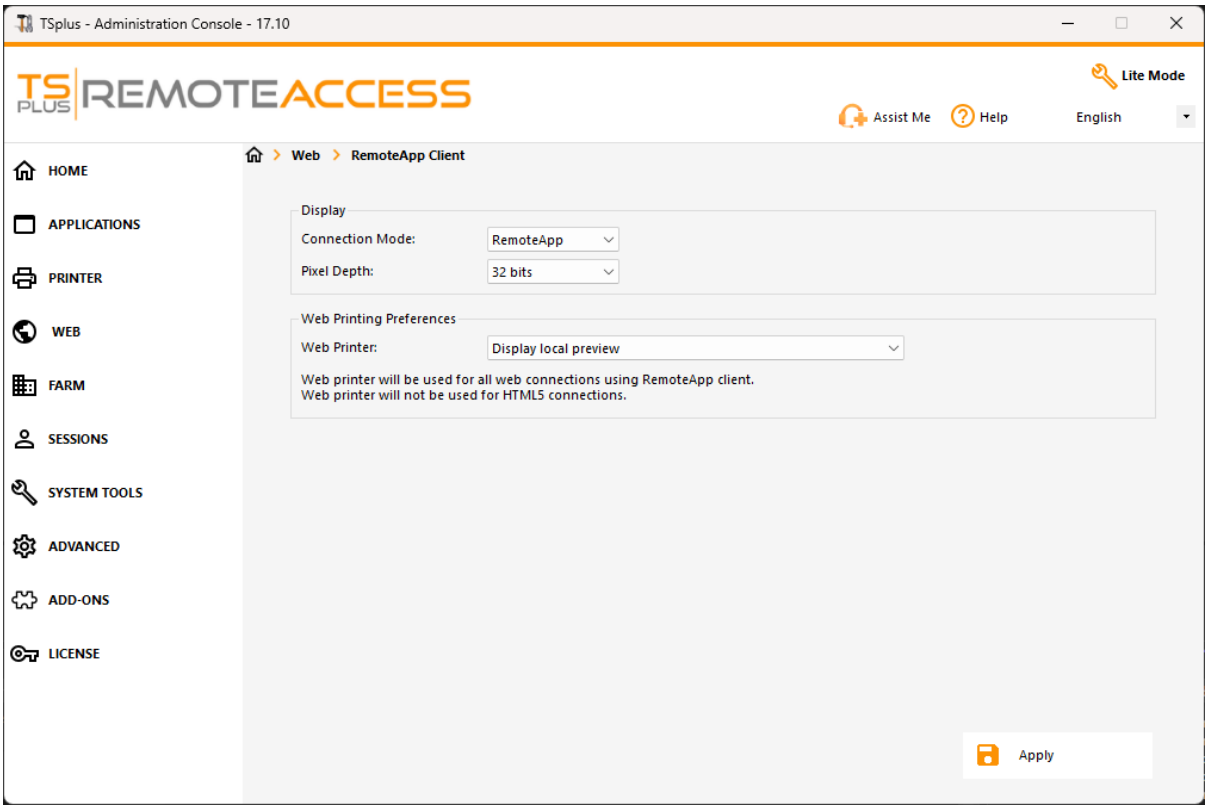
- Auf der Client-Seite ist die Installation von RDP6 oder höher erforderlich.

- Auf der Serverseite muss TSplus auf einem Computer installiert werden, der Windows 7 bis Windows Server 2019 ausführt.

Hinweis RemoteApp wird auf Windows 10 1803 und 1809 Home Windows 2019 Essentials Editions nicht unterstützt.

Sie können die Anzeige- und Druckeinstellungen des RemoteApp-Clients auf der Registerkarte Web des Admintools ändern:





Minimierte Anwendungen können direkt in der Windows-Taskleiste gefunden werden, wie eine lokale Anwendung.

In diesem Beispiel werden Firefox und Paint lokal gestartet; Notepad, Word und Foxit werden remote gestartet.



Für den Remoteapp-Verbindungsclient können Sie wählen, eine einzigartige Anwendung zu veröffentlichen, die nahtlos beim Anmelden des Benutzers gestartet wird. Sie können auch Anwendungen mit dem TSplus Remote Taskbar , das Floating Panel oder das Anwendungsfenster .

Windows-Client unter Proxy-Umgebung ausführen

In der Regel unterstützt das SSH-Paket HTTP(S)-Proxys, und dies sollte ausreichen, um die meisten bekannten Proxys zu überwinden.

Es gibt jedoch bestehende sehr schwierige Fälle, in denen die Proxy-Umgebung nicht richtig erkannt werden kann, von Drittanbieter-Software verborgen ist oder die Zielserver hinter Reverse-Proxys stehen.

Für solche schwierigen Fälle enthält die Software eine Non-SSH-Lösung namens „Rettungsmodus“.

Wenn Sie eine HTML5-Verbindung herstellen können, können Sie sicher sein, dass diese Software Ihnen hilft, native Socket-Verbindungen über Websocket (FF, Chrome, Opera, IE10 usw.) oder XHR (IE6-IE9) herzustellen.

Seien Sie vorsichtig, einige Proxys erlauben Websocket/XHR Traffic nur über die HTTPS-Schicht, verwenden Sie also die HTTPS-Adresse anstelle von HTTP.

Wenn der Proxy keine Proxy-Authentifizierung anfordert und Sie über den Browser auf Seiten zugreifen können:

1. Öffnen Sie http(s)://yourserver.com__/software/html5/jwres/__
2. Warten Sie auf eine erfolgreiche Verbindung (und autorisieren Sie die Java-Ausführung, falls gefragt)
3. Klicken Sie auf den roten Text „Link öffnen“, um die funktionierende Webzugangsseite zu öffnen.
4. Verwenden Sie den Windows-Client-Zugriff wie gewohnt

Wenn Proxy-Anfragen eine Proxy-Authentifizierung erfordern und Sie über den Browser auf Seiten zugreifen können:

1. Öffnen Sie http(s)://yourserver.com__/software/html5/jwres/__
2. Wenn der Proxy eine Authentifizierung für Java-Applets anfordert, drücken Sie „Abbrechen“.
3. Klicken Sie auf „Download LocalWebserver“ und führen Sie es nach dem erfolgreichen Download aus, um den lokalen HTTP-Server auf Port 18888 zu starten.
4. Klicken Sie auf „Applet-Zwangsladung von http://localhost:18888 ”, dies lädt die Seite neu

und lädt JARs von einem lokalen HTTP-Server.

5. Warten auf erfolgreiche Verbindung
6. Klicken Sie auf den roten Text „Link öffnen“, um die funktionierende Webzugangsseite zu öffnen.
7. Verwenden Sie den Windows-Client-Zugriff wie gewohnt

Sichern eines TSplus-Servers

Übersicht

Die Sicherung eines jeden Servers ist eine nie endende Geschichte, in der jeder Experte ein weiteres Kapitel hinzufügen könnte.

TSplus profitiert von und ist kompatibel mit der bestehenden Sicherheitsinfrastruktur in einem Unternehmen (Active Directory, GPOs, HTTPS-Server, SSL oder SSL-Telekommunikationssysteme, VPN, Zugangskontrolle mit oder ohne Ausweiskarten usw.).

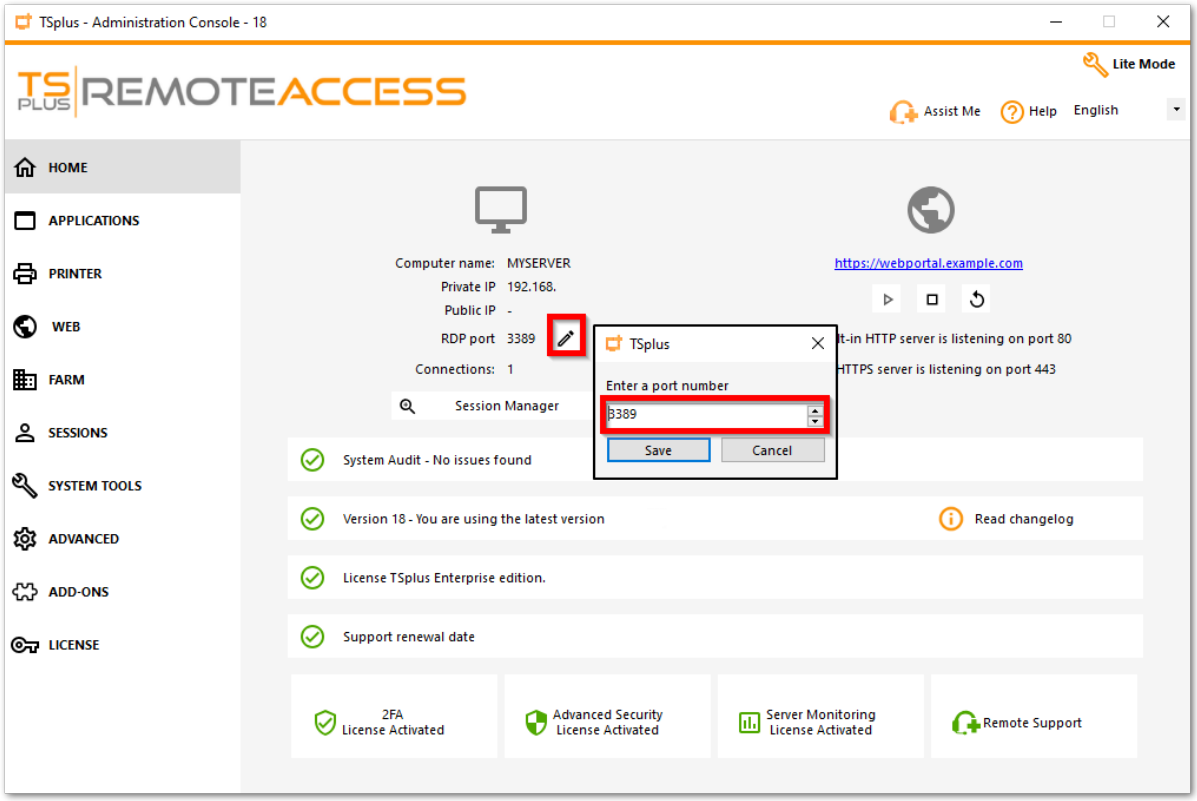
Für Kunden, die ihre Server einfach sichern möchten, bietet TSplus eine Reihe von einfachen und effektiven Möglichkeiten, um ein gutes Sicherheitsniveau durchzusetzen.

Mit dem AdminTool können Sie eine andere TCP/IP-Portnummer für den RDP-Dienst auswählen, um Verbindungen zu akzeptieren. Die Standardnummer ist 3389.

Sie können einen beliebigen beliebigen Port wählen, vorausgesetzt, dass er in Ihrem Netzwerk nicht bereits verwendet wird und dass Sie die gleiche Portnummer in Ihren Firewalls und in jedem TSplus-Benutzerzugangsprogramm festlegen.

TSplus bietet eine einzigartige Portweiterleitungs- und Tunnelungsfunktion: Unabhängig vom festgelegten RDP-Port ist das RDP auch über die HTTP- und HTTPS-Portnummer verfügbar!

Wenn Benutzer von außerhalb Ihres Netzwerks auf Ihren TSplus-Server zugreifen möchten, müssen Sie sicherstellen, dass alle eingehenden Verbindungen über den gewählten Port an den TSplus-Server weitergeleitet werden. Klicken Sie auf der Registerkarte "Start" auf die Stift-Schaltfläche neben dem "RDP-Port":



Ändern Sie den RDP-Port und speichern Sie.

Server-seitige Sicherheitsoptionen

Das AdminTool ermöglicht es Ihnen, den Zugriff für jeden Benutzer zu verweigern, der kein von dem Administrator generiertes TSplus-Verbindungsprogramm verwendet. In diesem Fall wird jeder Benutzer, der versucht, eine Sitzung mit einem anderen Remote Desktop-Client als dem TSplus-Client zu öffnen (vorausgesetzt, er hat die richtige Serveradresse, die Portnummer, ein gültiges Anmeldekonto und ein gültiges Passwort), automatisch getrennt.

Der Administrator kann entscheiden, dass nur Mitglieder der Remote Desktop-Benutzergruppe wird erlaubt sein, eine Sitzung zu öffnen.

Der Administrator kann entscheiden, dass ein Passwort erforderlich ist, um eine Sitzung zu öffnen.

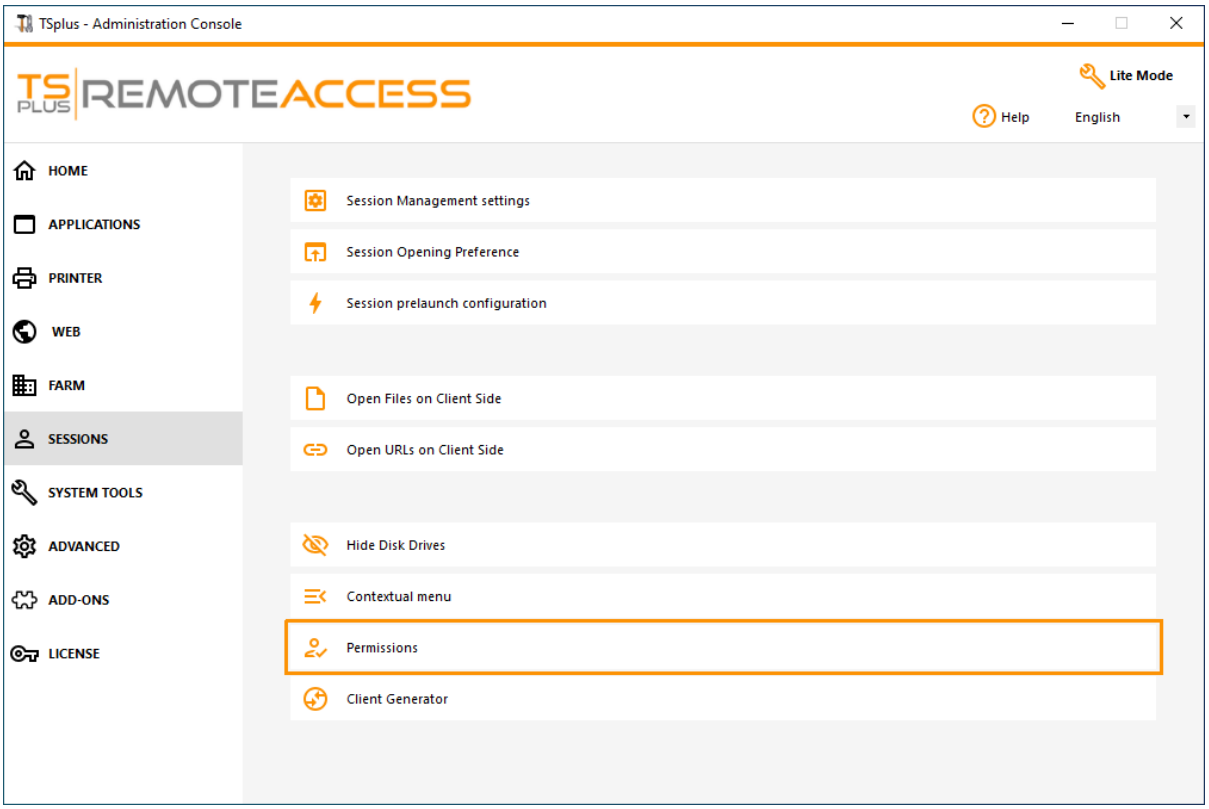
Durch die Festlegung der anwendbaren lokalen Gruppenrichtlinie kann der Administrator angeben, ob ein Verschlüsselungsniveau für alle Daten, die während einer Terminaldienste-Sitzung zwischen dem Client und dem Remote-Computer gesendet werden, durchgesetzt werden soll.

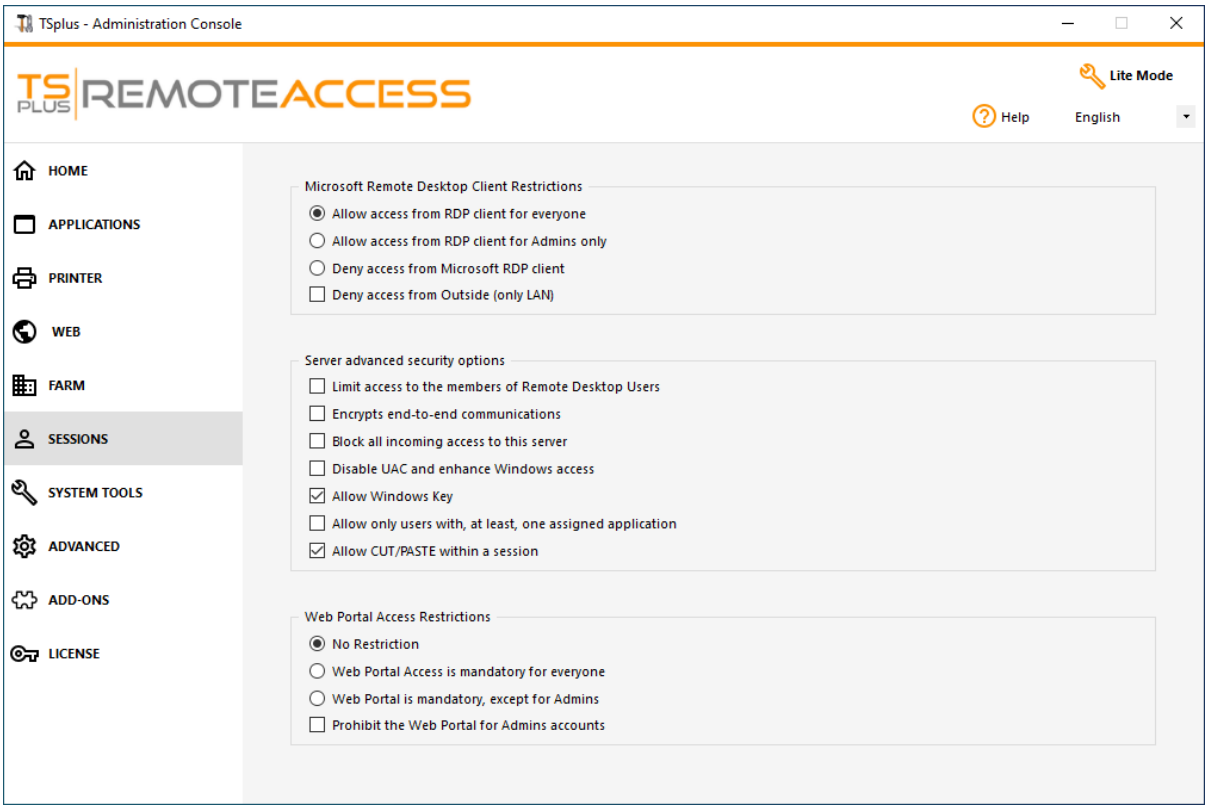
Wenn der Status auf Aktiviert gesetzt ist, wird die Verschlüsselung für alle Verbindungen zum Server auf das vom Administrator festgelegte Niveau eingestellt. Standardmäßig ist die Verschlüsselung auf Hoch eingestellt.

Der Administrator kann auch als Regel festlegen, dass nur Benutzer mit einem TSplus-Verbindungsclient eine Sitzung öffnen können.

Jeder eingehende Zugriff mit einem standardmäßigen RDP oder einem Webzugriff wird automatisch abgelehnt.

Sie finden mehrere Optionen für erweiterte Sicherheit, wenn Sie auf die Registerkarte Sitzungen - Berechtigungen klicken:





- **Zugriff vom Microsoft RDP-Client für alle erlauben:** Erlaubt jedem Benutzer, sich mit mstsc.exe zu verbinden.
- **Zugriff nur für Administratoren vom Microsoft RDP-Client erlauben:** Erlaubt nur Administratoren, sich mit mstsc.exe zu verbinden.
- **Zugriff vom Microsoft RDP-Client verweigern:** Verhindern Sie, dass sich jemand mit mstsc.exe verbinden kann.
- **Zugriff von außen verweigern:** Es bedeutet, dass nur private IPs aus dem LAN eine Sitzung öffnen können.
- **Zugriff auf die Mitglieder der Remote Desktop-Benutzer beschränken:** Dieses Limit gilt nur für diese lokale Gruppe von Benutzern (die Sie sehen können, indem Sie auf die Benutzer und Gruppen-Kachel .
- **Verschlüsselt die End-to-End-Kommunikation:** Hochgradig verschlüsselt die Kommunikation zwischen Client und Server mit 128-Bit-Verschlüsselung. Verwenden Sie dieses Niveau, wenn die Clients, die auf den Terminalserver zugreifen, ebenfalls 128-Bit-Verschlüsselung unterstützen.
- **Blockieren Sie den gesamten eingehenden Zugriff auf diesen Server:** Alle aktiven Sitzungen bleiben aktiv, während alle eingehenden Verbindungsversuche blockiert werden. Stellen Sie sicher, dass Sie physisch auf die Konsole des Servers zugreifen können, wenn Sie dieses Kästchen aktivieren. Verwenden Sie diese Option nicht, wenn Ihr Server in einer Cloud-Umgebung gehostet wird.
- **Deaktivieren Sie UAC und verbessern Sie den Windows-Zugriff:** Deaktiviert die Benutzerkontensteuerung, entfernt alle unerwünschten Sicherheits-Pop-ups von Windows. Benutzerbeschränkung (Nachrichten) beim Starten von Anwendungen.
- **Das Kontrollkästchen „Windows-Taste erlauben“** Erlauben Sie die Verwendung der Windows-Tasten und -Kombinationen innerhalb einer TSplus-Sitzung.
- **Erlauben Sie nur Benutzern mit mindestens einer zugewiesenen Anwendung:** Benutzer

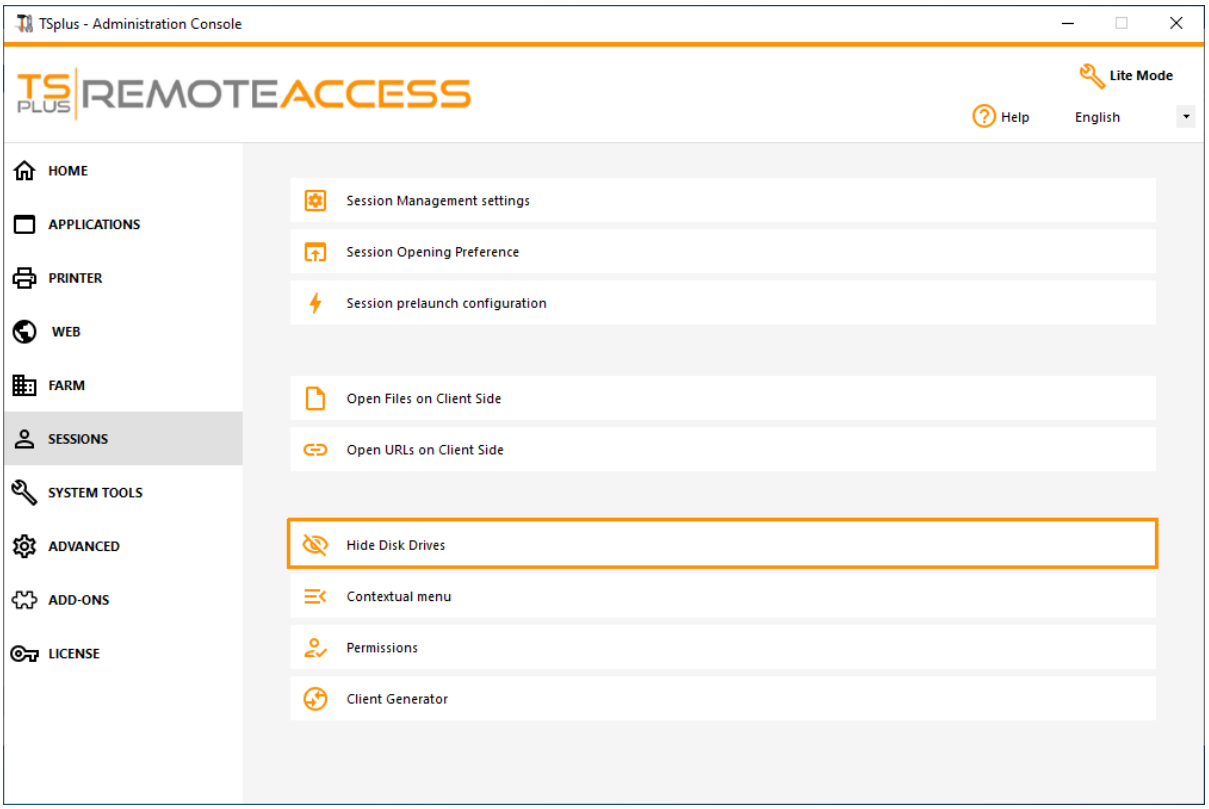
mit einer Anwendung und mehr dürfen eine Sitzung öffnen.

- **Erlauben Sie CUT/PASTE innerhalb einer Sitzung:** Das Deaktivieren dieses Kästchens wird die CTRL C/CTRL V-Befehle deaktivieren.

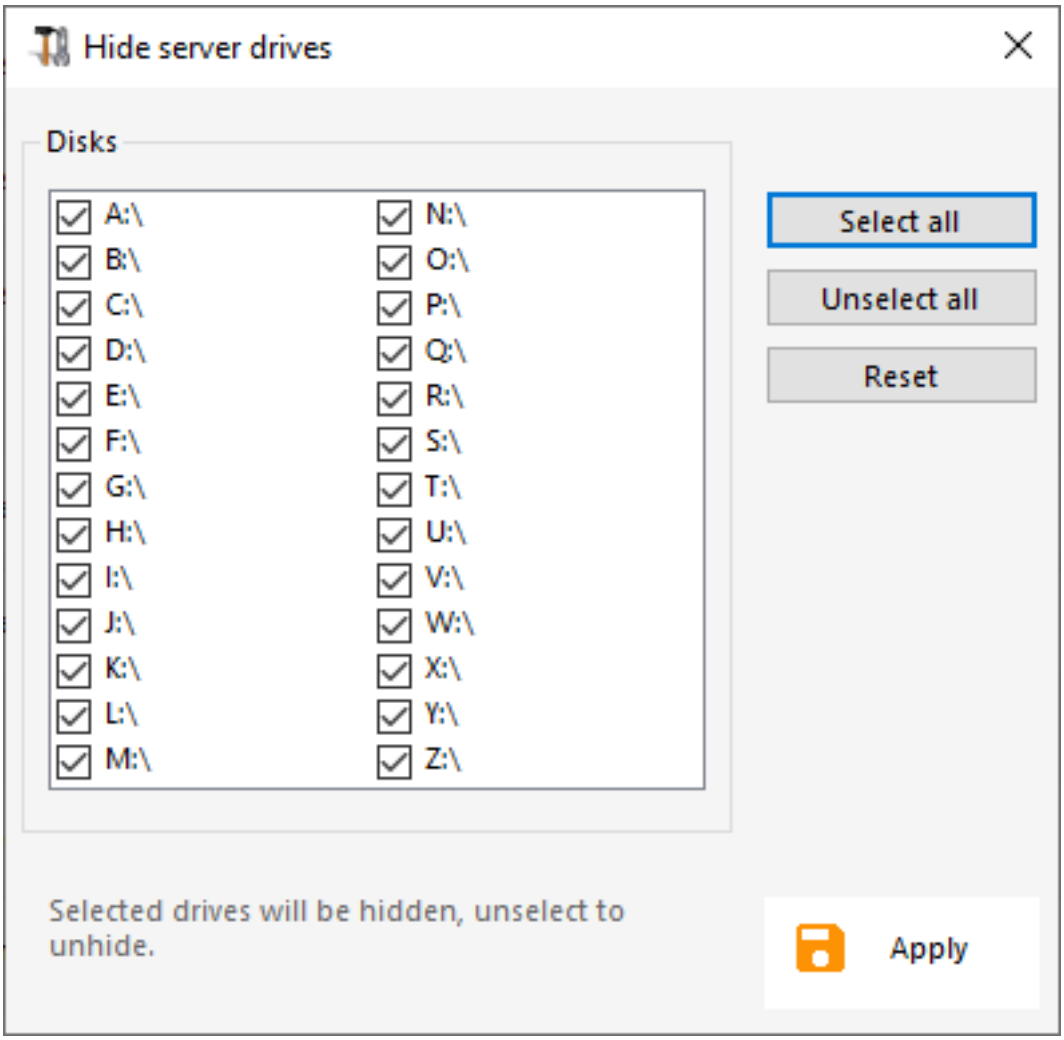
Zugriffsrestriktionen für das Webportal

- Keine Einschränkung
- Webportal ist für alle verpflichtend: Benutzer können sich nur über das Webportal verbinden.
- Webportal ist obligatorisch, außer für Administratoren: Benutzer können nur über das Webportal eine Verbindung herstellen, außer Administratoren.
- Webportal für Administratorkonten verbieten: Administratoren können sich nicht über das Webportal verbinden.

Das AdminTool enthält ein Werkzeug, das das Verstecken der Serverlaufwerke ermöglicht, um zu verhindern, dass Benutzer über "Mein Computer" oder die standardmäßigen Windows-Dialogfelder auf Ordner zugreifen. Klicken Sie auf der Registerkarte "Sitzungen" auf "Laufwerke ausblenden".



Dieses Tool funktioniert global. Das bedeutet, dass selbst der Administrator nach Anwendung der Einstellungen keinen normalen Zugriff auf Laufwerke hat. Im folgenden Beispiel wurden alle Treiber mit der Schaltfläche „alle auswählen“ ausgewählt, die alle Kästchen entsprechend den Laufwerken aktiviert, die für alle verborgen werden.



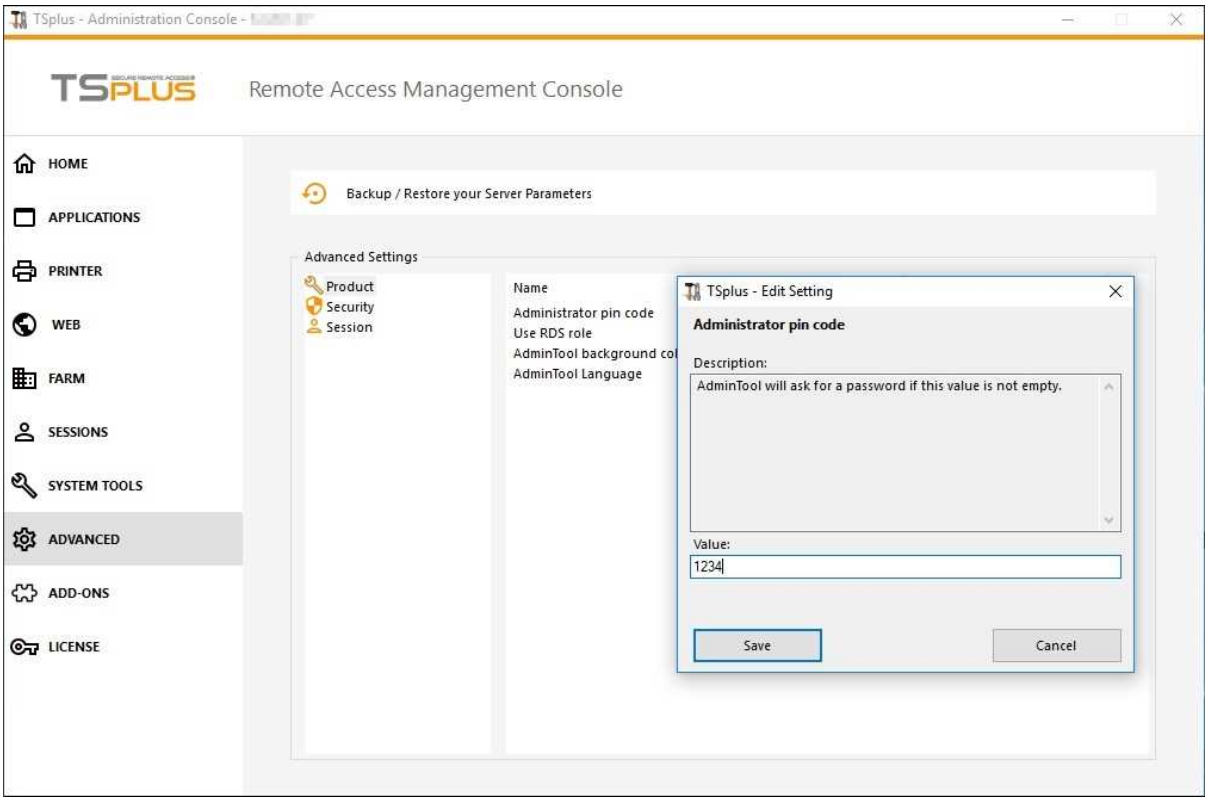
Hinweise: Diese Funktionalität ist leistungsstark und deaktiviert nicht den Zugriff auf die Festplatten. Sie verhindert lediglich, dass der Benutzer sie anzeigt.

Das Tool kennzeichnet die Festplattenlaufwerke als verborgen, fügt jedoch auch die EIGENSCHAFT VERBORGEN zu den gesamten Stammordnern und der Benutzerliste in Dokumente und Einstellungen hinzu.

Wenn der Administrator diese Dateien sehen möchte, muss er:

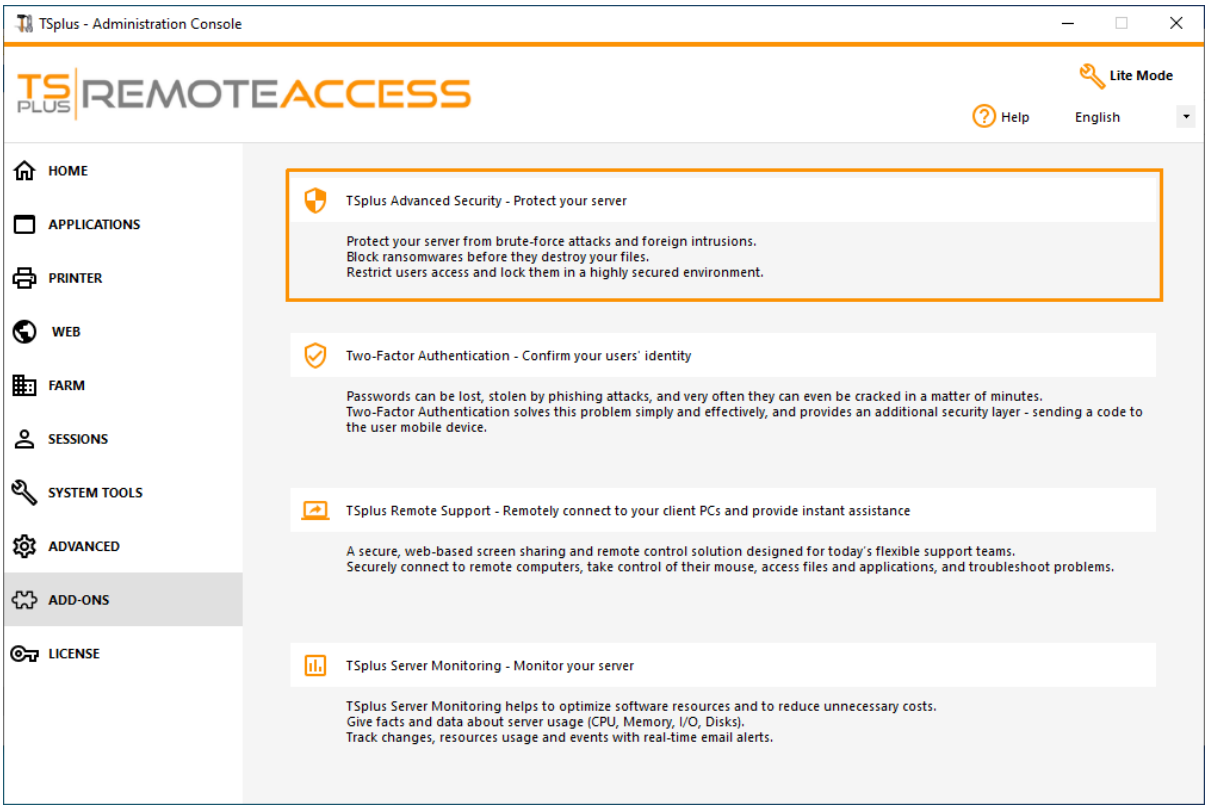
1. Geben Sie den Laufwerksbuchstaben ein. Zum Beispiel: **D:** was Sie zum D: Laufwerk führen wird.
2. Einschalten **VERSTECKTE DATEIEN UND ORDNER ANZEIGEN** in den Eigenschaften der Ordneransicht.

Der Administrator kann den Zugriff auf das Administrator-Tool sichern, indem er einen PIN-Code festlegt, der bei jedem Start abgefragt wird, im Reiter "Erweitert" des AdminTools, unter den Produkteinstellungen:

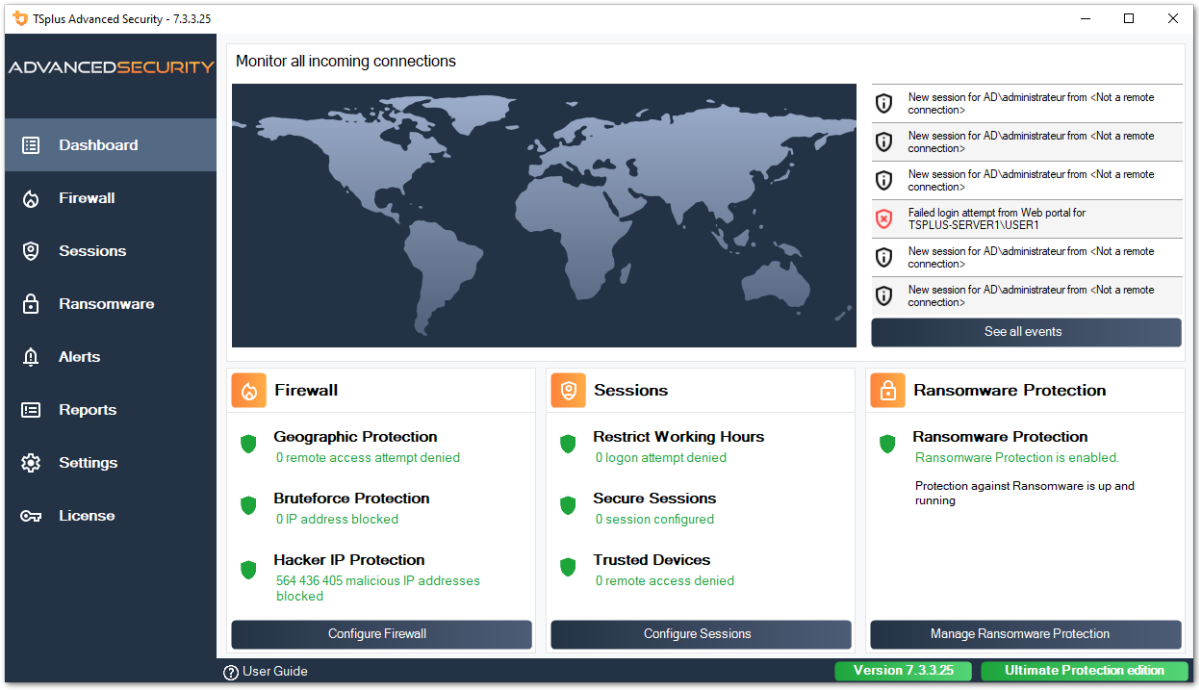


TSplus Advanced Security Ultimate

Seit der Version TSplus 11.40 finden Sie ein einzigartiges Sicherheits-Add-on-Tool, das Sie im Tab Add-Ons starten können:



Was leistungsstarke Funktionen mit sich bringt, dokumentiert auf diese Seite .



Die Rolle des Bruteforce Protection im Webportal wird beschrieben unter diese Seite .

Zwei-Faktor-Authentifizierung

Seit der Version TSplus 12 können Sie die Zwei-Faktor-Authentifizierung als Add-On für Ihr TSplus Web-Portal aktivieren.



Weitere Informationen zu diesem erstaunlichen neuen Feature finden Sie auf diese Seite .

SSL-Zertifikate

SSL-Zertifikate werden auf diesen Seiten im Detail behandelt:

- TSplus bietet ein benutzerfreundliches Tool zur Erstellung eines kostenlosen und gültigen SSL-Zertifikats an: Kostenloses und einfach zu installierendes SSL-Zertifikat
- HTTPS & SSL-Drittanbieterzertifikate .

- Wählen Sie Ihr Cipher-Suiten zur Verbesserung der Sicherheit .

TSplus Zugriffsprogramm Sicherheitsoptionen:

Der TSplus-Client-Generator bietet die Möglichkeit, auf seiner Registerkarte Sicherheit den TSplus-Client zu sperren auf:

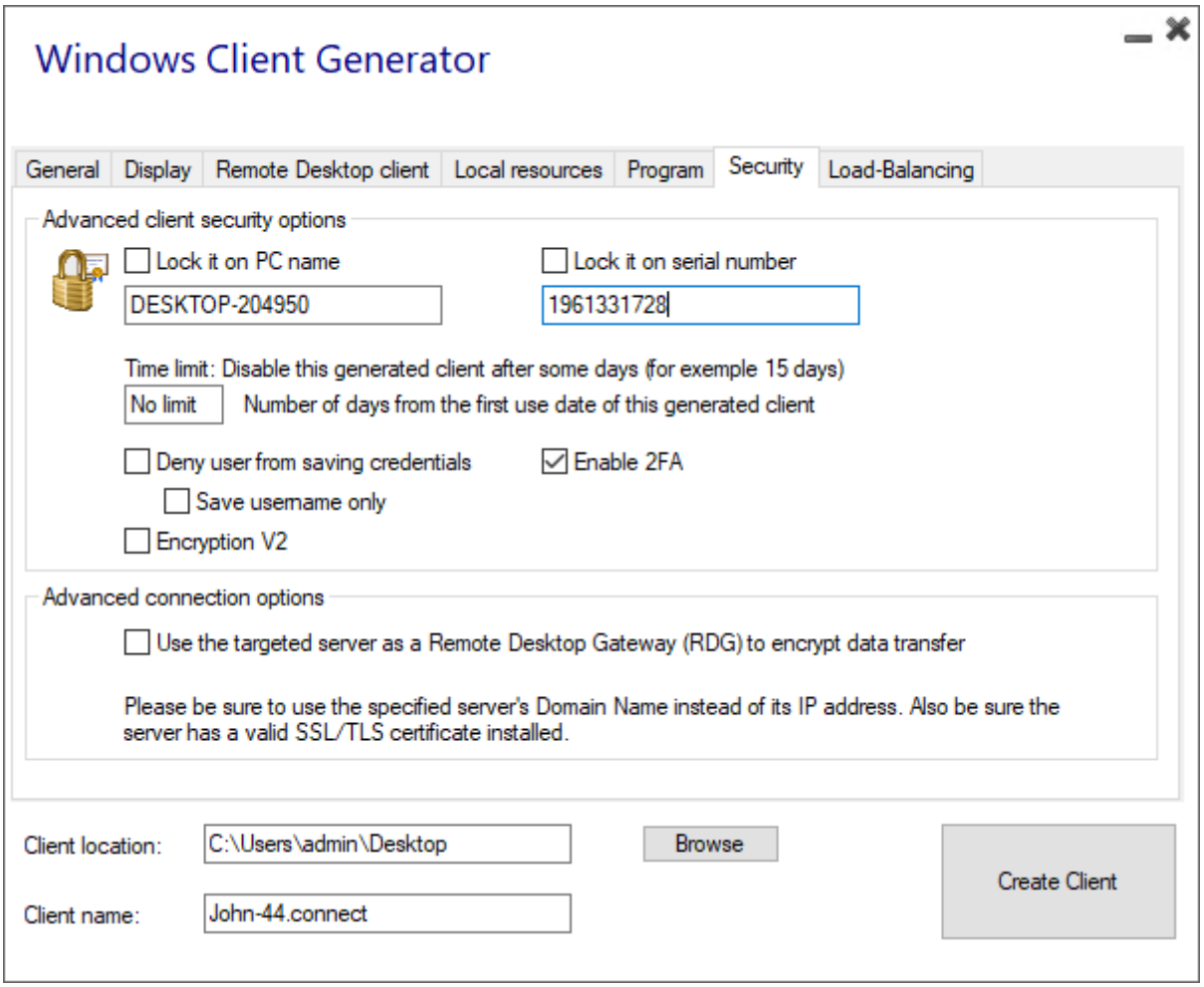
- Ein spezifischer PC-Name. Das bedeutet, dass dieses Programm von keinem anderen PC aus gestartet werden kann.

- Eine physische Laufwerksseriennummer (PC HDD oder USB-Stick). Dies ist eine sehr einfache und leistungsstarke Möglichkeit, ein hohes Maß an Sicherheit zu gewährleisten.

  Der einzige Weg, sich zu verbinden, ist mit einem bestimmten Client, und dieser bestimmte Client kann nur von einem bestimmten USB-Stick oder PC-HDD gestartet werden.

  Einige unserer Kunden liefern USB-Sticks mit Fingerabdrucklesern an jeden ihrer Benutzer, und jedes generierte Programm ist an die Seriennummer des Geräts gebunden.

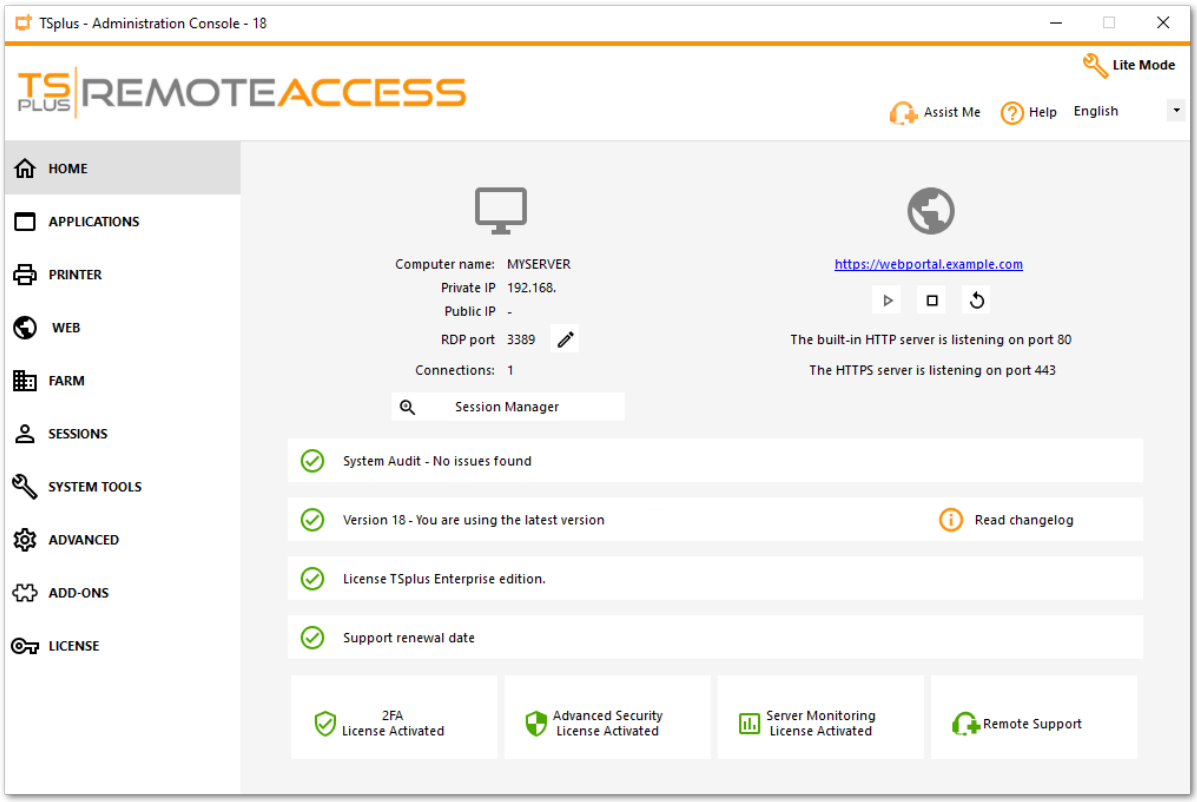
  Auf diese Weise können sie den Zugriff auf das Programm des Kunden selbst einschränken und gleichzeitig sicherstellen, dass es nicht vom USB-Stick kopiert und anderswo verwendet werden kann.



Für weitere Informationen zu Sicherheitsfunktionen, überprüfen Sie TSplus Portable Client Generator Dokumentation und unsere FAQ.

Serververwaltung

Auf der Registerkarte "Start" des AdminTools können Sie alle benötigten Informationen zu Ihrem TSplus-Server einsehen:



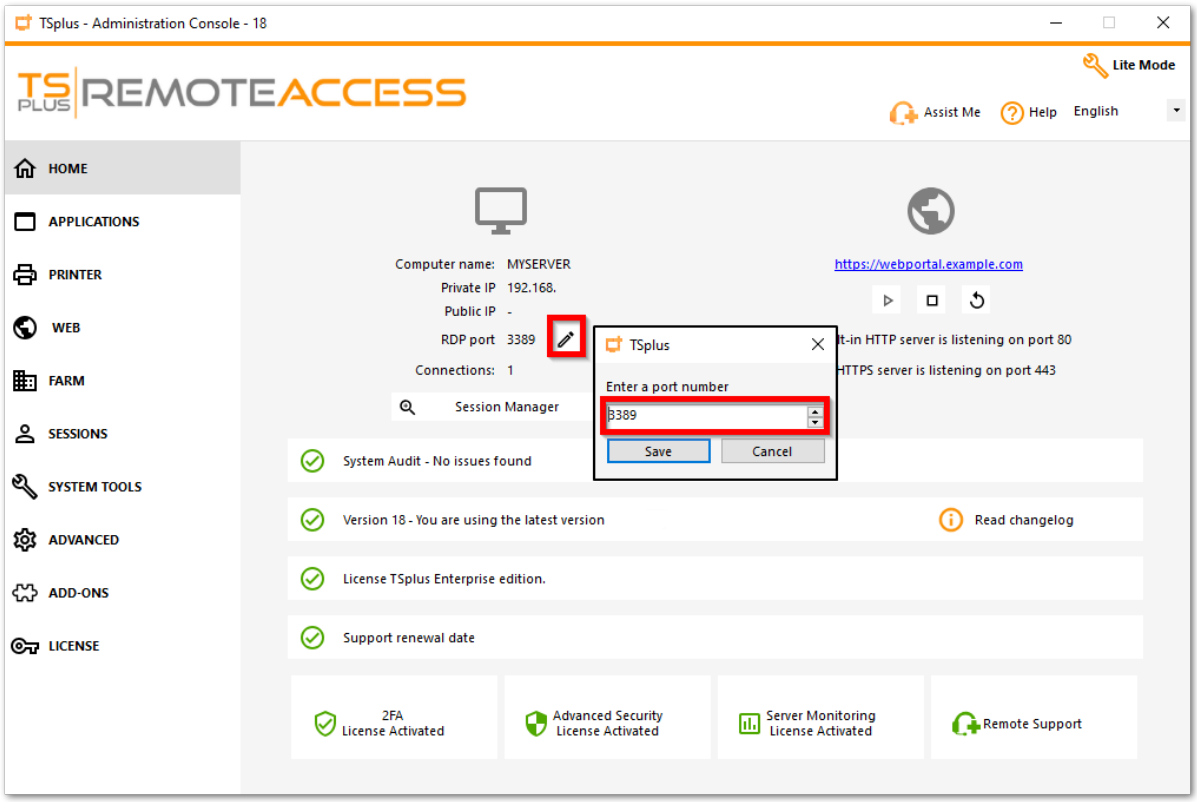
Ändern der RDP-Portnummer und Einrichten der Firewall

Mit dem AdminTool können Sie eine andere TCP/IP-Portnummer auswählen, die der RDP-Dienst für eingehende Verbindungen akzeptieren soll. Die Standardnummer ist 3389. Sie können jeden beliebigen Port wählen, vorausgesetzt, er wird nicht bereits in Ihrem Netzwerk verwendet und Sie stellen die gleiche Portnummer in Ihren Firewalls und in jedem TSplus-Benutzerzugangsprogramm ein.

TSplus bietet eine einzigartige Portweiterleitungs- und Tunnelungsfunktion: Unabhängig vom

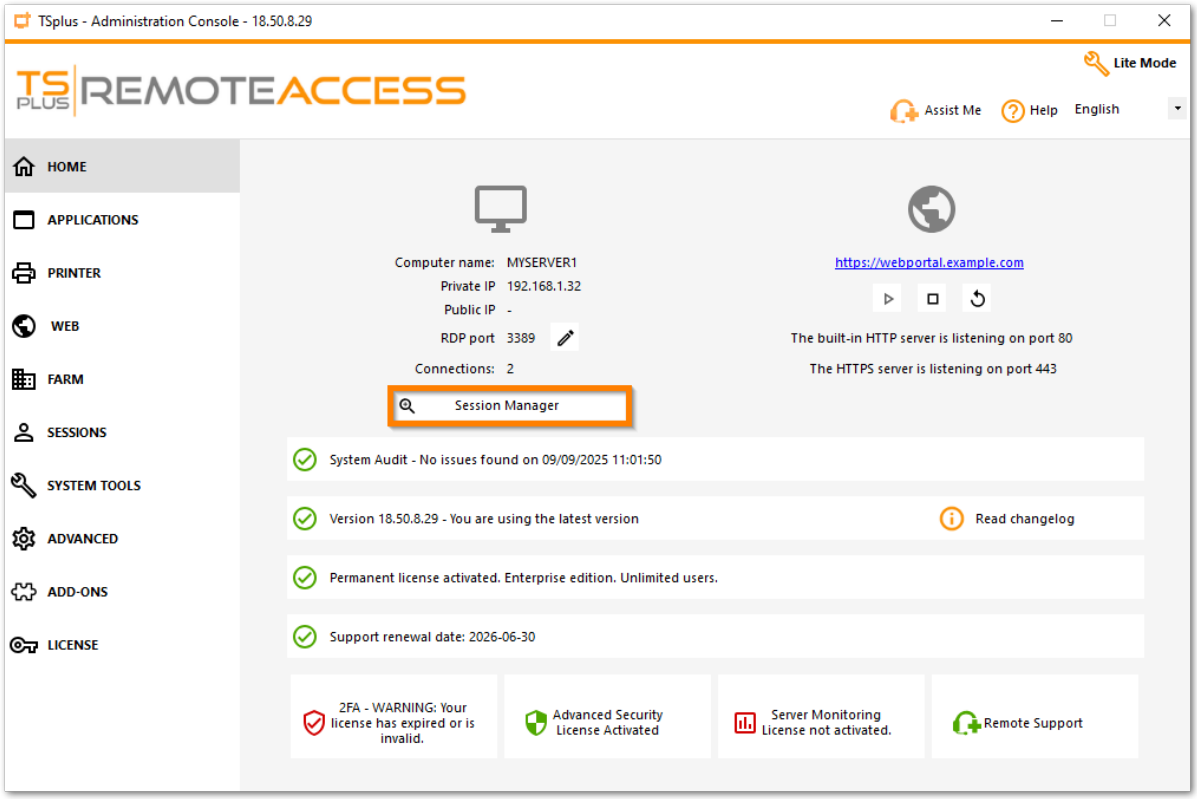
festgelegten RDP-Port ist das RDP auch über die HTTP- und HTTPS-Portnummer verfügbar!

Wenn Benutzer von außerhalb Ihres Netzwerks auf Ihren TSplus-Server zugreifen möchten, müssen Sie sicherstellen, dass alle eingehenden Verbindungen über den gewählten Port an den TSplus-Server weitergeleitet werden.

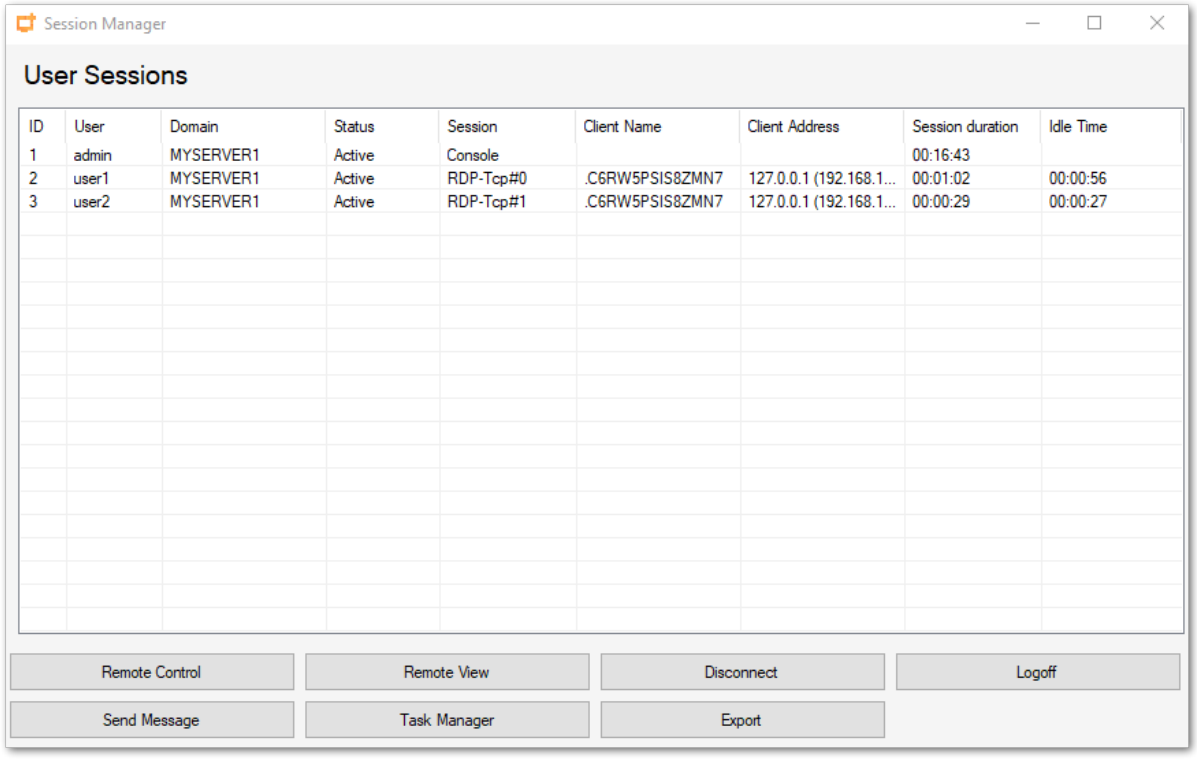


Verwaltung von Benutzern und Sitzungen

Der Sitzungsmanager befindet sich direkt unter dem RDP-Port:



Sie können den Task-Manager Ihres Servers anzeigen und haben die Möglichkeiten, eine Fernsteuerung zu aktivieren, sich zu trennen, sich abzumelden oder eine Nachricht an Ihre Benutzer zu senden.



Sie können die Fernsteuerung über eine Remote-Sitzung mit einem Administratorkonto auf den

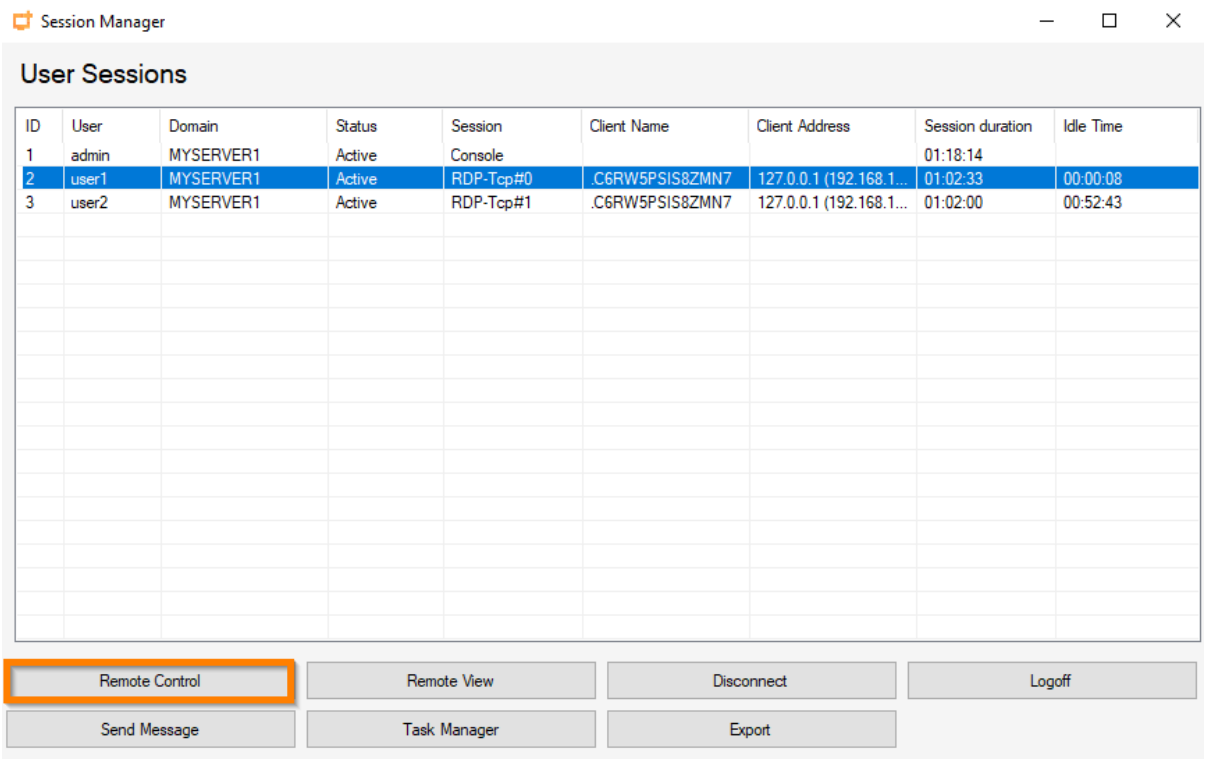
folgenden Betriebssystemen aktivieren:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7
- Windows 8.1
- Windows 10 Pro und höher

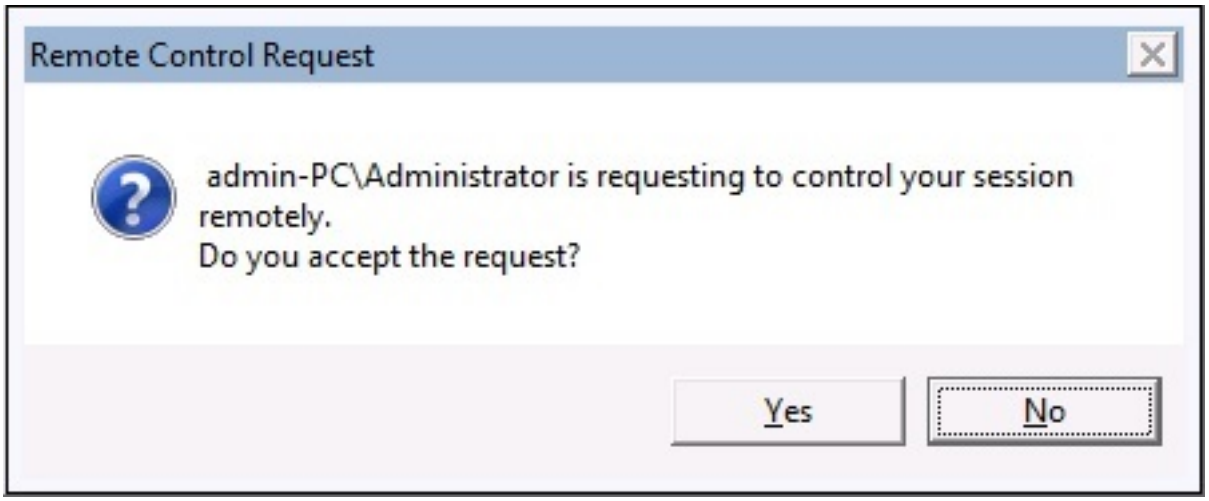
Auf Windows XP, 2003, Vista und 2008 gibt es keinen Fernsteuerungsbutton.

Unter Windows 2012 und 8 erscheint eine Nachricht, die Sie auffordert, auf 2012 R2 oder 8.1 zu aktualisieren.

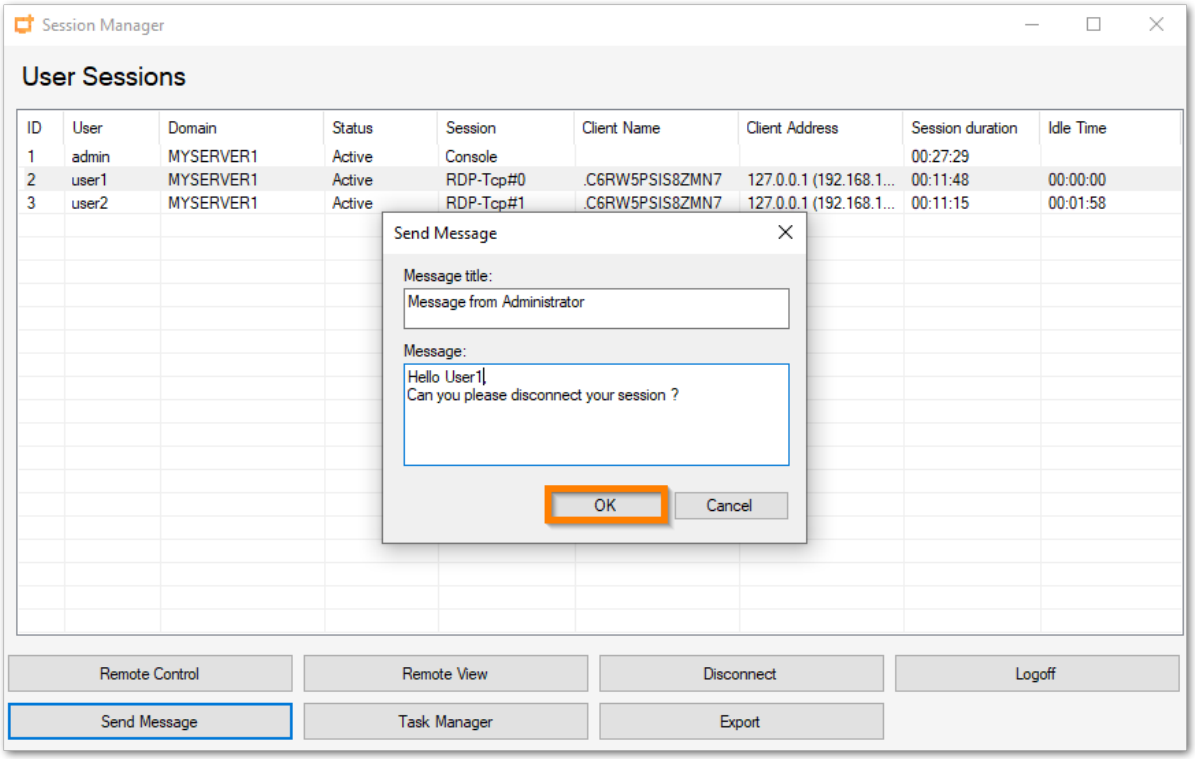
Wenn Sie die Fernsteuerung für die Sitzung eines Benutzers aktivieren, erscheint diese Nachricht, die die Tastenkombination zum Beenden der Sitzung angibt:



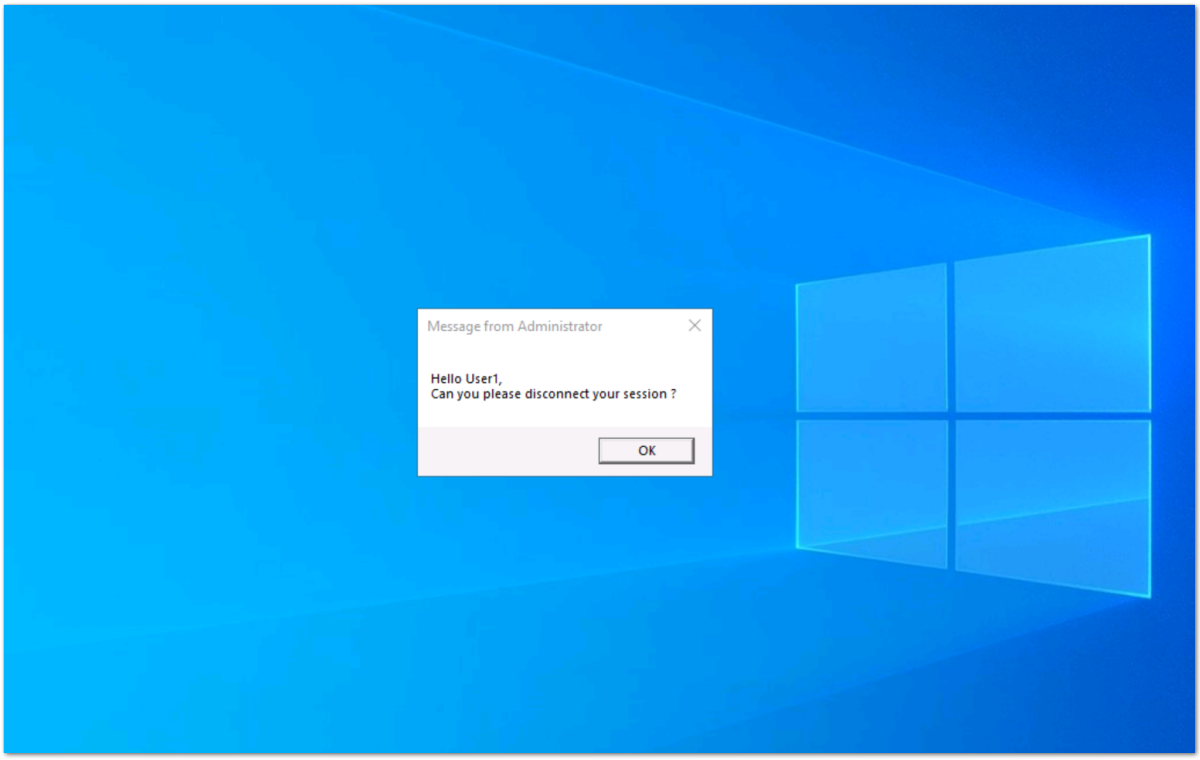
Auf der Client-Seite erscheint diese Nachricht, um die Fernsteuerung zu akzeptieren:



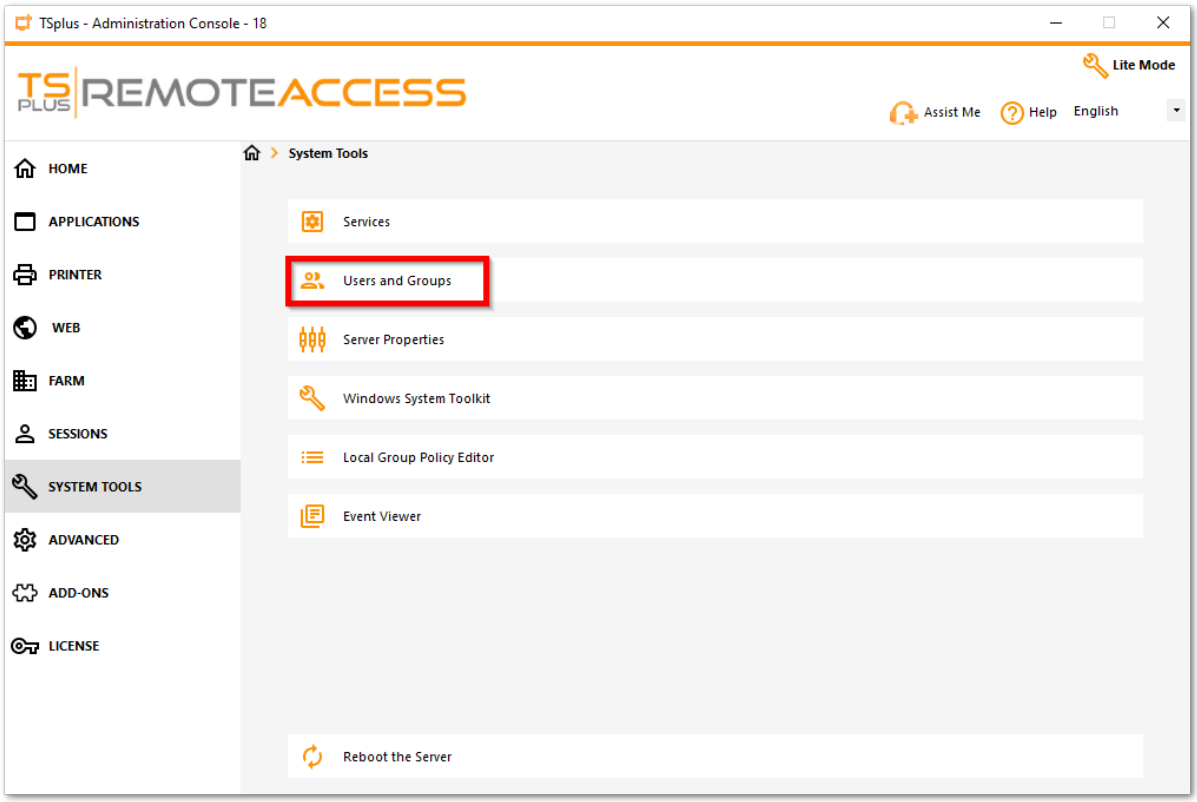
Sie können auch eine Nachricht an Ihren Benutzer senden:



Nachricht auf der Serverseite gesendet



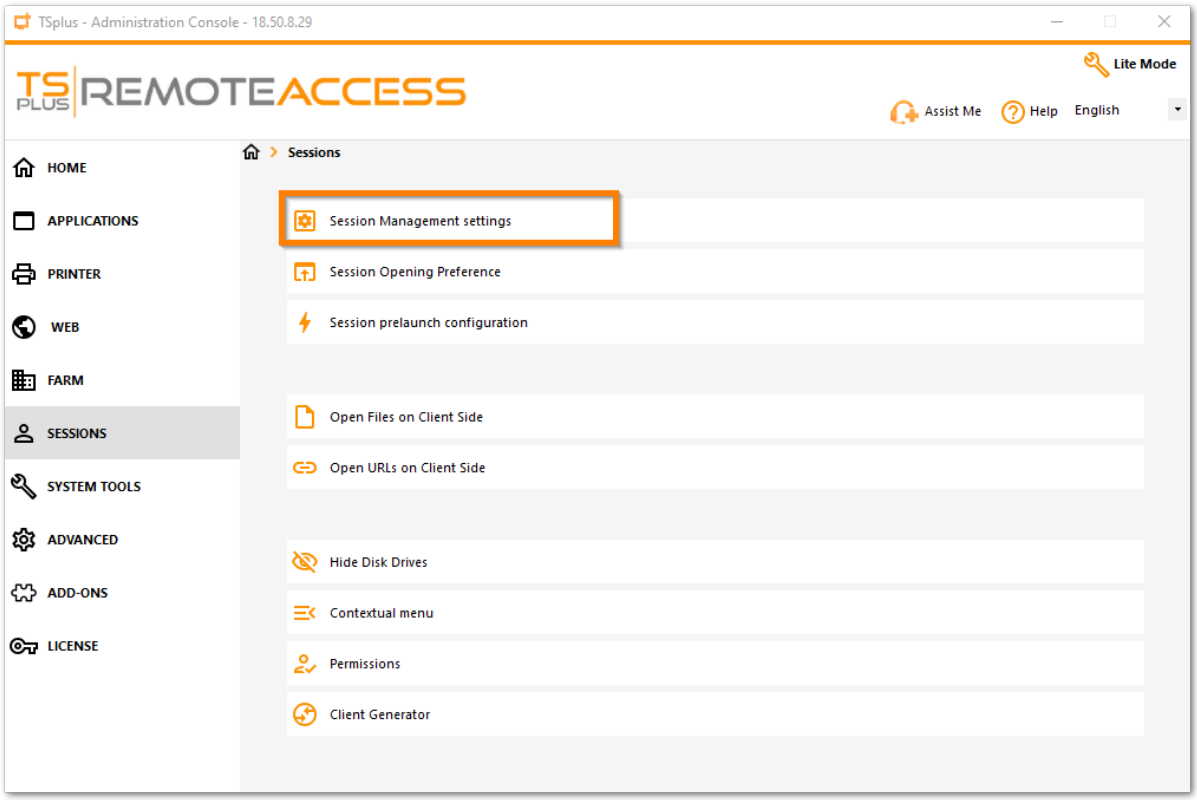
Nachricht, die auf der Client-Seite erscheint

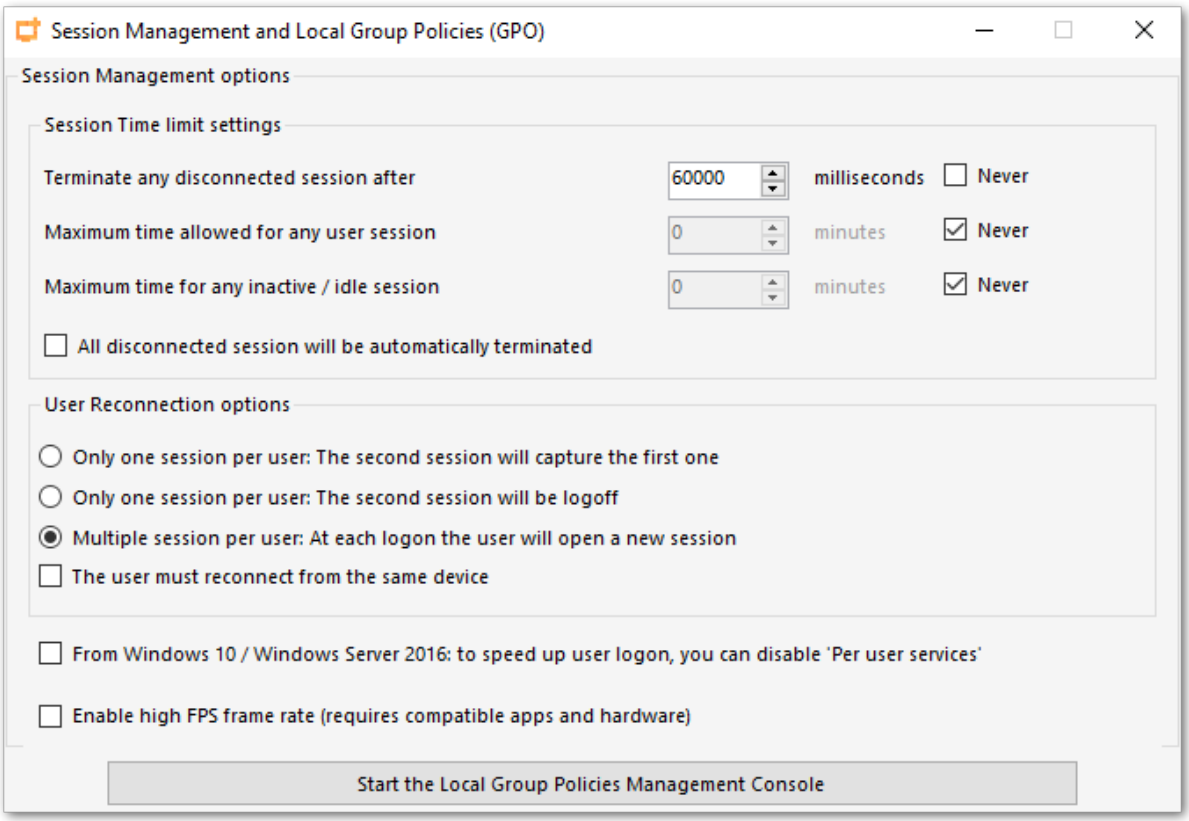


Siehe diese Dokumentation für weitere Informationen.

- Mit dem Tab "Sitzungsverwaltungseinstellungen (GPO)" können Sie verschiedene

Verbindungseinstellungen für jede Sitzung und jeden Benutzer festlegen:



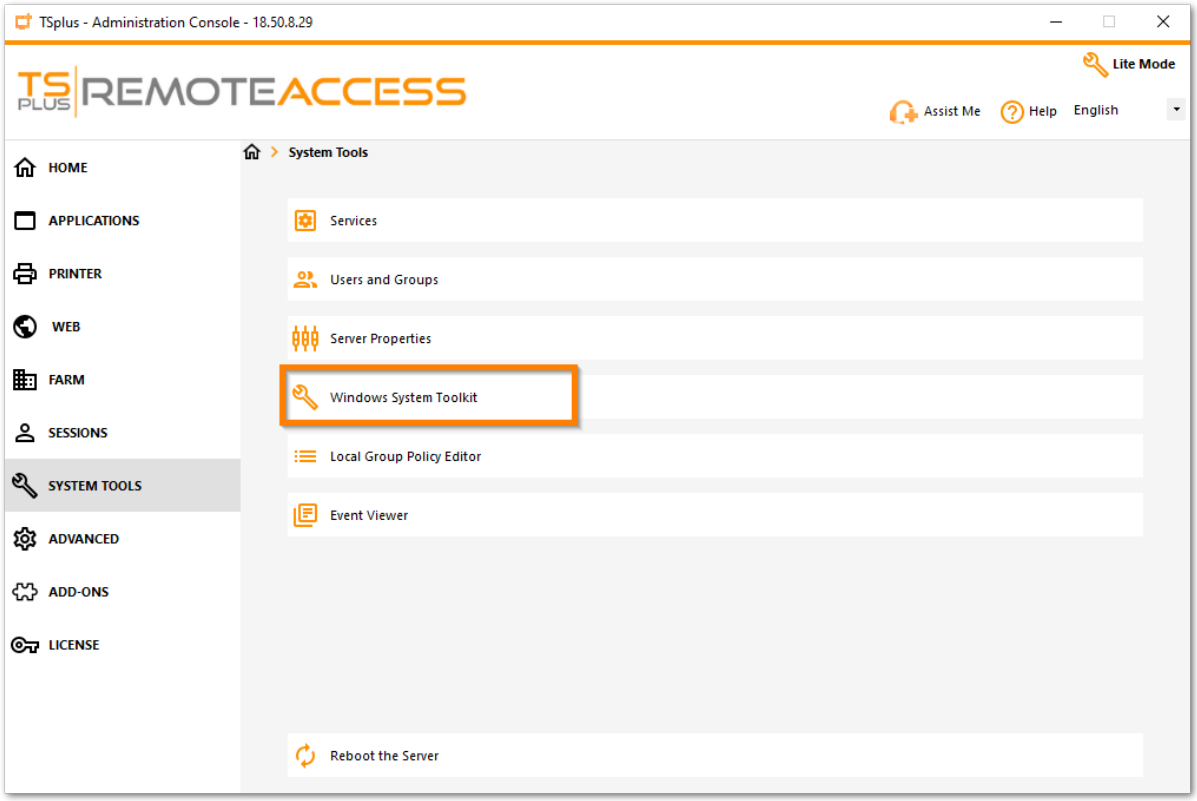


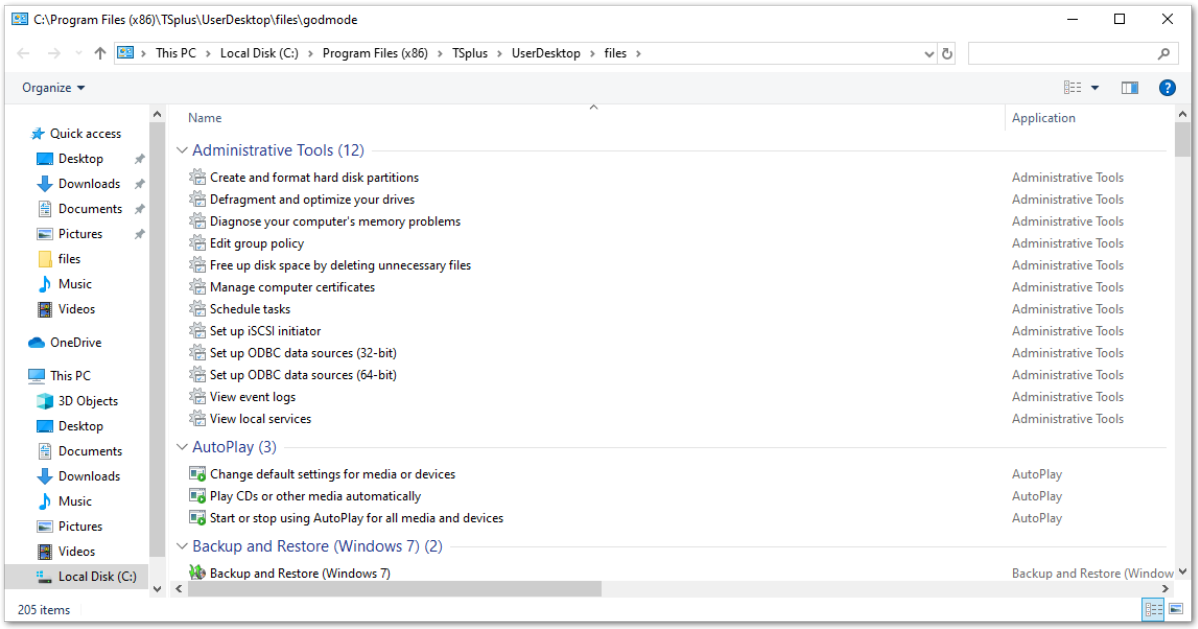
Windows Server 2016 führte einen neuen „Pro-Benutzer-Dienst“ ein, der es den Diensten

ermöglicht, alle Prozesse pro Benutzer zu starten, was die Anmeldezeiten der Benutzer verlangsamt.

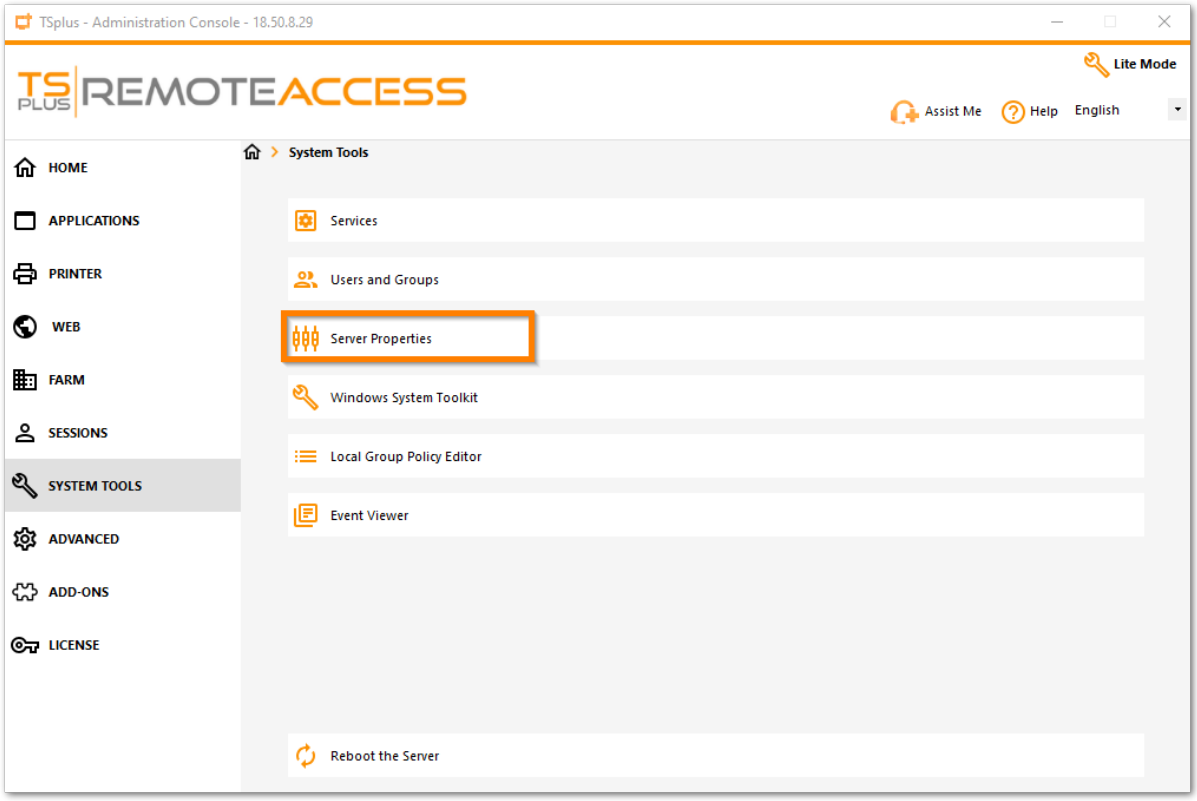
Seit der Veröffentlichung von TSplus 11.70 können Sie **Benutzerbezogene Dienste deaktivieren, um die Anmeldungen der Benutzer zu beschleunigen.** .

- Das Windows Toolkit ist ein erweitertes Steuerfeld, das alle Windows-Administrationswerkzeuge zusammenfasst.

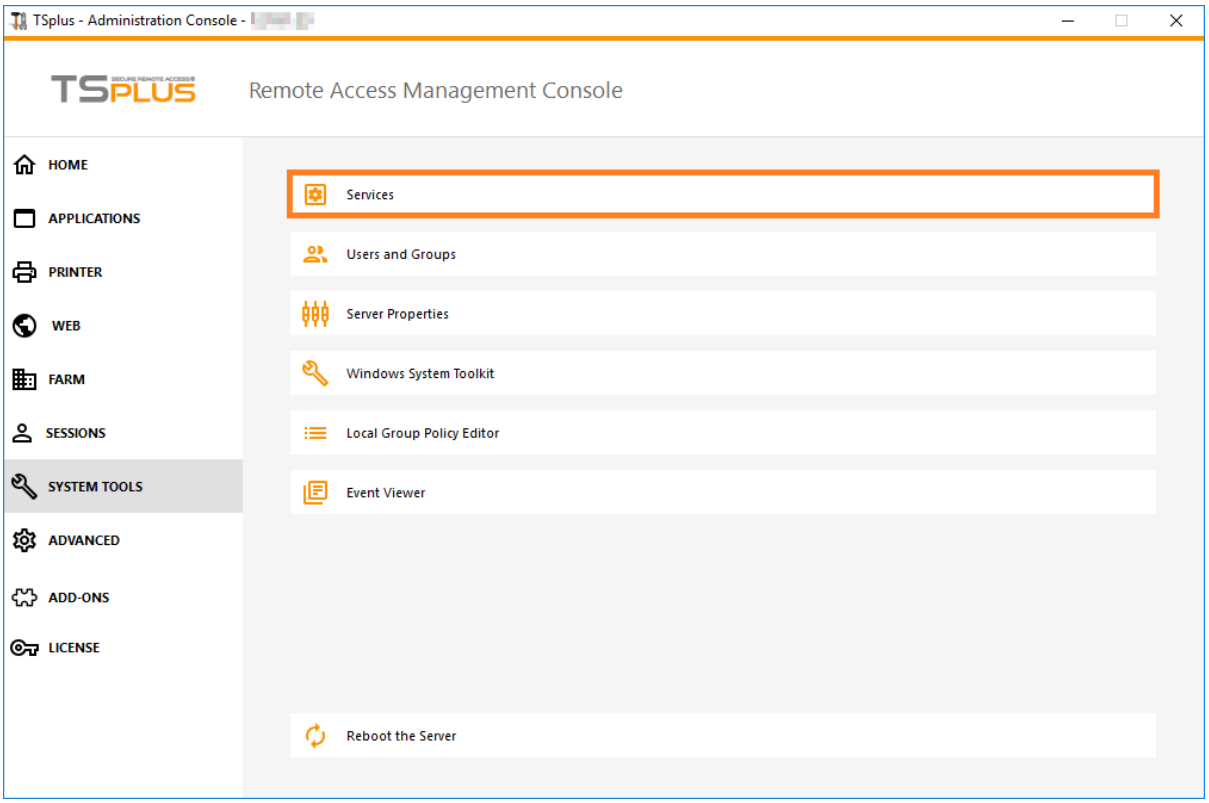




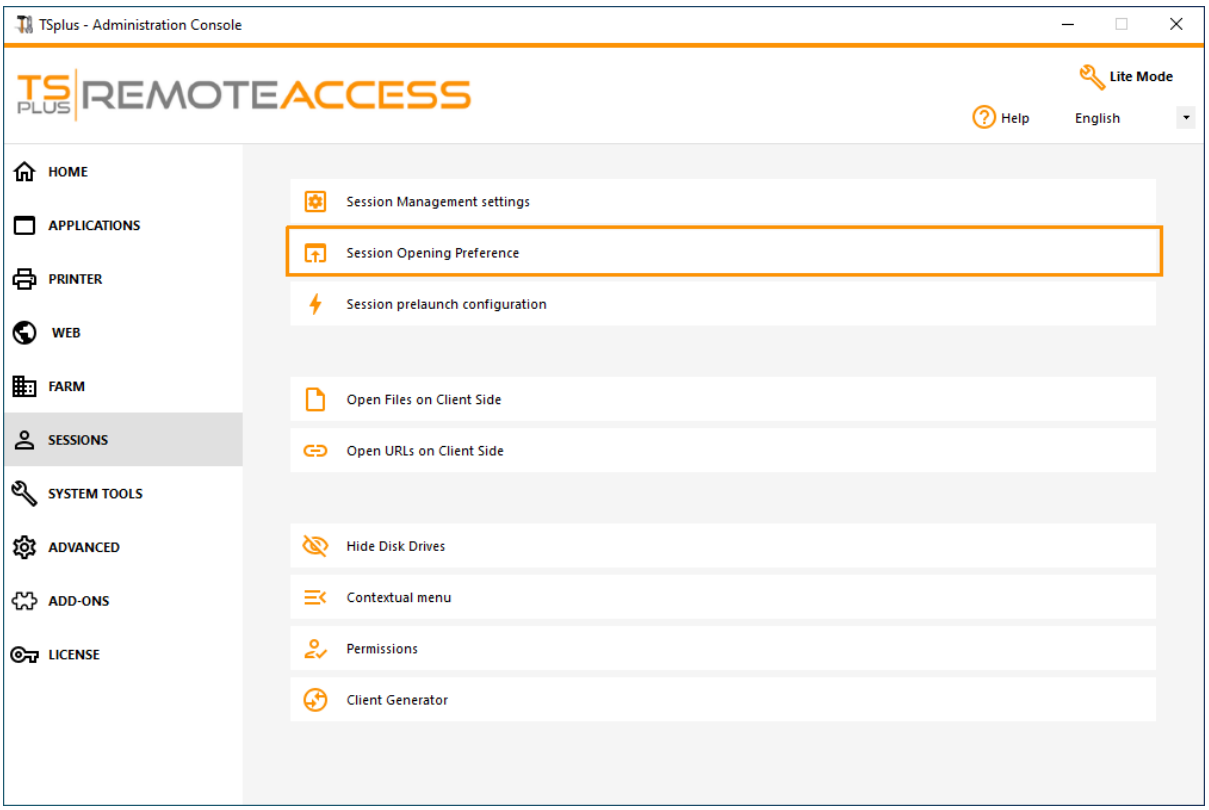
- Sie können auch die Registerkarte „Servereigenschaften“ öffnen, um einen Überblick über das Steuerfeld zu erhalten.



- Sie können alle Dienste auf Ihrem Server und deren Status auf der Kachel Dienste anzeigen.

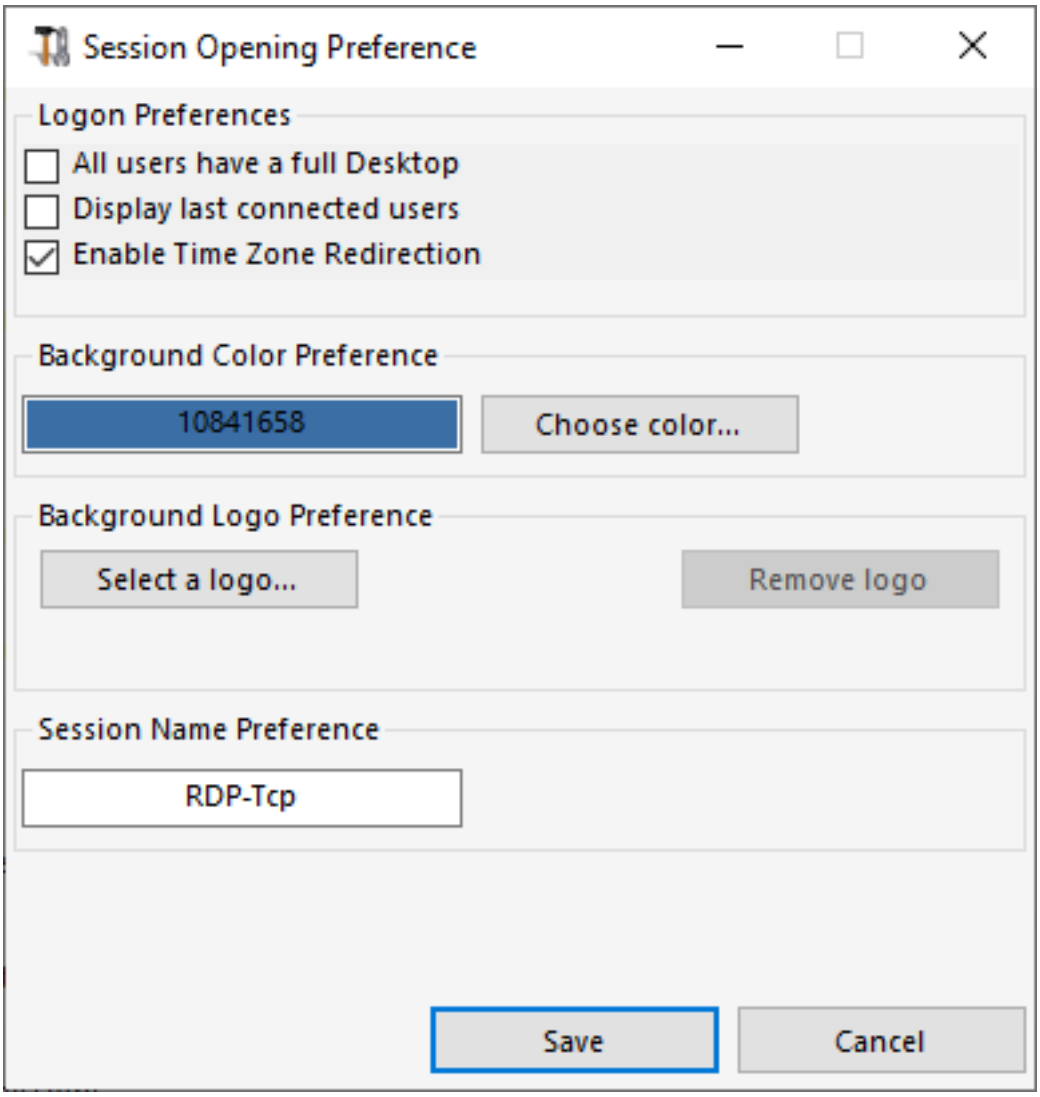


Die Sitzungseröffnungspräferenz ermöglicht es Ihnen, Ihre Shell-Sitzungspräferenz, Ihre Anmeldeeinstellungen, die Hintergrundfarbe Ihrer Sitzungen auszuwählen, Ihr eigenes Logo hinzuzufügen und es nach Ihren Wünschen umzubenennen.



Standardmäßig sind diese Anmeldeeinstellungen aktiviert:

- Die “ **Fortschrittsanzeige während der Anmeldung anzeigen** ”.
- “ **Aktivieren Sie die Zeitzonenumleitung** ” die es dem Client-Computer ermöglicht, seine Zeitzoneneinstellungen an die Remote Desktop Services-Sitzung weiterzuleiten. Wenn Sie diese Richtlinieneinstellung aktivieren, senden Clients, die in der Lage sind, die Zeitzone weiterzuleiten, ihre Zeitzoneninformationen an den Server.



Sie können auch **einen vollständigen Desktop einrichten** für alle Ihre Benutzer und **zeige die zuletzt verbundenen Benutzer an** indem Sie die entsprechenden Kästchen ankreuzen. Sie können **passen Sie die Sitzungen Ihrer Benutzer an** indem Sie eine neue Hintergrundfarbe, ein anderes Logo oder keines hinzufügen und den Sitzungsnamen Ihrer Wahl verwenden.

- Seit der Veröffentlichung von TSplus 11.70 können Sie verwenden **TSplus WinXshell** als Alternative zur Windows-Shell.

Nach dem Windows-Update vom 10. Oktober sahen Administratoren, die ihren Benutzern erlaubten, einen Remote Desktop zu starten, die Windows-Shell als ein Problem an.

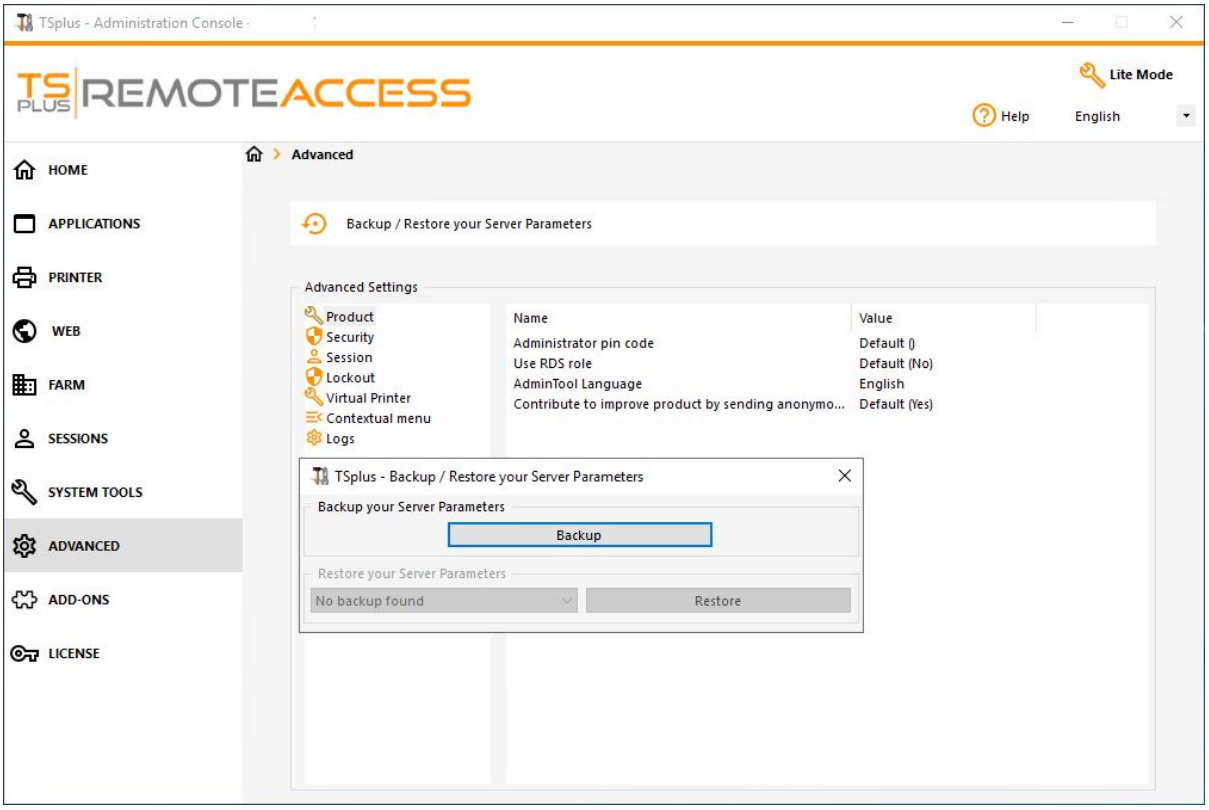
Das Hauptproblem liegt im Öffnen der Sitzung/Schwarzbildschirmproblem, wenn ein vollständiger Desktop mehreren Benutzern unter Windows 10 und Server 2016 zugewiesen ist.

Es bietet Funktionen und eine grafische Erfahrung, die der Windows 2016 Windows-Shell ähnlich sind, wie die Anzeige der Startschaltfläche und der Taskleiste von 2016.

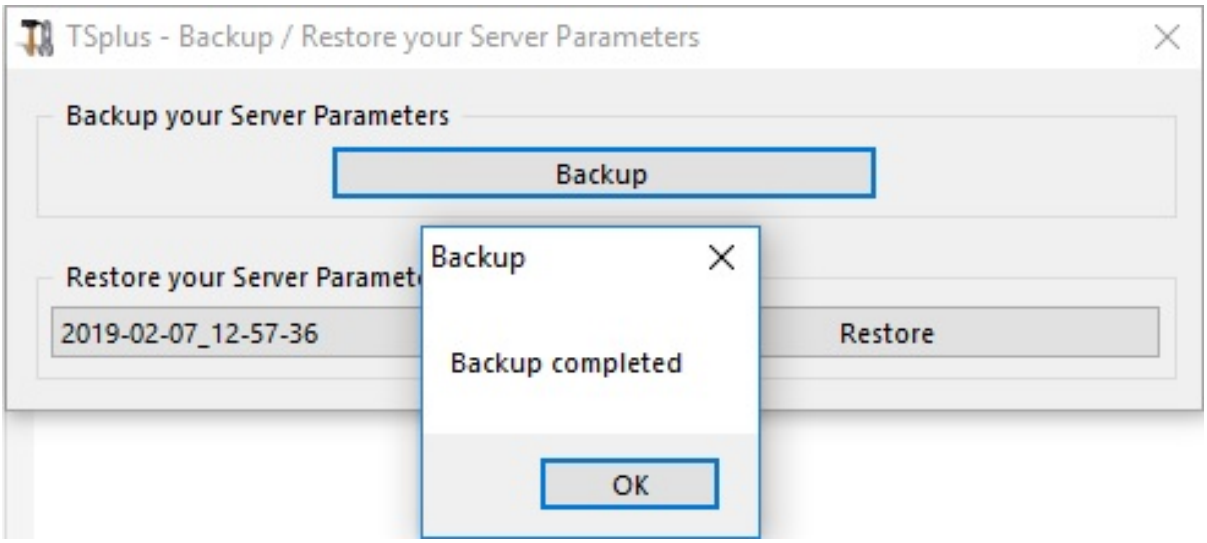
Es ist besonders nützlich, wenn Sie **verwenden Sie Windows 10 oder Windows 16 Betriebssysteme** , **10 oder mehr Benutzer verwalten** und **wünschen, ihnen einen vollständigen Desktop zuzuweisen** .

Sicherungsparameter

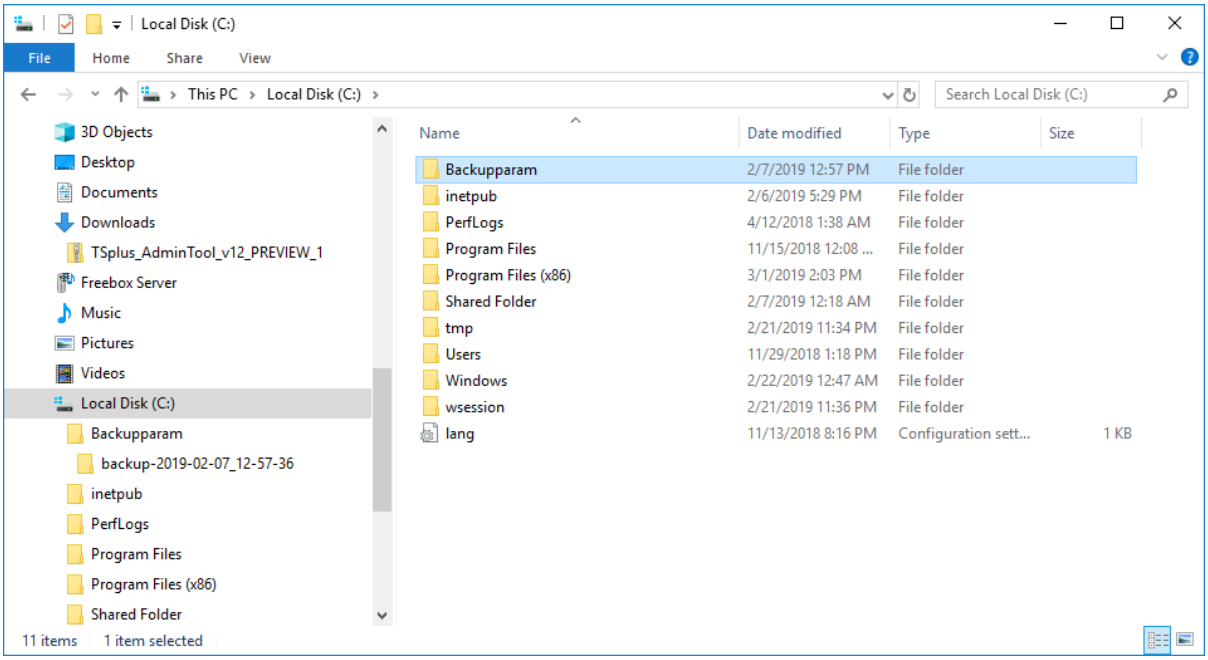
Sie können Ihre Serverparameter sichern oder wiederherstellen, indem Sie auf die Kachel mit demselben Namen im Tab "Erweitert" klicken:



Klicken Sie auf die Schaltfläche Backup, um ein Backup zu erstellen, das datiert wird und zur Liste Ihrer Wiederherstellungspunkte hinzugefügt wird:



Die Sicherungsdatei befindet sich im Ordner C:\Backupparam:



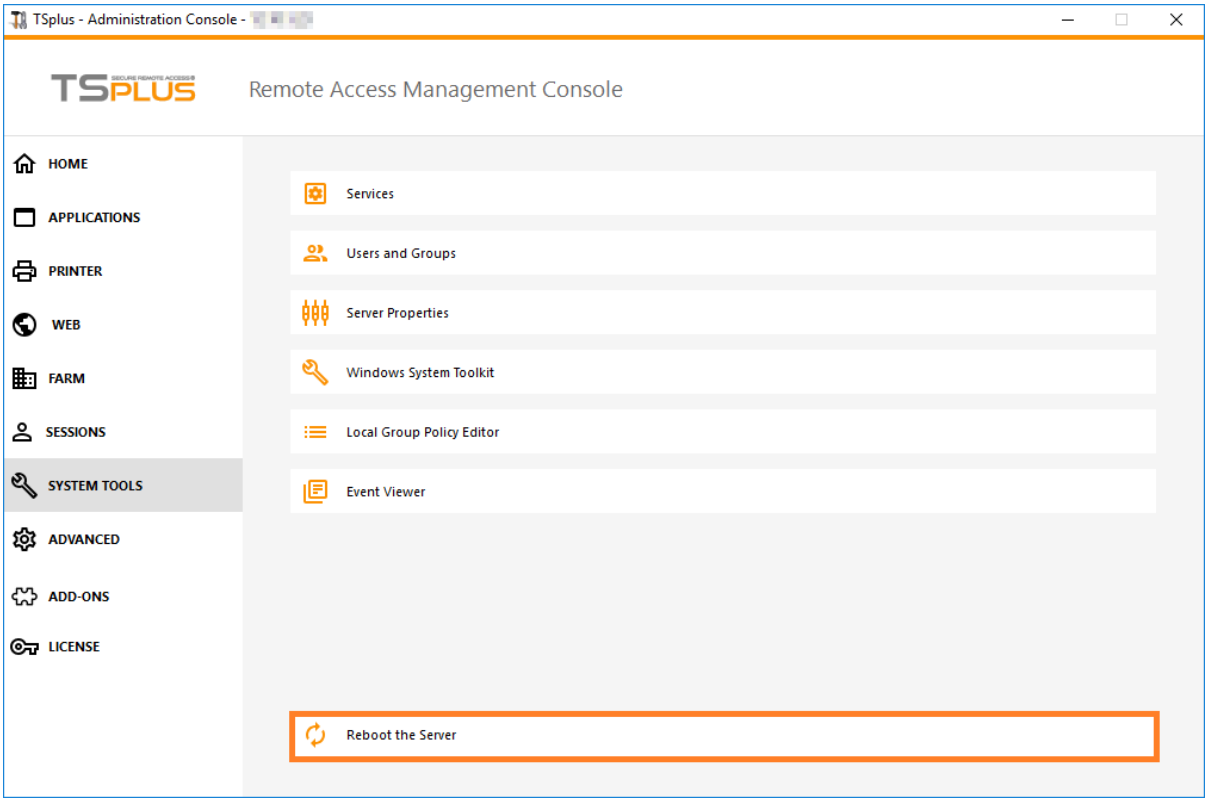
Kopieren Sie den Ordner auf den neuen Server, nachdem Sie TSplus Remote Access installiert haben, und stellen Sie das Backup wieder her.

Sie können dann 15 Tage lang mit der Testversion überprüfen, ob die Funktionsweise der Konten und der Zugriff korrekt ist, bevor Sie Ihre Lizenz endgültig migrieren.

Mehr Informationen dazu Dokumentation .

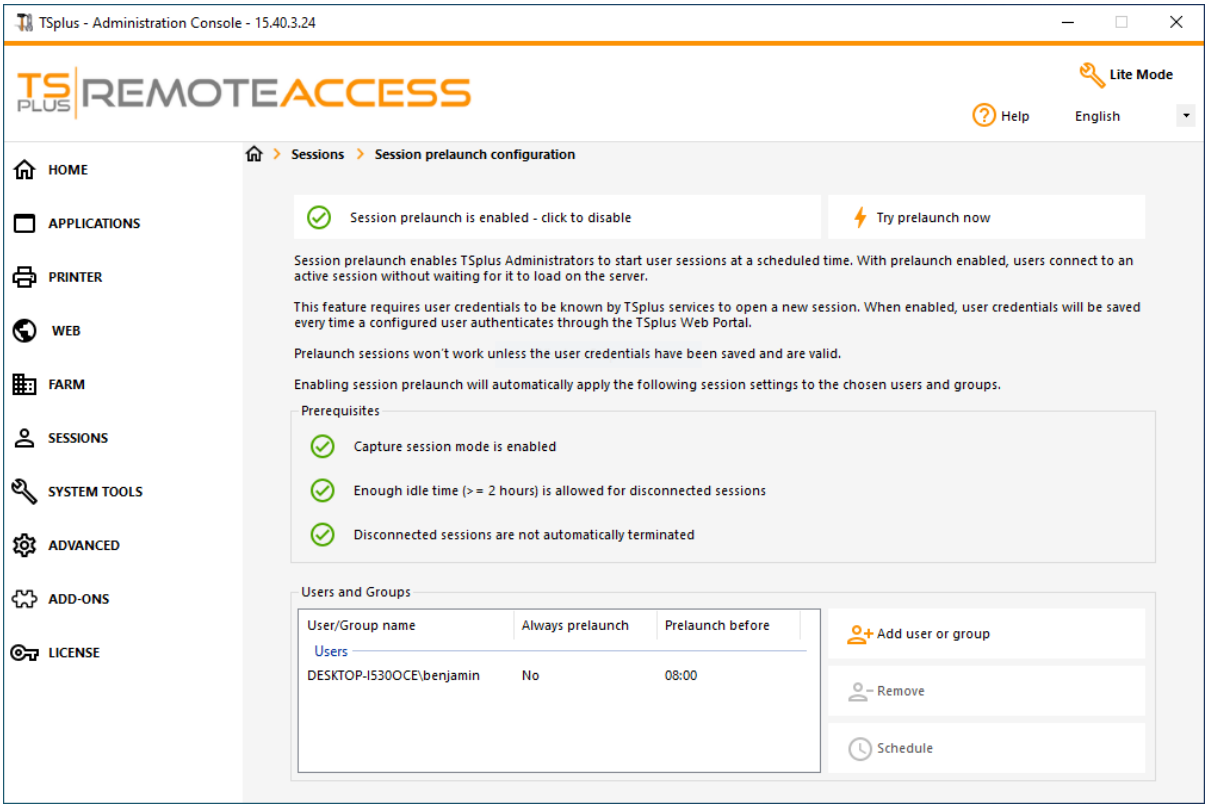
Starten Sie Ihren Server neu

Die Registerkarte „Server neu starten“ ermöglicht es Ihnen, Ihren Server neu zu starten.


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

Sitzungsvorbereitung

Greifen Sie auf das Menü zur Konfiguration des Sitzungs-Prelaunch über die Registerkarte Sitzungen > Einstellungen im Admintool zu, indem Sie auf das Feld „Konfiguration des Sitzungs-Prelaunch“ klicken.

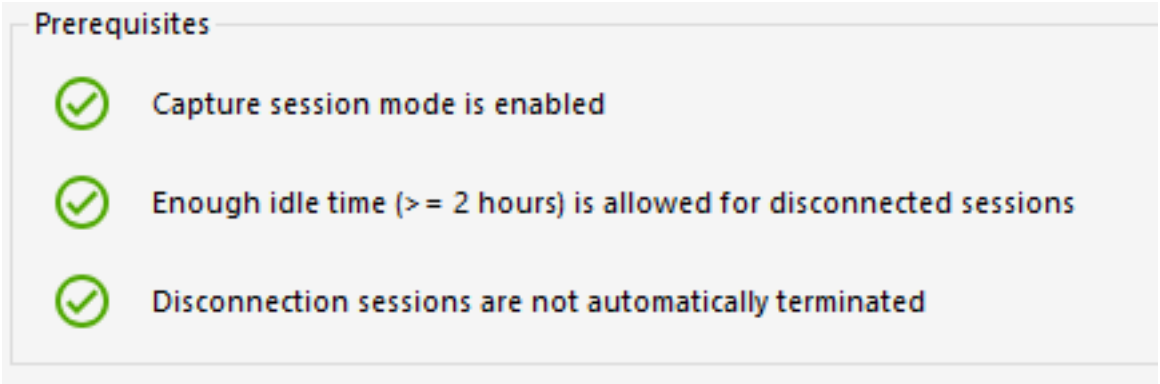


Übersicht

Die Funktion zur Vorabstart der Sitzung ermöglicht es den Tsplus Remote Access-Administratoren, Benutzersitzungen so zu konfigurieren, dass sie vor einer geplanten Zeit gestartet werden. Die Idee ist, die Sitzung jedes konfigurierten Benutzers im Voraus vorzubereiten und zu laden, sodass, sobald ein Benutzer sich verbindet, er seine spezifische Sitzung erfasst. Dies kann die Wartezeiten für die Verbindung von Minuten auf Sekunden verkürzen.

Voraussetzungen

Prelaunch erfordert, dass mehrere Voraussetzungen erfüllt sind.



1 - Um eine Sitzung zu erfassen, **Die Sitzungsaufnahme muss aktiviert sein.** Das bedeutet, dass Sie von dieser Funktion nicht profitieren können, wenn die Multi-Session-Konfiguration für Ihre Benutzer obligatorisch ist.

2 - Da die vorbereitete Sitzung im Voraus geladen werden muss, um vorhanden zu sein (nicht abgemeldet), wenn der Benutzer sich verbindet und sie erfasst, **Es muss eine Mindestanzahl von 2 Stunden Leerlaufzeit für getrennte Sitzungen erlaubt sein.** Sie können natürlich auch die Sitzungseinstellungen so festlegen, dass eine getrennte Sitzung niemals abgemeldet wird.

3 - Da die vorbereitete Sitzung nach dem Laden getrennt wird, um die Gesamtressourcennutzung zu reduzieren, **Die Sitzungseinstellungen müssen so konfiguriert werden, dass getrennte Sitzungen nicht automatisch abgemeldet werden.**

Wichtiger Hinweis! Jeder konfigurierte Benutzer muss sich mindestens einmal über das TSplus Webportal authentifizieren, nachdem die Funktion zur Vorabstart der Sitzung aktiviert wurde, damit die TSplus-Dienste die konfigurierte Benutzersitzung öffnen können.

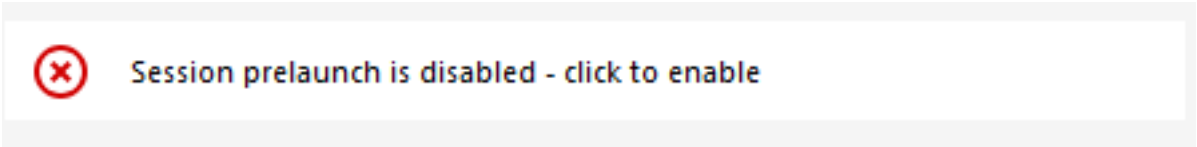
Session Prelaunch-Kompatibilitäten

Session-Vorbereitung ist mit HTML5-Sitzungen und generischen RDP-Sitzungen kompatibel, die über den generierten Client oder mstsc geöffnet werden.

Es ist jedoch nicht kompatibel mit der Remote App-Verbindung oder benutzerdefinierten RDP-Verbindungen, die zum Öffnen eines bestimmten Programms hergestellt wurden.
Als Ergebnis werden Verbindungen, die vom TSplus Web Application Portal kommen, nicht unterstützt.

Aktivieren Sie die Funktion

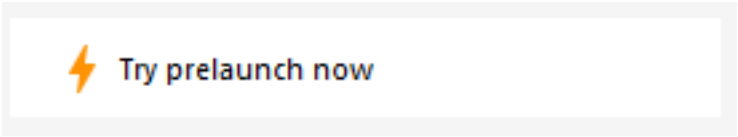
Um die Funktion zur Vorabstart der Sitzung zu aktivieren, klicken Sie einfach auf die Kachel mit der Aufschrift „Sitzungsvorabstart ist deaktiviert - klicken Sie hier, um zu aktivieren“ oben im Fenster.



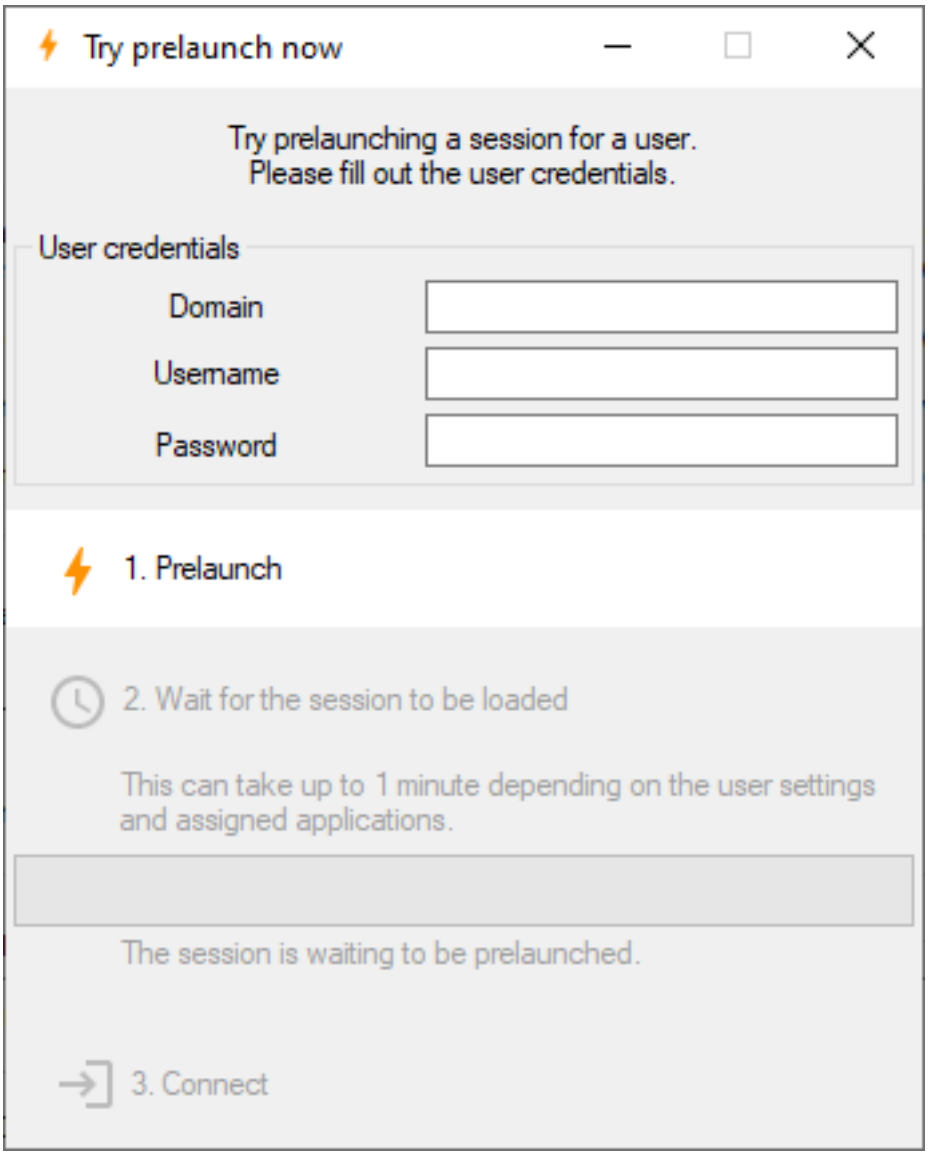
Wenn eine der Voraussetzungen beim Aktivieren der Sitzungsvorbereitung nicht erfüllt ist, werden Sie gefragt, ob Sie die Sitzungseinstellungen automatisch so konfigurieren möchten, dass die Voraussetzungen erfüllt sind und die Funktion genutzt werden kann. Beachten Sie, dass das Ändern der Sitzungseinstellungen einen Neustart erfordern kann.

Testen Sie den Sitzungs-Vorstart

Sobald aktiviert, können Sie die Funktion schnell testen, indem Sie auf die Schaltfläche „Jetzt Prelaunch ausprobieren“ oben klicken.



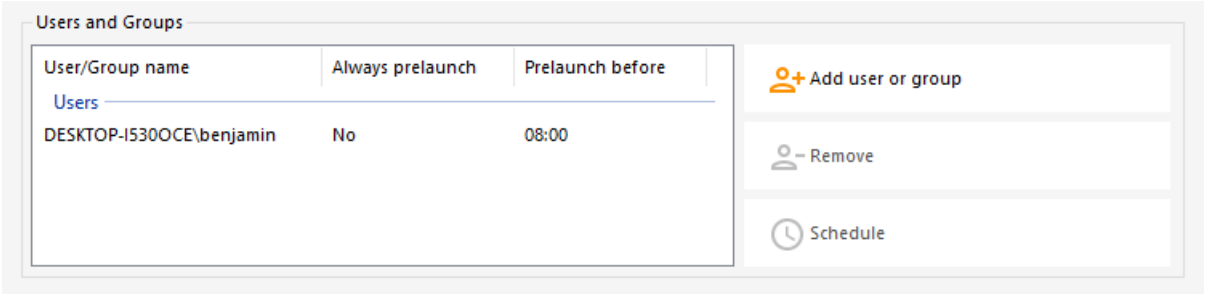
In dem Fenster, das erscheint, geben Sie die Benutzeranmeldeinformationen ein, damit die TSplus-Dienste die Sitzung für diesen spezifischen Benutzer vorstarten können.



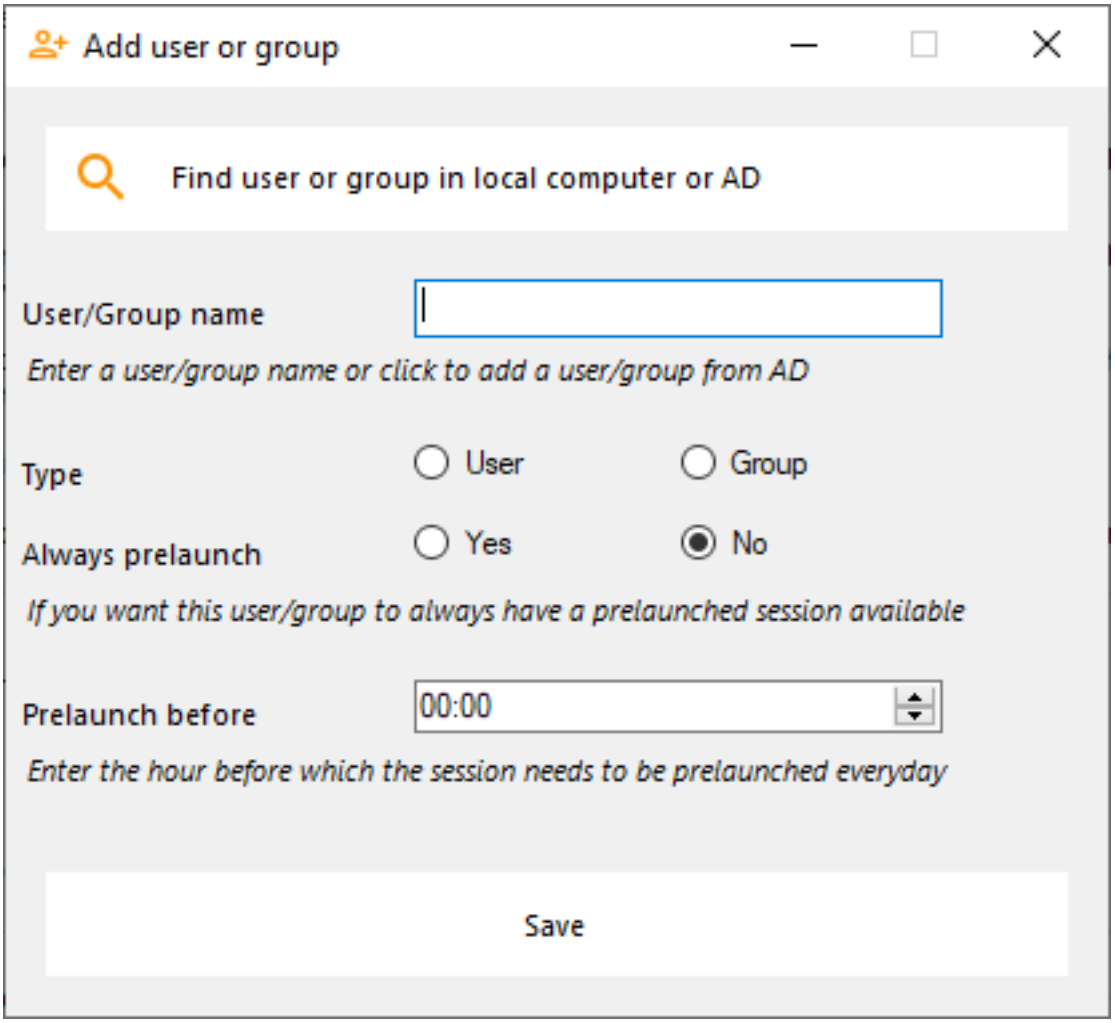
Klicken Sie auf „Prelaunch“, um eine neue Sitzung für diesen Benutzer zu starten und zu laden. Warten Sie, bis es vollständig geladen ist, und klicken Sie dann auf „Verbinden“, um die neu geladene Sitzung zu erfassen.

Verwalten Sie konfigurierte Benutzer und Gruppen

Um Sitzungs-Vorabstart-Benutzer und -Gruppen hinzuzufügen, klicken Sie einfach auf „Benutzer oder Gruppe hinzufügen“.
Um einen konfigurierten Benutzer zu bearbeiten oder zu entfernen, wählen Sie den entsprechenden Benutzer/die entsprechende Gruppe in der Liste der konfigurierten Benutzer/Gruppen aus und klicken Sie dann auf „Zeitplan“, um die Zeit „Vorstart“ zu ändern, oder auf die Schaltfläche „Entfernen“, um den Benutzer zu entfernen.



Nachdem Sie auf „Benutzer oder Gruppe hinzufügen“ geklickt haben, werden Sie nach dem Namen des Benutzers/der Gruppe gefragt, die konfiguriert werden soll, sowie nach der Zeit, bevor die Sitzung geladen werden muss, die hier als „Vorstart“ bezeichnet wird.
Sie können auch diesen Benutzer/diese Gruppe so konfigurieren, dass immer eine Sitzung vorab gestartet wird, wenn Sie sich verbinden, anstatt sie planen zu müssen, indem Sie „Ja“ bei der Option „Immer vorab starten“ auswählen.



Wie man die Unterstützung von Websockets für den Apache-Reverse-Proxy einrichtet

1. Zuerst ändern Sie die folgende Variable auf false www\software\html5\settings.js > W.xhrreverse = false; (wenn Sie es nicht auf false ändern, wird es immer versuchen, xhr anstelle von Websockets zu verwenden, was wir nicht mehr wollen)

2. installieren Sie Apache mit proxy_wstunnel-Unterstützung (ältere Apaches ohne proxy_wstunnel werden nicht unterstützt!)

3. erlauben Sie in der Apache-Konfiguration (httpd.conf usw.) folgende Module. 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. nehmen wir an, Sie möchten über den Unterordner „/html5/“ auf das HTML5-Hauptportal zugreifen. Als Beispiel http://your_ip_or_domain.net/html5/ und TSplus ist im Intranet auf dem Server „intranetxyz“ installiert, fügen Sie dann die folgende Konfiguration (httpd.conf usw.) hinzu.

   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. Apache neu starten, um die Änderungen wirksam werden zu lassen.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung fügt eine zusätzliche Sicherheitsebene hinzu und **verhindert den Zugriff auf die Sitzung Ihrer Benutzer, selbst wenn jemand ihr Passwort kennt** .

Eine Kombination aus zwei verschiedenen Faktoren wird verwendet, um ein höheres Maß an Sicherheit zu erreichen:

1. etwas, das sie wissen **ein Passwort** .

2. etwas, das sie haben, ein **Gerät - wie ein Smartphone - mit einer installierten Authentifizierungs-App.** .

Sie können eine der folgenden Authentifizierungs-Apps verwenden, um fortzufahren. Diese Apps sind auf einer Vielzahl von Plattformen verfügbar:

- Authy
- Google Authenticator
- Microsoft Authenticator

Jedes Mal, wenn sich ein Benutzer in seine Remote-Sitzung anmeldet, benötigt er sein Passwort und einen Verifizierungscode, der auf seinem Mobiltelefon verfügbar ist. Nach der Konfiguration zeigt die Authenticator-App einen Verifizierungscode an, um ihm oder ihr zu ermöglichen, sich jederzeit anzumelden. Es funktioniert sogar, wenn das Gerät offline ist.

ODER Sie können entscheiden, die Bestätigungscodes zu erhalten durch **SMS** In diesem Fall müssen Sie ein kostenloses Konto bei erstellen Twilio .

Die **2FA-Codes werden als TOTP generiert** (einmaliges zeitbasiertes Passwort), und sind daher für den einmaligen Gebrauch.

Daher ist es nicht möglich, einen bereits verwendeten 2FA-Code erneut zu verwenden. Dies verhindert den Diebstahl und die anschließende Verwendung eines 2FA-Codes, indem der Benutzer beobachtet wird, während er seinen Code eingibt.

Anforderungen

Die Zwei-Faktor-Authentifizierung erfordert TSplus Remote Access **Mobile-Web** oder **Unternehmen** Editionen.

Die Zwei-Faktor-Authentifizierung wird unterstützt durch:

- TSplus Remote Access **Webportal** , sowohl für HTML5- als auch für Remoteapp-Verbindungen
- TSplus Connection Client, für Clients, die seit Version 15.30.3.15 erstellt wurden, mit 2FA-Unterstützung ausdrücklich aktiviert. Siehe Portable Client Generator Unterstützung für Zwei-Faktor-Authentifizierung
- 2FA bezieht sich auf Windows-Benutzer und nicht auf Web-Anmeldeinformationen

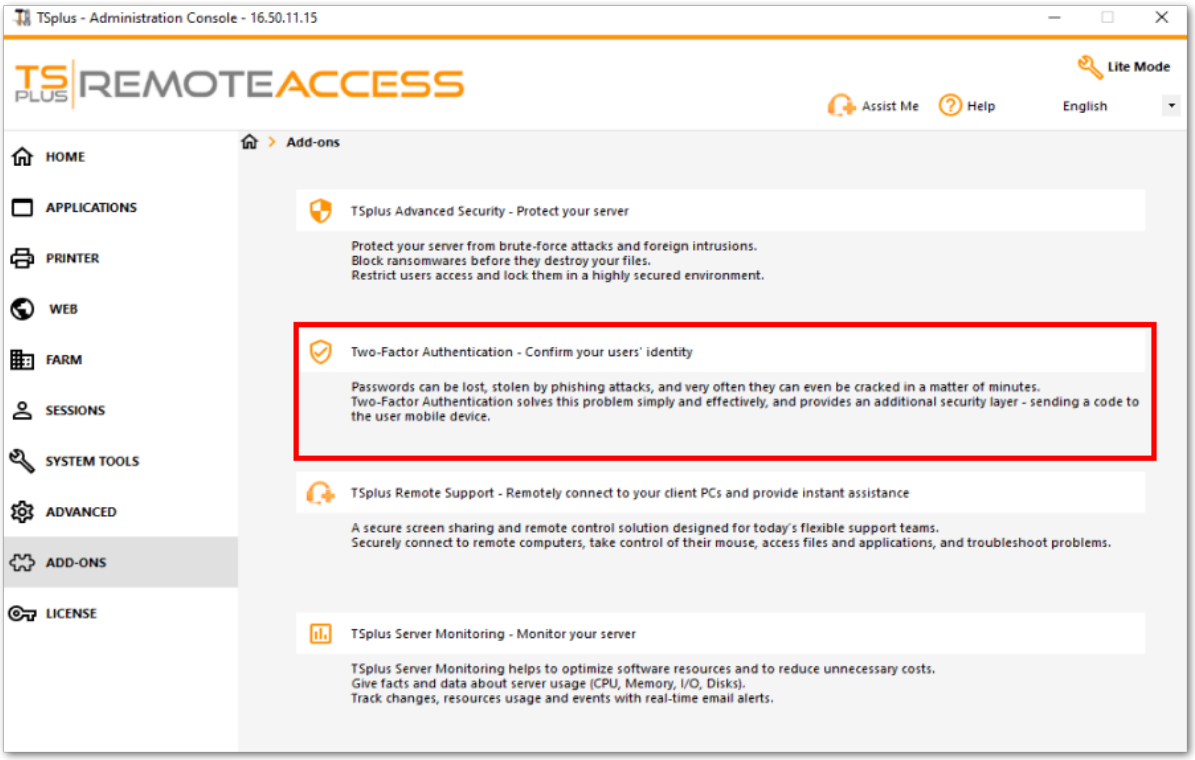
Dieser Authentifizierungsmodus unterstützt kein Login über den standardmäßigen Microsoft Remote Desktop-Client (mstsc.exe).

Um eine noch sicherere Lösung zu bieten, werden RDP-Verbindungen für Benutzer mit aktivierter Zwei-Faktor-Authentifizierung verweigert.

Als Voraussetzung müssen der TSplus-Server und die Geräte rechtzeitig sein. Sehen Sie die Zeit-Synchronisierung und Einstellungen Abschnitte für weitere Konfigurationsinformationen.

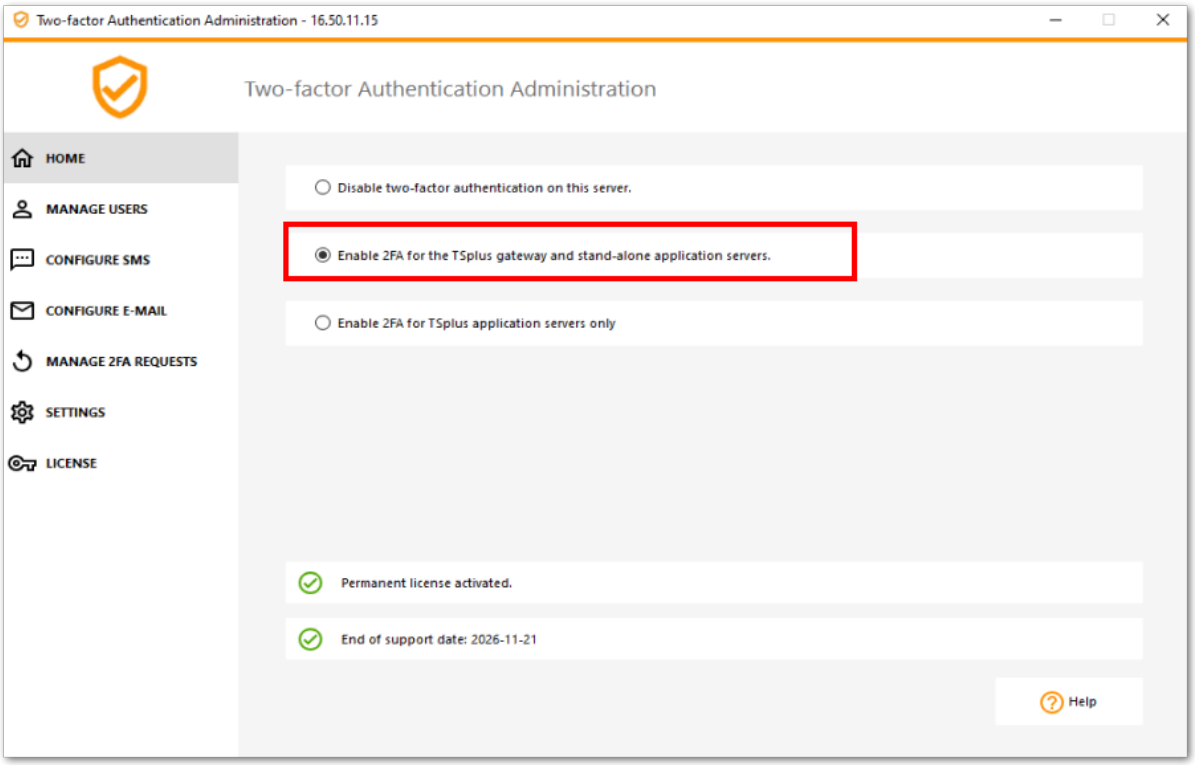
Aktivierung der Lizenz für das Add-On zur Zwei-Faktor-Authentifizierung

Die Funktion der Zwei-Faktor-Authentifizierung ist im Add-On-Tab des AdminTools zu finden:



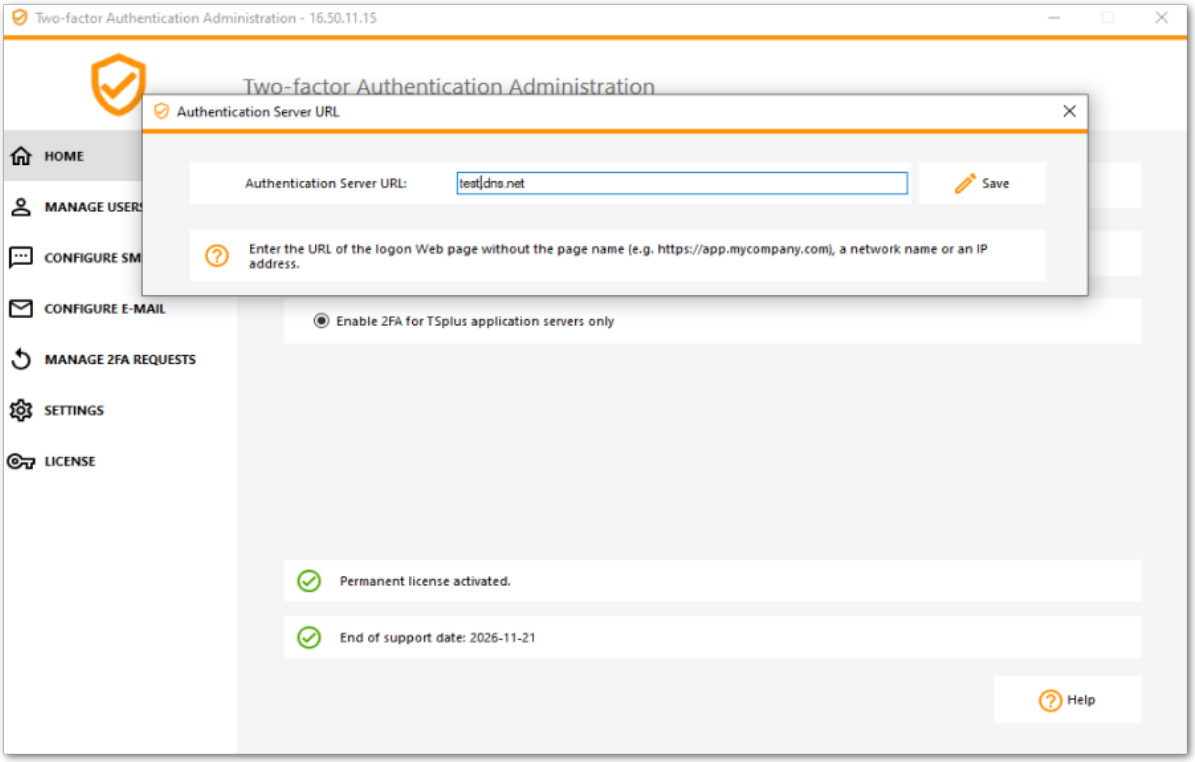
Führen Sie die folgenden Schritte aus, um die Zwei-Faktor-Authentifizierung für Ihren TSplus-Server oder Ihre Bereitstellung zu aktivieren. Wenn Ihre TSplus-Bereitstellung so konfiguriert ist, dass mehrere Server verwendet werden, führen Sie diese Aufgabe auf dem TSplus-Server aus, der als einziger Zugangspunkt für Benutzer oder mit der Rolle des Reverse-Proxys exponiert ist.

1. Öffnen Sie die Anwendung zur Verwaltung der Zwei-Faktor-Authentifizierung. Der Status der Zwei-Faktor-Authentifizierung und der Lizenzstatus werden angezeigt:

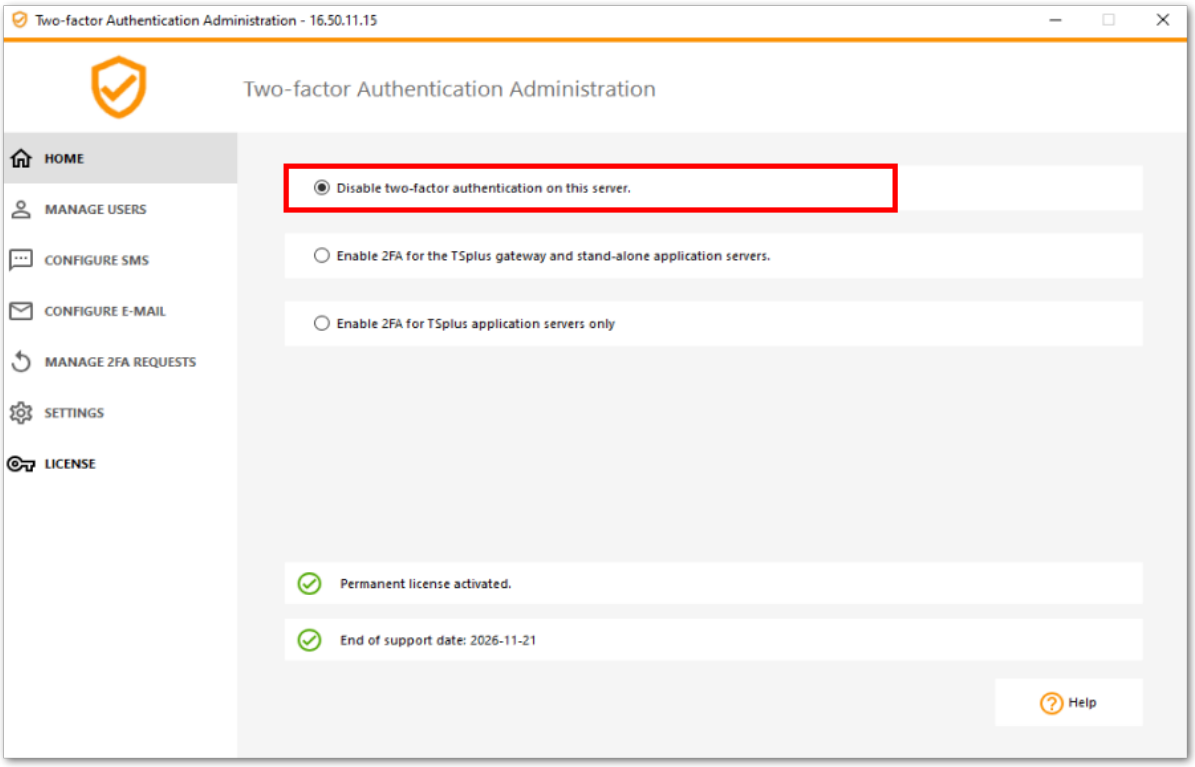


Standardmäßig ist 2FA für das TSplus-Gateway und die eigenständigen Anwendungsserver aktiviert.

Sie können es nur für TSplus-Anwendungsserver aktivieren, indem Sie die URL des Authentifizierungsservers eingeben:



Oder deaktivieren Sie es:

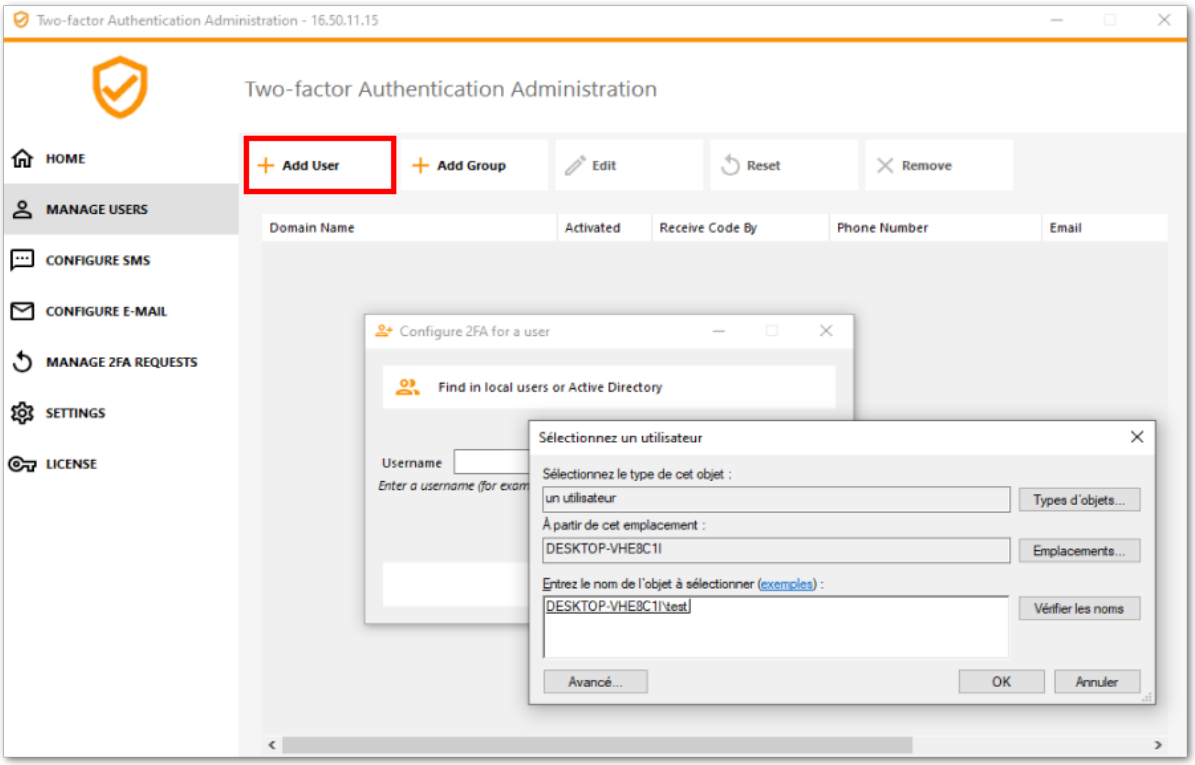


Benutzer und Gruppen hinzufügen

Sobald die Zwei-Faktor-Authentifizierung aktiviert ist, können Sie Benutzer für die Zwei-Faktor-Authentifizierung konfigurieren.

1. Von der Verwaltung Anwendung zur Zwei-Faktor-Authentifizierung klicken Sie auf die Benutzer verwalten Tab.

2. Dann klicken Sie auf Hinzufügen Benutzern und/oder Benutzergruppen auszuwählen. Die Benutzer oder Gruppen auswählen Box öffnet sich.



3. Fügen Sie so viele Benutzer und Gruppen hinzu, wie erforderlich, und klicken Sie dann auf OK Die Benutzer und Gruppen werden zur Liste hinzugefügt und für die Zwei-Faktor-Authentifizierung aktiviert.

Hier sind Befehle zum Hinzufügen von Benutzern/Gruppen
3 Arten möglicher Argumente:

nur der domainName
TwoFactor.Admin.exe /addusers domainName1

- fügt den Benutzer mit den Standardwerten hinzu (Empfangsmethode = App, E-Mail- und Telefonfelder nicht eingegeben)

der domainName und die Empfangsmethode
TwoFactor.Admin.exe /addusers domainName1;SMS

- fügt den Benutzer mit der gewünschten Empfangsmethode hinzu, versucht jedoch nicht, sie zu aktivieren

der domainName, die Empfangsmethode, das Telefonfeld (auch wenn leer), das E-Mail-Feld (auch wenn leer)
*TwoFactor.Admin.exe /addusers domainName1;SMS;+33606060606; username1@truc.net domainName2;E-Mail;; username2@truc.net domainName3;SMS; +33606060607;domainName4

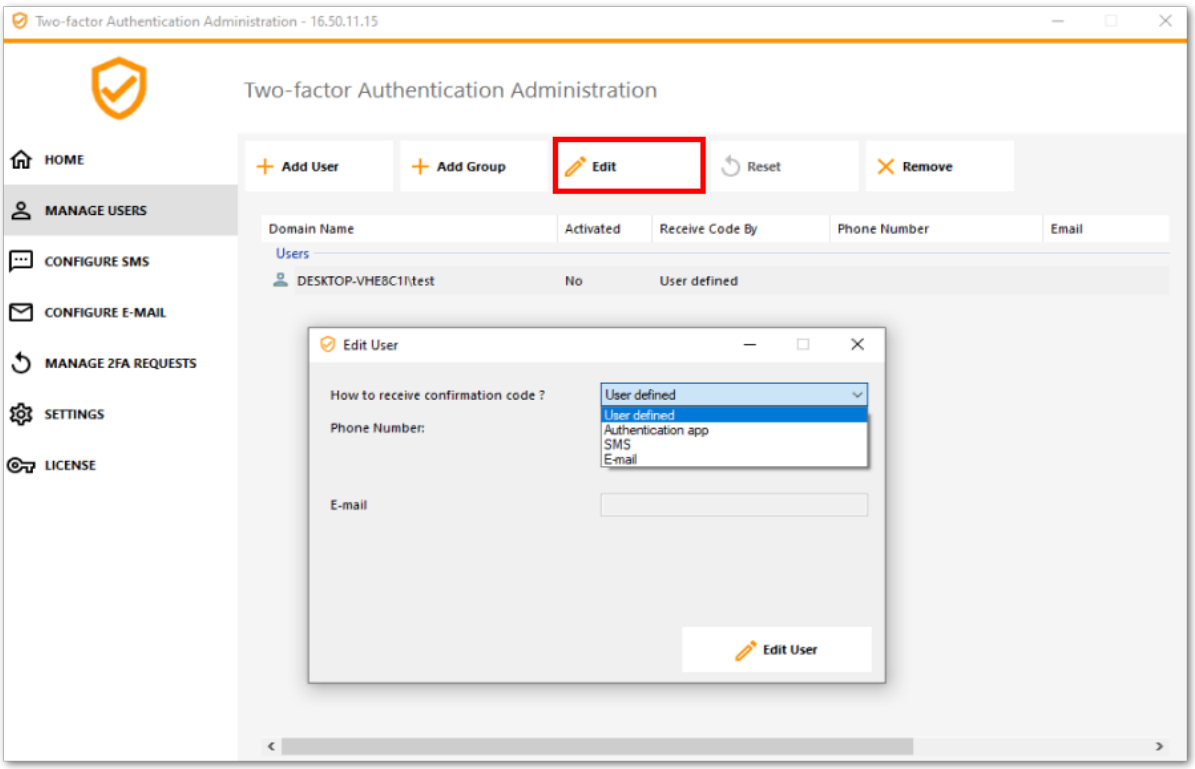
- Das gleiche Verhalten wie im HMI, wenn wir einen Benutzer hinzufügen und dann mit den korrekten Informationen bearbeiten: wir versuchen, den Benutzer zu aktivieren.

Wie im letzten Beispiel gezeigt, können mehrere Benutzer angegeben werden (durch ein Leerzeichen getrennt). Die verschiedenen Felder eines Benutzers sind durch ein Semikolon getrennt.

Für einzelne Gruppen:
TwoFactor.Admin.exe /addgroups gruppe1 gruppe2 gruppe3

Benutzer bearbeiten

Auf demselben Kachel können Sie die Art und Weise bearbeiten, wie Benutzer Verifizierungscodes erhalten, indem Sie einen Benutzer auswählen und auf die Schaltfläche „Bearbeiten“ klicken.

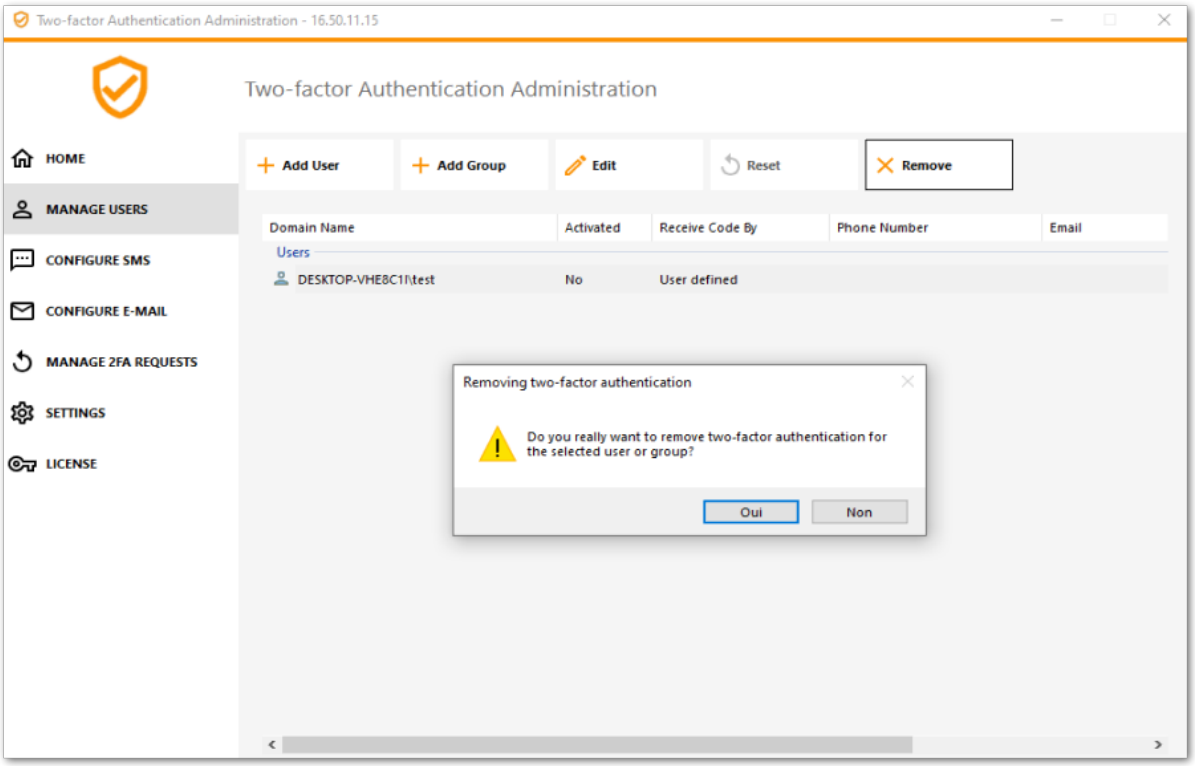


Der Benutzer erhält standardmäßig Verifizierungscodes in der Authentifizierungs-App. Sie können wählen, dass er/sie diese per SMS oder E-MAIL erhält, indem Sie die Option auswählen.

Ausgewählte SMS und die Telefonnummer des Benutzers im Feld hinzugefügt oder E-MAIL ausgewählt und die E-Mail des Benutzers hinzugefügt.

Benutzer und Gruppen entfernen

Um Benutzer oder Gruppen zu entfernen, wählen Sie den Benutzer oder die Gruppe aus und klicken Sie dann auf Entfernen Eine Bestätigungsnachricht wird angezeigt.



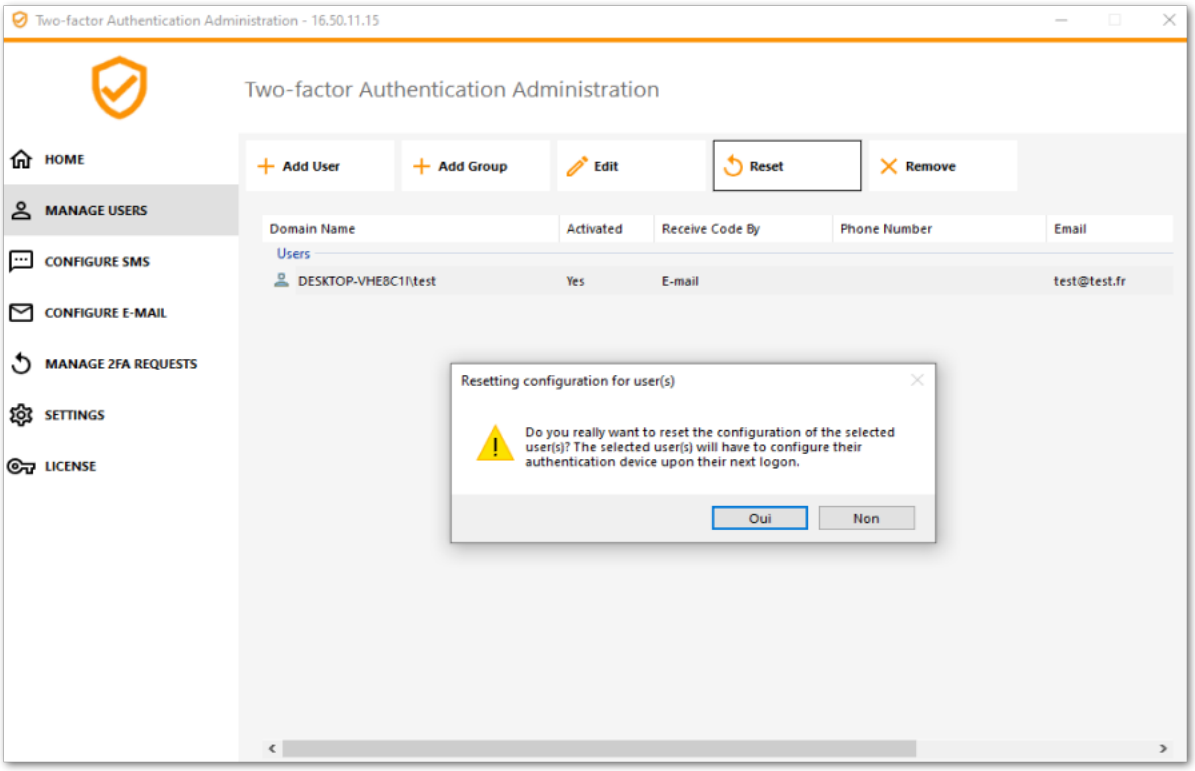
Klicken Ja Der Benutzer oder die Gruppe wird aus seiner Liste entfernt und kann sich nicht mehr mit Zwei-Faktor-Authentifizierung verbinden.

Konfiguration für Benutzer zurücksetzen

Im Falle des Verlusts des authentifizierenden Geräts für einen Benutzer oder wenn der Benutzer den geheimen QR-Code erneut anzeigen muss, müssen Sie die Benutzerauthentifizierungseinstellungen zurücksetzen.

1. Von der Verwaltung Anwendung zur Zwei-Faktor-Authentifizierung klicken Sie auf die Benutzer verwalten Tab.

2. Wählen Sie einen oder mehrere aktivierte Benutzer aus und klicken Sie dann auf Zurücksetzen Eine Bestätigungsnachricht wird angezeigt.



3. Klicken Ja Die ausgewählten Benutzer erhalten beim nächsten Login einen neuen QR-Code, den sie in der Authentifizierungs-App ihres Geräts scannen müssen.

Sie können auch die Telefonnummer des Benutzers ändern, damit er einen Bestätigungscode auf seinem neuen Gerät erhalten kann.

Benutzer für die Zwei-Faktor-Authentifizierung anmelden

Sobald ein Benutzer für die Verwendung der Zwei-Faktor-Authentifizierung aktiviert wurde, wird bei seiner nächsten erfolgreichen Anmeldung über das TSplus-Webportal eine Aktivierungsnachricht angezeigt.



Um die erforderlichen Schritte abzuschließen, haben Sie zwei Möglichkeiten: entweder Codes über eine Authenticator-App zu generieren oder den Benutzer Codes per SMS empfangen zu lassen.

Codes mit einer Authenticator-Anwendung empfangen

Der Benutzer muss eine Authentifizierungs-App auf einem tragbaren Gerät, wie seinem Smartphone, installieren.

Sie können eine der folgenden Authentifizierungs-Apps verwenden, um fortzufahren. Diese Apps sind auf einer Vielzahl von Plattformen verfügbar:

- Authy
- Google Authenticator

- Microsoft Authenticator

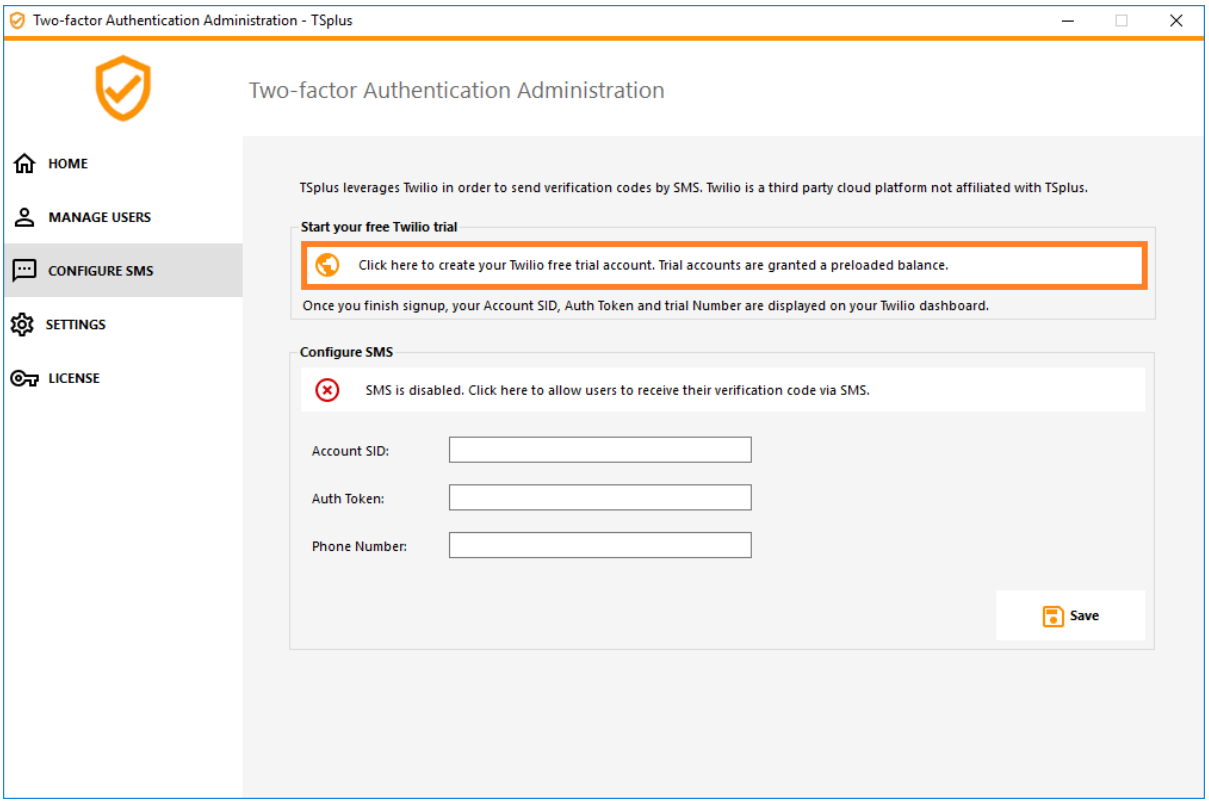
Bitte verwenden Sie die Dokumentation jeder App für weitere Details, wie Sie Ihr TSplus-Konto hinzufügen können.

SMS konfigurieren

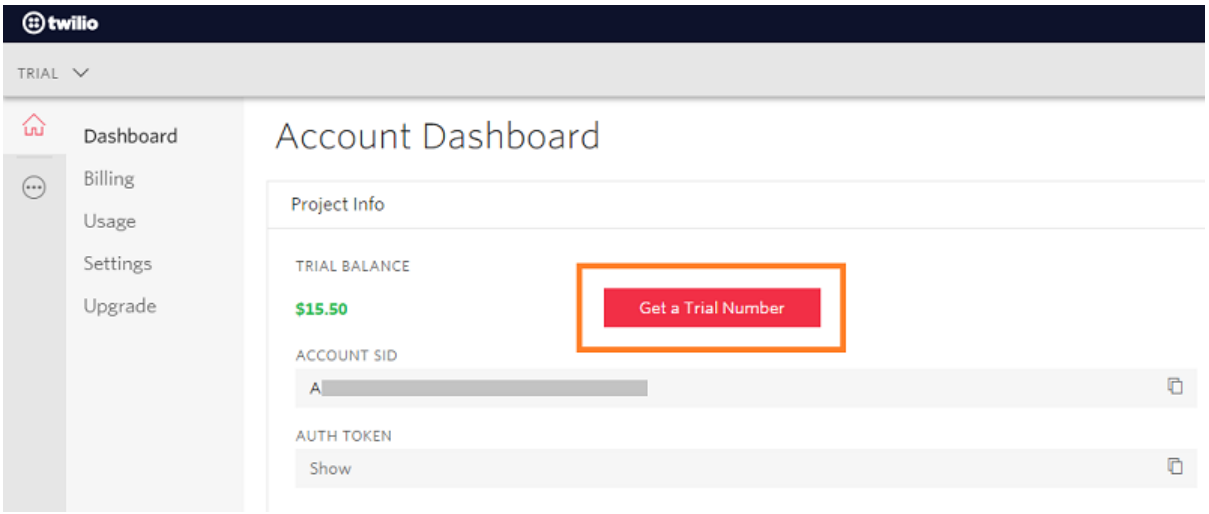
Um zu gewährleisten, dass der Benutzer Bestätigungscodes per SMS erhält, müssen Sie dies zuerst aktivieren. Klicken Sie auf die SMS konfigurieren Tab:

TSplus nutzt Twilio, um Verifizierungscodes per SMS zu senden. Twilio ist eine Drittanbieter-Cloud-Plattform, die nicht mit TSplus verbunden ist.

1. Erstellen Sie einfach ein kostenloses Konto auf Twilio indem Sie auf die Schaltfläche unten „Starten Sie Ihre kostenlose Testversion mit Twilio“ klicken:

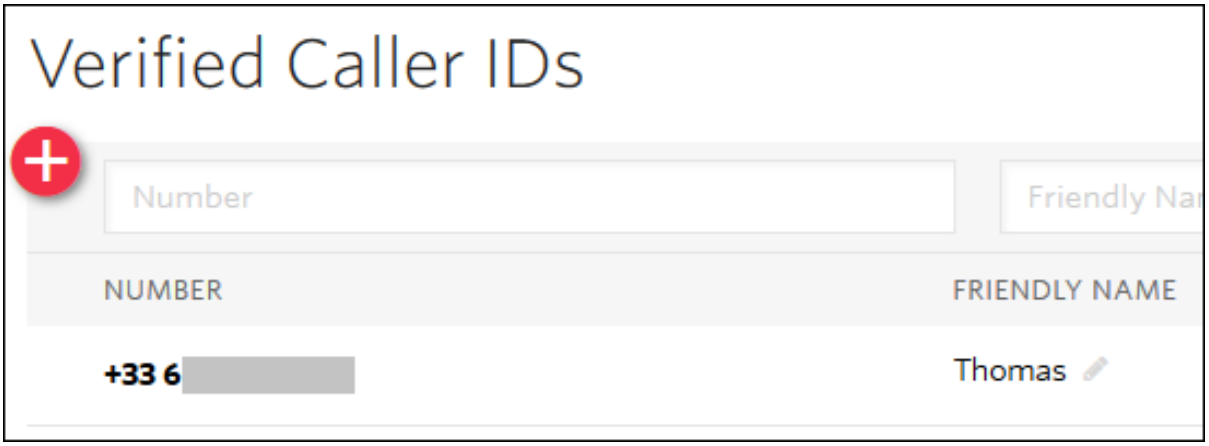


2. Auf Ihrem Twilio-Konto-Dashboard Sie müssen Ihre Testnummer aktivieren:

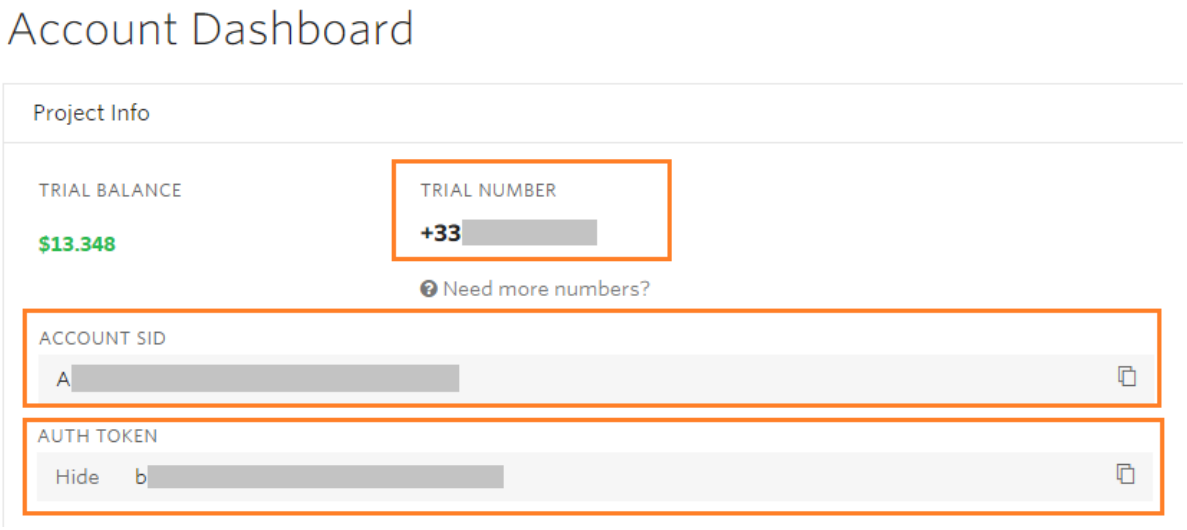


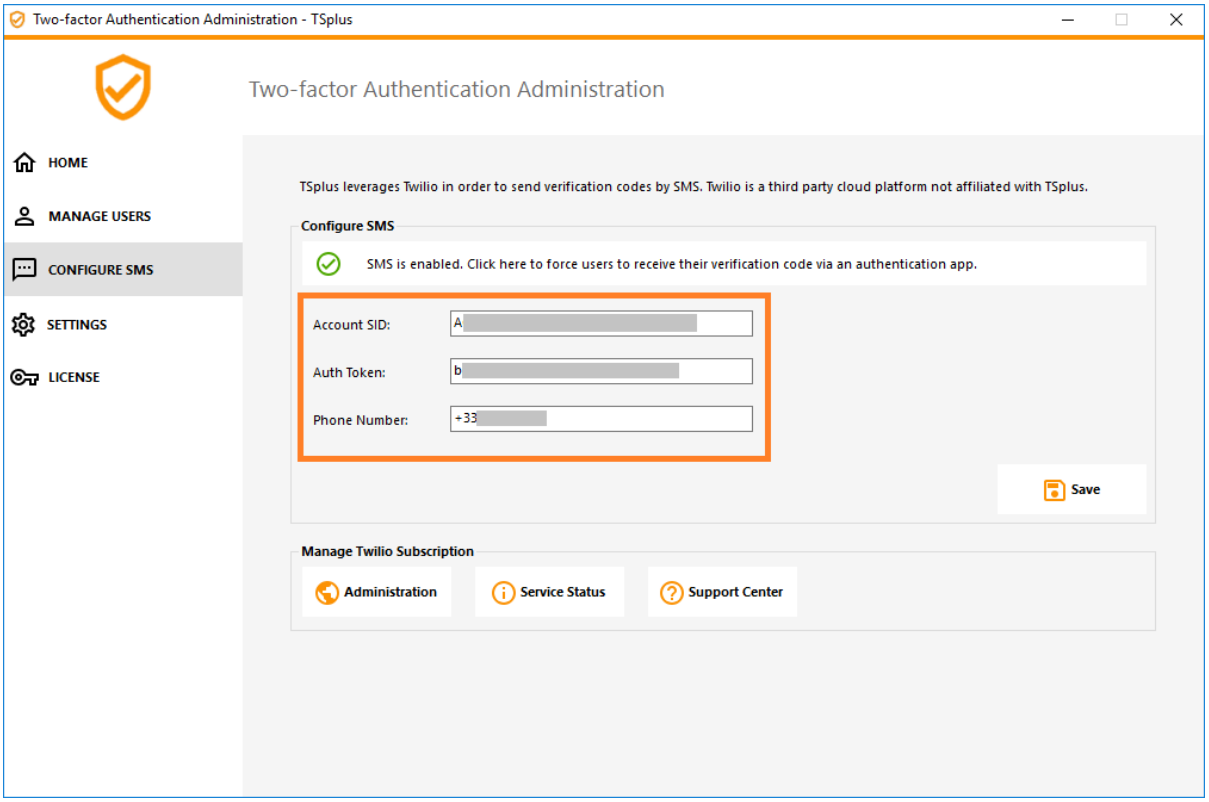
3. Der nächste Schritt ist nur für Testversionen erforderlich. Er ermöglicht es Twilio, die tatsächliche Telefonnummer zu überprüfen, an die SMS gesendet werden.

Geben Sie diese Nummer unter dem ein "Telefonnummern" Menü - "Verifizierte Anrufer-IDs" Tab :

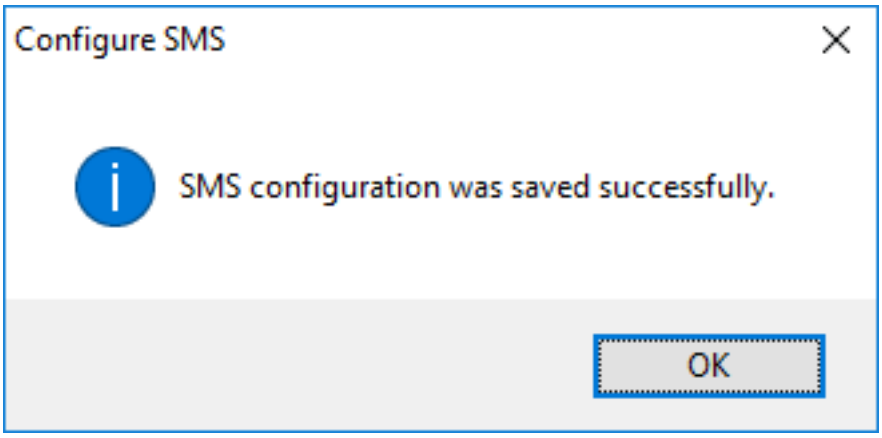


4. Sie können dann Ihre Kontos-ID, Authentifizierungstoken und eingeben **Testnummer** als die Telefonnummer auf dem SMS konfigurieren Tab von TSplus:





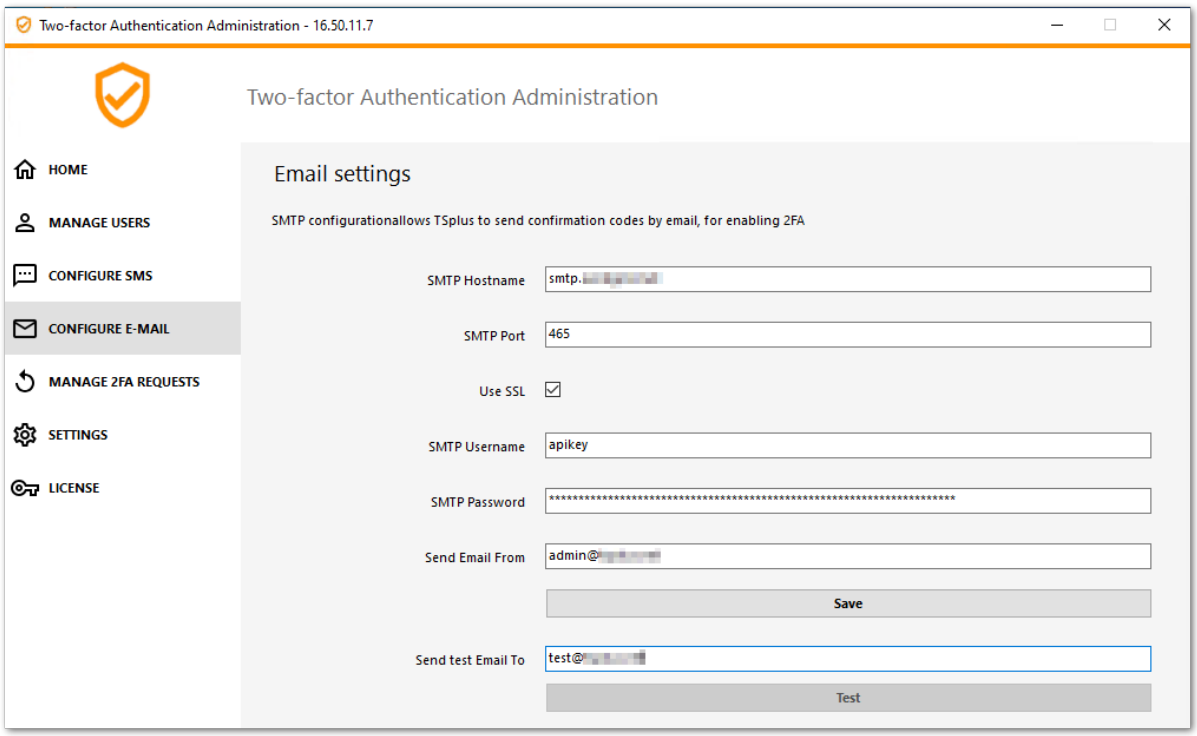
Dann klicken Sie auf Speichern. Die folgende Nachricht wird angezeigt:



Sie können Ihr Twilio-Abonnement auf dem Twilio-Abonnement verwalten Abschnitt, am Ende der SMS konfigurieren Verwalten Sie Ihr Konto, sehen Sie den Service-Status oder erreichen Sie das Twilio Support Center, indem Sie einfach auf die entsprechenden Schaltflächen klicken.

E-MAIL KONFIGURIEREN

Damit der Benutzer Bestätigungscodes per E-MAIL erhält, müssen Sie zuerst Ihr SMTP-E-Mail konfigurieren.



Anmeldung mit Zwei-Faktor-Authentifizierung

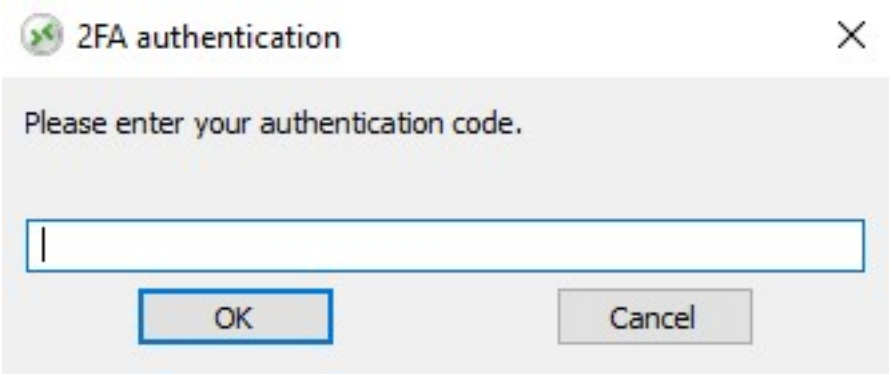
Sobald ein Benutzer sein TSplus-Konto in seiner Authentifizierungs-App konfiguriert hat, kann er sich mit seinem Passwort und dem von seiner Authentifizierungs-App, per SMS oder E-Mail

bereitgestellten Code verbinden.

Vom TSplus Remote Access Webportal:



Vom TSplus generierten Client:



TSplus-Anwendungsserver und Client-Geräte müssen die gleiche Zeit teilen. Das bedeutet, dass die Uhrzeit und das Datum des Servers mit einem Zeitserver synchronisiert werden müssen. Client-Geräte müssen ebenfalls eine Zeit-Synchronisierung haben, unabhängig von der Zeitzone, in der sie konfiguriert sind.

Wenn eine Authentifizierungsanfrage von einem Gerät kommt, dessen Datum und Uhrzeit nicht synchronisiert sind, oder wenn das Datum und die Uhrzeit des Servers nicht synchronisiert sind, kann diese Anfrage abgelehnt werden.

Die Validierung der Informationen zwischen dem Gerät und dem Server bezieht sich auf die UTC-Zeit.

Im **Einstellungen** Abschnitt, der Discrepency-Parameter wird verwendet, um den Gültigkeitszeitraum des Codes in Intervallen von 30 Sekunden zu verwalten.

Beispiel für Validierung oder gültige Authentifizierung:

- der Server ist mit einem Zeitserver synchronisiert, die Zeitzone ist UTC + 2, es ist 14:30 Uhr
- Das Gerät ist mit einem Zeitserver synchronisiert, die Zeitzone ist UTC + 1, es ist 13:30 Uhr.
- der Discrepency-Parameter ist auf 60 konfiguriert, d.h. eine Gültigkeitsdauer des Codes von 30 Minuten
- auf UTC-Zeit bezogen sind die Gerätez Zeit und die Serverzeit identisch.

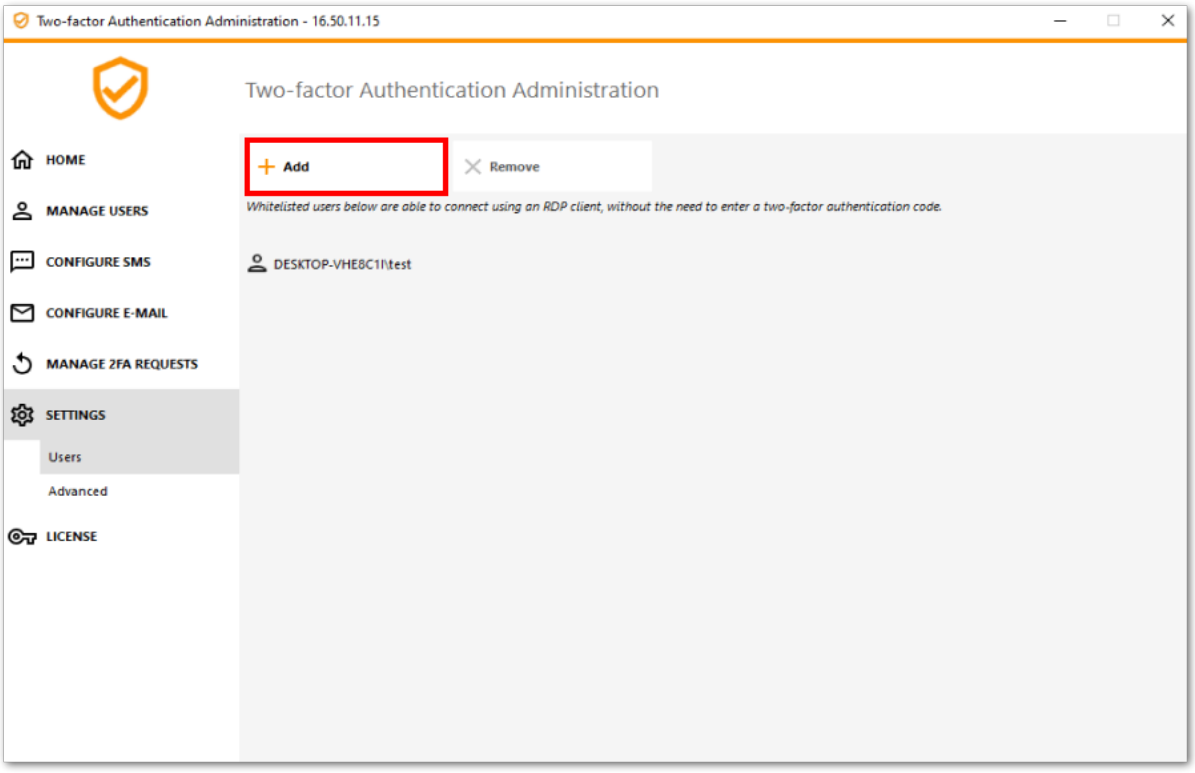
Beispiel für gültige oder ungültige Authentifizierung:

- der Server ist mit einem Zeitserver synchronisiert, die Zeitzone ist UTC + 2, es ist 14:30 Uhr
- Das Gerät ist nicht mit einem Zeitserver synchronisiert, die Zeitzone ist UTC-1, die Uhrzeit ist manuell auf 13:30 Uhr eingestellt.
- der Discrepency-Parameter ist auf 60 konfiguriert, d.h. eine Gültigkeitsdauer des Codes von 30 Minuten
- Die Serverzeit, die sich auf die UTC-Zeit bezieht, ist 12:30 Uhr.
- Die von dem Gerät mitgeteilte Zeit, die auf UTC-Zeit verweist, ist 14:30 Uhr.
- Der Unterschied beträgt 120 Minuten, der Validierungscode wird daher abgelehnt.

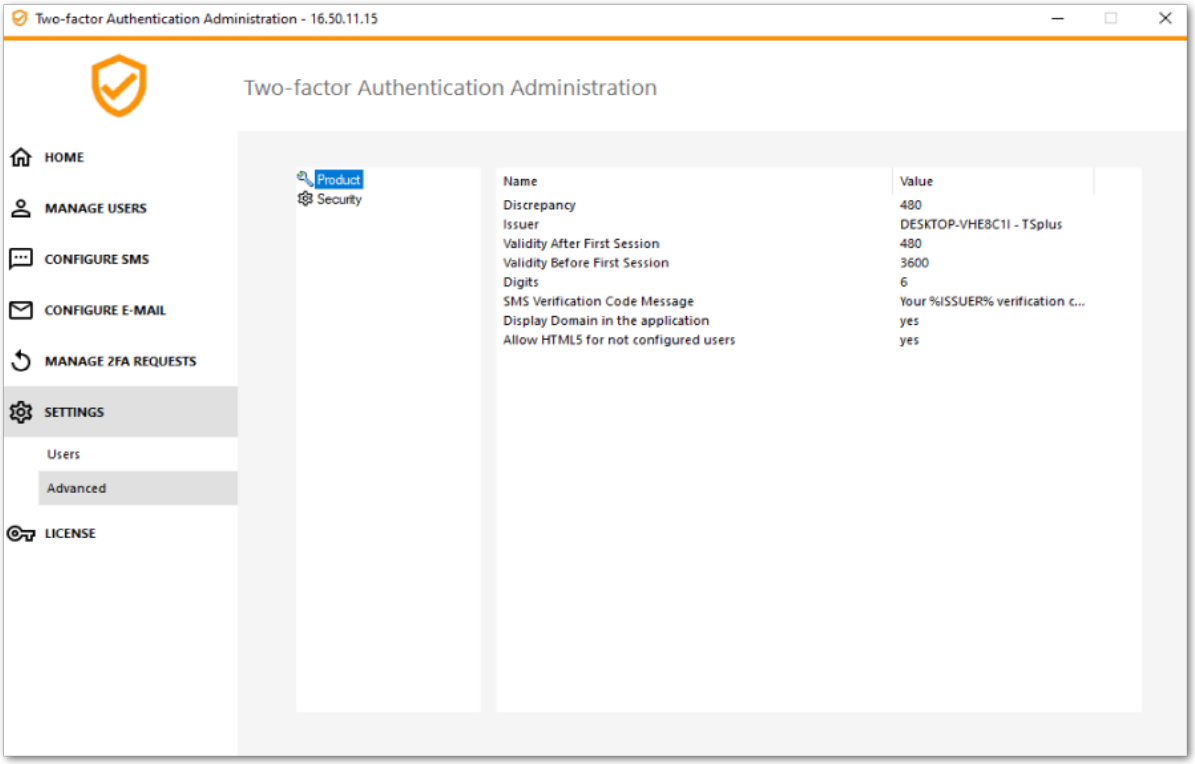
Einstellungen

Die Registerkarte Einstellungen ermöglicht es Ihnen, **Benutzer auf die Whitelist setzen, damit sie sich mit einem RDP-Client verbinden können, ohne einen Zwei-Faktor-Authentifizierungscode eingeben zu müssen.**

Klicken Sie auf die Schaltfläche „Hinzufügen“, um einen Benutzer hinzuzufügen, und entfernen Sie einen Benutzer, indem Sie ihn auswählen und auf die Schaltfläche „Entfernen“ klicken.



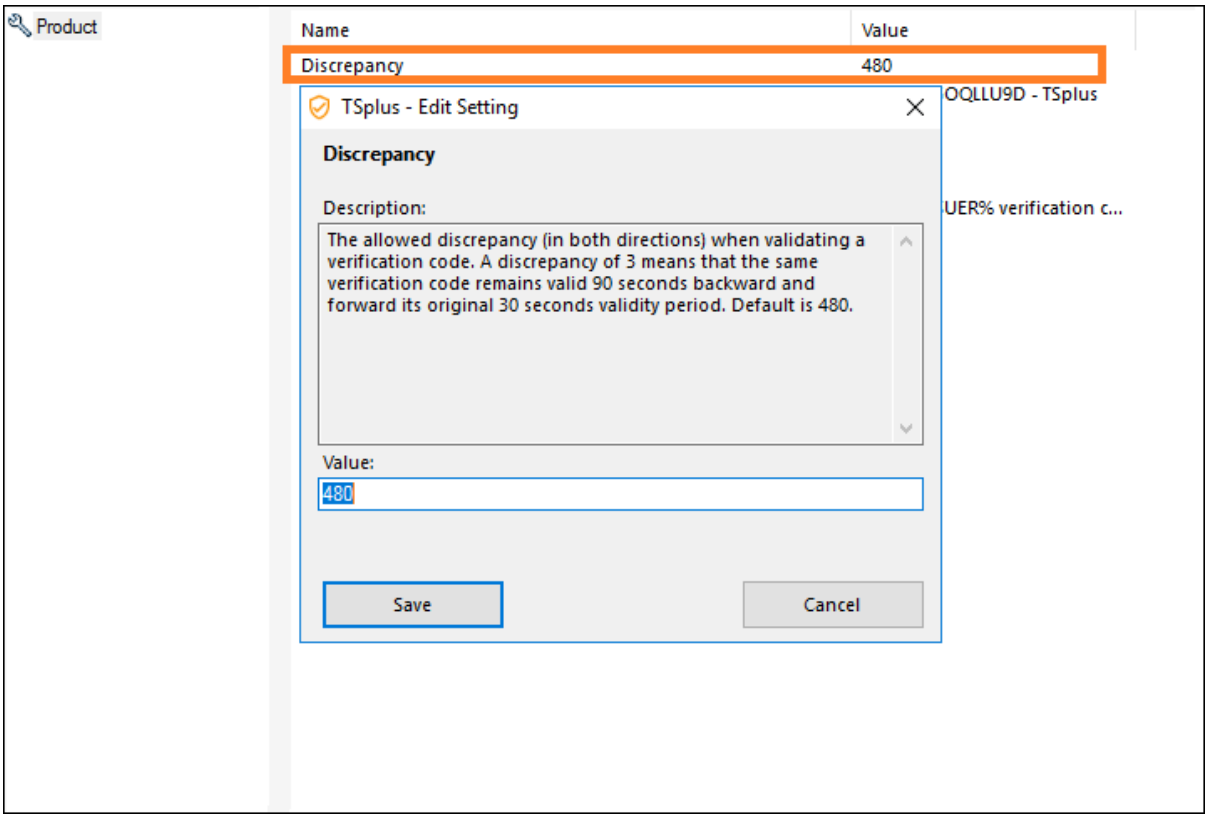
Der Reiter "Erweitert" ermöglicht es Ihnen, die Einstellungen für die Zwei-Faktor-Authentifizierung im Detail zu konfigurieren.



Abweichung

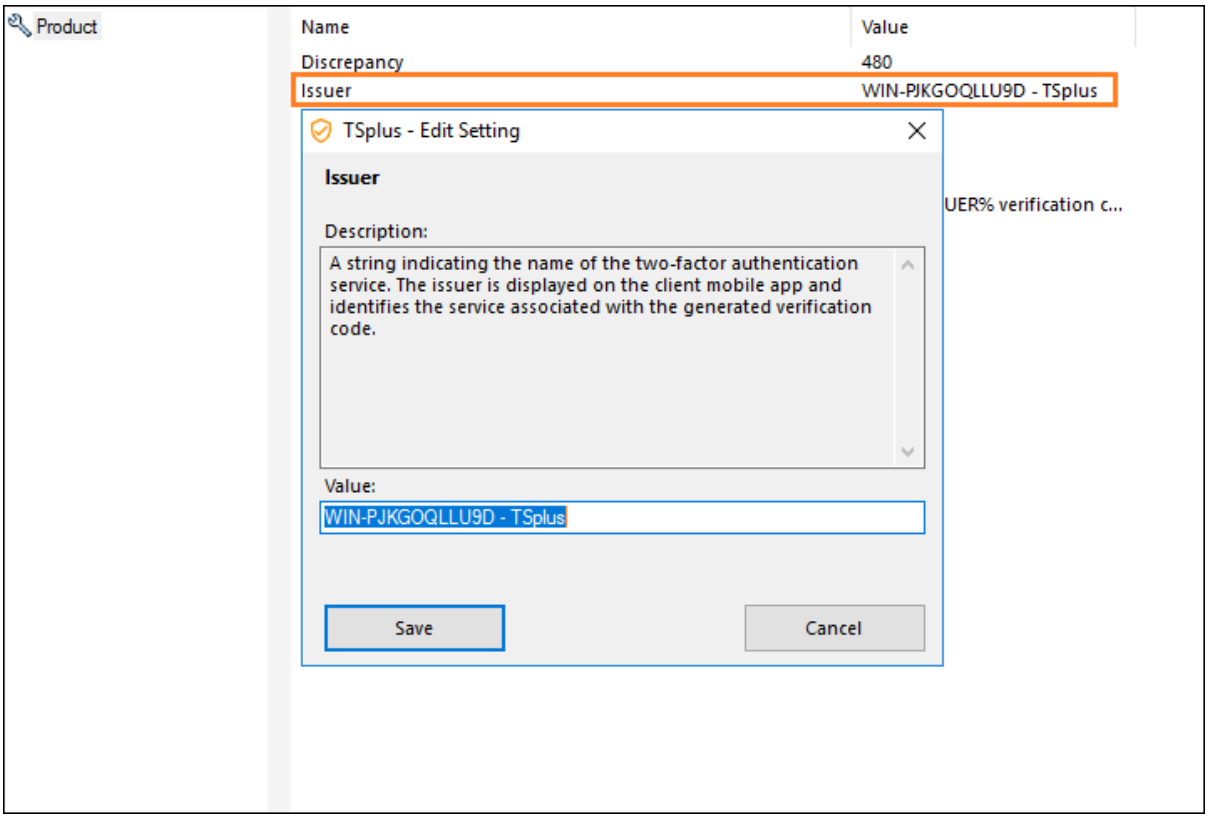
Sie können den Abweichungswert ändern, mit dem Sie die Validierungszeit eines Bestätigungscodes festlegen können.

Eine Abweichung von 3 bedeutet, dass der gleiche Verifizierungscode 90 Sekunden vor und nach seiner ursprünglichen Gültigkeitsdauer von 30 Sekunden gültig bleibt. Der Standardwert beträgt 480, was bedeutet, dass 480 x 30 Sekunden = 4 Stunden.



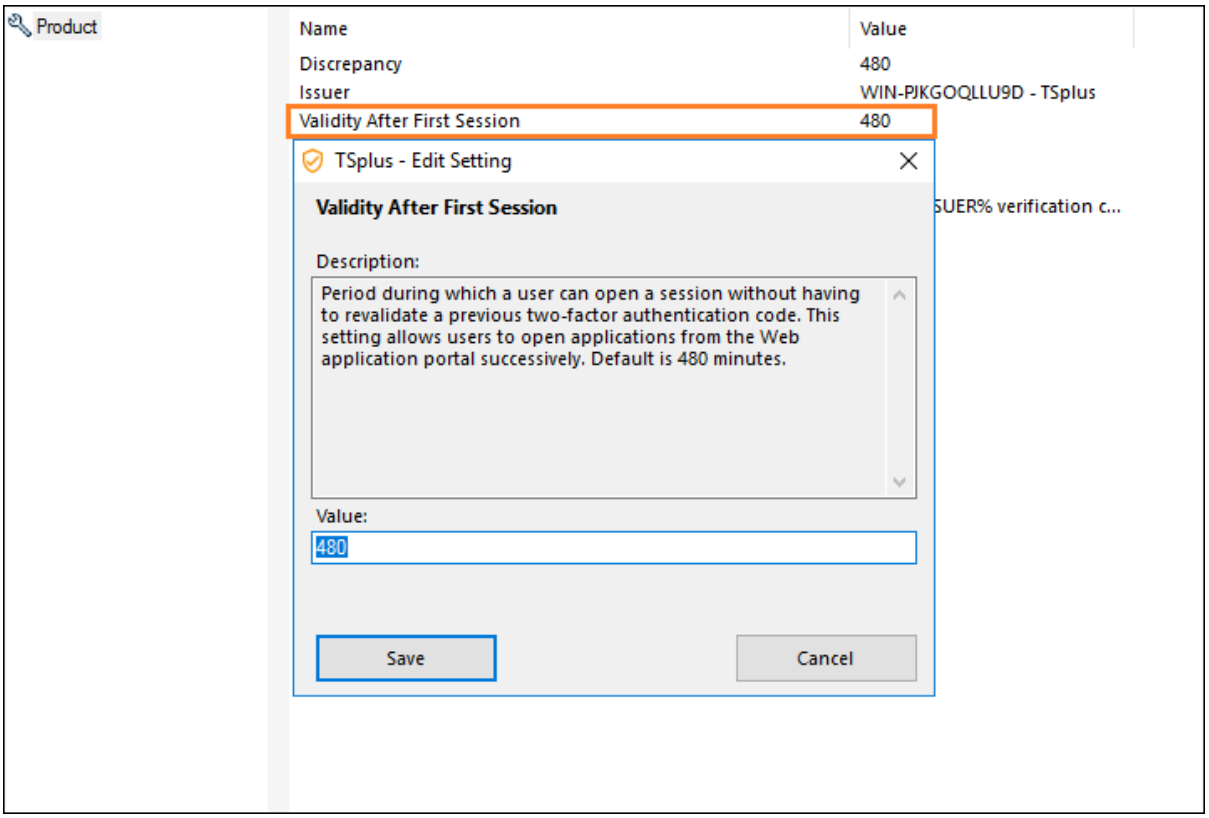
Herausgeber

Ein String, der den Namen des Zwei-Faktor-Authentifizierungsdienstes angibt. Der Aussteller wird in der mobilen App des Clients angezeigt und identifiziert den Dienst, der mit dem generierten Bestätigungscode verbunden ist. Standardmäßig besteht er aus dem Namen des Servers mit TSplus.



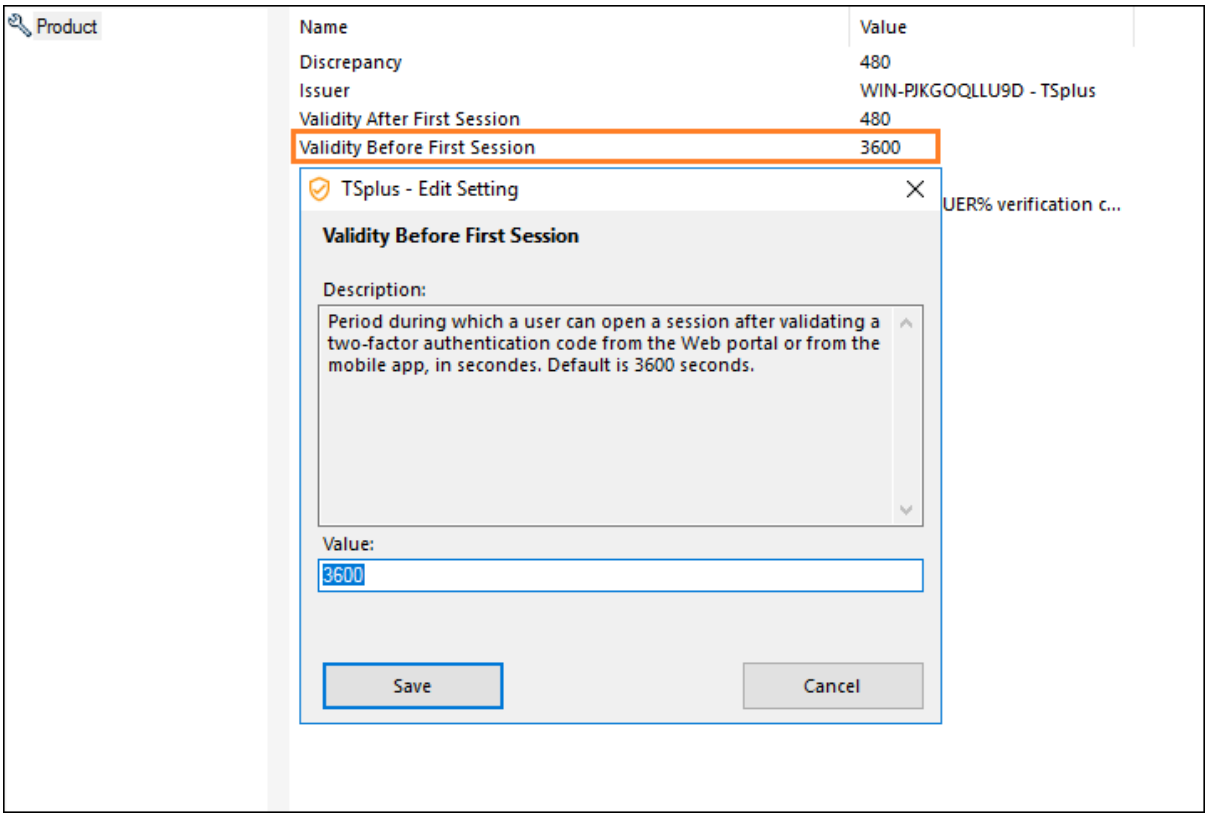
Gültigkeit nach der ersten Sitzung

Zeitraum, in dem ein Benutzer eine Sitzung öffnen kann, ohne einen vorherigen Zwei-Faktor-Authentifizierungscode erneut validieren zu müssen. Diese Einstellung ermöglicht es Benutzern, Anwendungen nacheinander über das Webanwendungsportal zu öffnen. Standardmäßig sind es 480 Minuten.



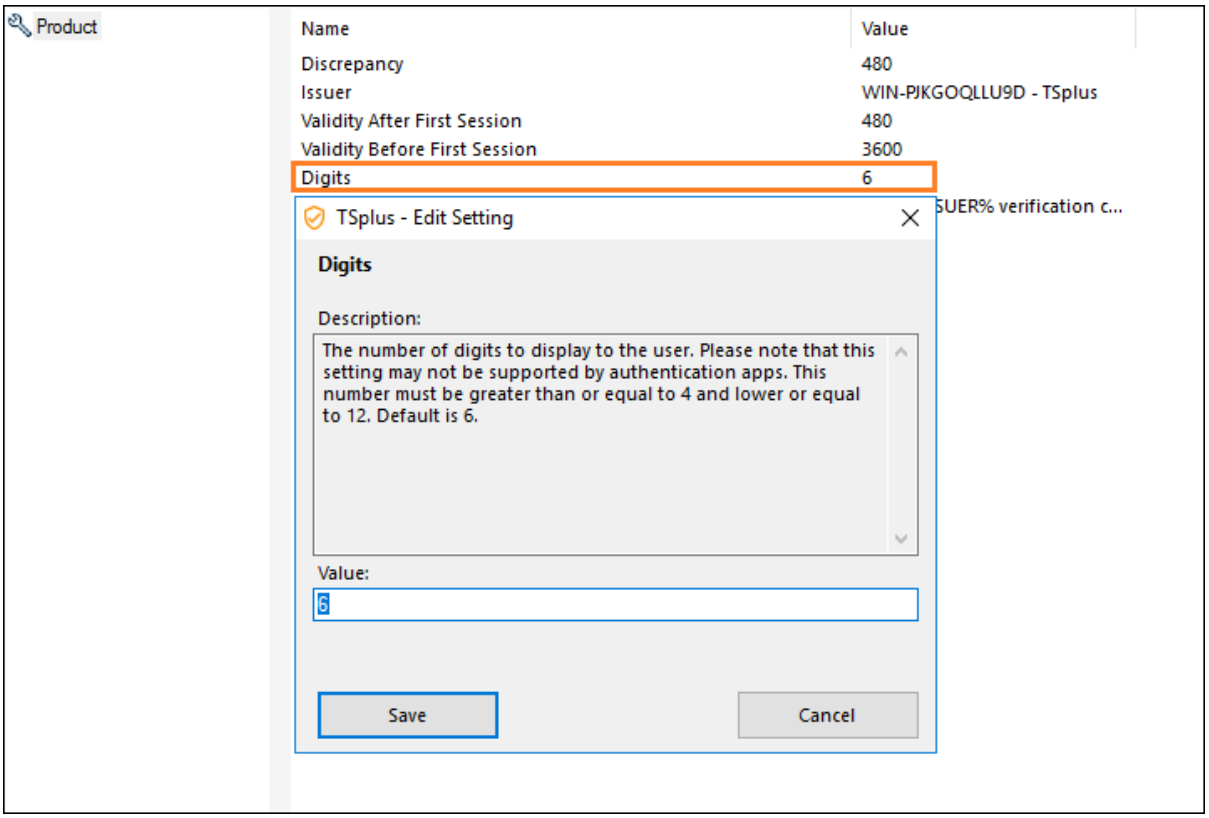
Gültigkeit vor der ersten Sitzung

Zeitraum, in dem ein Benutzer eine Sitzung öffnen kann, nachdem er einen Code zur Zwei-Faktor-Authentifizierung über das Webportal oder die mobile App validiert hat, in Sekunden. Standardmäßig sind es 3600 Sekunden.



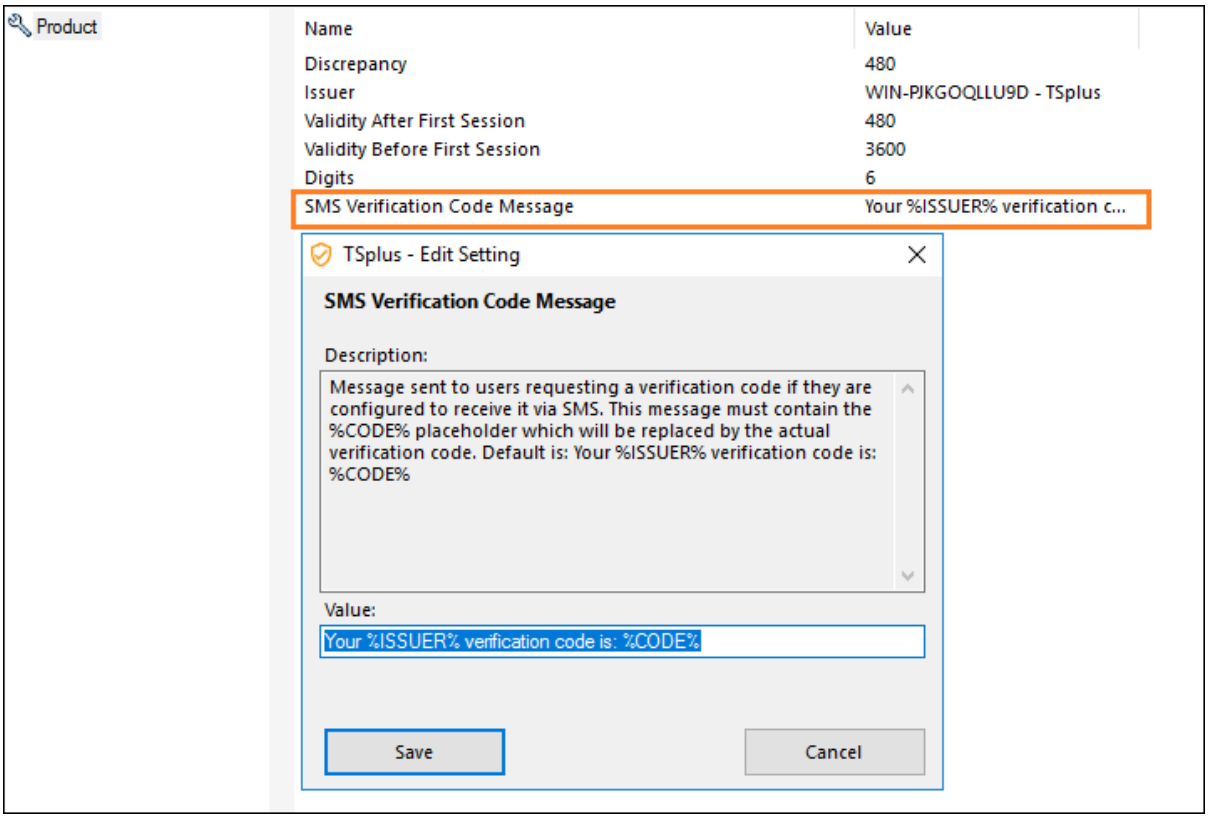
Digits

Die Anzahl der anzuzeigenden Ziffern für den Benutzer. Bitte beachten Sie, dass diese Einstellung möglicherweise nicht von Authentifizierungs-Apps unterstützt wird. Diese Zahl muss größer oder gleich 4 und kleiner oder gleich 12 sein. Standard ist 6.



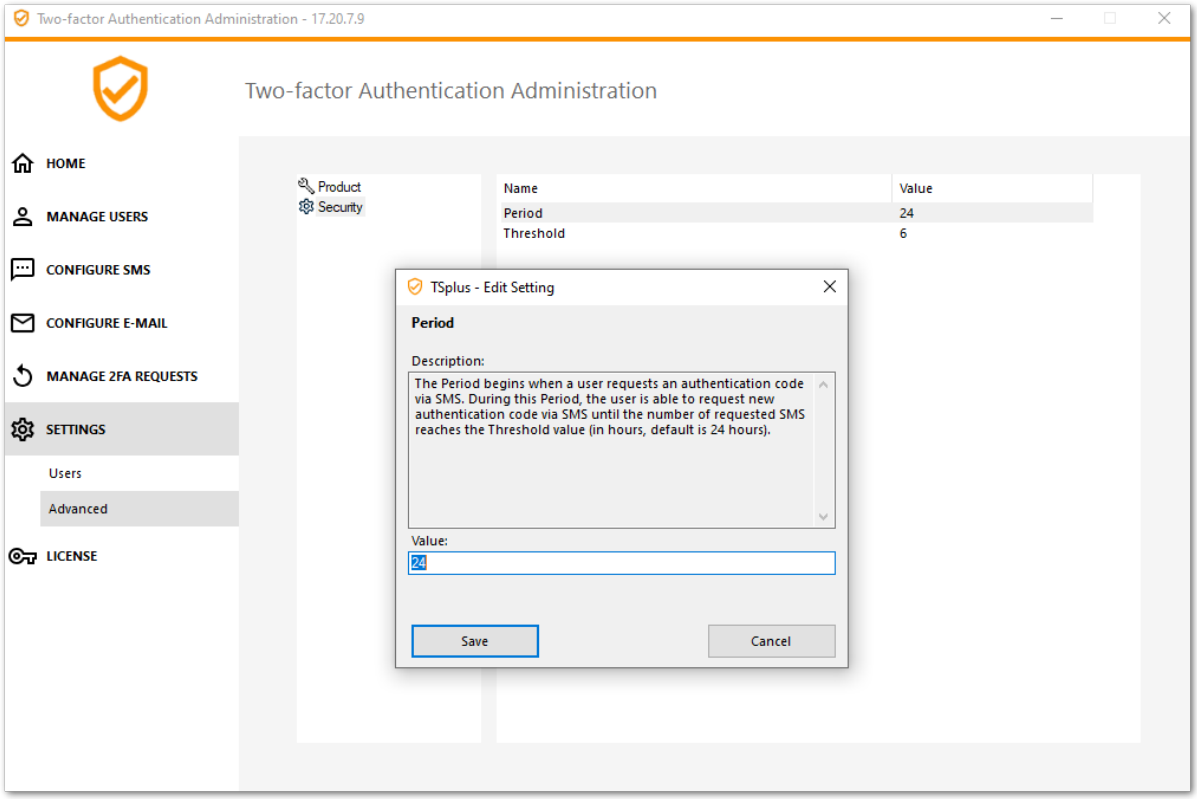
SMS-Bestätigungscode-Nachricht

Nachricht an Benutzer, die um einen Bestätigungscode gebeten werden, wenn sie so konfiguriert sind, dass sie ihn per SMS erhalten. Diese Nachricht muss den Platzhalter %CODE% enthalten, der durch den tatsächlichen Bestätigungscode ersetzt wird. Standardmäßig lautet: Ihr %ISSUER% Bestätigungscode lautet: %CODE%



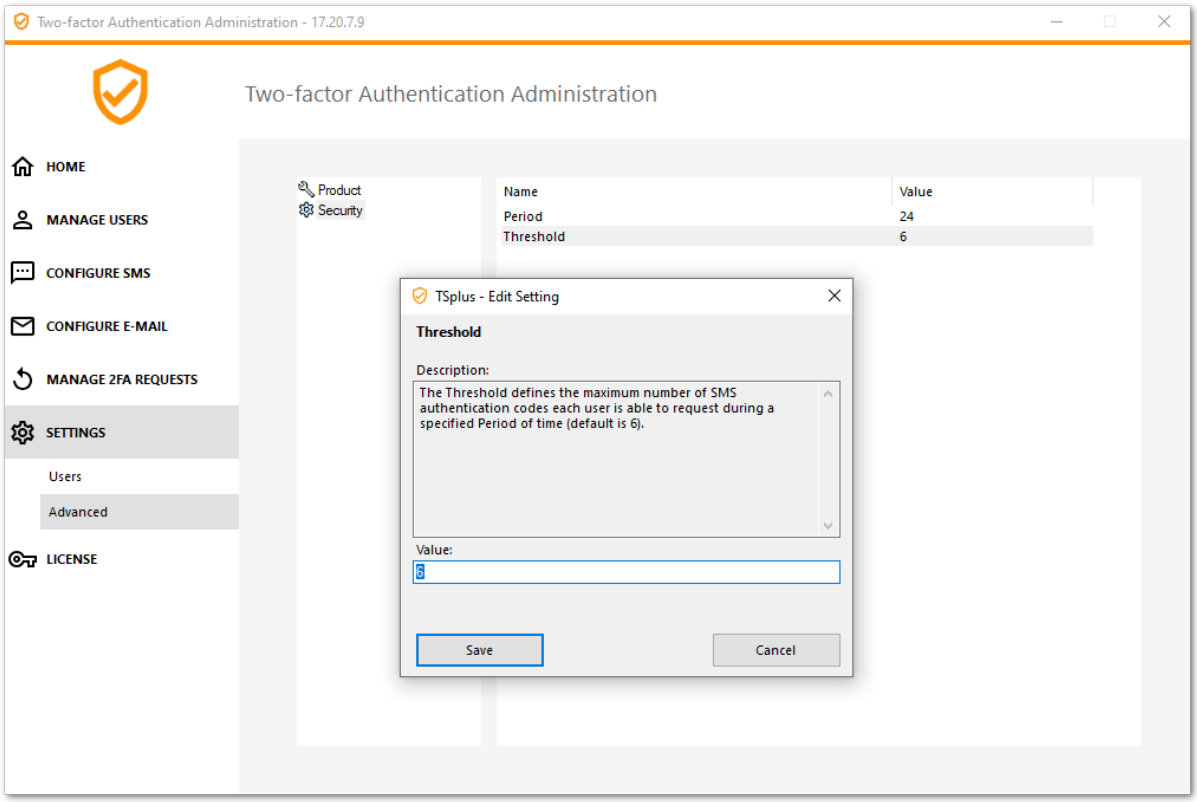
SMS-Sicherheitszeitraum

Der Zeitraum beginnt, wenn ein Benutzer einen Authentifizierungscode per SMS anfordert. Während dieses Zeitraums kann der Benutzer einen neuen Authentifizierungscode per SMS anfordern, bis die Anzahl der angeforderten SMS den Schwellenwert (in Stunden, Standard ist 24 Stunden) erreicht.



SMS-Sicherheitsgrenze

Der Schwellenwert definiert die maximale Anzahl von SMS-Authentifizierungscodes, die jeder Benutzer während eines bestimmten Zeitraums anfordern kann (Standard ist 6).



Universal Printer (novaPDF)

Der TSplus Universal Printer ermöglicht es Ihnen, Dokumente von jedem PC oder mobilen Gerät, das von TSplus Remote Access unterstützt wird, vorzuschauen oder zu drucken. Der Universal Printer ist relevant von einer HTML5-Sitzung und wenn er über einen generierten Client verbunden ist. Der Universal Printer ist nicht relevant, wenn der standardmäßige RDP-Client (mstsc.exe) verwendet wird, da Drucker zwischen Server und Client geteilt werden können.

Starting Remote Access version 17, Universal Printer nutzt novaPDF (https://www.novapdf.com/) um 100 % branchenspezifische PDF (Portable Document Format) Dateien aus dem Remote-Dokument zu erstellen. Das generierte PDF-Dokument wird dann an den gewünschten lokalen Drucker gesendet. Der Universal Printer (novaPDF) ersetzt den Universal Printer (CustPDF) und den Universal Printer (GhostScript), die eingestellt und nicht mehr auf Ihrem Remote Access-Server installiert werden können.

Zwei Drucker stehen für das Remote-Drucken zur Verfügung: Universal Printer und Virtual Printer. Obwohl der Virtual Printer eine bessere Druckleistung bietet, ist er nicht mit dem HTML5-Client kompatibel und erfordert die Installation einer Client-Anwendung. Daher wird der Universal Printer als Standarddrucker nach der Einrichtung von Remote Access festgelegt. Siehe TSplus Virtual Printer .

Anforderungen

NovaPDF11Service-Dienst sollte in der Ausschlussliste jeder aktiven Firewall oder Antivirensoftware stehen.

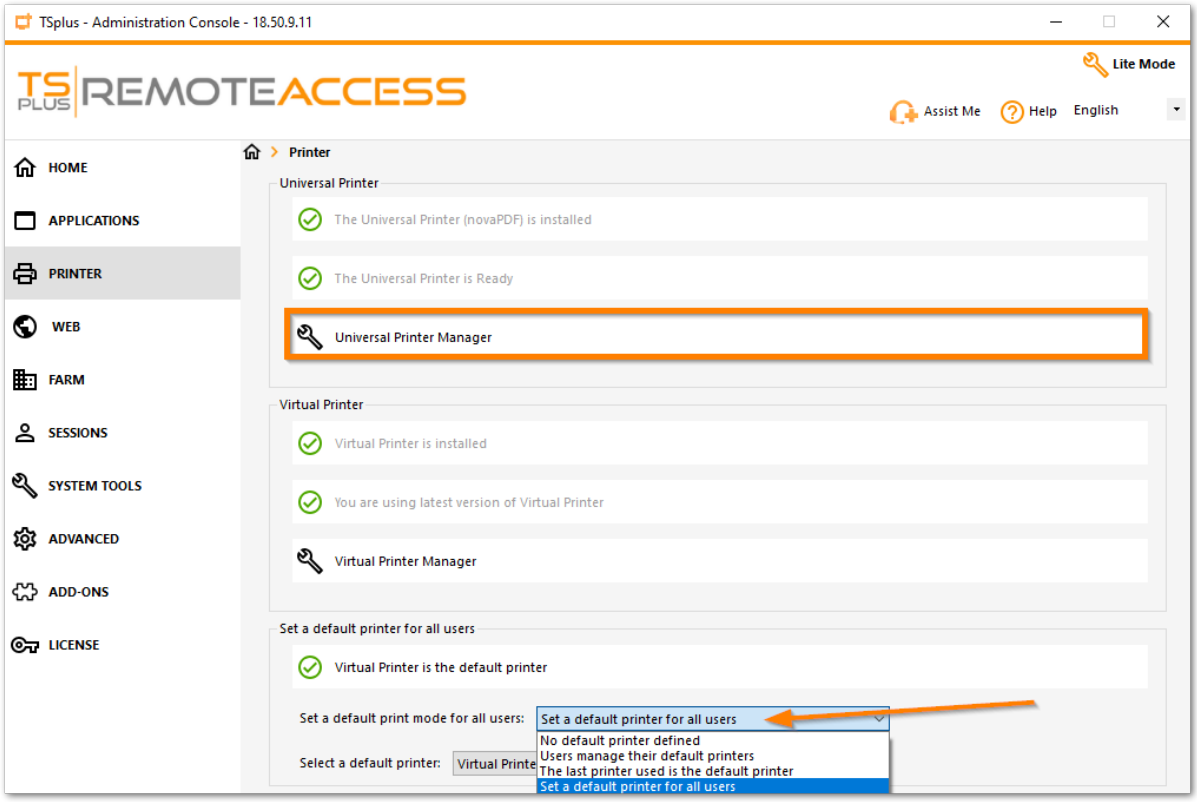
Konfigurieren Sie den Universaldrucker

Um Ihren Universal Printer zu konfigurieren, öffnen Sie das AdminTool und klicken Sie auf die Drucker Menü.

Um auf das Steuerfeld des Universal Printers zuzugreifen, navigieren Sie bitte über das AdminTool: Drucker > Universal Printer Manager.

Einen Standarddrucker für alle Benutzer festlegen

- Kein Standarddrucker definiert: Die Standarddruckerkonfiguration des Benutzers ist nicht betroffen.
- Benutzer verwalten ihre Standarddrucker: die Option „Windows meinen Standarddrucker verwalten lassen“ ist deaktiviert, und es liegt daher am Benutzer, seinen Standarddrucker auszuwählen.
- Der letzte verwendete Drucker ist der Standarddrucker: die Option „Windows meinen Standarddrucker verwalten lassen“ ist aktiviert.
- Einen Standarddrucker für alle Benutzer festlegen: der Administrator zwingt den Benutzer, den Standarddrucker festzulegen.



Der Abschnitt Universaldrucker zeigt vier Kacheln, die es Administratoren ermöglichen, zu:

- Überprüfen Sie den Status der Universal Printer-Installation. Wenn der Universal Printer nicht installiert ist, wird durch Klicken auf die Kachel der Universal Printer installiert.
- Überprüfen Sie den Druckstatus des Universaldruckers. Wenn der Universaldrucker nicht bereit ist, Druckaufträge zu empfangen, kann die Kachel zusätzliche relevante Informationen über den Fehler anzeigen.
- Überprüfen Sie, ob der Universaldrucker als Standarddrucker festgelegt ist. Wenn der Universaldrucker nicht als Standarddrucker festgelegt ist, wird er durch Klicken auf die Kachel

als Standarddrucker festgelegt. Bitte beachten Sie, dass dieses Verhalten von Ihren Benutzern überschrieben werden kann, sofern ihnen dies gestattet ist.

- Die Fliese mit dem Namen **Universeller Drucker-Manager** führt zu einem detaillierteren Bildschirm, der zusätzliche Aktionen und Eigenschaften bietet, wie das Entfernen des Universaldruckers.

Universeller Drucker-Manager

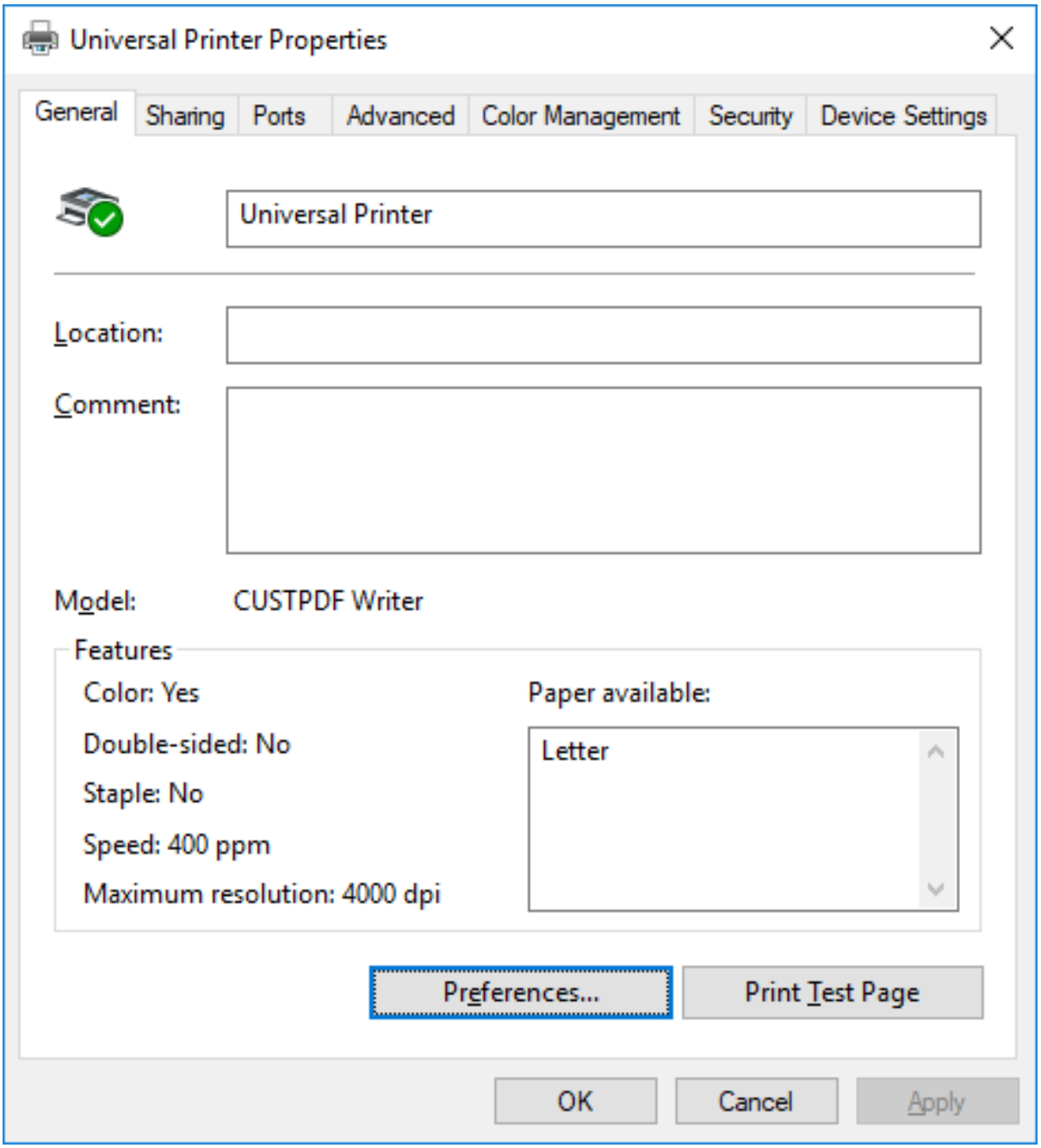
Der Universal Printer Manager ermöglicht es dem Administrator, den Status des Universal Printers zu überprüfen, den Universal Printer zu entfernen, auf die Druckwarteschlange und die Druckereigenschaften zuzugreifen.

Insbesondere ermöglicht die Schaltfläche am Ende der Seite den Administratoren:

- **Entfernen Sie den Universaldrucker** Deinstallieren Sie den Universal Printer. Er kann später von diesem Bildschirm aus neu installiert werden.

- **Drucker anzeigen** Öffnet ein Fenster, in dem Sie den Status Ihrer Druckdokumente sehen, den Druckauftrag pausieren, fortsetzen oder abbrechen können. Sie können auch Ihre Druckeinstellungen und -eigenschaften festlegen.

- **Universelle Druckereigenschaften** öffnet dieses Fenster, in dem Sie alle Druckeigenschaften sehen können. Nach der Registerkarte Allgemein gibt es Registerkarten für Freigabe, Ports, Erweitert, Farbmanagement, Sicherheit und Geräteeinstellungen. Am unteren Rand des Popup-Fensters befindet sich der Drucker **Eigenschaften** ermöglicht es Administratoren, die Seitengröße für den Druck von A4 auf jedes beliebige Druckformat einzustellen. Sie können auch zwischen zwei Druckausrichtungen wählen: Hochformat oder Querformat.

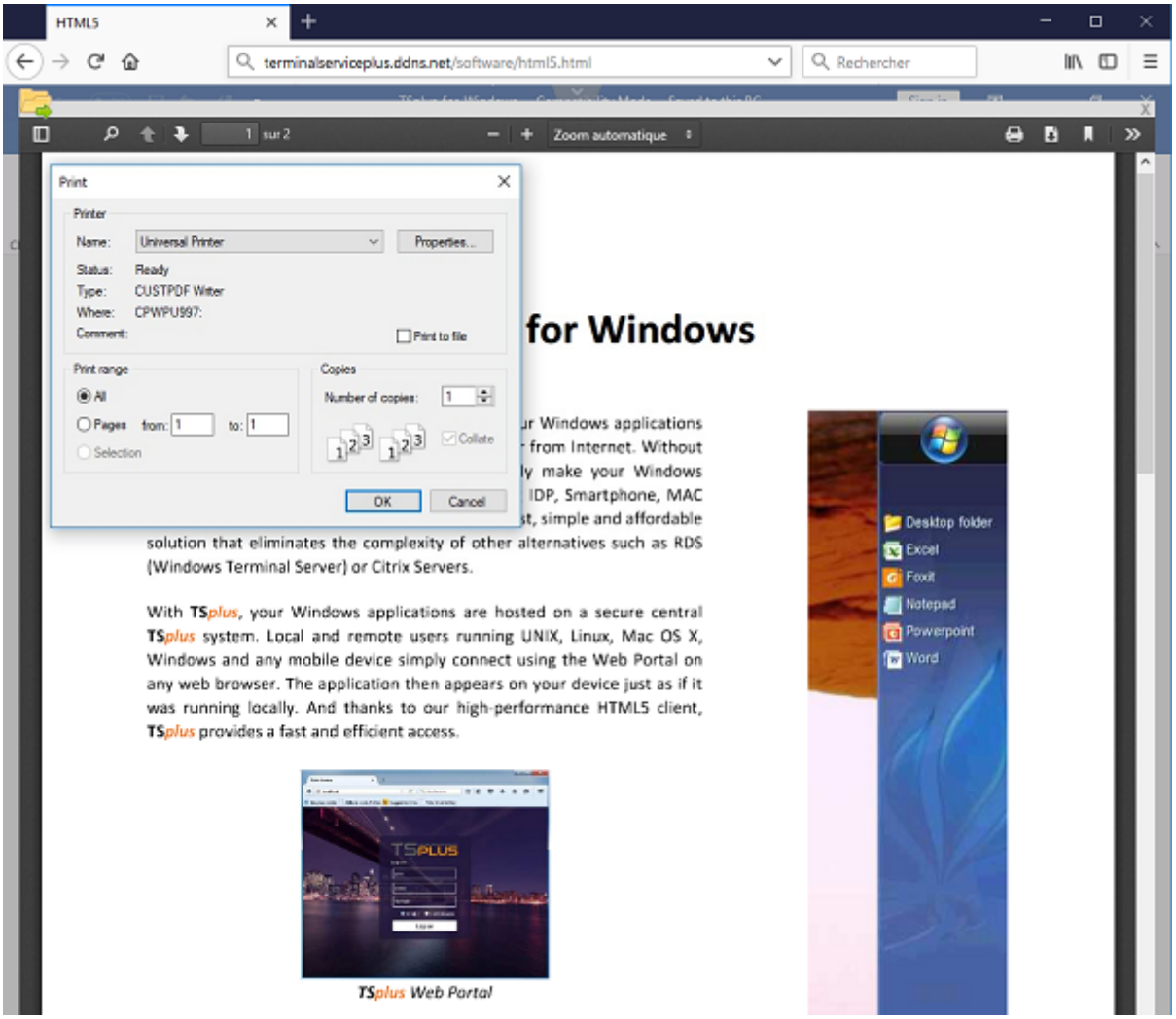


Hinweis: Der Universal Printer nutzt novaPDF, mit dem Administratoren Profile erstellen können, um Schriftarten, Grafiken, Wasserzeichen, Überlagerungen und mehr über die zu definieren. **Profile verwalten** Schaltfläche befindet sich unten im Abschnitt Seitenformat und Ausrichtung im Popup-Fenster der Druckereigenschaften. Sollte ein Profil standardmäßig ausgewählt sein, dann die **Zeigen Sie das Dialogfeld "Profile auswählen" vor dem Drucken an** kann überprüft werden, um dem Benutzer die Auswahl eines Profils vor dem Drucken zu ermöglichen. Bitte beachten Sie die novaPDF-Dokumentation für weitere Details zu Profilen: Profilmanager .

Drucken mit dem Universaldrucker

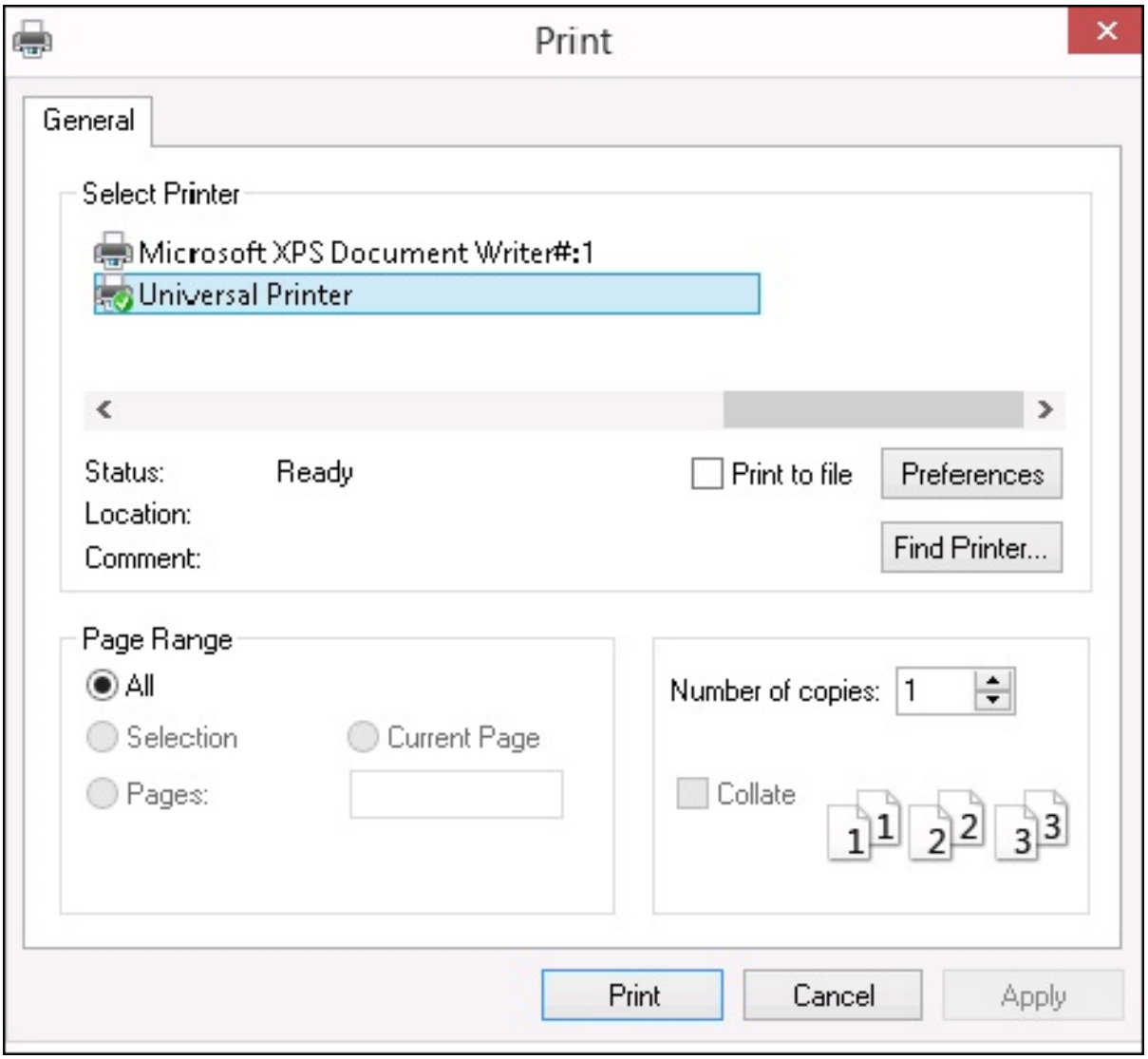
Während des Druckens mit diesem Drucker wird das Dokument in der Druckwarteschlange automatisch von dem Universal Printer (novaPDF) in eine PDF-Datei umgewandelt.





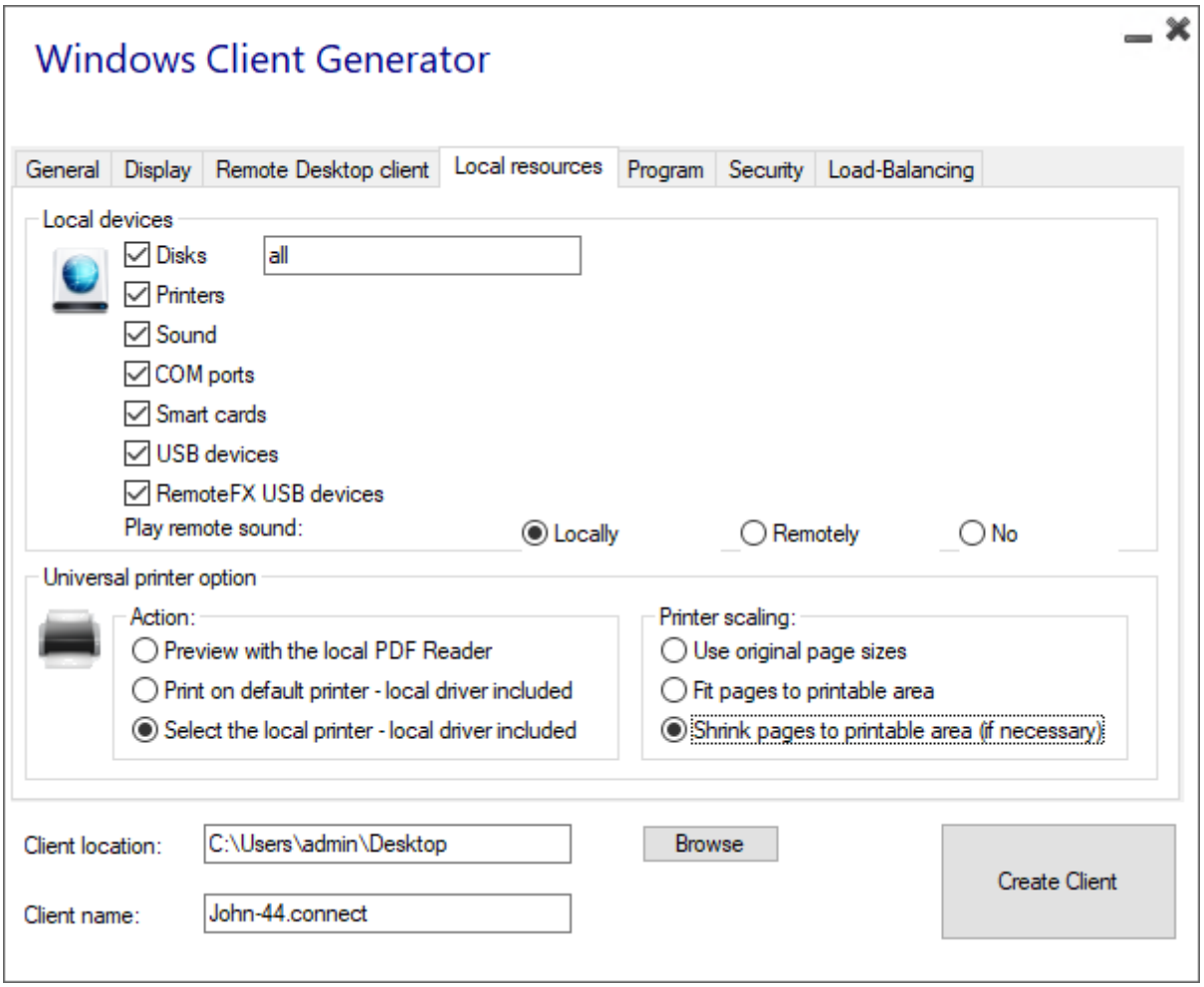
Die generierte PDF-Datei wird dann an den lokalen PDF-Reader des Arbeitsplatzes des Benutzers gesendet.

Jeder Druckauftrag wird geöffnet, sobald er auf der lokalen Festplatte des Benutzers bereit ist. Der Druckprozess beginnt, sobald die PDF-Datei auf die Client-Seite übertragen wurde, was garantiert, dass der Druckauftrag ohne Verzögerung gestartet wird.



Drucken von Optionen mit dem Client-Generator konfigurieren

Sie können aus 3 Druckoptionen im Tab Lokale Ressourcen von der wählen. Portabler Client-Generator
Wenn Sie den TSplus-Verbindungsclient verwenden, müssen Sie mindestens die **C: Laufwerk oder alle Festplatten**



- **Lokale PDF-Reader-Vorschau** Das Dokument wird auf der Arbeitsstation des Clients bereitgestellt, und der lokale Standard-PDF-Reader öffnet die empfangene PDF-Datei. Der Benutzer kann es dann drucken oder eine Kopie auf seinem lokalen Datenträger speichern (dieses Verhalten wird beim Drucken aus einer HTML5-Sitzung erwartet).

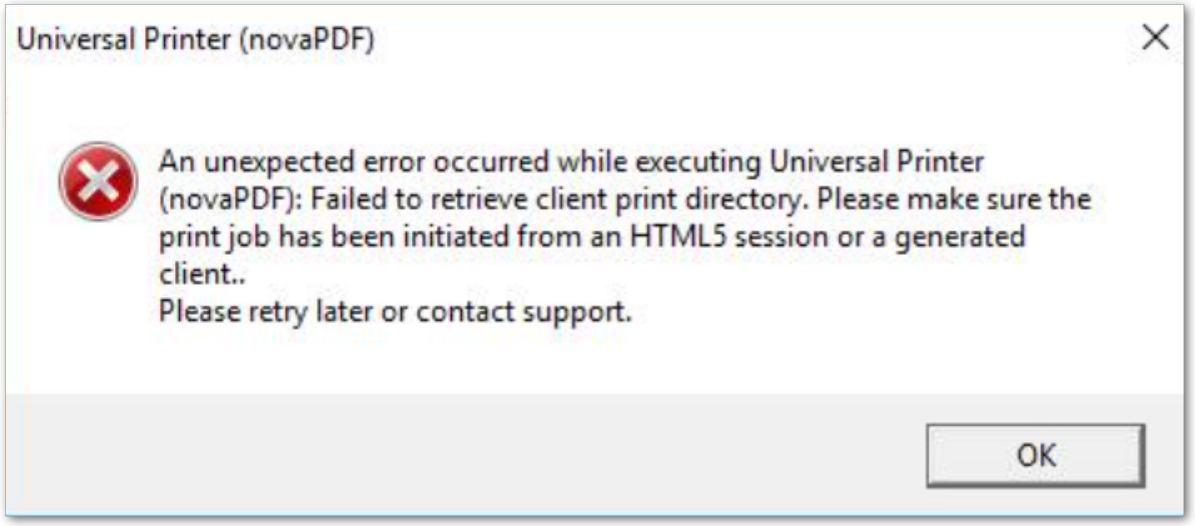
- **Drucken auf dem Standarddrucker des Benutzers** Das Dokument wird automatisch von dem Standarddrucker des Benutzers gedruckt (diese Option ist nur verfügbar, wenn der TSplus-Verbindungsclient verwendet wird). Diese Option wird für Benutzer bevorzugt, die tagsüber viele Druckaufträge drucken müssen und denselben Drucker zu diesem Zweck verwenden.

- **Wählen Sie einen lokalen Drucker** der Benutzer kann einen seiner lokalen Drucker auswählen (diese Option ist nur verfügbar, wenn der TSplus-Verbindungsclient verwendet wird).

Heutzutage kommen viele Menschen beim Lesen von PDF-Dateien ohne eine externe Anwendung aus. Sowohl Firefox als auch Chromium, die Open-Source-Version des Chrome-Browsers von Google, werden mit integrierten PDF-Readern ausgeliefert, sodass für die meisten

Benutzer kein externes Plugin mehr erforderlich ist.

ZU IHRER INFORMATION
Wenn das Laufwerk C: nicht zugeordnet ist, erhält der Benutzer diese Fehlermeldung.



novaPDF-Drucker konfigurieren

Von **Druckereinstellungen** > **Werkzeuge** > **Passwort** , Sie können:

- Standardpasswort bearbeiten
- Ändern Sie die Sprache der Benutzeroberfläche des Profilmanagers
- Überwachen Sie den Fortschritt von Druckaufträgen in Echtzeit
- Überprüfen Sie die Druckerhistorie

Druckauftrag in einem neuen Tab öffnen

Standardmäßig werden Druckaufträge aus einer HTML5-Sitzung wie vor Version 17.10 in einem Pop-up angezeigt.

Es ist möglich, dieses Verhalten zu ändern und Druckaufträge in einem neuen Tab des Browsers mit der folgenden Einstellung zu öffnen: **Admin-Tool** > **Erweitert** > **Sitzung** > **Druckaufträge in neuem Tab öffnen**

Profilee

Profiles ermöglicht es, Layouts, Wasserzeichen, Komprimierungsstufen und vieles mehr anzupassen. Der Profilmanager erlaubt es Ihnen, Profile zu verwalten. Profile bestehen aus Konfigurationen, die beim Drucken mit dem Universal Printer verwendet werden. Zum Beispiel können Sie verschiedene Druckprofile einrichten, die auf spezifische Ausgabeanforderungen

zugeschnitten sind, wie das Verteilen von PDFs, hochwertiges Drucken, Überprüfungszwecke oder das Kennzeichnen von Dokumenten als vertraulich.

Um den Profil-Manager zu öffnen, öffnen Sie Geräte und Drucker, klicken Sie mit der rechten Maustaste auf den Universaldrucker und wählen Sie Druckeinstellungen. Klicken Sie dann auf die **Profile verwalten** Taste. Das Standardpasswort lautet: pass@word1

Verstehen der Standardprofile

- **Standardprofil** Das Standardprofil ist dafür vorgesehen, um ein einzelnes oder mehrere Dokumente gleichzeitig zu drucken. Geeignet für die meisten Szenarien.
- **Druckprofil für geöffnete Dokumente** Verwenden Sie dieses Profil, um ein Dokument automatisch zu drucken, wenn es mit einem PDF-Viewer geöffnet wird. Dieses Profil ist nützlich, um einen Klick beim Drucken aus einer HTML5-Sitzung zu sparen.

Beim Öffnen einer HTML5-Sitzung wird das Profil für geöffnete Dokumente automatisch für den aktuellen Benutzer ausgewählt. Die automatische Druckfunktion in der HTML5-Sitzung wird jedoch deaktiviert, wenn eine andere Sitzung derzeit für denselben Benutzer im RDP-Modus geöffnet ist. In diesem Fall wird standardmäßig das Standardprofil angewendet.

Hinweis Das Profil für geöffnete Dokumente kann für UWP-Anwendungen wie Notepad in Windows 11 nicht automatisch ausgewählt werden, da diese Anwendungen so konzipiert sind, dass sie in vollständiger Isolation mit dem System laufen. Es bleibt jedoch möglich, dass der Benutzer das zu verwendende Profil manuell auswählt und es standardmäßig für die nächsten Druckaufträge auswählt. Momentan gibt es keinen Workaround. Die Neugestaltung des novaPDF-Druckers, die für das nächste große Release von novaPDF im vierten Quartal 2024 geplant ist, wird diese Einschränkung aufheben.

Welches Profil kann der Benutzer wählen?

Standardmäßig können Benutzer auswählen, welches Profil sie aus den beiden Standardprofilen verwenden möchten. Benutzer dürfen ein Profil als aktiv auswählen, und das Dialogfeld "Profil auswählen" wird für die nächsten Druckaufträge nicht angezeigt. Administratoren können ein oder mehrere Profile definieren, die allen Benutzern zur Verfügung stehen. Diese Entscheidung hat Vorrang vor den Auswahlmöglichkeiten der Benutzer. Siehe https://www.novapdf.com/printer-manager-profiles-help.html .

Wichtig Es wird empfohlen, die vorhandenen Profile zu kopieren, um personalisierte Profile zu erstellen, da vorhandene Profile mehrere Funktionen enthalten, die für die meisten Installationen erforderlich sind, wie eingebettete Schriftarten im generierten PDF-Dokument.

Fehlerbehebung

Bitte finden Sie unten Fehlerbehebungstipps zur Behebung von Problemen mit dem Universal

Printer (novaPDF).

Aktuell bleiben

- Das Aktualisieren des Verbindungsclients kann einige Probleme beheben, die auf der Client-Seite auftreten.
- Überprüfen Sie das Änderungsprotokoll, um zu sehen, ob eine neuere Version Ihr Problem behebt bei https://dl-files.com/TSplus-changelog.html
- Denken Sie daran, dass das Entwicklungsteam nur die neueste Codebasis unterstützen kann.

Verstehen, welcher Teil des Druckprozesses fehlgeschlagen ist

- Wurde der Druckauftrag in der Druckwarteschlange erstellt? Was ist sein Status?

Protokolle zur Druckfehlererfassung

- **Sitzungsöffnungsprotokolle** insbesondere nützlich bei Problemen wie dem fehlgeschlagenen Abrufen des Druckverzeichnisses des Clients, das sich befindet unter **C:\wsession\trace** .
- **AdminTool-Anwendungsprotokolle** befindlich bei **C:\Program Files (x86)\TSplus\UserDesktop\files** .
- **Universal Printer-Protokolle** , das Druckauftrags an die Client-Seite zu senden, die sich befindet unter **C:\wsession\UniversalPrinter\logs** .
- **Sitzungsereignisprotokolle** für den druckenden Benutzer, Handhabung von Wiederverbindungen, befindet sich in **%appdata%\UniversalPrinter\logs** .

Protokolle für Druckerinstallationsprobleme sammeln

- **Einrichtungsprotokoll** 2024-02-XX #XX.txt verfügbar in der **%temp%** Verzeichnis.
- **universelle Druckermanagement** _XX022024.txt befindet sich unter **C:\Program Files (x86)\TSplus\UserDesktop\files** .
- Alle .txt-Dateien, die sich in **C:\Program Files (x86)\TSplus\UserDesktop\files\UniversalPrinter** .

Protokollierung von Fehlern beim Drucken auf der Client-Seite, wenn der Verbindungsclient verwendet wird

- **version.dat** Datei. Bitte immer empfehlen, den Connection Client auf die neueste Version zu

aktualisieren.

- **Verbindungsclient** und **Universeller Drucker-Client** Protokolle. Diese Protokolle können aktiviert werden, indem der folgende Schlüsselwert in der Registrierung erstellt wird: **HKEY_LOCAL_MACHINE\Software\Digital River\ConnectionClient\Debug" = "true"** Die resultierenden Protokolle befinden sich hier: **C:\Benutzer \RDP6\logs** .

Aktualisierung von TSplus Remote Access

Überprüfen Sie unsere Fehlerbehebungen und Verbesserungen, indem Sie auf klicken _ Änderungsprotokoll _

Unser Entwicklungsteam arbeitet täglich daran, die Stabilität und Kompatibilität von TSplus mit den neuesten Versionen der Microsoft-Betriebssysteme und den neuesten Updates sicherzustellen.

Wir sind stolz darauf, Ihnen jede Woche neue Funktionen und Verbesserungen anzubieten.

Deshalb wird empfohlen, Ihren Server auf dem neuesten Stand zu halten.

Wenn ein Problem mit "2 Sitzungen pro Server" auftritt, typischerweise nach Windows-Updates am zweiten Dienstag des Monats, überprüfen Sie bitte Ihre TSplus Remote Access (oder TSplus LTS 18/17) Version.

Eine neue Version wird bald veröffentlicht, um die Kompatibilität mit dem neuesten Windows-Update wiederherzustellen.

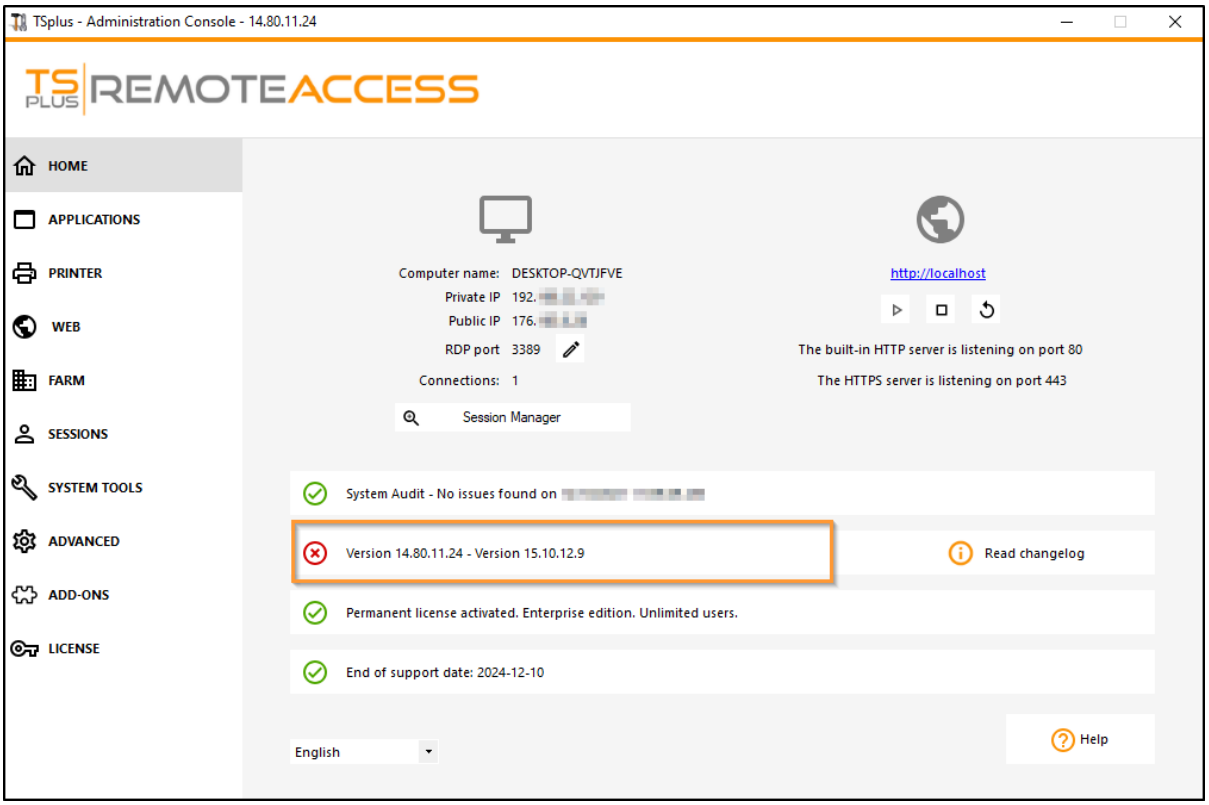
Als vorübergehende Lösung können Sie das Windows-Update des Tages deinstallieren und neu starten.

Wichtig: Vermeiden Sie die Deinstallation von TSplus Remote Access oder das Wiederherstellen eines älteren Systemabbilds. Diese Aktionen können Lizenzkonflikte auslösen, die viel komplexer zu lösen sind. In den meisten Fällen reicht ein einfacher Neustart aus, um Kompatibilitätskorrekturen automatisch anzuwenden.

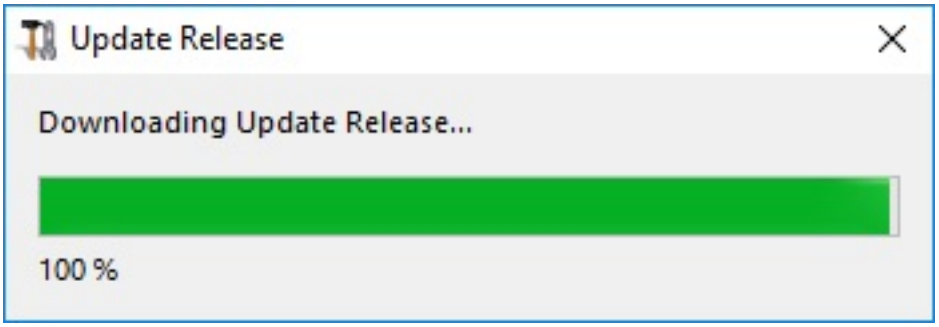
Durch das Abonnieren unserer jährlichen Support- und Update-Dienste haben Sie Zugriff auf die neuesten Updates und Fehlerbehebungen.

Um zu sehen, welche TSplus-Version Sie haben und sie zu aktualisieren:

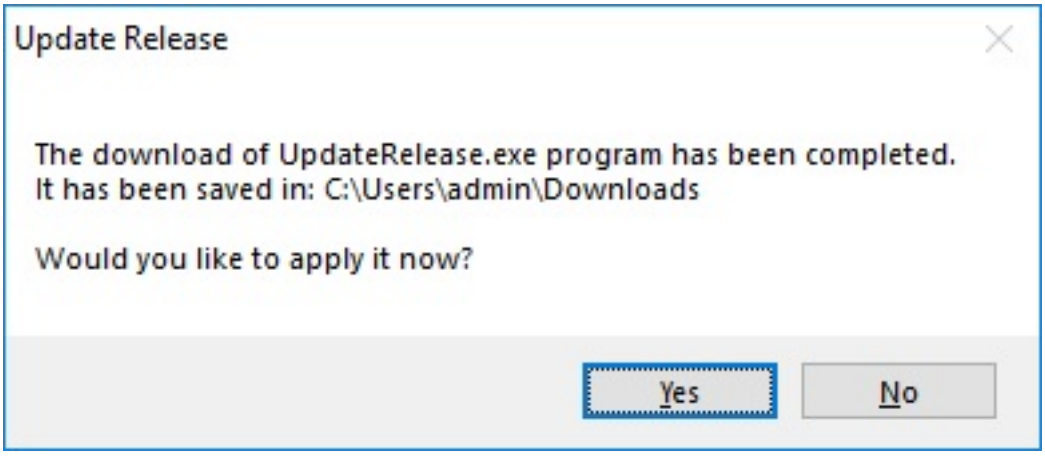
- Sie können den Status Ihrer TSplus-Version im Home-Tab Ihres AdminTools überprüfen:



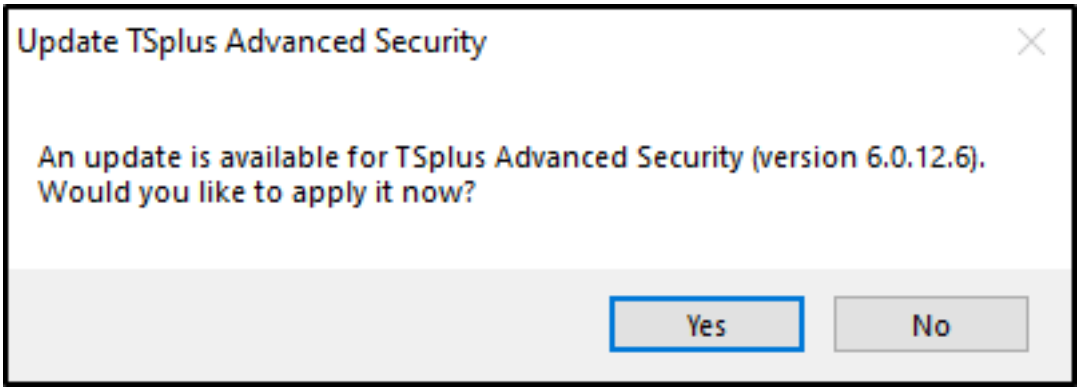
- Sie können dann darauf klicken. Seit der Version TSplus 11.50 lädt das AdminTool automatisch herunter…



…und wendet das Update-Release-Programm auf Anfrage an:



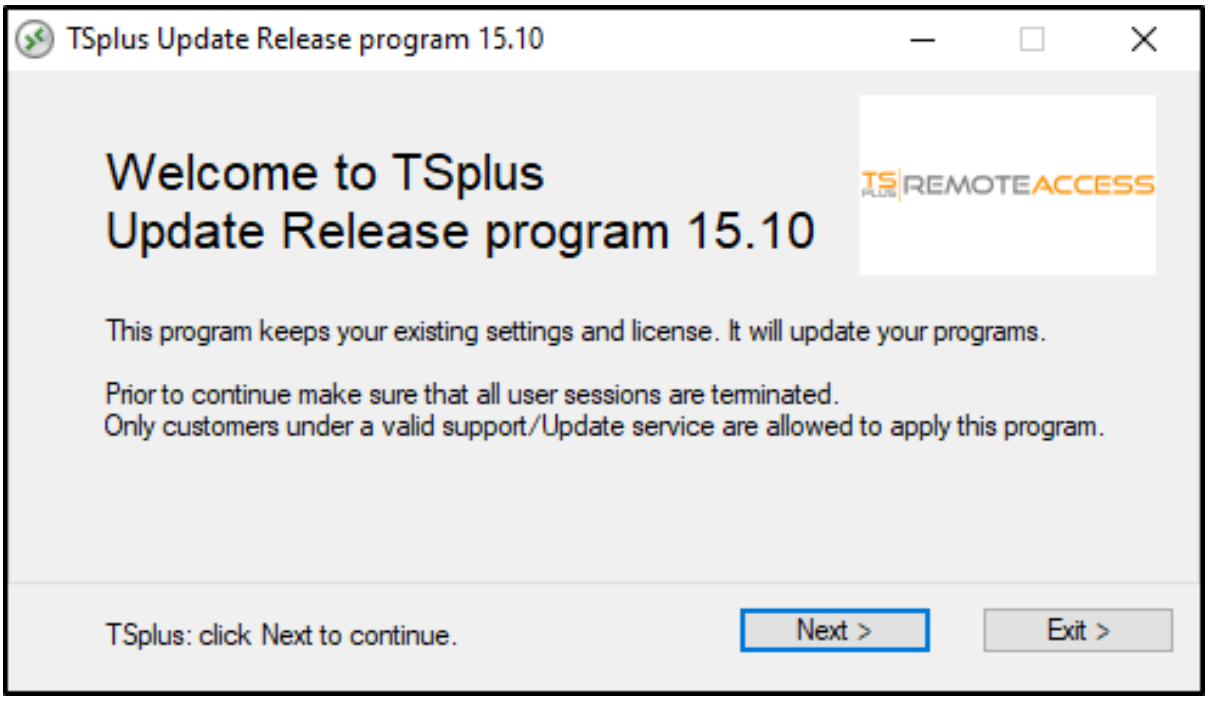
- Seit der Version TSplus 11.40 haben Sie die Wahl, zu installieren TSplus Advanced Security unser leistungsstarkes Sicherheits-Add-On in seiner ultimativen Testversion (Alle Sicherheitsfunktionen 2 Wochen lang kostenlos nutzbar) zu Ihrem TSplus-System:

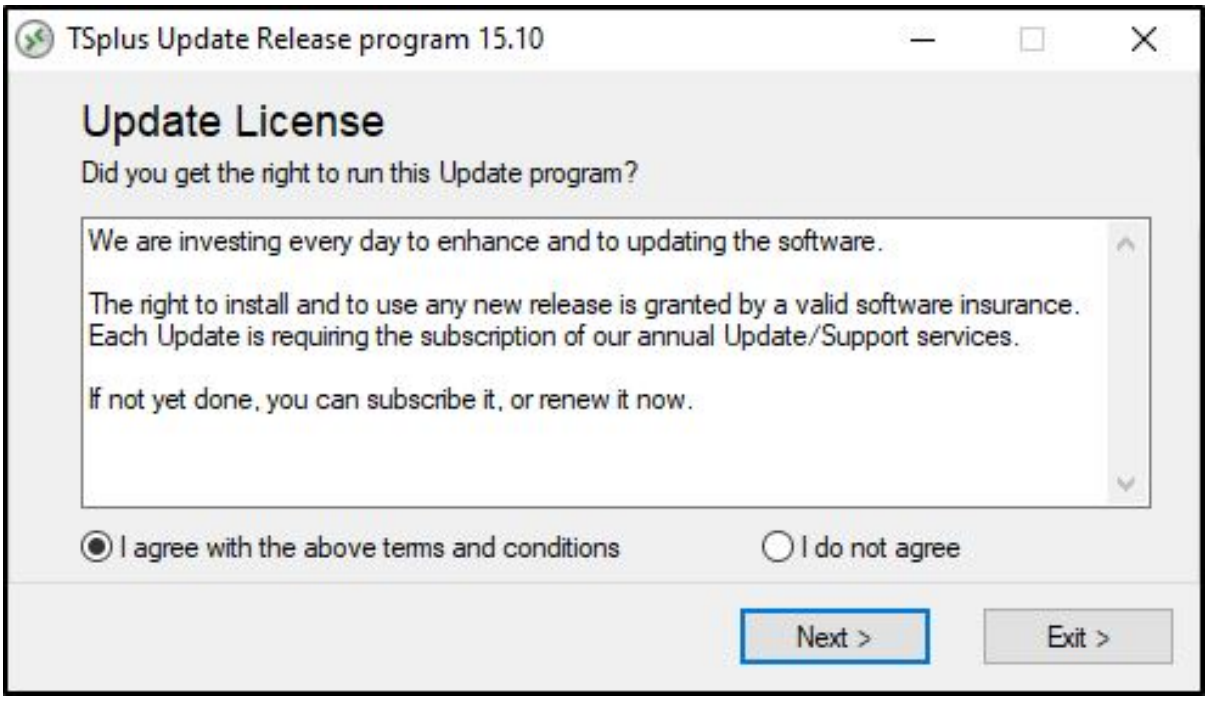


Sie können es weiterhin über diesen Link herunterladen: Aktualisierung veröffentlichen und wenden Sie es manuell an.

Das Update-Release-Programm ist darauf ausgelegt, Ihre aktuellen TSplus-Einstellungen sicher zu halten.

Wenn Sie sich noch nicht für die TSplus Update-/Supportdienste angemeldet haben oder wenn Ihr Abonnement abgelaufen ist, können Sie das Update-Release-Programm nicht ausführen:

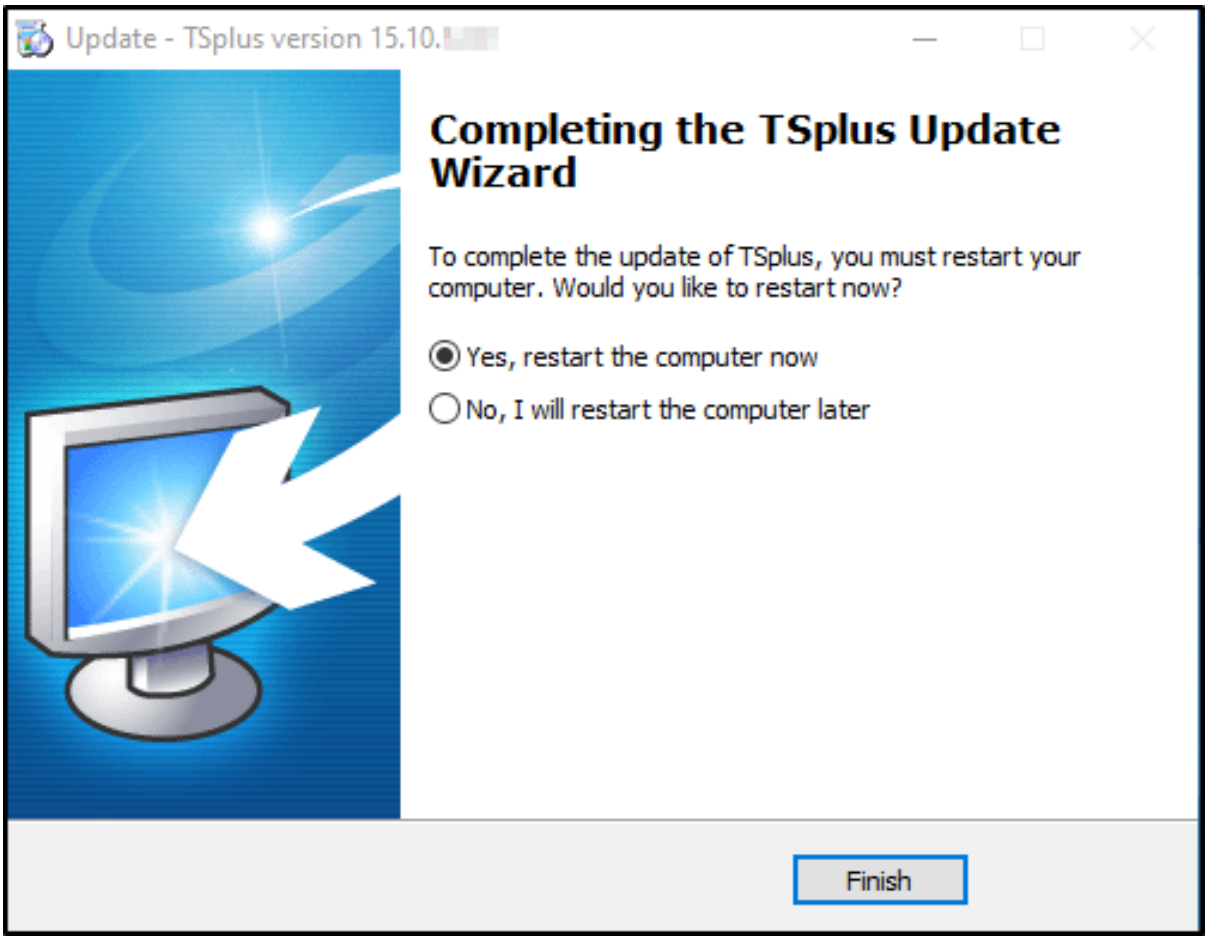




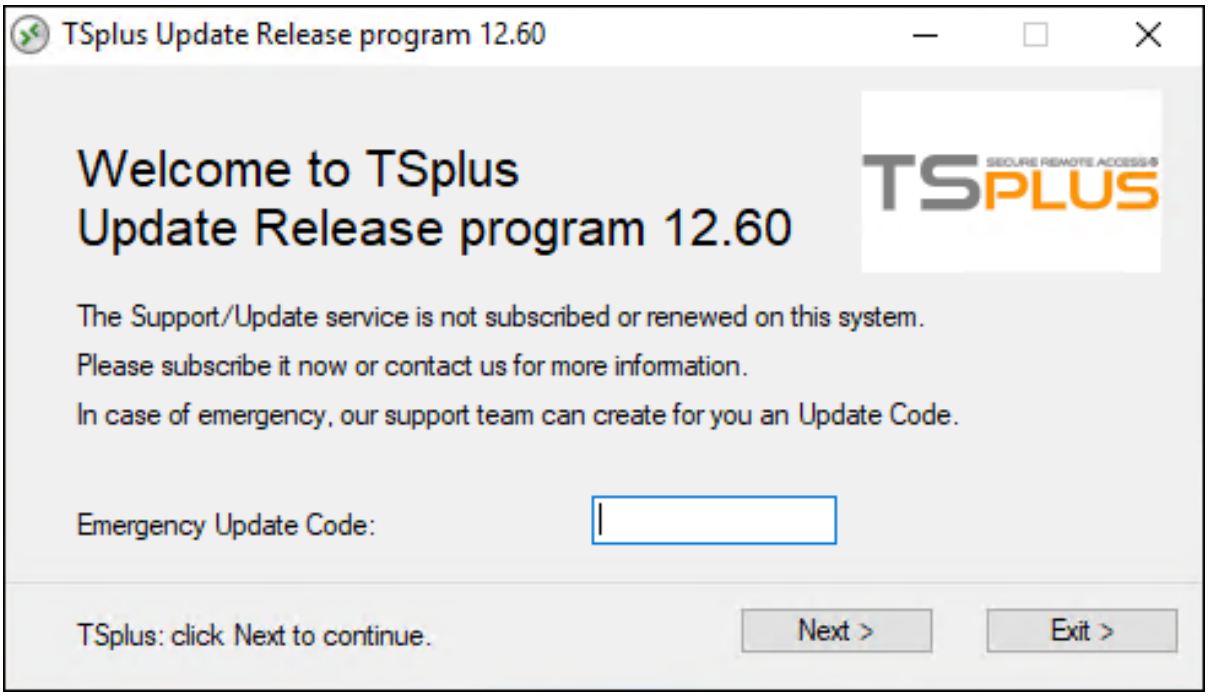
In einem solchen Fall empfehlen wir Ihnen, Ihre Bestellung auf unserer Store-Seite aufzugeben.

Sie erhalten die richtigen Informationen, um Ihre support.lic-Datei herunterzuladen. Die Aktivierung Ihrer Update-/Supportdienste ist ein einfacher Prozess, der beschrieben wird. hier .

Wenn das Update abgeschlossen ist, ist ein Neustart erforderlich:



Für Versionen vor v14 kann das TSplus Support-Team auf Anfrage einen Notfall-Update-Code bereitstellen, der das Update-Release-Programm freischaltet.



Update-Problem:

Überprüfen Sie die fehlende Datei

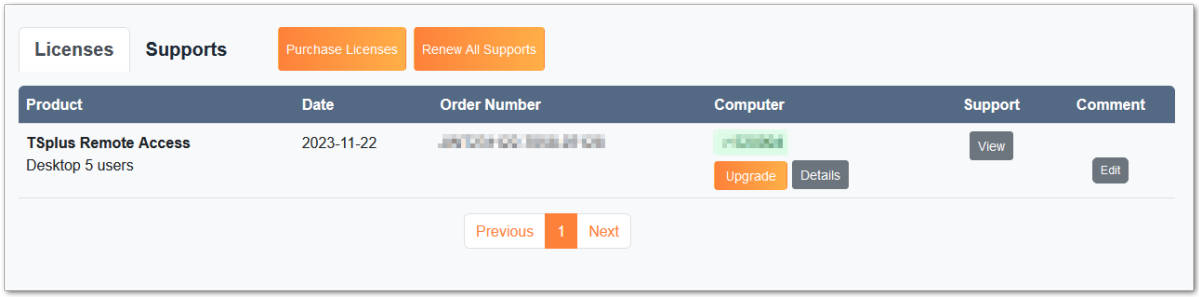
C:\Program Files (x86)\TSplus\reboot_required.dat

1. Wenn diese Datei vorhanden ist, löschen Sie sie.
2. Starten Sie Ihren Server
3. Führen Sie das Update erneut über diesen Link aus, indem Sie hier klicken: Aktualisierung veröffentlichen

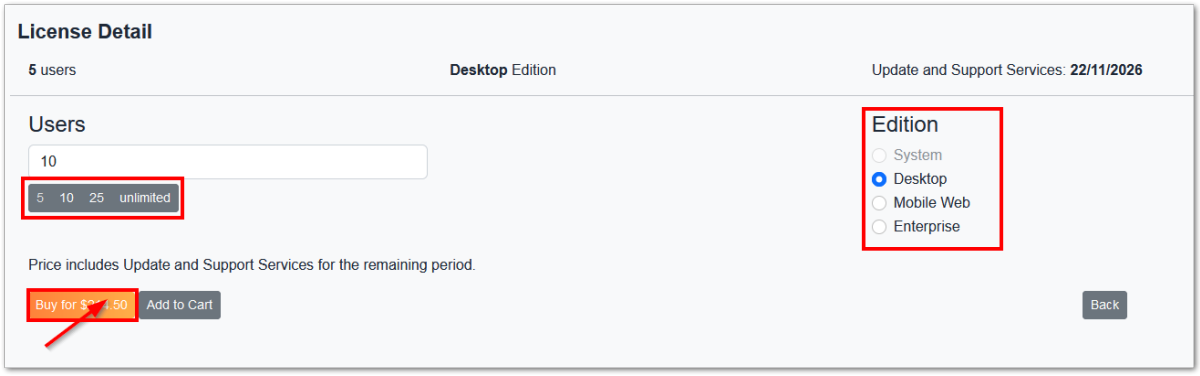
---

Ihre TSplus-Version aktualisieren

Wenn Sie Ihre aktuelle Version von TSplus aktualisieren möchten, um mehr Benutzer oder mehr Funktionen hinzuzufügen, registrieren Sie sich in Ihrem Lizenzportal.



Wählen Sie Ihre Upgrade-Option (Benutzer und Version) aus und klicken Sie auf **Kaufen für** um in unserem Geschäft fortzufahren.



Nach Ihrem Kauf wird das Update sofort und sichtbar in Ihrem Lizenzportal sein.
Sie müssen auch dasselbe Verfahren auf Ihrem Gerät befolgen, damit es mit Ihrer Lizenz verknüpft ist.

Klicken Sie auf Ihrem Server auf die **Aktualisieren Sie Ihre Lizenz** Schaltfläche im AdminTool > Lizenz-Registerkarte.

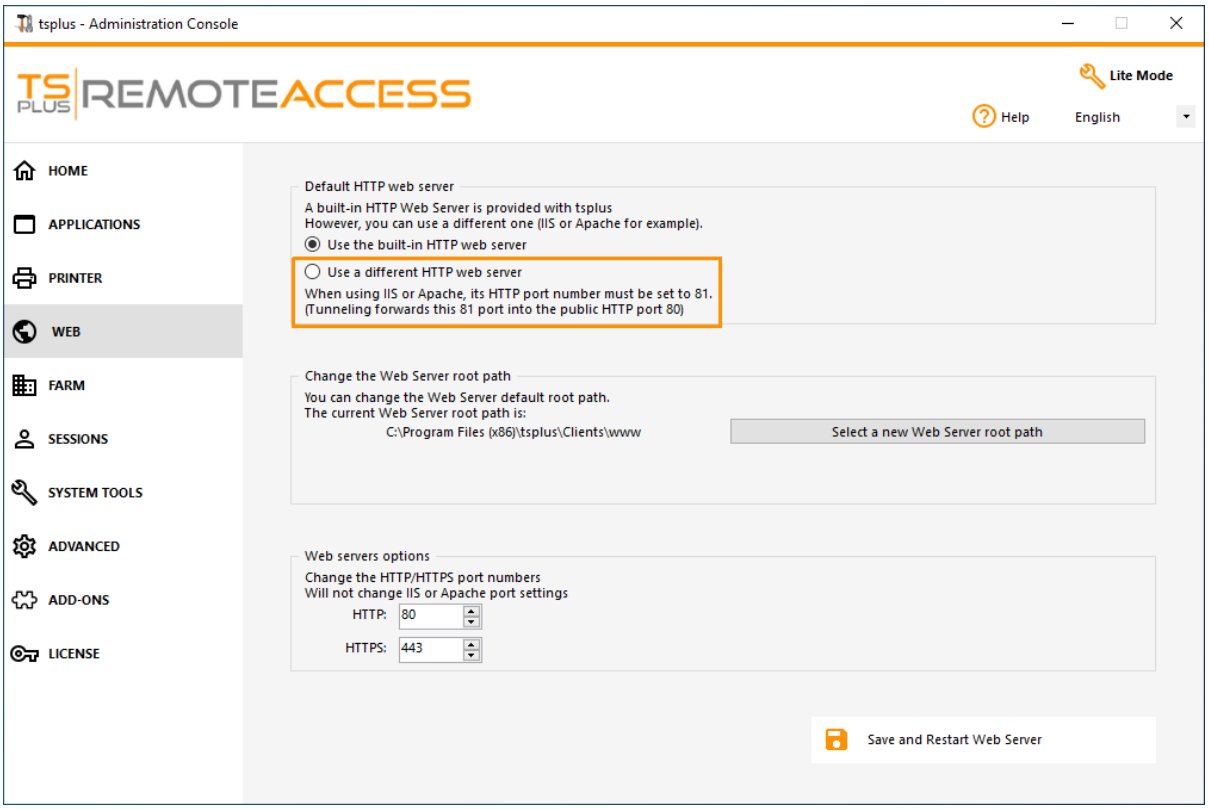
Wie man Apache anstelle des Standard-Webservers von Terminal Service Plus verwendet

Voraussetzungen

Es kann eine gute Idee sein, um Update Terminal Service Plus um sicherzustellen, dass Sie die neuesten TSplus-Programme erhalten.

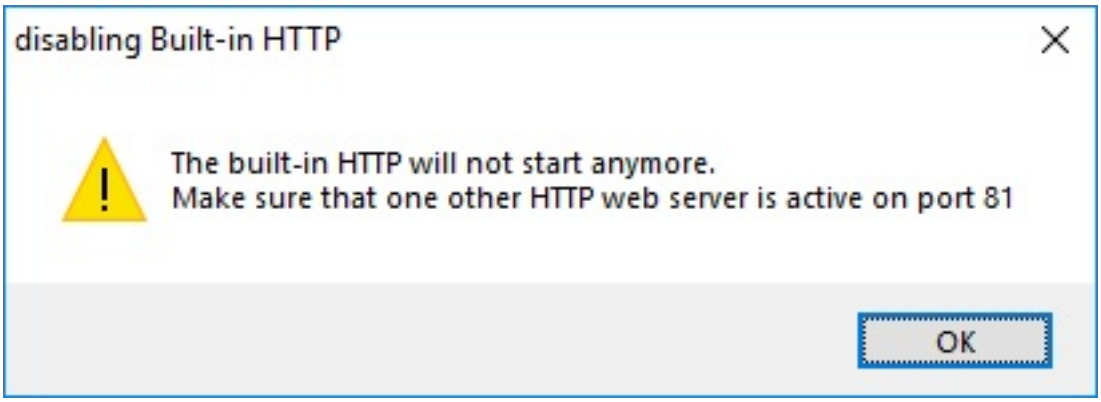
1. Starten Sie das AdminTool und gehen Sie zum Webserver-Tab

Klicken Sie auf die Kachel "Webserver verwalten", überprüfen Sie **Verwenden Sie einen anderen HTTP-Webserver** weil Sie Apache verwenden möchten.



Dann verwenden Sie die Schaltfläche **Wählen Sie einen neuen Webserver-Stammverzeichnispfad aus** um TSplus mitzuteilen, wo das neue Webordner-Wurzelverzeichnis sein wird.

TSplus wird die angeforderten Dateien/Ordner in diesen neuen Stammordner kopieren, und zu diesem Zeitpunkt ist die TSplus-Einstellung für Apache fast abgeschlossen. Ein Pop-up wird Ihnen empfehlen, den Apache-HTTP-Port auf 81 zu ändern.



Es ist jetzt an der Zeit, Apache einzurichten.

2. Apache einrichten

Ändern Sie das HTTP von 80 auf 81.

Die spezifische Vorgehensweise hängt von Ihrer Apache-Version und Ihren aktuellen Apache-Einstellungen ab.

Wir empfehlen Ihnen, vor der Änderung von Apache-Einstellungsdateien eine Sicherungskopie anzufertigen, damit Sie diese bei Bedarf wiederherstellen können.

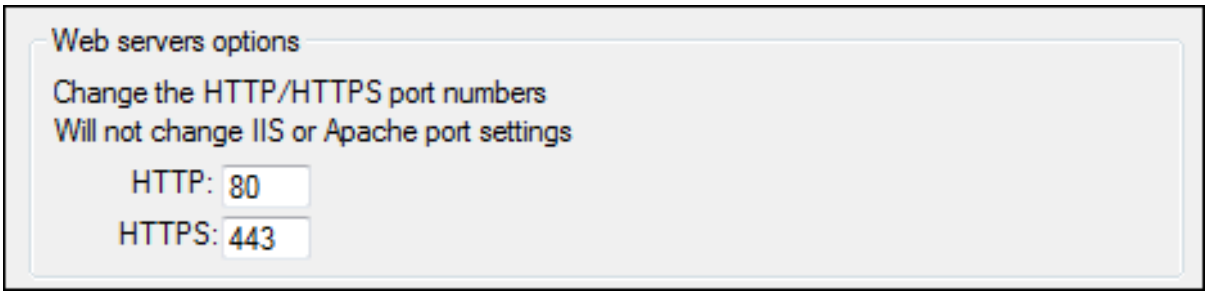
Normalerweise können Sie den Apache-Anhörport ändern, indem Sie die Datei httpd.conf im Verzeichnis „Apache\conf“ bearbeiten:

Hören 81

Sobald es erledigt ist, starten Sie den Apache-Dienst neu.

3. Zurück zum TSplus Webserver-Management-Tool

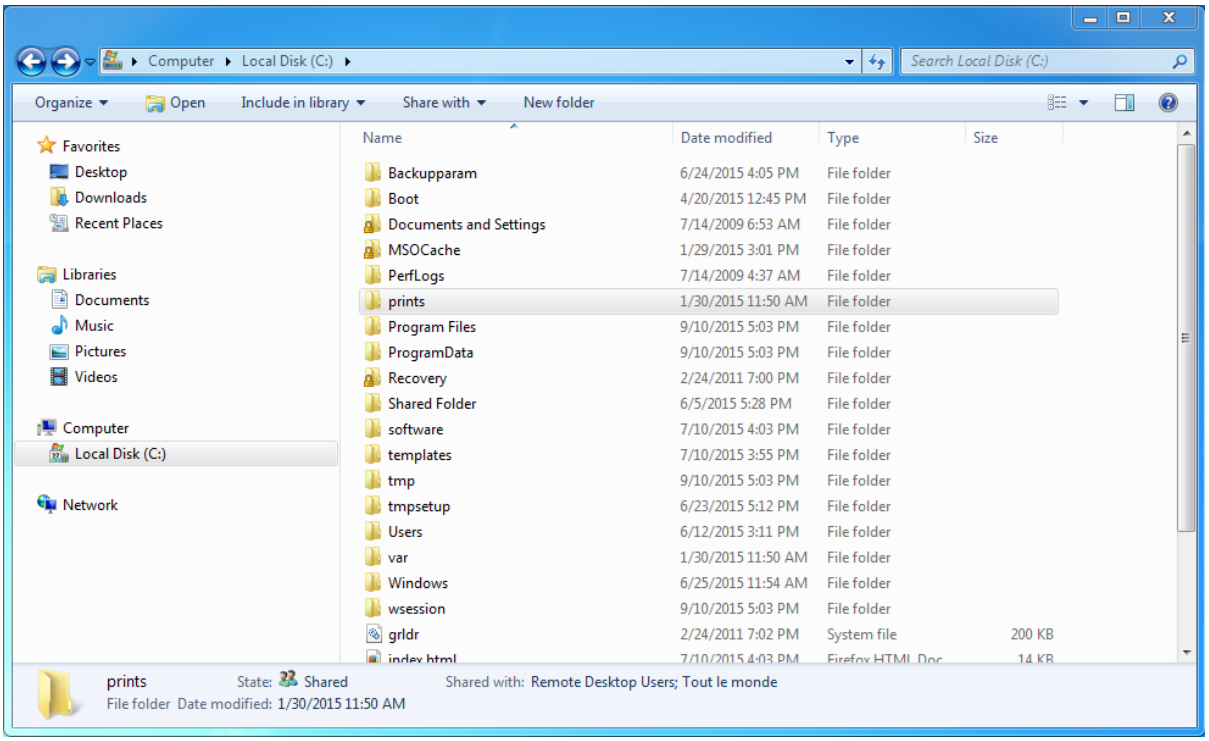
Sie können die HTTP- und HTTPS-Ports im TSplus Web Management-Tool festlegen. Wir empfehlen die Verwendung von Standardports, aber diese Funktion kann nützlich sein, um Konflikte mit einem anderen Prozess zu vermeiden.

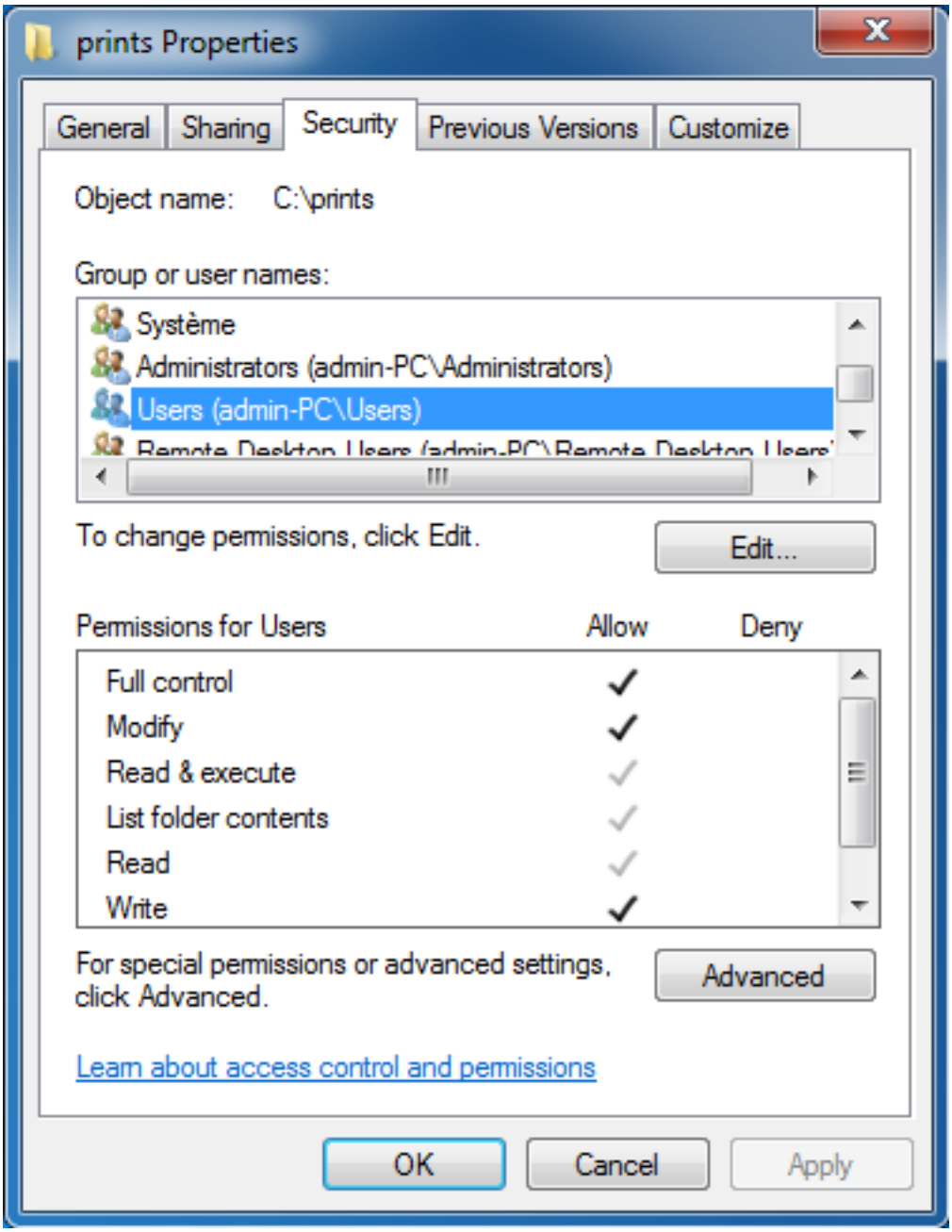


4. Letzte Schritte

Für den Universal Printer müssen wir in der PRINTS-Ordner schreiben können.

Überprüfen Sie, dass alle Benutzer… volle Rechte auf den …/Druckordner haben.


Computer ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Organize
Open
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
Backupparam 6/24/2015 4:05 PM File folder
Boot 4/20/2015 12:45 PM File folder
Documents and Settings 7/14/2009 6:53 AM File folder
MSOCache 1/29/2015 3:01 PM File folder
PerfLogs 7/14/2009 4:37 AM File folder
prints 1/30/2015 11:50 AM File folder
Program Files 9/10/2015 5:03 PM File folder
ProgramData 9/10/2015 5:03 PM File folder
Recovery 2/24/2011 7:00 PM File folder
Shared Folder 6/5/2015 5:28 PM File folder
software 7/10/2015 4:03 PM File folder
templates 7/10/2015 3:55 PM File folder
tmp 9/10/2015 5:03 PM File folder
tmpsetup 6/23/2015 5:12 PM File folder
Users 6/12/2015 3:11 PM File folder
var 1/30/2015 11:50 AM File folder
Windows 6/25/2015 11:54 AM File folder
wsession 9/10/2015 5:03 PM File folder
grldr 2/24/2011 7:02 PM System file 200 KB
index.html 7/10/2015 4:03 PM Firefox HTML Doc 14 KB
prints State: Shared Shared with: Remote Desktop Users; Tout le monde
File folder Date modified: 1/30/2015 11:50 AM



Dann wählen Sie die .html-Datei aus, die Sie als Webzugriffsseite verwenden möchten in:

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

und kopiere es als index.html in deinen Web-Stammordner, typischerweise ist dies das Verzeichnis „Apache\htdocs“.

5. Spezifische Einstellungen für TSplus Gateway Portal, Lastenausgleich und/oder HTML5-Dateiübertragung

Wenn Sie dieses auf Apache basierende System als TSplus Gateway Portal verwenden und/

oder die Load Balancing-Funktion des TSplus Gateway Portals nutzen und/oder die HTML5-Dateiübertragungsfunktion verwenden möchten, müssen Sie die Ausführung von TSplus GCI-Skripten durch Apache zulassen.

Zuerst müssen Sie das CGI-Modul in Apache aktiviert haben.

Bearbeiten Sie die Datei httpd.conf im Verzeichnis „Apache\conf“ und suchen Sie nach einer Zeile, die wie folgt aussieht:

;LoadModule cgi_module modules/mod_cgi.so

Entfernen Sie das „;“, um das CGI-Modul zu aktivieren:

LoadModule cgi_module modules/mod_cgi.so

Dann finden Sie eine Zeile, die mit beginnt:

AddHandler cgi-script

Und fügen Sie die .exe-Erweiterung hinzu, um .exe-Dateien als CGI-Programme von Apache behandeln zu lassen:

AddHandler cgi-script .exe

Schließlich müssen Sie Apache mitteilen, dass der TSplus-Ordner „cgi-bin“ CGI-Programme enthält. Dazu müssen Sie die folgende Zeile in die Datei httpd.conf im Verzeichnis „Apache\conf“ hinzufügen:

ScriptAlias /cgi-bin/ “C:/Program Files (x86)/TSplus/Clients/www/cgi-bin/”

Sobald es erledigt ist, starten Sie den Apache-Dienst neu.

Wenn Sie Probleme bei der Einrichtung von CGI auf Ihrem Apache-Server haben, wenden Sie sich bitte an die Offizielle Apache-Dokumentation

Überprüfen Sie Ihre Einstellungen: Um Ihre Einstellungen zu validieren, öffnen Sie bitte einen Webbrowser auf Ihrem Server und gehen Sie zu http://localhost/cgi-bin/hb.exe Wenn Sie eine Apache-Fehlerseite erhalten, haben Sie ein Problem mit Ihrer Apache-Konfiguration. Wenn Sie eine Zeile Text/Zahlen erhalten, ist alles in Ordnung!

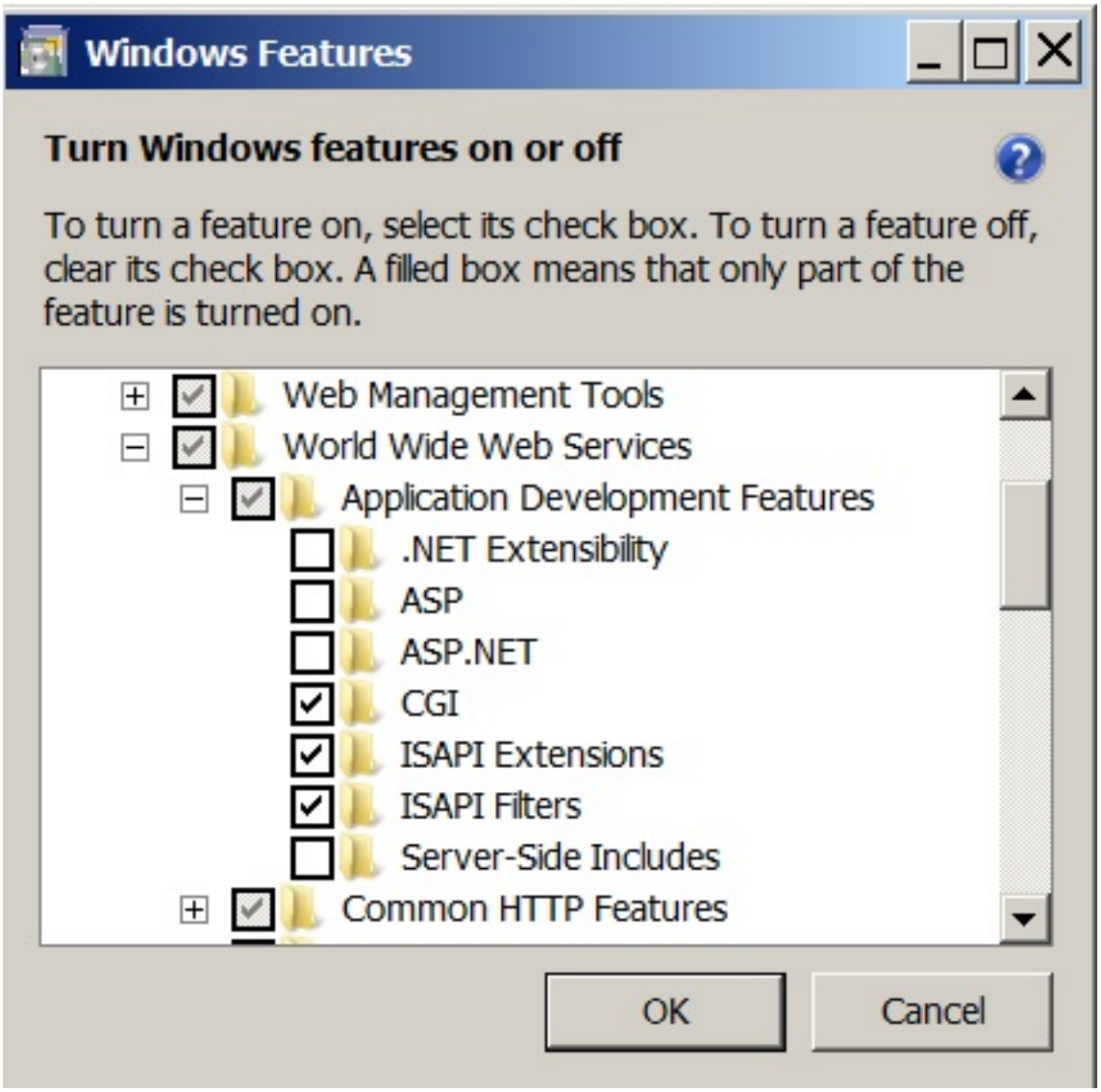
Wie man IIS anstelle der Standard-Webserver von Terminal Service Plus verwendet

Voraussetzungen

Es kann eine gute Idee sein, um Update Terminal Service Plus um sicherzustellen, dass Sie die neuesten TSplus-Programme erhalten.

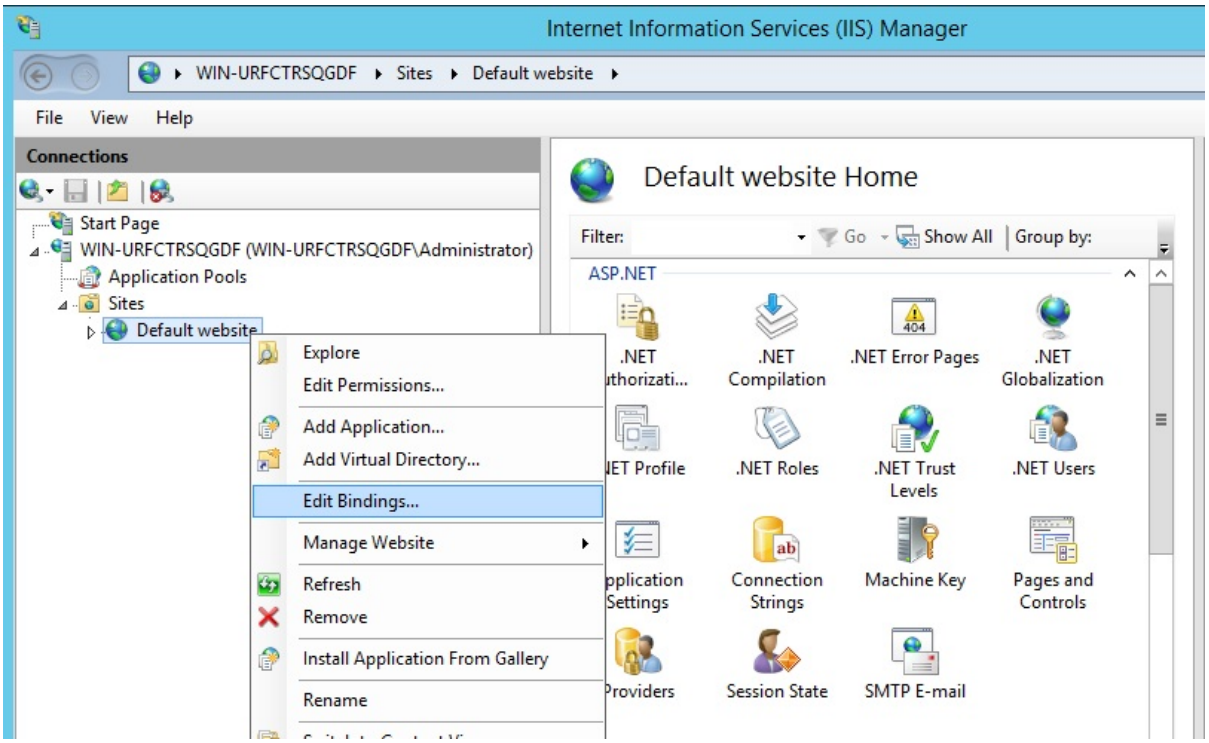
1. IIS-Konfiguration

- Installieren Sie IIS mit den folgenden Modulen: CGI, ISAPI-Erweiterungen und ISAPI-Filter.

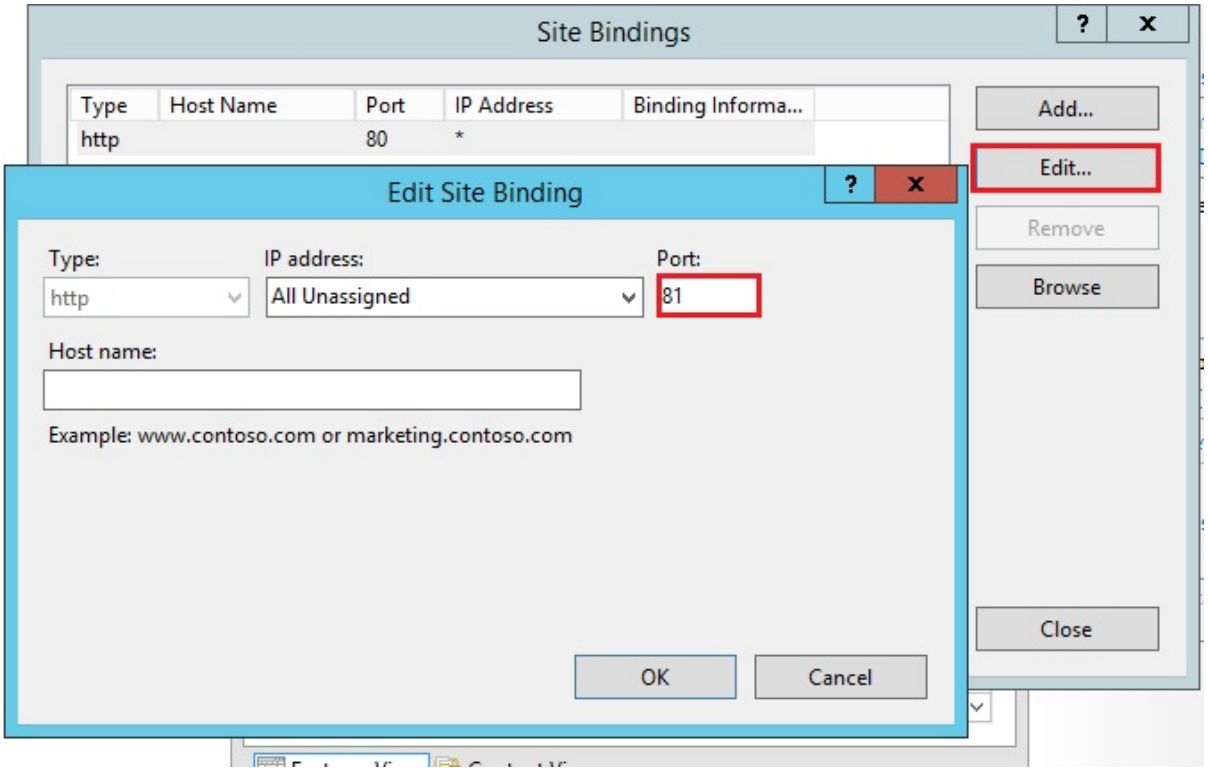


- IIS-Port konfigurieren:

Greifen Sie auf die IIS-Verwaltungskonsole zu, erweitern Sie die Liste unter Ihrem Servernamen, erweitern Sie dann das Menü „Sites“ und klicken Sie mit der rechten Maustaste auf „Default Web Site“ und klicken Sie auf „Bindungen bearbeiten“.



Klicken Sie auf „http“ und „Bearbeiten“. Ändern Sie den Port auf 81 und klicken Sie auf Ok, und klicken Sie dann auf Schließen:



Deaktivieren Sie den Port 443 oder ändern Sie diesen Port in einen anderen freien Port.

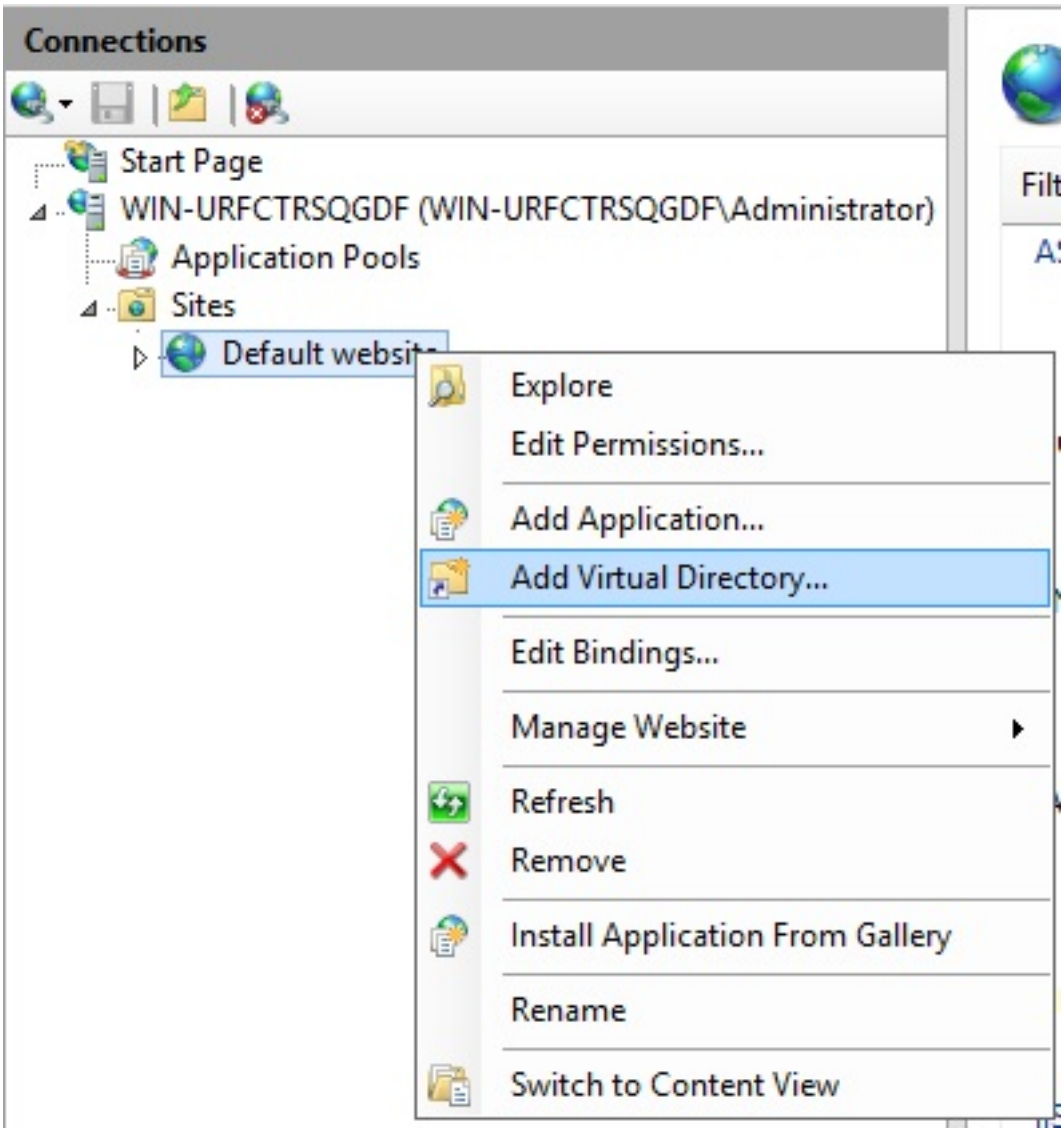
Dann starten Sie den IIS-Manager neu.

2. Erstellen Sie ein virtuelles Verzeichnis für CGI

NB: Alle Dateien aus dem Standard-Webstammverzeichnis (C:\Program Files (x86)\TSplus\Clients\www) werden nicht kopiert, wenn das Verzeichnis des Webstammverzeichnisses geändert wird.

Sie müssen sie manuell überprüfen und kopieren, wenn Sie auf den IIS-Webserver migrieren.

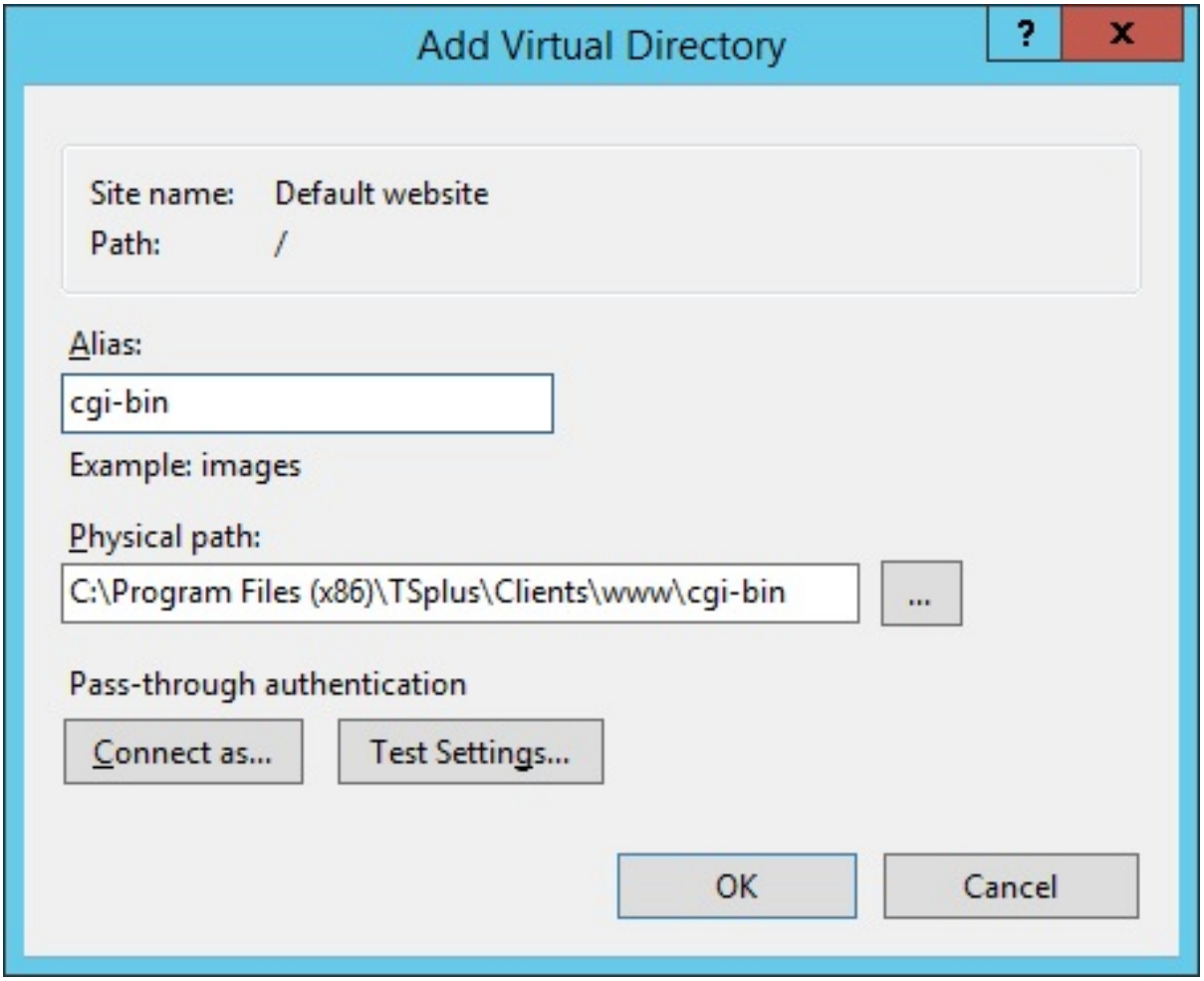
Im linken Menübereich erweitern Sie das Menü unter Ihrem Server, dann „Sites“, und klicken mit der rechten Maustaste auf Ihre Site, um ein neues „virtuelles Verzeichnis“ hinzuzufügen, wie im Bild unten gezeigt:



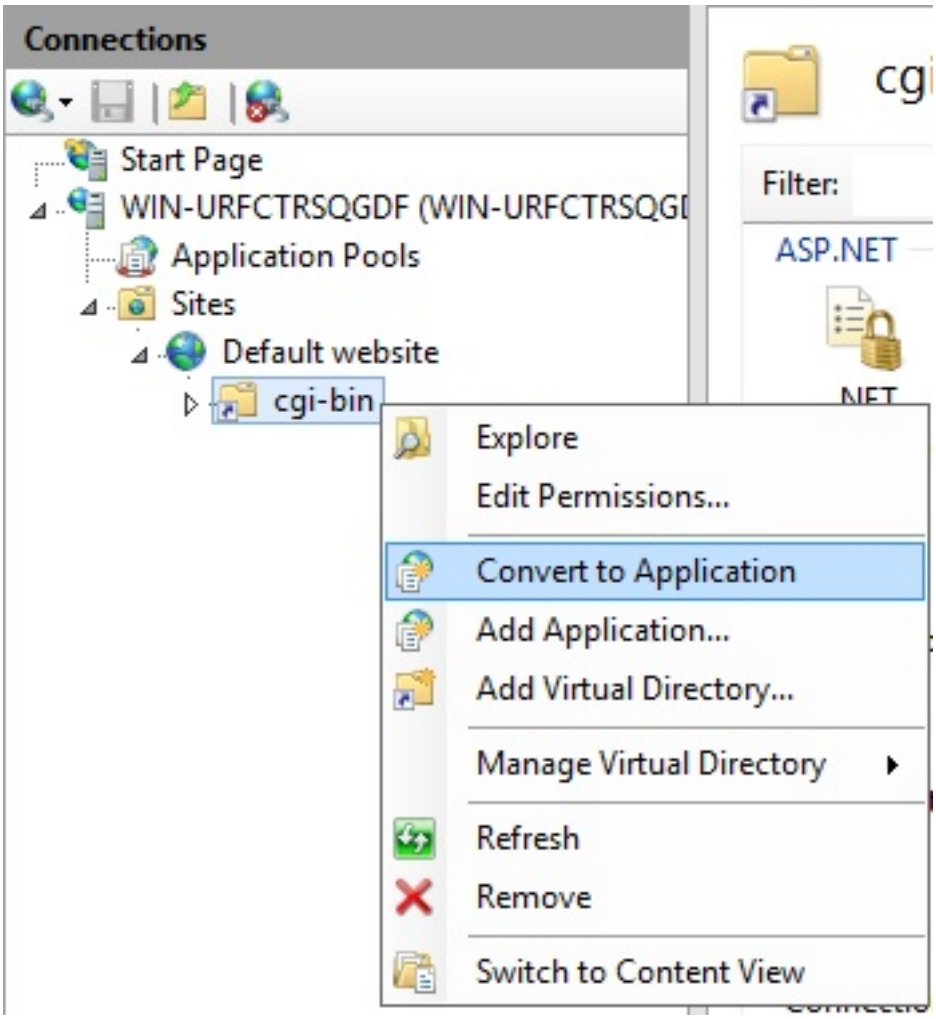
Auf dem sich öffnenden Fenster füllen Sie wie folgt aus:

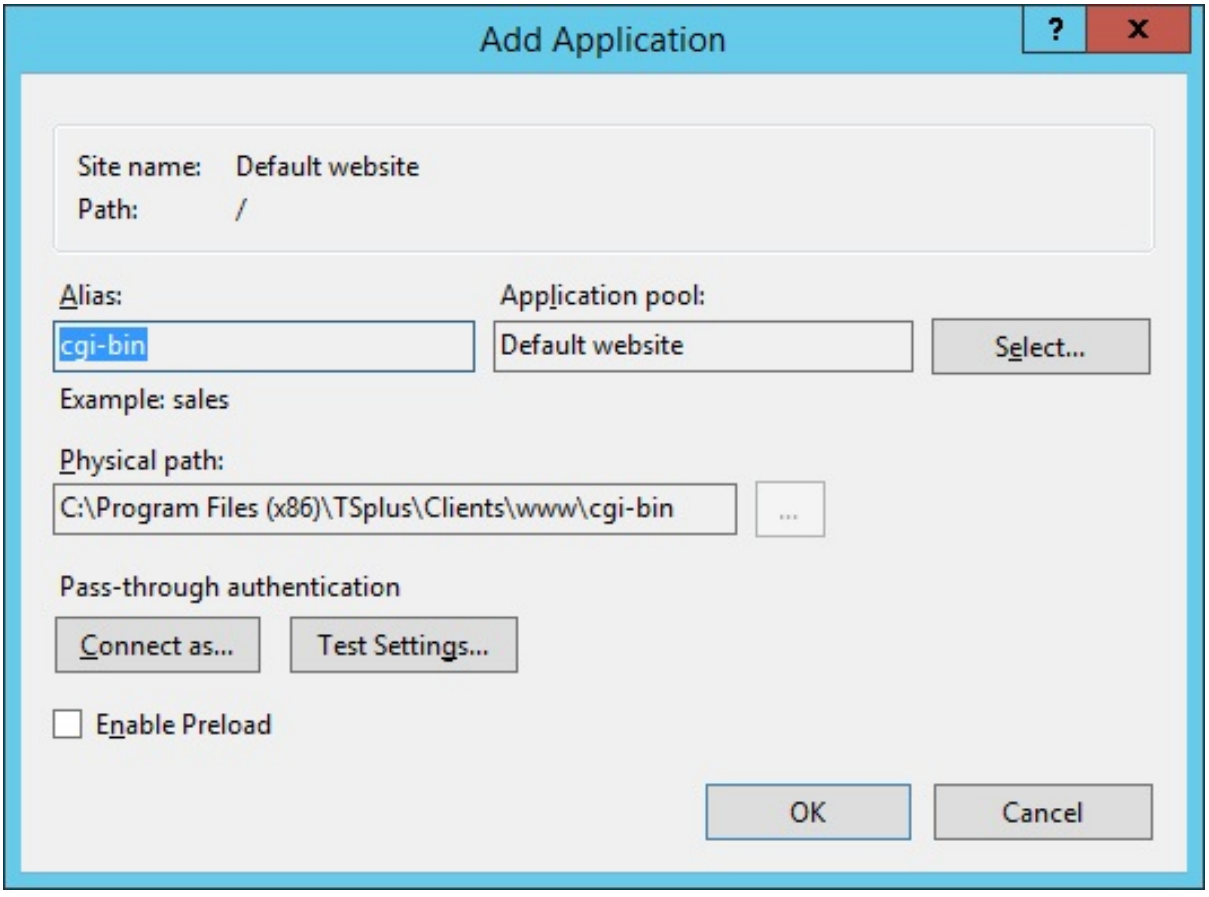
Alias: cgi-bin

Physikalischer Pfad: C:\Program Files(x86)\TSplus\Clients\www\cgi-bin

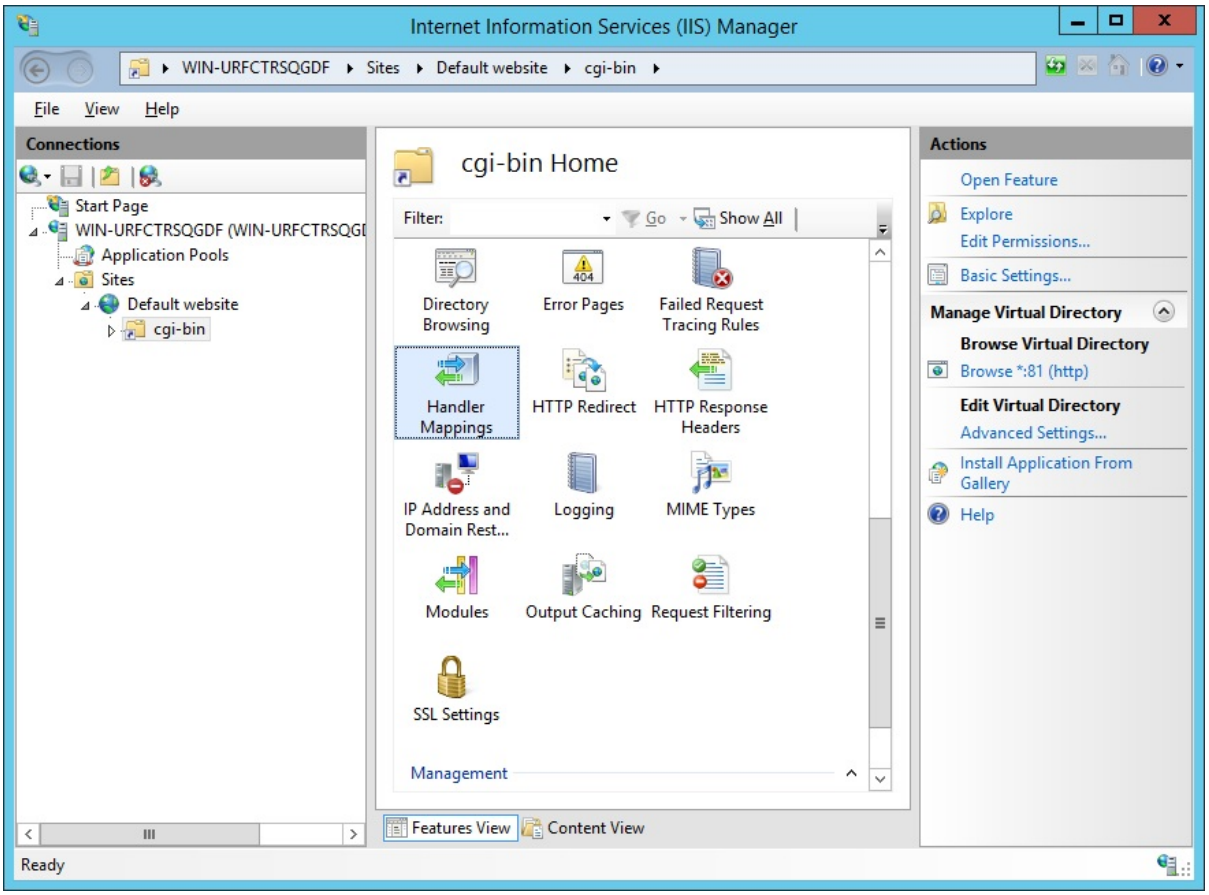


Dann klicken Sie auf „OK“ und Sie werden sehen, dass das virtuelle Verzeichnis „cgi-bin“ zu Ihrer IIS-Website hinzugefügt wurde. Klicken Sie nun mit der rechten Maustaste auf dieses virtuelle Verzeichnis „cgi-bin“ und klicken Sie auf „In Anwendung umwandeln“. Klicken Sie auf „OK“ und akzeptieren Sie die Standardeinstellungen.


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

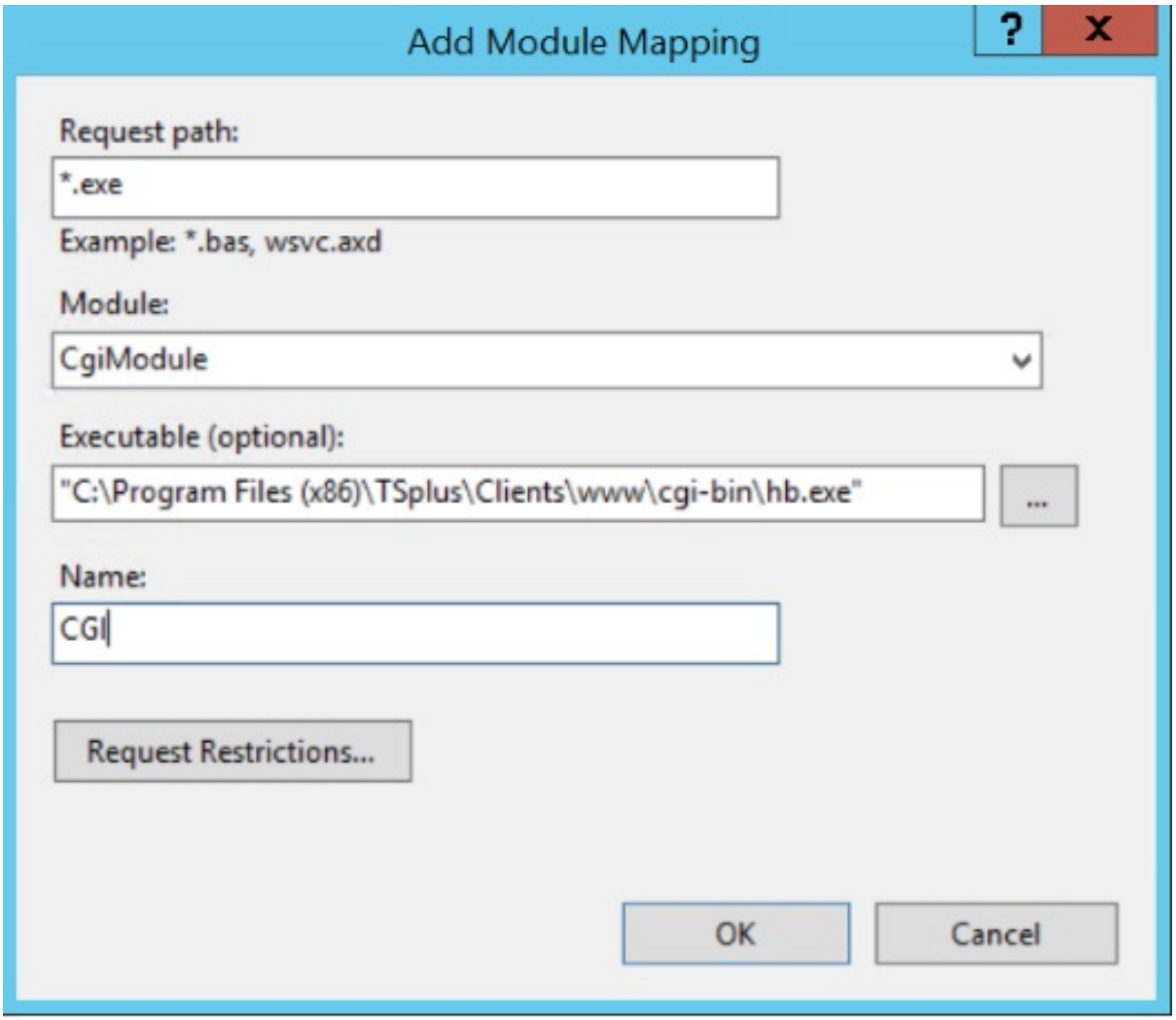

Add Application
Site name: Default website
Path: /
Alias:
cgi-bin
Example: sales
Application pool:
Default website
Select...
Physical path:
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin
...
Pass-through authentication
Connect as...
Test Settings...
Enable Preload
OK
Cancel

Dann wählen Sie das Symbol „Handler-Zuordnungen“ für diesen Ordner auf der rechten Seite des Managerfensters aus.

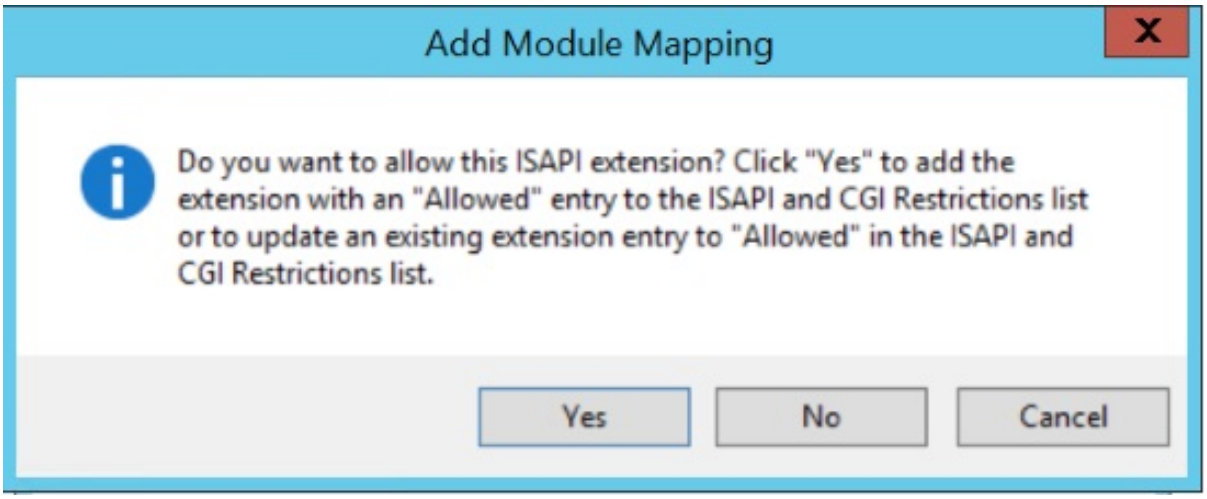


Doppelklicken Sie in der Liste der Handlerzuordnungen auf „CGI-exe“.

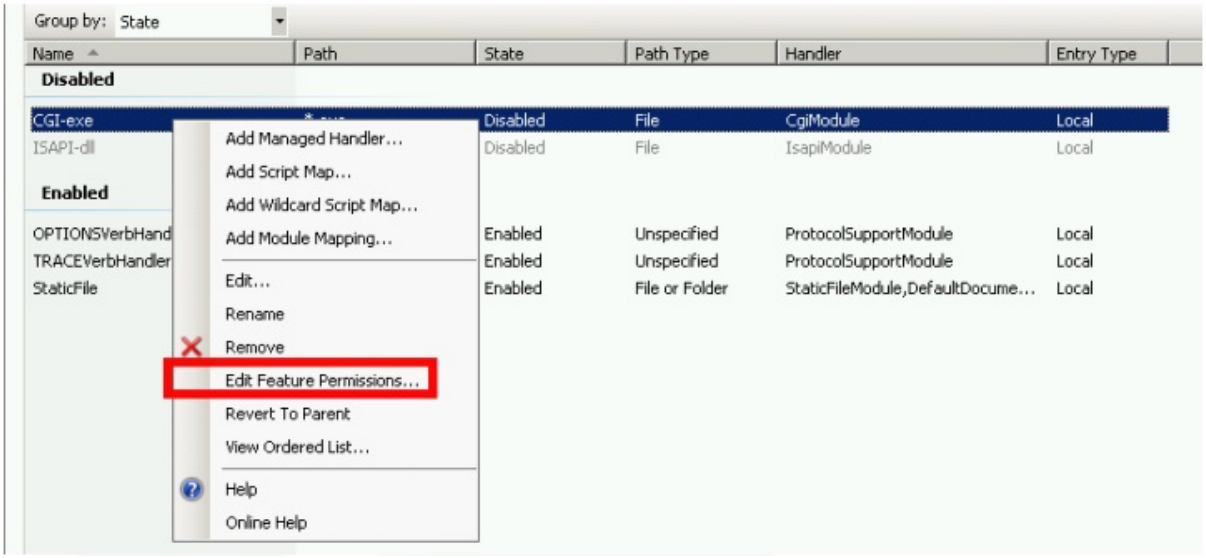
Dann suchen Sie die hb.exe ausführbare Datei im Eigenschaftenfeld für ausführbare Dateien und klicken Sie auf OK.



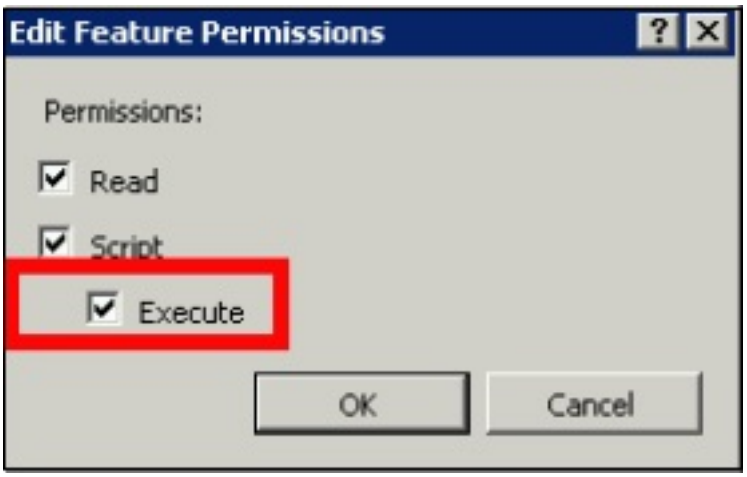
Ein Bestätigungsaufforderung erscheint. Klicken Sie auf „OK“, um diese ISAPI-Erweiterung zuzulassen.



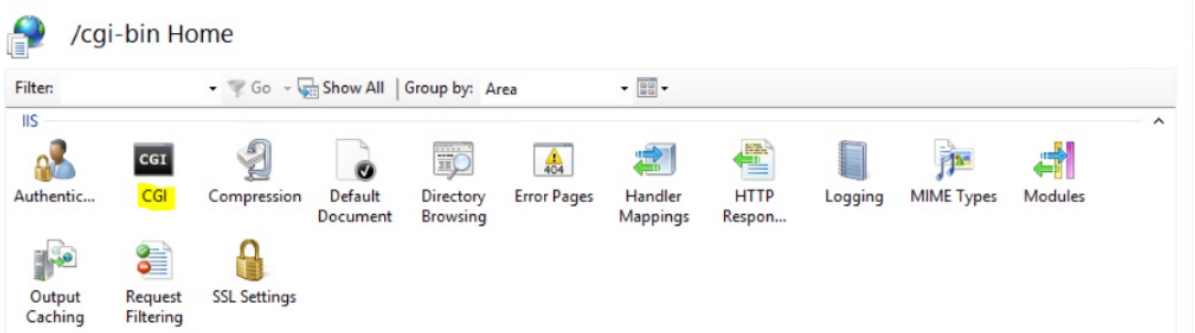
Jetzt auf „Feature-Berechtigungen bearbeiten“ klicken:



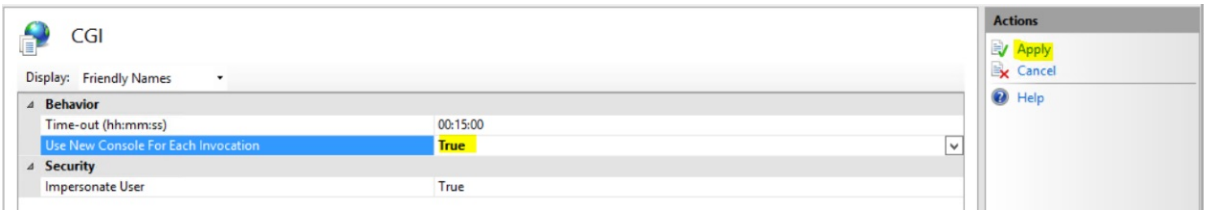
Überprüfen Sie das Kontrollkästchen "Ausführen" und klicken Sie auf OK:



Zurück zum “CGI-bin” Home, klicken Sie auf “CGI”, um die CGI-Eigenschaften zu öffnen:



Ändern Sie den Wert von „Neue Konsole für jede Invocation verwenden“ auf „Wahr“. Klicken Sie dann auf „Übernehmen“, um die Änderungen zu speichern.

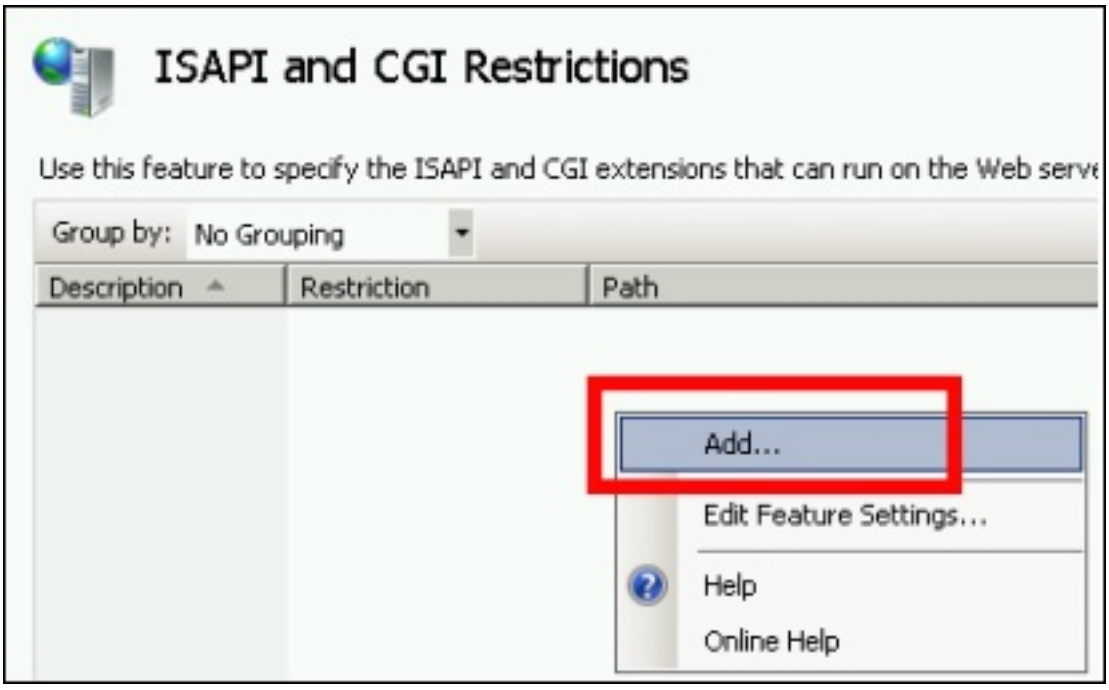


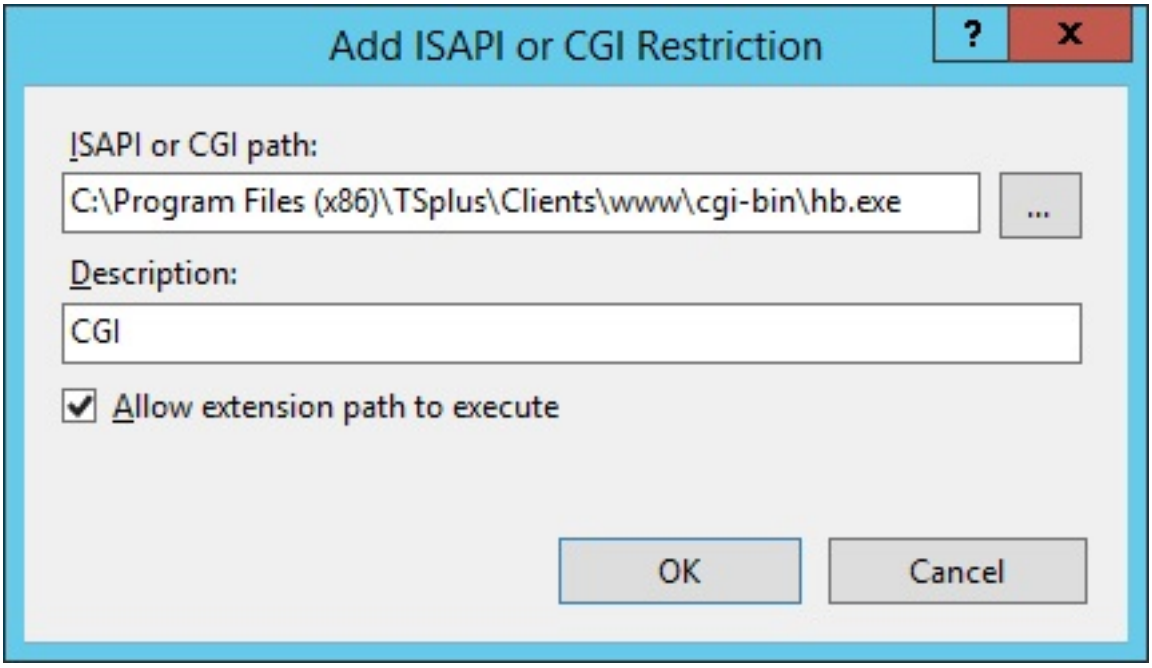
3. Konfigurieren Sie die Berechtigung für die CGI-Erweiterung

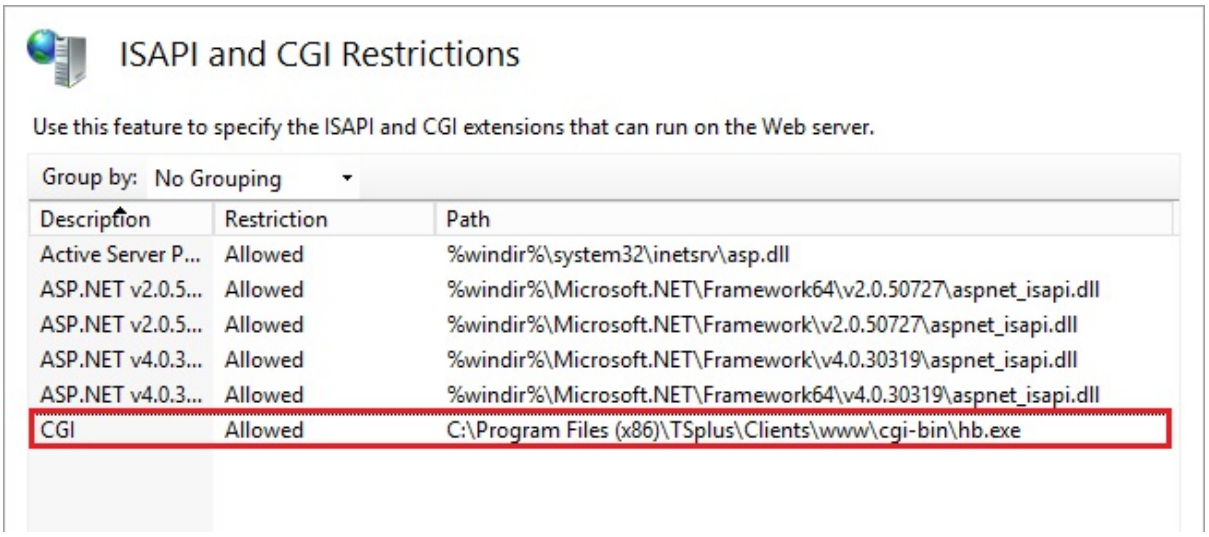
Jetzt ist der letzte Schritt, die CGI-Erweiterung auf dem Server auszuführen. Klicken Sie auf das Symbol „ISAPI- und CGI-Einschränkungen“. Dies kann gefunden werden, indem Sie auf den Maschinenname im Menü auf der linken Seite des Fensters klicken.



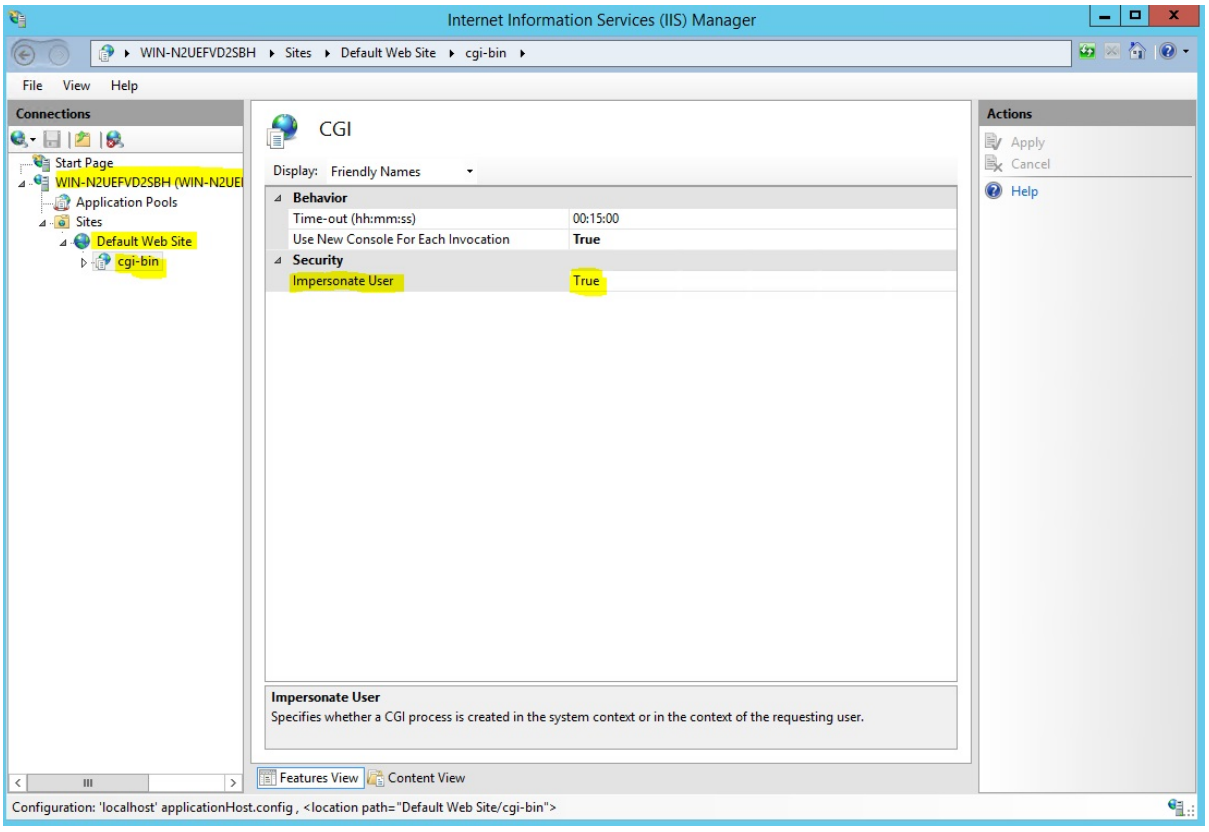
Auf der Seite „ISAPI- und CGI-Einschränkungen“ klicken Sie auf der rechten Seite des Fensters auf „Hinzufügen …“. Geben Sie nun den vollständigen Pfad zur Datei „hb.exe“ an, die im TSplus-Ordner gehostet wird. Stellen Sie sicher, dass Sie die Option „Erlauben, dass der Erweiterungspfad ausgeführt wird“ aktivieren, da Veranschaulichen Sie die folgenden Bilder:


ISAPI and CGI Restrictions
Use this feature to specify the ISAPI and CGI extensions that can run on the Web serve
Group by: No Grouping
Description
Restriction
Path
Add...
Edit Feature Settings...
Help
Online Help


Add ISAPI or CGI Restriction
?
X
ISAPI or CGI path:
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\hb.exe
...
Description:
CGI
Allow extension path to execute
OK
Cancel



Stellen Sie sicher, dass im CGI-Bereich Ihres Servers die Einstellung „Benutzer impersonieren“ für „Standardwebsite“ und „cgi-bin“ auf „Wahr“ gesetzt ist.



- Vollzugriff für den Benutzer „IUSR“ im Verzeichnis gewähren
  C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- Bitte stellen Sie sicher, dass die Berechtigungsvererbung aktiviert ist, wenn der IUSR-Benutzer für die vollständige Kontrolle über das Verzeichnis konfiguriert ist.
  C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- Vollzugriff für den Benutzer „IUSR“ im Verzeichnis gewähren C:\Program Files (x86)\TSplus\Clients\webserver\twofa

4. Mime-Typen in IIS hinzufügen

Öffnen Sie eine Eingabeaufforderung als Administrator und führen Sie die folgenden Befehle aus:

Terminalfenster

```
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent
/+[fileExtension='.dat',mimeType='text/plain']
```

Terminalfenster

```
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent
/+[fileExtension='.',mimeType='text/plain']
```

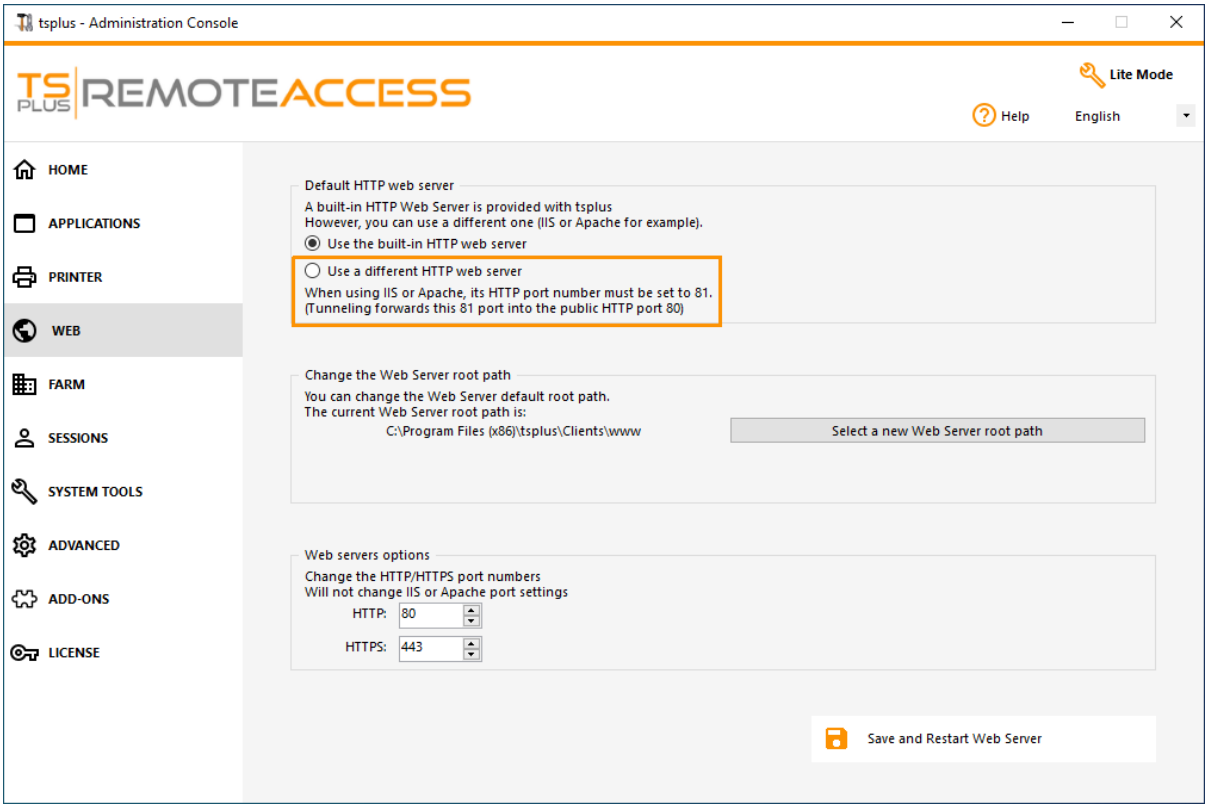
IIS neu starten.

5. IIS-Verzeichnisberechtigungen konfigurieren

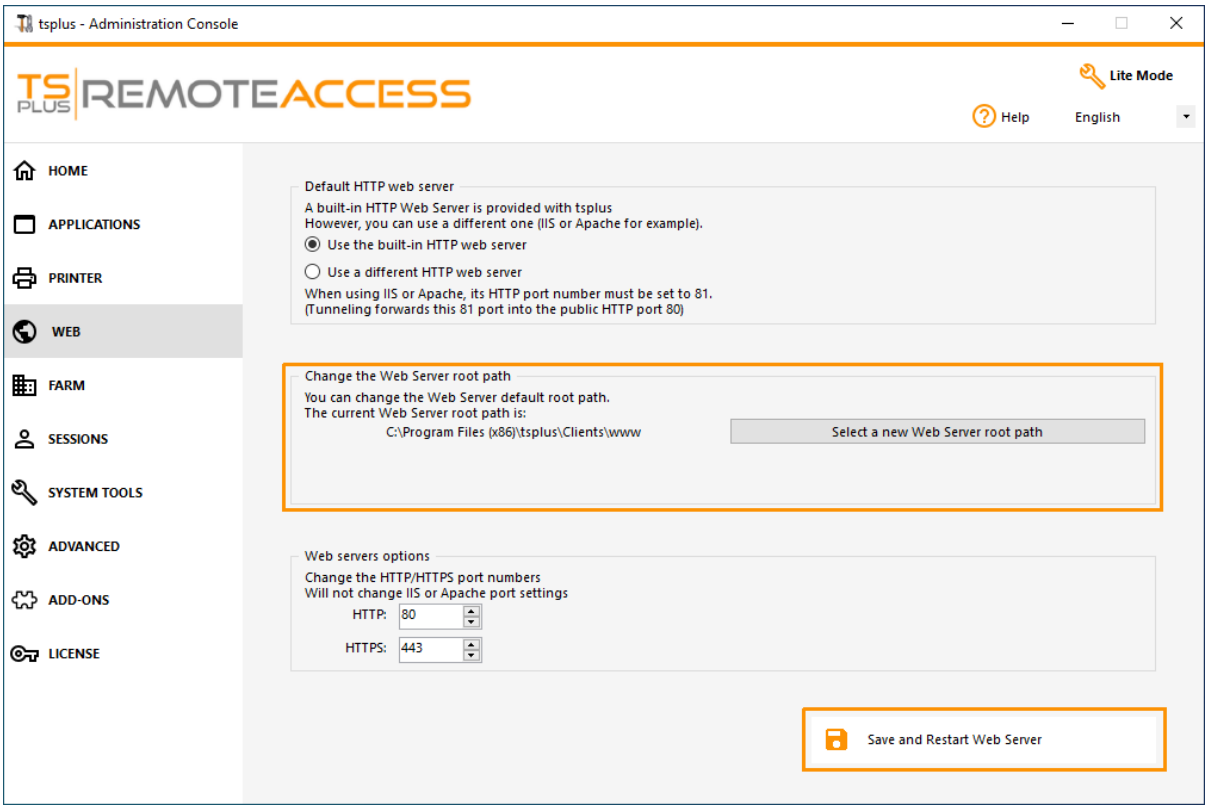
Vollzugriff für die Gruppe „Jeder“ im Verzeichnis „C:\inetpub\wwwroot“ gewähren

6. Konfigurieren Sie TSplus

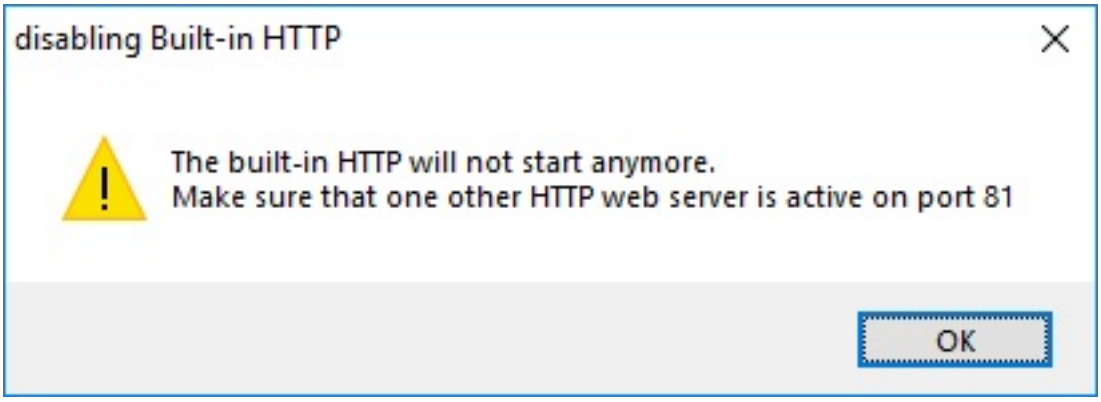
Gehe zum Webserver-Tab des AdminTools und wähle dann die Option „Einen anderen HTTP-Server verwenden“ aus.

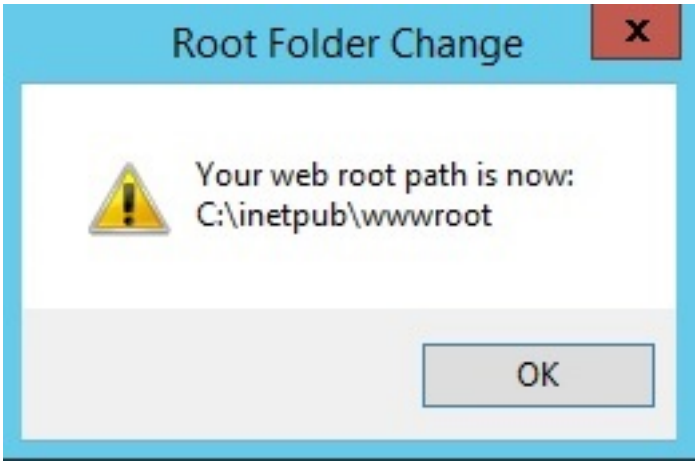


Dann klicken Sie im selben Fenster auf „Wählen Sie einen neuen Webserver-Stammverzeichnispfad aus“ und geben Sie den Pfad des IIS-Verzeichnisses ein, der etwa so aussehen sollte: „C: \ inetpub \ wwwroot“. Klicken Sie nun auf „Speichern und das AdminTool neu starten“.



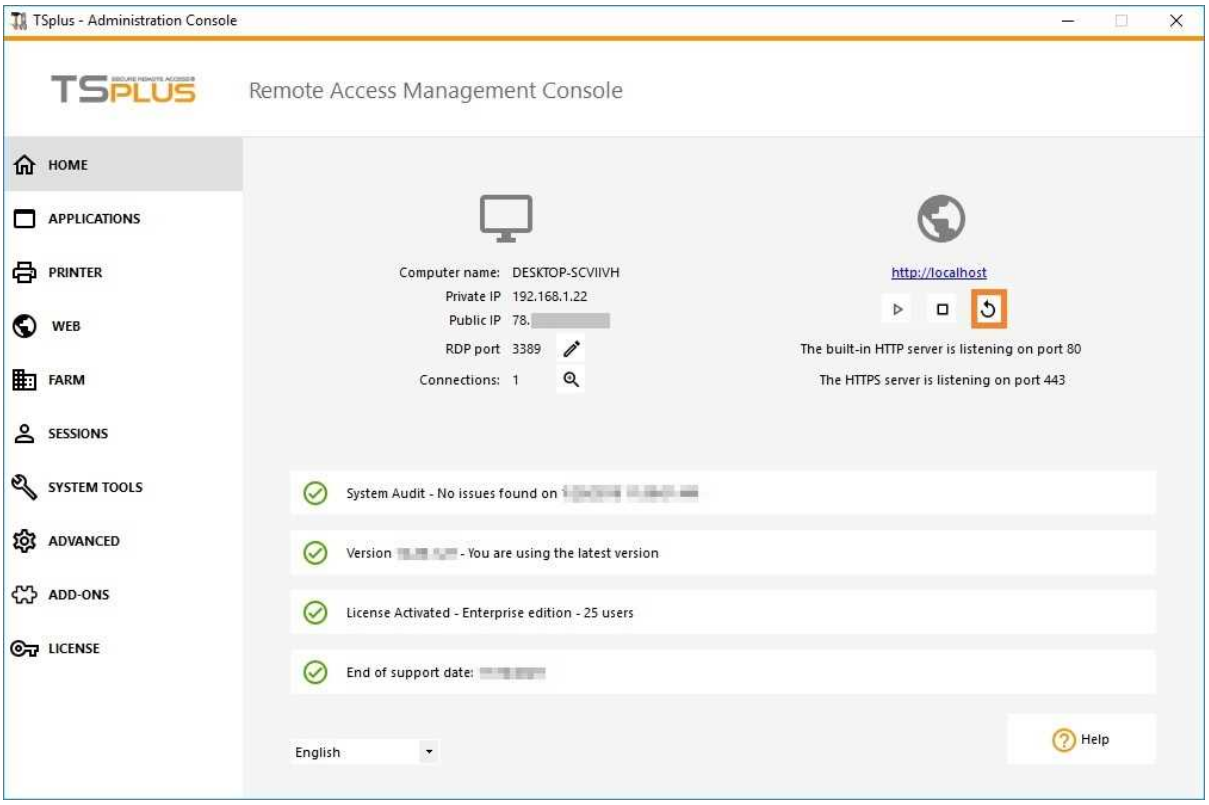
Die folgenden Nachrichten werden angezeigt:





Warten. Das Admintool wird automatisch geschlossen. Öffnen Sie dann das Admintool erneut und klicken Sie auf das Web-Kachel.

Schließlich die Webserver neu starten:



7. Test mit lokalem Host

Warnung Verwenden Sie ein anderes Benutzerkonto.

Wenn Sie mit Ihrem aktuellen Benutzerkonto von Ihrer eigenen RDP-Sitzung zum Server versuchen, werden Sie getrennt und können sich nicht erneut verbinden.



Zusätzliche Aktionen:

RemoteApp konfigurieren

Der Ordner „remoteapp“ im IIS-Webstamm (c:\inetpub\www\cgi-bin\remoteapp) muss ebenfalls volle Berechtigungen für den IUSR-Benutzer haben, andernfalls wird ein 704-Fehler angezeigt, wenn versucht wird, RemoteApp zu verwenden.

Konfigurieren Sie 2FA

Bei einer frischen Installation, bei der 2FA noch nie aktiviert wurde, gibt es keinen Ordner mit dem Namen
C:\Program Files (x86)\TSplus\Clients\webserver\twofa, oder die twofactorauth.ini-Datei.

Es ist notwendig:

- 2FA im AdminTool aktivieren, um diesen Ordner und diese .ini-Datei zu erstellen.
- dann 2FA deaktivieren
- dann wenden Sie die IUSR-Benutzerberechtigungen auf den neu erstellten twofa-Ordner an.

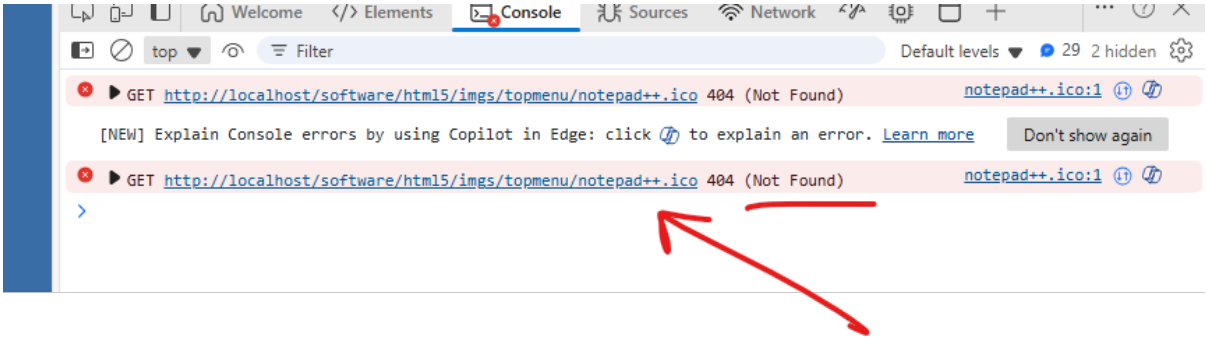
Das Versäumnis, diesen Schritt abzuschließen (auch wenn Sie nicht beabsichtigen, 2FA zu verwenden), wird Benutzer daran hindern, sich mit einer Fehlermeldung anzumelden, die besagt, dass die Anmeldeinformationen ungültig sind.

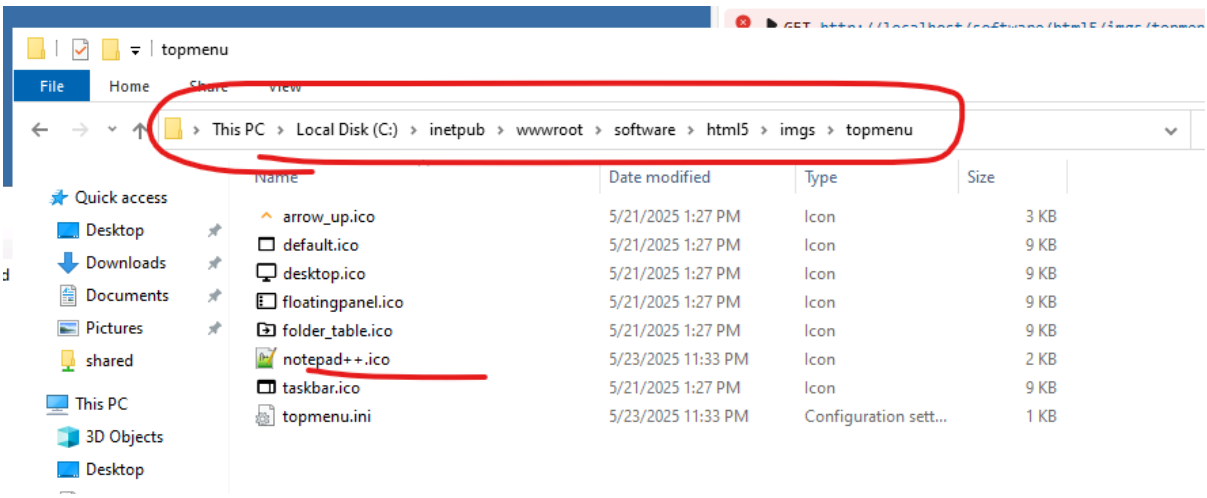
8. Doppelte Escaping erlauben

Um Downloads zu ermöglichen, müssen Sie „Doppelte Escapierung zulassen“ in der Anforderungsfilterung innerhalb von IIS aktivieren. Diese Änderung ermöglicht es IIS, Sonderzeichen wie „+“ in Dateinamen korrekt zu verarbeiten. So aktivieren Sie „Doppelte Escapierung zulassen“ in IIS:

1. IIS-Manager öffnen: Starten Sie den Internetinformationsdienste (IIS) Manager.

2. Navigieren Sie zu Anforderungsfilterung: Wählen Sie im IIS-Manager den Ordner oder die Website aus, die die Datei mit dem „+“-Zeichen enthält. Doppelklicken Sie dann im Funktionsbereich auf „Anforderungsfilterung“.

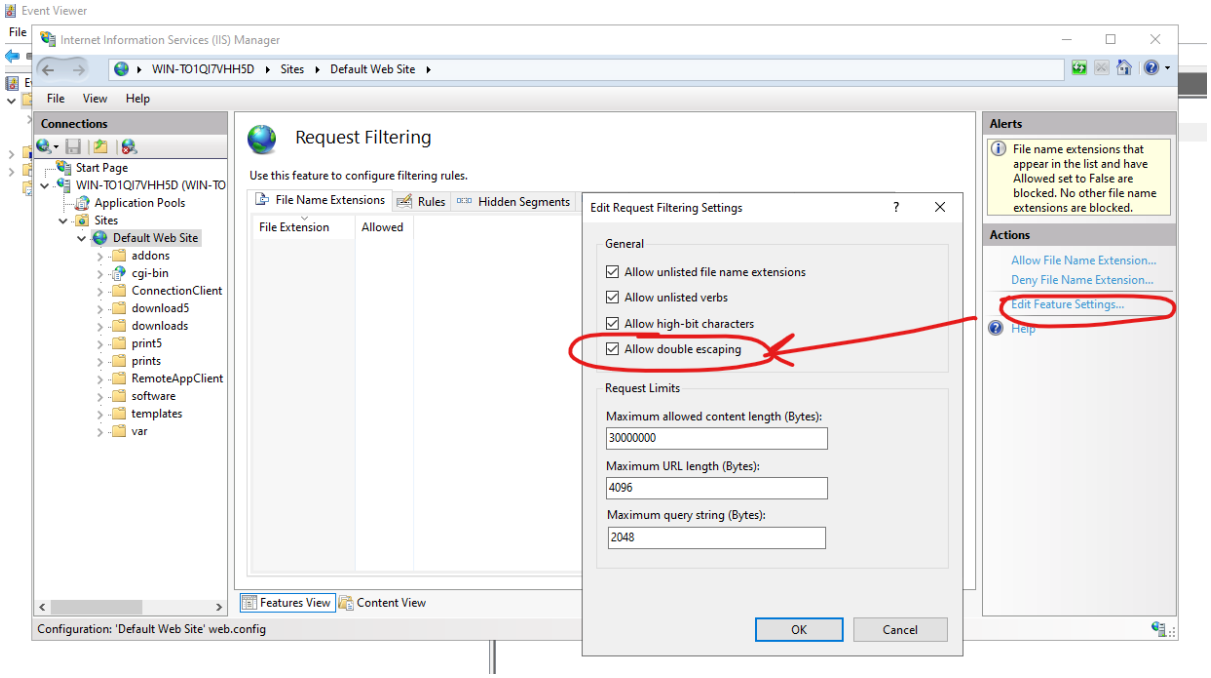




3. Feature-Einstellungen bearbeiten: Klicken Sie im Aktionsbereich auf „Feature-Einstellungen bearbeiten“.

4.

Aktivieren Sie die doppelte Escape-Erlaubnis: Aktivieren Sie im Dialogfeld "Anforderungsfiltereinstellungen bearbeiten" das Kontrollkästchen für "Doppelte Escape-Erlaubnis zulassen."



5. IIS neu starten (optional): Das Neustarten von IIS kann helfen, sicherzustellen, dass die Änderungen wirksam werden.

Verwendung von Servern hinter einem Reverse Proxy

Es ist möglich, Server hinter Reverse-Proxys über xhr-Polling zu verwenden, mit einigen Einschränkungen.

Wie beschrieben Websockets sind kein Teil des HTTP-Protokolls, auch wenn die erste HTTP-Anfrage wie eine HTTP-Anfrage aussieht, ist sie es tatsächlich nicht. Daher unterstützen die meisten bekannten Reverse-Proxys keine Websockets und verwerfen viele wichtige Bereiche der ersten Websocket-Anfrage.

Wenn Sie wissen, dass der Server hinter einem Reverse-Proxy steht, deaktivieren Sie Websockets, indem Sie diese Option in Clients\www\software\html5\settings.js festlegen:

disablewebsocket = true;

Das wird die Nutzung von erzwingen XHR-Abfrage und Verzögerungen bei der Verbindung vermeiden.

Wenn Sie keine Datei mit dem Namen „settings.js“ im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software\html5“ haben, dann ist Ihre TSplus-Version älter und diese Dokumentation gilt nicht. Bitte aktualisieren Sie zuerst Ihr System oder kontaktieren Sie den Support.

Bitte beachten Sie, dass die Verwendung von XHR-Polling aufgrund seiner Verbindungsnatur nicht so stabil ist wie Websockets.

Die andere Einschränkung bei der Verwendung von Xhr-Polling über einen Reverse-Proxy ist die schlechte Unterstützung beim Hochladen von Dateien. Während der Arbeit mit XHR in direkter Verbindung, beispielsweise über einen Apache-Reverse-Proxy, kann Apache versehentlich den Upload der Datei unterbrechen.

TSplus Virtual Printer v2

Eine neue Version des Virtual Printer ist jetzt verfügbar!
Diese Version enthält ein wichtiges Update für die Virtual Printer-Komponente (v1.x -> v2.x).

Warum: Der Virtual Printer v2 ist das neueste Flaggschiff von Fabulatech, das viele Verbesserungen bringt und Probleme behebt, die von Kunden gemeldet wurden.

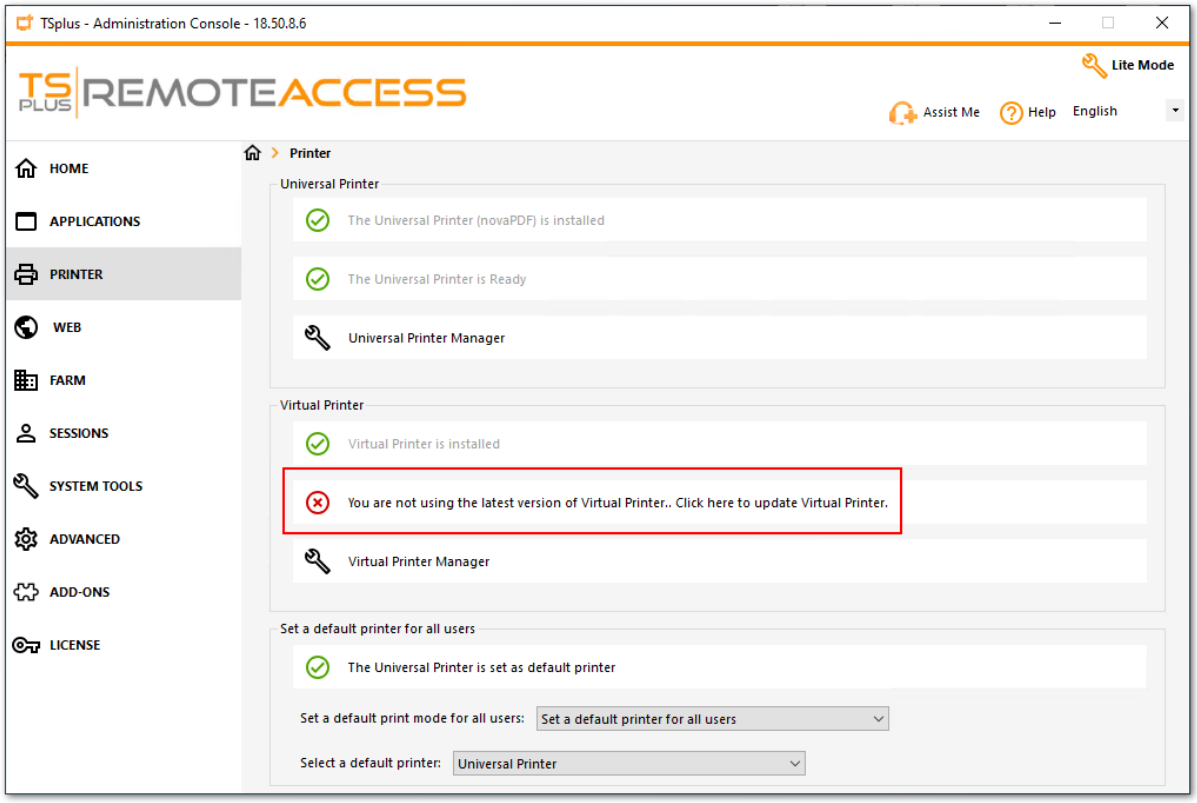
Achtung: Virtual Printer v1.x und v2.x sind nicht kompatibel, Sie benötigen die gleiche Hauptversion auf beiden Client- und Serverseiten, um ordnungsgemäß zu funktionieren.

Keine Panik: Das UpdateRelease bringt nur die neuen Virtual Printer Setup-Programme (Client und Server).
Sie befinden sich in C:\Program Files (x86)\TSplus\UserDesktop\files\addons .
Es liegt an Ihnen, das tatsächliche Update des virtuellen Druckers manuell über AdminTools auszulösen.

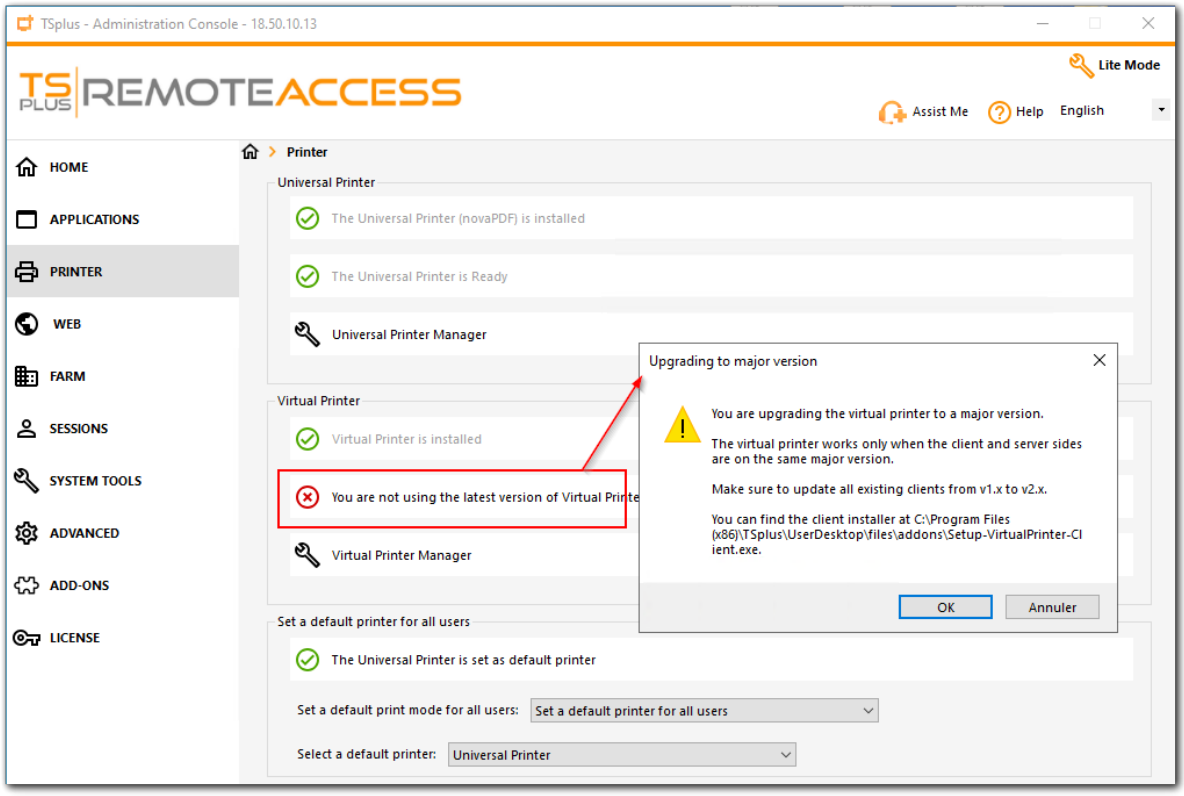
Links : TSplus Setup Voll TSplus UpdateRelease Rebrand-Update-Version

Wie aktualisieren?

Nach der Installation des UpdateRelease wird AdminTools erkennen, dass eine neue Version des virtuellen Druckers verfügbar ist.
Bis Sie auf die Schaltfläche „Hinweis aktualisieren“ klicken, bleibt Ihre derzeit installierte Version des virtuellen Druckers unverändert, und alles wird wie zuvor weiter funktionieren.

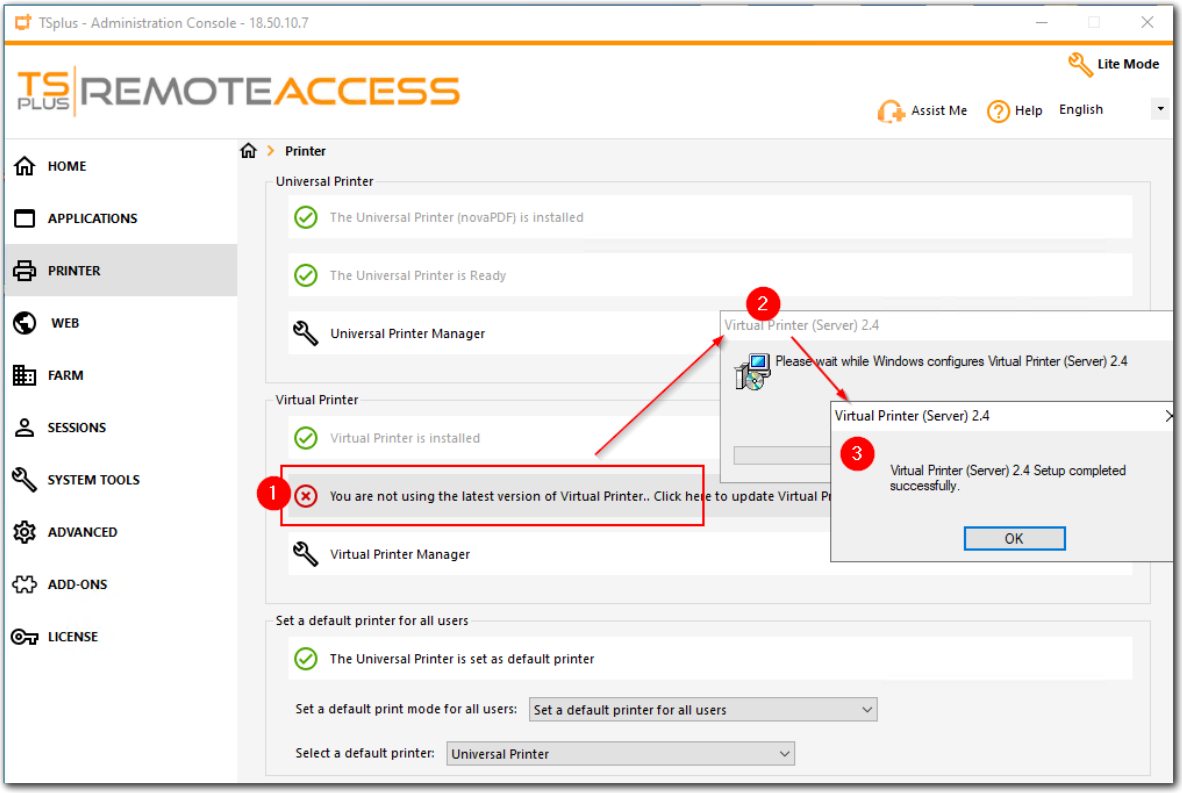


OK, aber wir sind hier, um die neue VP-Version zu installieren, also klicken wir auf die Schaltfläche „Update-Benachrichtigung“.

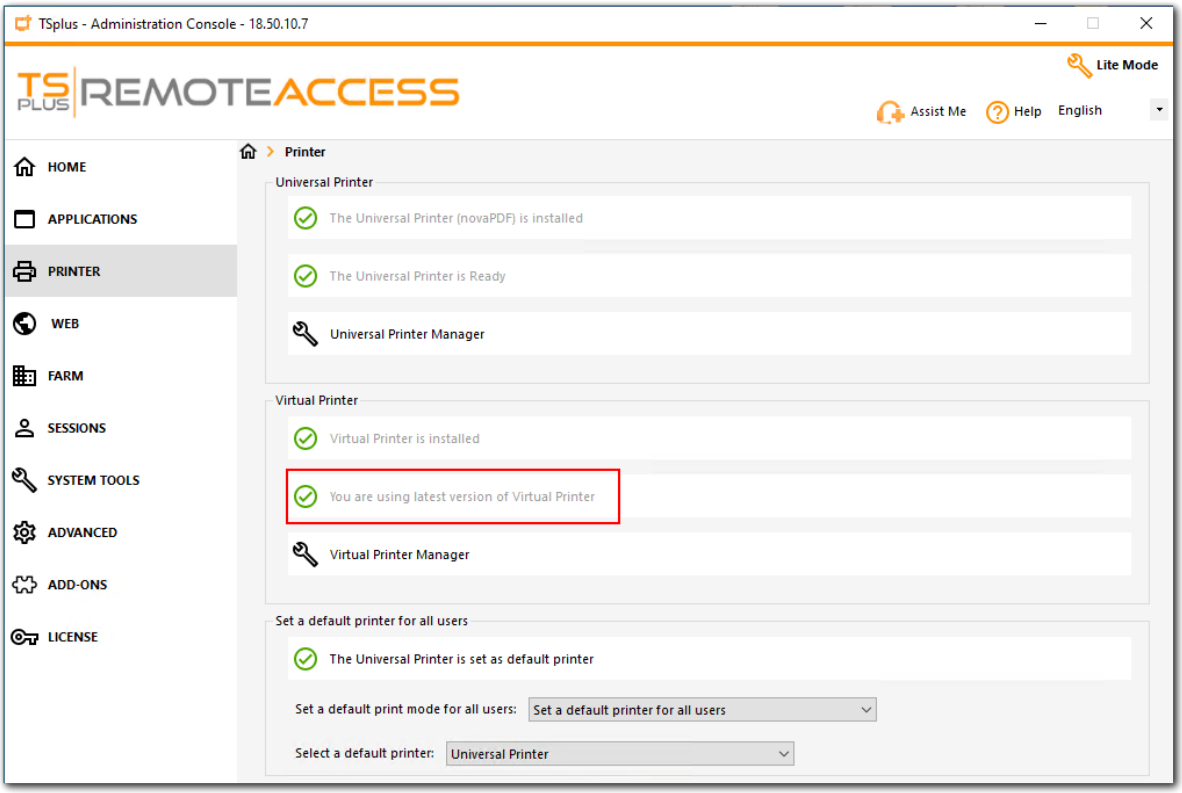


Ein Bestätigungsdialog fragt, ob Sie den virtuellen Drucker wirklich auf die nächste Hauptversion

aktualisieren möchten. Klicken Sie auf „OK“.



Sobald installiert, erkennt das AdminTools, dass Sie auf dem neuesten Stand sind.



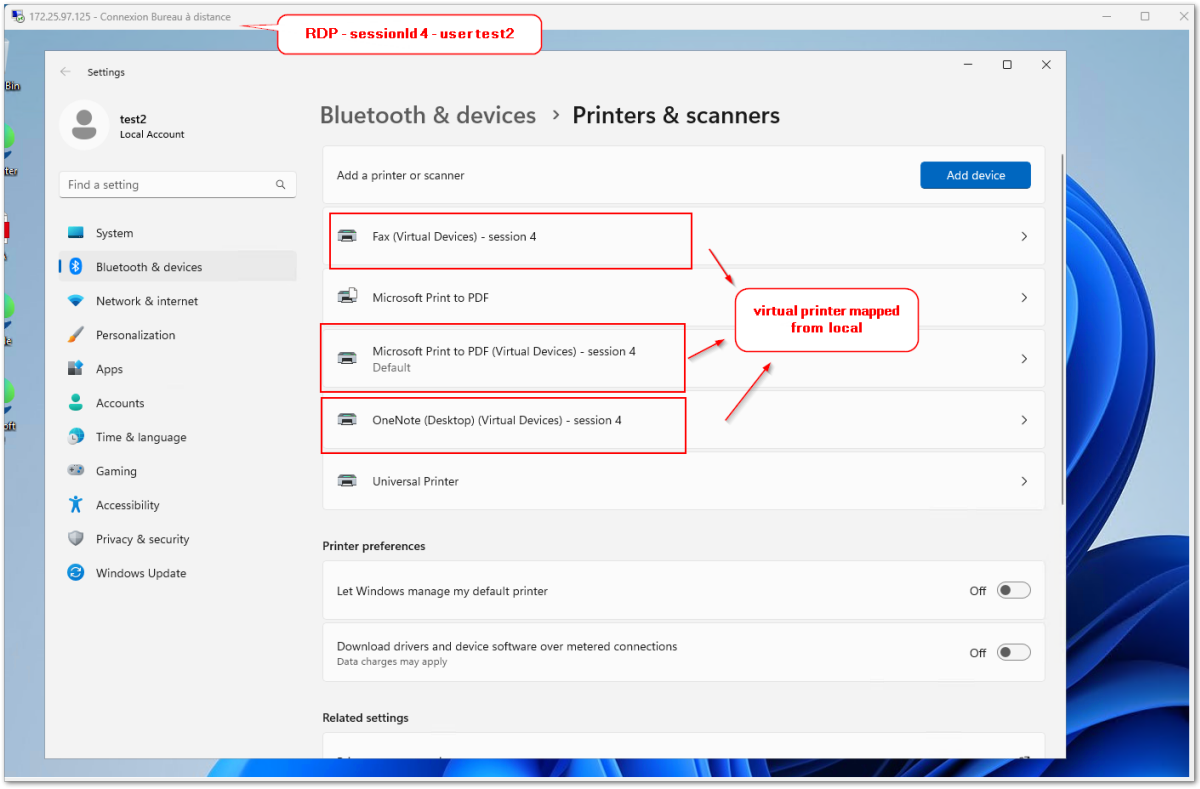
Achtung: In diesem Schritt können nur Clients, die die gleiche Hauptversion (v2.x) ausführen, über den virtuellen Drucker auf diesem Server drucken. Stellen Sie sicher, dass Sie das Update von Server und Clients koordinieren. Der Client-Installer befindet sich in „C:\Program Files (x86)\TSplus\UserDesktop\files\addons\Setup-VirtualPrinter-Client.exe“.

Breaking Change !

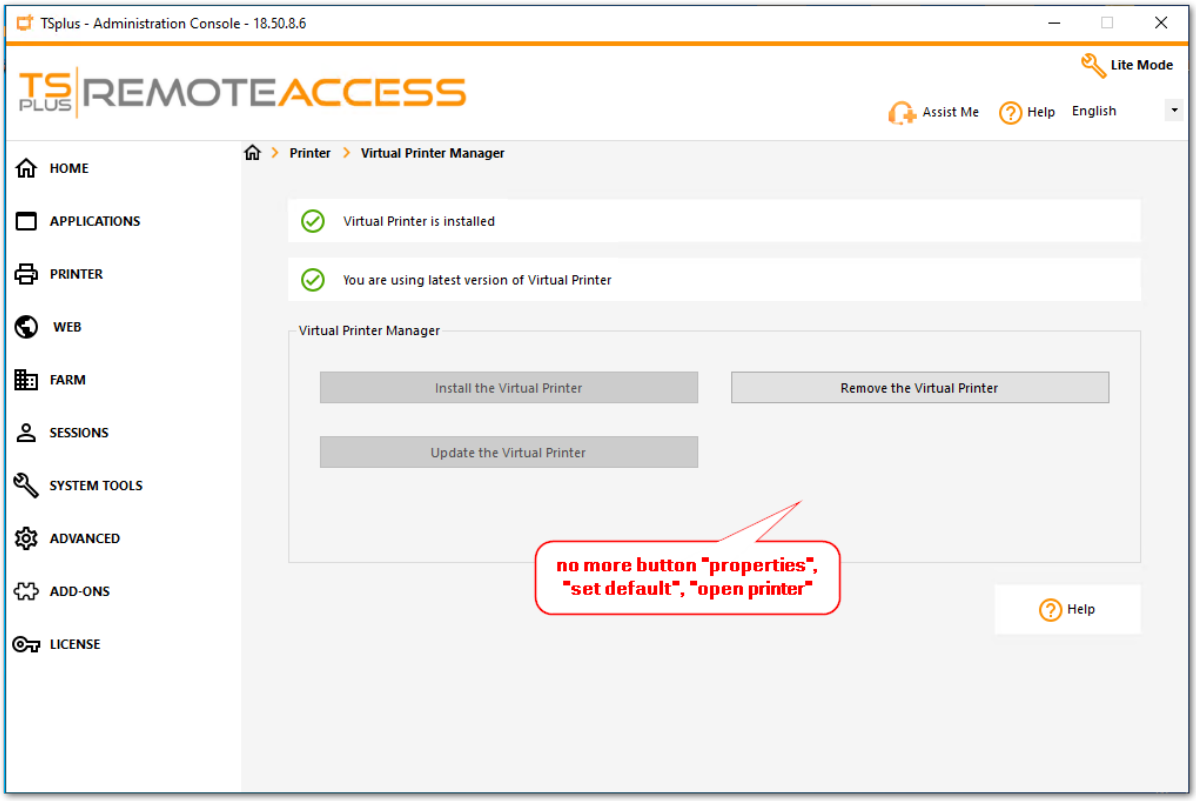
Es gibt nicht mehr ein einzelnes „Virtual Printer“-Gerät in der Druckerliste. Stattdessen wird jeder lokale Drucker jetzt einem entsprechenden virtuellen Drucker in der RDP-Sitzung zugeordnet.

Im Screenshot unten ist der Benutzer „test2“ mit der RDP-Sitzung #4 verbunden. Beim Öffnen des Druckerpanels,
er kann seine lokalen Drucker sehen und verwenden. Jeder Druckername folgt diesem Format: $printerName (Virtuelle Geräte) - Sitzung $sessionId .

Die Tatsache, dass der Benutzer jetzt jeden seiner lokalen Drucker einzeln sieht, ist eine große Verbesserung der Benutzererfahrung, und deshalb drängt Fabulatech auf diese neue Version.

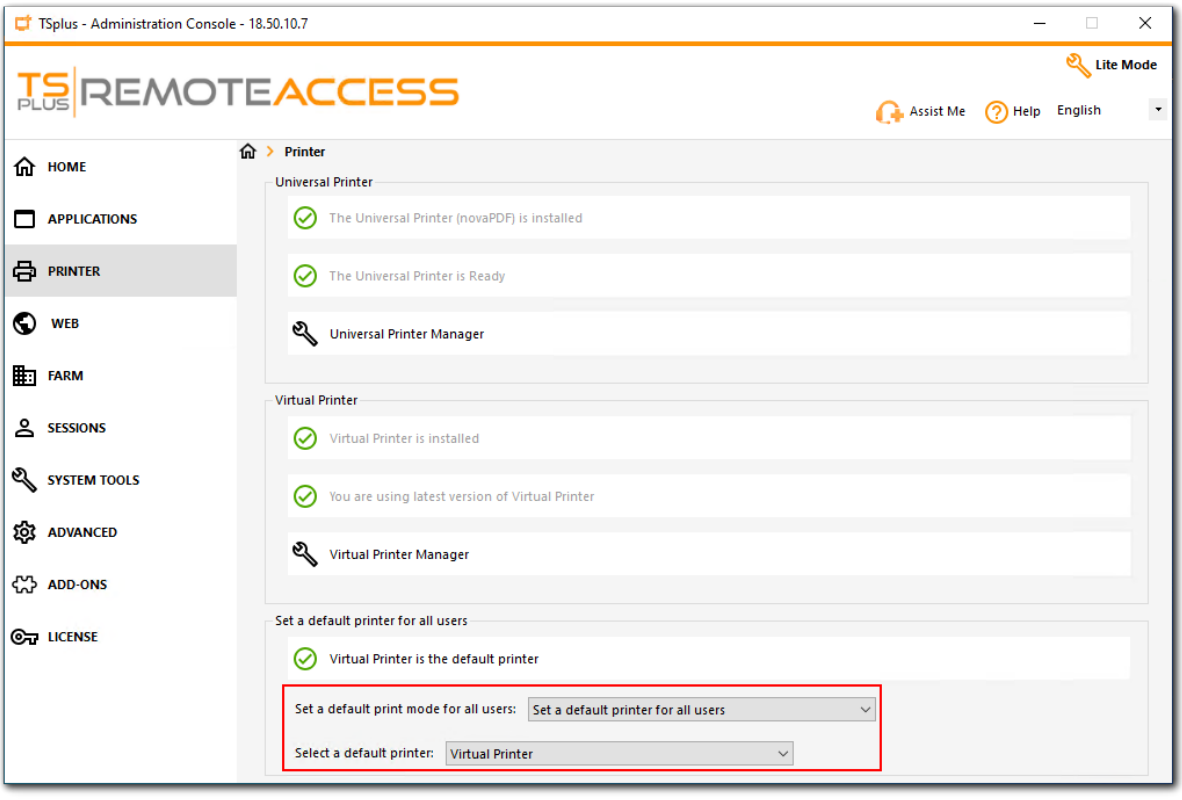


Wegen dessen haben wir einige Teile der AdminTools-Benutzeroberfläche angepasst, wie den Virtual Printer Manager: Einige Schaltflächen wurden entfernt.

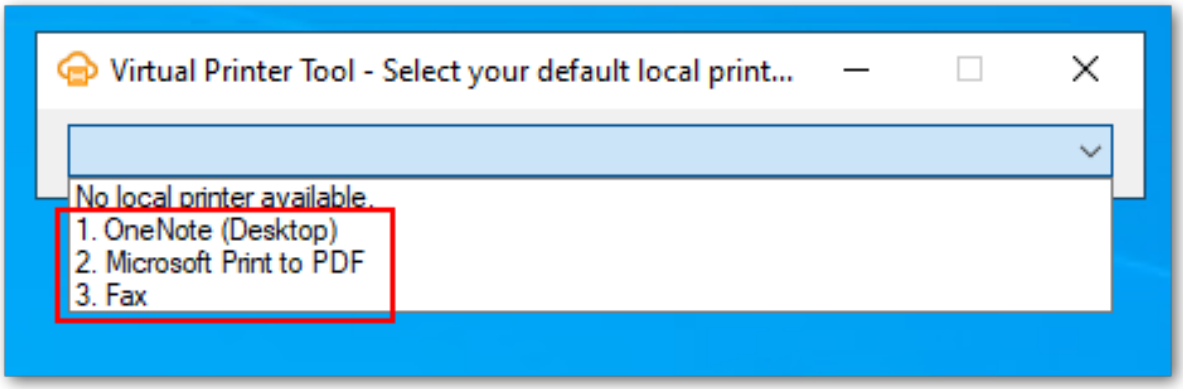


Wie konfiguriert man?

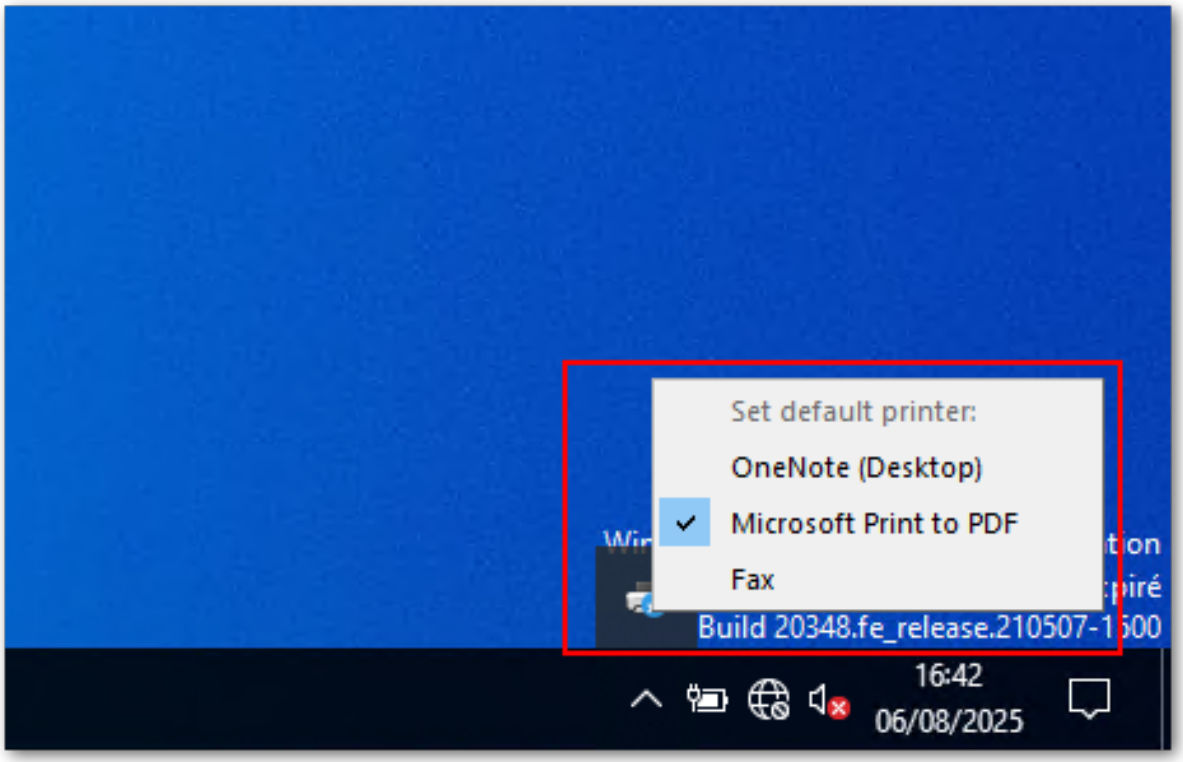
Die Konfiguration bleibt weiterhin gleich in den AdminTools und sollte wie zuvor funktionieren.



Wenn Sie die Virtual Printer Tools verwenden, ändert sich nichts und es funktioniert wie zuvor.



Wenn Sie den Selektor in der Symbolleiste verwenden, ändert sich nichts und es funktioniert wie zuvor.



Wie man den Namen der zugeordneten Geräte des Virtuellen Druckers anpasst?

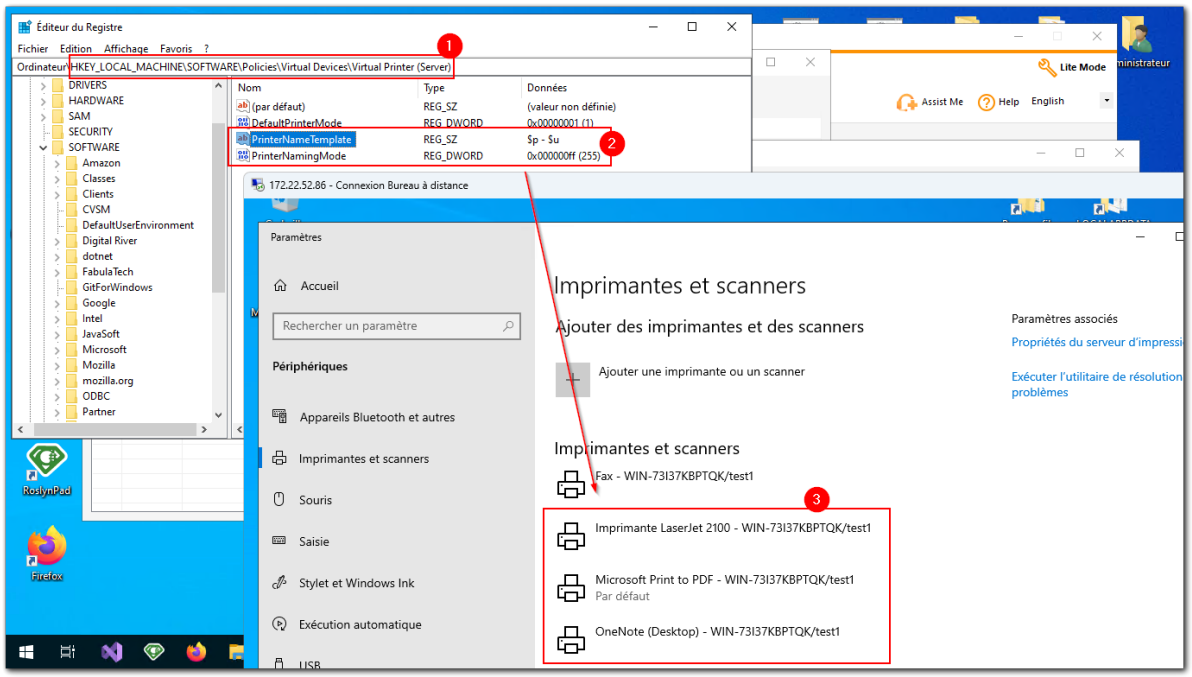
Auf dem Server führen Sie die angehängte „customize-virtual-printer-name.reg“ aus. Herunterladen

Es werden 2 Schlüssel in Ihrer Registrierung hinzugefügt.
HKEY_LOCAL_MACHINE\SOFTWARE\Richtlinien\Virtuelle Geräte\Virtueller Drucker (Server)
Der PrinterNameTemplate ist die Vorlagenzeichenfolge, und es stehen 3 Variablen zur Verfügung:

- $p - Druckername
- $u - vollständiger Benutzername (domain/user oder compname/user)
- $s - Sitzungsnummer

Angesichts einiger Fabuletch-Einschränkungen : **Die Angabe von $p und $u oder $p und $s ist obligatorisch.**
Es ist erforderlich, da die Druckernamen auf dem Server für verschiedene Benutzer eindeutig sein sollten.

Beispiel: PrinterNameTemplate = “$p $u”, das Ergebnis sehen Sie im Screenshot der RDP-Sitzung unten.



Erweiterte Konfiguration

Die erweiterte Konfiguration für den Virtual Printer v2 kann serverseitig über Gruppen- oder lokale Richtlinienobjekte unter Computerconfiguration > Administrative Vorlagen > Virtuelle Geräte > Virtual Printer (Server) verwaltet werden.

Die folgenden Einstellungen sind für die Integration von Remote Access relevant:

- Standarddruckerauswahlmodus: Definiert, wie der Standarddrucker jedes Mal zugewiesen wird, wenn sich ein Benutzer in eine Remote-Sitzung einloggt.

- Druckernamen-Vorlage: Gibt das Namensformat für virtuelle Drucker aus Benutzersitzungen an.
- Limitqualität für große Drucke: Reduziert die Druckqualität für Seiten, die eine bestimmte Größe überschreiten, um den Großformatdruck zu beschleunigen und gleichzeitig die maximale Qualität für kleinere Seiten zu erhalten.

Für vollständige Konfigurationsdetails konsultieren Sie bitte die Dokumentation zu Virtual Printer GPO unter https://www.fabulatech.com/printer-for-remote-desktop-server-help/gpo.html

TSplus Virtual Printer

Der TSplus Virtual Printer ist eine neue Alternative zu klassischen Remote-Desktop-Drucklösungen, die unzuverlässig, hardwareabhängig und schwer zu verwalten sein können. Der einzigartige Kompressionsalgorithmus des virtuellen Druckers verbessert die Übertragungsgeschwindigkeit von Remote-Druckaufträgen, indem er den Datentransfer minimiert und gleichzeitig die Bildqualität aufrechterhält.

Hinweis Der TSplus HTML5-Client wird nicht unterstützt und erfordert die TSplus Universal Printer .

Vorteile

- Einzelbenutzer- und Mehrbenutzerumgebungsunterstützung.
- Nullkonfiguration ist erforderlich.
- Funktioniert mit allen virtuellen Maschinen.
- Gemischte 32- und 64-Bit-Umgebung.

Voraussetzungen

TSplus Virtual Printer OS-Kompatibilitätsliste:

- Windows **7**
- Windows **8/8.1**
- Windows **10**
- Windows **11**
- Windows **Server 2008 R2**
- Windows **Server 2012 R2**
- Windows **Server 2016**

- Windows **Server 2019**
- Windows **Server 2022**
- Windows **Server 2025**

Der TSplus Virtual Printer ist kompatibel mit:

- Der von TSplus generierte Client
- Der TSplus RemoteApp-Client
- Das TSplus RemoteApp-Plugin bei der Verwendung des Webportals
- Der Microsoft Remote Desktop-Client

Es ist nicht kompatibel mit:

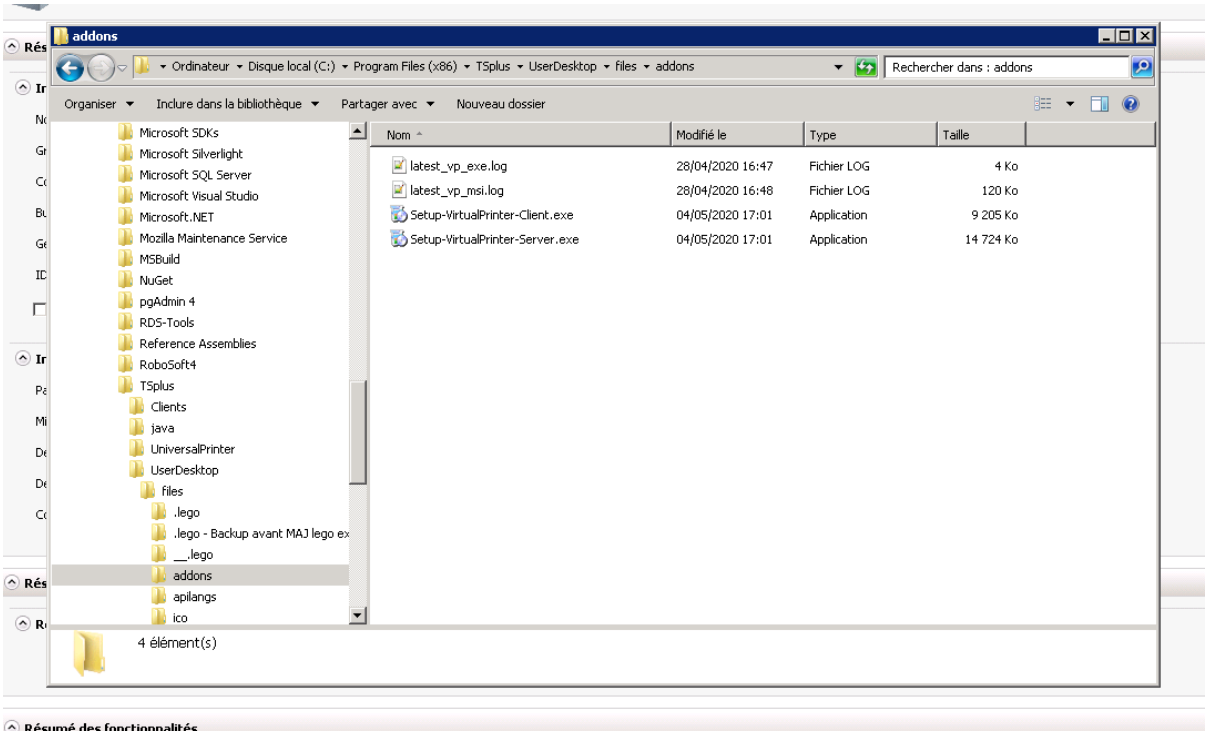
- Der TSplus HTML5-Client
- Hardcodierte Thin-Client-Geräte, bei denen die Client-Seiteneinrichtung nicht installiert werden kann.

Zwei Teile

Der TSplus Virtual Printer besteht aus zwei Komponenten:

- Eine serverseitige Komponente, die mit TSplus Remote Access installiert wird.
- Eine Desktop-Komponente, die auf der Windows-Arbeitsstation des Endbenutzers installiert ist.

Beide Setups sind direkt auf der Serverseite im Ordner „C:\Program Files (x86)\TSplus\UserDesktop\files\addons“ verfügbar und heißen „Setup-VirtualPrinter-Server.exe“ und „Setup-VirtualPrinter-Client.exe“.



Die Client-Installation ist ebenfalls von Ihrem TSplus-Webserver aus verfügbar, über den untenstehenden Link:

yourtsplusserveriporpublicdomain/addons/Setup-VirtualPrinter-Client.exe

Sie können auch eine stille Installation des Clients über eine Befehlszeile durchführen, indem Sie das Setup mit den folgenden Parametern ausführen:

/SUPPRESSMSGBOXES /VERYSILENT /SILENT /no_ui

Loslegen

TSplus Virtual Printer wird während der ersten TSplus-Installation automatisch installiert und ist während der Testphase direkt verfügbar.

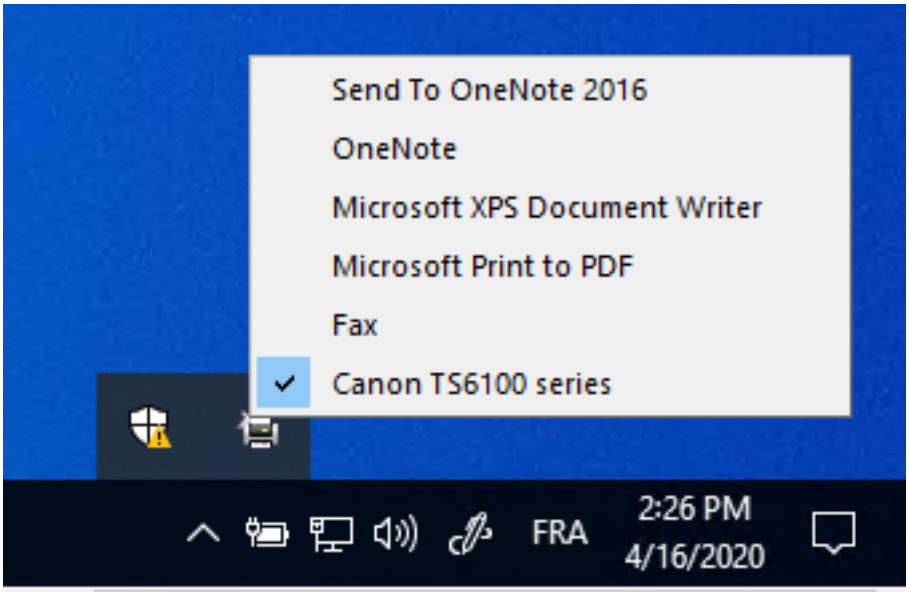
Sobald TSplus installiert ist, müssen Sie den „Virtual Printer Client“ auf dem Computer des Benutzers installieren.

Wenn Sie sich remote mit Ihrem TSPlus-Server verbinden, indem Sie entweder **Microsoft RDP-Client** mstsc **TSplus generierter Client** oder **Web Portal RemoteApp-Plugin** , Sie können von Ihrer Remote-Sitzung aus auf Ihren lokalen Drucker mit dem Drucker „Virtual Printer“ drucken. Standardmäßig ist der ausgewählte lokale Drucker der lokale Standarddrucker.

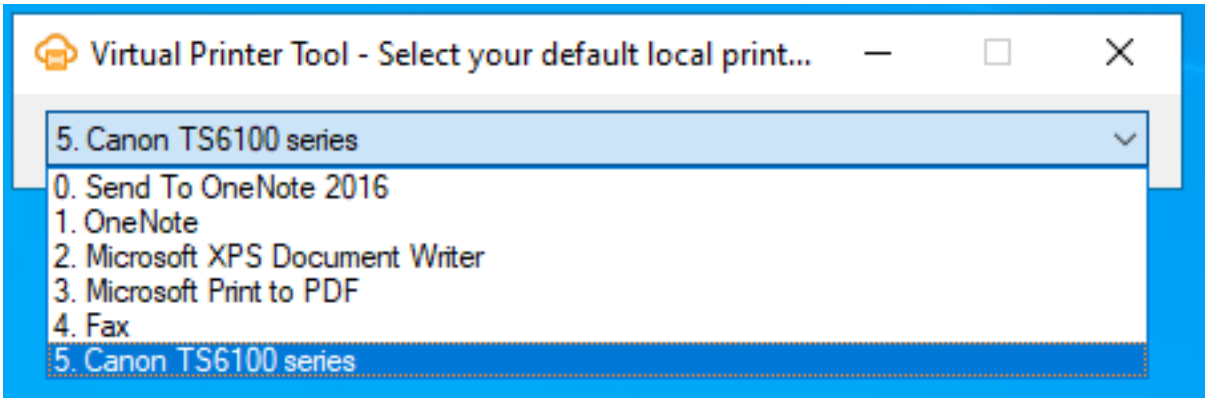
Sie haben 2 Möglichkeiten, den lokalen Drucker, der dem „Virtual Printer“ Drucker zugeordnet ist, je nach Ihrer Situation zu ändern:

1.Wenn Sie den vollständigen Desktop verwenden, können Sie auswählen, welcher lokale

Drucker verwendet werden soll, indem Sie das Symbol des virtuellen Druckers im Systray verwenden:



2.Wenn Sie keinen Zugriff auf den vollständigen Desktop haben, müssen Sie das "Virtual Printer Tool" mit dem Namen "VirtualPrinterTool.exe" verwenden, das sich in "C:\Program Files (x86)\TSplus\UserDesktop\files" befindet. Hinweis: Sie können entweder die Anwendung dem Benutzer zuweisen oder sie automatisch beim Anmelden über die erweiterten Einstellungen des Virtual Printers ausführen lassen.



Konfiguration

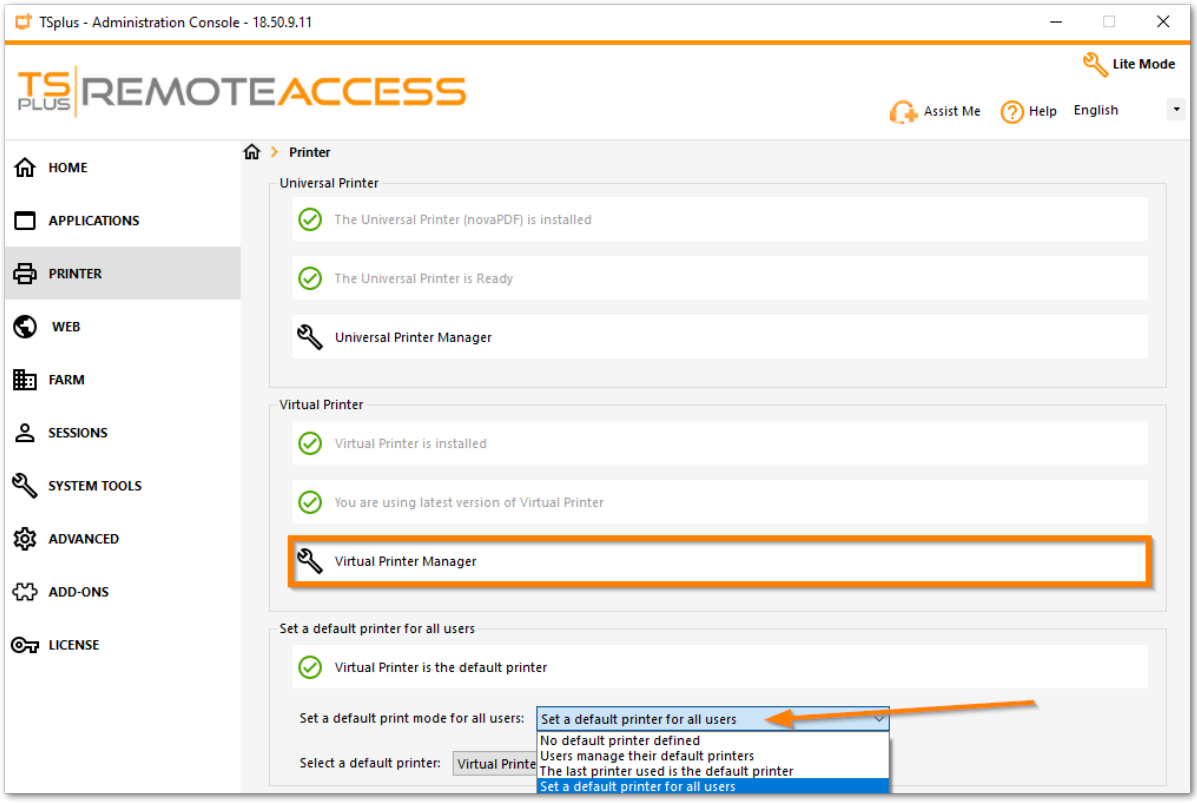
Um auf das Steuerfeld des TSplus Virtual Printer zuzugreifen, navigieren Sie bitte über das AdminTool: Drucker > Virtueller Druckermanager.

Einen Standarddrucker für alle Benutzer festlegen

- Kein Standarddrucker definiert: Die Standarddruckerkonfiguration des Benutzers ist nicht

betroffen.

- Benutzer verwalten ihre Standarddrucker: die Option „Windows meinen Standarddrucker verwalten lassen“ ist deaktiviert, und es liegt daher am Benutzer, seinen Standarddrucker auszuwählen.
- Der letzte verwendete Drucker ist der Standarddrucker: die Option „Windows meinen Standarddrucker verwalten lassen“ ist aktiviert.
- Einen Standarddrucker für alle Benutzer festlegen: der Administrator zwingt den Benutzer, den Standarddrucker festzulegen.



Fehlerbehebung des Virtuellen Druckers

Wenn der Virtuelle Drucker nicht funktioniert, ist die häufigste Ursache, dass entweder die clientseitige Software „Druckanwendung“ nicht im Task-Manager des lokalen Computers des Benutzers ausgeführt wird oder dass die Virtuelle Drucker (Server)-Software auf dem lokalen Computer des Benutzers installiert wurde, anstatt die Virtuelle Drucker (Arbeitsplatz)-Version (Setup-VirtualPrinter-Client.exe). Im Folgenden sind die Schritte zur Fehlersuche im Detail für sowohl die Client- als auch die Serverseite aufgeführt.

Bitte beachten Sie, dass der Virtual Printer nicht mit unserem HTML5-Client kompatibel ist. Wenn Sie den HTML5-Client verwenden, nutzen Sie bitte stattdessen den Universal Printer.

Fehlerbehebungshandbuch

Wie aktiviert man eine Volumenlizenz vom Server nach der Einrichtung?

Wenn Sie Ihr Produkt ohne Befehlszeile installiert haben, dann ist es als Testversion installiert.

Aktivieren

Um Ihre Volumenlizenz zu aktivieren, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

- **Remote Access & Two-Faktor-Authentifizierung**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /Benutzer 1 (1 bis 50 oder unbegrenzt)
  /Edition Enterprise (Desktop, MobileWeb, Enterprise)
  /supportyears 1 (1,2,3 nur)

Beispiel : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 30 /edition Enterprise /supportyears 1

Beispiel : 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
  /Edition Ultimate Essentials oder Ultimate
  /supportyears 1 (1,2,3 nur)

Beispiel : 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
  /Benutzer 1 (1 für Startup, 5 für Essentials, 10 für Business)
  /supportyears 1 (1 für Startup, 5 für Essentials, 10 für Business)

Beispiel : C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 5 /supportyears 1

- **Sie können meine folgenden zusätzlichen Parameter hinzufügen:**
  — Ihre Kommentare Geben Sie die Kommentare an, die Sie im Lizenzportal an die Lizenz anhängen möchten.
  — /verysilent Führen Sie das Installationsprogramm im Hintergrund aus. Dies ermöglicht die Integration dieses Installationsprogramms in Ihre eigenen Initialisierungs- oder Automatisierungsskripte.

Beispiel : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users unlimited /edition Enterprise /supportyears 3 /comments "Dies ist ein Kommentar"*

Parameter

Dieser Befehl nimmt die folgenden Parameter:

wenn Sie gerne mit Befehlszeilen arbeiten und sich fragen, welche anderen Befehlszeilen verfügbar sind, besuchen Sie bitte diese spezifische Dokumentation)

Update-Support

Um Ihr Update-/Support-Abonnement zu verlängern, wählen Sie 1, 2 oder 3 im Betrieb der Verlängerungszeit.
Verwenden Sie diesen Befehl:

AdminTool.exe /vl /renewsupport YOUR-VOLUME-LICENSE-KEY /supportyears 1"

Fehlende Unterstützung hinzufügen

Dieser Befehl ist besonders nützlich, wenn der Kunde vergessen hat, den Support während der Installation zu aktivieren, oder wenn er ein bestimmtes Enddatum für seinen Supportzeitraum festlegen muss.

Führen Sie diesen Befehl als Administrator aus und ersetzen Sie die Details durch Ihre eigenen Lizenzinformationen und das bevorzugte Support-Enddatum:

AdminTool.exe /vl /activate-support IHR-VOLUMEN-LIZENZSCHLÜSSEL /users [number] /edition [edition] /endofsupport [YYYY-MM-DD]

Um die Unterstützung für einen Remote Access 5-Benutzer mit der Printer-Edition bis zum 25. Juli 2026 zu aktivieren, geben Sie ein:

AdminTool.exe /vl /activate-support YOUR-VOLUME-LICENSE-KEY /users 5 /edition Printer /endofsupport 2026-07-25

Dieses neue Feature erleichtert die Verwaltung von Supportzeiträumen, sodass die Kunden immer wissen, wann ihr Supportzeitraum beginnt und endet.

Wie zeigt man die verbleibenden Lizenzguthaben für einen Volumenlizenzschlüssel an?

Um die verbleibenden Lizenzguthaben für einen Volumenlizenzschlüssel anzuzeigen, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

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

Parameter

Dieser Befehl kann vier Parameter annehmen:

- VOLU-MELI-CENS-EKEY : Verwenden Sie Ihren eigenen Volumenlizenzschlüssel
- /login JOHNDOE : Geben Sie das Login des Partners an, der mit dem Volumenlizenzschlüssel verbunden ist.
- /Edition Essentials: Geben Sie den optionalen Editionsparameter für Advanced Security und Server Monitoring Produkte an.
- /silent : führt den Befehl still aus

Die Ausgabe wird in der benutzerspezifischen Umgebungsvariable mit dem Namen gespeichert. VOLUMEN_LIZENZ_GUTHABEN Es kann erforderlich sein, den Wert von VOLUMEN_LIZENZ_GUTHABEN von einem anderen Prozess, unter Verwendung des Befehls: echo %VOLUME_LICENSE_CREDITS%

Bitte finden Sie unten die erwarteten Editionen für Advanced Security und Server Monitoring Produkte:

- Advanced Security: „Essentials“, „Ultimate“
- Server Monitoring: „Essentials“, „Startup“, „Business“

Die folgenden ausführbaren Dateien müssen verwendet werden, um die jeweilige Anzahl der verbleibenden Credits zu finden:

- Remote Access: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

- Advanced Security: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- Server Monitoring: 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
- Remote Work: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

---

Titel: „Wie zeigt man die verbleibenden Supportguthaben für einen Volumenlizenzschlüssel an?“

Um die verbleibenden Supportguthaben für einen Volumenlizenzschlüssel anzuzeigen, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE [/edition Essentials] [/silent]

Parameter

Dieser Befehl kann vier Parameter annehmen:

- VOLU-MELI-CENS-EKEY : Verwenden Sie Ihren eigenen Volumenlizenzschlüssel
- /login JOHNDOE : Geben Sie das Login des Partners an, der mit dem Volumenlizenzschlüssel verbunden ist.
- /Edition Essentials: Geben Sie den optionalen Editionsparameter für Advanced Security und Server Monitoring Produkte an.
- /silent : führt den Befehl im Hintergrund aus.

Die Ausgabe wird in der benutzerspezifischen Umgebungsvariable mit dem Namen gespeichert. VOLUMEN_LIZENZ_GUTHABEN Es kann erforderlich sein, den Wert von VOLUMEN_LIZENZ_GUTHABEN von einem anderen Prozess, unter Verwendung des Befehls: echo %VOLUME_LICENSE_CREDITS%

Bitte finden Sie unten die erwarteten Editionen für Advanced Security und Server Monitoring Produkte:

- Advanced Security: „Essentials“, „Ultimate“
- Server Monitoring: „Essentials“, „Startup“, „Business“

Die folgenden ausführbaren Dateien müssen verwendet werden, um die jeweilige Anzahl der verbleibenden Credits zu finden:

- Remote Access: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- Advanced Security: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- Server Monitoring: 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
- Remote Work: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

Wie man eine Lizenz vom Server deaktiviert?

Um einen Server, der mit einem Volumenlizenzschlüssel aktiviert wurde, zu deaktivieren, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

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

Wie aktiviert man eine Lizenz vom Server?

Um einen Server zu aktivieren, der zuerst mit einem Volumenlizenzschlüssel aktiviert und später deaktiviert wurde, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

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

Wie man eine Lizenz im Lizenzportal deaktiviert?

Sie müssen zuerst die Lizenz im Lizenzportal deaktivieren, und dann sicherstellen, dass der neue Status auf Ihrem Server angewendet wird, indem Sie seinen Status über die Verwaltungsanwendung oder die Befehlszeile aktualisieren.

Zuerst können Sie sowohl in der Liste der Lizenzen als auch auf den Lizenzdetails-Seiten auf die Schaltfläche „Deaktivieren“ klicken, um die ausgewählte Lizenz zu deaktivieren.

Die Lizenz wechselt vom Status „Aktiviert“ in den Status „Deaktivierung…“, was bedeutet, dass sie derzeit darauf wartet, dass der Server sich selbst deaktiviert.
Dann wird der Server am nächsten Tag automatisch deaktiviert, wenn er über einen Internetzugang verfügt.

Sie können dies auch manuell tun, indem Sie die folgende Befehlszeile als erhöhten Administrator ausführen:

AdminTool.exe /license /refresh

Beachten Sie, dass es nicht erforderlich ist, den Befehl zum Aktualisieren für alle installierten Software auszuführen. Die Aktualisierung wird von allen Produkten unterstützt, die mit dem Lizenzierungssystem von 2020 kompatibel sind.

Die Lizenz wird in Ihrer Lizenznutzung berücksichtigt, bis Ihr Server das Lizenzportal kontaktiert und seinen deaktivierten Status anerkannt hat.

Wie installiert man einen Volumenlizenzserver in einem Schritt?

Um einen Volumenlizenzserver in einem Schritt zu installieren, benötigen Sie:

- Laden Sie das Produkt-Setup-Programm herunter
- Verwenden Sie Ihren Volumenlizenzschlüssel
- Führen Sie das Setup-Programm mit Ihrem Volumenlizenzschlüssel als Parameter aus.

Ihr Volumenlizenzschlüssel ist derselbe für jede Installation eines neuen Servers. Wenn Sie sich nicht daran erinnern, melden Sie sich in Ihrem Konto im Lizenzportal an. Ihr Volumenlizenzschlüssel wird oben auf der Startseite (Lizenzen) angezeigt.

Um eine Volumenlizenz über ein Skript zu installieren und zu aktivieren, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments "Dies ist ein Kommentar"

Die skriptbasierte Aktivierung mit Volume License 2020 ist für die folgenden Produkte und alle ihre umbenannten Versionen verfügbar:

- Remote Access
- Erweiterte Sicherheit (auch bekannt als RDS-Knight)
- Server Monitoring (ehemals Server Genius)
- Zwei-Faktor-Authentifizierung

Parameter

Dieser Befehl nimmt die folgenden Parameter:

- **Remote Access & Two-Faktor-Authentifizierung**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /Benutzer 1 (1 bis 50 oder unbegrenzt)

/Edition Enterprise (Desktop, MobileWeb, Enterprise)
/supportyears 1 (1,2,3 nur)

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  TSplus-Security.exe
  /Edition Ultimate Essentials oder Ultimate
  /supportyears 1 (1,2,3 nur)

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>
  ServerMonitoring.exe
  /Benutzer 1 (1 für Startup, 5 für Essentials, 10 für Business)
  /supportyears 1 (1 für Startup, 5 für Essentials, 10 für Business)

Skriptmethoden

Um Setup-PRODUCT.exe mit der richtigen Befehlszeile zu starten, können Sie 3 Methoden verwenden:

1. Verwenden Sie Ihre eigenen Methoden für Verwaltungsskripte

2. Erstellen Sie eine Verknüpfung von Setup-PRODUCT.exe und bearbeiten Sie die Eigenschaften, um die Befehlszeile am Ende des Pfads hinzuzufügen.

3. Öffnen Sie einfach eine „Eingabeaufforderung“, indem Sie die Windows-Taste und die „R“-Taste gleichzeitig drücken, dann „cmd“ eingeben und die „Enter“-Taste drücken, um zu bestätigen. Diese Methode mit der Tastenkombination funktioniert auf jeder vorhandenen Windows-Version zum Zeitpunkt des Verfassens dieses Dokuments.

4. Sobald die Eingabeaufforderung erscheint, ändern Sie das aktuelle Verzeichnis in das Verzeichnis, in dem sich Ihr Installationsprogramm befindet (normalerweise Ihr Download-Ordner). Geben Sie beispielsweise ein:

   cd C:\Program Files (x86)\TSplus\UserDesktop\files

Und schließlich geben Sie den vollständigen Befehl ein, um das Setup-Programm mit den folgenden Parametern auszuführen, wobei Sie die gewünschten Werte angeben:

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “Dies ist ein Kommentar”

Finden Sie das relevante Administrationsprogramm

Die folgenden Programme unterstützen Volumenlizenzbefehle.
Der Programmname und der Speicherort hängen vom Produkt und seinem Installationsordner ab:

Remote Access & Two-Faktor-Authentifizierung
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

Die Programmausführung erfolgt im Hintergrund. Dies ermöglicht die Integration Ihres Lizenzaktivierungsprozesses in Ihre eigenen Initialisierungs- oder Automatisierungsskripte.

Titel: „Fehlerbehebung bei Aktivierungs-, Aktivierungs-, Deaktivierungs- und Aktualisierungsbefehlen“

Sollten Sie ein Problem untersuchen wollen und/oder beim Prototyping Ihrer Skripte, können Sie Erfolgs- und Fehlermeldungen erhalten, indem Sie sich die anschauen. **VolumeLicensing.log** Datei im Stammverzeichnis des Programms gefunden.

Titel: „So konfigurieren Sie einen Proxy-Server für den Internetzugang“

Proxy-Einstellungen, die während der Installation definiert wurden, werden gespeichert und zur Durchführung von Operationen an Lizenzen verwendet. Wenn keine Proxy-Einstellungen definiert wurden, verwendet das Volumenlizenzierungsprogramm die Proxy-Einstellungen von Internet Explorer (sofern in der laufenden Sitzung und/oder für den Windows-Dienst konfiguriert).

Sie können die Proxy-Einstellungen auch manuell konfigurieren, indem Sie die folgende Befehlszeile als erweiterter Administrator ausführen:

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

Parameter

#	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.

wenn Sie gerne mit Befehlszeilen arbeiten und sich fragen, welche anderen Befehlszeilen verfügbar sind, besuchen Sie bitte diese spezifische Dokumentation)

Titel: „So erhalten Sie Unterstützung für Volumenlizenzierung“

Das Support- und Serviceteam für Volumenlizenzierung wird Ihnen gerne helfen, falls Sie bei der

Installation und Ausführung der Volumenlizenzierung auf einem Server auf Probleme oder Schwierigkeiten stoßen.

Der einfachste Weg, das Team für Volumenlizenzierung Support & Services zu kontaktieren, besteht darin, ein Ticket in unserem Online-Helpdesk zu öffnen unter: https://support.tsplus.net

Wie aktualisiere ich die Benutzer einer Volumenlizenz vom Server?

Um die Anzahl der Benutzer zu ändern, die mit Ihrer aktivierten Volumenlizenz verbunden sind, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /users 10

Parameter

Dieser Befehl benötigt zwei Parameter:

- VOLU-MELI-CENS-EKEY : Verwenden Sie Ihren eigenen Volumenlizenzschlüssel
- Benutzer unbegrenzt: Verwenden Sie eine beliebige Zahl von 1 bis 50 oder "unbegrenzt"

Bitte beachten Sie, dass:

- Dieser Befehl gilt nicht für Advanced Security und 2FA Add-On.
- Server Monitoring akzeptiert nur die Zahlen 1, 5 und 10, die den drei verfügbaren Editionen von Server Monitoring entsprechen.
- Nur TSplus Remote Work akzeptiert eine Benutzeranzahl von mehr als 50.

Titel: „Wie aktualisiere ich die Edition einer Volumenlizenz vom Server?“

Um die Edition zu ändern, die mit Ihrer aktivierten Volumenlizenz verknüpft ist, führen Sie die folgende Befehlszeile als erweiterter Administrator aus:

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /edition Enterprise

Parameter

Dieser Befehl benötigt zwei Parameter:

- VOLU-MELI-CENS-EKEY : Verwenden Sie Ihren eigenen Volumenlizenzschlüssel
- Enterprise Edition

Bitte beachten Sie, dass:

- Dieser Parameter gilt nicht für Remote-Arbeit, Remote-Support, Serverüberwachung, 2FA-Add-On und Server Genius.
- Mögliche Editionen sind „Desktop“, „MobileWeb“ oder „Enterprise“ für Remote Access.
- Mögliche Editionen sind „Essentials“ oder „Ultimate“ für Advanced Security

wenn Sie gerne mit Befehlszeilen arbeiten und sich fragen, welche anderen Befehlszeilen verfügbar sind, besuchen Sie bitte diese spezifische Dokumentation)

Update-Support

Um Ihr Update-/Support-Abonnement zu verlängern, wählen Sie 1, 2 oder 3 im Betrieb der Verlängerungszeit.
Verwenden Sie diesen Befehl: AdminTool.exe /vl /renewsupport VOLU-MELI-CENS-EKEY / supportyears 1

Dieser Befehl ist nur ab Version 15.60.11.8 verfügbar.

Volumenlizenzierung

Volume Licensing ist eine Skriptlizenzierungslösung, die von TSplus für seine Lösungen bereitgestellt wird. Die folgenden Produkte unterstützen die Aktivierung mit Volume Licensing 2020: Remote Access, Remote Work, Advanced Security (auch bekannt als RDS-Knight), Remote Support oder Server Monitoring (ehemals Server Genius).

Wenn Ihr Volumenlizenzkonto im Lizenzverwaltungsportal erstellt wird, wird das Volumenlizenzteam Folgendes bereitstellen:

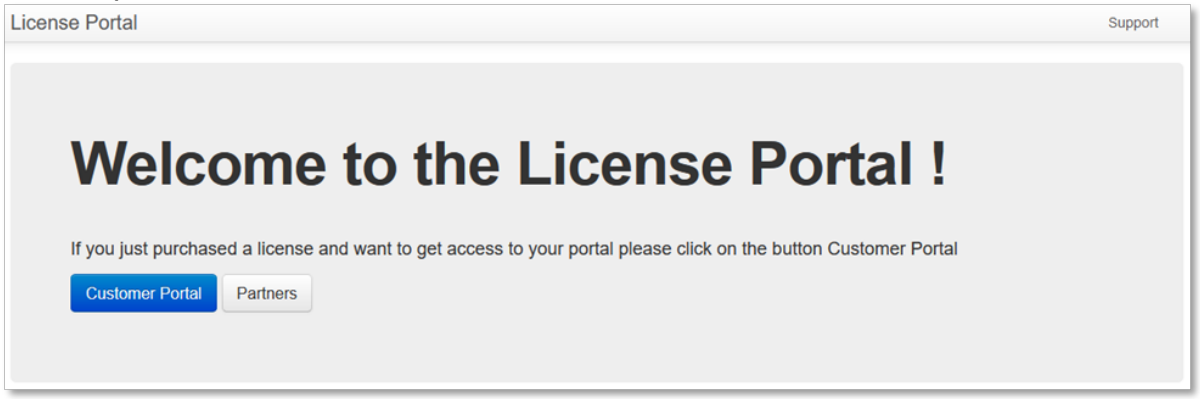
1. Ihr Volumenlizenzschlüssel (bitte halten Sie diese Informationen vertraulich)
2. Ihre Anmeldeinformationen für den Zugriff auf das Lizenzverwaltungsportal
3. Dieses Volume-Lizenzierung 2020 Administrationshandbuch

VIRTUAL PRINTER IST NICHT MEHR LIZENZIERT
Bitte beachten Sie, dass seit dem 15. März 2022 und der Version 15.40.3.14 der Virtual Printer nicht mehr lizenziert ist und in allen Editionen von TSplus Remote Access enthalten ist.

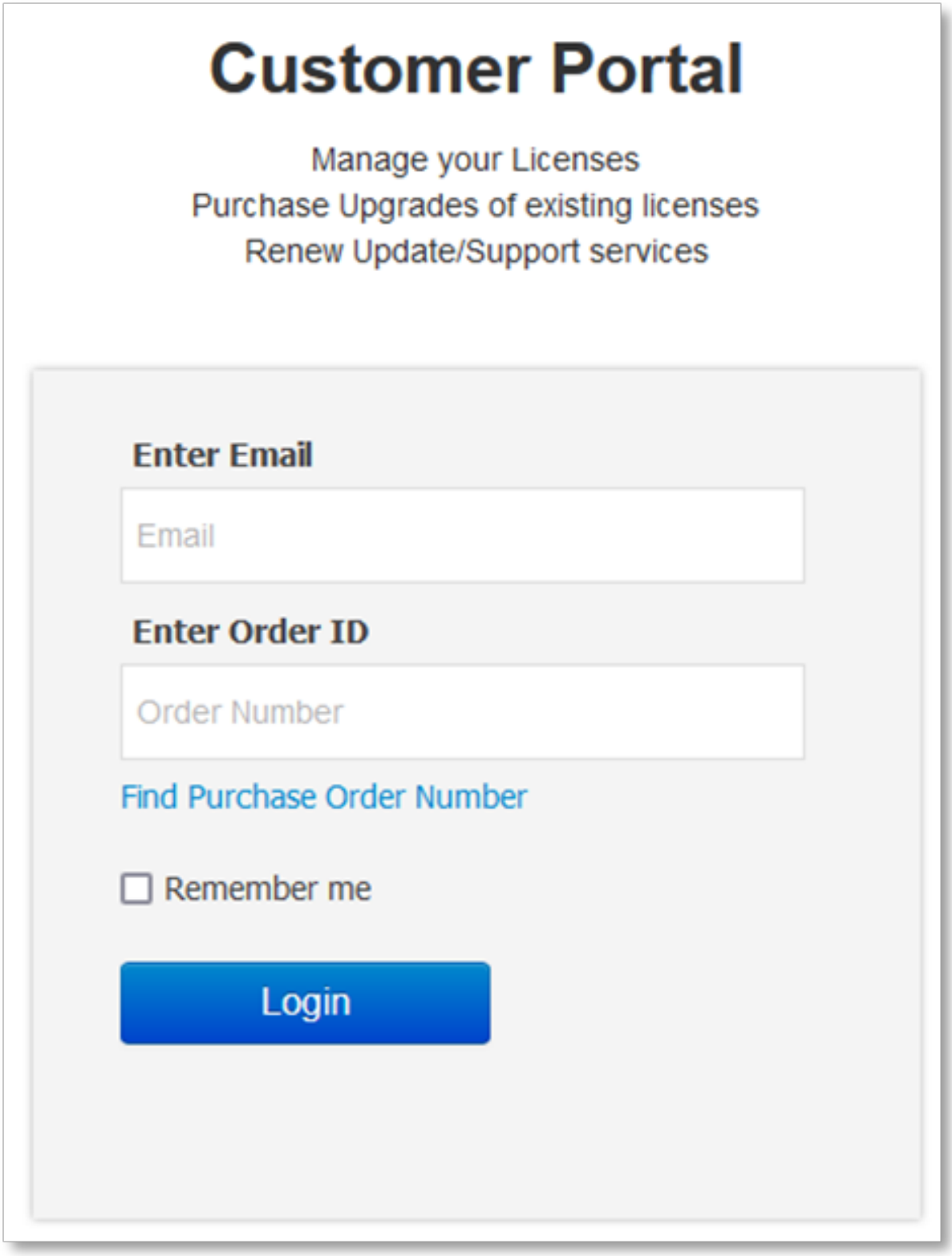
Wie verwalten Sie Ihre Volumenlizenzen?

Ihre Volumenlizenzen und Ihr Guthaben können im TSplus Lizenzportal überprüft und verwaltet werden.
Das TSplus Lizenzportal ist unter der folgenden URL verfügbar: https://license.tsplus.net

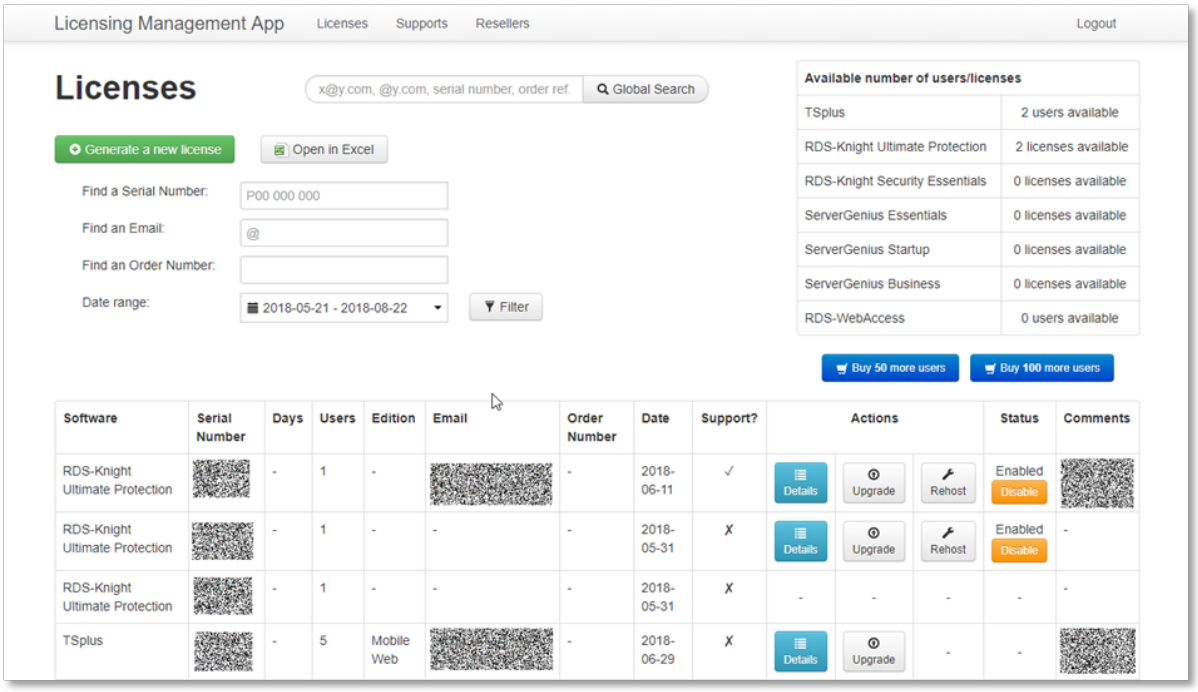
Um sich mit Ihrem Konto zu verbinden und darauf zuzugreifen, klicken Sie zunächst auf das Kundenportal, um den Bereich für Kunden zu erreichen:



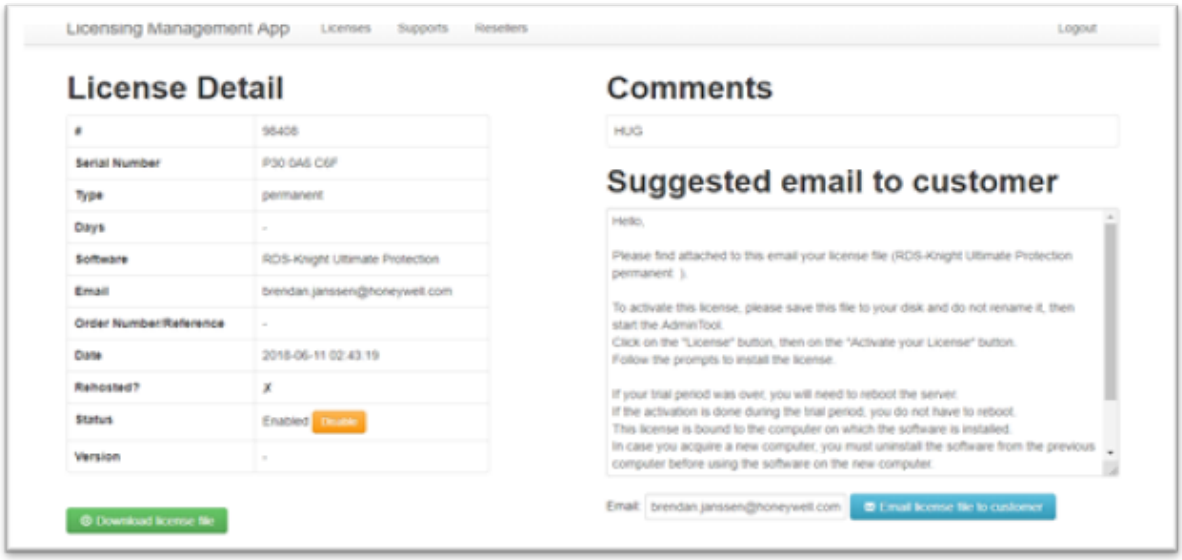
Dann geben Sie Ihre Anmeldeinformationen ein, um auf Ihr Konto zuzugreifen:



Sobald Sie sich angemeldet haben, sehen Sie die folgende Tabelle, in der alle Ihre Lizenzen aufgeführt sind. Es ist die Hauptseite, auf der Sie alle Ihre Lizenzen verwalten können. Wenn Sie noch keine Volumenlizenz aktiviert haben, wird diese Seite leer sein.



Um die Einzelheiten der Lizenzhistorie zu überprüfen, klicken Sie auf die Schaltfläche „Details“ der Lizenz, die Sie studieren möchten. Sie erhalten die Lizenzdetails-Seite, wie im Bild unten gezeigt.



TSplus Web App

TSplus Web App ist eine Progressive Web App (PWA), die moderne Browser-APIs nutzt, um ein nahtloses Remote Access-Erlebnis ohne umständliche Softwareinstallation oder komplizierte Verbindungsclients zu bieten. Entwickelt, um branchenübliche HTML5-Anzeigestandards und Kommunikationsprotokolle zu verwenden, erscheint die TSplus Web App als native Verbindungslösung, unabhängig davon, welches Gerät Sie verwenden.

Vorteile

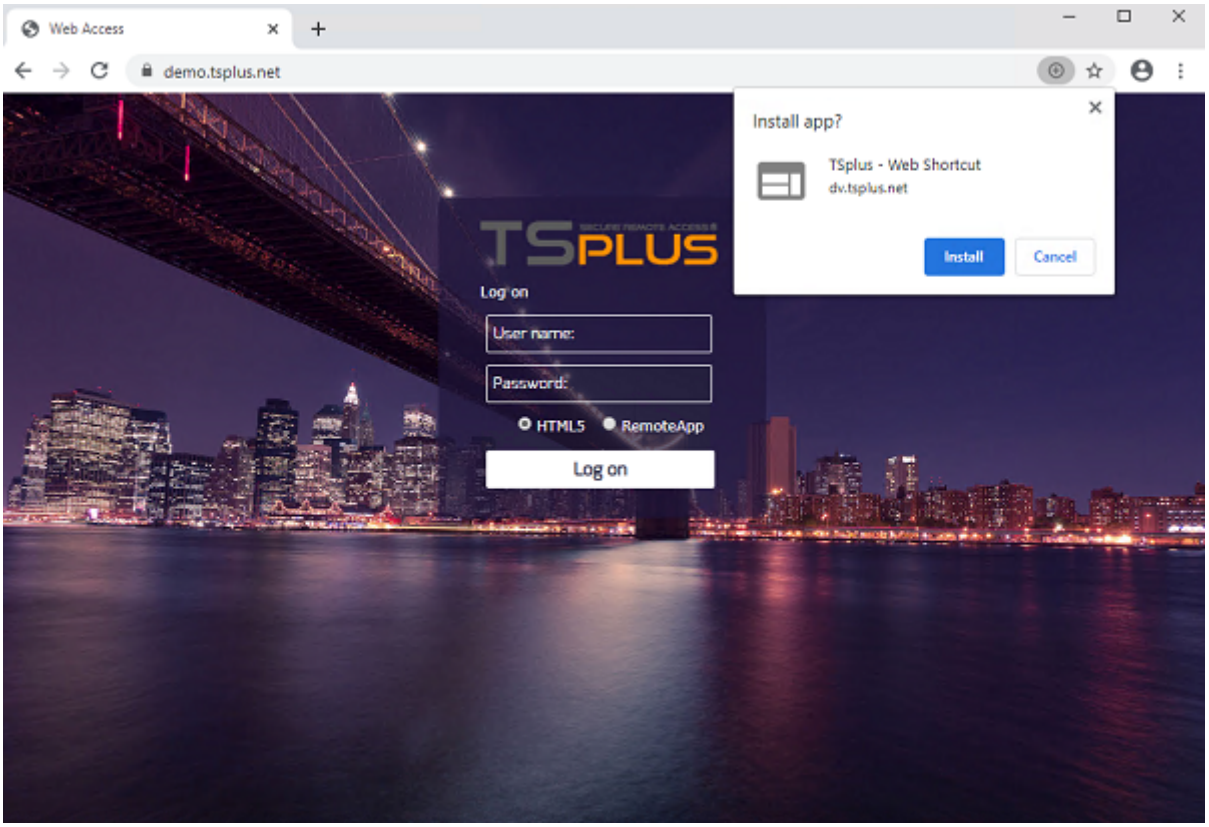
Die neue TSplus WebApp bietet verbesserte Leistung und Wert durch die folgenden Verbesserungen gegenüber älteren Anwendungen und Verbindungsclients:

- Schnellere Ladezeiten aufgrund des geringen Software-Fußabdrucks.
- Geringerer Datenverbrauch - TSplus Web App nutzt gängige browserbasierte Verkehrsverwaltung, um den Datenverbrauch zu minimieren.
- Nahtlose Benutzererfahrung - vom Anmeldebildschirm bis zur Anwendungsdarstellung bietet die TSplus WebApp dem Benutzer das Erscheinungsbild der Verwendung nativer Anwendungen.
- Keine weiteren Browser-Tabs oder verlorene Sitzungen aufgrund zu vieler geöffneter Browserfenster. Das Verhalten der TSplus Web App bietet die gleichen Multitasking-Optionen wie jede andere Anwendung auf höchster Ebene.

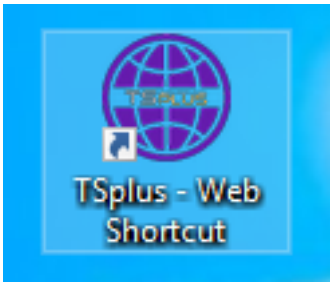
Installation - PC

Navigieren Sie zu Ihrem Unternehmens-TSplus-Webportal mit Ihrem bevorzugten gängigen Webbrowser (HTTPS-Konfiguration erforderlich).
Für die Verwendung in Firefox müssen Sie die installieren PWAS Add-On.

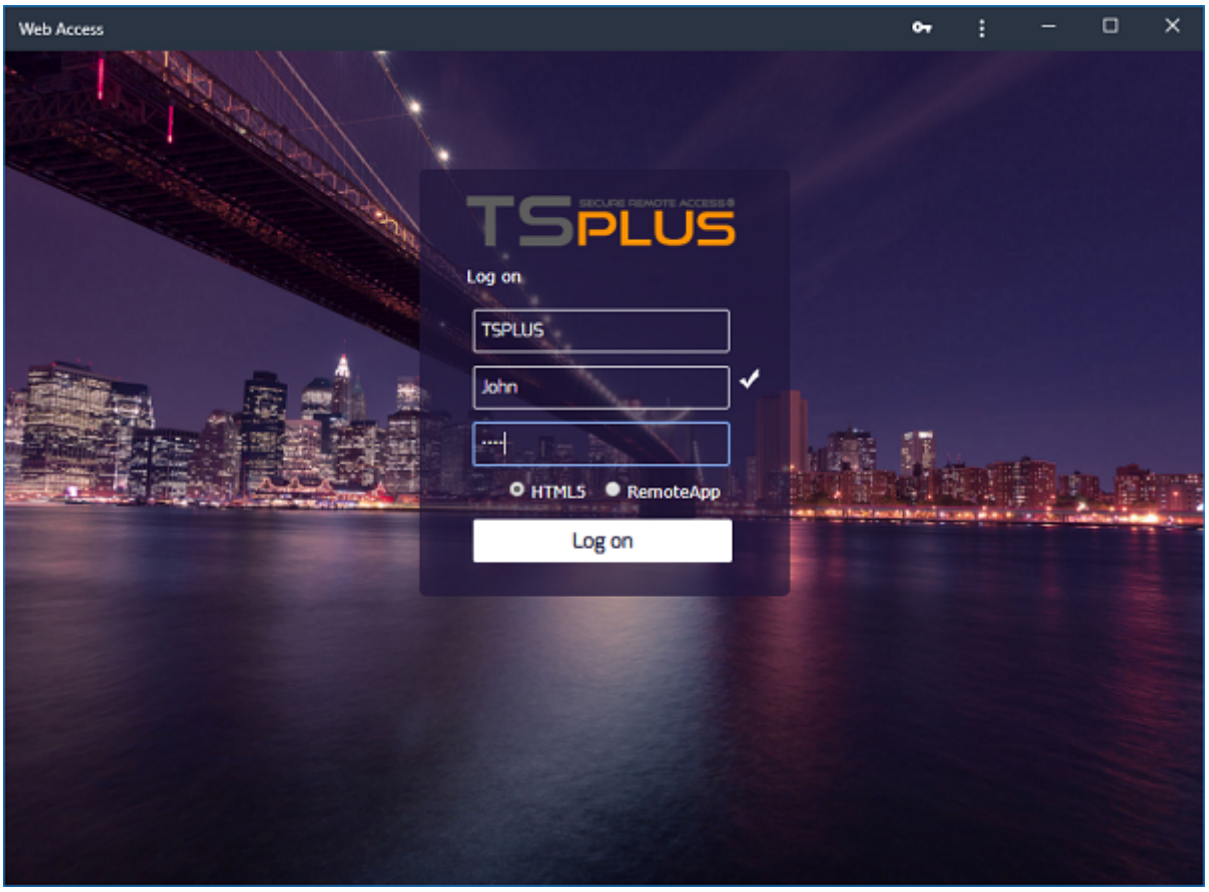
Klicken Sie auf die Schaltfläche +, die sich auf der rechten Seite der Navigationsleiste befindet. Wenn Sie dazu aufgefordert werden, klicken Sie auf 'Installieren'.



Die Installation dauert nur eine Sekunde. Es wird ein Symbol auf Ihrem Desktop erstellt:



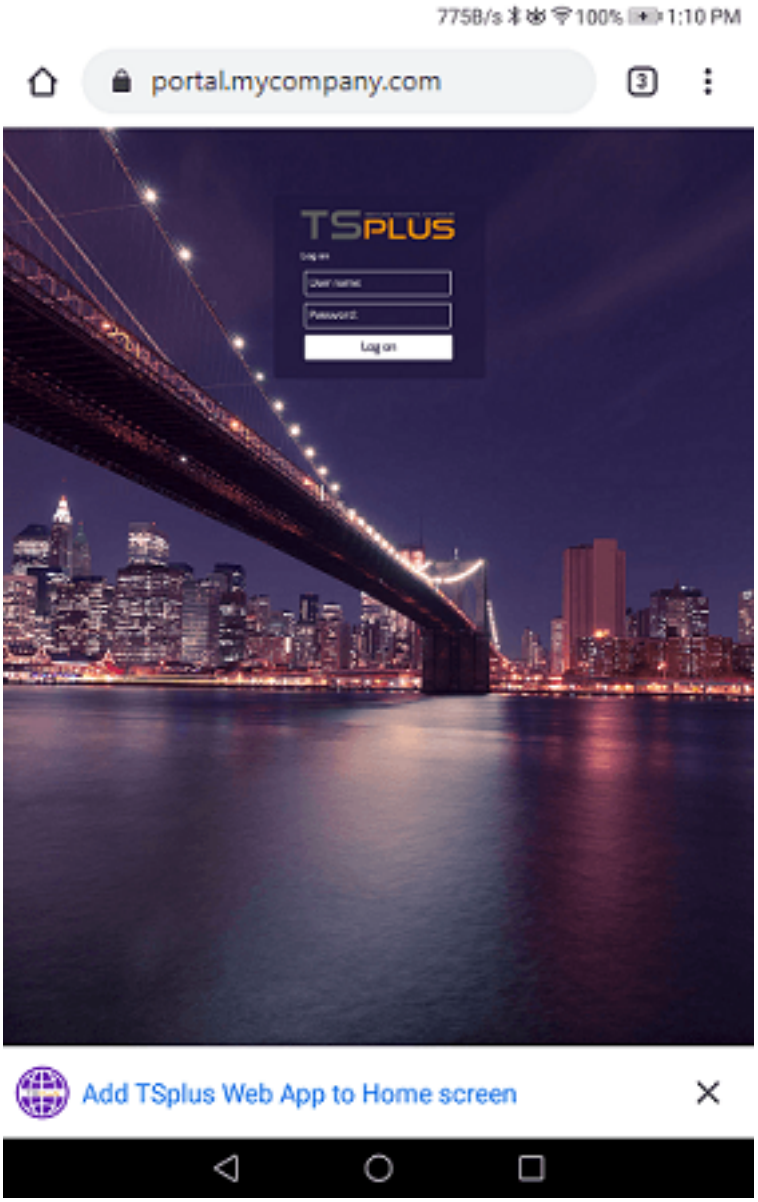
Und die Webanwendung wird sofort nach Abschluss geöffnet:



Installation - Android Mobile Device

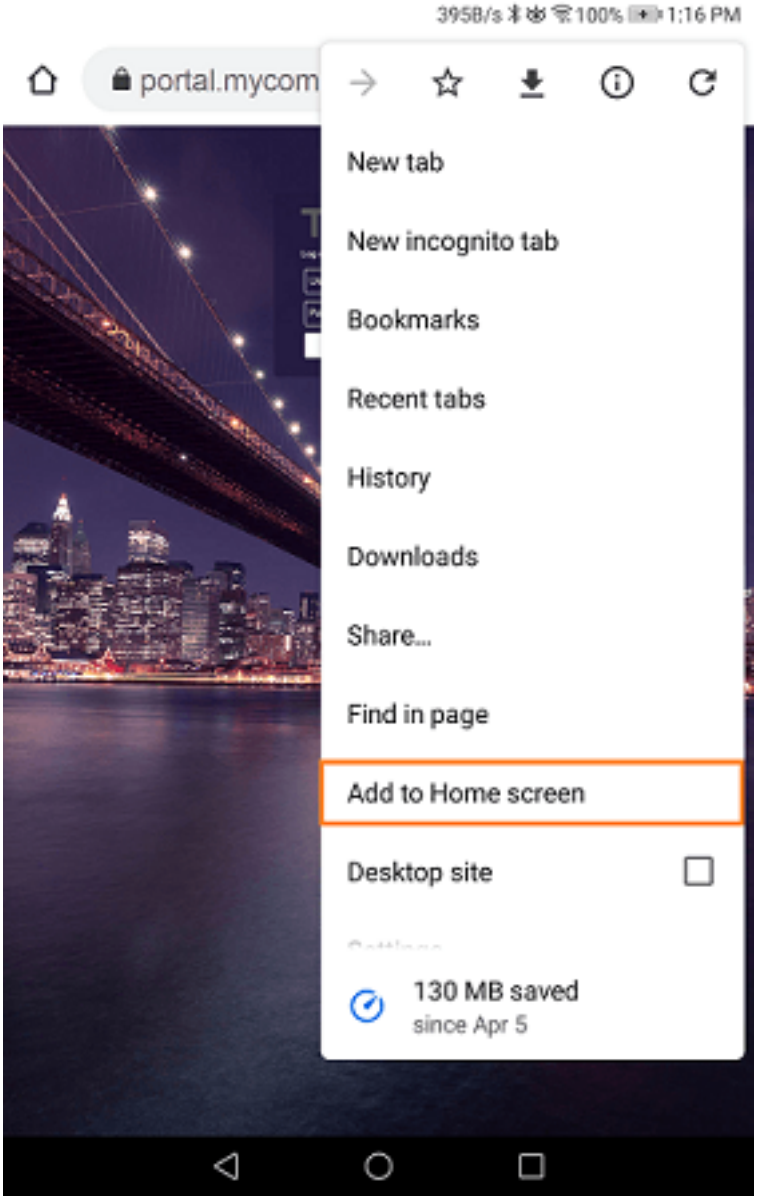
Navigieren Sie zu Ihrem Unternehmens-TSplus-Webportal mit Ihrem bevorzugten gängigen mobilen Webbrowser. **HTTPS-Protokoll ist auf dem TSplus-Server erforderlich.**

Das Webportal bietet die Möglichkeit, die TSplus Web-App zu Ihrem Startbildschirm hinzuzufügen, indem Sie auf die Nachricht „TSplus Web-App zum Startbildschirm hinzufügen“ am unteren Rand des Fensters klicken.

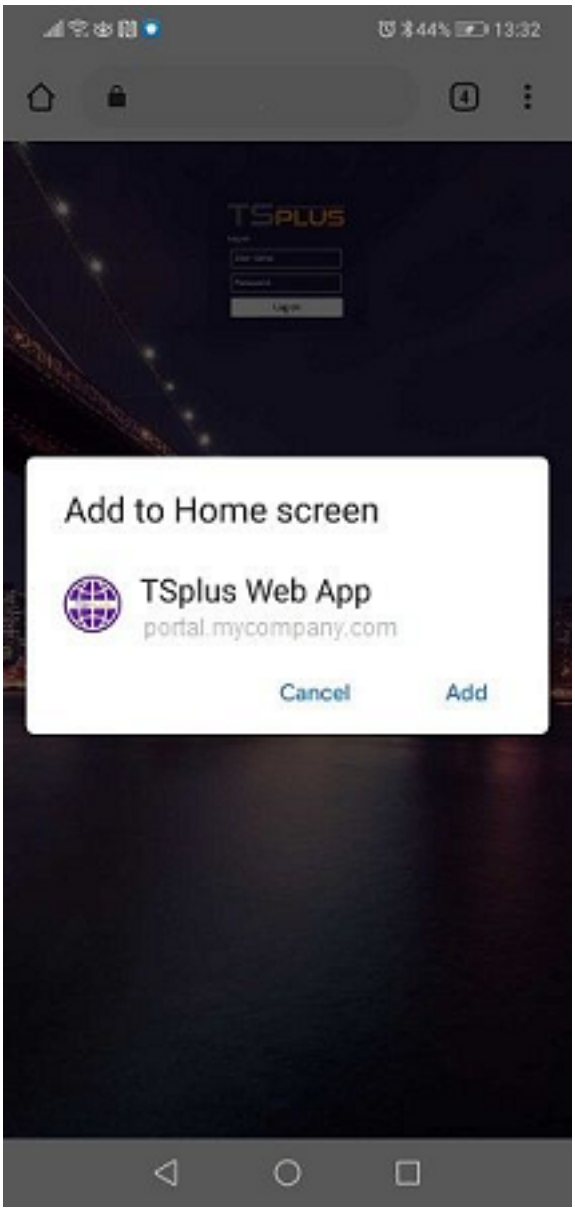


Oder indem Sie auf das Menü mit den 3 Punkten oben rechts im Fenster klicken und auf „Hinzufügen“ klicken.

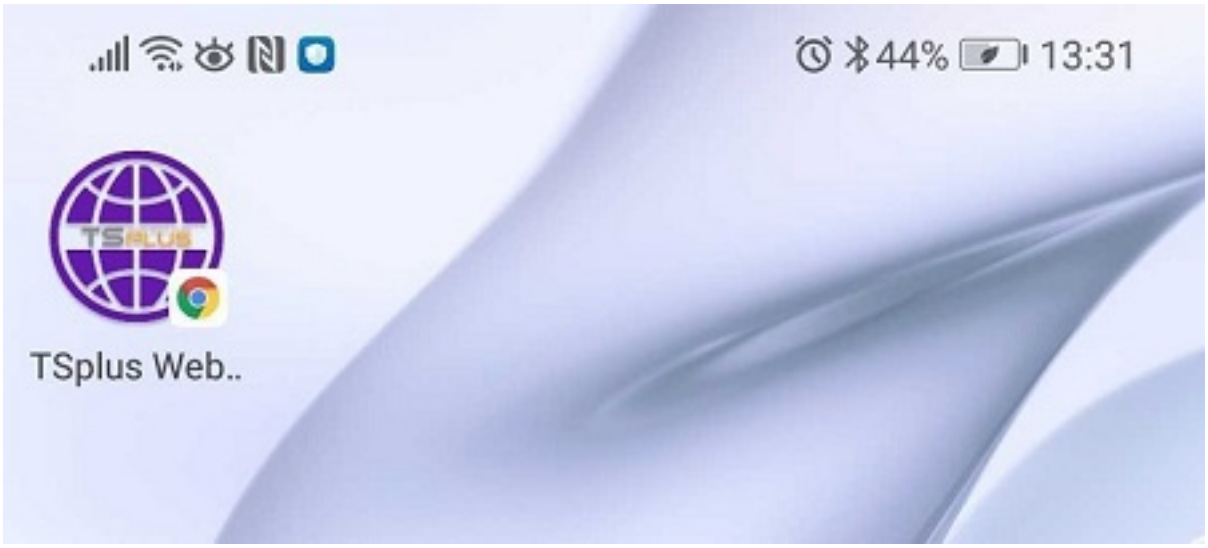
Nachdem der Benutzer die Option "Zum Startbildschirm hinzufügen" akzeptiert hat, wird er den folgenden Bildschirm sehen:



Tippen Sie auf die Schaltfläche „Hinzufügen“ und der Vorgang ist abgeschlossen:



Die TSplus Web-App ist jetzt direkt vom Startbildschirm Ihres mobilen Geräts aus zugänglich.



Installation - Apple iOS Mobilgeräte

Der Installationsprozess der Web-App auf iOS ähnelt dem Android-Prozess. Navigieren Sie einfach zum TSplus Web Portal mit dem Safari-Webbrowser. Klicken Sie auf die Schaltfläche "Teilen":

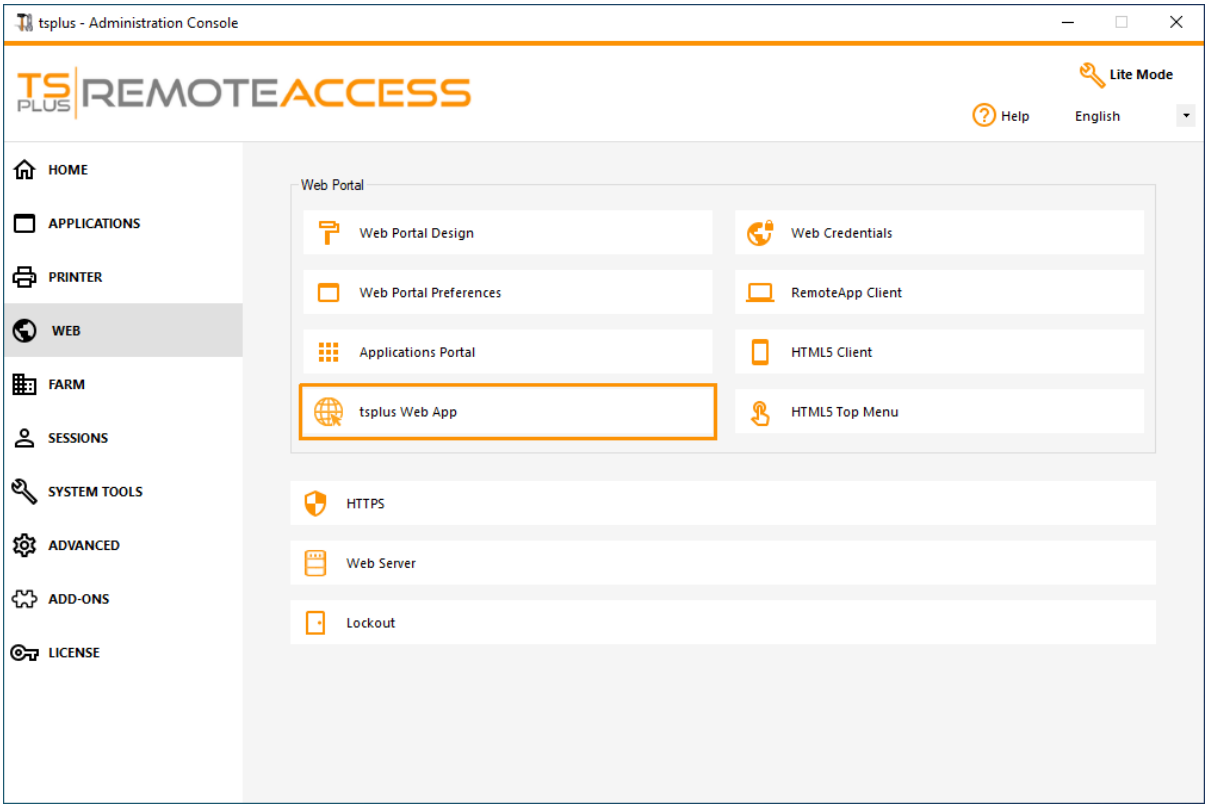


Dann klicken Sie auf „Zum Startbildschirm hinzufügen“.

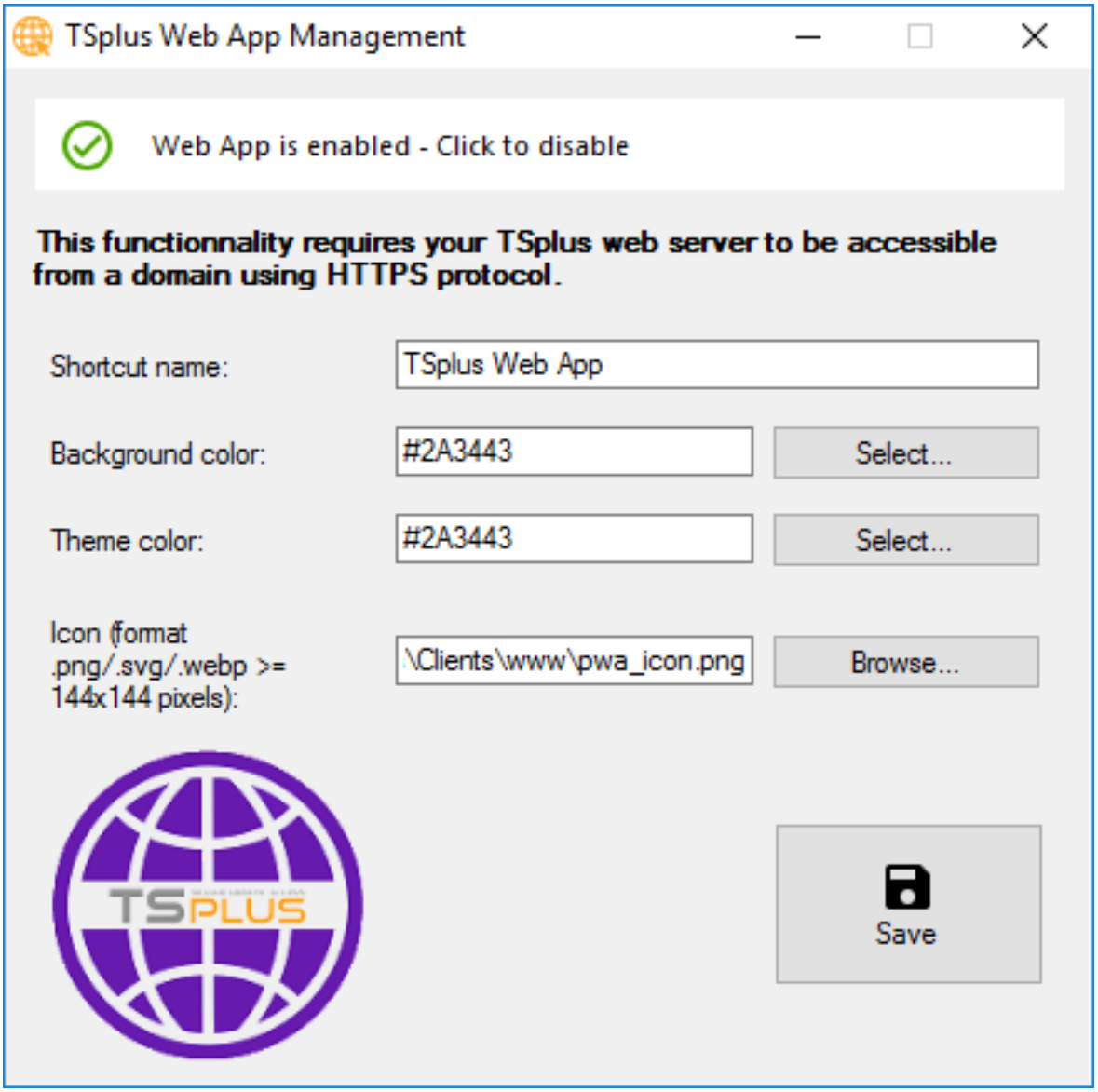
Hinweis: Der Chrome-Browser unterstützt die Web-App-Funktion auf iOS nicht.

Management

Sie können die Webanwendung verwalten, indem Sie zum TSplus Admin Tool Web - Web Portal-Bereich gehen und auf das TSplus Web App-Kachel klicken:



Die Webanwendung ist standardmäßig aktiviert, kann jedoch deaktiviert werden. Es ist möglich, den Namen der Verknüpfung, den Hintergrund und die Farbthemen sowie das Symbol der TSplus Webanwendung zu ändern.



Klicken Sie einfach auf „Speichern“, um Ihre Änderungen zu speichern.

Webanwendungen-Portal: Parameter in der URL-Adresse

Wenn Sie die Standard-Login-Webzugangsseite von Terminal Service Plus beim Verwenden des umgehen möchten, Webanwendungen-Portal und direkt zur Seite des Webanwendungsportals gehen, müssen Sie mehrere Parameter in der URL-Adresse angeben:

- Benutzeranmeldung
- Benutzerpasswort
- Benutzerdomain
- Server
- Hafen
- Client-Typ (HTML5 oder Windows)

Hier ist ein Beispiel für eine vollständige URL-Adresse für den Benutzer „demo“ mit dem Passwort „demo“ auf unserem Demokserver mit einem HTML5-Client:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo&domain=&server=127.0.0.1&port=3389&type=html5

Die Parameter für Domain, Server, Port und Typ sind optional, die folgende URL-Adresse hat genau das gleiche Verhalten:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo

Um einen Windows-Client zu verwenden, verwenden Sie:

&type=remoteaccess

Mit diesen Parametern in der URL-Adresse können Sie direkt zur Seite des Webanwendungsportals gehen.

Sie müssen nicht alle diese Parameter gleichzeitig angeben: Die nicht angegebenen Parameter haben ihren standardmäßig konfigurierten Wert.

Wenn Sie die Standardanmeldung von Terminal Service Plus beim Verwenden des HTML5-Clients umgehen möchten, überprüfen Sie diese Seite .

Webanwendungen-Portal

Terminal Service Plus Web Application Portal bietet eine einzige, flexible Lösung, die die Bereitstellung von Anwendungen und Desktops sowie das Lebenszyklusmanagement optimieren kann, um die IT-Kosten zu senken. Durch die zentrale Verwaltung und webbasierte Bereitstellung von On-Demand-Anwendungen kann die IT die Erfolgsquote der Anwendungsbereitstellung verbessern, indem sie rollenbasierte Verwaltung, Anwendungssteuerung, Sicherheit und Benutzersupport bereitstellt.

Terminal Service Plus Web Application Portal virtualisiert und transformiert Windows-Apps und Desktops in einen sicheren On-Demand-Service.

Mit dem Webanwendungsportal können Sie Microsoft Windows-Anwendungen (Geschäftsanwendungen, Office-Anwendungen…) im Internet veröffentlichen.

Wie bei Citrix können Ihre Benutzer direkt über das Internet auf ihre Anwendungen zugreifen, indem sie einfach auf das Anwendungssymbol auf der Portal-Webseite klicken, direkt in ihrem eigenen Internetbrowser.

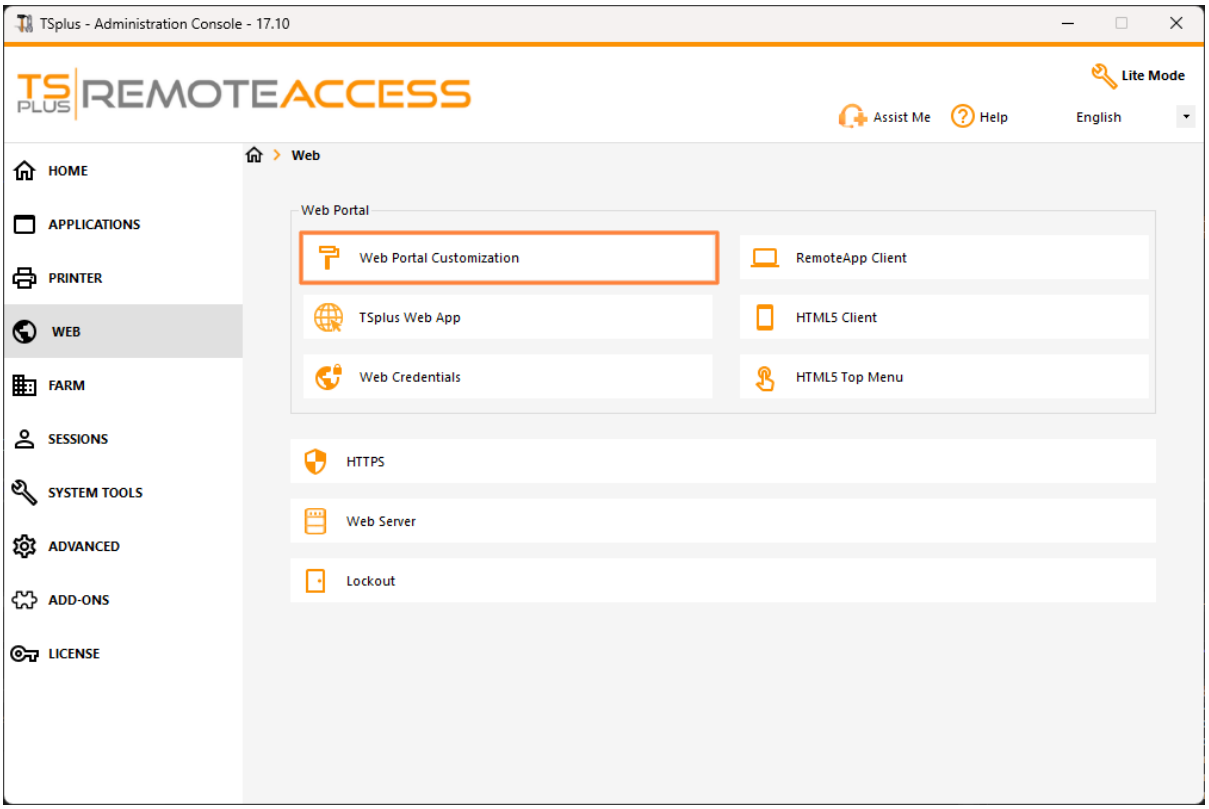
Verwalten Ihrer Webanwendungen

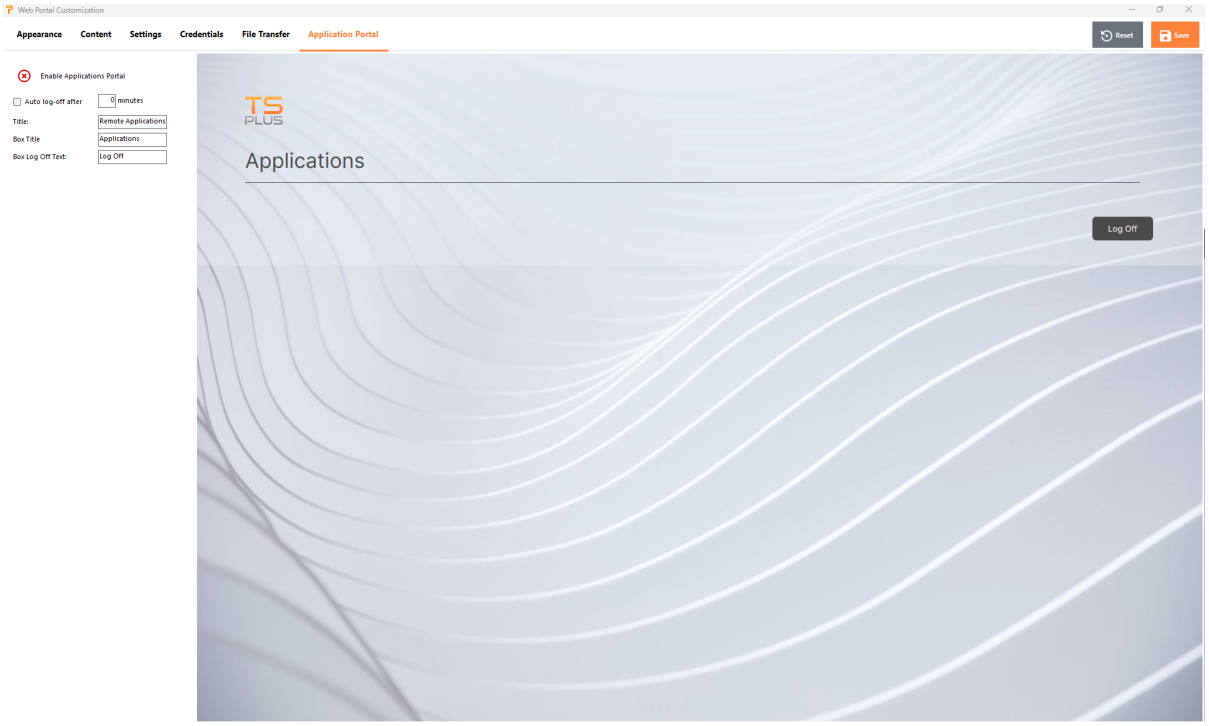
Die Funktion des Webanwendungsportals ist **vollständig integriert** in Terminal Service Plus. Es bedeutet, dass alle Anwendungen, die durch die Funktion zur Veröffentlichung von Anwendungen von Terminal Service Plus veröffentlicht werden, im Webanwendungsportal verwendet werden können.

Wenn Sie mehr über diesen Veröffentlichungsprozess erfahren möchten, können Sie gerne unsere Dokumentation über lesen. Anwendungsbereitstellung und Anwendungen Benutzern oder Gruppen zuweisen .

Gestaltung Ihres Webanwendungsportals

Im Admin-Tool öffnen Sie die Registerkarte „Web“ und klicken Sie auf das Kachel „Webportal-Anpassung“ und gehen Sie zur Kachel „Anwendungsportal“.





Um eine Webzugriffsseite mit der aktivierten Funktion Webanwendungsportal zu erstellen, **Aktivieren Sie das Kontrollkästchen „Anwendungsportal aktivieren“.** Sie können Ihre Webzugriffsseite nach Ihren Wünschen anpassen und dann auf „Speichern“ klicken, um diese neue Webzugriffsseite zu veröffentlichen.

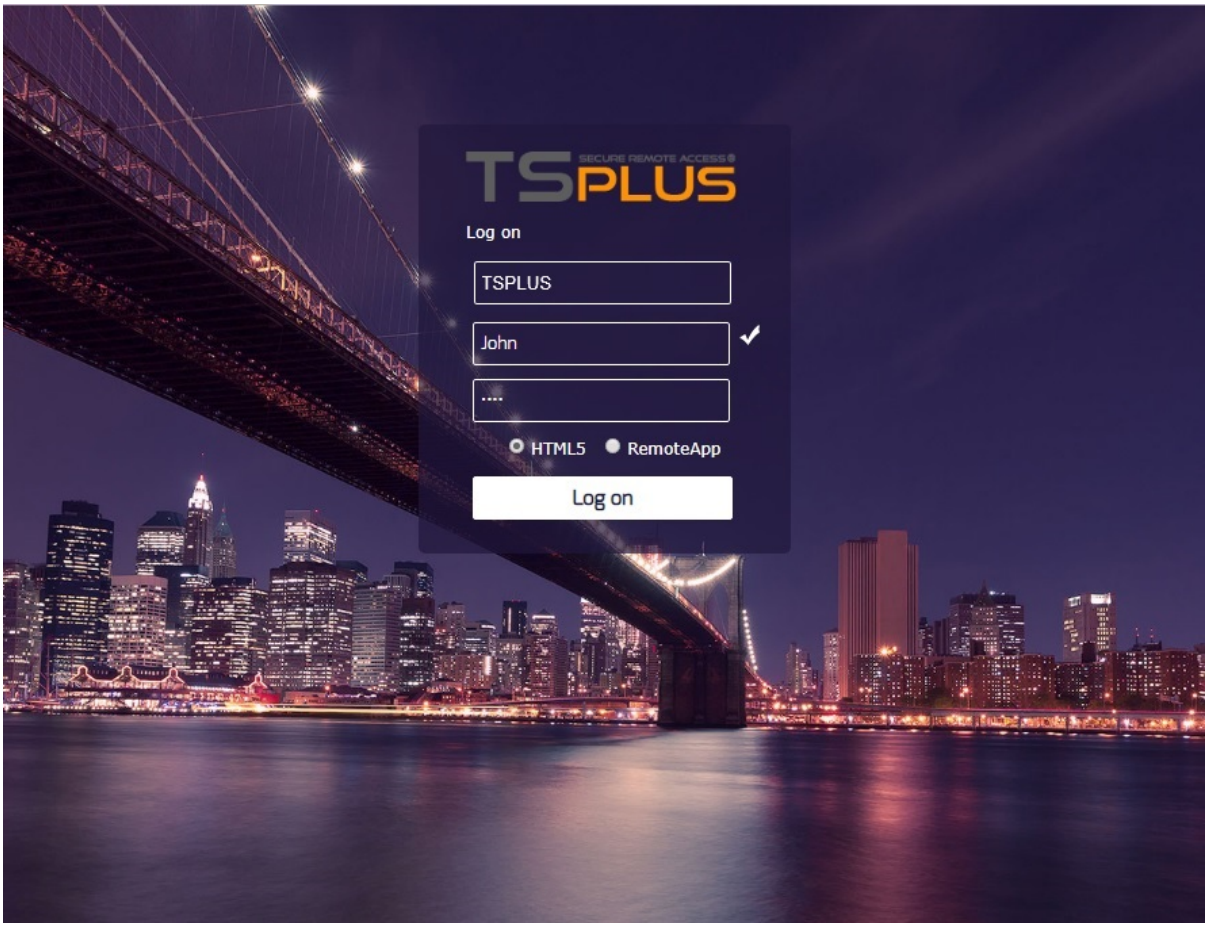
Hinweis: Sie können die Farben des Feldes und des Feldrandes nur für die klassischen Themen ändern, die auf dem Erscheinungsbild-Registerkarte .

Verwendung des Webanwendungsportals

In diesem Beispiel haben wir die neue Webzugriffsseite mit dem Standardnamen „index“ veröffentlicht.

Um darauf zuzugreifen, öffnen Sie einen Webbrowser und gehen Sie zu http:// your_server_name/ (in diesem Beispiel verwenden wir http://localhost , direkt vom Server selbst).

Die erste angezeigte Webseite ist die Standard-Logon-Seite von Terminal Service Plus:

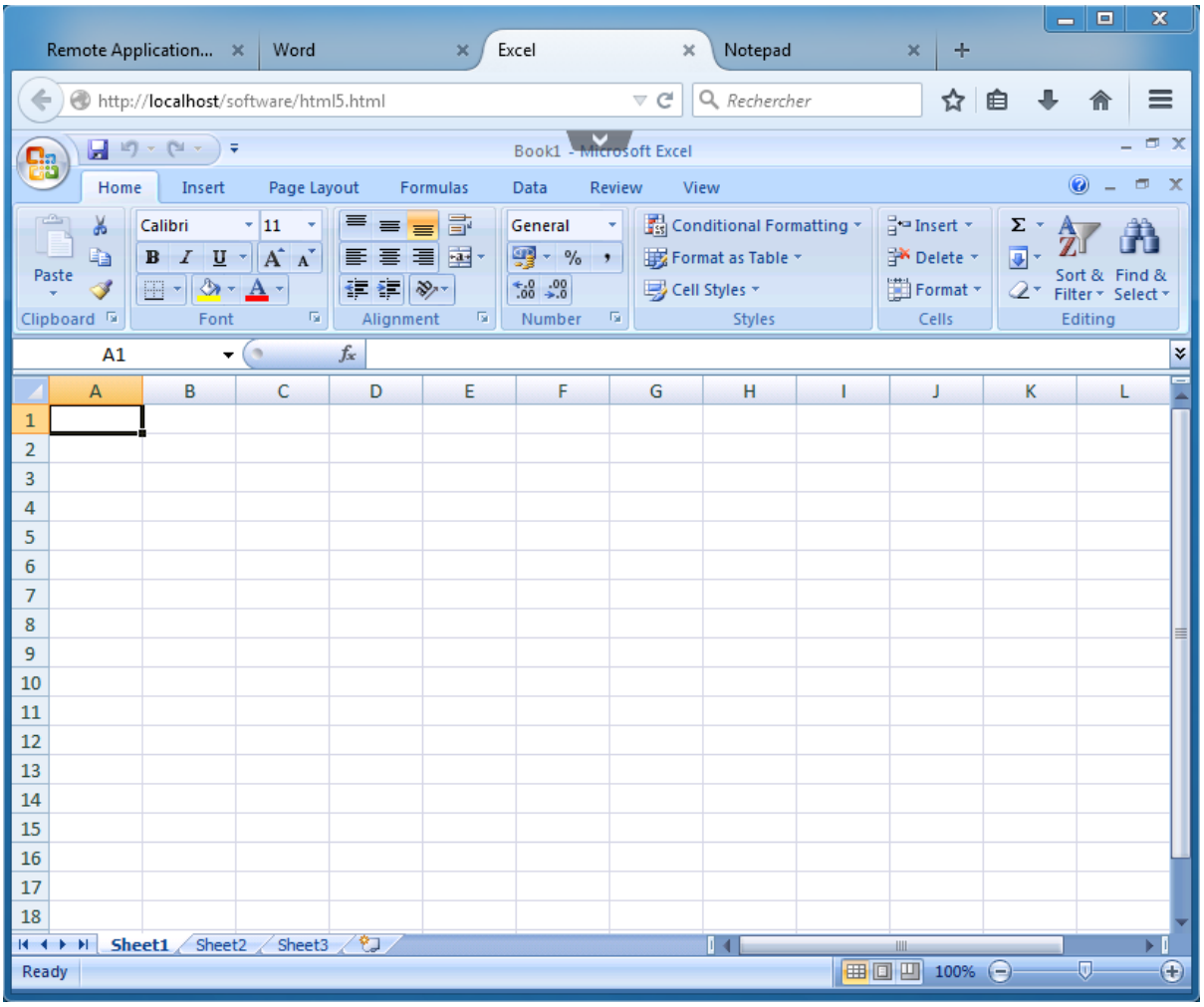


Sobald Sie sich angemeldet haben, wird eine neue Webseite angezeigt, dies ist das Webanwendungsportal:

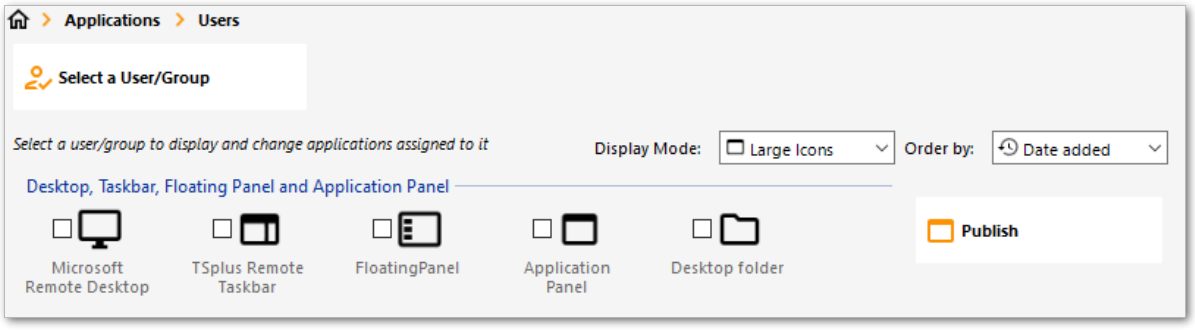


Wie Sie sehen können, erhält der Benutzer ein Symbol für jede veröffentlichte Anwendung, auf die er Zugriff hat.

Der Benutzer kann jetzt auf ein oder mehrere Symbole klicken, um die entsprechende Anwendung in einem neuen Tab remote zu öffnen.

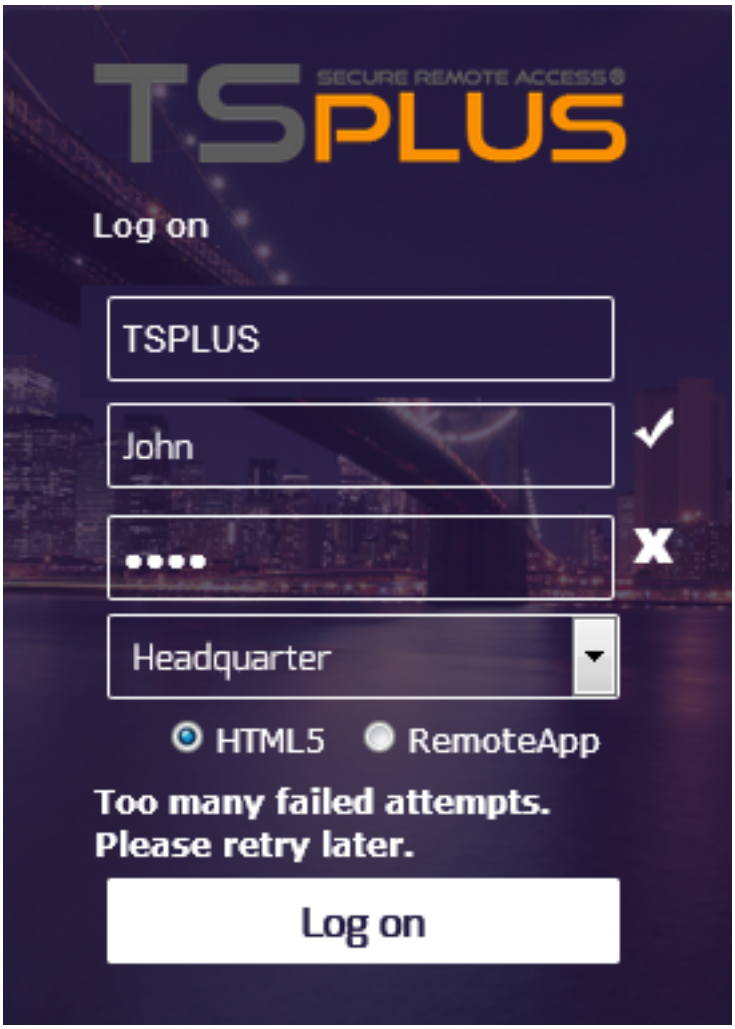


Wenn Sie nur das Anwendungsportal verwenden möchten, ohne eine Windows-Sitzung, die Remote-Taskleiste, das Floatingpanel,… zu öffnen, müssen Sie alle Kästchen, die mit dem Benutzerprofil verbunden sind, deaktivieren.



Seit der Veröffentlichung von TSplus 11.40 werden Brute-Force-Angriffe auf das Webportal jetzt blockiert, wenn Benutzer falsche Anmeldeinformationen eingeben.

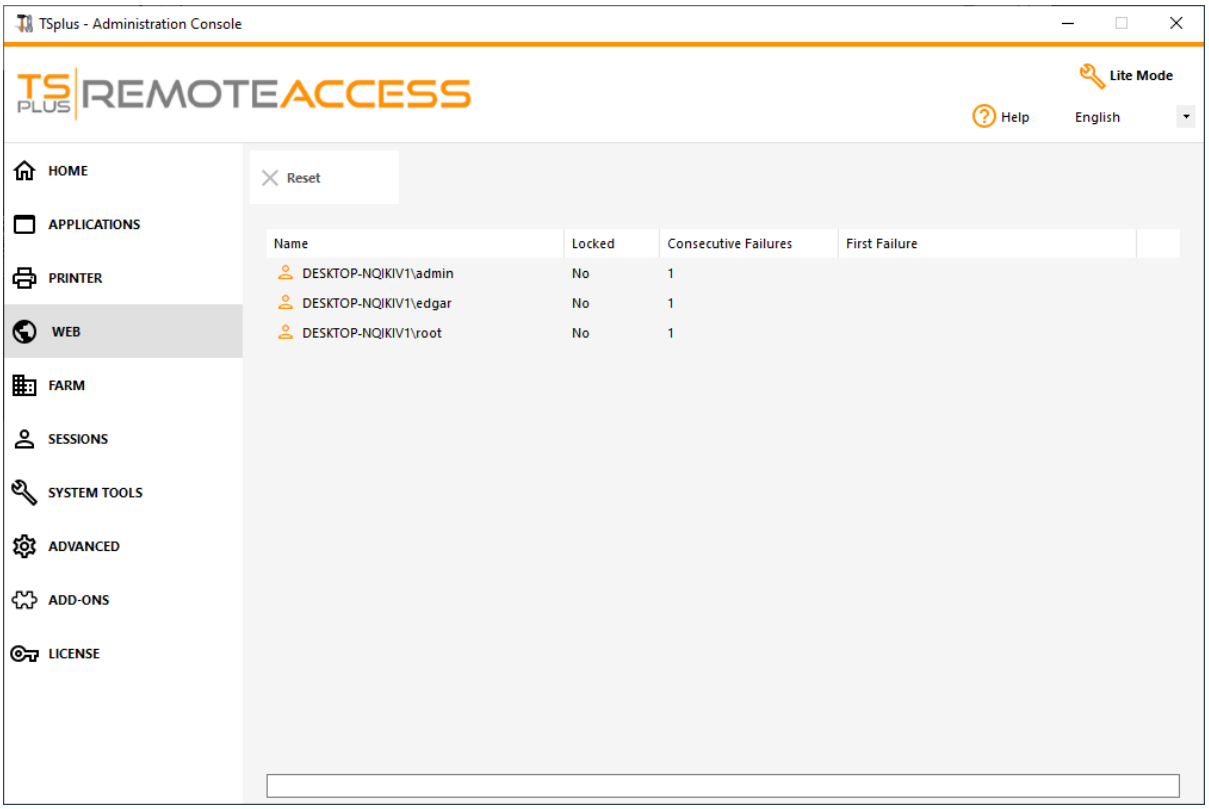
Nach 10 Versuchen innerhalb von 15 Minuten wird das Webportal dem Benutzer den Zugriff für 30 Minuten verweigern (anpassbar auf die Erweiterte - Sperrseite des AdminTools) :



Diese sind die Standard Einstellungen, die im hb.exe.config Datei, die sich im TSplus Ordner befindet, anpassbar sind:

TSplus\Clients\www\cgi-bin\hb.exe.config im Abschnitt „appSettings“.

Sie können alle blockierten Verbindungen und Protokolle von Benutzern über die Sperrfunktion von TSplus überprüfen:



Diese Funktionalität ist sichtbar und aktiv nach der ersten Verbindung zum Webportal.

Wichtige Hinweise

- Die Funktion des Webanwendungsportals ist kompatibel mit Farm / Gateway-Konfiguration und es unterstützt auch Lastverteilung .
- In einer Farm-/Gateway-Konfiguration müssen die Anwendungen zum Zeitpunkt der Veröffentlichung auf jedem Server der Farm zugewiesen werden.
- In Bezug auf die Lizenzierung von Terminal Service Plus kann ein Benutzer mehrere Anwendungen gleichzeitig öffnen, ohne dass dies mehr als 1 Benutzer zählt.

Web-Autologon: Verbindung über das Web ohne Portal

Übersicht

Terminal Service Plus Web Portal ermöglicht es Benutzern, sich von jedem Webbrowser aus einfach mit ihren Windows-Anmeldeinformationen mit ihren Remote-Servern zu verbinden.

Manchmal möchten Sie jedoch automatisch eine Verbindung herstellen, wenn Sie eine bestimmte URL-Adresse aufrufen. Diese Funktion wird Web-Autologon genannt.

Mit Web-Authentifizierung verbinden Sie sich mit den in spezifischen Terminal Service Plus-Dateien angegebenen Einstellungen (Anmeldung, Passwort, Ports, …).

Vorsicht

Wenn Sie diese Funktion verwenden, können Ihr Benutzername und Ihr Passwort für jeden sichtbar sein, der die Seite besucht.

Zusätzlich, wenn alle Ihre Benutzer denselben Benutzernamen teilen, kann es möglich sein, dass Benutzer sensible Informationen von anderen Benutzern sehen, die denselben Benutzernamen teilen.

Diese Funktion ist nur für spezifische Anwendungsfälle gedacht und wird nicht empfohlen.

Web-Authentifizierung mit HTML5-Client

Sie können sich direkt verbinden, indem Sie zu navigieren. http://your-server/software/html5.html

Sie können die Verbindungseinstellungen ändern, indem Sie die folgende Datei mit Notepad oder einem beliebigen Texteditor (wie Notepad++ - verwenden Sie nicht MS Word) bearbeiten:

C:\Program Files (x86)\TSplus\Clients\www\software\html5\settings.js

Sie müssen mindestens einen Benutzernamen und ein Passwort angeben, um von der Web-Autologon-Funktion zu profitieren.

Sie müssen möglicherweise die Seite in Ihrem Webbrowser aktualisieren, nachdem Sie diese Datei geändert haben.

Web-Authentifizierung mit dem RemoteApp-Webclient

Sie können sich direkt verbinden, indem Sie zu navigieren. http://your-server/software/remoteapp2.html

Sie können die Verbindungseinstellungen ändern, indem Sie die folgende Datei mit Notepad oder einem beliebigen Texteditor (wie Notepad++ - verwenden Sie nicht MS Word) bearbeiten:

C:\Program Files (x86)\TSplus\Clients\www\software\remoteapp2.js

Sie müssen mindestens einen Benutzernamen und ein Passwort angeben, um von der Web-Autologon-Funktion zu profitieren.

Sie müssen möglicherweise die Seite in Ihrem Webbrowser aktualisieren, nachdem Sie diese Datei geändert haben.

Aktivieren Sie mehrere Benutzersitzungen mit denselben Anmeldeinformationen.

Wenn Sie mehrere Benutzersitzungen mit denselben Anmeldeinformationen aktivieren möchten, können Sie dieses Verfahren befolgen.

Sie können die Datei index.html kopieren, die sich befindet in:

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

so oft wie Ihre Anzahl an Benutzern. Sie können es umbenennen und dann über die URL darauf zugreifen: http://nameofyourserver.com/renamedindex.html

Bearbeiten Sie den Abschnitt, der den Benutzerdaten entspricht:

Zugriffskonfiguration ---------- var user = ""; // Anmeldename, der beim Verbinden mit dem Remote-Server verwendet werden soll ("" lassen, um den auf dieser Seite eingegebenen Anmeldenamen zu verwenden) var pass = ""; // Passwort, das beim Verbinden mit dem Remote-Server verwendet werden soll ("" lassen, um das auf dieser Seite eingegebene Passwort zu verwenden) var domain = "";

Sie können die index.html-Datei so oft kopieren, wie Sie möchten. Wenn Sie sie mit dem Benutzernamen umbenennen, wird es einfacher für Sie, einen persönlichen Link bereitzustellen.

Web-Anmeldeinformationen

Übersicht

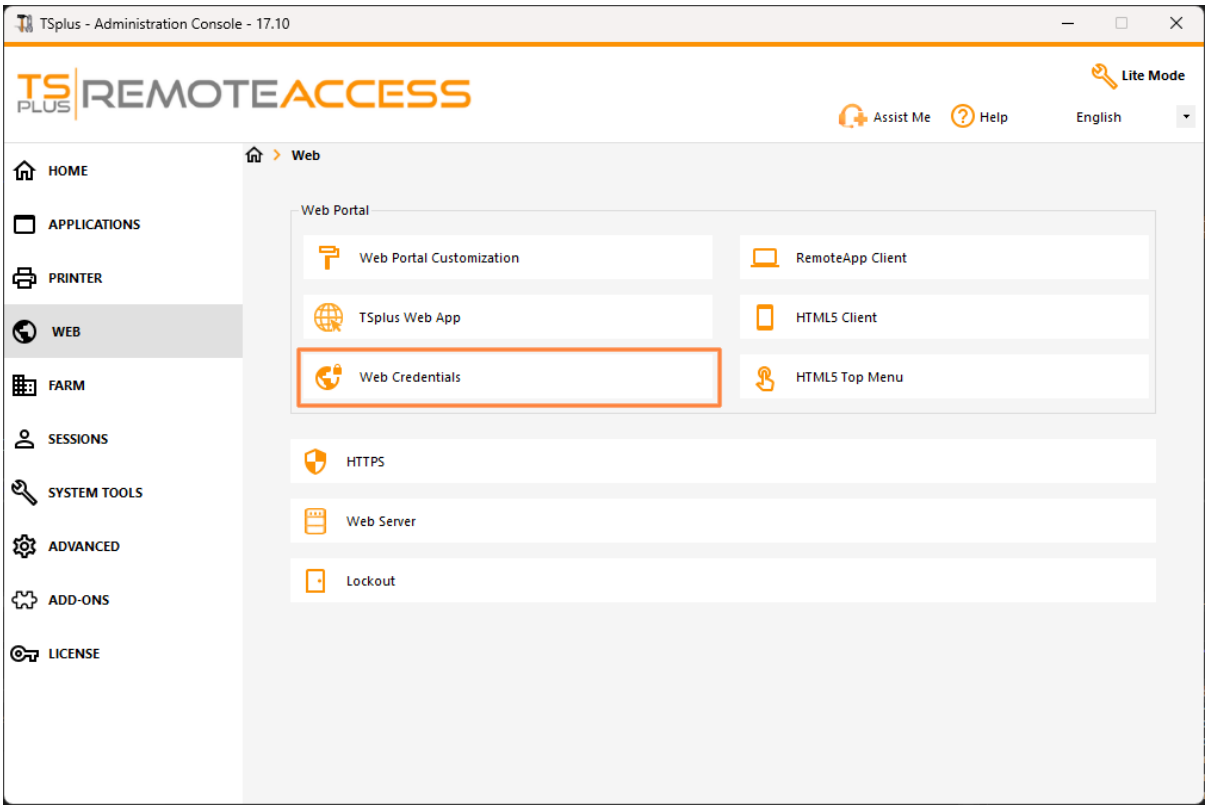
Terminal Service Plus Web Credentials ist ein hochmodernes, einzigartiges Feature, das es Benutzern ermöglicht, sich nur mit einer E-Mail-Adresse oder einer PIN zu verbinden.

Mit Webanmeldeinformationen können Sie den Zugriff auf Ihren Server mit der E-Mail-Adresse eines Benutzers oder mit einem einfachen PIN-Code sichern, der von Ihrer Geschäftsanwendung generiert wird. Einer der großen Vorteile dieser Funktion ist, dass diese Anmeldeinformationen (E-Mail oder PIN-Code) reine Webanmeldeinformationen sind: Der Benutzer wird nicht wissen, welches Windows-Benutzerkonto er gerade verwendet, und er muss kein echtes Windows-Login/Passwort kennen, um sich mit seiner Anwendung zu verbinden!

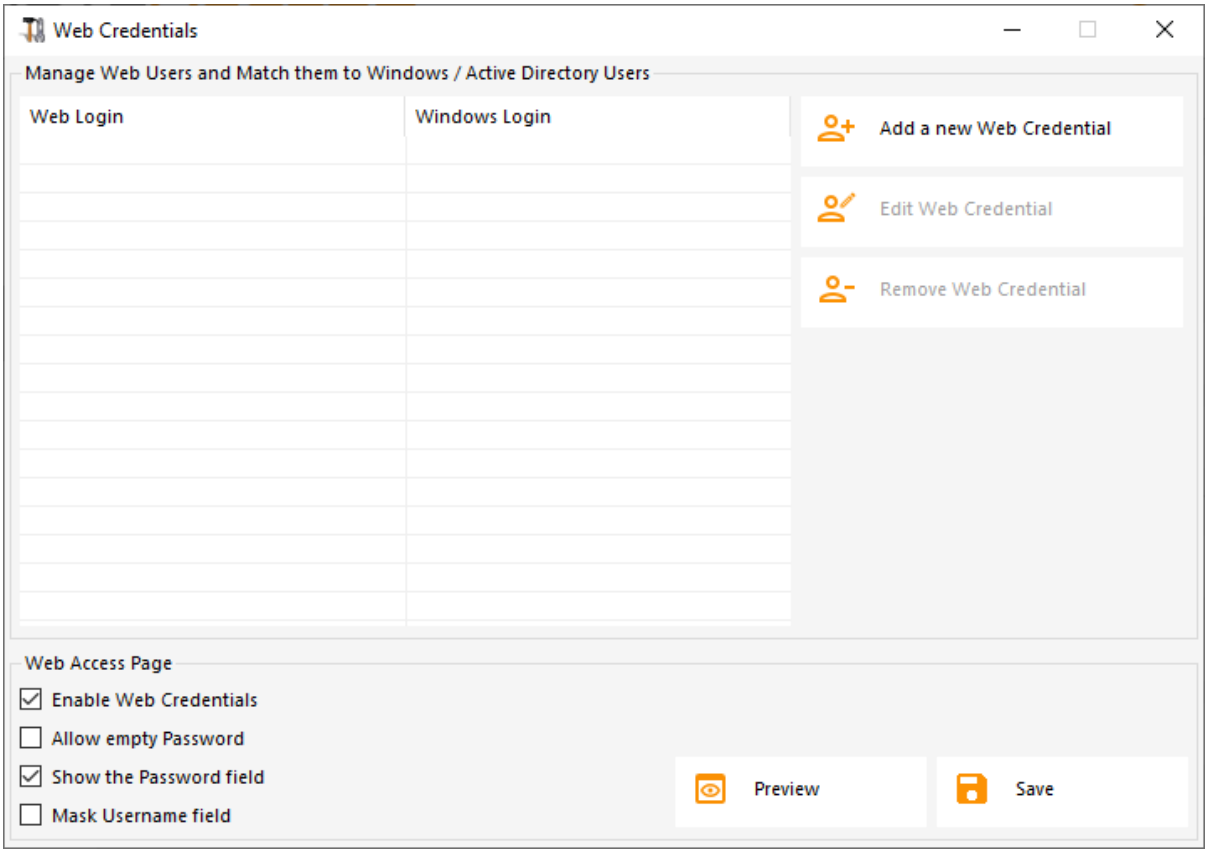
Mit Webanmeldeinformationen können Sie benutzerdefinierte reine Webanmeldeinformationen definieren und diese mit jedem vorhandenen Windows / Active Directory-Benutzerkonto verknüpfen. Der Benutzer kann sich dann mit diesen benutzerdefinierten Anmeldeinformationen verbinden, anstelle der Windows / Active Directory-Anmeldeinformationen.

Verwalten Ihrer Webanmeldeinformationen

Im Admin-Tool den Reiter „Web“ öffnen und auf die Kachel „Web-Anmeldeinformationen“ klicken.

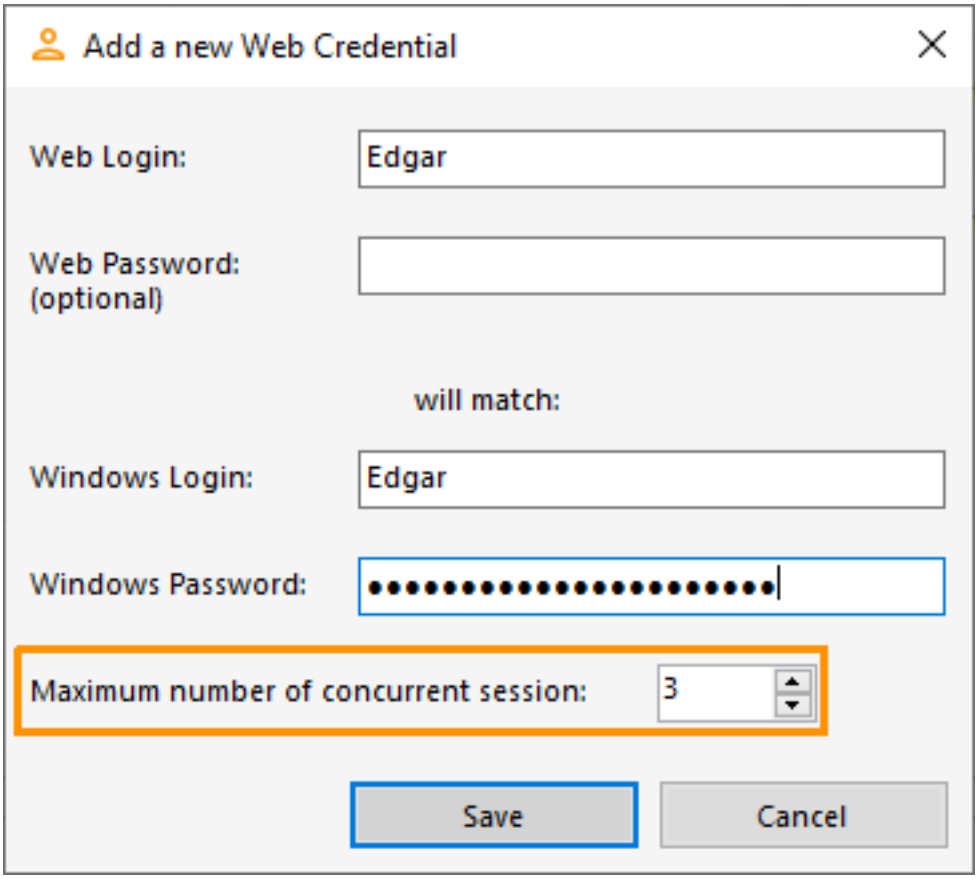


Der Webanmeldeinformationen-Manager wird geöffnet und zeigt dieses Fenster an:



Sie können jetzt ein neues Web-Zugangsdaten erstellen, indem Sie ein benutzerdefiniertes Login und ein (optional) Passwort mit einem vorhandenen Windows / Active Directory-

Benutzerkonto abgleichen, wie unten gezeigt:



Seit der Version 9.50 von TSplus können Sie auch die maximale Anzahl gleichzeitiger Sitzungen für einen Benutzer festlegen.

Sie können auch eine vorhandene Webanmeldeinformation bearbeiten und entfernen, wodurch Sie benutzerdefinierte Anmeldeinformationen ändern oder deaktivieren, die Sie konfiguriert haben.

Alternativ können Sie Webanmeldeinformationen über eine Befehlszeile erstellen:

- Im Windows-Startmenü, im Ausführungsfeld, geben Sie ein: 'cmd.exe' (oder in Programme/ Zubehör > 'Windows Power Shell')
- Dann geben Sie ein, um zum richtigen Ordner zu gelangen: cd “C:\Program Files (x86)\TSplus\UserDesktop\files”, und drücken Sie dann die Eingabetaste, um zu bestätigen.
- Um eine neue Web-Anmeldeinformation hinzuzufügen, geben Sie ein: AdminTool.exe / webcredentials-add your_web_login your_web_password your_windows_login your_windows_password maximum_concurrent_sessions
- Um eine leere Anmeldeinformation hinzuzufügen, geben Sie zwei doppelte Anführungszeichen ein: "" um einen leeren Text anzuzeigen.
- Um eine Webanmeldeinformation zu löschen, geben Sie ein: AdminTool.exe /webcredentials-remove your_web_login

wenn Sie gerne mit Befehlszeilen arbeiten und sich fragen, welche anderen Befehlszeilen

verfügbar sind, besuchen Sie bitte diese spezifische Dokumentation)

Wichtige Hinweise

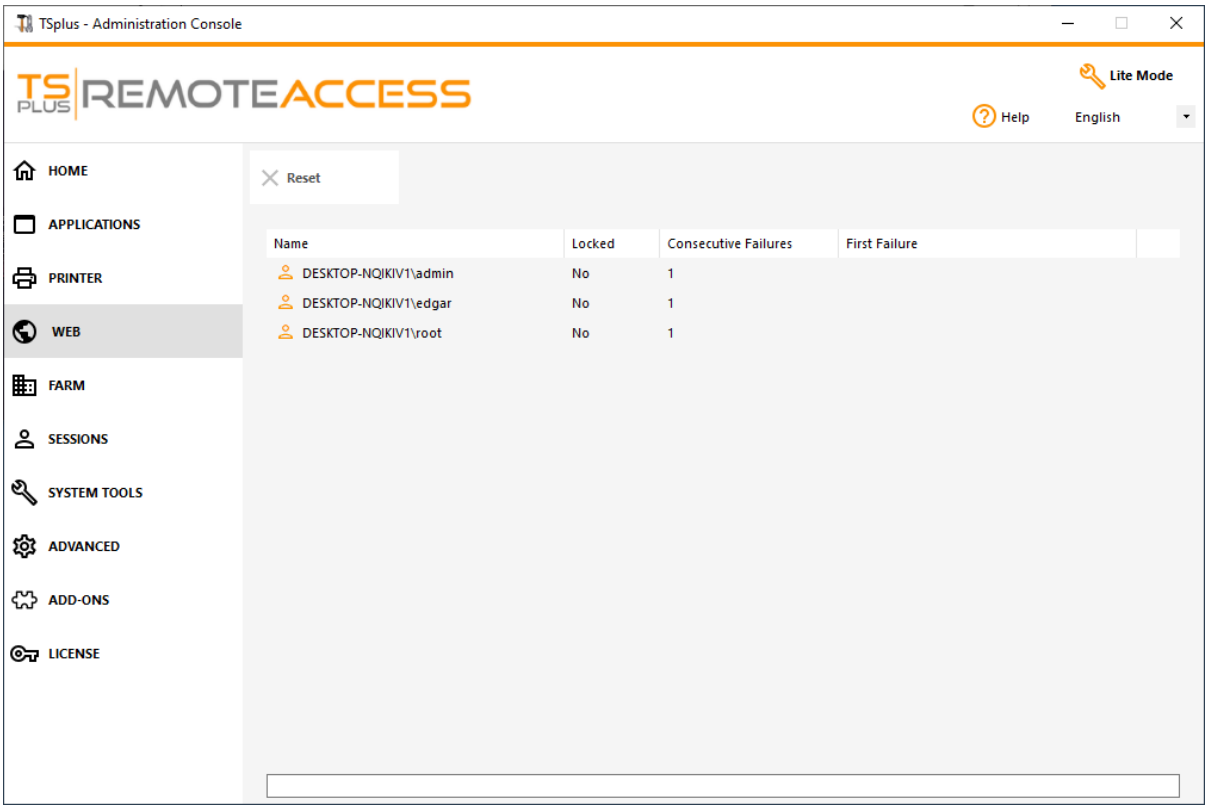
Bitte beachten Sie die folgenden Einschränkungen:

- '[', ']' und '°' Zeichen werden in den Passwortfeldern nicht unterstützt.
- In einem Farm / Gateway-Konfiguration Webanmeldeinformationen unterstützen nur die Lastenausgleichsmodus (es funktioniert nicht im serverzugewiesenen Modus).
- In einer Farm-/Gateway-Konfiguration mit Lastenausgleichsmodus müssen die Web-Anmeldeinformationen zum Zeitpunkt auf jedem Server der Farm definiert werden.
- 2FA ist nicht mit der Webanmeldeinformationen-Funktion kompatibel.

Web-Sperre

TSplus Web-Sperrung, eingeführt mit Version 12.40, ist eine Benutzeroberfläche für die Webportal-Sperrfunktion, um Konten zu entsperren und erweiterte Einstellungen zu bearbeiten:

FAQ: zur Konfiguration der Sperrfunktion des HTML5-Webportals

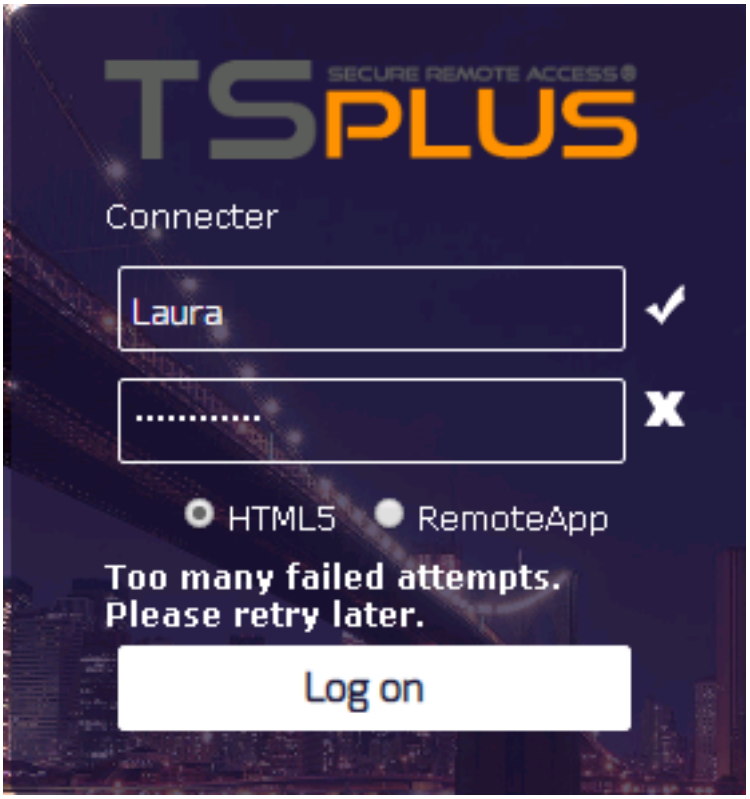


Sperren überwacht fehlgeschlagene Web-Login-Versuche auf Ihrem TSplus-Server. Es protokolliert die Versuche und blockiert automatisch den entsprechenden Benutzer, nachdem die autorisierte Anzahl fehlgeschlagener Versuche erreicht wurde.

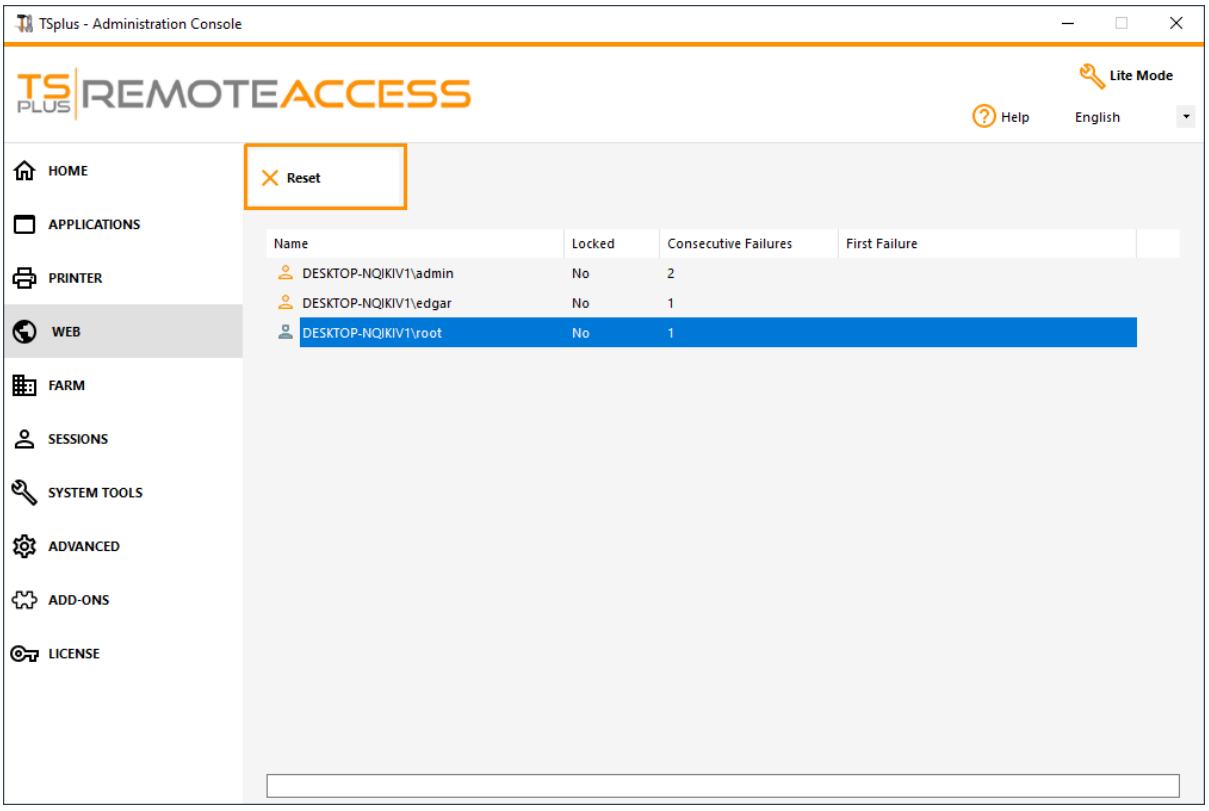
Sie werden leicht erkennen, ob eine Adresse in der Spalte „Gesperrt“ gesperrt wurde.

Die nächste Spalte zeigt die Anzahl der aufeinanderfolgenden Fehler für jeden Benutzer an.

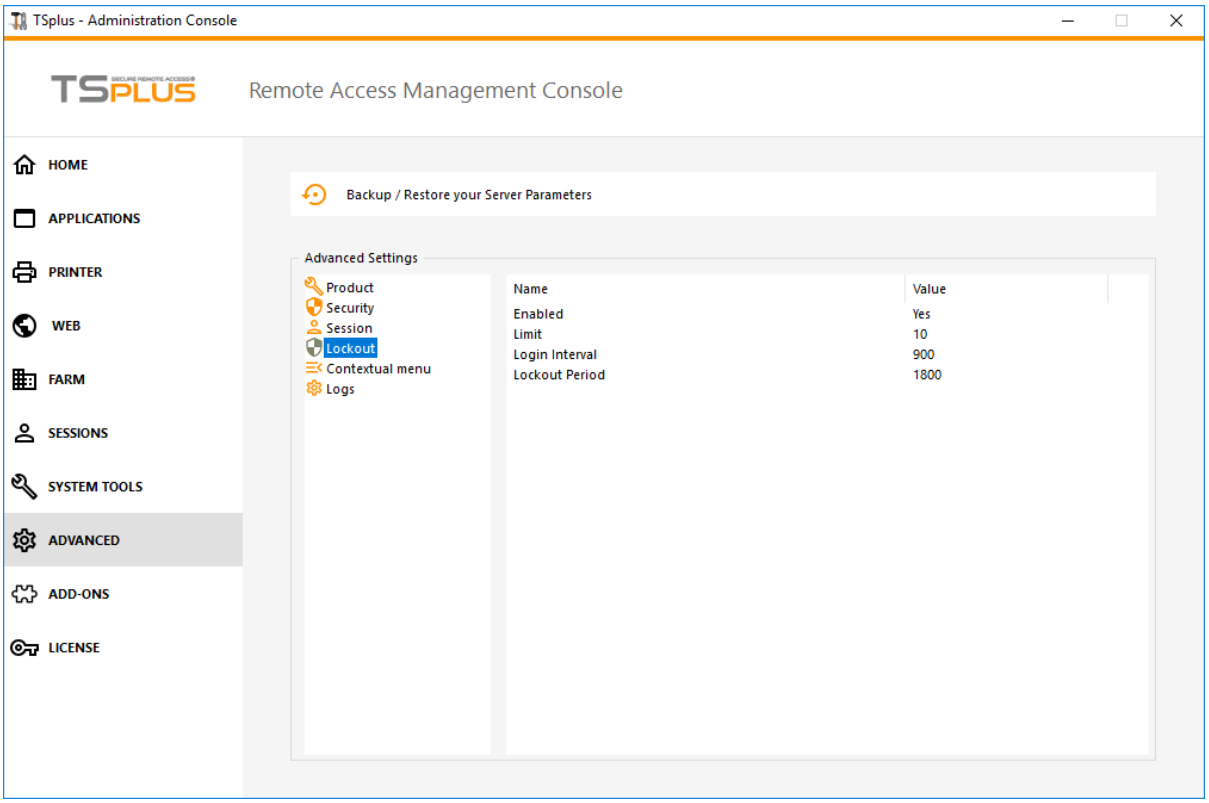
Im Webportal wird dem Benutzer angezeigt, dass zu viele fehlgeschlagene Versuche unternommen wurden:



Benutzer können schnell aus dieser Liste entfernt, entsperrt und aus der benutzerfreundlichen Verwaltungsoberfläche im Web-Tab des AdminTools auf die Whitelist gesetzt werden. Klicken Sie einfach auf den Benutzer, den Sie zurücksetzen oder entsperren möchten, und klicken Sie dann auf „Zurücksetzen“.



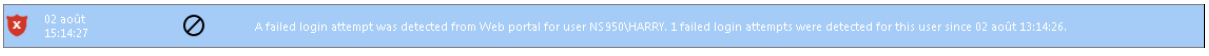
Die Schwelle für die Benutzerblockierung kann vom Administrator im Tab "Erweiterte Einstellungen" des AdminTools konfiguriert werden.



Überprüfen Sie die Dokumentation, um die Sperreinstellungen zu konfigurieren.

TSplus Advanced Security Integration mit Sperrung

Wenn ein fehlgeschlagener Anmeldeversuch im Webportal erkannt wurde, wird TSplus Advanced Security dies anzeigen. **“Lockout-Ereignis”, das einem Benutzernamen im Sicherheitsereignisprotokoll entspricht** :



Ein fehlgeschlagener Anmeldeversuch wurde vom Webportal für den Benutzer … 1 fehlgeschlagener Anmeldeversuch wurde für diesen Benutzer seitdem erkannt…

TSplus Advanced Security BruteForce Protection

TSplus Advanced Security Bruteforce Protection deckt die ab **Aspekt der Client-IP-**

Adressen Daher funktioniert es auch für RDP-Verbindungen.

Fehlgeschlagene Brute-Force-Verbindungsversuche , sind auch im Ereignisprotokoll von TSplus Advanced Security sichtbar (private IP-Adressen sind ausgeschlossen, um das Blockieren von Proxys zu vermeiden):



„Ein fehlgeschlagener Verbindungsversuch wurde von der IP-Adresse … erkannt. Diese IP-Adresse ist nicht auf der Whitelist und wird nach mehreren fehlgeschlagenen Verbindungsversuchen blockiert. Bereitgestellter Benutzername: Harry.“

Für weitere Informationen zu Lockout und BruteForce-Schutz, überprüfen Sie diese Dokumentation und die Bruteforce-Schutz-Dokumentation

Webanmeldeseite: So ändern Sie den Anmeldesplashscreen

Übersicht

Wenn die Remote-Verbindung geladen wird, zeigt der HTML5-Client einen standardmäßigen Begrüßungsbildschirm wie im Screenshot unten an:



Sie können diesen Inhalt anpassen, indem Sie eine JavaScript-Konfigurationsdatei ändern.

HTML5-Client

Erstellen Sie Ihren benutzerdefinierten Splashscreen-Inhalt

Jeder Inhalt in Text oder HTML kann für den Splashscreen verwendet werden.

Auch, wenn Sie einfache Anführungszeichen (’) oder doppelte Anführungszeichen (”) verwenden müssen, müssen Sie einen Backslash vor (’ und ”) schreiben, anstatt nur die Anführungszeichen.

Schließlich beachten Sie bitte, dass der Inhalt in nur 1 Zeile geschrieben werden muss.

Das folgende Beispiel ist ein gültiger Inhalt für den Splashscreen:

Dies ist mein benutzerdefiniertes Splashscreen

Bitte sagen Sie "Hallo"!
Es wird ein Titel angezeigt (“Das ist mein benutzerdefinierter Splashscreen”), ein Text (“Bitte sagen Sie Hallo!”) und das animierte Ringbild wie im standardmäßigen TSplus Splashscreen.

Ändern der Splashscreen-Daten, um Ihre eigenen Inhalte zu verwenden

Wenn Sie keine Datei mit dem Namen „settings.js“ im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software\html5“ haben, dann ist Ihre TSplus-Version älter und diese Dokumentation gilt nicht. Bitte aktualisieren Sie zuerst Ihr System oder kontaktieren Sie den Support.

Editieren Sie die Datei „settings.js“, die sich im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software\html5“ befindet. Wir empfehlen Ihnen, einen Texteditor wie Notepad oder Notepad++ zu verwenden. nicht verwenden Sie Word).

Suche nach der Zeile, die mit diesem beginnt:

W.splashscreencontent = ”

Ersetzen Sie es vollständig durch die folgende Zeile:

W.splashscreencontent = “Ihr angepasster Inhalt hier”;

Vergessen Sie nicht die abschließenden Anführungszeichen und das Semikolon (”;).

Wenn Sie die Dauer des Anmelde-Splashscreens in HTML5 verlängern möchten, können Sie dies tun, indem Sie den Wert in Millisekunden ändern:

W.splashscreentime = 5000; //Dauer der Splashscreen-Wiedergabe.

Wir empfehlen Ihnen, den Cache Ihres Browsers zu leeren, nachdem Sie die geänderte HTML-Seite gespeichert haben.

Webanmeldeseite: So schließen Sie das Anmeldeformular nach der Anmeldung

Übersicht

Auf der Web-Login-Seite, wenn der Benutzer auf die Schaltfläche „Anmelden“ klickt, wird der gewählte Client (HTML5 oder Windows) in einem neuen Tab des Browsers geöffnet.

Manchmal, und genauer gesagt, wenn Sie den Windows-Client verwenden, möchten Sie möglicherweise das Anmeldeformular für den Benutzer ausblenden, um zu vermeiden, dass der Benutzer erneut auf die Schaltfläche „Anmelden“ klickt.

Je nach verwendetem Internetbrowser haben Sie zwei Möglichkeiten, dieses Standardverhalten zu ändern. Beide Lösungen erfordern, dass Sie eine JavaScript-Datei ändern.

Lösung A: Schließen des Anmeldetabs - Nur für Internet Explorer

In dieser Lösung wird beim Klicken des Benutzers auf die Schaltfläche „Anmelden“ der gewählte Client in einem neuen Tab des Browsers geöffnet und der Anmeldetab schließt sich selbst. Je nach Version von Internet Explorer kann ein kleines Nachrichtenfenster angezeigt werden, in dem der Benutzer gefragt wird, ob er bestätigen möchte, dass er diesen Tab schließen möchte.

Bearbeiten Sie die Datei „common.js“, die im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software“ gespeichert ist. Wir empfehlen Ihnen, einen Texteditor wie Notepad oder Notepad++ zu verwenden. nicht verwenden Sie Word).

Suche nach diesen Zeilen:

```
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);
}
```

Und ersetzen Sie sie durch diese Zeilen:

```
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();
```

Wir empfehlen Ihnen, den Cache Ihres Browsers zu leeren, nachdem Sie die geänderte JavaScript-Datei gespeichert haben.

Lösung B: Weiterleitung des Anmeldetabs zu einer anderen Webseite - Für alle Browser

In dieser Lösung wird beim Klicken des Benutzers auf die Schaltfläche „Anmelden“ der gewählte Client in einem neuen Tab des Browsers geöffnet, und der Anmeldetab navigiert automatisch zu einer anderen Webseite.

Sie können jede vorhandene Internetadresse (URL) wie „ verwenden. http://google.com oder http://your_intranet/your/page.html, oder Sie können Ihre eigene Webseite erstellen, indem Sie “thankyou.html” als URL verwenden und eine Datei mit dem Namen “thankyou.html” im Ordner “C:\Program Files (x86)\TSplus\Clients\www” erstellen und HTML-Inhalt darin einfügen.

Bearbeiten Sie die Datei „common.js“, die im Ordner „C:\Program Files (x86)\TSplus\Clients\www\software“ gespeichert ist. Wir empfehlen Ihnen, einen Texteditor wie Notepad oder Notepad++ zu verwenden. nicht verwenden Sie Word).

Suche nach diesen Zeilen:

```
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);
}
```

Und ersetzen Sie sie durch diese Zeilen:

```
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";
```

Wir empfehlen Ihnen, den Cache Ihres Browsers zu leeren, nachdem Sie die geänderte JavaScript-Datei gespeichert haben.

Webanmeldeseite: So öffnen Sie den HTML5-Client im selben Tab

Übersicht

Auf der Web-Login-Seite, wenn der Benutzer auf die Schaltfläche „Anmelden“ klickt, wird der HTML5-Client in einem neuen Tab des Browsers geöffnet.

Sie können dieses Verhalten ändern und den HTML5-Client so einstellen, dass er im selben Browser-Tab wie die Web-Anmeldeseite geöffnet wird, indem Sie eine JavaScript-Datei ändern.

Modifizieren der custom.js-Datei

Bearbeiten Sie die Datei „custom.js“, die im Ordner „C:\Program Files (x86)\TSplus\Clients\www“ gespeichert ist. Wir empfehlen Ihnen, einen Texteditor wie Notepad oder Notepad++ zu verwenden. nicht verwenden Sie Word).

Fügen Sie diese Zeile hinzu:

var openinsamewindow = true;

Wir empfehlen Ihnen, den Cache Ihres Browsers zu leeren, nachdem Sie die geänderte JavaScript-Datei gespeichert haben.

Modifizieren der common_applications.js-Datei

Wenn Sie die Funktion des Terminal Service Plus Web Applications Portals verwenden, müssen Sie eine zweite Datei bearbeiten. Bearbeiten Sie die Datei "common_applications.js", die im Ordner "C:\Program Files (x86)\TSplus\Clients\www\software" gespeichert ist. Wir empfehlen Ihnen, einen Texteditor wie Notepad oder Notepad++ zu verwenden. nicht verwenden Sie Word).

Suche nach diesen Zeilen:

```
if (childurl != '') {
  window.name = childname;
  location.href = childurl + '#';
}
```

Und ersetzen Sie sie durch diese Zeilen:

```
  if (childurl != '') {
    window.name = childname;
    location.href = childurl + '#';
  }
```

Wir empfehlen Ihnen, den Cache Ihres Browsers zu leeren, nachdem Sie die geänderte JavaScript-Datei gespeichert haben.

Webportal mit SSO (Beta)

Wichtige Voraussetzungen und Einschränkungen

Webportal 2026 mit SSO ist für die **Kreativ** Thema und verwendet alle Anpassungen aus AdminTool > Web > Webportal-Anpassung. Wenn das ausgewählte Thema nicht **Kreativ** , das Webportal wird nicht angezeigt.

Wenn in einem Farm aktiviert, müssen alle Server die ausführen **gleiche Remote Access-Version** und aktiviert werden für **Webportal 2026 mit SSO**

Diese Funktion ist **Beta** und sollte **nicht** auf Produktionsservern bereitgestellt werden.

Warum ein neues Webportal?

Im Vergleich zum vorherigen Webportal bietet diese Implementierung höhere Zuverlässigkeit und bessere Leistung unter Last. Außerdem ermöglicht es:

- **Erweiterte SSO-Funktionen**
  - Windows-Integrationsauthentifizierung (Negotiate / Kerberos / NTLM)
  - Integration eines Identitätsanbieters von Drittanbietern (derzeit SAML)
- **Stärkere Sicherheitskontrollen**
  - Eingebaute Anti-Fälschungsschutzmaßnahmen
  - Endpoint-Ratenbegrenzung
  - Moderne Authentifizierung und Cookie-/Sitzungssteuerung

Seine Architektur wird es uns ermöglichen, etwaiges Feedback zu Sicherheitsprüfungen leicht zu berücksichtigen.

Es ist auch ein **zugänglicheres Produkt** durch Empfehlungen und verbesserten Kontrast.

Webserver-Flexibilität (Kestrel standardmäßig)

Die Anwendung ist nicht an einen Front-End-Webserver gebunden. Standardmäßig läuft sie auf **Kestrel** (HTTP-Port 81). Es kann von **IIS** oder **Apache** als Reverse-Proxy durch Ändern der Webserver-Konfiguration.

Beispiel: Apache-Reverse-Proxy für den Webportal-Dienst

```
# Apache VirtualHost example
ProxyPreserveHost On
ProxyPass        /  http://127.0.0.1:81/
ProxyPassReverse /  http://127.0.0.1:81/

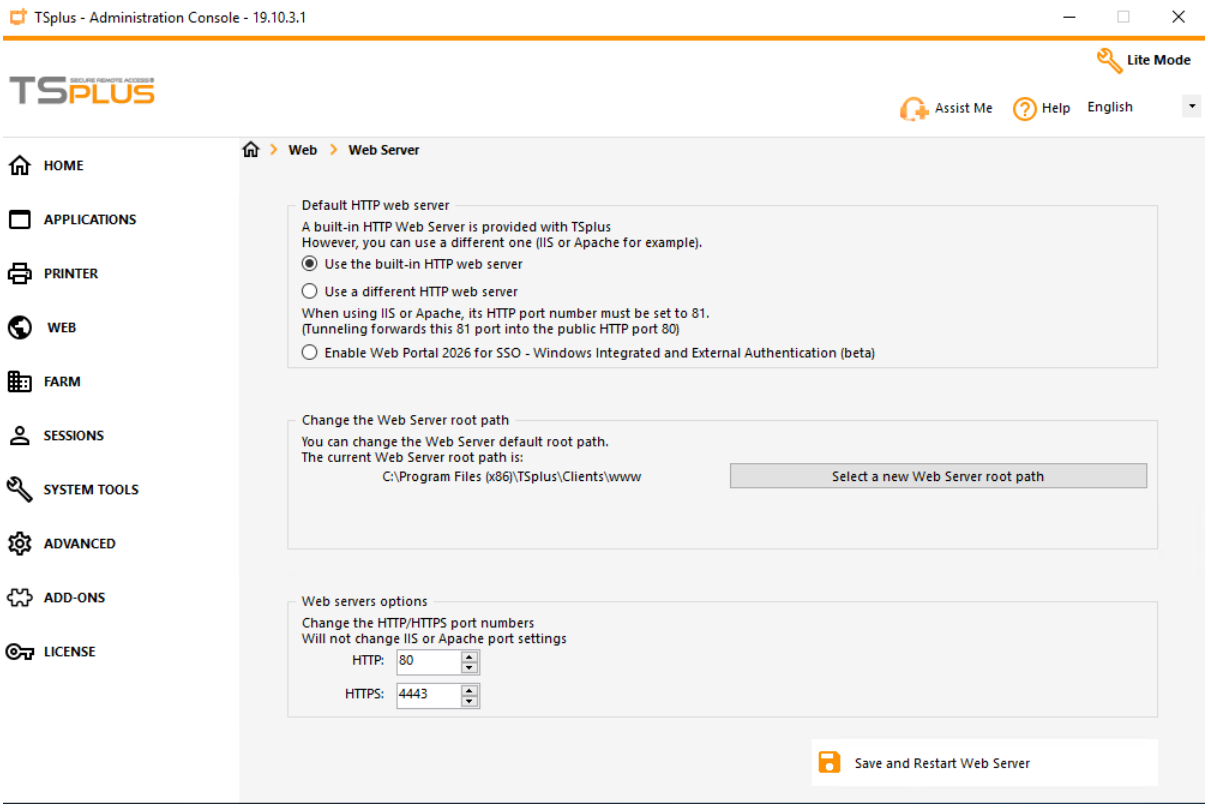
RequestHeader set X-Forwarded-Proto "https"
RequestHeader set X-Forwarded-For "%{REMOTE_ADDR}s"
```

Dies hält die Logik des Webportals unverändert, während Apache die öffentliche HTTP/HTTPS-Exposition verwaltet.

Bitte kontaktieren Sie das Entwicklungsteam, wenn Sie interessiert sind, da dieses Szenario derzeit nicht über das AdminTool-Programm zugänglich ist und manuell konfiguriert werden muss.

Webportal 2026 mit SSO aktivieren

1. Öffnen **Admin-Tool**
2. Gehe zu: Web > Webserver
3. Aktivieren: **Webportal 2026 mit SSO**



Wichtig Diese Option ist Beta. Nur in Testumgebungen verwenden.

Unterstützte Anmeldemodi

Webportal 2026 mit SSO unterstützt:

- Traditionelles Anmeldeformular mit Windows-Anmeldeinformationen
- Webanmeldeinformationen. Siehe: https://docs.tsplus.net/tsplus/web-credentials/
- Windows-Integrationsauthentifizierung (automatisch in vertrauenswürdigen / lokalen Szenarien)
- Externer Identitätsanbieter über **SAML** wie Entra ID (ehemals Azure AD) oder Okta

Hinweis: Unterstützung für externe Authentifizierung über **OIDC** geplant später, auf Anfrage

2FA-Verhalten

2FA wird auf Standardkontoflüsse angewendet, einschließlich:

- Anmeldeformular mit Windows-Anmeldeinformationen
- Web-Anmeldeinformationen
- Windows-Integrationsauthentifizierung

Externe Authentifizierungsanbieter setzen häufig ihre eigene MFA / 2FA durch. Daher gilt die in dem Remote Access 2FA Add-on festgelegte 2FA-Konfiguration nicht für dieses Szenario.

Der lokale Netzwerkumgehung ist verfügbar über CustomSettings:TwoFaBypassForLocalNetwork Parameter, der in der Datei enthalten ist: C:\Program Files (x86)\TSplus\Clients\webportal\appsettings.json , wo C:\Program Files (x86)\TSplus ist der TSplus Remote Access-Setup-Ordner. Wenn aktiviert, erfolgt die Umgehung nur, wenn Client und Gateway im selben privaten Subnetz sind.

Windows-Authentifizierungsfluss konfigurieren

Für Benutzer, die sich mit Windows-Authentifizierung anmelden, ist eines der Folgenden erforderlich:

1. Vorregistrieren Sie Anmeldeinformationen mit dem TSplus-Befehl: AdminTool.exe / windowscredential-addorupdate Siehe Dokumentation unter https://docs.tsplus.net/tsplus/commands-list/#add-or-update-credentials-to-the-windows-credentials-manager-windowscredential-addorupdate
2. Oder lassen Sie den Benutzer sich einmal über das Anmeldeformular des Webportals mit Windows-Anmeldeinformationen anmelden.

Für die Konfiguration der Windows-Integrationsauthentifizierung siehe bitte: Windows-Integrationsauthentifizierung in einer Active Directory-Domäne aktivieren. Da dieser Authentifizierungsmodus mühsam zu konfigurieren ist, ziehen es die Kunden oft vor, einen externen Identitätsanbieter einzurichten.

Externe Authentifizierung (SAML) konfigurieren

Erforderliche Einstellungen für die externe Anwendung

Die externe Anwendung muss wie folgt konfiguriert werden:

- Single Sign-On-URL muss auf den SAML-Consumer-Service-Endpunkt des Webportals eingestellt werden, z.B. https://mywebportal.company.com/Saml/acs
- Audience-URI (SP-Entitäts-ID) muss auf den Domainnamen oder die IP-Adresse des Webportals eingestellt werden, z. B. https://mywebportal.company.com
- Name-ID-Format muss eingestellt werden **E-Mail-Adresse**
- Anwendungsbenutzername muss eingestellt werden **E-Mail** , da der linke Teil den Benutzernamen des Windows-Kontos identifiziert

Erforderliche Einstellungen in appsettings.json

Die Datei appsettings.json befindet sich in C:\Program Files (x86)\TSplus\Clients\webportal ,

wo C:\Program Files (x86)\TSplus ist der TSplus Remote Access-Setup-Ordner.

Bearbeiten Sie die Saml2 Abschnitt:

- IdP-Metadaten
- Herausgeber
- SingleSignOnZiel (optional if metadata provides it)
- SingleLogoutDestination (optional if metadata provides it)
- Zertifikatbezogene Felder

Zum Beispiel, die Verwendung des Drittanbieter-Identitätsanbieters Okta:


```
"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#"
}
```


Die Issuer-Einstellung legt die Audience-URI fest, wie sie auf der Seite des externen Identitätsanbieters definiert ist.

wenn die SignatureValidierungszertifikatdatei Die Einstellung ist auf einen anderen Wert als gesetzt. **None** , stellen Sie bitte sicher, dass das Zertifikat auf dem Anwendungsserver als gültig betrachtet wird. Dies kann erfordern, dass das Zertifikat zur Liste der vertrauenswürdigen Zertifikate maschinenweit hinzugefügt wird.

Verfügbarkeit des Windows-Passworts für den Sitzungsstart

Für die externe SAML-Authentifizierung erfordert das Starten von Sitzungen weiterhin verwendbare Windows-Anmeldeinformationen. Verwenden Sie eine der:

1. Windows-Anmeldeinformationen mit Befehl registrieren: AdminTool.exe /windowscredential-addorupdate Siehe Dokumentation unter https://docs.tsplus.net/tsplus/commands-list/#add-or-update-credentials-to-the-windows-credentials-manager-windowscredential-addorupdate
2. Oder Passwort von IdP-Anspruch weiterleiten, indem Sie einstellen CustomSettings:UseSamlPasswordClaim zum Anspruchstyp, der das Windows-Passwort enthält.

Typischerweise wird das Webportal den Teil vor dem '@' der Benutzer-E-Mail-Adresse als Benutzernamen des Windows-Kontos verwenden.

Bitte beachten Sie, dass die externe Authentifizierung derzeit nur mit lokalen Benutzern funktioniert.

Wenn kein Passwort aus dem Anspruchs- oder Berechtigungsstore verfügbar ist, schlägt die Benutzervalidierung fehl.

Vollständige Referenz der appsettings.json-Konfigurationsdatei

Die Datei appsettings.json befindet sich in C:\Program Files (x86)\TSplus\Clients\webportal , wo C:\Program Files (x86)\TSplus ist der TSplus Remote Access-Setup-Ordner.

Protokollierung

Parameter	Zweck	Mögliche Werte	Standardmä
Protokollierung:Protokollebene:Standard	Globales minimales Protokollniveau.	Verfolgen , Debug , Information , Warnung , Fehler , Kritisch , None	Information
Logging:LogLevel:Microsoft.AspNetCore	ASP.NET Core-	Gleich wie	Warnung

	Framework-Protokollebene.	oben	
Logging:LogLevel:Microsoft.AspNetCore.Authentication	Authentifizierungs-Subsystem-Protokollebene.	Gleich wie oben	Warnung

Globale Host-Einstellung

Parameter	Zweck	Mögliche Werte	Standardmäßig
ErlaubteHosts	Host-Header-Filterung zum Schutz von ASP.NET Core-Hosts.	* (all) oder durch Semikolons getrennte Hostliste	*

IpRateLimiting

Parameter	Zweck	Mögliche Werte	Standardmäßig
IpRateLimiting:EndpointRateLimitingAktivieren	Ermöglicht endpoint-spezifische Drosselungsregeln.	wahr / falsch	wahr
IpRateLimiting:StackBlockedRequests	Wenn wahr , blockierte Anfragen erhöhen weiterhin die Zähler.	wahr / falsch	falsch
IpRateLimiting:HttpStatusCode	HTTP-Status, der zurückgegeben wird, wenn die Anfrage blockiert wird.	Ganzzahliger HTTP-Code (typischerweise 429)	429
IpRateLimiting:RealIpHeader	Header, der verwendet wird, um die Client-IP hinter dem Proxy aufzulösen.	Kopfzeile	X-Forwarded-For
IpRateLimiting:ClientIdHeader	Optionaler Client-ID-Header für benutzerdefinierte Ratenbegrenzung.	Kopfzeile	X-ClientId

IpRateLimiting:AllgemeineRegeln

Jedes Regelobjekt hat:

Parameter	Zweck	Mögliche Werte	Standard in der gelieferten Datei
Endpoint	Routen-/Methodenmuster zum Schutz.	Format VERB:/pfad	Mehrere Standardwerte (siehe unten)
Periode	Bewertungsfenster.	z.B. 1s , 1m , 5m , 1h , 1d	5m (für alle Standardregeln)
Limit	Maximale Anfragen im Zeitraum.	Positive ganze Zahl	5 (für alle Standardregeln)

Saml2

Parameter	Zweck	Mögliche Werte	Stand
Saml2:IdPMetadata	IdP-Metadaten-URL zum Laden der SAML-Anbieter-Konfiguration.	Gültige HTTPS-URL	""
Saml2:Aussteller	SP-Entitäts-ID (diese Identität des Webportals).	URI-Zeichenfolge	""
Saml2:SingleSignOnDestination	IdP SSO-Endpunkt-URL (kann aus Metadaten automatisch aufgelöst werden).	HTTPS-URL	""
Saml2:SingleLogoutDestination	IdP SLO-Endpunkt-URL (kann aus Metadaten automatisch aufgelöst werden).	HTTPS-URL	""
Saml2:Signaturalgorithmus	XML-Signaturalgorithmus.	URI-Wert, der von der SAML-Bibliothek akzeptiert wird	http:/ www. xmlds sha25
Saml2:SigningCertificateFile	Lokale SP-Signaturzertifikatdatei (relativ zum Basisverzeichnis der App).	Dateiname/Pfad	""
Saml2:SigningCertificatePassword	Passwort für die Signaturzertifikatdatei.	String	""
Saml2:Signaturvalidierungszertifikatdatei	IdP-Zertifikatdatei zur Validierung von Signaturen (optional, wenn Metadaten Zertifikate bereitstellen).	Dateiname/Pfad	""
Saml2:ZertifikatValidierungsmodus	Zertifikatkettenvalidierungsmodus.	None ,	Chai

		PeerTrust , ChainTrust , Peer- oder Kettenvertrauen , CustomRootTrust	
Saml2:Widerrufsmodus	Zertifikatwiderrufsverhalten.	NoCheck , Online , Offline	Offlin
Saml2:XmlCanonicalizationMethod	XML-Kanonisierungsalgorithmus-URI.	XML-DSig-Kanonalisierungs-URI	http:/ www. xml-e

Benutzerdefinierte Einstellungen

In appsettings.json diese Werte werden als Zeichenfolgen gespeichert true / false) und durch .NET-Konfigurationsbindung auf Booleans abgebildet.

Parameter	**Zweck**	
CustomSettings:VerwendeAnwendungsvollesPfad	Steuert, ob der vollständige Anwendungs-Pfad verwendet wird, wenn zugewiesene Apps aufgelistet oder gestartet werden.	
CustomSettings:AktivierenAutoWindowsAuthentifizierungAufLocalhost	Ermöglicht die automatische Windows-Authentifizierung im localhost/Loopback-Szenario.	
CustomSettings:PasswortverschlüsselungAktivieren	Verschlüsselt die Domain/ Benutzername/Passwort in der HTML5-Startverbindungszeichenfolge unter Verwendung von RSA-Parametern.	
CustomSettings:TwoFaBypassForLocalNetwork	Umgeht das Webportal 2FA, wenn der Client im selben privaten Subnetz wie der Server ist.	
CustomSettings:UseSamlPasswordClaim	SAML-Anspruchstyp, der als weitergeleitetes Windows-Passwort für den Sitzungsstart verwendet wird.	

Fehlerbehebung

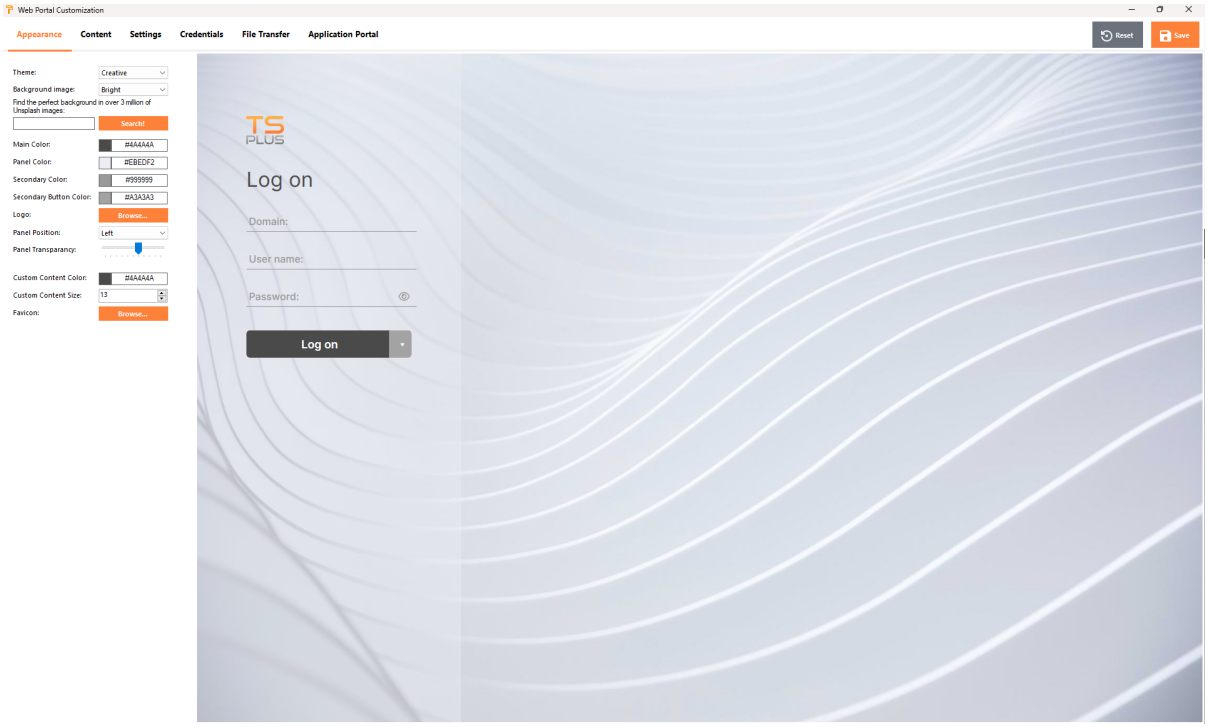
Webportal 2026 mit SSO-Protokollen kann über AdminTool > Erweitert > Protokolle > Webportal-Protokoll aktiviert werden.

Das Ergebnis WebPortal.log Das Protokoll befindet sich in C:\Program Files (x86)\TSplus\Clients\webportal , wo C:\Program Files (x86)\TSplus ist der TSplus Remote Access-Setup-Ordner.

Erstellen und Anpassen von HTML-Webzugriffseiten mit der Webportal-Anpassung

Mit der Anpassung des Webportals können Sie Ihre eigenen benutzerdefinierten HTML-Webzugriffseiten erstellen - und es gibt keine Notwendigkeit, ein Webentwickler zu sein !

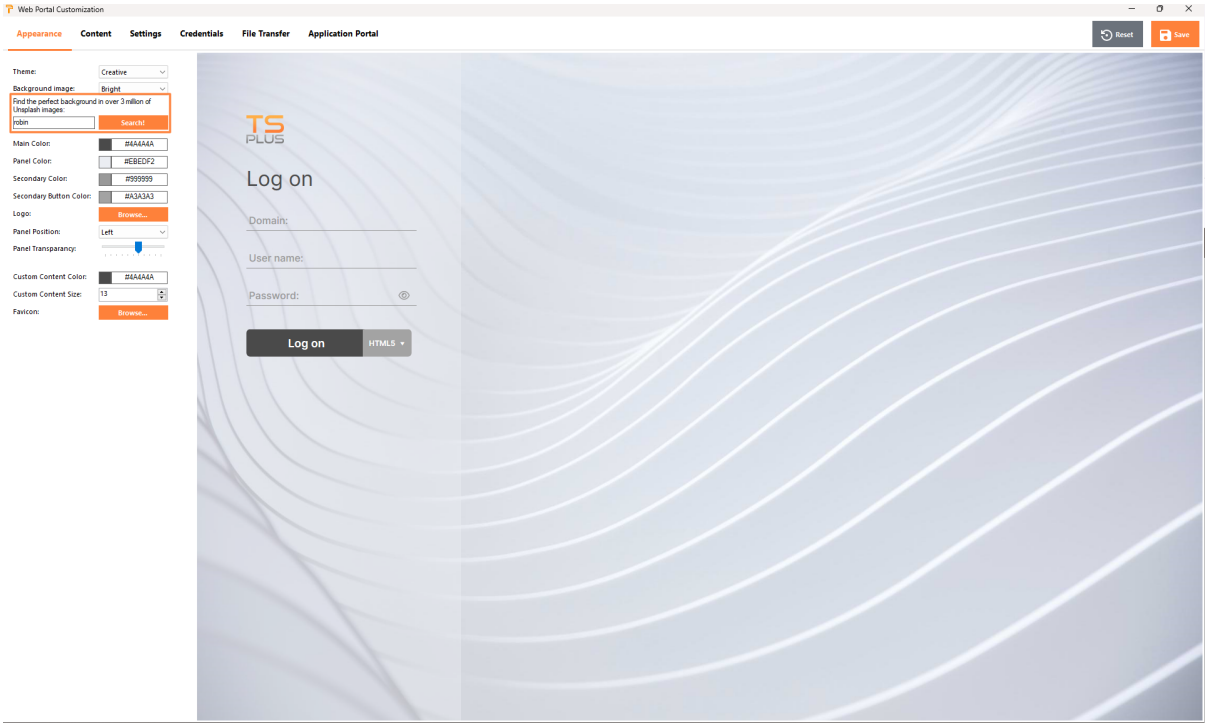
Webportal-Anpassung - Erscheinungsbild



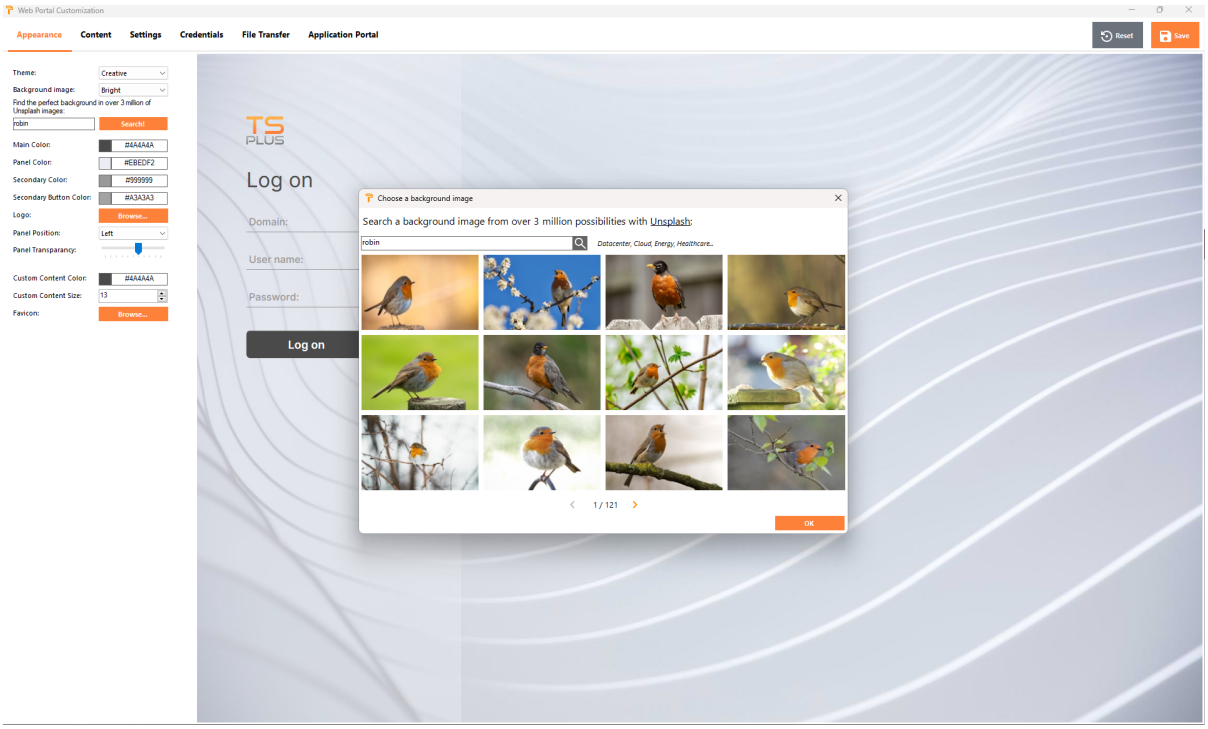
Mit dem Tab Erscheinung können Sie alle grafischen Einstellungen anpassen und Ihr eigenes Logo hinzufügen.

Sie haben die Wahl zwischen einer Sammlung von Fotos oder Sie können Ihre eigenen hinzufügen. Sie können auch ein beliebiges Farbschema mit der Hintergrundfarbe Ihrer Wahl festlegen oder eines der klassischen Themen verwenden.

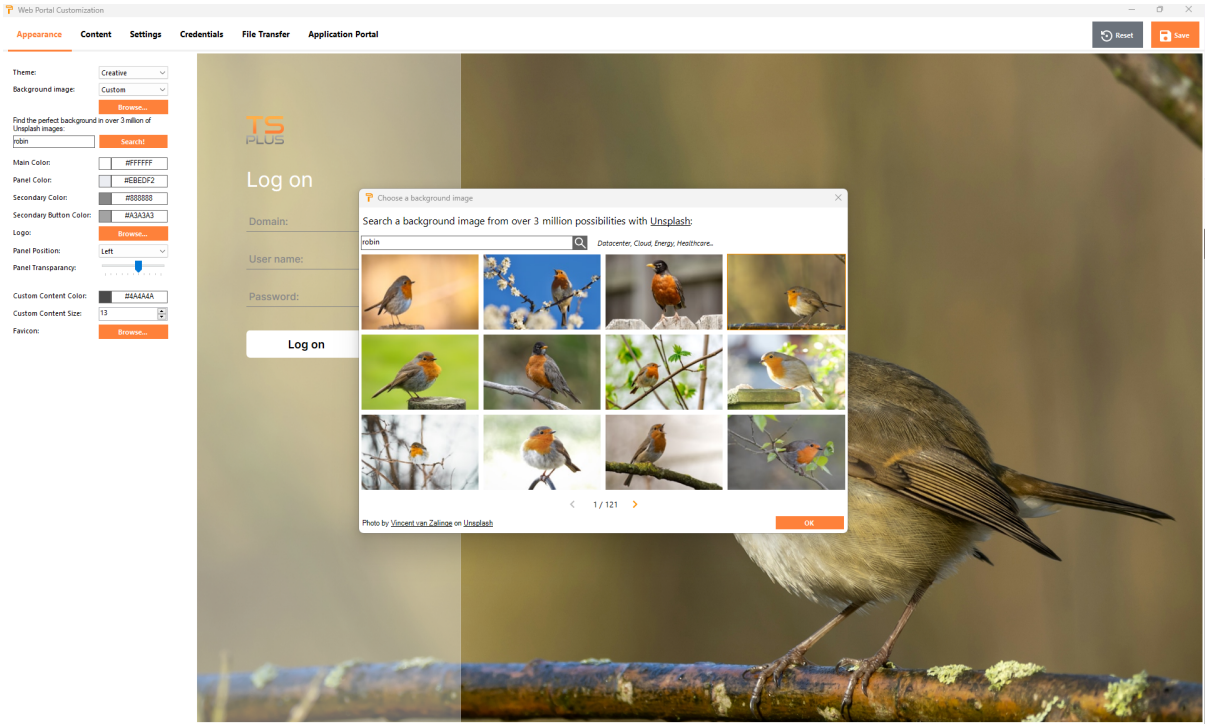
Sie können auch ein Schlüsselwort eingeben, um ein Hintergrundbild aus der Unsplash-Bibliothek zu suchen:



Ich werde eine Sammlung von Bildern zur Auswahl anzeigen.

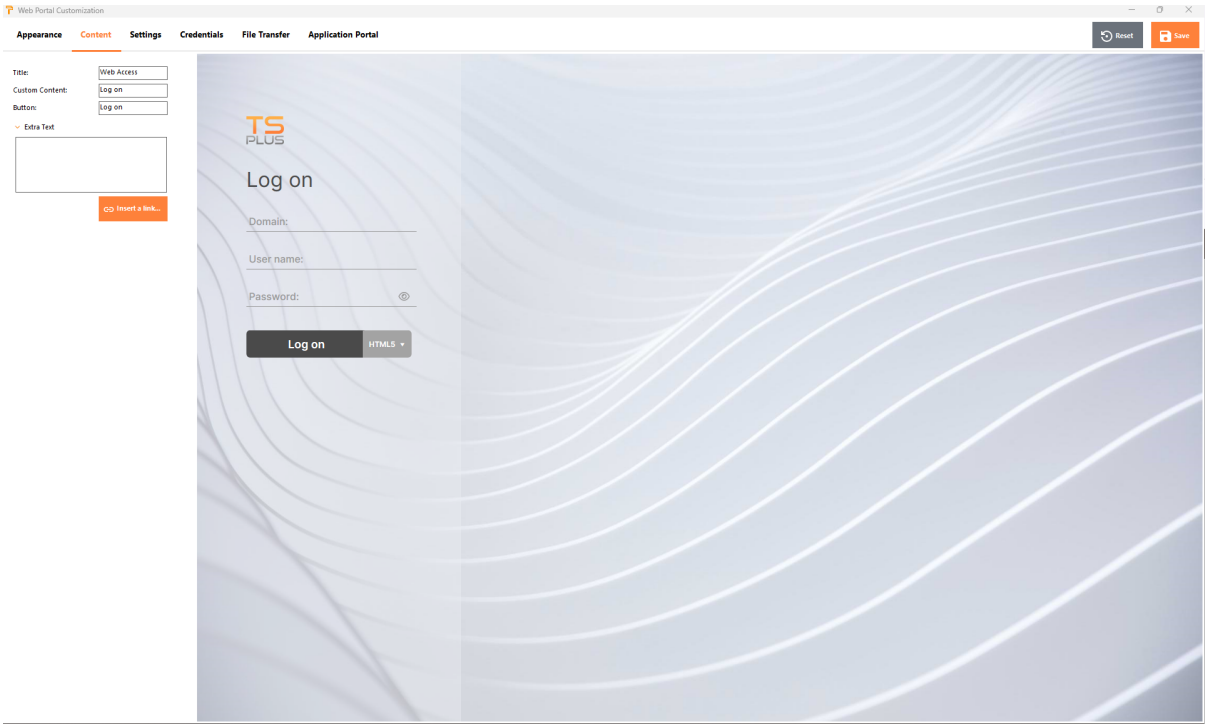


Wählen Sie Ihr Lieblingsbild aus, um das Ergebnis auf Ihrem Webportal zu sehen:

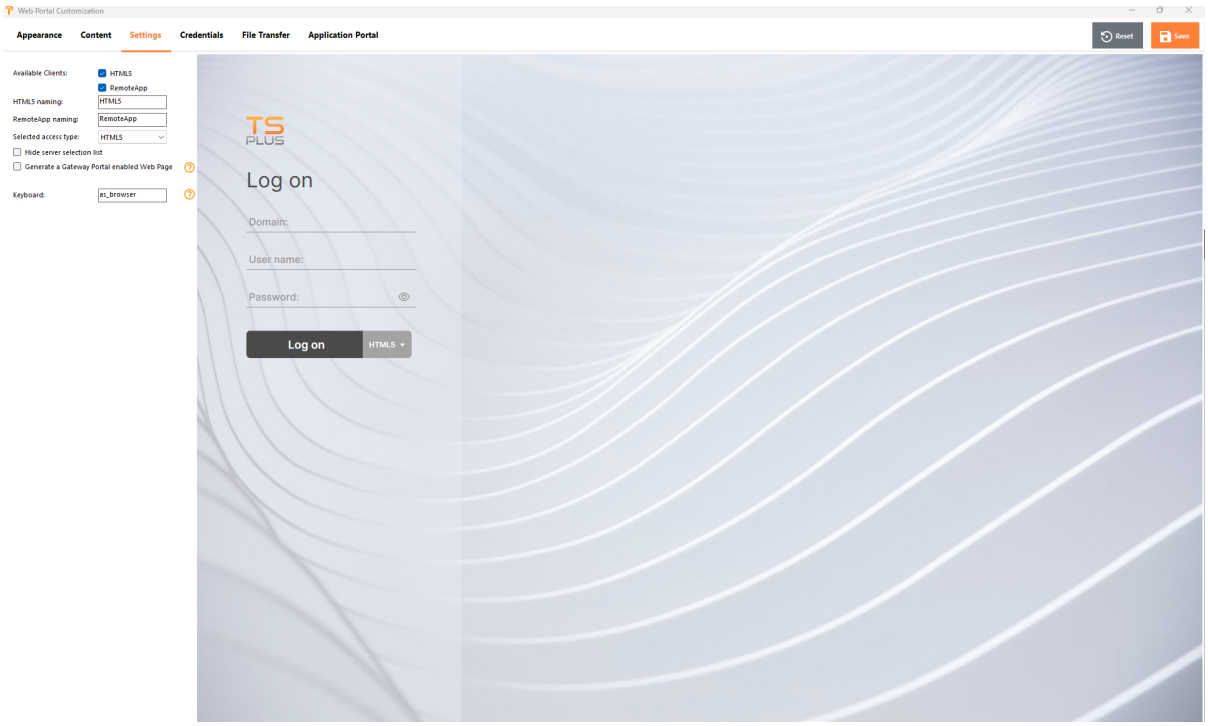


Die Farbthemen passen sich automatisch an das gewählte Bild an, sobald Sie Ihre Auswahl mit der Schaltfläche „Ok“ bestätigen. Natürlich können Sie die Farben nach Belieben weiterhin personalisieren.

Webportal-Anpassung - Inhalt

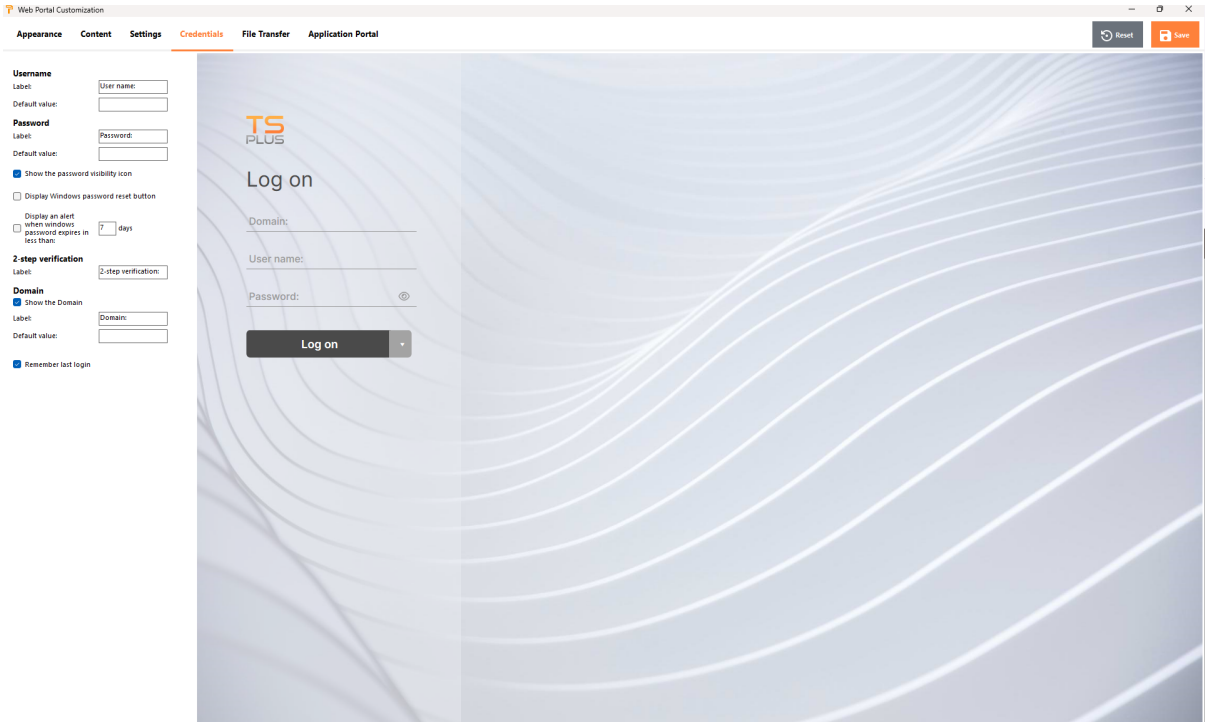


Webportal-Anpassung - Einstellungen

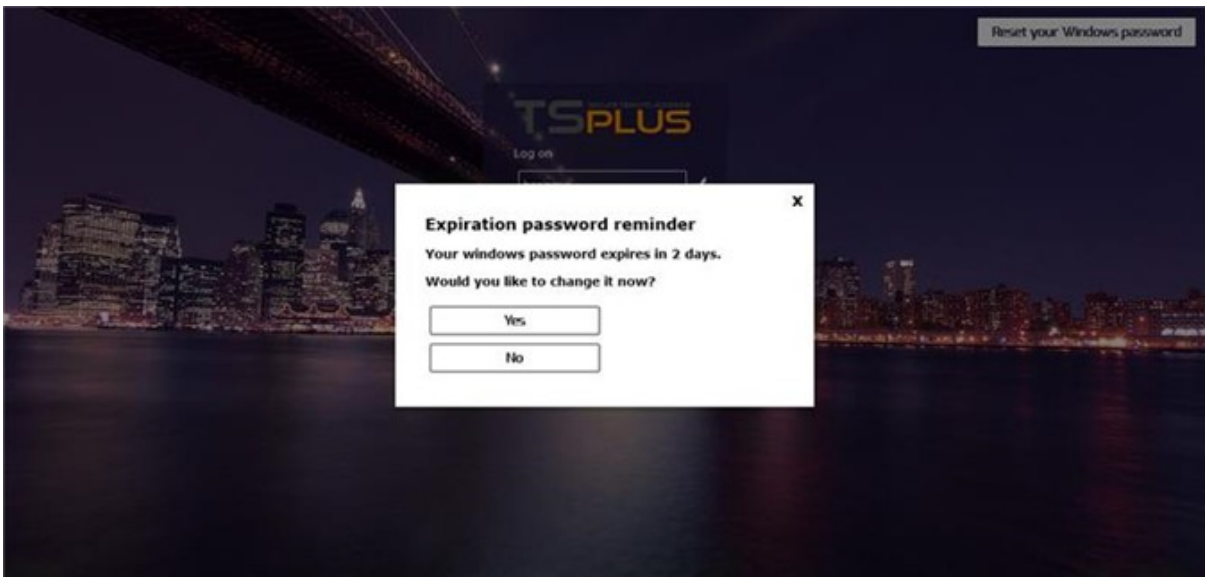


- “ **Verfügbare Clients** Wählen Sie zwischen 2 Arten von Webverbindungsclients. Wenn beide aktiviert sind, hat der Benutzer die Wahl. Sie können den Namen, der für diese Optionen in Ihrem Webportal verwendet wird, ändern. Sie können auch auswählen, welche Option standardmäßig ausgewählt ist, wenn beide Optionen verfügbar sind.
- “ **Gateway-Portal** Überprüfen Sie es, um eine aktivierte Gateway-Portal-Seite zu aktivieren. Diese Funktion fügt einen zusätzlichen Authentifizierungsschritt hinzu, wenn Sie einen Server einem Benutzer oder einer Gruppe zuweisen.
- “ **Tastatur** Nur für fortgeschrittene Administratoren, die spezielle Tastaturanpassungen benötigen.

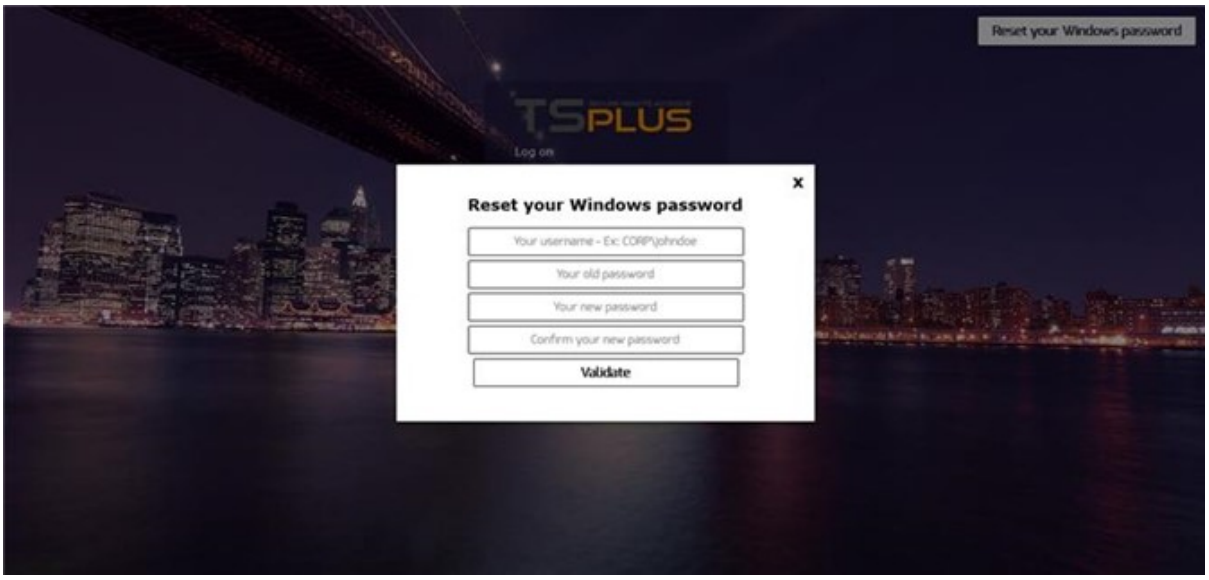
Webportal-Anpassung - Anmeldeinformationen



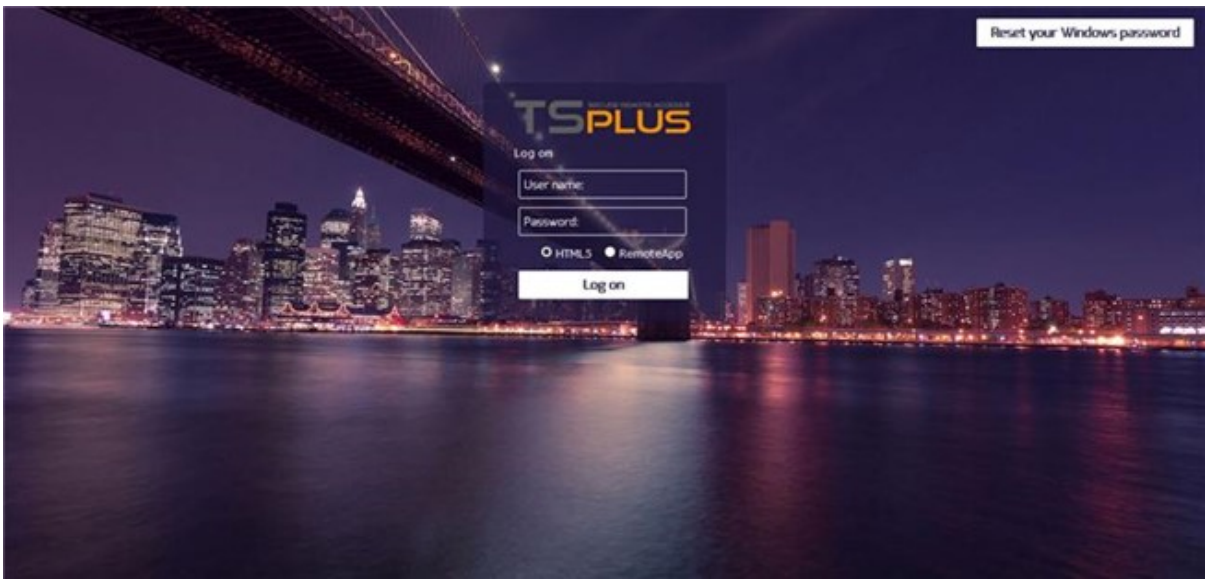
- “ **Bezeichnung** : Sie können den Text ändern, der zur Bezeichnung des Benutzernamens, des Passworts, … verwendet wird.
- “ **Standardwerte** Sie können ein Standard-Login, ein Passwort und eine Domain angeben, die die Anmeldefelder automatisch ausfüllen. Alle hier vorhandenen Einstellungen werden in der index.html-Datei gespeichert, die kopiert und nach Ihren Wünschen umbenannt werden kann.
- “ **Domainfeld anzeigen** Wenn aktiviert, wird das Feld Domain in die Anmeldeinformationsanfrage einbezogen.
- “ **Passwort** Sie können eine Warnmeldung hinzufügen, die während der Verbindung über das Webportal angezeigt wird, um den Benutzer über das Ablaufdatum seines Passworts zu informieren. Zum Beispiel wird das folgende Pop-up angezeigt, wenn das Windows-Passwort des Benutzers in weniger als 3 Tagen abläuft:



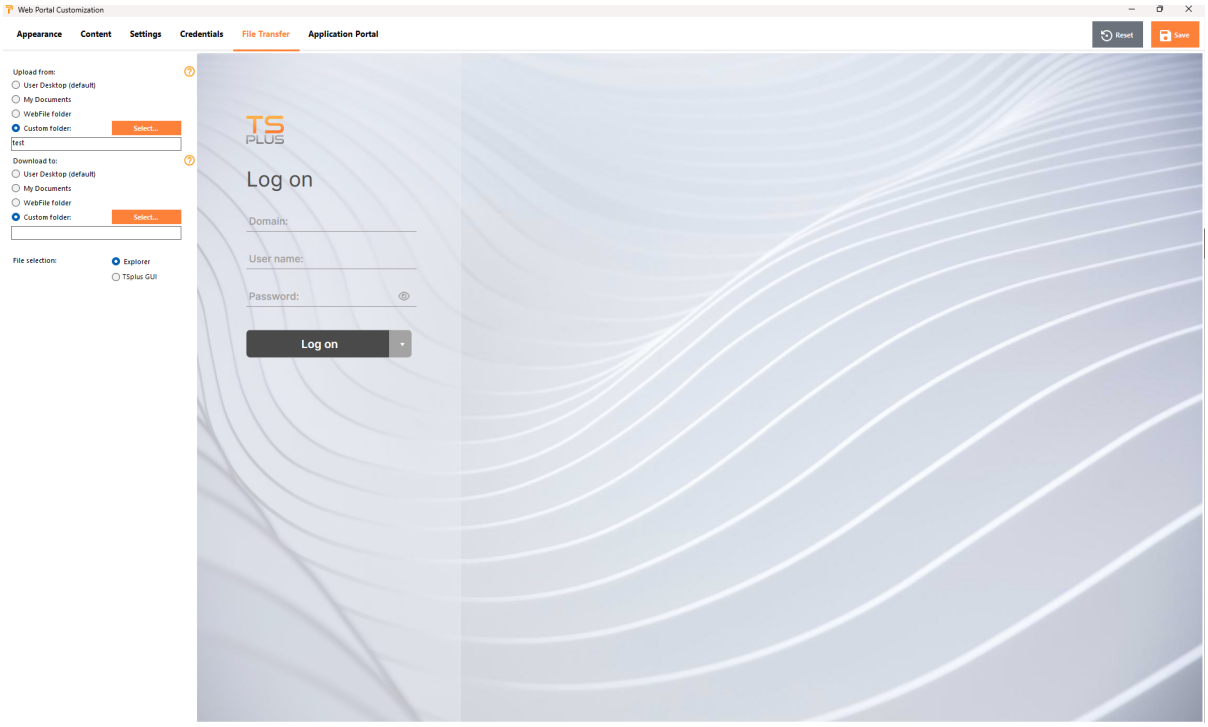
Wie erwähnt, gibt es ihm die Möglichkeit, es direkt über das Webportal zu ändern, indem er das direkt darunter angezeigte Pop-up verwendet:



Sie können den Benutzer auch direkt in die Lage versetzen, seine Fenster jederzeit zu ändern, indem Sie die Option „Schaltfläche zum Zurücksetzen des Windows-Passworts anzeigen“ aktivieren.

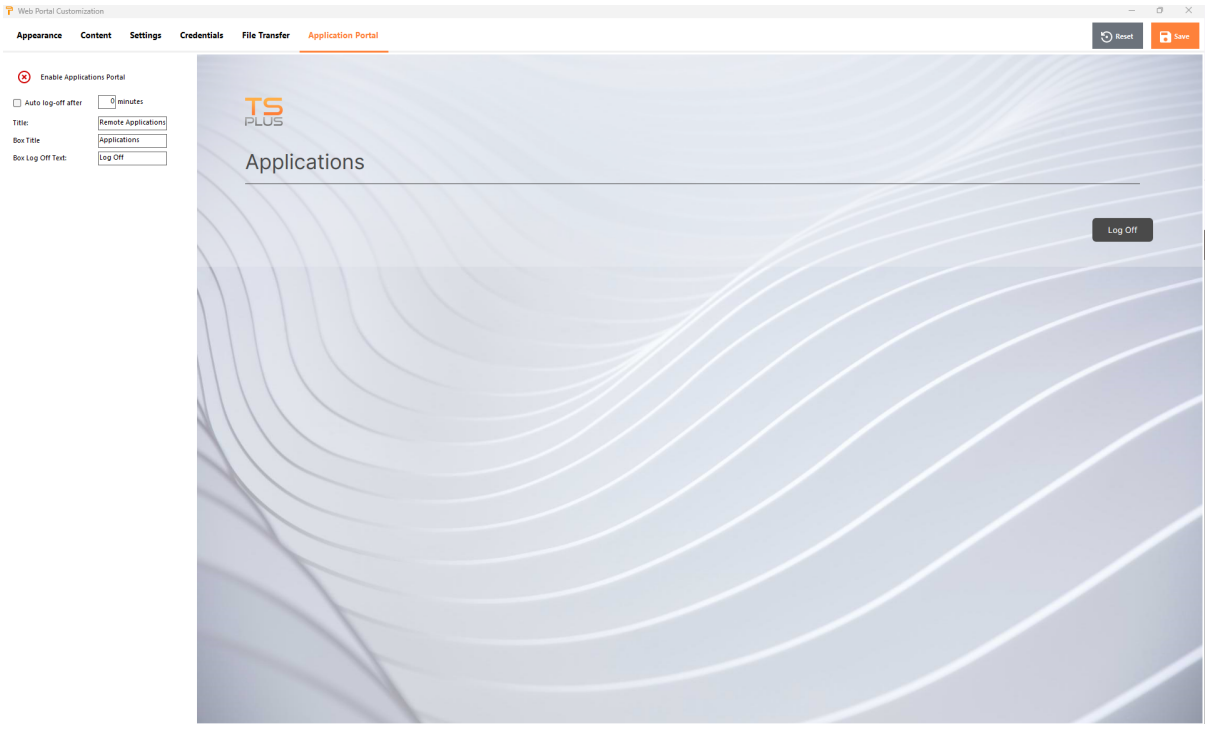


Webportal-Anpassung - Dateiübertragung



- “ **Hochladen - Herunterladen** Wählen Sie Quell- und Zielpfade für Datei-Uploads und -Downloads aus.

Webportal-Anpassung - Anwendungsfeld



Weitere Informationen zum Anwendungsportal sind verfügbar. hier .

Eingeben von Werten speichern und auf Standardwerte zurücksetzen

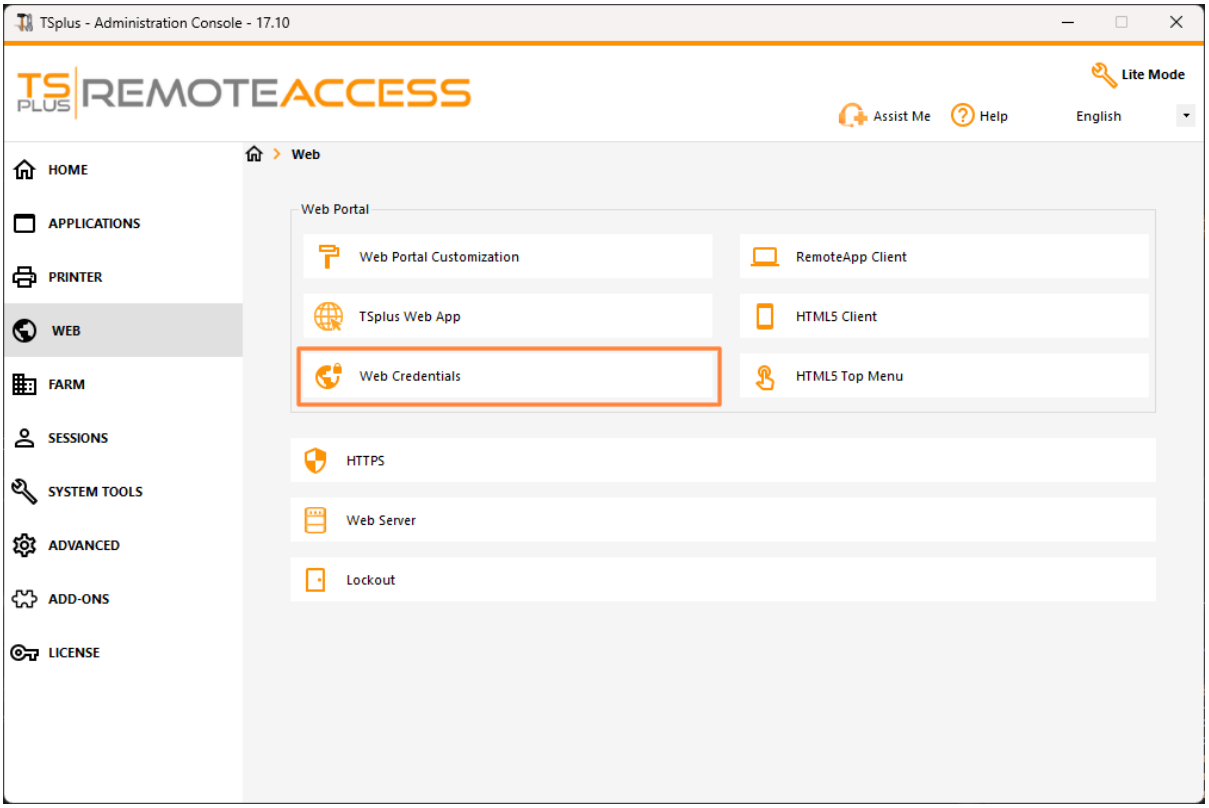
Vergessen Sie nicht, auf die Schaltfläche „Speichern“ zu klicken, um alle Ihre Änderungen zu speichern.

Wenn Sie diese Werte auf die ursprünglichen Werte zurücksetzen möchten, klicken Sie auf die Schaltfläche „Zurücksetzen“.

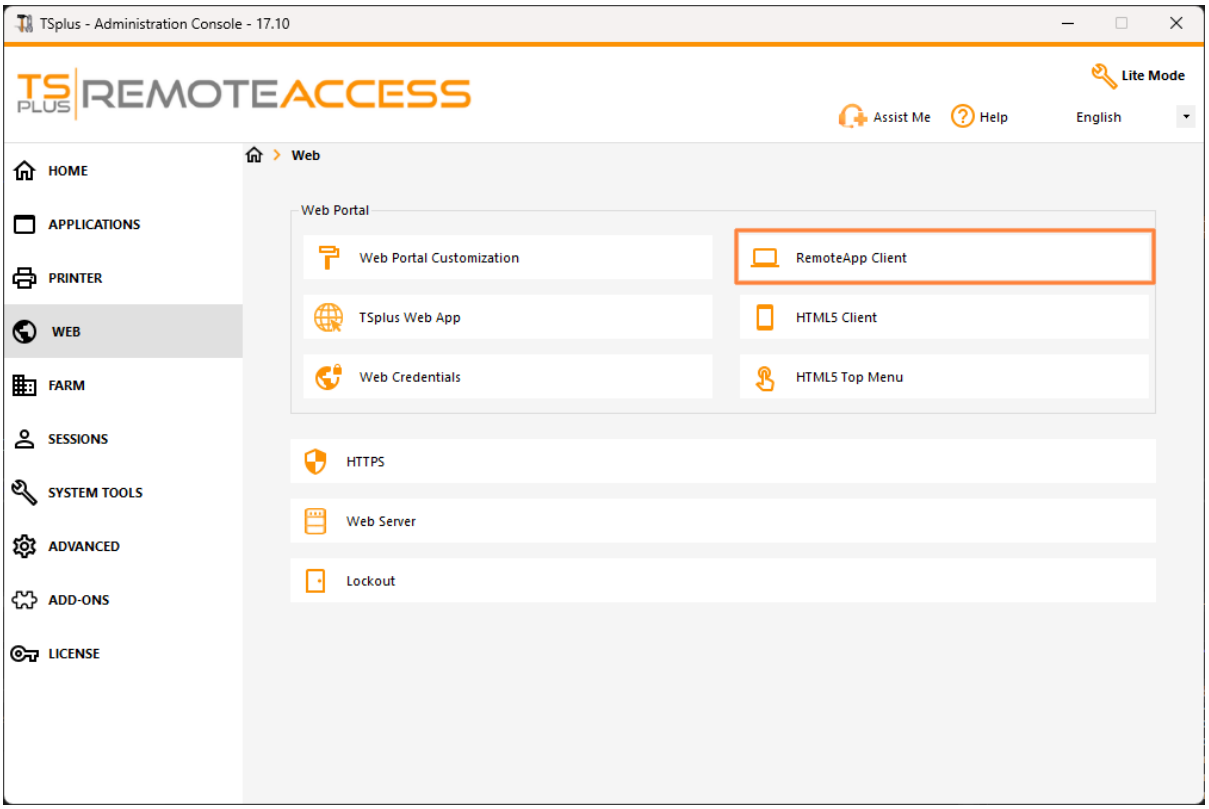
Web-Anmeldeinformationen

Der Abschnitt „Webanmeldeinformationen“ ermöglicht es Ihnen, die Funktion zu aktivieren (oder zu deaktivieren) Web-Anmeldeinformationen Funktion.

Wenn Sie Webanmeldeinformationen verwenden, möchten Sie möglicherweise leere Passwörter zulassen. Wenn Sie nur Webanmeldeinformationen mit leeren Passwörtern haben, empfehlen wir, die Option „Passwortfeld anzeigen“ zu deaktivieren, um die Anmeldeseite weiter zu vereinfachen.

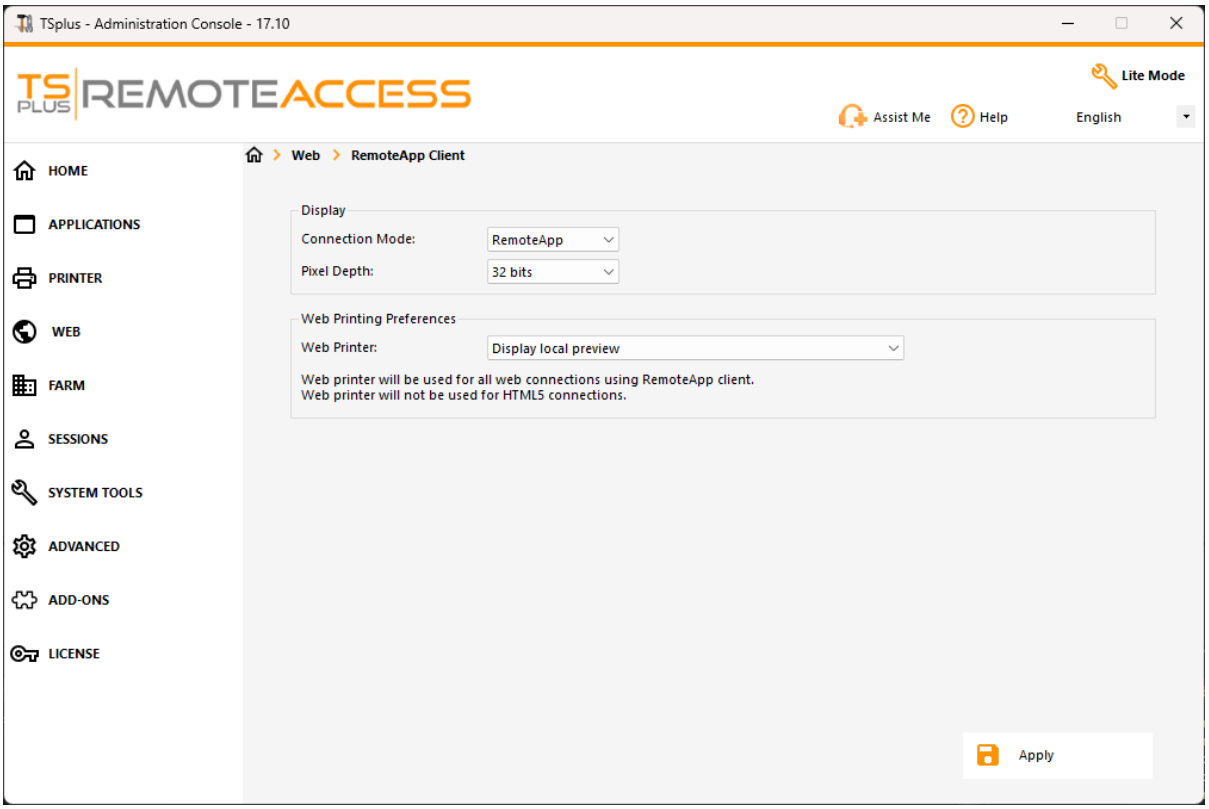


Remote App-Kachel

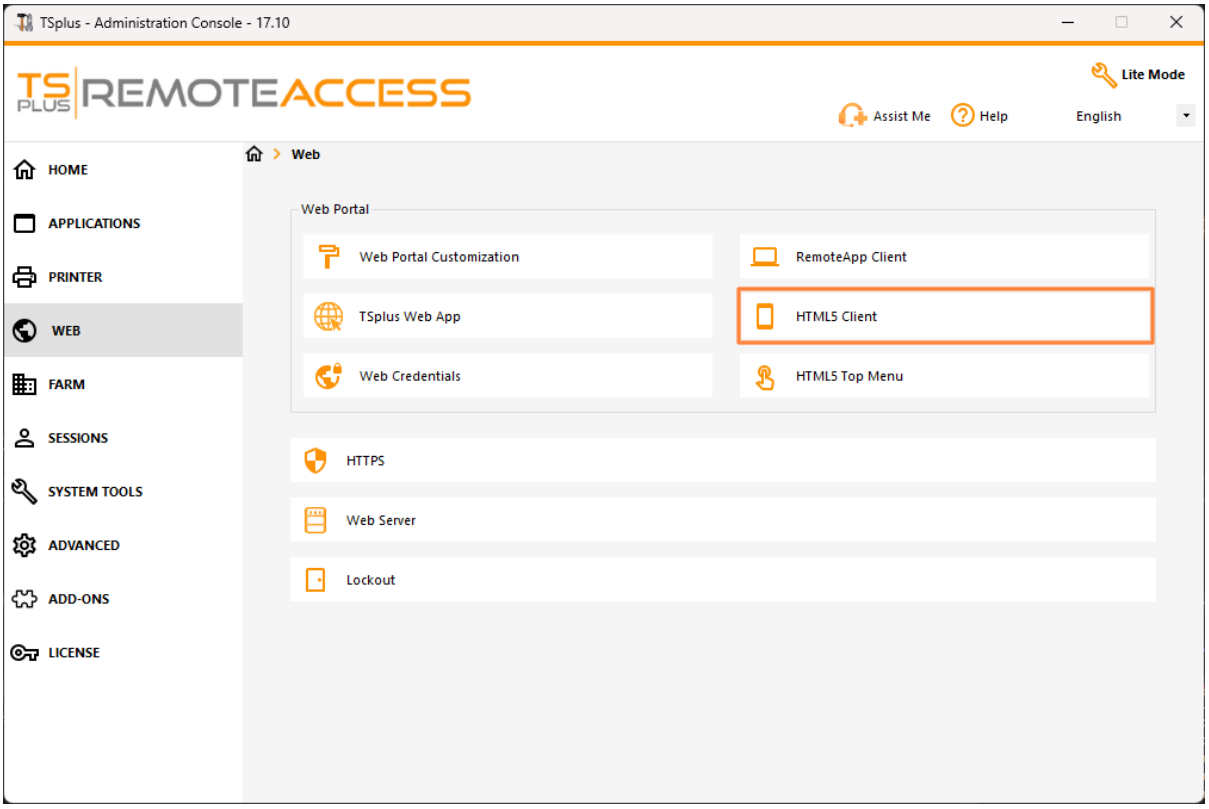


Diese Kachel ist für spezifische Einstellungen von Windows-Clients.

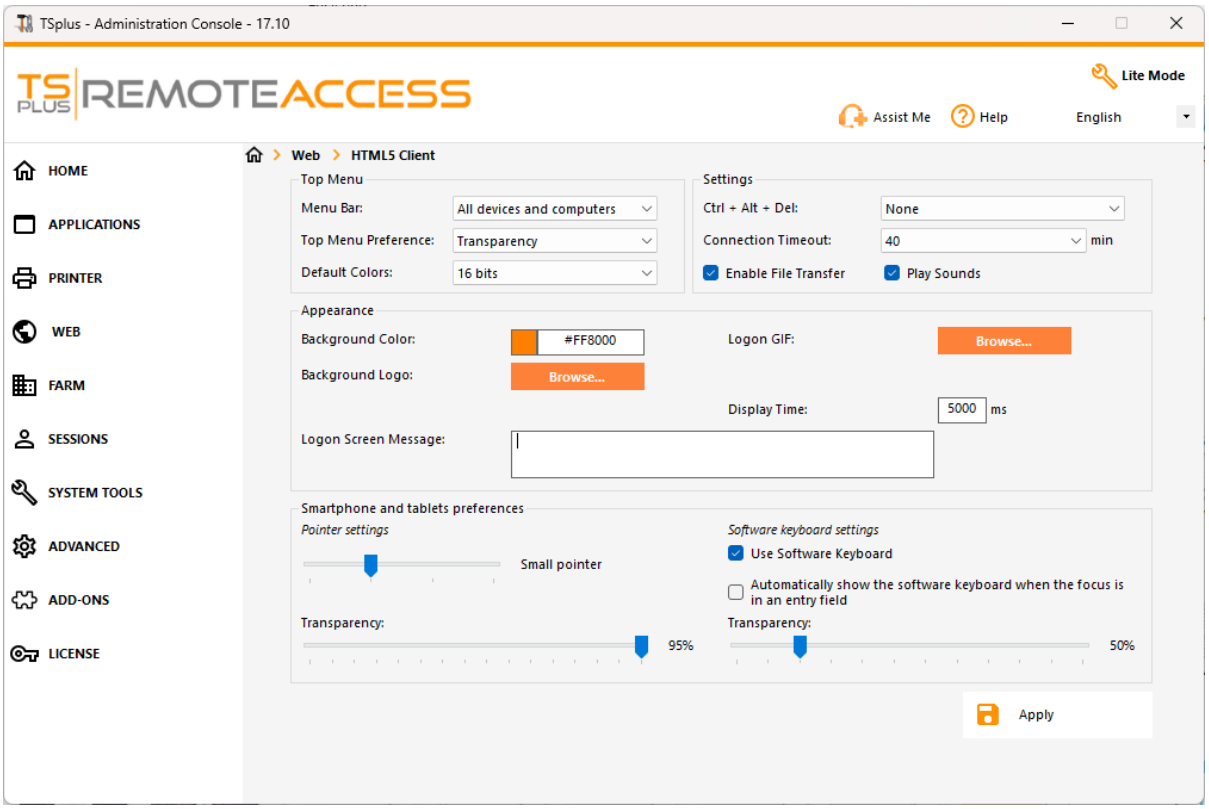
Sie können Ihre Anzeige zwischen RemoteApp (Fernverbindung ohne den Remote-Desktop) oder Standard-RDP wählen. Sie können auch entscheiden, ob Dokumente auf dem Standarddrucker des Benutzers, eine lokale Vorschau oder die Auswahl des lokalen Druckers gedruckt werden sollen.



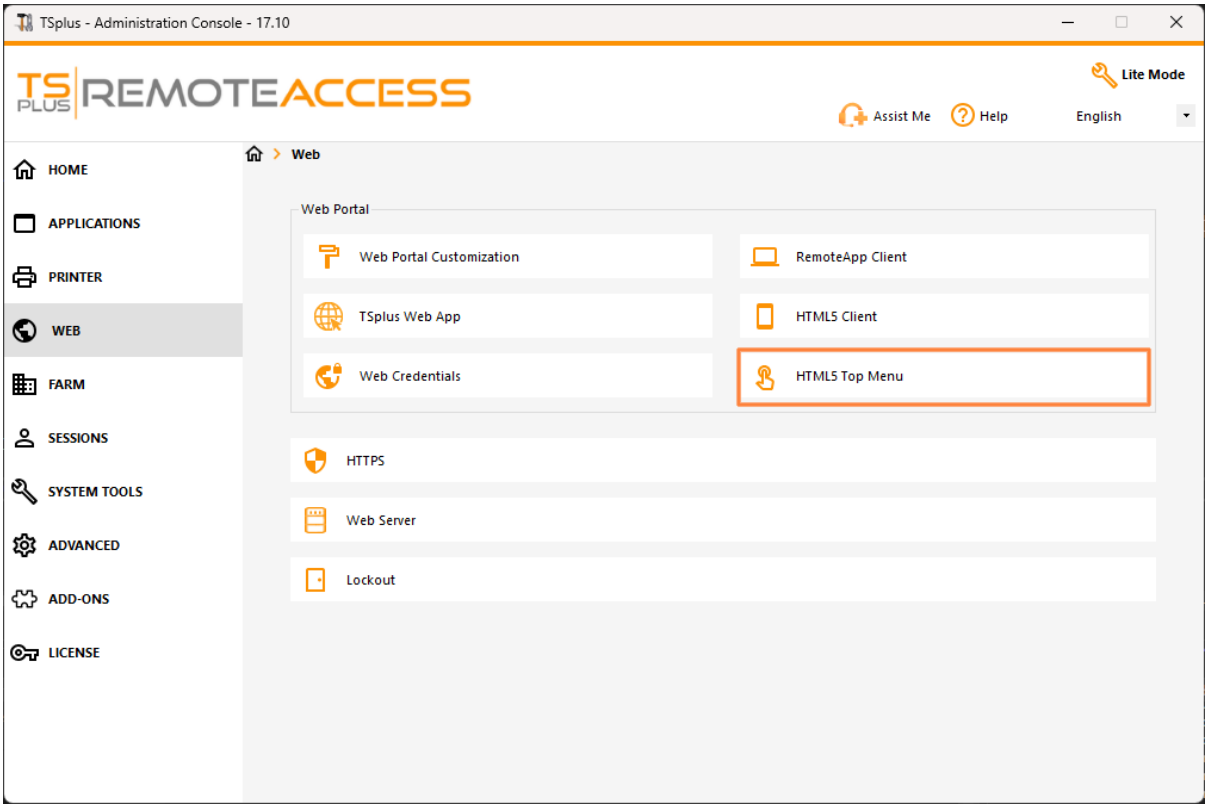
HTML5-Client-Kachel



Auf diesem Kachel können Sie die Parameter für die HTML5-Client-Webanzeige bearbeiten. Weitere Informationen zu diese Seite .



HTML5 Top-Menüfliese



Diese Kachel ermöglicht es Ihnen, die Anwendungen auszuwählen, die auf Ebene 1 oder 2 im oberen Menü Ihrer generierten Remote-Websitzung angezeigt werden sollen. Sie können diese

Anwendungen auch bearbeiten, damit sie auf einem bestimmten Clienttyp angezeigt werden: PC, mobil, iOS… oder auf allen.

