

Handbuch

Remote HMI V7 Industrial-Grade Thin-Client Firmware



Betriebsanleitung Version:	01.00.00
Ausgabe:	25.04.2025

Inhaltsverzeichnis

1	Über diese Dokumentation	7
1.1	Eingetragene Marken	7
1.2	Zielgruppe	7
1.3	Gestaltungsmerkmale im Text	7
1.4	Kontaktdaten	8
2	Beschreibung	9
2.1	Funktion	9
2.2	Lizenzmodelle	10
2.3	Konfigurationsdatei	10
2.4	Unterstützte Remote-Protokolle	10
2.4.1	RDP	11
2.4.2	VNC	11
2.4.3	KVM over IP	12
2.4.4	Kamera und Internet	12
2.5	Sicherheitskonzept	12
2.5.1	Systemschutz	12
2.5.2	Benutzerrollen	13
2.6	Display-Auflösungen	14
2.7	Bedienoberfläche	15
2.7.1	Register	18
2.7.2	Informationen	18
2.7.3	Basiseinstellungen	19
2.7.4	Status der Ethernet-Verbindung	19
2.7.5	Applikationen	20
2.7.6	Adressbuch	21
2.7.7	Bedienelemente	21
2.7.7.1	Virtuelle Tastatur	22
2.7.8	Anmelden	23
2.8	Remote HMI Device Manager	24
3	Schnell-Start	25
3.1	Netzwerk-Adapter einrichten	25
3.2	Remote-Verbindungen einrichten	26
3.2.1	Remote Verbindungen einrichten	26
3.2.2	RDP-Verbindung einrichten	28
3.2.3	VNC-Verbindung einrichten	29
3.2.3.1	Host für die VNC-Verbindung vorbereiten	30

3.2.3.2	Thin-Client vorbereiten	30
3.2.4	Thin-Client einrichten	31
3.2.5	KVM over IP-Verbindung einrichten	31
3.2.6	Kamerverbindung einrichten	32
3.2.7	Öffnen des Web Browsers im Kioskmodus	33
3.3	Remote-Verbindung testen.....	33
3.4	Benutzerrollen aktivieren	34
3.5	Weitere Möglichkeiten zur Konfiguration.....	34
4	Erste Schritte für den Operator	35
4.1	Startmenü.....	35
4.2	Virtuelle Tastatur nutzen.....	37
4.3	Remote-Verbindung starten.....	40
4.4	Settings im Dashboard nutzen.....	42
4.4.1	Touchscreen kalibrieren.....	43
4.4.2	Helligkeit des Displays anpassen.....	44
4.4.3	Kontextmenü am Touchscreen öffnen.....	45
4.4.4	Touchscreen reinigen.....	45
4.5	Applikationen starten	46
4.6	Status der Ethernet-Verbindung aufrufen	47
4.7	Multi-Display nutzen	47
5	Adressbuch	48
5.1	Optionen im Adressbuch	48
5.2	Remote Verbindungen einrichten	50
5.2.1	RDP-Verbindung einrichten.....	51
5.2.2	VNC-Verbindung einrichten.....	52
5.2.3	Host für die VNC-Verbindung vorbereiten	53
5.2.4	Thin-Client für die VNC-Verbindung vorbereiten	53
5.3	Remote-Verbindung testen.....	54
5.4	Remote-Verbindungen verwalten	54
6	App-Verwaltung.....	56
6.1	Optionen im Register Applications.....	56
6.2	Apps hinzufügen.....	58
6.3	Apps verwalten.....	60
7	Netzwerk	62
7.1	Optionen im Register Networks	62
7.2	Adapter Informationen	63
7.3	Über DHCP	63

7.4	Über DNS	64
7.5	Netzwerk-Adapter einrichten	64
7.6	Teaming-Funktion	65
8	Settings.....	67
8.1	Optionen im Register Settings	67
8.2	Systeminformationen anzeigen	68
8.3	Maintenance.....	68
8.3.1	In den Admin-Account der Windows-Oberfläche wechseln	70
8.3.2	System neu starten	70
8.3.3	System herunterfahren.....	70
8.3.4	Advanced Startup	71
8.3.5	Einstellungen zurücksetzen.....	71
8.3.6	Peripherie-Gerät koppeln oder hinzufügen.....	72
8.3.7	Event Log aufrufen.....	73
8.3.8	Pro-Lizenz aktivieren.....	74
8.3.9	Windows aktivieren	75
8.4	System- und Proxy-Einstellungen.....	77
8.4.1	Computernamen ändern	77
8.4.2	Datum-, Zeit- und Zahlenformat ändern	77
8.4.3	Stromverbrauch	77
8.4.4	Einstellungen für den Proxy-Server ändern.....	77
8.4.5	Remote-Zugriff konfigurieren.....	78
8.4.6	Anmeldedaten für den Admin-Account hinterlegen	78
8.5	Protection	79
8.5.1	Firewall und Virenschutz aktivieren	79
8.5.2	Schreibschutz für die SSD aktivieren	79
8.5.3	USB-Lockdown aktivieren	80
8.5.4	Systemverhalten bei Neustart konfigurieren.....	81
8.6	Display-Einstellungen	81
8.6.1	Display-Einstellungen anpassen	82
8.6.2	Multi-Display-Einstellungen anpassen.....	83
8.7	User Interface.....	83
8.7.1	Größe des Menüs und der virtuellen Tastatur verändern	83
8.7.2	Tastaturlayout ändern	84
8.7.3	Funktionen der Bedienoberfläche konfigurieren	85
8.7.4	Tastatur und Zeigegerät Sharing.....	85
8.7.5	Übernahme von Änderungen konfigurieren.....	86
8.8	Keyboard Wedge.....	87

8.8.1	Gerät hinzufügen	87
8.8.2	COM-Schnittstelle parametrieren	88
8.9	Access Control	89
8.9.1	Benutzerrollen aktivieren.....	89
8.9.2	Automatischen Logout aktivieren	90
8.10	Connections	90
8.10.1	Mehrere parallele Verbindungen erlauben	90
8.10.2	Verbindungen automatisch neu aufbauen	90
8.10.3	Status des Host automatisch prüfen.....	91
8.11	Import und Export	91
8.11.1	Gerätedatei importieren	92
8.11.2	Gerätedatei exportieren	93
8.12	Firmware updates.....	94
8.12.1	Firmware-Update durchführen	94
9	Gewusst wie	96
9.1	Störungen beheben	96
9.2	VNC-Server-Dienst auf dem Host aktivieren.....	98
9.2.1	VNC-Server-Parameter	98
9.3	DRDC-Client-Verbindung	99
10	Digitale Signatur.....	100
10.1	Digitale Signatur von Programmen der R. STAHL HMI Systems	100
10.2	Überprüfung der digitalen Signatur	100
10.3	Details der digitalen Signatur.....	101
10.4	Überprüfung des Zertifikats	102
10.5	Quelle.....	102

1 Über diese Dokumentation

Die Dokumentation beschreibt die Einrichtung und Verwendung der Remote HMI V7 Firmware, kurz Firmware genannt.

Zur Konfiguration der Firmware und Verwaltung der Lizenzen ist der Remote Device Manager verfügbar, kurz Device-Manager genannt.

1.1 Eingetragene Marken

Die in dieser Dokumentation genannten Produkte und Dienste sind eingetragene Marken und damit Eigentum der jeweiligen Hersteller.

1.2 Zielgruppe

Diese Dokumentation richtet sich an Administratoren und Betriebsingenieure, die die Berechtigung haben, HMI-Systeme zu parametrieren und die Remote-Verbindungen einzurichten.

1.3 Gestaltungsmerkmale im Text

Diese Dokumentation verwendet folgende Symbole, Auszeichnungen und Hinweise:

HINWEIS	
Hinweise zur Systemsicherheit und zur Vermeidung von Datenverlust.	
	Wichtige Informationen zum Verständnis oder Optimieren von Arbeitsabläufen.
	Hinweise auf Funktionen der Pro-Lizenz

- Aufzählung

Überschrift einer Handlungsanweisung

1. Auszuführender Arbeitsschritt
Zwischenergebnis
 2. Auszuführender Arbeitsschritt
- Ergebnis der Handlung

Apply

kennzeichnet einen Button in der Oberfläche

Dashboard

kennzeichnet ein Register, Menü oder eine Funktion der Oberfläche

[F8]

kennzeichnet eine Taste der Tastatur

1.4 Kontaktdaten

R. STAHL HMI Systems GmbH

Adolf-Grimme-Allee 8

50829 Köln

Deutschland

Telefon: +49 221 76806-1200

Telefax: +49 221 76806-4200

Web-Adresse: r-stahl.com

Support Kontaktdaten

Telefon: +49 22176806-5000

E-Mail: Support.dehm@r-stahl.com

2 Beschreibung

2.1 Funktion

Die Remote HMI V7 Firmware ist eine für die Prozessindustrie entwickelte Thin-Client Software, die zusammen mit den Bediengeräten der SERIE 500 ausgeliefert wird. Mit der Firmware werden Remote-Verbindungen zu einem oder mehreren Workstations oder Application-Servern aufgebaut und abgesichert. So ist der Remote-Zugriff von einer Bedienstation auf eine oder mehrere Workstations oder Server möglich.

Systemfunktionen

Funktion	Beschreibung
Zugriffsrechte	3-stufige Zugriffsverwaltung Systemeinstellungen und Installation von Anwendungen nur durch den Administrator
Auto Connect	Automatischer Verbindungsaufbau mit dem Host nach dem Start
Diagnose-Funktion	Erkennen von Netzwerkausfällen oder Ausfällen des Hosts
Teaming (Backup)	Redundanz durch automatisches Umschalten auf einen anderen Netzwerkadapter
Netzwerk Test	Integrierte Ping-Funktionalität zur Überwachung der Remote-Verbindungen
Clean Touchscreen	Sperre der Touchscreen-Funktion zur Reinigung des Geräts
Touchscreen-Anpassung	Anpassung des Touchscreens durch den Bediener (Helligkeit, rechte Maustaste, Kalibrierung)
Pro Folgende Funktionen sind nur mit einer Pro-Lizenz verfügbar:	
Multi-Session-Betrieb	Parallele Remote-Verbindungen, die einen schnellen Wechsel zwischen den Verbindungen oder die gleichzeitige Darstellung auf einem geteilten Bildschirm erlauben
App-Verwaltung	Schneller Zugriff auf Applikationen und Anwendungsprogramme
Kameraverbindung	Einrichten einer Kameraverbindung auf dem HMI
Tastatur- und Zeigegerät Sharing	Gemeinsame Nutzung von Tastatur und Zeigegerät mit anderen HMI's

Einsatz mit den Geräteplattformen:

- GETAC Tablet F110 G6
ORCA xxA
SHARK i5 Siemens
MANTA mITX Apollo Lake

Die Geräte werden über die Ethernet-Schnittstelle in das Ethernet eingebunden. Die Anzahl der verfügbaren Ethernet-Adapter ist abhängig von der Geräteplattform.

Unterstützte Zeigegeräte

Als Zubehör sind verschiedene Zeigegeräte, wie Trackball, Joystick oder Touchpad erhältlich. Diese werden auch in Kombination mit Industrietastaturen von der Firmware unterstützt. Wenn Sie weitere Informationen benötigen, wenden Sie sich bitte an: R. STAHL HMI Systems GmbH.

2.2 Lizenzmodelle

Folgende Lizenzmodelle der Firmware sind für die Thin-Clients verfügbar:

- **Basis**
Grundlizenz zum Aufbau von Remote-Verbindungen und zur Konfiguration der Firmware sowie zum Import und Export von Einstellungen
- **Pro**
Lizenz-Erweiterung erlaubt das Nutzen und Verwalten von Applikationen, die Nutzung mehrerer simultaner Remote-Verbindungen, Keyboard-Sharing, Kameraverbindungen, den Import und Export von Einstellungen.

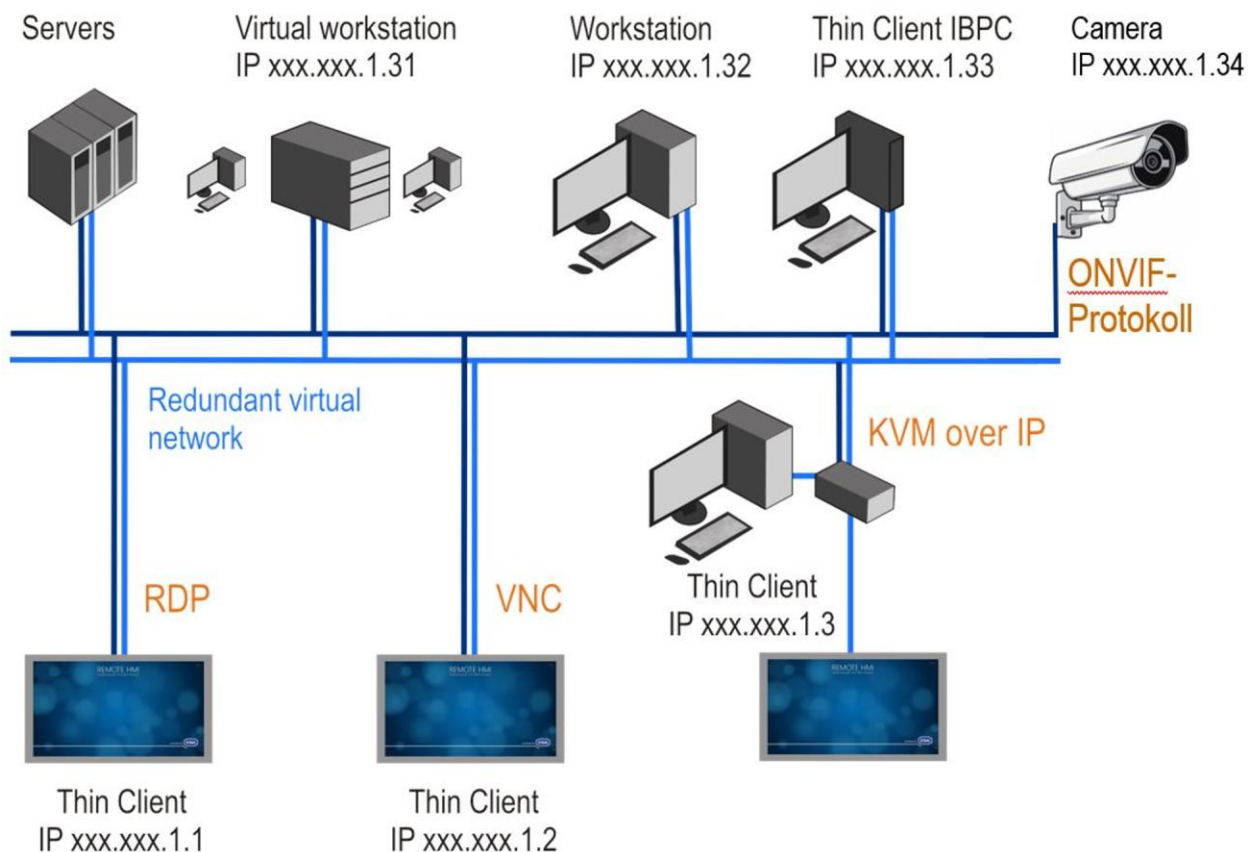
2.3 Konfigurationsdatei

Die Konfigurationsdatei enthält die Geräteparameter und Einstellungen des Thin-Client. Sie können nur am Thin-Client geöffnet werden.

Die Konfigurationsdatei "RemoteHMI.config" kann in das Root-Verzeichnis eines USB-Massenspeichers oder auf ein Netzlaufwerk exportiert werden. Die exportierte Datei ist verschlüsselt und kann zum Beispiel nach einem Reset oder in ein anderes Gerät importiert werden (siehe [8.11 Import und Export](#)).

2.4 Unterstützte Remote-Protokolle

Die HMI-Bedienstationen und Industrial-Box-PCs werden als Thin-Clients eingebunden und nutzen die im Netz verfügbaren Ressourcen. Abhängig von der Netzwerkarchitektur und den Zugriffsrechten kann über die IP-Adresse eine Remote-Verbindung zu jedem Ethernet-Teilnehmer aufgebaut werden. Die Firmware unterstützt das Remote Desktop Protocol (RDP), Virtual Network Computing (VNC) und Keyboard Video Mouse over Internet Protocol (KVM over IP). Über die Firmware kann der Thin-Client auf den verbundenen Workstations oder virtuellen Servern installierte Anwendungen aufrufen.



Im Beispiel ist ein redundantes virtuelles Netz dargestellt. Es verbindet die Thin-Clients über eine RDP-, VNC- oder KVM-over-IP-Verbindung mit den Workstations und Servern. Auf diese Weise kann jeder Thin-Client auf die verbundenen Systeme zugreifen und dort Anwendungen aufrufen.

2.4.1 RDP

Das Remote Desktop Protocol (RDP) ist ein Fernzugriffsprotokoll. Es ermöglicht das Darstellen und steuern des Bildschirminhalts einer entfernten Workstation. RDP ist integraler Bestandteil aller Windows-Betriebssysteme.

Für den RDP Zugriff wird auf dem Server eine eigene Session geöffnet, auf die nur der verbundene Client Zugriff hat.

Die Größe des dargestellten Bildschirminhalts wird durch die Displaygröße des Thin-Client bestimmt. Wenn der Bildschirminhalt nur auf einer Hälfte des Thin-Client dargestellt wird, wird er entsprechend skaliert.

Wenn mehrere RDP-Verbindungen auf einen Server zugreifen sollen, ist ein Windows Server erforderlich. Für den Zugriff auf den Windows-Server benötigt jeder Client eine Clientzugriffslizenz, um sich mit dem Server zu verbinden. Die Vergabe der Lizenzen ist abhängig vom Betriebssystem des Servers.

Zur Adressierung kann der Computernamen oder die IP-Adresse des Servers verwendet werden. Wenn Sie redundante Verbindungen ermöglichen wollen, empfehlen wir die Nutzung der Namensauflösung (DNS).

2.4.2 VNC

Virtual Network Computing (VNC) ist ein plattformunabhängig nutzbarer Server-Dienst. VNC arbeitet nach dem Client-Server-Modell.

Der VNC-Server-Dienst zeigt den Bildschirminhalt eines entfernten PCs (Server) auf einem lokalen Rechner (Client) an. Der Client dagegen sendet die Tastatur- und Mausbewegungen an den entfernten Server. So können die Ressourcen, Anwendungen und Programme des Servers genutzt werden.

Die Displaygröße des Servers bestimmt die Größe des dargestellten Bildschirminhalts. Wenn das Serverdisplay ein anderes Seitenverhältnis als das Display des Thin-Client hat, wird der Bildschirminhalt gestaucht oder mit schwarzen Rändern dargestellt.

VNC erlaubt einen mehrfach Zugriff auf den Server. Die Anzeige der Clients wird dabei synchronisiert.

Auf dem ferngesteuerten PC (Host) muss der VNC-Server-Dienst installiert sein. Der Thin-Client greift über eine VNC-Viewer-Applikation auf den VNC-Server zu. Für die Installation und die Konfiguration des VNC-Dienstes auf dem Server und dem Client sind Administrationsrechte erforderlich. Für die VNC-Kommunikation zwischen Server und Client sind diese Rechte nicht erforderlich.

VNC-Server-Dienste sind von verschiedenen Anbietern erhältlich. Abhängig vom VNC-Server weisen diese Dienste unterschiedliche Funktionalitäten auf.



Ausführliche Informationen sowie die Beschreibung zum VNC-Server-Dienst können Sie der Dokumentation der jeweiligen Anbieter entnehmen.

Um eine VNC-Verbindung aufbauen zu können, muss der VNC-Server-Dienst auf dem Host aktiviert sein. Die zur Verbindung notwendige IP-Adresse bezieht der VNC-Server-Dienst aus den Einstellungen der Netzwerkverbindung des PC. Abhängig von der Konfiguration wird die IP-Adresse manuell festgelegt oder von einem DHCP-Server zugewiesen. Im Adressbuch der Firmware wird diese IP-Adresse als Server-IP der VNC-Verbindung festgelegt.

Der Verbindungsaufbau ist von der Einstellung im VNC-Server abhängig und erfolgt als:

- direkte Verbindung ohne Passwortabfrage
- Verbindung mit VNC-Passwort
- Verbindung mit Windows-Passwort

2.4.3 KVM over IP

KVM over IP ermöglicht den Remote-Zugriff auf Keyboard-Video-Mouse-Systeme (KVM). Bei diesen Systemen wird eine Workstation über eine externe KVM-over-IP-Box mit Tastatur, Maus und Monitor verbunden. Die KVM-over-IP-Box wird über die Ethernet-Schnittstelle in das Netzwerk eingebunden. Die Datenübertragung erfolgt im VNC-Protokoll. Für den Aufbau der Verbindung ist ein VNC-Server-Dienst installiert. Die zum KVM-System gehörende Workstation benötigt keinen Netzwerkanschluss und keine Softwareinstallation.

2.4.4 Kamera und Internet

Mit der Kameraoption wird über die Angabe der IP-Adresse eine Kamera ausgewählt. Diese Option ist nur in der PRO Lizenz möglich. Durch die Angabe einer Internetadresse öffnet sich ein Browserfenster über den gesamten Bildschirm. Es kann immer nur eine aktive Verbindung hergestellt werden.

2.5 Sicherheitskonzept

2.5.1 Systemschutz

Der Thin-Client ist als geschlossenes System auf Windows® 10 IoT Enterprise LTSC 2021 konzipiert.

Serienmäßig wird der Thin-Client mit dem Betriebssystem Windows 10 IoT Enterprise und aktiviertem Windows 10 LTSC ausgeliefert.

Wenn Windows 10 LTSC nicht aktiviert ist, zum Beispiel nach einem System-Recovery, kann die Aktivierung im Menü **Maintain** erfolgen (siehe [8.3.9 Windows aktivieren](#)).

Es wird empfohlen, die Firewall und den Virenschutz zu aktivieren und alle notwendigen Sicherheitsupdates zuzulassen.

Weitere Maßnahmen zum Schutz des Prozessnetzes müssen vom Betreiber sichergestellt werden.

Sicherheitsfunktionen im Überblick

Funktion	Beschreibung
Betriebssystem	Basierend auf dem Microsoft 10 IoT Enterprise LTSC 2019 / 2021
Remote-Desktop-Protocol	Microsoft RDP 10 mit Sicherheitsfunktionen
Firewall	Aktive Windows Firewall zum Schutz vor Netzwerkattacken
Unified Write Filter (UWF)	Schutz des Laufwerks vor Integration von Malware oder Korumpieren von Systemdateien
HORM	Schnellstart von einem Systemabbild
USB lockdown	Individuelle Sperrung oder Freigabe von USB-Ports für USB-Endgeräte und Sticks
Virenschutz	Aktiver Microsoft Defender zum Schutz vor Viren, Installation weiterer Virenschutzprogramme möglich
Zugriffsrechte	Verfügbare Remote-Verbindungen und Anwendungen über Benutzerrollen einstellbar

2.5.2 Benutzerrollen

Das Zugriffskonzept der Remote Firmware beruht auf drei Benutzerrollen. Diese sind hierarchisch strukturiert.

Benutzerrolle	Beschreibung
Operator (Standarduser)	Der Operator kann zwischen den Anzeigen der verbundenen Systeme wechseln und die Systeme remote bedienen. Dem Operator stehen die Basiseinstellungen zur Verfügung, er kann keine Änderungen an der Firmware vornehmen.
Engineer	Der Betriebsingenieur kann Remote-Verbindungen einrichten, parametrieren und löschen. Mit der Pro-Lizenz kann er bereits vorhandene Applikationen in der Firmware hinzufügen, aber nicht auf die Windows-Oberfläche des Thin-Client zugreifen. Folgende Einstellungen kann der Engineer vornehmen: • Displays • User Interface • Connections • Keyboard Wedge
Admin	Der Administrator hat volle Zugriffsrechte auf die Windows-Oberfläche des Thin-Client. Zusätzlich zu den Möglichkeiten des Betriebsingenieurs kann er Applikationen und Treiber von Drittanbietern auf dem Thin-Client installieren. Er kann das Netzwerk konfigurieren sowie Systemeinstellungen über die Remote HMI-Menü-Oberfläche hinaus vornehmen sowie in die reguläre Windows-Oberfläche als Admin einloggen. Folgende Einstellungen im Register Settings sind dem Administrator vorbehalten: • Maintenance • System & Proxy • Protection • Access Control • Export & Import • Update

Die Benutzerrollen Admin und Engineer können im Menü **Access Control** über Passwörter geschützt werden.

Beim ersten Start der Firmware sind die Benutzerrollen deaktiviert und die Firmware startet mit der Benutzerrolle Admin. Der Passwortschutz ist nicht aktiv.

HINWEIS

Zugriffskontrolle über Benutzerrollen "Admin" und "Engineer"

Der Zugriff über die Benutzerrollen Admin und Engineer sollte nur Mitarbeitern gestattet sein, die mit der Administration von Thin-Clients vertraut sind.

2.6 Display-Auflösungen

Für alle Verbindungsarten unterstützt der Thin-Client die Darstellung von nicht nativen Displayauflösungen. Bei nicht nativen Auflösungen entspricht die Video-Ausgabe des Servers nicht der tatsächlichen physikalischen Auflösung des Thin-Client-Displays. Auflösungen ab 640x480 (VGA) bis hin zu 2560x2048 (QSXGA) sind wählbar. Je nach Verbindungstyp und Displayauflösung ist das Darstellungs- und Skalierungsverhalten unterschiedlich.

Die unterstützten HMI-Plattformen stellen jede reguläre Server-Displayauflösung von VGA bis QSXGA korrekt dar. Das Seitenverhältnis wird unter Ausnutzung der maximal möglichen Displayauflösung beibehalten. Die Bedienbarkeit des Thin-Client über den Touchscreen ist auch bei auftretenden schwarzen Rändern sichergestellt.

Anzeige einer RDP-Verbindung

Die Video-Ausgabe des Servers wird standardmäßig mit der nativen Auflösung des Thin-Client gestartet.

Anzeige einer VNC-Verbindung

Die Video-Ausgabe des Servers wird standardmäßig in der maximal möglichen Größe unter Beibehaltung des korrekten Seitenverhältnisses dargestellt. Hierzu wird entweder per Hardware oder per Software skaliert, um die maximal mögliche Bildqualität sicherzustellen.

Server-Auflösungen oberhalb der nativen Thin-Client-Displayauflösung werden vollständig dargestellt. Bei starker Abweichung der Auflösung des Servers von der nativen Auflösung des Thin-Client, können kleine Strukturen nur eingeschränkt erkannt werden. Die Skalierung kann bei Bedarf angepasst werden, so dass das komplette Thin-Client-Display genutzt wird. Dabei kann es zu einer verzerrten Darstellung kommen.

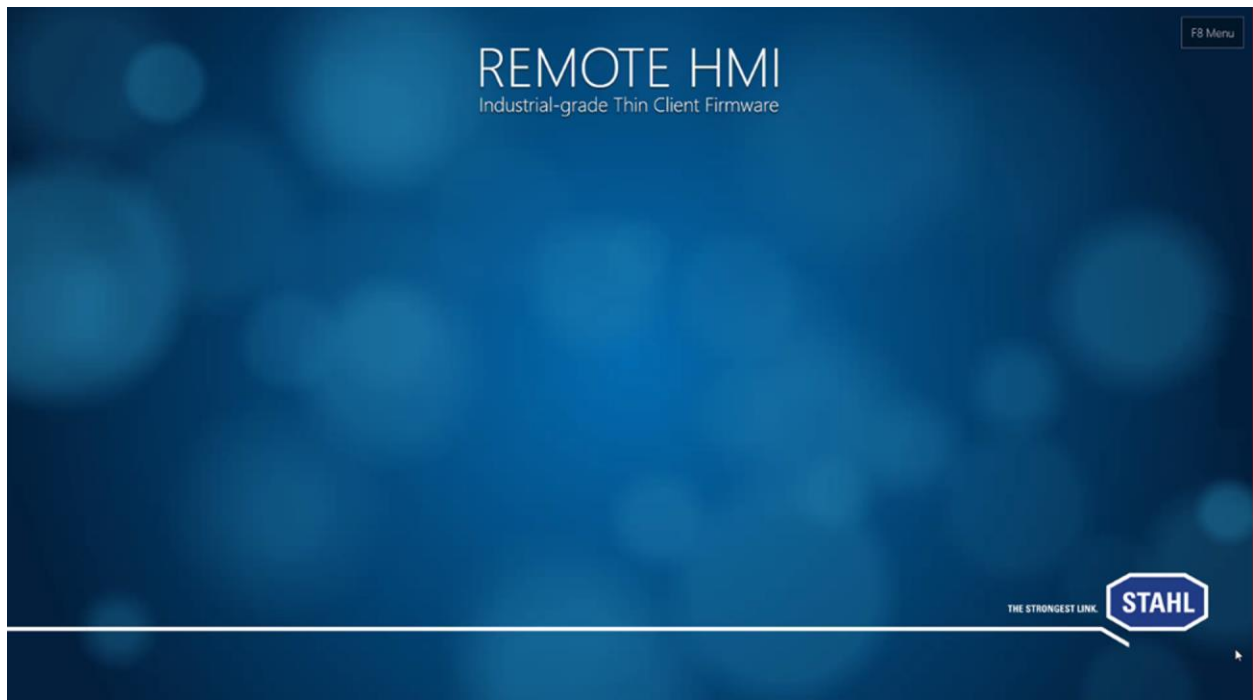
Anzeige einer KVM-over-IP-Verbindung

Die Video-Ausgabe des Servers wird vollständig in der maximal möglichen Größe unter Beibehaltung des korrekten Seitenverhältnisses dargestellt, solange die Server-Auflösung gleich oder unterhalb der nativen Thin-Client-Display-Auflösung liegt. Für die nicht nativen Auflösungen können schwarze horizontale und/oder vertikale Ränder erscheinen.

Bei Server-Auflösungen oberhalb der nativen Thin-Client-Displayauflösung schaltet der Thin-Client in den Panning-Modus. In diesem Fall ist nur ein Teil der Server-Bildausgabe zu sehen. Der Ausschnitt kann bei Anschlägen des Mauszeigers an eine Bildschirmkante verschoben werden.

2.7 Bedienoberfläche

Das System startet in folgendem Bildschirm.



Sie haben folgende Möglichkeiten, um das Dashboard zu öffnen:

- über den Button *F8 Menu*
- durch Drücken der Funktionstaste [F8/Fn] beim ORCA / [P2] bei Getac Tablet
- durch langes Drücken auf das Tastatur-Icon

Die Funktionstaste [F8] kann im Menü **User Interface** geändert werden.



Minimiertes Dashboard

- 1 Navigationselement, dieses führt zum erweiterten Dashboard
- 2 Schnellzugriff auf angelegte Remote-Verbindungen
- 3 Schnellzugriff auf Applikationen (verfügbar für Pro-Lizenz, wenn Applikationen installiert und freigegeben sind)
- 4 Benutzerrolle, Button öffnet den Anmeldedialog

Das erweiterte Dashboard ist abhängig von der System-Konfiguration.



Dashboard

- 1 Registerleiste
- 2 Systeminformationen
- 3 Basiseinstellungen für das HMI-Bedienterminal
- 4 Status der Ethernet-Verbindung
- 5 Benutzerrolle, Button öffnet den Anmeldedialog
- 6 Schnellzugriff auf Applikationen (verfügbar für Pro-Lizenz, wenn Applikationen installiert und eingerichtet sind)
- 7 Schnellzugriff auf angelegte Remote-Verbindungen
- 8 Hinweise zur Systemsicherheit

2.7.1 Register

In der Registerleiste sind folgende Funktionen verfügbar:

Register	Beschreibung
Dashboard	Übersicht über Adressbuch, System- und Verbindungsinformationen, Basisfunktionen und aktivierten Apps
Address Book	Diagnose und Verwaltung der Remote-Verbindungen
Applications	Anzeige und Verwaltung der Applikationen
Networks	Anzeige und Einrichtung der Netzwerk-Adapter
Settings	Menüs zur Anzeige und Einstellung von System-, Sicherheits- und Netzwerkparametern

2.7.2 Informationen

Die Systeminformationen enthalten folgende Daten:

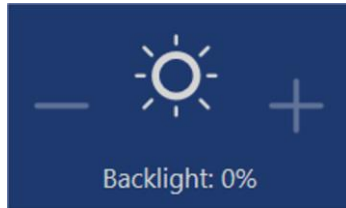
- **Date & Time** Datum und Uhrzeit
- **System** Daten zum Thin-Client
- **Free RAM** verfügbarer Speicher
- **User** aktuelle Benutzerrolle
- **Network 1** Status, IP-Adresse und Geschwindigkeit für Netzwerkadapter 1
- **Network 2** Status, IP-Adresse und Geschwindigkeit für Netzwerkadapter 2

2.7.3 Basiseinstellungen

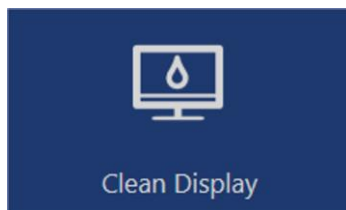
Die Basiseinstellungen enthalten Buttons zum Bedienen des Touchscreens. Wenn kein Touchscreen angeschlossen ist, sind die Funktionen ausgegraut.



Der Button startet die Kalibrierung des Touchscreens. Wenn zwei Touchscreens angeschlossen sind, können Sie jeden Touchscreen separat kalibrieren.



Der Button passt die Hintergrundbeleuchtung des Displays an.



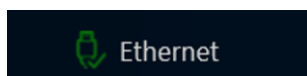
Der Button sperrt die Touchfunktion des Displays für 30 Sekunden. Dadurch wird das unbeabsichtigte Ausführen von Buttons zum Beispiel während der Reinigung verhindert.



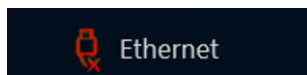
Der Button simuliert einen Rechtsklick auf dem Touchscreen, um zum Beispiel das Kontextmenü von Anwendungen aufzurufen.

2.7.4 Status der Ethernet-Verbindung

Die Anzeige gibt den Status der Ethernet-Verbindung wieder.



Ethernet-Adapter ist bereit



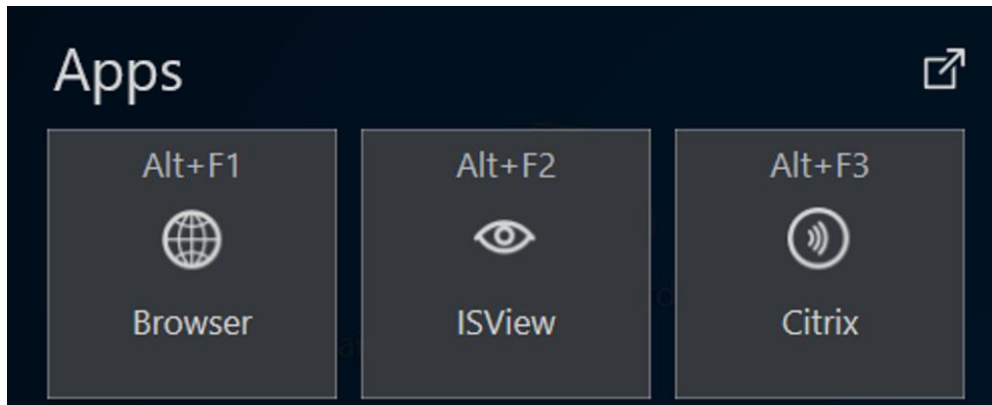
Ethernet-Adapter ist nicht bereit

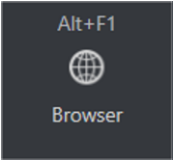
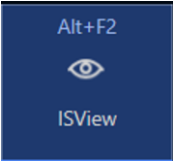
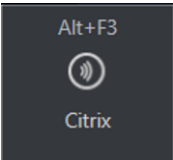


Adresskonflikt, Ethernet-Adapter ist nicht bereit

2.7.5 Applikationen

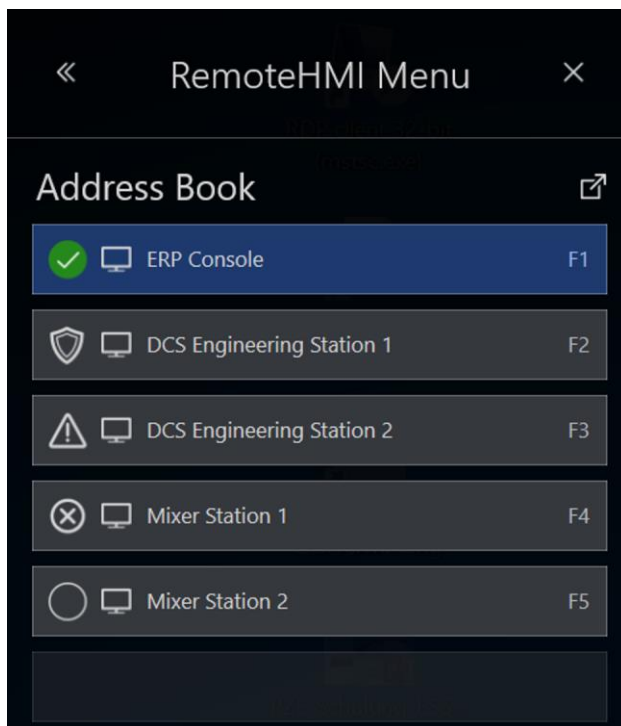
Applikationen können nur mit der Pro-Lizenz der Firmware genutzt werden. Wenn Anwendungen (Apps) eingerichtet wurden, werden diese als Button angezeigt. Es können mehrere Apps gestartet werden. Der Status der App wird angezeigt.



Anzeige	Bedeutung
	inaktive App
	aktive App
	im Hintergrund geöffnete App

2.7.6 Adressbuch

Die Remote-Verbindungen sind im Adressbuch wählbar.



Status der Remote-Verbindung

Symbol	Bedeutung
	verbunden
	nicht verbunden
	keine Verbindung möglich
	Default, wird beim Start automatisch verbunden
	verbunden, parallele Remote-Verbindung, im Hintergrund aktiv (für Multi-Session-Verbindungen ist eine Pro-Lizenz erforderlich)
	Auto-Reconnect, automatische Wiederverbindung

2.7.7 Bedienelemente

Elemente zur Navigation

	öffnet das erweiterte Dashboard
	minimiert das Dashboard
	springt zum Register oder Menü

Bedienelemente

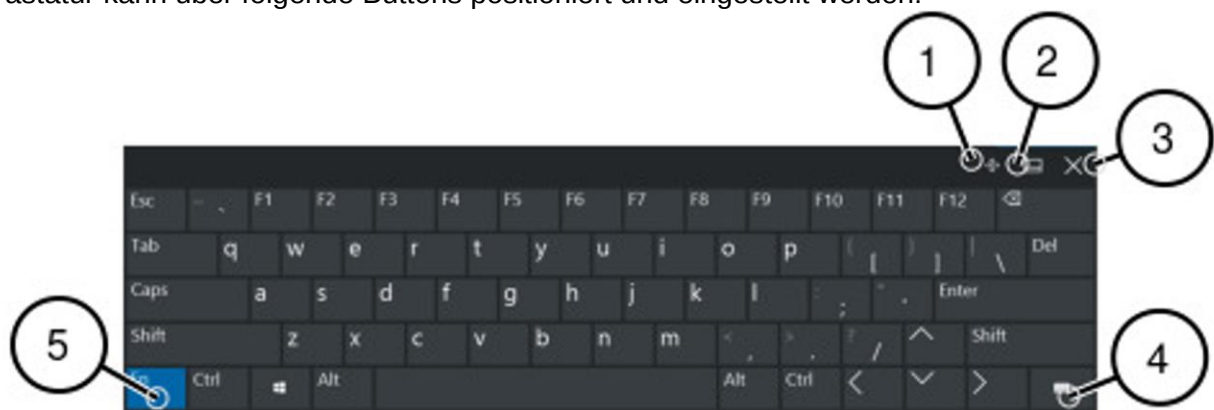
Abhängig vom Menü sind unterschiedliche Bedienelemente verfügbar.

Element	Bedeutung
	Schalter aktiviert
	Schalter deaktiviert
	Button Ein ausgegrauter Button steht nicht zur Verfügung
	Eingabefeld
	Schieberegler
	Checkbox aktiviert
	Checkbox deaktiviert

2.7.7.1 Virtuelle Tastatur

Der Thin-Client ist mit einer virtuellen Tastatur ausgestattet, wodurch eine Bedienung ohne weitere Eingabegeräte möglich ist.

Die virtuelle Tastatur besteht aus mehreren Tastaturblöcken. Diese können bei Bedarf ein- und ausgeblendet werden. Ebenso besteht die Möglichkeit, die Größenansicht der Tastatur zu verändern. Kontrolliert wird diese Funktionalität über den KEYBOARD Kontrollblock. Die Tastatur kann über folgende Buttons positioniert und eingestellt werden:



Gesamtansicht der virtuellen Tastatur (US-amerikanisches Tastaturlayout)

- 1 Erlaubt das freie Positionieren der Tastatur
- 2 Positioniert die Tastatur am unteren Rand
- 3 Schließt die Tastatur
- 4 Öffnet die Tastatur-Eigenschaften
- 5 Blendet die Funktionstasten ein

Die virtuelle Tastatur wird automatisch mit dem Booten des Thin-Client gestartet. Das Icon der virtuellen Tastatur erscheint am oberen Bildrand.

Bei einer aktiven Remote-Verbindung kann das Icon der virtuellen Tastatur an eine beliebige Position verschoben werden. Damit überdeckt die Tastatur nur weniger wichtige Teile der Applikation. Diese Position wird auch bei einer späteren Wiederherstellung der Remote-Verbindung wiederhergestellt. Die virtuelle Tastatur muss nicht erneut positioniert werden.

Tastaturkurzbefehle (Hotkeys)

Über den Touchscreen werden die Steuertasten Ctrl, Alt, Shift, Caps und Windows wie folgt genutzt:

- Taste wurde berührt, Farbe wechselt



- Funktion der Tasten wurde ausgeführt, Farbe wechselt zurück



Ohne Remoteverbindung sind alle Steuertastenkombinationen ohne Funktion.

Die Windows-Taste kann in Kombination mit einer weiteren Taste eine Funktion des Windows Betriebssystems nutzen. Bei doppelter Betätigung öffnet sie das Startmenü.

Für die Taste Caps ist auch auf der virtuellen Tastatur eine entsprechende LED vorhanden.

Mauszeiger

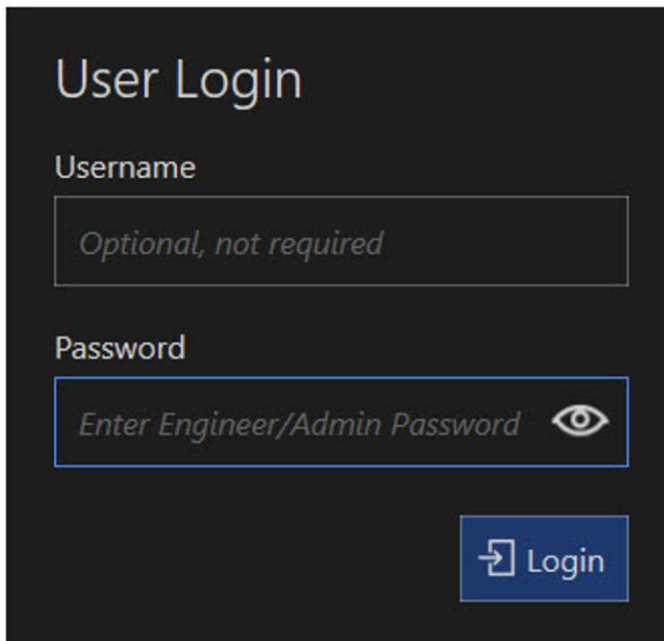
Bei KVM-over-IP- und VNC-Verbindungen stellt der Thin-Client zwei verschiedene Mauszeiger dar, die die Position der Maus auf dem Thin-Client oder Host anzeigen.

- Mauszeiger des Thin-Client: Punkt
- Mauszeiger des Host: Pfeil

Die Mauszeiger laufen asynchron. Abhängig von der Performance des VNC-Servers können sich Verzögerungen ergeben und der Remote-Zeiger "hinkt" hinterher.

2.7.8 Anmelden

Das Anmelden ist nur erforderlich, wenn die Benutzerrollen aktiviert sind. Der Operator hat ohne Anmeldung Zugriff auf das System.

A screenshot of a "User Login" interface. It has a dark background. At the top, the text "User Login" is displayed in a light blue font. Below it, there are two input fields. The first is labeled "Username" and contains the placeholder text "Optional, not required". The second is labeled "Password" and contains the placeholder text "Enter Engineer/Admin Password" along with an eye icon on the right side. At the bottom right, there is a blue button with a white arrow icon and the text "Login".

Durch Klicken auf das Augensymbol kann das Passwort unsichtbar eingegeben werden. Um das Passwort sichtbar zu machen, muss es gelöscht und erneut eingegeben werden.



Im Auslieferungszustand sind die Benutzerrollen deaktiviert und der *Admin* ist der Standard-Benutzer.
Bei aktivierten Benutzerrollen ist die Eingabe eines Passwortes für die Benutzerrollen *Engineer* und *Admin* erforderlich. Der Username wird nicht benötigt.

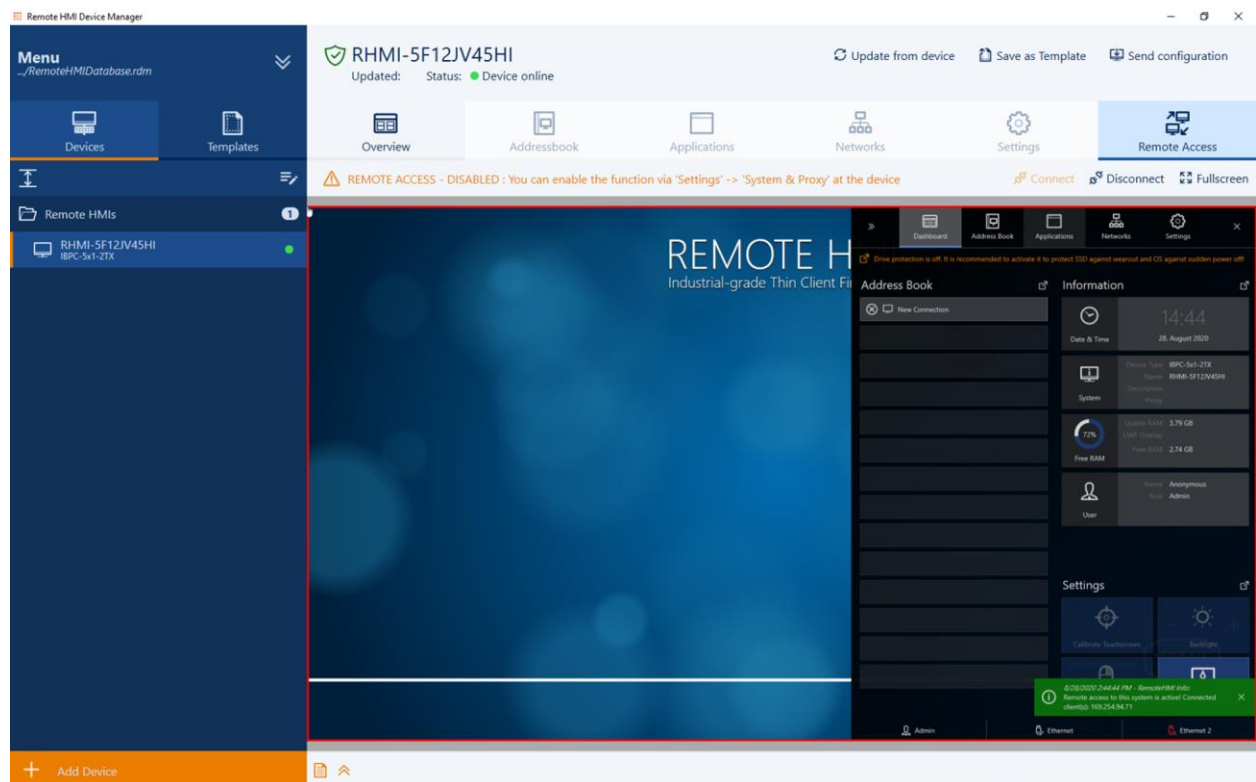
Benutzer wechseln

1. Öffnen Sie den **User Login**.
 2. Geben Sie das Passwort ein.
 3. Bestätigen Sie mit [Login].
- Das RemoteHMI-Menü öffnet sich.

2.8 Remote HMI Device Manager

Der Remote HMI Device Manager ergänzt die Firmware. Er wird zur zentralen Parametrierung der Firmware und zur Verwaltung der Lizenzen genutzt. Der Zugriff des Device-Managers muss in der Firmware im Menü **System & Proxy** freigegeben werden. Wenn der Zugriff freigegeben ist, können über Templates mehrere Thin-Clients mit gleichen Einstellungen konfiguriert und parametrisiert werden.

Darüber hinaus kann vom Device-Manager über die Funktion **Remote Access** auf den Thin-Client zugegriffen werden. Der Remote-Zugriff über VNC muss im Menü **System & Proxy** freigegeben werden.



Remote HMI Device Manager im Zugriff auf die Firmware eines IBPC

Bei der Parametrierung der Firmware findet keine „Live-Übertragung“ geänderter Einstellungen statt. Der Benutzer vor Ort kann jede Änderung ablehnen bzw. auf einen anderen Zeitpunkt verschieben.

3 Schnell-Start



Hinweis zum ersten Start

Die Firmware startet in der Benutzerrolle "Admin". Die Benutzerrollen und der Passwortschutz sind nicht aktiv. Aktivieren Sie nach Abschluss der Konfiguration die Benutzerrollen.

Sie haben folgende Möglichkeiten, um das Dashboard zu öffnen:

- über den Button *F8 Menu*
- durch Drücken der Funktionstaste [F8/Fn] / [P2]
- durch langes Drücken auf das Tastatur-Icon

Die Funktionstaste [F8] kann im Menü **User Interface** geändert werden.

Dashboard öffnen

1. Öffnen Sie im Startbildschirm das Remote-HMI-Menü.
2. Springen Sie über  direkt in das Adressbuch.
3. Oder öffnen Sie über den Doppelpfeil das erweiterte Dashboard.

3.1 Netzwerk-Adapter einrichten

Bei Auslieferung ist die automatische Adresszuordnung **Auto config via DHCP** aktiviert.

Netzwerk-Adresse automatisch einrichten

1. Öffnen Sie das Register **Networks**.
 2. Prüfen Sie ob **Auto config via DHCP** aktiviert ist.
 3. Klicken Sie auf *Apply*, um die automatische Zuordnung durch den DHCP-Server zu starten.
- IP-Adresse, Gateway und Subnetzmaske sind konfiguriert.

Netzwerk-Adresse manuell einstellen

1. Öffnen Sie das Register **Networks**.
 2. Deaktivieren Sie **Auto config via DHCP**, um die Adresse manuell einzurichten.
 3. Geben Sie unter **Local IP address** die IP-Adresse des Netzwerk-Adapters ein.
 4. Geben Sie unter **Subnet Mask** die Subnetzmaske ein.
 5. Wenn der Thin-Client auf ein anderes Netzwerk zugreifen soll, geben Sie unter **Gateway** die IP-Adresse des Gateway ein.
 6. Klicken Sie auf *Apply*, um die Änderungen zu übernehmen.
- IP-Adresse, Gateway und Subnetzmaske sind konfiguriert.

DNS-Server automatisch konfigurieren

1. Öffnen Sie das Register **Networks**.
 2. Aktivieren Sie **Auto DNS Server Addresses**, um die automatische Adresszuordnung zu aktivieren.
 3. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
- Die IP-Adressen der gefundenen DNS-Server werden eingetragen.

DNS-Server manuell konfigurieren

1. Öffnen Sie das Register **Networks**.
2. Geben Sie unter **Primary DNS Server** die IP-Adresse des ersten DNS-Servers ein.
3. Geben Sie unter **Secondary DNS Server** die IP-Adresse des zweiten DNS-Servers ein.
4. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.

3.2 Remote-Verbindungen einrichten

3.2.1 Remote Verbindungen einrichten

Automatischer Logon am Server

Die automatische Anmeldung am Server kann in den Einstellungen der Remote-Verbindung konfiguriert werden. Hierfür müssen Sie den Benutzernamen und das Passwort für den Server kennen.



Nur Benutzer, die die Berechtigung haben, remote auf den Server zu zugreifen, können sich am Server anmelden. Prüfen Sie die Berechtigung des Benutzers auf dem Server bzw. der KVM-Box.

Displayposition der Remote-Verbindung

Folgende Darstellungsoptionen sind möglich:

Symbol	Bezeichnung	Bedeutung
	Full display	zeigt den vollen Bildschirm an
	Left display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen auf der linken Seite an
	Right display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen auf der rechten Seite an
	Upper display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen oben an
	Lower display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen unten an
	Bottom left corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der unteren linken Ecke an
	Bottom right corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der unteren rechten Ecke an
	Top left corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der oberen linken Ecke an
	Top right corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der oberen rechten Ecke an
	Picture in picture	Skaliert den Bildschirminhalt einer Kamera und zeigt diesen immer im Vordergrund an freier Position an. Diese Option steht nur für Kameras zur Verfügung.

Verhalten der Firmware bei Verlust der Verbindung

Das Verhalten der Remote-Verbindung bei Neustart oder Verlust der Verbindung kann wie folgt konfiguriert werden:

Auto connect on system startup	 On	Stellt bei Neustart automatisch eine Verbindung her, wird durch das Symbol  im Adressbucheintrag angezeigt
	 Off	Bei Neustart muss der Verbindungsaufbau manuell gestartet werden
Auto reconnect on connection loss	 On	Stellt bei Verlust der Verbindung automatisch eine Verbindung her, wird durch das Symbol  im Adressbuch angezeigt.
	 Off	Bei Verlust der Verbindung muss der Verbindungsaufbau manuell gestartet werden

Für Nutzer der Pro-Lizenz

Pro	Das System erlaubt die parallele Nutzung mehrerer aktiver Remote-Verbindungen (Multi-Session-Verbindungen). Während die eine Remote-Verbindung auf dem Bildschirm angezeigt wird, bleibt die andere Verbindung im Hintergrund aktiv. Im Adressbuch sind die Verbindungen wie folgt gekennzeichnet:  im Vordergrund aktive Verbindung  im Hintergrund aktive Verbindung
------------	--

Die parallele Nutzung mehrerer Remote-Verbindungen wird im Menü **Settings** unter **Connections** aktiviert. Siehe auch:

- [8.10.1 Mehrere parallele Verbindungen erlauben](#)

3.2.2 RDP-Verbindung einrichten

Zur Konfiguration benötigen Sie die IP-Adresse oder den Namen des Servers. Diese sind in den Systemeigenschaften des Servers abgelegt.

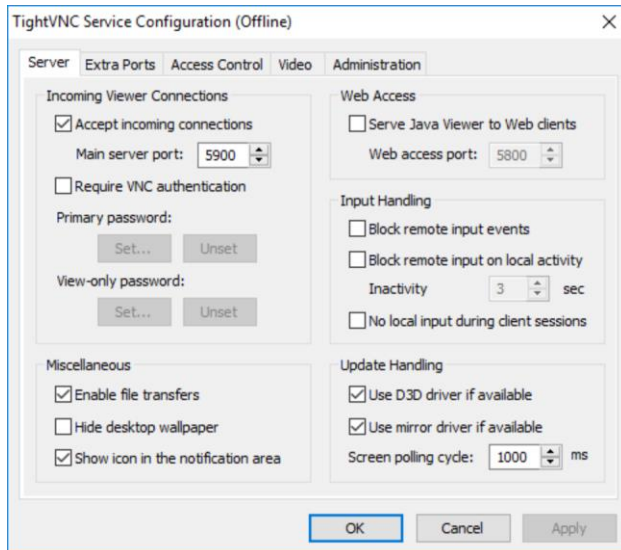


Der Remote-Zugriff muss für RDP-Verbindungen in den Systemeigenschaften des Servers explizit erlaubt werden. Der Remote-Zugriff muss für den Benutzer konfiguriert sein.

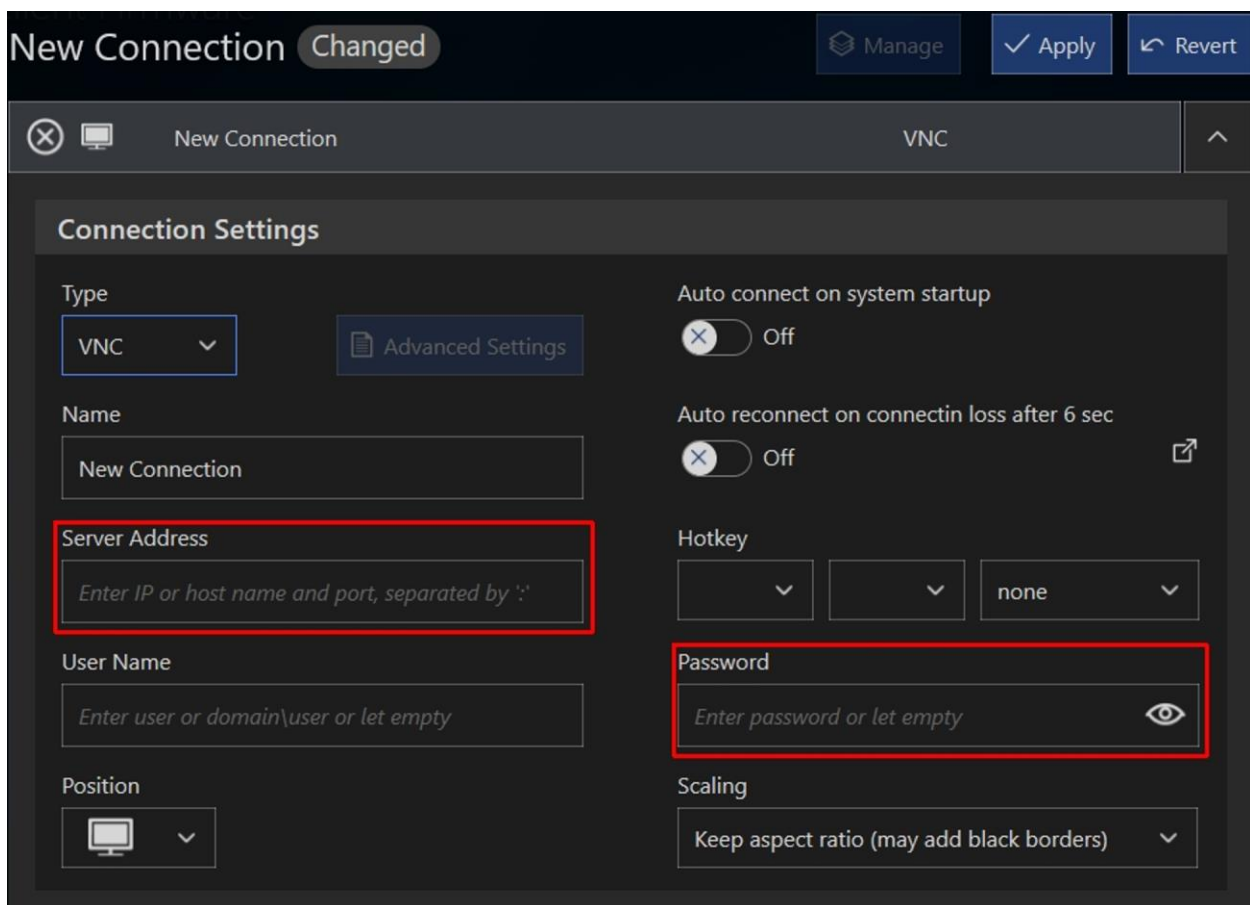
1. Öffnen Sie das Register **Address Book**.
2. Klicken Sie auf + *Add*.
Ein neuer Adressbucheintrag wird erzeugt.
3. Klicken Sie auf *Edit*.
4. Wählen Sie in den **Connection Settings** über das Drop-down-Feld **Type** "RDP".
5. Geben Sie unter **Name** die Bezeichnung für die Verbindung ein.
6. Tragen Sie unter **Server Address** die IP-Adresse oder den Namen des Servers ein.
 - HINWEIS:
Um den automatischen Zugriff auf den verbundenen Server zu gewährleisten, müssen Sie die korrekten Anmeldedaten hinterlegen. Beachten Sie, dass möglicherweise ein Domänenname mit dem Benutzernamen verwendet werden muss.
7. Geben Sie unter **User Name** und **Password** die Anmeldedaten des Servers ein.
8. Wenn der Aufruf der Remote-Verbindung über die Tastatur möglich sein soll, legen Sie unter **Hotkey** einen Tastaturkürzel an.
9. Wählen Sie unter **Show on** die Anzeigeeoption.
10. Legen Sie die minimale Benutzerrolle für den manuellen Aufbau der Verbindung fest.
 - HINWEIS:
Hat der Benutzer keine Berechtigung die Verbindung aufzubauen, ist diese im Adressbuch ausgegraut.
11. Klicken Sie auf *Apply*, um die Verbindung einzurichten.
 - Die Verbindung wird im Adressbuch angezeigt.

3.2.3 VNC-Verbindung einrichten

Auf dem Thin-Client ist ein VNC-Client vorinstalliert. Der VNC-Server-Dienst muss auch auf dem Server installiert sein. Die Installation erfordert Administrator-Rechte auf dem Host-PC und dem Server.



Um die Verbindung einzurichten, benötigen Sie die IP-Adresse des VNC-Servers und abhängig von der Konfiguration das VNC-Passwort.



3.2.3.1 Host für die VNC-Verbindung vorbereiten

Die Vorgehensweise ist abhängig vom VNC-Server-Dienst. Nähere Informationen sind der Hersteller-Dokumentation zum VNC-Server-Dienst zu entnehmen.

HINWEIS

Für den Vorgang sind Administratorrechte erforderlich.

1. Stellen Sie sicher, dass der Host vom Thin-Client erreicht werden kann. Wenn beide im selben Netzwerk sind, ist das grundsätzlich der Fall.
 2. Stellen Sie sicher, dass der VNC-Server-Dienst auf dem Host installiert und aktiviert ist (siehe [9.2 VNC-Server-Dienst auf dem Host aktivieren](#)).
 3. Wenn die Netzwerkverbindung über eine Firewall abgesichert ist, müssen Sie die Firewall konfigurieren. Erlauben Sie die Netzwerk-Kommunikation über den Port, auf dem der VNC-Server-Dienst empfangsbereit ist (standardmäßig 5900).
 4. Wenn die Netzwerkverbindung über einen Router abgesichert ist, müssen Sie den Router konfigurieren. Stellen Sie für die Weiterleitung der Netzwerk-Kommunikation jeden konfigurierten Port ein, auf dem der VNC-Server-Dienst empfangsbereit ist (standardmäßig 5900).
 5. Prüfen Sie, ob der VNC-Server-Dienst ordnungsgemäß arbeitet und eingehende Verbindungen akzeptiert.
- Der Host ist vorbereitet.

3.2.3.2 Thin-Client vorbereiten

Die Vorgehensweise ist abhängig vom VNC-Server-Dienst. Nähere Informationen sind der Hersteller-Dokumentation zum VNC-Server-Dienst zu entnehmen.

HINWEIS

Für den Vorgang sind Administratorrechte erforderlich.

1. Stellen Sie sicher, dass der Thin-Client den Host erreichen kann. Wenn beide im selben Netzwerk sind, ist das grundsätzlich der Fall.
 2. Wenn die VNC-Verbindung des Thin-Client über einen Proxy-Server abgesichert ist, müssen Sie im VNC-Viewer den Proxy-Server angeben.
- Der Thin-Client ist vorbereitet.

3.2.4 Thin-Client einrichten



Wenn die Port-Nummer des VNC-Servers vom Standardport abweicht, muss die IP-Adresse um die Port-Nummer erweitert werden, zum Beispiel:
192.168.1.23:5901

1. Öffnen Sie das Register **Address Book**.
2. Klicken Sie auf **+Add**.
Ein neuer Adressbucheintrag wird erzeugt.
3. Klicken Sie auf **Edit**.
4. Wählen Sie in den **Connection Settings** über das Drop-down-Feld **Type** "VNC".
5. Geben Sie unter **Name** die Bezeichnung für die Verbindung ein.
6. Tragen Sie unter **Server Address** die IP-Adresse des Servers ein.
 - HINWEIS:
Um den automatischen Zugriff auf den verbundenen Server zu gewährleisten, müssen Sie die korrekten Anmeldedaten hinterlegen.
7. Geben Sie die Anmeldedaten des Servers ein.
8. Wenn der Aufruf der Remote-Verbindung über die Tastatur möglich sein soll, legen Sie unter **Hotkey** einen Tastaturkurzbefehl an.
9. Wählen Sie unter **Show on** die Anzeigeeoption.
10. Legen Sie die minimale Benutzerrolle für den manuellen Aufbau der Verbindung fest.
 - HINWEIS:
Hat der Benutzer keine Berechtigung die Verbindung aufzubauen, ist diese im Adressbuch ausgegraut.
11. Klicken Sie auf **Apply**, um die Verbindung einzurichten.
 - ▶ Die Verbindung wird im Adressbuch angezeigt.

3.2.5 KVM over IP-Verbindung einrichten

Für den Verbindungsaufbau ist ein VNC-Server-Dienst erforderlich, dieser läuft auf der KVM-Box.

Um die Verbindung einzurichten, benötigen Sie die IP-Adresse des VNC-Servers und abhängig von der Konfiguration das VNC-Passwort.

1. Öffnen Sie das Menü **Address Book**.
2. Klicken Sie auf **+Add**.
Ein neuer Adressbucheintrag wird erzeugt.
3. Öffnen Sie den Adressbucheintrag.
4. Wählen Sie in den **Connection Settings** über das Drop-down-Feld **Type** "KVM".
5. Geben Sie im Feld **Name** die Bezeichnung für die Verbindung ein.
6. Tragen Sie im Feld **Server Address** die IP-Adresse der KVM-Box ein.
7. Geben Sie unter **User Name** und **Password** die Anmeldedaten der KVM-Box ein.
8. Wenn der Aufruf der Remote-Verbindung über die Tastatur möglich sein soll, legen Sie unter **Hotkey** einen Tastaturkurzbefehl an.
9. Wählen Sie unter **Show on** die Anzeigeeoption.

10. Legen Sie die minimale Benutzerrolle für den manuellen Aufbau der Verbindung fest.
 - HINWEIS:
Hat der Benutzer keine Berechtigung die Verbindung aufzubauen, ist diese im Adressbuch ausgegraut.
11. Klicken Sie auf *Apply*, um die Verbindung einzurichten.
 - ▶ Die Verbindung wird im Adressbuch angezeigt.

3.2.6 Kameraverbindung einrichten

The screenshot shows the 'Connection Settings' window with the following elements:

- Type:** A dropdown menu set to 'Camera' and an 'Advanced Settings' button.
- Auto connect on system startup:** A toggle switch set to 'Off'.
- Auto reconnect on connection loss:** A toggle switch set to 'Off'.
- Name:** A dropdown menu showing 'Scanning for cameras, found 10...' and a 'Scan for Cameras' button.
- Camera Address:** A text input field with the placeholder 'Enter IP or host name and port, separated by ':''.
- Hotkey:** Three dropdown menus, the last one set to 'none'.
- User Name:** A text input field with the placeholder 'Enter user or let empty'.
- Password:** A text input field with the placeholder 'Enter password or let empty' and a visibility icon.
- Camera Profile:** A dropdown menu set to 'No profile selected yet' and a 'Load Camera Profiles' button.
- Position:** A dropdown menu with a monitor icon.
- Scaling:** A dropdown menu set to 'Keep aspect ratio (may add black borders)'.

Das Bild zeigt einen Screenshot der Connection Settings Seite der Remote HMI Software. Die folgenden Optionen stehen zur Auswahl:

- ▶ **Name:** Hier kann der Anwender einer Kamera einen spezifischen Namen zuordnen, um die Identifizierung innerhalb der Software zu vereinfachen.
- ▶ **Camera Address:** Hier muss der Anwender die IP Adresse, URL oder Anschluss der Kamera eingeben. Dies ist für den Verbindungsaufbau nötig.
- ▶ **Username:** Zur verbesserten Sicherheit kann hier ein Benutzername mit Berechtigung zum Zugriff auf die Kamera definiert.
- ▶ **Camera Profile:** Der Anwender kann hier ein Kameraprofil auswählen oder definieren, mit Merkmalen wie z.B. Auflösung, Bildfrequenz oder anderen.
- ▶ **Position:** Hier wird für die Beobachtung bestimmter Bereiche die Position oder Ausrichtung der Kamera bestimmt.

- ▶ **Hotkey:** Für eine effizientere Bedienung können hier Hotkeys zum schnellen Zugriff auf die Kameraübertragung oder einzelne Funktionen definiert werden.
- ▶ **Password:** Dieses Feld ist zur Eingabe eines Passwortes für die Kamera vorgesehen, damit nur autorisierte Anwender Zugriff auf die Übertragung haben.
- ▶ **Scaling:** Hier kann die Skalierung angepasst werden, damit das Bild korrekt auf dem Display des HMI erscheint.

3.2.7 Öffnen des Web Browsers im Kioskmodus

Diese Option ermöglicht das Öffnen des Webbrowsers im Kioskmodus. Durch Eingabe der Internetadresse öffnet sich ein Browserfenster über den gesamten Bildschirm. Die Verbindung wird durch Eingabe des Verbindungsnamens oder der URL hergestellt. Es kann immer nur eine Verbindung genutzt werden.

3.3 Remote-Verbindung testen

Sie können die Remote-Verbindung im Adressbuch testen.

Remote-Verbindung starten

- Schließen Sie die Einstellungsmaske der Remote-Verbindung.
- Klicken Sie in der Liste auf die Remote-Verbindung, die Sie testen wollen.
- Wenn Sie einen Tastaturkürzbefehl konfiguriert haben, prüfen Sie, ob die Remote-Verbindung auch über die Tastatur startet.

Wenn eine Verbindung aufgebaut wurde, wechselt das Symbol zu .

Remote-Verbindung startet nicht

Wenn keine Verbindung aufgebaut werden konnte, wechselt das Symbol zu . Das System gibt eine Fehlermeldung aus.

- Prüfen Sie, ob Sie alle Einstellungen korrekt eingegeben haben.

Wenn der Host verfügbar ist, grenzen Sie das Problem über folgende Prüfungen ein:

RDP-Verbindung prüfen

1. Prüfen Sie in den Systemeinstellungen des Servers, ob eine RDP-Verbindung erlaubt ist.
2. Prüfen Sie, ob der Thin-Client als Benutzer am Server angelegt ist und die notwendigen Zugriffsrechte hat.

VNC-Verbindung prüfen

1. Prüfen Sie, ob der VNC-Server-Dienst richtig konfiguriert ist.
2. Prüfen Sie, ob die Port-Nummer korrekt angegeben ist.

KVM-over-IP-Verbindung prüfen

1. Prüfen Sie die Konfiguration der KVM-Box.
2. Prüfen Sie, ob die Port-Nummer korrekt angegeben ist.

3.4 Benutzerrollen aktivieren

Benutzerrollen aktivieren

1. Öffnen Sie das Menü **Access Control**.
2. Aktivieren Sie unter **Main** die 3-stufige Zugriffskontrolle.
3. Aktivieren Sie **Limit Operator access to Dashboard**, um die Registerleiste im Dashboard für den Operator auszublenden.
Für den Operator sind nur noch die Daten im Dashboard sichtbar.
4. Geben Sie unter **Login Passwords** unterschiedliche Passwörter für die Benutzerrollen "Engineer" und "Admin" ein.
5. Wiederholen Sie die Passworteingabe. Wenn die Passwörter falsch sind, gibt das System eine Fehlermeldung aus.
6. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
 - Die Benutzer "Engineer" und "Admin" müssen sich mit ihrem Passwort anmelden.

3.5 Weitere Möglichkeiten zur Konfiguration

Protection

In diesem Menü können Sie die Firewall, den Virenschutz, den UWF-Filter aktivieren und die Nutzung von USB-Geräten blockieren. Siehe auch:

- [8.5.1 Firewall und Virenschutz aktivieren](#)
- [8.5.2 Schreibschutz für die SSD aktivieren](#).
- [8.5.3 USB-Lockdown aktivieren](#)
- [8.5.4 Systemverhalten bei Neustart konfigurieren](#)

Display

In diesem Menü können Sie die Darstellung auf dem Display anpassen oder einen Bildschirmschoner aktivieren. Siehe auch:

- [8.6.1 Display-Einstellungen anpassen](#)
- [8.6.2 Multi-Display-Einstellungen anpassen](#), wenn zwei Displays am Thin-Client angeschlossen sind.

Für Nutzer der Pro-Lizenz

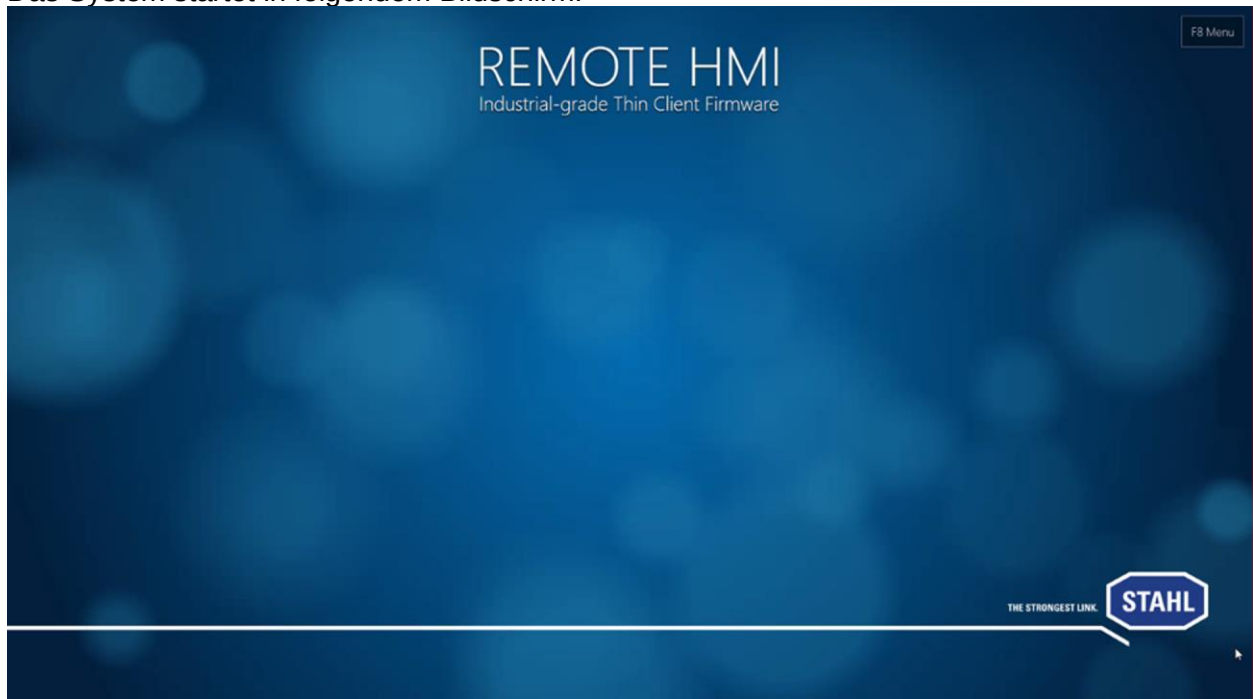
Damit Benutzer die Anwendungen auf dem Thin-Client nutzen können, müssen Sie die Anwendungen installieren und im Register **Applications** einen Link hinzufügen. Siehe auch:

- [6.2 Apps hinzufügen](#)

4 Erste Schritte für den Operator

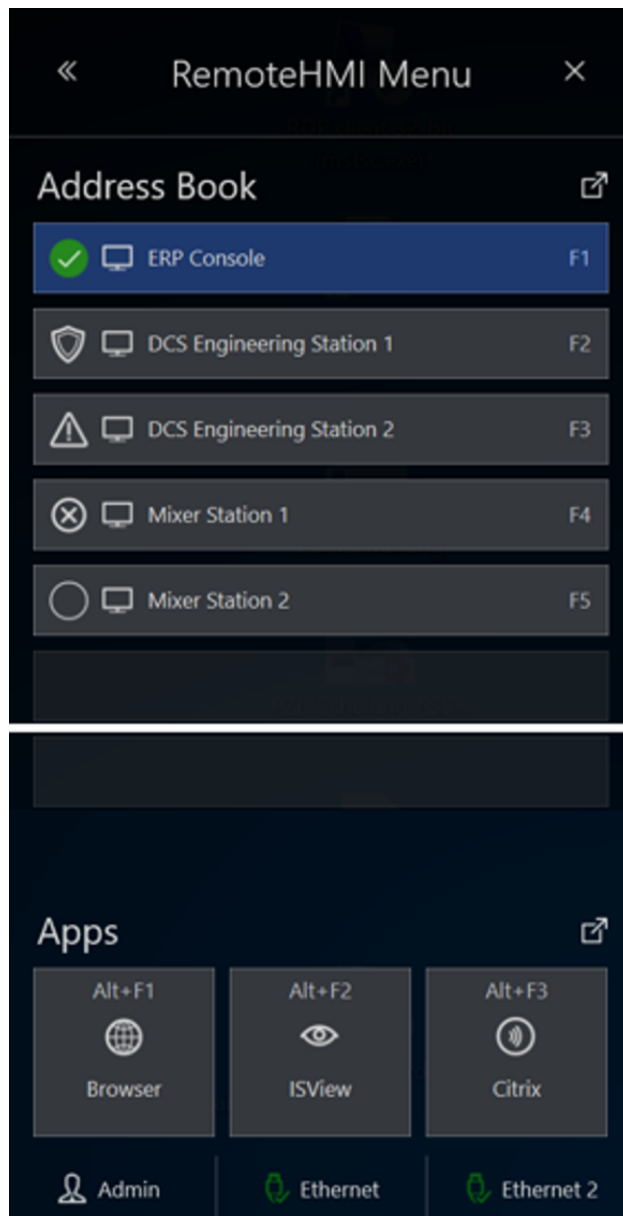
4.1 Startmenü

Das System startet in folgendem Bildschirm.



Dashboard öffnen

1. Klicken Sie im Startbildschirm auf den Button *F8 Menu*, drücken Sie die Funktionstaste [F8/Fn] / [P2] oder drücken Sie für mehrere Sekunden auf das Tastatur-Icon. Das minimierte Dashboard öffnet sich.



Elemente zur Navigation

◀◀ öffnet das erweiterte Dashboard

▶▶ minimiert das Dashboard

🔗 springt zum Register oder Menü

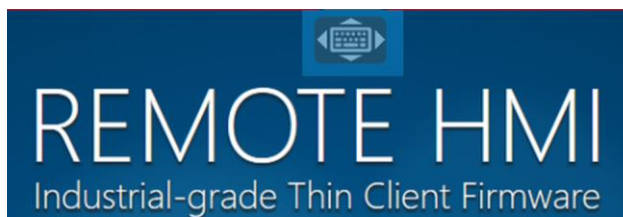
4.2 Virtuelle Tastatur nutzen

- Berühren Sie das Tastaturicon, um die Tastatur zu öffnen.
Wenn das Konfigurationsmenü aktiv ist, wird das Tastaturicon oberhalb der Menüleiste angezeigt.
Wenn eine Remote-Verbindung aktiv ist, wird das Tastaturicon am oberen rechten Bildrand angezeigt.



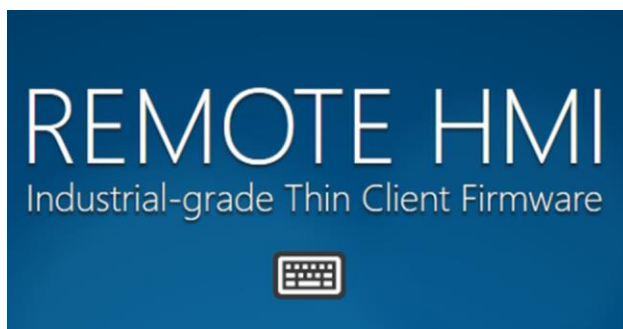
Icon der virtuellen Tastatur verschieben

- Bewegen Sie den Mauszeiger auf das Tastaturicon.
- Berühren Sie mit der linken Maustaste das Tastaturicon und halten Sie es für einige Sekunden, bis der Cursor die Ansicht für die Objektverschiebung annimmt.



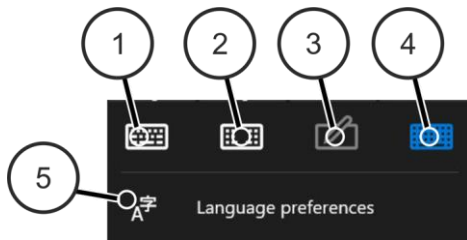
Das Tastaturicon in der Ansicht Objektverschiebung

- Verschieben Sie das Tastaturicon an die gewünschte Stelle.
► Die Position der Tastatur wird gespeichert. Beim nächsten Start der Remote-Verbindung wird die Tastatur dort positioniert.



Tastatur-Eigenschaften anpassen

- Berühren Sie das Tastaturicon, um die Tastatur zu öffnen.
- Berühren Sie die Taste .
Die Tastatur-Einstellung öffnet sich. Sie haben folgende Optionen:



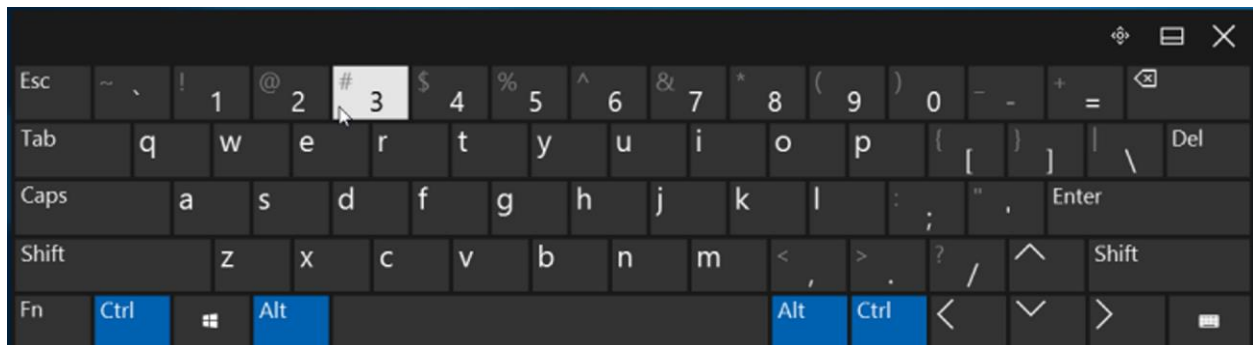
- 1 Zeigt die Tastatur ohne Steuerzeichen an
- 2 Zeigt die Tastatur zur Cursorsteuerung und Positionierung sowie die Sondertasten an
- 3 Öffnet die Handschrifterkennung
- 4 Zeigt die Tastatur mit allen Steuerzeichen an
- 5 Öffnet die Spracheinstellungen für die Tastatur



Die Windows-Taste kann in Kombination mit einer weiteren Taste eine Funktion des Windows Betriebssystems nutzen. Bei doppelter Betätigung öffnet sie das Startmenü.

Steuertasten Shift, Ctrl, Alt und Windows nutzen

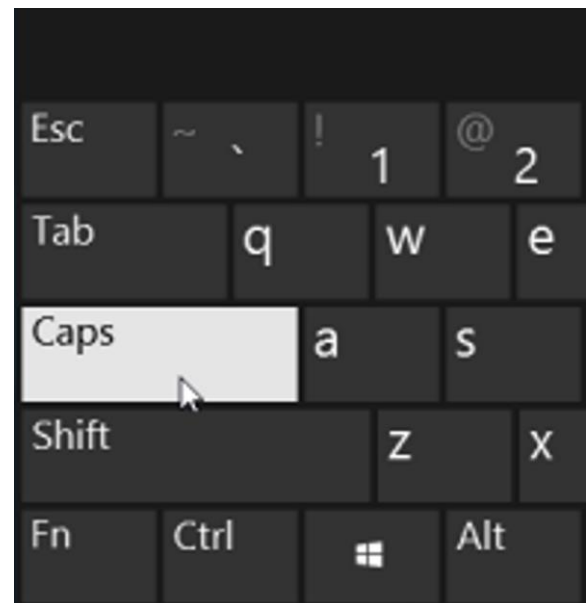
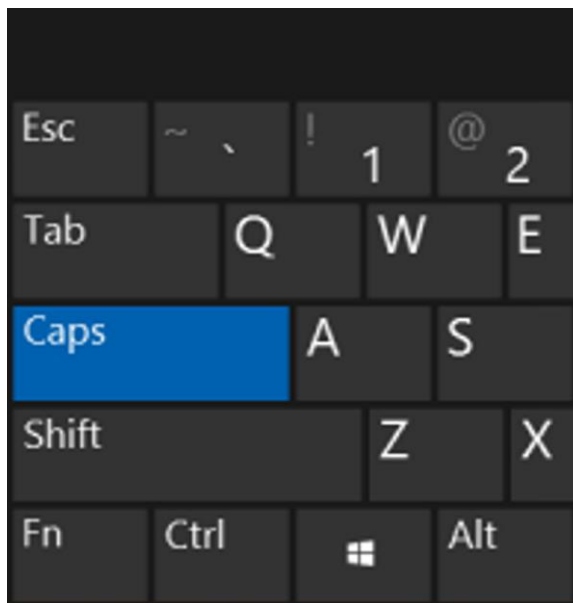
- Berühren Sie zuerst die Steuertaste.
Die Taste wechselt die Farbe.
- Berühren Sie die nächste Taste der Tastenkombination.



- Wenn die Tastenkombination vollständig ist, wird die Funktion ausgeführt und die Farbe wechselt zurück.

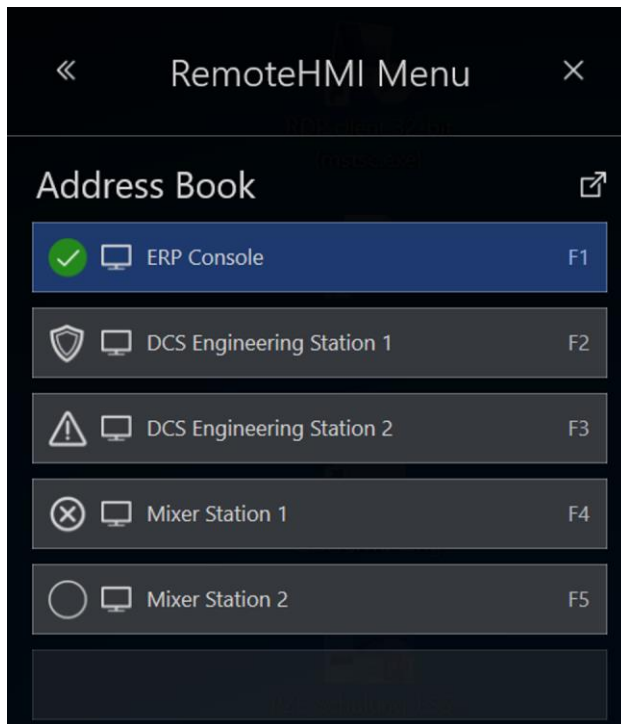
Feststelltaste (Caps) nutzen

1. Berühren Sie zuerst die Feststelltaste.
Die Farbe wechselt und bleibt erhalten.
 2. Berühren Sie die nächste Taste der Tastenkombination.
 3. Berühren Sie die Feststelltaste erneut, um die Taste zu deaktivieren.
- Die Farbe der Feststelltaste wechselt zurück.



4.3 Remote-Verbindung starten

Die Remote-Verbindungen sind im Adressbuch wählbar.



Status der Remote-Verbindung

Symbol	Bedeutung
	verbunden
	nicht verbunden
	keine Verbindung möglich
	Default, wird beim Start automatisch verbunden
	verbunden, parallele Remote-Verbindung, im Hintergrund aktiv (für Multi-Session-Verbindungen ist eine Pro-Lizenz erforderlich)
	Auto-Reconnect, automatische Wiederverbindung

Remote-Verbindung starten / wechseln

1. Klicken Sie im **Dashboard** auf die Remote-Verbindung, die Sie aktivieren wollen.
2. Wenn im **Address Book** eine Tastaturkombination oder Funktionstaste angegeben ist, können Sie die Remote-Verbindung auch über die Tastatur starten.

Wenn eine Verbindung aufgebaut wurde, wechselt das Symbol zu . Die vorher aktive Remote-Verbindung wird deaktiviert.



Wenn ein Eingabefenster für den Benutzernamen und das Passwort erscheint, müssen Sie beides eingeben, um auf den Server zugreifen zu können. Den Benutzernamen und das Passwort erhalten Sie von Ihrem Netzwerk-Administrator.



Wenn die parallele Nutzung mehrerer Remote-Verbindungen aktiviert ist, können Sie zwischen den verbundenen PCs wechseln. Beide Verbindungen bleiben bestehen.

Mehrere Remote-Verbindungen parallel nutzen



Pro-Lizenz erforderlich.

1. Klicken Sie im **Dashboard** auf die Remote-Verbindung, die Sie zusätzlich aktivieren wollen.
2. Wenn im **Address Book** eine Tastenkombination oder Funktionstaste angegeben ist, können Sie die Remote-Verbindung auch über die Tastatur starten. Wenn die Verbindung zum anderen PC aufgebaut wurde, werden die Verbindungen wie folgt angezeigt:

✓ im Vordergrund aktive Verbindung

✓ im Hintergrund aktive Verbindung

✓	🖥️	Server 2019	192.168.2.1	RDP	▼
✓	🖥️	Server 2012	192.168.2.2	RDP	▼

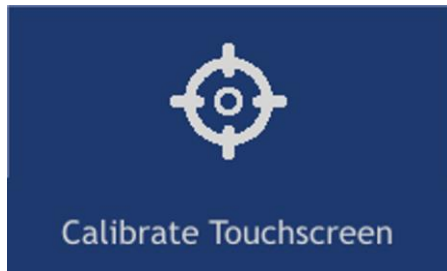
3. Klicken Sie auf die gewünschte Verbindung, um die Ansicht zu wechseln.
 - Beide Verbindungen bleiben bestehen.

Remote-Verbindung startet nicht

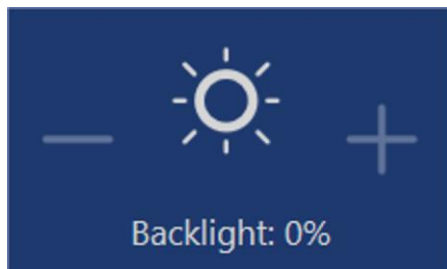
Wenn keine Verbindung aufgebaut werden konnte, wechselt das Symbol zu . Das System gibt eine Fehlermeldung aus. Merken Sie sich den Inhalt der Meldung, diese hilft bei der Fehlerbehebung.

- Informieren Sie einen Admin oder einen Engineer, um die Verbindungsprobleme zu beheben.
- Geben Sie den Inhalt der Fehlermeldung an diesen weiter.

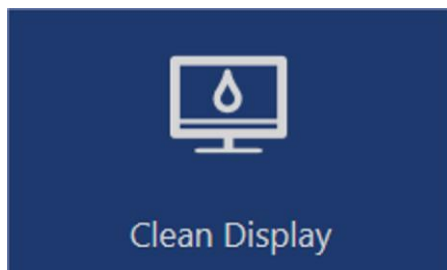
4.4 Settings im Dashboard nutzen



Der Button startet die Kalibrierung des Touchscreens. Wenn zwei Touchscreens angeschlossen sind, können Sie jeden Touchscreen separat kalibrieren.



Der Button passt die Hintergrundbeleuchtung des Displays an.



Der Button sperrt die Touchfunktion des Displays für 30 Sekunden. Dadurch wird das unbeabsichtigte Ausführen von Buttons zum Beispiel während der Reinigung verhindert.



Der Button simuliert einen Rechtsklick auf dem Touchscreen, um zum Beispiel das Kontextmenü von Anwendungen aufzurufen.



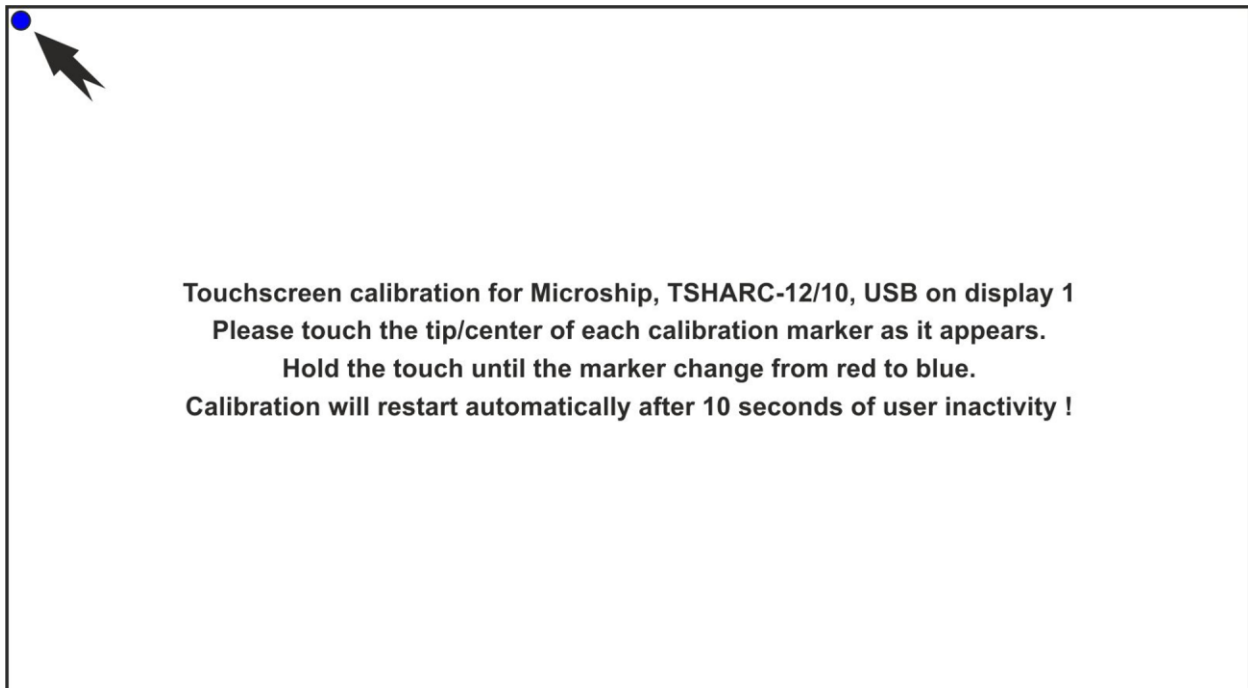
Der Button baut eine Netzwerkverbindung über einen Wireless Router auf.

4.4.1 Touchscreen kalibrieren

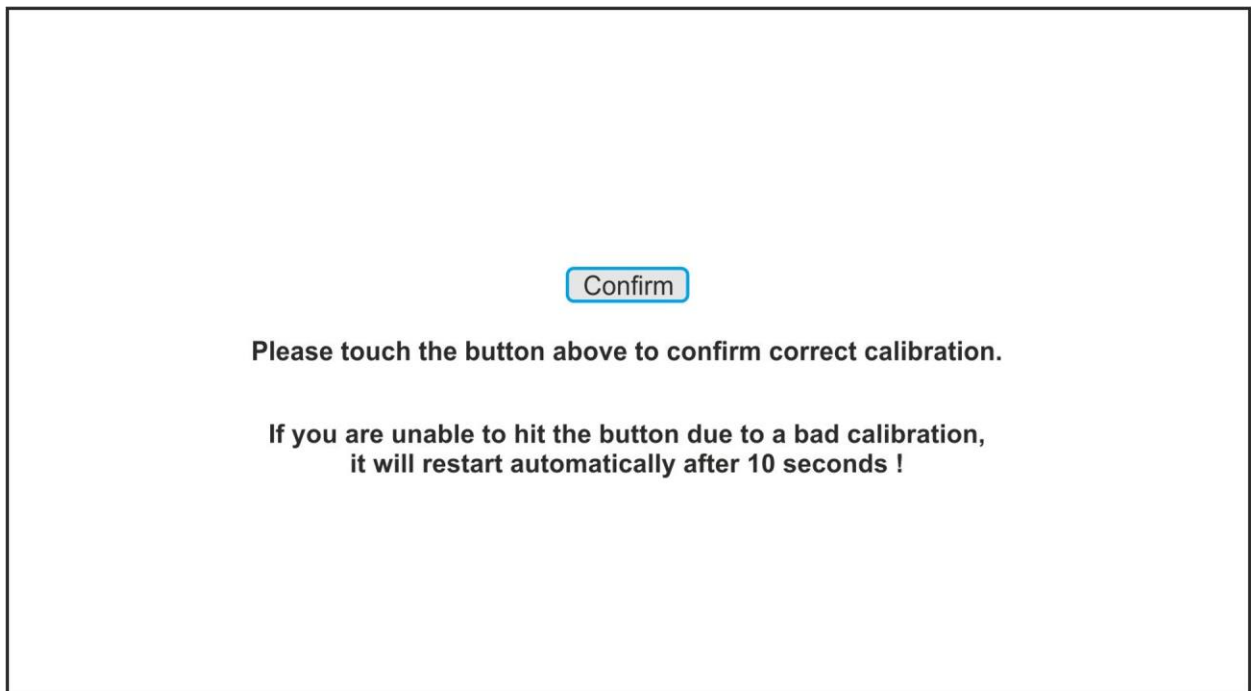
Die Kalibrierung erfolgt über definierte Kalibrierungspunkte (oben links, Mitte links, unten links, oben Mitte, Mitte Mitte, unten Mitte, oben rechts, Mitte rechts, unten rechts). Diese werden während der Kalibrierung nacheinander angezeigt.

Einen Touchscreen kalibrieren

1. Tippen Sie auf **Calibrate Touchscreen** um das Kalibrieren zu starten.
Die Anzeige wird einfarbig und der erste Kalibrierungspunkt wird angezeigt.



1. Tippen Sie auf den Kalibrierungspunkt und halten Sie diesen gedrückt, bis die Markierung die Farbe von blau auf rot und zurück auf blau gewechselt hat (visuelles Feedback).
Der nächste Kalibrierungspunkt wird angezeigt.
2. Wiederholen Sie den ersten Schritt für jeden Kalibrierungspunkt. Achten Sie darauf, die Punkte exakt zu treffen.
Wenn der letzte Kalibrierungspunkt gewählt wurde, erscheint folgende Anzeige:
Please touch the button above to confirm correct calibration.



1. Bestätigen Sie die Kalibrierung mit **Confirm**.

► Wenn der Touchscreen kalibriert ist, kehrt die Anzeige zum RemoteHMI-Menü zurück.



Wenn die Kalibrierung nicht korrekt ausgeführt wurde, ist eine Bestätigung der Kalibrierung nicht möglich. Der Vorgang startet automatisch nach 10 Sekunden.

Wenn zwei Touchscreens angeschlossen sind, ist der Button zweigeteilt. Sie können jeden Touchscreen separat kalibrieren.

1. Die linke Hälfte des Buttons **Calibrate Touchscreen 1** startet das Kalibrieren des ersten Touchscreens.
2. Die rechte Hälfte des Buttons **Calibrate Touchscreen 2** startet das Kalibrieren des zweiten Touchscreens.

4.4.2 Helligkeit des Displays anpassen



Um die Lebensdauer der Hintergrundbeleuchtung zu erhöhen, empfehlen wir die Funktion **Backlight Auto Dimming** zu aktivieren (siehe [8.6 Display-Einstellungen](#)).

- Tippen Sie auf +, um die Helligkeit des Displays zu erhöhen.
- Tippen Sie auf -, um die Helligkeit des Displays zu verringern.

4.4.3 Kontextmenü am Touchscreen öffnen

Eine kurze Berührung des Touchscreens simuliert die linke Maustaste. Wenn Sie das Kontextmenü von Anwendungen öffnen wollen, müssen Sie den Rechtsklick simulieren.



Rechtsklick deaktiviert



Rechtsklick aktiviert

Kontextmenü einer Anwendung aufrufen

1. Tippen Sie auf **Touchscreen Rightclick**, um die Funktionen der rechten Maustaste zu aktivieren.
2. Legen Sie den Finger oder Stift auf die Stelle, an der Sie „rechtsklicken“ wollen. Es erscheint ein Kreis um den Berührungspunkt.
3. Halten Sie den Finger oder Stift auf dem Touchscreen, bis sich der Kreis schließt.
4. Lassen Sie den Finger oder Stift los, sobald sich der Kreis geschlossen hat.
 - Das Kontextmenü öffnet sich.

Wenn sich kein Kontextmenü öffnet, ist in dem angeklickten Bereich kein Kontextmenü verfügbar.

Wenn Sie den Finger oder Stift loslassen, bevor sich der Kreis geschlossen hat, wird der Rechtsklick abgebrochen.

4.4.4 Touchscreen reinigen

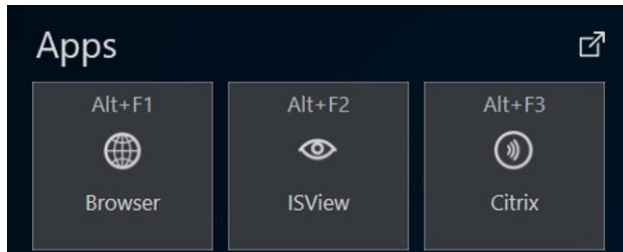
- Tippen Sie auf **Clean Display**, um die Touchfunktionen für 30 Sekunden zu sperren.
- Reinigen Sie den Touchscreen.

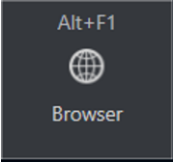
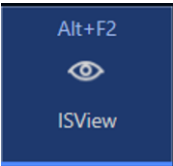
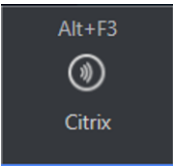
4.5 Applikationen starten

Pro

Pro-Lizenz erforderlich.

Applikationen können nur mit der Pro-Lizenz der Firmware genutzt werden. Wenn Anwendungen (Apps) eingerichtet wurden, werden diese als Button angezeigt. Es können mehrere Apps gestartet werden. Der Status der App wird angezeigt.



Anzeige	Bedeutung
	inaktive App
	aktive App
	im Hintergrund geöffnete App

App aufrufen

1. Klicken Sie im **Dashboard** auf die gewünschte App.
 2. Wenn im Button eine Tastaturkombination oder Funktionstaste angegeben ist, können Sie die App auch über die Tastatur starten.
- Die App wird gestartet.

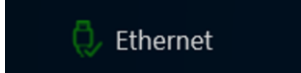


Wenn Sie keinen Zugriff auf die App haben, wenden Sie sich an den Administrator.

4.6 Status der Ethernet-Verbindung aufrufen

Status der Ethernet-Verbindung aufrufen

1. Öffnen Sie das **Dashboard**.
2. Klicken Sie in der unteren Leiste auf den Button der Ethernet-Verbindung.



Die Status-Informationen werden angezeigt.

3. Oder öffnen Sie über  das **erweiterte Dashboard**.
Alle Informationen zum System werden in der rechten Hälfte angezeigt.

4.7 Multi-Display nutzen

Wenn zwei Displays am Thin-Client angeschlossen sind, sind folgende Darstellungen möglich:

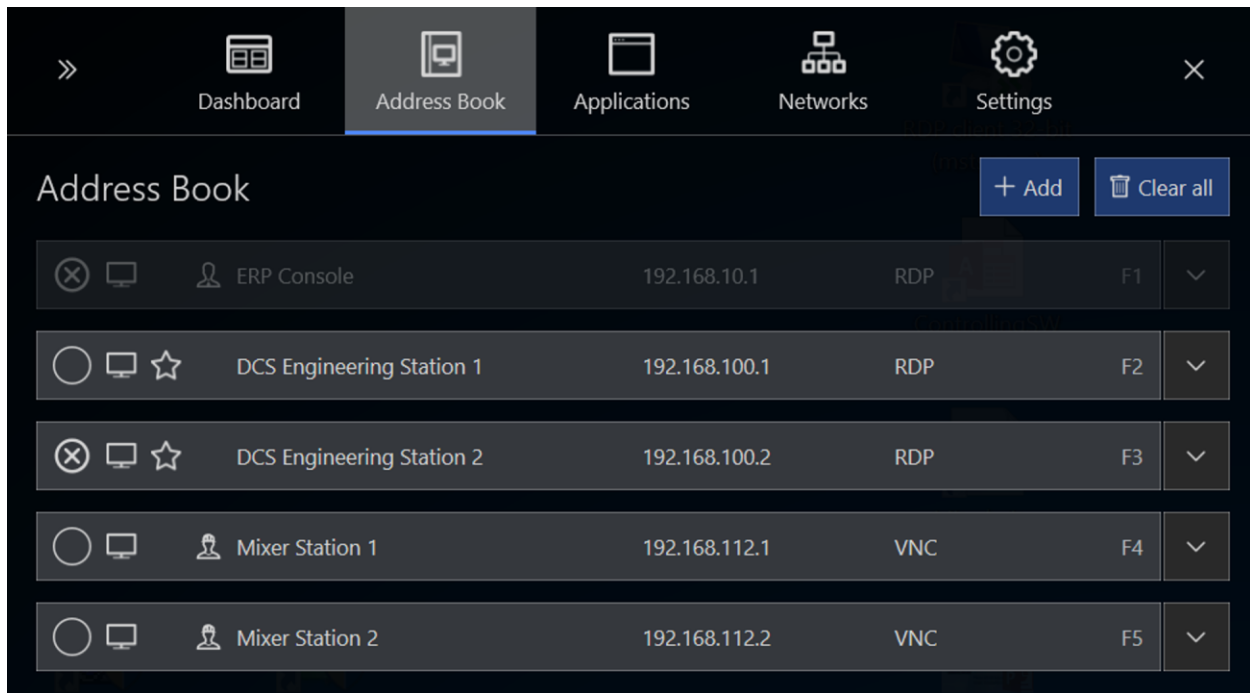
- Auf beiden Displays werden die gleichen Inhalte dargestellt.
- Auf beiden Displays werden unterschiedliche Inhalte dargestellt. Die Darstellung des Hauptdisplays wird durch das zweite Display erweitert.

5 Adressbuch

Im Register **Address Book** können Sie konfigurierte Remote-Verbindungen aufrufen, verwalten oder neue Remote-Verbindungen erstellen.

5.1 Optionen im Adressbuch

Das Register **Address Book** listet alle angelegten Remote-Verbindungen auf.



Wenn eine Verbindung im Adressbuch ausgegraut ist, hat der Benutzer keine Berechtigung die Verbindung zu wählen.



Die parallele Nutzung mehrerer Remote-Verbindungen (Multi-Session-Verbindung) ist nur mit der PRO-Lizenz möglich und muss im Menü **Connections** aktiviert werden.

Wenn die parallele Nutzung mehrerer Remote-Verbindungen aktiviert ist, werden die Verbindungen wie folgt angezeigt:



Status der Remote-Verbindung

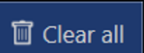
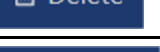
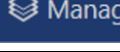
Symbol	Bedeutung
	verbunden
	nicht verbunden
	keine Verbindung möglich
	Default, wird beim Start automatisch verbunden
	verbunden, parallele Remote-Verbindung, im Hintergrund aktiv (für Multi-Session-Verbindungen ist eine Pro-Lizenz erforderlich)
	Auto-Reconnect, automatische Wiederverbindung

Navigationselemente

-  öffnet einen Eintrag in der Liste
-  schließt einen Eintrag in der Liste

Funktionen im Adressbuch

Die Bearbeitungsmöglichkeiten und Buttons sind abhängig vom Untermenü.

	Hinzufügen	Fügt einen neuen Eintrag hinzu
	Alles löschen	Löscht alle Einträge in der Liste
	Bearbeiten	Öffnet den markierten Eintrag zum Bearbeiten
	Kopieren	Kopiert den markierten Eintrag und öffnet die Kopie zum Bearbeiten
	Löschen	Löscht den markierten Eintrag
	Verwalten	Springt in die Listenebene zurück
	Anwenden	Übernimmt die Eingaben
	Rückgängig	Verwirft die Eingaben
	Nach oben	Verschiebt den markierten Eintrag in der Liste nach oben
	nach unten	Verschiebt den markierten Eintrag in der Liste nach unten
	Profil bearbeiten	Öffnet den Dialog zum Ändern des Remote-Profiles

Tastaturkurzbefehl für den Aufruf von Remote-Verbindungen

Die Remote-Verbindung kann über die Tastatur gewählt werden, wenn ein Tastaturkurzbefehl unter **Hotkey** angelegt ist. Es können drei Tasten belegt werden.

Erste Taste	Zweite Taste	Dritte Taste
[Shift]	[Ctrl]	none
[Ctrl]	[Alt]	[F1] ... [F12]

Die Ctrl-Taste darf nicht doppelt gewählt werden.

5.2 Remote Verbindungen einrichten

Automatischer Logon am Server

Die automatische Anmeldung am Server kann in den Einstellungen der Remote-Verbindung konfiguriert werden. Hierfür müssen Sie den Benutzernamen und das Passwort für den Server kennen.



Nur Benutzer, die die Berechtigung haben, remote auf den Server zu zugreifen, können sich am Server anmelden. Prüfen Sie die Berechtigung des Benutzers auf dem Server bzw. der KVM-Box.

Displayposition der Remote-Verbindung

Folgende Darstellungsoptionen sind möglich:

Symbol	Bezeichnung	Bedeutung
	Full display	zeigt den vollen Bildschirm an
	Left display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen auf der linken Seite an
	Right display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen auf der rechten Seite an
	Upper display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen oben an
	Lower display half	Skaliert den Remote-Bildschirminhalt und zeigt diesen unten an
	Bottom left corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der unteren linken Ecke an
	Bottom right corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der unteren rechten Ecke an
	Top left corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der oberen linken Ecke an
	Top right corner	Skaliert den Remote-Bildschirminhalt und zeigt diesen in der oberen rechten Ecke an



Picture in picture

Skaliert den Bildschirminhalt einer Kamera und zeigt diesen immer im Vordergrund an freier Position an. Diese Option steht nur für Kameras zur Verfügung.

Verhalten der Firmware bei Verlust der Verbindung

Das Verhalten der Remote-Verbindung bei Neustart oder Verlust der Verbindung kann wie folgt konfiguriert werden:

Auto connect on system startup	 On	Stellt bei Neustart automatisch eine Verbindung her, wird durch das Symbol  im Adressbucheintrag angezeigt
	 Off	Bei Neustart muss der Verbindungsaufbau manuell gestartet werden
Auto reconnect on connection loss	 On	Stellt bei Verlust der Verbindung automatisch eine Verbindung her, wird durch das Symbol  im Adressbuch angezeigt.
	 Off	Bei Verlust der Verbindung muss der Verbindungsaufbau manuell gestartet werden

Für Nutzer der Pro-Lizenz

Pro	Das System erlaubt die parallele Nutzung mehrerer aktiver Remote-Verbindungen (Multi-Session-Verbindungen). Während die eine Remote-Verbindung auf dem Bildschirm angezeigt wird, bleibt die andere Verbindung im Hintergrund aktiv. Im Adressbuch sind die Verbindungen wie folgt gekennzeichnet:  im Vordergrund aktive Verbindung  im Hintergrund aktive Verbindung
------------	--

Die parallele Nutzung mehrerer Remote-Verbindungen wird im Menü **Settings** unter **Connections** aktiviert. Siehe auch:

- [8.10.1 Mehrere parallele Verbindungen erlauben](#)

5.2.1 RDP-Verbindung einrichten

Zur Konfiguration benötigen Sie die IP-Adresse oder den Namen des Servers. Diese sind in den Systemeigenschaften des Servers abgelegt.



Der Remote-Zugriff muss für RDP-Verbindungen in den Systemeigenschaften des Servers explizit erlaubt werden. Der Remote-Zugriff muss für den Benutzer konfiguriert sein.

1. Öffnen Sie das Register **Address Book**.
2. Klicken Sie auf + *Add*.
Ein neuer Adressbucheintrag wird erzeugt.
3. Klicken Sie auf *Edit*.
4. Wählen Sie in den **Connection Settings** über das Drop-down-Feld **Type** "RDP".
5. Geben Sie unter **Name** die Bezeichnung für die Verbindung ein.

6. Tragen Sie unter **Server Address** die IP-Adresse oder den Namen des Servers ein.
 - HINWEIS:
Um den automatischen Zugriff auf den verbundenen Server zu gewährleisten, müssen Sie die korrekten Anmeldedaten hinterlegen. Beachten Sie, dass möglicherweise ein Domänenname mit dem Benutzernamen verwendet werden muss.
7. Geben Sie unter **User Name** und **Password** die Anmeldedaten des Servers ein.
8. Wenn der Aufruf der Remote-Verbindung über die Tastatur möglich sein soll, legen Sie unter **Hotkey** einen Tastaturkurbefehl an.
9. Wählen Sie unter **Show on** die Anzeigeeoption.
10. Legen Sie die minimale Benutzerrolle für den manuellen Aufbau der Verbindung fest.
 - HINWEIS:
Hat der Benutzer keine Berechtigung die Verbindung aufzubauen, ist diese im Adressbuch ausgegraut.
11. Klicken Sie auf *Apply*, um die Verbindung einzurichten.
 - ▶ Die Verbindung wird im Adressbuch angezeigt.

5.2.2 VNC-Verbindung einrichten

Auf dem Thin-Client ist ein VNC-Client vorinstalliert. Der VNC-Server-Dienst muss auch auf dem Server installiert sein. Die Installation erfordert Administrator-Rechte auf dem Host-PC und dem Server.

Um die Verbindung einzurichten, benötigen Sie die IP-Adresse des VNC-Servers und abhängig von der Konfiguration das VNC-Passwort.



Wenn die Port-Nummer des VNC-Servers vom Standardport abweicht, muss die IP-Adresse um die Port-Nummer erweitert werden, zum Beispiel:
192.168.1.23:5901

1. Öffnen Sie das Register **Address Book**.
2. Klicken Sie auf *+Add*.
Ein neuer Adressbucheintrag wird erzeugt.
3. Klicken Sie auf *Edit*.
4. Wählen Sie in den **Connection Settings** über das Drop-down-Feld **Type** "VNC".
5. Geben Sie unter **Name** die Bezeichnung für die Verbindung ein.
6. Tragen Sie unter **Server Address** die IP-Adresse des Servers ein.
 - HINWEIS:
Um den automatischen Zugriff auf den verbundenen Server zu gewährleisten, müssen Sie die korrekten Anmeldedaten hinterlegen.
7. Geben Sie die Anmeldedaten des Servers ein.
8. Wenn der Aufruf der Remote-Verbindung über die Tastatur möglich sein soll, legen Sie unter **Hotkey** einen Tastaturkurbefehl an.
9. Wählen Sie unter **Show on** die Anzeigeeoption.
10. Legen Sie die minimale Benutzerrolle für den manuellen Aufbau der Verbindung fest.
 - HINWEIS:
Hat der Benutzer keine Berechtigung die Verbindung aufzubauen, ist diese im Adressbuch ausgegraut.

11. Klicken Sie auf *Apply*, um die Verbindung einzurichten.

- Die Verbindung wird im Adressbuch angezeigt.

5.2.3 Host für die VNC-Verbindung vorbereiten

Die Vorgehensweise ist abhängig vom VNC-Server-Dienst. Nähere Informationen sind der Hersteller-Dokumentation zum VNC-Server-Dienst zu entnehmen.

HINWEIS

Für den Vorgang sind Administratorrechte erforderlich.

1. Stellen Sie sicher, dass der Host vom Thin-Client erreicht werden kann. Wenn beide im selben Netzwerk sind, ist das grundsätzlich der Fall.
 2. Stellen Sie sicher, dass der VNC-Server-Dienst auf dem Host installiert und aktiviert ist (siehe [9.2 VNC-Server-Dienst auf dem Host aktivieren](#)).
 3. Wenn die Netzwerkverbindung über eine Firewall abgesichert ist, müssen Sie die Firewall konfigurieren. Erlauben Sie die Netzwerk-Kommunikation über den Port, auf dem der VNC-Server-Dienst empfangsbereit ist (standardmäßig 5900).
 4. Wenn die Netzwerkverbindung über einen Router abgesichert ist, müssen Sie den Router konfigurieren. Stellen Sie für die Weiterleitung der Netzwerk-Kommunikation jeden konfigurierten Port ein, auf dem der VNC-Server-Dienst empfangsbereit ist (standardmäßig 5900).
 5. Prüfen Sie, ob der VNC-Server-Dienst ordnungsgemäß arbeitet und eingehende Verbindungen akzeptiert.
- Der Host ist vorbereitet.

5.2.4 Thin-Client für die VNC-Verbindung vorbereiten

Die Vorgehensweise ist abhängig vom VNC-Server-Dienst. Nähere Informationen sind der Hersteller-Dokumentation zum VNC-Server-Dienst zu entnehmen.

HINWEIS

Für den Vorgang sind Administratorrechte erforderlich.

1. Stellen Sie sicher, dass der Thin-Client den Host erreichen kann. Wenn beide im selben Netzwerk sind, ist das grundsätzlich der Fall.
 2. Wenn die VNC-Verbindung des Thin-Client über einen Proxy-Server abgesichert ist, müssen Sie im VNC-Viewer den Proxy-Server angeben.
- Der Thin-Client ist vorbereitet.

5.3 Remote-Verbindung testen

Remote-Verbindung startet nicht

Wenn keine Verbindung aufgebaut werden konnte, wechselt das Symbol zu . Das System gibt eine Fehlermeldung aus.

- Prüfen Sie, ob Sie alle Einstellungen korrekt eingegeben haben.

Wenn der Host verfügbar ist, grenzen Sie das Problem über folgende Prüfungen ein:

RDP-Verbindung prüfen

1. Prüfen Sie in den Systemeinstellungen des Servers, ob eine RDP-Verbindung erlaubt ist.
2. Prüfen Sie, ob der Thin-Client als Benutzer am Server angelegt ist und die notwendigen Zugriffsrechte hat.

VNC-Verbindung prüfen

1. Prüfen Sie, ob der VNC-Server-Dienst richtig konfiguriert ist.
2. Prüfen Sie, ob die Port-Nummer korrekt angegeben ist.

KVM-over-IP-Verbindung prüfen

1. Prüfen Sie die Konfiguration der KVM-Box.
2. Prüfen Sie, ob die Port-Nummer korrekt angegeben ist.

5.4 Remote-Verbindungen verwalten

Navigationselemente



öffnet einen Eintrag in der Liste



schließt einen Eintrag in der Liste



Um die Einstellungen bearbeiten zu können, darf die Verbindung nicht aktiv sein.

Verbindung in der Liste verschieben

1. Öffnen Sie in den Eintrag im Register **Address Book** mit .
 2. Klicken Sie auf , um den Eintrag in der Liste nach oben zu verschieben.
 3. Klicken Sie auf , um den Eintrag in der Liste nach unten zu verschieben.
- Die Verbindung wird in der Liste verschoben.

Einstellungen der Verbindung ändern

1. Deaktivieren Sie die Verbindung im Register **Address Book**.
2. Öffnen Sie den Eintrag.
3. Klicken Sie auf *Edit*, um die Einstellungen zu bearbeiten.
4. Ändern Sie die gewünschten Einstellungen.

5. Klicken Sie auf *Apply*, um die Änderungen zu übernehmen.
Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.
6. Klicken Sie auf *Manage*, um die Liste zu bearbeiten.
Mit [↖] schließen Sie den Eintrag und kehren zur Liste zurück.

Verbindung löschen

1. Deaktivieren Sie die Verbindung im Register **Address Book**.
2. Öffnen Sie die Verbindung.
3. Klicken Sie auf *Delete*, um die Verbindung zu löschen.
4. Bestätigen Sie die Sicherheitsmeldung.
► Die Verbindung wird gelöscht.

Verbindung kopieren

1. Deaktivieren Sie die Verbindung im Register **Address Book**.
2. Öffnen Sie den Eintrag.
3. Klicken Sie auf *Copy*, um die Einstellungen zu kopieren.
Eine neuer Eintrag wird erzeugt.
4. Öffnen Sie den Eintrag und ändern Sie die notwendigen Einstellungen.
5. Klicken Sie auf *Apply*, um die Änderungen zu übernehmen.
Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.
6. Klicken Sie auf *Manage*, um die Liste zu bearbeiten.
Mit [↖] schließen Sie den Eintrag und kehren zur Liste zurück.

6 App-Verwaltung

Pro

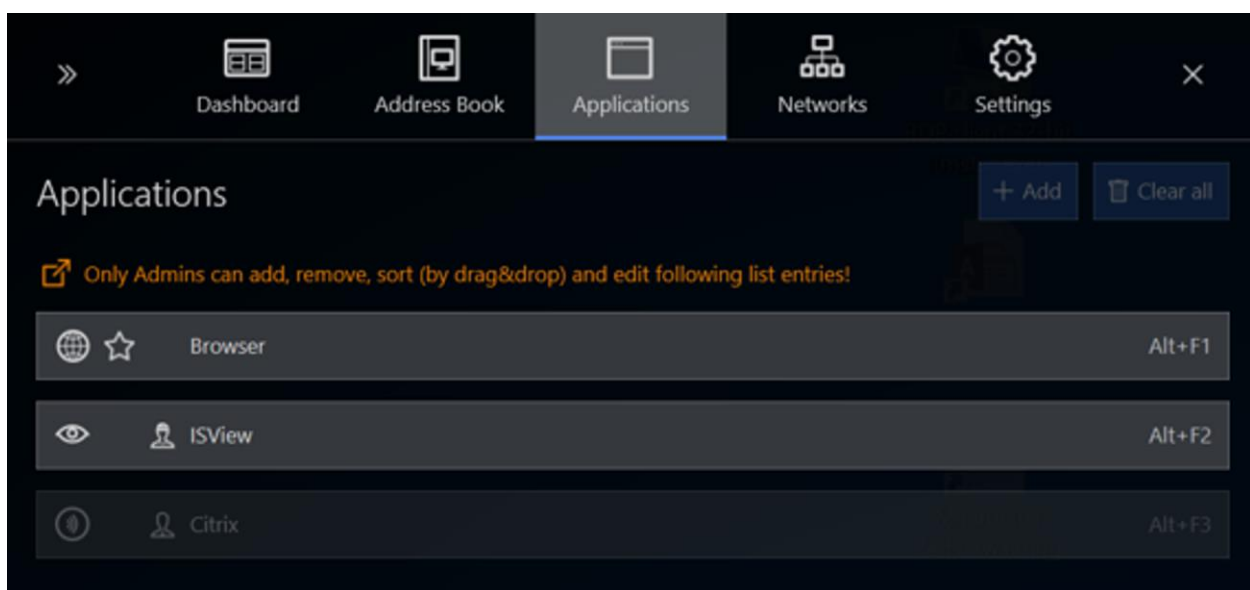
Pro-Lizenz erforderlich.

Im Register **Applications** können Sie Links zu Windows Tools und Anwendungen, Antivirensoftware oder EXE-Anwendungen wie Citrix Receiver hinzufügen und verwalten. Über verschiedene Einstellungen können Sie das Aussehen und Verhalten der App konfigurieren und den Zugriff über die Benutzerrollen regeln.

Bevor Sie eine Anwendung hinzufügen, muss sie auf dem Thin-Client installiert werden. Der Thin-Client muss die Systemvoraussetzungen für die App erfüllen.

6.1 Optionen im Register Applications

Das Register **Applications** listet alle verfügbaren Apps auf.



Wenn ein Eintrag in der Liste ausgegraut ist, hat der Benutzer keine Berechtigung, den Eintrag zu wählen.

Symbole in der App-Liste

Sie können das Icon, das in der App-Liste angezeigt wird, frei wählen. Um den Nutzern die Bedienung zu erleichtern, wird empfohlen, gängige Symbole zu verwenden.

Symbole



Auswahl von Icons, geben die Art Anwendung wieder



Engineer, Admin: Gibt an, wer die App starten darf.

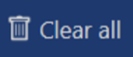
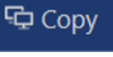
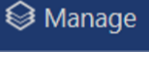
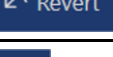
Wenn kein Symbol angezeigt wird, sind alle Benutzerrollen berechtigt die App zu starten.



Default, wird beim Start automatisch verbunden

Funktionen im Register Applications

Die Bearbeitungsmöglichkeiten und Buttons sind abhängig vom Untermenü.

	Hinzufügen	Fügt einen neuen Eintrag hinzu
	Alles löschen	Löscht alle Einträge in der Liste
	Bearbeiten	Öffnet den markierten Eintrag zum Bearbeiten
	Kopieren	Kopiert den markierten Eintrag und öffnet die Kopie zum Bearbeiten
	Löschen	Löscht den markierten Eintrag
	Verwalten	Springt in die Listenebene zurück
	Anwenden	Übernimmt die Eingaben
	Rückgängig	Verwirft die Eingaben
	Nach oben	Verschiebt den markierten Eintrag in der Liste nach oben
	nach unten	Verschiebt den markierten Eintrag in der Liste nach unten
	Terminieren	Erzwingt das Beenden einer geöffneten Anwendung mit möglichem Datenverlust
	Datei wählen	Öffnet das Auswahl-Fenster für ausführbare Dateien

Navigationselemente

-  öffnet einen Eintrag in der Liste
-  schließt einen Eintrag in der Liste

Tastaturkurzbefehl für den Aufruf von Anwendungen

Die Anwendung kann über die Tastatur gewählt werden, wenn ein Tastaturkurzbefehl unter **Hotkey** angelegt ist. Es können drei Tasten belegt werden.

Erste Taste	Zweite Taste	Dritte Taste
[Shift]	[Ctrl]	none
[Ctrl]	[Alt]	[F1] ... [F12]

Die Ctrl-Taste darf nicht doppelt gewählt werden.

	Jeder Tastaturkurzbefehl (Hotkey) kann nur einmal vergeben werden.
---	--

Kommandozeilenparameter

Sie können für jede App einen Kommandozeilenparameter definieren, um anwendungsspezifische Parameter zu übergeben.

Beispiel:

Im Browser ruft der Parametereintrag -k www.stahl.de die Internetseite www.stahl.de im Kiosk-Modus auf.



Die zulässigen Kommandozeilenparameter können Sie der Beschreibung der jeweiligen Anwendung entnehmen.

Ausführungsstufe - Application privilege level

Stufe	Bedeutung
Run as standard user	Startet die Anwendung mit Standard-Rechten
Run as administrator user	Startet die Anwendung mit Administrator-Rechten Name und Passwort des Admin-Accounts können im Menü System & Proxy hinterlegt werden.
Run elevated	Startet die Anwendung mit erweiterten Administrator-Rechten Name und Passwort des Admin-Accounts können im Menü System & Proxy hinterlegt werden.

6.2 Apps hinzufügen

Pro-Lizenz erforderlich.

HINWEIS**Kompatibilität mit Software von Drittanbietern**

Die Firmware ist qualifiziert für Software, die mit den unterstützten HMI-Geräten ausgeliefert wird. Für die Funktionalität von Software anderer Anbieter übernimmt R. STAHL HMI Systems GmbH keine Garantie. Stellen Sie die Kompatibilität der Software anderer Anbieter vor der Installation sicher.

Systemvoraussetzung und Lauffähigkeit der Anwendung prüfen

1. Stellen Sie sicher, dass die Anwendung kompatibel ist.
2. Prüfen Sie, ob die Systemvoraussetzungen erfüllt sind.
3. Prüfen Sie, ob die Anwendung auf dem Thin-Client installiert werden kann. Dies erfolgt im Admin-Account.
4. Prüfen Sie, ob die Anwendung einwandfrei funktioniert.
 - Wenn alle Bedingungen erfüllt sind, ist die Anwendung kompatibel und lauffähig.

Anwendung hinzufügen

1. Öffnen Sie das Register **Applications**.
2. Klicken Sie auf **+Add**.
Ein neuer Eintrag wird erzeugt.
3. Öffnen Sie den Eintrag.
4. Wählen Sie unter **Icon** über das Drop-down-Feld ein passendes Symbol.
5. Aktivieren Sie **Autostart**, wenn die Anwendung automatisch starten soll.
6. Geben Sie unter **Name** die Bezeichnung für die Anwendung ein.
7. Wenn der Aufruf der Remote-Verbindung über die Tastatur möglich sein soll, legen Sie unter **Hotkey** einen Tastaturkurbefehl an.
8. Geben Sie im Feld **Path** den Dateipfad ein oder öffnen Sie mit dem Button *Select File* den Windows Explorer, um das Programm zu suchen. Wählen Sie die Programmdatei aus und bestätigen Sie den Dialog mit *Open*.
9. Wenn Sie anwendungsspezifische Parameter übergeben wollen, geben Sie unter **Parameters** einen Kommandozeilen-Parameter ein. Informationen zu den möglichen Parametern finden Sie im Handbuch der Anwendung.
10. Stellen Sie unter **Application privilege level** ein, wie die Anwendung gestartet werden soll.
11. Aktivieren Sie **Close RemoteHMI menu on app start**, wenn die Firmware beim Start der Anwendung geschlossen werden soll.
 - HINWEIS:
Wenn das Ausführen der Anwendung Administrator- oder erweiterte Rechte erfordert, können Sie die Anmeldedaten für das Administrator-Konto unter **Use predefined admin login credentials** hinterlegen. Dadurch müssen die Anmeldedaten beim Start der App nicht eingegeben werden.
12. Aktivieren Sie **Use predefined admin login credentials**, wenn die Anwendung über die Anmeldedaten des Thin-Client geöffnet werden soll. Geben Sie den Benutzernamen und das Passwort ein.
13. Legen Sie unter **Min user role required to start app manually** die minimale Benutzerrolle für den Start der Anwendung fest.
 - HINWEIS:
Wenn der Benutzer keine Berechtigung hat, die Anwendung manuell zu starten, ist diese im Register Applications ausgegraut.
14. Klicken Sie auf *Apply*, um die Eingaben zu übernehmen.
Die Anwendung wird im Dashboard und im Register Applications angezeigt.
15. Klicken Sie auf *Manage*, um die App in der Liste zu verschieben.
Mit [↖] schließen Sie den Eintrag und kehren zur Liste zurück.
16. Prüfen Sie, ob sich die App bei Klick auf den Eintrag korrekt öffnet.

6.3 Apps verwalten

Navigationselemente

-  öffnet einen Eintrag in der Liste
-  schließt einen Eintrag in der Liste

Anwendung in der Liste verschieben

1. Öffnen Sie im Register **Applications** den gewünschten Eintrag mit [].
2. Klicken Sie auf ↑, um den Eintrag in der Liste nach oben zu verschieben.
3. Klicken Sie auf ↓, um den Eintrag in der Liste nach unten zu verschieben.

Einstellungen der Anwendung ändern

1. Öffnen Sie im Register **Applications** den gewünschten Eintrag.
2. Klicken Sie auf *Edit*, um die Einstellungen zu bearbeiten.
3. Nehmen Sie die gewünschten Änderungen vor.
4. Klicken Sie auf *Apply*, um die Änderungen zu übernehmen.
Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.
5. Klicken Sie auf *Manage*, um die Liste zu bearbeiten.

Anwendung kopieren

1. Prüfen Sie die Kompatibilität und Lauffähigkeit der Anwendung, bevor Sie einen Link zu einer neuen Anwendung erstellen (siehe [6.2 Apps hinzufügen](#)).
2. Öffnen Sie das Menü **Applications**.
3. Öffnen Sie in den gewünschten Eintrag.
4. Klicken Sie auf *Copy*, um die Einstellungen der Anwendung zu kopieren.
Eine neuer Eintrag wird erzeugt.
5. Klicken Sie auf *Select File* und wählen Sie im Windows Explorer das Programm aus.
6. Öffnen Sie den Eintrag und ändern Sie die Einstellungen wie unter Apps hinzufügen beschrieben.
7. Klicken Sie auf *Apply*, um die Änderungen anzuwenden.
Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.
8. Klicken Sie auf *Manage*, um die App in der Liste zu verschieben.
Mit [] schließen Sie den Eintrag und kehren zur Liste zurück.

Anwendung beenden



Grundsätzlich sollten Sie Anwendungen regulär beenden, um Datenverlust zu vermeiden. Wenn sich eine Anwendung nicht über den normalen Weg beenden lässt, können Sie das Terminieren erzwingen.

1. Öffnen Sie im Register **Applications** den gewünschten Eintrag.
2. Klicken Sie auf *Terminate*, um das Beenden der Anwendung zu erzwingen.
3. Bestätigen Sie die Sicherheitsmeldung.
- Die Anwendung wird beendet.

Link zur Anwendung löschen



Über den Button *Delete* wird nur der Link zur Anwendung gelöscht, die Anwendung aber nicht deinstalliert.
Das Programm können Sie nur in der Windows-Oberfläche deinstallieren.

1. Öffnen Sie im Register **Applications** den gewünschten Eintrag.
 2. Klicken Sie auf *Delete*, um den Link zu löschen.
 3. Bestätigen Sie die Sicherheitsmeldung.
- Der Link zur App wird gelöscht.

7 Netzwerk

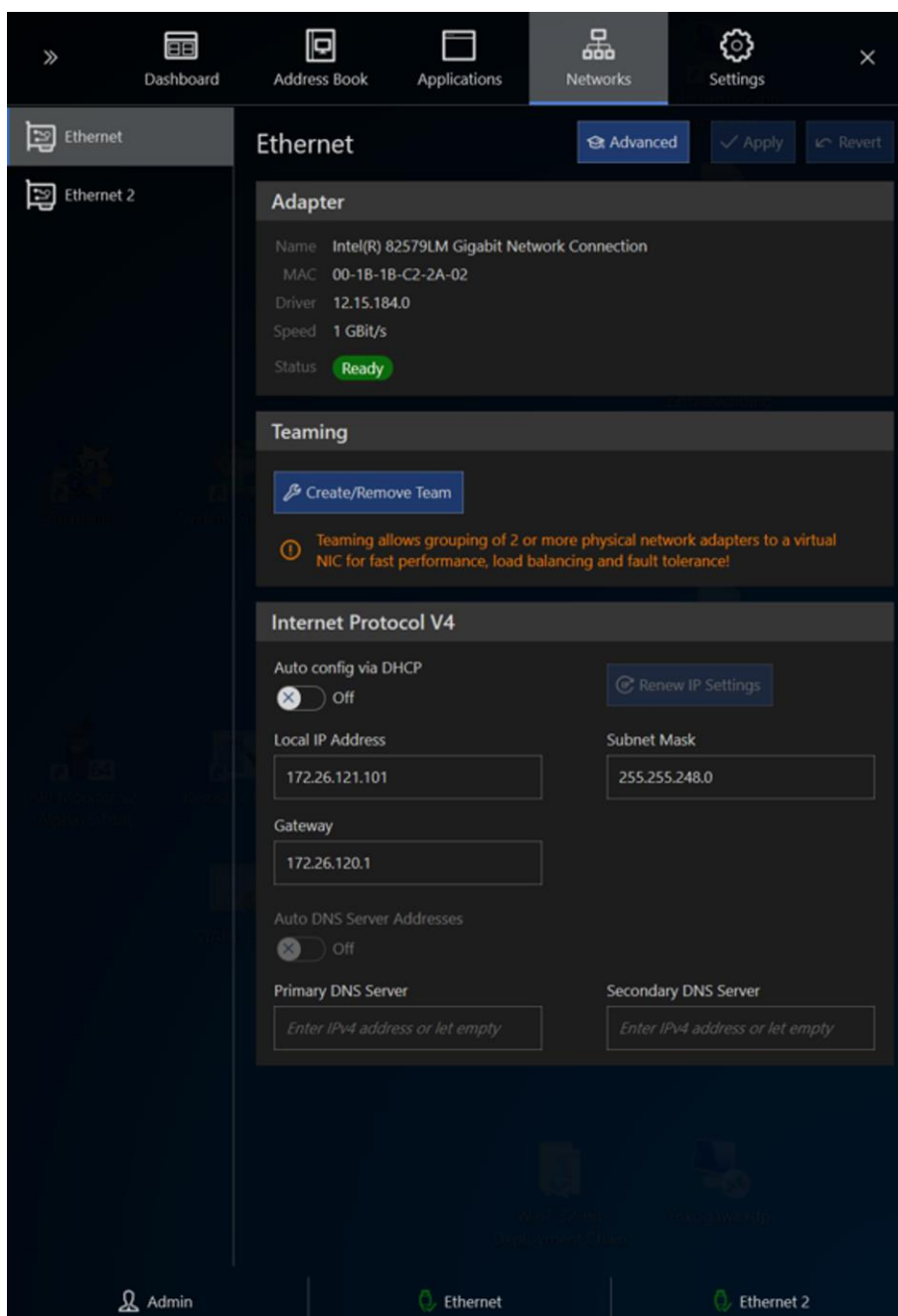
Im Register **Networks** können Sie den Thin-Client für die Teilnahme im Netzwerk konfigurieren. Die Anzahl und Bezeichnung der verfügbaren Ethernet-Adapter sind abhängig von der Hardware des Thin-Client.

7.1 Optionen im Register Networks

HINWEIS

IT-Netzwerk-Kenntnisse erforderlich

Einstellungen auf der Windows-Netzwerkebene können einen Einfluss auf das gesamte Netzwerk haben. Verwenden Sie den Button **Advanced** nur, wenn Sie sich mit den Windows-Netzwerkeinstellungen auskennen. Ist das nicht der Fall, bitten Sie Ihren Netzwerk-Administrator um Hilfe.



Buttons im Register Networks

 Advanced	Erweiterte Funktionen	Öffnet die Windows-Netzwerkeinstellungen
 Apply	Anwenden	Übernimmt die Eingaben
 Revert	Rückgängig	Verwirft die Eingaben
 Create/Remove Team	Team erstellen/entfernen	Öffnet den Dialog zur Teaming-Funktion
 Renew IP Settings	IP-Einstellungen erneuern	Fordert die Erneuerung der IP-Konfiguration beim DHCP-Server an

7.2 Adapter Informationen

Der Bereich **Adapter** listet Informationen zum ausgewählten Ethernet-Adapter auf.

Name	Name des Ethernet-Adapters
MAC	MAC-Adresse des Ethernet Adapters
Driver	Version des Adapter-Treibers
Speed	Geschwindigkeit der Ethernet-Verbindung
Status	Status der Ethernet-Verbindung

7.3 Über DHCP

Dynamic Host Configuration Protocol - DHCP

Die Adresszuordnung mit DHCP funktioniert nach dem Client-Server-Prinzip. Der Client fordert die IP-Adresskonfiguration von einem DHCP-Server an, der die angeforderten Daten in seiner Datenbank nachschlägt.

Der DHCP-Server kann dem Thin-Client folgende Einstellungen zuweisen:

- IP-Adresse
- Subnetzmaske
- Standard-Gateway
- DNS-Server-Adresse

Auto config via DHCP

Bei der automatischen Zuordnung schickt der Client seine Adressanfrage an alle Netzwerkteilnehmer. Der DHCP-Server antwortet mit einem Daten-Paket, das neben einer möglichen, freien IP-Adresse und der MAC-Adresse des Clients auch die Subnetzmaske sowie die IP-Adresse und ID des Servers enthält. Der Client entnimmt der Antwort die benötigten Daten und informiert den DHCP-Server. Der Server bestätigt die TCP/IP-Parameter und sendet zusätzliche Informationen zum Beispiel den DNS-Server an den Client zurück. Die automatisch vergebene Adresse speichert der DHCP-Server zusammen mit der MAC-Adresse in der Datenbank. Diese Zuordnung bleibt dauerhaft bestehen.

Weiterführende Themen:

- [7.5 Netzwerk-Adapter einrichten](#)

7.4 Über DNS

Domain Name System - DNS

DNS ist ein Dienst, der Domain-Namen in numerische Adressen auflöst. Grundlage des DNS ist ein Verzeichnissystem, das den Namensraum (Domain-Name-Space) verwaltet. Wenn eine neue Domain zum Beispiel im Internet erstellt wird, speichert ein DNS-Server den Domain-Namen und die zugehörige IP-Adresse. Diese Datenbank nutzt er, um eingehende Anfragen zum Domain-Name-Space zu beantworten.

Mit Hilfe der Firmware können zwei DNS-Server adressiert werden.

Auto DNS Server Addresses

Über diese Funktion kann ein DNS-Server automatisch adressiert werden, wenn zum Beispiel die IP-Adresse der DNS-Servers nicht bekannt ist.

Weiterführende Themen:

- [7.5 Netzwerk-Adapter einrichten](#)

7.5 Netzwerk-Adapter einrichten

Bei Auslieferung ist die automatische Adresszuordnung **Auto config via DHCP** aktiviert.

Netzwerk-Adresse automatisch einrichten

1. Öffnen Sie das Register **Networks**.
 2. Prüfen Sie ob **Auto config via DHCP** aktiviert ist.
 3. Klicken Sie auf *Apply*, um die automatische Zuordnung durch den DHCP-Server zu starten.
- IP-Adresse, Gateway und Subnetzmaske sind konfiguriert.

Netzwerk-Adresse manuell einstellen

1. Öffnen Sie das Register **Networks**.
 2. Deaktivieren Sie **Auto config via DHCP**, um die Adresse manuell einzurichten.
 3. Geben Sie unter **Local IP address** die IP-Adresse des Netzwerk-Adapters ein.
 4. Geben Sie unter **Subnet Mask** die Subnetzmaske ein.
 5. Wenn der Thin-Client auf ein anderes Netzwerk zugreifen soll, geben Sie unter **Gateway** die IP-Adresse des Gateway ein.
 6. Klicken Sie auf *Apply*, um die Änderungen zu übernehmen.
- IP-Adresse, Gateway und Subnetzmaske sind konfiguriert.

DNS-Server manuell konfigurieren

1. Öffnen Sie das Register **Networks**.
2. Geben Sie unter **Primary DNS Server** die IP-Adresse des ersten DNS-Servers ein.
3. Geben Sie unter **Secondary DNS Server** die IP-Adresse des zweiten DNS-Servers ein.
4. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.

7.6 Teaming-Funktion

Durch das Teaming können Sie:

- Die Ethernet-Adapter im Team als Stand-by-Adapter verwenden, um eine Redundanz zu realisieren und die Ausfallsicherheit zu erhöhen.
- Die Geschwindigkeit der Ethernet-Adapter zusammenfassen, um die Leistung zu erhöhen.

Die Teaming-Funktion fügt mehrere physikalische Netzwerkverbindungen zu einem virtuellen "Netzwerk Interface Controller" (NIC) zusammen.

HINWEIS

Funktion "Teaming"

Teaming ist eine erweiterte Funktion für die Serverumgebung. Mit Teaming können viele physikalische Adapter zu einem Team zusammengefasst werden, das über Funktionen zum Lastenausgleich und Ausfallsicherheit verfügt.

HINWEIS

IT-Netzwerk-Kenntnisse erforderlich

Die Einstellung erfolgt auf der Systemebene über das "Realtek - Ethernet Diagnostic Utility". Führen Sie die Funktion nur aus:

- Wenn Sie sich mit virtuellen Netzwerkkarten auskennen
- Wenn beide Adapter einwandfrei funktionieren

Team erstellen

1. Öffnen Sie das Register **Networks**.
2. Klicken Sie auf + *Create/Remove Team*.
Es öffnet sich das Teaming-Fenster, das alle notwendigen Schritte auflistet.
3. Warten Sie, bis sich das Fenster "Realtek Diagnostic Utility" öffnet. Das kann bis zu 30 Sekunden dauern.
4. Markieren Sie im linken Ausschnitt den gewünschten "PCIe Controller".
5. Wählen Sie im mittleren Ausschnitt "Teaming".
6. Wählen Sie im rechten Ausschnitt "Create Team".
Das Fenster "Create Team" öffnet sich.
7. Geben Sie eine Bezeichnung für das Team ein, diese erscheint später in der Liste der Ethernet-Adapter.
 - HINWEIS:
Sie können nur eine der folgenden Funktionen aktivieren:
"Fast/Giga EtherChannel"
"Link Aggregation / LACP"
8. Aktivieren Sie "Fast/Giga EtherChannel", um bei Ausfall des ersten Adapters auf den zweiten Adapter umzuschalten.
9. Aktivieren Sie "Link Aggregation / LACP", um die Bandbreite durch die gleichzeitige Nutzung beider Adapter zu erhöhen.

10. Wählen Sie die physikalischen Netzwerkadapter aus, die Sie zu einem Team zusammenfassen wollen.
11. Bestätigen Sie die Eingabe mit "OK".
Der neue virtuelle Adapter wird im Fenster "Realtek Diagnostic Utility" im linken Ausschnitt angezeigt.
12. Markieren Sie das Team und prüfen Sie die Einstellungen im rechten Abschnitt.
13. Schließen Sie das Fenster "Realtek Diagnostic Utility".
14. Kehren Sie zur Firmware zurück und führen Sie einen Neustart aus.
 - Der virtuelle Adapter wird im Register **Networks** angezeigt.

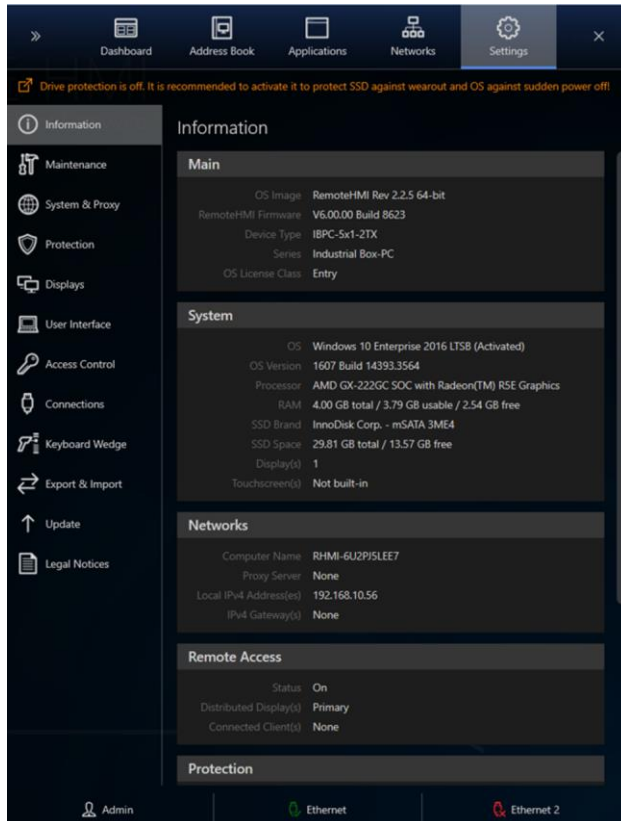
Team entfernen

1. Öffnen Sie das Register **Networks**.
2. Klicken Sie auf + *Create/Remove Team*.
Es öffnet sich das Teaming-Fenster, das alle notwendigen Schritte auflistet.
3. Warten Sie, bis sich das Fenster "Realtek Diagnostic Utility" öffnet. Das kann bis zu 30 Sekunden dauern.
4. Markieren Sie im linken Ausschnitt den virtuellen Adapter.
5. Öffnen Sie das Kontextmenü und wählen Sie "Remove".
6. Bestätigen Sie die Warnmeldung mit "OK".
Der virtuelle Adapter ist entfernt.
7. Kehren Sie zur Firmware zurück und führen Sie einen Neustart aus.
 - Der virtuelle Adapter wird aus dem Register **Networks** entfernt.

8 Settings

Das Register **Settings** enthält verschiedene Funktionen zur Konfiguration der Firmware durch den Engineer oder Admin.

8.1 Optionen im Register Settings



Das Register **Settings** enthält folgende Menüs:

Menü	Inhalt	Bearbeitung durch
Information	Aktuelle Daten, Einstellungen und Konfigurationen des Systems Je nach Geräteplattform unterscheiden sich die Menüeinträge.	
Maintenance	Funktionen, die zur Wartung des Thin-Client notwendig sind, erlaubt das Hinzufügen von Software und Treibern von Drittanbietern Aktivierung der Pro-Lizenz und von Windows LTSC	Admin
System & Proxy	Einstellungen zu Gerätenamen (im Netzwerk) und Proxy-Server	Engineer / Admin
Protection	Einstellungen zur Systemsicherheit	Engineer / Admin
Displays	Einstellungen für bis zu 6 Displays	Engineer / Admin
User Interface	Verhalten des RemoteHMI-Menüs	Admin
Access Control	Einrichtung der geschützten Benutzerrollen	Admin

Connections	Einstellungen der Verbindungsoptionen	Engineer / Admin
Keyboard Wedge	Einstellung der COM-Schnittstellen für externe Scanner oder Lesegeräte	Engineer / Admin
Export & Import	Funktionen zum Export und Import der Gerätekonfiguration	Engineer / Admin
Updates	Aktualisierung der Firmware	Admin
Legal Notice	Information zu den Lizenzbestimmungen der auf dem Thin-Client verwendeten Software	

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.2 Systeminformationen anzeigen

Das Menü **Information** listet die aktuellen Daten, Einstellungen und Konfigurationen des System auf. Je nach Geräteplattform unterscheiden sich die Menüeinträge.

Menü	Inhalt
Main	Anzeige der wesentlichen Systeminformationen, OS-Image und Firmware-Version
System	Informationen zu Hardware und Betriebssystem Die Anzeige variiert abhängig vom Gerätetyp
Network	Informationen zu Computernamen und Adressen des Proxy-Servers, des Geräts und Gateways
Remote Access	Angaben zum Status der Remote-Verbindungen
Protection	Aktuelle Einstellungen zur Systemsicherheit
Components	Anzeige von Komponenten
Serial Numbers	Anzeige von Seriennummern des HMI, Electronic Box und der Display Box

8.3 Maintenance

Im Menü **Maintenance** können Sie Arbeiten auf der Windows Systemebene ausführen.

- [8.3.1 In den Admin-Account der Windows-Oberfläche wechseln](#)
- [8.3.2 System neu starten](#)
- [8.3.3 System herunterfahren](#)
- [8.3.4 Advanced Startup](#)
- [8.3.5 Einstellungen zurücksetzen](#)
- [8.3.6 Peripherie-Gerät koppeln oder hinzufügen](#)
- [8.3.7 Event Log aufrufen](#)
- [8.3.8 Pro-Lizenz aktivieren](#)
- [8.3.9 Windows aktivieren](#) (via Internet oder Telefon)

Funktionen im Menü Maintenance

Main		
<i>Maintain System</i>	System warten	Erlaubt das Einloggen in das Administrator-Konto mit regulärer Windows Oberfläche
<i>Restart System</i>	System neu starten	Führt einen Neustart aus
<i>Shutdown System</i>	System herunterfahren	Führt das System herunter
<i>Reset all Settings</i>	Alle Einstellungen zurücksetzen	Setzt alle Einstellungen auf die Werkseinstellungen zurück
Device		
<i>Add/Pair Device</i>	Gerät hinzufügen / koppeln	Öffnet die Windows-Systemsteuerung, um Peripherie-Geräte hinzuzufügen oder Bluetooth-Geräte mit dem Thin-Client zu koppeln
<i>Adjust Pointing Device</i>	Mouse anpassen	Öffnet die Systemeigenschaften der Mouse am Thin-Client
Event Log		
<i>View Event Log</i>	Event Log öffnen	Öffnet den Event-Log-Viewer des Thin-Client
Pro Edition License Activation		
<i>Activate Pro License</i>	Pro Lizenz aktivieren	Aktiviert die Pro-Einzellizenz online (Internet-Zugang des Thin-Client erforderlich)
<i>Apply Pro License</i>	Pro Lizenz übernehmen	Aktiviert die Pro-Einzellizenz offline (PC/Endgerät mit Internet-Zugang erforderlich)
Windows Activation (nur sichtbar, wenn Windows LTSC nicht aktiviert ist)		
<i>Activate over Internet</i>	Übers Internet aktivieren	Aktiviert Windows LTSC (Internet-Zugang des Thin-Client erforderlich)
<i>Activate by phone</i>	Per Telefon aktivieren	Öffnet den Telefon-Dialog zur Aktivierung von Windows LTSC

8.3.1 In den Admin-Account der Windows-Oberfläche wechseln

Sie können eine Systemwartung im Administrator-Konto und z.B. die Installation von Applikationen auf dem Thin-Client durchführen.

HINWEIS

IT-Netzwerk-Kenntnisse erforderlich

Einstellungen auf der Systemebene können zu einem Ausfall des Geräts führen. Wechseln Sie nur auf die Systemebene, wenn Sie sich mit den erweiterten Einstellungen auskennen. Ist das nicht der Fall, bitten Sie Ihren Netzwerk-Administrator um Hilfe.

1. Öffnen Sie das Menü **Maintenance**.
2. Klicken Sie im Bereich **Main** auf *Maintain System*.
Es erscheint eine Sicherheitsabfrage.
3. Bestätigen Sie die Sicherheitsabfrage mit Yes.
Das System wechselt zum Anmeldebildschirm und erlaubt das Einloggen in das Administrator-Konto der regulären Windows-Oberfläche.
4. Führen Sie die notwendigen Änderungen am System durch.
 - In der Regel ist ein Neustart erforderlich, um die Änderungen zu übernehmen.

8.3.2 System neu starten

1. Öffnen Sie das Menü **Maintenance**.
2. Klicken Sie im Bereich **Main** auf *Restart System*.
Es erscheint eine Sicherheitsabfrage.
3. Bestätigen Sie die Sicherheitsabfrage mit Yes.
 - Das System startet neu.

8.3.3 System herunterfahren

Für bestimmte Änderungen in der Firmware ist ein Neustart des Thin-Clients erforderlich.

1. Öffnen Sie das Menü **Maintenance**.
2. Klicken Sie im Bereich **Main** auf *Shutdown System*.
Es erscheint eine Sicherheitsabfrage.
3. Bestätigen Sie die Sicherheitsabfrage mit Yes.
 - Das System fährt herunter.

8.3.4 Advanced Startup

"Advanced Startup" ist ein spezielles Menü, das erweiterte Optionen zur Fehlerbehebung und Wartung des Betriebssystems bietet. Es ermöglicht, verschiedene Tools und Modi zu verwenden, um Probleme zu beheben, Diagnosen durchzuführen oder das System zu konfigurieren. Hier sind die Hauptfunktionen und Optionen, die über "Advanced Startup" zugänglich sind:

1. Zugriff auf erweiterte Reparatur- und Wiederherstellungsoptionen

- **Systemwiederherstellung:** Setzt das System auf einen vorherigen Wiederherstellungspunkt zurück, ohne persönliche Dateien zu löschen.
- **Systemabbild-Wiederherstellung:** Stellt das System von einem zuvor erstellten Abbild (Backup) wieder her.

2. Problembehandlung (Troubleshoot)

- **Einstellungen zurücksetzen:** Ermöglicht das Zurücksetzen von Windows auf die Werkseinstellungen, mit oder ohne Beibehaltung persönlicher Dateien.
- **Eingabeaufforderung:** Öffnet eine Befehlszeile für erweiterte Diagnosen und Reparaturen.
- **Startreparatur:** Behebt häufige Probleme, die den Start von Windows verhindern.
- **Start-Einstellungen ändern:** Ermöglicht das Booten im abgesicherten Modus oder das Deaktivieren erweiterter Treiberoptionen.

3. Boot-Optionen

- **Boot-Manager anzeigen:** Wähle zwischen verschiedenen installierten Betriebssystemen.
- **Start von einem anderen Gerät:** Ermöglicht das Booten von einer CD/DVD, einem USB-Stick oder über das Netzwerk.

4. Treiber und Einstellungen anpassen

- **Deaktivierung der Treibersignaturprüfung:** Nützlich für die Installation nicht signierter Treiber.
- **Deaktivierung erzwungener Neustarts bei Fehlern:** Ermöglicht das Anzeigen von Bluescreen-Fehlern (BSOD).

5. UEFI/BIOS-Optionen

- **UEFI-Firmware-Einstellungen:** Erlaubt den Zugriff auf BIOS-/UEFI-Einstellungen, z.B. zum Aktivieren von Secure Boot oder Ändern der Boot-Reihenfolge.

8.3.5 Einstellungen zurücksetzen

Sie können die Einstellungen der Firmware auf den Auslieferungszustand zurücksetzen.

Ein Reset bedeutet:

- Löschen der Adressbuch-Einträge
- Löschen der Applikationsliste
- Zurücksetzen der Netzwerk-Konfiguration auf "automatisch"

Nicht geändert werden:

- Tastatur-Layout
- Windows Text- und Elementgröße
- Computer Name

Sie können die Adressbuch-Einträge, die Applikationsliste und Netzwerkeinstellungen über einen Export separat speichern. Über einen Import können Sie intakte Einstellungen wieder laden (siehe [8.11 Import und Export](#)).

HINWEIS

IT-Netzwerk-Kenntnisse erforderlich

Führen Sie den Reset nur durch, wenn Sie sich mit der Konfiguration des Thin-Client auskennen.

1. Öffnen Sie das Menü **Maintenance**.
2. Klicken Sie im Bereich **Main** auf *Reset all Settings*.
Es erscheint eine Sicherheitsabfrage.
3. Bestätigen Sie die Sicherheitsabfrage mit Yes.
 - Das System wird auf den Auslieferungszustand zurückgesetzt.

8.3.6 Peripherie-Gerät koppeln oder hinzufügen

In diesem Dialog können Sie Peripherie-Geräte, wie USB- oder Bluetooth-Geräte koppeln oder hinzufügen.

1. Öffnen Sie das Menü **Maintenance**.
2. Schließen Sie das neue Gerät am Thin-Client an.
3. Klicken Sie im Bereich **Device** auf *Add/Pair Device*.
Das System wechselt auf die Systemebene zum Fenster **Control Panel/Hardware and Sound/Devices and Printers**.
4. Fügen Sie ein neues Gerät über *Add a device* hinzu.
5. Der Systemdialog zum Hinzufügen eines Geräts startet.
6. Wählen Sie den Gerätetyp aus.
7. Folgen Sie den Anweisungen im Systemdialog.
8. Nach der Installation der Gerätetreiber und der Konfiguration des Geräts, können Sie das Gerät nutzen.
9. Testen Sie, ob das Gerät einwandfrei funktioniert.

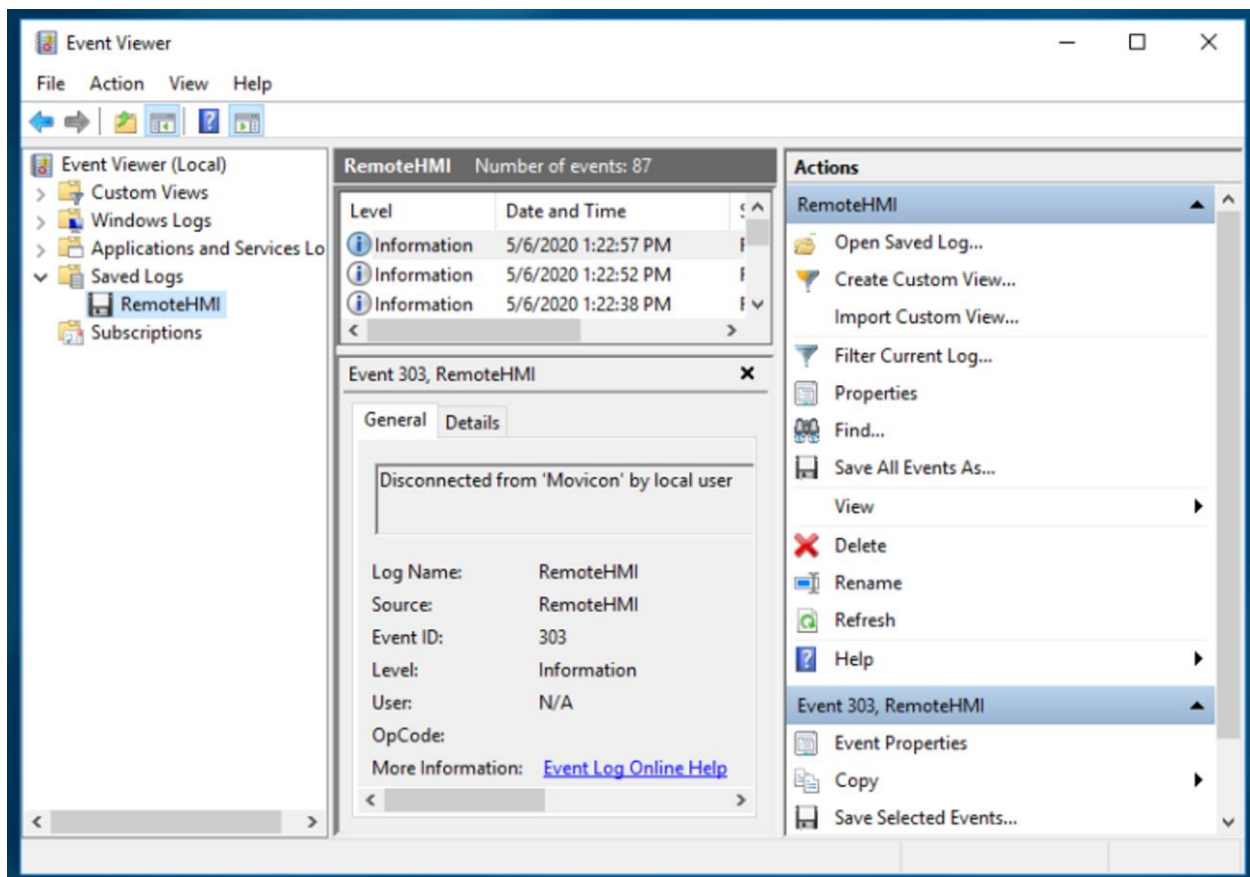
8.3.7 Event Log aufrufen

Liste der Ereignisse öffnen

1. Öffnen Sie das Menü **Maintenance**.
2. Klicken Sie im Bereich **Event Log** auf *View Event Log*.
Das System wechselt auf die Systemebene zum "Event Viewer".



Die Auflistung der letzten Ereignisse kann einige Zeit beanspruchen. Warten Sie, bis sich die Liste aufgebaut hat.



- Der Liste können Sie alle Ereignisse entnehmen.

8.3.8 Pro-Lizenz aktivieren

	Der UWF-Filter muss deaktiviert sein, um den Vorgang ausführen zu können.
	Wenn der Thin-Client einen Internet-Zugang hat, können Sie die Pro-Lizenz Online aus der Firmware heraus aktivieren. Im anderen Fall müssen Sie den Aktivierungscode auf der Internetseite remotehmi-licensing.stahl.de anfordern.

Lizenz Online über einen Internet-Zugang aktivieren

1. Öffnen Sie das Menü **Maintenance**.
2. Stellen Sie sicher, dass der Thin-Client Zugang zum Internet hat.
3. Wählen Sie im Bereich **Pro Edition License Activation** die Funktion **Online**.
4. Geben Sie unter **Product key** den erhaltenen Lizenzschlüssel ein.
5. Geben Sie unter **Company Name** den Firmennamen ein.
6. Geben Sie unter **Name** den Namen des Lizenznehmers ein.
7. Geben Sie unter **Email Address** die E-Mailadresse des Lizenznehmers ein.
8. Klicken Sie auf *Activate Pro License*.
Das System gibt eine Meldung aus.
Wenn die Aktivierung erfolgreich war, wird der Bereich **Pro Edition License Activation** ausgeblendet.

Lizenz Offline aktivieren

	Zur Aktivierung der Lizenz benötigen Sie die Installations-ID des Geräts und den Produktschlüssel (Lizenzschlüssel). Zusätzlich wird ein Gerät mit Internet-Zugang benötigt.
---	--

1. Öffnen Sie das Menü **Maintenance**.
2. Wählen Sie im Bereich **Pro Edition License Activation** die Funktion **Offline**.
3. Öffnen Sie im Browser folgende Internetseite remotehmi-licensing.stahl.de.
4. Wählen Sie die Seite **License Activation**.

5. Füllen Sie das Formular aus und fordern Sie den Aktivierungscode an.

Product key : XXXXX-XXXX-XXXX-XXXX-XXXX
 Make sure you enter the product key in the format XXXX-XXXX-XXXX-XXXX-XXXX.

Installation ID : Enter Installation ID
 Please check the license page for the Installation ID

Name : Enter your name
 Email : Enter your email address
 The activation key will be send to this email address

Company : Enter company name
 Address : Enter address

City : City State : State Zip/Postal Code : Zip Country : Country

REQUEST CODE NEED ANY HELP ?

- HINWEIS:
 Sie erhalten den Aktivierungscode automatisch per E-Mail adressiert an die im Formular angegebene E-Mailadresse. Dies kann bis zu 5 Minuten dauern. Wenn Sie keine E-Mail erhalten, sehen Sie im Spam-Ordner nach.
6. Geben Sie im Menü **Maintenance** unter **Product key** den Produktschlüssel und unter **Activation Code** den erhaltenen Aktivierungscode ein.
7. Klicken Sie auf *Apply Pro License*.
 Das System gibt eine Meldung aus.
 Wenn die Aktivierung erfolgreich war, wird der Bereich **Pro Edition License Activation** ausgeblendet.

8.3.9 Windows aktivieren

	Der UWF-Filter muss deaktiviert sein, um den Vorgang ausführen zu können.
---	---

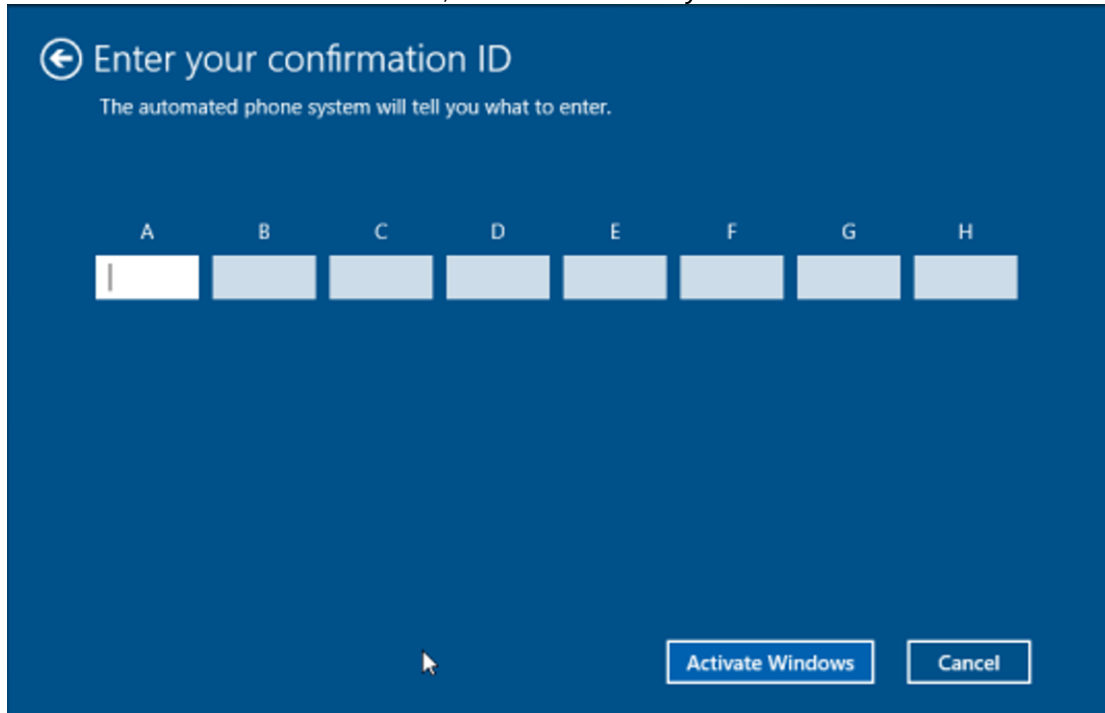
Das Betriebssystem Windows 10 IoT Enterprise LTSC ist bei Auslieferung bereits aktiviert. Wenn zum Beispiel nach dem Wiederherstellen des Systems Windows 10 IoT Enterprise LTSC deaktiviert ist, können Sie es per Telefon oder über einen Internet-Zugang aktivieren. Ein Systemdialog leitet Sie durch die telefonische Aktivierung.

Betriebssystem per Telefon aktivieren

	Die Aktivierung erfolgt über den telefonischen Service-Dienst von Microsoft.
---	--

1. Öffnen Sie das Menü **Maintenance**.
2. Klicken Sie im Bereich **Windows Activation** auf *Activate by phone*.
 Der Systemdialog zur Windows Aktivierung startet.
3. Wählen Sie im Fenster **Select your country or region** das gewünschte Land oder die Region aus.
4. Klicken Sie auf *Next*, um ins Fenster **Call and provide your installation ID** zu wechseln.
5. Wählen Sie die angegebene Telefonnummer und folgen Sie den Anweisungen im Telefondialog.

6. Klicken Sie auf *Next*, um ins Fenster **Enter your confirmation ID** zu wechseln.
7. Geben Sie die Bestätigungs-ID ein.
8. Klicken Sie auf *Activate Windows*, um das Betriebssystem zu aktivieren.

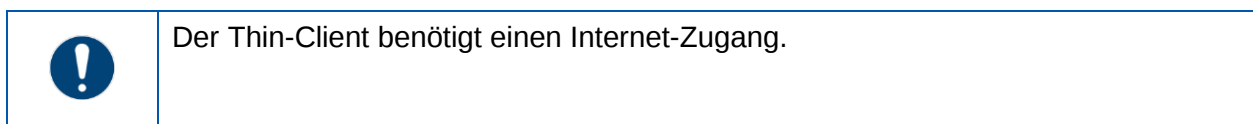


Das System gibt eine Meldung aus.

Wenn die Aktivierung erfolgreich war, wird der Bereich **Windows Activation** ausgeblendet.

- Im Menü **Information** wird unter **System** das aktivierte Betriebssystem aufgeführt.

Betriebssystem über einen Internet-Zugang aktivieren



1. Öffnen Sie das Menü **Maintenance**.
 2. Klicken Sie im Bereich **Windows Activation** auf *Activate over Internet*.
Der Vorgang kann bis zu einer Minute dauern.
 3. Warten Sie bis das System eine Meldung ausgibt.
Wenn die Aktivierung erfolgreich war, wird der Bereich **Windows Activation** ausgeblendet.
- Im Menü **Information** wird unter **System** das aktivierte Betriebssystem aufgeführt.

8.4 System- und Proxy-Einstellungen

Im Menü **System & Proxy** haben Sie folgende Möglichkeiten:

- [8.4.1 Computernamen ändern](#)
- [8.4.4 Einstellungen für den Proxy-Server ändern](#) für VNC- und Remote HMI Device Manager (RDM)
- [8.4.5 Remote-Zugriff konfigurieren](#)
- [8.4.6 Anmeldedaten für den Admin-Account hinterlegen](#)

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.4.1 Computernamen ändern

Der Thin-Client kann über die IP-Adresse oder den Computernamen im Netzwerk adressiert werden. Der Computername kann z.B. bei Remote-Zugriff auf den Thin-Client via VNC verwendet werden. Deshalb sollte der Computername im Netzwerk eindeutig sein.

1. Geben Sie unter **Computer Name** den Namen ein.
 - HINWEIS:
In umfangreichen Netzen kann die Eingabe einer Beschreibung sinnvoll sein, um das Gerät schneller identifizieren zu können.
2. Geben Sie unter **Description** eine aussagekräftige Beschreibung zum Gerät ein.

8.4.2 Datum-, Zeit- und Zahlenformat ändern

Mit dieser Option kann das Format für Datum und Zeitangabe geändert werden.

8.4.3 Stromverbrauch

Über das Betriebssystem kann der Stromverbrauch systemweit verwaltet werden. Das System fährt herunter und, wenn nötig, schnell wieder hoch.

8.4.4 Einstellungen für den Proxy-Server ändern

Durch den Proxy-Server können Zugriffe zum Beispiel auf Internet-Ressourcen kontrolliert und eingeschränkt werden. Die Weiterleitung der Clientanfrage an den Zielservers erfolgt mit der IP-Adresse des Proxy-Servers.

Proxy-Server verwenden

1. Ermitteln Sie die IP-Adresse oder den Netzwerknamen des Proxy-Servers.
2. Aktivieren Sie die Funktion **Use a Proxy Server**.
3. Geben Sie die IP-Adresse oder den Netzwerknamen des Proxy-Servers ein.

Proxy-Server nicht verwenden

1. Deaktivieren Sie die Funktion **Use a Proxy Server**.

8.4.5 Remote-Zugriff konfigurieren

Remote-Zugriff auf den Thin-Client via VNC und RDM konfigurieren

1. Aktivieren Sie **Allow configuration export/import via RemoteHMI Device Manager**, um den Export und Import der Konfiguration des Thin-Client über den RemoteHMI Device Manager zu erlauben.
2. Aktivieren Sie **Allow remote access via VNC**, um den VNC-Remote-Zugriff auf den Thin-Client zu erlauben.
3. Geben Sie ein Passwort für die Fernsteuerung ein.
4. Geben Sie optional ein Passwort für den Remote-Zugriff ohne Bedienerlaubnis ein.
5. Klicken Sie auf *Advanced VNC Server Config*, wenn Sie die VNC-Einstellungen ändern müssen.
6. Stellen Sie unter **Input blocking during remote access** das Zugriffsverhalten während einer Fernverbindung ein.
7. Aktivieren Sie **Off**, um die lokale und die Remote-Bedienung während des Remote-Zugriffs zu erlauben.
8. Aktivieren Sie **Local**, um die lokale Bedienung am Thin-Client während des Remote-Zugriffs zu sperren.
9. Aktivieren Sie **Remote on local activity, inactivity timeout = 3 sec**, um durch die lokale Bedienung die Remote-Bedienung während des Remote-Zugriffs zu sperren. Die Sperre wird aufgehoben, wenn für eine festgelegte Sperrzeit keine lokale Bedienung erfolgt. Die Sperrzeit beträgt bei Auslieferung 3 Sekunden und kann angepasst werden.
10. Um die Sperrzeit anzupassen, klicken Sie auf *Advanced VNC Server Config*.

8.4.6 Anmeldedaten für den Admin-Account hinterlegen

In den **Windows Admin Account Login Credentials** können Sie die Anmeldedaten für den Zugriff auf das Windows Administrator-Konto hinterlegen. Die Anmeldedaten werden benötigt, wenn über die Firmware Applikationen gestartet werden sollen, die Administrator- oder erweiterte (elevated) Rechte erfordern.

Das Hinterlegen der Anmeldedaten

- verhindert, dass bei jedem Start der App die Anmeldedaten neu angegeben werden müssen
 - erlaubt das Starten der App durch Benutzer, die die Anmeldedaten nicht kennen
1. Geben Sie unter **Name** und **Password** die Anmeldedaten des Windows Admin-Accounts ein.

8.5 Protection

Im Menü **Protection** haben Sie folgende Möglichkeiten:

- [8.5.1 Firewall und Virenschutz aktivieren](#)
- [8.5.2 Schreibschutz für die SSD aktivieren](#)
- [8.5.3 USB-Lockdown aktivieren](#)
- [8.5.4 Systemverhalten bei Neustart konfigurieren](#)

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.5.1 Firewall und Virenschutz aktivieren

Es wird empfohlen, die Windows Firewall und den Virenschutz zu aktivieren und alle notwendigen Sicherheitsupdates zuzulassen. Bei der Auslieferung sind diese Funktionen aktiviert.

Windows-Sicherheit aktivieren



Das automatische Herunterladen der Sicherheitsupdates erfordert einen Internetzugang am Thin-Client. Wenn die Funktion deaktiviert ist, müssen Sie die Updates manuell überwachen, bereitstellen und auf der Systemebene ausführen.

1. Aktivieren Sie die **Windows Firewall**.
2. Aktivieren Sie den **Windows Defender**
3. Aktivieren Sie die **Windows Security Updates**, um das Installieren der Sicherheitsupdates zu zulassen.

8.5.2 Schreibschutz für die SSD aktivieren

Der Unified Write Filter (UWF) ist ein Schreibschutz für die SSD und kann im Menü **Protection** aktiviert werden. Der UWF dient dem Schutz vor unbeabsichtigtem Schreiben auf der SSD und leitet alle schreibenden Zugriffe in einen Overlay-Puffer im Arbeitsspeicher (RAM) um.

Der UWF verhindert so einen vorzeitigen Verschleiß (Wearout) der SSD und ein Korumpieren von Systemdateien bei einem plötzlichen Netzausfall. Darüber hinaus werden Viren oder Trojaner nicht dauerhaft im System gespeichert, da alle Änderungen im Overlay-Puffer beim Ausschalten entfernt werden.

HINWEIS

Neustart des Systems erforderlich

Das Aktivieren des Speicherschutzes (UWF) erfordert einen Neustart des Systems.

Schutz des Datenspeichers aktivieren

1. Aktivieren Sie im Menü **Protection** die Funktion **Drive Protection (UWF)**.
2. Bestätigen Sie die Aufforderung zum Neustart.
 - Nach dem Neustart ist der Schutz des Datenspeichers aktiviert.

8.5.3 USB-Lockdown aktivieren

Abhängig von Ihrem Sicherheitskonzept können Sie im Menü **Protection** die Verwendung von USB-Geräten blockieren oder die Verwendung für angeschlossene USB-Geräte freigeben. Über die Teach-In-Funktion können weitere Geräte freigeben werden.

Verwendung von USB-Massenspeichern blockieren

1. Aktivieren Sie unter USB-Lockdown die Funktion **Block USB mass storage devices only**.
2. Bestätigen Sie die Auswahl mit *Apply*.
Alle USB-Speichergeräte sind gesperrt.

Verwendung von neuen USB-Geräten blockieren



Mit dieser Funktion werden alle USB-Geräte blockiert, die nicht am Thin-Client angeschlossen sind oder zuvor angeschlossen waren.

1. Öffnen Sie das Menü **Protection**.
 2. Aktivieren Sie unter USB-Lockdown die Funktion **Block access to USB devices**.
 3. Aktivieren Sie **Block new USB devices only**.
 4. Bestätigen Sie die Auswahl mit *Apply*.
Die Kenndaten der angeschlossenen USB-Geräte werden gespeichert.
- Neue USB-Geräte sind gesperrt.

Verwendung von angeschlossenen USB-Geräten freigeben

1. Aktivieren Sie unter USB-Lockdown die Funktion **Block access to USB devices**.
 2. Schließen Sie die USB-Geräte an, die Sie freigeben wollen.
 3. Aktivieren Sie **Block all USB devices except connected**.
 4. Bestätigen Sie die Auswahl mit *Apply*.
Die Kenndaten der angeschlossenen USB-Geräte werden gespeichert.
- Alle registrierten USB-Geräte sind für die Nutzung freigegeben.

Verwendung weiterer USB-Geräte freigeben (Teach-In)

1. Aktivieren Sie unter USB-Lockdown die Funktion **Block all USB devices except connected**.
 2. Deaktivieren Sie **Block access to USB devices**.
 3. Entfernen Sie bei Bedarf bereits angeschlossene USB-Geräte und schließen Sie die neuen USB-Geräte an.
 4. Aktivieren Sie den Eintrag **Block new USB devices only**.
 5. Wiederholen Sie die Schritte 2 bis 4, um weitere Geräte hinzuzufügen.
 6. Wenn Sie alle Geräte hinzugefügt haben, klicken Sie auf *Apply*.
- Alle registrierten USB-Geräte sind für die Nutzung freigegeben.

8.5.4 Systemverhalten bei Neustart konfigurieren

Die HORM-Funktion (Hibernate Once Resume Many) erlaubt einen schnellen Start des Thin-Client aus einem fixen Systemabbild (Snapshot). Das System befindet sich nach dem Start wieder exakt in dem Zustand, in dem der letzte HORM-Snapshot erstellt wurde. Dies bedeutet, dass laufende Applikationen der Pro-Version nicht neu gestartet werden müssen, sondern sofort zur Verfügung stehen.

HINWEIS

Backup der Gerätekonfiguration erforderlich

Das Erstellen eines Snapshots (Abbild des Arbeitsspeichers) erfordert einen Neustart des Systems.

- Erstellen Sie ein Backup Ihrer Gerätekonfiguration, um Datenverlust zu vermeiden (siehe [8.11 Import und Export](#)).

Snapshot des Arbeitsspeichers erstellen

1. Aktivieren Sie den Speicherschutz unter **Drive Protection (UWF)**.
2. Aktivieren Sie die Funktion **Resume System from same snapshot on every device startup**.
3. Bestätigen Sie die Auswahl mit *Apply*.
4. Bestätigen Sie die Aufforderung zum Neustart.
5. Klicken Sie auf *Snapshot*, um ein Abbild des Arbeitsspeichers zu erstellen.
6. Bestätigen Sie die Aufforderung zum Neustart, um den Snapshot zu erstellen und das System neu zu starten.



Der Neustart kann einige Zeit in Anspruch nehmen.

Falls das System nicht ordnungsgemäß startet, kann es mit dem "Recovery Stick" in den Auslieferungszustand zurückgesetzt werden. Der Stick wird mit dem Gerät ausgeliefert.

Abhängig vom Recovery Stick können Sie auch die Gerätekonfiguration als Backup sichern.

8.6 Display-Einstellungen

Im Menü **Display** haben Sie folgende Möglichkeiten:

- [8.6.1 Display-Einstellungen anpassen](#)
- [8.6.2 Multi-Display-Einstellungen anpassen](#)

Über folgende Parameter können Sie die Darstellung auf dem Display anpassen:

- **Resolution:** Auflösung und Ausrichtung
- **Multi Display:** Anordnung (Topology) und Hauptbildschirm (bei Anschluss von mehrerer Displays)
- **Scaling:** Skalierung
- **Windows Text and Items:** Größe der Text- und Bildelemente für Windows Anwendungen
- **Screen Saver:** Bildschirmschoner

- **Backlight Auto Dimming:** Automatisches Dimmen der Hintergrundbeleuchtung (für einen Touchscreen)

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.6.1 Display-Einstellungen anpassen

Auflösung anpassen

1. Wählen Sie unter **Resolution** die Auflösung der angeschlossenen Displays (maximal 6).
2. Aktivieren Sie **Portrait Mode**, um die Bildinhalte im Hochformat darzustellen.

Skalierung anpassen

1. Aktivieren Sie **Always stretch to fullscreen**, um Bildinhalte immer im Vollbild darzustellen.
Die Funktion kann zu einer verzerrten Darstellung führen.
2. Aktivieren Sie **Maintain aspect ratio**, um das Seitenverhältnis der Bildinhalte beizubehalten.

Windows Text- und Elementgröße ändern



Die Einstellungen sind nur für lokale Anwendungen und RDP-Verbindungen unter Windows 10/Server 2012 gültig.
Eine größere Darstellung erhöht die Bedienbarkeit des Touchscreens.
Einstellungen über 100 % können zu einer fehlerhaften Darstellung von lokalen und per RDP ausgeführten Apps führen.

- Wählen Sie die gewünschte Größe der Windows-Elemente, empfohlene Einstellung 125 %.
- Wenn lokale oder per RDP ausgeführte Apps fehlerhaft dargestellt werden, setzen Sie die Einstellung auf 100 % zurück.

Bildschirmschoner einschalten

1. Aktivieren Sie unter **Screen Saver** den Bildschirmschoner.
2. Stellen Sie unter **After user inactivity of** die Zeitspanne zur Aktivierung des Bildschirmschoners ein (1 bis 60 Minuten).
3. Klicken Sie auf *Advanced*, um die Einstellungen für den Bildschirmschoner zu öffnen.
4. Wählen Sie einen Bildschirmschoner und bestätigen Sie die Eingabe.
5. Öffnen Sie das Menü **Display**.
 - Der Bildschirmschoner startet, sobald der Benutzer länger als die festgelegte Aktivierungszeit inaktiv war.

Hintergrundbeleuchtung automatisch dimmen



Um die Lebensdauer der Hintergrundbeleuchtung zu erhöhen, empfehlen wir die Funktion **Backlight Auto Dimming** zu aktivieren.

1. Aktivieren Sie unter **Backlight Auto Dimming** das automatische Dimmen der Hintergrundbeleuchtung.
 2. Stellen Sie unter **After user inactivity of** die Zeitspanne zur Aktivierung der Dimmfunktion ein (1 bis 60 Minuten).
 3. Stellen Sie unter **to brightness level** den Pegel ein, auf den gedimmt werden soll (1 % bis 80 %).
- Die Hintergrundbeleuchtung wird auf den Pegel gedimmt, sobald der Benutzer länger als die festgelegte Aktivierungszeit inaktiv war.

8.6.2 Multi-Display-Einstellungen anpassen

Sie können die Auflösung und Ausrichtung für jedes Display einstellen. Zusätzlich können Sie die Anordnung (Topology) und den Hauptbildschirm wählen.



Die Bezeichnung der Displays in der Firmware entspricht dem Port, an dem das Display angeschlossen ist.

Anordnung der Displays anpassen

1. Wählen Sie im Feld **Topology** die Auflösung des jeweiligen Displays.
2. Aktivieren Sie die Funktion **Clone**, wenn die Bildschirminhalte auf beiden Displays dargestellt werden sollen.
3. Aktivieren Sie die Funktion **Extend**, wenn das zweite Display die Darstellung des Hauptdisplays erweitern soll.
4. Wählen Sie die unter **Primary Display Position** den Hauptbildschirm (**left, right**).

8.7 User Interface

Im Menü **User Interface** haben Sie folgende Möglichkeiten:

- [8.7.1 Größe des Menüs und der virtuellen Tastatur verändern](#)
- [8.7.2 Tastaturlayout ändern](#)
- [8.7.3 Funktionen der Bedienoberfläche konfigurieren](#)

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.7.1 Größe des Menüs und der virtuellen Tastatur verändern



Die Größe der Tastatur kann auf Shark-Geräten mit Intel i7 CPU nicht über die Firmware verändert werden.

Größe des Menüs und der Tastatur einstellen

1. Öffnen Sie das Menü **User Interface**.
2. Stellen Sie unter **RemoteHMI Menu** über den Schieberegler die Größe des Menüs ein.
3. Stellen Sie unter **Virtual Keyboard** über den Schieberegler die Größe der Tastatur ein.

Gerätespezifische Werkseinstellungen wiederherstellen

1. Öffnen Sie das Menü **User Interface**.
2. Klicken Sie unter **RemoteHMI Menu** auf *Default*, um die gerätespezifischen Werkseinstellungen für die Menügröße wiederherzustellen.
3. Klicken Sie in **Virtual Keyboard** auf *Default*, um die gerätespezifischen Werkseinstellungen für die Tastaturgröße wiederherzustellen.

8.7.2 Tastaturlayout ändern

Das Tastatur-Sprachlayout ist werksseitig auf das US amerikanische Layout "QWERTY" eingestellt. Die Einstellung betrifft die virtuelle und eine extern angeschlossene Tastatur (optional). Das Sprachlayout ist unabhängig von Design, Kodierung, Lage und Anzahl der Tasten auf der physischen Tastatur.



Innerhalb der Thin-Client-Systemkonsole ist die Sprache auf Englisch eingestellt und kann **NICHT** verändert werden!

Die Firmware unterstützt für die virtuelle und extern angeschlossene Tastatur verschiedene Sprachlayouts. Die Länderkürzel der Sprachlayouts entstammen der ISO 3166-1, Unterspalte ALPHA-2.

Länderkürzel	Name des Landes
BE	Belgien
BR	Brasilien
CH	Schweiz
CZ	Tschechische Republik
DE	Deutschland
DK	Dänemark
ES	Spanien
FI	Finnland
FR	Frankreich
GR	Griechenland
HU	Ungarn
IT	Italien
NL	Niederlande
NO	Norwegen
PL	Polen
PT	Portugal

RU	Russische Föderation
SE	Schweden
SI	Slowenien
TR	Türkei
US	Vereinigte Staaten von Amerika

Tastaturlayout einstellen

1. Öffnen Sie das Menü **User Interface**.
2. Wählen Sie in **Keyboard-Layout** das gewünschte Tastaturlayout aus.
3. Wenn das benötigte Tastaturlayout nicht angezeigt wird, können Sie über *Add/Remove* ein weiteres Layout hinzufügen.

8.7.3 Funktionen der Bedienoberfläche konfigurieren

Tastaturkurzbefehl (Hotkey) zum Öffnen der Firmware

Sie können das Öffnen der Firmware wie folgt festlegen:

- Der Hotkey schaltet das Dashboard zwischen dem geschlossenen und minimierten Zustand (Standard)
- Der Hotkey schaltet das Dashboard zwischen dem geschlossenen, minimierten und erweiterten Zustand (**Hotkey toggles all 3 menu states**)

Unter **Ignore hotkeys if RemoteHMI menu is closed** können Sie festlegen, ob die verwendeten Tastaturkurzbefehle zum Aufruf von Remote-Verbindungen und Applikationen bei geschlossenem Dashboard ignoriert werden sollen. Die definierten Tastaturkurzbefehle sind nur wirksam, wenn das Dashboard geöffnet ist. Diese Funktion erlaubt die Verwendung von gleichen Tastaturkurzbefehlen auch für andere Zwecke.

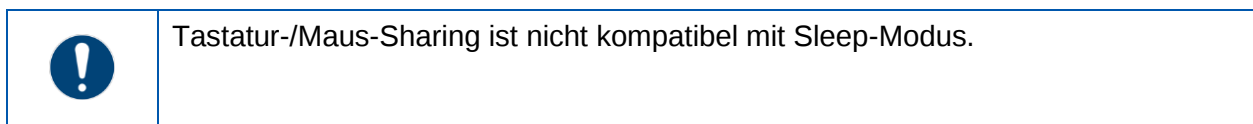
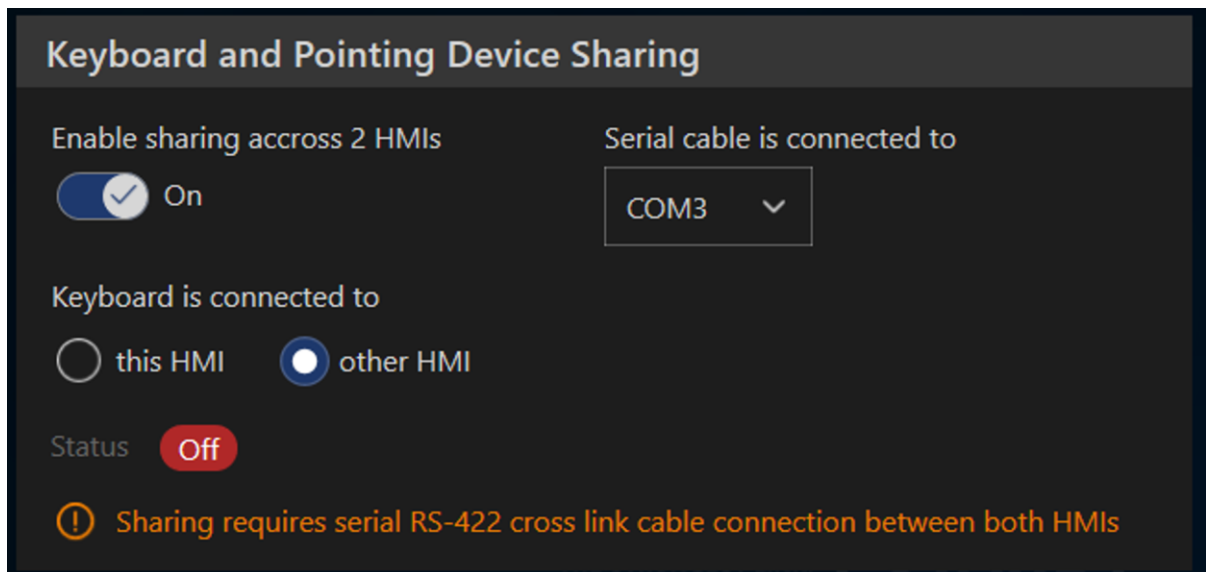
Wenn ein Tastaturkurzbefehl zum Öffnen des Dashboards definiert ist, ist dieser immer aktiv. Er wird durch diese Funktion nicht beeinflusst.

Bedienoberfläche konfigurieren

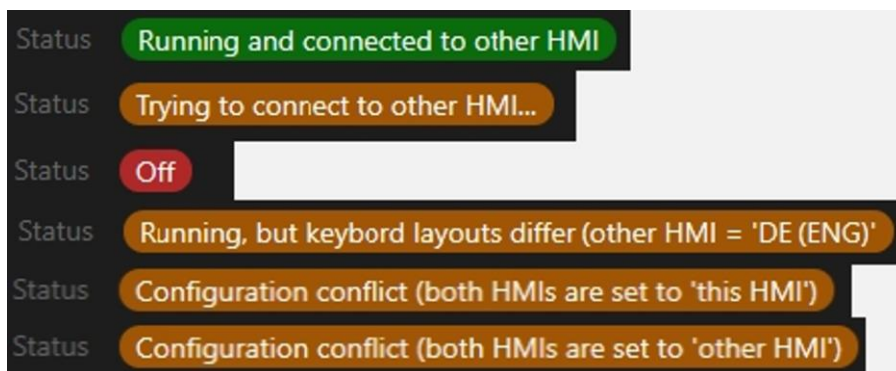
1. Öffnen Sie das Menü **User Interface**.
2. Aktivieren Sie **Show computer name in title**, um den Computernamen im verkleinertem Dashboard anzuzeigen.
3. Aktivieren Sie **Auto hide after connect**, um das Dashboard nach erfolgreichem Verbindungsaufbau auszublenden.
4. Aktivieren Sie **Hotkey toggles all 3 menu states**, um alle drei Menü Zustände über den Tastaturkurzbefehl zu schalten.
5. Legen Sie den Tastaturkurzbefehl zum Öffnen des Dashboards fest.
6. Aktivieren Sie **Ignore hotkeys if RemoteHMI menu is closed**, wenn die Tastaturkurzbefehle bei geschlossenem Menü ignoriert werden sollen.

8.7.4 Tastatur und Zeigegerät Sharing

Im Menü "Keyboard und Pointing Device Sharing" kann die Tastatur und das Zeigegerät mit anderen HMIs geteilt werden. Um diese Funktion zu nutzen, müssen beide HMIs mit einem RS-422 crosslinked-Kabel verbunden sein.



Wird die Sharing-Option aktiviert, erscheint dieses Fenster, in dem der Status des Tastatur-Sharing angezeigt wird.

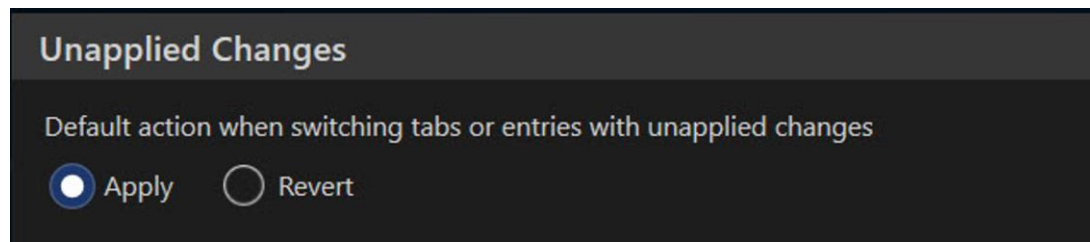


Ist die Verbindung aufgebaut, leuchten auf beiden HMIs die Tastaturicons dauerhaft.

Das HMI welches gerade aktiv ist, bei dem leuchtet das Tastaturicon grün  und bei dem HMI welches im Standby ist, leuchtet das Tastaturicon orange . Wird die Verbindung unterbrochen, fangen beide Icons an zu blinken, wobei die Farbgebung erhalten bleibt.

8.7.5 Übernahme von Änderungen konfigurieren

1. Öffnen Sie das Menü **User Interface**.
2. Aktivieren Sie **Apply**, wenn die Änderungen beim Verlassen des Registers übernommen werden sollen.
 - Sobald Sie in einen anderen Reiter wechseln, werden die Einstellungen übernommen.
3. Aktivieren Sie **Revert**, wenn die Änderungen über den Button *Apply* übernommen werden sollen.



Wenn Sie nicht auf *Apply* klicken, werden die Änderungen verworfen.

8.8 Keyboard Wedge

Die Funktion **Keyboard Wedge** sendet ASCII-basierte Daten einer seriellen Schnittstelle als Tastatur-generierte Zeichen an den Host. Die übertragenen Daten werden in der Zielapplikation wie reale Eingaben der Tastatur interpretiert. Mit der Funktion können Scans von Lesegeräten wie Barcode-Scanner oder RFID-Leser in Tastatureingaben umgewandelt werden.

HINWEIS
Für den Vorgang sind Administratorrechte erforderlich.

Im Menü **Keyboard Wedge** haben Sie folgende Möglichkeiten:

- [8.8.1 Gerät hinzufügen](#)
- [8.8.2 COM-Schnittstelle parametrieren](#)

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.8.1 Gerät hinzufügen

Treiber von einem USB-Massenspeicher installieren

	Der UWF-Filter muss deaktiviert sein, um den Gerätetreiber installieren zu können.
---	--

1. Prüfen Sie, ob der Thin-Client den Systemvoraussetzungen des Eingabegeräts entspricht.
2. Stellen Sie sicher, dass der USB-Massenspeicher ein bekanntes Gerät ist oder deaktivieren Sie den USB-Lockdown.
3. Öffnen Sie das Menü **Maintenance**.
4. Öffnen Sie über *Add / Remove Device* die Systemeinstellung des Thin-Client.
5. Installieren Sie den Gerätetreiber auf dem Thin-Client.
6. Schließen Sie das Eingabegerät an einen freien COM-Port an. Die Bezeichnung des COM-Ports ist abhängig von der HMI-Geräteplattform.
7. Öffnen Sie das Menü **Keyboard Wedge**.
8. Aktivieren Sie **Simulate keyboard input via a connected reader/scanner device**.
9. Klicken Sie auf + *Add / Auto Connect*, um das Gerät zu verbinden.

8.8.2 COM-Schnittstelle parametrieren



Die Konfiguration der COM-Schnittstelle muss der Spezifikation des Lesegeräts entsprechen, um eine korrekte Datenübertragung zu gewährleisten.

Port	Legt den seriellen Anschluss fest, an dem die Daten des Lesegeräts empfangen werden
Baudrate	Legt die Datenübertragungsrate des COM-Ports fest, muss dem Lesegerät entsprechen 2400 / 4800 / 9600 / 19200 / 38400
Data Bits	Gibt die Länge der übertragenen Datenbits an 7: Ein Zeichen ist 7 Bit lang 8: Ein Zeichen ist 8 Bit lang (üblicher Wert)
Stop Bits	Gibt die Anzahl der Bits an, die das Ende einer Zeichenübertragung kennzeichnen 1: Stoppbit ist ein Bit lang (üblicher Wert) 2: Stoppbit ist zwei Bits lang
Parity	Gibt an, ob und wie das Paritätsprüfbit berechnet werden soll NONE: kein Bitprüfverfahren EVEN: Summe der Bits eines zu übertragenden Zeichens ist gerade ODD: Summe der Bits eines zu übertragenden Zeichens ist ungerade

1. Öffnen Sie das Menü **Keyboard Wedge**.
2. Wählen Sie unter **Serial Communication** den COM-Port des angeschlossenen Geräts.
3. Wählen Sie die passende Baudrate für das angeschlossene Gerät.
4. Legen Sie die Parameter **Data Bits**, **Stop Bits** und **Parity** für die serielle Schnittstelle fest.
Eine aktive Verbindung wird im Status angezeigt.

Behandlung von Steuerzeichen konfigurieren



Sie können festlegen, ob vom Barcodescanner gesendete Steuerzeichen für den Zeilenumbruch das Drücken der Eingabetaste (Enter) simulieren sollen. Dies kann erforderlich sein, damit ein eingescannter Barcode korrekt abgeschlossen und übernommen wird.

CR: englisch carriage return
LF: englisch line feed

1. Aktivieren Sie **Translate CR to Enter-key**, um "CR" als Steuerzeichen zu verwenden.
2. Aktivieren Sie **Translate LF to Enter-key**, um "LF" als Steuerzeichen zu verwenden.

Server Tastaturlayout einstellen



Damit die eingescannten Zeichen vor allem Sonderzeichen korrekt verarbeitet werden, müssen die Tastaturlayouts der beteiligten Geräte übereinstimmen. Wenn der Thin-Client auf das US-Layout eingestellt ist, muss dieses Layout auch auf dem verbundenen Server eingestellt sein. Bei Verbindungen über eine KVM-Box müssen Sie das Layout zusätzlich in der Bedienoberfläche der KVM-Box einstellen.

Folgende Einstellungen sind unter **Server Keyboard Layout** möglich:
US Amerikanische Tastaturbelegung: QWERTY-Anordnung
DE Deutsche Tastaturbelegung: QWERTZ-Anordnung
FR Französische Tastaturbelegung: AZERTY-Anordnung

1. Setzen Sie **Server Keyboard Layout** auf "US", um die einwandfreie Funktion zu gewährleisten.

Verzögerung der Datenübertragung einstellen



KVM Keystroke Delay bestimmt die Verzögerung, die eingehalten wird, bis das nächste Zeichen an eine KVM-Box weitergeleitet wird. Die Verzögerung stellt sicher, dass bei einem schnellen Zeichenempfang keine Zeichen bei der Übermittlung an den Host verloren gehen. In der Regel ist der Standardwert ausreichend.

1. Vergrößern Sie den Wert nur, wenn bei der Datenübertragung Zeichen verloren gehen.
2. Stellen Sie über den Schieberegler oder die Pfeile die Verzögerung ein, Einstellbereich 1 bis 50 ms.

8.9 Access Control

Im Menü **Access Control** können Sie die dreistufige Benutzerkontrolle aktivieren und das automatische Abmelden des Benutzers konfigurieren.

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.9.1 Benutzerrollen aktivieren

Benutzerrollen aktivieren

1. Öffnen Sie das Menü **Access Control**.
2. Aktivieren Sie unter **Main** die 3-stufige Zugriffskontrolle.
3. Aktivieren Sie **Limit Operator access to Dashboard**, um die Registerleiste im Dashboard für den Operator auszublenden.
Für den Operator sind nur noch die Daten im Dashboard sichtbar.
4. Geben Sie unter **Login Passwords** unterschiedliche Passwörter für die Benutzerrollen "Engineer" und "Admin" ein.
5. Wiederholen Sie die Passworteingabe. Wenn die Passwörter falsch sind, gibt das System eine Fehlermeldung aus.
6. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
► Die Benutzer "Engineer" und "Admin" müssen sich mit ihrem Passwort anmelden.

8.9.2 Automatischen Logout aktivieren

Für die Benutzerrollen Admin und Engineer kann ein automatischer Logout eingestellt werden. Der Benutzer wird automatisch ausgeloggt, sobald er länger als die festgelegte Logoutzeit inaktiv war.

1. Öffnen Sie das Menü **Access Control**.
2. Aktivieren Sie **Auto Logout**, um das automatische Abmelden des Benutzers zu aktivieren.
3. Stellen Sie unter **after user not operating RemoteHMI Menu for** die Logoutzeit ein (1 bis 60 Minuten).

8.10 Connections

Im Menü **Connections** haben Sie folgende Möglichkeiten:

- [8.10.1 Mehrere parallele Verbindungen erlauben](#)
- [8.10.2 Verbindungen automatisch neu aufbauen](#)
- [8.10.3 Status des Host automatisch prüfen](#)

Einstellungen übernehmen oder verwerfen

1. Klicken Sie auf *Apply*, um die Einstellungen zu übernehmen.
2. Klicken Sie auf *Revert*, um die Änderungen zu verwerfen.

8.10.1 Mehrere parallele Verbindungen erlauben

Pro	Pro-Lizenz erforderlich.
------------	--------------------------

Die Funktion **Allow Multiple simultaneous connections** erlaubt die parallele Nutzung mehrerer Remote-Verbindungen (Multi-Session-Verbindungen). So können Sie:

- Die Ansichten zwischen den Remote-Verbindungen wechseln, ohne die Verbindung zu beenden
- Mehrere Remote-Verbindungen auf einem geteilten Display darstellen
- Mehrere Remote-Verbindungen auf zwei oder mehr Displays darstellen

Multi-Session-Verbindung aktivieren

1. Öffnen Sie das Menü **Connections**.
2. Aktivieren Sie **Allow Multiple simultaneous connections**, um den Aufbau mehrerer Remote-Verbindungen zu zulassen.

8.10.2 Verbindungen automatisch neu aufbauen

Unter **On connection loss, auto reconnect** können Sie global die Wartezeit einstellen, nach der bei einem Verbindungsverlust eine Neuverbindung versucht wird

	Die Funktion muss einzeln für jede Remote-Verbindung im Adressbucheintrag aktiviert werden.
---	---

- Öffnen Sie das Menü **Connections**.
- Stellen Sie unter **On connection loss, auto reconnect after** ein, nach wie vielen Sekunden der Verbindungsaufbau wieder gestartet werden soll (1 bis 30 Sekunden).

8.10.3 Status des Host automatisch prüfen

Über die Funktion **Connection Health Check** sendet der Thin-Client zyklisch Pings (Echorequests) an alle im Adressbuch konfigurierten Server. Das Ergebnis des Requests wird als Status der Verbindung im Adressbuch dargestellt.

Der Connection-Health-Check funktioniert nur korrekt, wenn die Firewalls der Server eine Antwort auf einen Echorequest zulassen.

Wenn ein Echorequest nicht erwünscht ist, können Sie die Funktion abschalten. In diesem Fall wird der Status der Verbindung im Adressbuch nicht angezeigt.

Health Check aktivieren

1. Öffnen Sie das Menü **Connections**.
 2. Wenn Sie eine Firewall verwenden, prüfen Sie, ob die Firewall einen Echorequest erlaubt und aktivieren Sie den Echorequest.
 3. Aktivieren Sie **Ping servers to show reachable state on Address Book buttons**, um die Remote-Verbindungen ständig zu überprüfen.
 4. Klicken Sie auf *Apply*.
- Der Thin-Client überwacht die Remote-Verbindungen und zeigt den Status der aktiven Verbindungen an.



Wenn ein Echorequest des Host nicht möglich oder nicht erwünscht ist, deaktivieren Sie **Ping servers to show reachable state on Address Book buttons**.

Die Remote-Verbindungen werden nicht überwacht. Es wird kein Status der Verbindungen angezeigt.

8.11 Import und Export

Die Firmware unterstützt den Import und Export der meisten Einstellungen in die verschlüsselte Datei "RemoteHMI.config". Die Datei kann auf einen USB-Massenspeicher oder auf ein Netzlaufwerk exportiert werden. Beim Import können über einen Filter die Einstellungen gewählt werden, deren Übernahme nicht gewünscht ist (z.B. Netzwerkeinstellungen).

Mit Hilfe dieser Funktion können Sie:

- Die Geräte-Konfiguration nach dem Zurücksetzen des Geräts wiederherstellen
- Die Geräte-Konfiguration auf einen anderen Thin-Client übertragen

Im Menü **Import & Export** haben Sie folgende Möglichkeiten:

- [8.11.1 Gerätedatei importieren](#)
- [8.11.2 Gerätedatei exportieren](#)

HINWEIS

Für den Vorgang sind Administratorrechte erforderlich.

8.11.1 Gerätedatei importieren



Der UWF-Filter muss deaktiviert sein, um den Vorgang ausführen zu können.

HINWEIS

USB-Massenspeicher im Ex-Bereich

Verwenden Sie im Ex-Bereich ausschließlich USB-Massenspeicher in eigensicherer Ausführung.

Für Arbeiten im Ex-Bereich ist ein USBi-Stick erhältlich.

Sie können folgende Einstellungen beim Import ausschließen:

- **Application List:** Liste der Applikationen (siehe [6 App-Verwaltung](#))
- **Network Settings:** Netzwerkeinstellungen (siehe [7 Netzwerk](#))
- **Access Control Password:** Passwörter der Zugriffsberechtigung (siehe [8.9 Access Control](#))

HINWEIS

Nur bekannte Passwörter importieren!

Stellen Sie sicher, dass Ihnen die eingestellten Passwörter bekannt sind, bevor Sie den Import starten.

Konfigurationsdatei von einem USB-Massenspeicher importieren

1. Wenn der USB-Lockdown aktiviert ist, stellen Sie sicher, dass der USB-Massenspeicher ein bekanntes Gerät ist oder deaktivieren Sie den USB-Lockdown.
2. Schließen Sie den USB-Massenspeicher an.
3. Öffnen Sie das Menü **Import & Export**.
4. Wählen Sie im Importfilter die nicht benötigten Konfigurationen.
5. Aktivieren Sie **USB Flash Drive**.
6. Klicken Sie auf *Import*.
Der Fortschritt des Imports wird angezeigt.
Wenn der Vorgang erfolgreich beendet wurde, gibt die Firmware eine Meldung aus.
7. Wenn eine Fehlermeldung ausgegeben wird, prüfen Sie ob, der USB-Massenspeicher richtig gesteckt und nicht schreibgeschützt ist.
8. Entfernen Sie den USB-Massenspeicher, bevor Sie das Gerät neu starten.
 - HINWEIS:
Wenn ein Sie einen bootbaren Recovery PE Lite USB-Massenspeicher nicht entfernen, erwartet das Gerät bei einem Neustart eine Installation der Firmware!
9. Klicken Sie auf *Apply*, um die importierten Einstellungen zu übertragen.
10. Starten Sie das Gerät neu, um die geänderte Konfiguration zu aktivieren.

Konfigurationsdatei von einem Netzlaufwerk importieren

1. Speichern Sie die Import-Datei auf dem Netzlaufwerk.
2. Wählen Sie im Importfilter die nicht benötigten Konfigurationen.
3. Aktivieren Sie **Network**.
4. Klicken Sie auf *Select*, um das Netzlaufwerk im Windows Explorer zu wählen.
5. Klicken Sie auf *Import*.
Der Fortschritt des Imports wird angezeigt.
Wenn der Vorgang erfolgreich beendet wurde, gibt die Firmware eine Meldung aus.
6. Klicken Sie auf *Apply*, um die importierten Einstellungen zu speichern.
7. Starten Sie das Gerät neu, um die geänderte Konfiguration zu aktivieren.

8.11.2 Gerätedatei exportieren**Konfigurationsdatei auf einen USB-Massenspeicher exportieren**

1. Wenn der USB-Lockdown aktiviert ist, stellen Sie sicher, dass der USB-Massenspeicher ein bekanntes Gerät ist oder deaktivieren Sie den USB-Lockdown.
2. Schließen Sie den USB-Massenspeicher an.
3. Aktivieren Sie **USB Flash Drive**.
4. Klicken Sie auf *Export*.
Der USB-Massenspeicher wird geprüft.
Wenn keine Konfigurationsdatei vorhanden ist, wird diese sofort gespeichert.
5. Wenn bereits eine Konfigurationsdatei vorhanden ist, bestätigen Sie das Überschreiben der vorhandenen Datei.
Wenn der Vorgang erfolgreich beendet wurde, gibt die Firmware eine Meldung aus. Die Datei RemoteHMI.config ist im Root-Verzeichnis des USB-Massenspeichers gespeichert.
6. Entfernen Sie den USB-Massenspeicher.



Wenn ein Sie einen bootbaren Recovery PE Lite USB-Massenspeicher nicht entfernen, erwartet das Gerät bei einem Neustart eine Installation der Firmware!

Konfigurationsdatei auf ein Netzlaufwerk exportieren

1. Aktivieren Sie **Network**.
2. Klicken Sie auf *Select*, um das Netzlaufwerk im Windows Explorer zu wählen.
3. Klicken Sie auf *Export*.
Das Netzlaufwerk wird geprüft.
Wenn keine Konfigurationsdatei vorhanden ist, wird diese sofort gespeichert.
4. Wenn bereits eine Konfigurationsdatei vorhanden ist, bestätigen Sie das Überschreiben der vorhandenen Datei.
Wenn der Vorgang erfolgreich beendet wurde, gibt die Firmware eine Meldung aus. Die Datei RemoteHMI.config ist auf dem Netzlaufwerk gespeichert.

8.12 Firmware updates

Im Menü Update können Sie ein **Update** der Firmware von einem USB-Massenspeicher oder einem Netzlaufwerk durchführen.

HINWEIS

Für den Vorgang sind Administratorrechte erforderlich.

Der UWF-Filter muss deaktiviert sein, um die Firmware speichern zu können. Im Menü werden folgende Informationen angezeigt

- Installed: Revisionsstand der installierten Firmware
- Available: Verfügbare Firmware, erscheint wenn eine Update-Datei gefunden wurde
- Source: Quelle des verfügbaren Updates, erscheint wenn eine Update-Datei gefunden wurde

8.12.1 Firmware-Update durchführen

HINWEIS

USB-Massenspeicher im Ex-Bereich

Verwenden Sie im Ex-Bereich ausschließlich USB-Massenspeicher in eigensicherer Ausführung.

Für Arbeiten im Ex-Bereich ist ein USBi-Stick erhältlich.

Firmware Update von einem USB-Massenspeicher durchführen

HINWEIS

Datenverlust bei Abbruch der Update-Installation

Während des Vorgangs startet die Firmware neu. Unterbrechen Sie den Vorgang nicht und schalten Sie das Bedienterminal nicht aus.

1. Wenn der USB-Lockdown aktiviert ist, stellen Sie sicher, dass der USB-Massenspeicher ein bekanntes Gerät ist oder deaktivieren Sie den USB-Lockdown.
2. Schließen Sie den USB-Massenspeicher an.
3. Klicken Sie auf *Check for Update*.
Die Firmware durchsucht die angeschlossenen USB-Geräte nach verfügbaren Updates. Wenn ein Update verfügbar ist, wird es unter **Available** angezeigt.
4. Klicken Sie auf *Install Update*, um das Update zu installieren.
Die Update-Installation startet.
Wenn das Update beendet ist, wird im Menü das Änderungsprotokoll angezeigt.
5. Entfernen Sie den USB-Massenspeicher.

Firmware-Update von einem Netzlaufwerk durchführen

HINWEIS

Datenverlust bei Abbruch der Update-Installation

Während des Vorgangs startet die Firmware neu. Unterbrechen Sie den Vorgang nicht und schalten Sie das Bedienterminal nicht aus.



Die Update-Datei erhalten Sie von unserem Support.

1. Speichern Sie die Update-Datei auf dem Netzlaufwerk.
 2. Klicken Sie auf *Select*, um das Netzlaufwerk im Windows Explorer zu wählen.
 3. Klicken Sie auf *Check for Update*.
Die Firmware durchsucht das Netzlaufwerk nach verfügbaren Updates.
Wenn ein Update verfügbar ist, wird es unter **Available** angezeigt.
 4. Klicken Sie auf *Install Update*, um das Update zu installieren.
Die Update-Installation startet.
- Wenn das Update beendet ist, gibt das System eine Meldung aus.

9 Gewusst wie ...

9.1 Störungen beheben

Bedienung des Touchscreen ist ungenau		
Ursache	Was tun?	Wer?
Touchscreen verdreckt	• Display reinigen	Operator
Kalibrierung fehlerhaft	• Touchscreen kalibrieren	Operator
Displayfront beschädigt	• Display ersetzen (reparieren)	Engineer

Anzeige der Basisstation ist schwarz		
Ursache	Was tun?	Wer?
Kabelverbindung zwischen Basisstation und HMI-Gerät unterbrochen	• Kabel auf Beschädigung prüfen. • Stecker auf korrekten Sitz prüfen. • Defekte Teile austauschen.	Engineer

Bildschirm ist schwarz und Tastatur leuchtet		
Ursache	Was tun?	Wer?
Einmaliges Störereignis zum Beispiel durch Überspannung	• Remote HMI neu starten.	Engineer

Bildschirm ist schwarz und Tastatur leuchtet nicht		
Ursache	Was tun?	Wer?
Kabelverbindung zwischen Basisstation und HMI-Gerät unterbrochen	• Kabel auf Beschädigung prüfen. • Stecker auf korrekten Sitz prüfen. • Sicherung prüfen. • Sicherung prüfen.	Engineer

Die Netzwerkverbindung setzt häufig aus oder ist instabil		
Ursache	Was tun?	Wer?
Kabel nicht korrekt im Klemmkasten aufgelegt	• Verdrahtung des HMI-Geräts prüfen.	Engineer
Kabellänge überschritten	• Support / CSO kontaktieren.	Engineer

Das System startet nach der Aufforderung zum Neustart nicht		
Ursache	Was tun?	Wer?
Der zuletzt ausgeführte Vorgang hat einen fatalen Systemfehler verursacht.	System mit dem Recovery-Stick auf den Auslieferungszustand zurücksetzen.	Engineer

Bluetooth Barcodescanner funktioniert nicht		
Ursache	Was tun?	Wer?
Akku/Batterie zu schwach	- Akku laden. - Batterie tauschen.	Engineer
Barcodescanner nicht mit der Basisstation gekoppelt	Barcodescanner und Basisstation koppeln.	Engineer
Kabelverbindung zwischen Basisstation und HMI-Gerät unterbrochen	- Kabel auf Beschädigung prüfen. - Stecker auf korrekten Sitz prüfen. - Defekte Teile austauschen.	Engineer
Falschen Passkey zur Verbindungsherstellung eingegeben	Korrekten Passkey eingeben (siehe Dokumentation zum Barcodescanner)	Engineer
Barcodescanner defekt	Defekten Barcodescanner austauschen oder reparieren.	Engineer

Kabelgebundener Barcodescanner funktioniert nicht		
Ursache	Was tun?	Wer?
Kabelverbindung zwischen Barcodescanner und Basisstation unterbrochen	- Kabel auf Beschädigung prüfen. - Stecker auf korrekten Sitz prüfen. - Defekte Teile austauschen.	Engineer
Barcodescanner defekt	Defekten Barcodescanner austauschen oder reparieren.	Engineer

Verbindung des Remote HMI Device Manager zum Thin-Client nicht möglich		
Ursache	Was tun?	Wer?
Netzwerk falsch konfiguriert	Netzwerkconfiguration prüfen.	Engineer
Zugriff des Device-Managers auf den Thin-Client nicht erlaubt	Im Menü User Interface den Zugriff erlauben.	Engineer

9.2 VNC-Server-Dienst auf dem Host aktivieren

Im Folgenden ist das Vorgehen für den TightVNC-Server dargestellt. Um eine VNC-Verbindung aufbauen zu können, muss der VNC-Server-Dienst auf dem Host aktiviert sein. Die zur Verbindung notwendige IP-Adresse bezieht der VNC-Server-Dienst aus den Einstellungen der Netzwerkverbindung des PC. Abhängig von der Konfiguration wird die IP-Adresse manuell festgelegt oder von einem DHCP-Server zugewiesen. Im Adressbuch der Firmware wird diese IP-Adresse als Server-IP der VNC-Verbindung festgelegt.

Der Verbindungsaufbau ist von der Einstellung im VNC-Server abhängig und erfolgt als:

- direkte Verbindung ohne Passwortabfrage
- Verbindung mit VNC-Passwort
- Verbindung mit Windows-Passwort

9.2.1 VNC-Server-Parameter

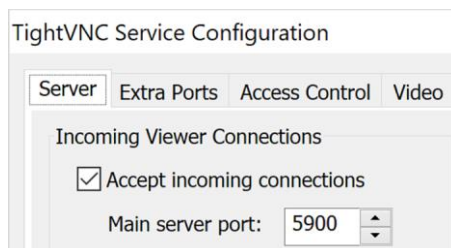
Die nachfolgend aufgeführten Parameter sind zur Konfiguration der VNC-Verbindung notwendig. Die konkrete Bezeichnung ist abhängig vom verwendeten VNC-Server-Dienst.

VNC-Server-Adresse

Die VNC-Server-Adresse entspricht der IP-Adresse des Servers oder dem Servernamen. In der Regel bieten die VNC-Server-Dienste verschiedene Möglichkeiten, um die Adresse zu ermitteln, mit der der Server im Netz aufgerufen werden kann. In den Einstellungen des VNC-Servers können zusätzlich zur IP-Adresse Portnummern vergeben werden, mit der der Server im Netz aufgerufen werden kann. Die Zieladresse des Host muss sich im Netzwerk des Thin-Client befinden bzw. muss vom Thin-Client erreichbar sein!

Ports

Accept connections on port



Definiert den Port der Serververbindung für die Datenübermittlung (Standard Port 5900).

Wenn Sie wegen Netzwerkkonflikten einen anderen Port verwenden, müssen Sie diesen konfigurieren. Beachten Sie die Einstellungen einer Firewall.

VNC-Passwort

VNC-Serverapplikationen authentifizieren den Benutzer einer VNC-Verbindung über ein Passwort. Folgende Passwort-Verfahren sind möglich:

None

Legt kein Passwort fest. Der VNC-Server auf dem Host erlaubt jedem Remote-Rechner (Remote HMI) den Zugriff, der über seine Adresse eine VNC-Verbindung anfordert.

VNC-Passwort

Definiert je nach VNC-Serverapplikation ein oder mehrere Passwörter, die der VNC-Server-Dienst vom Client zur Authentifizierung anfordert.

Windows-Passwort

Verwendet die Windows Zugangsauthentifizierung. Der VNC-Server-Dienst gewährt dem Client den Zugriff auf den Host, wenn die Anmeldung mit dem gültigen Windows-Passwort erfolgt.

Single sign on

Verwendet die Windows Zugangsauthentifizierung und die Authentifizierung durch den Windows basierten Login. Der VNC-Server-Dienst gewährt dem Client den Zugriff, wenn der Benutzer sich mit einem gültigen Windows-Login authentifiziert.

Encryption

Die meisten VNC-Server nutzen für die Übertragung der Bild-, Maus und Tastaturinformationen eine Verschlüsselung, um diese vor unberechtigtem Zugriff zu schützen.

Always on

Daten werden immer verschlüsselt

Prefer on

Daten sind immer verschlüsselt sind, es sei denn, der Thin-Client fordert keine Verschlüsselung an (Standard). Die Einstellung ist erforderlich, wenn in der Konfiguration keine Verschlüsselung angefordert wird.

Prefer off

Daten werden nicht verschlüsselt, es sei denn, der Thin-Client fordert eine Verschlüsselung an. Die Einstellung ist erforderlich, wenn in der Konfiguration eine Verschlüsselung angefordert wird.

Prompt local user to accept connections

Erlaubt dem Anwender des Host die Verbindungsanfrage anzunehmen oder zurückzuweisen. Da im Regelfall der Host für den direkten Remote-Zugriff eingesetzt wird, ist diese Einstellung für die Thin-Client-Verbindung nicht relevant.

Start VNC Server automatically with Windows

Legt fest, dass der Dienst des VNC-Server automatisch mit dem Hochfahren (Starten) von Windows aktiviert wird. Wenn diese Funktion nicht aktiviert ist, muss der Remote-Zugriff nach einem Systemstart des Host-PCs explizit gestartet werden.

9.3 DRDC-Client-Verbindung

Der DeltaV®-Remote-Desktop-Connection-Client (DRDC) von EMERSON erlaubt den Zugriff auf eine virtualisierte Operator- oder Engineering-Workstation innerhalb einer DeltaV®-Virtualisierungsarchitektur. So ist über das Ethernet der Zugriff auf Anwendungen möglich, die auf einem Prozessleitsystem laufen.

Eine DRDC-Verbindung fügen Sie über eine App im Register **Applications** hinzu (siehe [6.2 Apps hinzufügen](#)).

Pro

Pro-Lizenz erforderlich.

10 Digitale Signatur

10.1 Digitale Signatur von Programmen der R. STAHL HMI Systems

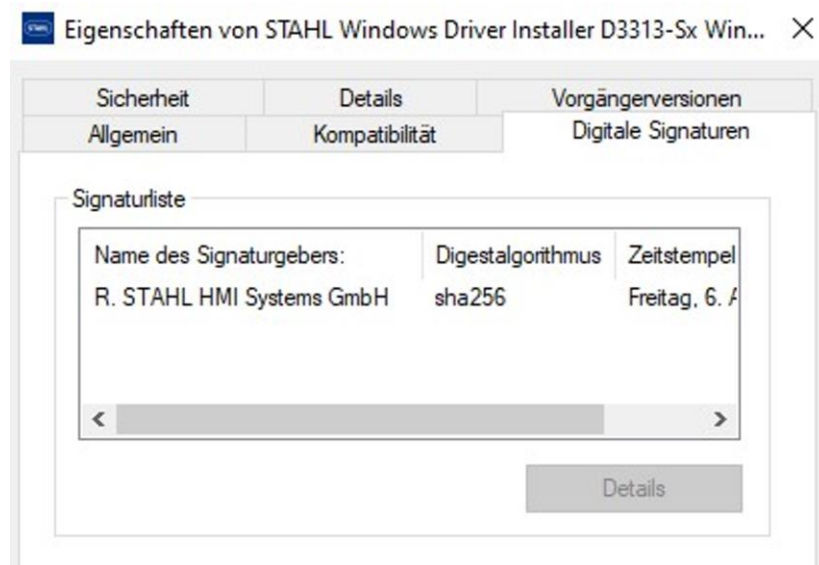
Alle Programmdateien von R. STAHL HMI Systems, die ausführbaren Code (RemoteHMI, DeviceControlPanel etc.) enthalten, sind digital signiert, einschließlich des Setup. Die digitale Signatur wird dazu verwendet, um sicherzustellen, dass Programmdateien nach ihrer Veröffentlichung nicht verändert wurden und dass die Software vom Hersteller stammt. Sie basieren auf digitale Zertifikate, welche von einer hierfür berechtigten und vertrauenswürdigen Stelle an eine Person (oder ein Unternehmen) ausgegeben wurden, die durch diese Stelle identifiziert wurde.

Um eine digitale Signatur zu überprüfen, müssen zwei Teile verifiziert werden:

- **Digitale Signatur:** Es handelt sich hierbei um einen verschlüsselten Hashwert, der von einer Hashfunktion für eine Datei erzeugt und mit dem privaten Schlüssel des unterliegenden Zertifikats verschlüsselt wurde.
- **Zertifikat:** Eine Software stammt vom Hersteller, wenn sie mit seinem Zertifikat signiert wurde. Daher muss überprüft werden, ob das korrekte Zertifikat verwendet wurde und ob das Zertifikat gültig ist. Im Einzelnen sollten der Aussteller des Zertifikats, der Eigentümer, der Zertifizierungspfad, die Seriennummer und der Fingerabdruck überprüft werden.

10.2 Überprüfung der digitalen Signatur

Die hierfür notwendige Information befindet sich auf dem Karteireiter Digitale Signaturen: Lokalisieren Sie die Datei im Explorer, klicken mit der rechten Maustaste auf die Datei, so dass sich das Kontext-Menü öffnet und wählen Eigenschaften. Wenn Sie diesen Karteireiter nicht sehen, dann wurde die Datei nicht unterschrieben oder die Signatur wurde entfernt - die Überprüfung ist fehlgeschlagen.



Wählen Sie – sofern vorhanden - immer SHA-256 an und klicken Sie auf Details.

10.3 Details der digitalen Signatur

Ein neues Fenster öffnet sich, welches generelle Informationen zur Signatur anzeigt. Die wichtigste Aussage auf dieser Seite ist, dass die digitale Signatur gültig ist.



Informationen der digitalen Signatur
Die digitale Signatur ist gültig.

Signaturgeberinformationen

Name:

E-Mail:

Signaturzeitpunkt:

Gegensignaturen

Name des Signa...	E-Mail-Adresse:	Zeitstempel
GlobalSign TSA f...	Nicht verfügbar	Dienstag, 23. Juli 20...

Die Signatur ist dann gültig, wenn:

- die Datei - nachdem sie unterschrieben wurde - nicht mehr verändert wurde: Der berechnete Hashwert, basierend auf der ausgewählten Hashfunktion, entspricht dem entschlüsselten Hashwert in der Signatur.
- die Zertifizierungskette vollständig ist, und
- das zugrundeliegende Zertifikat (welches ein gefälschtes sein kann) in Ordnung ist.

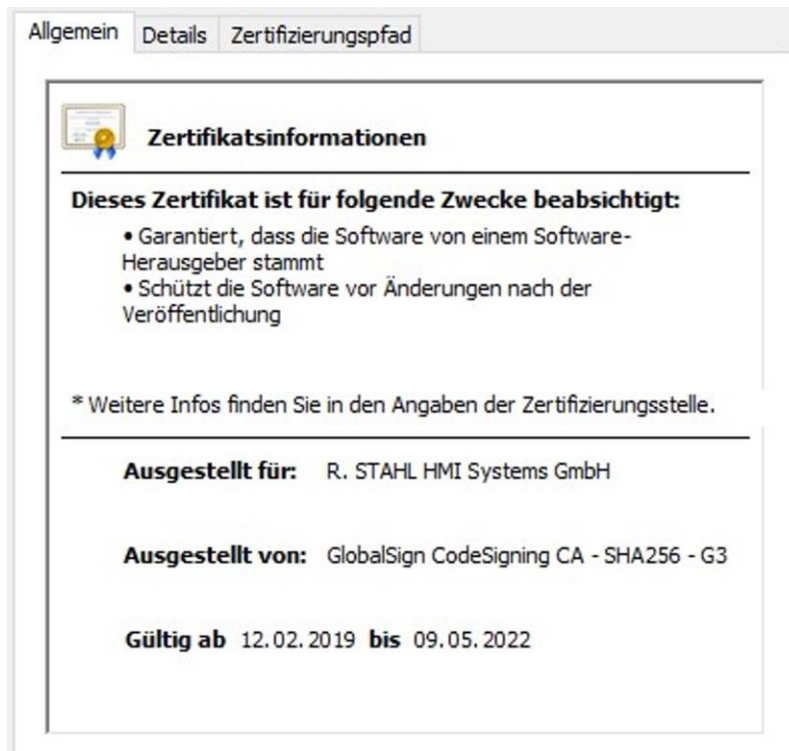
Ansonsten erscheint eine Fehlermeldung, markiert durch ein Fehlersymbol, als Beispiel:



Informationen der digitalen Signatur
Die digitale Signatur ist ungültig.

10.4 Überprüfung des Zertifikats

Klicken Sie auf Zertifikat anzeigen, um das verwendete Zertifikat zu überprüfen.



Es öffnet sich ein neues Fenster mit drei Karteireitern, die Details zum Zertifikat anzeigen, welches für die Signatur der Datei verwendet wurde. Es sind nun die beiden Felder "Ausgestellt für" und "Ausgestellt von" zu betrachten, deren Werte wie folgt sein müssen, ansonsten ist die Überprüfung fehlgeschlagen.

Ausgestellt für: R.Stahl HMI Systems GmbH
Ausgestellt von: GlobalSign Code Signing CA
oder: Sectigo Public Code Signing CA EV R36

Sofern Sie weitere Elemente überprüfen möchten (Fingerabdruck, Seriennummer etc.) setzen Sie sich bitte mit dem technischen Support in Verbindung, so dass wir Ihnen die passenden Prüfsumme mitteilen. Sie ist je nach Produkt von unterschiedlichen Ausstellern signiert worden.

10.5 Quelle

Textpassagen entnommen aus:

[TurboSFV - Validation of digital signatures \(Code Signing\)](#)

R. STAHL HMI Systems GmbH
Adolf-Grimme-Allee 8
D 50829 Köln

T:	(Sales Support)	+49 221 768 06 - 1200
	(Technischer Support)	+49 221 768 06 - 5000
F:		+49 221 768 06 - 4200
E:	(Sales Support)	sales.dehm@r-stahl.com
	(Technischer Support)	support.dehm@r-stahl.com

r-stahl.com

