Aperio GT 450 DX

IT-Manager- und Labor-Administratorhandbuch

CE

MAN-0483-de, Revision B | Mai 2022

Aperio GT 450 DX IT-Manager- und Labor-Administratorhandbuch

Dieses Dokument gilt für den Aperio GT 450 DX-Controller, die Aperio GT 450 DX-Konsole und die Aperio GT 450 DX SAM DX-Versionen 1.1 und höher.

Hinweis zum Urheberrecht

Kundenressourcen

- Besuchen Sie für die neuesten Informationen zu den Aperio-Produkten und -Dienstleistungen von Leica Biosystems bitte www.LeicaBiosystems.com/Aperio.

Kontaktinformationen – Leica Biosystems Imaging, Inc.

Hauptsitz	Kundenbetreuung	Allgemeine Angaben
Leica Biosystems Imaging, Inc. 1360 Park Center Drive Vista, CA 92081 USA Tel.: +1 (866) 478-4111 (gebührenfrei) Internationale Direktwahlnummer: +1 (760) 539-1100	Bei Fragen oder Serviceanfragen kontaktieren Sie Ihren örtlichen Supportvertreter. https://www.leicabiosystems.com/service-support/technical-support/	Tel. USA/Kanada: +1 (866) 478-4111 (gebührenfrei) Internationale Direktwahlnummer: +1 (760) 539-1100 E-Mail: ePathology@LeicaBiosystems.com

Bevollmächtigter Vertreter der Europäischen Union	Verantwortliche Person für Großbritannien
EC REP CEpartner4U, Esdoornlaan 13 3951 DB Maarn Niederlande	Leica Microsystems UK Larch House, Woodlands Business Park Milton Keynes, England, Großbritannien, MK14 6FG

Importeur	
Leica Biosystems Eisfeld GmbH Heidelberger Straße 17-19 69226 Nussloch, Deutschland	Leica Microsystems UK Larch House, Woodlands Business Park Milton Keynes, England, Großbritannien, MK14 6FG

IVD CE UKCA

UDI 00815477020297, 00815477020389

REF 23GT450DXIVD, 23SAMSWDXIVD

Inhalt

Hinweise

Revisionsprotokoll

Rev.	Veröffentlicht	Betroffene Abschnitte	Detail
B	Mai 2022	Alle	Mehrere Tippfehler korrigiert.
A	April 2022	Alle	Neue Version für das Produkt Aperio GT 450 DX. Basiert auf dem vorhandenen *Aperio GT 450 DX IT-Manager- und Labor-Administratorhandbuch*, MAN-0459, Revision B. Nicht übersetzt.

Vorsichtshinweise und Hinweise

- **Berichterstattung von schwerwiegenden Ereignissen** – Alle schwerwiegenden Ereignisse, die im Zusammenhang mit dem Aperio GT 450 DX auftreten, müssen dem Hersteller und der zuständigen Behörde in dem Mitgliedsstaat, in dem der Benutzer und/oder der Patient ansässig ist, gemeldet werden.
- **Spezifikationen und Leistung** – Für die Gerätespezifikationen und Leistungsmerkmale ziehen Sie das Dokument *Aperio GT 450 DX Scanner Spezifikationen* zurate.
- **Installation** – Das Aperio GT 450 DX muss von einem geschulten Vertreter von Leica Biosystems Technische Dienstleistungen installiert werden.
- **Reparatur** – Reparaturen müssen von einem geschulten Vertreter von Leica Biosystems Technische Dienstleistungen durchgeführt werden. Bitten Sie nach Abschluss von Reparaturarbeiten den Techniker von Leica Biosystems, eine Betriebsprüfung durchzuführen, um zu bestätigen, dass sich das Produkt in einem guten Betriebszustand befindet.
- **Zubehör** – Für Informationen zur Verwendung des Aperio GT 450 DX mit Drittzubehör wie einem Laborinformationssystems (LIS), das nicht von Leica Biosystems zur Verfügung gestellt wird, kontaktieren Sie Ihren Vertreter von Leica Biosystems Technische Dienstleistungen.
- **Qualitätskontrolle** – Für Informationen zu Bildqualitätsprüfungen siehe das *Aperio GT 450 DX Benutzerhandbuch*.
- **Wartung und Fehlerbehebung** – Für Informationen zur Wartung siehe das *Aperio GT 450 DX Benutzerhandbuch*.
- **Cybersicherheit** – Beachten Sie, dass Workstations und Server anfällig für Malware, Viren, Datenkorruption und Datenschutzlücken sind. Arbeiten Sie gemeinsam mit den IT-Administratoren am Schutz Ihrer Workstations und befolgen Sie die Kennwort- und Sicherheitsrichtlinien Ihrer Einrichtung.

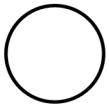
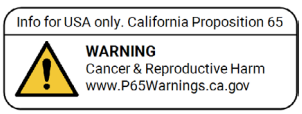
  Aperio-Empfehlungen zum Schutz Ihres SAM DX-Servers finden Sie in *„Kapitel 6: Cybersicherheits- und Netzwerkrichtlinien“ auf Seite 37*.

  Wenn eine mutmaßliche Schwachstelle in der Aperio GT 450 DX-Cybersicherheit oder ein Ereignis festgestellt wird, kontaktieren Sie Leica Biosystems Technische Dienstleistungen bezüglich Unterstützung.
- **Schulungen** – Dieses Handbuch ist kein Ersatz für eine ausführliche Bedienerschulung durch Leica Biosystems oder weitere eingehendere Einweisungen.
- **Sicherheit** – Der Sicherheitsschutz ist möglicherweise beeinträchtigt, wenn das Gerät auf nicht vom Hersteller vorgeschriebene Art benutzt wird.

Symbole

Die folgenden Symbole erscheinen auf dem Etikett Ihres Produkts oder in dieser Benutzeranleitung:

Symbol	Verordnung/ Norm	Beschreibung
	ISO 15223-1 – 5.4.3	Gebrauchsanweisung beachten.
	ISO 15223-1 – 5.1.1	Hersteller
	ISO 15223-1 – 5.1.3	Herstellungsdatum
	ISO 15223-1 – 5.1.2	Bevollmächtigter Vertreter der Europäischen Union
	ISO 15223-1 – 5.1.8	Importeur
	AS/NZS 4417.1	Das Gerät entspricht den Anforderungen der Australian Communications Media Authority (ACMA) (Sicherheit und EMV) für Australien und Neuseeland.
	ISO 15223-1 – 5.1.7	Seriennummer
	ISO 15223-1 – 5.5.1	In-vitro-Diagnostikum.
	ISO 15223-1 – 5.1.6	Katalog-Nummer
	ISO 15223-1 – 5.7.10	Eindeutiger Produktidentifikator
	EU 2017/746 Artikel 18	Das Gerät verfügt über das CE-Zeichen (Conformité Europëenne) und erfüllt die Anforderungen der EU-Verordnung 2017/746.
	Verordnungen über Medizinprodukte 2002	Das Gerät entspricht den Anforderungen der britischen Konformitätsbewertung.
	ISO 15223-1 – 5.4.4	Vorsicht
	SO 7010 – W001	Allgemeiner Warnhinweis

Symbol	Verordnung/ Norm	Beschreibung
	IEC 61010-1	TÜV Product Services haben bescheinigt, dass die aufgelisteten Produkte sowohl den US-amerikanischen als auch den kanadischen Sicherheitsanforderungen entsprechen.
	IEC 60417-5031	Dieses Gerät ist nur für Gleichstrom geeignet.
	IEC 60417-5007	Ein. Weist auf die Verbindung zum Stromnetz hin, zumindest bei Netzschaltern oder ihren Positionen und in allen Fällen, in denen die Sicherheit eine Rolle spielt.
	IEC 60417-5008	Aus. Weist auf die Trennung vom Stromnetz hin, zumindest bei Netzschaltern und in allen Fällen, in denen die Sicherheit eine Rolle spielt.
	ISO 15523-1 5.7.3	Temperaturgrenze
	ISO 15223-1 5.3.8	Begrenzung der Feuchtigkeit
	2012/19/EU	Das Gerät fällt unter die Richtlinie 2012/19/EU (WEEE-Richtlinie) für Elektro- und Elektronik-Altgeräte und muss unter besonderen Bedingungen entsorgt werden.
	Elektronischer Industriestandard SJ/T11364 der Volksrepublik China	Das Gerät enthält bestimmte toxische oder gefährliche Elemente und kann während seiner umweltsicheren Verwendungsdauer verwendet werden. Die Zahl in der Mitte des Logos gibt die Verwendungsdauer (in Jahren) an, in der das Produkt umweltsicher verwendet werden kann. Der äußere Kreis weist darauf hin, dass dieses Produkt recycelt werden kann.
	IEC 60825-1	Das Gerät ist ein Laserprodukt der Klasse 1, das den internationalen Normen und den US-Anforderungen entspricht.
	CA Proposition 65	Dieses Produkt kann Sie Chemikalien aussetzen, die dem Staat Kalifornien als krebserregend und fortpflanzungsschädigend bekannt sind. Besuchen Sie für weitere Informationen https://www.P65Warnings.ca.gov.
	N/A	Das Gerät wird in den USA aus US-amerikanischen und ausländischen Komponenten hergestellt.

Kundendienst-Kontakte

Bitte wenden Sie sich für technische Unterstützung an die Niederlassung Ihres Landes.

Australien:
96 Ricketts Road
Mount Waverly, VIC 3149
AUSTRALIEN
Tel.: 1800 625 286 (gebührenfrei)
Von 8:30 Uhr bis 17:00 Uhr, Montag-Freitag, AEST
E-Mail: lbs-anz-service@leicabiosystems.com

Österreich:
Leica Biosystems Nussloch GmbH
Technisches Kundendienstzentrum
Heidelberger Straße 17
Nussloch 69226
DEUTSCHLAND
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +43 1 486 80 50 50
E-Mail: support.at@leicabiosystems.com

Belgien:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +32 2 790 98 50
E-Mail: support.be@leicabiosystems.com

Kanada:
Tel.: +1 844 534 2262 (gebührenfrei)
Internationale Direktwahlnummer: +1 (760) 539-1150
E-Mail TechServices@leicabiosystems.com

China:
17F, SML Center No. 610 Xu Jia Hui Road, Huangpu District
Shanghai, PRC PC:200025
CHINA
Tel.: +86 4008208932
Fax +86 (21) 6384-1389
E-Mail: service.cn@leica-microsystems.com
Remote-Support-E-Mail: tac.cn@leica-microsystems.com

Dänemark:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +45 44 54 01 01
E-Mail: support.dk@leicabiosystems.com

Deutschland:
Leica Biosystems Nussloch GmbH
Technisches Kundendienstzentrum
Heidelberger Straße 17
Nussloch 69226
DEUTSCHLAND
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +49 (6441) 29-4555
E-Mail: support.de@leicabiosystems.com

Irland:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +44 (1908) 577-650
E-Mail: support.ie@leicabiosystems.com

Spanien:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +34 (902) 119-094
E-Mail: support.spain@leicabiosystems.com

Frankreich:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +33 (811) 000-664
E-Mail: support.fr@leicabiosystems.com

Italien:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +39 (0257) 486-509
E-Mail: support.italy@leicabiosystems.com

Japan:
1-29-9 Takadanobaba, Shinjuku-ku
Tokio 169-0075
JAPAN

Niederlande:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +31 70 413 21 00
E-Mail: support.nl@leicabiosystems.com

Neuseeland:
96 Ricketts Road
Mount Waverly, VIC 3149
AUSTRALIEN
Tel.: 0800 400 589 (gebührenfrei)
Von 8:30 Uhr bis 17:00 Uhr, Montag-Freitag, AEST
E-Mail: lbs-anz-service@leicabiosystems.com

Portugal:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +35 1 21 388 9112
E-Mail: support.pt@leicabiosystems.com

Russische Föderation
BioLine LLC
Pinsky lane 3 letter A
St. Petersburg 197101
RUSSISCHE FÖDERATION
Tel.: 8-800-555-49-40 (gebührenfrei)
Landesweite Telefonnummer: +7 812 320 49 49
E-Mail: main@bioline.ru

Schweden:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +46 8 625 45 45
E-Mail: support.se@leicabiosystems.com

Schweiz:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +41 (71) 726-3434
E-Mail: support.ch@leicabiosystems.com

Großbritannien:
Tel.: 0080052700527 (gebührenfrei)
Landesweite Telefonnummer: +44 (1908) 577-650
E-Mail: support.uk@leicabiosystems.com

USA:
Tel.: +1 844 534 2262 (gebührenfrei)
Internationale Direktwahlnummer: +1 (760) 539-1150
E-Mail TechServices@leicabiosystems.com

1 Einleitung

Dieses Kapitel stellt den Scanner Administration Manager DX (SAM DX) für den Einsatz mit einem oder mehreren Aperio GT 450 DX Scannern vor.

Der Aperio GT 450 DX ist ein Hellfeld-Whole-Slide-Hochleistungsscanner für Objektträger, der das kontinuierliche Laden mit einer Kapazität von 450 Objektträgern in 15 Racks, priorisiertes Rack-Scannen, automatische Bildqualitätsprüfungen und eine Scangeschwindigkeit von ca. 32 Sekunden bei einer 40-fachen Scanvergrößerung für einen Bereich von 15 mm x 15 mm unterstützt. Der Aperio GT 450 DX wurde dafür entwickelt, sich in Ihre Netzwerkumgebung einzufügen und die bestmögliche Sicherheit und Leistung bereitzustellen.

Der Aperio GT 450 DX ist zur Verwendung durch geschulte Histologietechniker in der klinischen Pathologie vorgesehen, während die Aperio GT 450 SAM DX-Software zur Verwendung durch IT-Fachleute und Laboradministratoren bestimmt ist.

Das Aperio GT 450 DX ist für den Einsatz in klinischen Pathologielaboren mit mittlerem bis hohem Volumen vorgesehen, die Krankenhäuser, Referenzlabore oder andere klinischen Einrichtungen mit Pathologieleistungen unterstützen.

Stellen Sie sicher, dass entsprechende gute Laborpraktiken bzw. andere, von Ihrer Einrichtung geforderten Vorschriften und Verfahren zur Präparation, Bearbeitung, Lagerung und Entsorgung der Objektträger eingehalten werden. Verwenden Sie dieses Gerät nur für diesen Zweck und nur in der in dem *Aperio GT 450 DX Benutzerhandbuch* beschriebenen Weise.

Komponente	Beschreibung
Scanner Administration Manager DX (SAM DX)-Server	Der SAM DX-Server stellt eine Verbindung zu mehreren Aperio GT 450 DX-Scannern her und führt die SAM DX-Client-Anwendungssoftware aus.
Scanner Administration Manager DX (SAM DX)-Client-Anwendungssoftware	Die SAM DX-Client-Anwendungssoftware ermöglicht die IT-Integration, PIN-Konfiguration und den Dienstzugriff auf mehrere Scanner von einem einzelnen Client-Desktop-Computer für IT-Fachleute.
Workstation, Monitor und Tastatur	Für die Verwendung von SAM DX zur Verwaltung der GT 450 DX-Scanner sind eine Workstation, ein Monitor und eine Tastatur erforderlich, die an Ihr Local Area Network (LAN) angeschlossen sind und Zugriff auf den SAM DX-Server haben.

Der Aperio GT 450 DX enthält den Scanner Administration Manager DX (SAM DX), der die IT-Integration und den Dienstzugriff auf bis zu 4 Scanner von einem einzelnen Client-Desktop-Computer aus ermöglicht. SAM DX ermöglicht die Einrichtung, Konfiguration und Überwachung jedes Scanners. SAM DX wird auf einem Server installiert, der sich in demselben Netzwerk wie der oder die Scanner und andere Komponenten für die Bildverwaltung befindet.

Funktionen von SAM DX sind:

- Webbasierte Benutzeroberfläche, kompatibel mit den meisten aktuellen Browsern, um in Ihrer ganzen Einrichtung den Zugriff zu ermöglichen.

- Rollenbasierter Zugriff für Benutzer. Eine Bediener-Rolle ermöglicht es Benutzern, Konfigurationseinstellungen anzuzeigen, während eine Administrator-Rolle dem Benutzer das Ändern der Einstellungen erlaubt.
- Scanner-spezifische Konfigurationseinstellungen für Benutzerzugriff-PINs und Zeitüberschreitungen. Der Zugriff auf jeden Scanner im System kann mit verschiedenen Zugriffs-PINs konfiguriert werden.
- Zentrale Anzeige der Statistiken und Ereignisprotokolle. In der SAM DX-Benutzeroberfläche können Informationen über jeden Scanner im System angezeigt, überprüft und verglichen werden.
- Unterstützung für mehrere Scanner mit zentraler Konfiguration und Überwachung.
- Sofortige Anzeige des Scanner-Status. Die Startseite zeigt an, welche Scanner online sind und welche nicht.
- Dienste für die Verarbeitung von Protokolldaten und Ereignissen via Mirth Connect an eine Datenbank auf dem Dateisystem.

Über dieses Handbuch

Dieses Handbuch richtet sich an Labor-Administratoren, IT-Manager und alle anderen, die für die Verwaltung des Aperio GT 450 DX in ihrem Einrichtungsnetzwerk verantwortlich sind. Für allgemeine Informationen über die Verwendung des Scanners siehe *Aperio GT 450 DX Benutzerhandbuch*.

Das nächste Kapitel dieses Handbuchs erklärt die Aperio GT DX 450-Netzwerkarchitektur und zeigt die Datenströme von einer Komponente des Systems zur anderen.

Die folgenden Kapitel erklären den Einsatz der Anwendung Scanner Administration Manager DX (SAM DX) zur Konfiguration des oder der Aperio GT 450 DX Scanner, einschließlich des Hinzufügens von Benutzerkonten zu SAM DX und der Konfiguration von Zugriffs-PINs für jeden Scanner. Aufgaben, die nur von Leica-Kundendienstmitarbeitern ausgeführt werden können, sind nicht in diesem Handbuch enthalten.

Verwenden Sie die folgende Tabelle für Informationen über bestimmte Aufgaben.

Aufgabe	Siehe
Erfahren Sie, wie sich GT 450 DX-Scanner und der Scanner Administration Manager DX (SAM DX)-Server in Ihr Netzwerk einfügen.	*„Kapitel 2: Aperio GT 450 DX Netzwerkarchitektur“ auf Seite 15*
Erfahren Sie, wie die Daten zwischen dem Aperio GT 450 DX, dem SAM DX-Server und optionalen Bild- und Datenverwaltungsservern übertragen werden.	*„Empfohlene Netzwerkkonfiguration für den Aperio GT 450 DX“ auf Seite 17*
Melden Sie sich bei der Scanner Administration Manager DX (SAM DX)-Client-Anwendungssoftware an.	*„Anmeldung bei SAM DX“ auf Seite 12*
Ändern Sie Konfigurationseinstellungen für DICOM oder die DSR-Kommunikation mit dem SAM DX-Server und Scanner.	*„Scanner-Configuration Settings (Konfigurationseinstellungen)“ auf Seite 23*
Zeigen Sie Informationen über einen Scanner im System an.	*„Kapitel 3: Konfiguration des Aperio GT 450 DX“ auf Seite 19*
Überprüfen Sie, ob ein Scanner online ist.	*„Die SAM DX-Benutzeroberfläche“ auf Seite 13*
Zeigen Sie die Seriennummer, Softwareversion oder Firmwareversion eines Scanners im System an.	*„Scanner System Information: Info Page (Scanner-Systeminformationen: Seite „Info“)“ auf Seite 21*

Aufgabe	Siehe
Überprüfen Sie Scanner-Statistiken und -Verlauf.	*„Anzeige von Scanner-Statistiken“ auf Seite 31*
Prüfen Sie fortgeschrittene Konfigurationseinstellungen wie z. B. Kameraeinstellungen.	*„Anzeige von Scanner-Informationen und -Einstellungen“ auf Seite 30*
Fügen Sie einen neuen Benutzer für den Scanner Administration Manager DX (SAM DX) hinzu.	*„Einen Benutzer hinzufügen“ auf Seite 34*
Löschen Sie ein Benutzerkonto aus SAM DX.	*„Einen Benutzer löschen“ auf Seite 35*
Ändern Sie das Kennwort eines Benutzers.	*„Ändern Ihres Kennworts“ auf Seite 36*
Entsperren Sie ein gesperrtes Benutzerkonto.	*„Ein Benutzerkonto entsperren“ auf Seite 35*
Diagnostizieren Sie ein Problem durch Überprüfung der Ereignis- und Fehlerprotokolle.	*„Arbeiten mit dem Ereignisprotokoll“ auf Seite 32*
Suchen Sie nach Updates für die Software.	*„Anzeige von Scanner-Informationen und -Einstellungen“ auf Seite 30*
Prüfen Sie Cybersecurity- und Netzwerkempfehlungen für Aperio GT 450 DX.	*„Kapitel 6: Cybersicherheits- und Netzwerkrichtlinien“ auf Seite 37*

Verwandte Dokumente

Über den Touchscreen des Aperio GT 450 DX verfügbare Videos enthalten Anweisungen für grundlegende Arbeiten wie das Laden und Entladen von Racks.

Zusätzliche Informationen über den Betrieb des Aperio GT 450 DX finden Sie in den folgenden Dokumenten:

- *Kurzanleitung für Aperio GT 450 DX* – Erste Schritte mit dem Aperio GT 450 DX.
- *Aperio GT 450 DX Benutzerhandbuch* – Erfahren Sie mehr über den Aperio GT 450 DX.
- *Aperio GT 450 DX Spezifikationen* – Detaillierte Spezifikationen des Aperio GT 450 DX.

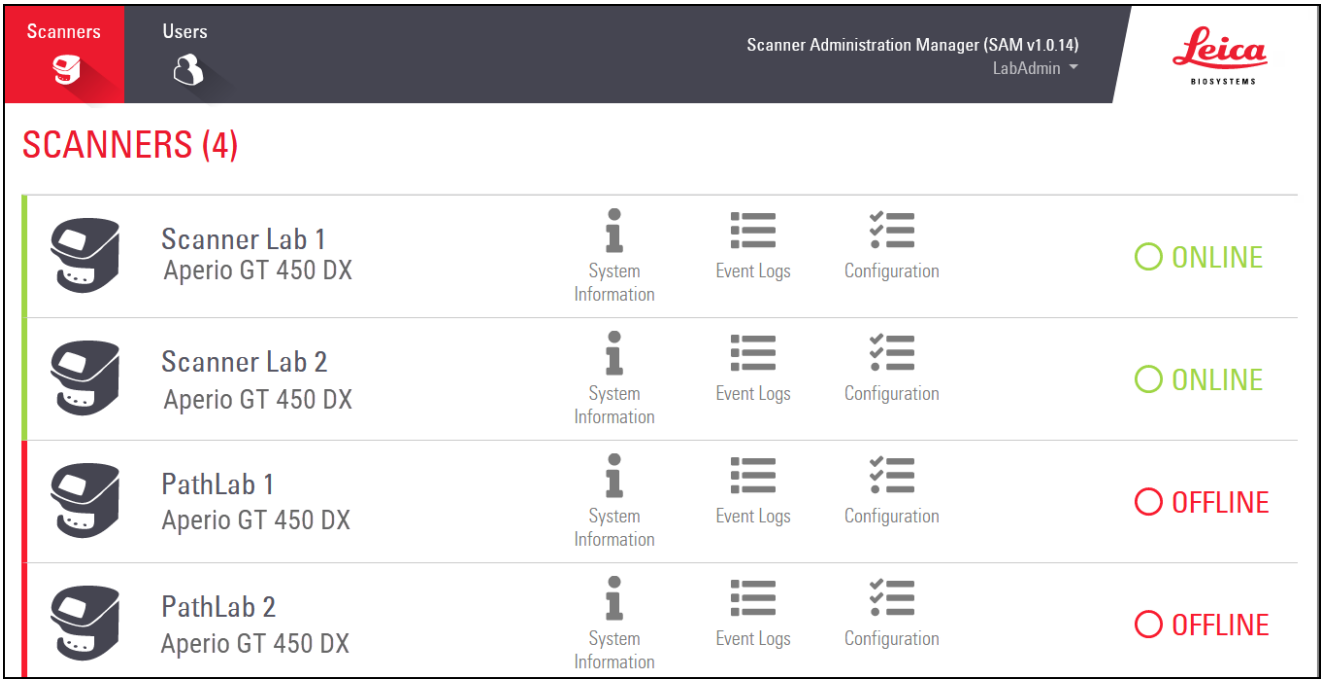
Anmeldung bei SAM DX

Wenn Aperio GT 450 DX installiert und konfiguriert wurde, ist der nächste Schritt der Einsatz des Scanner Administration Manager DX (SAM DX) für die Verwaltung der Aperio GT 450 DX-Scanner und -Benutzer.

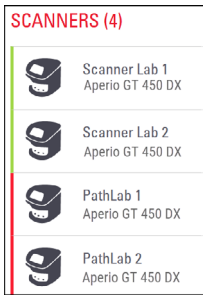
1. Öffnen Sie einen Internet-Browser und geben Sie die Adresse des SAM DX-Servers ein. (Der Leica-Kundendienstmitarbeiter übergibt diese Adresse dem IT-Beauftragten der Einrichtung, in der das System installiert ist. Kontaktieren Sie Ihr IT-Personal, falls Sie diese Adresse nicht kennen.)
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Falls Sie sich zum ersten Mal anmelden, verwenden Sie die von Ihrem Systemadministrator oder dem Kundendienstmitarbeiter von Leica Biosystems mitgeteilten Anmeldedaten.
3. Klicken Sie auf **Log In** (Anmelden).

Die SAM DX-Benutzeroberfläche

Unten sehen Sie die SAM DX-Startseite mit der Scanner-Liste. Beachten Sie, dass Benutzer mit der Rolle „Operator“ (Bediener) die Konfigurationssymbole nicht sehen können.



Im Folgenden werden die vier grundlegenden Bereiche der Seite beschrieben.

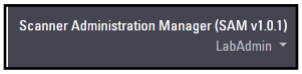


Scanner-Liste

Diese Liste zeigt alle Scanner im System an, einschließlich des benutzerdefinierten oder „benutzerfreundlichen“ Namens und des Scanner-Modells. Benutzer mit der Rolle „Lab Admin“ (Labor-Administrator) können auf einen Scanner-Namen in diesem Bereich klicken, um die Optionen zum Bearbeiten des Scanners anzuzeigen.

Scanner-Statusbereich

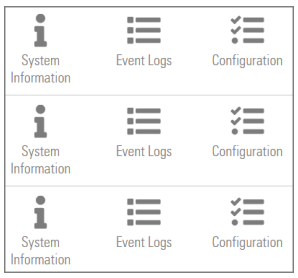
In diesem Bereich sehen Sie den Status jedes Scanners.



Benutzeranmeldung

Hier wird der Benutzername des aktuellen SAM DX-Benutzers angezeigt.

Klicken Sie auf Ihren Anmeldenamen, um Links für das Ändern Ihres Kennworts und die Abmeldung einzublenden.



Befehlsbereich

Hier befinden sich die Symbole für den Zugriff auf die Bereiche „System Information“ (Systeminformationen), „Event Log“ (Ereignisprotokoll) und „Configuration“ (Konfiguration).

Beachten Sie, dass das Konfigurationssymbol nur für Benutzer mit der Rolle „Lab Admin“ (Labor-Administrator) sichtbar ist.

2 Aperio GT 450 DX Netzwerkarchitektur

Dieses Kapitel enthält eine grundlegende Architekturübersicht davon, wie der Aperio GT 450 DX und der SAM DX-Server sich in Ihr Netzwerk einfügen.

Ein Ausfall des IT-Netzwerks kann zu einer Verzögerung der Diagnose/Prognose führen, bis das Netzwerk wiederhergestellt ist.

Aperio GT 450 DX Architektur

Der Aperio GT 450 DX wurde mit Blick auf IT-Benutzerfreundlichkeit und -Sicherheit entwickelt. Er ist im Auslieferungszustand vorbereitet für die Integration mit Ihrem Bild- und Datenverwaltungssystem (IDMS), einem LIS und anderen Netzwerksystemen.

Der Aperio GT 450 DX enthält einen Aperio GT 450 DX, den Aperio Scanner Administration Manager DX (SAM DX)-Server, Kabel und Stecker. Jede Instanz des SAM DX-Servers kann vier Aperio GT 450 DX-Scanner betreiben und in Ihrem Netzwerk können mehrere SAM DX-Server integriert werden.

Die SAM DX-Client-Anwendungssoftware befindet sich auf dem SAM DX-Server und enthält Folgendes:

- SAM DX-Software für die Konfiguration des Scanners
- Webbasierte Benutzeroberfläche für die Scanner-Administration und Konfiguration
- Protokoll- und Nachrichtendienste für Ereignisse und Fehler
- DICOM-Server für die Konvertierung von DICOM-Bilddateien in SVS und ihre Übertragung an das Bildspeichersystem

Unterstützte Bildtypen

Der Aperio GT 450 DX erzeugt SVS-Dateien oder DICOM-Bilder. Das Bildformat .SVS ist das Standardformat.

Sie können die DICOM-Bildausgabe erst aktivieren, wenn Ihre IT-Umgebung die in der *Aperio DICOM-Konformitätserklärung* beschriebenen Anforderungen erfüllt. Außerdem muss sich ein Vertreter von Leica Biosystems Technische Dienstleistungen als Leica Admin bei SAM DX anmelden und die optionalen Funktionen für den Scanner aktivieren, den Sie für DICOM konfigurieren möchten. Näheres dazu unter *„Aktivieren der DICOM-Bildausgabe“ auf Seite 28*.

Allgemeine Angaben

Es gelten die folgenden Richtlinien:

- Die Netzwerkfreigabe, auf der Bilder gespeichert werden (DSR), kann sich auf demselben Server wie das IDMS oder an einem anderen Ort im lokalen Netzwerk befinden.
- Die Meldungsdienste enthalten eine Instanz von Mirth Connect und die Bereitstellung verschiedener Kanäle für die Transformation und Übermittlung von Scanner-Nachrichten (Scan-Ereignisse und -Protokolle).

Vor der Installation der Aperio GT 450 DX-Scanner, der SAM DX-Client-Anwendungssoftware und des SAM DX-Servers bestimmt der Techniker von Leica Biosystems die beste Architektur für die Installation, basierend auf Projektnutzung, derzeitiger Netzwerkkonfiguration und anderen Faktoren. Dies schließt die Entscheidung mit ein, welche Komponenten auf welchem physischen Server im Netzwerk installiert werden. Die verschiedenen Komponenten und Dienste können auf verschiedenen Servern oder gemeinsam auf einem einzigen Server installiert werden.

Anforderungen an die Netzwerkbandbreite

Für die Verbindung zwischen dem Aperio GT 450 DX und dem SAM DX-Server beträgt die benötigte Bandbreite ein Gigabit-Ethernet mit einer Geschwindigkeit gleich oder größer 1 Gb pro Sekunde (Gbps). Für die Verbindung zwischen dem SAM DX-Server und dem Bildspeicher (DSR) beträgt die benötigte Bandbreite 10 Gb pro Sekunde.

Wie der Aperio GT 450 DX sich in Ihr Netzwerk einfügt

Dies sind die Hauptkomponenten des Aperio GT 450 DX und des SAM DX-Systems:

- **Aperio GT 450 DX –** Ein oder mehrere Aperio GT 450 DX-Scanner können über das Netzwerk mit einem SAM DX-Server verbunden werden. Jeder SAM DX-Server unterstützt mehrere Scanner.
- **Aperio Scanner Administration Manager DX Server (SAM DX-Server) –** Der SAM DX-Server enthält die Scanner Administration Manager-Client-Anwendungssoftware, das Thema dieses Handbuchs. Der SAM DX-Server bietet den DICOM-Image-Konverter zum Konvertieren von DICOM-Bildern in das SVS-Image-Dateiformat. (Aperio GT 450 DX-Scanner übertragen verschlüsselte DICOM-Bilder an den SAM DX-Server.) SAM DX verwaltet auch die Scannerkonfigurationseinstellungen und die Nachrichtenübermittlung über Mirth-Verbindungen.
- **Digital Slide Repository Server (DSR-Server) –** Dieser Server (auch als Bildspeichersystem-Server bekannt) enthält alle Objektträgerbilder vom Scanner sowie die Infrastruktur für ihre Verwaltung. Das Repository kann sich auf einer Netzwerkfreigabe eines Servers in Ihrem Netzwerk oder auf einem optionalen Aperio eSlide Manager-Server befinden.
- **SAM DX Workstation/Konsole –** Über einen Webbrowser (Firefox, Chrome oder Edge) auf einem PC oder Laptop in Ihrem Netzwerk können Administratoren und Bediener über die Konsole Ereignisdaten und -statistiken anzeigen. Administratoren können auch Benutzerkonten hinzufügen, PINs festlegen und Konfigurationsänderungen vornehmen.
- **Datenbank –** Die MS SQL Server-Datenbank, die Benutzerdaten, Einstellungsdaten, über Statistikberichte gemeldete Daten und Ereignisse sowie in den Protokollen gemeldete Fehler enthält.
- **Netzwerk-Dateifreigabe –** Der Ort in Ihrem Netzwerk, an dem Ereignisprotokolle gespeichert werden.

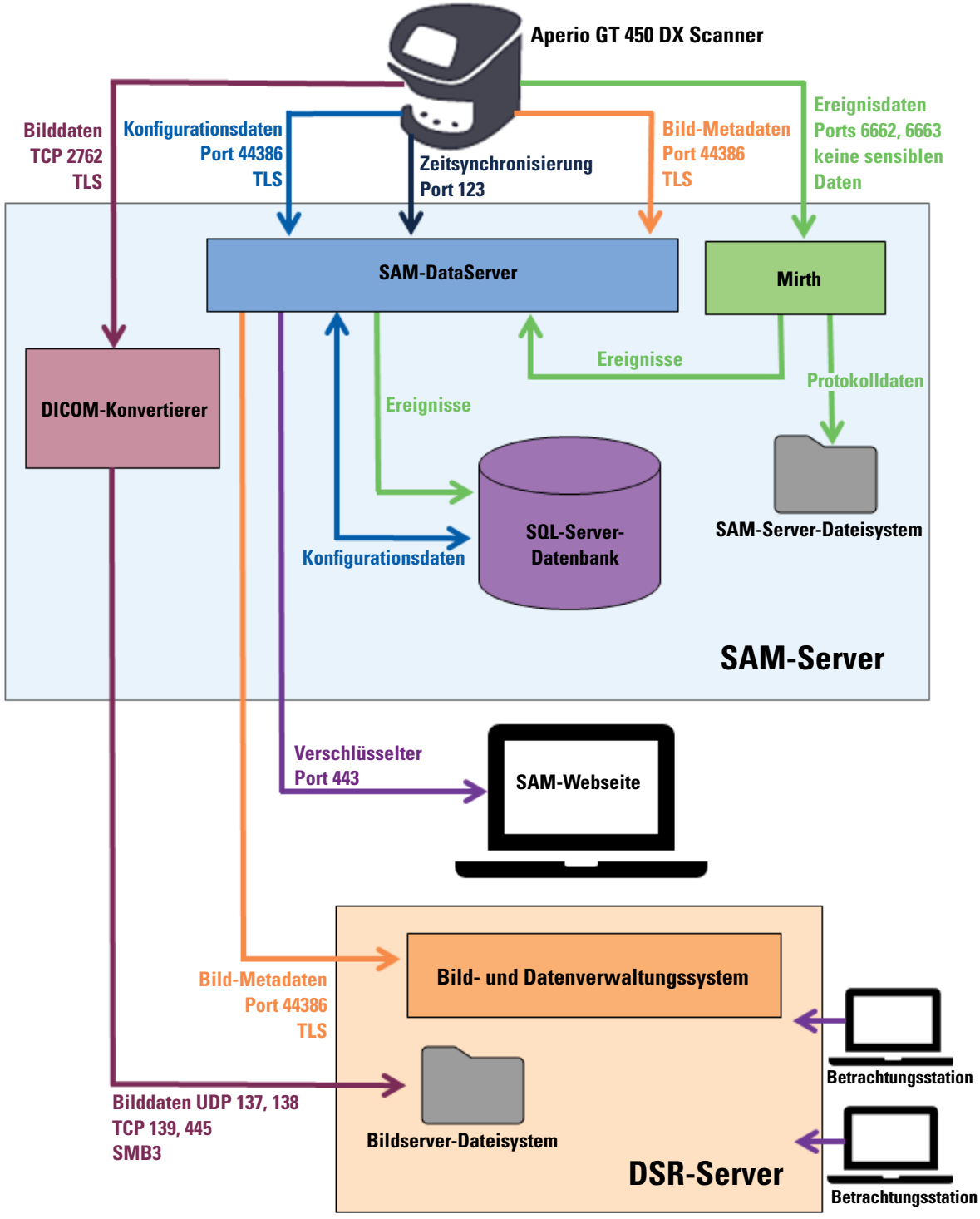
Sicherer Zugriff

Der Zugriff über die SAM DX-Benutzeroberfläche ist per SSL abgesichert. Bei der Installation werden selbstsignierte SSL-Zertifikate installiert. Um Sicherheitsmeldungen des Browsers zu vermeiden, können Kunden ihre eigenen Sicherheitszertifikate verwenden.

Um Ihr Netzwerk vor Cybersicherheitsangriffen zu schützen, empfehlen wir Ihnen, ungenutzte Ports und Dienste in Ihrem Netzwerk zu deaktivieren.

Empfohlene Netzwerkkonfiguration für den Aperio GT 450 DX

In diesem Abschnitt wird beschrieben, wie Sie den Aperio GT 450 DX in Ihre IT-Umgebung einbinden, um optimale Leistung zu erzielen.



Datentyp	Beschreibung	Port
Bilddaten	Der Scanner sendet DICOM-Bilddaten an den DICOM-Konvertierer. Die Daten werden mit TLS-Verschlüsselung gesendet. Konfigurieren Sie die Kommunikation zwischen dem Scanner und dem DICOM-Konvertierer mithilfe der Einstellungen „Hostname“ und „Port“ auf der Konfigurationsseite **Images** (Bilder).	TCP 2762
	Der DICOM-Konvertierer sendet die Bilddaten (entweder als konvertierte SVS-Datei oder als DICOM-Rohdaten) an das Bild- und Datenverwaltungssystem (IDMS) auf dem DSR-Server. Die Daten werden mit SMB3-Verschlüsselung gesendet. Konfigurieren Sie die Kommunikation zwischen dem DICOM-Konvertierer und dem DSR mithilfe der Einstellung „File Location“ (Dateipfad) auf der Seite **Images** (Bilder).	UDP 137, 138 TCP 139, 445
	Bilder können an Viewing Stations gesendet werden, die mit dem DSR verbunden sind.	80, 443
Scanner-Konfigurationsdaten	Der Scanner sendet eine Anfrage nach den Konfigurationsdaten an den SAM DX DataServer. Der SAM DX DataServer sendet die Konfigurationsdaten an den Scanner zurück. Die Daten werden mit TLS-Verschlüsselung gesendet. Die Kommunikation zwischen dem Scanner und dem SAM DX DataServer wird am Scanner konfiguriert.	44386
	Der SAM DX DataServer speichert die Konfigurationsdaten in der SQL Server-Datenbank auf dem SAM DX-Server.	
	Der SAM DX DataServer zeigt die Konfigurationsdaten auf der SAM DX-Webseite an.	
Zeitsynchronisation	Die Zeitsynchronisation zwischen SAM DX und mehreren Scannern wird mithilfe des Netzwerkzeitprotokolls durchgeführt.	UDP 123
Bild-Metadaten	Der Scanner sendet Bild-Metadaten an den SAM DX DataServer. Die Daten werden mit TLS-Verschlüsselung gesendet. Die Kommunikation zwischen dem Scanner und dem SAM DX DataServer wird am Scanner konfiguriert.	44386
	Der SAM DX DataServer sendet Bild-Metadaten an den IDMS auf dem DSR. Die Daten werden mit TLS-Verschlüsselung gesendet. Konfigurieren Sie die Kommunikation zwischen dem SAM DX DataServer und dem Scanner mithilfe der Hostname- und Port-Einstellungen auf der Seite **DSR**.	
Meldungs- und Ereignisdaten	Der Scanner sendet Protokolle und Ereignisdaten an den Mirth Connect Server. Es werden keine sensiblen Daten übertragen. Konfigurieren Sie die Kommunikation zwischen dem Scanner und dem Mirth Connect Server auf der Konfigurationsseite **Event Handling** (Ereignisbehandlung).	6662, 6663
	Der Mirth Connect Server kopiert kritische Ereignis- und Fehlerdaten auf den SAM DX DataServer und dann sendet der SAM DX DataServer diese Daten an die SQL-Datenbank. Dies sind die Daten, die mithilfe der SAM DX-Ereignisprotokolle gemeldet werden.	
	Der SAM DX DataServer zeigt die Ereignisdaten auf der SAM DX-Webseite an.	
	Der Mirth Connect Server verarbeitet die Protokolldaten und fügt sie dem Ereignisprotokoll hinzu, das sich auf dem Dateisystem befindet. Die Kommunikation zwischen Mirth und dem Ereignisprotokoll wird in der Anwendungskonfiguration von Mirth eingestellt. Sie ist nicht in SAM DX verfügbar.	

„Scanner-Configuration Settings (Konfigurationseinstellungen)“ auf Seite 23 enthält Informationen über die Konfiguration der verschiedenen Verbindungen zwischen den Komponenten und Diensten über die SAM DX-Benutzeroberfläche.

3 Konfiguration des Aperio GT 450 DX

Dieses Kapitel enthält Informationen über die Änderung der Scannereinstellungen, der Systeminformationen oder der Konfiguration. Die Scanner-Konfiguration legt fest, wie der Scanner mit SAM DX kommuniziert und wie SAM DX mit den verschiedenen Komponenten im Netzwerk kommuniziert, einschließlich des IDMS-Servers, des DICOM-Bildkonvertierers und anderer. Ebenfalls enthalten sind die Verfahren für die Zuweisung von PINs für den Zugriff auf den Scanner.

Allgemeine Hinweise

Nur Benutzer mit der Rolle „Lab Admin“ (Labor-Administrator) können die Konfiguration bearbeiten. Bediener können die Konfigurationseinstellungen ansehen, aber keine Änderungen daran vornehmen.

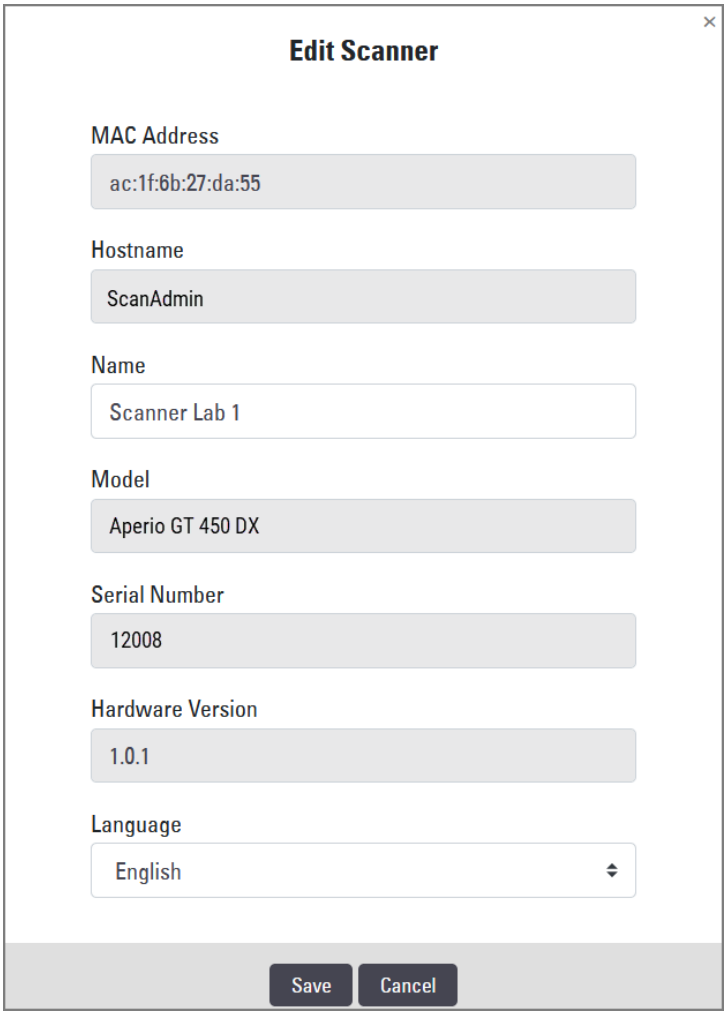
Einige der Konfigurationseinstellungen legen fest, wie der Scanner mit SAM DX kommuniziert, etwa „Mac Address“ (Mac-Adresse) und „Hostname“. Die Einstellung „Serial Number“ (Seriennummer) identifiziert den Scanner eindeutig. Die Einstellungen „Calibration“ (Kalibrierung) legen fest, wie der Scanner arbeitet. Diese Einstellungen können nur vom Leica-Supportpersonal verändert werden und werden in ausgegrauten Feldern angezeigt.

Es gibt drei Sätze mit Scanner-Konfigurationsparametern:

- *Scanner-Basiseinstellungen*, etwa Netzwerkadresse, Name und Anzeigesprache
- *Scanner-Systeminformationen*, etwa allgemeine Informationen und detaillierte Scanner- und Kameraeinstellungen
- *Scanner-Konfigurationseinstellungen*, etwa Kommunikationseinstellungen für den DICOM-Bildkonvertierer und dem DSR-Server, die Ereignisverwaltung, Zeitzone und die PIN-Verwaltung

Jeder Parametersatz wird in diesem Kapitel behandelt.

Scanner-Basiseinstellungen

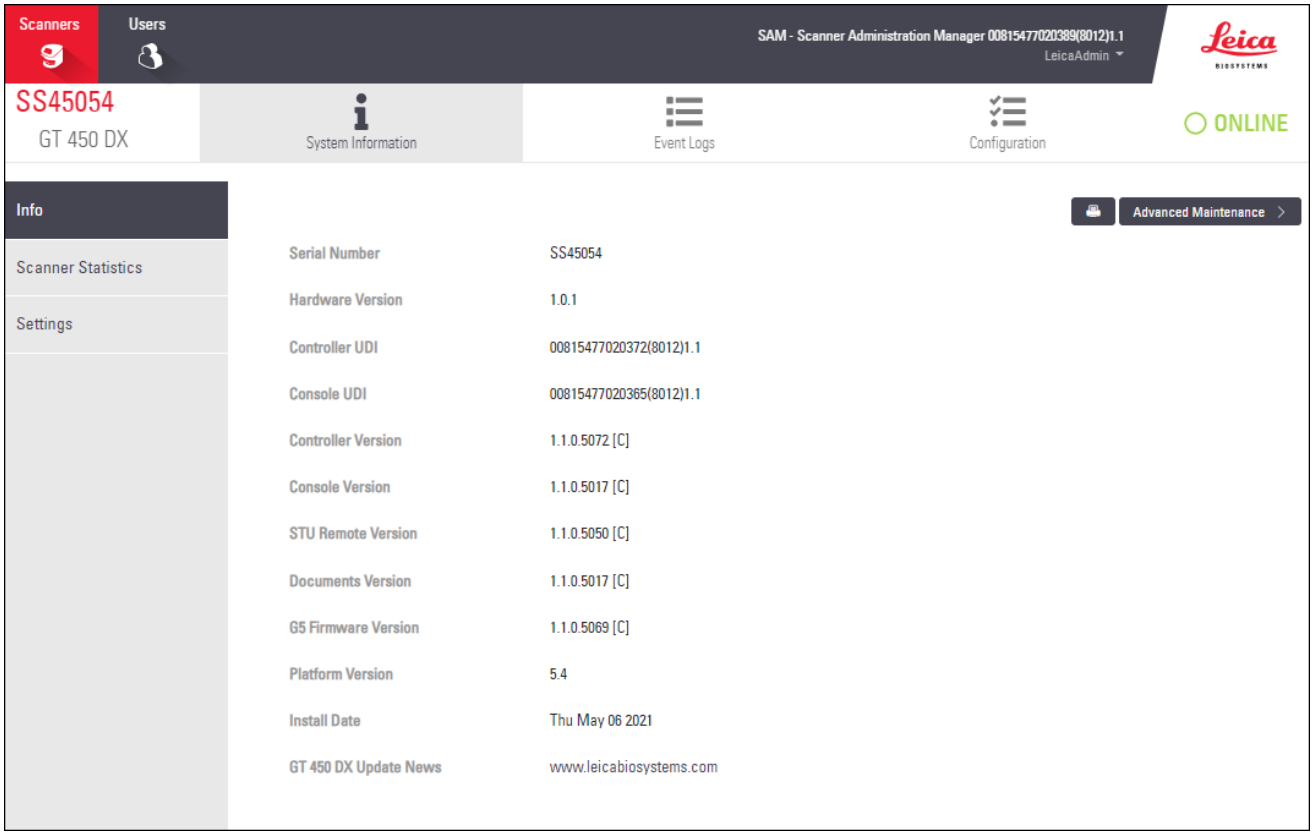


Um das Dialogfeld „Edit Scanner“ (Scanner bearbeiten) anzuzeigen:

1. Bestätigen Sie, dass das Symbol **Scanners** (Scanner) im Banner ausgewählt ist und die Seite die Liste der Scanner anzeigt. Klicken Sie auf das Symbol **Scanners** (Scanner), um die Liste anzuzeigen, falls erforderlich.
2. Fahren Sie mit der Maus über den Namen des Scanners, bis das Bearbeiten-Symbol erscheint, dann klicken Sie auf den Namen des Scanners.
3. Bearbeiten Sie die verfügbaren Einstellungen nach Ihrem Bedarf:
   - Geben Sie einen benutzerfreundlichen Namen ein, um den Scanner in Ihrer Einrichtung zu identifizieren. (Dieser benutzerfreundliche Name wird auf der Hauptseite angezeigt.)
   - Wählen Sie, falls erforderlich, eine neue Sprache für die Meldungen im Bedienfeld des Scanners.
   - Siehe *„Anhang B: Zusammenfassung der Scanner-Einstellung und Konfigurationsoptionen“ auf Seite 43* für zusätzliche Informationen zu jeder Option.
4. Klicken Sie auf **Save** (Speichern), um Ihre Änderungen zu speichern.

Falls Sie einen neuen Scanner einrichten oder ändern müssen, wie der Scanner mit anderen Servern im Netzwerk kommuniziert, fahren Sie fort mit *„Scanner-Configuration Settings (Konfigurationseinstellungen)“ auf Seite 23*.

Scanner System Information: Info Page (Scanner-Systeminformationen: Seite „Info“)



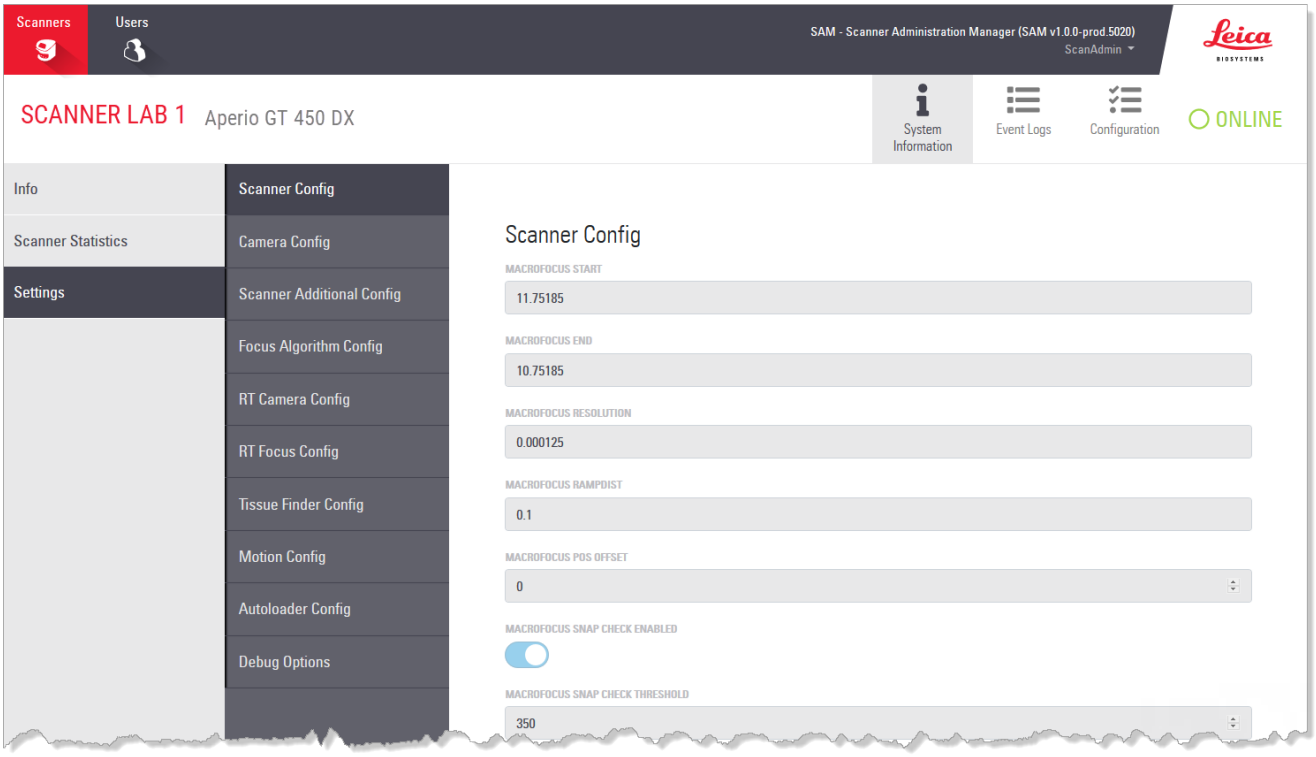
Um die Seite mit den Systeminformationen anzuzeigen:

1. Bestätigen Sie, dass das Symbol **Scanners** (Scanner) im Banner ausgewählt ist und die Seite die Liste der Scanner anzeigt. Klicken Sie auf das Symbol **Scanners** (Scanner), um die Liste anzuzeigen, falls erforderlich.
2. Klicken Sie auf das Symbol **System Information** (Systeminformationen) rechts neben dem gewünschten Scanner.
3. Klicken Sie auf **Info** (Info) in der seitlichen Menüleiste.

Auf der Seite „Info“ der Systeminformationen können Sie sich die Scanner-Einstellungen ansehen. (Sie können auf dieser Seite keine Änderungen vornehmen).

Die Firmware- und Hardwareversionen werden automatisch aktualisiert, sobald SAM DX eine Verbindung mit dem Scanner herstellt.

Scanner-System Information: Settings Page (Systeminformationen: Seite Einstellungen)



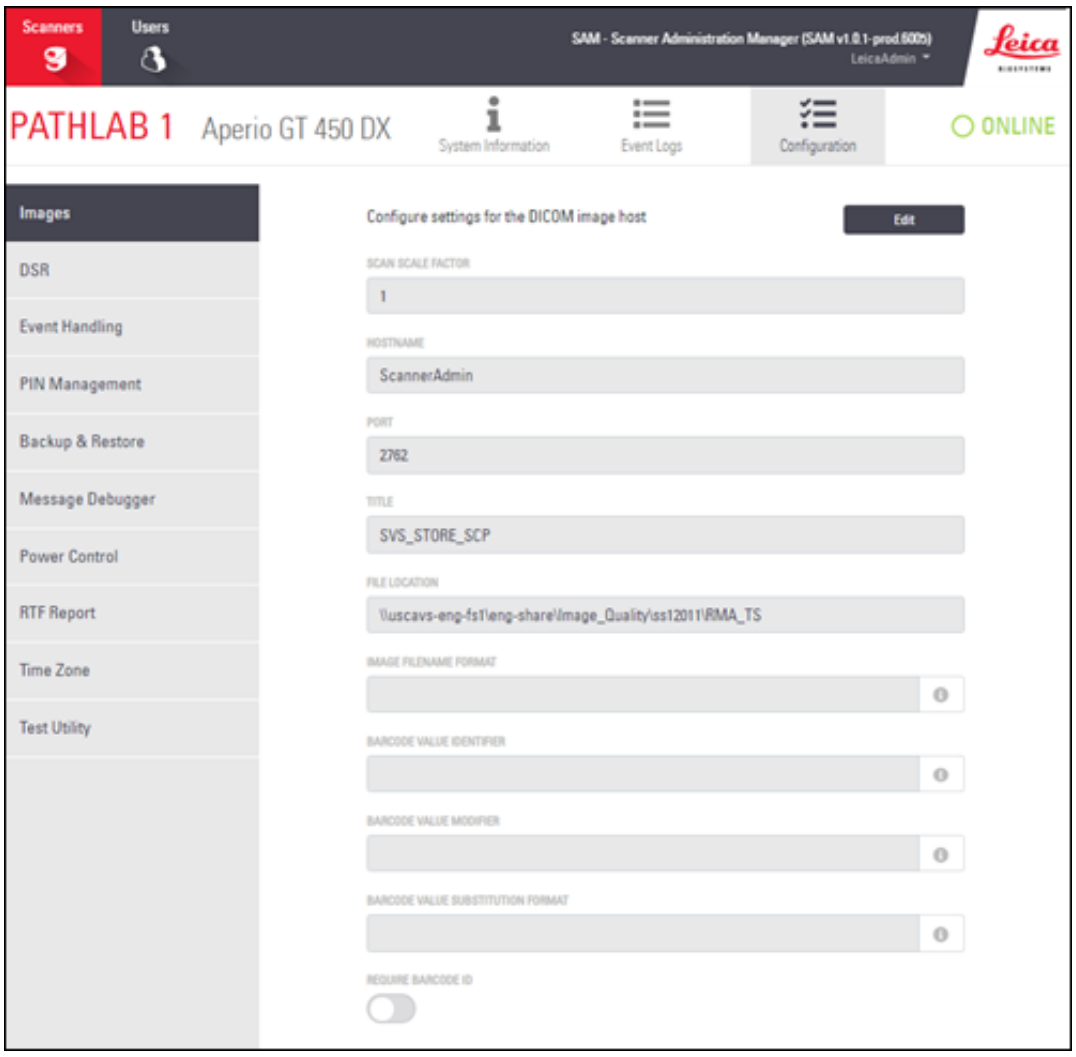
Die Seite „Settings“ (Einstellungen) der Systeminformationen zeigt Konfigurationseinstellungen für Kamera, Scanner, Fokusalgorithmus, Bewegung und AutoLoader an. (Die obenstehende Illustration zeigt nur manche der verfügbaren Einstellungen.) Die meisten oder alle der Einstellungen auf dieser Seite werden für Sie von einem Mitarbeiter von Leica Biosystems konfiguriert, wenn der Scanner installiert wird. Allerdings können Sie während einer Fehlerbehebung dazu aufgefordert werden, die Einstellungen zu überprüfen.

Falls eine Änderung vorgenommen werden muss, wird Ihnen der Techniker von Leica Biosystems genaue Anweisungen erteilen. Nehmen Sie niemals Änderungen an diesen Einstellungen vor, außer ein Techniker von Leica Biosystems hat Sie dazu aufgefordert.

Um mit der Seite „Settings“ (Einstellungen) der Systeminformationen Einstellungen anzusehen oder zu bearbeiten:

1. Bestätigen Sie, dass das Symbol **Scanners** (Scanner) im Banner ausgewählt ist und die Seite die Liste der Scanner anzeigt.
2. Klicken Sie auf das Symbol **System Information** (Systeminformationen) rechts neben dem gewünschten Scanner.
3. Klicken Sie auf **Settings** (Einstellungen) in der seitlichen Menüleiste.
4. Verwenden Sie die Bildlaufleiste, um die Liste der verfügbaren Einstellungen anzuzeigen.

Scanner-Configuration Settings (Konfigurationseinstellungen)



Die Einstellungen auf diesen Seiten werden von einem Mitarbeiter von Leica Biosystems für Sie konfiguriert, wenn der Scanner installiert wird. Allerdings können Sie während einer Fehlerbehebung dazu aufgefordert werden, die Einstellungen zu überprüfen. Sie müssen möglicherweise Änderungen an den Einstellungen vornehmen, wenn Änderungen an Ihrem Netzwerk vorgenommen werden, die eine oder mehrere der Kommunikationseinstellungen beeinflussen. Nur Benutzer mit der Rolle „Lab Admin“ (Labor-Administrator) können die Konfiguration bearbeiten.

Es gibt mehrere Konfigurationsseiten, jeweils eine für die Einstellungen „Images“ (Bilder) (DICOM-Konvertierer), DSR, „Event handling“ (Ereignisbehandlung), „PIN Management“ (PIN-Verwaltung) und „Time Zone“ (Zeitzone).

- Die Einstellungen unter **Images** (Bilder) steuern die Kommunikation mit dem Server, auf dem sich der DICOM-Konvertierer befindet, und definieren, wo die konvertierten SVS-Bilddaten gespeichert werden. Sie können außerdem weitere Parameter einstellen. Siehe *„Seite „Images“ (Bilder)“ auf Seite 25*.
- Die Einstellungen unter **DSR** (Digital Slide Repository) steuern die Kommunikation mit dem Bildspeichersystem (dem DSR), auf dem die Bild-Metadaten gespeichert werden.

- Die Einstellungen unter **Event Handling** (Ereignisbehandlung) steuern die Kommunikation mit dem Server, auf dem Scanner-Meldungen und -Ereignisse verarbeitet werden (Mirth). Weitere Informationen über Ereignisprotokolle finden Sie unter *„Arbeiten mit dem Ereignisprotokoll“ auf Seite 32*.
- Die Einstellungen unter **PIN Management** (PIN-Verwaltung) ermöglichen Ihnen die Erstellung einer oder mehrerer PINs für den Zugriff auf den Scanner. Weitere Einzelheiten finden Sie unter *„PIN-Verwaltung“ auf Seite 27*.

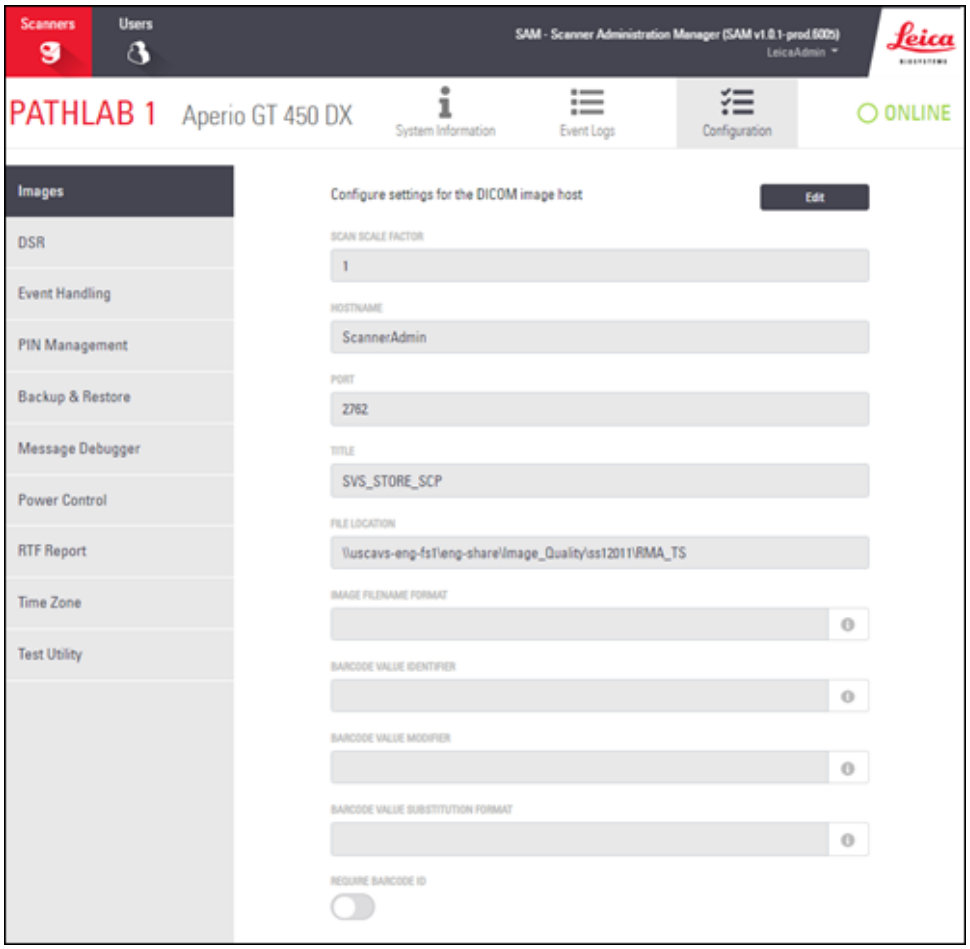
Um mithilfe der Konfigurationsseiten Einstellungen anzusehen oder zu bearbeiten:

1. Bestätigen Sie, dass das Symbol **Scanners** (Scanner) im Banner ausgewählt ist und die Seite die Liste der Scanner anzeigt.
2. Klicken Sie auf das **Configuration** (Konfiguration) rechts neben dem Scanner, den Sie konfigurieren möchten. Die Konfigurationsseite „Images“ (Bilder) wird angezeigt.
3. Öffnen Sie die Konfigurationseinstellungen für „Images“ (Bilder) (DICOM), DSR, „Event Handling“ (Ereignisbehandlung), „PIN Management“ (PIN-Verwaltung) oder „Time Zone“ (Zeitzone).
   - Klicken Sie in der seitlichen Menüleiste auf **Images** (Bilder), **DSR**, **Event Handling** (Ereignisbehandlung), **PIN Management** (PIN-Verwaltung) oder **Time Zone** (Zeitzone).
   - Klicken Sie auf **Edit** (Bearbeiten), um Änderungen auf der jeweiligen Seite vorzunehmen. Beachten Sie, dass Sie keine Änderungen in ausgegrauten Feldern vornehmen können.

   Siehe *„PIN-Verwaltung“ auf Seite 27* für Informationen zum Hinzufügen, Löschen oder Verändern von PINs oder dem Ändern der Zeitüberschreitung.
4. Wenn Sie Änderungen vornehmen, klicken Sie auf **Save** (Speichern), um die Änderungen zu speichern und zum Betrachtermodus zurückzukehren.

Siehe *„Anhang B: Zusammenfassung der Scanner-Einstellung und Konfigurationsoptionen“ auf Seite 43* für zusätzliche Informationen zu jeder Option.

Seite „Images“ (Bilder)



Die Seite **Images** (Bilder) enthält Einstellungen für die folgenden Parameter:

- Der Speicherort, an den die gescannten Bilder gesendet werden (einschließlich Servername und Speicherort der Datei).
- Beachten Sie, dass die Felder „Title“ (Titel) und „Scan Scale Factor“ (Scan-Skalierungsfaktor) für interne Zwecke vorgesehen sind. Sie sollten diese Felder daher nur ändern, wenn Sie dazu von Leica Biosystems Technical Support aufgefordert werden.
- Das Format des Bilddateinamens (siehe unten).
- Barcode-Management (siehe unten).

Der Laboradministrator kann auf die Schaltfläche **Edit** (Bearbeiten) klicken, um die Einstellungen auf dieser Seite zu verändern.

„Image File Name Format“ (Format des Bilddateinamens)

Standardmäßig beginnt der Dateiname des gescannten Bildes mit der numerischen ImageID des Bildes, gefolgt von einem Unterstrich und einem sechsstelligen Code, der mit einer Dateiendung endet, die das Format der Datei angibt.

Sie können zu Beginn des Feldes Ihren eigenen Text eingeben und dann die folgenden Schlüsselwörter in beliebiger Reihenfolge hinzufügen. Die Schlüsselwörter müssen vollständig aus Großbuchstaben bestehen und von { }-Zeichen umgeben sein. Wir empfehlen, die Schlüsselwörter zur besseren Lesbarkeit durch Unterstriche zu trennen.

- BARCODEID – Barcodewert-Kennung (siehe nächsten Abschnitt)
- RACK – Rack-Nummer
- SLIDE – Objektträgerposition im Rack
- IMAGEID – Eindeutige Kennung für das Bild

Wenn Sie beispielsweise alle von diesem Scanner gescannten Bilder als von ScannerA stammend identifizieren möchten und darüber hinaus angeben möchten, von welchem Rack und von welcher Position im Rack der Objektträger stammt, können Sie ein Format für den Namen der Bilddatei erstellen, das wie folgt aussieht:

ScannerA_{RACK}_{SLIDE}

Der daraus resultierende Dateiname beginnt mit dem Text „ScannerA“, gefolgt von der Rack-Nummer und der Objektträgerposition im Rack. Danach folgen ein Unterstrich, ein sechsstelliger Code und die Dateierweiterung. Ein Beispiel:

ScannerA_5_2_210164.SVS

„Barcode Management“ (Barcode Management)

Der Barcode ist eine Textzeichenfolge, die in der gescannten Bilddatei gespeichert ist und in Ihrem Digitalbild-Verwaltungssystem angezeigt werden kann.

Je nach den in Ihrer Institution verwendeten Verfahren können sich auf dem Glasträger-Etikett mehrere Barcodes befinden. In diesem Fall können Sie ermitteln, welcher Barcode dem gescannten Bild zugeordnet und im eSlide-Verwaltungssystem angezeigt wird.

Geben Sie dazu im Feld **Barcode Value Identifier** (Barcodewert-Kennung) einen Suchbegriff in Form eines regulären Ausdrucks ein.

(Ein regulärer Ausdruck, regex oder regexp, ist eine Folge von Zeichen, die ein Suchmuster definieren. Beispielsweise gibt \d{6} an, dass ein Barcode mit sechs aufeinanderfolgenden Ziffern verwendet wird. Wenn Sie mit regulären Ausdrücken nicht vertraut sind, wenden Sie sich für Unterstützung bitte an den technischen Support von Leica Biosystems.)

Einige Einrichtungen integrieren zur Kontrolle (nicht druckbare) Zeichen in ihre Barcodes. Wenn Sie diese Zeichen herausfiltern oder ersetzen wollen, geben Sie die Zeichen, die Sie ändern möchten, in Form eines regulären Ausdrucks in das Feld **Barcode Value Modifier** (Barcodewert-Änderung) ein. Mit [\x00-\x1f\x7f] legen Sie beispielsweise fest, dass alle nicht druckbaren Zeichen geändert werden.

Eine genauere Spezifizierung der zu ersetzenden, nicht druckbaren Zeichen, die mit dem Feld **Barcode Value Modifier** (Barcodewert-Änderung) übereinstimmen, erfolgt über den Wert im Feld **Barcode Value Substitution Format** (Barcodewert-Ersetzungsformat). Durch einen Wert „?“ in Kombination mit einem Wert [\x00-\x1f\x7f] des Feldes **Barcode Value Modifier** (Barcodewert-Änderung) werden beispielsweise alle nicht druckbaren Zeichen mit einem Fragezeichen „?“ ersetzt. Wenn Sie die Zeichen, die mit den Zeichen im Feld **Barcode Value Modifier** (Barcodewert-Änderung) übereinstimmen, löschen möchten, lassen Sie diesen Wert leer.

Wenn Ihre Verfahren erfordern, dass jedes gescannte Bild mit einem Barcode gespeichert wird, schieben Sie die Schaltfläche **Require Barcode ID** (Barcode-ID erforderlich) nach rechts. Wenn diese Option aktiviert ist, überspringt der Scanner Objektträger, die nicht mit einem Barcode versehen sind oder bei denen der Scanner den Barcode nicht lesen kann.

Mit den in diesem Abschnitt beschriebenen Funktionen können weitergehende Änderungen am Barcode vorgenommen werden. Wenn Sie Bedarf an zusätzlichen Steuerungsmöglichkeiten des vom Aperio GT 450 DX zurückgemeldeten Barcode-Strings haben, kontaktieren Sie Leica Biosystems Technische Dienstleistungen.

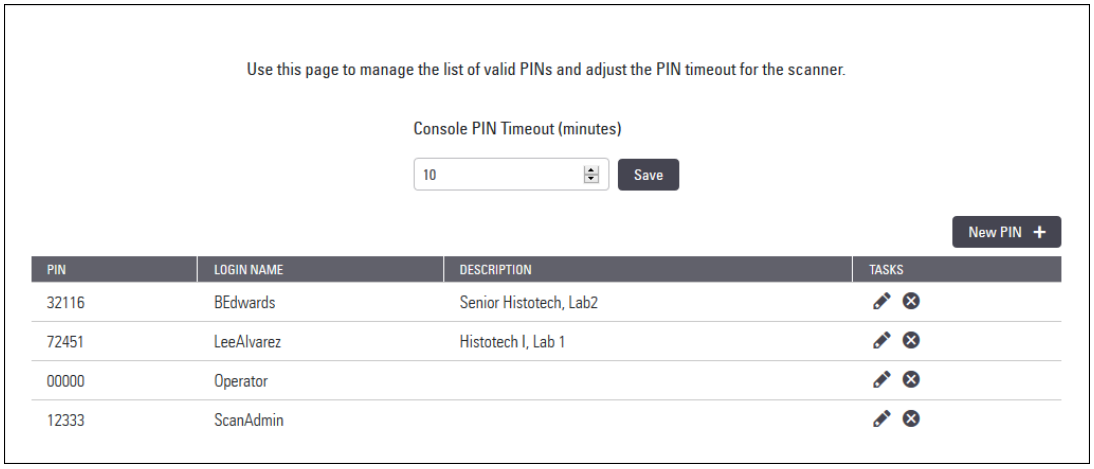
PIN-Verwaltung

PINs kontrollieren den Zugriff auf den Scanner. (Zur Freischaltung des Scanners muss jeder Bediener eine PIN eingeben.)

Jede PIN ist einem bestimmten Benutzer des Scanners zugeordnet. Wenn ein Bediener mit einer PIN auf den Scanner zugreift, zeichnet der Scanner den Namen des Benutzers der PIN im internen Scanner-Protokoll auf. (Die PIN selbst wird nicht protokolliert.) Der Scanner bleibt entsperrt, solange der Bediener aktiv ist. Falls niemand am Scanner aktiv ist, bevor die festgelegte Zeit abläuft, sperrt sich der Scanner automatisch, bis ein Bediener eine gültige PIN eingibt.

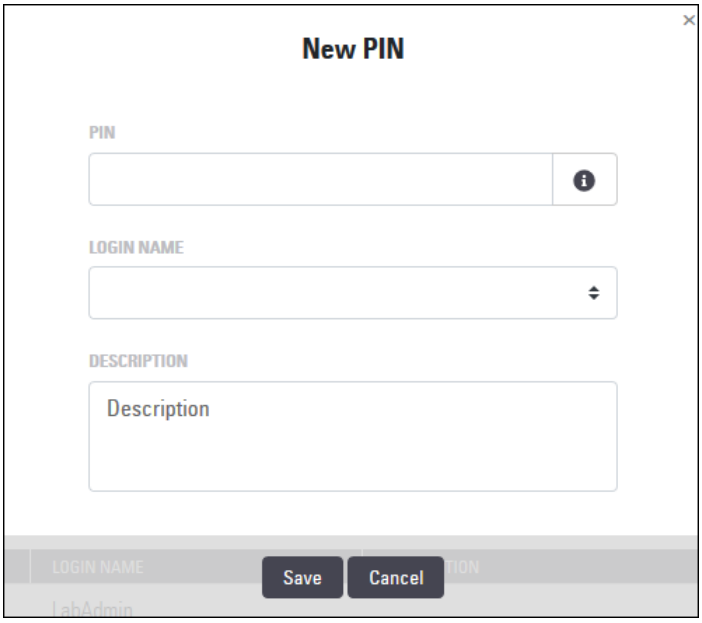
- Sie müssen für jeden Scanner mindestens eine PIN festlegen, und PINs gelten jeweils für genau einen Scanner. Sie können für jeden Scanner im System entweder den SAM DX oder verschiedene PINs festlegen, abhängig davon, was für die Arbeitsabläufe in Ihrer Einrichtung am besten geeignet ist.
- Eine PIN begrenzt nicht die Funktionen, auf die ein Bediener am Scanner zugreifen kann.
- Wenn Sie die Zeitüberschreitung für die Anmeldung festlegen, wählen Sie eine Zeit, die für die Bediener bequem ist, ohne so lang zu sein, dass der Scanner unbeobachtet und für Missbrauch offen sein kann.

Konfiguration einer PIN und Zeitüberschreitung



1. Bestätigen Sie, dass das Symbol **Scanners** (Scanner) im Banner ausgewählt ist und die Seite die Liste der Scanner anzeigt.
2. Klicken Sie auf das **Configuration** (Konfiguration) rechts neben dem Scanner.
3. Klicken Sie auf **PIN Management** (PIN-Verwaltung) in der seitlichen Menüleiste.
4. Geben Sie in das Feld **Console PIN Timeout** (Zeitüberschreitung Konsolen-PIN) einen Wert (in Minuten) ein. Der Scanner sperrt sich automatisch nach diesem Zeitraum ohne Aktivität.

5. Klicken Sie auf **New PIN+** (Neue PIN+), um eine neue PIN hinzuzufügen. Der Bildschirm „New PIN“ (Neue PIN) wird angezeigt.



- Geben Sie die PIN in das Feld „PIN“ ein (fünf Ziffern). PINs können nur Ziffern enthalten; Buchstaben oder Sonderzeichen sind nicht erlaubt.
- Wählen Sie aus der Dropdown-Liste Login Name (Login-Name) einen Benutzer aus. In dieser Liste werden nur Benutzer angezeigt, die keine PIN haben. (Informationen zum Hinzufügen von Benutzern finden Sie in *„Kapitel 5: Benutzerverwaltung“ auf Seite 33.)*
- Geben Sie optional unter „Description“ (Beschreibung) eine Beschreibung des Benutzers ein, der diese PIN verwenden wird.
- Klicken Sie auf **Save** (Speichern), um zur Liste der PINs zurückzukehren.

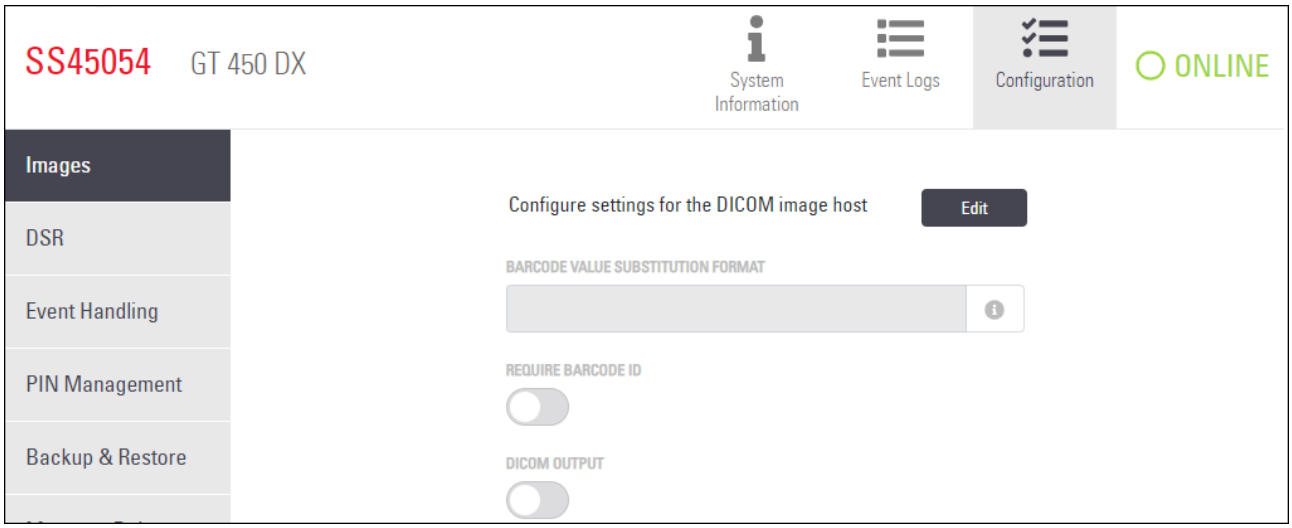
Aktivieren der DICOM-Bildausgabe

Der Aperio GT 450 DX kann Bilddateien entweder im SVS- oder DICOM-Format ausgeben. (Das Bilddateiformat .SVS ist das Standardformat.)

Sie können SAM DX verwenden, um die DICOM-Ausgabe für bestimmte Scanner zu aktivieren.

*Sie können die DICOM-Bildausgabe erst aktivieren, wenn Ihre IT-Umgebung die in der **Aperio DICOM-Konformitätserklärung** beschriebenen Anforderungen erfüllt. Außerdem muss sich ein Vertreter von Leica Biosystems Technische Dienstleistungen als Leica Admin bei SAM DX anmelden und die **optionalen Funktionen** für den Scanner aktivieren, den Sie für DICOM konfigurieren möchten.*

1. Melden Sie sich bei SAM DX als Administrator an, gehen Sie auf die SAM DX-Hauptseite und klicken Sie auf **Configuration** (Konfiguration) neben dem Scanner, den Sie für DICOM konfigurieren möchten.
2. Klicken Sie links auf das Fenster **Images** (Bilder).



3. Klicken Sie auf die Schaltfläche **Edit** (Bearbeiten) neben **Configure settings for DICOM image host** (Einstellungen für DICOM-Bildhost konfigurieren).
4. Schieben Sie die Schaltfläche **DICOM Output** (DICOM-Ausgabe) nach rechts. (Die Schaltfläche **Edit** (Bearbeiten) ändert sich zur Schaltfläche **Save** (Speichern).)
5. Klicken Sie auf **Save** (Speichern).

Bei Verwendung eines Scanners, der für die Ausgabe von DICOM-Bildern konfiguriert wurde, zeigt die Konsole „(DICOM)“ oben auf der Seite „Konsole“ an:

Aperio GT 450 DX (DICOM)

4 Anzeige der Systeminformationen

Dieses Kapitel beschreibt, wie Sie die verschiedenen Konfigurationsoptionen und Einstellungen des SAM DX-Servers anzeigen können.

Anzeige von Scanner-Informationen und -Einstellungen

In der folgenden Tabelle finden Sie Anweisungen für die Anzeige von Scanner- und Systemeinstellungen.

In vielen Fällen können Sie diese Einstellungen nicht verändern, aber der technische Kundendienst von Leica Biosystems kann Sie während einer Fehlerbehebung oder Wartung nach den Angaben fragen. Einige Einstellungen können nur von Benutzern mit der Rolle „Lab Admin“ (Labor-Administrator) eingesehen werden.

Gewünschte Anzeige:	Vorgehensweise:
MAC-Adresse	Wählen Sie den Scanner aus dem Hauptbildschirm aus, um das Dialogfeld „Edit Scanner“ (Scanner bearbeiten) zu öffnen.
Scanner Hostname (Scanner-Hostname)	
Scanner Friendly Name (Benutzerfreundlicher Scanner-Name)	
Scanner Model (Scanner-Modell)	
Scanner Language (Scanner-Sprache)	
Scanner Serial Number (Scanner-Seriennummer)	Wählen Sie den Scanner aus dem Hauptbildschirm aus, um das Dialogfeld „Edit Scanner“ (Scanner bearbeiten) zu öffnen. Oder: Klicken Sie auf **System Information** (Systeminformationen) für den Scanner und dann auf **Info** (Info) in der seitlichen Menüleiste.
Scanner Firmware Version (Scanner-Firmwareversion)	Klicken Sie auf **System Information** (Systeminformationen) für den Scanner und dann auf „Info“ in der seitlichen Menüleiste.
Scanner Hardware Version (Scanner-Hardwareversion)	
Scanner Installation Date (Scanner-Installationsdatum)	
DICOM Server Settings (DICOM-Servereinstellungen)	Klicken Sie auf **Configuration** (Konfiguration) für den Scanner und dann auf **Images** (Bilder) in der seitlichen Menüleiste.

Gewünschte Anzeige:	Vorgehensweise:
DSR Server Settings (DSR-Servereinstellungen)	Klicken Sie auf **Configuration** (Konfiguration) für den Scanner und dann auf **DSR** in der seitlichen Menüleiste.
Event Handling (Mirth server) Settings (Einstellungen für Ereignisbehandlung (Mirth-Server))	Klicken Sie auf **Configuration** (Konfiguration) für den Scanner und dann auf **Event Handling** (Ereignisbehandlung) in der seitlichen Menüleiste.
Camera Configuration Settings (Kamera-Konfigurationseinstellungen)	Klicken Sie auf **System Information** (Systeminformationen) für den Scanner und dann auf **Settings** (Einstellungen) in der seitlichen Menüleiste.
Scanner Additional Config Settings (Zusätzliche Scanner-Konfig.-Einstellungen)	
Focus Algorithm Config Settings (Fokusalgorithmus-Konfig.-Einstellungen)	
Motion Config XML File (Bewegungskonfig.-XML-Datei)	
Autoloader Config XML File (AutoLoader-Konfig.-XML-Datei)	
List of Users (Benutzerliste)	Klicken Sie auf das Symbol **Users** (Benutzer) in der oberen Leiste.
List of PINs (PIN-Liste)	Klicken Sie auf **Configuration** (Konfiguration) für den Scanner und dann auf **PIN Management** (PIN-Verwaltung) in der seitlichen Menüleiste.

Anzeige von Scanner-Statistiken

Die SAM DX-Konsole kann dieselben Scanner-Statistiken anzeigen wie diejenigen, die auf dem Steuerfeld des Scanners verfügbar sind.

Benutzer mit der Rolle „Operator“ (Bediener) oder „Lab Admin“ (Labor-Administrator) können die Statistiken anzeigen.

Um die Scanner-Statistiken anzuzeigen:

1. Bestätigen Sie, dass das Symbol „Scanners“ (Scanner) im Banner ausgewählt ist und die Seite die Liste der Scanner anzeigt.
2. Klicken Sie auf das Symbol **System Information** (Systeminformationen) rechts neben dem Scanner.
3. Klicken Sie auf **Scanner Statistics** (Scanner-Statistiken) in der seitlichen Menüleiste.
4. Wählen Sie den Anzeigezeitraum aus den Optionen oberhalb der Tabelle.
5. Klicken Sie auf  , um die Statistiken auszudrucken. Verwenden Sie den Druckdialog, um den Drucker und andere Druckoptionen festzulegen.

Arbeiten mit dem Ereignisprotokoll

Um das Ereignisprotokoll anzuzeigen:

1. Bestätigen Sie, dass das Symbol „Scanners“ (Scanner) im Banner ausgewählt ist und die Seite die Liste der Scanner anzeigt.
2. Klicken Sie auf das **Symbol Event Logs** (Ereignisprotokolle) rechts neben dem Scanner.
   Der Bildschirm zeigt alle Fehler und Ereignisse an, seit die Anzeige das letzte Mal geleert wurde. Von diesem Bildschirm aus können Sie Folgendes tun:
   - Klicken Sie auf die Schaltfläche **Download All Logs** (Alle Protokolle herunterladen), um eine .zip-Datei im Download-Ordner des SAM DX-Servers zu speichern.

     *Um die Schaltfläche **Download All Logs** (Alle Protokolle herunterladen) verwenden zu können, muss Ihre Workstation mit dem lokalen Netzwerk Ihrer Einrichtung verbunden sein und Zugang zum SAM DX-Server haben; Sie können nicht von außerhalb des LAN auf den SAM DX-Server zugreifen, um diese Funktion zu nutzen.*
   - Klicken Sie auf **Clear Current Screen** (Aktuelle Anzeige leeren), um die Einträge vom Bildschirm zu entfernen. Beachten Sie, dass hierdurch nicht die Einträge im Protokoll gelöscht werden.

Sichern von Protokolldateien

Wir empfehlen, die auf den SAM DX-Server heruntergeladenen Scanner-Protokolldateien zu sichern und die Sicherungen an einem anderen Ort abseits der Einrichtung aufzubewahren. Wir empfehlen, die Windows-Ereignisprotokolle auf dem SAM DX-Server zu sichern und die Sicherungen an einem anderen Ort abseits der Einrichtung aufzubewahren.

Warnungen bei der Anmeldung

Die Datei „Console.log“ enthält Ereignisse zur Benutzeranmeldung, z. B. erfolgreiche Anmeldungen mit Benutzernamen. Sie enthält außerdem Warnungen über fehlgeschlagene Anmeldungen.

Das Protokoll kann auch „Möglicher unbefugter Zugriff erkannt“ anzeigen, wenn beim Fernzugriff auf den Scanner über SSH Unstimmigkeiten bei der Anmeldung auftreten.

5 Benutzerverwaltung

Dieses Kapitel beschreibt, wie Sie Benutzerkonten für SAM DX konfigurieren.

Bevor ein Benutzer sich bei SAM DX anmelden kann, um die System- und Scanner-Einstellungen anzusehen oder zu ändern, muss er über ein Benutzerkonto verfügen. SAM DX-Benutzerkonten sind gültig für alle Scanner bei SAM DX.

Der Administrator erstellt Konten für alle Benutzer und weist dem Benutzer zu diesem Zeitpunkt eine Rolle zu. Die Rolle des Benutzers legt fest, was dieser Benutzer im System tun kann und was nicht.

Beschreibung der Rollen

Es gibt drei Benutzerrollen:

- Rolle „Operator“ (Bediener)
- Rolle „Lab Admin“ (Labor-Administrator)
- Rolle „Leica Support“ (Leica-Kundendienst)

Rolle	Beschreibung

Rolle „Operator“ (Bediener)	Dies ist eine allgemeine Rolle, die sich für die meisten Benutzer eignet. Benutzer mit der Rolle „Operator“ (Bediener) können die meisten Systemeinstellungen einsehen und Folgendes tun:
	• den Status jedes Scanners anzeigen
	• Systeminformationen für jeden Scanner anzeigen
	  • Seite „Info“
	  • Scanner Statistics (Scanner-Statistiken)
	  • Seite „Settings“ (Einstellungen)
	• das „Event Log“ (Ereignisprotokoll) ansehen
	• das eigene Kennwort ändern
	Bediener können die für einen Scanner festgelegten PINs nicht einsehen oder ändern.
	Bediener können die Benutzerliste nicht einsehen oder Einstellungen für andere Benutzer ändern.

Rolle	Beschreibung

Rolle „Lab Admin“ Labor-Administrator	Diese Rolle bietet administrativen Zugang und eignet sich für Benutzer, die andere Benutzerkonten hinzufügen oder verwalten oder Änderungen am System vornehmen müssen. Zusätzlich zu den einem Bediener offenstehenden Funktionen können Benutzer mit Administratorrolle Folgendes tun:
	• andere Benutzerkonten hinzufügen, bearbeiten und löschen
	• Kennwörter von Benutzern ändern
	• „System Information“ (Systeminformationen) anzeigen und einige Einstellungen bearbeiten
	• die Einstellungen unter „Configuration“ (Konfiguration) bearbeiten:
	  • Images (Bilder)
	  • DSR
	  • Event Handling (Ereignisbehandlung)
	  • PIN-Verwaltung

Rolle „Leica Support“ (Leica-Kundendienst)	Dies ist eine geschützte Rolle, die Sie nicht für Benutzer verwenden können. Diese Rolle (mit dem Benutzernamen „Leica Admin“) kann nicht aus dem System gelöscht werden. Sie wird von Leica-Kundendienstmitarbeitern für die Fehlerbehebung, Wartung und für Reparaturfunktionen verwendet und ist in der Lage, Scanner zum System hinzuzufügen oder sie zu entfernen.

Verwalten von Benutzern

Nur Benutzer mit der Rolle „Lab Admin“ (Labor-Administrator) können die Liste der Benutzer bearbeiten oder bestehende Benutzerkonten bearbeiten.

Einen Benutzer hinzufügen

1. Wählen Sie **Users** (Benutzer) im oberen Menüband auf der Hauptseite.
2. Klicken Sie auf **Add User** (Benutzer hinzufügen) unten auf der Seite mit der Benutzerliste.
3. Geben Sie die Daten des neuen Benutzerkontos ein:
   - Das Feld „Login Name“ (Anmeldename) kann 1 bis 296 Zeichen lang sein und aus Buchstaben, Ziffern und Sonderzeichen bestehen.
   - der vollständige Name des Benutzers
4. Geben Sie ein anfängliches Kennwort für den Benutzer ein. Für Kennwörter gelten folgende Anforderungen:
   - mindestens 10 Zeichen
   - mindestens ein Großbuchstabe und ein Kleinbuchstabe
   - mindestens eine Ziffer
   - mindestens ein Sonderzeichen: ! @ # $ % ^ * oder _
   - unterscheidet sich von den letzten 5 Kennwörtern

5. Wählen Sie eine Rolle: „Lab Admin“ (Labor-Administrator) oder „Operator“ (Bediener).
6. Klicken Sie auf **Save** (Speichern).

Einen Benutzer bearbeiten

1. Wählen Sie **Users** (Benutzer) im oberen Menüband auf der Hauptseite.
2. Klicken Sie auf **Edit** (Bearbeiten) neben dem Namen des Benutzers, den Sie bearbeiten möchten.
3. Geben Sie die neuen Daten ein.
   Beachten Sie, dass Sie die Rolle eines bestehenden Benutzerkontos nicht verändern können.
4. Klicken Sie auf **Save** (Speichern).

Einen Benutzer löschen

1. Wählen Sie **Users** (Benutzer) im oberen Menüband auf der Hauptseite.
2. Klicken Sie auf **Delete** (Löschen) neben dem Namen des Benutzers, den Sie löschen möchten.
3. Bestätigen Sie, dass Sie den Benutzer löschen möchten, oder klicken Sie auf **Cancel** (Abbrechen).

Ein Benutzerkonto entsperren

Nach drei erfolglosen Anmeldeversuchen beim SAM DX-Server sperrt SAM DX den Zugang für diesen Benutzer.

Ein Benutzer mit der Rolle „Lab Admin“ (Labor-Administrator) kann Bedienerkonten entsperren. (Der Benutzer „LeicaAdmin“ (Leica-Administrator) kann alle Konten entsperren.)

1. Wählen Sie **Users** (Benutzer) im oberen Menüband auf der Hauptseite.
2. Klicken Sie auf **Unlock** (Entsperren) neben dem Namen des Benutzerkontos, das Sie entsperren möchten.

Ändern Ihres Kennworts

Nachdem ein Benutzer sich erfolgreich angemeldet hat, kann er sein eigenes Kennwort ändern:

1. Wählen Sie den Benutzernamen im oberen rechten Bereich der Hauptseite aus.
2. Klicken Sie auf den Link **Change Password** (Kennwort ändern).
3. Geben Sie ein neues Kennwort ein. Anforderungen an das Kennwort sind:
   - mindestens 10 Zeichen
   - mindestens ein Großbuchstabe und ein Kleinbuchstabe
   - mindestens eine Ziffer
   - mindestens ein Sonderzeichen: ! @ # $ % ^ * oder _
   - unterscheidet sich von den letzten 5 Kennwörtern
4. Bestätigen Sie das Kennwort und klicken Sie auf **OK**.

6 Cybersicherheits- und Netzwerkrichtlinien

In diesem Kapitel wird behandelt, wie Aperio GT 450 DX und Aperio SAM DX geschützte elektronische Gesundheitsdaten (EPHI) schützen und Cybersicherheitsbedrohungen abwehren. Wir besprechen zudem die Maßnahmen, die Sie ergreifen können, um den SAM DX-Server auf Ihrem Netzwerk zu schützen. Dieses Kapitel bietet Informationen für IT-Netzwerkadministratoren, Aperio-Produktadministratoren und Aperio-Produktendnutzer.

VORSICHT: Lesen Sie alle Richtlinien in diesem Kapitel, um Informationen zum Schutz von Aperio GT 450 DX und Aperio SAM DX vor Bedrohungen der Cybersicherheit zu erhalten.

Die Empfehlungen in diesem Abschnitt beziehen sich auf den Windows-basierten Server, der dem Hosten des SAM DX dient. Die Sicherheits- und Netzwerkeinstellungen werden über das Betriebssystem und die administrativen Tools von Windows konfiguriert. Die Informationen hier dienen ausschließlich Referenzzwecken. Spezifische Anweisungen finden Sie in Ihrer Windows-Dokumentation.

Es kann sein, dass Ihre Einrichtung restriktivere Sicherheitseinstellungen und -konfigurationen benötigt als die hier aufgeführten. Sollte das der Fall sein, benutzen Sie die strikteren Richtlinien und Anforderungen, die von Ihrer Einrichtung vorgegeben sind.

Nach der Installation des Aperio GT 450 DX übergibt der Mitarbeiter von Leica Biosystems Ihrem IT-Personal sensible Cybersicherheitselemente wie SSL-Zertifikatsdaten, Festplatten-Verschlüsselungsschlüssel für den SAM DX-Server usw. Diese Elemente gehen in das Eigentum des Kunden über, und es liegt in seiner Verantwortung, diese Informationen zu schützen.

Aperio GT 450 DX und Aperio SAM DX Cybersicherheitsfunktionen

Die Cybersicherheitsfunktionen des Aperio GT 450 DX-Produkts schützen auch bei einer Gefährdung der Cybersicherheit wichtige Funktionen. Diese beinhalten:

- Um Schwachstellen in der Cybersicherheit zu verringern, sind die jeweiligen Betriebssysteme auf der Aperio GT 450 DX VPU und dem SAM DX-Server mit CIS (Center for Internet Security) Benchmarks verstärkt gesichert.
- Der Aperio GT 450 DX-Scanner und SAM DX sind nicht für die Speicherung sensibler Daten vorgesehen, sondern nur für den Export/Upload von Daten zu verbundenen Anwendungen auf separaten Netzwerkservern. Die Verbindung zwischen dem Aperio GT 450 DX-Scanner und dem SAM DX-Server wird über eine verschlüsselte, sichere SSL/TLS-Verbindung authentifiziert.
- Die Funktion „Listing erlauben/verweigern“ wird auf dem Aperio GT 450 DX-Scanner verwendet und für die Verwendung auf dem SAM DX-Server empfohlen. Dadurch wird verhindert, dass nicht autorisierte Software auf diesen Komponenten ausgeführt werden kann.

- Zur täglichen Wartung des Aperio GT 450 DX-Scanners gehört ein täglicher Neustart des Geräts. (Näheres dazu siehe *Aperio GT 450 DX Benutzerhandbuch*.) Dadurch wird die Firmware aktualisiert.
- Die GT 450 DX-Datei „Console.log“ enthält Ereignisse zur Anmeldung mit Benutzernamen. Sie kann auch „Möglicher unbefugter Zugriff erkannt“ anzeigen, wenn beim Fernzugriff auf den Scanner über SSH Unstimmigkeiten bei der Anmeldung auftreten. Einzelheiten zum Herunterladen der Protokolldateien finden Sie unter *„Arbeiten mit dem Ereignisprotokoll“ auf Seite 32*.

Datenschutz

Daten im Ruhezustand werden durch Verschlüsselung geschützt. Aufgrund der Einschränkungen des Betriebssystems können geschützter Gesundheitsdaten (Protected Health Information, PHI) in Übertragung jedoch nicht geschützt werden. Leica Biosystems empfiehlt, Daten während der Übertragung durch die Verwendung von SSL mit starken Sicherheitsprotokollen wie Transport Layer Security (TLS) oder durch Verschlüsselung auf Netzwerkebene wie IPSec oder SSH-Tunneling zu schützen.

Physische Sicherheitsvorkehrungen für Aperio GT 450 DX

- Schützen Sie den Aperio GT 450 DX-Scanner vor unbefugtem Zugriff, indem Sie den physischen Zugang zu diesem einschränken.

Schutz des SAM DX-Servers

Die folgenden Abschnitte beschreiben Empfehlungen zum Schutz des SAM DX-Servers.

Kennwort-, Anmeldungs- und Benutzerkonfigurationsschutzmaßnahmen

- Wir empfehlen die folgenden Anforderungen an die Kennwortkomplexität für Benutzer, die sich beim webbasierten SAM DX-Client anmelden:
  - Kennwörter müssen mindestens 8 Zeichen enthalten, darunter:
    - einen Großbuchstaben
    - eine numerische Ziffer
    - einen Kleinbuchstaben
    - eines der folgenden Sonderzeichen: ! @ # $ % ^ * _
  - die fünf zuletzt verwendeten Kennwörter dürfen nicht wiederverwendet werden
- Nach drei ungültigen Anmeldeversuchen wird das Benutzerkonto gesperrt. Der Benutzer kann sich an einen SAM DX-Administrator wenden, um das Konto entsperren zu lassen.
- Wir empfehlen, die zur Anmeldung bei SAM DX verwendeten Workstations so zu konfigurieren, dass sich Bildschirmanzeigen nach 15-minütiger Inaktivität ausschalten und der Benutzer sich nach dieser Zeit erneut anmelden muss.
- Wenn Sie Benutzer zu SAM DX hinzufügen, benutzen Sie aus Sicherheitsgründen keine Benutzernamen wie „Admin“, „Administrator“ oder „Demo“.

Physische Schutzmaßnahmen für den SAM DX-Server

- Schützen Sie den SAM DX-Server und die zur Anmeldung bei SAM DX verwendeten Client-Workstations vor unbefugtem Zugriff, indem Sie den physischen Zugang zu ihnen einschränken.
- Um den SAM DX-Server vor Malware-Angriffen zu schützen, gehen Sie beim Einsetzen von USB-Laufwerken und anderen Wechselmedien mit Vorsicht vor. Ziehen Sie die Deaktivierung von nicht verwendeten USB-Anschlüssen in Erwägung. Wenn Sie ein USB-Laufwerk oder ein anderes Wechselmedium anschließen, sollten Sie die Geräte mit einem Anti-Malware-Programm scannen.

Administrative Schutzmaßnahmen für den SAM DX-Server

- Richten Sie die Benutzer-Genehmigungen ein, die es ihnen ermöglichen, nur auf die Teile des Systems zuzugreifen, die sie für ihre Arbeit benötigen. Für den SAM DX-Server sind die Benutzerrollen „Operator“ (Bediener) und „Lab Admin“ (Labor-Administrator), die unterschiedliche Berechtigungen haben.
- Schützen Sie den SAM DX und die Client-Workstations vor unbefugtem Zugriff, indem Sie Standard-IT-Techniken benutzen. Beispiele:
  - Firewalls – Wir empfehlen Ihnen, die Windows-Firewall auf Client-Workstations zu aktivieren.
  - „Listing erlauben“, ein administratives Tool, das Sie nur autorisierte Programme aufrufen lässt, sollte auf dem SAM DX-Server implementiert sein.
- Leica Biosystems empfiehlt die Verwendung von SQL Standard (2019 oder höher) oder Enterprise SQL Server, die Datenbankverschlüsselung unterstützen.
- Gehen Sie bei der Pflege und Verwendung von Servern mit der üblichen Sorgfalt vor. Eine Unterbrechung der Netzwerkverbindungen oder das Ausschalten der Server während der Datenverarbeitung (z. B. bei der Analyse von Digitalbildern oder der Erzeugung von Prüfberichten) kann zu Datenverlust führen.
- Ihre IT-Abteilung muss den Server warten und Sicherheitspatches und Hotfixes von Windows und Aperio anwenden, die für das System eventuell verfügbar sind.
- Sie sollten einen Server auswählen, der so konfiguriert werden kann, dass er Eindringungsversuche wie Zufallskennwort-Angriffe erkennt, Konten automatisch sperrt, die für solche Angriffe benutzt werden, und Administratoren über solche Ereignisse benachrichtigt.
- Befolgen Sie die Sicherheitsrichtlinie Ihrer Institution, um in der Datenbank gespeicherte Daten zu schützen.
- Wir empfehlen Ihnen, „Listing erlauben“ auf dem Server zu implementieren, so dass nur autorisierte Anwendungen ausgeführt werden können.

  Wenn Sie „Listing erlauben“ nicht benutzen, sollten Sie unbedingt eine Antivirus-Software auf dem Server installieren. Lassen Sie den Antivirus-Scan alle 30 Tage laufen.

  Wir empfehlen Ihnen außerdem, die Antivirus-Software so zu konfigurieren, dass Dateien vom Typ .SVS und .DICOM ebenso wie der Dateispeicher vom „Scannen bei Zugriff“ ausgeschlossen werden, da diese Dateien sehr groß sein können und regelmäßig aufgerufen werden, während sie gescannt werden und während Benutzer die Digitalbilder anzeigen. Viren-Scans sollten auf einen Zeitpunkt außerhalb der Hauptarbeitszeiten terminiert werden, da sie CPU-intensiv sind und das Scannen stören können.
- Sichern Sie die Festplatten im Server regelmäßig.

- Für die SAM DX-DSR-Netzwerkverbindung empfehlen wir Ihnen, einen Speicherserver zu benutzen, der das SMB3-Netzwerk-Protokoll zum Schutz von Daten während der Übertragung unterstützt. Wenn der DSR-Server SMB3 oder höher nicht unterstützt, ist eine Schadensbegrenzung erforderlich, um die Daten während der Übertragung zu schützen.
- Wir empfehlen Ihnen, die Inhalte der Server-Festplatten zu verschlüsseln.
- Die File-Shares auf dem Server sollten unter Verwendung von akzeptierten IT-Praktiken vor unbefugtem Zugriff geschützt werden.
- Sie sollten Windows Event-Protokollierung auf Ihrem Server aktivieren, um Benutzerzugriffe und Änderungen an Datenordnern aufzuzeichnen, die Patienteninformationen und -bilder enthalten. Sie sollten auch eine Sicherungskopie der Protokolldateien erstellen und diese an einem Ort abseits der Einrichtung aufbewahren. Siehe *„Arbeiten mit dem Ereignisprotokoll“ auf Seite 32*.

Verwendung von Standardsoftware

Bei der Durchführung von Analysen der Cybersicherheit sollten Sie berücksichtigen, welche Softwarekomponenten von Drittanbietern von der Leica Biosystems-Software verwendet werden. Leica Biosystems führt Listen über alle von Aperio GT 450 DX und SAM DX verwendeten Standardsoftwares (OTS, Off the Shelf Software). Wenn Sie Informationen zu verwendeten OTS wünschen, wenden Sie sich bitte an Ihren Vertriebs- oder Kundenbetreuer von Leica Biosystems und fragen Sie nach den Software-Stücklisten für Aperio GT 450 DX und SAM DX.

Support und Cybersicherheitspatches

Beachten Sie, dass technischer Support und Cybersicherheitspatches für Aperio GT 450 DX und Aperio SAM DX nach der im *Aperio GT 450 DX Benutzerhandbuch* angegebenen Produktlebensdauer möglicherweise nicht mehr verfügbar sind.

A Fehlerbehebung

Dieser Anhang enthält Ursachen und Lösungen für Probleme mit dem SAM DX-Server und verwandten Komponenten. Er enthält ebenfalls häufige Fehlerbehebungsverfahren, die eventuell vom Labor-Administrator des Aperio GT 450 DX durchgeführt werden müssen. Für allgemeine Fehlerbehebungsinformationen für den Scanner-Bediener siehe *Aperio GT 450 DX Benutzerhandbuch*.

Fehlerbehebung im Scanner Administration Manager DX (SAM DX)-Server

Problem	Ursache	Lösung
Fehlermeldung „Credentials are Invalid“ (Ungültige Anmeldedaten) während der Anmeldung	Die von SAM DX genutzte DataServer-Instanz ist nicht aktiv.	Starten Sie den DataServer-Dienst auf dem SAM DX-Server. Siehe *„Neustart des DataServer“ auf Seite 42*.
	Ungültige Anmeldedaten	Überprüfen Sie die Feststelltaste usw. Bestätigen Sie die Anmeldedaten mit dem Administrator.
Nach einem Update sind neue Funktionen nicht in der SAM DX-Benutzeroberfläche verfügbar.	Anwendung ist im Browser-Cache gespeichert.	Beenden Sie SAM DX und leeren Sie dann Ihren Browser-Cache.
Der Scanner ist eingeschaltet und mit SAM DX verbunden (erhält seine Einstellungen), aber SAM DX zeigt den Scanner als offline an und es werden keine statistischen Daten (Anzahl der Scans usw.) gemeldet.	Mirth läuft nicht auf dem SAM DX-Server.	Siehe *„Sicherstellen, dass Mirth aktiv ist“ auf Seite 42*.
	Ports sind nicht geöffnet.	Stellen Sie sicher, dass Port 6663 in der Firewall geöffnet ist und vom Scanner erreicht werden kann.

Problem	Ursache	Lösung
Die Scanner-Protokolldateien befinden sich nicht im Scanner-Protokollordner.	Mirth läuft nicht auf dem SAM DX-Server.	Siehe *„Neustart des DataServer“ unten*.
	Protokollausgabeordner ist fehlerhaft konfiguriert.	Überprüfen Sie die Registerkarte „Configuration Map“ (Konfigurationsplan) unter „Settings“ (Einstellungen) (AppLog_Dir).
	Mirth-Fehler	Überprüfen Sie das Mirth-Dashboard auf Fehler bezüglich des Kanals „ScannerAppLogWriter“ und lesen Sie das Mirth-Fehlerprotokoll für weitere Informationen.
	Ports sind nicht geöffnet.	Stellen Sie sicher, dass Port 6663 in der Firewall geöffnet ist und vom Scanner erreicht werden kann.
Die SAM DX-GUI ist nicht erreichbar oder gibt beim Verbindungsversuch einen Fehlercode zurück.	IIS-Fehler	Stellen Sie sicher, dass IIS und die Webseite aktiv sind und dass die Ports, auf denen SAM DX aktiv ist, in der Firewall geöffnet sind.
	Konfigurationsfehler bei anonymer Authentifizierung in IIS.	Überprüfen Sie die IIS-Konfiguration. Siehe *„IIS-Konfigurationsfehler“* unten.

Neustart des DataServer

Öffnen Sie auf dem Server den Dienst-Manager und stellen Sie sicher, dass der Dienst „ApDataService“ aktiv ist. Falls der Dienst nicht gestartet werden kann oder das Problem weiterhin besteht, sehen Sie sich die DataServer-Protokolle für weitere Informationen an (üblicherweise in C:\Program Files (x86)\Aperio\DataServer\Logs).

Sicherstellen, dass Mirth aktiv ist

Stellen Sie sicher, dass der Mirth Connect-Server auf dem Server aktiv ist. Falls er aktiv ist, stellen Sie sicher, dass die „Konfigurationsplan-Einstellungen“ so konfiguriert sind, dass sie zum richtigen DataServer-Host (SAM DX_Host) und -Port (SAM DX_Port) führen und die korrekte SSL- oder Nicht-SSL-Verbindung (SAM DX_UriSchema) verwenden. Falls das Dashboard in Mirth Connect Fehler im Kanal „ScannerEventProcessor“ meldet, sehen Sie sich für weitere Details die Mirth-Fehlerprotokolle an. Falls der DataServer nicht aktiv ist, könnte das zu Mirth-Kanalfehlern führen. Stellen Sie sicher, dass Port 6663 in der Firewall geöffnet ist und vom Scanner erreicht werden kann.

IIS-Konfigurationsfehler

Um diese Einstellung zu überprüfen, öffnen Sie die Webseite in IIS und gehen Sie zur Einstellung „Authentication“ (Authentifizierung). Finden und bearbeiten Sie den Eintrag „Anonymous Authentication“ (Anonyme Authentifizierung) und stellen Sie sicher, dass der spezifische Benutzer auf „IUSR“ (kein Kennwort) festgelegt ist. Falls die Seite aktiv ist und alle Einstellungen korrekt sind, prüfen Sie bitte die IIS-Protokolle für weitere Details.

B Zusammenfassung der Scanner-Einstellung und Konfigurationsoptionen

Dieser Anhang enthält eine Liste aller Einstellungen und Konfigurationsoptionen. Verwenden Sie diese Tabellen als Checkliste, während Sie die Informationen sammeln, die Sie beim Hinzufügen oder Neukonfigurieren eines Scanners benötigen. Beachten Sie, dass die meisten dieser Einstellungen und Konfigurationsoptionen während der Installation von einem Leica Biosystems-Mitarbeiter für Sie festgelegt werden.

Grundlegende Scanner-Informationen

Labor-Administratoren können den Namen des Scanners auf der Scanner-Seite wählen, um die Scanner-Basiseinstellungen anzuzeigen. (Bediener können einige der Einstellungen von der Seite „System Information“ (Systeminformationen) sehen.) Alle in einem grauen Kasten dargestellten Einstellungen können von Labor-Administratoren und Bedienern nicht verändert werden.

Einstellung	Beschreibung	Anzeigen/Bearbeiten	
		Administrator	Bediener
Mac Address (MAC-Adresse)	Während der Installation festgelegt.	Ansicht	Keine
Hostname	Während der Installation festgelegt.	Ansicht	Keine
Friendly Name (Benutzerfreundlicher Name)	Vom örtlichen Administrator festgelegter Name oder Beschreibung für den Scanner, wird auf der Startseite „Scanners“ (Scanner) angezeigt.	Anzeigen/ Bearbeiten	Keine
Model (Modell)	Aperio GT 450 DX	Ansicht	Keine
Serial Number (Seriennummer)	Während der Installation festgelegt und beim Start überprüft.	Ansicht	Ansicht
Hardware Version (Hardwareversion)	Beim Start überprüft	Ansicht	Ansicht
Language (Sprache)	Steuert die für Menüs und Meldungen im Scanner verwendete Sprache.	Anzeigen/ Bearbeiten	Keine
Zusätzliche Versionsinformationen	Verfügbar für den Lab Administrator (Labor-Administrator) auf der Seite „Scanner Information“ (Scanner-Informationen). Einige dieser Felder werden auch dem Bediener auf der Seite „System Information“ (Systeminformationen) angezeigt.	Ansicht	Ansicht

Scanner-Konfiguration

Verwenden Sie die folgende Tabelle, um die Informationen zu sammeln, die Sie für jeden Scanner im System benötigen werden. Nachdem der Kundendienstmitarbeiter von Leica Ihren Scanner installiert, sollten Sie die Einstellungen gegebenenfalls für die spätere Verwendung aufzeichnen.

Option	Beschreibung	Anzeigen/Bearbeiten	
		Administrator	Bediener
Images Configuration (Bilder-Konfiguration)			
Scan Scale Factor (Scan-Skalierungsfaktor)	Nur für den internen Gebrauch. Nur ändern, wenn Sie dazu von Leica Biosystems Technical Support aufgefordert werden.	Anzeigen/ Bearbeiten	Keine
Hostname	Name des Servers, auf dem der DICOM-Bildkonvertierer ausgeführt wird. • Verwenden Sie **ScannerAdmin**, falls der DICOM-Konvertierer auf dem SAM DX-Server installiert ist. • Andernfalls verwenden Sie den Hostnamen des Servers, auf dem der DICOM-Konvertierer installiert ist.	Anzeigen/ Bearbeiten	Keine
Port	Der bei der Installation festgelegte Port, den der DICOM-Konvertierer verwendet. Der Standard ist 2762.	Anzeigen/ Bearbeiten	Keine
Title (Bezeichnung)	Nur für den internen Gebrauch. Nur ändern, wenn Sie dazu von Leica Biosystems Technical Support aufgefordert werden.	Anzeigen/ Bearbeiten	Keine
File Location (Dateipfad)	Der vollständige Pfad zur Dateifreigabe, auf der der Konvertierer die Bilder nach der Konversion speichert. Dies ist ein Ort im Netzwerk, an dem konvertierte SVS-Dateien gespeichert werden.	Anzeigen/ Bearbeiten	Keine
Image filename format (Format des Bilddateinamens)	Legt Basisdateiname für die gescannte Bilddatei fest.	Anzeigen/ Bearbeiten	Keine
Barcode value identifier (Barcodewert-Kennung)	Legt Basisformat für den Barcode fest.	Anzeigen/ Bearbeiten	Keine
DSR Configuration (DSR-Konfiguration)			
Hostname	Hostname des Servers, auf dem die Metadaten gespeichert werden. (Die Einstellung „File Location“ (Dateipfad) oben ist die Dateifreigabe, auf der Bilder gespeichert werden.)	Anzeigen/ Bearbeiten	Keine
Port	Der verschlüsselte Port wird für DSR verwendet. Der Standard ist 44386.	Anzeigen/ Bearbeiten	Keine

Option	Beschreibung	Anzeigen/Bearbeiten	
		Administrator	Bediener
Event Handling Configuration (Konfiguration der Ereignishandhabung)			
Hostname	Name des Servers, auf dem der Mirth Connect Server ausgeführt wird. • Verwenden Sie **ScannerAdmin**, falls der Mirth Connect Server auf dem SAM DX-Server installiert ist. • Andernfalls verwenden Sie den Hostnamen des Servers, auf dem die für SAM DX genutzte Mirth-Instanz installiert ist.	Anzeigen/ Bearbeiten	Keine
Log Port (Protokoll-Port)	Der bei der Installation festgelegte Port, den Mirth für Protokolldaten verwendet. Der Standard ist 6662.	Anzeigen/ Bearbeiten	Keine
Event Port (Ereignis-Port)	Der bei der Installation festgelegte Port, den Mirth für Ereignisdaten verwendet. Der Standard ist 6663.	Anzeigen/ Bearbeiten	Keine
PIN Management (PIN-Verwaltung)			
Login Timeout (Zeitüberschreitung für Anmeldung)	Zeitintervall (in Minuten), nach dem der Scanner den Bildschirm und die Steuerfelder sperrt, wenn für diesen Zeitraum keine Bedienerinteraktion stattgefunden hat. Gültige Werte sind alle ganzen Zahlen größer null.	Anzeigen/ Bearbeiten	Keine
Edit Settings: Pin (Einstellungen bearbeiten: PIN)	Ein 5-stelliger Code zum Entsperren des Scanners. Nur Ziffern	Anzeigen/ Bearbeiten	Keine
Edit Settings: Description (Einstellungen bearbeiten: Beschreibung)	Identifizierende Angaben für die PIN. Dies ist ein Feld mit einer allgemeinen Beschreibung und kann Ziffern, Buchstaben sowie Satzzeichen enthalten.	Anzeigen/ Bearbeiten	Keine
Time Zone (Zeitzone)			
Scanner time zone (Scanner-Zeitzone)	Vom SAM DX-Administrator konfiguriert	Anzeigen/ Bearbeiten	Keine

C Bindung eines SSL-Zertifikats an Aperio SAM DX

Der Zugriff über die Aperio SAM DX-Benutzeroberfläche ist per SSL abgesichert. Bei der Installation werden selbstsignierte SSL-Zertifikate installiert. Um Sicherheitsmeldungen des Browsers zu vermeiden, können Kunden ihre eigenen Sicherheitszertifikate verwenden.

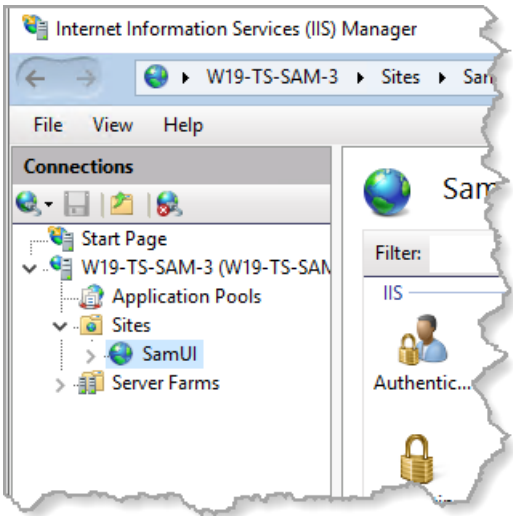
Wenn Ihre Einrichtung ihr eigenes SSL-Zertifikat zur Sicherung der Aperio SAM DX-Benutzeroberfläche verwenden möchte, muss dieses SSL-Zertifikat importiert und mit SAM DX verknüpft werden.

In diesem Abschnitt wird beschrieben, wie Sie die SSL-Zertifikatsbindung aktualisieren, um die SAM DX-Benutzeroberfläche in Microsoft IIS zu sichern.

Befolgen Sie die Anweisungen des SSL-Zertifikatsanbieters, um das SSL-Zertifikat in Microsoft IIS zu importieren. Befolgen Sie dann die nachstehenden Anweisungen, um das Zertifikat an SAM DX zu binden.

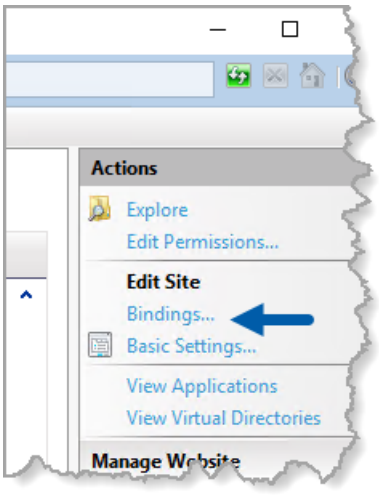
Zuweisen des SSL-Zertifikats zu Ihrer Website

1. Klicken Sie auf dem SAM DX-Server auf die Windows-Schaltfläche **Start** und geben Sie **inetmgr** ein.
2. Weisen Sie das SSl-Zertifikat Ihrer Website zu, indem Sie den Unterabschnitt **Sites** (Website) im Menü **Connections** (Verbindungen) auf der linken Seite erweitern und Ihre Website auswählen:

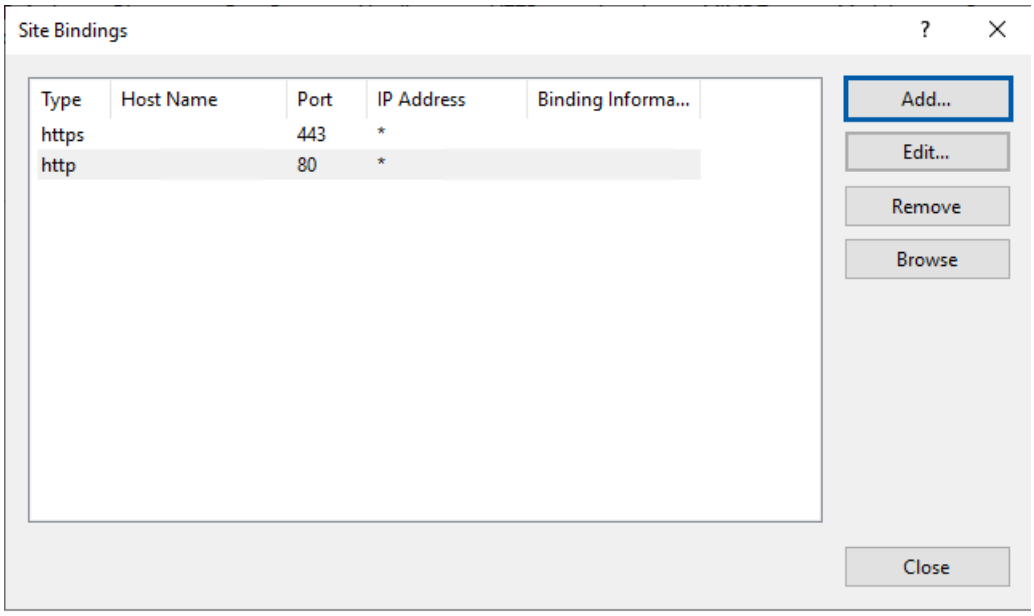


Bindung des SSL-Zertifikats

1. Suchen Sie im Bereich „Actions“ (Aktionen) auf der rechten Seite das Menü **Edit Site** (Site bearbeiten) und wählen Sie die Option **Bindings** (Bindungen) aus.

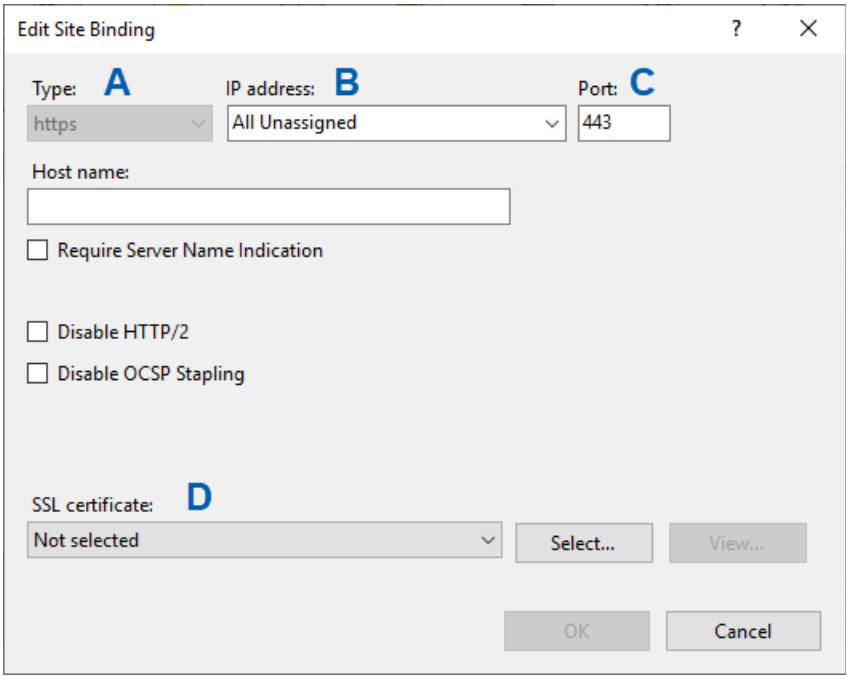


2. Klicken Sie auf der rechten Seite des Fensters „Site Bindings“ (Sitebindungen) auf **Add** (Hinzufügen):

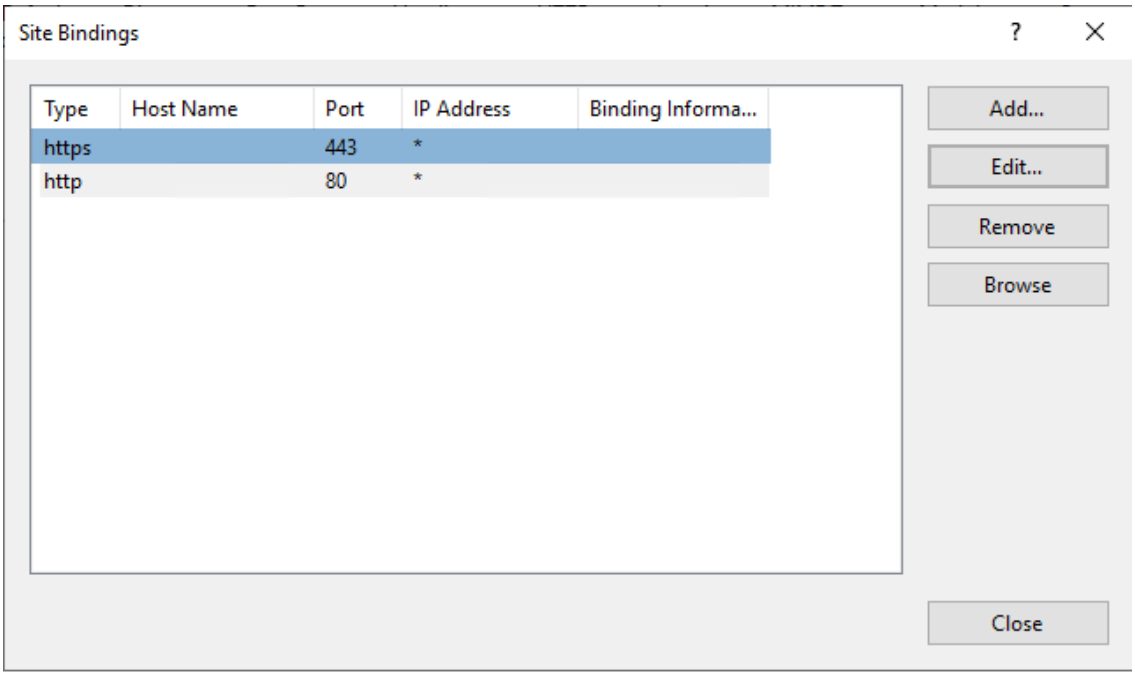


3. Ändern Sie im Fenster „Add Site Binding“ (Sitebindung hinzufügen) die unten aufgeführten Felder:
   a. Wählen Sie im Feld „Type“ (Typ) **https** aus.
   b. Wählen Sie im Feld „IP address“ (IP-Adresse) die IP-Adresse Ihrer Website oder **All Unassigned** (Keine zugewiesen) aus.
   c. Tragen Sie im Feld „Port“ den Port 443 (Standard) ein.
   d. Wählen Sie im Feld „SSL certificate“ (SSL-Zertifikat) das zuvor importierte Zertifikat aus, das Sie anhand des benutzerfreundlichen Namens identifizieren können.

*Das Kontrollkästchen **Require Server Name Indication** (Angabe des Servernamens erfordern) muss aktiviert werden, wenn mehrere SSL-Zertifikate auf dem Server vorhanden sind.*



4. Klicken Sie auf **OK**, damit der neue https-Eintrag im Fenster „Site Bindings“ (Sitebindungen) erscheint:



Das Zertifikat ist nun installiert und die SAM DX-Benutzeroberfläche sollte über HTTPS zugänglich sein.

Index

K

L

M

N

P

R

S

V

W

Z