



Abbildung ähnlich wie Produkt

Draco SIRA User Station K488

Benutzer- handbuch

Einleitung



Dieses Handbuch enthält wichtige Sicherheitshinweise und Anweisungen, um das Produkt einzurichten und zu betreiben. Lesen Sie das Handbuch sorgfältig, bevor Sie sich dem Produkt zuwenden. Beachten Sie die allgemeinen Sicherheitshinweise (siehe Kapitel 2, Seite 11) und die zusätzlichen Hinweise in den jeweiligen Kapiteln

Produktidentifikation

Die Modell- und Seriennummer unserer Produkte befinden sich auf dem Boden der Geräte. Beziehen Sie sich immer auf diese Information, wenn Sie Kontakt mit Ihrem Händler oder dem Support der IHSE GmbH aufnehmen (siehe Kapitel 14, Seite 182).

Warenzeichen und Handelsmarken

Alle Warenzeichen und Handelsmarken, die in diesem Handbuch erwähnt werden, werden anerkannt als Eigentum des jeweiligen Inhabers.

Gültigkeit dieses Benutzerhandbuchs

Dieses Handbuch gilt für alle Geräte, der auf der Titelseite genannten Serie(n). Unterschiede zwischen den verschiedenen Modellen sind eindeutig beschrieben.

Der Hersteller behält sich das Recht vor, Spezifikationen, Funktionen oder Schaltkreise der hier beschriebenen Serie ohne Ankündigung zu ändern. Informationen in diesem Handbuch können ohne Ankündigung geändert, erweitert oder gelöscht werden. Die jeweils aktuelle Version des Handbuchs finden Sie im Download-Bereich unserer Webseite.

Copyright

© 2026. Alle Rechte vorbehalten. Dieses Handbuch darf ohne ausdrückliche, schriftliche Genehmigung des Herstellers in keiner Art und Weise reproduziert oder verändert werden.

Verfügbare Dokumentation

Name	Format	Beschreibung	Bereitstellung
Benutzerhandbuch	PDF	Bietet einen Überblick über die Produkte zusammen mit technischen Daten und Sicherheitsinformationen. Beinhaltet alle notwendigen Instruktionen für den grundlegenden Betrieb der Produkte.	Download von der Webseite
Kurzanleitung	Druck	Beinhaltet eine Kurzanleitung zur schnellen Installation sowie Sicherheitsinformationen	Im Lieferumfang enthalten

Kontakt

IHSE GmbH

Benzstraße 1

88094 Oberteuringen

Germany

phone: +49 7546-9248-0

fax: +49 7546-9248-48

e-mail: info@ihse.com

website: <https://www.ihse.com>

Inhaltsverzeichnis

Inhaltsverzeichnis.....	3
1 Wichtige Informationen.....	8
1.1 Firmware und Software	8
1.2 Symbole für Warnhinweise und ergänzende Informationen	8
1.3 Begriffe und Schreibweisen	8
1.4 Verwendungszweck	9
1.5 Zertifikate/Richtlinien	10
1.5.1 EU-Konformitätserklärung	10
1.5.2 WEEE	10
2 Sicherheitshinweise	11
3 Beschreibung.....	12
3.1 Systemübersicht.....	12
3.1.1 System mit Matrix	12
3.1.2 System ohne Matrix	12
3.2 Produkttypen	13
3.2.1 Draco SIRA User Station	13
3.2.2 Draco SIRA CON-Units	13
3.2.3 Draco SIRA Stand-Alone-Unit	13
3.3 Zubehör	13
3.4 Lieferumfang	13
3.5 Produkteigenschaften.....	14
3.6 Produktansichten.....	14
3.7 Statusanzeige.....	15
3.7.1 Stromversorgung	15
3.7.2 Netzwerkverbindung	15
4 Installation.....	16
4.1 User Station an Monitor befestigen.....	16
4.2 Kabel und Zubehör anschließen	16
4.3 Erste Anmeldung an der Draco SIRA User Station	17
5 Einführung in die Software.....	18
5.1 Symbolleiste	18
5.2 Hauptmenü.....	19
5.2.1 Port-Navigator (Start).....	19
5.2.2 Port-Scanner (Start).....	20
5.2.3 User-Station-Konfiguration (Start)	20
5.2.4 Firefox Web Browser	20
5.2.5 Fensterverwaltung	21
5.2.6 Fensteranordnungen.....	22
5.2.7 Hilfe	23
5.2.8 Beenden.....	25
5.3 Systemeinstellungen	26
5.3.1 Datum und Zeit	26
5.3.2 Standort- und Wettereinstellungen	28

5.3.3	Tastatur	30
5.3.4	Monitor	32
5.3.5	Maus	34
5.3.6	Netzwerk	35
5.4	KVM-Clients nutzen.....	47
5.4.1	Automatisches Verbinden.....	48
5.5	Serielle Clients nutzen.....	49
5.5.1	Emulator-Menü	49
5.5.2	Power-Menü.....	52
6	Konfiguration	53
6.1	Geräte hinzufügen (Draco SIRA CON-Units).....	53
6.1.1	Geräte editieren	55
6.1.2	Geräte löschen.....	56
6.1.3	Geräte importieren	56
6.2	KVM-Ports konfigurieren	59
6.3	Zugriff auf KVM/serielle Switches und Ports.....	62
6.4	Targets verwalten und Zugangsmethoden.....	63
6.4.1	Targets und Zugangsmethoden hinzufügen	64
6.4.2	Targets und Zugangsmethoden ändern und löschen.....	71
6.4.3	Bekannte Einschränkungen bei den Targets.....	77
7	Navigation und Zugang.....	78
7.1	Der Port-Navigator	78
7.1.1	Suchfunktion	79
7.1.2	Filterfunktion	79
7.1.3	Geräte- und Portstatus identifizieren	80
7.1.4	Externe Medien identifizieren.....	81
7.1.5	Zugriff auf Geräte und Ports über das Geräte-Menü.....	81
7.1.6	Auf Targets zugreifen.....	82
7.1.7	Fensterverwaltung und Fensteranordnungen (Layouts).....	83
7.2	Der Port-Scanner	83
7.2.1	Port-Scanner konfigurieren.....	84
7.2.2	Arbeiten mit dem Port Scanner.....	85
7.2.3	Port-Scanner Tabellenansicht.....	86
8	Benutzervoreinstellungen	87
8.1	Zugangs-Clients-Einstellungen	87
8.2	Tastatur-Makros verwalten.....	91
8.2.1	Erstellen von Tastatur/Hotkey-Makros.....	91
8.2.2	Makros ändern und löschen.....	92
8.2.3	Makros ausführen	93
8.3	Audioeinstellungen	93
8.4	Hotkeys und Gesten.....	95
8.5	Fensteranordnungen (Window Layouts).....	98
8.6	Port-Scanner-Einstellungen	100

8.7	Bildschirmfoto (Screenshot)-Einstellungen	102
8.7.1	Screenshots aufnehmen	103
8.8	Passwort ändern	104
9	Administrationsfunktionen einstellen	105
9.1	Nutzer	105
9.1.1	Neue Nutzer erstellen	106
9.1.2	Nutzer ändern oder löschen	107
9.2	Gruppen	109
9.2.1	Anlegen einer neuen Gruppe.....	109
9.2.2	Gruppen ändern oder löschen	112
9.2.3	Authentifizierung von User Stations und KVM/Seriellen Switches	113
9.3	Autologin	114
9.4	LDAP	116
9.4.1	LDAP-Server hinzufügen	116
9.4.2	LDAP-Server bearbeiten oder löschen	122
9.4.3	Aktivieren/Deaktivieren der LDAP-Authentifizierung	122
9.4.4	Suche nach LDAP-Nutzern und -Gruppen	123
9.4.5	Konfiguration der maximalen Anzahl von Suchergebnissen und der Einstellungen für die lokale Authentifizierung	124
9.4.6	Anmelden mit LDAP.....	125
9.4.7	Fehlermeldung bei LDAP-Anmeldung	125
9.5	Vertrauenswürdige Zertifikate	126
9.5.1	CA-Zertifikate installieren.....	126
9.5.2	Installierte Zertifikate entfernen	126
9.6	Server-Zertifikate.....	127
9.6.1	Anzeigen des aktuellen Server-Zertifikats	127
9.6.2	Privaten Schlüssel und Zertifikat importieren	128
9.6.3	Selbst Signiertes Zertifikat erstellen	129
9.7	Sicherheitseinstellungen	130
9.7.1	FIPS-Modus aktivieren/deaktivieren	130
9.7.2	Geräte-Zertifikatsüberprüfungen aktivieren/deaktivieren.....	131
9.7.3	Überprüfung von Schlüsseln und Zertifikaten für SSH-, RDP-, WEB- und ESXi-Clients aktivieren.....	131
9.7.4	Passwort-Einstellungen	133
9.7.5	Nutzersperren	133
9.7.6	Links und Weiterleitungen	134
9.7.7	Nutzungsbedingungen.....	135
9.8	Anzeigeeinstellungen	136
9.8.1	Monitor entsperren.....	137
9.9	Anpassungen	138
9.10	Fernsteuerungs-Einstellungen	141
9.10.1	Fernsteuerung via Web-Browser	141
9.10.2	Fernsteuerung via API	142

9.11	Tastatur - / Mausmitbenutzung.....	144
9.11.1	Beispiel einer erweiterten vertikalen Konfiguration.....	144
9.11.2	Konfiguration	145
9.12	Netzwerkspeicher	148
9.13	Spracheinstellungen.....	150
10	Wartung	152
10.1	Reinigung	152
10.2	Ereignisprotokoll.....	152
10.2.1	Ereignisprotokolle archivieren.....	153
10.3	Sicherung und Wiederherstellung	155
10.3.1	Sicherungsdatei erstellen.....	155
10.3.2	Sicherungsdatei wieder einspielen	156
10.3.3	Sicherungsdateien exportieren und importieren	156
10.3.4	Sicherungsdateien löschen.....	157
10.4	Werkseinstellungen	158
10.4.1	Beim Start auf Werkseinstellungen zurücksetzen	159
10.5	Software aktualisieren	160
10.6	Kundendienst	161
10.6.1	Kundendienstzugang	162
10.6.2	Protokollierungsstufe	163
10.7	Netzwerkd Diagnose.....	164
10.8	Über das Gerät.....	165
11	API-Konfiguration	166
11.1	Session erstellen und anmelden	166
11.2	Anmelden	166
11.3	Session schließen / Abmelden	167
11.4	Zugangsfunktionalität	168
11.4.1	Get Geräte und Targets	168
11.4.2	Get Geräte und Ports.....	168
11.4.3	Get Targets und Zugangspunkte	169
11.5	Verwaltung von Zugangs-Client-Sessions	170
11.5.1	Client-Sessions erstellen	170
11.5.2	Zugangs-Client schließen	171
11.5.3	Benannte Szenen (auch bekannt als Window Layouts)	171
11.5.4	Fensterverwaltung	172
11.6	Wartung.....	172
11.6.1	Identitätsdaten	172
11.6.2	Firmware-Funktionen	172
11.6.3	Firmware-Update	173
11.6.4	Backup/Wiederherstellen	173
12	BIOS-Einstellungen	177

13 Technische Daten	178
13.1 Pinbelegungen	179
13.1.1 DisplayPort - Upstream	179
13.1.2 DisplayPort - Downstream	179
13.1.3 HDMI	180
13.1.4 USB, Typ A	180
13.1.5 USB, Typ C	180
13.1.6 RJ45 (LAN)	180
13.2 Leistungsaufnahme	181
13.3 Abmessungen	181
13.4 Gewicht	181
13.5 Umweltbedingungen und Emissionen	181
13.6 MTBF	181
14 Technischer Support	182
14.1 Checkliste Kontaktaufnahme	182
14.2 Checkliste Versand	182
15 Anhänge	183
15.1 Anhang A: Empfehlungen zu offenen Ports	183
15.2 Anhang B: Unterstützung für den Mausmodus für Dual Video Portgruppen und M-KVM-Targets	184
16 Glossar	185
17 Index	187
18 Abbildungsverzeichnis	189
19 Änderungsprotokoll	194

1 Wichtige Informationen

1.1 Firmware und Software

Die Informationen in diesem Handbuch beziehen sich auf die neueste Software, die zum Zeitpunkt der Veröffentlichung des Handbuchs verfügbar ist. Die Aktualisierungen des Benutzerhandbuchs entnehmen Sie bitte dem Änderungsprotokoll (siehe Kapitel 19, Seite 194).

1.2 Symbole für Warnhinweise und ergänzende Informationen

Die Bedeutung der Symbole, die in diesem Handbuch für Warnhinweise und hilfreiche Informationen verwendet werden, werden nachfolgend beschrieben:



WARNUNG

WARNUNG kennzeichnet eine Gefahr, die zu Tod oder schwerer Verletzung führen kann, wenn sie nicht vermieden wird.



VORSICHT

VORSICHT kennzeichnet eine Gefahr, die zu leichter oder mittlerer Verletzung führen kann, wenn sie nicht vermieden wird.

HINWEIS

HINWEIS kennzeichnet Informationen, deren Nichtbeachtung die Funktionsfähigkeit Ihres Geräts oder die Sicherheit Ihrer Daten gefährdet.

 Dieses Symbol kennzeichnet Hinweise für Besonderheiten am Gerät oder im Gebrauch von Geräte- und Funktionsvarianten.

 Dieses Symbol kennzeichnet Hinweise für vom Hersteller empfohlene Vorgehensweisen für eine effektive Ausschöpfung des Gerätepotenzials.

1.3 Begriffe und Schreibweisen

Zur besseren Lesbarkeit und leichteren Zuordnung werden in diesem Handbuch einheitliche Begriffe und Schreibweisen verwendet.

Die folgenden Begriffe werden für Produkte und Systembeschreibungen verwendet:

Begriff	Beschreibung
Quelle	Computer, Grafikkarte (USB-, Video, Audio- und Datenquellen)
Senke	Konsole (Monitor, Tastatur, Maus, optional auch Audio- und USB-Geräte)
CPU-Unit	Encoder zum Anschluss an die Quelle.
CON-Unit	Decoder zum Anschluss an die Peripheriegeräte.

Folgende Schreibweisen werden für Tastaturkommandos verwendet:

Tastaturkommando	Beschreibung
Taste	Taste auf der Tastatur
Taste + Taste	Tasten gleichzeitig drücken
Taste, Taste	Tasten nacheinander drücken
2x Taste	Taste 2x schnell hintereinander drücken (wie Maus-Doppelklick)

Folgende Schreibweisen werden z. B. für Beschreibungen von Dateien oder zum Aktualisieren der Firmware verwendet:

Beispiel	Beschreibung
Config.txt	Z. B. Dateiname
#CFG	Z. B. Dateiinhalt

Folgende Schreibweisen werden für Softwarebeschreibungen verwendet:

Schreibweise	Beschreibung
Fettdruck	Darstellung von Elementen in der Software wie z. B. Menüs oder Buttons
Fettdruck > Fettdruck	Auswahl eines Menüpunkts im Hauptmenü oder der Symbolleiste, z. B., Hauptmenü > Hilfe

Maustaste	Beschreibung
Linke Maustaste	Primäre Maustaste* (Standard in den meisten Betriebssystemen)
Rechte Maustaste	Sekundäre Maustaste*

* Es sei denn, Sie haben die Mauseinstellungen im verwendeten Betriebssystem angepasst.

Beschreibungen, die "Klick", "Mausklick" oder "Doppelklick" enthalten, bedeuten jeweils einen Klick mit der primären (linken) Maustaste. Wenn die rechte Maustaste verwendet werden muss, wird dies in der Beschreibung explizit angegeben.

1.4 Verwendungszweck

Draco SIRA (Secure IP Remote Access) User Stations ermöglichen einen hochsicheren Fernzugriff auf entfernte PCs und Server über verschlüsselte TCP/IP-Datenströme. Die Datenströme werden entweder von einer Draco SIRA CON-Einheit (für den Matrixbetrieb) oder einem eigenständigen Draco SIRA-Gerät erzeugt. Über die User Station können Benutzer entfernte Systeme effizient anzeigen, steuern und bedienen.

HINWEIS

Störungen bei Überschreitung der Störfestigkeitsgrenzwerte

Bei einer Überschreitung der in der EN55024 aufgeführten Grenzwerte kann eine zuverlässige und störungsfreie Funktion der Geräte nicht gewährleistet werden.

HINWEIS

Mögliche Funkstörungen im Wohnbereich

Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funktionsstörungen verursachen. In diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

- ➔ Die in diesem Handbuch angegebenen Sicherheits- und Installationsanweisungen befolgen.
- ➔ Verbindungskabel gemäß den Längen- und Typenangaben in diesem Handbuch verwenden.

1.5 Zertifikate/Richtlinien

1.5.1 EU-Konformitätserklärung

Die EU-Konformitätserklärung für die Produktserie finden Sie unter:

www.ihse.de/eu-konformitaetserklaerung

Eine Kopie der originalen, produktspezifischen EU-Konformitätserklärung kann auf Nachfrage zur Verfügung gestellt werden. Kontaktdetails finden Sie auf Seite 2 in diesem Handbuch.

1.5.2 WEEE



Das Geräteetikett trägt ein Symbol (durchgestrichene Mülltonne) zur Kennzeichnung von Elektro- und Elektronikgeräten. Der Hersteller erfüllt die EU-Richtlinie 2012/19/EU zur Reduktion der zunehmenden Menge an Elektronikschrott aus nicht mehr benutzten Elektro- und Elektronikgeräten. Der Hersteller ist ein WEEE-registriertes Unternehmen (Registrierungsnummer DE39900275).

Gerät entsorgen/zurücknehmen

- ➔ Das Symbol einer durchgestrichenen Mülltonne auf Elektro- und Elektronikgeräten weist darauf hin, dass das Produkt und das mitgelieferte elektronische Zubehör (z. B. Netzteile, Kabel) am Ende der Lebensdauer nicht über den Haus- oder Gewerbemüll entsorgt werden dürfen.
- ➔ Durch eine unverantwortliche Entsorgung des Produkts können Sie Unbefugten eine vorschriftswidrige Nutzung ermöglichen und sich und Dritte der Gefahr schwerer Verletzungen aussetzen, sowie die Umwelt verunreinigen.
- ➔ Der Hersteller nimmt Altgeräte zurück und gewährleistet eine fachgerechte Entsorgung. Bitte wenden Sie sich an den technischen Support des Herstellers, um die Rückgabe eines zu entsorgenden Gerätes anzumelden.
- ➔ Es liegt in der Verantwortung des Kunden, persönliche Daten auf dem zu entsorgenden Gerät zu löschen.

2 Sicherheitshinweise

Beachten Sie die folgenden Hinweise, um einen zuverlässigen und sicheren Langzeitbetrieb Ihres Geräts zu gewährleisten:

- ➔ Gerät nur gemäß dieser Bedienungsanleitung verwenden. Die Nichtbeachtung der beschriebenen Instruktionen kann zu Personenschäden führen, Schäden am Gerät verursachen oder die Sicherheit Ihrer Daten gefährden.
- ➔ Alle erforderlichen ESD-Maßnahmen treffen.

WARNUNG

Gefahr eines Stromschlags durch frei zugängliche Stromanschlüsse bei geöffnetem Chassis
Gefahr von Quetschungen, Schürfungen oder Abscherung von Fingerkuppen durch drehenden Lüfter bei geöffnetem Chassis

Wenn das Chassis geöffnet wird, während das Gerät mit Strom versorgt wird, kann es zu einem Stromschlag kommen, wenn die interne Verdrahtung berührt wird. Wird im geöffneten Chassis ein laufender Lüfter berührt, kann es zu Quetschungen, Abschürfungen oder Abscherung von Fingerkuppen kommen.

Es gibt keine notwendigen Wartungsarbeiten, die ein Öffnen des Chassis erfordern.

- ➔ Entfernen Sie NICHT die Abdeckung des Chassis.
- ➔ Installieren Sie das Gerät NICHT in Umgebungen, in denen sich Kinder aufhalten können.

Installationsort

Während des Betriebs können das Gerät und die Netzteile warm werden. In feuchter Umgebung kann es zu Schäden am Gerät kommen.

- ➔ Verwenden Sie das Gerät nur in geschlossenen, trockenen Räumen.
- ➔ Verwenden Sie das Gerät nur in einem Raum mit ausreichender Belüftung.
- ➔ Beim Einbau in Schaltschränke sind über dem Gerät mindestens 0,5 HE Freiraum zur Belüftung erforderlich.
- ➔ Stellen Sie keine Netzteile auf das Gerät.
- ➔ Vorhandene Belüftungsöffnungen am Gerät müssen jederzeit frei sein.
- ➔ Platzieren Sie das Gerät bei Untertischmontage in ausreichendem Abstand zum Bediener.
- ➔ Platzieren Sie alle Netzsteckdosen inklusive der Steckdosen für mitgelieferte externe Netzteile leicht zugänglich und direkt nebeneinander.

Anschluss

- ➔ Prüfen Sie das Gerät und das Netzteil vor dem Anschließen auf sichtbare Schäden.
- ➔ Schließen Sie das Gerät nur an, wenn das Chassis und die Anschlüsse unbeschädigt sind.
- ➔ Verwenden Sie ausschließlich die original gelieferten Netzteile oder vom Hersteller freigegebene Ersatzgeräte.
- ➔ Verwenden Sie nur Netzteile ohne sichtbare Beschädigungen am Chassis oder an Kabeln.
- ➔ Verbinden Sie die Netzteile ausschließlich mit geerdeten Steckdosen.
- ➔ Stellen Sie sicher, dass eine Erdverbindung zwischen der Steckdose und dem Wechselspannungseingang des Netzteils besteht.
- ➔ Benutzen Sie nur vom Hersteller gelieferte Stromkabel.

Gerät vom Stromkreis trennen

HINWEIS

Die Gerätestecker auf der Geräteseite können eine Verriegelung enthalten. Im Falle einer notwendigen schnellen und vollständigen Trennung der Geräte inklusive eventuell vorhandener Netzteile vom Stromkreis:

- ➔ Ziehen Sie alle zugehörigen Kabelstecker aus den Netzsteckdosen.
- ➔ Oder stellen Sie den Netzschalter der Netzsteckdosen (falls verfügbar) auf „Aus“.

3 Beschreibung

3.1 Systemübersicht

3.1.1 System mit Matrix

Dies ist ein Beispiel eines Systems mit einer Draco tera Matrix und Draco SIRA CON-Units.

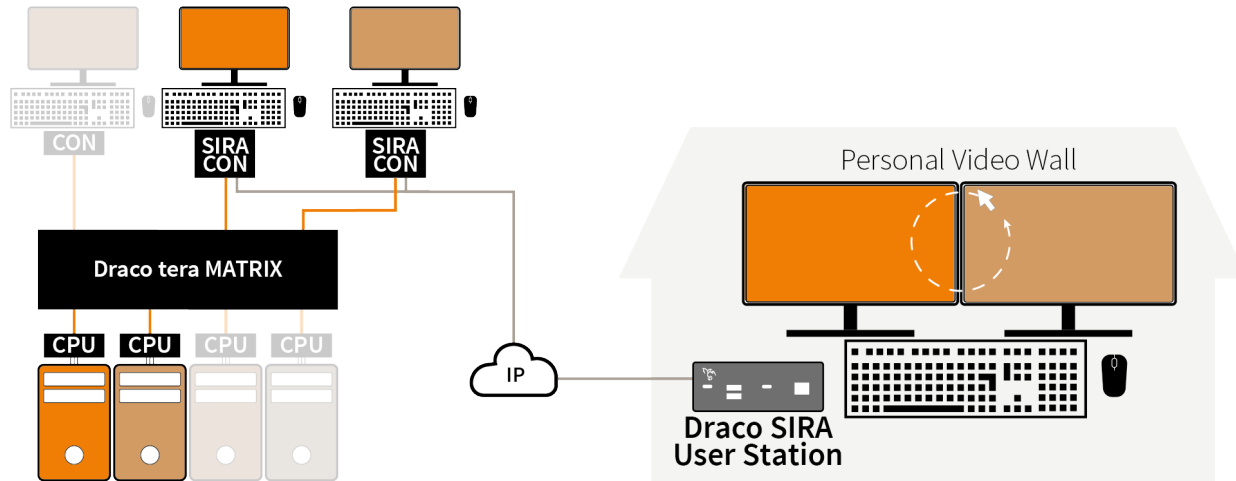


Abb. 1 Installationsbeispiel mit Draco tera Matrix

Die Draco SIRA CON-Units werden über Cat-X- oder Glasfaserkabel an die Matrix angeschlossen (Link 1, Link 2). Sie dienen wie jede andere Standard-CON-Unit als lokale Arbeitsstationen; Monitor, Tastatur und Maus werden an sie angeschlossen. Darüber hinaus erzeugen sie verschlüsselte TCP/IP-Datenströme, die über ein Kabel an das Netzwerk weitergeleitet werden. Die User Station ist ebenfalls an das Netzwerk angeschlossen.

3.1.2 System ohne Matrix

Dies ist ein Beispiel mit Draco SIRA Stand-Alone-Units.

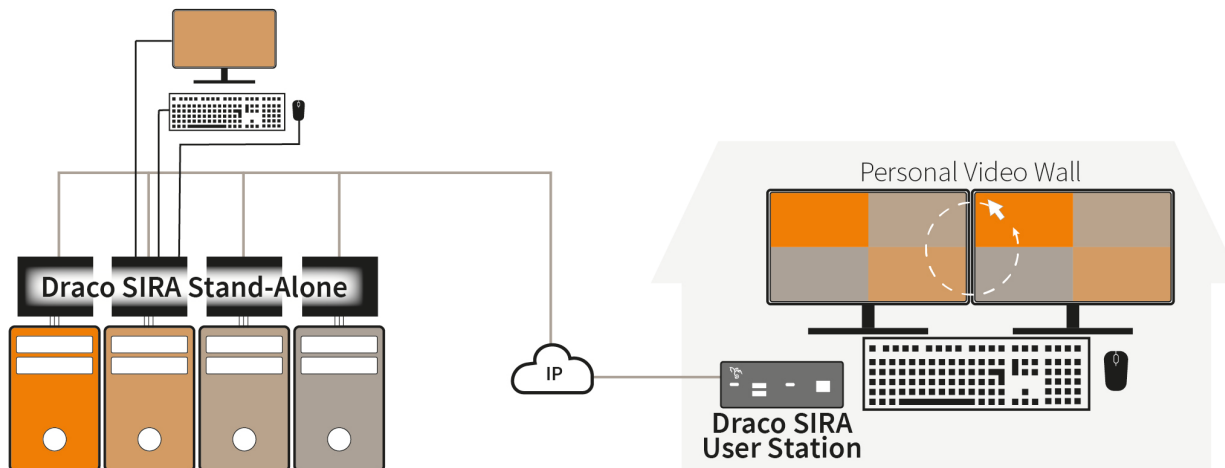


Abb. 2 Installationsbeispiel mit Draco SIRA Stand-Alone-Units

Jeder Computer benötigt eine eigenständige Stand-Alone-Unit, die über die Anschlüsse einer Standard-CPU-Unit (Video-Eingang und USB Typ B) sowie über die Anschlüsse einer Standard-CON-Unit (2x USB-HID Typ A und Video-Ausgang) verfügt.

Der Computer wird über ein Videokabel und ein USB-Kabel vom Typ A-B an die Stand-Alone-Unit angeschlossen. Durch den Anschluss eines Monitors sowie einer Tastatur und einer Maus an die Unit kann ein lokaler Arbeitsplatz eingerichtet werden.

Die Stand-Alone-Unit erzeugt verschlüsselte TCP/IP-Datenströme, die über ein Kabel an das Netzwerk weitergeleitet werden. Die User Station ist ebenfalls an das Netzwerk angeschlossen.

3.2 Produkttypen

3.2.1 Draco SIRA User Station

Art.-Nr.	Netzwerk-Schnittstellen	Video-Schnittstellen	USB-Schnittstellen
K488-UST-R1	1x 1 Gbit LAN (RJ45, 10/100/1000 Mbps) 1x 2,5 Gbit LAN (RJ45, 10/100/2500 Mbps)	1x HDMI 2.0a 1x DisplayPort 1.2a	2x USB Typ C 3.2 (einschließlich DisplayPort 1.2a) 2x USB Typ A 3.2 2x USB Typ A 2.0

In Verbindung mit der Draco SIRA User Station benötigen Sie mindestens einen der folgenden Extender.

3.2.2 Draco SIRA CON-Units

Art.-Nr.	Verbindung zur Matrix		HDMI-Auflösung/ Frame Rate	USB-Schnittstellen	Netzwerk-Schnittstellen
R488-BIPC	1x	Cat X (RJ45, 1G)	1x bis zu 3840x2160@30 Hz	2x USB Typ A	1x 1 Gbit LAN (RJ45)
R488-BIPCR	2x				
R488-BIPS	1x	Glasfaser (SFP, LC Duplex SM, 1G)	1x bis zu 3840x2160@30 Hz	2x USB Typ A	1x 1 Gbit LAN (RJ45)
R488-BIPSR	2x				

3.2.3 Draco SIRA Stand-Alone-Unit

Art.-Nr.	HDMI-Auflösung	CPU-Teil		CON-Teil	
		Video-Port	USB-Port	Video-Port	USB-Ports
R488-BIPHHL	Bis zu 3840x2160 @ 30 Hz	1x HDMI-Eingang	1x USB Typ B	1x HDMI-Ausgang	2x USB Typ A

3.3 Zubehör

Art.-Nr.	Beschreibung	Schnittstelle
VC-HD2HDSL-018-MM	HDMI-Kabel Stecker/Stecker, 1,8 m mit 1x SupraLock	Video
247-U1	USB-Kabel Typ A-B, 1,8 m	USB/USB-HID
247-U2	USB-Kabel Typ A-B, 3,0 m	USB/USB-HID
436-USB20	USB-Verlängerungskabel Typ A-A, 3,0 m	USB/USB-HID
459-1S	SFP Single-Mode, LC Duplex, bidirektional, 1G,	Glasfaser, 1G

3.4 Lieferumfang

Der Lieferumfang umfasst je nach Bestellung die folgenden Positionen und kann je nach Lieferland und Kundenspezifikation variieren:

Produkttyp	Lieferumfang
User Station	• 1x Draco SIRA User Station • 1x DC-Netzteil • 1x Vesa Befestigungs-Kit • Kurzanleitung

 Falls etwas fehlen sollte, bitte Ihren Händler kontaktieren.

3.5 Produkteigenschaften

- Unterstützung von KVM- und Serial-over-IP-Verbindungen zu Target-Servern
- Unterstützung von RDP, VNC, SSH, ESXi und Web-Targets
- Unterstützung von Monitoren mit HDMI- oder DisplayPort-Schnittstelle
- Bis zu vier Monitore möglich
- Zwei LAN-Verbindungen möglich
- Unterstützt virtuelle Medien, einschließlich externe DVD- und USB-Laufwerke oder Netzwerk-Speicher

 Virtuelle Medien werden nur unterstützt, wenn das KVM-Device dies unterstützt und Sie über die Berechtigung zur Nutzung virtueller Medien verfügen (siehe Abschnitt 6.4.1.3, Seite 68).

- USB Audio
- Authentifizierung an Target-Servern über optionale SmartCard
- Authentifizierung und Autorisierung über LDAP

3.6 Produktansichten

Vorderansicht

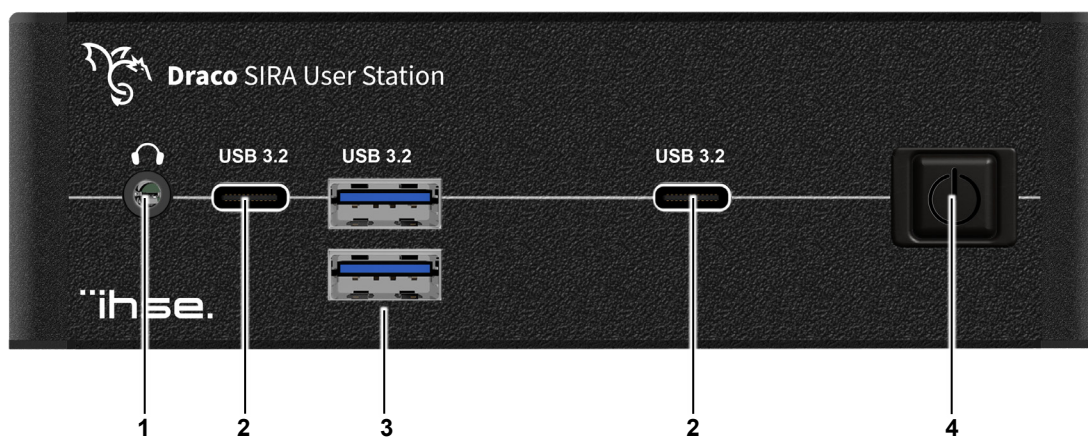


Abb. 3 **Frontseite**

- | | | | |
|---|--|---|-------------------------|
| 1 | 3,5 mm Anschluss für analoges Audio* | 3 | 2x USB 3.2 Typ A |
| 2 | USB 3.2 Typ C (inkl. DisplayPort 1.2a) | 4 | Ein/Ausschalter mit LED |

* Audio-Ausgangsport kann Lautsprecher und Mikrofon unterstützen über eine 3,5 mm Y-Kabel (nicht im Lieferumfang enthalten).

Rückansicht

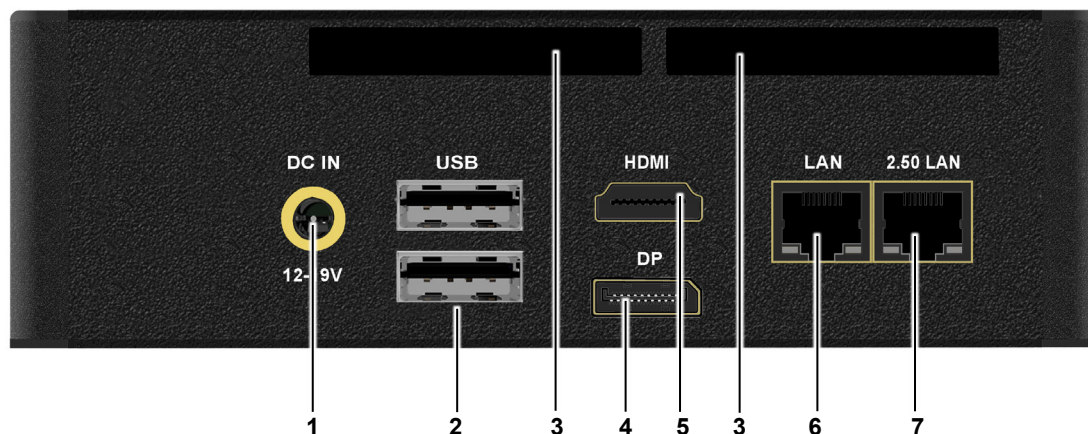


Abb. 4 Rückseite

- | | |
|-------------------------|---------------------|
| 1 DC-Eingang 12-19 V | 5 HDMI-Anschluss |
| 2 2x USB Typ A | 6 LAN-Port 1 Gbit |
| 3 Lüftungsschlitze | 7 LAN-Port 2,5 Gbit |
| 4 DisplayPort-Anschluss | |

3.7 Statusanzeige

3.7.1 Stromversorgung

Der Ein/Ausschalter an der Vorderseite beinhaltet eine LED, die leuchtet, wenn die User Station läuft.

3.7.2 Netzwerkverbindung

Die LAN-Anschlüsse sind mit zwei LEDs in den Farben Grün und Orange ausgestattet.

LED	Status	Beschreibung
 grün	Aus	Keine Netzwerk-Verbindung vorhanden.
	An	Netzwerk-Verbindung vorhanden.
 orange	Aus	Keine Datenübertragung.
	Blinkend	Daten werden übertragen.

4 Installation

HINWEIS

Sicherstellen, dass die Verbindungskabel, Schnittstellen und die Handhabung der Geräte den Anforderungen entsprechen (siehe Kapitel 13, ab Seite 178).

➔ Schalten Sie die User Station aus und ziehen Sie das Stromversorgungskabel ab.

4.1 User Station an Monitor befestigen

Sie können die User Station an der Rückseite eines Monitors mit 75- oder 100-mm-VESA-Standard befestigen. Im Lieferumfang sind zwei Montageplatten enthalten.



Abb. 5 VESA-Montageplatten

1. Schalten Sie den Monitor aus und trennen Sie ihn von der Stromversorgung.
2. Schrauben Sie die VESA-Montageplatten fest an der Rückseite des Monitors an mit vier Schrauben.
3. Entfernen Sie an beiden Seiten der User Station zwei Schrauben.



Abb. 6 Zu entfernende Schrauben

4. Setzen Sie die User Station zwischen die Montageplatten und richten Sie die beiden Schraubenlöcher auf jeder Seite an den entsprechenden Löchern der Montageplatten aus.
5. Schrauben Sie die zuvor entfernten Schrauben wieder ein und ziehen Sie sie fest.
Die Draco SIRA User Station ist nun sicher am Monitor befestigt.

4.2 Kabel und Zubehör anschließen

1. Trennen Sie alle Geräte von der Stromversorgung.
1. Schließen Sie eine USB-Tastatur und eine USB-Maus an der Front- oder Rückseite an die USB-A Ports an.
2. Optional: Verbinden Sie Mikrofon oder Lautsprecher über den Audio-Port an der Frontseite mit der User Station.
3. Verbinden Sie die Draco SIRA User Station mit dem Netzwerk über ein oder beide LAN-Ports an der Rückseite.
4. Schließen Sie mindestens einen (bis zu vier) Monitor über HDMI- oder DisplayPort-Ports an der Rückseite oder über einen USB-C 3.2 Ports an der Frontseite an die User Station an.

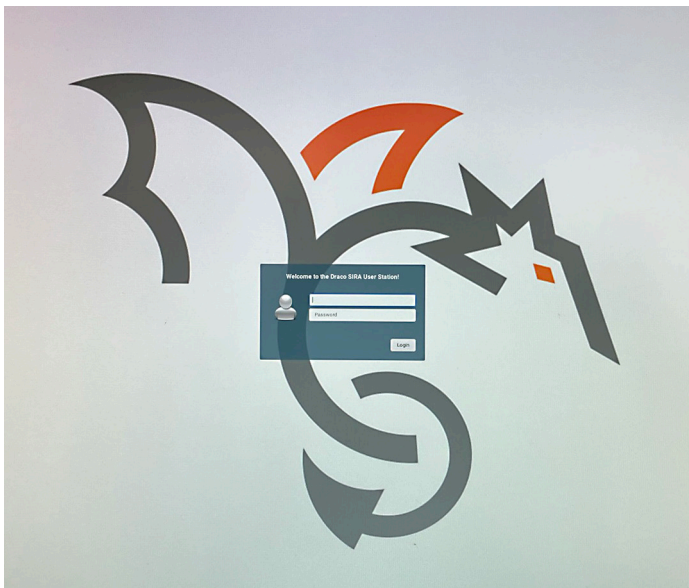
i HDMI und DisplayPort übertragen Video- und Audiosignale. Ihre Monitore müssen die Audioübertragung unterstützen, wenn Audio übertragen werden soll. Maximal vier Monitore werden unterstützt.

5. Schließen Sie das externe DC-Netzteil über den DC-Eingang an der Rückseite der User Station an und verbinden Sie es mit dem Stromnetz.
6. Schalten Sie die Draco SIRA User Station ein mit dem Ein/Ausschalter an der Vorderseite. Schalten Sie dann alle anderen Geräte ein (Monitor, etc.).

4.3 Erste Anmeldung an der Draco SIRA User Station

Nach dem Einschalten fährt die User Station hoch und die Anmeldemaske erscheint.

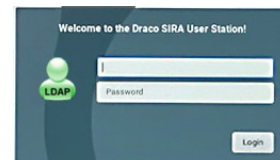
In der unteren Leiste werden das Systemdatum, die Uhrzeit und das Tastaturlayout (Standard: US-Englisch) angezeigt sowie das Symbol zum Neustarten oder Herunterfahren der User Station-



Das Anmelde-Symbol zeigt an, welcher Authentifizierungstyp verwendet wird:

Lokal (siehe Bild links)

- LDAP



- CC-SG



Abb. 7 **Anmeldemaske**

Ein Kontrollkästchen für die lokale Authentifizierung wird angezeigt, sobald der Benutzername „admin“ eingegeben wird, sowie für alle Benutzer, wenn die Option „Zugriff für lokale Benutzer zulassen“ im LDAP- oder CC-SG-Integrationsmodus aktiviert ist

- ➡ Verwenden Sie für die erste Anmeldung die werkseitigen Standard-Anmeldedaten (Groß-/Kleinschreibung beachten). Benutzername ist „admin“, Passwort ist ebenfalls „admin“.

i Hinweis: Bei der ersten Anmeldung muss das Standardpasswort in ein sicheres Passwort geändert werden.

5 Einführung in die Software

Nach dem Einschalten fährt die User Station hoch und der Login-Dialog erscheint (siehe vorheriger Abschnitt).

- ➔ Geben Sie Benutzernamen und Passwort ein und drücken die Taste **Enter** oder klicken Sie den Button **Login**. Der Startbildschirm erscheint.

Bei der ersten Anmeldung wird eine Willkommensmeldung angezeigt. Der Port Navigator wird standardmäßig geöffnet.

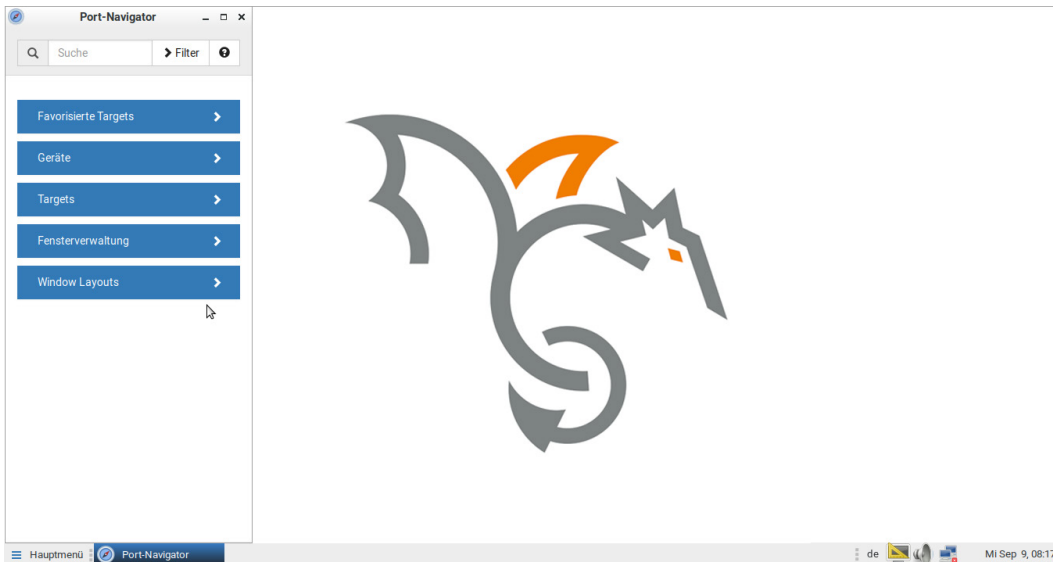


Abb. 8 **Hauptbildschirm mit geöffnetem Port Navigator**

5.1 Symbolleiste

Eine Symbolleiste befindet sich am unteren Rand des Bildschirms. Diese Symbolleiste zeigt den Button **Hauptmenü**, Shortcut-Symbole, geöffnete Menüs sowie alle geöffneten Fenster von User Station, KVM- und Serial Clients an.

Der Port Navigator wird standardmäßig geöffnet und kann über das Hauptmenü geschlossen und anschließend wieder geöffnet werden.

Die Symbolleiste enthält die folgenden Elemente:

i Abb. 8 zeigt die Standardbuttons und -Symbole. Es können mehr Symbole dazukommen, wenn Systemeinstellungen geändert werden, z.B. bezüglich des Monitors (siehe Abschnitt 5.3.4, Seite 32).

Button/Symbol	Beschreibung
Hauptmenü	Enthält die wichtigsten Befehle der User Station und die Systemeinstellungen (siehe nächster Abschnitt)
Offene Fenster	Wenn ein Fenster geöffnet wird, wird dessen Name in der Symbolleiste angezeigt. In Abbildung 8 wurde lediglich der Port Navigator geöffnet. Sie können mit der rechten Maustaste auf das Symbol eines beliebigen geöffneten Fensters klicken, um es zu minimieren, zu maximieren, zu verschieben, in der Größe anzupassen oder zu schließen.
Shortcut-Symbole	Zum Anzeigen/Konfigurieren der Systemeinstellungen. Bewegen Sie den Mauszeiger über ein Symbol, um Informationen anzuzeigen, oder klicken Sie mit der rechten Maustaste darauf, um die Einstellungen zu konfigurieren.
	Über dieses Symbol wird die Lautstärke eingestellt. Wenn Sie daraufklicken, wird ein Schieberegler zum Einstellen der Lautstärke angezeigt. Rechtsklicken zeigt einen Eintrag an, um die Lautsprecher stumm zu schalten.

Symbol	Beschreibung
de	Das Sprachkürzel zeigt das aktuelle Tastaturlayout an (Standard: en (American English)). Klicken wechselt zwischen den möglichen Optionen durch (Standard: en - Englisch (US), de - Deutsch, fr - Französisch). Rechtsklicken öffnet ein Shortcut-Menü mit den folgenden Einträgen: • Belegungen: Ändert das Tastaturlayout. • Tastatureinstellungen: Öffnet den Tastatureinstellungen-Dialog (siehe Abschnitt 5.3.3, Seite 30). • Aktuelle Belegung anzeigen.
	Netzwerk-Symbol, wenn Sie daraufklicken, wird eine Liste aller verfügbaren Ethernet-Netzwerke und -Verbindungen angezeigt. Rechtsklicken öffnet ein Shortcut-Menü mit den folgenden Einträgen: • Netzwerke aktivieren: Aktiviert oder deaktiviert die Netzwerkfunktion (Standard: aktiviert) • Verbindungsinformationen: Zeigt die Netzwerkinformationen der User Station an, einschließlich der IPv4- und IPv6-Adressen. • Verbindungen bearbeiten...: Öffnet den Dialog der Netzwerkverbindungen (siehe Abschnitt 5.3.6, Seite 35).
Mi Feb 18, 08:17	Datum und Zeit, zeigt Wochentag, Datum und aktuelle Zeit an. Wenn Sie daraufklicken, öffnet sich ein Kalender. Um den Kalender zu schließen, klicken Sie wieder auf das Datum. Rechtsklicken zeigt einen Eintrag zum Öffnen des Dialogs zur Einstellung von Datum und Zeit (siehe Abschnitt 5.3.1, Seite 26).

5.2 Hauptmenü

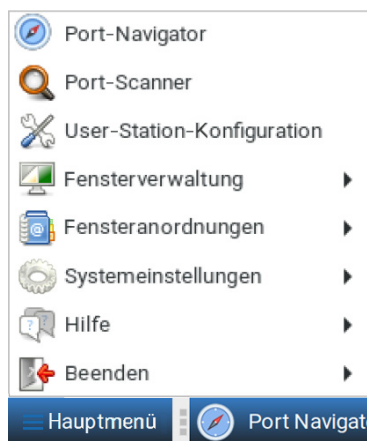


Abb. 9 **Hauptmenü**

5.2.1 Port-Navigator (Start)

Der Port-Navigator wird standardmäßig gestartet. Sie können ihn im Hauptmenü manuell starten und schließen (mehr zum Port-Navigator siehe Abschnitt 7.1, Seite 78).

5.2.2 Port-Scanner (Start)

Der Port-Scanner zeigt eine Auswahl an Ports an, die Sie auswählen können, indem Sie jede Verbindung über einen bestimmten Zeitraum hinweg scannen. Sie können eine KVM-Verbindung zu jedem im Scanner angezeigten Port herstellen.

Der Port-Scanner kann bei Aktivierung auch Target-Snapshots auf einem externen USB-Stick oder einem Netzwerkspeicher speichern. Dies ist für forensische oder Überwachungszwecke nützlich (siehe Port-Scanner-Einstellungen in Abschnitt 7.2.1, Seite 84) für detaillierte Informationen zu Konfiguration und Benutzerrechten).

➔ Starten Sie den Port-Scanner über das Hauptmenü.

5.2.3 User-Station-Konfiguration (Start)

Die User-Station-Konfiguration zeigt verschiedene Optionen zur Konfiguration der Draco SIRA User Station an (siehe Kapitel 6, ab Seite 53).

➔ Starten Sie die User-Station-Konfiguration über das Hauptmenü.

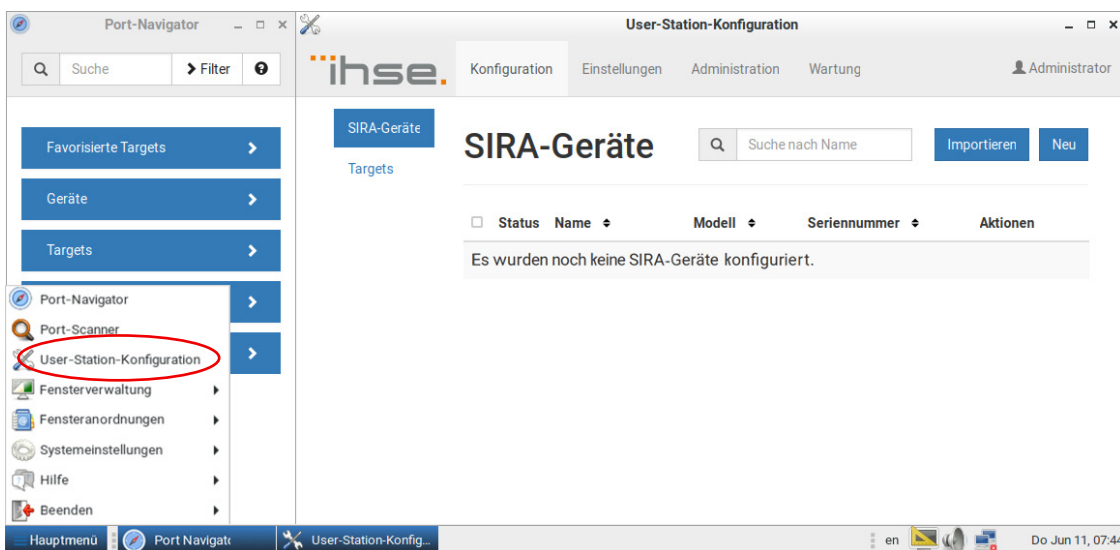


Abb. 10 Hauptmenü und User-Station-Konfigurationsseite

5.2.4 Firefox Web Browser

Administratoren oder Benutzer mit der Berechtigung „Webbrowser starten“ können die Option „Mit Firefox öffnen“ für Web-Targets konfigurieren, entweder für alle Targets (Client-Einstellungen aufrufen) oder für bestimmte Ziele (Zugriffspunkt-Prioritäten). Die Firefox-Option wird im Hauptmenü angezeigt, wenn Sie sich mit der entsprechenden Berechtigung angemeldet haben.

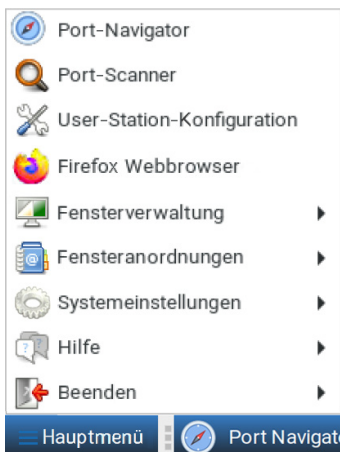


Abb. 11 Hauptmenü mit Firefox Eintrag

5.2.5 Fensterverwaltung

Die Fensterverwaltung hilft Ihnen dabei, geöffnete Sessions zu organisieren. Alle Client-Typen sind dabei berücksichtigt. Andere Fenster der User Station, wie beispielsweise der Port Navigator oder der Port Scanner, sind nicht in der Fensterverwaltung enthalten.

Wenn mehr als ein Monitor an die User Station angeschlossen ist, funktioniert diese Funktion auf jedem Monitor separat. Fenster werden nicht von einem Monitor auf einen anderen verschoben.

Informationen zum Speichern und Wiederherstellen von **Window Layouts** finden Sie im nächsten Abschnitt.

So verwenden Sie die Fensterverwaltung:

1. Klicken Sie auf **Hauptmenü > Fensterverwaltung** und wählen Sie eine Option aus.

Oder

2. Öffnen Sie den **Port-Navigator**, dann das Menü **Fensterverwaltung** und wählen Sie eine Option aus.

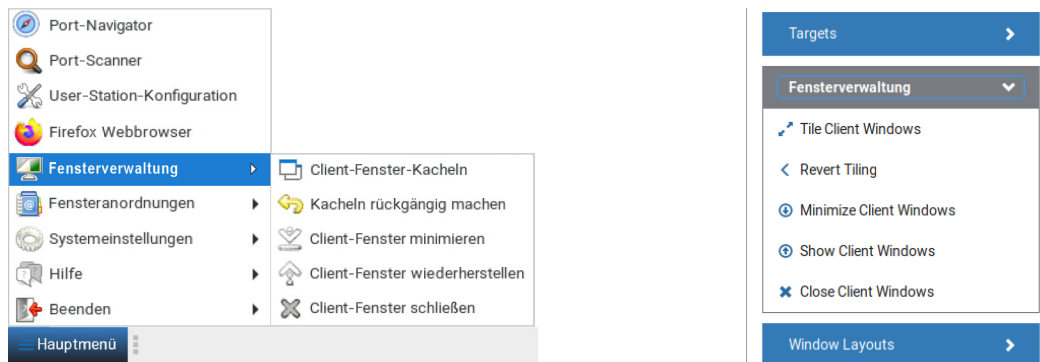


Abb. 12 Zwei Arten, die Fensterverwaltung zu öffnen

Option	Beschreibung
Client-Fenster-Kacheln	Ordnet alle Client-Fenster in einem gekachelten Layout auf dem Desktop an. Minimierte Fenster werden wieder maximiert.
Kacheln rückgängig machen	Macht den letzten Kachelmodus rückgängig und stellt die vorherigen Fenstergrößen wieder her. Zuvor minimierte Fenster werden erneut minimiert.
Client-Fenster minimieren	Minimiert alle Client-Fenster in die Symbolleiste.
Client-Fenster wiederherstellen	Alle Client-Fenster in der Symbolleiste werden auf dem Bildschirm dargestellt.
Client-Fenster schließen	Schließt alle Client-Fenster

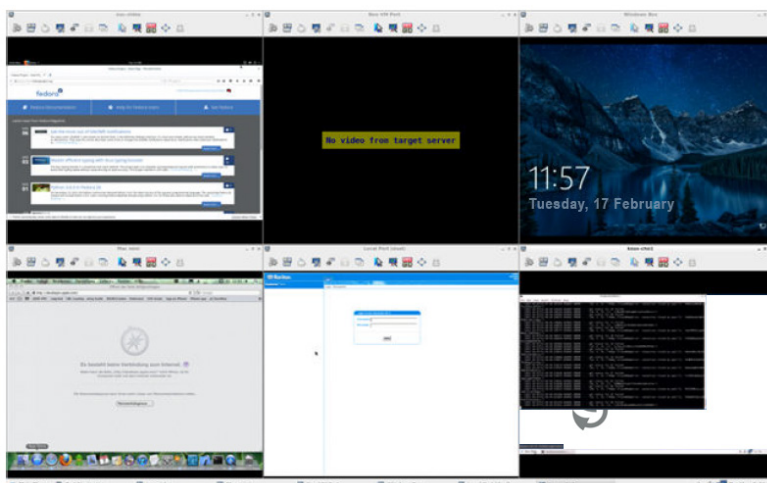


Abb. 13 Beispiel eines gekachelten Layouts

5.2.6 Fensteranordnungen

Mit der Funktion „Fensteranordnungen“ (Window Layouts) können Sie Layouts der geöffneten Access-Client-Fenster speichern, sodass das jeweilige Layout bei Auswahl wiederhergestellt wird. Die gespeicherten Window Layout-Daten umfassen die visuellen Attribute jeder Access-Client-Sitzung, wie Größe, Position und Anzeigemonitor, sowie die jeweiligen Verbindungsinformationen.

Layouts werden benutzerspezifisch gespeichert. Die von einem Benutzer gespeicherten Layouts stehen anderen Benutzern nicht zur Verfügung. Pro Benutzer sind maximal 16 benannte Layouts zulässig.

Sie können über den Port-Navigator (Window Layouts) oder das Hauptmenü (Fensteranordnungen) darauf zugreifen.

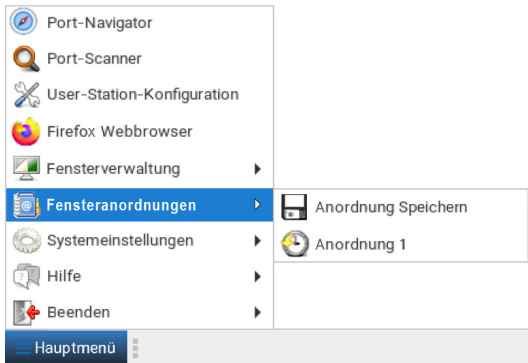


Abb. 14 **Fensteranordnungs-Optionen über Hauptmenü**

Speichern eines Window Layouts

1. Ordnen Sie Ihre Client-Fenster nach Belieben an. Sie können in ihrer Größe frei geändert und auf allen Monitoren positioniert werden.
2. Klicken Sie **Hauptmenü > Fensteranordnungen > Anordnung speichern**.
Wenn bereits gespeicherte Layouts vorhanden sind, enthält das Menü auch eine Option zum Speichern als neues Layout oder zum Überschreiben benannter Layouts. Neuen Layouts werden automatisch Namen (Nummern) zugewiesen.
Es erscheint eine Nachricht, die das Speichern des Layouts bestätigt und den Namen anzeigt.

Wiederherstellen eines Layouts

- ➔ Klicken Sie auf **Hauptmenü > Fensteranordnungen**, dann auf die Anordnung, die Sie wiederherstellen möchten.
Oder
 - ➔ Öffnen Sie den Port-Navigator, klicken Sie auf **Window Layouts** und klicken Sie in der Liste auf das Layout, das Sie wiederherstellen möchten.
- Wenn das Layout ausgewählt wird, werden alle derzeit geöffneten Clients geschlossen und das ausgewählte Layout wiederhergestellt. Bei der Wiederherstellung eines Layouts sind einige Targets möglicherweise nicht verfügbar. Die Client-Fenster für diese Targets werden dennoch mit ihren visuellen Eigenschaften wiederhergestellt, zusammen mit einer Fehlermeldung, dass keine Verbindung zu ihrem Target hergestellt werden kann.

5.2.7 Hilfe

1. Klicken Sie **Hauptmenü > Hilfe**.

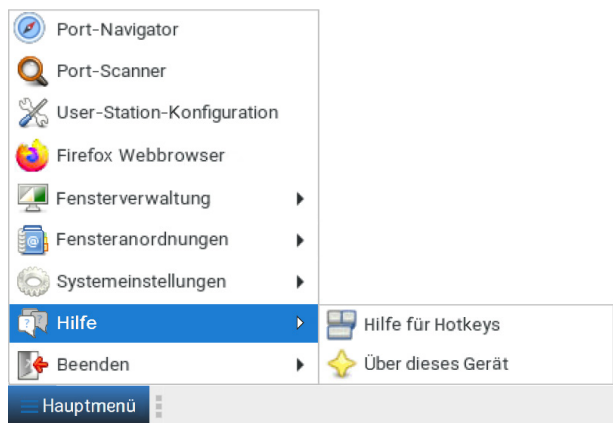


Abb. 15 **Hilfsoptionen über das Hauptmenü**

5.2.7.1 Informationen über das Gerät anzeigen

- ➔ Klicken Sie **Über dieses Gerät**, um ein Fenster zu öffnen, das Informationen über die User Station enthält einschließlich Software-Version und Kontaktdaten.

5.2.7.2 Informationen über Hotkeys anzeigen

- ➔ Klicken Sie **Hilfe für Hotkeys**, um eine Liste vordefinierter und durch den Benutzer konfigurierbarer Hotkeys anzuzeigen, die in der Software implementiert sind. Damit lassen sich Dialoge öffnen, Fenster verschieben oder ihre Größe ändern, Target-Fenster öffnen oder Operationen durchführen.

Die meisten Hotkeys auf dem Desktop können vom Benutzer konfiguriert werden (**Einstellungen > Hotkeys und Gesten**), einschließlich der Möglichkeit, sie zu deaktivieren. Die unten aufgeführten Hotkeys sind die werkseitigen Standard-Hotkeys. Nicht in dieser Liste enthalten sind Funktionen, deren Hotkeys standardmäßig deaktiviert sind.

Draco SIRA User Station-Funktionen

Hotkey	Funktion
Strg+Alt+N	Port Navigator starten.
Strg +Alt+C	Konfiguration starten.
Strg +Alt+L	User Station sperren.
Strg +Alt+Del	User Station herunterfahren oder neu starten.

Fensterverwaltungs-Funktionen

Die folgenden Hotkeys sind nützlich, um das aktuell aktive Fenster zu schließen oder zwischen Fenstern zu wechseln.

Hotkey	Funktion
Alt+F4	Aktives Fenster schließen.
Alt+Tab	Fokus auf das nächste Fenster umschalten.
Umschalt+Alt+Tab	Fokus auf das vorherige Fenster umschalten.

Die folgenden Tasten dienen zum Verschieben oder Ändern der Größe geöffneter Fenster sowie zum Wechseln zwischen Fenstern. Sie lassen sich nicht einzeln konfigurieren, können jedoch global aktiviert oder deaktiviert werden. Beachten Sie, dass die Tasten des Ziffernblocks unabhängig vom Status der Num-Taste funktionieren. Die Tasten 4, 6, 8 und 2 des Ziffernblocks dienen als Pfeiltasten nach links, rechts, oben und unten.

Hotkey	Funktion
Umschalt+Windows+ [Links/Rechts/Hoch/ Runter]	Wechselt vom aktuell aktiven Fenster zu dem Fenster, das sich in der angegebenen Richtung befindet.
Strg+Alt+Umschalt+ [Links/Rechts]	Das aktive Fenster auf den vorherigen/nächsten Monitor verschieben.
Strg+Alt+Umschalt+ [Links/Rechts/Hoch/ Runter] oder Strg+Alt+ [Ziffernfeld 1/3/7/9]	Das aktive Fenster an den linken/rechten/oberen/unteren Rand des aktuellen Monitors verschieben.
Strg+Umschalt+ [Links/Rechts/Hoch/ Runter]	Das aktive Fenster an den nächstgelegenen Rand in der angegebenen Richtung verschieben.
Strg+Win+ [Links/Rechts/Hoch/ Runter]	Vergrößert das aktive Fenster, bis es den nächstgelegenen Rand in der angegebenen Richtung berührt. Als Ränder gelten die Außenränder des anderen Fensters, die Bildschirmränder bei Konfigurationen mit mehreren Bildschirmen oder die Desktop-Grenzen. Befindet sich der Fensterrand bereits am Bildschirmrand, wird das Fenster stattdessen verkleinert.
Alt+Windows+ [Links/Rechts/Hoch/ Runter]	Verkleinert das aktive Fenster so weit, bis es den nächstgelegenen Rand in der angegebenen Richtung berührt. Als Ränder gelten die Außenränder des anderen Fensters, die Bildschirmränder bei Konfigurationen mit mehreren Bildschirmen oder die Desktop-Ränder. Wird kein Rand gefunden, wird das Fenster auf die Hälfte seiner Größe verkleinert.

Zugangs-Client-Funktionen

Die folgenden Hotkeys sind nur während einer aktiven Target-Verbindung verfügbar.

Hotkey	Funktion
Strg+Alt+M	Single-Cursor-Modus verlassen (nur KVM-Clients). Nur verfügbar im Single-Cursor-Modus. Der Single-Cursor-Modus ist nicht verfügbar, wenn dieser Hotkey deaktiviert ist.
Strg+Alt+F	Bei KVM- und VNC-Clients den Vollbildmodus aktivieren oder deaktivieren.
Strg+Alt+Enter	Bei RDP-Clients den Vollbildmodus aktivieren oder deaktivieren.
F11	Bei SSH-, Serial-, oder ESXi-Clients den Vollbildmodus aktivieren oder deaktivieren.

Target Hotkeys

Sie können Target Hotkeys für den schnellen Zugriff auf KVM-Ports oder andere Targets konfigurieren.

1. Bei KVM-Ports öffnen Sie die Konfiguration, wählen Sie ein KVM-Gerät, wählen Sie einen Port und klicken Sie auf **Einstellungen bearbeiten**.
2. Bei anderen Targets wählen sie Targets, dann einen Access Point für dieses Target und klicken Sie dann auf **Einstellungen bearbeiten**.
3. Wählen Sie den Hotkey aus, den Sie für diesen Port verwenden wollen und klicken Sie auf **OK**.
Mögliche Hotkeys sind:

Hotkey	Funktion
Strg+Umschalt+	Funktionstaste (F1...F12)
	Buchstabe
Strg+Alt+	Zahl
	Buchstabe
Umschalt+Alt+	Funktionstaste (F1...F12)
	Buchstabe
Strg+Umschalt+Alt+	Funktionstaste (F1...F12)
	Buchstabe

 Einige Hotkeys werden möglicherweise vom User Station-System überschrieben. Testen Sie alle Hotkeys, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Hotkeys, die für User Station-Funktionen oder Zugangs Client-Funktionen konfiguriert sind, können nicht als Target-Hotkeys verwendet werden.

5.2.8 Beenden

1. Klicken Sie **Hauptmenü > Beenden**.

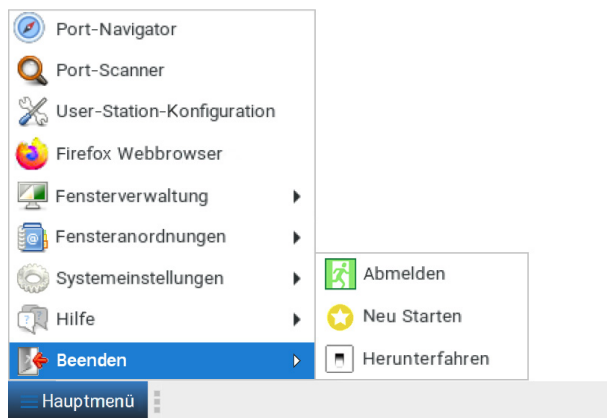


Abb. 16 **Beenden Menü über das Hauptmenü**

2. Klicken Sie auf die gewünschte Option.

- Abmelden: Der Benutzer wird abgemeldet.
- Neu Starten: Die User Station wird neu gestartet.
- Herunterfahren: Die User Station wird heruntergefahren und dann ausgeschaltet. Sie sollten immer dieses Software-Kommando benutzen, um die User Station auszuschalten.

HINWEIS

Schalten Sie die Draco SIRA User Station niemals aus, indem Sie den Ein-/Ausschalter gedrückt halten oder das Stromkabel abziehen, da dies zu Schäden an der User Station führen kann.

➔ Drücken Sie kurz den Ein-/Ausschalter, um ein sanftes Herunterfahren einzuleiten. Offene Sessions werden nicht gespeichert.

5.3 Systemeinstellungen

➔ Klicken Sie auf **Hauptmenü > Systemeinstellungen**.

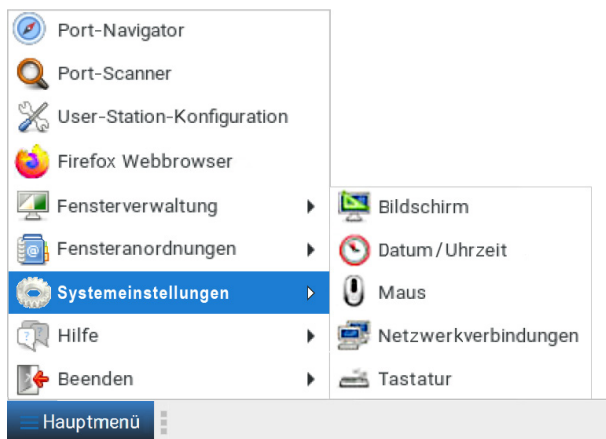


Abb. 17 Systemeinstellungen über Hauptmenü

5.3.1 Datum und Zeit

➔ Klicken Sie auf **Hauptmenü > Systemeinstellungen > Datum / Zeit**. Der Datum/Zeit-Dialog erscheint.

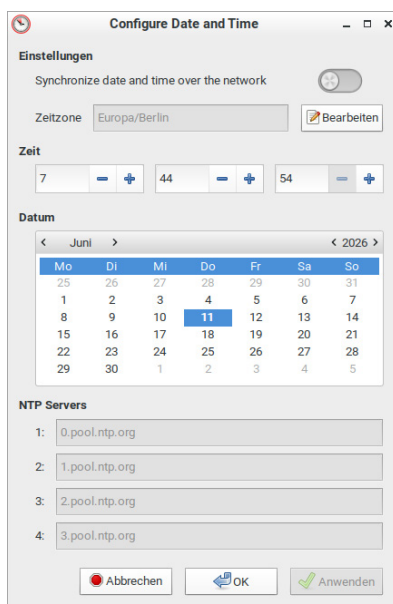


Abb. 18 Systemeinstellungen - Konfiguration von Datum und Zeit

Datum und Zeit können manuell eingestellt oder mit einem NTP-Server synchronisiert werden. Bei beiden Versionen ist die Einstellung der Zeitzone wichtig. Wenn sie korrekt eingestellt ist, sollte sie nicht geändert werden, es sei denn, es ist zwingend nötig.

Zeitzone

1. Klicken Sie auf den Button **Bearbeiten** im „Configure Date and Time“-Dialog, um die „Zeitzonenauswahl“ Landkarte anzuzeigen.
2. Nutzen Sie die Suchbox, um Ihre Stadt oder Zone zu finden. Klicken Sie darauf, um sie hervorzuheben und klicken Sie dann auf **OK**.

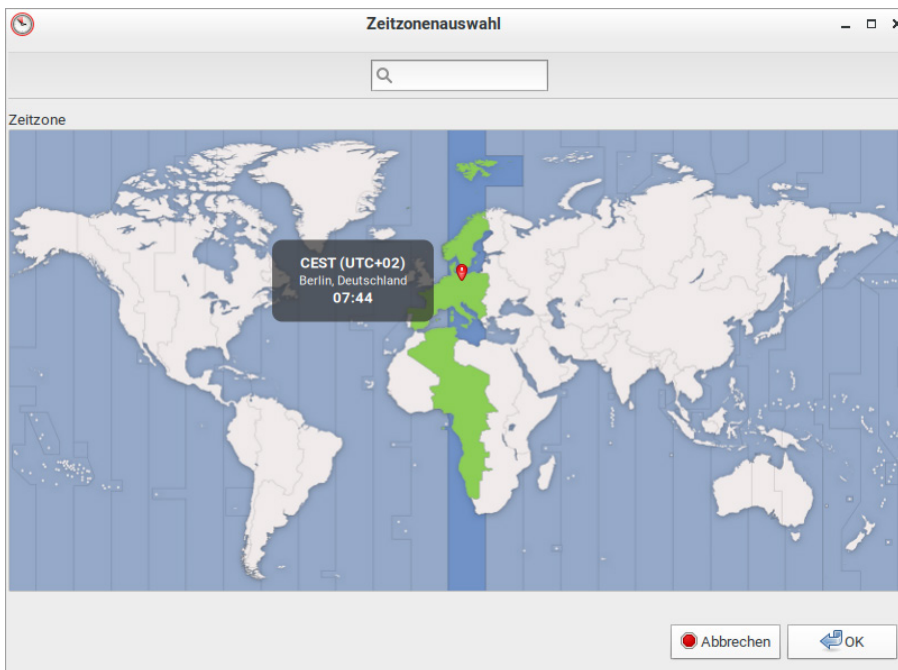


Abb. 19 Systemeinstellungen - **Auswahl der Zeitzone**

- Wird die Zeit mit einem NTP-Server synchronisiert, wirken sich Zeitzoneänderungen auf die auf dem Bildschirm angezeigte Uhrzeit, die Sommerzeit und die interne UTC-basierte Uhr der User Station aus.
- Bei manueller Einstellung von Datum und Zeit ändert eine Änderung der Zeitzone die auf dem Bildschirm angezeigte Uhrzeit nicht, aber die interne UTC-basierte Uhr wird geändert.

5.3.1.1 Manuelle Einstellung von Datum und Zeit

1. Wählen Sie, wenn nötig, die korrekte Zeitzone aus und klicken Sie auf **OK**.
2. Nutzen Sie die "Zeit" und "Datum" Abschnitte, um die aktuellen Daten einzustellen.

 Der Zeit-Abschnitt nutzt eine 24-Stunden-Uhr.

3. Klicken Sie den Button **Anwenden**.

5.3.1.2 NTP-Server verwenden

1. Im Dialog „Configure Date and Time“ schalten Sie die Funktion *Synchronize date and time over the network* ein.
2. Klicken Sie auf **Edit** und wählen Sie die korrekte Zeitzone aus, wenn nötig.
3. Klicken Sie auf **OK**.

 Es kann einige Minuten dauern, bis die NTP-Uhrzeit übernommen wird. Es wird empfohlen, keine Windows-NTP-Server zu verwenden.

5.3.2 Standort- und Wettereinstellungen

1. Klicken Sie auf die Zeitanzeige in der Symbolleiste. Ein Kalender wird geöffnet.
2. Klappen Sie den Abschnitt „Ort“ auf.

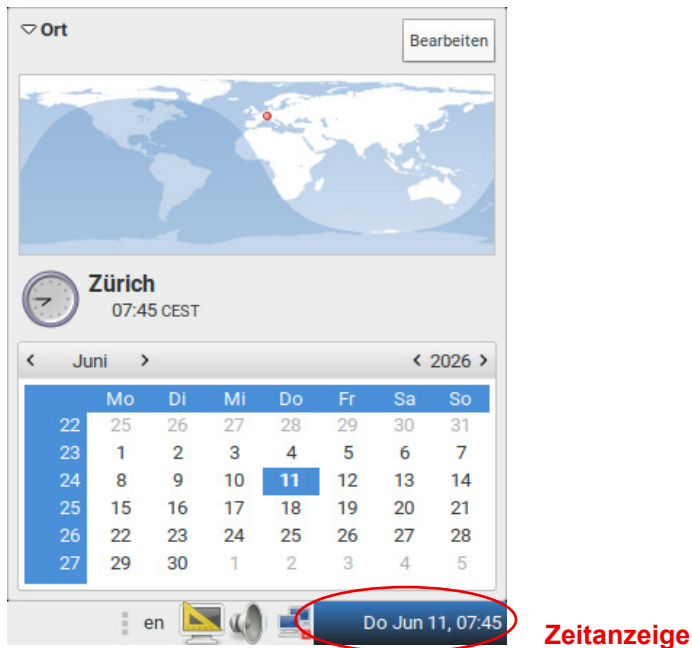


Abb. 20 Systemeinstellungen - Zeitanzeige, Kalender und Standort

3. Klicken Sie auf **Bearbeiten**. Der Dialog „Uhreinstellungen“ wird geöffnet.
4. Klicken Sie auf den Reiter **Ort**.

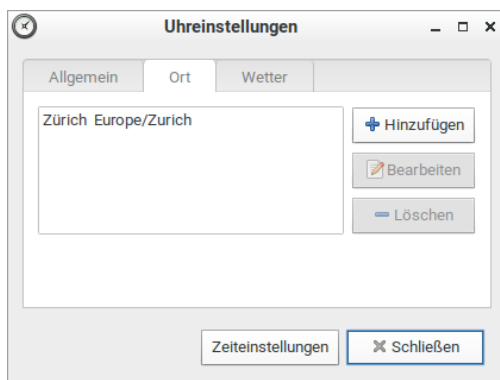


Abb. 21 Systemeinstellungen - Uhreinstellungen - Ort

Hinzufügen eines Ortes

1. Klicken Sie auf **Hinzufügen**, um eine Stadt oder ein Land zu spezifizieren. Sie können den Namen in das Feld „Name des Ortes“ tippen und dann den korrekten Eintrag aus der Liste auswählen, die erscheint.

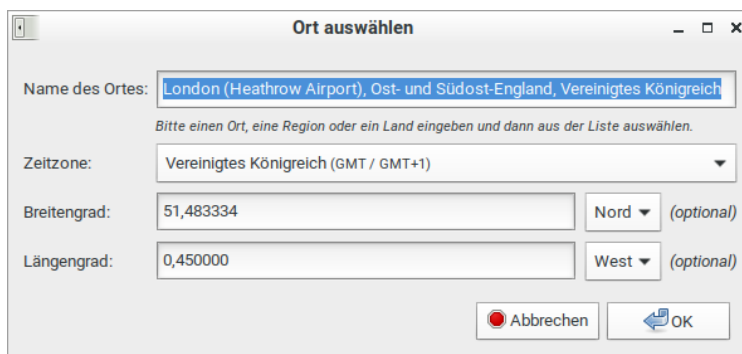


Abb. 22 Systemeinstellungen - Uhreinstellungen - Ort auswählen

2. Wenn die Stadt oder das Land in der Liste nicht enthalten ist, können Sie manuell die „Zeitzone“, „Breitengrad“ und „Längengrad“ eingeben.
3. Klicken Sie auf **OK**.
4. Um einen Ortseintrag zu ändern oder zu löschen, wählen Sie ihn auf der Registerkarte *Ort* aus und klicken Sie entweder auf **Bearbeiten** oder auf **Löschen**.

Klicken auf den Button **Zeiteinstellungen** öffnet den Datum/Zeit-Dialog (siehe Abschnitt 5.3.1, Seite 26).

Wettereinstellungen

1. Im Dialog „Uhreinstellungen“, klicken Sie auf den Reiter *Wetter*.

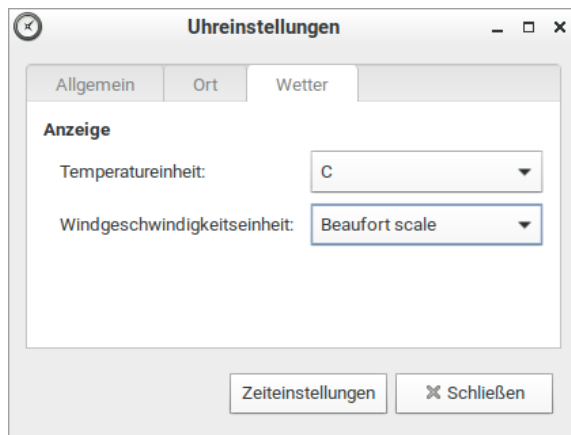


Abb. 23 Systemeinstellungen - Uhreinstellungen - **Wetter**

2. Legen Sie die Temperatureinheit fest. Sie können wählen zwischen C (Grad Celsius), F (Grad Fahrenheit) oder K (Kelvin).
3. Legen Sie die Einheit für die Windgeschwindigkeit fest. Sie können wählen zwischen m/s, km/h, mph, knots oder die Beaufort-Skala.

Allgemeine Einstellungen

1. Im Dialog Uhreinstellungen, klicken Sie den Reiter *Allgemein*.

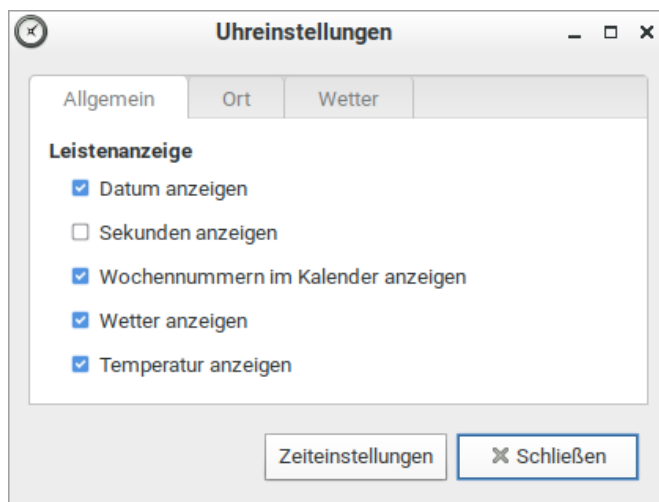


Abb. 24 Systemeinstellungen - Uhreinstellungen - **Allgemein**

2. Unter „Leistenanzeige“ wählen Sie die Informationen aus, die in der Symbolleiste am unteren Rand angezeigt werden sollen.

Datum und Sekunden, wenn ausgewählt, erscheinen in der Symbolleiste bei der Uhrzeit. KW-Nummern, wenn ausgewählt, werden im Kalender angezeigt. Wetter und Temperatur, wenn ausgewählt, erscheinen an zwei Positionen:

- In der Symbolleiste
- Im Abschnitt Ort: Wenn Sie den Mauszeiger über das Wettersymbol unterhalb des Ortsnamens bewegen, werden weitere Informationen angezeigt, darunter das Wetter, die Temperatur, die Windgeschwindigkeit sowie die Zeiten für Sonnenauf- und Sonnenuntergang.

✓ Wenn die Zeitzoneneinstellung des Systems von der des ausgewählten Standorts abweicht und Sie über Systemadministratorrechte verfügen, erscheint rechts neben dem Standortnamen eine Schaltfläche „Festlegen“, sobald Sie den Mauszeiger darüber bewegen. Sie können auf die Schaltfläche klicken, um die Zeitzone des Standorts als Systemzeitzone festzulegen.

5.3.3 Tastatur

1. Klicken Sie auf **Hauptmenü > Systemeinstellungen > Tastatur**. Der Dialog „Tastatur-Einstellungen“ wird geöffnet.

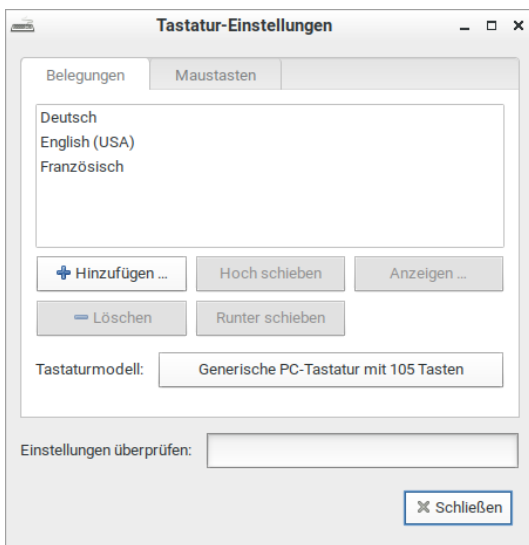


Abb. 25 Systemeinstellungen - Tastatur-Einstellungen

Auf der Registerkarte „Belegungen“ werden die verfügbaren Tastaturlayouts aufgelistet. Dieselbe Tastaturliste wird auch angezeigt, wenn Sie auf das Tastatursymbol in der Symbolleiste klicken (siehe Abschnitt 5.1, Seite 18).

Änderungen in einer Liste wirken sich auch auf die andere Liste aus.

Es werden maximal vier Belegungen unterstützt. Wenn Sie bereits vier in der Liste haben, müssen Sie eines entfernen, bevor Sie eine neue Belegung hinzufügen können.

Geben Sie im Feld „Einstellungen überprüfen:“ einen beliebigen Text ein, um die aktuelle Tastatureinstellung zu überprüfen.

2. Klicken Sie auf **+ Hinzufügen**, um eine neue Belegung in die Liste aufzunehmen.

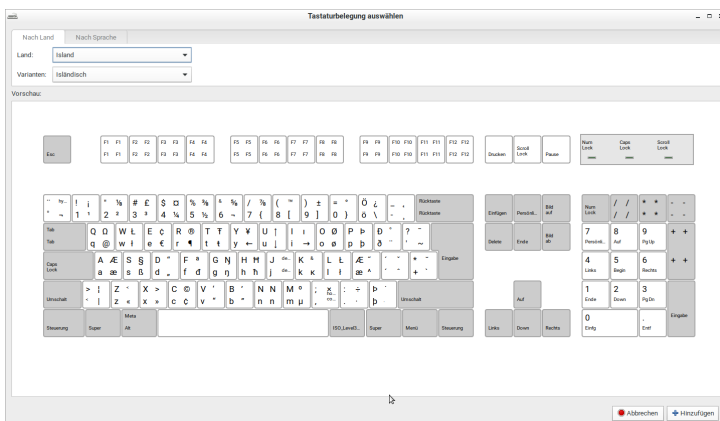


Abb. 26 Systemeinstellungen - Tastatur-Einstellungen - Neue Belegung auswählen

- Wählen Sie eine Belegung nach Land oder Sprache aus, um eine Vorschau der Tastaturbelegung anzuzeigen.
- Klicken Sie auf **Hinzufügen**, um die ausgewählte Belegung zu der Liste hinzuzufügen vorausgesetzt, es sind nicht schon vier Belegungen in der Liste.
- Sie können das Tastaturmodell festlegen, indem Sie auf das Feld „Tastaturmodell“ klicken.

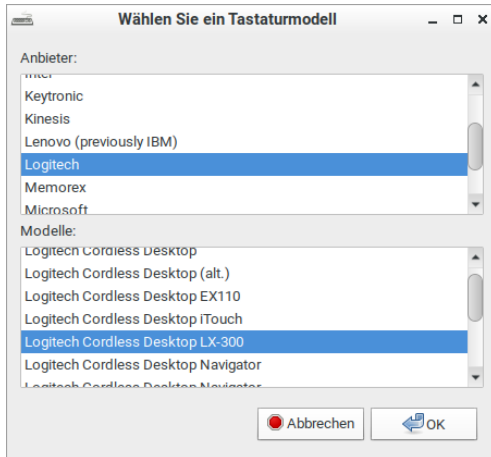


Abb. 27 Systemeinstellungen - Tastatur-Einstellungen - **Liste von Tastaturherstellern und Modellen**

- Wählen Sie den Hersteller und das Modell ihrer Tastatur aus und klicken Sie **OK**.

Maustasten

- Klicken Sie auf den Reiter **Maustasten**.

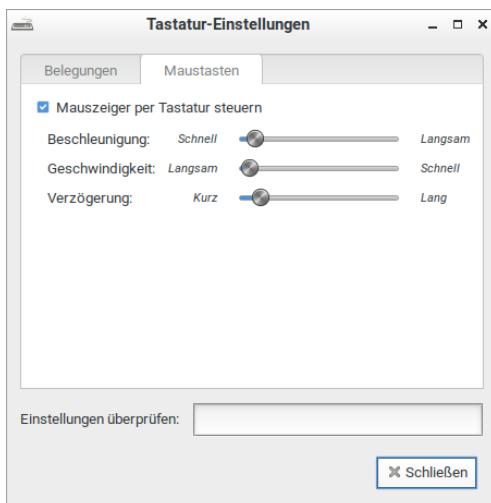


Abb. 28 Systemeinstellungen - Tastatur-Einstellungen - **Maustasten**

- Wenn Sie den Mauszeiger/Cursor über den Ziffernblock steuern möchten, aktivieren Sie das Kontrollkästchen „Mauszeiger per Tastatur steuern“.

Bei aktivierter Option funktioniert jede Taste des Ziffernblocks wie in der folgenden Tabelle angegeben.

Taste	Funktion
0	Ausgewählter Button wird gedrückt
-	Ausgewählter Button wird losgelassen
1	Cursor bewegt sich in die untere linke Ecke
2	Cursor bewegt sich nach unten
3	Cursor bewegt sich in die untere rechte Ecke
4	Cursor bewegt sich nach links
5	Klick auf den selektierten Button

Taste	Funktion
6	Cursor bewegt sich nach rechts
7	Cursor bewegt sich in die obere linke Ecke
8	Cursor bewegt sich nach oben
9	Cursor bewegt sich in die obere rechte Ecke
/	Primären Button auswählen
-	Alternativen Button auswählen
+	Doppelklick auf den ausgewählten Button
Enter	Enter

- Verwenden Sie die Schieberegler für „Beschleunigung“, „Geschwindigkeit“ und „Verzögerung“, um die entsprechenden Funktionen anzupassen. Links ist langsamer, rechts ist schneller.
- Klicken Sie auf **Schließen**.

5.3.4 Monitor

- Klicken Sie auf **Hauptmenü > Systemeinstellungen > Monitor**. Der Dialog „Bildschirmeinstellungen“ erscheint.

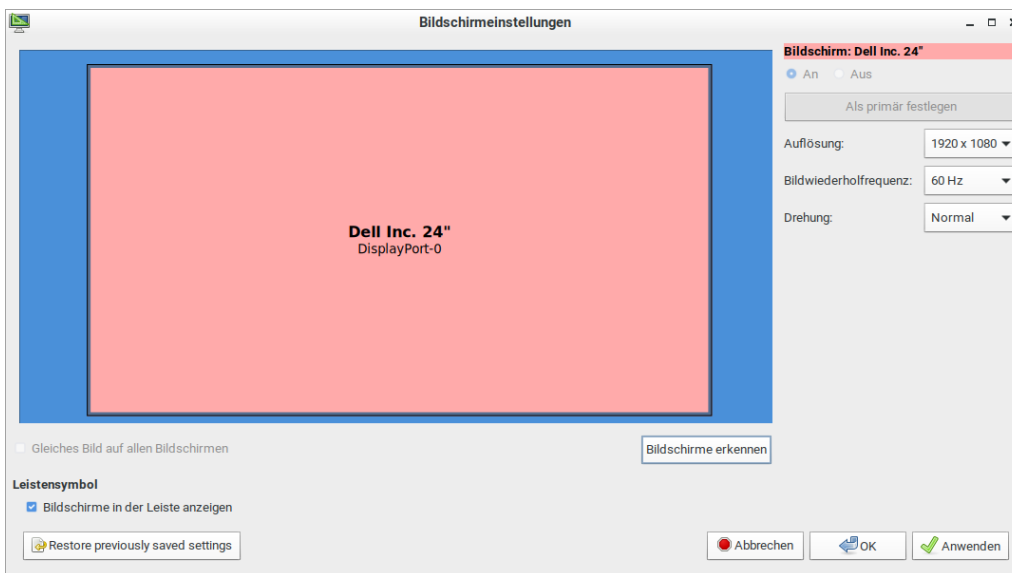


Abb. 29 Systemeinstellungen - Bildschirmeinstellungen

- Führen Sie eine der folgenden Funktionen aus oder konfigurieren Sie sie:

Einstellung/Button	Funktion
An/Aus	Schalten Sie diesen Monitor ein oder aus, wenn mehr als ein Monitor an die User Station angeschlossen ist. Diese Einstellung ist deaktiviert, wenn nur ein Monitor angeschlossen ist.
Als primär festlegen	Klicken Sie auf diesen Button, um diesen Monitor als primären Monitor festzulegen, wenn mehrere Monitore angeschlossen sind. Diese Schaltfläche ist deaktiviert, wenn nur ein Monitor angeschlossen ist oder wenn dieser Monitor bereits der primäre Monitor ist.
Auflösung	Legt die Video-Auflösung fest für diesen Monitor.
Bildwiederhol- frequenz	Legt die Bildwiederholfrequenz für diesen Monitor fest.
Drehung	Legt fest, wie das Bild auf dem Bildschirm gedreht werden soll, falls dies gewünscht ist. Sie können zwischen „Normal“, „Links“, „Rechts“ und „Auf dem Kopf“ wählen.

Gleiches Bild auf allen Bildschirmen	Wenn mehr als ein Monitor angeschlossen ist, legen Sie fest, dass auf allen Monitoren dasselbe Bild angezeigt wird. Diese Einstellung ist deaktiviert, wenn nur ein Monitor angeschlossen ist.
Bildschirme erkennen	Klicken Sie auf diesen Button, wenn ein angeschlossener Monitor nicht erkannt wird. In der Regel ist es nicht erforderlich, diese Funktion zu nutzen, wenn nur ein Monitor angeschlossen ist.
Bildschirme in der Leiste anzeigen	Legt fest, dass das Monitor-Symbol in der Symbolleiste erscheint.  Anklicken dieses Shortcut-Symbols öffnet den Dialog "Bildschirmeinstellungen".
Restore previously saved settings	Klicken Sie auf diese Schaltfläche, um die zuvor gespeicherten Einstellungen aller Monitore wiederherzustellen.

3. Wenn Sie Einstellungen geändert haben, klicken Sie auf „**OK**“, um die Änderungen zu speichern und das Dialogfeld zu schließen, auf „**Anwenden**“, um die Änderungen zu speichern und das Dialogfeld geöffnet zu lassen, oder auf „**Abbrechen**“, um die Änderungen zu verwerfen und das Dialogfeld zu schließen.

☒ Wenn Sie **OK** oder **Anwenden** klicken, erscheint eine Abfrage.

4. Klicken Sie **Vorherige Einstellungen wiederherstellen**, um die originalen Einstellungen wieder herzustellen oder **Diese Einstellungen beibehalten**, um die neuen Einstellungen anzuwenden.

5.3.5 Maus

Der Dialog „Mauseinstellungen“ wirkt sich ausschließlich auf die Funktionsweise Ihrer Maus in der Draco SIRA User Station aus. Diese Einstellungen haben keinen Einfluss auf Ihre Maus in den Fenstern des KVM-Clients.

1. Klicken Sie auf **Hauptmenu > Systemeinstellungen > Maus**. Der Dialog „Einstellungen für die Maus“ erscheint.

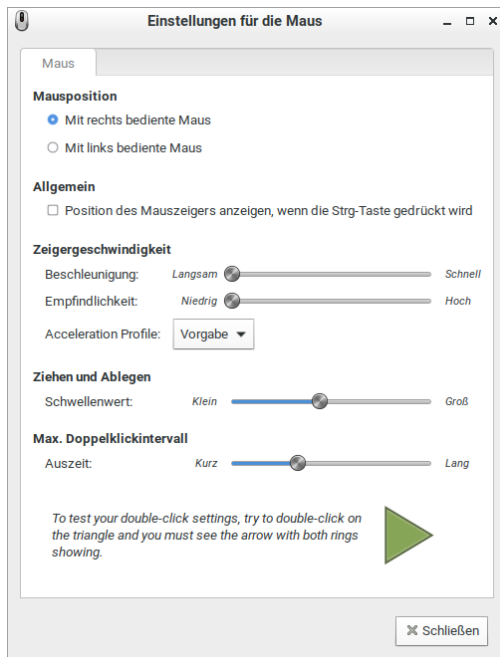


Abb. 30 Systemeinstellungen - **Einstellungen für die Maus**

Einstellung	Beschreibung
Mausposition	Wählen Sie entweder „Mit rechtes bediente Maus“ oder „Mit links bediente Maus“.
Allgemein	Mit der Option, die Position des Zeigers anzuzeigen, wenn die Strg-Taste gedrückt wird.
Zeigergeschwindigkeit	Sie können die Beschleunigung und die Empfindlichkeit einstellen.
Ziehen und Ablegen	Sie können den Schwellenwert für Drag-and-Drop-Vorgänge anpassen.
Max. Doppelklick-intervall	Sie können die Länge von kurz bis lang einstellen. Doppelklicken Sie auf das grüne Dreieck, um die Einstellung zu testen.

2. Klicken Sie auf **Schließen**, um diesen Dialog zu beenden.

5.3.6 Netzwerk

5.3.6.1 Ethernet-Verbindungen

Sie können beide LAN-Anschlüsse der User Station mit demselben oder mit unterschiedlichen Subnetzen verbinden. Wenn Sie beim Einschalten oder Neustarten der User Station beide LAN-Anschlüsse mit dem Netzwerk bzw. den Netzwerken verbunden haben, wählt die User Station nach dem Zufallsprinzip eine der Netzwerkverbindungen als Standardverbindung aus. Wenn Sie jedoch die Netzwerkeinstellungen einer der beiden Verbindungen ändern, wird die „zuletzt“ geänderte Verbindung automatisch zur Standardverbindung.

✓ Die Standardverbindung können Sie im Dialogfeld „Netzwerk-Informationen“ über das Netzwerksymbol erkennen (siehe Abschnitt 5.1, Seite 18).

Standardmäßig sind sowohl IPv4- als auch IPv6-Adressierung für beide LAN-Ports aktiviert, und die Standard-Netzwerkeinstellungen lauten:

- IPv4: Automatic (DHCP)
- IPv6: Automatic

Sie können zusätzliche Ethernet-Optionen festlegen, z. B. MTU und Wake-on-LAN. Außerdem können Sie Bond-Geräte konfigurieren. Wie das geht, wird in diesem Abschnitt beschrieben.

Netzwerk-Einstellungen ändern

1. Klicken Sie auf **Hauptmenü > Systemeinstellungen > Netzwerkverbindungen**. Der “Netzwerk-Verbindungen” Dialog erscheint mit zwei werkseitig angelegten Standardverbindungen für zwei LAN-Anschlüsse.

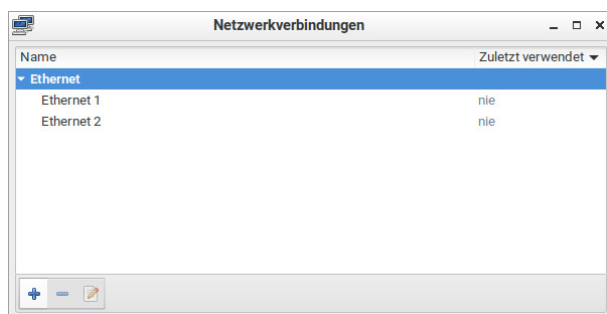


Abb. 31 Systemeinstellungen - Netzwerkverbindungen - **Startmenü**

- *Ethernet 1* ist für LAN-Port 1
- *Ethernet 2* ist für LAN-Port 2

Symbol	Funktion
	Neue Netzwerkverbindung hinzufügen.
	Eine Netzwerkverbindung löschen.
	Bearbeitungssymbol zur Änderung einer Netzwerkverbindung.

2. Wählen Sie die gewünschte Verbindung aus und klicken Sie auf das Bearbeitungssymbol in der unteren linken Ecke. Ein Dialogfeld erscheint.

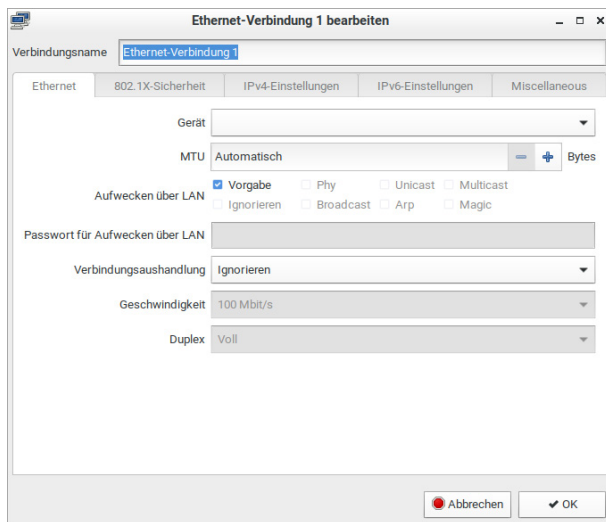


Abb. 32 Systemeinstellungen - Netzwerkverbindungen - **Verbindung ändern**

3. Geben Sie bei Bedarf einen neuen Namen in das Feld „Verbindungsname“ ein.
4. Klicken Sie auf die Registerkarte „IPv4-Einstellungen“ oder „IPv6-Einstellungen“, um die Netzwerkeinstellungen korrekt zu konfigurieren (siehe folgende Seiten).
5. Klicken Sie auf **OK**. Die neuen Netzwerkeinstellungen werden übernommen.

✓ Die aktuellen IP-Adressen können Sie im Dialogfeld „Verbindungsinformationen“ abrufen, das sich öffnet, wenn Sie auf das Netzwerksymbol in der Symbolleiste klicken.

Weitere Ethernet-Einstellungen

Funktion	Beschreibung
Gerät	Diese Option bindet diese Verbindung an das Netzwerkgerät, das entweder durch seinen Schnittstellennamen, seine permanente MAC-Adresse oder beides angegeben wird. Beispiele: „em1“, „3C:97:0E:42:1A“, „em1 (3C:97:0E:42:1A:19)“
MTU	Wählen Sie „Automatisch“ oder klicken Sie auf plus/minus , um die maximale Anzahl der Bytes pro Paket festzulegen.
Aufwecken über LAN	Lassen Sie die Einstellung auf „Standard“ oder deaktivieren Sie die Standardauswahl, um die anderen Optionen zu aktivieren. Für „Magic“ ist ein Wake-on-LAN-Passwort erforderlich, das in das dann aktive Feld „Passwort für Aufwecken über LAN“ eingegeben werden kann.
Verbindungsaushandlung	Sie können wählen zwischen „Ignorieren“, „Automatisch“ oder „Manuell“. Wenn Sie „Manuell“ auswählen, müssen Sie „Geschwindigkeit“ und „Duplex“ einstellen.  Wenn „Manuell“ ausgewählt wird, werden die Werte für „Geschwindigkeit“ und „Duplex“ ohne Überprüfung der Gerätekompatibilität erzwungen. Im Zweifelsfall wählen Sie hier „Ignorieren“ oder „Automatisch“.

IPv4-Einstellungen

1. Klicken Sie auf den Reiter *IPv4-Einstellungen*.

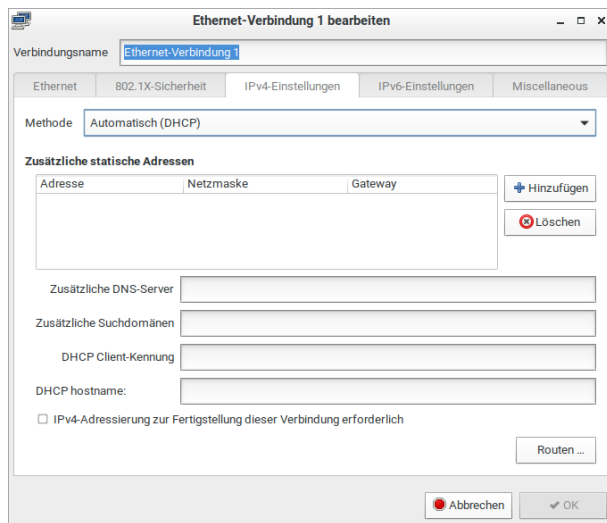


Abb. 33 Systemeinstellungen - Netzwerkverbindungen - Registerkarte **IPv4-Einstellungen**

2. Wählen Sie eine Methode aus den folgenden Optionen aus.

- **Automatisch (DHCP)**
 Der DHCP-Server im Netzwerk weist der User Station sowie den DNS-Servern und Domänen automatisch eine IPv4-Adresse zu.
 Für diese Methode können die folgenden Einstellungen konfiguriert werden (Beschreibung auf der nächsten Seite):
 - Zusätzliche DNS-Server
 - Zusätzliche Suchdomänen
 - DHCP Client-Kennung
 - DHCP hostname
 - IPv4-Adressierung zur Fertigstellung dieser Verbindung erforderlich
 - Routen
- **Automatisch (DHCP), nur Adressen**
 Der DHCP-Server im Netzwerk weist der User Station automatisch eine IPv4-Adresse zu, es sind jedoch keine DNS-Server oder Domänenserver angegeben.
 Es können dieselben Einstellungen vorgenommen werden wie bei der oben genannten Methode „Automatisch (DHCP)“.
- **Manuell**
 Wählen Sie diese Methode, wenn Sie der User Station manuell eine statische IP-Adresse zuweisen möchten. Es müssen mindestens eine IPv4-Adresse, eine Netzmaske und ein Gateway angegeben werden.
 - ➔ Klicken Sie im Abschnitt „Adresse“ auf **Hinzufügen** und geben Sie dann die IPv4-Adresse, die Netzmaske und das Gateway der User Station ein.
 - ➔ Klicken Sie auf **Löschen**, um eine manuelle IPv4-Adresse zu löschen.
 Für diese Methode können die folgenden Einstellungen konfiguriert werden:
 - DNS-Server
 - Suchdomänen
 - IPv4-Adressierung zur Fertigstellung dieser Verbindung erforderlich
 - Routen
- **Deaktiviert**
 Die IPv4-Netzwerkeinstellungen sind alle deaktiviert.

Einstellung	Beschreibung
Zusätzliche DNS-Server	Optional. Sie können die IP-Adressen eines oder mehrerer zusätzlicher DNS-Server für die Auflösung von Hostnamen angeben. Trennen Sie mehrere Server durch Kommas.
Zusätzliche Suchdomänen	Optional. Sie können IP-Adressen einer oder mehrerer zusätzlicher Domänen für die Auflösung von Hostnamen angeben. Trennen Sie mehrere Server durch Kommas.
DNS-Server	Geben Sie die IP-Adressen eines oder mehrerer DNS-Server an. Trennen Sie mehrere Server durch Kommas.
Suchdomänen	Geben Sie die IP-Adressen einer oder mehrerer Domänen für die Auflösung von Hostnamen an. Trennen Sie mehrere Server durch Kommas.
DHCP Client-Kennung	Optional. Sie können eine DHCP-Client-ID angeben, um diese User Station im Netzwerk zu identifizieren.
DHCP hostname	Optional. Sie können einen bevorzugten Hostnamen angeben, der an den DHCP-Server gesendet und für die DNS-Namensauflösung verwendet werden soll.
IPv4-Adressierung zur Fertigstellung dieser Verbindung erforderlich	Wenn diese Option deaktiviert ist, kann entweder die IPv4- oder die IPv6-Adressierung zum Aufbau der Verbindung verwendet werden. Wenn diese Option aktiviert ist, wird zum Aufbau der Verbindung ausschließlich die IPv4-Adressierung verwendet.
Routen	Optional. Konfigurieren Sie das IPv4-Routing für diese User Station. • Klicken Sie auf Hinzufügen, um eine oder mehrere Routing-Adressen hinzuzufügen, die die User Station im Netzwerk erreichen soll. • Um eine existierende Route zu löschen, wählen Sie sie aus und klicken Sie auf Löschen. • <i>Automatisch bezogene Routen ignorieren:</i> Aktivieren Sie dieses Kontrollkästchen nur, wenn Sie manuell festgelegte Routen verwenden möchte. • <i>Diese Verbindung nur für Ressourcen dieses Netzwerks verwenden.</i> Wenn diese Option ausgewählt ist, wird diese Verbindung nur zum Abrufen von Ressourcen aus dem Netzwerk verwendet. Sie wird niemals als Standard-Netzwerkverbindung verwendet. • Klicken Sie auf OK, um die Routen zu speichern und die Dialogbox zu schließen.

IPv6-Einstellungen

1. Klicken Sie auf den Reiter *IPv6-Einstellungen*.

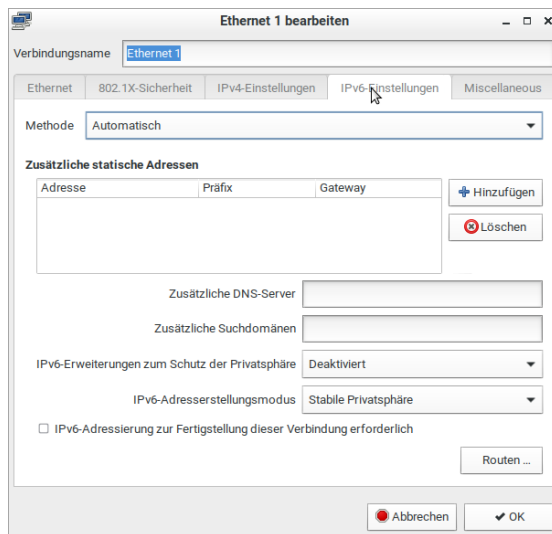


Abb. 34 Systemeinstellungen - Netzwerkverbindungen - Registerkarte **IPv6-Einstellungen**

2. Wählen Sie eine "Methode" aus den folgenden Optionen aus.

- **Automatisch**

Bei der IPv6-Autokonfiguration wird der User Station automatisch eine IPv6-Adresse zugewiesen, und die Informationen zu DNS-Servern und Domänen werden vom DHCP-Server abgerufen.

Für diese Methode können die folgenden Einstellungen konfiguriert werden (Beschreibung auf der nächsten Seite)

- Zusätzliche DNS-Server
- Zusätzliche Suchdomänen
- IPv6-Erweiterungen zum Schutz der Privatsphäre
- IPv6 Adresserstellungsmodus
- IPv6-Adressierung zur Fertigstellung dieser Verbindung erforderlich
- Routen

- **Automatisch, nur Adressen**

Bei der IPv6-Autokonfiguration wird der User Station automatisch eine IPv6-Adresse zugewiesen, es werden jedoch keine DNS-Server oder Domänenserver angegeben.

Für diese Methode können die folgenden Einstellungen vorgenommen werden (Beschreibung auf der nächsten Seite):

- DNS-Server
- Suchdomänen
- IPv6-Erweiterungen zum Schutz der Privatsphäre
- IPv6 Adresserstellungsmodus
- IPv6-Adressierung zur Fertigstellung dieser Verbindung erforderlich
- Routen

- **Automatisch, nur DHCP**

Der DHCPv6-Server im Netzwerk weist der User Station automatisch eine IPv6-Adresse zu und legt DNS-Server und Domänen fest.

Für diese Methode sind die folgenden Einstellungen konfigurierbar (Beschreibung auf der nächsten Seite):

- IPv6 Adresserstellungsmodus
- IPv6-Adressierung zur Fertigstellung dieser Verbindung erforderlich
- Routen

- **Manuell**

Wählen Sie diese Methode, wenn Sie der User Station manuell eine statische IPv6-Adresse zuweisen möchten. Es müssen mindestens eine IPv6-Adresse, ein Präfix und ein Gateway angegeben werden.

- ➡ Klicken Sie im Abschnitt „Adresse“ auf **Hinzufügen** und geben Sie dann die IPv6-Adresse, Präfix und Gateway der User Station ein.
- ➡ Klicken Sie auf **Löschen**, um eine manuelle IPv6-Adresse zu löschen.

Für diese Methode können die folgenden Einstellungen konfiguriert werden:

- DNS-Server
- Suchdomänen
- IPv6 Adresserstellungsmodus
- IPv6-Adressierung zur Fertigstellung dieser Verbindung erforderlich
- Routen

- **Deaktiviert**

Die IPv6-Netzwerkeinstellungen sind alle deaktiviert.

Setting	Description
DNS-Server	Geben Sie die IP-Adressen eines oder mehrerer DNS-Server an. Trennen Sie mehrere Server durch Kommas.
Suchdomänen	Geben Sie die IP-Adressen einer oder mehrerer Domänen für die Auflösung von Hostnamen an. Trennen Sie mehrere Server durch Kommas.
IPv6-Erweiterungen zum Schutz der Privatsphäre	Legen Sie fest, ob und wie Datenschutz-Erweiterungen auf die IPv6-Adressierung angewendet werden. • Deaktiviert: Deaktiviert Datenschutz-Erweiterungen. • Aktivieren (öffentliche Adresse bevorzugen): Aktiviert Datenschutz-Erweiterungen, eine öffentliche Adresse wird jedoch bevorzugt. • Aktivieren (temporäre Adresse bevorzugen): Aktiviert Datenschutz-Erweiterungen, wobei eine temporäre Adresse bevorzugt wird.
IPv6 Adress-erstellungsmodus	Legen Sie fest, wie die Adresse generiert werden soll. • Stabile Privatsphäre • EUI 64
IPv6-Adressierung zur Fertigstellung dieser Verbindung erforderlich	Wenn diese Option deaktiviert ist, kann entweder die IPv4- oder die IPv6-Adressierung zum Aufbau der Verbindung verwendet werden. Wenn diese Option aktiviert ist, wird zum Aufbau der Verbindung ausschließlich die IPv6-Adressierung verwendet.
Routen	Optional. Konfigurieren Sie das IPv6-Routing für diese User Station. • Klicken Sie auf Hinzufügen, um eine oder mehrere Routing-Adressen hinzuzufügen, die die User Station im Netzwerk erreichen soll. • Um eine existierende Route zu löschen, wählen Sie sie aus und klicken Sie auf Löschen. • <i>Automatisch bezogene Routen ignorieren:</i> Aktivieren Sie dieses Kontrollkästchen nur, wenn Sie manuell festgelegte Routen verwenden möchte. • <i>Diese Verbindung nur für Ressourcen dieses Netzwerks verwenden.</i> Wenn diese Option ausgewählt ist, wird diese Verbindung nur zum Abrufen von Ressourcen aus dem Netzwerk verwendet. Sie wird niemals als Standard-Netzwerkverbindung verwendet. • Klicken Sie auf OK, um die Routen zu speichern und die Dialogbox zu schließen.

802.1X-Sicherheitseinstellungen

1. Klicken Sie auf den Reiter **802.1X-Sicherheit**.

Abb. 35 Systemeinstellungen - Netzwerkverbindungen - Registerkarte **802.1X-Sicherheit**

i LAN 1 und LAN 2 Einstellungen sind getrennt.

2. Aktivieren Sie „802.1X-Sicherheit für diese Verbindung verwenden“.

3. Wählen Sie eine Legitimierungs-Methode aus der Drop-Down-Liste aus.

Die folgenden Methoden stehen zur Verfügung:

MD5

1. Benutzername und Passwort eingeben.
2. Aktivieren Sie „Passwort anzeigen“, um das unmaskierte Passwort zu sehen.

TLS

1. Identität und Domäne eingeben.
2. Unter „CA certificate“ ein CA-Zertifikat auswählen.
3. Benutzerzertifikat (User certificate) aus der Drop-Down-Liste auswählen.
4. CA- und Benutzer-Zertifikats-Passwörter festlegen, wenn erforderlich.
5. User private key aus der Drop-Down-Liste auswählen.
6. User key password eingeben.

PWD

1. Benutzername und Passwort eingeben.
2. Aktivieren Sie „Passwort anzeigen“, um das unmaskierte Passwort zu sehen.

FAST

Legitimierung	FAST
Anonyme Identität	
☒ Automatische PAC-Bereitstellung erlauben	Anonym
PAC-Datei	(keine)
Innere Legitimierung	GTC
Benutzername	
Passwort	
☐ Passwort anzeigen	

1. Anonyme Identität eingeben.
2. Wenn „Automatische PAC-Bereitstellung“ aktiviert ist, eine Bereitstellungsmethode aus der Liste auswählen.
3. PAC-Datei hochladen.
4. Eine Methode für die innere Legitimierung aus der Liste auswählen.
5. Benutzername und Passwort eingeben.

Tunneled TLS

Legitimierung	Getunneltes TLS
Anonyme Identität	
Domäne	
CA certificate	(keine)
CA certificate password	
☐ Show passwords	
☐ CA-Zertifikat ignorieren	
Innere Legitimierung	PAP
Benutzername	
Passwort	
☐ Passwort anzeigen	

1. Anonyme Identität und Domäne eingeben.
2. Unter „CA certificate“ ein CA-Zertifikat auswählen.
3. CA-Zertifikats-Passwort festlegen, wenn erforderlich.
4. Aktivieren Sie „CA-Zertifikat ignorieren“, wenn das CA-Zertifikat ignoriert werden soll.
5. Eine Option für die innere Legitimierung aus der Liste auswählen.
6. Benutzername und Passwort eingeben.

Protected EAP (PEAP)

Legitimierung	Geschütztes EAP (PEAP)
Anonyme Identität	
Domäne	
CA certificate	(keine)
CA certificate password	
☐ Show passwords	
☐ CA-Zertifikat ignorieren	
PEAP-Version	Automatisch
Innere Legitimierung	MSCHAPv2
Benutzername	
Passwort	
☐ Passwort anzeigen	

1. Anonyme Identität und Domäne eingeben.
2. Wenn die Option „Kein CA-Zertifikat erforderlich“ ausgewählt ist, wird das Feld „CA-Zertifikat“ deaktiviert, andernfalls:
3. CA-Zertifikat aus der Drop-Down-Liste auswählen.
4. CA-Zertifikats-Passwort festlegen, wenn erforderlich.
5. PEAP-Version aus der Drop-Down-Liste auswählen.
6. Eine Option für die innere Authentifizierung aus der Liste auswählen.
7. Benutzername und Passwort eingeben.

➔ Klicken Sie auf **OK**, um die Einstellungen zu speichern oder auf **Abbrechen**, um sie zu verwerfen.

Weitere Einstellungen (Miscellaneous)

1. Klicken Sie auf den Reiter *Miscellaneous*.

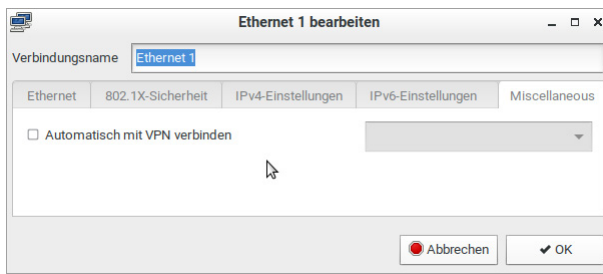


Abb. 36 Systemeinstellungen - Netzwerkverbindungen - Registerkarte **Miscellaneous**

1. Wählen Sie die Option „Automatisch mit VPN verbinden“, um sicherzustellen, dass Ihr konfiguriertes VPN automatisch verwendet wird, sobald das ausgewählte Netzwerk aktiv ist.
2. Klicken Sie auf **OK**, um die Einstellung zu speichern oder auf **Abbrechen**, um sie zu verwerfen.

5.3.6.2 Bond-Verbindungen

Das Bonding von Netzwerkkarten (NIC) ist eine weitere Möglichkeit, Ethernet-Netzwerke redundant auszugestalten. Zwei oder mehr Netzwerkkarten und ihre physischen Verbindungen zu den Switches werden logisch gebündelt und dem IP-Protokoll als eine einzige virtuelle Netzwerkkarte präsentiert. Fällt eine der physischen Verbindungen aus, wird der Datenverkehr auf eine andere Netzwerkkarte umgeleitet, ohne dass das IP-Schicht oder die darüber liegenden Schichten von dieser Umleitung Kenntnis haben.

Dieser Ansatz schützt vor einfachen Ethernet-Fehlern, wie beispielsweise einer defekten Netzwerkkarte oder einem defekten Kabel, zwischen dem Host und seinem lokalen IP-Switch.

Sie können Netzwerk-Bonding-Geräte so konfigurieren, dass sie die Standard-Ethernet-Konfiguration ersetzen. Diese Konfiguration verdoppelt die maximale Netzwerkgeschwindigkeit, wenn beide Anschlüsse genutzt werden, und bietet Redundanz. Das Netzwerk der Draco SIRA User Station funktioniert auch dann weiter, wenn einer der Anschlüsse ausfällt.

1. Klicken Sie auf **Hauptmenü > Systemeinstellungen > Netzwerkverbindungen**. Der Netzwerkverbindungen-Dialog wird angezeigt.

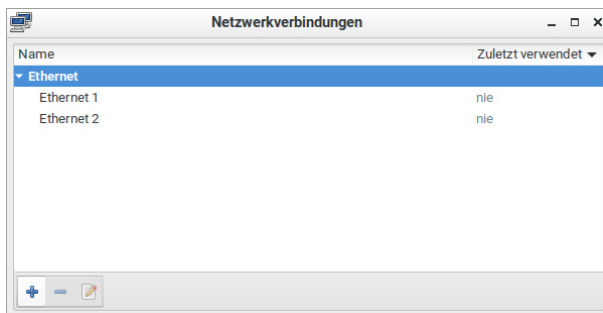


Abb. 37 Systemeinstellungen - **Netzwerkverbindungen**

2. Klicken Sie auf das Hinzufügen Symbol (Pluszeichen).
3. Unter „Verbindungstyp wählen“ wählen Sie „Gebündelt“ aus und klicken Sie dann auf **Erstellen**. Der “Bond-Verbindung 1 bearbeiten” Dialog wird geöffnet.

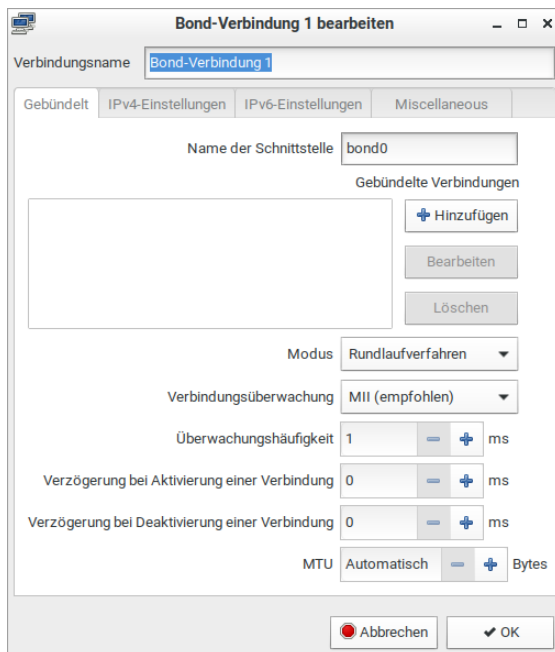


Abb. 38 Systemeinstellungen - Netzwerkverbindungen - **Bond-Verbindung bearbeiten 1**

4. In der Registerkarte *Gebündelt* können Sie einen Namen für die Schnittstelle eingeben und die anderen Parameter einstellen.
5. Klicken Sie dann **Hinzufügen**. Eine Dialogbox erscheint.
6. Wählen Sie als Verbindungstyp „Bond“ aus und klicken Sie auf **Erstellen**, um den ersten Bond-Verbindungslink für die erste Netzwerkkarte zu erstellen.

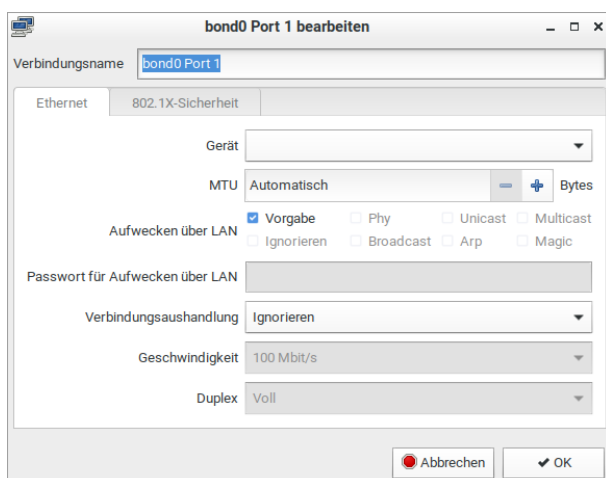


Abb. 39 Systemeinstellungen - Netzwerkverbindungen - **Bond-Verbindung bearbeiten 2**

7. Wählen Sie im Feld „Gerät“ die MAC-Adresse der Schnittstelle aus.
8. Stellen Sie die anderen Parameter wunschgemäß ein und klicken Sie auf **OK**.
9. Klicken Sie wieder auf **Hinzufügen**, um den zweiten Bond-Link hinzuzufügen, der automatisch denselben Verbindungstyp hat.
10. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
11. Kehren Sie zum Dialog **Hauptmenü > Systemeinstellungen > Netzwerk** zurück.

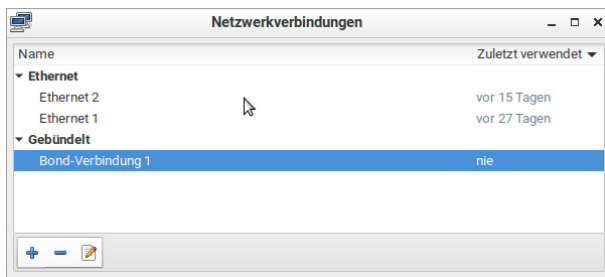


Abb. 40 Systemeinstellungen - Netzwerkverbindungen - **Netzwerkverbindungen mit gebündelter Verbindung**

12. Löschen Sie die alten Ethernet-Einträge und behalten Sie den neu erstellten Bond-Eintrag.

5.3.6.3 OpenVPN-Verbindungen

Eine OpenVPN-Konfiguration kann auf die User Station hochgeladen werden, um für alle Verbindungen einen VPN-Client zu verwenden. Sie müssen eine gültige Konfigurationsdatei mit den Zertifikatsdaten des Servers im Dateiformat .OVPN bereitstellen. Einzelheiten zur Erstellung der Datei finden Sie in der OpenVPN-Dokumentation. Sobald die Datei hochgeladen ist und Ihre Konfiguration die Option „Automatisch verbinden“ enthält, wird die VPN-Verbindung hergestellt, wenn die Draco SIRA User Station neu gestartet wird.

Damit CC-SG-Benutzer eine Verbindung über das VPN herstellen können, muss die Netzwerkeinrichtung zuvor von einem lokalen Benutzer vorgenommen werden.

OpenVPN-Verbindung hinzufügen

1. Klicken Sie **Hauptmenü > Systemeinstellungen > Netzwerkverbindungen**. Der „Netzwerkverbindungen“ Dialog erscheint.
2. Klicken Sie auf das Symbol Hinzufügen (Pluszeichen). Eine Dialogbox wird geöffnet.
3. Im „Verbindungstyp wählen“ Dialog wählen Sie „Gespeicherte VPN-Konfiguration importieren“ aus und klicken Sie dann auf **Erstellen**. Ein Dialog zum Hochladen erscheint.

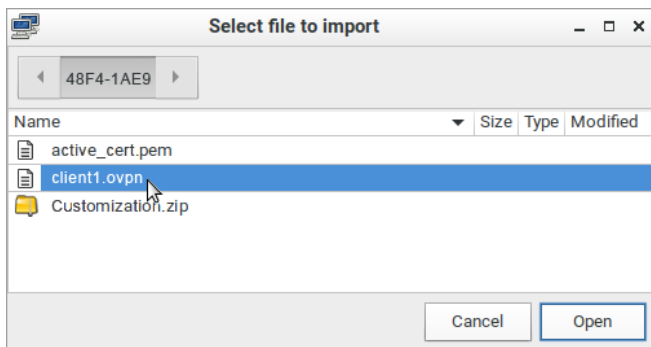


Abb. 41 Systemeinstellungen - Netzwerkverbindungen - **Dialog zum Hochladen einer VPN-Konfiguration**

4. Wählen Sie die *.ovpn Konfigurationsdatei aus und klicken Sie auf **Öffnen/Open**.
Der VPN-Client wird zur Liste der Netzwerkverbindungen hinzugefügt.

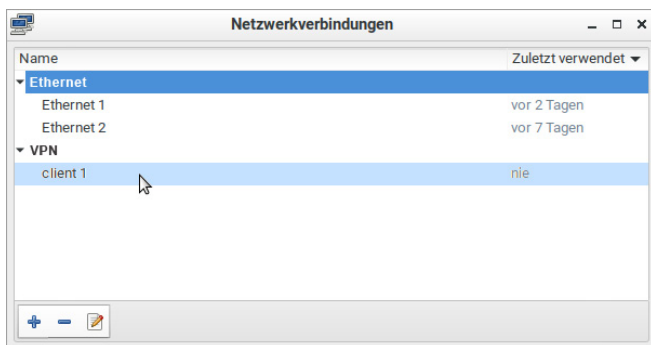


Abb. 42 Systemeinstellungen - Netzwerkverbindungen - **Liste der Netzwerkverbindungen**

5. Klicken Sie auf die VPN-Verbindung, um sie auszuwählen und dann auf das Symbol Hinzufügen (Pluszeichen).

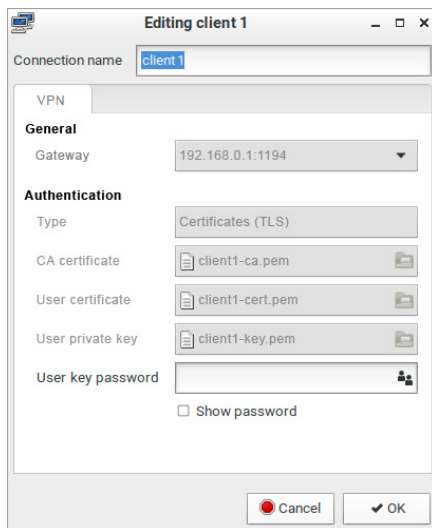


Abb. 43 Systemeinstellungen - Netzwerkverbindungen - Konfigurieren der VPN-Verbindung

6. Sie können den Namen der VPN-Verbindung ändern und/oder ein Passwort eingeben.
7. Klicken Sie auf **OK**.

Wenn die VPN-Verbindung hergestellt ist, zeigt das Netzwerksymbol in der Symbolleiste an, dass sie aktiv ist. Das „Schloss“-Symbol wird angezeigt, wenn sich ein Benutzer bei aktiver VPN-Verbindung anmeldet.

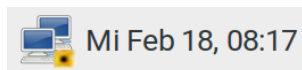


Abb. 44 Symbolleiste mit VPN-Schloss-Symbol

8. Um automatisch eine Verbindung zum VPN herzustellen, wählen Sie die VPN-Verbindung in der Liste der Netzwerkverbindungen aus, klicken Sie auf das Symbol „Bearbeiten“, wechseln Sie zur Registerkarte „Miscellaneous“ und aktivieren Sie die Option „Automatisch mit VPN verbinden“ (siehe Seite 43).

5.4 KVM-Clients nutzen

Nach dem Zugriff auf einen Port öffnet sich das KVM-Client-Fenster. Das Videosignal des an den Port angeschlossenen Target-Computers wird im KVM-Client-Fenster angezeigt. Sie können die angeschlossene Tastatur und Maus verwenden, um den Target-Computer zu steuern.



Abb. 45 KVM-Client-Fenster

Die Symbolleiste ist in zwei Hälften unterteilt. Die linke Hälfte enthält die folgenden Symbole, mit denen Sie Einstellungen und Eigenschaften ändern können.

Symbol	Beschreibung
	Verbindungseigenschaften: Steuert die Leistung des Videostreams über Ihre Verbindung zum Zielsystem. Zeigt Informationen wie Bildwiederholrate (FPS) und Videoauflösung an. Die werkseitigen Standardeinstellungen sind für die meisten Verbindungen ideal, daher wird davon abgeraten, die Einstellungen zu ändern, sofern dies nicht erforderlich ist.
	Tastatur: Zeigt eine Liste der verfügbaren Hotkey-Makros an und sendet das ausgewählte Makro an den Target-Computer.
	Maus: Wechselt zwischen dem Single-Mausmodus und verschiedenen Doppel-Mausmodi oder synchronisiert zwei Mauszeiger auf dem Bildschirm.
	Videoeinstellungen: Passt die Einstellungen für die Videoerkennung und die Farbkalibrierung an.
	Audio-, Massenspeicher- und Smartcard-Geräte: Verbindet ein virtuelles Medienlaufwerk oder einen Smartcard-Leser mit dem Target-Computer oder trennt die Verbindung, sofern der Target-Computer virtuelle Medien unterstützt. Sie können beispielsweise einen USB-Stick am Target-Computer anschließen. Darüber hinaus können Sie die Audioverbindung zum Target-Computer konfigurieren.
	Stromversorgung: Schaltet den Target-Computer ein, aus oder führt einen Neustart durch, sofern eine PDU angeschlossen ist.
	Einstellungen für externe Geräte. Rufen Sie die Einstellungen für den Betrieb eines externen Geräts auf.
	Ansicht: Zeigt verschiedene Anzeigeooptionen an, wie z. B. „Video skalieren“ und „Vollbildmodus“.

Die rechte Hälfte enthält die folgenden Shortcuts für häufig verwendete Funktionen. Diese Funktionen sind auch in der linken Gruppe verfügbar, doch die Shortcuts ermöglichen einen schnellen Zugriff per Mausklick.

Symbol	Beschreibung
	Maus synchronisieren: Erzwingt im Dual-Maus-Modus, dass der Mauszeiger des Target-Computers mit dem der User Station übereinstimmt.
	Video automatisch anpassen: Erzwingt eine erneute Erkennung des Videosignals, um die Videoanzeige anzupassen.
	Sende Strg+Alt+Del: Sendet die Tastenkombination Strg+Alt+Entf an den Target-Computer, um sicherzustellen, dass sie dort ausgeführt wird.
	Vollbildmodus: Zeigt das Video des Target-Computers im Vollbildmodus an. ➔ Drücken Sie Strg+Alt+F , um den Vollbildmodus zu beenden.
	Fenster an Target anpassen: Das KVM-Client-Fenster wurde an die Bildschirmgröße des Target-Computers angepasst.
	Audio stumm schalten: Audio an/ausschalten.
	Mikrofon ausschalten: Mikrofon an/ausschalten.
	Num Caps Scroll: Zeigt den Status von Num Lock, Caps Lock und Scroll an. Aktive Funktionen sind fett gedruckt.

5.4.1 Automatisches Verbinden

Sollte die Verbindung zu den KVM-Targets unterbrochen werden, wird in den meisten Fällen nach einer Wartezeit von 30 Sekunden ein automatischer Wiederverbindungsversuch unternommen. Diese Wartezeit verlängert sich von 30 Sekunden auf 1 Minute, 2, 5, 10 und 15 Minuten, falls die Verbindung nicht erfolgreich ist.

Bei einer Unterbrechung der Verbindung erscheint eine Meldung mit Informationen zum Zeitplan für die erneute Verbindung sowie Optionen zum Abbrechen oder Beenden.

Eine automatische Wiederherstellung der Verbindung wird nicht versucht, wenn der Verbindungsfehler auf folgende Ursachen zurückzuführen ist:

- Konfigurationsfehler festgestellt. Das Zertifikat muss hochgeladen werden.
- Benutzer-Authentifizierung fehlgeschlagen.
- Benutzer-Autorisierung fehlgeschlagen.
- Der Benutzer wurde von einem Administrator aktiv abgemeldet.
- Die Version des KVM-Geräts wird vom Client nicht unterstützt.

 Im FIPS-Modus kann die User Station keine Verbindung zu einem KVM-Target herstellen, wenn die Sicherheitseinstellungen des Geräts auf „Nur TLS 1.3“ festgelegt sind. Auch die Verbindung zu RDP-Adress-Clients schlägt fehl.

5.5 Serielle Clients nutzen

Nach dem Zugriff auf einen Port öffnet sich das Fenster „Serial Client“. Die Ausgabe der seriellen Konsole des Target-Computers, der an den Port angeschlossen ist, wird in der HTML-Seriellen Konsole (HSC) angezeigt. Sie können die angeschlossene Tastatur und Maus verwenden, um mit dem Target-Computer zu kommunizieren.

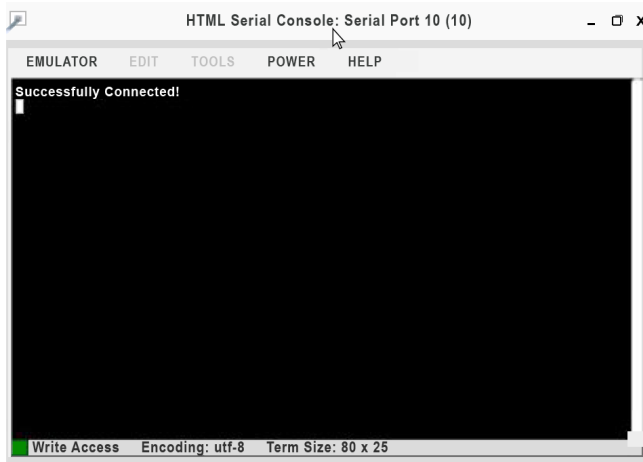


Abb. 46 Fenster des seriellen Clients

Über das Menü der Symbolleiste können Sie auf Untermenüoptionen zugreifen, um bestimmte Aufgaben auf dem Target-Computer auszuführen.

Option	Beschreibung
Emulator	Der Emulator bietet Zugriff auf die Optionen „Einstellungen“, „Verlauf abrufen“, „Verlauf löschen“, „Schreibzugriff anfordern“, „Schreibsperre anfordern“, „Schreibsperre aufheben“, „Unterbrechung senden“, „Port zurücksetzen“, „Verbundene Benutzer“ und „Beenden“.
Edit	Das Edit Menü ist deaktiviert.
Tools	Das Tools Menü ist deaktiviert.
Power	Über „Power“ können Sie auf die Optionen „Power Status“, „Power On“, „Power Off“ und „Power Cycle“ zugreifen.
Help	Über die Hilfe gelangen Sie zur Option „Info“.

5.5.1 Emulator-Menü

➔ Klicken Sie auf **Emulator** in der Symbolleiste. Eine Drop-Down-Liste mit Optionen erscheint.

Einstellungen

1. Klicken Sie in der Emulator Drop-Down-Liste auf „Settings“. Der Dialog „Terminal Properties“ erscheint mit den Standardeinstellungen.



Abb. 47 Settings - Terminal Properties

2. Stellen Sie die Terminalgröße ein, indem Sie die Anzahl der Spalten und Zeilen auswählen. Standardeinstellung ist 80 x 25.
3. Vorder- und Hintergrundfarbe festlegen. Standardeinstellung ist weiß auf schwarz.
4. Stellen Sie die Schriftgröße ein. Standardeinstellung ist 11.
5. Stellen Sie die Scrollback-Zahl ein, die die Anzahl der Zeilen angibt, die zum Scrollen zur Verfügung stehen.
6. Wählen Sie im Drop-Down-Menü „Encoding“ eine der folgenden Optionen aus:
 - UTF-8
 - 8-bis ASCII
 - ISO-8859-1
 - ISO-8859-15
 - Shift-JIS
 - EUC-JP
 - EUC-KR
7. Wählen Sie im Drop-Down-Menü „Language“ eine Sprache aus den folgenden aus:
 - English
 - Bulgarian
 - Japanese
 - Korean
 - Chinese
8. Die Standardeinstellung bei “Backspace Sends” ist ASCII Del, Sie können Control-H über das Drop-Down-Menü auswählen.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern. Wenn Sie die Sprache ändern, wechselt das HSC zu der neuen Sprache, sobald der Dialog „Settings“ geschlossen wird.

Get History

Protokollinformationen können bei der Fehlersuche, der Fehlerbehebung oder der Verwaltung eines Target Geräts hilfreich sein. Die Funktion „Protokoll abrufen“:

- Ermöglicht es Ihnen, den aktuellen Verlauf der Konsolensitzungen einzusehen, indem die Konsolenmeldungen an das Target und vom Target angezeigt werden.
- Zeigt den letzten Konsolen-Meldungsverlauf mit einer Größe von bis zu 512 kB an. So kann der Benutzer die Ereignisse des Target Geräts im Zeitverlauf einsehen.

Wenn die Größenbeschränkung erreicht ist, wird der Text umgebrochen, wobei die ältesten Daten durch die neuesten überschrieben werden.

 Die Verlaufsdaten werden nur dem Benutzer angezeigt, der den Verlauf angefordert hat.

- ➔ Um den Sitzungsverlauf anzuzeigen, klicken Sie **Emulator > Get History**.
- ➔ Um den Sitzungsverlauf zu löschen, klicken Sie **Emulator > Clear History**.

Get Write Access

Nur Benutzer mit einer Berechtigung für den Port erhalten Schreibzugriff. Der Benutzer mit Schreibzugriff kann Befehle an das Target Gerät senden. Der Schreibzugriff kann über den Befehl „Get Write Access“ zwischen Benutzern übertragen werden, die im HSC arbeiten.

1. Um den Schreibzugriff zu aktivieren, klicken Sie **Emulator > Get Write Access**. Sie haben nun Schreibzugriff auf dem Target Gerät.
2. Wenn ein anderer Benutzer Schreibzugriff von Ihnen übernimmt:

- Der HSC zeigt in der Statusleiste vor „Schreibzugriff“ ein rotes Block-Symbol an.
- Dem Benutzer, der derzeit über Schreibzugriff verfügt, wird eine Meldung angezeigt, die ihn darauf hinweist, dass ein anderer Benutzer den Zugriff auf die Konsole übernommen hat.

Get Write Lock

Write Lock hindert andere Benutzer daran, den Schreibzugriff zu übernehmen, wenn Sie ihn verwenden.

- ➔ Um Write Lock zu aktivieren, klicken Sie auf **Emulator > Get Write Lock**. Wenn Write Lock nicht verfügbar ist, erscheint die Meldung „request rejected“.
- ➔ Um Write Lock zu deaktivieren, klicken Sie auf **Emulator > Write Unlock**.

Send Break

Bei einigen Zielsystemen, wie beispielsweise Sun-Solaris-Servern, muss ein Nullzeichen (Break) übertragen werden, um die OK-Eingabeaufforderung zu erzeugen. Dies entspricht der Eingabe von „STOP-A“ über die Sun-Tastatur.

Nur Benutzer mit Schreibzugriff können ein Break senden.

Senden eines absichtlichen Breaks an einen Sun-Solaris-Server:

1. Vergewissern Sie sich, dass Sie Schreibzugriff haben (Write Access)
2. Klicken Sie auf **Emulator > Send Break**. Eine „Send break Ack“ (acknowledgement) Nachricht erscheint.
3. Klicken Sie auf **OK**.

Reset Port

Reset Port setzt den physischen seriellen Port zurück und re-initialisiert die konfigurierten Werte bezüglich bps/bis, etc.

Connected Users

Das Kommando Connected Users erzeugt eine Liste aller Benutzer, die momentan mit demselben Port verbunden sind.

- ➔ Klicken Sie auf **Emulator > Connected Users**.

Ein Sternchen in der Spalte Write kennzeichnet den Benutzer, der Schreibzugriff an der Konsole hat.

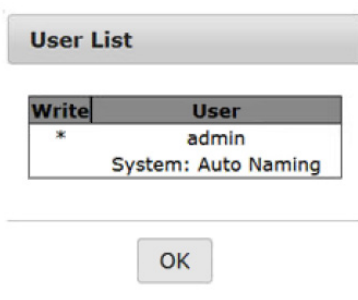


Abb. 48 Settings - Benutzerliste

Exit

- ➔ Klicken Sie auf **Emulator > Exit**, um das HSC zu schließen.

5.5.2 Power-Menü

 Sie müssen über die Berechtigung zum Verwalten der Stromversorgung des Targets verfügen, und für das Target müssen Stromversorgungszuordnungen konfiguriert sein. Wenn Sie nur über die Berechtigung „Zugriff“ und nicht über die Berechtigung „Stromversorgungssteuerung“ verfügen, werden Stromversorgungsaktionen abgelehnt.

Power-Status anzeigen

1. Klicken Sie auf **Power > Power Status**, um den Status der Anschlussstelle anzuzeigen, an die das Ziel angeschlossen ist.

Im Benachrichtigungsdialog wird der Status der Anschlussstelle als „On“ oder „Off“ angezeigt. Der Status kann auch anzeigen, dass keine Anschlussstelle zugeordnet ist oder keine Stromfreigabe für den Port vorliegt.



Abb. 49 **Power-Benachrichtigungen**

Durchführung von Stromversorgungsvorgängen

1. Klicken Sie auf **Power**. Ein Drop-Down-Menü erscheint.
2. Klicken Sie auf eine der Optionen Power On, Power Off oder Power Cycle. Eine Meldung erscheint.

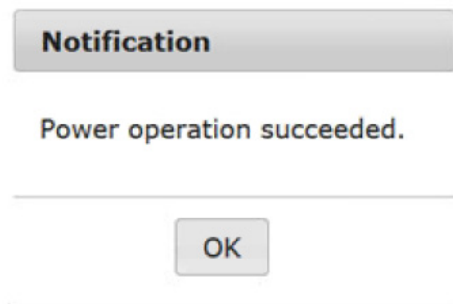


Abb. 50 **Nachricht nach erfolgreichem Stromversorgungsvorgang**

3. Klicken Sie auf **OK**.

6 Konfiguration

6.1 Geräte hinzufügen (Draco SIRA CON-Units)

Es sind Administratorrechte nötig, um Geräte anlegen, editieren und löschen zu können.

i Wenn die User Station mit einem Netzwerk verbunden ist, das kein DHCP unterstützt, müssen Sie die Netzwerkeinstellungen manuell konfigurieren, bevor Sie SIRA CON-Units hinzufügen (siehe Abschnitt 5.3.6, Seite 35).

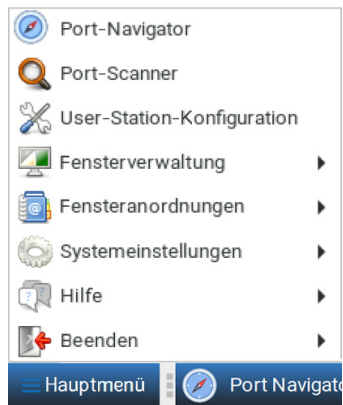


Abb. 51 **Hauptmenü**

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration** oder drücken Sie die Tastenkombination **Strg+Alt+C**.

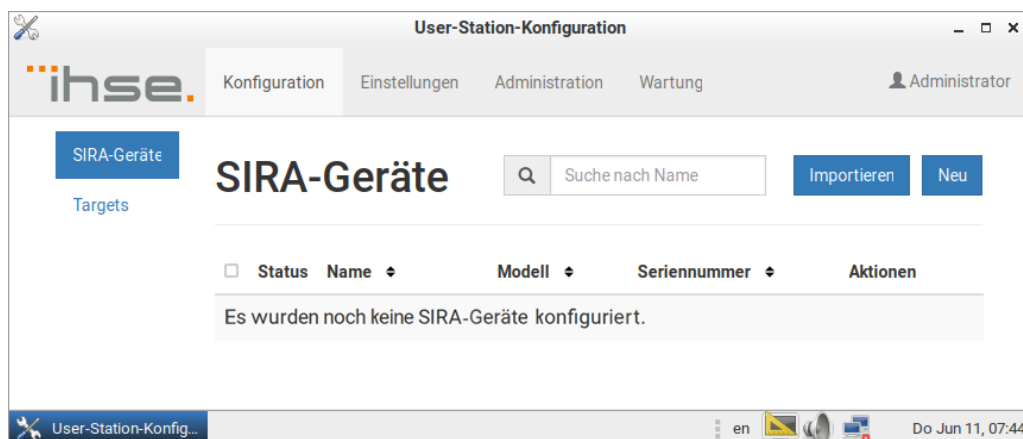


Abb. 52 **User-Station-Konfiguration**

2. Klicken Sie auf den Button **Neu**, um ein neues Gerät hinzuzufügen.

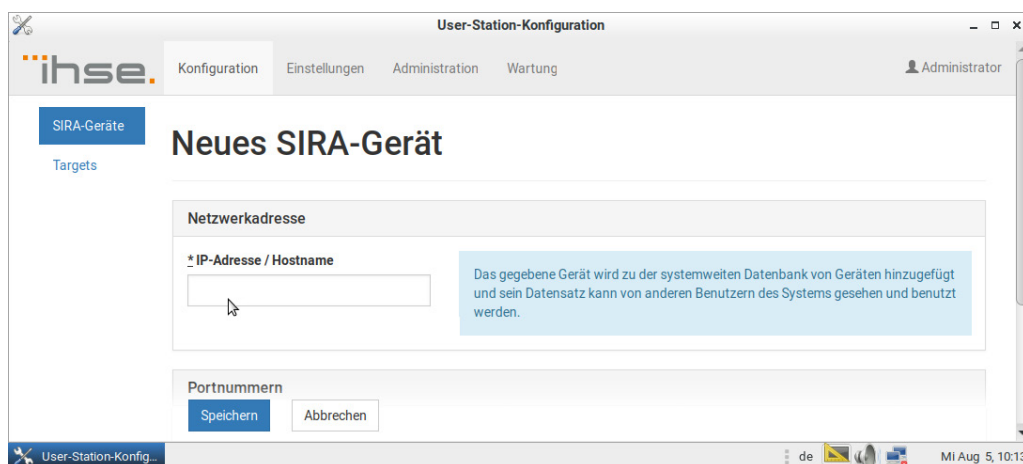


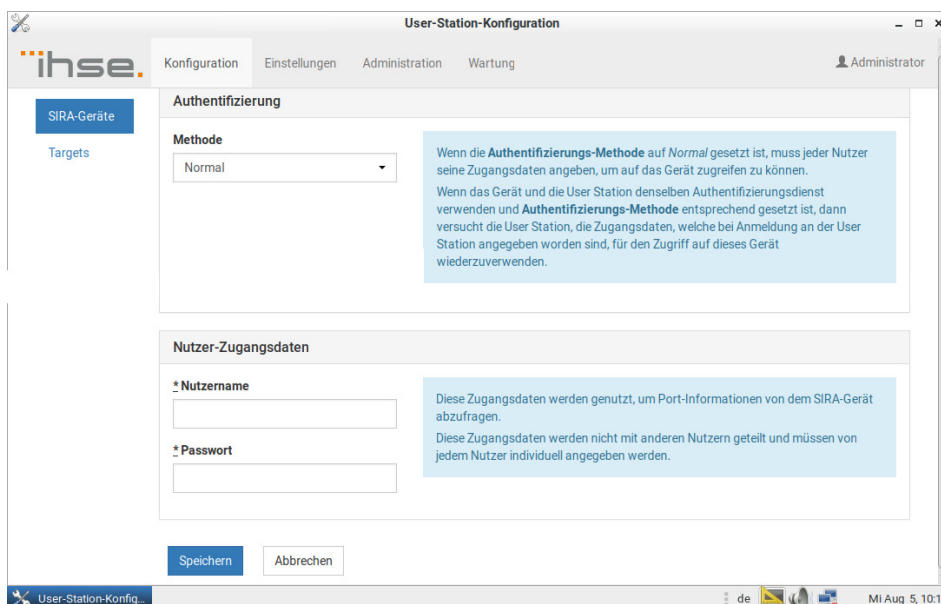
Abb. 53 **Konfiguration - Neues SIRA-Gerät anlegen**

3. Geben Sie die IPv4/IPv6-Adresse oder den Hostname der SIRA CON-Unit in das Feld „IP-Adresse/Hostname“ ein.
4. Scrollen Sie nach unten und stellen Sie weitere Parameter ein, wenn Sie möchten.
5. Die Standard-Ports sind eingetragen, können aber geändert werden.
6. Wählen Sie die Authentifizierungs-Methode. Zwei Methoden stehen zur Auswahl.

Methode	Beschreibung
Normal	Es müssen für die KVM-Netzwerk-Matrix Logindaten eingegeben werden.
LDAP-Single-Sign-On zulassen	Wenn Benutzer, KVM-Netzwerk-Matrizen und die User Station sich in derselben LDAP-Umgebung befinden, ist Single-Sign-On möglich.

 Wenn die Option „LDAP-Single-Sign-On zulassen“ aktiviert ist, können LDAP-Benutzer auf die Eingabe von Logindaten verzichten, da stattdessen ihre LDAP-Logindaten verwendet werden. Andernfalls werden die Logindaten für einen Extender benutzerspezifisch gespeichert. Andere Benutzer müssen ihre eigenen Logindaten für die von Ihnen hinzugefügten Extender eingeben und speichern.

7. Wenn Sie die Authentifizierungs-Methode „Normal“ verwenden, geben Sie Logindaten für die SIRA CON-Unit ein.



User-Station-Konfiguration

Konfiguration | Einstellungen | Administration | Wartung | Administrator

Authentifizierung

Methode: Normal

Wenn die **Authentifizierungs-Methode** auf *Normal* gesetzt ist, muss jeder Nutzer seine Zugangsdaten angeben, um auf das Gerät zugreifen zu können.

Wenn das Gerät und die User Station denselben Authentifizierungsdienst verwenden und **Authentifizierungs-Methode** entsprechend gesetzt ist, dann versucht die User Station, die Zugangsdaten, welche bei Anmeldung an der User Station angegeben worden sind, für den Zugriff auf dieses Gerät wiederzuverwenden.

Nutzer-Zugangsdaten

* Nutzername

* Passwort

Diese Zugangsdaten werden genutzt, um Port-Informationen von dem SIRA-Gerät abzufragen.

Diese Zugangsdaten werden nicht mit anderen Nutzern geteilt und müssen von jedem Nutzer individuell angegeben werden.

Speichern | Abbrechen

Abb. 54 Konfiguration - Neues SIRA-Gerät anlegen - **Nutzer-Zugangsdaten**

8. Klicken Sie auf den Button **Speichern**.
9. Wiederholen Sie die Schritte 2 bis 8, um weitere SIRA CON-Units anzulegen.

6.1.1 Geräte editieren

Angelegte SIRA CON Geräte werden im User-Station-Konfigurationsfenster aufgelistet.

Jedes Gerät hat vier Symbole in der Spalte Aktionen.

Wenn Sie nicht die Person sind, die neue Geräte zur User Station hinzugefügt hat, müssen Sie die Schritte weiter unten befolgen, um die Zugangsdaten für die neu hinzugefügten Geräte einzugeben.

 Informationen zum Unterschied zwischen den Anmeldedaten eines KVM-/seriellen Geräts und denen der User Station finden Sie im Abschnitt 9.2.3, Seite 113.

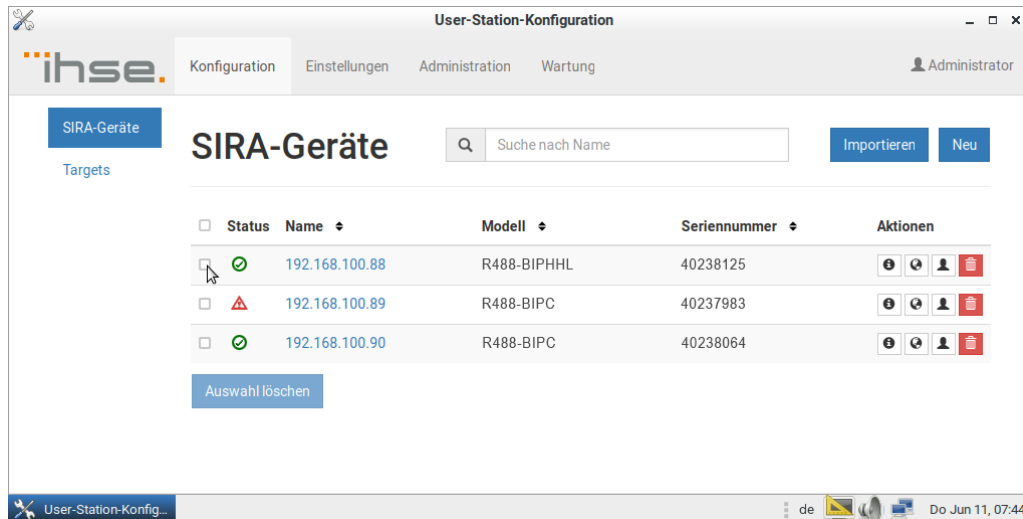


Abb. 55 Konfiguration - **SIRA-Geräte-Liste**

Symbol	Beschreibung
	Editierbutton, um IP-Adresse/Hostname oder Authentifizierungs-Methode zu ändern.
	Öffnet die Administrationsseite (Anmeldung nötig).
	Ermöglicht die Änderung der Anmeldedaten für dieses Gerät.
	Löschbutton, um dieses Gerät zu löschen.

Geräte-Ports anzeigen

- ➔ Klicken Sie auf das gewünschte SIRA-Gerät. Die Ports-Liste wird geöffnet (siehe Abschnitt 6.2, Seite 59).
Die Symbole in der Spalte „Status“ bedeuten folgendes:

Symbol	Beschreibung
	Portinformationen dieses Gerätes können angezeigt werden.
	Portinformationen dieses Gerätes können NICHT angezeigt werden. Mögliche Gründe hierfür: - Falsche Nutzer-Zugangsdaten wurden für dieses Gerät eingegeben. - Das Zertifikat dieses Gerätes kann nicht verifiziert werden (wenn Zertifikatsprüfung aktiviert ist). - Probleme mit der Netzwerkverbindung, z.B. das gewählte Gerät ist nicht mit dem Netzwerk verbunden.
	Portinformationen dieses Gerätes sind nicht verfügbar, da noch keine Nutzer-Zugangsdaten eingegeben wurden.

Ändern der IP-Adresse/Hostname oder der Authentifizierungsmethode

1. Klicken Sie auf den Editierbutton . Eine Seite mit allen Informationen des Gerätes erscheint.
2. Klicken Sie auf **Bearbeiten**.
3. Sie können jetzt die IP-Adresse oder den Hostnamen, Discovery- und HTTPS-Port oder die Authentifizierungsmethode ändern (siehe Abschnitt 6.1, Seite 53).
4. Klicken Sie auf **Speichern**.

Öffnen der Administrationsseite des Gerätes

1. Klicken Sie auf den Administratorbutton . Die Administrationsseite wird geöffnet.
2. Geben Sie die Admin-Benutzerdaten ein, um Zugang zu erhalten.

Eingeben von neuen Zugangsdaten für ein Gerät

1. Klicken Sie auf den Benutzerbutton  des gewünschten Gerätes.
2. Geben Sie neue Zugangsdaten ein.
3. Klicken Sie auf **Speichern**.

 Wenn Sie falsche Zugangsdaten für ein Gerät eingeben, werden Sie möglicherweise gesperrt, sofern auf diesem Gerät die Benutzersperre aktiviert ist und zu viele falsche Anmeldeversuche unternommen wurden. Wenden Sie sich in diesem Fall an den Systemadministrator.

6.1.2 Geräte löschen

Sie können ein einzelnes Gerät über das Papierkorbsymbol am Zeilenende löschen oder mehrere Geräte gleichzeitig.

1. Um ein einzelnes Gerät zu löschen, klicken Sie auf das Mülleimersymbol  in der Zeile des Gerätes.
2. Eine Bestätigungsmeldung erscheint. Klicken Sie auf **OK**, um das Gerät zu löschen.

Mehrere Geräte löschen

1. Um alle Geräte zu löschen, setzen Sie ein Häkchen in das Kästchen links neben „Status“ in der Kopfzeile der Tabelle. Alle Kästchen in der Liste werden aktiviert.
2. Wenn Sie nur einige Geräte löschen möchten, aktivieren Sie manuell das Kästchen jedes Gerätes, das Sie löschen möchten.
3. Nachdem Sie alle oder einige Geräte ausgewählt haben, klicken Sie auf den Button **Auswahl löschen**.

6.1.3 Geräte importieren

Mit den Funktionen „Massenimport“ und „Aktualisierung“ können Sie mehrere SIRA-Geräte gleichzeitig hinzufügen oder aktualisieren, indem Sie eine CSV-Datei erstellen, die sich im Stammverzeichnis eines angeschlossenen USB-Speichergeräts befindet.

Beim Import fügt die Draco SIRA User Station Geräte hinzu, die anhand ihrer IP-Adresse bzw. ihres Hostnamens als neu erkannt werden. Erkennt die User Station, dass ein in der CSV-Datei identifiziertes Gerät bereits im System vorhanden ist, werden die Daten beim Import entsprechend den Angaben in der CSV-Datei aktualisiert. Optional können Sie für jedes Gerät einen benutzerdefinierten Discovery-Port und einen HTTPS-Port festlegen, sowie die Benutzer-Anmeldedaten.

Format der CSV-Datei

Die CSV-Datei hat 5 Spalten, die durch Kommata getrennt werden:

- IP-Adresse oder Hostname
- Benutzername (optional)
- Passwort (optional)
- Discovery-Port (optional)
- HTTPS-Port (optional)

 Benutzername und Passwort sind optional. Werden sie nicht importiert, muss der Administrator diese später eingeben. Auch die Ports sind optional in der CSV-Datei. Werden Sie nicht spezifiziert, werden die Standard-Ports (5000 und 443) verwendet.

Beispiel einer Massenimport-CSV-Datei

```
IP address,username,password,discovery port,HTTPS port
192.168.100.100
192.168.100.120,reception,A1B2c3d4
192.168.100.130,office1,IdPWF-dn173,5000,443
```

SIRA-Geräte importieren oder aktualisieren

1. Klicken Sie auf **Importieren** im User-Station-Konfigurationsfenster.
Der Massenimport-Dialog enthält eine Liste aller CSV-Dateien, die sich im Stammverzeichnis eines angeschlossenen USB-Sticks oder einem Netzwerkspeicher befinden.

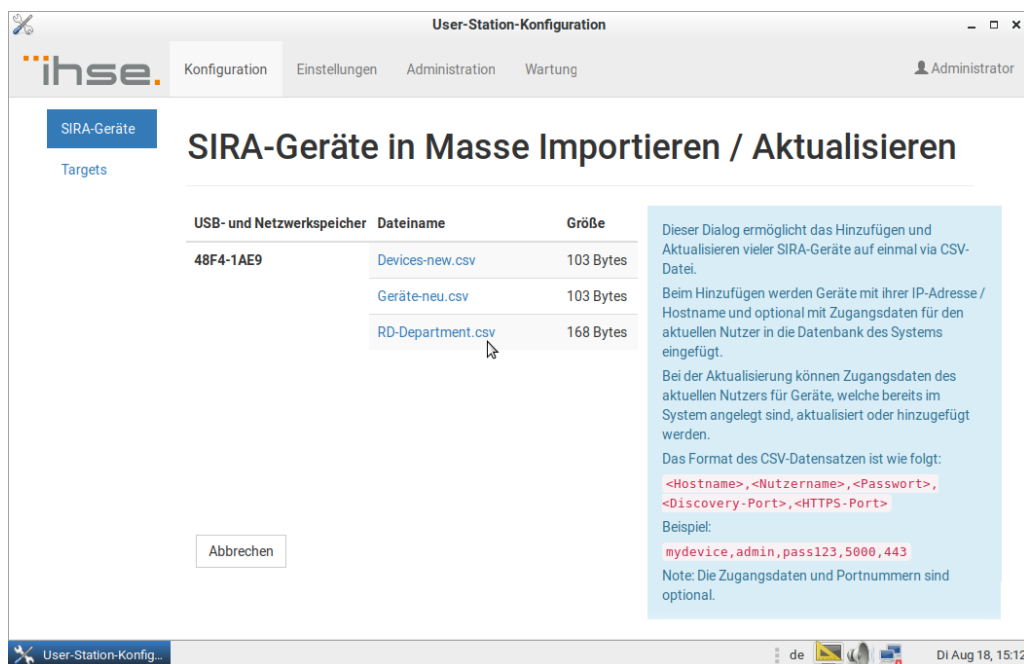


Abb. 56 Konfiguration - SIRA-Geräte - Massenimport-Dialog - Liste der gefundenen CSV-Dateien

2. Klicken Sie auf die CSV-Datei, die Sie importieren möchten.
Informationen zur Datei werden angezeigt.

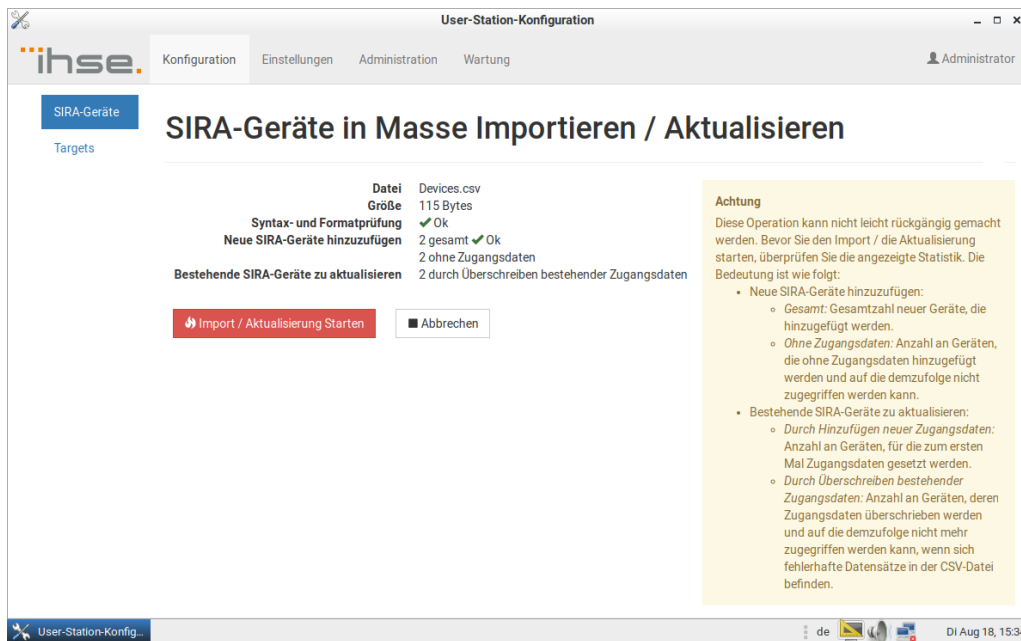


Abb. 57 Konfiguration - SIRA-Geräte - Massenimport-Dialog - Inhalt der ausgewählten CSV-Datei

Kategorie	Beschreibung
Datei	Name der CSV-Datei
Größe	Größe der CSV-Datei
Syntax- und Formatprüfung	Hier werden Fehler aufgelistet, wenn welche enthalten sind mit Zeile, Syntax- oder Formatfehler. Hinweis: Werden Fehler aufgelistet, erscheint eine Warnmeldung und der Importierbutton wird deaktiviert. Korrigieren Sie die Datei und versuchen Sie es erneut.
Neue SIRA-Geräte hinzufügen	Gesamte Anzahl der: • SIRA-Geräte, die hinzugefügt werden sollen. • SIRA-Geräte, die ohne Anmeldedaten hinzugefügt werden sollen.
Bestehende SIRA-Geräte zu aktualisieren	Gesamte Anzahl der: • SIRA-Geräte, die mit neuen Anmeldedaten versehen werden sollen. • SIRA-Geräte, die durch Überschreiben der bestehenden Anmeldedaten aktualisiert werden sollen.

3. Klicken Sie auf den Button **Import / Aktualisierung Starten**.
 Der Import startet und der Fortschritt wird im Dialog angezeigt. Ist der Import beendet, erscheint eine Erfolgsmeldung.

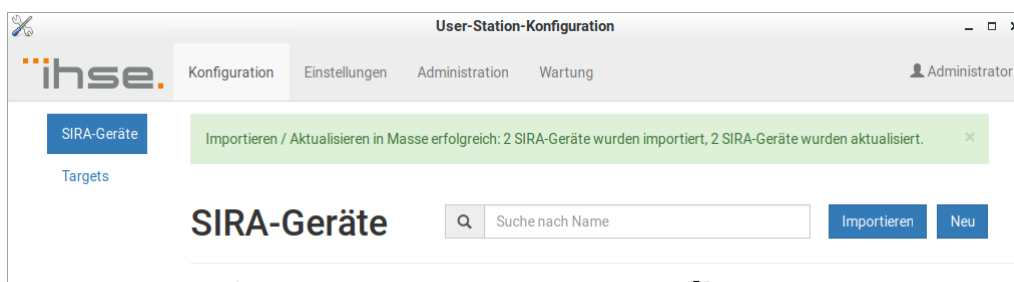


Abb. 58 Konfiguration - SIRA-Geräte - Meldung nach erfolgreichem Import / Aktualisierung

6.2 KVM-Ports konfigurieren

1. Klicken Sie in der Liste auf ein Gerät, um alle Anschlüsse dieses Geräts anzuzeigen, sofern diese zugänglich sind.

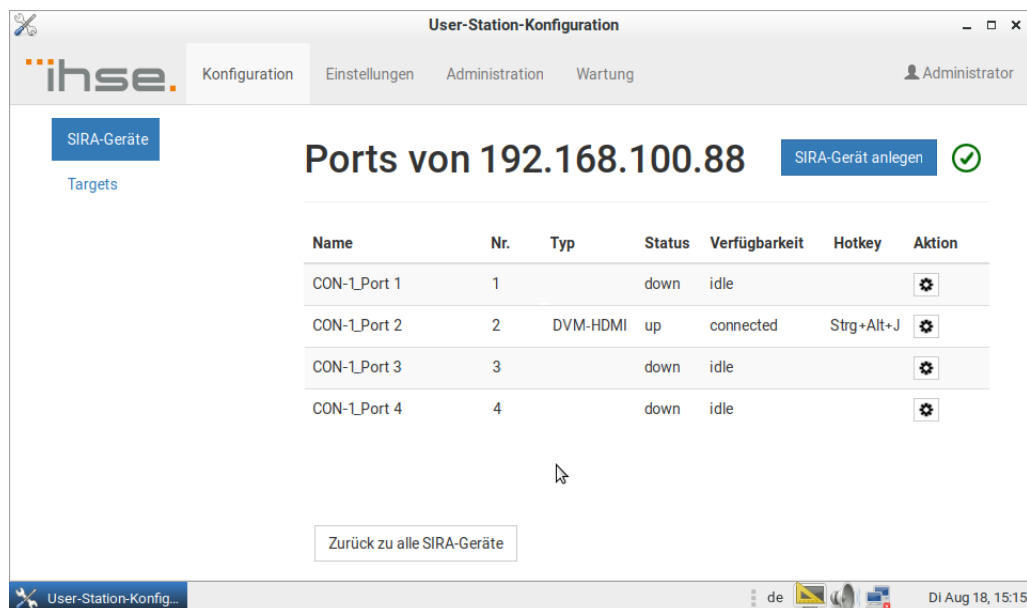


Abb. 59 Konfiguration - SIRA-Geräte - **Portliste**

2. Klicken Sie auf das Symbol  in der Spalte „Aktionen“. Ein Dialog wird geöffnet.
3. Stellen Sie die „Allgemeinen Einstellungen“ ein.

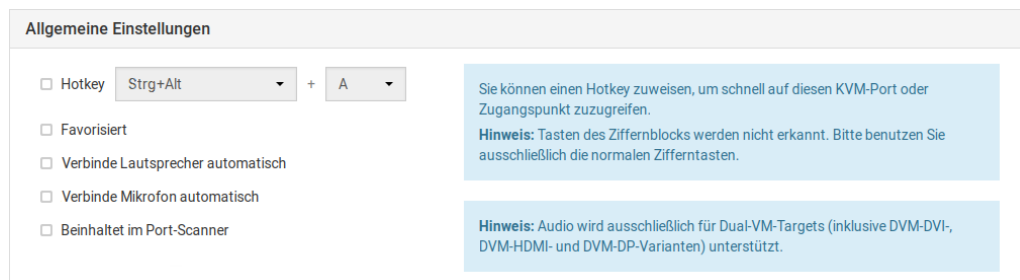


Abb. 60 Konfiguration - KVM-Ports - **Allgemeine Einstellungen**

Kontrollkästchen	Symbol in Liste	Beschreibung
Hotkey	Der Hotkey wird in der Spalte „Hotkey“ angezeigt.	Weisen Sie dem Port einen Hotkey zu, um schnell auf diesen zugreifen zu können. Zu den verfügbaren Optionen gehören: • Strg+Shift+<Schriftzeichen> • Strg+Alt+<Schriftzeichen> • Umschalt+Alt+<Schriftzeichen> • Strg+Shift+Alt+<Schriftzeichen> <Schriftzeichen> ist eine alphanumerische Taste oder eine Funktionstaste Einige Tastenkombinationen können nicht für den Port-Zugriff verwendet werden und stehen daher nicht zur Verfügung (siehe folgende Tabelle).
Favorisiert		Wird dieses Kontrollkästchen aktiviert, wird dieser KVM-Port im Panel „Favorisierte Targets“ des Port Navigators angezeigt (siehe Abschnitt 7.1, Seite 78)

Kontrollkästchen	Symbol in Liste	Beschreibung
Verbinde Lautsprecher automatisch		Die Lautsprecher werden beim Start des Target-Systems automatisch an diesen KVM-Anschluss angeschlossen.
Verbinde Mikrofon automatisch		Das Mikrofon wird beim Start des Target-Systems automatisch an diesen KVM-Anschluss angeschlossen.
Beinhaltet im Port-Scanner		Fügt diesen Port dem Port-Scanner hinzu (siehe Abschnitt 7.2, Seite 83).

Wird ein Kontrollkästchen aktiviert, erscheint das entsprechende Symbol in der Liste in der Spalte „Name“.

Hotkeys, die für Port-Zugang nicht zur Verfügung stehen

Hotkey	Beschreibung
Strg+Shift+ <Zahl>	<Zahl> = 0 bis 9
Strg+Shift+Alt+ <Zahl>	
Umschalt+Alt+ <Zahl>	
Strg+Alt+ <Funktionstaste>	<Funktionstaste> = F1 bis F12
Strg+Alt+C Strg+Alt+F Strg+Alt+L Strg+Alt+M Strg+Alt+N	Diese Tastenkombinationen können verwendet werden, wenn Sie sie zuvor als Tastenkombinationen der User Station deaktivieren.

4. Konfigurieren Sie die „Target-Fenster-Einstellungen“, wenn Ihnen die Standard-Einstellungen nicht zusagen.

Target-Fenster-Einstellungen

☒ Spezifische Target-Fenster-Einstellungen

☒ Skaliere Video
☒ Fensterdekorationen
☒ Zeige Werkzeugleiste
☐ Vollbildmodus
☐ Vollbildmodus bedeckt alle Monitore
☐ Starte im Single-Maus-Cursor-Modus
☐ Synchronisiere Maus bei Verbindung
☐ Automatische Videoerkennung bei Verbindung
☐ Erlaube Eingaben nur wenn fokussiert
☐ Auf aktuellen Monitor beschränken
 Cursor-Form (im Doppel-Cursor-Modus)

☐ Banner-Nachrichten Deaktivieren

Normalerweise benutzt die Draco SIRA User Station Target-Fenster-Einstellungen, die für alle Ports und Zugangspunkte gelten. Sie können diese Einstellungen jedoch für diesen bestimmten Port oder Zugangspunkt überschreiben, indem Sie **Spezifische Target-Fenster-Einstellungen** auswählen. Sie können die Standard-Einstellungen im Zugangs-Clients-Einstellungen-Dialog ändern:

Anmerkungen:

- Diese Einstellungen werden nicht für bereits geöffnete Zugangs-Clients übernommen.
- Um den Vollbildmodus zu verlassen, drücken Sie den Vollbildmodus-Hotkey (standardmäßig Strg+Alt+F) im Clienten.
- Um den Zugang im Vollbildmodus zu starten, muss ein entsprechender Hotkey konfiguriert sein, oder die Werkzeugleiste muss aktiviert sein. Wenn nicht, würde man als Nutzer im Vollbildmodus eingesperrt.

Abb. 61 Konfiguration - KVM-Ports - Target-Fenster-Einstellungen

- Klicken Sie auf den Button **Zugangs-Clients-Einstellungen**, um die Standard-Einstellungen für das Target-Fenster anzuzeigen (siehe Abschnitt 8.1, Seite 87).
- Wenn Sie eine dieser Einstellungen überschreiben möchten, aktivieren Sie das Kontrollkästchen „Spezifische Target-Fenster-Einstellungen“.
- Aktivieren Sie das Kontrollkästchen jeder Funktion, die Sie aktivieren möchten.
- Wenn Sie alle gewünschten Änderungen durchgeführt haben, klicken Sie auf **Speichern**.

Status der Datenabfrage von Ports

In der rechten oberen Ecke der „Portliste“ im Fenster „User-Station-Konfiguration“ wird ein Symbol angezeigt. Dieses Symbol gibt den Status der Datenabfrage der KVM-Ports am ausgewählten SIRA-Gerät an.

➔ Klicken Sie auf dieses Symbol, um zusätzliche Informationen anzuzeigen.

Das Symbol ändert sich je nach aktuellem Status des KVM-Ports.

Symbol	Beschreibung
	Portinformationen dieses Gerätes können angezeigt werden.
	Portinformationen dieses Gerätes können NICHT angezeigt werden. Mögliche Gründe hierfür: • Falsche Benutzer-Anmeldedaten wurden für dieses Gerät eingegeben. • Das Zertifikat dieses Gerätes kann nicht verifiziert werden (wenn Zertifikatsprüfung aktiviert ist). • Probleme mit der Netzwerkverbindung, z.B. das gewählte Gerät ist nicht mit dem Netzwerk verbunden.
	Portinformationen dieses Gerätes sind nicht verfügbar, da noch keine Benutzerdaten eingegeben wurden.

Der Status der Portdatenabfrage wirkt sich auf den Geräte- und Portstatus aus, der im Fenster „Port Navigator“ angezeigt wird.

6.3 Zugriff auf KVM/serielle Switches und Ports

Über das Fenster Port-Navigator kann auf Computer und Targets zugegriffen werden, die an Ports der SIRA-Geräte angeschlossen sind. Der Port-Navigator hat drei Paneele:

- **Favorisierte Targets** zeigt die Targets, die als Favorit gekennzeichnet wurden (siehe vorheriger Abschnitt).
- **Geräte** zeigt alle hinzugefügten Geräte und ihre Ports.
- **Targets** zeigt alle hinzugefügten KVM, seriellen, SSH, RDP und VNC Web ESXi Targets.

Der Port-Navigator wird standardmäßig angezeigt. Wenn nicht, können Sie ihn mit der Tastenkombination **Ctrl+Alt+N** starten oder durch Klicken auf **Hauptmenü > Port-Navigator**.

 Die User Station kann auf keinen KVM-Port zugreifen, der an einen mehrstufigen KVM-Switch oder einen Blade-Server angeschlossen ist.

1. Klicken Sie auf ein SIRA-Gerät im Panel Geräte.

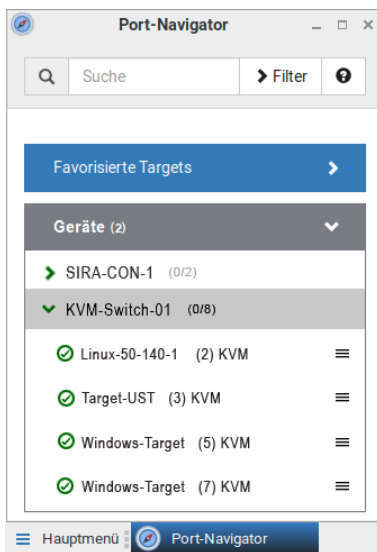


Abb. 62 **Port-Navigator und geöffnetes Geräte-Panel**

Standardmäßig werden nur „up“ Ports in der Liste unterhalb des gewählten Gerätes angezeigt. Für Dual-Port-Video muss nur der primäre Port „up“ sein, um angezeigt zu werden.

- Zahlen in Klammern sind die physischen Portnummern des KVM/seriellen Switches.
- Bei Dual-Port-Videos werden die primären und sekundären physischen Portnummern in Klammern angezeigt.

 Um Geräte-Ports anzuzeigen, die „down“ sind, siehe Abschnitt 7.1.2, Seite 79.

2. Klicken Sie auf das Symbol  des gewünschten Ports und wählen Sie entweder *Open in new KVM client* oder *Open in current KVM client* oder

klicken Sie auf den Portnamen:

- Einzelklicken öffnet den Port im aktiven KVM-Client-Fenster.
- Doppelklicken öffnet den Port in einem neuen KVM-Client-Fenster.
- Rechtsklicken zeigt die Optionen des KVM-Clients an.

Die Anzahl der verbundenen Sessions wird neben dem Gerätenamen angezeigt. Beispiel: Wenn 8 Ports verfügbar sind, von denen 4 belegt sind, lautet die Anzeige „<Gerätename> (4/8)“.

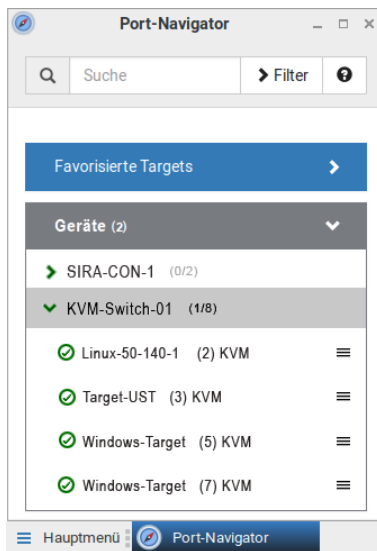


Abb. 63 Geräte-Panel, ein Port wird benutzt

✓ Das Verhalten der Mausklicks (links, Doppelklick, rechts) lässt sich individuell anpassen (siehe Abschnitt 8.1, Seite 87).

6.4 Targets verwalten und Zugangsmethoden

Targets und Zugangsmethoden werden im Konfigurationsfenster angelegt und verwaltet.

Es gibt verschiedene Möglichkeiten, Targets anzuzeigen, zu verwalten und eine Verbindung zu ihnen herzustellen – über KVM/seriellen Port-Zugang, RDP, SSH und VNC. Sie können außerdem den Zugang auf eine Webanwendung von ESXi-virtuellen Maschinen hinzufügen. Diese Methoden ermöglichen den Zugriff auf alle KVM/seriellen Targets sowie auf nicht-KVM/serielle Targets wie Server, Netzwerk-Switches, HLK-Geräte oder andere an Ihr Netzwerk angeschlossene Geräte.

Draco SIRA User Station Multi KVM-Zugangsmethode (M-KVM) ermöglicht es, zwei oder mehr KVM-Ports in einem virtuellen Multi-Monitor-KVM-Target zu vereinen.

Wenn ein Draco SIRA-Gerät hinzugefügt wird, erkennt die User Station automatisch die Anschlüsse und legt für jeden Anschluss ein Ziel mit einer KVM-Zugangsmethode an. Der Abschnitt „Targets“ in der User Station-Konfiguration und der Abschnitt „Geräte“ im Port-Navigator enthalten diese Informationen und ermöglichen den Zugriff. Der KVM-Zugang kann nicht manuell hinzugefügt werden; er basiert stets auf der Zugangsmöglichkeit auf das KVM-Gerät.

Die User Station bietet den vollen Funktionsumfang einer RDP-Software, die die Maus- und Tastatureingaben vom lokalen Computer erfasst und an den Remote-Target-Rechner weiterleitet. Der RDP-Client verfügt über eine „Grab-Keyboard“-Funktion, die standardmäßig aktiviert ist, die Sie jedoch deaktivieren können. Mit dieser Funktion können Sie alle Tastatureingaben – einschließlich des Netzschalters und anderer Tastenkombinationen – vom lokalen Betriebssystem erfassen, die dann vom Target-Rechner und nicht von der User Station verarbeitet werden. RDP ermöglicht zudem einen unterbrechungsfreien Zugriff auf die Bild- und Tonausgabe der Targetanwendungen.

6.4.1 Targets und Zugangsmethoden hinzufügen

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration** und klicken Sie dann auf **Targets**.
Die Liste der Targets erscheint.

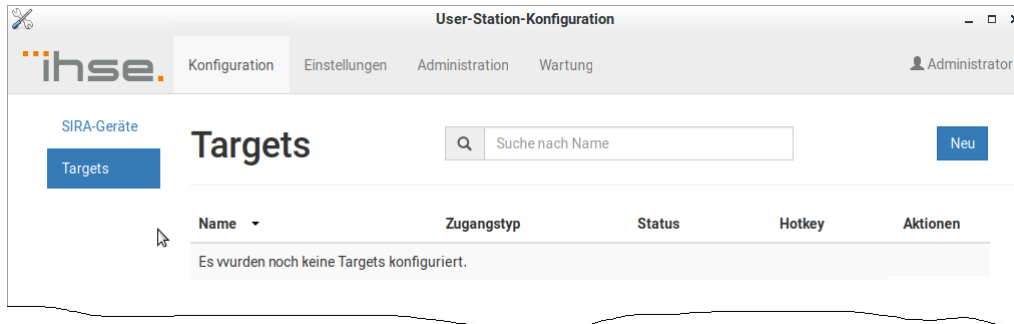


Abb. 64 Konfiguration - **Target-Liste**

2. Klicken Sie auf den Button **Neu**.

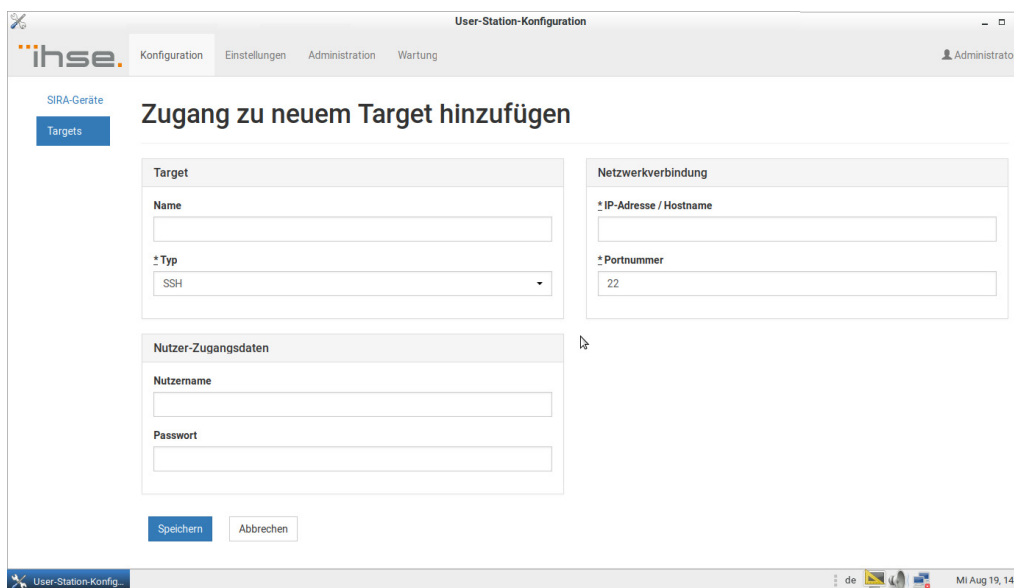


Abb. 65 Konfiguration - **Targets - Neues Target und Zugang hinzufügen**

3. Geben Sie einen Namen für das Target ein und wählen Sie einen Zugangstyp aus der Drop-Down-Liste „Typ“ aus.
4. Die nächsten Schritte hängen vom Zugangstyp ab.

6.4.1.1 SSH-, VNC- und RDP-Zugangstyp

1. Wählen Sie entweder SSH, VNC oder RDP aus der Drop-Down-Liste „Typ“ aus.
2. Geben Sie die IP-Adresse oder den Hostname des Targets ein.
3. Wenn Sie möchten, ändern Sie die Standard-Portnummer (22 für SSH; 5900 für VNC; 3389 für RDP).
4. Geben Sie Nutzer-Zugangsdaten ein (Name und Passwort).

User-Station-Konfiguration

Konfiguration | Einstellungen | Administration | Wartung | Administrator

SIRA-Geräte | **Targets**

Zugang zu neuem Target hinzufügen

Target
Name: Computer 1
Typ: RDP

Netzwerkverbindung
IP-Adresse / Hostname: 192.168.100.143
Portnummer: 3389

Nutzer-Zugangsdaten
Nutzername: admin
Passwort: *****

Speichern | Abbrechen

User-Station-Konfig- | de | MI Aug 19, 14:50

Abb. 66 Konfiguration - Targets - Neues Target mit SSH, RDP oder VNC Zugang hinzufügen

5. Klicken Sie auf **Speichern**.

Das neue Target mit dem ausgewählten Zugangstyp wird zur Target-Liste hinzugefügt. Es erscheint eine Übersicht über die Target- und Zugangsdaten mit Bearbeitungsbutton zum Ändern der Identitäts- oder Zugangsdaten einschließlich der Anmeldedaten.

User-Station-Konfiguration

Konfiguration | Einstellungen | Administration | Wartung | Administrator

SIRA-Geräte | **Targets**

Target Computer_01 und sein verknüpfter RDP-Zugang wurden erfolgreich erstellt

Target Computer 1

Zugang Hinzufügen

Identität
Name: Computer 1
Bearbeiten

RDP-Zugang
IP-Adresse / Hostname: 192.168.100.143
Portnummer: 3389
Zugangsdaten: ✓ gesetzt
Bearbeiten | Zugangsdaten | Einstellungen | Löschen

Zurück

de | MI Aug 19, 14:51

Abb. 67 Konfiguration - Targets - Neues Target mit RDP-Zugang hinzugefügt

- Klicken Sie auf **Zugang hinzufügen**, um einen weiteren Zugangstyp diesem Target hinzuzufügen.
- Wiederholen Sie die Schritte 1 bis 5.
- Wenn Sie alle Zugangstypen angelegt haben, klicken Sie auf **Zurück**. In der Target-Liste werden alle Zugangstypen, die angelegt wurden, angezeigt.

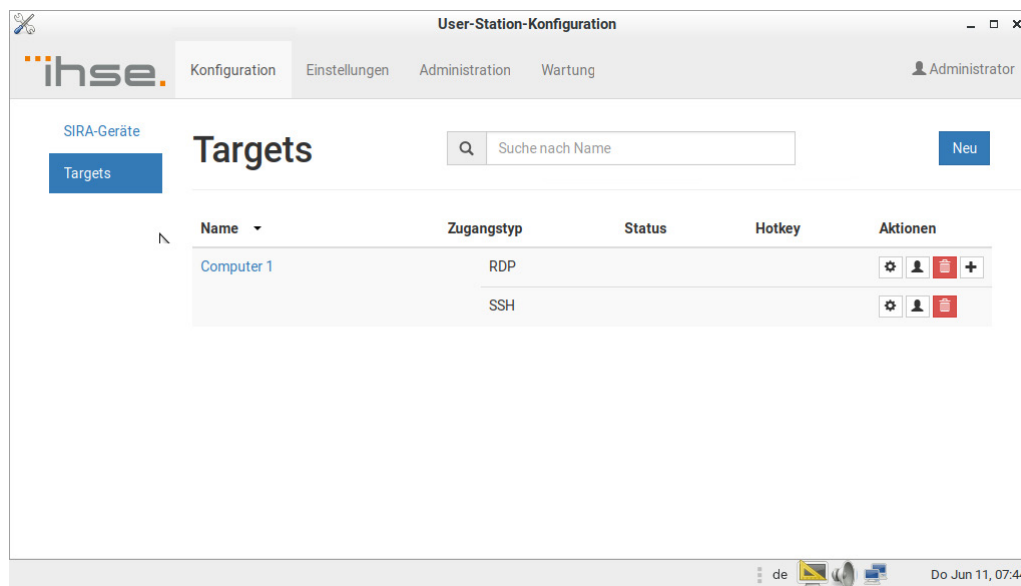


Abb. 68 Konfiguration - Target-Liste

Die Targets werden ebenfalls im Port Navigator-Fenster zusammen mit ihren Zugangstypen aufgelistet.

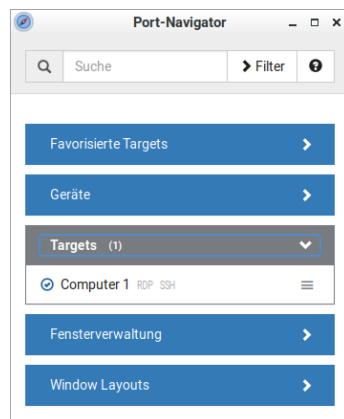


Abb. 69 Port-Navigator - Target-Liste

6.4.1.2 WEB-Zugang

Mit der WEB-Zugangsmethode können Sie eine Webanwendung im eigenen Web-Client der Draco SIRA User Station starten. Dies kann genutzt werden, um die Fernsteuerungsfunktion zum Steuern einer anderen User Station zu starten oder um auf die Web-Benutzeroberfläche eines anderen KVM-Geräts zuzugreifen (siehe Fernsteuerungsfunktion auf Seite 141).

Der Web-Client bietet lediglich eine einfache Navigation und unterstützt weder Java noch Plugins, das Hoch- und Herunterladen von Dateien, Audio- und Videodateien, Webcams und Mikrofone, das Öffnen neuer Fenster oder Registerkarten noch andere erweiterte Funktionen. Single Sign-On wird nicht unterstützt, sodass Sie bei jedem Start der Weboberfläche Ihre Anmeldedaten eingeben müssen.

Um den WEB-Zugang zu starten, benötigen Sie die Berechtigung „WEB-Zugang“. Um den WEB-Zugang zu konfigurieren, benötigen Sie die Berechtigung „Geräteverwaltung“ oder „Systemverwaltung“.

1. Wählen Sie als Zugangstyp „Web“.

Zugang zu Computer 1 hinzufügen

Zugang

* Typ
WEB

Web-Adresse

Geben Sie eine gültige URL inklusive Schema, Host, optional Port und Pfad an:
<Schema>://<Host>[:<Port>]/<Pfad>
Valide Schemata sind https und http.
Beispiel: https://www.example.com/test

* URL
192.168.12.28

Speichern Abbrechen

Abb. 70 Konfiguration - Targets - **Web-Zugang hinzufügen**

2. Geben Sie die URL ein im Format <schema>://<host>[:<port>]/<path>
Beispiel: https://www.example.com/test
Valide Schemata sind https und http.
3. Klicken Sie auf **Speichern**, um den Web-Zugang zu erstellen.

6.4.1.3 ESXi-Zugang

Mit der ESXi-Zugangsmethode können Sie über den User Station Navigator mithilfe des VMware „ESXi Embedded Host Client“ auf virtuelle VMware ESXi-Maschinen zugreifen und diese steuern. Der ESXi-Server muss den ESXi Embedded Host Client unterstützen und mindestens die Version 6.0 aufweisen. Beim Start wird die Remote-Konsole der virtuellen Maschine angezeigt. Single Sign-On wird nicht unterstützt, daher müssen Sie bei jedem Start der Schnittstelle Ihre Anmeldedaten eingeben.

Um ESXi-Zugang zu starten, benötigen Sie die Berechtigung „ESXi-Zugang“. Um den ESXi-Zugang zu konfigurieren, benötigen Sie die Berechtigung „Geräte-Administration“ oder „System-Administration“.

1. Wählen Sie als Zugangstyp „ESXi“.

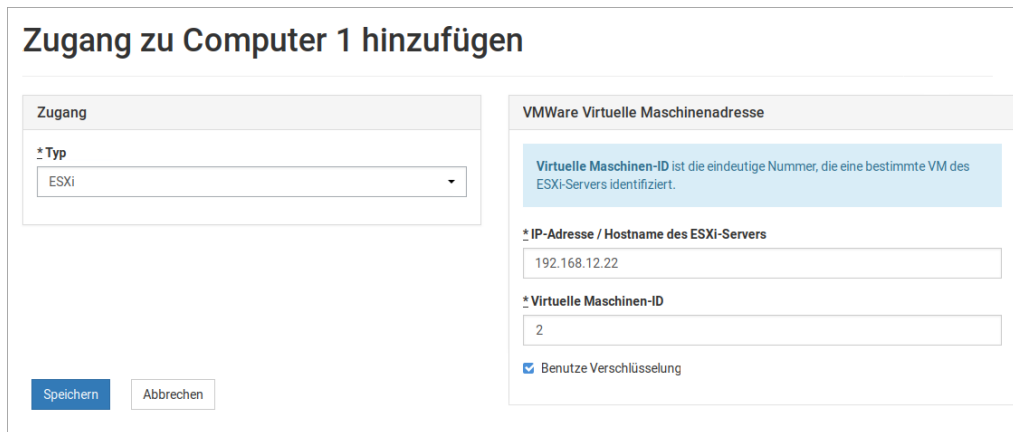


Abb. 71 Konfiguration - Targets - **ESXi-Zugang hinzufügen**

2. Geben Sie die IP-Adresse oder den Hostnamen des ESXi-Servers.
3. Geben Sie die ID der virtuellen Maschine ein.
Die ID befindet sich in der Adressleiste des Browsers, in der die URL zur virtuellen Maschine angezeigt wird. Die ID ist der letzte Teil der URL.
4. Aktivieren Sie „Benutze Verschlüsselung“, wenn Sie HTTPS als Protokoll verwenden wollen für den Zugang zur ESXi Remote Konsole.
5. Klicken Sie auf **Speichern**. Der ESXi-Zugang wird zum Target hinzugefügt und erscheint in der Target-Liste.

6.4.1.4 Multi-KVM-Zugang

Sie können zwei oder mehr KVM-Ports als virtuelles KVM-Target mit mehreren Monitoren konfigurieren. Die Draco SIRA User Station unterstützt bis zu sechs an dasselbe Target angeschlossene Bildschirme, wobei jeder Bildschirm über eine eigene SIRA CON-Unit verfügt. Jede CON-Unit wird der User Station hinzugefügt, und anschließend wird aus den KVM-Anschlüssen der CON-Units ein neues M-KVM-Target erstellt. Diese unabhängigen Ports werden als Portgruppe mit mehreren Monitoren behandelt.

 Es werden nur SIRA CON-Ports unterstützt, die mit demselben Target-PC verbunden sind. Die Bildschirmkonfiguration auf dem Target-PC muss mit der in der User Station ausgewählten Konfiguration übereinstimmen.

Um die Multi-KVM-Zugangsmethode zu konfigurieren, wählen Sie die KVM-Ports aus, die Sie virtuell gruppieren möchten, und legen Sie eine der unterstützten Ausrichtungen fest. Sobald der Multi-KVM-Zugang eingerichtet ist, werden diese Multi-Monitor-Zugangspunkte im Navigator als „M-KVM“ gekennzeichnet. Die enthaltenen KVM-Ports werden im Navigator weiterhin als separate Ports aufgeführt. Es ist möglich, eine Verbindung zu den einzelnen Ports unabhängig voneinander herzustellen. Dies wird jedoch nicht empfohlen, da die Maussteuerung auf den primären Port beschränkt ist. Die Multi-KVM-Targets können nicht zum Port-Scanner hinzugefügt werden, Sie können jedoch weiterhin die einzelnen Ports hinzufügen.

 Es ist wichtig, dass die Ausrichtung, die Anzahl der Ports und die Auswahl der KVM-Ports an der User Station mit der Bildschirmkonfiguration übereinstimmen. Die folgende Beispielabbildung zeigt die User Station und das Target-Betriebssystem (Bildschirmkonfiguration für einen Windows-PC mit vier horizontal angeordneten Bildschirmen). Verwenden Sie die Schaltfläche „Identifizieren“ im Windows-Betriebssystem, um zu überprüfen, ob die Positionierung der Bildschirme auf dem Target-System und der Draco SIRA User Station übereinstimmt.

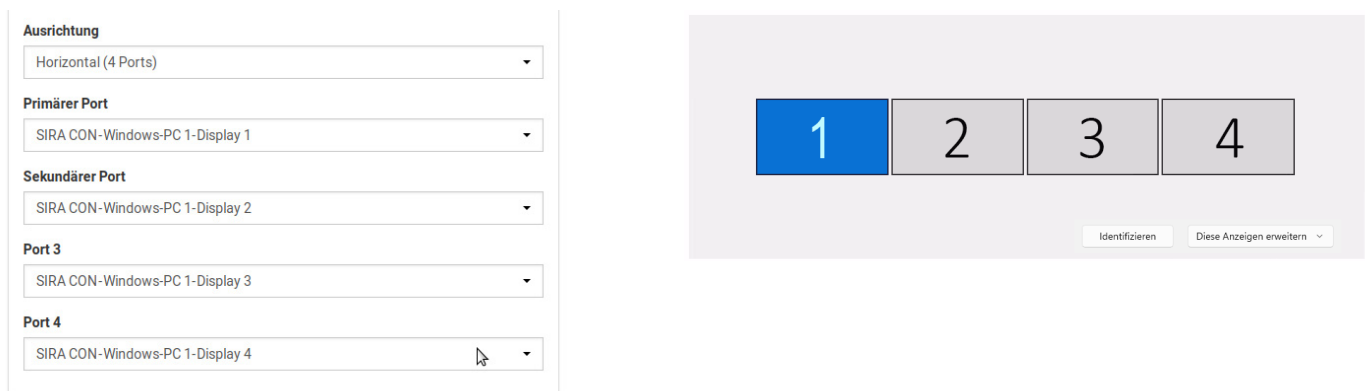


Abb. 72 Konfiguration - Targets - Beispiel für Multi-KVM-Zugang und Monitoranordnung des Targets

1. Erzeugen Sie ein Target für jede SIRA CON-Unit.
2. Wählen Sie „Multi KVM“ als Zugangstyp.

ihse. User-Station-Konfiguration Administrator

Konfiguration Einstellungen Administration Wartung

SIRA-Geräte Targets

Zugang zu Computer 1 hinzufügen

Zugang

Typ

Multi KVM

Multi-KVM-Zugang

Hier können Sie zwei oder mehr KVM-Ports zu einem virtuellen Multi-Monitor-KVM-Target konfigurieren. Die unabhängigen Ports werden behandelt, als wären sie Teil einer Multi-Monitor-Portgruppe.

Bitte wählen Sie den Primären Port (oben links) und den/die sekundären Port(s) (links neben oder unter dem primären Port) und die gewünschte Ausrichtung (vertikal oder horizontal, usw.).

Dies wird nur für Draco-SIRA-Geräte unterstützt.

Ausrichtung

Horizontal (4 Ports)

Primärer Port

SIRA CON-Windows-PC 1-Display 1

Sekundärer Port

SIRA CON-Windows-PC 1-Display 2

Port 3

SIRA CON-Windows-PC 1-Display 3

Port 4

SIRA CON-Windows-PC 1-Display 4

Speichern Abbrechen

Do Aug 27, 14:57

Abb. 73 Konfiguration - Targets - **Multi-KVM-Zugriff hinzufügen**

3. Wählen Sie die Ausrichtung für die Portgruppe mit der Anzahl der Monitore.
4. In die Felder für primären und sekundären Port müssen die KVM-Ports wie folgt ausgewählt werden:
 - Primärer Port: Der KVM-Port in der oberen linken Ecke.
 - Sekundärer Port: Der KVM-Port, der sich direkt rechts oder direkt unterhalb des primären Ports befindet.
 - Für Konfigurationen mit mehr als zwei Ports wählen Sie die Ports 3, 4, 5 und 6 aus. Die Felder erscheinen passend für jede gewählte Ausrichtung.
5. Klicken Sie auf **Speichern**.
Der neue M-KVM-Zugang wird zur Target-Liste hinzugefügt.

6.4.2 Targets und Zugangsmethoden ändern und löschen

Targets und Zugangsmethoden sind im Konfigurationsfenster der User Station und im Port Navigator aufgelistet. Der KVM-Zugang kann nicht gelöscht werden, alle anderen Zugangsmethoden lassen sich jedoch löschen. Ein Target muss über mindestens eine Zugangsmethode verfügen, andernfalls wird das Target gelöscht.

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration** und dann auf den Button **Targets**. Die Target-Liste erscheint.

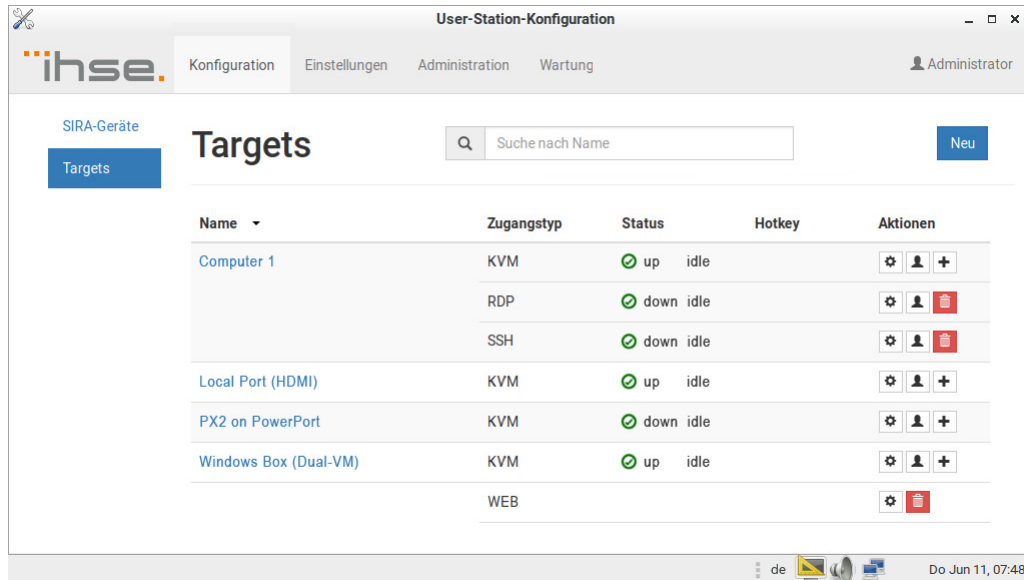


Abb. 74 Konfiguration - Target-Liste

Die Symbole in der Spalte „Aktionen“ bedeuten folgendes:

Symbol	Beschreibung
	Einstellungen ändern für KVM-Port und Zugang (siehe Abschnitt 6.2), ändern der Zugangseinstellungen für alle anderen Typen (siehe unten).
	Anmeldedaten ändern für alle Zugangsmethoden.
	Einem Target eine weitere Zugangsmethode hinzufügen.
	Löschen einer Zugangsmethode. KVM-Zugänge kann nicht gelöscht werden. Wenn die letzte Zugangsmethode gelöscht wird, wird das Target gelöscht.

6.4.2.1 Zugangseinstellungen ändern

Für jeden Zugangstyp können Sie allgemeinen Einstellungen sowie Einstellungen für das Target-Fenster konfigurieren. Die meisten Einstellungen gelten für alle Typen, doch gibt es in jeder Kategorie einige spezifische Einstellungen, die für die einzelnen Zugangstypen in den folgenden Beispielen erläutert werden.

Standardmäßig verwendet die Draco User Station Target-Fenster-Einstellungen, die für alle Ports und Zugangspunkte gelten. Sie können diese Einstellungen für einen bestimmten Port bzw. Zugangspunkt überschreiben, indem Sie „Spezifische Zielfenster-Einstellungen verwenden“ auswählen. Einzelheiten zu allen Einstellungen sowie zur Festlegung von Standardwerten finden Sie unter **Einstellungen > Zugangs-Clienten-Einstellungen** im Kapitel 8).

Allgemeine Einstellungen für alle Zugangstypen

1. Klicken Sie auf das Editiersymbol  in der Zeile eines Zugangs. Ein Fenster wird geöffnet.
2. Konfigurieren Sie die allgemeinen Einstellungen.

Allgemeine Einstellungen

☐ Hotkey

Ctrl+Alt

+

A

☐ Favorisiert
 ☐ Verbinde Lautsprecher automatisch
 ☐ Verbinde Mikrofon automatisch

Sie können einen Hotkey zuweisen, um schnell auf diesen KVM-Port oder Zugangspunkt zuzugreifen.

Hinweis: Tasten des Ziffernblocks werden nicht erkannt. Bitte benutzen Sie ausschließlich die normalen Zifferntasten.

Abb. 75 Konfiguration - Targets - **Allgemeine Einstellungen**

Nicht alle in der folgenden Tabelle beschriebenen Kontrollkästchen sind für alle Zugriffstypen verfügbar.

Checkbox	Symbol in Liste	Beschreibung
Hotkey	Der Hotkey wird in der Spalte Hotkey angezeigt.	Weisen Sie eine Tastenkombination zu, um schnell auf diesen Port zugreifen zu können. Zu den verfügbaren Optionen gehören: • Strg+Shift+< Schriftzeichen > • Strg+Alt+< Schriftzeichen > • Umschalt+Alt+< Schriftzeichen > • Strg+Umschalt+Alt+< Schriftzeichen > < Schriftzeichen > ist eine alphanumerische Taste oder eine Funktionstaste Einige Tastenkombinationen können nicht für den Port-Zugriff verwendet werden und stehen daher nicht zur Verfügung (siehe folgende Tabelle).
Favorisiert		Wird diese Checkbox aktiviert, wird dieser Port im Panel „Favorisierte Targets“ angezeigt (siehe Abschnitt 7.1, ab Seite 78).
Verbinde Lautsprecher automatisch		Lautsprecher werden beim Start der Targetanwendung automatisch an diesem Anschluss aktiviert.
Verbinde Mikrofon automatisch		Das Mikrofon wird automatisch beim Start der Targetanwendung an diesem Anschluss aktiviert.

Nicht zur Verfügung stehende Hotkeys für Portzugang

Hotkey	Beschreibung
Strg+Umschalt+ <Zahl>	<Zahl> = 0 to 9
Strg+Umschalt+Alt+ <Zahl>	
Umschalt+Alt+ <Zahl>	
Strg+Alt+ <Funktionstaste>	<Funktionstaste> = F1 bis F12
Strg+Alt+C Strg+Alt+F Strg+Alt+L Strg+Alt+M Strg+Alt+N	Diese Tastenkombinationen können verwendet werden, wenn Sie sie zunächst als Tastenkombinationen der User Station deaktivieren.

Target-Fenster-Einstellungen für RDP-Zugang

1. Klicken Sie auf das Editiersymbol  in der Zeile eines RDP-Zugangs. Das Fenster zur Änderung der RDP-Zugangs-Einstellungen wird geöffnet.

Target-Fenster-Einstellungen

☐ Spezifische Target-Fenster-Einstellungen

☒ Fensterdekorationen

☐ Vollbildmodus

Ändern der Fenstergröße

Feste Größe

Übertragungsqualität

Mittel

Bevorzugte Auflösung

1024 x 768

Als Multi-Monitor-Target anzeigen

Deaktiviert

Desktop-Skalierung

100%

☒ Fange alle Tastatur- und Einschalter-Ereignisse ab

Normalerweise benutzt die Draco SIRA User Station Target-Fenster-Einstellungen, die für alle Ports und Zugangspunkte gelten. Sie können diese Einstellungen jedoch für diesen bestimmten Port oder Zugangspunkt überschreiben, indem Sie **Spezifische Target-Fenster-Einstellungen** auswählen. Sie können die Standard-Einstellungen im Zugangs-Clients-Einstellungen-Dialog ändern:

Zugangs-Clients-Einstellungen

Anmerkungen:

- Diese Einstellungen werden nicht für bereits geöffnete Zugangs-Clients übernommen.
- Der Vollbildmodus-Hotkey ist **Strg+Alt+Eingabetaste**.
- Multi-Monitor-RDP-Targets werden immer im Vollbildmodus angezeigt.

RDP-Zertifikat

Es ist für diesen Zugang kein RDP-Zertifikat gespeichert.

Anmerkungen:

Ein RDP-Zertifikat ist ein kryptographisches Zertifikat, das zur Identifizierung von Computern über das RDP-Protokoll verwendet wird. Je nach Sicherheitseinstellungen kann eventuell nur eine RDP-Verbindung zu bekannten Geräten aufgebaut werden.

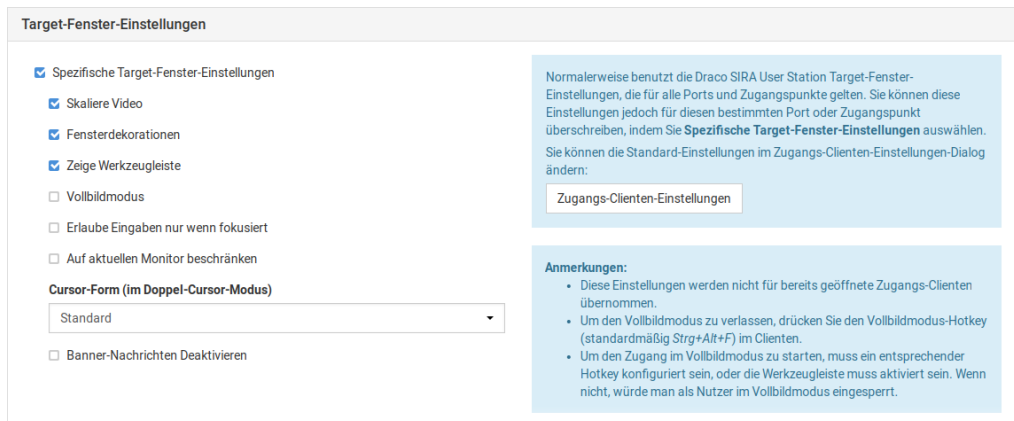
Falls ein Zertifikat für diesen Zugang gespeichert ist, können Sie hier seinen Fingerabdruck sehen oder es löschen.

Abb. 76 Konfiguration - Targets - Target-Fenster-Einstellungen für RDP-Zugang

2. Klicken Sie auf den Button **Zugangs-Clients-Einstellungen**, um die Standard-Target-Fenster-Einstellungen anzuzeigen (siehe Abschnitt 8.1, ab Seite 87).
3. Wenn Sie eine dieser Einstellungen überschreiben möchten, aktivieren Sie das Kontrollkästchen „Spezifische Target-Fenster-Einstellungen“.
4. Wählen Sie die gewünschten Werte für die Parameter aus.
5. Klicken Sie auf **Speichern**.

Target-Fenster-Einstellungen für VNC-Zugang

1. Klicken Sie auf das Editiersymbol  in der Zeile eines VNC-Zugangs. Das Fenster zur Änderung der VNC-Zugangs-Einstellungen wird geöffnet.



Target-Fenster-Einstellungen

☒ Spezifische Target-Fenster-Einstellungen

☒ Skaliere Video

☒ Fensterdekorationen

☒ Zeige Werkzeugleiste

☐ Vollbildmodus

☐ Erlaube Eingaben nur wenn fokussiert

☐ Auf aktuellen Monitor beschränken

Cursor-Form (im Doppel-Cursor-Modus)

Standard

☐ Banner-Nachrichten Deaktivieren

Normalerweise benutzt die Draco SIRA User Station Target-Fenster-Einstellungen, die für alle Ports und Zugangspunkte gelten. Sie können diese Einstellungen jedoch für diesen bestimmten Port oder Zugangspunkt überschreiben, indem Sie **Spezifische Target-Fenster-Einstellungen** auswählen. Sie können die Standard-Einstellungen im Zugangs-Clients-Einstellungen-Dialog ändern:

[Zugangs-Clients-Einstellungen](#)

Anmerkungen:

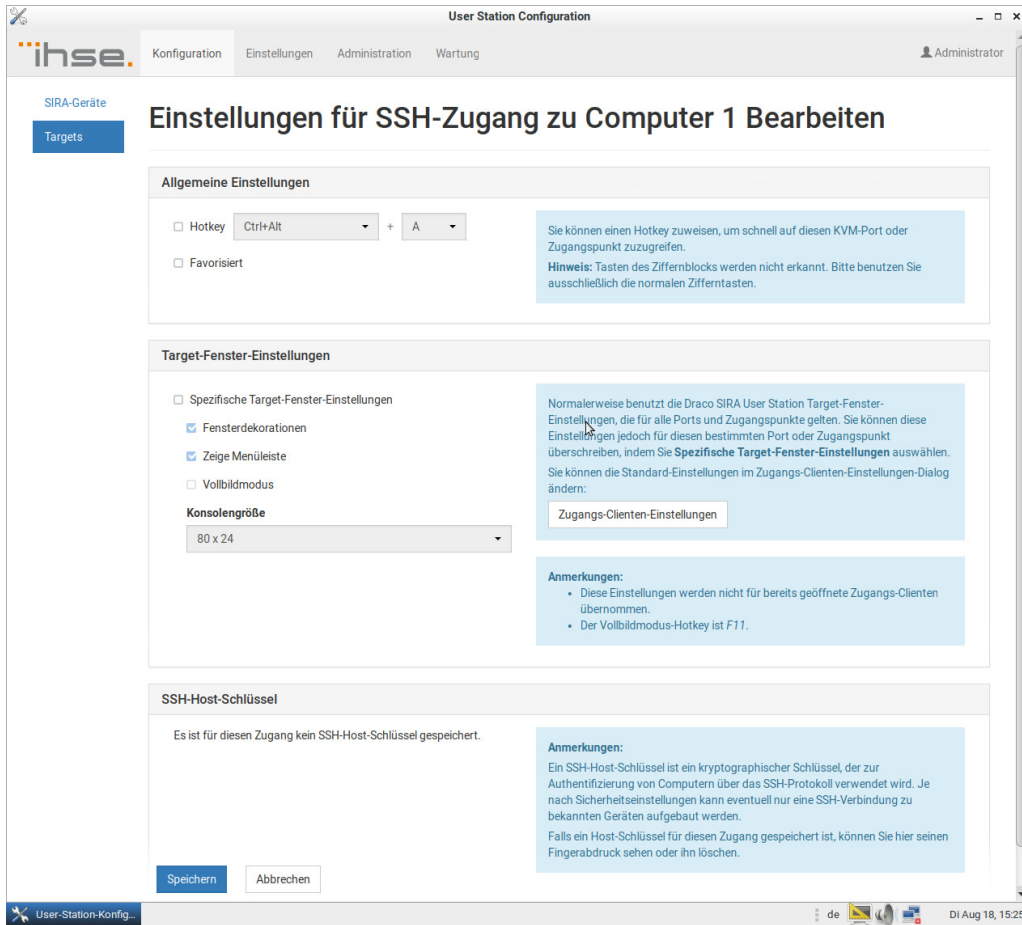
- Diese Einstellungen werden nicht für bereits geöffnete Zugangs-Clients übernommen.
- Um den Vollbildmodus zu verlassen, drücken Sie den Vollbildmodus-Hotkey (standardmäßig **Strg+Alt+F**) im Clienten.
- Um den Zugang im Vollbildmodus zu starten, muss ein entsprechender Hotkey konfiguriert sein, oder die Werkzeugleiste muss aktiviert sein. Wenn nicht, würde man als Nutzer im Vollbildmodus eingesperrt.

Abb. 77 Konfiguration - Targets - **Target-Fenster-Einstellungen für VNC-Zugang**

2. Klicken Sie auf den Button **Zugangs-Clients-Einstellungen**, um die Standard-Target-Fenster-Einstellungen anzuzeigen (siehe Abschnitt 8.1, Seite 87).
3. Wenn Sie eine dieser Einstellungen überschreiben möchten, aktivieren Sie das Kontrollkästchen „Spezifische Target-Fenster-Einstellungen“.
4. Aktivieren/Deaktivieren Sie die Parameter nach Ihren Wünschen.
5. Klicken Sie auf **Speichern**.

Target-Fenster-Einstellungen für SSH-Zugang

1. Klicken Sie auf das Editiersymbol  in der Zeile eines SSH-Zugangs. Das Fenster zur Änderung der SSH-Zugangs-Einstellungen wird geöffnet.



User Station Configuration

ihse. Konfiguration Einstellungen Administration Wartung Administrator

SIRA-Geräte

Einstellungen für SSH-Zugang zu Computer 1 Bearbeiten

Allgemeine Einstellungen

☐ Hotkey Ctrl+Alt + A

☐ Favorisiert

Sie können einen Hotkey zuweisen, um schnell auf diesen KVM-Port oder Zugangspunkt zuzugreifen.
Hinweis: Tasten des Ziffernblocks werden nicht erkannt. Bitte benutzen Sie ausschließlich die normalen Zifferntasten.

Target-Fenster-Einstellungen

☐ Spezifische Target-Fenster-Einstellungen

☒ Fensterdekorationen

☒ Zeige Menüleiste

☐ Vollbildmodus

Konsolengröße
80 x 24

Normalerweise benutzt die Draco SIRA User Station Target-Fenster-Einstellungen, die für alle Ports und Zugangspunkte gelten. Sie können diese Einstellungen jedoch für diesen bestimmten Port oder Zugangspunkt überschreiben, indem Sie **Spezifische Target-Fenster-Einstellungen** auswählen. Sie können die Standard-Einstellungen im Zugangs-Clients-Einstellungen-Dialog ändern:
[Zugangs-Clients-Einstellungen](#)

Anmerkungen:

- Diese Einstellungen werden nicht für bereits geöffnete Zugangs-Clients übernommen.
- Der Vollbildmodus-Hotkey ist F11.

SSH-Host-Schlüssel

Es ist für diesen Zugang kein SSH-Host-Schlüssel gespeichert.

Anmerkungen:

Ein SSH-Host-Schlüssel ist ein kryptographischer Schlüssel, der zur Authentifizierung von Computern über das SSH-Protokoll verwendet wird. Je nach Sicherheitseinstellungen kann eventuell nur eine SSH-Verbindung zu bekannten Geräten aufgebaut werden.
Falls ein Host-Schlüssel für diesen Zugang gespeichert ist, können Sie hier seinen Fingerabdruck sehen oder ihn löschen.

[Speichern](#) [Abbrechen](#)

User-Station-Konfig... de DI Aug 18, 15:25

Abb. 78 Konfiguration - Targets - SSH-Zugang ändern

2. Klicken Sie auf den Button **Zugangs-Clients-Einstellungen**, um die Standard-Target-Fenster-Einstellungen anzuzeigen (siehe Abschnitt 8.1, Seite 87).
3. Wenn Sie eine dieser Einstellungen überschreiben möchten, aktivieren Sie das Kontrollkästchen „Spezifische Target-Fenster-Einstellungen“.
4. Aktivieren/Deaktivieren Sie die Checkboxes nach Ihren Wünschen.
5. Klicken Sie auf **Speichern**.

Target-Fenster-Einstellungen für WEB-Zugang

1. Klicken Sie auf das Editiersymbol  in der Zeile eines WEB-Zugangs. Das Fenster zur Änderung der WEB-Zugangs-Einstellungen wird geöffnet.

Einstellungen für WEB-Zugang zu IHSE Home Page Bearbeiten

Target-Fenster-Einstellungen

☐ Spezifische Target-Fenster-Einstellungen

☒ Fensterdekorationen

☒ Zeige Menüleiste

☐ Vollbildmodus

Normalerweise benutzt die Draco SIRA User Station Target-Fenster-Einstellungen, die für alle Ports und Zugangspunkte gelten. Sie können diese Einstellungen jedoch für diesen bestimmten Port oder Zugangspunkt überschreiben, indem Sie **Spezifische Target-Fenster-Einstellungen** auswählen. Sie können die Standard-Einstellungen im Zugangs-Clients-Einstellungen-Dialog ändern:

[Zugangs-Clients-Einstellungen](#)

Anmerkungen:

- Diese Einstellungen werden nicht für bereits geöffnete Zugangs-Clients übernommen.
- Der Vollbildmodus-Hotkey ist F11.

[Speichern](#) [Abbrechen](#)

Abb. 79 Konfiguration - Targets - **WEB-Zugang ändern**

2. Klicken Sie auf den Button **Zugangs-Clients-Einstellungen**, um die Standard-Target-Fenster-Einstellungen anzuzeigen (siehe Abschnitt 8.1, Seite 87).
3. Wenn Sie eine dieser Einstellungen überschreiben möchten, aktivieren Sie das Kontrollkästchen „Spezifische Target-Fenster-Einstellungen“.
4. Aktivieren/Deaktivieren Sie die Checkboxes nach Ihren Wünschen.
5. Klicken Sie auf **Speichern**.

Target-Fenster-Einstellungen für ESXi-Zugang

1. Klicken Sie auf das Editiersymbol  in der Zeile eines ESXi-Zugangs. Das Fenster zur Änderung der ESXi-Zugangs-Einstellungen wird geöffnet.

Einstellungen für ESXi-Zugang zu Computer 1 Bearbeiten

Target-Fenster-Einstellungen

☐ Spezifische Target-Fenster-Einstellungen

☒ Fensterdekorationen

☐ Vollbildmodus

☐ Vollbildmodus bedeckt alle Monitore

Normalerweise benutzt die Draco SIRA User Station Target-Fenster-Einstellungen, die für alle Ports und Zugangspunkte gelten. Sie können diese Einstellungen jedoch für diesen bestimmten Port oder Zugangspunkt überschreiben, indem Sie **Spezifische Target-Fenster-Einstellungen** auswählen. Sie können die Standard-Einstellungen im Zugangs-Clients-Einstellungen-Dialog ändern:

[Zugangs-Clients-Einstellungen](#)

Anmerkungen:

- Diese Einstellungen werden nicht für bereits geöffnete Zugangs-Clients übernommen.
- Der Vollbildmodus-Hotkey ist F11.

[Speichern](#) [Abbrechen](#)

Abb. 80 Konfiguration - Targets - **ESXi-Zugang ändern**

2. Klicken Sie auf den Button **Zugangs-Clients-Einstellungen**, um die Standard-Target-Fenster-Einstellungen anzuzeigen (siehe Abschnitt 8.1, Seite 87).
3. Wenn Sie eine dieser Einstellungen überschreiben möchten, aktivieren Sie das Kontrollkästchen „Spezifische Target-Fenster-Einstellungen“.
4. Aktivieren/Deaktivieren Sie die Checkboxes nach Ihren Wünschen.
5. Klicken Sie auf **Speichern**.

6.4.2.2 Konfigurierte Zugänge löschen

1. Um einen Zugang zu löschen, klicken Sie auf das Mülleimer-Symbol  in der Zeile des Zugangs.
2. Eine Bestätigungsmeldung erscheint. Klicken Sie auf **OK**.

 Ein KVM-Zugang kann nicht gelöscht werden. Löschen des letzten Zugangs löscht das Target.

6.4.3 Bekannte Einschränkungen bei den Targets

Im Vergleich zu typischen KVM-Client-Sessions gibt es einige bekannte Einschränkungen hinsichtlich der Funktionsweise von Target-Zugangs-Sessions.

- Beim Öffnen einer Sitzung stehen für KVM und VNC die Optionen „Open in new“ und „Open in currant“ zur Verfügung, für RDP und SSH jedoch nicht. Diese unterstützen lediglich die Option „Open in new“.
- VNC: Nur die RFB-Protokollversionen 3.3 bis 3.8 werden unterstützt. Proprietäre Erweiterungen und Versionen werden nicht unterstützt, z.B.:
 - RealVNC Protokollversion 4.x und 5.x
 - TightVNC Authentifizierung
 - UltraVNC Authentifizierung
 - Verbindungen über TLS, die proprietär sind für einige VNC-Server
- Wenn RDP-Verbindungen zu Windows-Targets fehlschlagen, prüfen Sie folgende Einstellungen:
 - Öffnen Sie das „Edit Group Policy“ Tool über die Systemsteuerung oder über den Windows Suchdialog (Windowstaste + R, tippen Sie dann gpedit.msc ein).
 - Navigieren Sie zu: **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment**.
 - Deaktivieren Sie die Option „Für alle Remotedesktopdienste-Sitzungen den standardmäßigen Hardware-Grafikadapter verwenden“
- Der integrierte Browser der Draco User Station unterstützt nicht:
 - Java Applets oder Flash
 - Pop-ups
 - Auto-fill
 - Passwort-Erinnerung
 - Langzeit-Cookies

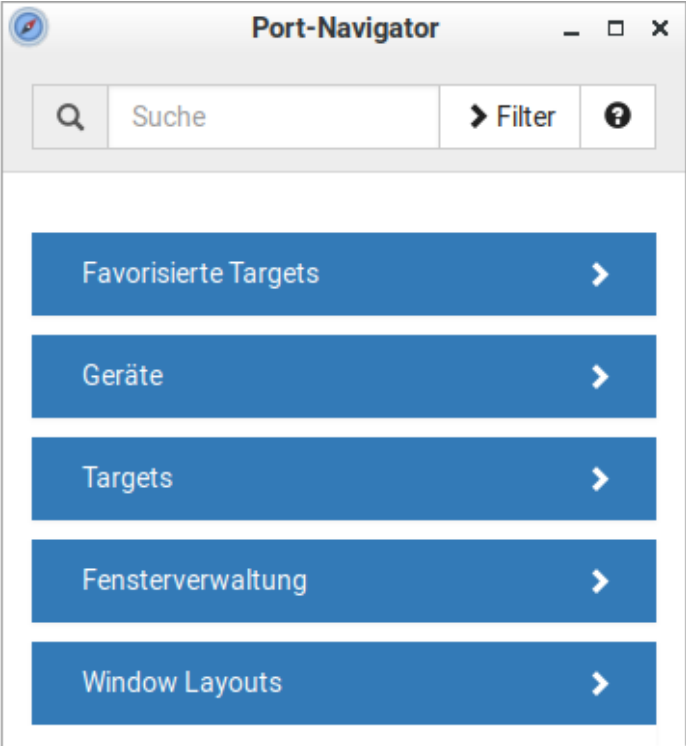
 Für eine optimierte Webunterstützung verwenden Sie den Firefox-Webbrowser.

- Der RDP-Client unterstützt weder virtuelle Medien noch SmartCard-Authentifizierung und andere USB-Geräte.
- Wenn das RDP-Target im Fokus ist, lässt sich die Draco User Station nicht durch kurzes Drücken der Ein-/Aus-Taste ausschalten. Sie müssen den RDP-Client entweder minimieren oder in den Hintergrund verschieben, um die User Station auszuschalten. Ist jedoch die Option „Alle Tastatur- und Ein-/Aus-Tastenergebnisse erfassen“ in den Client-Zugriffseinstellungen deaktiviert, ändert sich dieses Verhalten.

7 Navigation und Zugang

7.1 Der Port-Navigator

Der Port-Navigator wird standardmäßig angezeigt. Wenn nicht, können Sie ihn öffnen durch Klicken von **Strg+Alt+N** oder durch Klicken auf **Hauptmenü > Port-Navigator**.



Der Port-Navigator enthält drei Menüs für den Zugriff auf Ihre Ports und andere Ziele:

- Favorisierte Targets
- Geräte
- Targets

Und zwei Menüs für das Verwalten der Client-Fenster:

- Fensterverwaltung
- Window Layouts

Der Navigator speichert das zuletzt geöffnete Menü und zeigt dieses wieder an, wenn der Navigator erneut geöffnet wird.

Abb. 81 Port-Navigator

Bereich	Beschreibung
Favorisierte Targets	Enthält eine Liste aller Targets, die als favorisiert gekennzeichnet wurden (siehe Abschnitt 6.2, Seite 59).
Geräte	Enthält eine Liste aller SIRA-Geräte.
Targets	Enthält eine Liste aller Targets. Targets mit KVM-Zugang zeigen auch den Port-Status an.
Fensterverwaltung	Offene Sessions mit Fensterverwaltungstools verwalten (siehe Abschnitt 5.2.5, Seite 21).
Window Layouts	Auf gespeicherte Layouts zugreifen (siehe Abschnitt 5.2.6, Seite 22).

7.1.1 Suchfunktion

Über das Suchfeld können Sie nach Geräten oder Ports suchen, die dem Suchbegriff des Benutzers entsprechen.

- Öffnen Sie das Menü, in dem Sie suchen wollen.
 - Um nach einem Gerät zu suchen, klicken Sie auf **Geräte**. Um zusätzlich zu einem Gerät auch nach KVM-Ports eines bestimmten Geräts zu suchen, klicken Sie auf das gewünschte Gerät, damit dessen Ports angezeigt werden, bevor Sie die Suchfunktion nutzen.
Hinweis: Die User Station durchsucht keine Ports von Geräten, die nicht ausgewählt sind.
 - Um nur nach einem Port zu suchen, klicken Sie auf **Targets**.
 - Um nach einem favorisierten Target zu suchen, klicken Sie auf **Favorisierte Targets**.
- Geben Sie den Suchbegriff bzw. die Suchbegriffe in das Suchfeld ein. Bei der Eingabe wird die Groß-/Kleinschreibung nicht berücksichtigt.
- Das derzeit geöffnete Menü zeigt sofort die Suchergebnisse an.

7.1.2 Filterfunktion

Standardmäßig zeigt der Port-Navigator nur Geräte an, mit denen die Kommunikation problemlos funktioniert und die Ports und Targets aktiv sind. Sie können die Anzeigekriterien mithilfe von Filtern ändern.

- Klicken Sie auf **Filter**. Die folgenden Checkboxes erscheinen:

Bezeichnung	Checkbox	Gerätestatus
Geräte-Konnektivität	☒ Normal	Das Gerät kann mit der User Station kommunizieren und der Gerätestatus ist normal.
	☐ Fehler	Das Gerät kann nicht mit der User Station kommunizieren.
	☒ Unbekannt	Das Gerät kann mit der User Station kommunizieren, aber seinen Status nicht bestimmen.
Target- und Port-Status -Verfügbarkeit	☒ Verfügbar und ungenutzt	Der Port ist aktiv und adressierbar, aber es sind keine Sessions offen.
	☒ Verfügbar und verbunden	Der Port oder das Target sind aktiv und es ist mindestens eine Session offen.
	☒ Verfügbar und belegt	Der Port oder das Target sind aktiv und beschäftigt mit einer exklusiven Session.
	☐ Nicht verfügbar	Der Port ist nicht aktiv.
Target-Zugangstyp	☒ KVM ☒ Ser ☒ VNC ☒ RDP ☒ SSH ☒ WEB ☒ ESXi	

- Aktivieren oder deaktivieren Sie die entsprechenden Kontrollkästchen, um festzulegen, was angezeigt werden soll.
- Deaktivieren Sie die Target-Zugangstypen, die Sie nicht benötigen.
- Klicken Sie wieder auf **Filter**, um die Checkboxes zu schließen.

7.1.3 Geräte- und Portstatus identifizieren

Im Port-Navigator-Fenster werden verschiedene Symbole und Farben verwendet, um den aktuellen Status der hinzugefügten Geräte und Ports anzuzeigen.

Informationen zu den Symbolen und Farben erhalten Sie durch Klicken auf das Fragezeichen-Symbol. .

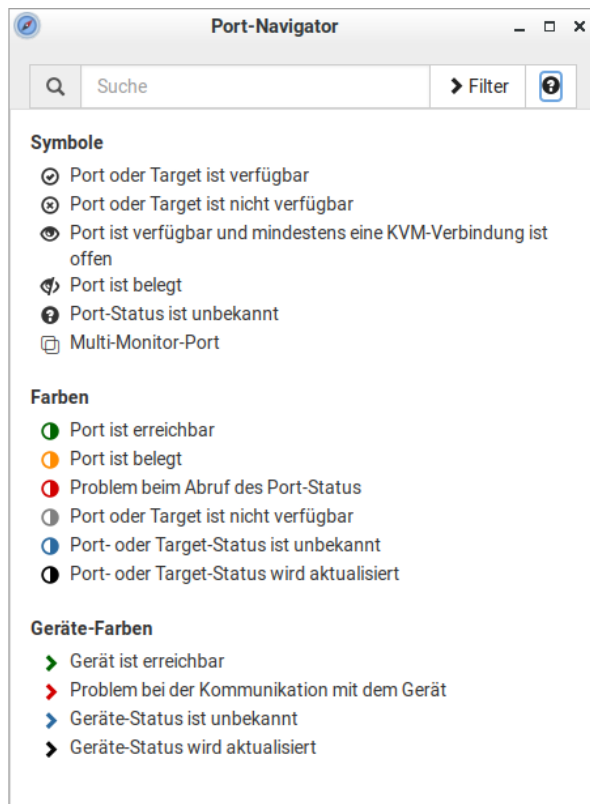


Abb. 82 Port-Navigator - Erklärung der Symbole und Farben

Portstatus bei Dual Video

Der primäre Port muss den Status „Up“ aufweisen, damit eine Verbindung zu beiden Ports hergestellt werden kann. Da keine direkte Verbindung zum sekundären Port hergestellt werden kann, wird dessen Status im Navigator nicht angezeigt.

Wenn der sekundäre Port den Status „Down“ aufweist, besteht dennoch eine Dual-Monitor-Verbindung zu beiden Ports. Auf dem sekundären Client wird entweder die Meldung „Kein Bild“ oder eine Fehlermeldung wie „Wechsel zum Port nicht möglich“ angezeigt.

7.1.4 Externe Medien identifizieren

Wenn externe Medien über virtuelle Medien an einen Port angeschlossen werden, werden die Mediensymbole hinter dem Namen bzw. der Nummer des Ports angezeigt.

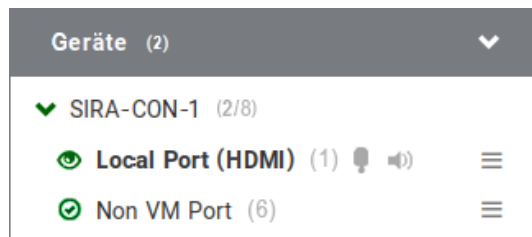


Abb. 83 Port-Navigator - **Geräte-Menü** - Port mit Mediensymbolen

Symbol	Beschreibung
	Massenspeicher
	ISO/CD-Gerät
	Mikrofon
	Lautsprecher
	SmartCard-Lesegerät

7.1.5 Zugriff auf Geräte und Ports über das Geräte-Menü

1. Klicken Sie auf **Geräte**. Das Menü wird geöffnet und eine Liste aller Geräte angezeigt.

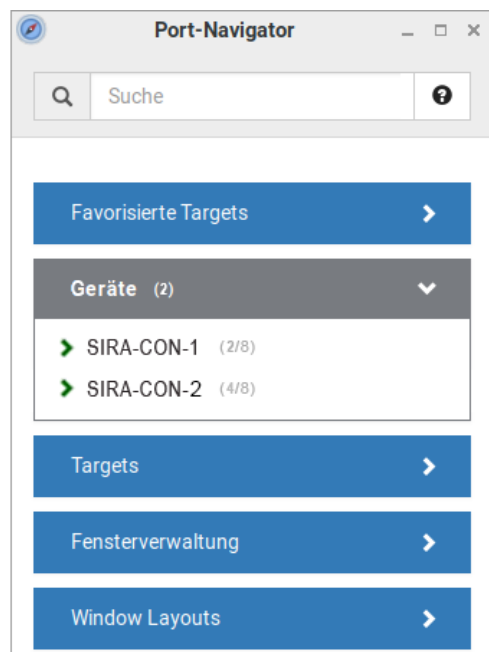


Abb. 84 Port-Navigator - **Geräte-Menü geöffnet**

2. Klicken Sie auf ein Gerät, um die Ports dieses Geräts anzuzeigen.



Abb. 85 Port-Navigator - **Ports des ausgewählten Geräts**

Standardmäßig wird unter dem ausgewählten Gerät nur eine Liste der aktiven (up) Ports angezeigt. Bei Dual-Video mit zwei Ports muss nur der primäre Port aktiv sein, damit es angezeigt wird.

- Die Zahlen in Klammern geben die physischen Portnummern am KVM-/seriellen Switch an.
- Bei Dual-Port-Video werden der primäre und der sekundäre physische Port in Klammern angegeben.

☒ Um Port anzuzeigen, die nicht aktiv (down) sind siehe Abschnitt 7.1.2, Seite 79.

3. Klicken Sie auf das Symbol des gewünschten Ports und wählen Sie entweder *Open in new KVM client* oder *Open in current KVM client* oder

Klicken Sie auf den Portnamen:

- Einzelklicken öffnet die Verbindung im aktuellen KVM-Client-Fenster.
- Doppelklicken öffnet die Verbindung in einem neuen KVM-Client-Fenster
- Rechtsklicken zeigt die Optionen des KVM-Clients an.

Die Anzahl der verbundenen Sessions wird neben dem Gerätenamen angezeigt. Beispiel: Wenn 8 Ports verfügbar sind, von denen 4 belegt sind, lautet die Anzeige „<Gerätename> (4/8)“.

7.1.6 Auf Targets zugreifen

1. Klicken Sie auf **Targets**. Eine Liste aller Targets wird angezeigt. Targets mit KVM-Zugang zeigen auch den Portstatus an.

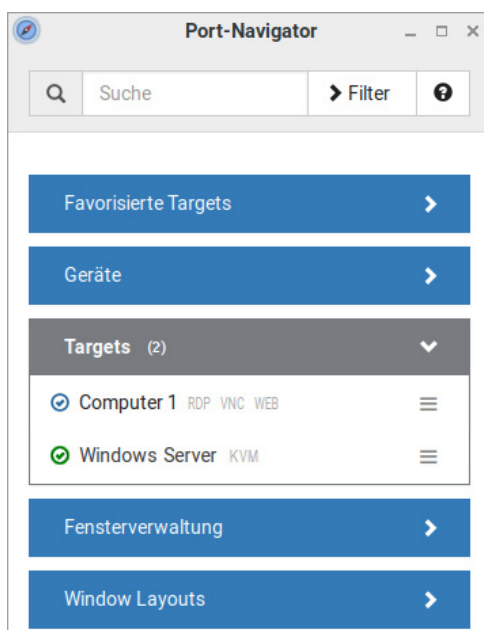


Abb. 86 Port-Navigator - **Target-Menü geöffnet**

2. Klicken Sie auf einen Target-Namen, um den entsprechenden Client zu öffnen. Sind mehrere Zugangspunkte definiert, gilt die folgende Hierarchie für die Auswahl des zu verwendenden Zugangstyps.

M-KVM, KVM, SER, RDP, VNC, SSH, WEB, ESXi

3. Neben dem Target-Namen werden alle konfigurierten Zugangsmethoden aufgelistet. Klicken Sie direkt auf die Zugangsmethode, um den entsprechenden Client zu öffnen. Sind mehrere Zugangspunkte desselben Typs definiert, wird der zuletzt hinzugefügte geöffnet.
4. Rechtsklicken Sie auf den Target-Namen oder klicken Sie auf das Symbol , um alle Zugangsmethoden für dieses Target anzuzeigen.

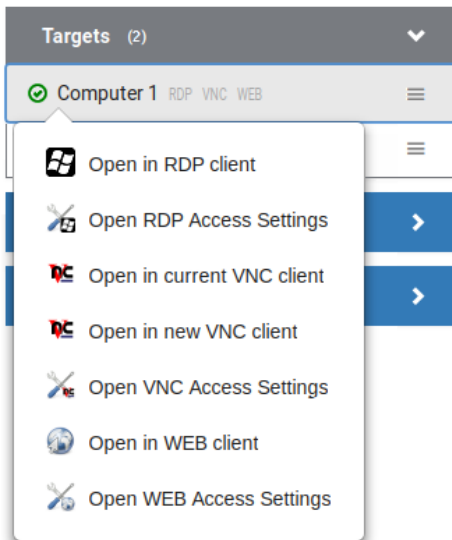


Abb. 87 Port-Navigator - **Zugangsmethoden für dieses Target**

5. Klicken Sie auf den gewünschten Eintrag. Wenn Sie auf einen "Open xx Access Settings" Eintrag klicken, öffnet sich das Konfigurationsmenü für diese Zugangsmethode (siehe Abschnitt 6.4.2, Seite 71).

 Wenn für KVM- oder VNC-Targets ein zweiter oder dritter Monitor verfügbar ist, können Sie das Target wahlweise auf dem zweiten oder dritten Monitor öffnen. Außerdem finden Sie im Kontextmenü den Eintrag „Port-Einstellungen öffnen“, über den Sie direkt zur Konfiguration des Ports gelangen. Bei Dual-Port-Videokarten wird anstelle der Portnamen der Name der Dual-Port-Videogruppe angezeigt. Dual-Port-Gruppen, deren primärer Port aktiv ist, werden in der Liste angezeigt.

7.1.7 Fensterverwaltung und Fensteranordnungen (Layouts)

- ➔ Verwalten offener Sessions mit Fensterverwaltungstool (siehe Abschnitt 5.2.5, Seite 21).
- ➔ Layouts speichern und auf gespeicherte Layouts zugreifen (siehe Abschnitt 5.2.6, Seite 22).

7.2 Der Port-Scanner

Der Port-Scanner zeigt eine Auswahl von Ports an, die Sie festlegen, indem er jede Verbindung über einen bestimmten Zeitraum hinweg scannt. Sie können eine KVM-Verbindung zu jedem im Scanner angezeigten Port herstellen. Der Port-Scanner kann zudem Target-Snapshots auf einem externen USB-Gerät speichern, sofern diese Funktion aktiviert ist. Dies ist für forensische oder Überwachungszwecke nützlich. Einzelheiten zur Konfiguration und zu den Benutzerrechten finden Sie im Abschnitt 9.2.1.1, Seite 111.

Ports werden einbezogen, indem bei der Konfiguration des Ports die Einstellung "Include in Port Scanner" aktiviert wird (siehe Abschnitt 6.2, Seite 59).

Protokoll-Einträge werden für jeden einzelnen gescannten Port oder zu Beginn und am Ende der Scan-Sitzung erstellt. Die Funktionen zur Fensterverwaltung gelten nicht für das Fenster „Port-Scanner“.

7.2.1 Port-Scanner konfigurieren

1. Klicken Sie auf **Hauptmenü > Port-Scanner**.

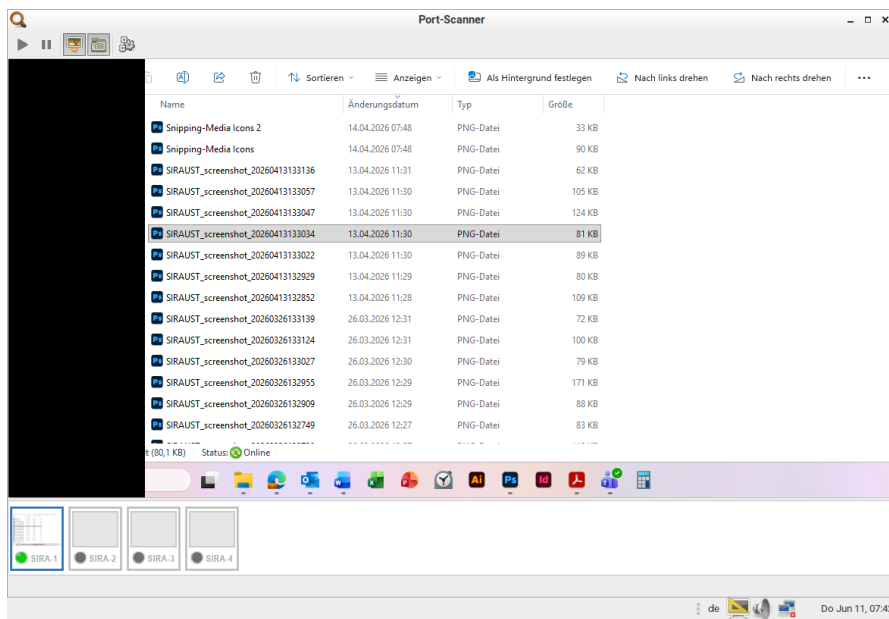


Abb. 88 Port-Scanner-Fenster

2. Klicken Sie auf das Symbol , um das Konfigurationsfenster für den Port-Scanner zu öffnen.

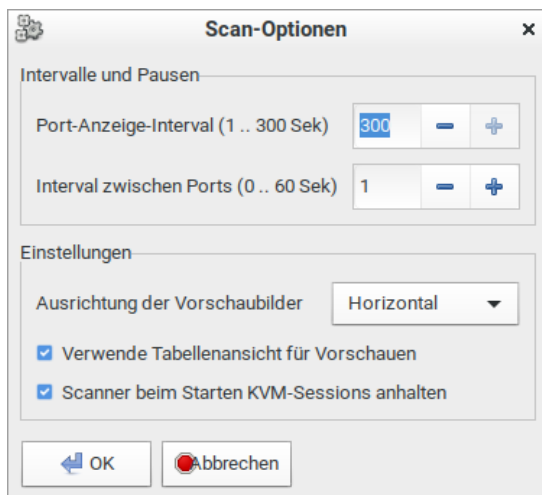


Abb. 89 Port-Scanner - Scan-Optionen

3. Konfigurieren Sie die „Intervalle und Pausen“.

- 3.1. Port-Anzeige-Interval: Wählen Sie hier die Anzahl an Sekunden, die jeder Port angezeigt wird, bevor zum nächsten geschaltet wird.
- 3.2. Interval zwischen Ports: Wählen Sie die Anzahl der Sekunden, die pausiert wird, bevor zum nächsten Port geschaltet wird.

4. Konfigurieren Sie die „Einstellungen“:

- 4.1. Ausrichtung der Vorschaubilder: Wählen Sie hier, ob Sie die Vorschaubilder in einer Zeile unten dargestellt haben möchten (horizontal) oder in einer Spalte am rechten Rand (vertikal).
- 4.2. Verwende Tabellenansicht für Vorschauen: Aktivieren Sie diese Checkbox, um die Tabellenansicht zu aktivieren (siehe Abschnitt 7.2.3, Seite 86).
- 4.3. Scanner beim Starten KVM-Sessions anhalten: Aktivieren Sie diese Checkbox, wenn der Scanvorgang beendet werden soll, wenn Sie über einen Port eine vollständige KVM-Session öffnen.

5. Klicken Sie auf **OK**.

7.2.2 Arbeiten mit dem Port Scanner

Die Symbole in der Toolbar haben die folgende Bedeutung:

Symbol	Beschreibung
	Scanvorgang starten bzw. wieder aufnehmen.
	Scanvorgang pausieren.
	Anzeigen oder ausblenden des Vorschaubildes (live Video).
	Anzeigen oder ausblenden der Vorschaubilder
	Öffnen der Scanner-Optionen für die Konfiguration.

Die Vorschau zeigt alle Ports, die für den Port-Scanner ausgewählt wurden. Der gerade angezeigte Port ist im Vorschaubereich hervorgehoben.

1. Klicken Sie einmal auf ein Vorschaubild, um eine Vorschau des Ports im Scanner anzuzeigen.
2. Doppelklicken Sie auf ein Vorschaubild, um eine KVM-Session an diesem Port zu öffnen.

 Die Standardaktion bei einem Doppelklick kann unter „Start-Einstellungen“ konfiguriert werden (siehe Abschnitt 8.1, ab Seite 87).

3. Klicken Sie mit der rechten Maustaste auf ein Vorschaubild, um ein Menü mit weiteren Optionen zu öffnen.

Open in new KVM client
Open in current KVM client
Continue Scan with port Linux-50-140-1
Remove from Scanner
Temporarily Remove from Scanner

Abb. 90 Port-Scanner - **Untermenü der Vorschaubilder**

Eintrag	Beschreibung
Open in new KVM client	Startet eine KVM-Session in einem neuen Fenster.
Open in current KVM client	Startet eine KVM-Session im aktuellen Fenster.
Continue Scan with port <port name>	Startet scannen des ausgewählten Ports.
Remove from scanner	Deaktiviert die Einstellung „Beinhaltet im Port-Scanner“ für den Port.
Temporarily remove from Scanner	Der Port wird für diesen Scanvorgang nicht berücksichtigt; im nächsten ist er dann wieder dabei.

7.2.3 Port-Scanner Tabellenansicht

Der Port-Scanner der User Station bietet eine „Tabellen“- oder „Matrix“-Ansicht für Ports verschiedener Geräte. Die Tabellenansicht zeigt mehrere Vorschaubilder in einer Zeilen-/Spaltenansicht gleichzeitig und ohne Scrollen an. Die Anzahl der Ports ist unbegrenzt, kann je nach Bedarf variieren, und alle Ports sind in der Tabellenansicht sichtbar. Die Tabellenansicht des Port-Scanners kann Ports von mehr als einem SIRA-Gerät anzeigen. Die Vorschaubilder werden automatisch in ihrer Größe angepasst und so angeordnet, dass alle Ports im Port-Scanner sichtbar sind.

 Die Miniaturansichten in der Tabellenansicht werden regelmäßig aktualisiert. Aufgrund technischer Einschränkungen bei der Rechenleistung und den Grafikressourcen sind in der Rasteransicht keine Live-Aktualisierungen möglich.

Wie die Rasteransicht funktioniert

- Der Bereich mit den Vorschaubildern kann optional als Tabellenansicht dargestellt werden, in der alle Vorschaubilder auf einmal ohne Scrollbalken angezeigt werden.
- Größe und Position der Vorschaubilder passen sich automatisch an die Größe des Bereichs an bzw. werden optimal angepasst.
- Der Bereich mit den Vorschaubildern kann auf Wunsch den gesamten Platz einnehmen; der Bereich mit der Live-Vorschau kann ausgeblendet werden.

8 Benutzervoreinstellungen

- ➔ Klicken Sie im Fenster User-Station-Konfiguration auf **Einstellungen**, um die folgenden Benutzervoreinstellungen anzupassen:



Abb. 91 Menü Einstellungen

8.1 Zugangs-Clienten-Einstellungen

Sie können Einstellungen für alle Zugangstypen sowie allgemeine Start- und Verbindungseinstellungen konfigurieren. Benutzer mit Systemadministratorrechten können Standard-Einstellungen für alle neuen Benutzer konfigurieren.

1. Klicken Sie auf **Einstellungen** im User-Station-Konfigurationsfenster. Die Zugangs-Clienten-Einstellungen-Seite erscheint mit den momentanen Voreinstellungen.
2. Klicken Sie auf **Bearbeiten**, um die folgenden Einstellungen zu ändern.

Video-Target-Fenster-Einstellungen

Diese Einstellungen legen die Anfangseinstellungen fest, die mit dem Zugangs-Clienten auf die Video-Targets angewendet werden.

Video-Target-Fenster-Einstellungen		
Skaliere Video	☐	(KVM, M-KVM, VNC)
Positionierung	☐	Automatisch (KVM, VNC)
Fensterdekorationen	☒	(KVM, M-KVM, VNC, RDP, ESX)
Zeige Werkzeugleiste	☒	(KVM, M-KVM, VNC)
Vollbildmodus	☐	(KVM, M-KVM, VNC, RDP, ESX)
Single-Maus-Cursor-Modus	☐	(KVM, M-KVM)
Synchronisiere Maus	☐	(KVM, M-KVM)
Automatische Videoerkennung	☐	(KVM, M-KVM)
Erlaube Eingaben nur wenn fokussiert	☐	(KVM, M-KVM, VNC)
Fange alle Tastatur- und Einschalter-Er...	☒	(RDP)
Auf aktuellen Monitor beschränken	☐	(KVM, M-KVM, VNC)
Cursor-Form	☐	Standard (KVM, M-KVM, VNC)
Banner-Nachrichten Deaktivieren	☐	(KVM, M-KVM, VNC)
Ändern der Fenstergröße	☐	Feste Größe (RDP)
Übertragungsqualität	☐	Mittel (RDP)
Bevorzugte Auflösung	☐	1024 x 768 (RDP)
Als Multi-Monitor-Target anzeigen	☐	Deaktiviert (RDP)
Desktop-Skalierung	☐	100% (RDP)

Abb. 92 Einstellungen - Zugangs-Clienten-Einstellungen - Video-Target-Fenster-Einstellungen

Parameter	Beschreibung
Skaliere Video	Aktivieren/Deaktivieren der Videoskalierungs-Funktion.
Positionierung	Bestimmt, wo das Client-Fenster auf dem Bildschirm erscheint: • Automatisch: Die Position ist nicht festgelegt. Das erste Fenster kann in der linken oberen Ecke sein, das zweite in der unteren rechten. • Linke Obere Ecke • Rechte Obere Ecke Hinweis: Für Dual- oder Multi-KVM-Targets: Wenn mehr als zwei Fenster involviert sind, werden alle Fenster in der linken oberen Ecke gestartet.
Fensterdekoration	Anzeigen oder ausblenden der Fensterdekoration.
Zeige Werkzeugleiste	Anzeigen oder ausblenden der Client-Symbolleiste
Vollbildmodus	Aktivieren/Deaktivieren des Vollbildmodus für KVM, M-KVM, VNC, RDP und ESXi Sessions.
Single-Maus-Cursor-Modus	Hinweis: Wenn diese Einstellung aktiviert ist, müssen Sie zu Beginn der Sitzung in das KVM-Fenster klicken, um die Maus zu lokalisieren. Für Dual-Monitor-Targets: Der KVM-Client oben links wird in den Vordergrund geholt (anstelle des primären), da dieser die Maus steuert.
Synchronisiere Maus	Wenn diese Option aktiviert ist, wird die Maus beim Herstellen einer Verbindung zu KVM- und M-KVM-Zielen automatisch synchronisiert, sofern der Mausmodus auf „Intelligent“ oder „Standard“ eingestellt ist. Hinweis: Wenn Sie über die die Symbolleiste in den Einzelm Mausmodus wechseln, gibt es die Option „Synchronize Mouse after leaving Single Cursor mode“, die für KVM- und M-KVM-Ziele gilt, die den intelligenten oder Standard-Mausmodus verwenden.
Automatische Video-erkennung	Wenn diese Option aktiviert ist, führt das KVM-Target automatisch eine Erkennung durch, sobald der KVM-Client eine Verbindung herstellt.
Erlaube Eingaben nur wenn fokussiert	Wenn diese Option aktiviert ist, sind Mauseingaben auf KVM-, M-KVM- und VNC-Zielen nur zulässig, wenn das Client-Fenster im Fokus ist.
Fange alle Tastatur- und Einschalt-Ereignisse ein	Wählen Sie diese Option aus, um alle Tastatureingaben (einschließlich des Netzschalters und anderer Tastenkombinationen) vom lokalen Betriebssystem zu erfassen.
Auf aktuellen Monitor beschränken	Wählen Sie diese Option aus, um die KVM-, M-KVM- und VNC-Targets auf den aktuellen Monitor zu beschränken.
Cursor-Form	Individuelle Cursorform auswählen. • Zur Verfügung stehen: Standard, Punkt, Fadenkreuz, Transparent • Nutzen Sie die Option transparent, um den Mauscursor auszublenden.
Banner-Nachrichten deaktivieren	Wählen Sie diese Option aus, um Banner-Meldungen aus KVM-, M-KVM- und VNC-Sitzungen zu entfernen.
Ändern der Fenstergröße	Wählen Sie die Art der Größenanpassung für RDP-Sessions aus. • Zur Auswahl stehen: Feste Größe, Dynamische Auflösungsänderung, Skalieren
Übertragungsqualität	Wählen Sie die gewünschte Übertragungsqualität für RDP-Sitzungen aus: • Zur Auswahl stehen: Beste Qualität (Langsam), Mittel, Schnell (Niedrige Qualität).
Bevorzugte Auflösung	Wählen Sie die gewünschte Auflösung für RDP-Sessions aus.

Als Multi-Monitor Target anzeigen	Wählen Sie die Multi-Monitor-Voreinstellung für RDP-Sessions aus. Zur Auswahl stehen: Deaktiviert, Benutze 2 Monitore, Benutze 3 Monitore, Benutze 4 Monitore und Benutze alle Monitore
Desktop-Skalierung	Wählen Sie einen Skalierungsprozentsatz für den Desktop für RDP-Sitzungen aus.

Konsolenfenster-Einstellungen

Diese Optionen gelten für SSH und seriellen Zugang.

Konsolenfenster-Einstellungen	
Fensterdekorationen	☒ (SSH, Ser)
Zeige Menüleiste	☒ (SSH)
Vollbildmodus	☐ (SSH, Ser)
Konsolengröße	80 x 24 (SSH, Ser)

Abb. 93 Einstellungen - Zugangs-Clients-Einstellungen - **Konsolenfenster-Einstellungen**

Parameter	Beschreibung
Fensterdekorationen	Anzeigen oder ausblenden der Fensterdekorationen.
Zeige Menüleiste	Anzeigen oder ausblenden der Menüleiste.
Vollbildmodus	Aktivieren oder deaktivieren des Vollbildmodus für Konsolensitzungen. Bei SSH und seriell lautet die Tastenkombination für den Vollbildmodus F11.
Konsolengröße	Wählen Sie die gewünschte Konsolengröße aus. Die angegebene Größe des seriellen Clients ist möglicherweise nicht korrekt.

Web-Target-Fenster-Einstellungen

Web-Target-Fenster-Einstellungen	
Fensterdekorationen	☒ (Web)
Zeige Werkzeugleiste	☒ (Web)
Vollbildmodus	☐ (Web)

Abb. 94 Einstellungen - Zugangs-Clients-Einstellungen - **Web-Target-Fenster-Einstellungen**

Parameter	Beschreibung
Fensterdekorationen	Anzeigen oder ausblenden der Fensterdekorationen.
Zeige Werkzeugleiste	Anzeigen oder ausblenden der Symbolleiste.
Vollbildmodus	Vollbildmodus für Web-Sessions aktivieren oder deaktivieren. Bei Websitzungen ist die Tastenkombination für den Vollbildmodus F11.

Starteinstellungen

Mit diesen Optionen lässt sich das Klickverhalten der Maustasten im Port Navigator konfigurieren.

Starteinstellungen	
Linker Maus-Button-Klick	Bestehenden KVM-Clients umschalten
Maus-Button-Doppelklick	Öffne einen neuen KVM-Clients
Mittlerer Button-Klick	Öffne einen neuen KVM-Clients
Port-Hotkey-Aktion	Bestehenden KVM-Clients umschalten
Mehrere Verbindungen zu einem Target	☐

Abb. 95 Einstellungen - Zugangs-Clients-Einstellungen - **Starteinstellungen**

Mögliche Optionen	Beschreibung
Bestehenden KVM-Clients umschalten	Leitet den zuletzt aktiven Zugangs-Client nach Möglichkeit auf den ausgewählten Port oder Access Point um. Andernfalls wird ein neuer Zugangs-Client geöffnet.
Öffne einen neuen KVM-Clients	Es wird immer ein neuer Zugangs-Client gestartet.
Öffne einen neuen KVM-Clients auf einem zweiten Monitor	Es wird immer ein neuer Zugangs-Client auf dem zweiten Monitor gestartet, sofern dieser verfügbar ist.
Mehrere Sessions für ein Target: Aktiviert	Es wird ein zweites Fenster für das Target geöffnet, wenn: (1) Öffne einen neuen KVM-Clients ausgewählt ist und (2) PC Share für dieses Gerät aktiviert wurde.
Deaktiviert	Deaktiviert den Doppelklick mit der linken Maustaste oder den Klick mit der mittleren Maustaste.

Verbindungseinstellungen

Wird ein KVM-Client auf einen anderen Port umgeschaltet, während eine virtuelle Medienverbindung besteht, wird diese Verbindung beendet. Mit dieser Option können Sie festlegen, ob in diesem Fall eine Warnung angezeigt werden soll.

Verbindungseinstellungen	
Warne bei Trennung von Virtual Media	☐

Abb. 96 Einstellungen - Zugangs-Clients-Einstellungen - **Verbindungseinstellungen**

3. Wenn Sie alles eingestellt haben, klicken Sie auf **Speichern**.

Sobald die Einstellungen konfiguriert und gespeichert wurden, stehen weitere Optionen zur Verfügung.

- ➔ Klicken Sie auf den Button **Als Standard setzen**, um diese Einstellungen als Standardeinstellungen für alle neuen Benutzer und solche, die ihre Einstellungen noch nie geändert haben, zu speichern (System-Administratorrechte sind hierfür nötig).
- ➔ Klicken Sie auf den Button **Setze alle spezifischen Einstellungen zurück**, um alle Target/Port-spezifischen Einstellungen des aktuellen Benutzers zu löschen.

8.2 Tastatur-Makros verwalten

Es können Tastatur-Makros erstellt und gespeichert werden, die anstelle von physischen Tastenkombinationen verwendet werden, sodass die für den Target-Server bestimmten Aktionen ausschließlich an diesen gesendet und nur von ihm interpretiert werden. Andernfalls könnten sie von der User Station selbst interpretiert werden.

8.2.1 Erstellen von Tastatur/Hotkey-Makros

1. Klicken Sie **User-Station-Konfiguration > Einstellungen > Tastatur-Makros**. Die entsprechende Seite erscheint.

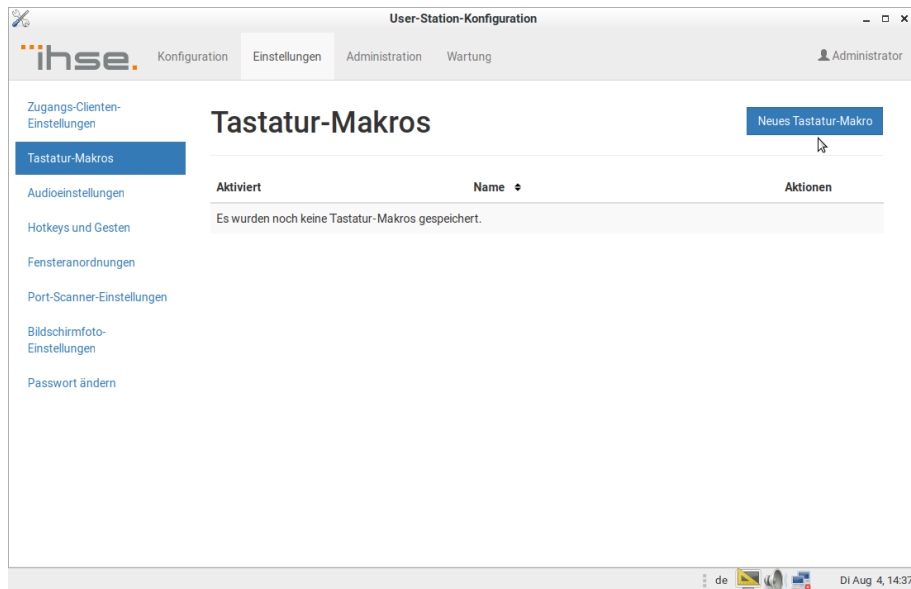


Abb. 97 Einstellungen - Tastatur-Makros

2. Klicken Sie auf den Button **Neues Tastatur-Makro**.

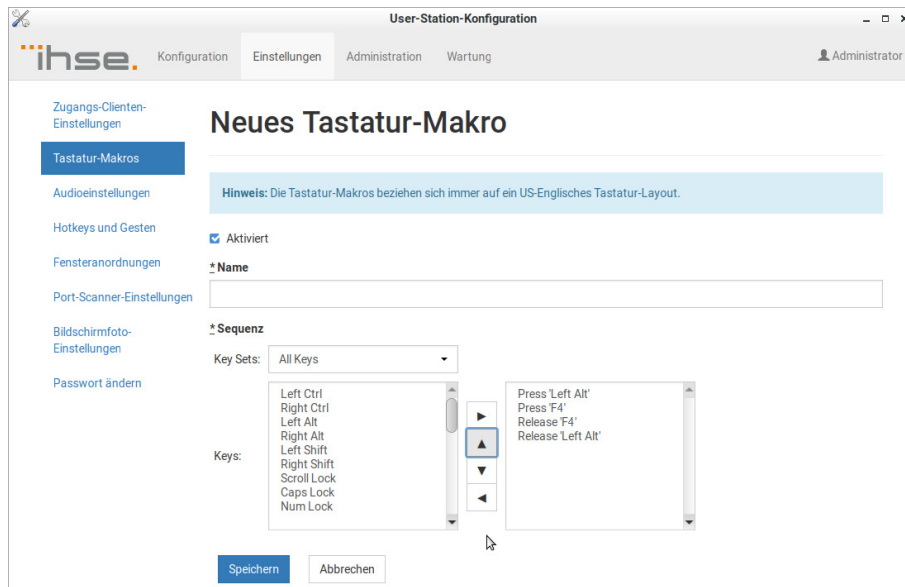


Abb. 98 Einstellungen - Tastatur-Makros - Neues Makro anlegen

3. Aktivieren Sie die Checkbox „Aktiviert“, so dass das neue Makro im KVM-Client der User Station erscheint.
4. Geben Sie einen Namen für das Tastatur-Makro ein. Die Felder, die mit * markiert sind, müssen ausgefüllt werden.
5. Geben Sie eine Sequenz ein.
 - 5.1. Wählen Sie den Tastensatz (z. B. Buchstaben, Zahlen, Symbole, F1–F24 usw.) aus, der die gewünschten Tasten enthält. Alle Tasten des ausgewählten Tastensatzes werden im Feld „Keys“ aufgelistet. Wenn Sie „All keys“ auswählen, werden alle möglichen Tasten aufgelistet.

- 5.2. Klicken Sie auf die gewünschte Taste in der Liste und klicken Sie auf ►, um sie in das rechte Feld zu kopieren oder doppelklicken Sie einfach auf eine Taste. Ein **Release** Tastenbefehl wird automatisch hinzugefügt für jede Taste im rechten Feld.
- 5.3. Um eine Taste aus dem rechten Feld zu löschen, klicken Sie darauf und dann auf ◀.
- 5.4. Um eine Taste im rechten Feld nach oben oder unten zu verschieben, klicken Sie auf ▲ bzw. ▼.
6. Klicken Sie auf **Speichern**. Das neue Makro wird der Liste der Tastatur-Makros auf der Makros-Seite hinzugefügt (siehe nächste Abbildung).

Beispiel

Sie können ein Tastatur-Makro erstellen, um ein Fenster zu schließen mit der Tastenkombination **Links Alt+F4**. Das Makro sieht folgendermaßen aus:

```
Press Left Alt
Press F4
Release F4
Release Left Alt
```

8.2.2 Makros ändern und löschen

1. Um alle erstellten Makros anzuzeigen, klicken Sie auf **Einstellungen > Tastaturmakros**.

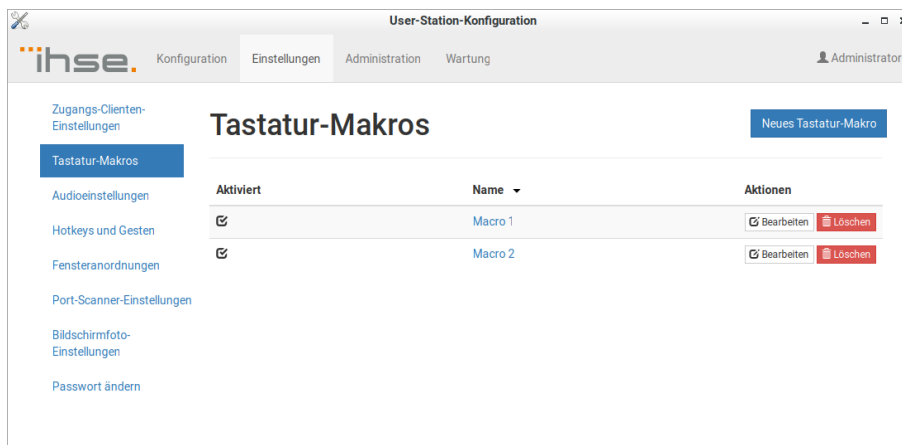


Abb. 99 Einstellungen - Tastatur-Makros - Liste der Makros

Ein aktiviertes Makro wird durch ein angekreuztes Kontrollkästchen in der Spalte „Aktiviert“ angezeigt.

Durch Klicken auf die Spaltenüberschrift „Name“ kann die Namensliste sortiert werden.

Ändern eines Makros

1. Klicken Sie auf den Button **Bearbeiten** (in der Spalte „Aktionen“) in der Zeile des Makros, das Sie ändern wollen.
2. Führen Sie die gewünschten Änderungen beim Namen oder der Sequenz durch und klicken Sie auf **Speichern**.

Löschen eines Makros

1. Klicken Sie auf den Button **Löschen** (in der Spalte „Aktionen“) in der Zeile des Makros, das Sie löschen wollen.
2. Es erscheint eine Aufforderung zur Bestätigung. Klicken Sie auf **OK**.

8.2.3 Makros ausführen

Damit ein Makro ausgeführt werden kann, muss das Kontrollkästchen in der Spalte „Aktiviert“ aktiviert sein.

1. Klicken Sie im KVM-Client-Fenster auf das Symbol  in der Symbolleiste. Eine Liste der aktiven Makros wird angezeigt.

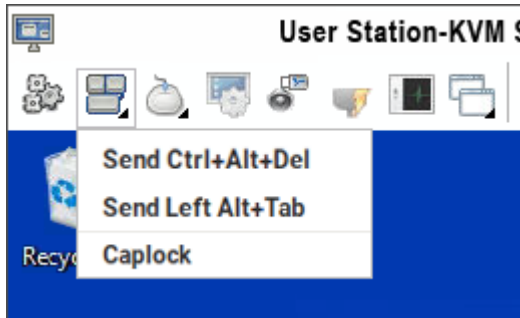


Abb. 100 Client-Fenster - Liste der aktiven Makros

2. Klicken Sie auf das gewünschte Makro, um es an den Target-Server zu senden.

8.3 Audioeinstellungen

Die von der User Station standardmäßig verwendeten Geräte für die Audiowiedergabe und -aufnahme sind die analogen Lautsprecher und das Mikrofon an der Vorderseite.

Sie können dies ändern, indem Sie andere Audiogeräte für die Audiowiedergabe und/oder -aufnahme auswählen.

 Die hier von einem beliebigen Benutzer vorgenommenen Änderungen an der Audiokonfiguration gelten für die jeweilige User Station, sodass sich die Änderungen auf alle Benutzer dieser User Station auswirken.

1. Klicken Sie im User-Station-Konfigurations-Fenster auf **Einstellungen** und dann auf **Audioeinstellungen**. Die Audio Settings Seite erscheint mit den aktuellen Audiowiedergabe- und Aufnahmeeinheiten.

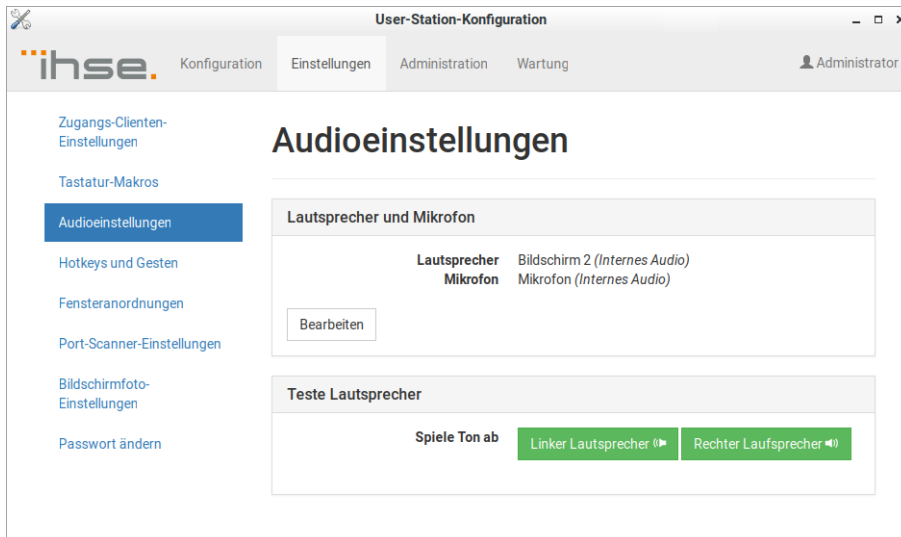


Abb. 101 Einstellungen - Audioeinstellungen

2. Klicken Sie auf den Button **Bearbeiten**, um die Einstellungen zu ändern.

Audioeinstellungen bearbeiten

Lautsprecher

☒  Bildschirm 2
Internes Audio

☐  Bildschirm 3
Internes Audio

☐  Bildschirm 4
Internes Audio

☐  Bildschirm 1
Internes Audio

☐  Lautsprecher / Kopfhörer
Internes Audio

Mikrofon

☒  Mikrofon
Internes Audio

☐  Lautsprecher

☐  Headset

☐  Mikrofon

☐  Kein Audiogerät angeschlossen

Abb. 102 Einstellungen - **Audioeinstellungen bearbeiten**

- Wählen Sie im Abschnitt „Lautsprecher“ das gewünschte Audiowiedergabegerät aus. Nicht verfügbare Audiowiedergabegeräte sind mit dem Symbol  gekennzeichnet.
- Wählen Sie im Abschnitt „Mikrofon“ das gewünschte Audioaufnahmegerät aus.
- Klicken Sie auf **Speichern**.
- Um zu prüfen, ob die aktuell ausgewählten Lautsprecher funktionieren, klicken Sie auf die Schaltflächen **Linker Lautsprecher** und **Rechter Lautsprecher**.

8.4 Hotkeys und Gesten

Sie können Hotkeys und Gesten aktivieren, deaktivieren und anpassen, um die User Station zu steuern, Fenster zu verwalten oder KVM-Client-Funktionen zu bedienen. Diese Hotkeys und Gesten werden auf der User Station ausgeführt und nicht an die von Ihnen betriebenen Target-Server übertragen. Sie können die Einstellungen des aktuellen Benutzers auf alle neuen Benutzer oder auf diejenigen Benutzer anwenden, die noch keine Hotkey-Einstellungen festgelegt haben, indem Sie auf **Als Standard setzen** klicken.

☒ Viele Funktionen sind standardmäßig programmiert und aktiviert.

Eine komplette Liste aller vorprogrammierter Hotkeys der User Station finden Sie unter **Hauptmenü > Hilfe > Hilfe für Hotkeys** (siehe Abschnitt 5.2.7.2, Seite 23).

Es gibt mehrere Kategorien von Hotkeys und Gesten:

Hotkeys für Funktionen der User Station

Hotkeys für Funktionen der User Station	
Port-Navigator	Strg+Alt+N
User-Station-Konfiguration	Strg+Alt+C
Port-Scanner	Deaktiviert
Client-Fenster Kacheln	Deaktiviert
Kacheln rückgängig machen	Deaktiviert
Client-Fenster Minimieren	Deaktiviert
Client-Fenster Wiederherstellen	Deaktiviert
Client-Fenster Schließen	Deaktiviert
Bildschirmfoto Desktop	Druck
Bildschirmfoto Aktives Fenster	Strg+Druck
Bildschirm Sperren	Strg+Alt+L
Herunterfahren	Strg+Alt+Entf
Neue Fensteranordnung	Deaktiviert
Fensteranordnung Überschreiben	Deaktiviert
Monitor-Einstellungen Wiederherstellen	Deaktiviert

Abb. 103 Einstellungen - Hotkeys und Gesten - **Funktionen der User Station**

Diese Hotkeys werden stets lokal vom Desktop der User Station verarbeitet. Sie werden nicht an einen Target-Server gesendet, wenn Sie sie innerhalb einer KVM-Session verwenden. Wenn Sie einen dieser Hotkeys, wie beispielsweise **Alt+Tab** oder **Strg+Alt+Entf**, in KVM-Sessions verwenden möchten, müssen Sie sicherstellen, dass dieser Hotkey nicht in dieser Kategorie zugewiesen ist, oder die Funktion deaktivieren, der er zugewiesen ist.

Hotkeys for Fensterverwaltung

Hotkeys und Gesten für Fensterverwaltung	
Fenster Schließen	Alt+F4
Nächstes Fenster	Alt+Tab
Letztes Fenster	Umschalt+Alt+Tab
Wechseltasten	☒
Bewegungstasten	☒
Ziehen mit Alt-Taste	☒
Fokus folgt der Maus	☐

Abb. 104 Einstellungen - Hotkeys und Gesten - **Fensterverwaltung**

Sie können Hotkeys konfigurieren, um Fenster zu schließen, zwischen Fenstern zu wechseln oder sie auf dem Desktop zu verschieben.

Option	Beschreibung
Wechseltasten	Wenn aktiviert, können Sie Umschalt+Windows+<Pfeiltaste> verwenden, um zwischen offenen Fenstern umzuschalten.
Bewegungstasten	Mit den Bewegungstasten (siehe Tabelle unten) können Sie das Fenster im Vordergrund auf dem Desktop verschieben. Sie können diese Funktion deaktivieren.
Ziehen mit Alt-Taste	Wenn diese Option aktiviert ist, können Sie Fenster auf dem Desktop der Draco SIRA User Station mit der Maus verschieben. Deaktivieren Sie diese Funktion, wenn Sie möchten, dass „Alt-Drag“ auf den Target-Server angewendet wird.
Fokus folgt der Maus	Wenn diese Funktion aktiviert ist, ermöglicht sie eine nahtlose Mausreaktion im Fenster, über dem sich der Mauszeiger befindet.

Hotkeys für **Bewegungstasten**

Hotkey	Funktion
Strg+Alt+ ↑	Verschiebt das Fenster auf dem Monitor in die angegebene Richtung an den Bildschirmrand.
Strg+Alt+ ↓	
Strl+Alt+ ←	
Strg+Alt+ →	
Strg+Alt+1 (des Zahlenfelds)	Verschiebt das Fenster auf dem Monitor in die angegebene Richtung in die Ecke des Bildschirms.
Strg+Alt+3 (des Zahlenfelds)	
Strg+Alt+5 (des Zahlenfelds)	
Strg+Alt+7 (des Zahlenfelds)	
Strg+Shift+ ↑	Verschiebt das Fenster in die angegebene Richtung, bis sein Rand die nächstgelegene Kante berührt, die eine der folgenden ist: • Kante eines anderen Fensters • Monitorkanten in einer Dual-Monitor Konfiguration • Rand des Desktops
Strg+Shift+ ↓	
Strg+Shift+ ←	
Strg+Shift+ →	
Strg+Window+ ↑	Vergrößert das Fenster in die angegebene Richtung, bis sein Rand die nächstgelegene Kante berührt, die eine der folgenden ist: • Kante eines anderen Fensters • Monitorkanten in einer Dual-Monitor-Konfiguration • Rand des Desktops
Strg+Window+ ↓	
Strg+Window+ ←	
Strg+Window+ →	
	Hinweis: Wenn der Fensterrand bereits am Bildschirmrand anliegt, wird stattdessen die Fenstergröße verkleinert

KVM-Client-Hotkeys

KVM-Client-Hotkeys	
Single-Maus-Cursor-Modus	Strg+Alt+M
Vollbildmodus	Strg+Alt+F
Synchronisiere Maus	Deaktiviert
Automatische Videoerkennung	Deaktiviert

Abb. 105 Einstellungen - Hotkeys und Gesten - **KVM Client Hotkeys**

Sie können im KVM-Client Tastenkombinationen für bestimmte Funktionen konfigurieren. Beachten Sie: Wenn Sie die Tastenkombination für den Single-Mausmodus deaktivieren, wird diese Funktion deaktiviert.

Hotkeys für KVM und serielle Ports, Target-Zugang und Fensteranordnungen

KVM- und Serielle Port-Hotkeys

Port-Name	SIRA-Gerät
Es sind zur Zeit keine Port-Hotkeys definiert.	

Target-Zugangs-Hotkeys

Zugang	Target
Es sind zur Zeit keine Target-Zugangs-Hotkeys definiert.	

Fensteranordnungs-Hotkeys

Fensteranordnung
Es sind zur Zeit keine Fensteranordnungs-Hotkeys definiert.

Bearbeiten

Als Standard Setzen

Abb. 106 Einstellungen - Hotkeys und Gesten - Hotkeys für Ports, Target-Zugang und Fensteranordnungen

Sie können Hotkeys für KVM- und serielle Ports, den Zugriff auf Target-Systeme sowie Fensteranordnungen (Window Layouts) konfigurieren (siehe Abschnitt 6.4.2.1, Seite 71).

HotKeys und Gesten konfigurieren

- Klicken Sie auf **Hauptmenü > User-Konfiguration > Einstellungen > Hotkeys und Gesten**. Die Seite „Hotkeys und Gesten“ wird geöffnet und zeigt die aktuellen Einstellungen aller Kategorien an (wie oben und auf den vorherigen Seiten dargestellt)).
- Klicken Sie auf **Bearbeiten**.

Hotkeys und Gesten Bearbeiten

Hotkeys für Funktionen der User Station

Port-Navigator

Strg+Alt+N

User-Station-Konfiguration

Strg+Alt+C

Strg+Alt+C

Shift+Alt+C

Strg+Shift+C

Strg+Shift+Alt+C

Deaktiviert

Deaktiviert

Kacheln Rückgängig Machen

Deaktiviert

Speichern

Abbrechen

Die hier konfigurierten Hotkeys werden immer lokal durch den Desktop der Draco SIRA User Station verarbeitet. Sie werden nicht an das Target gesendet, wenn Sie sie innerhalb einer Target-Verbindung benutzen.

Falls Sie solche Hotkeys wie Alt+Tab oder Strg+Alt+Entf innerhalb einer Target-Verbindung benutzen möchten, sollten Sie diese Desktop-Hotkeys auf eine andere Tastenkombination konfigurieren oder deaktivieren.

Abb. 107 Einstellungen - Hotkeys und Gesten - Hotkeys und Gesten bearbeiten

- Wählen Sie im Drop-Down-Menü eine Tastenkombination oder den Eintrag „Deaktiviert“ aus, um die Tastenkombination zu löschen.

2. Klicken Sie auf **Speichern**. Die vorherige Seite erscheint.

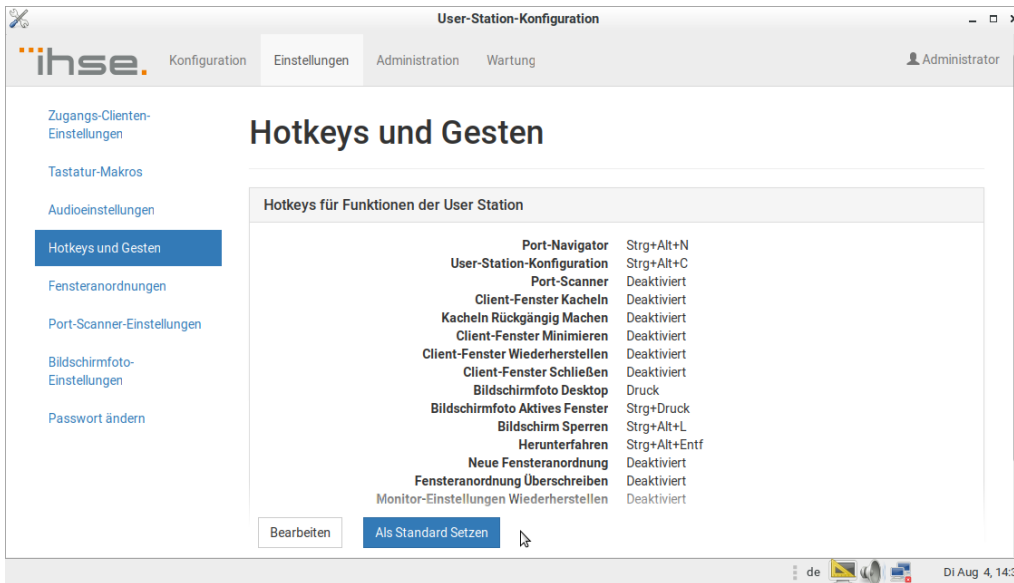


Abb. 108 Einstellungen - Hotkeys und Gesten

3. Klicken Sie auf **Als Standard setzen**, um diese Einstellungen allen neuen Benutzern zuzuweisen, die noch keine eigenen Einstellungen vorgenommen haben.

 Diese Einstellungen bleiben erhalten, bis der Benutzer eigene auswählt.

8.5 Fensteranordnungen (Window Layouts)

Mit der Funktion „Fensteranordnungen“ können Sie Layouts der geöffneten Client-Fenster verwalten, sodass das jeweilige Layout bei Auswahl wiederhergestellt werden kann. Die gespeicherten Layout-Daten umfassen die visuellen Attribute jeder Client-Session, wie Größe, Position und Anzeigemonitor, sowie die jeweiligen Verbindungsinformationen.

Layouts werden benutzerspezifisch gespeichert. Die von einem Benutzer gespeicherten Layouts stehen anderen Benutzern nicht zur Verfügung. Pro Benutzer sind maximal 16 benannte Layouts zulässig.

Sie können über den Port-Navigator oder das Hauptmenü auf die Fensteranordnungen zugreifen. Informationen zum Erstellen von Fensteranordnungen finden Sie im Abschnitt 5.2.6, Seite 22.

Layouts verwalten

Mit den Werkzeugen zur Verwaltung von Window Layouts können Sie festlegen, dass ein Layout beim Anmelden wiederhergestellt wird, das Laden beim Anmelden verzögern, Layouts umbenennen oder löschen sowie ihnen Tastenkombinationen zuweisen.

1. Klicken Sie auf **Hauptmenü > User-Konfiguration > Einstellungen > Fensteranordnungen**. Die entsprechende Seite wird geöffnet.

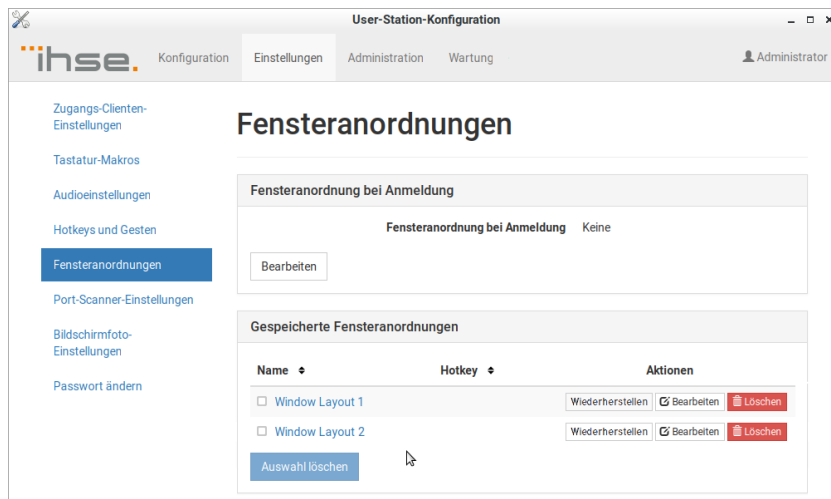


Abb. 109 Einstellungen - Fensteranordnungen (Layouts)

2. Klicken Sie auf den Button **Bearbeiten** im Feld „Fensteranordnung bei Anmeldung“.
3. Wählen Sie aus der Drop-Down-Liste ein Layout aus, das beim Anmelden geladen werden soll. Die Drop-Down-Liste enthält die Namen aller gespeicherten Layouts sowie zwei weitere Einträge:
 - *Keine*: Es wird kein Layout beim Login geladen.
 - *Wie bei der Abmeldung gespeichert*: Bei der nächsten Abmeldung wird der Status aller Clients als Layout gespeichert, und dieses Layout wird bei der nächsten Anmeldung wiederhergestellt. Diese Art von gespeichertem Layout überschreibt kein benanntes Layout, das zum Zeitpunkt der Abmeldung ausgewählt war.

 Das „Abmeldungs“ Layout wird 30 Sekunden nach dem Login und dann alle 15 Sekunden gespeichert.

4. Wählen Sie bei Bedarf eine Verzögerung für das Laden eines Layouts aus. Die Standardeinstellung beträgt 0 Sekunden, es sind bis zu 30 Sekunden möglich

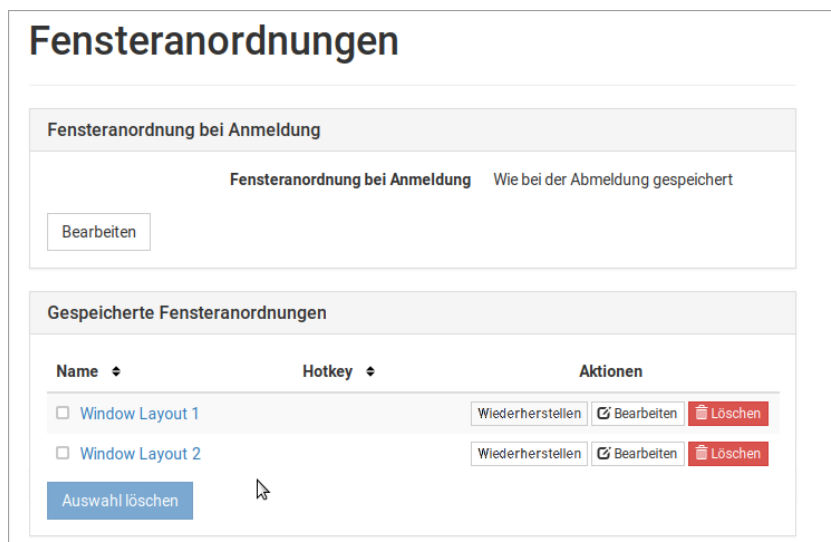


Abb. 110 Einstellungen - Fensteranordnungen - Layout ausgewählt

Im Abschnitt „Gespeicherte Fensteranordnungen“ werden alle gespeicherten Layouts aufgelistet und es stehen verschiedene Optionen zur Verfügung.

- ➔ Klicken Sie auf den Button **Wiederherstellen**, um das Layout anzuwenden. Diese Option hat dieselbe Wirkung wie die Auswahl des Layouts im Hauptmenü.
- ➔ Klicken Sie auf **Bearbeiten** in der Zeile eines Layouts, um Name und Hotkey zu ändern. Namen müssen zwischen 4 und 32 Zeichen lang sein, Hotkeys werden auf Verfügbarkeit getestet.

- ➔ Klicken Sie auf **Löschen** in der Zeile eines Layouts, um dieses Layout zu löschen. Um mehr als ein Layout zu löschen, wählen Sie sie aus und klicken Sie dann auf den Button **Auswahl löschen** unterhalb der Liste. Sie werden aufgefordert, die Löschung zu bestätigen.

Wenn eine Verzögerungszeit konfiguriert ist, wird beim Einloggen die folgende Meldung angezeigt, bevor das Fensterlayout wiederhergestellt wird.

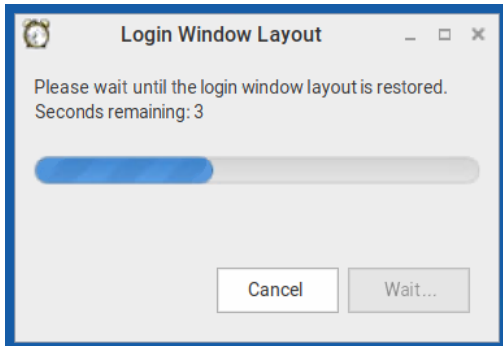


Abb. 111 **Nachricht über Verzögerungszeit**

8.6 Port-Scanner-Einstellungen

Sie können die Intervalle, Pausen und die Ausrichtung des Scanners konfigurieren und festlegen, wie die vom Scanner erfassten Momentaufnahmen gespeichert werden sollen. Die Intervalle und die Ausrichtung können auch im Fenster „Port-Scanner“ konfigurieren werden (siehe Abschnitt 7.2.1, Seite 84).

Die Schnappschuss-Einstellungen werden jedoch nur hier angezeigt.

1. Klicken Sie auf **Hauptmenü > User-Konfiguration > Einstellungen > Port-Scanner Settings**. Die entsprechende Seite wird geöffnet und zeigt die aktuellen Einstellungen an.

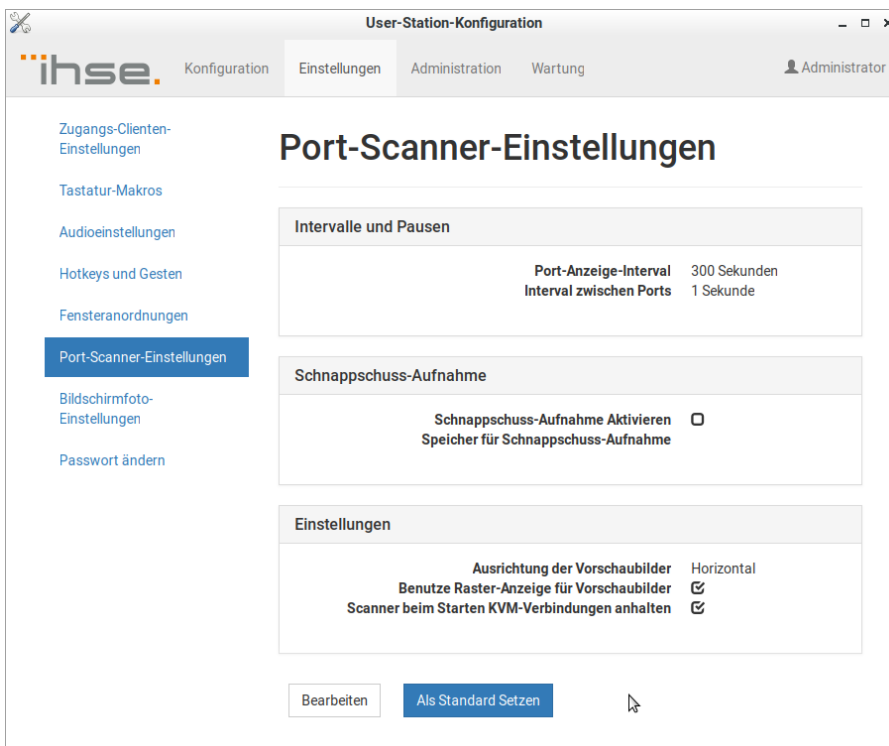
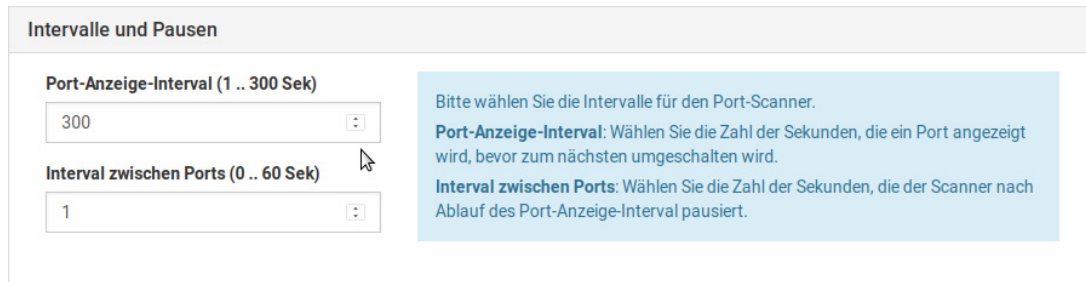


Abb. 112 **Einstellungen - Port-Scanner-Einstellungen**

2. Klicken Sie auf **Bearbeiten**, um Änderungen durchzuführen.

Intervalle und Pausen



Intervalle und Pausen

Port-Anzeige-Interval (1 .. 300 Sek)
300

Interval zwischen Ports (0 .. 60 Sek)
1

Bitte wählen Sie die Intervalle für den Port-Scanner.

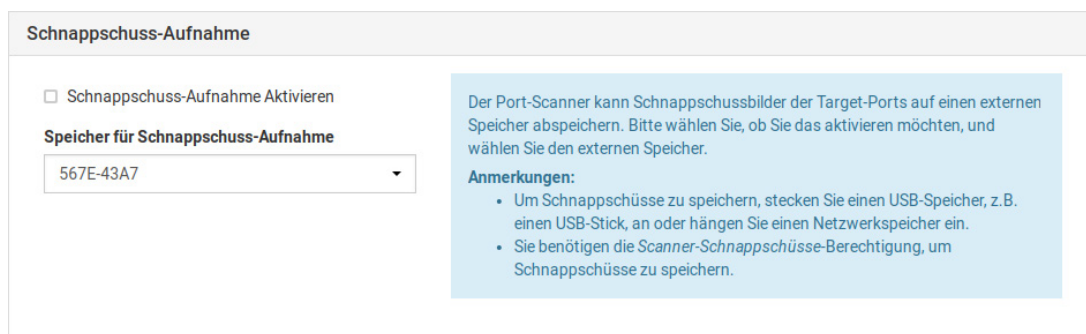
Port-Anzeige-Interval: Wählen Sie die Zahl der Sekunden, die ein Port angezeigt wird, bevor zum nächsten umgeschaltet wird.

Interval zwischen Ports: Wählen Sie die Zahl der Sekunden, die der Scanner nach Ablauf des Port-Anzeige-Interval pausiert.

Abb. 113 Einstellungen - Port-Scanner-Einstellungen - Intervalle und Pausen einstellen

- Ändern Sie die Werte für „Port-Anzeige-Interval“ und „Interval zwischen Ports“ durch Klicken auf die **hoch/runter Pfeile** im entsprechenden Feld.

Schnappschuss-Aufnahme



Schnappschuss-Aufnahme

☐ Schnappschuss-Aufnahme Aktivieren

Speicher für Schnappschuss-Aufnahme
567E-43A7

Der Port-Scanner kann Schnappschusbilder der Target-Ports auf einen externen Speicher abspeichern. Bitte wählen Sie, ob Sie das aktivieren möchten, und wählen Sie den externen Speicher.

Anmerkungen:

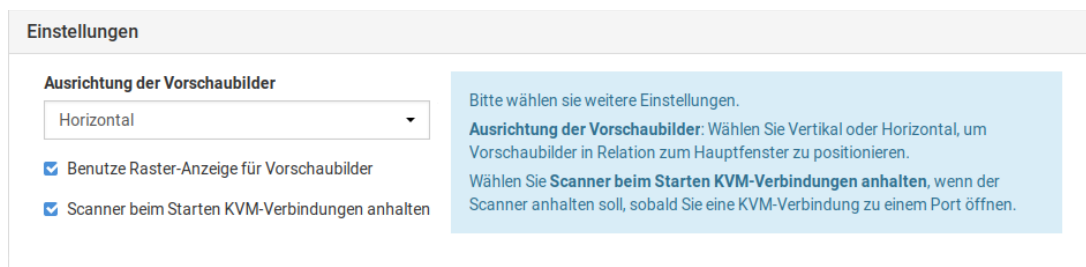
- Um Schnappschüsse zu speichern, stecken Sie einen USB-Speicher, z.B. einen USB-Stick, an oder hängen Sie einen Netzwerkspeicher ein.
- Sie benötigen die Scanner-Schnappschüsse-Berechtigung, um Schnappschüsse zu speichern.

Abb. 114 Einstellungen - Port-Scanner-Einstellungen - Schnappschuss-Aufnahmen aktivieren

☒ Stellen Sie sicher, dass Sie die Anforderungen im blauen Kasten erfüllen.

- Aktivieren Sie die Schnappschuss-Aufnahme, indem Sie das Kontrollkästchen anklicken.
- Wählen Sie ein Speichermedium aus der Drop-Down-Liste aus (USB-Stick oder eingebundener Netzwerkspeicher).

Einstellungen



Einstellungen

Ausrichtung der Vorschaubilder
Horizontal

☒ Benutze Raster-Anzeige für Vorschaubilder

☒ Scanner beim Starten KVM-Verbindungen anhalten

Bitte wählen sie weitere Einstellungen.

Ausrichtung der Vorschaubilder: Wählen Sie Vertikal oder Horizontal, um Vorschaubilder in Relation zum Hauptfenster zu positionieren.

Wählen Sie **Scanner beim Starten KVM-Verbindungen anhalten**, wenn der Scanner anhalten soll, sobald Sie eine KVM-Verbindung zu einem Port öffnen.

Abb. 115 Einstellungen - Port-Scanner-Einstellungen - Weitere Einstellmöglichkeiten

- Wählen Sie unter „Ausrichtung der Vorschaubilder“ die Option „Vertikal“ oder „Horizontal“, um die Vorschaubilder entweder am unteren (horizontal) oder rechten (vertikal) Rand anzuzeigen.
- Aktivieren Sie das Kontrollkästchen „Benutze Raster-Anzeige für Vorschaubilder“, um eine optionale Rasteransicht zu erhalten, in der alle Vorschaubilder auf einmal ohne Scroll-Leisten angezeigt werden.
- Aktivieren Sie das Kontrollkästchen „Scanner beim Starten (von) KVM-Verbindungen anhalten“, wenn der Scanvorgang beim Öffnen eines Ports in einer vollständigen KVM-Session angehalten werden soll.
- Klicken Sie auf **Speichern**.

8.7 Bildschirmfoto (Screenshot)-Einstellungen

Sie können ein Speichermedium konfigurieren, auf dem Bildschirmfotos gespeichert werden. Das Speichern von Screenshots ist nur für Benutzer möglich, denen Sie die Berechtigung „Systemadministration“ oder „Screenshot erstellen“ erteilt haben.

Außerdem müssen Sie eine Tastenkombination für die Erstellung von Screenshots konfigurieren.

1. Klicken Sie auf **Hauptmenü > User-Konfiguration > Einstellungen > Bildschirmfoto-Einstellungen**. Die entsprechende Seite wird geöffnet. Standardmäßig sind keine Einstellungen konfiguriert.

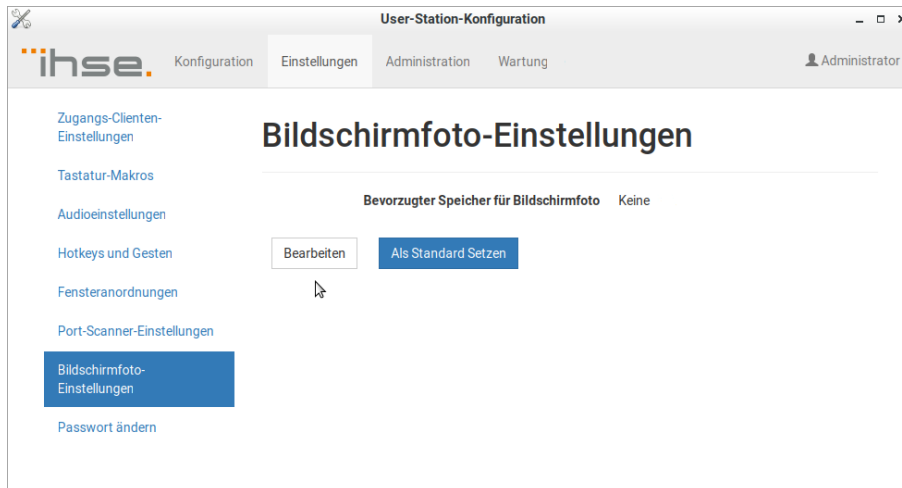


Abb. 116 Einstellungen - **Bildschirmfoto-Einstellungen**

2. Schließen Sie einen USB-Stick an oder richten Sie einen Netzwerkspeicher ein (siehe Abschnitt 9.12, Seite 148).
3. Klicken Sie auf **Bearbeiten**. Die Bevorzugte Speicher-Liste ist nun zugänglich.
4. Wählen Sie ein Speichermedium aus und klicken Sie auf **Speichern**.

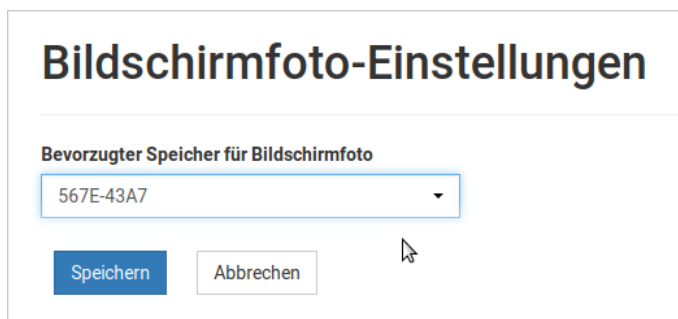


Abb. 117 Einstellungen - Bildschirmfoto-Einstellungen - **Ausgewähltes Speichermedium**

5. Um diesen bevorzugten Speicherort als Standard für alle neuen Benutzer und bestehenden Benutzer, die ihre Einstellungen noch nicht geändert haben, festzulegen, klicken Sie auf **Als Standard setzen** (Systemadministratorrechte erforderlich).

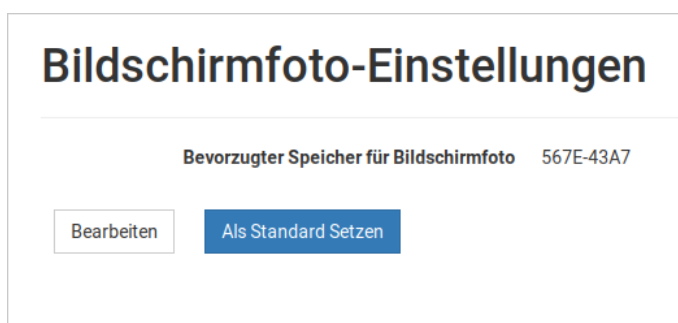


Abb. 118 Einstellungen - Bildschirmfoto-Einstellungen - **Als Standardspeicher festlegen**

8.7.1 Screenshots aufnehmen

Um Screenshots zu erstellen, müssen Sie einer Benutzergruppe angehören, die über die Berechtigung „Screenshot erstellen“ sowie über eine Berechtigung wie „Gerätezugriff“ verfügt, die Ihnen die Anmeldung ermöglicht (siehe Berechtigungen im Abschnitt 9.2.1.1, Seite 111).

Für diese Funktion muss ein Hotkey eingerichtet werden.

Die Screenshots werden auf einem angeschlossenen USB-Speichergerät oder einem eingebundenen Netzwerkspeicher gespeichert. Werden mehrere USB-Speichergeräte erkannt, wird das erste Gerät in der alphabetisch sortierten Liste ausgewählt.

 Aktive RDP-Sitzungen können die Befehle zum Erstellen von Screenshots beeinträchtigen. Wenn eine RDP-Sitzung geöffnet ist, klicken Sie unbedingt auf den Desktop der Draco SIRA User Station, bevor Sie einen Screenshot erstellen.

Hotkey für die Erstellung eines Screenshots aktivieren

1. Klicken Sie auf **Hauptmenu > User-Station-Konfiguration > Einstellungen > Hotkeys und Gesten**.
2. Suchen Sie die Einträge „Bildschirmfoto Desktop“ und „Bildschirmfoto Aktives Fensters“.

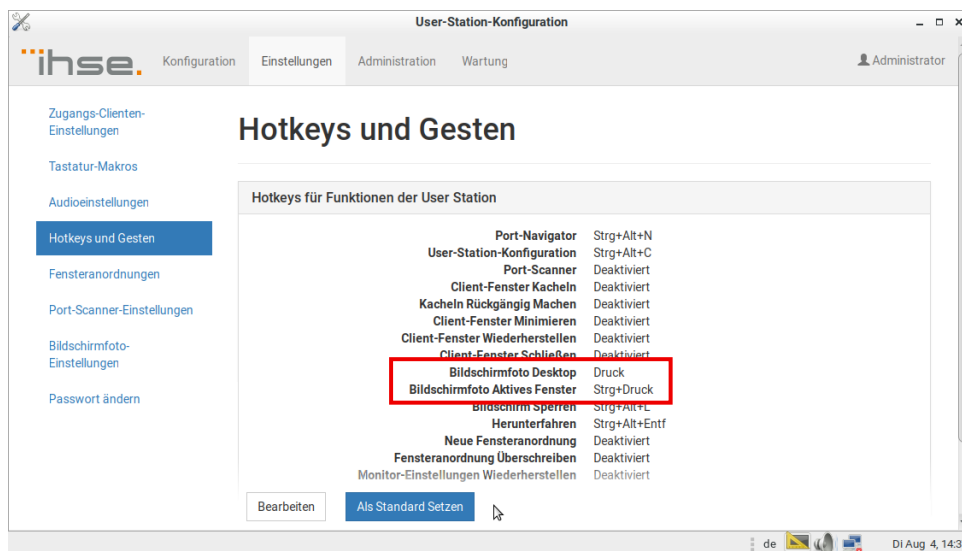


Abb. 119 Einstellungen - Hotkeys und Gesten - Hotkeys für Bildschirmfotos (Screenshots)

3. Wenn die Funktionen aktiviert sind, können Sie die angezeigten Tastenkombinationen verwenden.
4. Wenn die Funktionen deaktiviert sind oder Sie den Hotkey ändern möchten, klicken Sie auf **Bearbeiten** und wählen Sie dann im Drop-Down-Menü einen Hotkey für die Funktion aus.
5. Klicken Sie auf **Speichern**.

Wenn mit dem konfigurierten Hotkey ein Screenshot aufgenommen wird, wird dieser direkt auf dem konfigurierten Speichermedium gespeichert, und es erscheint eine Bestätigung.

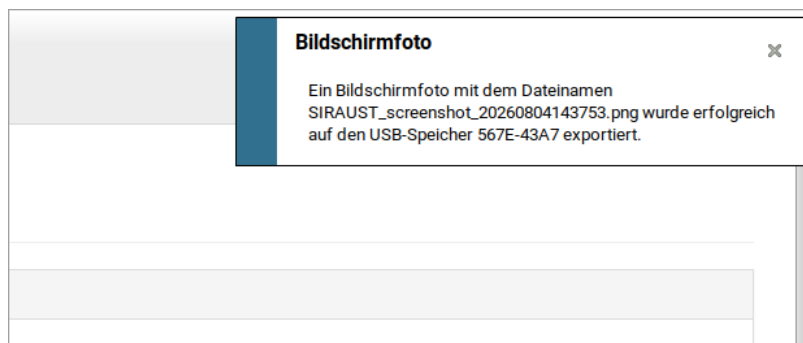


Abb. 120 Bestätigungsmeldung eines Bildschirmfotos (Screenshot)

8.8 Passwort ändern

Sie können Ihr Passwort ändern.

1. Klicken Sie auf **Hauptmenü > User-Konfiguration > Einstellungen > Passwort ändern**. Die entsprechende Seite wird geöffnet.

ihse. Konfiguration Einstellungen Administration Wartung Administrator

Zugangs-Clients-Einstellungen
Tastatur-Makros
Audioeinstellungen
Hotkeys und Gesten
Fensteranordnungen
Port-Scanner-Einstellungen
Bildschirmfoto-Einstellungen
Passwort ändern

Passwort ändern

* Passwort

* Passwort-Wiederholung

Speichern Abbrechen

Achtung: Starke Passwörter werden erzwungen. Das folgende gilt für Passwörter:

- Die minimale Länge ist 8 Zeichen.
- Es muss mindestens einen Kleinbuchstaben enthalten.
- Es muss mindestens einen Großbuchstaben enthalten.
- Es muss mindestens eine Ziffer enthalten.
- Sie dürfen die letzten 5 Passwörter nicht wieder verwenden.

Abb. 121 Einstellungen - **Passwort ändern**

2. Geben Sie ein neues Passwort ein, das den in dem blauen Feld angegebenen Regeln entspricht. Geben Sie es zur Bestätigung noch einmal ein.
3. Klicken Sie auf **Speichern**.

9 Administrationsfunktionen einstellen

- ➔ Klicken Sie im Fenster „User-Station-Konfiguration“ auf **Administration**, um die folgenden Funktionen einzustellen:

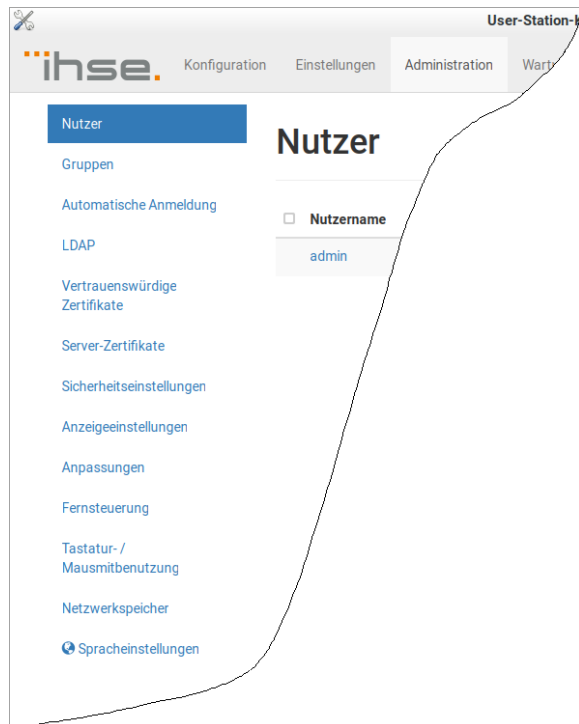


Abb. 122 Untermenü Administration

9.1 Nutzer

Die Draco SIRA User Station verfügt über ein integriertes Administratorkonto (admin), das sich ideal für die erstmalige Anmeldung und die Systemadministration eignet. Dieses admin-Konto kann nicht gelöscht werden.

1. Klicken Sie auf **Hauptmenü > User-Konfiguration > Administration**. Die Seite für die Nutzerkonfiguration wird geöffnet. Sie enthält eine Liste aller Nutzer.

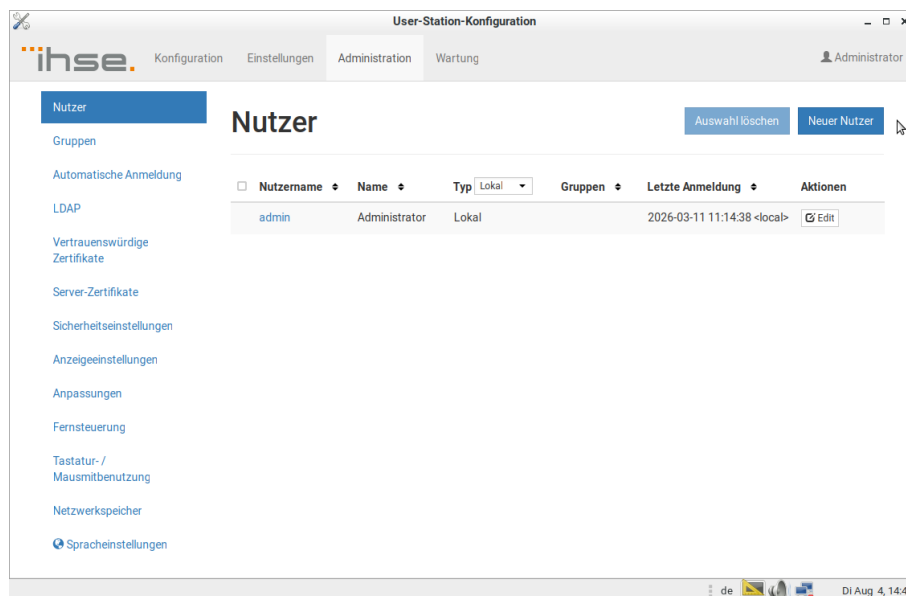


Abb. 123 Administration - Nutzer - Nutzerliste

9.1.1 Neue Nutzer erstellen

Sie können Nutzerprofile mit konfigurierbaren Berechtigungen hinzufügen, um die User Station zu bedienen und zu steuern.

i Die Nutzerprofile der Draco SIRA User Station legen fest, welche Berechtigungen den Nutzern an der User Station gewährt werden, nicht jedoch an den KVM-Geräten (siehe Abschnitt 9.2.3, Seite 113).

1. Klicken Sie auf den Button **Neuer Nutzer**. Die folgende Seite erscheint.

Abb. 124 Administration - Nutzer - **Neuer Nutzer**

2. Geben Sie die Daten des neuen Nutzers ein. Die mit * markierten Felder sind Pflichtangaben.

Feld	Beschreibung
* Nutzername	Name für das Einloggen an der User Station. 2 bis 255 Zeichen - Gesperrtes Zeichen: Doppelpunkt (:)
Authentifikation über LDAP	Aktivieren Sie dieses Kontrollkästchen, wenn dieser Benutzer über LDAP authentifiziert werden soll (siehe Abschnitt 9.4, Seite 116). Wenn dieses Kontrollkästchen nicht aktiviert ist, wird dieser Benutzer über die lokale Datenbank der User Station authentifiziert, und Sie müssen die Benutzerkennwörter auf der User Station speichern.
E-mail	Eine E-mail-Adresse des Benutzers.
Name	Klarname oder Spitzname des Benutzers.
* Passwort,	Passwort für das Einloggen an der User Station.
* Passwort-Wiederholung	Mindestens 8 Zeichen, darunter mindestens: 1 Kleinbuchstabe, 1 Großbuchstabe und 1 Zahl sind erforderlich.
* Ausgewählte Gruppen	Durch die Zuordnung zu Gruppen werden diesem Nutzer Berechtigungen gewährt (siehe Abschnitt 9.2.1, Seite 109). Verwenden Sie die Pfeiltasten, um die Gruppen nach Bedarf zu verschieben. Der Nutzer wird Mitglied der Gruppen sein, die in der Liste „Ausgewählte Gruppen“ aufgeführt sind. Es muss mindestens eine Gruppe ausgewählt werden.

3. Klicken Sie auf **Speichen** und das Profil des neuen Nutzers wird angezeigt.

Nutzer wurde erfolgreich erstellt. ×

Nutzer

Neuer Nutzer

Nutzername	Mustermann
Typ	Lokal
Name	Max Mustermann
E-Mail	
Berechtigungen	Einstellungen ändern Geräte-Zugang Den Port-Scanner starten Bildschirmfotos aufnehmen
Gruppen	Devices Users
Letzte Anmeldung	
Letzte Anmeldung von	
Nutzersperre	Nicht gesperrt

Zurück zur Nutzerübersicht
Bearbeiten
Löschen

Abb. 125 Administration - Nutzer - **Neuen Nutzer erstellt**

9.1.2 Nutzer ändern oder löschen

1. Klicken Sie im User-Station-Konfigurationsfenster auf **Administration > Nutzer**. Eine Liste aller Nutzer erscheint.

Nutzer

Auswahl löschen
Neuer Nutzer

☐	Nutzername	Name	Typ	Gruppen	Letzte Anmeldung	Aktionen
☐	Musterfrau	Lia Musterfrau	Lokal	Devices Administrators Devices Users	2026-04-23 13:24:05 <local>	☒ Bearbeiten Löschen
☐	Mustermann	Max Mustermann	Lokal	Devices Users		☒ Bearbeiten Löschen
☒	admin	Administrator	Lokal		2026-04-23 13:05:29 <local>	☒ Bearbeiten Löschen

Abb. 126 Administration - Nutzer - **Liste der Nutzer**

2. Wählen Sie im Feld „Typ“ eine Option aus, um den gewünschten Nutzertyp oder alle Typen anzuzeigen.
 - Local: Zeigt nur lokale Nutzer an, die über die lokale Datenbank der User Station authentifiziert sind.
 - LDAP: Zeigt die Nutzer an, die über LDAP authentifiziert sind.
 - All: Zeigt alle Nutzer an. Nur der Nutzer admin kann alle Nutzer anzeigen.
3. Klicken Sie auf den Nutzernamen eines Nutzers, um dessen Daten anzuzeigen.

Nutzer Neuer Nutzer

Nutzername	Mustermann
Typ	Lokal
Name	Max Mustermann
E-Mail	
Berechtigungen	Einstellungen ändern Geräte-Zugang Den Port-Scanner starten Bildschirmfotos aufnehmen
Gruppen	Devices Users Office 1
Letzte Anmeldung	
Letzte Anmeldung von	
Nutzersperre	Nicht gesperrt

Zurück zur Nutzerübersicht
Bearbeiten
Löschen

Abb. 127 Administration - Nutzer - **Details eines Nutzers**

Nutzerdaten ändern

✓ Der integrierte Admin-Benutzer kann nicht gelöscht werden, seine Einstellungen können jedoch mit Ausnahme der Berechtigungen (Nutzergruppen) geändert werden.

1. Klicken Sie auf den Button **Bearbeiten** in der Zeile des Benutzers oder zeigen Sie dessen Details an und klicken Sie in diesem Fenster auf den Button **Bearbeiten**. Die Seite „Nutzer“ wird geöffnet.

Nutzer

* **Nutzername**
Mustermann

☐ Authentifikation über LDAP

E-Mail
max.mustermann@muster.de

Name
Max Mustermann

Passwort

Passwort-Wiederholung

* **Ausgewählte Gruppen**
Devices Users
Office 1

Verfügbare Gruppen
System Administrators
Devices Administrators
Restricted Users

Achtung: Starke Passwörter werden erzwungen. Das folgende gilt für Passwörter:

- Die minimale Länge ist 8 Zeichen.
- Es muss mindestens einen Kleinbuchstaben enthalten.
- Es muss mindestens einen Großbuchstaben enthalten.
- Es muss mindestens eine Ziffer enthalten.
- Sie dürfen die letzten 5 Passwörter nicht wieder verwenden.

Speichern Abbrechen

Abb. 128 Administration - Users - **Nutzerdaten ändern**

2. Führen Sie die gewünschten Änderungen durch. Der Login-Name kann nicht geändert werden. Beachten Sie die Regeln für das Passwort in der blauen Box.
3. Klicken Sie auf **Speichern**.

Löschen eines oder mehrerer Nutzer

1. Um einen einzelnen Nutzer zu löschen, klicken Sie auf den Button **Löschen** in der Zeile des Nutzers.
2. Um mehrere Nutzer zu löschen, setzen Sie ein Häkchen in das Kästchen links vom Nutzernamen bei allen zu löschenden Nutzern. Klicken Sie dann auf den Button **Auswahl löschen**.
3. In beiden Fällen erscheint eine Bestätigungsmeldung. Klicken Sie dort auf **OK**.

9.2 Gruppen

Eine Gruppe legt fest, welche Berechtigungen ihre Mitglieder haben.

Es gibt mehrere Standard-Gruppen.

Gruppe	Standard-Berechtigungen
System Administrators	Systemadministration
Devices Administrators	Geräteverwaltung, Gerätezugang
Devices Users	Gerätezugang, Voreinstellungen ändern, Port-Scanner starten
Restricted Users	Nur Gerätezugang

Sie können eine neue Gruppe anlegen, wenn die Standard-Gruppen Ihren Anforderungen nicht entsprechen.

9.2.1 Anlegen einer neuen Gruppe

1. Klicken Sie im Hauptmenü **User-Station-Konfiguration > Administration > Gruppen**. Die entsprechende Seite mit den Standard-Nutzergruppen erscheint.

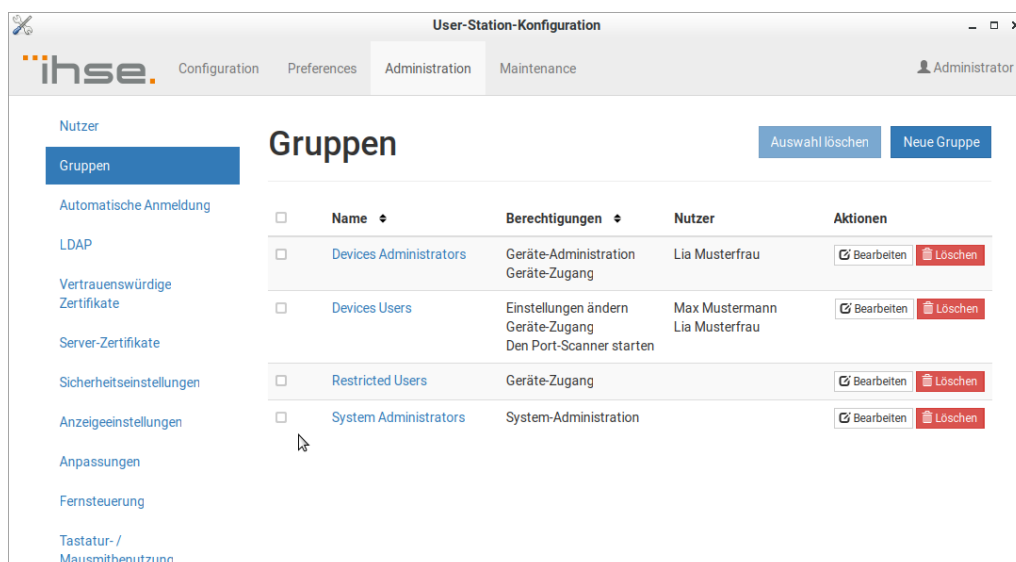


Abb. 129 Administration - Gruppen

2. Klicken Sie auf **Neue Gruppe**. Die Seite „Neue Gruppe“ erscheint.
3. Geben Sie einen Namen ein und aktivieren Sie die gewünschten Berechtigungen für die neue Benutzergruppe. Eine ausführliche Beschreibung der Berechtigungen finden Sie auf der nächsten Seite.

Neue Gruppe

*** Name**

*** Berechtigungen**

☒ Geräte-Zugang
☐ ESXi-Zugang
☐ Web-Zugang
☐ VNC-Zugang
☐ RDP-Zugang
☐ SSH-Zugang
☒ Einstellungen ändern
☐ Geräte-Administration
☐ Den Port-Scanner starten
☐ Scanner-Schnappschüsse speichern
☒ Bildschirmfotos aufnehmen
☐ System-Administration

Die **Geräte-Zugang**-Berechtigung enthält die Berechtigungen:

- Zum Anmelden
- Öffnen von KVM- und seriellen Verbindungen

Die **VNC-Zugang**-, **RDP-Zugang**-, **SSH-Zugang**-, **Web-Zugang**- und **ESXi-Zugang**-Berechtigungen enthalten die Berechtigung:

- Zum Öffnen von VNC-, RDP-, SSH-, Web- und ESXi-Verbindungen

Die **Einstellungen ändern**-Berechtigung enthält die Berechtigungen:

- Ändern persönlicher Einstellungen

Die **Geräte-Administration**-Berechtigung enthält die Berechtigungen:

- Einstellungen ändern-Berechtigung
- Den Port-Scanner starten-Berechtigung
- Geräte-Zugang-Berechtigung
- VNC-Zugang-, RDP-Zugang-, SSH-Zugang-, Web-Zugang- und ESXi-Zugang-Berechtigung
- SIRA-Geräte hinzuzufügen und zu entfernen
- VNC-, RDP-, SSH-, Web und ESXi-Zugangspunkt zu erstellen, modifizieren und zu entfernen

Die **Den Port-Scanner starten**-Berechtigung enthält die Berechtigungen:

- Starten des Port-Scanners

Die **Scanner-Schnappschüsse speichern**-Berechtigung enthält die Berechtigungen:

- Aufnehmen von Schnappschüssen mit dem Port-Scanner
- Starten des Port-Scanners

Die **Bildschirmfotos aufnehmen**-Berechtigung enthält die Berechtigungen:

- Zum Aufnehmen und Speichern von Bildschirmfotos auf einem USB-Speicher oder Netzwerkspeicher

Die **System-Administration**-Berechtigung enthält alle anderen Berechtigungen

Abb. 130 Administration - Gruppen - Neue Gruppe erstellen

- Klicken Sie auf **Speichern**. Die Daten der neuen Nutzergruppe werden angezeigt. Die Gruppe wird zur Liste hinzugefügt und kann Nutzern zugewiesen werden.

9.2.1.1 Beschreibung der Berechtigungen

Berechtigung	Erlaubte Prozesse
Geräte-Zugang	- Einloggen an der User Station. - KVM- und serielle Sessions öffnen.
ESXi-Zugang WEB-Zugang	ESXi- bzw. WEB-Sessions öffnen.
VNX-Zugang RDP-Zugang SSH-Zugang	- VNC-, RDP- oder SSH-Sessions öffnen. - Diese Berechtigungen allein gewähren noch keine Login-Rechte. Der Benutzer muss außerdem Mitglied einer Gruppe sein, die über Berechtigungen für die Systemadministration, die Geräteverwaltung oder den Gerätezugriff verfügt.
Einstellungen ändern	- Persönliche Einstellungen ändern. - Benutzer, die nicht über diese Berechtigung verfügen, können weder die User-Station-Konfiguration noch das Window Layout noch die Systemeinstellungen aufrufen.
Geräte-Administration	- Einloggen an der User Station. - Einstellungen ändern - Gerätezugang - Port-Scanner starten. - Erlaubnis für ESXi-Zugang, WEB-Zugang, VNC-Zugang, RDP-Zugang und SSH-Zugang - Hinzufügen und Entfernen von SIRA CON Geräten - Hinzufügen, ändern und löschen von ESXi-, WEB-, VNC-, RDP- und SSH-Zugängen
Den Port Scanner starten	Port-Scanner starten
Bildschirmfotos aufnehmen	- Mit dem Hotkey Screenshots erstellen und auf USB-Stick oder Netzwerkspeicher speichern. - Diese Berechtigung allein gewährt keine Login-Rechte. Der Benutzer muss außerdem Mitglied einer Gruppe sein, die über Berechtigungen für die Systemadministration, die Geräteverwaltung oder den Gerätezugriff verfügt
Scanner-Schnappschüsse speichern	- Port-Scanner starten. - Schnappschüsse vom Port-Scanner erstellen.
System-Administration	Alle Prozesse der User Station sind erlaubt.

9.2.2 Gruppen ändern oder löschen

- Um alle Gruppen anzuzeigen, klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Gruppen**.

Gruppen				
		Auswahl löschen		Neue Gruppe
☐	Name ▾	Berechtigungen ▾	Nutzer	Aktionen
☐	Devices Administrators	Geräte-Administration Geräte-Zugang	Lia Musterfrau	☒ Bearbeiten ☐ Löschen
☐	Devices Users	Einstellungen ändern Geräte-Zugang Den Port-Scanner starten	Max Mustermann Lia Musterfrau	☒ Bearbeiten ☐ Löschen
☐	Office 1	Geräte-Zugang Einstellungen ändern Den Port-Scanner starten Bildschirmfotos aufnehmen	Daria Armin Laura Simon	☒ Bearbeiten ☐ Löschen
☐	Restricted Users	Geräte-Zugang	Praktikant	☒ Bearbeiten ☐ Löschen
☐	System Administrators	System-Administration		☒ Bearbeiten ☐ Löschen

Abb. 131 Administration - Gruppe - Liste der Nutzergruppen

In der Spalte „Nutzer“ werden die Namen von maximal fünf Nutzern aufgeführt, die dieser Gruppe angehören. Ist der echte Name nicht im Benutzerprofil enthalten, wird der Anmeldenamen des Benutzers angezeigt.

- Klicken Sie auf den Namen einer Gruppe, um deren Details anzuzeigen.

Gruppen		Neue Gruppe
Name Office 1 Berechtigungen Geräte-Zugang Einstellungen ändern Den Port-Scanner starten Bildschirmfotos aufnehmen Nutzer Daria* Armin* Laura* Simon*		
Zurück zur Gruppenübersicht	Bearbeiten	Löschen

Abb. 132 Administration - Gruppe - Details einer Nutzergruppe

- Um die Einstellungen einer Gruppe zu ändern, klicken Sie entweder in der Liste der Gruppen oder in den Details der Gruppe auf den Button **Bearbeiten**.
- Führen Sie die gewünschten Änderungen durch und klicken Sie auf **Speichern**.

Gruppen löschen

- Um eine einzelne Gruppe zu löschen, klicken Sie auf den Button **Löschen** entweder in der Liste der Gruppen oder in der Seite der Details der Gruppe.
- Um mehrere Gruppen zu löschen, setzen Sie ein Häkchen in das Kästchen links vom Namen bei allen zu löschenden Gruppen. Klicken Sie dann auf den Button **Auswahl löschen**.
- In beiden Fällen erscheint eine Bestätigungsmeldung.
Sollte sich ein Nutzer nach dem Löschen dieser Gruppe nicht mehr anmelden können, wird in der Bestätigungsmeldung eine Warnung angezeigt, wie sie in der folgenden Abbildung dargestellt ist.

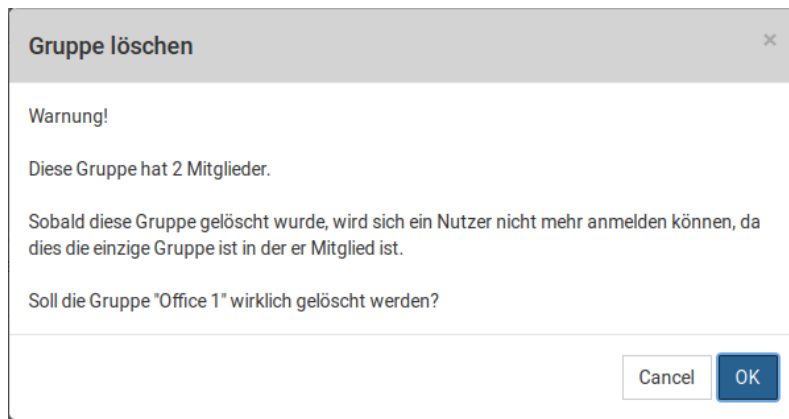


Abb. 133 Administration - Gruppen - Mögliche Warnmeldung bei Löschen von Gruppen

4. Klicken Sie auf **OK**, um die Gruppe(n) zu löschen oder auf **Cancel**, um den Vorgang abubrechen.

9.2.3 Authentifizierung von User Stations und KVM/Seriellen Switches

Die Logindaten, die Sie für die Anmeldung an der Draco SIRA User Station verwenden, können sich von den Logindaten unterscheiden oder mit diesen übereinstimmen, die Sie für den Zugriff auf die Port-Informationen eines beliebigen SIRA CON-Geräts oder seriellen Switches eingeben.

Logindaten für die User Station

Die Logindaten für die User Station legen fest, welche Aufgaben und Berechtigungen Sie auf der User Station ausführen dürfen, nicht jedoch, welche Aufgaben und Berechtigungen Sie auf KVM-/serielle Switches und KVM-/serielle-Ports ausführen können.

Beispielsweise legen die Logindaten der User Station fest, ob Sie Daten von KVM-/seriellen Switches hinzufügen oder entfernen können oder ob Sie die Einstellungen der User Station sichern und wiederherstellen können.

Ausführliche Informationen dazu, was Sie auf einer User Station tun können, finden Sie im Abschnitt 9.2.1.1, Seite 111.

Logindaten für das SIRA CON-Gerät bzw. den seriellen Switch

Die für KVM-/serielle Switche eingegebenen Nutzer-Logindaten legen fest, welche Aufgaben/Berechtigungen Sie beim Zugriff auf an KVM-Ports angeschlossene Computergeräte (d. h. Target-Server) ausführen dürfen.

Beispielsweise bestimmen die Nutzer-Logindaten für den KVM-/seriellen Switch, ob Sie auf alle KVM-/serielle Ports dieses KVM-/seriellen Switches zugreifen können oder ob Sie die Funktionen zur Steuerung virtueller Medien oder der Stromversorgung an einem KVM-/seriellen Port bzw. Target-Server ausführen können.

Aus diesem Grund dürfen Nutzer der User Station die Logindaten von KVM-/seriellen Switchen NICHT gemeinsam nutzen, und jeder Nutzer muss seine eigenen Nutzerdaten für die jeweiligen KVM-/seriellen Switches eingeben und speichern (siehe 6.1.1, Seite 55).

Ist LDAP jedoch aktiviert, können Sie Ihre KVM-/serielle Switches mit einer speziellen Einstellung hinzufügen, die Single Sign-On ermöglicht (siehe Abschnitt 6.1, Seite 53) und weitere Details der LDAP-Hilfe entnehmen (siehe Abschnitt 9.4, Seite 116).

Ausführliche Informationen dazu, welche Möglichkeiten Ihnen ein KVM-/serieller Port-/Target-Server bietet, finden Sie im Benutzerhandbuch für Draco SIRA CON-Extender, das auf unserer Website www.ihse.com verfügbar ist.

Die folgende Tabelle veranschaulicht verschiedene Kombinationen von Nutzer-Logindaten für User Stationen und KVM-Geräte.

Nutzerkonto für User Station	Aufgaben, die Sie an der User Station ausführen können	Nutzerkonto für SIRA CON	Aufgaben, die Sie an einem KVM-Port bzw. auf einem Target-Server ausführen können
admin	Sie können alles machen, inklusive: - System-Administration z.B. Backup oder Software-Update - Geräteverwaltung z.B. SIRA-Geräte - Gerätezugang, z.B. Zugang zu den Daten aller SIRA-Geräte und Ports.	user-A	Es werden eingeschränkte Berechtigungen gewährt: - Portzugang - Kein Zugang zu virtuellen Medien - Keine Kontrolle über die Stromversorgung
user-1	Es werden eingeschränkte Berechtigungen gewährt: - Gerätezugang - Keine Geräteverwaltung - Keine System-Administration	admin	Sie können alles machen, inklusive: - Portzugang - Zugang zu virtuellen Medien - Kontrolle über Stromversorgung
admin	Sie können alles machen, siehe oben	admin	Sie können alles machen, siehe oben

9.3 Autologin

Aktivieren Sie die Funktion „Automatische Anmeldung“, damit ein ausgewählter Benutzer beim Hochfahren automatisch bei der Draco SIRA User Station angemeldet wird. Um den Benutzer zu wechseln, melden Sie sich ab und melden Sie sich anschließend als neuer Benutzer an. Die automatische Anmeldung wird sowohl für lokale als auch für LDAP-Anmeldungen unterstützt.

✓ Für die automatische Anmeldung für Konfigurationen mit gemeinsamer Nutzung von Tastatur und Maus siehe Abschnitt 9.11, Seite 144.

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Automatische Anmeldung**. Die entsprechende Seite erscheint.

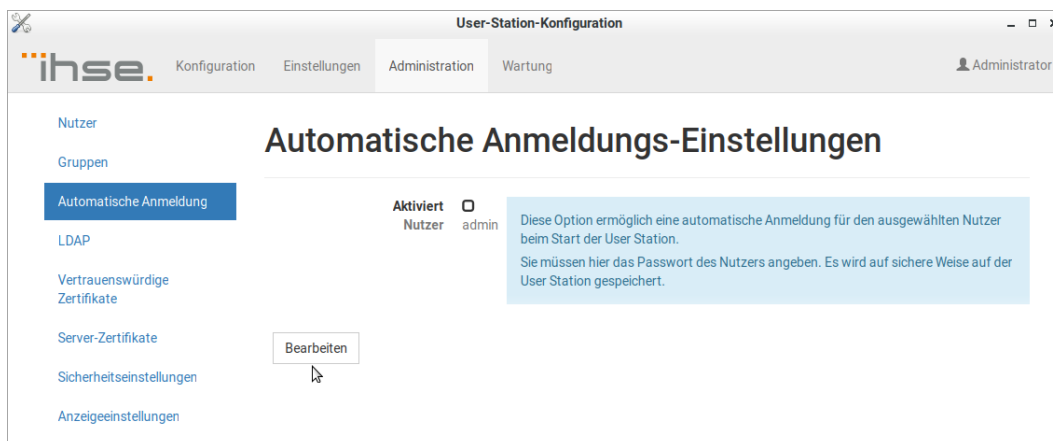


Abb. 134 Administration - Automatische Anmeldungs-Einstellungen

2. Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern. Die Bearbeitungsseite wird geöffnet.

Automatische Anmeldungs-Einstellungen bearbeiten

☒ Aktiviert 

Nutzer

Mustermann ▼

Passwort

.....

Speichern **Abbrechen**

Diese Option ermöglicht eine automatische Anmeldung für den ausgewählten Nutzer beim Start der User Station.
Sie müssen hier das Passwort des Nutzers angeben. Es wird auf sichere Weise auf der User Station gespeichert.

Abb. 135 Administration - Automatische Anmeldungs-Einstellungen - **Einstellungen bearbeiten**

3. Setzen Sie ein Häkchen in die Checkbox „Aktiviert“, um die automatische Anmeldung zu aktivieren.
4. Wählen Sie den gewünschten Nutzernamen aus der Drop-Down-Liste aus.
5. Geben Sie ein Passwort ein.
6. Klicken Sie auf **Speichern**. Die Einstellungen werden gespeichert und die Bearbeitungsseite wird geschlossen.

9.4 LDAP

Die externe LDAP-Authentifizierung verfügt über die folgenden zwei Modi:

- Authentifizierung und Autorisierung über LDAP
- Nur Authentifizierung über LDAP

 Um die Single-Sign-On-Funktion in der Draco SIRA User Station nutzen zu können, müssen Ihre Geräte, die User Station und Ihre Nutzer in derselben LDAP-Umgebung vorhanden sein, und der Wert des „Login-Name-Attributs“ muss mit der UID übereinstimmen.

Authentifizierung und Autorisierung über LDAP

1. Erstellen Sie auf dem/den LDAP-Server(n) sowohl Nutzer als auch Nutzergruppen für die User Station.
2. Erstellen Sie auf der User Station Nutzergruppen, deren Gruppennamen mit denen auf dem/den LDAP-Server(n) übereinstimmen.
 - Sie können außerdem gewünschte Nutzergruppen vom LDAP-Server in die User Station importieren, nachdem Sie eine LDAP-Suche nach Benutzergruppenobjekten durchgeführt haben (siehe weiter unten in diesem Abschnitt).
 - Nutzernamen für diesen LDAP-Authentifizierungsmodus sind auf der User Station nicht erforderlich.

 LDAP-Aliase, die es einem Benutzer ermöglichen, mehrere Anmeldungen zu haben, beispielsweise mehrere allgemeine Namen, funktionieren im LDAP-Authentifizierungs- und Autorisierungsmodus nicht.

Nur Authentifizierung über LDAP

1. Erstellen Sie auf dem/den LDAP-Server(n) Benutzer für die User Station.
 - Auf dem/den LDAP-Server(n) sind keine Benutzergruppen erforderlich.
2. Legen Sie auf der User Station sowohl Nutzer als auch Gruppen an. Die Nutzernamen müssen mit denen auf dem/den LDAP-Server(n) übereinstimmen, die Passwörter werden jedoch nicht auf der User Station gespeichert.
 - Sie können außerdem gewünschte Nutzernamen vom LDAP-Server in die User Station importieren, nachdem Sie eine LDAP-Suche nach Benutzerobjekten durchgeführt haben (siehe weiter unten in diesem Abschnitt).
 - Im Gegensatz zum anderen Modus funktioniert der LDAP-Alias im Modus „Nur LDAP-Authentifizierung“ einwandfrei.

Für beide LDAP-Authentifizierungsmodi ist eine Konfiguration der User Station erforderlich

1. LDAP-Server hinzufügen (siehe nächster Abschnitt).
2. LDAP-Authentifizierung aktivieren (siehe Abschnitt 9.4.3, Seite 122).

 Wenn „admin“ als Benutzername eingegeben und LDAP aktiviert ist, erscheint auf der Anmeldeseite ein zusätzliches Kontrollkästchen „Lokal authentifizieren“. Sie können „Lokal authentifizieren“ auswählen, um die Authentifizierung über die lokale Datenbank der User Station anstelle des/der LDAP-Server(s) durchzuführen, unabhängig vom LDAP-Authentifizierungsmodus.

9.4.1 LDAP-Server hinzufügen

Um die externe LDAP-Authentifizierung zu nutzen, muss mindestens ein LDAP-Server zur User Station hinzugefügt werden. Wenn Sie mit den LDAP-Einstellungen nicht vertraut sind, wenden Sie sich bitte an Ihren LDAP-Administrator.

Wenn mehrere LDAP-Server hinzugefügt wurden, bestimmt die Reihenfolge der LDAP-Server die Priorität der Authentifizierung. Die User Station stellt zur Nutzerauthentifizierung zunächst eine Verbindung zum ersten LDAP-

Server her, dann zum zweiten, falls der erste LDAP-Server ausfällt, und so weiter, bis der Nutzer erfolgreich authentifiziert wurde. Wenn alle LDAP-Server die Authentifizierung nicht bestehen, wird dem Nutzer der Zugriff verweigert

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > LDAP**. Die LDAP-Seite wird geöffnet.

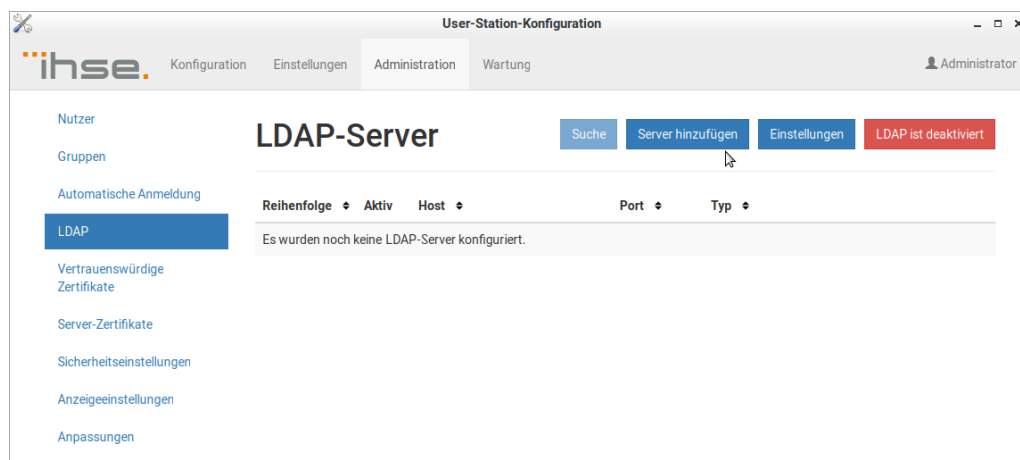


Abb. 136 Administration - LDAP-Server

2. Klicken Sie auf **Server hinzufügen**. Die neuen Server hinzufügen Seite erscheint mit 5 Gruppen von Einstellmöglichkeiten.
3. Unter „Allgemein“ legen Sie die grundlegenden LDAP-Einstellungen fest.

Abb. 137 Administration - LDAP Servers - Allgemeine Einstellungen

Parameter	Beschreibung
Typ	Typ des neuen LDAP-server: • Active Directory Server: Microsoft Active Directory • LDAP server: Open LDAP
Reihenfolge	Die Reihenfolge dieser LDAP-Server bestimmt die Priorität bei der Authentifizierung, wenn mehrere LDAP-Server vorhanden sind. Wenn Sie mehr als einen LDAP-Server hinzufügen, können Sie die Priorität ändern, indem Sie die laufende Nummer eines beliebigen vorhandenen LDAP-Servers auswählen. Der vorhandene LDAP-Server und alle nachfolgenden Server rücken in der Reihenfolge um eine Position nach unten.
Aktiv	Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie möchten diesen LDAP-Server vorübergehend deaktivieren.

4. Geben Sie die Daten des LDAP-Servers im Bereich „Verbindung“ ein.

Verbindung

Domain

ihse.com

☐ Hostname nutzen

Hostname/IP-Adresse

☐ TLS/SSL benutzen

Port

389

Standardwert: 389

☒ Server-Zertifikat verifizieren

[Zertifikatsverwaltung](#)

Abb. 138 Administration - LDAP-Server - **Verbindungseinstellungen**

Parameter	Beschreibung
Domain	Konfigurierbar, wenn „Typ“ auf „Active Directory-Server“ eingestellt ist. Der Domänenname des Active Directory-Servers. In der Regel kann die User Station den Hostnamen des Active Directory-Servers anhand seines Domänennamens und über DNS ermitteln. Wenn Sie das folgende Kontrollkästchen „Hostname nutzen“ aktivieren, wird dieses Verhalten außer Kraft gesetzt.
Hostname nutzen	Konfigurierbar, wenn „Typ“ auf „Active Directory-Server“ eingestellt ist. Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Hostnamen oder die IP-Adresse des Active Directory-Servers manuell angeben möchten.
Hostname/IP-Adresse	Hostname oder IP-Adresse des LDAP-Servers
TLS/SSL benutzen	Aktivieren Sie dieses Kontrollkästchen, wenn für den LDAP-Server eine sichere Verbindung erforderlich ist.
Port	TCP-Port für die LDAP-Authentifizierung, dessen Standardwert einer der folgenden Werte ist: 389 (Standard) 636 (TLS/SSL)
Server-Zertifikat verifizieren	Kann konfiguriert werden, wenn das Kontrollkästchen „TLS/SSL verwenden“ aktiviert ist.
Zertifikatsverwaltung	Klicken Sie auf diesen Link, um bei Bedarf ein CA-Zertifikat zu installieren (siehe Abschnitt 9.5, Seite 126).

 Derzeit wird bei verschlüsselten LDAP-Verbindungen kein FIPS-zertifizierter kryptografischer Code verwendet.

5. Geben Sie unter Autorisierung die Autorisierungsdaten ein.

Authorisierung

Base DN

IHSE

Nutzername-Attribut

sAMAccountName

Standardwert: sAMAccountName

Suchfilter

(objectClass=user)

Standardwert: (objectClass=user)

Suchbereich

Alle Ebenen darunter

Zugangsdaten

Nutzer-Zugangsdaten

Admin DN

Admin-Passwort

....

☐ Authorisierung nach der Suche

Standardwert: false

Abb. 139 Administration - LDAP-Server - Autorisierungseinstellungen

Parameter	Beschreibung
Base DN	Distinguished Name (DN) der Suchbasis, die den Ausgangspunkt der LDAP-Suche bildet • Beispiel: ou=dev, dc=testlab, dc=com
Nutzername-Attribut	Das Attribut der LDAP-Nutzerklasse, das den Anmeldenamen angibt. Beachten Sie, dass in diesem Feld nur relative Distinguished Names (RDNs) angegeben werden können. • Beispiel: cn
Suchfilter	Suchkriterien zum Auffinden von LDAP-Benutzerobjekten innerhalb der Verzeichnisstruktur.
Suchbereich	Die Tiefe, in der nach LDAP-Benutzerobjekten gesucht wird, beginnend auf der Verzeichnisebene beim „Base DN“. • Eins: Durchsucht ein Level unterhalb der base DN, die base DN ist nicht dabei. • Alle Ebenen darunter: Durchsucht alle Level unterhalb der base DN, die ebenfalls durchsucht wird.
Zugangsdaten	Wenn für die Authentifizierung eines Benutzers eine LDAP-Suche erforderlich ist, geben Sie die entsprechenden Suchzugangsdaten an: • Keine Suche: Es wird keine LDAP-Suche durchgeführt. • anonym: Ermöglicht die LDAP-Suche ohne spezifizierte Suchzugangsdaten. • Nutzer-Zugangsdaten: Ermöglicht die LDAP-Suche durch Eingabe der entsprechenden Suchzugangsdaten – DN und Passwort.

Admin DN Admin Password	Konfigurierbar, wenn „Zugangsdaten suchen“ auf „Nutzer-Zugangsdaten“ eingestellt ist. Distinguished Name und Passwort des Administratornutzers, der zur Durchführung der LDAP-Suche berechtigt ist.
Autorisierung nach der Suche	Konfigurierbar, wenn „Zugangsdaten“ NICHT auf „Keine Suche“ gesetzt ist. Aktivieren Sie dieses Kontrollkästchen, wenn der LDAP-Autorisierungs-Vorgang mit einem DN durchgeführt werden soll, der aus einer Suche nach dem Nutzer abgeleitet wurde, der sich anzumelden versucht. Diese Checkbox ist standardmäßig: - Deaktiviert für den „Active Directory Server“ - Aktiviert für den LDAP-Server.

6. Um LDAP-Gruppen für die Autorisierung zu nutzen, konfigurieren Sie den Bereich „Gruppen“.

Gruppen

☒ Gruppen für die Autorisierung auswerten
☐ Gruppen-DN für Suche benutzen
Gruppen-DN für Suche

Gruppen-ID-Attribut

Standardwert: sAMAccountName
Gruppenmitgliedsattribut

Standardwert: member
Gruppensuchfilter

Standardwert: (objectClass=group)
Gruppensuchbereich

Abb. 140 Administration - LDAP-Server - Gruppeneinstellungen

Parameter	Beschreibung
Gruppen für die Autorisierung auswerten	Aktivieren Sie dieses Kontrollkästchen, wenn eine Autorisierung über LDAP vorgesehen ist. Wenn diese Option deaktiviert ist, wird die Autorisierung von der User Station verwaltet, und dieser LDAP-Server übernimmt lediglich die Authentifizierung.
Gruppen-DN für Suche benutzen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie anstelle des „Basis-DN“ für Benutzergruppen nach einem bestimmten Basis-DN suchen möchten. Wenn diese Option deaktiviert ist, wird für die Gruppensuche der „Basis-DN“ verwendet.
Gruppen-DN für Suche	Konfigurierbar, wenn „Gruppen-DN für Suche benutzen“ aktiviert ist. Der spezielle Basis-DN für die Gruppensuche.
Gruppen-ID-Attribut	Das Attribut der LDAP-Gruppenklasse, das die ID der Gruppe angibt, die zum Abgleich mit lokalen Gruppennamen verwendet wird.
Gruppenmitgliedsattribut	Das Attribut der LDAP-Gruppenklasse, das die Benutzer angibt, die einer Gruppe angehören. Sein Wert muss einer der folgenden sein: - Nutzer-DN. - Wert des „Nutzername-Attributs“.  Wenn der Wert nicht einer dieser beiden ist, funktioniert die Erkennung von Gruppenmitgliedern möglicherweise nicht wie erwartet.
Gruppensuchfilter	Suchkriterien zum Auffinden von LDAP-Gruppenobjekten innerhalb der Verzeichnisstruktur.
Gruppensuchbereich	Die Tiefe, in der nach LDAP-Gruppenobjekten gesucht wird; sie beginnt auf der Verzeichnisebene, die durch den „Base DN“ oder einen „Base DN für die Gruppensuche“ angegeben wird. - Eins: Durchsucht ein Level unterhalb der base DN, die base DN ist nicht dabei. - Alle Ebenen darunter: Durchsucht alle Level unterhalb der base DN, die ebenfalls durchsucht wird.

7. Um zu prüfen, ob die Verbindung zum neuen LDAP-Server erfolgreich hergestellt werden kann, geben Sie den LDAP-Benutzernamen und das Passwort im Abschnitt „Verbindung testen“ ein und klicken Sie auf **Testen**.

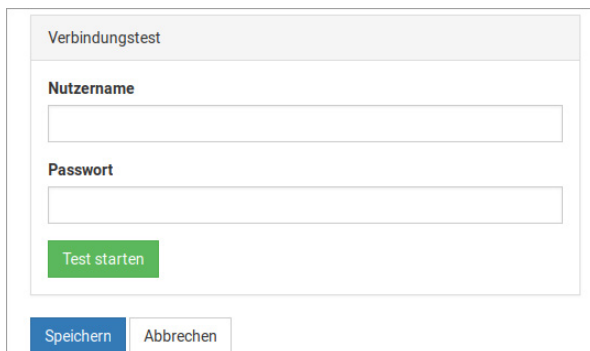


Abb. 141 Administration - LDAP-Servers -**Verbindungstest**

8. Klicken Sie auf **Speichern**.
9. Wiederholen Sie die Schritte, um bei Bedarf weitere LDAP-Server hinzuzufügen.

9.4.2 LDAP-Server bearbeiten oder löschen

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > LDAP**. Die LDAP-Seite wird mit einer Liste der konfigurierten LDAP-Server angezeigt.

LDAP-Server					
		Suche	Server hinzufügen	Einstellungen	LDAP ist deaktiviert
Reihenfolge	Aktiv	Host	Port	Typ	
1	☒	ihse.com	389	Active Directory Server	☒ Bearbeiten ☐ Löschen
2	☒	192.168.6.92	389	LDAP Server	☒ Bearbeiten ☐ Löschen
3	☐	192.168.6.108	389	Active Directory Server	☐ Bearbeiten ☐ Löschen
4	☒	tw.otechadd.com	636	Active Directory Server	☒ Bearbeiten ☐ Löschen

Abb. 142 Administration - LDAP-Server - **Liste konfigurierter LDAP-Server**

2. Klicken Sie auf den Button **Bearbeiten** in der Zeile des LDAP-Servers, dessen Einstellungen Sie bearbeiten möchten. Die entsprechende Seite wird geöffnet.
3. Nehmen Sie die erforderlichen Änderungen an den angezeigten Einstellungen vor (siehe Abbildungen im vorherigen Abschnitt)
4. Klicken Sie auf **Speichern**.

Löschen eines LDAP-Servers

1. Klicken Sie auf den Button **Löschen** in der Zeile des LDAP-Servers, den Sie aus der Liste entfernen wollen. Eine Bestätigungsmeldung erscheint.
2. Klicken Sie auf **OK**.

9.4.3 Aktivieren/Deaktivieren der LDAP-Authentifizierung

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > LDAP**, um die LDAP-Seite zu öffnen. Der Button oben rechts kennzeichnet die momentane LDAP-Authentifizierungseinstellung.

Button	Beschreibung
LDAP ist deaktiviert	LDAP-Authentifizierung ist deaktiviert, dies ist die Standardeinstellung. Wenn diese Funktion deaktiviert ist, werden alle Nutzer über die lokale Datenbank der User Station authentifiziert, sodass ihre Zugangsdaten auf der User Station verfügbar sein müssen. Daher können sich nur lokale Nutzer anmelden.
LDAP ist aktiviert	LDAP-Authentifizierung ist aktiviert. Solange diese Funktion aktiviert ist, werden alle Benutzer über die LDAP-Server authentifiziert, sodass sich nur LDAP-Benutzer anmelden können. Der einzige lokale Benutzer, der sich anmelden kann, ist der Standard-Administrator <i>admin</i> .

2. Klicken Sie auf den Button, um zwischen diesen beiden Einstellungen umzuschalten.

✓ Auf der Seite „LDAP-Einstellungen bearbeiten“ können Sie auch die LDAP-Authentifizierung aktivieren oder deaktivieren. Um nur einen bestimmten LDAP-Server zu aktivieren oder zu deaktivieren, setzen Sie ein Häkchen in das Kontrollkästchen des LDAP-Servers in der Spalte „Aktiv“ bzw. entfernen Sie das Häkchen.

9.4.4 Suche nach LDAP-Nutzern und -Gruppen

Wenn die LDAP-Authentifizierung aktiviert ist, ist auch die Schaltfläche „Suche“ aktiviert, und Sie können bei Bedarf manuell nach LDAP-Nutzern oder -Gruppen suchen.

Reihenfolge	Aktiv	Host	Port	Typ	
1	☒	ihse.com	389	Active Directory Server	Bearbeiten Löschen
2	☒	192.168.6.92	389	LDAP Server	Bearbeiten Löschen
3	☐	192.168.6.108	389	Active Directory Server	Bearbeiten Löschen
4	☒	tw.otechadd.com	636	Active Directory Server	Bearbeiten Löschen

Abb. 143 Administration - LDAP-Servers - **LAPD-Authentifizierung aktiviert**

1. Klicken Sie auf den Button **Suche**. Die entsprechende Seite wird geöffnet.

Abb. 144 Administration - LDAP-Servers - **Suchmenü**

2. Im "Server" Feld wählen Sie den gewünschten LDAP-Server aus der Liste der aktiven LDAP-Server aus.
3. Die folgenden Einstellungen auf dieser Seite sind bereits mit den Werten des ausgewählten LDAP-Servers vorgelegt, Sie können sie jedoch an Ihre Suchanforderungen anpassen. Wenn Sie mit den LDAP-Einstellungen nicht vertraut sind, wenden Sie sich bitte an Ihren LDAP-Administrator.

Parameter	Beschreibung
Zugangsdaten	Ein oder zwei Optionen sind verfügbar, abhängig von der Konfiguration des gewählten LDAP-Servers. • Gespeicherte admin-Zugangsdaten: Die admin-Daten, die in der Konfiguration des LDAP-Servers gespeichert sind, werden verwendet. • Benutzerdefiniert: Die Zugangsdaten in den folgenden zwei Feldern werden verwendet.
Bind DN, Passwort	Wenn „benutzerdefiniert“ ausgewählt ist, müssen diese Felder ausgefüllt werden.
Typ	Die Art der zu durchsuchenden Benutzerdaten – Nutzer oder Gruppe.
Base DN	Distinguished Name der Suchbasis, die den Startpunkt der LDAP-Suche darstellt.

Suchfilter	Suchkriterien zum Auffinden von LDAP-Benutzerobjekten innerhalb der Verzeichnisstruktur.
Suchbereich	Die Tiefe der Suche nach LDAP-Nutzer und -Gruppen, die beim Verzeichnislevel startet, das durch „Base DN“ definiert ist. • Base: Suche nur in der base DN • Erste Ebene darunter: Suche in einem Level unterhalb des base DN, ohne den base DN • Alle Ebenen darunter: Suche in allen Level unterhalb des base DN, einschließlich des base DN.

4. Klicken Sie auf **Suchen**.

5. Aus den Suchergebnissen können Sie die gewünschten LDAP-Nutzer oder -Gruppen auswählen und sie der User Station hinzufügen, indem Sie auf eine der folgenden Optionen klicken:

Option	Beschreibung
Als lokalen Nutzer hinzufügen	Dieser Button wird für diejenigen Nutzer angezeigt, die noch nicht zur User Station hinzugefügt wurden. ➔ Klicken Sie auf diesen Button, um den LDAP-Nutzer als lokalen Nutzer hinzuzufügen, der im Modus „Nur LDAP-Authentifizierung“ auch über LDAP authentifiziert werden kann. ➔ Die Authentifizierung wird von der User Station verwaltet. Stellen Sie daher sicher, dass dieser Nutzer Mitglied in mindestens einer Gruppe in der lokalen Datenbank ist.
Diese Gruppe hinzufügen	Dieser Button wird für diejenigen Gruppen angezeigt, die noch nicht zur User Station hinzugefügt wurden. ➔ Klicken Sie auf diesen Button, um die LDAP-Gruppe als Gruppe hinzuzufügen, der die Berechtigungen „Geräte-Zugang“, „Einstellungen ändern“ und „Den Port-Scanner starten“ zugewiesen sind ➔ Die Berechtigung „Scanner-Schnappschüsse speichern“ kann vom Administrator hinzugefügt werden. Informationen zum Ändern der Berechtigungen finden Sie im Abschnitt 9.2.2, Seite 112.
Ausgewähltes hinzufügen	➔ Um mehrere LDAP-Nutzer oder Gruppen gleichzeitig hinzuzufügen, aktivieren Sie deren Kontrollkästchen und klicken Sie anschließend auf diesen Button.

HINWEIS

Sie dürfen keine LDAP-Nutzer hinzufügen, deren Anmeldenamen nicht den Anforderungen der User Station für Anmeldenamen entsprechen. Diese LDAP-Nutzer können sich nicht bei der User Station anmelden. Informationen zu den Anforderungen an Anmeldenamen finden Sie im Abschnitt 9.1, Seite 105.

9.4.5 Konfiguration der maximalen Anzahl von Suchergebnissen und der Einstellungen für die lokale Authentifizierung

In den LDAP-Einstellungen können Sie Parameter für die maximale Anzahl an Suchergebnissen festlegen und lokalen Nutzern Zugriff gewähren.

1. Klicken Sie auf **Administration > LDAP** und dann auf den Button **Einstellungen**. Die entsprechende Seite wird geöffnet.

LDAP-Einstellungen bearbeiten

☒ Aktiviert

☒ Erlaube lokal authentifizierten Nutzern Zugang

Maximale Anzahl an Suchergebnissen

Abb. 145 Administration - LDAP-Server - **LAPD-Authentifizierung aktiviert**

- Die LDAP-Authentifizierung muss aktiviert sein, um die Begrenzung für die LDAP-Suchergebnisse festlegen zu können. Aktivieren Sie das Kontrollkästchen „Aktiviert“, falls es noch nicht aktiviert ist.
- Wählen Sie den gewünschten Wert in Feld „Maximale Anzahl an Suchergebnissen“ aus. Zur Auswahl stehen: 10, 100, 1000 oder 10.000.
- Aktivieren Sie das Kontrollkästchen „Erlaube lokal authentifizierten Nutzern Zugang“, um die lokale Authentifizierung auf dem Anmeldebildschirm zu aktivieren.
- Klicken Sie auf **Speichern**.

9.4.6 Anmelden mit LDAP

Wenn LDAP aktiviert ist, erscheint eine andere Anmeldebox nach dem Start. Das Symbol kennzeichnet den verwendeten Authentifizierungstyp: Lokal oder LDAP (siehe Abschnitt 4.3, Seite 17).

Wenn lokale Nutzer zugelassen sind (siehe vorheriger Abschnitt), steht den Nutzern zusätzlich ein Kontrollkästchen zur „lokalen Authentifizierung“ zur Verfügung.

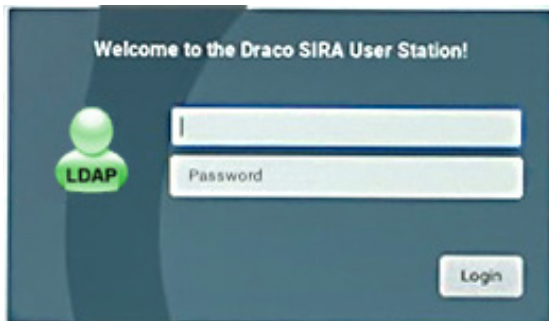


Abb. 146 Anmelden mit LDAP

9.4.7 Fehlermeldung bei LDAP-Anmeldung

Der Anmeldeversuch eines LDAP-Nutzers kann mit folgender Meldung im Ereignisprotokoll fehlschlagen:

- Login of <username> failed with hostname <IP address> does not match the certificate at LDAPs://<IP address>.

Lösung:

- Klicken Sie im Hauptmenü auf **User-Station-Konfiguration > Administration > LDAP**.
- Klicken Sie auf den Button **Bearbeiten** in der Zeile des LDAP-Servers.
- Geben Sie im Feld Hostname/IP-Adresse den Hostnamen anstelle der IP-Adresse ein oder deaktivieren Sie, wenn möglich, die Funktion „TLS/SSL benutzen“.

9.5 Vertrauenswürdige Zertifikate

In den folgenden Fällen müssen vertrauenswürdige Zertifikate auf der User Station installiert werden:

- Zum Herstellen der LDAP-Verbindung.
Wenden Sie sich an Ihren LDAP-Server-Administrator, um die CA-Zertifikatsdatei zu erhalten, und installieren Sie diese auf der User Station.
- Wenn der FIPS-Modus aktiviert ist, werden alle verschlüsselten Verbindungen zu KVM-/seriellen Switches mithilfe des FIPS-zertifizierten Verschlüsselungsalgorithmus verarbeitet, und die Authentizität dieser KVM-/seriellen Switches wird anhand ihrer Zertifikatskette überprüft. Sie müssen das vertrauenswürdige Gerät oder das Stammzertifikat jedes KVM-/seriellen Switches auf der User Station installieren, da sonst die Verbindung fehlschlägt.

9.5.1 CA-Zertifikate installieren

1. Schließen Sie einen USB-Stick an die User Station an oder binden Sie einen Netzwerkspeicher ein, der die entsprechende Zertifikatsdatei enthält. Zertifikatsdateien müssen einen der folgenden Dateitypen haben: PEM, DER, TXT, CER oder CRT und müssen ein PEM- oder DER-kodiertes Zertifikat enthalten.
2. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Vertrauenswürdige Zertifikate**.

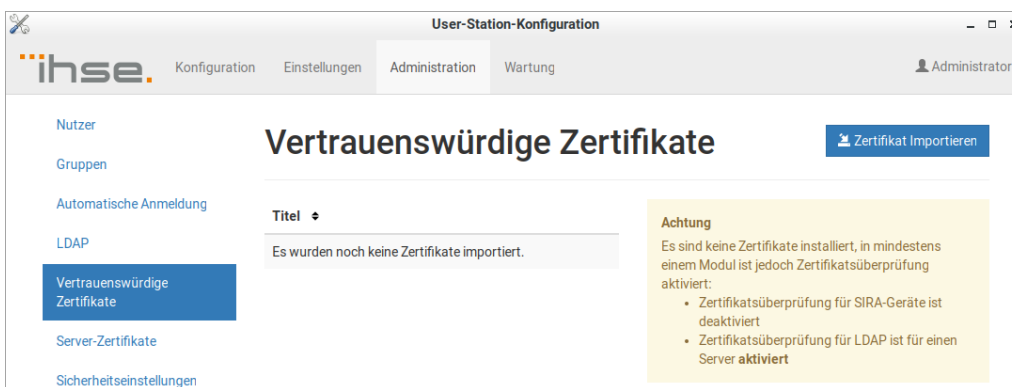


Abb. 147 Administration - Vertrauenswürdige Zertifikate

3. Klicken Sie auf den Button **Zertifikat importieren**. Die Importseite wird geöffnet mit einer Liste der erkannten Zertifikate.
4. Wählen Sie das gewünschte Zertifikat aus und klicken Sie auf „**Importieren**“. Der Inhalt des installierten Zertifikats wird angezeigt.
5. Klicken Sie auf **Zurück zu allen Zertifikaten**, um zur Startseite zurückzukommen.
6. Wenn Sie mehrere Zertifikate benötigen, wiederholen Sie die Schritte 3 bis 5.

9.5.2 Installierte Zertifikate entfernen

Sollte ein installiertes Zertifikat veraltet, ungültig oder nicht mehr erforderlich sein, können Sie es entfernen.

1. Klicken Sie auf **Administration > Vertrauenswürdige Zertifikate**. Eine Liste aller installierter Zertifikate erscheint.
2. Klicken Sie auf das rote Mülleimer-Symbol in der Zeile des Zertifikats, das Sie entfernen wollen. Sie können auch auf das Zertifikat klicken, um sich die Details anzeigen zu lassen, und dann auf den Button **Entfernen** klicken.
3. Eine Bestätigungsmeldung erscheint. Klicken Sie auf **OK**.

9.6 Server-Zertifikate

Netzwerkbasierende Dienste, wie beispielsweise die Fernsteuerung, werden mit TLS gesichert. Dazu muss auf der Draco SIRA User Station ein TLS-Zertifikat installiert werden.

Standardmäßig verfügt die Draco SIRA User Station über ein Demo-Zertifikat. Sie benötigen System-administratorrechte, um das Zertifikat anzuzeigen, herunterzuladen oder zu ändern. Ein neues Zertifikat kann auf zwei Arten installiert werden:

- Hochladen eines neuen Zertifikats und eines privaten Schlüssels (siehe Abschnitt 9.6.2, Seite 128).
- Erstellen eines privaten Schlüssels und eines selbstsignierten Zertifikats (siehe Abschnitt 9.6.3, Seite 129).

HINWEIS

Es wird dringend empfohlen, das vorinstallierte Demo-Serverzertifikat zu aktualisieren, wenn Sie die Fernsteuerungsfunktion nutzen möchten (siehe Abschnitt 9.10, Seite 141). Wird es nicht aktualisiert, wird folgende Warnmeldung angezeigt: „Sie verwenden weiterhin das vorinstallierte Serverzertifikat. Bitte ändern Sie es!“

9.6.1 Anzeigen des aktuellen Server-Zertifikats

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Server-Zertifikate**. Die Übersichtsinformationen zum vorinstallierten Zertifikat werden angezeigt.

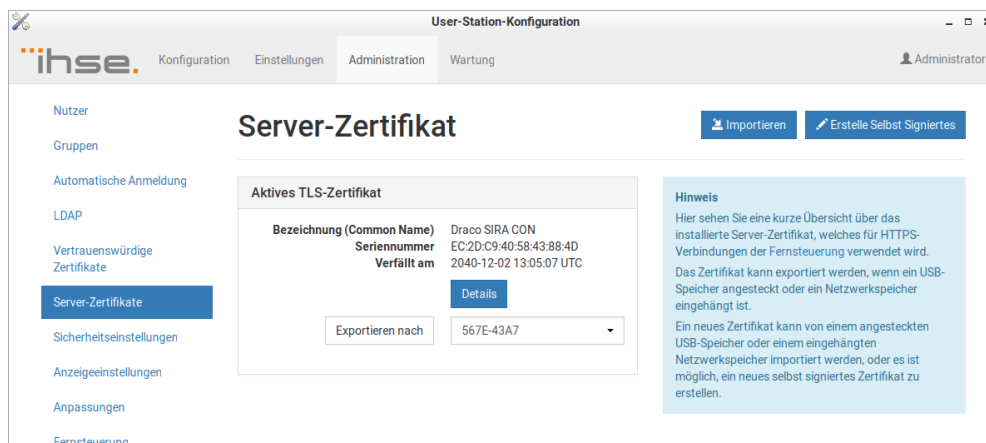


Abb. 148 Administration - Server-Zertifikat

2. Klicken Sie auf **Details**, um mehr Informationen des Zertifikats anzuzeigen.

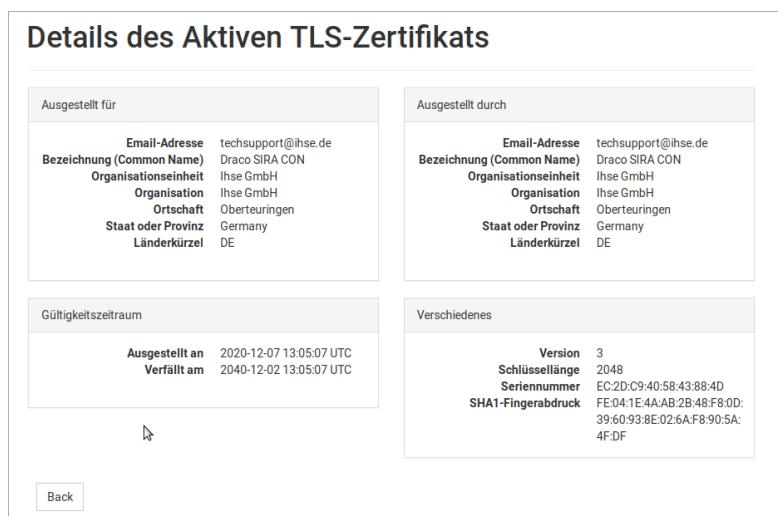


Abb. 149 Administration - Server-Zertifikate - Details des aktiven Zertifikats

Wenn ein USB-Stick angeschlossen oder ein Netzwerkspeicher eingebunden ist, können Sie die Datei exportieren.

3. Wählen Sie ein Speichermedium aus der Drop-Down-Liste aus und klicken Sie auf den Button **Exportieren nach**.

9.6.2 Privaten Schlüssel und Zertifikat importieren

Wenn Sie Ihren eigenen privaten Schlüssel und Ihr eigenes Zertifikat verwenden möchten, können Sie diese von einem angeschlossenen USB-Stick oder einem eingebundenen Netzwerkspeicher importieren.

Durch eine Passphrase geschützte Schlüssel werden nicht unterstützt. Der private Schlüssel und das Zertifikat müssen in einer Datei zusammengefasst sein. Folgende Dateiformate werden unterstützt:

- PEM Format (*.txt, *.pem)
- PCCS12 (*.p12, *.pfx)

Wenn das importierte Zertifikat ungültig ist, nicht den Regeln entspricht oder aus anderen Gründen nicht ausgewertet werden kann, wird eine Fehlermeldung angezeigt.

1. Schließen Sie einen USB-Stick an die User Station an, auf dem sich das entsprechende Zertifikat im Stammverzeichnis befindet, oder verwenden Sie einen eingebundenen Netzwerkspeicher.
2. Klicken Sie auf **Administration > Server-Zertifikat**.
3. Klicken Sie auf den Button **Importieren**. Die Dateinamen der Zertifikate, die im Stammverzeichnis des USB-Sticks oder des Netzwerkspeichers gefunden wurden, werden in einer Liste angezeigt.



Abb. 150 Administration - Server-Zertifikat - **Privaten Schlüssel und Zertifikat importieren**

4. Klicken Sie auf den Button **Importieren** in der Zeile des gewünschten Zertifikats. Die Datei wird importiert und validiert. Die Details des Zertifikats werden angezeigt.

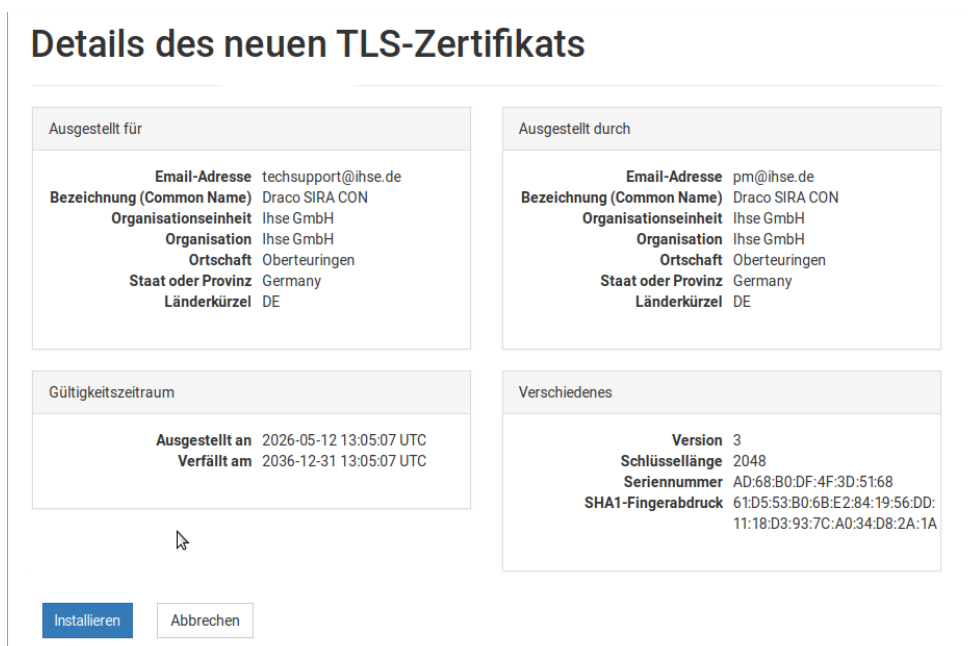


Abb. 151 Administration - Server-Zertifikat - **Installieren eines importierten Zertifikats**

5. Klicken Sie auf **Installieren**, um dieses Zertifikat zu verwenden. Danach muss die User Station neu gestartet werden. Führen Sie einen Neustart der User Station durch (siehe Abschnitt 5.2.8, Seite 25).

9.6.3 Selbst Signiertes Zertifikat erstellen

Wenn Sie ein selbstsigniertes Zertifikat verwenden möchten, können Sie den privaten Schlüssel und das Zertifikat mit Hilfe der User Station erstellen. Nachdem Sie das Zertifikat erstellt haben, können Sie es installieren.

1. Klicken Sie auf **Administration > Server-Zertifikate**.

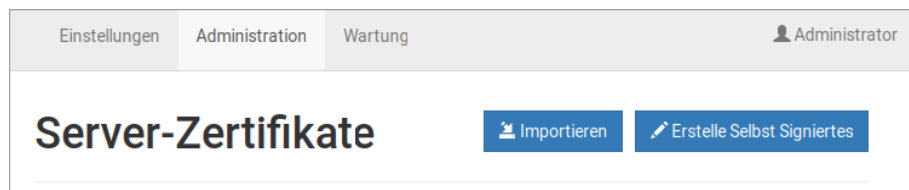


Abb. 152 Administration - Server-Zertifikate - **Button Erstelle Selbst Signiertes**

2. Klicken Sie auf den Button **Erstelle Selbst Signiertes**. Die Seite „Erstellen“ wird geöffnet.

Abb. 153 Administration - Server-Zertifikate - **Erstellen eines selbstsignierten Zertifikats**

3. Geben Sie die Zertifikatsdaten und Schlüsselparameter ein.

Feld	Werte
Länderkürzel	Muss aus 2 Großbuchstaben bestehen
Staat oder Provinz	Names des Staates, Landes oder der Provinz
Ortschaft	Name der Stadt, Ortschaft, etc.
Organisation	Optional
Organisationseinheit	Optional
Common Name	Muss ein Hostname sein
E-Mail	Optional
Schlüssellänge	2048 oder 3096
Gültigkeit in Tagen	1 bis 36525

4. Klicken Sie auf **Erstellen**. Das Zertifikat und die Schlüsseldetails werden angezeigt.
5. Klicken Sie auf **Installieren**, um dieses Zertifikat zu nutzen. Danach muss die User Station neu gestartet werden.
6. Starten Sie die User Station neu (siehe Abschnitt 5.2.8, Seite 25).

9.7 Sicherheitseinstellungen

Die User Station nutzt optional ein FIPS 140-2-Verschlüsselungsmodul, das die Sicherheitsanforderungen für kryptografische Module des Federal Information Processing Standard (FIPS) erfüllt, die in FIPS PUN 140-2, Anhang A: „Approved Security Functions“ (Zugelassene Sicherheitsfunktionen) definiert sind. Diese Standards dienen dem Schutz sensibler Informationen der US-Bundesregierung und der kanadischen Regierung durch kryptografische Sicherheitssysteme.

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Sicherheitseinstellungen**. Die entsprechende Seite wird geöffnet und zeigt die aktuellen Einstellungen an.

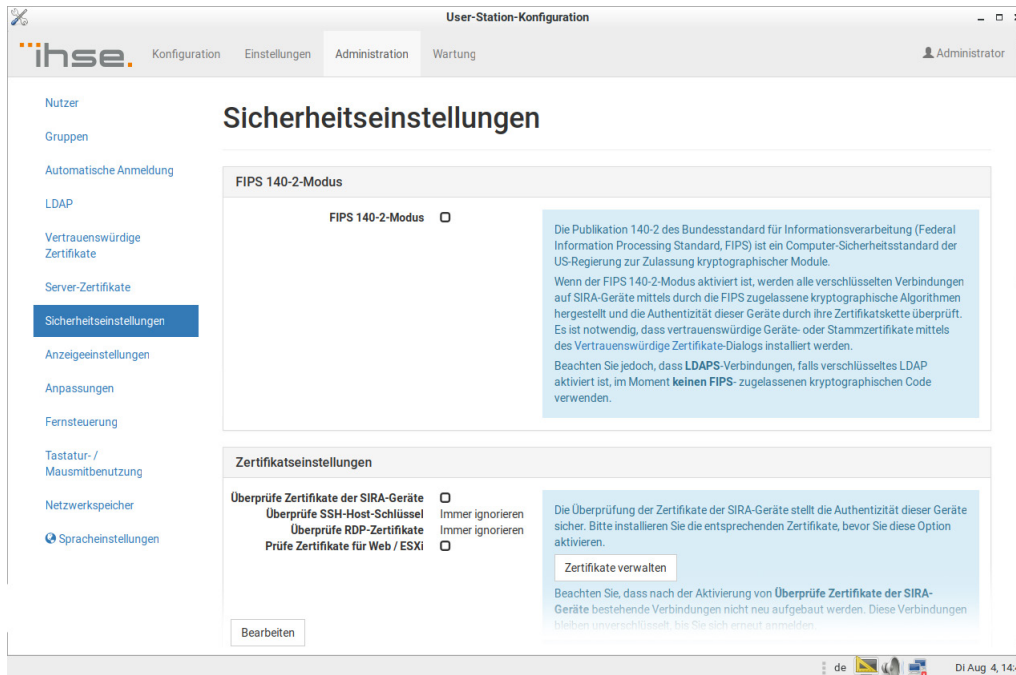


Abb. 154 Administration - Sicherheitseinstellungen

9.7.1 FIPS-Modus aktivieren/deaktivieren

Wenn der „FIPS 140-2-Modus“ aktiviert ist, werden alle verschlüsselten Verbindungen zu KVM-/seriellen Switchen unter Verwendung des FIPS-zertifizierten Verschlüsselungsalgorithmus verarbeitet, und die Authentizität dieser KVM-/seriellen Switches wird anhand ihrer Zertifikatskette überprüft.

 Derzeit wird bei verschlüsselten LDAP-Verbindungen kein FIPS-zertifizierter kryptografischer Code verwendet.

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.

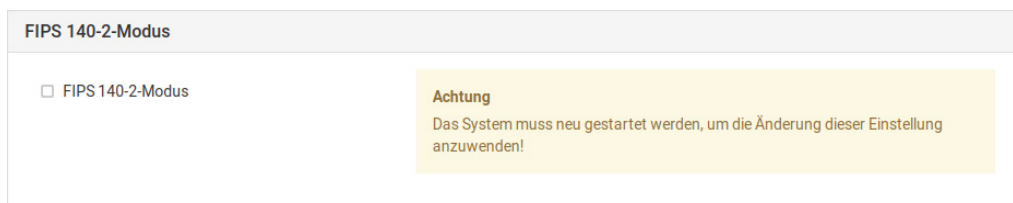


Abb. 155 Administration - Sicherheitseinstellungen - Bearbeiten: FIPS-Modus

2. Aktivieren Sie das Kontrollkästchen, um den FIPS 140-2-Modus zu aktivieren.

 Im FIPS-Modus kann die User Station keine Verbindung zu einem KVM-Target auf einem SIRA-Gerät herstellen, wenn die Sicherheitseinstellungen des Geräts ausschließlich auf TLS 1.3 festgelegt sind, und es gelingt ihr auch nicht, eine Verbindung mit RDP-Clients herzustellen.

3. Klicken Sie auf **Speichern** und auf **OK** in der Bestätigungsmeldung. Die User Station wird neu gestartet.
4. Warten Sie, bis die Anmeldebox erscheint.

9.7.2 Geräte-Zertifikatsüberprüfungen aktivieren/deaktivieren

Wenn die Option „Überprüfe Zertifikate der SIRA-Geräte“ aktiviert ist, wird die Authentizität von KVM-/seriellen Switches anhand ihrer Zertifikatskette überprüft. Sie müssen das vertrauenswürdige Geräte- oder Stammzertifikat jedes KVM-/seriellen Switches auf der User Station installieren, da sonst die Verbindung zu den KVM-/seriellen Switches fehlschlägt (siehe Abschnitt 9.5, Seite 126).

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.

Abb. 156 Administration - Sicherheitseinstellungen - **Bearbeiten: Zertifikatseinstellungen**

2. Aktivieren Sie die Checkbox „Überprüfe Zertifikate der SIRA-Geräte“.
3. Für diese Option müssen Zertifikate installiert sein. Klicken Sie auf den Button „Zertifikate verwalten“, um die Zertifikate zu überprüfen oder zu installieren (siehe Abschnitt 9.5, Seite 126). Die Überprüfung des Hostnamens anhand des Zertifikats ist zwingend erforderlich.
4. Klicken Sie auf **Speichern** und auf **OK** in der Bestätigungsmeldung.

9.7.3 Überprüfung von Schlüsseln und Zertifikaten für SSH-, RDP-, WEB- und ESXi-Clients aktivieren

Um die Sicherheit zu erhöhen, können Sie SSH-, RDP-, WEB- und ESXi-Schlüssel sowie Zertifikate speichern. Diese Schlüssel und Zertifikate werden pro Target und pro Benutzer gespeichert.

 Standardmäßig wird die Überprüfung von SSH-Schlüsseln sowie von RDP-, WEB- und ESXi-Zertifikaten ignoriert.

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.
2. Wählen Sie im Feld „Überprüfe SSH-Host-Schlüssel“ im Bereich „Zertifikatseinstellungen“ (siehe Abbildung oben) einen Eintrag aus dem Drop-Down-Menü aus. Sie können wählen zwischen:
 - Immer ignorieren
 - Akzeptiere bei erster Verbindung
 - Frage bei erster Verbindung
 - Immer nachfragen
 - Unbekannte Host-Schlüssel ablehnen
3. Klicken Sie auf **Speichern**. Der SSH-Schlüssel wird im Abschnitt „SSH-Host-Schlüssel“ auf der Seite „Einstellungen bearbeiten“ des SSH-Clients angezeigt (siehe nächste Abbildung).
4. Um einen SSH-Schlüssel zu löschen, klicken Sie auf **User-Station-Konfiguration > Targets**.
5. In der Target-Liste klicken Sie auf den Editierbutton  in der Zeile des SSH-Zugangs, dessen Schlüssel Sie löschen wollen.
6. Scrollen Sie nach unten zum Abschnitt SSH-Host-Schlüssel und klicken Sie auf den Button **Löschen**, um den Schlüssel zu löschen.

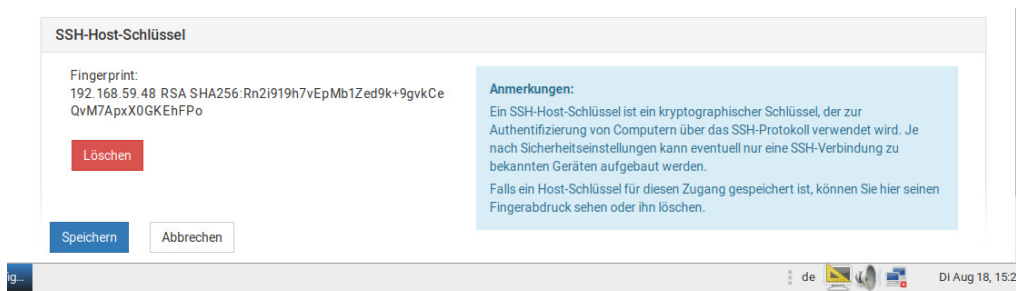


Abb. 157 Konfiguration- Targets - Bearbeitungsseite SSH-Zugang - SSH-Host-Schlüssel

RDP-Zertifikatsüberprüfung konfigurieren

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.
2. Wählen Sie im Feld „Überprüfe RDP-Zertifikate“ im Bereich „Zertifikateinstellungen“ einen Eintrag aus dem Drop-Down-Menü aus. Sie können wählen zwischen:
 - Immer ignorieren
 - Akzeptiere bei erster Verbindung
 - Frage bei erster Verbindung
 - Unbekannte Zertifikate ablehnen
3. Klicken Sie auf **Speichern**. Das RDP-Zertifikat wird in der Bearbeitungsseite des RDP-Zugangs angezeigt.
4. Um ein RDP-Zertifikat zu löschen, klicken Sie auf **User-Station-Konfiguration > Targets**.
5. In der Target-Liste klicken Sie den Editierbutton  in der Zeile des RDP-Zugangs, dessen Zertifikat Sie löschen wollen.
6. Scrollen Sie nach unten zum Abschnitt RDP-Zertifikat und klicken Sie auf den Button **Löschen**, um das RDP-Zertifikat zu löschen.

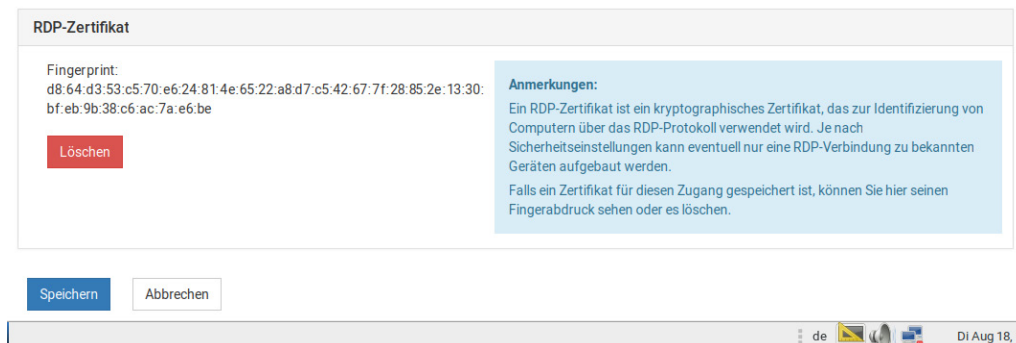


Abb. 158 Konfiguration- Targets - Bearbeitungsseite RDP-Zugang - RDP-Zertifikat

WEB- und ESXi-Zertifikatsüberprüfung konfigurieren

 Web- und ESXi-Zertifikate können unter „Vertrauenswürdige Zertifikate“ installiert werden (siehe Abschnitt 9.5, Seite 126).

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.
2. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen „Zertifikate für Web- und ESXi-Ziele überprüfen“ im Feld „Zertifikateinstellungen“ (siehe Abb. 156, Seite 131).
3. Scrollen sie nach unten und klicken Sie auf **Speichern**.

 Durch die Aktivierung der Zertifikatsüberprüfung für Web- und ESXi-Ziele werden HTTPS-Zertifikatsprüfungen erzwungen.

9.7.4 Passwort-Einstellungen

Zur Erhöhung der Sicherheit können die Passwortalterung und sichere Passwörter aktiviert werden. Die Passwortalterung zwingt Benutzer dazu, ihre Passwörter regelmäßig zu ändern. Bei sicheren Passwörtern können die erforderliche Länge und die erforderlichen Zeichen festgelegt sowie die Wiederverwendung alter Passwörter eingeschränkt werden.

✓ „Starke Passwörter“ ist standardmäßig aktiviert.

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.
2. Scrollen Sie nach unten zum Abschnitt „Passwort-Einstellungen“.

Passwort-Einstellungen

☐ Passwort-Gültigkeit einschränken

Passwort-Gültigkeitsdauer

60 Tage

☒ Starke Passwörter

Minimale Passwortlänge

8

☒ Erzwingen mindestens einen Kleinbuchstaben

☒ Erzwingen mindestens einen Großbuchstaben

☒ Erzwingen mindestens eine Ziffer

☐ Erzwingen mindestens ein Sonderzeichen

Anzahl letzter Passwörter

5

Um die Sicherheit des Systems zu erhöhen, können Sie eine Passwort-Gültigkeitsdauer einstellen, oder Sie können Starke Passwörter erzwingen.

Anmerkungen:

- Falls eine Passwort-Gültigkeitsdauer eingestellt ist und ein Nutzer das letzte Mal sein Passwort mit einer Firmware-Version ohne Unterstützung für Starke Passwörter geändert hat, wird dieser Nutzer bei der nächsten Anmeldung gezwungen, sein Passwort zu ändern, unabhängig von der eingestellten Gültigkeitsdauer.
- Die Einstellung Starke Passwörter wirkt sich nur auf neue Passwörter aus. Falls Nutzer "schwache" Passwörter haben und Starke Passwörter später aktiviert wird, werden diese nicht zum Ändern der Passwörter gezwungen.

Abb. 159 Administration - Sicherheitseinstellungen - Bearbeitungsseite - Passwordeinstellungen

3. Aktivieren Sie die Funktion „Passwort-Gültigkeit“ einschränken, wenn Sie die Gültigkeit begrenzen wollen.
4. Wählen Sie aus dem Drop-Down-Menü die gewünschte Zeitspanne aus (7, 14, 30, 60, 90, 180 oder 365 Tage).
5. Deaktivieren Sie das Kontrollkästchen „Starke Passwörter“, wenn Sie die Nutzer nicht dazu verpflichten möchten, Passwörter zu erstellen, die den festgelegten zusätzlichen Kriterien entsprechen.
6. Wenn Sie starke Passwörter möchten, wählen Sie die gewünschten Kriterien aus.
7. Wählen Sie eine Anzahl der letzten Passwörter aus, die nicht wieder verwendet werden dürfen. Beispiel: Wenn Sie hier 5 auswählen, kann ein Nutzer keines der letzten fünf Passwörter als neues Passwort verwenden.
8. Scrollen Sie nach unten und klicken Sie auf **Speichern**.

9.7.5 Nutzersperren

Die Optionen zu Nutzersperren legen die Kriterien fest, nach denen Benutzer nach einer bestimmten Anzahl erfolgloser Anmeldeversuche daran gehindert werden, eine Verbindung zum System herzustellen.

✓ Der Standard admin Nutzer ist von den Nutzersperren ausgenommen.

Wenn ein gesperrter Nutzer versucht, sich anzumelden, wird auf dem Anmeldebildschirm die Meldung „Authentifizierung fehlgeschlagen“ angezeigt. Die Nutzer werden nicht darüber informiert, dass sie gesperrt ist. Bei der Sperrung eines Nutzers wird eine Meldung im Ereignisprotokoll erstellt.

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.
2. Scrollen Sie nach unten zum Abschnitt „Nutzersperren“.

Nutzersperren

☒ Nutzer bei fehlgeschlagener Anmeldung sperren

Sperrdauer

10 Minuten

Anzahl Fehlversuche

3

Mit diesen Einstellungen können Nutzer nach einer angegebenen Anzahl von fehlgeschlagenen Anmeldeversuchen von der Benutzung des Systems gesperrt werden.

Abb. 160 Administration - Sicherheitseinstellungen - **Bearbeitungsseite - Nutzersperren**

- Aktivieren Sie die Checkbox „Nutzer bei fehlgeschlagener Anmeldung sperren“, um diese Funktion einzuschalten.
- Wählen Sie eine Zeitspanne aus der Drop-Down-Liste „Sperrdauer“ aus. So lange ist der Nutzer gesperrt.
- Definieren Sie unter „Anzahl Fehlversuche“ die Anzahl der Fehlversuche, die zu einer Sperrung führen. Mindestwert ist hier 3.
- Scrollen Sie nach unten und klicken Sie auf **Speichern**.

9.7.5.1 Entsperren eines Nutzers

Nutzer werden nach Ablauf der festgelegten Zeit automatisch entsperrt, oder ein System-Administrator kann den Nutzer in der Nutzerkonfiguration bereits früher entsperren. Der Sperrstatus wird in der Nutzerliste angezeigt.

Nutzer						Auswahl löschen	Neuer Nutzer
☐ Nutzername	Name	Typ Lokal	Gruppen	Letzte Anmeldung	Aktionen		
☐ Daria	Daria Muster	Local	Office 1	2026-05-20 08:02:58 <local>	☒ Bearbeiten ☐ Löschen		
☐ Musterfrau	Lia Musterfrau	Local	Devices Administrators Devices Users	2026-05-20 09:11:26 <local>	☒ Bearbeiten ☐ Löschen		
☐ Mustermann	Max Mustermann	Local	Devices Users Office 1	2026-05-20 08:12:05 <local>	☒ Bearbeiten ☐ Löschen ☒ Entsperren		
admin	Administrator	Local		2026-05-20 08:09:13 <local>	☒ Bearbeiten		

Abb. 161 Administration - Nutzer - **Nutzerliste**

- ➔ Klicken Sie auf den Button **Entsperren** in der Zeile des gesperrten Nutzers, um die Sperrung sofort aufzuheben.

9.7.6 Links und Weiterleitungen

Mit der Option „Links und Weiterleitungen“ können Sie Weiterleitungen oder Verknüpfungen zu externen Websites von WEB- und ESXi-Clients einrichten. Sie können festlegen, ob Links oder Weiterleitungen zu externen Seiten zulässig sind. Wenn Sie dies zulassen, können Sie außerdem Seiten in der Ausnahmeliste angeben, um das Sicherheitsrisiko zu minimieren.

☒ Standardmäßig sind Links und Weiterleitungen zu Web- und ESXi-Zielen untersagt.

- Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.
- Scrollen Sie nach unten zum Abschnitt „Links und Weiterleitungen“.

Abb. 162 Administration - Sicherheitseinstellungen - **Links und Weiterleitungen**

3. Im Abschnitt „Erlaube Links / Weiterleitungen für Web-Targets“ wählen Sie eine der folgenden Optionen aus:
 - Verbiete alle Links und Weiterleitungen (Standardeinstellung)
 - Erlaube die aufgelisteten Links und Weiterleitungen
 - Erlaube alle Links und Weiterleitungen
4. Wenn Sie die zweite Option ausgewählt haben, fügen Sie die URLs, die Sie zulassen möchten, zur Liste „Ausnahmeliste für Web-Targets“ hinzu.
5. Klicken Sie auf den blauen + Button, um weitere URLs der Liste hinzuzufügen.
6. Um eine URL zu löschen, klicken Sie auf den blauen - Button.
7. Machen Sie dasselbe für die ESXi-Targets.

☒ Die Anzahl der hinzugefügten Links ist unbegrenzt. Links und Weiterleitungen funktionieren nicht, wenn der Firefox-Webbrowser verwendet wird.

8. Scrollen Sie nach unten und klicken Sie auf **Speichern**.

9.7.7 Nutzungsbedingungen

Nachdem die Funktion „Zustimmung zu Nutzungsbedingungen erfordern“ aktiviert wurde, wird der Inhalt der Vereinbarung auf dem Anmeldebildschirm angezeigt. Benutzer müssen ein Kontrollkästchen aktivieren, um der Erklärung zuzustimmen und sich anzumelden.

Abb. 163 Anmeldemaske mit Nutzungsbedingungen

1. Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.

2. Scrollen Sie nach unten zum Abschnitt „Nutzungsbedingungen“.

Nutzungsbedingungen

☐ Zustimmung zu Nutzungsbedingungen erfordern

Text der Nutzungsbedingungen

Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

Abb. 164 Administration - Sicherheitseinstellungen - Nutzungsbedingungen

- Um die Funktion zu aktivieren, setzen Sie ein Häkchen im Kontrollkästchen „Zustimmung zu Nutzungsbedingungen erfordern“.
- Es wird ein Standardtext (in englisch) für die Bedingungen bereitgestellt. Sie können den Standardtext nach Belieben bearbeiten oder ersetzen.
- Klicken Sie auf **Speichern**.

9.8 Anzeigeeinstellungen

Das Display der User Station kann so konfiguriert werden, dass der Monitor bei Inaktivität ausgeschaltet wird und entweder der Bildschirm gesperrt oder der Nutzer automatisch abgemeldet wird. Diese Einstellungen umfassen die Bildschirmsperre, die Bildschirmskalierung und die Desktop-Skalierung und gelten einheitlich für alle Nutzer.

Sie benötigen System-Administrator-Rechte, um die Anzeigeeinstellungen zu konfigurieren.

 Port-Scanne-Sessions und KVM-Sessions verhindern nicht das Ausschalten des Monitors und/oder die Bildschirmsperre, wenn diese Optionen konfiguriert sind.

- Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Anzeigeeinstellungen**. Die entsprechende Seite erscheint.

ihse.

Konfiguration

Einstellungen

Administration

Wartung

Administrator

Nutzer
Gruppen
Automatische Anmeldung
LDAP
Vertrauenswürdige Zertifikate
Server-Zertifikate
Sicherheitseinstellungen
Anzeigeeinstellungen
Anpassungen
Fernsteuerung

Anzeigeeinstellungen

Bildschirmschoner-Einstellungen

Monitor im Leerlauf ausschalten

Nie

Bildschirm im Leerlauf sperren

☐

Skalierungseinstellungen

Desktop-Skalierung

100%

Bearbeiten

Abb. 165 Administration - Anzeigeeinstellungen

- Klicken Sie auf **Bearbeiten**, um die Bearbeitungsseite zu öffnen.

Abb. 166 Administration - Anzeigeeinstellungen - **Bearbeitungsseite**

3. Um den Monitor nach Ablauf einer Inaktivitätszeit auszuschalten, wählen Sie die Dauer aus:
 - Wählen Sie „Nie“, um den Monitor dauerhaft anzulassen.
 - Wählen Sie eine Zeit in Minuten aus (1, 2, 3, 4, 5, 10, 15, 30 oder 60 Minute(n)), nach der der Monitor bei Inaktivität ausgeschaltet wird.
4. Um den Bildschirm bei Inaktivität zu sperren, aktivieren Sie das Kontrollkästchen „Bildschirm im Leerlauf sperren“. Die Bildschirmsperre kann nur in Verbindung mit der Option „Monitor im Leerlauf ausschalten“ nach Ablauf der Inaktivitätszeit aktiviert werden. Wie Sie den Bildschirm entsperren, ist im folgenden Abschnitt beschrieben.
5. Im Abschnitt Skalierungseinstellungen wählen Sie unter „Desktop-Skalierung“ den Wert aus, der am besten zu Ihrem Monitor passt:
 - 100%
 - 200%

Wenn Sie einen 4K UHD Monitor nutzen, könnte 200% besser sein.
6. Klicken Sie auf **Speichern**.

9.8.1 Monitor entsperren

Wenn der Bildschirm der User Station gesperrt ist, werden keine Daten angezeigt.

Wenn Sie versuchen, den Bildschirm zu entsperren, erscheint eine Passwortabfrage. Nur der Nutzer, der den Bildschirm gesperrt hat, kann die User Station entsperren. Andere Nutzer müssen den momentanen Nutzer abmelden und anschließend wieder an der User Station anmelden, wenn sie diese bedienen möchten.

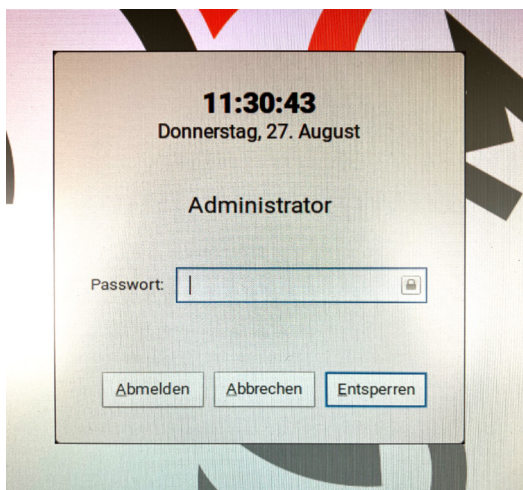


Abb. 167 **Bildschirm gesperrt**

Entsperren der User Station

1. Drücken Sie eine beliebige Taste auf der Tastatur.
2. Eine Passwort-Aufforderung erscheint (siehe Abbildung auf vorheriger Seite).
3. Geben Sie das Passwort des Nutzers ein, der die Bildschirmsperre initiiert hat (Administrator in der Abbildung).
4. Klicken Sie auf den Button **Entsperren**.

Abmelden von der User Station

1. Wenn Sie nicht der Nutzer sind, der den Bildschirmsperrmodus ausgelöst hat, klicken Sie auf den Button **Abmelden**. Ein Passwort ist nicht erforderlich.
2. Die übliche Anmeldebox erscheint, und Sie können sich mit Ihren Anmeldedaten anmelden.

9.9 Anpassungen

Um das Erscheinungsbild der Benutzeroberfläche Ihrer Draco SIRA User Station anzupassen, können Sie den standardmäßigen Draco-Desktop-Hintergrund, das Anwendungslogo und den Anmeldebildschirm durch eigene Bilder und Texte ersetzen. Hierfür sind System-Administratorrechte erforderlich.

Die Anpassungen gelten für alle Nutzer. Änderungen werden im Ereignisprotokoll zusammen mit dem Namen der Bilddatei und dem Namen des Nutzers, der die Änderung vorgenommen hat, protokolliert. Die Anpassungen werden bei Sicherungen und Wiederherstellungen berücksichtigt, während bei einer Werksrücksetzung die ursprünglichen Standardbilder wiederhergestellt werden. Sie können die Standardeinstellungen außerdem jederzeit wiederherstellen.

Bilddateien müssen zum Hochladen im Stammverzeichnis eines USB-Sticks oder eines eingebundenen Netzwerkspeichers gespeichert werden

Anforderungen an Bilder

- Desktop-Hintergrundbild:
JPG, PNG oder SVG Dateien bis zu 128 MB, gleichmäßige Hintergrundfarbe, die nicht transparent ist.
 - Anwendungslogo:
Erscheint im Konfigurationsmenü in der oberen linken Ecke. JPG, PNG oder SVG Bilder bis zu 512 kB, Anwendungslogos werden automatisch skaliert auf 110 x 48 Pixel oder 220 x 96 Pixel, wenn 200% Desktop-Skalierung eingestellt ist.
 - Logo in Anmeldebildschirm:
JPG, PNG oder SVG Dateien bis zu 512 kB, Logos werden automatisch skaliert auf 80 x 80 Pixel oder 160 x 160 Pixel, wenn 200 % Desktop-Skalierung eingestellt ist.
1. Speichern Sie die gewünschten Bilddateien auf einem USB-Stick und schließen Sie diesen an die User Station an, oder speichern Sie sie auf einem eingebundenen Netzwerkspeicher.
 2. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Anpassung**. Die entsprechende Seite wird geöffnet.

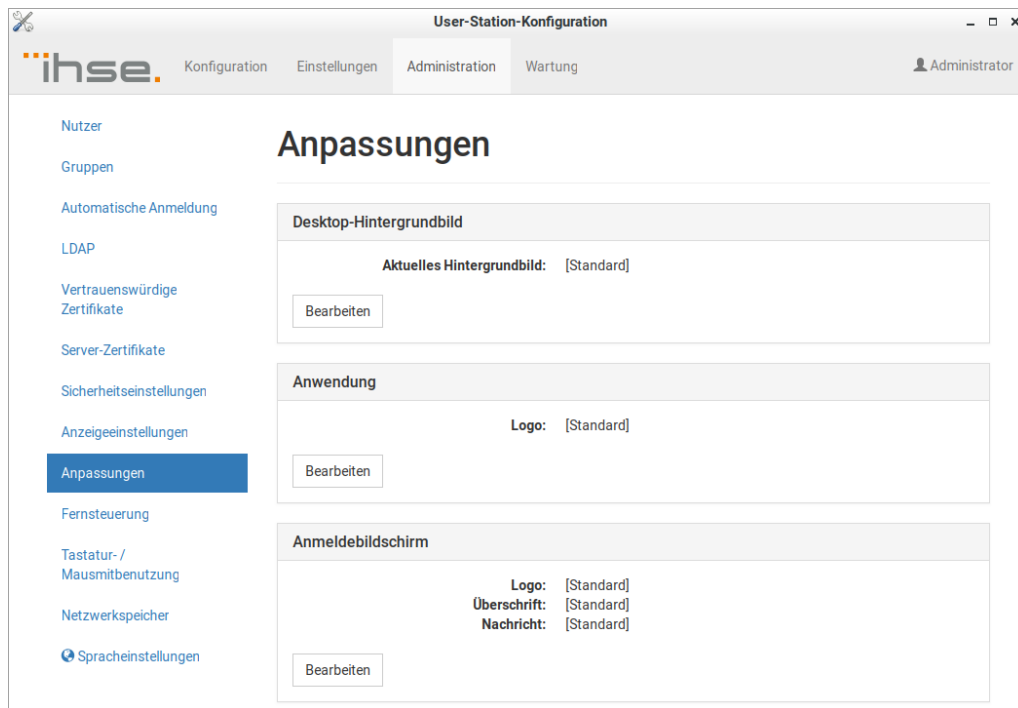


Abb. 168 Administration - Anpassungen

3. Klicken Sie auf den Button **Bearbeiten** in dem Bereich, den Sie ändern möchten.
 - Desktop-Hintergrundbild: nur das Hintergrundbild
 - Anwendung: nur das Anwendungslogo
 - Anmeldebildschirm: Logo, zusätzlich Kopfzeile und Textoptionen für Nachrichten.

Ausführliches Beispiel mit Änderung des Hintergrundbildes

1. Klicken Sie auf den Button **Bearbeiten** im Abschnitt „Desktop-Hintergrundbild“.



Abb. 169 Administration - Anpassungen - Desktop-Hintergrund ändern

Auf dem beigefügten USB-Stick wurden drei Bilder gefunden, die den Anforderungen an Desktop-Hintergrundbilder entsprechen und hier aufgeführt sind.

2. Wählen Sie das gewünschte Bild als Desktop-Hintergrund aus und klicken Sie in der Zeile des ausgewählten Bildes auf den Button **Übernehmen**.

Hintergrundbild wurde erfolgreich gesetzt.

Desktop-Hintergrundbild

Aktuelles Hintergrundbild: Castle.jpg

Standard Installieren

USB- und Netzwerkspeicher	Background Image	Size	
567E-43A7	1000031016.jpg	4.04 MB	Übernehmen
	Castle.jpg	382 KB	Übernehmen
	Darts.jpg	323 KB	Übernehmen

Achtung

Um das Desktop-Hintergrundbild zu ändern, stecken Sie einen USB-Speicher (z.B. einen USB-Stick), an oder hängen Sie einen Netzwerkspeicher ein, welcher die Bilddatei in seinem Hauptverzeichnis enthält.

Die Bilddatei muss die Endung .jpg, .png oder .svg (ohne Unterscheidung von Groß- und Kleinschreibung) haben, und es sind nur Dateien mit einer Maximalgröße von 128 MB erlaubt.

Das Hintergrundbild wird für alle Benutzer angewandt und das Standard-Hintergrundbild kann mit dem 'Standard Installieren'-Button wiederhergestellt werden.

Zurück

Abb. 170 Administration - Anpassungen - Desktop-Hintergrund geändert

Der Name des ausgewählten Bildes erscheint hinter „Aktuelles Hintergrundbild“ und der Button **Standard Installieren** ist aktiv.

Standard-Hintergrundbild wieder installieren

1. Klicken Sie auf den Button **Standard Installieren**, um das Standard-Hintergrundbild wieder zu installieren.
2. Ein Bestätigungsaufforderung erscheint. Klicken Sie auf **OK**, um das Standard-Hintergrundbild wieder zu verwenden oder auf **Cancel**, um das ausgewählte Bild zu behalten.
3. Nachdem das gewünschte Bild installiert ist, klicken Sie auf den Button **Zurück**, um zur Anpassungsseite zurückzukehren.

Auf dieselbe Weise ändern Sie die Logos in den anderen beiden Abschnitten. Im Abschnitt „Anmeldebildschirm“ können Sie zusätzlich die Überschrift ändern und eine Nachricht eingeben, die auf dem Anmeldebildschirm erscheint.

Anmeldebildschirm-Anpassung

Aktuelles Anmeldebildschirm-Logo:

Standard Installieren

USB- und Netzwerkspeicher	Anmeldebildschirm-Logo	Größe	
567E-43A7	1000031016.jpg	4.04 MB	Übernehmen
	Castle.jpg	382 KB	Übernehmen
	Darts.png	323 KB	Übernehmen

Achtung

Um das Anmeldebildschirm-Logo zu ändern, stecken Sie einen USB-Speicher (z.B. einen USB-Stick), an oder hängen Sie einen Netzwerkspeicher ein, welcher die Bilddatei in seinem Hauptverzeichnis enthält.

Die Bilddatei muss die Endung .jpg oder .png (ohne Unterscheidung von Groß- und Kleinschreibung) haben, und es sind nur Dateien mit einer Maximalgröße von 512 KB erlaubt.

Das Standard-Anmeldebildschirm-Logo kann mit dem 'Standard Installieren'-Button wiederhergestellt werden.

Überschrift

Willkommen auf der User Station

Nachricht

Frohes Schaffen!

Speichern

Abbrechen

Abb. 171 Administration - Anpassungen - Anmeldebildschirm geändert

4. Klicken Sie auf **Speichern**, um die Überschrift und die Nachricht zu speichern.

9.10 Fernsteuerungs-Einstellungen

Ein häufiger Anwendungsfall für die Fernsteuerung ist die Verbindung der gesteuerten User Station mit einem Wandmonitor, um die Anzeige verschiedener Target-Server über einen Webbrowser auf dem Monitor fernzusteuern. Stellen Sie über einen Webbrowser eine Verbindung zur Fernsteuerungsschnittstelle der User Station her, indem Sie die IP-Adresse oder den Hostnamen als URL eingeben. Melden Sie sich wie gewohnt an. Nach erfolgreicher Anmeldung zeigt die User Station den Port-Navigator genauso an, wie er in der lokalen Konsole erscheint. Das Auswählen und Öffnen von Ports funktioniert genauso wie in der lokalen Konsole, allerdings öffnen sich die KVM-Clients auf der ferngesteuerten User Station im Vollbildmodus. Wenn „Uneingeschränkter Navigator“ aktiviert ist, können Sie außerdem Funktionen zur Fensterverwaltung und zum Fensterlayout nutzen, mehrere Sessions starten und eine Ansicht außerhalb des Vollbildmodus verwenden.

Die Fernsteuerung kann auch über die RESTful-API (HTTPS & JSON) erfolgen, um die User Station programmgesteuert aus Kundenanwendungen heraus zu steuern. Es gibt zwei Hauptanwendungsfälle: das Starten von Sessions oder Fensterlayouts und/oder das Ausführen von Verwaltungsaufgaben.

➔ Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Fernsteuerung**. Die entsprechende Seite wird geöffnet.

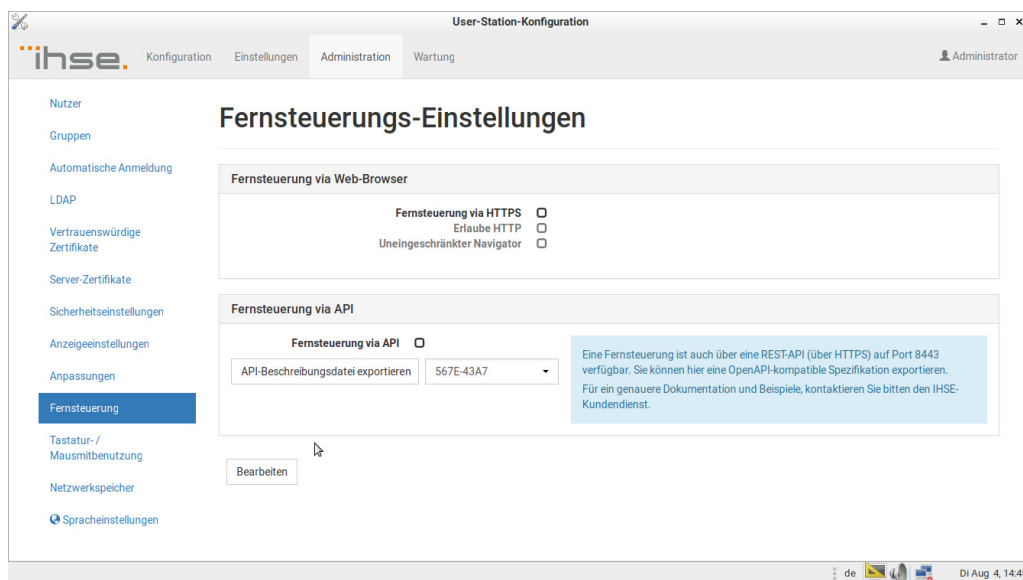


Abb. 172 Administration - Fernsteuerungs-Einstellungen

9.10.1 Fernsteuerung via Web-Browser

Die Fernsteuerung über den Webbrowser ermöglicht die Steuerung der User Station über einen Web-Browser, auf den mit einem Smartphone oder PC zugegriffen werden kann, das bzw. der über das Netzwerk mit der User Station verbunden ist.

Standardmäßig bietet die Fernsteuerung über den Web-Browser nur Vollbild-Sessions an, ohne Zugriff auf Fensterlayouts oder die Fensterverwaltung. Aktivieren Sie die Einstellung „Uneingeschränkter Navigator“, um diese Funktionen zu den Fernsteuerungssessions hinzuzufügen.

Zur Konfiguration der Fernsteuerungsfunktion sind Systemadministratorrechte erforderlich.

Unterstützte Browser

- Chrome 60+
- Firefox 52+
- Safari 11+
- Microsoft Edge 42+

1. Klicken Sie auf den Button **Bearbeiten**. Die Bearbeitungsseite wird geöffnet.

Fernsteuerung via Web-Browser

☐ Fernsteuerung via HTTPS
☐ Erlaube HTTP
☐ Uneingeschränkter Navigator

Diese Option aktiviert die Fernsteuerung der User Station via HTTPS. HTTP-Zugang ist möglich, wird aber nicht empfohlen.

Normalerweise werden ferngesteuerte Sitzungen auf eine Client-Verbindung im Vollbildmodus beschränkt. Wenn **Uneingeschränkter Navigator** aktiviert ist, dann erlaubt der fernbediente Navigator das Starten mehrerer Verbindungen im Nicht-Vollbildmodus gleichzeitig. Zusätzlich können im Uneingeschränkten Modus Fensteranordnungen und Fensterverwaltung verwendet werden.

Abb. 173 Administration - Fernsteuerungs-Einstellungen - **Fernsteuerung via Web-Browser einstellen**

2. Aktivieren Sie die Checkbox „Fernsteuerung via HTTPS“, um diese Funktion einzuschalten.
3. Aktivieren Sie das Kontrollkästchen „Erlaube HTTP“, um die Fernsteuerung über HTTPS und HTTP zu aktivieren. Wenn das Kontrollkästchen „Erlaube HTTP“ nicht aktiviert ist, wird HTTP auf HTTPS umgeleitet.
4. Aktivieren Sie „Uneingeschränkter Navigator“, um zusätzliche Funktionen zu aktivieren:
 - Der uneingeschränkte Navigator kann Sessions im Nicht-Vollbildmodus starten und mehrere Sessions gleichzeitig anzeigen.
 - Fensterlayouts und Fensterverwaltung können über die Fernsteuerung verwendet werden.
5. Klicken Sie auf **Speichern**.

9.10.2 Fernsteuerung via API

Die Draco SIRA User Station unterstützt eine Remote-RESTful-API über HTTPS, wodurch eine programmierte Fernsteuerung möglich ist, um:

- Zugangs-Client-Sessions oder Fensterlayouts zu starten
- Bestimmte administrative Aufgaben zu erledigen.
- Mehr über API siehe Kapitel 11, ab Seite 166

API-Überblick

- PI kann unabhängig von den regulären Fernbedienungseinstellungen aktiviert werden.
- API nutzt HTTPS (HTTP ist keine Option), Empfang über Port 8443.
- Wenn die Fernsteuerung aktiviert ist, ist API nur über Port 8443 verfügbar.
- Eine normale Fernbedienung kann nicht auf Port 8443 verwendet werden.
- API ist nicht über die üblichen Fernsteuerungsports 80 und 443 verfügbar
- API nutzt JSON-Dokumente für POST Request-Daten (Methodenparameter) und Responses.
- Ein Kontrollkästchen auf der Seite „Fernsteuerungs-Einstellungen“ aktiviert bzw. deaktiviert den API-Zugriff, der standardmäßig deaktiviert ist.
- Das Dokument mit der API-Beschreibung (im OpenAPI-Format) kann auf einen USB-Stick oder einen Netzwerkspeicher exportiert werden.
- Das TLS-Zertifikat kann über die Einstellung „Server-Zertifikate“ in der Konfiguration der User Station konfiguriert werden.

1. Klicken Sie auf den Button **Bearbeiten**. Die Bearbeitungsseite wird geöffnet.

Fernsteuerungs-Einstellungen bearbeiten

Fernsteuerung via Web-Browser

☒ Fernsteuerung via HTTPS
☐ Erlaube HTTP
☐ Uneingeschränkter Navigator

Diese Option aktiviert die Fernsteuerung der User Station via HTTPS. HTTP-Zugang ist möglich, wird aber nicht empfohlen.

Normalerweise werden ferngesteuerte Sitzungen auf eine Client-Verbindung im Vollbildmodus beschränkt. Wenn **Uneingeschränkter Navigator** aktiviert ist, dann erlaubt der fernbediente Navigator das Starten mehrerer Verbindungen im Nicht-Vollbildmodus gleichzeitig. Zusätzlich können im Uneingeschränkten Modus Fensteranordnungen und Fensterverwaltung verwenden.

Fernsteuerung via API

☒ Fernsteuerung via API
 567E-43A7

Eine Fernsteuerung ist auch über eine REST-API (über HTTPS) auf Port 8443 verfügbar. Sie können hier eine OpenAPI-kompatible Spezifikation exportieren.

Für ein genauere Dokumentation und Beispiele, kontaktieren Sie bitten den IHSE-Kundendienst.

Abb. 174 Administration - Fernsteuerungs-Einstellungen - **Fernsteuerung via API einstellen**

- Aktivieren Sie die Checkbox „Fernsteuerung via HTTPS“ im Abschnitt „Fernsteuerung via Web-Browser“.
- Aktivieren Sie die Checkbox „Fernsteuerung via API“.
- Um die API-Beschreibungsdatei zu exportieren, wählen Sie im Drop-Down-Menü einen angeschlossenen USB-Stick oder einen konfigurierten Netzwerkspeicher aus und klicken Sie auf die Schaltfläche „API-Beschreibungsdatei exportieren“.
- Klicken Sie auf **Speichern**.

API verwenden

- Erstellen Sie eine Anmelde-Session, um weitere Aufrufe zu authentifizieren. Es gibt API-Aufrufe zum Erstellen der Anmelde-Sessions.
- Die Remote-API-Session ist an eine lokale Nutzersession gebunden. Wenn sich ein API-Nutzer anmeldet, geschieht Folgendes:
 - Wenn der API-Benutzer bereits auf der lokalen Konsole angemeldet ist, übernimmt die API die Session.
 - Wenn auf der lokalen Konsole kein Nutzer angemeldet ist, wird der API-Nutzer automatisch angemeldet.
 - Wenn ein anderer Nutzer an der lokalen Konsole angemeldet ist, wird dieser abgemeldet und der API-Nutzer angemeldet.
- Sobald die Session erstellt wurde, nutzt die API HTTP-Cookies zur Authentifizierung. Beim Aufbau der Session erhält der Client Cookies. Diese Cookies müssen bei weiteren API-Anfragen mitgesendet werden.
- Nach Abschluss des Vorgangs kann sich der API-Nutzer von der Session abmelden. Durch die Abmeldung wird auch die Session auf der lokalen Konsole beendet (siehe API, Kapitel 11, ab Seite 166).

Zugang über iOS-Geräte

Sie müssen ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat auf Ihren Apple iOS-Geräten (iPad/iPhone) installieren, bevor Sie eine Verbindung zur Draco SIRA User Station herstellen können. Ist nur das Standardzertifikat vorhanden, wird der Zugriff verhindert. Je nach Browser wird möglicherweise eine Fehlermeldung wie „Diese Verbindung ist nicht privat“ angezeigt.

Bei der Erstellung von Zertifikaten sollte der „Common Name“ des Zertifikats mit der IP-Adresse bzw. dem Hostnamen übereinstimmen, die bzw. der für die Verbindung mit dem Gerät verwendet wird. Installieren Sie sowohl das Zertifikat der User Station als auch das CA-Zertifikat, mit dem das Zertifikat der User Station signiert wurde.

9.11 Tastatur - / Mausmitbenutzung

Mit der Tastatur-/Mausmitbenutzung können Sie mehrere Nutzerarbeitsplätze über eine einzige Tastatur und Maus steuern, die an einen der Nutzerarbeitsplätze angeschlossen ist. Dies kann in einem Kontrollraum mit mehreren Monitoren, die an verschiedene Arbeitsplätze angeschlossen sind, nützlich sein.

 Die Funktion zur gemeinsamen Nutzung von Tastatur und Maus unterstützt die Tasten „Caps“, „Num“ und „Scroll Lock“ nicht.

9.11.1 Beispiel einer erweiterten vertikalen Konfiguration

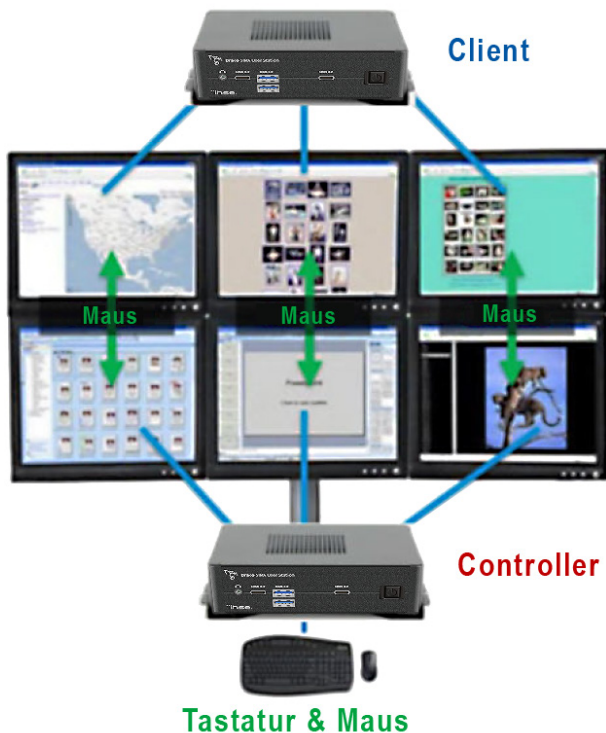


Abb. 175 Administration - Tastatur-/Mausmitbenutzung - Beispiel

Allgemeine Informationen

- Legen Sie eine User Station mit Tastatur und Maus als „Controller“ fest.
- Bezeichnen Sie alle anderen User Stations, mit denen Sie Tastatur und Maus gemeinsam nutzen möchten, als „Client“.
- Alle User Stations und Monitore müssen mit eindeutigen Bildschirmnamen versehen werden.
- Bildschirme können in beliebiger Anordnung bis zu einem 5×3-Raster hinzugefügt werden, solange jeder Bildschirm an mindestens einer Kante einen Nachbarn hat.
- Nach der Konfiguration bewegt sich die Maus entweder horizontal oder vertikal von Bildschirm zu Bildschirm.
- Jede User Station kann über einen Desktop mit mehreren Monitoren verfügen, sodass sich die Maus von den Rändern der einzelnen erweiterten Desktops aus bewegt.
- Jede User Station ist weiterhin unabhängig – KVM-Fenster können nicht von einer User Station auf eine andere gezogen werden.
- Die Monitore müssen zuerst konfiguriert werden (siehe Abschnitt 5.3.4, Seite 32).

Anordnung der Monitore für das Beispiel auf der vorherigen Seite

Einstellungen		
Bildschirmname	Client_1	
Anordnung der Bildschirme	Screen_Up_1	Screen_Up_2
	Screen_FRC_1	Screen_FRC_2

Abb. 176 Administration - Tastatur-/Mausmitbenutzung - Anordnung der Bildschirme

9.11.2 Konfiguration

Konfiguration der Clients

1. Melden Sie sich an einer Client User Station an.
1. Klicken Sie auf **Hauptmenü** > **User-Station-Konfiguration** > **Administration** > **Tastatur- /Mausmitbenutzung**. Die entsprechende Seite wird geöffnet.

Abb. 177 Administration - Tastatur-/Mausmitbenutzung - Startmenü

2. Klicken Sie auf den Button **Bearbeiten**. Die Bearbeitungsseite wird geöffnet.

Abb. 178 Administration - Tastatur-/Mausmitbenutzung - Client konfigurieren

3. Im Abschnitt „Allgemein“ aktivieren Sie die Checkbox „Aktiviert“.
4. Aktivieren Sie das Kontrollkästchen „Teile Fensteranordnungen“, damit gespeicherte Layouts in der Konfiguration für die Tastatur-/Mausmitbenutzung für alle Clients verfügbar sind.
 - Fensteranordnungen (Layouts) müssen auf allen User Stations manuell angelegt werden.
 - Wenn Sie ein Layout auf einer User Station wiederherstellen, stellen alle anderen User Stationen das Fensterlayout mit demselben Namen ebenfalls wieder her.
5. Aktivieren Sie das Kontrollkästchen „Melde Nutzer automatisch an/ab“, um Nutzer an allen mit der Tastatur-/Mausfreigabe verbundenen User Stations während der Nutzung der Konfiguration automatisch an- und abzumelden.
6. Geben Sie im Abschnitt „Client-Einstellungen“ einen Bildschirmnamen ein, um diesen Client zu identifizieren. Alle Bildschirme in der Konfiguration müssen eindeutige Namen haben mit:
 - Bis zu 64 Zeichen
 - Alphanumerische Zeichen sind erlaubt
 - Binde- und Unterstrich sind erlaubt
7. Geben Sie die IP-Adresse bzw. den Hostnamen der Controller-User Station ein, an die Tastatur und Maus angeschlossen sind.
8. Klicken Sie auf **Speichern** und wiederholen Sie diesen Vorgang für alle Client-Bildschirme.

Konfiguration der Controller User Station

1. Melden Sie sich an der Controller User Station an.
2. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Tastatur- /Mausmitbenutzung**. Die entsprechende Seite wird geöffnet.
3. Klicken Sie auf den Button **Bearbeiten**.

Tastatur- / Mausmitbenutzung Bearbeiten

Allgemein

☒ Aktiviert

* **Modus**

Controller

☒ Teile Fensteranordnungen

☐ Melde Nutzer automatisch an/ab

Mit dieser Funktion ist es möglich, ein Set von Tastatur und Maus zwischen mehreren User Stations zu teilen.

Bitte wählen Sie aus, ob Sie diese Einstellung aktivieren möchten und wählen Sie die Rolle dieser User Station:

- Controller: Die Tastatur und Maus dieser User Station mit anderen teilen
- Client: Die Tastatur und Maus einer anderen User Station mitbenutzen

Hinweise:

- Sie können zwar Tastatur und Maus mitbenutzen, es ist jedoch nicht möglich, Fenster von einer User Station zur anderen zu bewegen.
- Um Fensteranordnungen auf allen beteiligten User Stations wiederherzustellen, müssen Sie *Teile Fensteranordnungen* auf allen User Stations aktivieren, und Sie müssen die Fensteranordnungen auf allen User Stations manuell unter dem gleichen Namen erstellen.
- Um auf allen beteiligten User Stations Nutzer automatisch an- und abzumelden, die User Stations gemeinsam herunterzufahren und neu zu starten, müssen Sie *Melde Nutzer automatisch an/ab* auf allen User Stations aktivieren. Nutzernamen und Passwörter müssen an allen verbundenen Geräten übereinstimmen.

Controller-Einstellungen

* **Bildschirmname**

Front_Room_Control

* **Anordnung der Bildschirme**

Screen_Up_1	Client_1	Screen_Up_2		
Screen_FRC_1	Front_Room_Control	Screen_FRC_2		

The Screen Name is the name which identifies this User Station. It must be unique among all User Stations sharing one set of keyboard and mouse.

Please specify the Screen Names of all User Stations sharing keyboard and mouse and their arrangement in the grid below. This User Station's Screen Name must be part of the screen arrangement.

Speichern

Abbrechen

Abb. 179 Administration - Tastatur-/Mausmitbenutzung - Controller konfigurieren

4. Im Abschnitt „Allgemein“ aktivieren Sie die Checkbox „Aktiviert“.
5. Wählen Sie im Feld „Modus“ „Controller“ aus.
6. Aktivieren Sie das Kontrollkästchen „Teile Fensteranordnungen“, damit gespeicherte Layouts in der Konfiguration für die Tastatur-/Mausmitbenutzung für alle Clients verfügbar sind.
7. Aktivieren Sie das Kontrollkästchen „Melde Nutzer automatisch an/ab“, um Nutzer an allen mit der Tastatur-/Mausmitbenutzung verbundenen User Stations während der Nutzung der Konfiguration automatisch an- und abzumelden.
8. Geben Sie im Abschnitt „Controller-Einstellungen“ einen Bildschirmnamen ein, um diesen Controller Bildschirm zu identifizieren. Alle Bildschirme in der Konfiguration müssen eindeutige Namen haben mit:
 - Bis zu 64 Zeichen
 - Alphanumerische Zeichen sind erlaubt
 - Binde- und Unterstrich sind erlaubt
9. Geben Sie im Feld „Anordnung der Bildschirme“ den Namen dieses Controller-Bildschirms und aller Client-Bildschirme an der Stelle ein, die ihrer Position in der Anordnung entspricht.
 - Stellen Sie sicher, dass die hier eingegebenen Namen genau mit den Namen im Feld „Bildschirmname“ in der jeweiligen Client-Konfiguration übereinstimmen.
 - Doppelte Namen sind nicht zulässig, jeder Name darf nur einmal vorhanden sein.
 - Jeder Bildschirm muss mindestens einen benachbarten Bildschirm haben, entweder daneben, darüber oder darunter.
10. Klicken Sie auf **Speichern**.

Tastatur- / Mausmitbenutzung wurde erfolgreich aktualisiert. ×

Tastatur- / Mausmitbenutzung

Allgemein

Aktiviert ☒

Modus Controller (Die Tastatur und Maus dieser User Station mit anderen teilen)

Teile Fensteranordnungen ☒

Melde Nutzer automatisch an/ab ☐

Einstellungen

Bildschirmname

Anordnung der Bildschirme

Front_Room_Control

Screen_Up_1	Client_1	Screen_Up_2
Screen_FRC_1	Front_Room_Control	Screen_FRC_2

Bearbeiten

Abb. 180 Administration - Tastatur-/Mausmitbenutzung - Überblick der Konfiguration

9.12 Netzwerkspeicher

Sie können Netzwerkspeicher in der Draco SIRA User Station konfigurieren. Diese Speicher werden ähnlich wie USB-Speicher zur Installation von Updates, zum Exportieren von Diagnosedaten oder zur Sicherung und Wiederherstellung von Dateien verwendet.

Zwei Speichertypen werden unterstützt:

- NFS (Network File System)
- CIFS/SMB (Common Internet File System, Server Message Block)

Sie können die automatische Einbindung des Speichers beim Systemstart aktivieren oder dies manuell vornehmen.

 Wenn FIPS aktiviert ist, funktioniert die Verbindung zu CIFS/SMB-Speichern nicht.

Wichtige Informationen zum Netzwerkspeicher in der Draco SIRA User Station

- Sie benötigen Administratorrechte, um Netzwerkspeicher zu konfigurieren.
- Die Anzahl der Speicher ist nicht begrenzt.
- Der Netzwerkspeicher steht für alle Import- und Exportvorgänge zur Verfügung und wird ebenso wie USB-Sticks angezeigt.
- Netzwerkspeicher sind eine globale Einstellung und können von allen Nutzern genutzt werden.
- Bei der Erstellung, Änderung und Löschung von Netzwerkspeichern werden Einträge im Ereignisprotokoll erstellt.

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Netzwerkspeicher**. Die entsprechende Seite wird geöffnet.

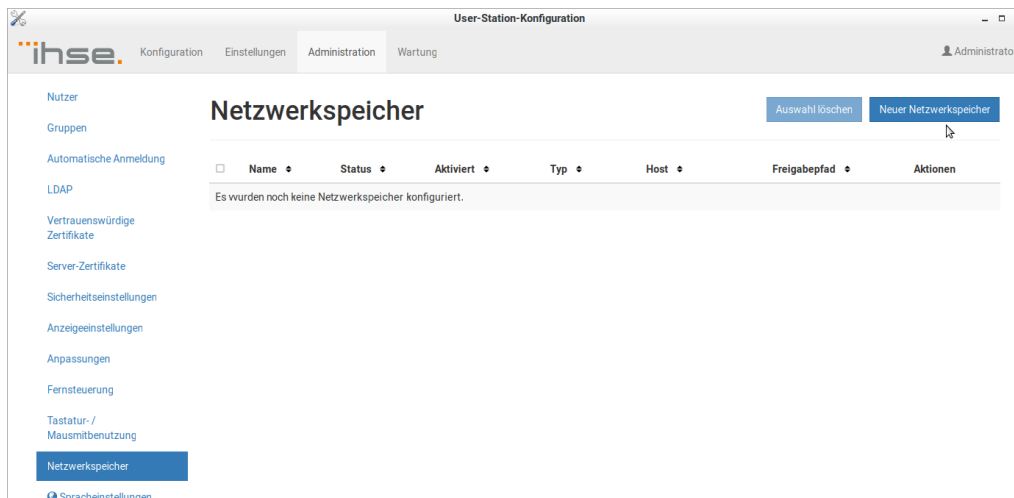


Abb. 181 Administration - **Netzwerkspeicher**

2. Klicken Sie auf den Button **Neuer Netzwerkspeicher**. Die Bearbeitungsseite wird geöffnet.

Neuer Netzwerkspeicher

Name

☒ Aktiviert

Typ

Host

Freigabepfad

Domäne

Nutzername

Passwort

Hier können Sie Netzwerkspeicher konfigurieren. Diese Speicher werden wie USB-Speicher benutzt, so können Sie z.B. Software-Aktualisierungen installieren, diagnostische Daten exportieren oder sie für Sicherungen und Wiederherstellungen benutzen.

Im Moment werden nur Freigaben vom Typ NFS (Network File System) und CIFS / SMB (Common Internet File System, Server Message Block) unterstützt.

Setzen Sie die Konfiguration auf Aktiviert, um ein automatisches Einhängen des Speichers beim Systemstart zu aktivieren. Sie können jederzeit den Netzwerkspeicher hier manuell einhängen.

Das Host-Feld muss auf den Hostnamen oder die IP-Adresse der Speicher-Servers gesetzt werden. Pfad ist der Pfad zum Speicherverzeichnis oder der Freigabe in der Form `/pfad/zur/freigabe`.

NFS-Speicher unterstützen keine Art der Authentifizierung. CIFS-Speicher unterstützen entweder anonyme Verbindungen (als Gast), oder authentifizierte Verbindungen. Um den Gäste-Modus zu verwenden, lassen Sie das Nutzernamen-Feld leer.

Abb. 182 Administration - Netzwerkspeicher - **Neuen Netzwerkspeicher anlegen**

- Geben Sie einen Namen für den Netzwerkspeicher ein.
- Aktivieren Sie die Checkbox „Aktiviert“. Dadurch wird das Speichermedium beim Systemstart automatisch eingebunden; andernfalls wird die manuelle Einbindung aktiviert.
- Wählen Sie den Typ, NFS oder CIFS/SMB.
- Geben Sie Hostname oder IP-Adresse ein.
- Geben Sie einen Freigabepfad ein in der Form `/path`.

Wenn Sie „CIFS/SMB“ auswählen, werden die Felder „Domäne“, „Benutzername“ und „Passwort“ aktiviert. Diese sind für NFS nicht erforderlich.

☒ Bei CIFS/SMB ist die Authentifizierung optional. Wenn keine Angaben gemacht werden, wird eine anonyme/Gast-Einbindung verwendet.

- Geben Sie beim Erstellen eines CIFS/SMB-Speichers die Domäne, den Benutzernamen und das Passwort ein, falls Sie dies wünschen.
- Klicken Sie auf **Speichern**.

Netzwerkspeicher wurde erfolgreich erstellt.

Netzwerkspeicher

☐	Name	Status	Aktiviert	Typ	Host	Freigabepfad	Aktionen
☐	Windows	🟢	🔗	NFS	192.168.57.134	/directory_1	Bearbeiten Löschen
☐	Linux	🟢	🔗	CIFS / SMB	192.168.57.126	/root	Bearbeiten Löschen

Abb. 183 Administration - Netzwerkspeicher - **Neuer Netzwerkspeicher angelegt**

Netzwerkspeicher ändern oder löschen

1. Klicken Sie auf **Administration > Netzwerkspeicher**. Eine Liste aller Netzwerkspeicher erscheint.

Netzwerkspeicher							Auswahl löschen	Neuer Netzwerkspeicher
☐	Name	Status	Aktiviert	Typ	Host	Freigabepfad	Aktionen	
☐	Windows	✓	☑	NFS	192.168.57.134	/directory_1		
☐	Linux	✓	☑	CIFS / SMB	192.168.57.126	/root		

Abb. 184 Administration - Netzwerkspeicher - **Liste der verfügbaren Netzwerkspeicher**

- Um einen Netzwerkspeicher zu bearbeiten, klicken Sie in der Zeile dieses Speichers auf die Schaltfläche „Bearbeiten“. Die Bearbeitungsseite wird geöffnet.
- Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf den Button **Speichern**.
- Um einen einzelnen Netzwerkspeicher zu löschen, klicken Sie in der Zeile dieses Speichers auf den Button **Löschen**.
- Um mehrere Netzwerkspeicher zu löschen, wählen Sie diese aus und klicken Sie auf den Button **Auswahl löschen**.

9.13 Spracheinstellungen

Mit der Funktion zur Spracheinstellung können Sie die Benutzeroberfläche der User Station sowie die Systemsprache ändern. Sie können aus den folgenden Sprachen wählen:

- English
- French: Français
- German: Deutsch
- Chinese (Simplified): 中文（简体）
- Japanese: 日本語

Nachdem Sie eine neue Sprache ausgewählt haben, müssen Sie die User Station neu starten, damit die Sprache in allen Bereichen vollständig aktualisiert wird. Bitte beachten Sie, dass einige Texte nicht in allen Sprachen verfügbar sind. Die Spracheinstellung wird bei der Sicherung und Wiederherstellung mitgesichert, bei einem Zurücksetzen auf die Werkseinstellungen wird jedoch Englisch als Sprache eingestellt.

Chinesische und japanische Eingabemethoden werden nicht unterstützt.

Ändern der Sprache

- Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Administration > Spracheinstellungen**. Die aktuelle Sprache wird angezeigt.

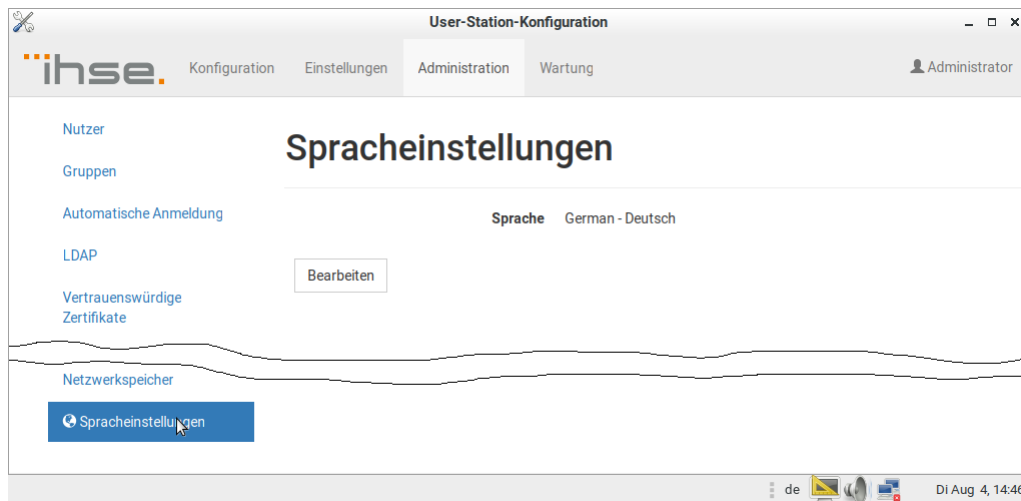


Abb. 185 Administration - Spracheinstellungen

2. Klicken Sie auf den Button **Edit**. Die Bearbeitungsseite wird geöffnet.

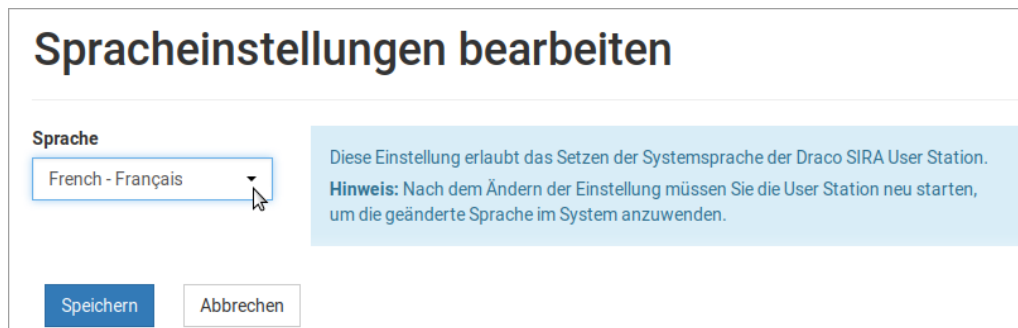


Abb. 186 Administration - Spracheinstellungen - Sprache ändern

3. Wählen Sie aus dem Drop-Down-Menü die gewünschte Sprache aus.
4. Klicken Sie auf **Speichern**. Die Änderung wird sofort in der Benutzeroberfläche sichtbar, Sie müssen die User Station jedoch neu starten, um sicherzustellen, dass die Sprachaktualisierung vollständig übernommen wird.

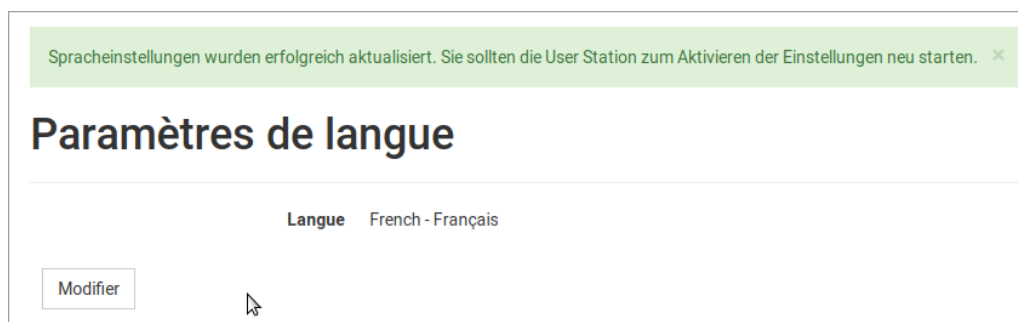


Abb. 187 Administration - Spracheinstellungen - Sprache geändert

10 Wartung

10.1 Reinigung

HINWEIS

Mögliche Beschädigung der mechanischen und elektronischen Komponenten

Die User Station sowie das Zubehör können durch Reinigung mit feuchten oder aggressiven Reinigungsmitteln beschädigt werden. Werden sie dennoch mit feuchten oder aggressiven Reinigungsmitteln gereinigt und dabei beschädigt, erlischt die Herstellergarantie.

➔ Staubablagerungen mit einem trockenen, antistatischen Tuch vom Gerät entfernen.

10.2 Ereignisprotokoll

Das Ereignisprotokoll ist ein Protokoll auf Anwendungsebene, das die Aktivitäten an der User Station aufzeichnet. Es erfasst, wer eine bestimmte Aufgabe ausgeführt hat und wann dies geschehen ist. Dazu gehören beispielsweise das An- und Abmelden, das Herstellen einer Verbindung zu einem KVM-Port, Software-Updates und Ähnliches. Das Ereignisprotokoll erfasst zudem Systemvorfälle, die auf andere Weise nicht angezeigt werden können, wie beispielsweise die LDAP-Authentifizierung sowie Autorisierungsvorgänge und -entscheidungen.

Das Ereignisprotokoll unterscheidet sich von der Diagnoseprotokolldatei, die von der User Station heruntergeladen werden kann und die rohen Systemprotokolle enthält, die sich nicht ohne Weiteres lesen oder filtern lassen

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Wartung**. Die Ereignisprotokollseite wird geöffnet.

The screenshot shows the 'Ereignisprotokoll' (Event Log) page in the 'User-Station-Konfiguration' application. The page has a sidebar with navigation links: 'Ereignisprotokoll', 'Sicherheit und Wiederherstellung', 'Werkzeiteinstellungen', 'Softwareaktualisierung', 'Kundendienst', 'Netzwerkd Diagnose', and 'Über das Gerät'. The main content area displays a table of events with columns: 'Datum (CEST +0200)', 'Ereigniswichtigkeit', 'Ereignistyp', and 'Beschreibung'. The 'Suchen' (Search) button is located in the top right corner of the main content area. The table shows several events, including system events, authentication events, and a warning about a network issue.

Datum (CEST +0200)	Ereigniswichtigkeit	Ereignistyp	Beschreibung
2026-09-02 08:07:15	Info	Systemereignis	Bildschirmfoto durch Nutzer admin von <lokal> aufgenommen
2026-09-02 08:06:41	Info	Systemereignis	Bildschirmfoto durch Nutzer admin von <lokal> aufgenommen
2026-09-02 08:06:06	Info	Systemereignis	Entry ESXi Zugang zu 'Computer 1' wurde durch Nutzer admin von <lokal> erstellt
2026-09-02 08:05:16	Info	Authentifizierungsereignis	Lokaler Nutzer admin von <lokal> wurde angemeldet
2026-09-02 08:01:50	Fehler	Systemereignis	Automatisches Einhängen des Netzwerkspeichers Windows fehlgeschlagen: mount.nfs: Network is unreachable
2026-09-02 08:01:46	Info	Systemereignis	System gestartet
2026-08-27 15:25:31	Info	Systemereignis	System heruntergefahren
2026-08-27 15:25:28	Info	Authentifizierungsereignis	Lokaler Nutzer admin von <lokal> wurde angemeldet
2026-08-27 14:57:23	Info	Systemereignis	Bildschirmfoto durch Nutzer admin von <lokal> aufgenommen
2026-08-27 14:55:25	Info	Systemereignis	Bildschirmfoto durch Nutzer admin von <lokal> aufgenommen
2026-08-27 13:39:18	Info	Systemereignis	Bildschirmfoto durch Nutzer admin von <lokal> aufgenommen
2026-08-27 11:25:22	Info	Systemereignis	Die Einstellungen für Nutzungsbedingungen wurden durch Nutzer admin von <lokal> geändert. Nutzungsbedingungen sind nun deaktiviert.
2026-08-27 11:25:05	Info	Authentifizierungsereignis	Lokaler Nutzer admin von <lokal> wurde angemeldet
2026-08-27 11:24:46	Info	Authentifizierungsereignis	Lokaler Nutzer admin von <lokal> wurde angemeldet

Abb. 188 Wartung - Ereignisprotokoll

Die Suchfunktionen befinden sich oben auf der Seite. Die Einträge der letzten sieben Tage im Ereignisprotokoll werden unten auf der Seite angezeigt.

Sie können nach den folgenden Kriterien suchen:

- Datum: Wählen Sie eine Zeitspanne in den „Von“ und „Bis“ Feldern.
- Ereignistyp: Siehe folgende Tabelle, wenn Authentifizierungsereignisse ausgewählt ist, erscheint ein Nutzer-Feld mit Drop-Down-Menü zur Auswahl eines Nutzers.
- Ereigniswichtigkeit: Info, Warnung oder Fehler
- Ereignisse pro Seite: Wählen Sie aus, wie viele Datensätze pro Seite in den Suchergebnissen angezeigt werden sollen.

Das Ereignisprotokoll enthält die folgenden Ereignistypen:

Ereignistyp	Beschreibung
Authentifizierung	Enthält Benutzername, Authentifizierungstyp (lokal oder LDAP) und von wo (lokal oder IP-Adresse)
LDAP	Fehler und Informationen über LDAP-Authentifizierung und -Autorisierung
KVM-Zugang	Zugang zu KVM-Ports mit Gerät, Port, Nutzernamen und von wo (lokal oder IP-Adresse)
Serieller Zugang	Zugang zu seriellen Ports mit Gerät, Port, Nutzernamen und von wo (lokal oder IP-Adresse)
RDP, SSH, VNC, Web und ESXi Zugang	Geöffnete und geschlossene Zugangs-Sessions des jeweiligen Typs
System	Systemänderungen z.B. Nutzer oder Geräte hinzufügen, Screenshots erstellen oder Nutzungsbedingungen ändern

- Wählen Sie die gewünschten Suchkriterien aus und klicken Sie auf den Button **Suchen**.
- Wenn die Anzahl der Protokolleinträge die Anzahl der Einträge pro Seite übersteigt, verwenden Sie die Buttons **Nächste** und **Vorherige**, um weitere Seiten anzuzeigen.

10.2.1 Ereignisprotokolle archivieren

Ereignisprotokoll-Datensätze können archiviert werden, um die Datenbank zu entlasten. Ereignisprotokoll-Archive werden stets innerhalb der User Station erstellt und gespeichert. Die erstellte Datei ist eine komprimierte CSV-Datei, die pro Datensatz eine Zeile sowie alle Attribute des Datensatzes enthält. Jeder Datensatz verfügt über einen Zeitstempel in UTC.

Alle gespeicherten Archive werden mit den folgenden Details aufgelistet:

- Erstelldatum
- Dateiname
- Größe

Sie können jederzeit ein manuelles Archiv erstellen (siehe nächster Abschnitt).

Die User Station legt außerdem automatisch ein Archiv an, wenn die Gesamtzahl der Ereignisprotokolleinträge einen bestimmten Schwellenwert erreicht (siehe Abschnitt 10.2.1.3, Seite 154).

10.2.1.1 Ereignisprotokoll-Archiv erstellen

- Klicken Sie auf **Administration > Wartung**. Die Ereignisprotokollseite wird geöffnet.
- Klicken Sie auf den Button **Archive**. Die folgende Seite wird geöffnet.

Ereignisprotokollarchiv

Ältester Eintrag: 2026-05-05 07:32:12

Alle Einträge, die älter als eingestellt sind, werden archiviert.

Alter

Datum

Dateiname
Status
Größe
Datum (CEST +0200)

Es wurden noch keine Archive angelegt.

Hinweis: Bitte stecken einen USB-Speicher, z.B. einen USB-Stick, an oder hängen Sie einen Netzwerkspeicher ein, um Archive zu exportieren.

Abb. 189 Wartung - Ereignisprotokoll - Archivieren

3. Wählen Sie aus, nach welchen Kriterien die Datensätze in das Archiv aufgenommen werden sollen: nach Alter oder nach Datum:
 - Im Feld „Alter“: Wählen Sie eine Zeitspanne, zur Wahl stehen: Älter als 1 Woche, Älter als 1, 2, oder 6 Monate, Älter als 1, 2, 5 oder 10 Jahre. Es gibt zusätzlich den Eintrag „Älter als der ausgewählte Zeitpunkt“.
 - Wählen Sie im Feld „Alter“ den Eintrag „Älter als der ausgewählte Zeitpunkt“, um das Feld „Datum“ zu aktivieren.
4. Klicken Sie auf das Kalendersymbol und wählen Sie ein Datum aus. Um eine bestimmte Uhrzeit auszuwählen, klicken Sie auf das Uhrensymbol unten im Kalender und wählen Sie eine Uhrzeit aus.
Alle protokollierten Ereignisse, die älter sind als das ausgewählte „Alter“ oder älter als das ausgewählte „Datum“, werden archiviert werden.
5. Klicken Sie auf den Button **Archivieren** und dann auf **OK** im Bestätigungsdialog.

Das Archiv SIRAUST_log_archive_20260901000000_134da2.zip wurde erfolgreich erstellt

Ereignisprotokollarchiv

Ältester Eintrag: 2026-09-02 08:01:46

Alle Einträge, die älter als eingestellt sind, werden archiviert.

Alter

Älter als der ausgewählte Zeitpunkt

Datum

2026-05-01 00:00:00 +02:00

Archivieren

Dateiname	Status	Size	Date (CEST +0200)	
SIRAUST_log_archive_20260901000000_134da2.zip	Fertig	2.95 KB	2026-05-26 14:34:30	

Hinweis: Bitte stecken einen USB-Speicher, z.B. einen USB-Stick, an oder hängen Sie einen Netzwerkspeicher ein, um Archive zu exportieren.

Zurück

Abb. 190 Wartung - Ereignisprotokoll - Archivierung beendet

10.2.1.2 Ereignisprotokollarchive exportieren und löschen

1. Klicken Sie auf das Exportsymbol , um die Archiv-zip-Datei auf einen angeschlossenen USB-Stick oder einen konfigurierten Netzwerkspeicher zu exportieren.
2. Klicken Sie auf das Löschsymbolsymbol , um die Archiv-zip-Datei nach Bestätigung zu löschen.

10.2.1.3 Automatische Archivierung

Die User Station erstellt automatisch Archive, wenn die Datenbank aufgrund zu vieler Einträge voll ist. Die automatische Archivierung erfolgt anhand von zwei Schwellenwerten: „Warnung“ und „Kritisch“. Die Schwellenwerte werden einmal täglich überprüft. Werden die Schwellenwerte erreicht, erscheint eine Fehlermeldung im Ereignisprotokoll. Das Archiv wird automatisch erstellt, sobald der Schwellenwert „Kritisch“ erreicht ist.

Schwellenwert Warnung

Sobald 2 Millionen Einträge erreicht sind, wird auf der Seite „Ereignisprotokoll“ eine Warnmeldung angezeigt.

Das Ereignisprotokoll enthält mehr als 2 Millionen Einträge. Bitte archivieren Sie die Einträge im Ereignisprotokoll, da andernfalls die automatische Archivierung gestartet wird, sobald das Ereignisprotokoll mehr als 3 Millionen Einträge umfasst.

Schwellenwert Kritisch

Die kritische Schwelle liegt bei 3 Millionen Einträgen. Es wird ein automatisches Archiv erstellt, das alle Protokolleinträge oberhalb der Warnschwelle von 2 Millionen Einträgen enthält. Die automatische Archivierung wird nicht sofort nach Erreichen von 3 Millionen Einträgen ausgelöst, sondern läuft einmal täglich.

Die Erstellung des automatischen Archivs wird im Ereignisprotokoll unter dem Benutzernamen <system> protokolliert.

10.2.1.4 Speicherung von Archivdateien

Der Speicherplatz für die Aufbewahrung von Ereignisprotokoll-Archiven auf der User Station ist begrenzt. Wenn kein Speicherplatz mehr verfügbar ist, wird beim Versuch, ein neues Archiv zu erstellen, eine Fehlermeldung angezeigt.

Bei Bedarf können Sie Dateien vor dem Löschen auf einen externen Speicher exportieren (siehe vorherige Seite).

Sie müssen Archivdateien löschen, bevor Sie ein neues Archiv erstellen können (siehe vorherige Seite).

Wenn der Speicherplatz voll ist und ein automatisches Archiv erstellt werden muss, werden die ältesten Archive automatisch gelöscht, bis genügend Platz für das neue Archiv vorhanden ist.

Das Löschen jedes Archivs wird im Ereignisprotokoll protokolliert.

10.3 Sicherung und Wiederherstellung

Mit der User Station können Sie die aktuellen Einstellungen und Daten mit einem Klick speichern. Standardmäßig werden die Sicherungsdateien in der User Station gespeichert.

Falls Sie die vorherigen Einstellungen und Daten wiederherstellen müssen, wählen Sie die gewünschte Sicherungsdatei aus und führen Sie den Wiederherstellungsbefehl aus.

 Die folgenden Systemeinstellungen werden nicht in der Sicherungsdatei gespeichert und können daher nicht wiederhergestellt werden.

- Netzwerk-Einstellungen
- Ereignisprotokollarchive
- Sicherungsdateien

 Sie können Sicherungsdateien von einem USB-Stick oder einem Netzwerkspeicher exportieren oder importieren (siehe weiter unten in diesem Abschnitt)

10.3.1 Sicherungsdatei erstellen

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Wartung > Sicherung und Wiederherstellung**. Die entsprechende Seite wird geöffnet.



Abb. 191 Wartung - Sicherung und Wiederherstellung

2. Klicken Sie auf den Button **Sicherung Erstellen**. Die Sicherungsdatei wird erstellt und angezeigt mit Name, Datum, Software-Version und Größe.



Abb. 192 Wartung - Sicherung und Wiederherstellung - **Sicherungsdatei erstellt**

10.3.2 Sicherungsdatei wieder einspielen

Wenn bereits Sicherungsdateien vorhanden sind, werden diese alle auf der Seite „Sicherung und Wiederherstellung“ aufgelistet.

1. Um Details zu einer Sicherungsdatei (Sicherungsarchiv) anzuzeigen, klicken Sie in der Liste darauf.

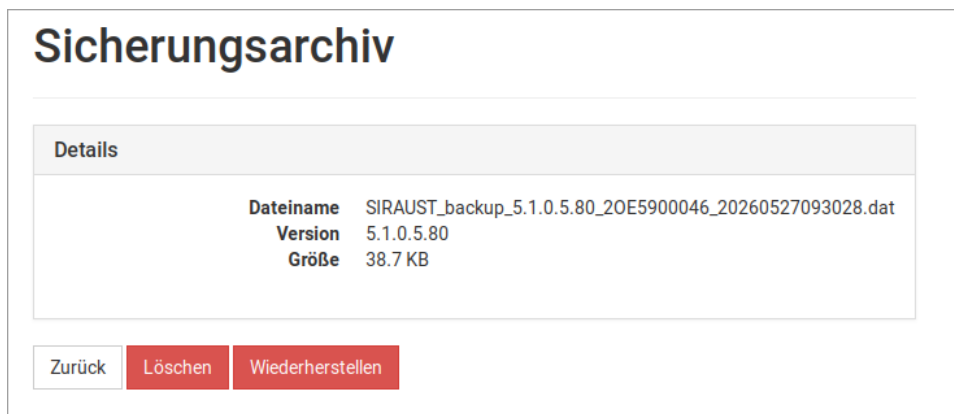


Abb. 193 Wartung - Sicherung und Wiederherstellung - **Details einer Sicherungsdatei**

2. Klicken Sie entweder auf das Wiederherstellungssymbol  in der Zeile der Sicherungsdatei oder auf den Button **Wiederherstellen** in den Details der Datei. Eine Bestätigungsaufforderung erscheint.
3. Klicken Sie auf **OK**, um die Sicherungsdatei wieder einzuspielen.

10.3.3 Sicherungsdateien exportieren und importieren

Um eine Sicherungsdatei zu exportieren oder zu importieren, müssen Sie zunächst einen USB-Stick an die User Station anschließen oder einen Netzwerkspeicher einrichten.

Sicherungsdatei exportieren

1. Schließen Sie einen USB-Stick an, der mit einem der folgenden Dateisysteme formatiert ist, oder richten Sie einen Netzwerkspeicher ein.
 - VFAT (FAT16, FAT32)
 - NTFS
 - EXT2, EXT3, EXT4
 - XFS

- Klicken Sie auf **Wartung > Sicherung und Wiederherstellung**. Die entsprechende Seite wird geöffnet.
Wenn die User Station einen angeschlossenen USB-Stick oder einen Netzwerkspeicher erkennt, erscheint das Exportsymbol  in der Spalte „Aktionen“.
- Klicken Sie auf das Exportsymbol  in der Zeile der gewünschten Sicherungsdatei.
Die ausgewählte Datei wird auf den angeschlossenen USB-Stick bzw. den Netzwerkspeicher exportiert und daher im Abschnitt „Sicherung von USB-Stick oder Netzwerkspeicher importieren“ aufgeführt.

Sicherungsdatei importieren

- Stellen Sie sicher, dass der angeschlossene USB-Stick oder der Netzwerkspeicher über Sicherungsdateien im Root-Verzeichnis verfügt.
Klicken Sie auf der Seite „Sicherung und Wiederherstellung“ auf den Button „Sicherung Importieren“. Die entsprechende Seite wird geöffnet.
Alle im Stammverzeichnis gefundenen Sicherungsdateien werden aufgelistet.

Sicherung von USB- oder Netzwerkspeicher Importieren

USB- und Netzwerkspeicher	Dateiname	Größe	Aktionen
567E-43A7	SIRAUST_backup_5.1.0.5.80_20E5900046_20260527093028.dat	38.7 KB	

[Zurück](#)

Hinweis

Um eine Sicherung zu importieren, stecken Sie einen USB-Speicher, z.B. einen USB-Stick, an oder hängen Sie einen Netzwerkspeicher ein, welcher die Sicherungsdatei in seinem Hauptverzeichnis enthält.

Abb. 194 Wartung - Sicherung und Wiederherstellung - Import einer Sicherungsdatei

- Klicken Sie auf das Importsymbol  der gewünschten Sicherungsdatei.
Die ausgewählte Sicherungsdatei wird importiert und in der Liste auf der Seite „Sicherung und Wiederherstellung“ angezeigt.

10.3.4 Sicherungsdateien löschen

So überprüfen Sie das Erstelldatum einer Sicherungsdatei, bevor Sie sie löschen:

Das Erstelldatum und der Zeitstempel sind im Dateinamen als letzte Ziffernfolge enthalten, nach der Softwareversion und manchmal der Seriennummer. Das Datum wird mit 8 Ziffern angegeben, die Uhrzeit mit 6 Ziffern.

Beispiel:

Name der Sicherungsdatei mit Versionsnummer, Seriennummer und Datums-/Zeitstempel:

SIRAUST_backup_5.1.0.5.80_20E5900046_20260527093028.dat

Software-Version: 5.1.0.5.80

Seriennummer: 20E5900046

Datum: 20260527 (27. Mai 2026)

Zeit: 093028 (9h:30min:28s)

- Klicken Sie auf **Wartung > Sicherung und Wiederherstellung**. Die Seite „Sicherung und Wiederherstellung“ öffnet sich mit einer Liste aller vorhandenen Sicherungsdateien.



Abb. 195 Wartung - **Sicherung und Wiederherstellung**

2. Klicken Sie auf das Löschsymbol  in der Zeile der Sicherungsdatei, die Sie löschen möchten oder klicken Sie auf den Dateinamen und dann auf den Button **Löschen** auf der Seite der Details.
3. Klicken Sie auf **OK** in der Bestätigungsnachricht.

10.4 Werkseinstellungen

Die Funktion „Auf Werkseinstellungen zurücksetzen“ setzt alle Einstellungen der User Station auf die werkseitigen Standardeinstellungen zurück. Gleichzeitig werden alle benutzerdefinierten Daten gelöscht, darunter:

- Alle KVM-Geräte, die der User Station hinzugefügt wurden
- Anmeldedaten für jedes KVM-Gerät
- Alle Targets und Zugänge
- Nutzer und Nutzergruppen
- „admin“ Nutzerprofil wird auf Werkseinstellungen zurückgesetzt
- Vordefinierte Nutzergruppen werden auf Werkeinstellungen zurückgesetzt
- Alle Nutzereinstellungen
- Systemeinstellungen
- Netzwerkeinstellungen
- Vertrauenswürdige Zertifikate
- Server-Zertifikate
- Deskto-Hintergrund
- Sicherungsdateien
- Ereignisprotokolldateien

1. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Wartung > Werkseinstellungen**. Die entsprechende Seite wird geöffnet.
2. Lesen Sie diese Seite, bevor Sie mit dem nächsten Schritt fortfahren.

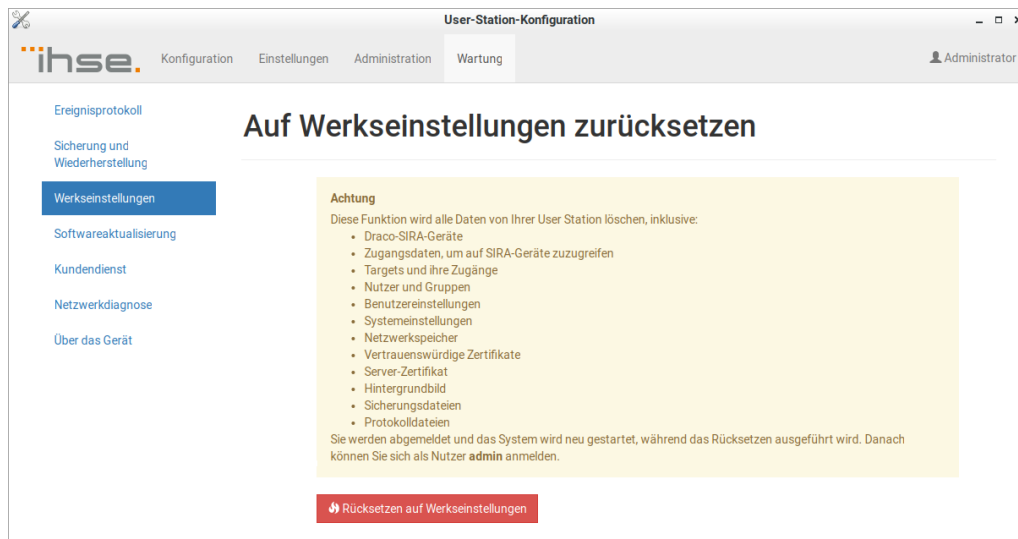


Abb. 196 Wartung - Auf Werkseinstellungen zurücksetzen

3. Klicken Sie auf **Rücksetzen auf Werkseinstellungen**. Eine Bestätigungsnachricht erscheint.
4. Klicken Sie auf **OK**, um das Zurücksetzen zu bestätigen oder auf **Cancel**, um den Vorgang abubrechen.

10.4.1 Beim Start auf Werkseinstellungen zurücksetzen

Zusätzlich zur Funktion „Auf Werkseinstellungen zurücksetzen“ im Menü Wartung der Konfiguration können Sie die User Station beim Geräte-Startvorgang auf die Werkseinstellungen zurücksetzen.

Nur der Administrator kann den Werksreset beim Start durchführen. Beachten Sie, dass durch den Werksreset alle benutzerdefinierten Daten gelöscht werden (siehe vorheriger Abschnitt).

1. Starten Sie die User Station oder führen Sie einen Neustart durch.
2. Wenn nach dem BIOS-Bild in der oberen linken Ecke des Bildschirms ein blinkender Textcursor erscheint, drücken Sie innerhalb einer Sekunde die Taste **Esc**.
Ein Menü mit zwei Optionen erscheint:
 - Boot Draco SIRA User Station
 - Reset Draco SIRA User Station to Factory Defaults
3. Wählen Sie **Reset Draco SIRA User Station to Factory Defaults**. Wenn Sie die andere Option wählen, fährt die User Station normal hoch ohne Werkseinstellungen.
4. Wenn Sie vom System zur Eingabe der Benutzerdaten aufgefordert werden, geben Sie die Admin-Zugangsdaten ein (Nutzername: admin, Standard-Passwort: admin).
5. Wenn die Administrator-Anmeldedaten korrekt sind, führt die User Station das Zurücksetzen auf die Werkseinstellungen durch und startet anschließend neu. Sind die Anmeldedaten falsch, kehrt die User Station zum Menü zurück.

10.5 Software aktualisieren

Die Software-Update-Funktion ermöglicht nur Software-Upgrades, keine Downgrades.

Um ein Software-Update durchzuführen, müssen die folgenden Voraussetzungen erfüllt sein:

- Version 5.1.xx ist mindestens nötig, um ein Update auf Version 5.2 durchführen zu können.
- Ein USB-Stick oder ein Netzwerkspeicher, auf dem sich die Datei für das Software-Update befindet.

Unterstützte Laufwerksformate sind:

- VFAT (FAT16, FAT32)
- NTFS
- EXT2, EXT3, EXT4
- Die Version der Software, die Sie installieren möchten, entspricht der derzeit auf Ihrer User Station installierten Softwareversion oder ist höher als diese (siehe Abschnitt 5.2.7.1, Seite 23).
- Für Software-Update-Dateien wenden Sie sich bitte an unseren technischen Support.

HINWEIS

Es wird dringend empfohlen, vor dem Software-Update eine Sicherungskopie aller Daten und Einstellungen zu erstellen und diese auf einen USB-Stick oder einen Netzwerkspeicher zu exportieren. (siehe Abschnitt 10.3, Seite 155).

1. Schließen Sie den USB-Stick mit der Software-Update-Datei an die User Station an oder binden Sie den Netzwerkspeicher mit der Update-Datei ein.
2. Melden Sie sich an der User Station als „admin“ oder als Benutzer mit System-Administratorrechten an.
3. Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Wartung > Softwareaktualisierung**. Die Seite „Softwareaktualisierung“ wird mit einer Liste der Software-Dateien geöffnet, die im Stammverzeichnis des USB-Sticks oder des Netzwerkspeichers gefunden wurden.

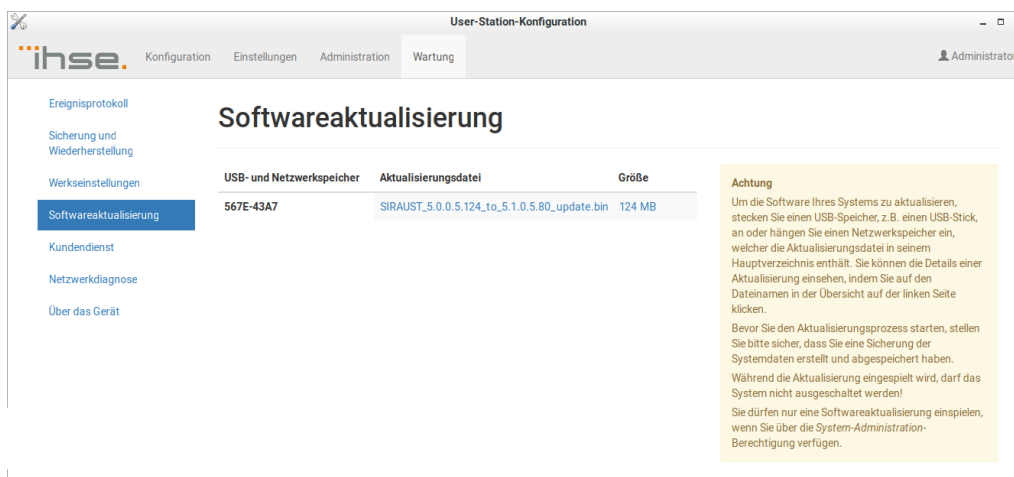


Abb. 197 Wartung - Softwareaktualisierung

4. Klicken Sie auf die gewünschte Datei. Sie wird analysiert und die Ergebnisse dargestellt. Überprüfen Sie die erforderliche Mindestversion und die Ergebnisse der Gültigkeitsprüfung.
5. Klicken Sie auf den Button **Starte Aktualisierung**.

HINWEIS

Schalten Sie die User Station während der Softwareaktualisierung nicht aus.

6. Klicken Sie auf **OK** in der Bestätigungsnachricht.
Wenn die Aktualisierung beendet ist, startet die User Station neu und die Anmeldemaske erscheint.

10.6 Kundendienst

Die Kundendienst-Seite bietet zwei Funktionen, die dem technischen Support von IHSE bei der Fehlerbehebung bei Problemen mit Ihrer User Station helfen.

1. Klicken sie auf **Hauptmenü > User-Station-Konfiguration > Wartung > Kundendienst**. Die entsprechende Seite wird geöffnet.

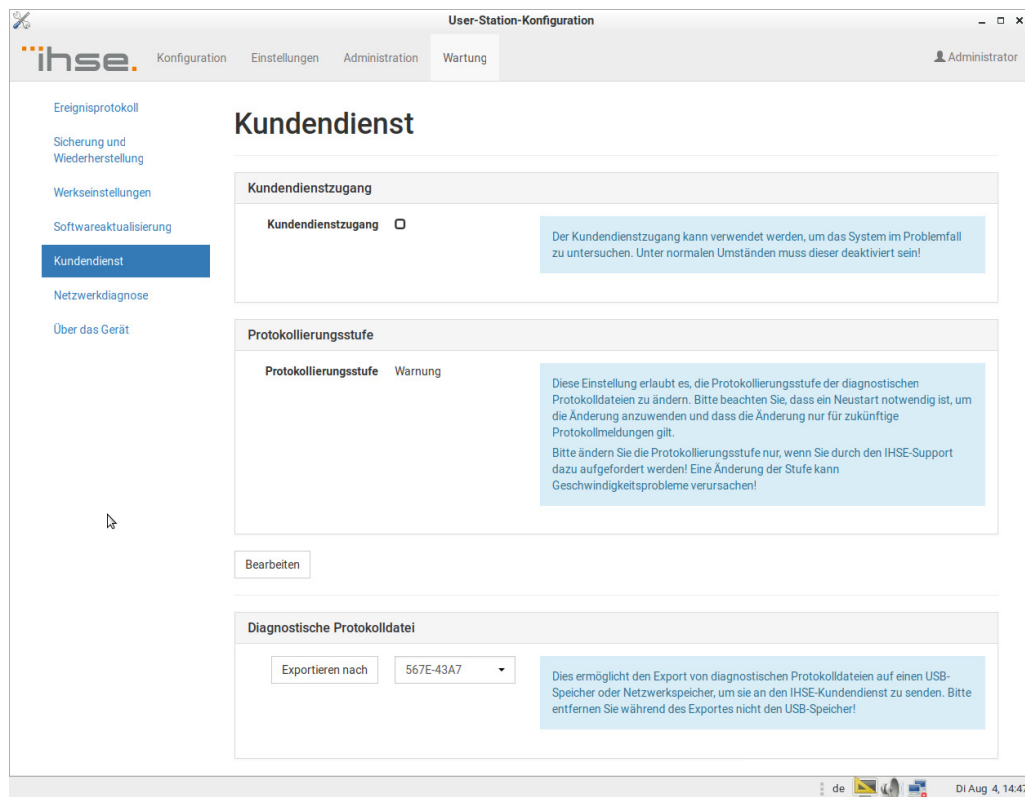


Abb. 198 Wartung - Kundendienst

Funktion	Beschreibung
Kundendienstzugang	Mit dieser Funktion kann der technische Support per Fernzugriff auf Ihre User Station zugreifen!
Protokollierungsstufe	Hier können Sie die Protokollstufe für die Diagnoseprotokolldatei festlegen. Diese Datei unterscheidet sich vom Ereignisprotokoll.
Diagnostische Protokolldatei	Diese Funktion lädt eine Diagnoseprotokolldatei Ihrer User Station herunter, die bei der Fehlerbehebung hilfreich ist.

2. Klicken Sie auf den Button **Bearbeiten**. Die Bearbeitungsseite wird geöffnet.

Kundendienststeinstellungen bearbeiten

Kundendienstzugang

☐ Kundendienstzugang
Passwort

Achtung

Ein eingeschalteter Kundendienstzugang ist eine Sicherheitslücke!

Protokollierungsstufe

Protokollierungsstufe

Warnung ▼

Diese Einstellung erlaubt es, die Protokollierungsstufe der diagnostischen Protokolldateien zu ändern. Bitte beachten Sie, dass ein Neustart notwendig ist, um die Änderung anzuwenden und dass die Änderung nur für zukünftige Protokollmeldungen gilt.

Bitte ändern Sie die Protokollierungsstufe nur, wenn Sie durch den IHSE-Support dazu aufgefordert werden! Eine Änderung der Stufe kann Geschwindigkeitsprobleme verursachen!

Speichern

Abbrechen

Abb. 199 Wartung - **Kundendienststeinstellungen bearbeiten**

10.6.1 Kundendienstzugang

HINWEIS

Die Funktion „Support-Anmeldung“ ermöglicht den Fernzugriff durch unseren technischen Support. Aus Sicherheitsgründen ist diese Funktion standardmäßig deaktiviert.

- ➔ Aktivieren Sie diese Funktion nur, wenn Sie vom technischen Support von IHSE dazu aufgefordert werden.
- ➔ Deaktivieren Sie diese Funktion unmittelbar nach Abschluss der Fehlerbehebung.

1. Klicken Sie auf den Button **Bearbeiten**.
2. Aktivieren Sie das Kontrollkästchen „Kundendienstzugang“ nur, wenn Sie vom technischen Support der IHSE dazu aufgefordert werden.
3. Klicken Sie auf **Speichern**.
4. Teilen Sie dem technischen Support von IHSE die IP-Adresse Ihrer User Station mit und befolgen Sie deren Anweisungen.
5. Deaktivieren Sie dieses Kontrollkästchen unmittelbar nach der Fehlerbehebung.

10.6.2 Protokollierungsstufe

Wenn die User Station nicht ordnungsgemäß funktioniert, können Sie die Diagnoseprotokolldatei der User Station auf einen angeschlossenen USB-Stick oder einen eingebundenen Netzwerkspeicher exportieren und die Datei zur Fehlerbehebung an den technischen Support von IHSE senden.

Sie benötigen die Berechtigung „Systemadministration“, um diesen Vorgang auszuführen.

 Die diagnostische Protokolldatei unterscheidet sich vom Ereignisprotokoll (für Ereignisprotokoll siehe Abschnitt 10.2, Seite 152).

Protokollierungsstufe einstellen

1. Klicken Sie auf **Wartung > Kundendienst**.
2. Klicken Sie auf den Button **Bearbeiten**.
3. Wählen Sie zunächst aus, welche Protokolle in die Diagnoseprotokolldatei aufgenommen werden sollen, indem Sie im Dropdown-Menü „Protokollstufe“ einen Eintrag auswählen. Sie können wählen zwischen
 - Debug
 - Info
 - Warnung
 - Fehler
 - Kritisch

 Die Auswahl von „Debug“ kann die Systemleistung beeinträchtigen.

4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **OK** in der Bestätigungsmeldung, um die Protokollierungsstufe einzustellen und die User Station neu zu starten.

Herunterladen der Diagnoseprotokolldatei

1. Stellen Sie sicher, dass an Ihrer User Station ein USB-Stick angeschlossen oder ein Netzwerkspeicher eingebunden ist.
2. Klicken Sie auf **Wartung > Kundendienst**.
3. Wählen Sie den USB-Stick oder den Netzwerkspeicher aus der Drop-Down-Liste aus.
4. Klicken Sie auf den Button **Export to**.

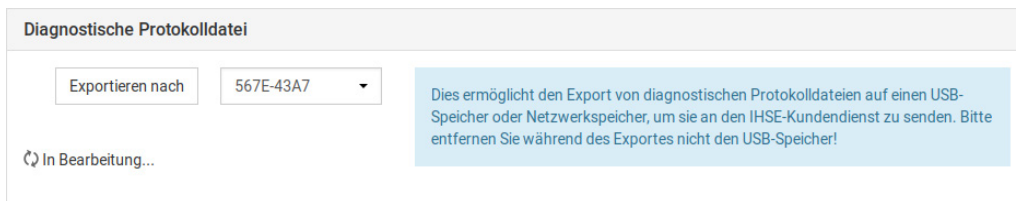


Abb. 200 Wartung - Diagnostische Protokolldatei - **Exportieren**

5. Warten Sie, bis die User Station den Export abgeschlossen hat und die Meldung „Erfolgreich beendet“ sowie den Namen der Diagnoseprotokolldatei anzeigt.

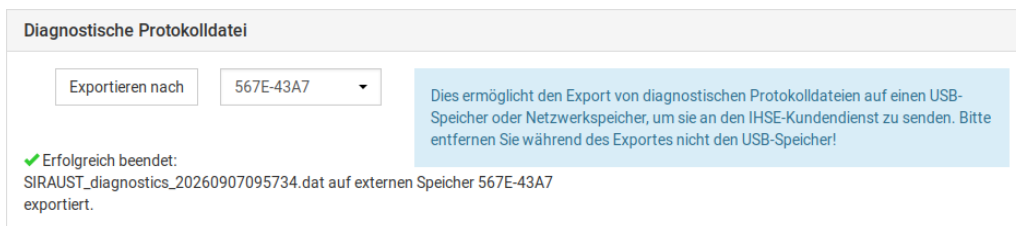


Abb. 201 Wartung - Diagnostische Protokolldatei - **Export erfolgreich beendet**

6. Senden Sie die Datei an den technischen Support von IHSE.

10.7 Netzwerkdiagnose

Die User Station liefert Informationen zum Status Ihrer Netzwerkschnittstellen.

- ➔ Klicken Sie auf **Hauptmenü > User-Station-Konfiguration > Wartung > Netzwerkdiagnose**. Die entsprechende Seite wird geöffnet.

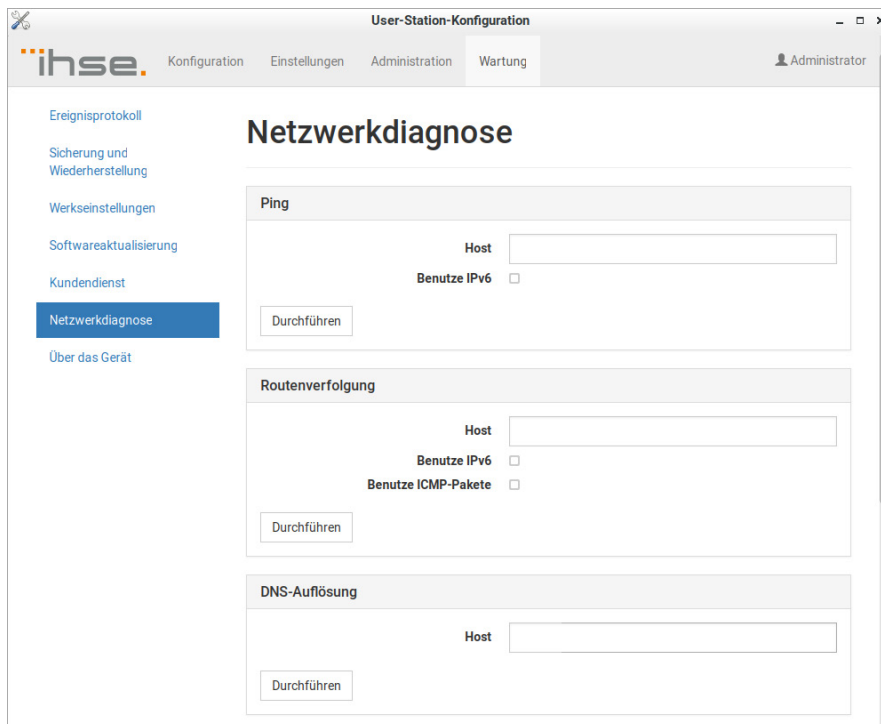


Abb. 202 Wartung - **Netzwerkdiagnose**

Um detaillierte Informationen zu einer der Schnittstellen zu erhalten, können Sie einen Ping-Befehl ausführen, eine Routenverfolgung durchführen oder eine DNS-Abfrage starten.

Ping

1. Geben Sie Hostname oder IP-Adresse in das Feld „Host“ im Bereich „Ping“ ein.
2. Aktivieren Sie das Kontrollkästchen „Benutze IPv6“, wenn Sie IPv6 anstelle von IPv4 verwenden möchten.
3. Klicken Sie auf den Button **Durchführen**. Die entsprechenden Informationen werden wie in der folgenden Abbildung dargestellt angezeigt.

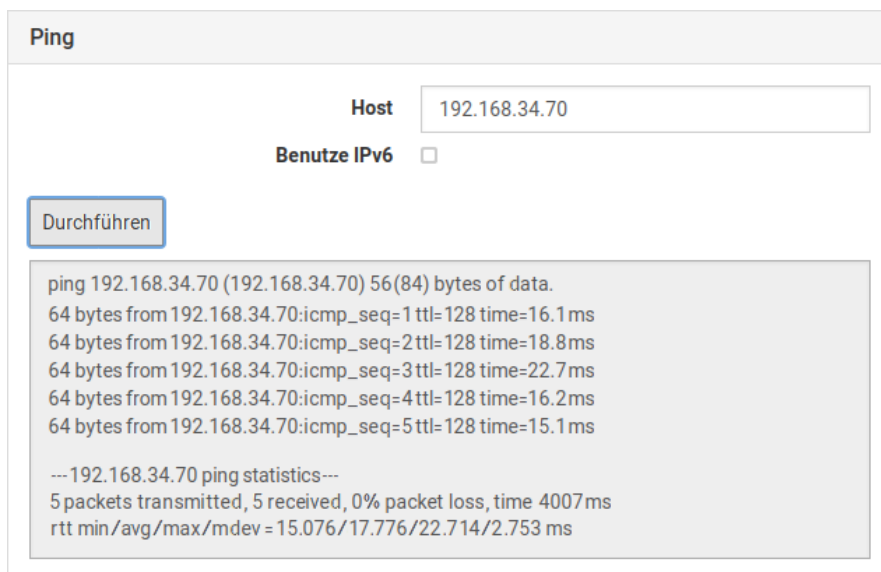


Abb. 203 Wartung - Netzwerkdiagnose - **Ping-Ergebnisse**

Routenverfolgung

1. Geben Sie Hostname oder IP-Adresse in das Feld „Host“ im Bereich „Routenverfolgung“ ein.
2. Aktivieren Sie das Kontrollkästchen „Benutze IPv6“, wenn Sie IPv6 anstelle von IPv4 verwenden möchten.
3. Aktivieren Sie das Kontrollkästchen „Benutze ICMP-Pakete“, wenn die Daten im ICMP-Format angezeigt werden sollen.
4. Klicken Sie auf den Button **Durchführen**. Die relevanten Informationen werden angezeigt.

DNS-Abfrage

1. Geben Sie Hostname oder IP-Adresse in das Feld „Host“ im Bereich „DNS-Auflösung“ ein.
2. Klicken Sie auf den Button **Durchführen**. Die relevanten Informationen werden angezeigt.

TCP-Verbindungen und TCP/UDP-Listen-Sockets

„Netzwerkdiagnose“ listet außerdem die aktuellen TCP-Verbindungen und TCP/UDP-Listen-Sockets auf.

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
ESTAB	0	0	[*]:8000	[*]:46202
ESTAB	0	0	[*]:8000	[*]:46204
ESTAB	0	0	[*]:8000	[*]:46212
ESTAB	0	0	[*]:43668	[*]:8000
ESTAB	0	0	[*]:46202	[*]:8000
ESTAB	0	0	[*]:46204	[*]:8000
ESTAB	0	0	[*]:8000	[*]:43668
ESTAB	0	709	[*]:46212	[*]:8000

Neu laden

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
udp	UNCONN	0	0	0.0.0.0:111	0.0.0.0:*
udp	UNCONN	0	0	[*]:111	[*]:*
tcp	LISTEN	0	4096	0.0.0.0:111	0.0.0.0:*
tcp	LISTEN	0	128	0.0.0.0:22	0.0.0.0:*
tcp	LISTEN	0	244	127.0.0.1:5432	0.0.0.0:*
tcp	LISTEN	0	500	127.0.0.1:34491	0.0.0.0:*
tcp	LISTEN	0	500	127.0.0.1:36429	0.0.0.0:*
tcp	LISTEN	0	511	0.0.0.0:8080	0.0.0.0:*
tcp	LISTEN	0	511	0.0.0.0:8000	0.0.0.0:*
tcp	LISTEN	0	4096	[*]:111	[*]:*
tcp	LISTEN	0	128	[*]:22	[*]:*
tcp	LISTEN	0	244	[*]:5432	[*]:*
tcp	LISTEN	0	511	[*]:8080	[*]:*
tcp	LISTEN	0	511	[*]:8000	[*]:*

Neu laden

Abb. 204 Wartung - Netzwerkdiagnose - TCP-Verbindungen und TCP/UDP-Listen-Sockets

- ➔ Klicken Sie auf den Button **Neu laden**, um die Daten in der entsprechenden Liste zu aktualisieren.

10.8 Über das Gerät

Auf der Seite „Über dieses Gerät“ werden die Firmware-Version, die Modellnummer und die MAC-Adressen angezeigt. Sie können diese Seite auf zwei Arten aufrufen:

1. Klicken Sie im User-Station-Konfigurationsfenster auf **Wartung > Über das Gerät**.
2. Klicken Sie im Hauptmenü auf **Hilfe > Über dieses Gerät**.

11 API-Konfiguration

11.1 Session erstellen und anmelden

Um API nutzen zu können, müssen sich Benutzer authentifizieren und eine Session erstellen. Der erste Schritt ist immer ein POST-Aufruf an `/session/login` mit den Anmeldedaten.

Parameter

Parameter	Beschreibung
user name	Der Anmeldename des Nutzers, notwendig.
password	Das Passwort des Nutzers, notwendig.
user type	The Nutzertyp, optional. Möglich sind: • "lokal" (Nutzer, die nur in der User Station existieren) • "ldap" (LDAP-authentifizierte Nutzer) • Sofern nichts angegeben ist, wird von einem lokalen Nutzer ausgegangen.

Response

Response	Beschreibung
result	Das Ergebnis des Authentifizierungsprozesses, möglich sind: • success: Die Authentifizierung war erfolgreich und der Nutzer ist angemeldet. Die Session kann sofort für weitere Vorgänge genutzt werden. • failed: Die Authentifizierung ist fehlgeschlagen. Entweder die Anmeldedaten sind oder der Nutzertyp ist falsch.
in_progress	Die Authentifizierung war erfolgreich, aber der Nutzer ist noch nicht sofort angemeldet. Stattdessen wird der Anmeldevorgang gestartet, der einige Zeit in Anspruch nimmt. Es gibt einen weiteren Response-Wert namens „auth_id“, mit dessen Hilfe man abwarten kann, bis der Anmeldevorgang abgeschlossen ist. Verwenden Sie ein POST an <code>URL/session/progress</code> um den Status des Anmeldevorgangs abzufragen. Hinweis: Sie können diese Session nicht für weitere Requests nutzen, bevor nicht der Anmeldevorgang beendet ist und Sie diesen finalen Status über <code>/session/progress</code> abgerufen haben.
auth_id	Die ID des Anmeldeprozesses. Wird nur benutzt, wenn „result“ „in_progress“ ist, wird benötigt für <code>/session/progress</code> , um den Fortschritt des Anmeldeprozess abzufragen.

11.2 Anmelden

Wenn der Anmeldevorgang asynchron gestartet wird und der Aufruf von `/session/login` das Ergebnis „in_progress“ zurückgibt, müssen Sie warten, bis der Anmeldevorgang abgeschlossen ist, bevor Sie weitere API-Aufrufe durchführen. Sie können den Status des Anmeldevorgangs abfragen, bis dessen Abschluss signalisiert wird. Verwenden Sie dazu den Aufruf `/session/progress`, um den Status abzurufen

Parameter

Parameter	Description
auth_id	Die Authentifizierungs-ID, die bei einem Aufruf von <code>/session/login</code> zurückkommt.

Response

Response	Description
progress	Der aktuelle Status/Fortschritt des Anmeldevorgangs, möglich sind: - unknown: Die auth_id ist ungültig oder der Anmeldeprozess konnte nicht korrekt gestartet werden. - initializing: Der Anmeldeprozess steht kurz vor dem Start. - started: Der Anmeldeprozess hat begonnen, ist aber noch nicht beendet. - Done: Der Anmeldeprozess ist beendet. Sie können diese Session jetzt für weitere API requests nutzen.

11.3 Session schließen / Abmelden

Wenn die Remote-API-Session nicht mehr benötigt wird, sollte sie geschlossen werden. Beim Schließen der Session wird der Nutzer von der User Station abgemeldet. Verwenden Sie dazu ein request an `/session/logout`.

Parameter

Es gibt keine Parameter.

Response

Response	Beschreibung
result	Ein boolescher Wert. „True“ bedeutet, dass die Abmeldung erfolgreich war, andernfalls „false“ (z. B. wenn der Benutzer aus anderen Gründen bereits abgemeldet war).
error	Optional, ein Fehler, wenn das Ergebnis „false“ ist.

Beispiel

1. Anmeldeprozess starten:

```
curl -c cookies.txt -b cookies.txt -H "Content-Type:application/json" -d '{"user name":"admin","password":
"IHSE_admin2026","user_type":"local"}' https://192.168.100.34:8443/api/v1/session/login
{"result":"in_progress","auth_id":"4dc950f2-2f8b-424b-ba31-d6fb33f943b7"}
```

2. Anmeldestatus abfragen:

```
curl -c cookies.txt -b cookies.txt -H "Content-Type:application/json" -d '{"auth_id":"4dc950f2-2f8b-424b-ba31-
d6fb33f943b7"}' https://192.168.100.34:8443/api/v1/session/progress
{"progress":"started"}
```

3. Einige Sekunden warten und neue Abfrage starten:

```
curl -c cookies.txt -b cookies.txt -H "Content-Type:application/json" -d '{"auth_id":"4dc950f2-2f8b-424b-ba31-
d6fb33f943b7"}' https://192.168.100.34:8443/api/v1/session/progress
{"progress":"done"}
```

4. Nutzen Sie die Session jetzt für weitere Requests.

5. Session schließen und abmelden:

```
curl -c cookies.txt -b cookies.txt -H "Content-Type:application/json" -d '{"auth_id":"4dc950f2-2f8b-424b-ba31-
d6fb33f943b7"}' https://192.168.100.34:8443/api/v1/session/logout
{"result":"true"}
```

Der Nutzer wird abgemeldet, die Session wird geschlossen.

11.4 Zugangsfunktionalität

11.4.1 Get Geräte und Targets

Die User Station unterstützt zwei Ansichten auf Target-Systeme:

- Zugangs-Geräte zentrische Ansicht: Es gibt Zugangsgeräte, wobei jedes Gerät über einen oder mehrere Ports zum Anschluss an die Target-Systeme verfügt.
- Targets-Ansicht: Es gibt Targets, von denen jedes über einen oder mehrere Wege (Zugangspunkte) erreichbar ist.

Für beide Ansichten gibt es Möglichkeiten, die Zugangsmethoden aufzulisten.

11.4.2 Get Geräte und Ports

Um alle Zugangsgeräte mit ihren Ports zu erhalten, senden Sie eine GET-Anfrage an die URL `/access/items`. Das Ergebnis ist ein Array von Elementen (Zugangsgeräten) mit allen Ports des Geräts. Einige der Ports sind möglicherweise nicht zugänglich (entweder aufgrund fehlender Berechtigungen oder weil ein Port nicht unterstützt wird). Außerdem kann ein Gerät über Portgruppen für mehrere Monitore verfügen. In diesem Fall sind die einzelnen Ports nicht zugänglich, wohl aber die Portgruppen.

Jedes der Elemente im Array enthält die folgenden Mitglieder:

- `id`: Die ID des Elements.
- `name`: Der Name des Elements.
- `ports`: Eine Reihe von Ports (siehe unten)
- `port_groups`: Eine Reihe von Multi-Monitor Portgruppen (siehe unten)

Jeder der Ports im Array weist die folgenden Eigenschaften auf:

- `id`: Die ID des Ports
- `name`: Der Name des Ports
- `port_type`: Der Typ des Ports (KVM, seriell oder nicht-unterstützter Porttyp)
- `status`: Der Portstatus des mit diesem Zugangspunkt verbundenen Ports (nur KVM-Zugangspunkte)
- `availability`: Der Verfügbarkeitsstatus des mit diesem Zugangspunkt verbundenen Ports (nur KVM-Zugangspunkte)
- `access_id`: Die ID des Zugangspunkts, der zu diesem Port gehört. Verwenden Sie die ID, um eine Zugangssitzung zu diesem Zugangspunkt dieses Ports herzustellen. Ist dieser Port nicht erreichbar, fehlt diese Eigenschaft.

Jede Portgruppe im Array hat die folgenden Eigenschaften:

- `id`: Die ID der Portgruppe
- `name`: Der Name der Portgruppe
- `port_ids`: Ein Satz von Port-IDs, die diese Portgruppe bilden.
- `access_id`: Die ID des Zugangspunkts, der zu dieser Portgruppe gehört. Verwenden Sie die ID, um eine Zugangssitzung zu diesem Zugangspunkt dieser Portgruppe herzustellen. Ist diese Portgruppe nicht erreichbar, fehlt diese Eigenschaft.

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type:application/json" https://192.168.100.34:8443/api/v1/access/items
{
  "items": [
    {
```

```

    "id":1,
    "name": "thre-SIRA CON",
    "ports": [
      {"id":6,"name": "thre-Mac-mini", "status": "up", "availability": "idle", "port_type": "kvm", "access_id":5},
      {"id":1,"name": "Local port (HDMI)", "status": "up", "availability": "idle", "port_type": "kvm", "access_id":2},
      {"id":2,"name": "Windows Box (Dual-VM)", "status": "up", "availability": "idle", "port_type": "kvm", "access_id":777},
      {"id":833,"name": "DSAM4 Port 1", "status": "down", "availability": "idle", "port_type": "serial", "access_id":1255},
      {"id":834,"name": "DSAM4 Port 2", "status": "down", "availability": "idle", "port_type": "serial", "access_id":1256},
      {"id":8,"name": "thre-SIRAUST", "status": "up", "availability": "idle", "port_type": "kvm", "access_id":7},
      {"id":7,"name": "thre-SIRAUST", "status": "up", "availability": "idle", "port_type": "kvm", "access_id":6},
    ]
    "port_groups":[
      {"id":1,"name": "Windows Box Dual", "port_ids":[3,4], "access_id":8},
    ]
  }
  {
    "id":594
    "name": "SIRAUST-101",
    "ports":[
      {"id":472,"name": "SIRA_User Station_Port1", "status": "up", "availability": "idle", "port_type": "kvm", "access_id":770}
    ]
    "port_groups":[ ]
  }
]
}

```

11.4.3 Get Targets und Zugangspunkte

Um alle Targets und deren Zugangspunkte abzurufen, senden Sie eine GET-Anfrage an die /access/targets URL. Sie erhalten ein Array mit Targets. Jedes Target verfügt über eine ID, einen Namen und ein Array mit Zugangspunkten. Jeder Zugangspunkt hat eine Zugangs-ID (erforderlich, um eine Zielverbindung zu diesem Zugangspunkt herzustellen) und einen Typ (KVM, seriell, SSH, VNC usw.). Die KVM- und seriellen Targets, die einen Port eines Zugangsgeräts darstellen, verfügen zudem über einen Status (up oder down) und eine Verfügbarkeitseinstellung.

Der Request gibt ein Array von Targets zurück. Jedes Target verfügt über die folgenden Elemente:

- id: Die ID des Targets
- name: Der Name des Targets
- access: Ein Array von Zugangspunkten zu diesem Target (siehe unten)

Jeder Zugangspunkt hat die folgenden Elemente:

- access_id: Die ID dieses Zugangspunkts. Verwenden Sie diese ID, um eine Zugangs-Session zu diesem Zugangspunkt diese Targets zu erstellen.
- access_type: Der Typ dieses Zugangspunkts (KVM, seriell, RDP, VNC, etc.). Der Typ multi_kvm bezieht sich auf ein vorkonfiguriertes Multi-Monitor-Target am Zugangsgerät, der Typ "virt_multi_kvm" ist ein virtuelles Multi-Monitor-Target, konfiguriert mit dieser User Station.

- **status:** Der Portstatus des mit diesem Zugangspunkt verbundenen Ports (nur KVM-Zugangspunkte)
- **availability:** Der Verfügbarkeitsstatus des mit diesem Zugangspunkt verbundenen Ports (nur KVM-Zugangspunkte)

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type:application/json" https://192.168.100.34:8443/api/v1/access/targets
```

```
{
  "targets":[
    {"id":2,"name":"Local Port (HDMI)","access":[{"access_id":2,"access_type":"kvm","status":"up","availability":"idle"}]}
  ],
  {"id":3,
    "name":"Windows Box (Dual-VM)",
    "access":[
      {"access_id":19,"access_type":"ssh",
      {"access_id":20,"access_type":"vnc",
      {"access_id":21,"access_type":"rdp",
      {"access_id":22,"access_type":"web",
      {"access_id":23,"access_type":"esxi",
      {"access_id":777,"access_type":"kvm","status":"up","availability":"idle"},
      {"access_id":781,"access_type":"virt_multi_kvm","status":"up","availability":"idle"},
    ]
  },
  {"id":4,"name":"Windows Box Dual","access":
    [{"access_id":4,"access_type":"kvm","status":"up","availability":"idle"}]}

  {"id":5,"name":"Mac-mini","access":
    [{"access_id":5,"access_type":"kvm","status":"up","availability":"idle"}]}

  {"id":6,"name":"SIRAUST","access":
    [{"access_id":6,"access_type":"kvm","status":"up","availability":"idle"}]}

  {"id":7,"name":"Windows Box","access":
    [{"access_id":7,"access_type":"kvm","status":"up","availability":"idle"}]}

  {"id":8,"name":"I-mac","access":
    [{"access_id":8,"access_type":"kvm","status":"up","availability":"idle"}]}
```

11.5 Verwaltung von Zugangs-Client-Sessions

11.5.1 Client-Sessions erstellen

Zugangs-Clients (KVM, VNC, RDP, SSH, etc.) können über API geöffnet und geschlossen werden.

Um eine Zugangs-Client-Session zu öffnen, POST zu der /access/open_client URL senden. Dieser Aufruf hat die folgenden Parameter:

- **access_id** (notwendig): Die Zugangspunkt ID, wie sie zu bekommen ist, siehe weiter oben (Get Geräte und Targets).
- **options** (optional): ein Array aus Schlüssel-Wert-Paaren zur Konfiguration der Session. Eine Liste der verfügbaren Optionen finden Sie in der API-Beschreibung.

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type:application/json" -d {"access_id": 2 } https://192.168.100.34:8443/api/v1/access/open_client
```

```
{"result":true}
```

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{ "access_id": 2, "options":[ { "key": "fullscreen", "value": "false" }, { "key": "x", "value": "1200" }, { "key": "y", "value": "800" }, { "key": "width", "value": "300" }, { "key": "height", "value": "200" }, { "key": "scale", "value": "true" } ] }' https://192.168.3.175:8443/api/v1/access/open_client
```

```
{"result":true}
```

11.5.2 Zugangs-Client schließen

Um eine Zugangs-Client-Session zu schließen, POST zu der /access/close_client URL senden. Dieser Aufruf hat einen Paramter: Zugangspunkt ID, wie sie zu bekommen ist, siehe weiter oben (Get Geräte und Targets)

Example

```
curl -c cookies.txt -b cookies.txt --H "Content-Type: application/json" -d '{"access_id": 2 }' https://192.168.3.175:8443/api/v1/access/close_client
```

```
{"result":true}
```

11.5.3 Benannte Szenen (auch bekannt als Window Layouts)

Benannte Szenen (oder Window Layouts) sind Sammlungen von Zugangs-Client-Fenstern, die mitsamt ihren Positionen und Größen gespeichert und wiederhergestellt werden können. Über die API können Benutzer derzeit eine Liste der verfügbaren Szenen abrufen und eine Szene wiederherstellen (oder öffnen). Es ist derzeit nicht möglich, neue Szenen zu erstellen oder bestehende Szenen zu überschreiben.

Liste aller Szenen erhalten

Um eine Liste der Szenen abzurufen, senden Sie eine GET-Anfrage an die /access/scenes URL. Die API gibt ein Array von Szenen zurück. Jede Szene verfügt über eine ID (Element „id“) und einen „Namen“. Eine der Szenen kann die aktive Szene sein (für diese Szene ist das Element „is_active“ auf „true“ gesetzt).

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/access/scenes {"named_scenes":[{"id":22,"name":"Window Layout 1","is_active":false},{ "id":23,"name":"Window Layout 2", "is_active":true}]}
```

Benannte Szene wiederherstellen

Um eine benannte Szene wiederherzustellen, POST zu der /access/open_scene URL senden. Diese Anfrage hat einen Parameter:

- scene_id (notwendig): Die ID der Szene, wie sie zu bekommen ist, siehe oben (Liste aller Szenen erhalten).

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{"scene_id": 23}' https://192.168.3.175:8443/api/v1/access/open_scene {"result":true}
```

11.5.4 Fensterverwaltung

Die User Station API bietet einige spezielle Funktionen zur Fensterverwaltung, mit denen Access-Client-Fenster angeordnet oder geschlossen werden können. Um einen solchen Vorgang auszuführen, senden Sie eine POST-Anfrage an die URL `/access/window_management`. Dieser Aufruf hat einen Parameter: den auszuführenden Vorgang. Dies kann einer der folgenden sein:

- `tile`: Die Fenster in Kacheln anordnen.
- `untile`: Den letzten „Kachel“-Vorgang rückgängig machen.
- `minimize`: Alle Fenster minimieren.
- `unminimize`: Die Fenster wiederherstellen.
- `close`: Alle Client-Fenster schließen.

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{"operation":"close"}' https://192.168.3.175:8443/api/v1/access/window_management
{"result":true}
```

11.6 Wartung

Die User Station unterstützt über die API einige grundlegende Wartungsfunktionen. Derzeit stehen Funktionen für die Identitätsprüfung, Firmware-Informationen sowie für Updates und die Sicherung bzw. Wiederherstellung von Einstellungen zur Verfügung.

 Für das Firmware-Update sowie die Sicherungs- und Wiederherstellungsfunktionen sind Systemadministratorrechte erforderlich.

11.6.1 Identitätsdaten

Um einige grundlegende Identitätsdaten abzurufen, senden Sie eine GET-Anfrage an die URL `/maintenance/identity`. Sie erhalten dann den Produktcode, den Hersteller, die Seriennummer des Geräts und die MAC-Adressen.

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/maintenance/identity
{"product":"SIRAUST","vendor":"IHSE GmbH","serial":"12345","mac":["80:EE:73:E2:31:45","80:EE:73:E2:31:46"]}
```

11.6.2 Firmware-Funktionen

Software-Versionen

Um Informationen zu den Firmware-Versionen abzurufen, senden Sie eine GET-Anfrage an die URL `/maintenance/firmware`. Das resultierende Objekt enthält die Versionen der installierten Firmware, des zugrunde liegenden Betriebssystems und des Linux-Kernels.

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/maintenance/firmware
{"firmware_version":"4.4.0.5.85.20210323123034","base_os_version":"CentOS Linux release 7.9.2009(Core)","kernel_version":"Linux 3.10.0-1160.6.1.el7.x86_64"}
```

11.6.3 Firmware-Update

Um ein Software-Upgrade durchzuführen, senden Sie eine POST-Anfrage an die URL `/firmware/upgrade`. Diese Anfrage enthält einen Parameter: die URI der Firmware-Datei. Die User Station lädt diese Firmware-Update-Datei herunter und wendet sie an, sofern es sich um ein gültiges Update-Image handelt. Dieser Aufruf gibt ein boolesches Ergebnis zurück, das angibt, ob das Update erfolgreich gestartet wurde oder nicht. Im Falle eines Fehlers wird zusätzlich eine Fehlermeldung zurückgegeben.

 Das Importieren des Firmware-Updates erfolgt synchron. Insbesondere der Download, aber auch das Entpacken, dauert einige Sekunden. Außerdem leitet dieser API-Aufruf lediglich das Update ein. Sobald der Import abgeschlossen ist und die Update-Datei gültig ist, kehrt diese API-Funktion zurück, und das eigentliche Update wird im Hintergrund durchgeführt. API-Nutzer haben keine Kontrolle über den eigentlichen Update-Vorgang. Nach Abschluss des Update-Vorgangs wird die User Station automatisch neu gestartet.

Beispiel

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{"uri":"https://192.168.2.101/SIRAUST_4.4.0.1.50_update.bin"}' https://192.168.3.175:8443/api/v1/maintenance/firmware/upgrade
```

```
{"result":false,"error":"The provided software version is too old! It must be equal or newer than the current version."}
```

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{"uri":"https://192.168.2.101/SIRAUST_4.4.0.1.98_update.bin"}' https://192.168.3.175:8443/api/v1/maintenance/firmware/upgrade
```

```
{"result":true}
```

11.6.4 Backup/Wiederherstellen

Mit der User Station Remote API können Sie auf System-Sicherungsdateien zugreifen. Sie können alle im System verfügbaren Sicherungsdateien auflisten, diese herunterladen oder hochladen sowie Sicherungsdateien wiederherstellen oder löschen.

Alle Backups im System abrufen

Um eine Liste aller derzeit im System verfügbaren Sicherungsdateien abzurufen, senden Sie eine GET-Anfrage an die URL `/maintenance/backups`.

Die Antwort ist ein Array namens „backups“, das alle Sicherungsdateien/Backups im System enthält. Jeder Eintrag verfügt über die folgenden Elemente:

- `id`: Die ID des Backups
- `filename`: Der Name der Datei, die diese Sicherung intern repräsentiert.
- `status`: Der Status des Updates. Da Updates asynchron erstellt werden, ist die Erstellung einer Sicherung möglicherweise noch nicht abgeschlossen, wenn Sie diese abrufen. Folgende Werte sind möglich:
 - `initialized`: Die Sicherung wurde gerade gestartet. Sie ist noch nicht erstellt.
 - `working`: Der Sicherungsvorgang hat begonnen, ist aber noch nicht abgeschlossen.
 - `complete`: Die Sicherung ist abgeschlossen und kann genutzt werden.

Ein Backup im System erhalten (nur Metadaten)

Wenn Sie nur an einem bestimmten Backup interessiert sind (z. B. wenn Sie darauf warten, dass der Backup-Vorgang abgeschlossen wird), müssen Sie nicht die gesamte Liste der Backups abfragen. Wenn Sie die ID eines Backups kennen, können Sie die Metadaten dieses Backups abrufen, indem Sie eine GET-Anfrage an die URL `/maintenance/backups/<id_of_the_backup>` URL senden.

Die Antwort ähnelt der obigen Liste, es wird jedoch nur eine Sicherungsdatei zurückgegeben.

Den Inhalt einer Sicherungsdatei abrufen

Um die Binärdaten einer Sicherungsdatei abzurufen, senden Sie eine GET-Anfrage an die URL `/maintenance/backups/<id_der_Sicherung>/content`. Dieser Aufruf gibt die Daten in Form einer Base64-kodierten Zeichenfolge zurück (oder eine Fehlermeldung, falls ein Fehler aufgetreten ist).

Eine Sicherung im System löschen

Um eine Sicherung im System zu löschen, senden Sie eine GET-Anfrage an die URL `/maintenance/backups/<id_der_Sicherung>/destroy`. Der Aufruf gibt das Ergebnis des Vorgangs zurück sowie eine Fehlermeldung, falls ein Fehler aufgetreten ist.

Eine neue Sicherung erstellen

Wenn Sie eine neue Sicherung des Systems im aktuellen Zustand erstellen möchten, senden Sie eine GET-Anfrage an die URL `/maintenance/backups/new`. Diese gibt das Ergebnis (erfolgreich oder fehlgeschlagen), die ID der neuen Sicherung (bei Erfolg) oder eine Fehlermeldung zurück, falls ein Fehler aufgetreten ist.

Sie können die von diesem Aufruf zurückgegebene ID für die spätere Verwendung der Sicherung nutzen, z.B. um sie später herunterzuladen. Bitte beachten Sie, dass die Sicherung im Hintergrund erstellt wird und nicht sofort verfügbar ist. Bitte rufen Sie die Details dieser Sicherung erst ab, wenn sich der Status auf „abgeschlossen“ geändert hat.

Eine Sicherungsdatei importieren

Außerdem besteht die Möglichkeit, Sicherungskopien in das System hochzuladen oder zu importieren. Verwenden Sie dazu eine POST-Anfrage an die URL `/api/v1/maintenance/backups/import`.

Sie können die Datei entweder direkt hochladen (mithilfe einer Base64-kodierten Zeichenfolge) (verwenden Sie den Parameter „content“) oder eine URL angeben (verwenden Sie den Parameter „uri“), von der die User Station die Sicherungsdatei herunterlädt. Diese Funktion gibt das Ergebnis (erfolgreich oder fehlgeschlagen), die ID der neuen Sicherung (bei Erfolg) oder eine Fehlermeldung zurück, falls ein Fehler aufgetreten ist.

Bitte beachten Sie, dass dieselbe Sicherungsdatei nicht mehrmals im System vorhanden sein darf. Das Hochladen einer bereits vorhandenen Sicherungsdatei schlägt fehl.

Ein Backup wiederherstellen

Um ein Backup wiederherzustellen, senden Sie eine GET-Anfrage an die URL `/maintenance/backups/<id_des_Backups>/restore`. Diese gibt das Ergebnis (erfolgreich oder fehlgeschlagen) sowie im Falle eines Fehlers eine Fehlermeldung zurück.

Bitte beachten Sie, dass dieser Aufruf lediglich den Wiederherstellungsprozess einleitet. Der Großteil der Arbeit bei der Wiederherstellung eines Backups erfolgt im Hintergrund, während die Webdienste heruntergefahren werden. Es ist nicht möglich, den Fortschritt oder den Status des Wiederherstellungsprozesses einzusehen. Wenn dieser Aufruf den Status „erfolgreich“ zurückgibt, bedeutet dies, dass die Wiederherstellung erfolgreich gestartet wurde. Dies bedeutet jedoch nicht, dass das Backup erfolgreich wiederhergestellt wurde.

Beispiel

- Rufen Sie zunächst eine Liste aller Backups im System ab.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups
{
  "backups":[
```

```
{
  "id":11,"filename":"SIRAUST_backup_4.4.0.5.85.20240324092030_12345_20240325104406.dat","status":
  "complete"},
  {
    "id":10,"filename":"SIRAUST_backup_4.4.0.5.85.20240324092030_12345_20240325104402.dat","status":
    "complete"}
  ]
}
```

- Existierende Backups löschen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups/10/destroy
```

```
{
  "result":true
}
```

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups/11/destroy
```

```
{
  "result":true
}
```

- Liste wieder anfordern, die jetzt leer ist.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups
```

```
{
  "backups":[]
}
```

- Eine neue Sicherungsdatei (Backup) erstellen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups/new
```

```
{
  "result":true,"backup_id":12
}
```

- Den Status dieser Sicherung abfragen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups/12
```

```
{
  "backup":
  {
    "id":12,"filename":"SIRAUST_backup_4.4.0.5.85.20240324092030_12345_20240325104912.dat","status":
    "working"
  }
}
```

- Die Sicherung ist noch nicht abgeschlossen (Status: „working“), einen Moment warten und es erneut versuchen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups/12
```

```
{
  "backup":
  {
    "id":12,"filename":"SIRAUST_backup_4.4.0.5.85.20240324092030_12345_20240325104912.dat","status":
    "complete"
  }
}
```

- Die Sicherung ist abgeschlossen. In eine Datei herunterladen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups/12/content > backup.txt
```

```
{
  "content":["..."]
}
```

- Die Sicherungsdatei löschen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/
maintenance/backups/12/destroy
```

```
{"result":true}
```

- Die Sicherungsdatei wieder hochladen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d "@backup.txt" https://192.168.3.175:8443/api/v1/maintenance/backups/import
```

```
{"result":true,"backup_id":13}
```

- Warten bis der Status dieser Sicherungsdatei „complete“ ist.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/maintenance/backups/13
```

```
{"backup":
```

```
{"id":12,"filename":"SIRAUST_backup_4.4.0.5.85.20240324092030_20240325104912.dat","status":"complete"}}
```

- Oder: Importieren der Sicherungsdatei über eine URL.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" -d '{"uri":"http://192.168.2.101/backup.bin"}' https://192.168.3.175:8443/api/v1/maintenance/backups/import
```

```
{"result":true,"backup_id":13}
```

- Jetzt diese Sicherungsdatei wiederherstellen.

```
curl -c cookies.txt -b cookies.txt -H "Content-Type: application/json" https://192.168.3.175:8443/api/v1/maintenance/backups/13/restore
```

```
{"result":true}
```

- Die Sicherung wird im Hintergrund wiederhergestellt. Nach Abschluss des Vorgangs wird die User Station neu gestartet.

12 BIOS-Einstellungen

Im Vergleich zu einem normalen PC stehen in der User Station nur eine begrenzte Anzahl von BIOS-Einstellungen zur Verfügung. Einige Einstellungen können geändert werden, um die Fehlerbehebung (Startreihenfolge), die Energieverwaltung und die Sicherheit zu ändern.

Aufrufen des BIOS

1. Die SIRA User Station einschalten oder neu starten.
2. Wenn der erste Bildschirm erscheint, die Taste **Entf** drücken.

Main Settings

Enthält eine Übersicht über die installierte Hardware: Prozessor, Arbeitsspeicher, BIOS-Version. Systemdatum und -uhrzeit können geändert werden.

Advanced Settings

Power Management

- Suspend Mode: Nicht unterstützt.
- Wake Up by USB: Nicht unterstützt.
- EuP Function: Enable automatic energy management.
 - Enabled: Maximale Energieeinsparung.
 - Disabled: Es können benutzerdefinierte Energieeinstellungen festgelegt werden.

Die folgenden Einstellungen können nur geändert werden, wenn EuP deaktiviert ist.

- Power-On after Power-Fail: Wählen Sie den Energiezustand aus, der nach einem Stromausfall angewendet werden soll (on, of, last state).
- Wake Up by Ring: Das Aufwecken der User Station über das Modem zulassen.
 - Siehe auch <https://en.wikipedia.org/wiki/Wake-on-ring> für detaillierte Informationen.
- Wake Up by LAN: Das Aufwecken der User Station über das LAN zulassen.
 - <https://en.wikipedia.org/wiki/Wake-on-LAN>
- PowerOn by RTC Alarm: Legen Sie eine Uhrzeit (Stunde, Minute, Sekunde) fest, zu der die User Station automatisch eingeschaltet wird.

Boot

Die Boot-Einstellungen dienen ausschließlich der Fehlerbehebung, beispielsweise wenn eine Neuinstallation des Betriebssystems erforderlich ist. Sie können die Boot-Reihenfolge ändern, einschließlich der Priorität der Festplatte und des USB-Laufwerks. Standardmäßig wird ausschließlich von der internen Festplatte gebootet.

Security

- Ein BIOS-Passwort festlegen oder löschen. Dies ist nützlich, um zu verhindern, dass Benutzer das BIOS aufrufen.

 Es wird empfohlen, ein BIOS-Passwort festzulegen. **Wichtig:** Vergessen Sie das BIOS-Passwort nicht!

- Flash Write Protection: Ändern Sie diese Einstellung nicht (sie wird für BIOS-Updates verwendet).

Save & Exit

Speichern oder verwerfen Sie die Änderungen an den BIOS-Einstellungen.

Laden Sie die Standardwerte des BIOS.

13 Technische Daten

Typ	Eigenschaften	
CPU	AMD Ryzen V2516	
Video	Controller	AMD Radeon™ Graphics
	HDMI	HDMI 2.0a, Auflösung bis zu 4096 x 2160 @ 60 Hz
	DisplayPort	DisplayPort 1.2a, DP++, Auflösung bis zu 4096 x 2160 @ 60 Hz
	Multi-Display	Bis zu 4 Monitore (einschließlich 2x USB Typ C Anschlüsse an der Vorderseite)
RAM	8 GB	
Speicher	128 GB SSD	
Netzwerk	LAN 1	10 / 100 / 1000 / 2500 Mbps
	LAN 2	10 / 100 / 1000 Mbps
Vorderseite I/O	Taste	EIN/AUS Schalter mit LED
	USB	2x USB 3.2 Gen2 Typ A
		2x USB 3.2 Gen2 Typ C (unterstützt DP1.2a Monitor-Ausgang)
Rückseite I/O	Audio	Kopfhörer- und Mikrofon-Anschluss: 3,5 mm Klinkenbuchse
	Monitor	HDMI 2.0a
		DisplayPort 1.2 a
	USB	2x USB 2.0 type A
	LAN (RJ45)	Gigabit LAN 2.5G
		Gigabit LAN
Stromanschluss	DC IN	12 - 19 V
	Input	100 - 240 VAC, 1,5 A, 50/60 Hz
Zertifizierungen	Output	19 VDC, 3,42 A, 65 W, Level VI
	EMV	FCC, CE, VCCI, RCM, BSMI
	Sicherheit	cUL, CB, KCC

13.1 Pinbelegungen

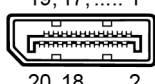
Upstream/Downstream

Die Pins der DisplayPort-Buchsen sind unterschiedlich belegt.

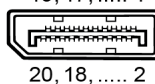
Upstream: Daten werden verschickt (z. B. Quelle, Grafikkarte, Videoausgang eines Gerätes)

Downstream: Daten werden empfangen (z. B. Senke, Monitor, Videoeingang eines Gerätes)

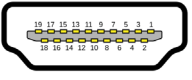
13.1.1 DisplayPort - Upstream

Anschluss	Pin	Signal	Pin	Signal
	1	ML_Lane 0 (p)	11	GND
	2	GND	12	ML_Lane 3 (n)
	3	ML_Lane 0 (n)	13	CONFIG1
	4	ML_Lane 1 (p)	14	CONFIG 2
	5	GND	15	AUX CH (p)
	6	ML_Lane 1 (n)	16	GND
	7	ML_Lane 2 (p)	17	AUX CH (n)
	8	GND	18	Hot Plug Erkennung
	9	ML_Lane 2 (n)	19	Spannungsversorgung: Masse
	10	ML_Lane 3 (p)	20	Spannungsversorgung: (+3,3 V/0,5 A)

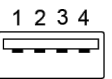
13.1.2 DisplayPort - Downstream

Anschluss	Pin	Signal	Pin	Signal
	1	ML_Lane 3 (n)	11	GND
	2	GND	12	ML-LANE 0 (p)
	3	ML_Lane 3 (p)	13	Config1/GND
	4	ML_Lane 2 (n)	14	Config2/GND
	5	GND	15	AUX CH (p)
	6	ML_Lane 2 (p)	16	GND
	7	ML_Lane 1 (n)	17	AUX CH (n)
	8	GND	18	Hot Plug Erkennung
	9	ML_Lane 1 (p)	19	Spannungsversorgung: Masse
	10	ML_Lane 0 (n)	20	Nicht angeschlossen

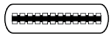
13.1.3 HDMI

Anschluss	Pin	Signal	Pin	Signal
	1	T.M.D.S data 2+	11	T.M.D.S clock GND
	2	T.M.D.S data 2 GND	12	T.M.D.S clock-
	3	T.M.D.S data 2-	13	CEC
	4	T.M.D.S data 1+	14	HEC Data+
	5	T.M.D.S data 1 GND	15	DDC Input (SCL)
	6	T.M.D.S data 1-	16	DDC Output (SDA)
	7	T.M.D.S data 0+	17	DDC/CEC/HEC GND
	8	T.M.D.S data 0 GND	18	+5V (DC) high impedance
	9	T.M.D.S data 0-	19	HEC Data-
	10	T.M.D.S clock+		

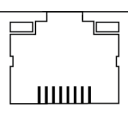
13.1.4 USB, Typ A

Anschluss	Pin	Signal	Farbe
	1	+5 V (DC)	Rot
	2	D -	Weiß
	3	D +	Grün
	4	GND	Schwarz

13.1.5 USB, Typ C

Anschluss	Pin	Name	Beschreibung	Pin	Name
A1.....A12  B12.....B1	A1	GND	DC Ground	B12	GND
	A2	SSTX1+	Super speed data transmit + (host to device)	B11	SSTX2+
	A3	SSTX1-	Super speed data transmit – (device to host)	B10	SSTX2-
	A4	VDD	DC power (+5 V)	B9	VDD
	A5	CC1	Power delivery communication line	B8	CC2
	A6	D+	Data transmit (host to device)	B7	D+
	A7	D-	Data transmit (device to host)	B6	D-
	A8	SBU1	Secondary bus	B5	SBU2
	A9	VDD	DC power (+5 V)	B4	VDD
	A10	SSRX2-	Super speed data receive - (device to host)	B3	SSRX1-
	A11	SSRX2+	Super speed data receive + (host to device)	B2	SSRX1+
	A12	GND	DC Ground	B1	GND

13.1.6 RJ45 (LAN)

Anschluss	Pin	Signal	Pin	Signal
	1	D1+	5	D3-
	2	D1-	6	D2-
	3	D2+	7	D4+
	4	D3+	8	D4-

13.2 Leistungsaufnahme

Produkttyp	Maximale Leistungsaufnahme
Draco SIRA User Station	49,78 W (19 V x 2,62 A)

13.3 Abmessungen

Produkttyp	Abmessungen (BxHxT) in mm
Draco SIRA User Station	130 x 40 x 109,25 mm

13.4 Gewicht

Produkttyp	Gewicht
Draco SIRA User Station	610g (1,35 lbs)

13.5 Umweltbedingungen und Emissionen

Parameter	Werte
Betriebstemperatur	-20 bis +40°C (-4 bis 104°F)
Lagertemperatur	-40 to 80°C (-40 to 176°F)
Rel. Luftfeuchtigkeit	5 - 90% (keine Kondensation)
Betriebshöhe	Max. 5.000 m (14.000 ft)
Wärmeableitung	Entspricht der Leistungsaufnahme in Watt (W)

13.6 MTBF

Mittlere Betriebsdauer zwischen Ausfällen: 222.265 h (60°C)

14 Technischer Support

Bitte lesen Sie vor einer Kontaktaufnahme das Benutzerhandbuch und installieren und konfigurieren Sie Ihre User Station entsprechend.

14.1 Checkliste Kontaktaufnahme

Bitte füllen Sie unsere Checkliste für Service- und Problemfälle (Download) aus. Die Checkliste wird zur Bearbeitung Ihrer Anfrage benötigt. Halten Sie bei der Kontaktaufnahme folgende Informationen bereit:

- Firma, Name, Telefonnummer und E-Mail-Adresse
- Typ und Seriennummer des Geräts
- Datum und Nummer des Kaufbelegs, ggf. Name des Händlers
- Ausgabedatum des vorliegenden Handbuchs
- Art, Umstände und ggf. Dauer des Problems
- Am Problem beteiligte Komponenten (z. B. Grafikquelle, Betriebssystem, Monitor, USB-HID-/USB-2.0-Geräte, Verbindungskabel)
- Ergebnisse aller bereits durchgeführten Maßnahmen

14.2 Checkliste Versand

1. Zur Einsendung Ihres Geräts benötigen Sie eine RMA-Nummer (Warenrückgabenummer). Kontaktieren Sie hierzu Ihren Händler.
2. Verpacken Sie die Geräte sorgfältig. Fügen Sie alle Teile bei, die Sie ursprünglich erhalten haben. Verwenden Sie möglichst den Originalkarton.
3. Vermerken Sie die RMA-Nummer gut lesbar auf Ihrer Sendung.

 Geräte, die ohne Angabe einer RMA-Nummer eingeschickt werden, werden nicht angenommen. Die Sendung wird unfrei und unbearbeitet an den Absender zurückgeschickt.

15 Anhänge

15.1 Anhang A: Empfehlungen zu offenen Ports

Listening Ports:

Standardmäßig hat die User Station keine offenen Listening-Ports, es sei denn, die folgenden Einstellungen sind aktiviert:

- 80 (HTTP) häufig verwendetes Internetprotokoll
- 443 (HTTPS) wenn Fernsteuerung aktiviert ist
- 22 (SSH) wenn Support-Zugriff aktiviert ist
- 24800 wenn Tastatur-/Mausmitbenutzung aktiviert ist
- 8443 für Remote API

Ausgehende TCP-Ports

- 5000 und 443 für die Kommunikation zum Gerät (konfigurierbar)
- 5900 für VNC-Targets (konfigurierbar; einige VNC-Clients nutzen andere Ports)
- 3389 für RDP-Targets (konfigurierbar)
- 22 für SSH-Targets (konfigurierbar)
- 80 und 443 für Web-Targets (konfigurierbar)
- 24800 für Tastatur-/Mausmitbenutzung
- LDAP nutzt die Ports 389 oder 636 (wenn TLS verwendet wird, beide sind konfigurierbar)

15.2 Anhang B:

Unterstützung für den Mausmodus für Dual Video Portgruppen und M-KVM-Targets

Wählen Sie je nach Betriebssystem den am besten geeigneten Mausmodus für Dual Video Portgruppen oder M-KVM-Ziele aus.

Windows Betriebssysteme

Empfehlung: Intelligent Mode funktioniert am besten, vorausgesetzt „Enhanced Pointer Precision“ ist auf dem Target deaktiviert (Control Panel/Mouse/Pointer Options) und die Mausgeschwindigkeit liegt bei 50 %.

- Standard Mode funktioniert ebenfalls, vorausgesetzt „Enhanced Pointer Precision“ ist deaktiviert und die Mausgeschwindigkeit beträgt 50 %.
- Die Maus synchronisiert sich im „Absolut Mouse Mode“ unter den neuesten Windows-Betriebssystemen nicht korrekt. Es sind zwei Mäuse da, eine für den Client und eine für das Betriebssystem. Diese sind nicht miteinander synchronisiert, sodass eine durchgehende Anzeige über alle Monitore hinweg nicht möglich ist.

 Die Bildschirmauflösung darf weder skaliert werden noch schwarze Ränder aufweisen.

Linux Betriebssysteme

Empfehlung: Der absolute Mausmodus funktioniert am besten.

Apple Betriebssysteme

Empfehlung: Es sollte der Einzel-Mausmodus verwendet werden, da die Maus bei Apple Mac-Target-Geräten mit M-KVM/zwei Videoanschlüssen in keinem Modus synchronisiert wird.

16 Glossar

Die folgenden Bezeichnungen werden in diesem Handbuch verwendet oder sind allgemein in der Video- und KVM-Technologie üblich.

Term	Beschreibung
AES/EBU	Bezeichnung für die Spezifikation einer Schnittstelle zur Übertragung digitaler Stereo-, Zweikanal- oder Mono-Audiosignale zwischen verschiedenen Geräten nach der Norm AES3
API	<u>A</u> pplication <u>P</u> rogramming <u>I</u> nterface, Schnittstelle zur Programmierung von Anwendungen
Cat X	Ledes Cat 5e (Cat 6, Cat 7) Kabel
Client	Eine Softwareanwendung, um auf entfernte Computer zuzugreifen.
CON-Unit	Decoder-Extendermodul zum Anschluss an die Konsole (Monitor(e), Tastatur und Maus; optional auch mit USB 2.0-Geräten)
CPU-Unit	Encoder-Extendermodul zum Anschluss an eine Quelle
DDC	Der Display Data Channel (DDC) ist eine serielle Kommunikationsschnittstelle zwischen Monitor und Quelle (Computer, CPU), die einen Datenaustausch über das Bildschirmkabel ermöglicht und es dem Betriebssystem erlaubt, den Bildschirmtreiber automatisch zu installieren und zu konfigurieren.
DisplayPort	Durch die VESA genormte Schnittstelle zur volldigitalen Übertragung von Audio- und Videodaten. Es wird zwischen den DisplayPort-Standards 1.1 und 1.2 unterschieden. Die Signale haben LVDS-Level.
Dual-Head / DH	System mit zwei Grafikanalysen
EDID	<u>E</u> xtended <u>D</u> isplay <u>I</u> dentification <u>D</u> ata ist ein Metadatenformat (128 Byte) für Anzeigegeräte zur Beschreibung ihrer Fähigkeit gegenüber einer Videoquelle (z. B. einer Grafikkarte).
ESD	Elektrostatische Entladung (ESD, electro-static discharge) beschreibt einen plötzlichen Stromfluss zwischen zwei elektrisch geladenen Objekten. Dies kann durch einen elektrischen Kurzschluss oder einen dielektrischen Durchschlag verursacht werden. Dies muss beim Auspacken der KVM-Extendermodule, bei der Montage und bei der ersten Verwendung berücksichtigt werden.
ESXi	VMware ESX ist ein von VMware entwickelter Typ-1-Hypervisor der Enterprise-Klasse zur Bereitstellung und zum Betrieb virtueller Rechner.
Glasfaser	Single-Mode oder Multi-Mode-Glasfaserkabel
Konsole	Monitor, Tastatur, Maus, Mediensteuerung, externe Umschaltlösung, usw.
KVM	Tastatur (Keyboard), Video und Maus
LDAP	<u>L</u> ightweight <u>D</u> irectory <u>A</u> ccess <u>P</u> rotocol ist ein offenes, plattformunabhängiges Protokoll, das den Zugriff auf und die Verwaltung von Verzeichnisdiensten ermöglicht.
LPCM	LPCM (Linear Pulse Code Modulation) ist ein Pulsmodulationsverfahren, oft verstanden als unkomprimiertes Datenformat. Durch das LPCM-Verfahren wird ein analoges Signal in ein digitales Signal umgewandelt mit gleichmäßig großen Wertebereichen.
Mini-DisplayPort	Durch die VESA genormte Schnittstelle zur volldigitalen Übertragung von Audio- und Videodaten. Die Signale haben LVDS-Level.
Mini-XLR	Industriestandard für elektrische Steckverbindungen (3-polig) zur Übertragung von digitalen Audio- und Steuersignalen
MTBF	<u>M</u> ean <u>T</u> ime <u>B</u> etween <u>F</u> ailure gibt die mittlere Betriebsdauer zwischen Ausfällen an und beschreibt die Zuverlässigkeit des Systems.
Multi-Mode	50 µm Multi-Mode-Glasfaserkabel

Term	Beschreibung
RCA (Cinch)	Nicht genormte Steckverbindung zur Übertragung von elektrischen Audio- und Videosignalen, vorrangig an Koaxialkabeln
RDP	Das Remote Desktop Protocol ist eine Netzwerkprotokoll von Microsoft für den Fernzugriff auf Computer.
S/PDIF	Schnittstellen-Spezifikation für die elektrische oder optische Übertragung digitaler Stereo-Audiosignale zwischen verschiedenen Geräten für die Anwendung im Unterhaltungselektronikbereich
SFP	SFPs (<u>S</u> mall <u>F</u> orm Factor <u>P</u> luggable) sind steckbare Schnittstellen-Module für Gigabit-Verbindungen. Es gibt sie für Cat X und Glasfaser.
Single-Head / SH	System mit einem Videoanschluss
Single-Mode	9 µm Single-Mode-Glasfaser
SSH	Das SSH File Transfer Protocol ist eine für die Secure Shell entworfene Alternative zum File Transfer Protocol (FTP). Es begnügt sich mit einer einzigen Verbindung zwischen Client und Server.
Target	Ein entfernter Computer oder Server, auf den mit Hilfe von verschiedenen Softwareanwendungen (Clients) zugegriffen werden kann.
TOSLINK	Standardisiertes Lichtwellenleiter-Verbindungssystem zur digitalen Übertragung von Audiosignalen (F05-Steckverbindung)
USB-HID	USB-HID-Geräte (Human Interface Device) ermöglichen es Benutzern mit Computern zu interagieren. Für die Installation ist kein spezieller Treiber notwendig. Beim Anschließen wird die Meldung „Neues USB-HID-Gerät gefunden“ eingeblendet. Zu den USB-HID-Geräten zählen neben Tastatur und Maus z. B. auch Grafiktablets und Touchscreens. Speicher-, Video- und Audiogeräte sind keine USB-HID-Geräte.
VNC	Virtual Network Computing ist eine Softwareanwendung für den Fernzugriff auf Computer.

17 Index

A

Administrationsfunktionen einstellen	105
Anmelden mit LDAP	125
Anpassungen	138
Anzeigeeinstellungen	136
API-Konfiguration	166
Authentifizierung	113
Autologin	114

B

Backup	155
Beenden	25
Begriffe und Schreibweisen	8
Benutzervoreinstellungen	87
BIOS-Einstellungen	177
Bond-Verbindungen	43

D

Diagnostische Protokolldatei	163
------------------------------------	-----

E

Empfehlungen zu offenen Ports	183
Ereignisprotokoll	152
Ereignisprotokolle archivieren	153
Ethernet-Verbindungen	35

F

Fensteranordnungen	22
Fensterverwaltung	21
Fernsteuerungs-Einstellungen	141
Filter	79
FIPS-Modus	130
Firefox Web Browser	20

G

Geräte editieren	55
Geräte hinzufügen	53
Geräte importieren	56
Geräte löschen	56
Geräte-Menü	81
Geräte-Zertifikate	131
Glossar	185
Gruppen	109

H

Hauptmenü	19
Beenden	25
Fensteranordnungen	22

Fensterverwaltung	21
Firefox Web Browser	20
Hilfe	23

Hilfe	23
Hotkeys und Gesten	95

I

Installation	16
--------------------	----

K

Konfiguration	53
Kundendienst	161
Kundendienstzugang	162
KVM-Clients nutzen	47
KVM-Ports konfigurieren	59

L

LDAP	116
LEDs	
Netzwerk-Verbindung	15
Stromversorgung	15

Lieferumfang	13
--------------------	----

Links und Weiterleitungen	134
---------------------------------	-----

M

Monitor entsperren	137
--------------------------	-----

N

Navigation und Zugang	78
Netzwerkdiagnose	164
Netzwerkeinstellungen	35
Netzwerkspeicher	148
Nutzer	105
Nutzer entsperren	134
Nutzer sperren	133
Nutzungsbedingungen	135

O

OpenVPN-Verbindungen	45
----------------------------	----

P

Passwort ändern	104
Passwort-Einstellungen	133
Pinbelegungen	179
DisplayPort Downstream	179
DisplayPort Upstream	179
HDMI	180
RJ45 (LAN)	180
USB, Typ A	180

USB, Typ C	180	Tastatur-Makros	91
Port-Navigator	78	Technische Daten	178
Port-Scanner	83	Abmessungen	181
Port-Scanner Tabellenansicht	86	Gewicht	181
Port-Scanner-Einstellungen	100	Leistungsaufnahme	181
Privater Schlüssel	128	MTBF	181
Produktansichten	14	Umweltbedingungen und Emissionen	181
Produkteigenschaften	14	Technischer Support	182
Produkttypen		Checkliste Kontaktaufnahme	182
CON-Units	13	Checkliste Versand	182
Stand-Alone-Unit	13	U	
User Station	13	Über das Gerät	165
R		Überprüfung von Schlüsseln und Zertifikaten	131
Richtlinien	10	Unterstützung für den Mausmodus	184
S		V	
Screenshot-Einstellungen	102	Vertrauenswürdige Zertifikate	126
Screenshots aufnehmen	103	Verwendungszweck	9
Selbst Signiertes Zertifikat	129	W	
Serielle Clients nutzen	49	Wartung	152
Server-Zertifikate	127	Reinigung	152
Sicherheitseinstellungen	130	WEEE	10
Sicherheitshinweise	11	Werkseinstellungen	158
Software-Update	160	Wiederherstellung	155
Spracheinstellungen	150	Window Layouts	98
Statusanzeige	15	Z	
Netzwerk-Verbindung	15	Zertifikate	10
Stromversorgung	15	Zubehör	13
Symbole für Warnhinweise	8	Zugangs-Clients-Einstellungen	87
Symbolleiste	18	Zugangsmethoden	63
Systemeinstellungen	26	Zugriff auf KVM/serielle Switches und Ports	62
Datum und Zeit	26		
Maus	34		
Monitor	32		
Netzwerk	35		
Standort und Wetter	28		
Tastatur	30		
Systemübersicht			
Matrix-System	12		
System ohne Matrix	12		
T			
Targets	63		
Targets öffnen	82		
Tastatur-/Mausmitbenutzung	144		

18 Abbildungsverzeichnis

Abb. 1	Installationsbeispiel mit Draco tera Matrix	12
Abb. 2	Installationsbeispiel mit Draco SIRA Stand-Alone-Units	12
Abb. 3	Frontseite	14
Abb. 4	Rückseite	15
Abb. 5	VESA-Montageplatten	16
Abb. 6	Zu entfernende Schrauben	16
Abb. 7	Anmeldemaske	17
Abb. 8	Hauptbildschirm mit geöffnetem Port Navigator	18
Abb. 9	Hauptmenü	19
Abb. 10	Hauptmenü und User-Station-Konfigurationsseite	20
Abb. 11	Hauptmenü mit Firefox Eintrag	20
Abb. 12	Zwei Arten, die Fensterverwaltung zu öffnen	21
Abb. 13	Beispiel eines gekachelten Layouts	21
Abb. 14	Fensteranordnungs-Optionen über Hauptmenü	22
Abb. 15	Hilfsoptionen über das Hauptmenü	23
Abb. 16	Beenden Menü über das Hauptmenü	25
Abb. 17	Systemeinstellungen über Hauptmenü	26
Abb. 18	Systemeinstellungen - Konfiguration von Datum und Zeit	26
Abb. 19	Systemeinstellungen - Auswahl der Zeitzone	27
Abb. 20	Systemeinstellungen - Zeitanzeige, Kalender und Standort	28
Abb. 21	Systemeinstellungen - Uhreinstellungen - Ort	28
Abb. 22	Systemeinstellungen - Uhreinstellungen - Ort auswählen	28
Abb. 23	Systemeinstellungen - Uhreinstellungen - Wetter	29
Abb. 24	Systemeinstellungen - Uhreinstellungen - Allgemein	29
Abb. 25	Systemeinstellungen - Tastatur-Einstellungen	30
Abb. 26	Systemeinstellungen - Tastatur-Einstellungen - Neue Belegung auswählen	30
Abb. 27	Systemeinstellungen - Tastatur-Einstellungen - Liste von Tastaturherstellern und Modellen	31
Abb. 28	Systemeinstellungen - Tastatur-Einstellungen - Maustasten	31
Abb. 29	Systemeinstellungen - Bildschirmeinstellungen	32
Abb. 30	Systemeinstellungen - Einstellungen für die Maus	34
Abb. 31	Systemeinstellungen - Netzwerkverbindungen - Startmenü	35
Abb. 32	Systemeinstellungen - Netzwerkverbindungen - Verbindung ändern	36
Abb. 33	Systemeinstellungen - Netzwerkverbindungen - Registerkarte IPv4-Einstellungen	37
Abb. 34	Systemeinstellungen - Netzwerkverbindungen - Registerkarte IPv6-Einstellungen	39
Abb. 35	Systemeinstellungen - Netzwerkverbindungen - Registerkarte 802.1X-Sicherheit	41
Abb. 36	Systemeinstellungen - Netzwerkverbindungen - Registerkarte Miscellaneous	43
Abb. 37	Systemeinstellungen - Netzwerkverbindungen	43
Abb. 38	Systemeinstellungen - Netzwerkverbindungen - Bond-Verbindung bearbeiten 1	44
Abb. 39	Systemeinstellungen - Netzwerkverbindungen - Bond-Verbindung bearbeiten 2	44
Abb. 40	Systemeinstellungen - Netzwerkverbindungen - Netzwerkverbindungen mit gebündelter Verbindung	45
Abb. 41	Systemeinstellungen - Netzwerkverbindungen - Dialog zum Hochladen einer VPN-Konfiguration	45
Abb. 42	Systemeinstellungen - Netzwerkverbindungen - Liste der Netzwerkverbindungen	45

Abb. 43	Systemeinstellungen - Netzwerkverbindungen - Konfigurieren der VPN-Verbindung	46
Abb. 44	Symbolleiste mit VPN-Schloss-Symbol	46
Abb. 45	KVM-Client-Fenster	47
Abb. 46	Fenster des seriellen Clients	49
Abb. 47	Settings - Terminal Properties	49
Abb. 48	Settings - Benutzerliste	51
Abb. 49	Power-Benachrichtigungen	52
Abb. 50	Nachricht nach erfolgreichem Stromversorgungsvorgang	52
Abb. 51	Hauptmenü	53
Abb. 52	User-Station-Konfiguration	53
Abb. 53	Konfiguration - Neues SIRA-Gerät anlegen	53
Abb. 54	Konfiguration - Neues SIRA-Gerät anlegen - Nutzer-Zugangsdaten	54
Abb. 55	Konfiguration - SIRA-Geräte-Liste	55
Abb. 56	Konfiguration - SIRA-Geräte - Massenimport-Dialog - Liste der gefundenen CSV-Dateien	57
Abb. 57	Konfiguration - SIRA-Geräte - Massenimport-Dialog - Inhalt der ausgewählten CSV-Datei	58
Abb. 58	Konfiguration - SIRA-Geräte - Meldung nach erfolgreichem Import / Aktualisierung	58
Abb. 59	Konfiguration - SIRA-Geräte - Portliste	59
Abb. 60	Konfiguration - KVM-Ports - Allgemeine Einstellungen	59
Abb. 61	Konfiguration - KVM-Ports - Target-Fenster-Einstellungen	60
Abb. 62	Port-Navigator und geöffnetes Geräte-Panel	62
Abb. 63	Geräte-Panel, ein Port wird benutzt	63
Abb. 64	Konfiguration - Target-Liste	64
Abb. 65	Konfiguration - Targets - Neues Target und Zugang hinzufügen	64
Abb. 66	Konfiguration - Targets - Neues Target mit SSH, RDP oder VNC Zugang hinzufügen	65
Abb. 67	Konfiguration - Targets - Neues Target mit RDP-Zugang hinzugefügt	65
Abb. 68	Konfiguration - Target-Liste	66
Abb. 69	Port-Navigator - Target-Liste	66
Abb. 70	Konfiguration - Targets - Web-Zugang hinzufügen	67
Abb. 71	Konfiguration - Targets - ESXi-Zugang hinzufügen	68
Abb. 72	Konfiguration - Targets - Beispiel für Multi-KVM-Zugang und Monitoranordnung des Targets	69
Abb. 73	Konfiguration - Targets - Multi-KVM-Zugriff hinzufügen	70
Abb. 74	Konfiguration - Target-Liste	71
Abb. 75	Konfiguration - Targets - Allgemeine Einstellungen	72
Abb. 76	Konfiguration - Targets - Target-Fenster-Einstellungen für RDP-Zugang	73
Abb. 77	Konfiguration - Targets - Target-Fenster-Einstellungen für VNC-Zugang	74
Abb. 78	Konfiguration - Targets - SSH-Zugang ändern	75
Abb. 79	Konfiguration - Targets - WEB-Zugang ändern	76
Abb. 80	Konfiguration - Targets - ESXi-Zugang ändern	76
Abb. 81	Port-Navigator	78
Abb. 82	Port-Navigator - Erklärung der Symbole und Farben	80
Abb. 83	Port-Navigator - Geräte-Menü - Port mit Mediensymbolen	81
Abb. 84	Port-Navigator - Geräte-Menü geöffnet	81
Abb. 85	Port-Navigator - Ports des ausgewählten Geräts	82

Abb. 86	Port-Navigator - Target-Menü geöffnet	82
Abb. 87	Port-Navigator - Zugangsmethoden für dieses Target	83
Abb. 88	Port-Scanner-Fenster	84
Abb. 89	Port-Scanner - Scan-Optionen	84
Abb. 90	Port-Scanner - Untermenü der Vorschaubilder	85
Abb. 91	Menü Einstellungen	87
Abb. 92	Einstellungen - Zugangs-Clients-Einstellungen - Video-Target-Fenster-Einstellungen	87
Abb. 93	Einstellungen - Zugangs-Clients-Einstellungen - Konsolenfenster-Einstellungen	89
Abb. 94	Einstellungen - Zugangs-Clients-Einstellungen - Web-Target-Fenster-Einstellungen	89
Abb. 95	Einstellungen - Zugangs-Clients-Einstellungen - Starteinstellungen	90
Abb. 96	Einstellungen - Zugangs-Clients-Einstellungen - Verbindungseinstellungen	90
Abb. 97	Einstellungen - Tastatur-Makros	91
Abb. 98	Einstellungen - Tastatur-Makros - Neues Makro anlegen	91
Abb. 99	Einstellungen - Tastatur-Makros - Liste der Makros	92
Abb. 100	Client-Fenster - Liste der aktiven Makros	93
Abb. 101	Einstellungen - Audioeinstellungen	93
Abb. 102	Einstellungen - Audioeinstellungen bearbeiten	94
Abb. 103	Einstellungen - Hotkeys und Gesten - Funktionen der User Station	95
Abb. 104	Einstellungen - Hotkeys und Gesten - Fensterverwaltung	95
Abb. 105	Einstellungen - Hotkeys und Gesten - KVM Client Hotkeys	96
Abb. 106	Einstellungen - Hotkeys und Gesten - Hotkeys für Ports, Target-Zugang und Fensteranordnungen ..	97
Abb. 107	Einstellungen - Hotkeys und Gesten - Hotkeys und Gesten bearbeiten	97
Abb. 108	Einstellungen - Hotkeys und Gesten	98
Abb. 109	Einstellungen - Fensteranordnungen (Layouts)	99
Abb. 110	Einstellungen - Fensteranordnungen - Layout ausgewählt	99
Abb. 111	Nachricht über Verzögerungszeit	100
Abb. 112	Einstellungen - Port-Scanner-Einstellungen	100
Abb. 113	Einstellungen - Port-Scanner-Einstellungen - Intervalle und Pausen einstellen	101
Abb. 114	Einstellungen - Port-Scanner-Einstellungen - Schnappschuss-Aufnahmen aktivieren	101
Abb. 115	Einstellungen - Port-Scanner-Einstellungen - Weitere Einstellmöglichkeiten	101
Abb. 116	Einstellungen - Bildschirmfoto-Einstellungen	102
Abb. 117	Einstellungen - Bildschirmfoto-Einstellungen - Ausgewähltes Speichermedium	102
Abb. 118	Einstellungen - Bildschirmfoto-Einstellungen - Als Standardspeicher festlegen	102
Abb. 119	Einstellungen - Hotkeys und Gesten - Hotkeys für Bildschirmfotos (Screenshots)	103
Abb. 120	Bestätigungsmeldung eines Bildschirmfotos (Screenshot)	103
Abb. 121	Einstellungen - Passwort ändern	104
Abb. 122	Untermenü Administration	105
Abb. 123	Administration - Nutzer - Nutzerliste	105
Abb. 124	Administration - Nutzer - Neuer Nutzer	106
Abb. 125	Administration - Nutzer - Neuen Nutzer erstellt	107
Abb. 126	Administration - Nutzer - Liste der Nutzer	107
Abb. 127	Administration - Nutzer - Details eines Nutzers	108
Abb. 128	Administration - Users - Nutzerdaten ändern	108

Abb. 129	Administration - Gruppen	109
Abb. 130	Administration - Gruppen - Neue Gruppe erstellen	110
Abb. 131	Administration - Gruppe - Liste der Nutzergruppen	112
Abb. 132	Administration - Gruppe - Details einer Nutzergruppe	112
Abb. 133	Administration - Gruppen - Mögliche Warnmeldung bei Löschen von Gruppen	113
Abb. 134	Administration - Automatische Anmeldungs-Einstellungen	114
Abb. 135	Administration - Automatische Anmeldungs-Einstellungen - Einstellungen bearbeiten	115
Abb. 136	Administration - LDAP-Server	117
Abb. 137	Administration - LDAP Servers - Allgemeine Einstellungen	117
Abb. 138	Administration - LDAP-Server - Verbindungseinstellungen	118
Abb. 139	Administration - LDAP-Server - Autorisierungseinstellungen	119
Abb. 140	Administration - LDAP-Server - Gruppeneinstellungen	120
Abb. 141	Administration - LDAP-Servers - Verbindungstest	121
Abb. 142	Administration - LDAP-Server - Liste konfigurierter LDAP-Server	122
Abb. 143	Administration - LDAP-Servers - LAPD-Authentifizierung aktiviert	123
Abb. 144	Administration - LDAP-Servers - Suchmenü	123
Abb. 145	Administration - LDAP-Server - LAPD-Authentifizierung aktiviert	125
Abb. 146	Anmelden mit LDAP	125
Abb. 147	Administration - Vertrauenswürdige Zertifikate	126
Abb. 148	Administration - Server-Zertifikat	127
Abb. 149	Administration - Server-Zertifikate - Details des aktiven Zertifikats	127
Abb. 150	Administration - Server-Zertifikat - Privaten Schlüssel und Zertifikat importieren	128
Abb. 151	Administration - Server-Zertifikat - Installieren eines importierten Zertifikats	128
Abb. 152	Administration - Server-Zertifikate - Button Erstelle Selbst Signiertes	129
Abb. 153	Administration - Server-Zertifikate - Erstellen eines selbstsignierten Zertifikats	129
Abb. 154	Administration - Sicherheitseinstellungen	130
Abb. 155	Administration - Sicherheitseinstellungen - Bearbeiten: FIPS-Modus	130
Abb. 156	Administration - Sicherheitseinstellungen - Bearbeiten: Zertifikateinstellungen	131
Abb. 157	Konfiguration- Targets - Bearbeitungsseite SSH-Zugang - SSH-Host-Schlüssel	132
Abb. 158	Konfiguration- Targets - Bearbeitungsseite RDP-Zugang - RDP-Zertifikat	132
Abb. 159	Administration - Sicherheitseinstellungen - Bearbeitungsseite - Passworteinstellungen	133
Abb. 160	Administration - Sicherheitseinstellungen - Bearbeitungsseite - Nutzersperren	134
Abb. 161	Administration - Nutzer - Nutzerliste	134
Abb. 162	Administration - Sicherheitseinstellungen - Links und Weiterleitungen	135
Abb. 163	Anmeldemaske mit Nutzungsbedingungen	135
Abb. 164	Administration - Sicherheitseinstellungen - Nutzungsbedingungen	136
Abb. 165	Administration - Anzeigeeinstellungen	136
Abb. 166	Administration - Anzeigeeinstellungen - Bearbeitungsseite	137
Abb. 167	Bildschirm gesperrt	137
Abb. 168	Administration - Anpassungen	139
Abb. 169	Administration - Anpassungen - Desktop-Hintergrund ändern	139
Abb. 170	Administration - Anpassungen - Desktop-Hintergrund geändert	140
Abb. 171	Administration - Anpassungen - Anmeldebildschirm geändert	140

Abb. 172	Administration - Fernsteuerungs-Einstellungen	141
Abb. 173	Administration - Fernsteuerungs-Einstellungen - Fernsteuerung via Web-Browser einstellen	142
Abb. 174	Administration - Fernsteuerungs-Einstellungen - Fernsteuerung via API einstellen	143
Abb. 175	Administration - Tastatur-/Mausmitbenutzung - Beispiel	144
Abb. 176	Administration - Tastatur-/Mausmitbenutzung - Anordnung der Bildschirme	145
Abb. 177	Administration - Tastatur-/Mausmitbenutzung - Startmenü	145
Abb. 178	Administration - Tastatur-/Mausmitbenutzung - Client konfigurieren	145
Abb. 179	Administration - Tastatur-/Mausmitbenutzung - Controller konfigurieren	146
Abb. 180	Administration - Tastatur-/Mausmitbenutzung - Überblick der Konfiguration	147
Abb. 181	Administration - Netzwerkspeicher	148
Abb. 182	Administration - Netzwerkspeicher - Neuen Netzwerkspeicher anlegen	149
Abb. 183	Administration - Netzwerkspeicher - Neuer Netzwerkspeicher angelegt	149
Abb. 184	Administration - Netzwerkspeicher - Liste der verfügbaren Netzwerkspeicher	150
Abb. 185	Administration - Spracheinstellungen	151
Abb. 186	Administration - Spracheinstellungen - Sprache ändern	151
Abb. 187	Administration - Spracheinstellungen - Sprache geändert	151
Abb. 188	Wartung - Eignisprotokoll	152
Abb. 189	Wartung - Ereignisprotokoll - Archivieren	153
Abb. 190	Wartung - Ereignisprotokoll - Archivierung beendet	154
Abb. 191	Wartung - Sicherung und Wiederherstellung	155
Abb. 192	Wartung - Sicherung und Wiederherstellung - Sicherungsdatei erstellt	156
Abb. 193	Wartung - Sicherung und Wiederherstellung - Details einer Sicherungsdatei	156
Abb. 194	Wartung - Sicherung und Wiederherstellung - Import einer Sicherungsdatei	157
Abb. 195	Wartung - Sicherung und Wiederherstellung	158
Abb. 196	Wartung - Auf Werkseinstellungen zurücksetzen	159
Abb. 197	Wartung - Softwareaktualisierung	160
Abb. 198	Wartung - Kundendienst	161
Abb. 199	Wartung - Kundendiensteinstellungen bearbeiten	162
Abb. 200	Wartung - Diagnostische Protokolldatei - Exportieren	163
Abb. 201	Wartung - Diagnostische Protokolldatei - Export erfolgreich beendet	163
Abb. 202	Wartung - Netzwerkdiagnose	164
Abb. 203	Wartung - Netzwerkdiagnose - Ping-Ergebnisse	164
Abb. 204	Wartung - Netzwerkdiagnose - TCP-Verbindungen und TCP/UDP-Listen-Sockets	165

19 Änderungsprotokoll

Diese Tabelle bietet einen Überblick über die wichtigsten verfügbaren Änderungen, wie beispielsweise neue Funktionen, geänderte Konfigurationen oder Bedienungsabläufe.

Ausgabe	Datum	Firmware-Version	Kapitel	Neue Funktionen/Änderungen
Rev. 0	07.10.2026	5.1.0.5.80		Erstausgabe