Haftungsausschluss

Rechtlicher Hinweis

Dieser Leitfaden und seine Inhalte (der „Leitfaden") werden von NXGEN bereitgestellt. Alle Rechte am Leitfaden und am darin verkörperten geistigen Eigentum — einschließlich, aber nicht beschränkt auf Marken, Handelsnamen, Logos und ähnliche Kennzeichen im oder am Leitfaden — sind gesetzlich geschützt. Sämtliche Rechte, Ansprüche und Anteile am Leitfaden und an damit verbundenen Schutzrechten verbleiben bei NXGEN und seinen Lizenzgebern.

Der Leitfaden wird unentgeltlich, „wie besehen" und ausschließlich zu Informationszwecken bereitgestellt, ohne jegliche Gewährleistung. Er ist weder dazu bestimmt noch geeignet, ein Rechtsverhältnis zwischen dem Leser und NXGEN oder seinen verbundenen Unternehmen zu begründen, einschließlich, aber nicht beschränkt auf Verpflichtungen von NXGEN oder seinen verbundenen Unternehmen gegenüber dem Leser.

Die Verpflichtungen von NXGEN und seinen verbundenen Unternehmen in Bezug auf von einem Kunden erworbene NXGEN-Produkte oder -Dienstleistungen richten sich ausschließlich nach den Bedingungen des Vertrags, unter dem diese Produkte oder Dienstleistungen erworben wurden.

Zur Klarstellung

Der Leser trägt das gesamte Risiko hinsichtlich der Nutzung, der Ergebnisse und der Leistung des Leitfadens. Soweit gesetzlich zulässig, schließt NXGEN alle Gewährleistungen aus, ob gesetzlich, ausdrücklich oder stillschweigend — einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck, des Rechtsbestands und der Nichtverletzung von Rechten Dritter — sowie jegliche Haftung oder Gewährleistung aus Vorschlägen, Spezifikationen oder Mustern im Zusammenhang mit dem Leitfaden.

Rollen und Berechtigungen

Updated 16 August 2026

Was RBAC tut

Role-Based Access Control (RBAC) in GCXONE gibt Administratoren eine detaillierte Kontrolle darüber, was Benutzer tun können und welche Entitäten sie sehen können.

> Schlüsselunterscheidung: Entitätszugriff vs. Berechtigungen
>
> Entitätszugriff und Berechtigungen sind separate Konzepte in GCXONE. Berechtigungen (konfiguriert in der Rolle) bestimmen, WELCHE Aktionen ein Benutzer ausführen kann. Der Entitätszugriff bestimmt, WELCHE Kunden, Standorte, Geräte und Sensoren sie sehen können. Die Anpassung auf Benutzerebene erfolgt nur über den Entitätszugriff – es gibt keine Außerkraftsetzung von Berechtigungen auf Benutzerebene.

Warum es wichtig ist

- „Ich muss zwischen mehreren Seiten wechseln, um zu sehen, welchen Zugriff eine Rolle tatsächlich gewährt."
- „Das Erstellen einer neuen Rolle dauert mit zu vielen Konfigurationsschritten ewig"
- „Ich kann nicht schnell erkennen, welche Berechtigungen meine Benutzer haben"
- „Zwei Benutzer in derselben Rolle benötigen Zugriff auf verschiedene Kunden, aber ich muss für jeden separate Rollen erstellen."

Wie es funktioniert

Eine Rolle ist die Kerneinheit der Zugriffskontrolle in GCXONE. Jede Rolle vereint drei Elemente:

Rolleninformationen und Benutzer: Grundlegende Rollendetails (Name, Beschreibung, Standardrollenumschaltung) und die dieser Rolle zugewiesenen Benutzer.

Modulberechtigungen: Auf welche Plattformmodule Benutzer zugreifen können und welche spezifischen Funktionen in jedem aktiviert sind. Berechtigungen bestimmen, WAS ein Benutzer tun kann.

Entitätszuweisungen: Auf welche Kunden, Standorte, Geräte und Sensoren Benutzer zugreifen können. Der Entitätszugriff bestimmt, WO ein Benutzer agieren kann. Entitätszuweisungen können auf zwei Ebenen konfiguriert werden:

- Entitäten auf Rollenebene: Entitäten, die innerhalb der Rolle selbst zugewiesen sind und von allen Benutzern in der Rolle gemeinsam genutzt werden
- Entitäten auf Benutzerebene: Entitäten, die einzelnen Benutzern über „Entitätszugriff bearbeiten“ zugewiesen werden, sodass verschiedene Benutzer in derselben Rolle auf verschiedene Kunden oder Standorte zugreifen können

> Tip
>
> Wenn bisher zwei Benutzer dieselben Berechtigungen benötigten (z. B. Administratorzugriff), aber unterschiedliche Kunden verwalteten, mussten Sie zwei separate Rollen erstellen. Erstellen Sie nun eine Rolle und passen Sie den Entitätszugriff pro Benutzer über „Entitätszugriff bearbeiten“ an.

Entitätshierarchie

GCXONE organisiert Entitäten in einer hierarchischen Struktur. Der Dienstanbieter ist das Konto der obersten Ebene (Ihr Mandant), und alle Entitäten sind darunter verschachtelt: Dienstanbieter → Kunde → Standort → Gerät → Sensor.

Kaskadierende Auswahl: Wenn Sie einen Kunden auswählen, werden automatisch alle darunter liegenden Standorte, Geräte und Sensoren einbezogen. Dadurch wird sichergestellt, dass neue Entitäten

automatisch einbezogen werden, wenn der Schalter „Untergeordnete Elemente einbeziehen“ verwendet wird, und die Konfiguration vereinfacht wird.

Berechtigungsauflösung : Wenn ein Benutzer mehrere Rollen hat (direkte Zuweisungen + Gruppenmitgliedschaften), werden alle Berechtigungen additiv kombiniert. Änderungen werden innerhalb von 5 Sekunden auf Web- und mobilen Plattformen wirksam.

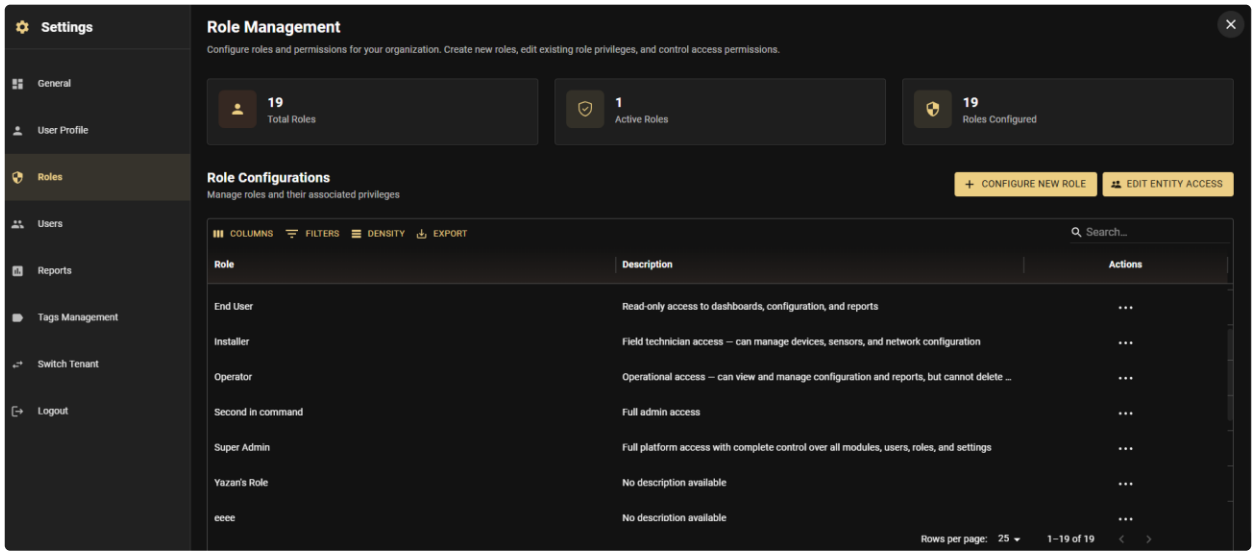
Schlüsselfunktionen

Standardrollen

GCXONE enthält vorkonfigurierte Rollen, um Ihnen den schnellen Einstieg zu erleichtern. Jede Rolle verfügt über einen definierten Satz an Modulberechtigungen. Der Entitätszugriff kann pro Benutzer weiter angepasst werden.

- Super Admin – Vollständiger Plattformzugriff mit vollständiger Kontrolle über alle Module, Benutzer, Rollen und Einstellungen. Vollständiger administrativer Zugriff auf alle Systemfunktionen. Kann alle Benutzer, Rollen und Berechtigungen verwalten. Voller Zugriff auf alle Entitäten. Konfigurieren Sie systemweite Einstellungen und Prüfprotokolle. Ein Superadministrator pro Mandant. Kann nicht gelöscht werden.
- Administrator – Administratorzugriff – kann Benutzer, Rollen, Konfiguration und Berichte verwalten, jedoch nicht die Abrechnung. Verwalten Sie Benutzer und Rollenzuweisungen. Systemeinstellungen konfigurieren. Erstellen und verwalten Sie Entitätsgruppen. Audit-Protokolle und Berichte anzeigen. Auf die Abrechnung kann nicht zugegriffen werden. Kritische Systemkomponenten können nicht gelöscht werden.
- Operator – Betriebszugriff – kann Konfigurationen und Berichte anzeigen und verwalten, aber keine Benutzer/Rollen löschen oder verwalten. Tägliche Überwachung und Alarmverarbeitung. Dashboards und Konfiguration anzeigen. Berichte erstellen und anzeigen. Erledigung operativer Aufgaben. Systemkomponenten können nicht gelöscht werden. Eingeschränkte Verwaltungsfunktionen.

- Installer – Zugriff für Außendiensttechniker – kann Geräte, Sensoren und Netzwerkkonfiguration verwalten. Verwalten Sie physische Geräte und Sensoren. Konfigurieren Sie die Netzwerkeinstellungen. Hardware installieren und einrichten. Beheben Sie Geräteprobleme. Benutzer oder Rollen können nicht verwaltet werden.
- Endbenutzer – Lesezugriff auf Dashboards, Konfiguration und Berichte. Dashboards und Grundkonfiguration anzeigen. Greifen Sie auf grundlegende Berichte zu. Zeigen Sie zugewiesene Kameras und Geräte an. Aktivieren/Deaktivieren für zugewiesene Geräte/Standorte. Keine Möglichkeit, Einstellungen zu ändern oder das System zu verwalten.



Sie können diese Standardrollen unverändert verwenden, sie anpassen oder neue Rollen von Grund auf erstellen.

Modulberechtigungen

Privilegien werden nach Plattformmodul organisiert. Jedes Modul verfügt über eine umschaltbare Zugriffsseite und detaillierte Funktionseinstellungen. Berechtigungen bestimmen, WELCHE Aktionen ein Benutzer auf der Plattform ausführen kann.

- Dashboard – Umschalten der Zugriffsseite, Kontenfilter, Funktionsfilter
- Management-Einblicke – Rolle aktivieren, Rolle bearbeiten und zusätzliche Analysefunktionen

- Konfiguration – Mobile Benutzer, Rollen, SubAnalytics, Health Check, Kundengruppen, Sensortabelle, Audits, Händlertabelle, Dienstanbietertabelle, IoT, Gruppen-/Stufentabelle, Kundengruppe, Dienstanbieter, Kunde, Standort, Konfigurations-Dashboard
- Suche nach Videoaktivitäten – Gespeichert bearbeiten, Filter verwenden, Live, Wiedergabe, Filter bearbeiten, Alarmfilter
- Marktplatz – Pulsansicht, Rollen, Zeitsynchronisierung, Gesundheitsprüfung, Timer-Zählung, Zen-Modus, Massenimport
- Video-Viewer – Videosteuerung, Funktionsumschaltung
- Alarmmanager – Videosteuerung, Funktionsumschaltung
- Karte – Karte bearbeiten, Sensor hinzufügen, IO hinzufügen, IO bearbeiten, Überprüfung verwalten, IO verwalten, Video Live, Live-Stream-Ansicht, Wandmonitor, Dashboard anzeigen

Jedes Modul verfügt über die Option „Alle auswählen/Alle entfernen“ für eine schnelle Massenkonfiguration sowie über einen Zugriffsseitenschalter, der das gesamte Modul aktiviert oder deaktiviert.

Entitätszugriff: Drei Modi

Beim Konfigurieren des Entitätszugriffs während der Rollenerstellung (oder -bearbeitung) stehen drei Modi zur Verfügung. Der Entitätszugriff bestimmt, WO ein Benutzer agieren kann – er steuert, welche Kunden, Standorte, Geräte und Sensoren für den Benutzer sichtbar und zugänglich sind.

- Kein Entitätszugriff – Benutzer haben standardmäßig keinen Entitätszugriff. Muss jedem Benutzer über „Entitätszugriff bearbeiten“ zugewiesen werden. Am besten geeignet für: Gemeinsame Rolle mit individuellen Entitätszuweisungen.
- Ausgewählte Entitäten – Benutzer sind auf die speziell ausgewählten Entitäten (mit oder ohne untergeordnete Elemente) beschränkt. Geeignet für: Bestimmte Unterlisten oder Mandanten mit identischem Zugriff.

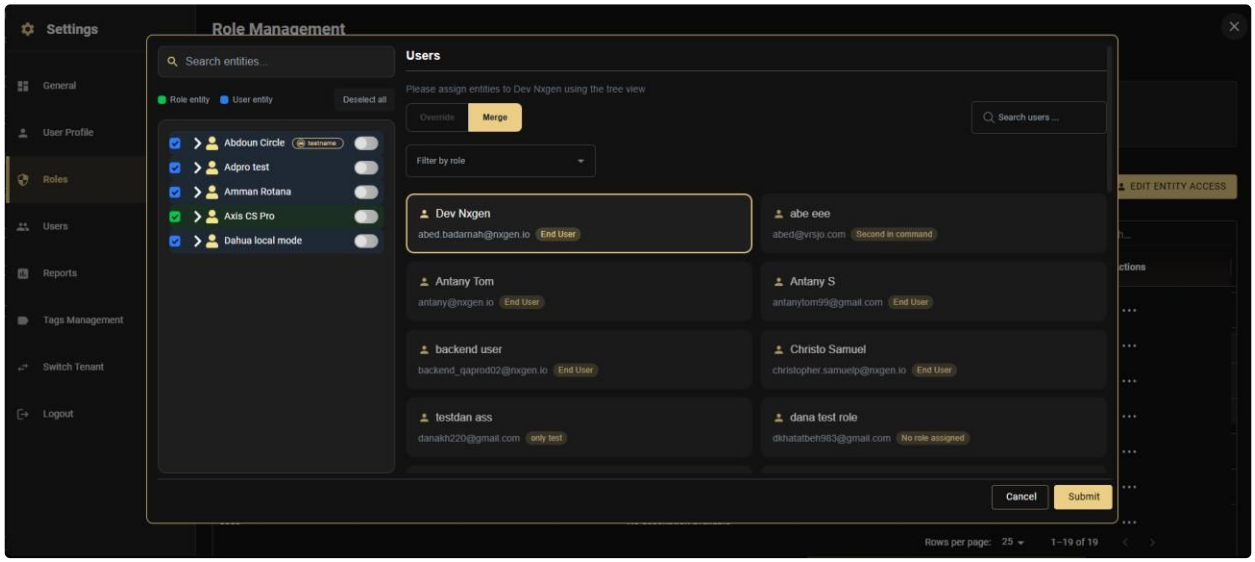
- Vollzugriff – Benutzer erhalten standardmäßig vollständigen Zugriff für alle Kunden, Standorte, Geräte und Sensoren. Geeignet für: Administrator- oder Superuser-Rollen, die uneingeschränkten Zugriff benötigen.

Unabhängig vom Modus: Sie können die Entitätsliste für bestimmte Benutzer jederzeit über „Entitätszugriff bearbeiten“ anpassen und die Zuweisungen auf Rollenebene überschreiben oder erweitern, während ihre Rollenprivilegien erhalten bleiben.

Der Schalter „Kinder einschließen“: Bei der Auswahl von Entitäten in der Baumansicht verfügt jede Entität über einen Schalter „Kinder einschließen“ (angezeigt als blauer Schieberegler neben dem Entitätsnamen). Dieser Schalter hat einen entscheidenden Einfluss darauf, wie der Zugriff funktioniert:

Ohne Kinder einschließen: Nur die manuell ausgewählten Entitäten sind enthalten. Wenn Sie Standort A und seine 5 Geräte und 30 Sensoren einzeln auswählen, erhält der Benutzer Zugriff auf genau diese Elemente. Zukünftige Geräte oder Sensoren, die unter dieser Site hinzugefügt werden, werden NICHT automatisch einbezogen – Sie müssten manuell zu „Entitätszugriff bearbeiten“ zurückkehren und das neue Gerät auswählen.

Mit „Untergeordnete Elemente einschließen“: Sie müssen nur die übergeordnete Entität auswählen (z. B. Standort A). Alle darunter liegenden Geräte und Sensoren werden automatisch einbezogen. Alle zukünftigen Geräte oder Sensoren, die auf dieser Website hinzugefügt werden, werden automatisch einbezogen – manuelle Aktualisierungen sind nicht erforderlich.



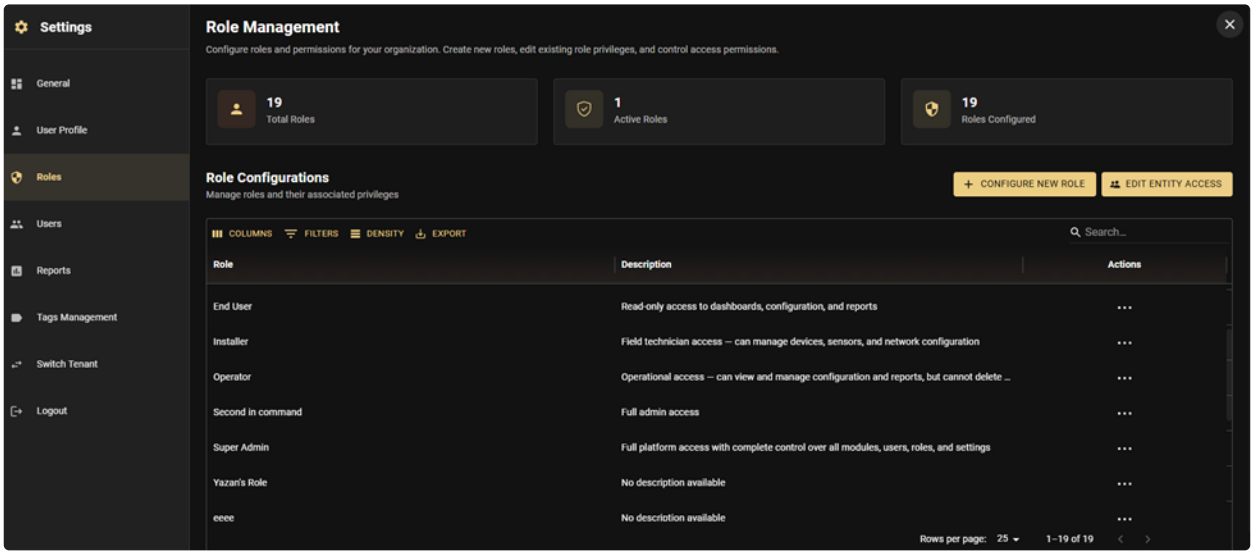
> Tip
>
> Verwenden Sie nach Möglichkeit „Untergeordnete Elemente einschließen“. Dies spart Zeit und stellt sicher, dass neue Geräte automatisch für die richtigen Benutzer zugänglich sind. Verwenden Sie die manuelle Auswahl nur, wenn Sie den Zugriff speziell auf einen festen Satz von Entitäten beschränken müssen.

Rollen verwalten

Navigation: Einstellungen → Rollen

Die Seite „Rollenverwaltung“ zeigt alle konfigurierten Rollen mit ihren Beschreibungen an und bietet zwei Hauptaktionsschaltflächen:

- Neue Rolle konfigurieren – Öffnet den geführten Rollenerstellungsassistenten
- Entitätszugriff bearbeiten – Öffnet die Entitätszugriffsverwaltungsschnittstelle pro Benutzer



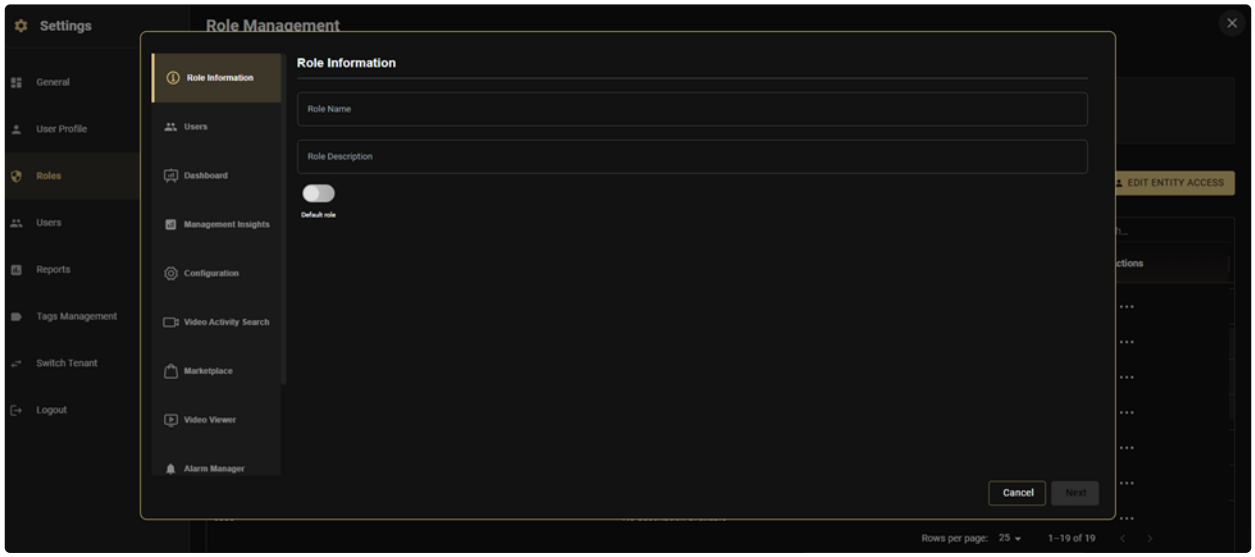
Eine Rolle erstellen

Navigation: Einstellungen → Rollen → Neue Rolle konfigurieren

Der Rollenerstellungsassistent führt Sie durch einen mehrstufigen Prozess. Auf jeden Schritt kann über die entsprechende Registerkarte in der linken Seitenleiste zugegriffen werden.

Schritt 1: Rolleninformationen

1. Rollenname – Ein eindeutiger Name, der die Rolle identifiziert (z. B. „Regionaler Administrator“, „Nur-Ansicht-Operator“)
2. Rollenbeschreibung – Eine kurze Beschreibung des Zwecks der Rolle
3. Standardrollenumschaltung – Wenn diese Rolle aktiviert ist, wird sie neuen Benutzern automatisch zugewiesen, wenn sie zur Plattform eingeladen werden. Dies ist nützlich für Rollen auf Basisebene wie „Endbenutzer“, mit denen jedes neue Teammitglied beginnen sollte.



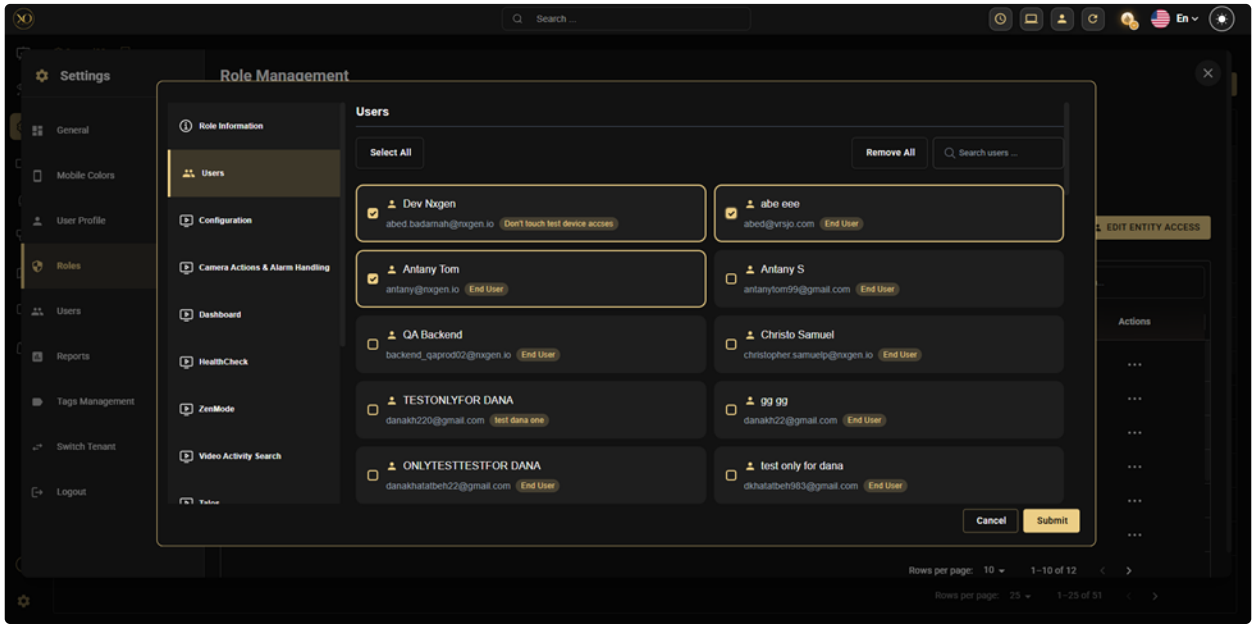
Der erste Schritt der Rollenverwaltung mit Feldern für Rollenname und Beschreibung sowie einem Schalter, um die Rolle als Standardrolle festzulegen.

Schritt 2: Benutzer

Wählen Sie aus, welche Benutzer dieser Rolle zugewiesen werden sollen. Im Schritt „Benutzer“ werden alle verfügbaren Benutzer in einem durchsuchbaren Raster mit ihren aktuellen Rollenabzeichen angezeigt.

Klicken Sie auf eine Benutzerkarte, um sie auszuwählen (hervorgehoben durch einen goldenen Rand).

Verwenden Sie „Alle auswählen“, „Alle entfernen“ oder „Benutzer suchen“ für die Massenverwaltung.



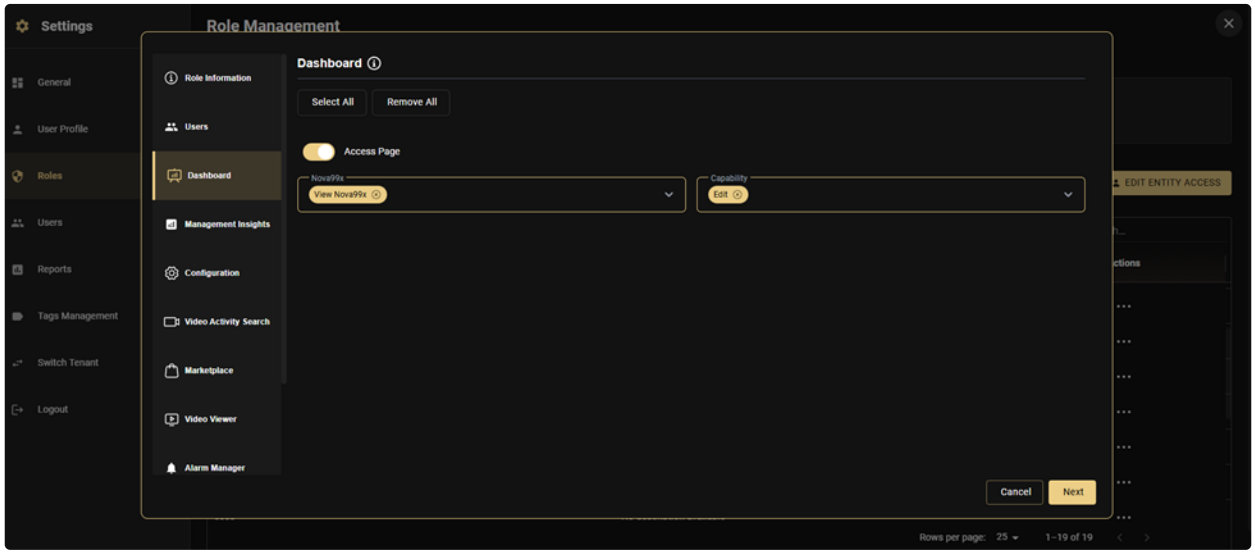
Schritt 3: Modulberechtigungen

Konfigurieren Sie den Zugriff für jedes Plattformmodul. Der Assistent stellt jedes Modul als separate

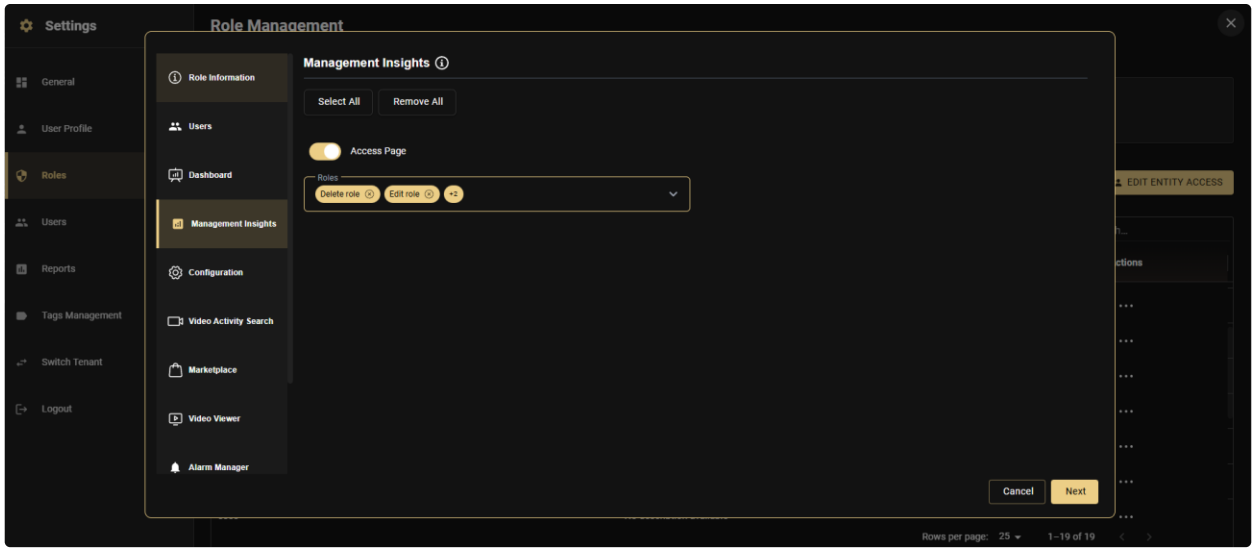
Registerkarte in der Seitenleiste dar. Für jedes Modul:

1. Schalten Sie die Zugriffsseite ein/aus, um das gesamte Modul zu aktivieren oder zu deaktivieren
2. Verwenden Sie „Alle auswählen/Alle entfernen“ für eine schnelle Massenauswahl von Funktionen
3. Wählen Sie einzelne Funktionen aus den Dropdown-Menüs aus, um den Zugriff zu optimieren

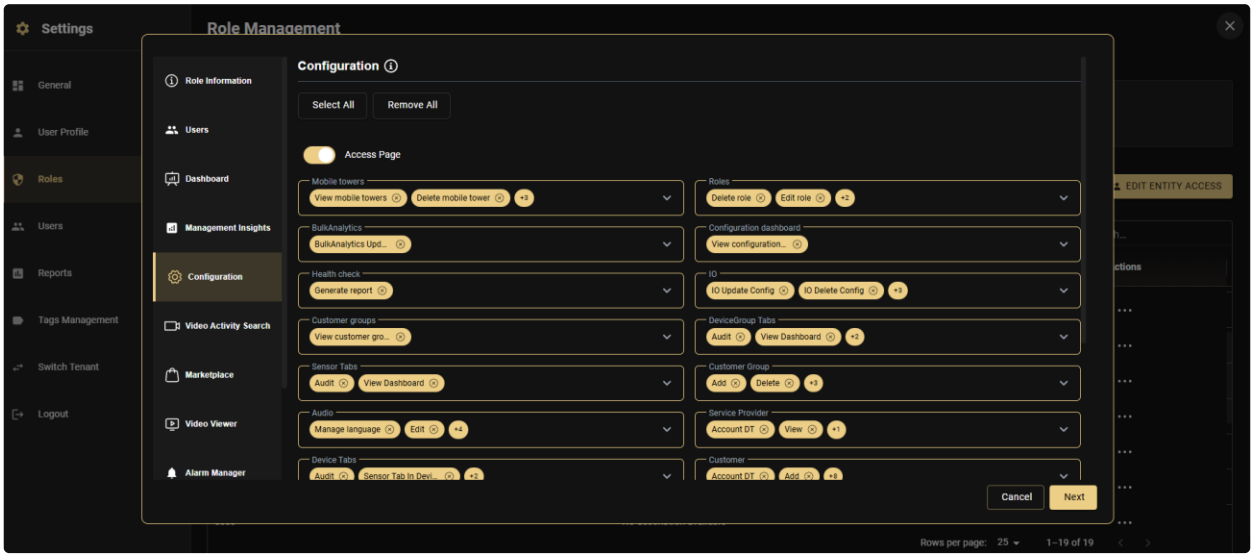
Dashboard:



Management-Einblicke:

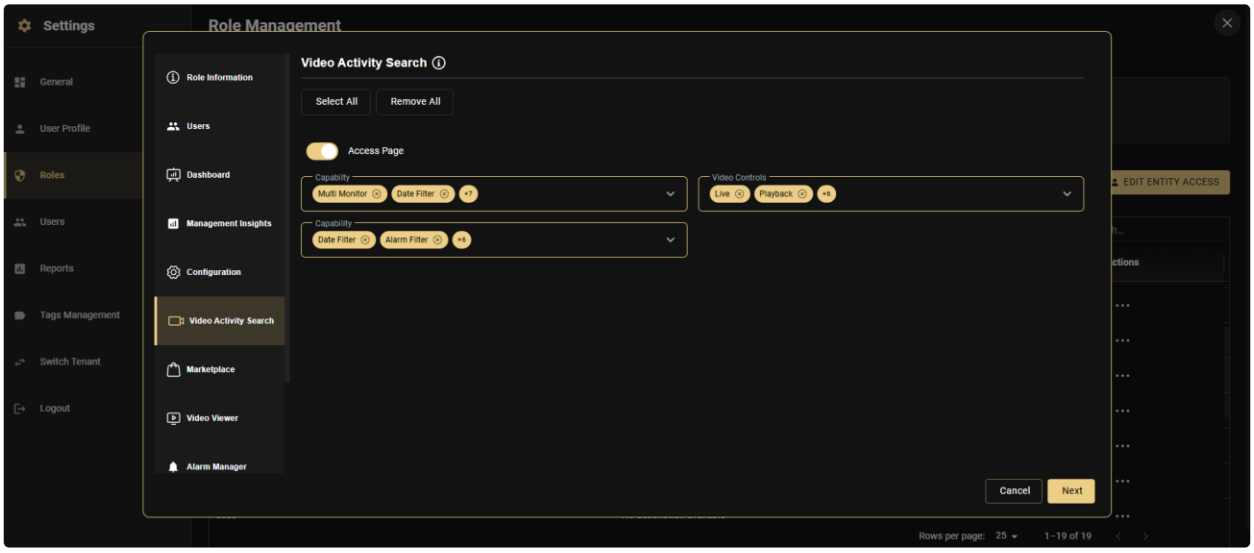


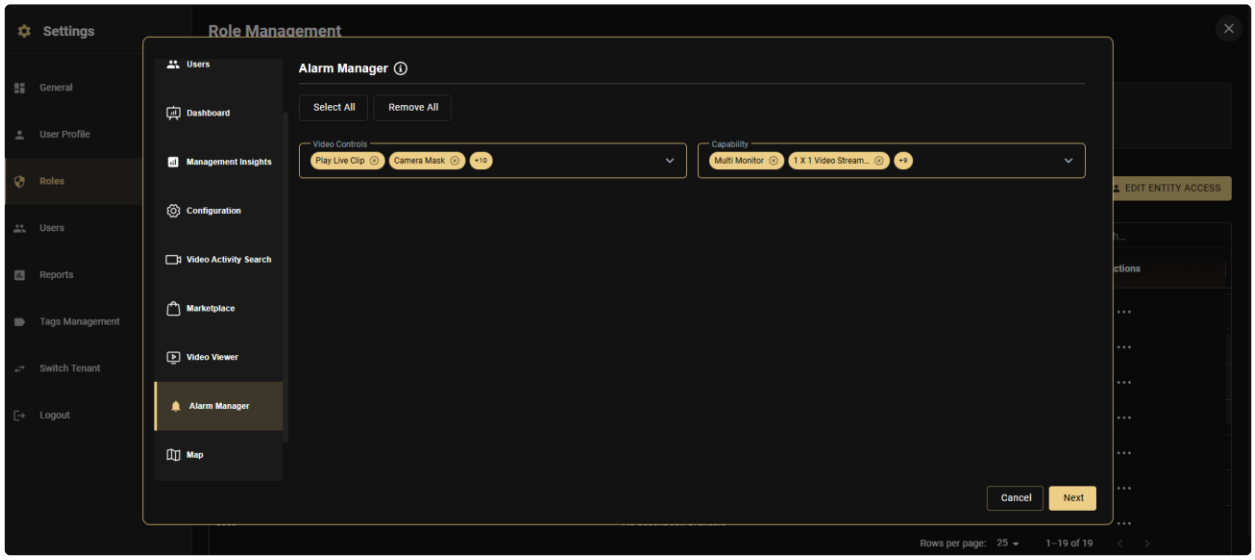
Konfiguration:



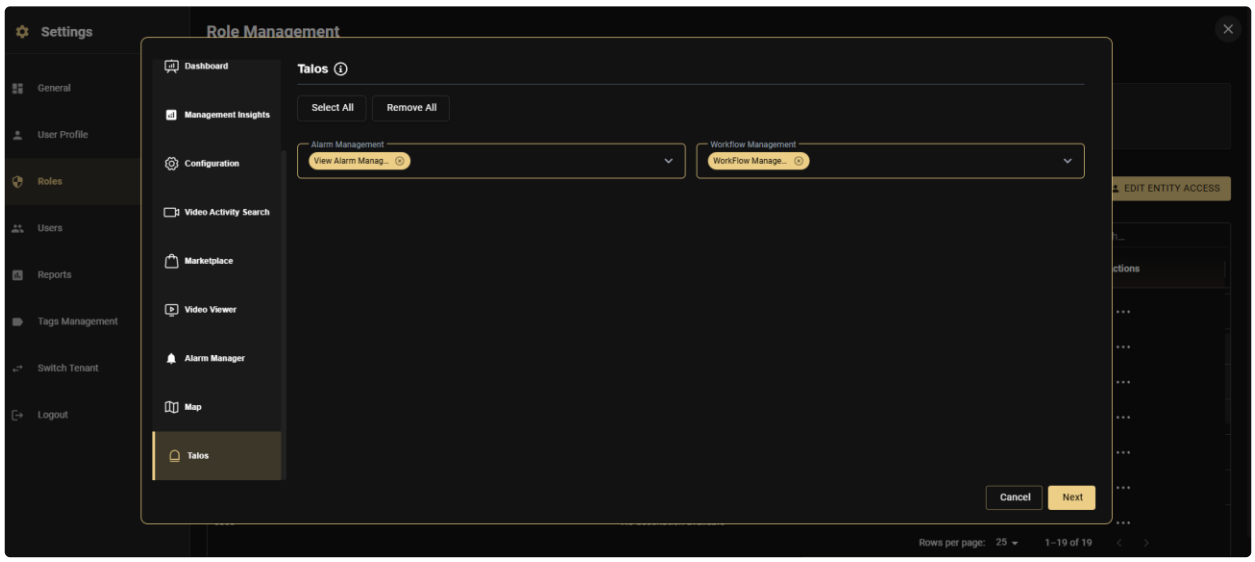
Der Schritt Configuration in der Rollenverwaltung, in dem jeder Bereich – Mobile Towers, Analytics, Health Check, Sensoren, Audio, Geräte, Rollen und weitere – eigene Berechtigungen erhält.

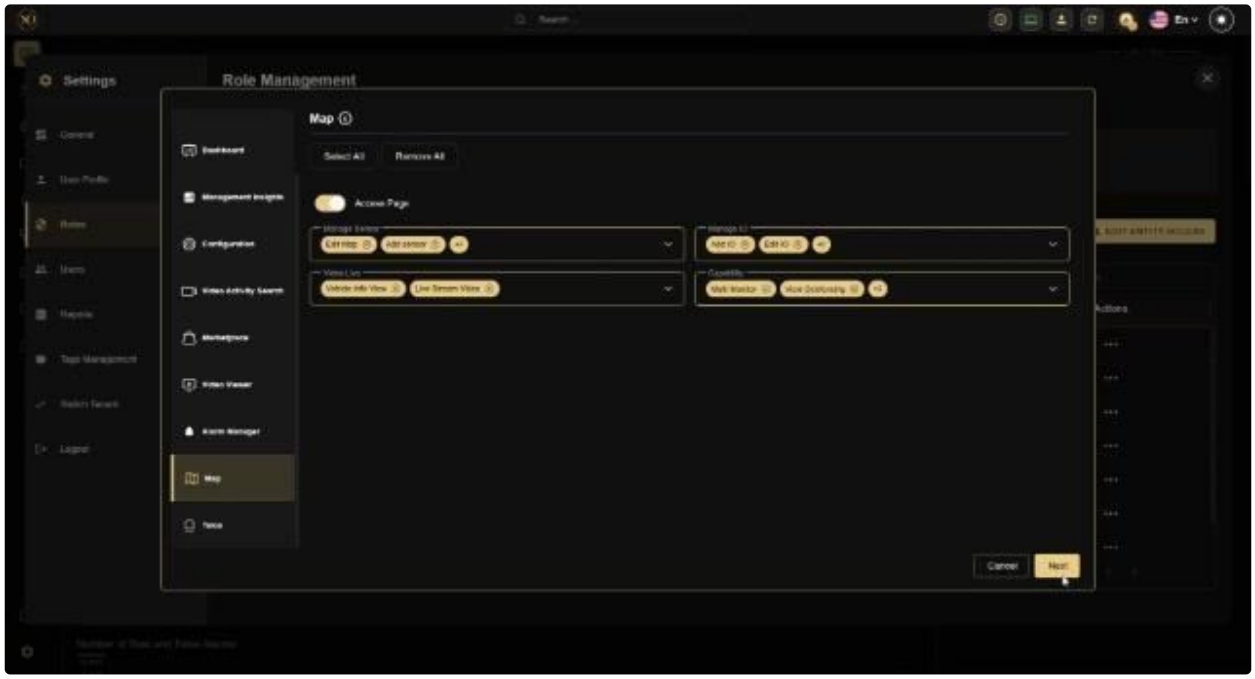
Videoaktivitätssuche:



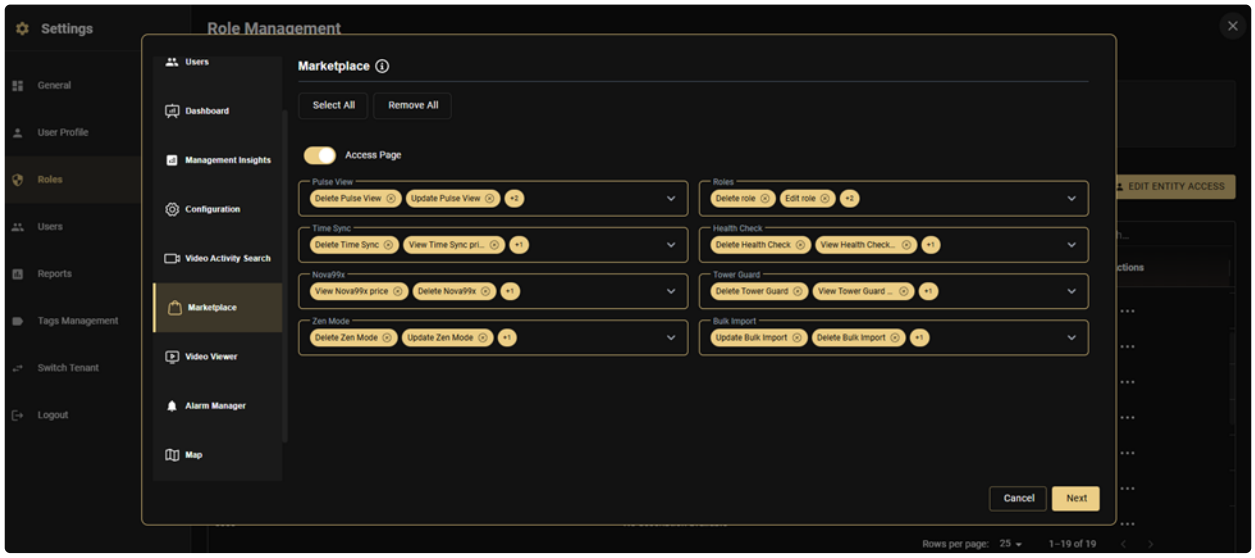


Alarmmanager:

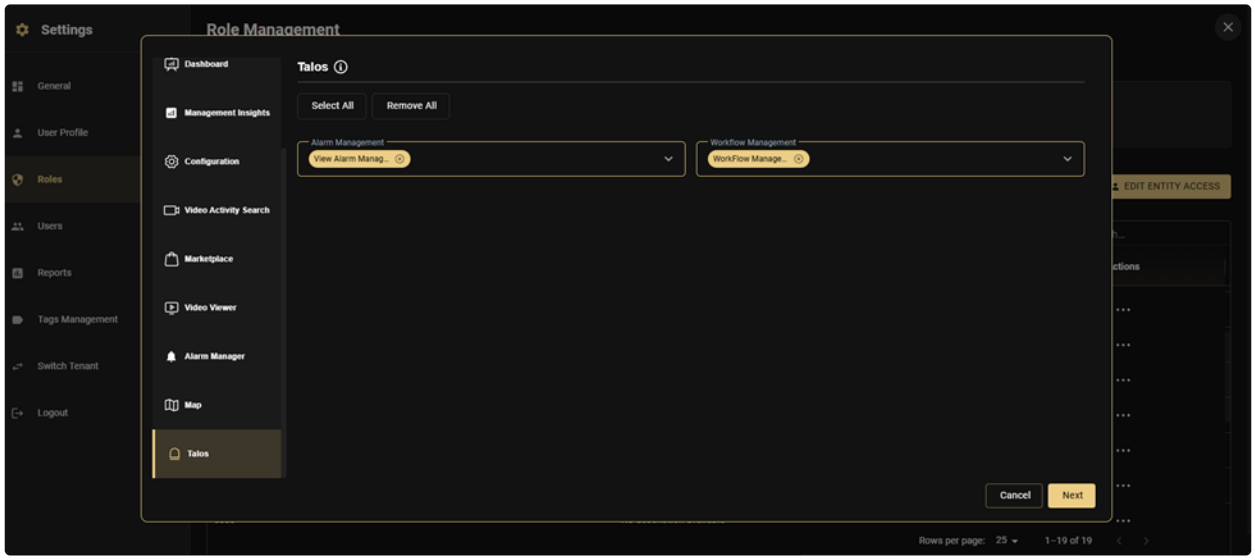




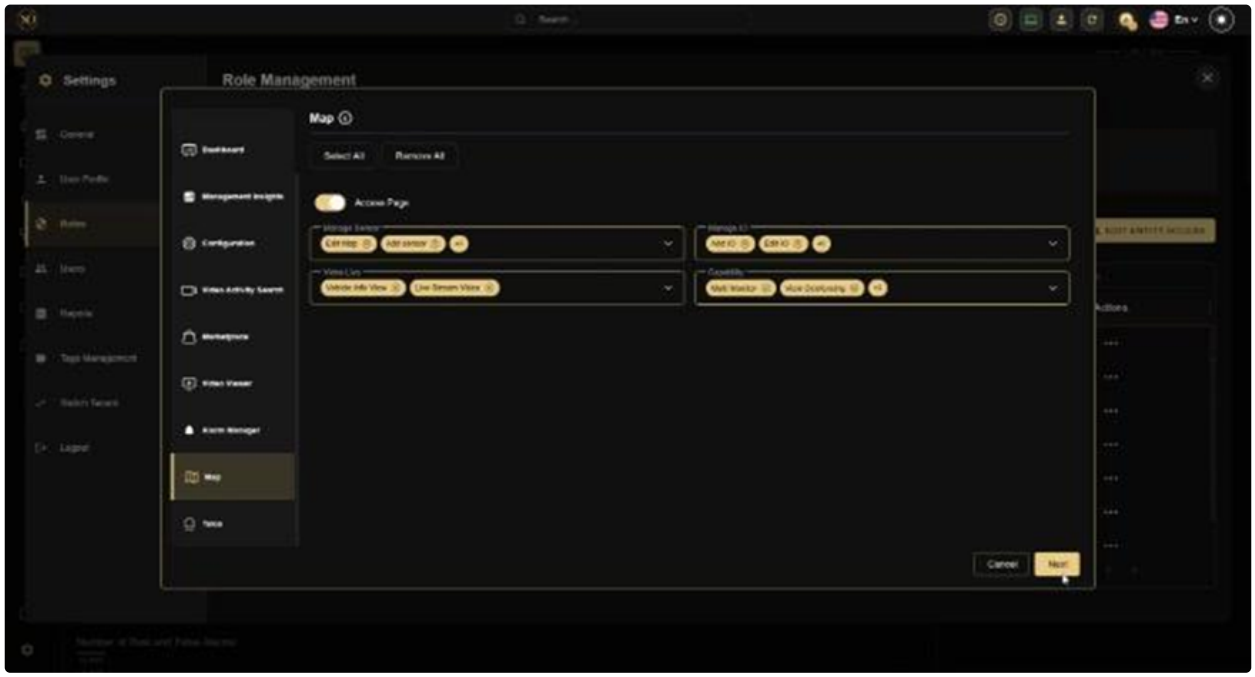
Marktplatz:



Talos:



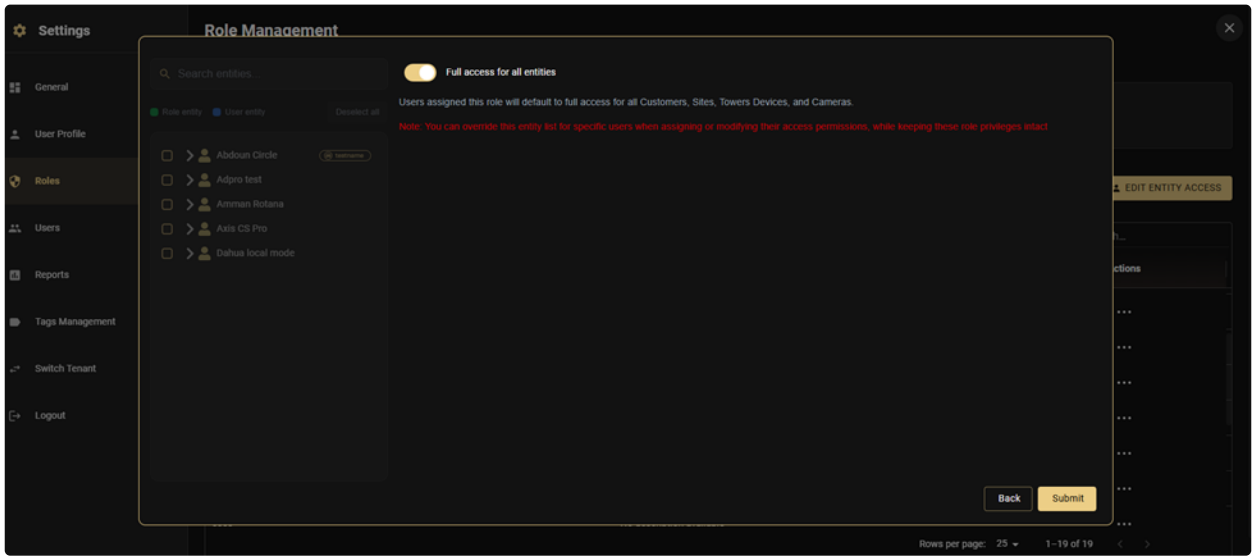
Karte:



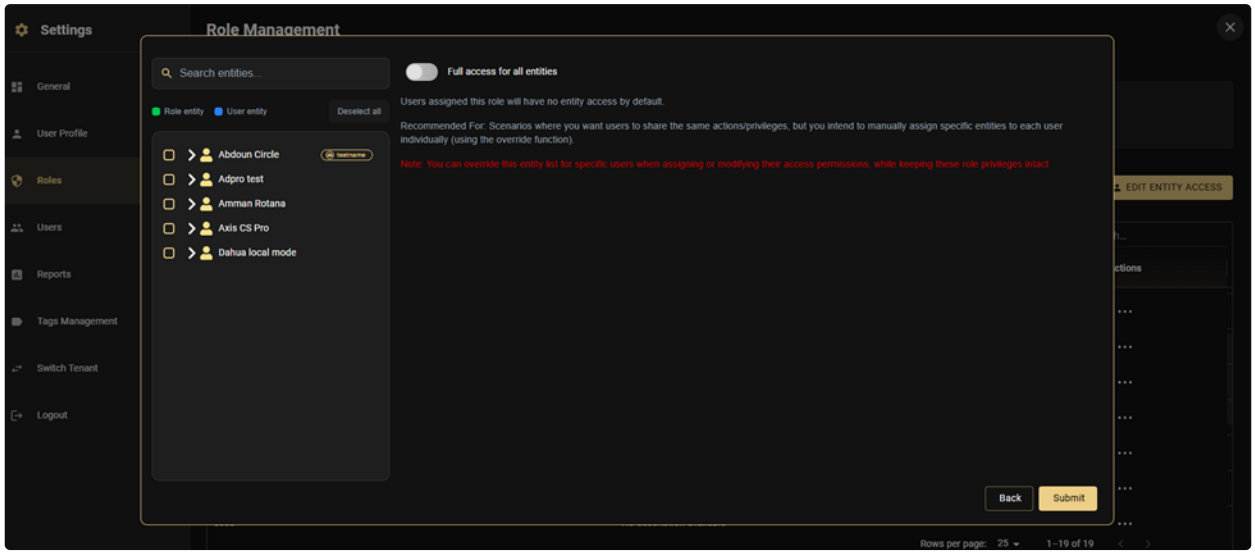
Schritt 4: Entitätszuweisung

Im letzten Schritt wird konfiguriert, auf welche Entitäten Benutzer dieser Rolle zugreifen können. Auf der linken Seite wird der Entitätsbaum mit Kontrollkästchen zur Auswahl und den Schaltern „Untergeordnete Elemente einbeziehen“ für jede Entität angezeigt.

Voller Zugriff für alle Entitäten (einschalten): Benutzer, denen diese Rolle zugewiesen ist, erhalten standardmäßig vollen Zugriff für alle Kunden, Standorte, Türme/Geräte und Kameras.

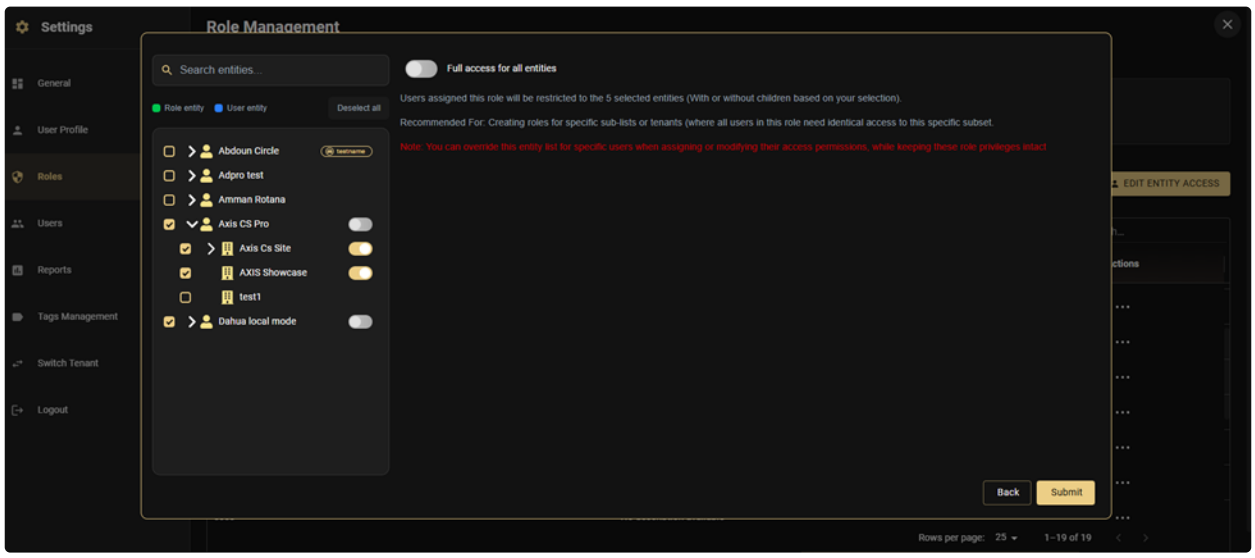


Kein Entitätszugriff (Ausschalten, keine Entitäten ausgewählt): Benutzer, denen diese Rolle zugewiesen ist, haben standardmäßig keinen Entitätszugriff. Empfohlen für Szenarios, in denen Sie möchten, dass Benutzer dieselben Berechtigungen haben, Sie jedoch jedem Benutzer mithilfe der Funktion „Entitätszugriff bearbeiten“ manuell bestimmte Entitäten zuweisen möchten.



Ausgewählte Entitäten (ausschalten, Entitäten aktiviert): Benutzer, denen diese Rolle zugewiesen wird, werden auf die ausgewählten Entitäten beschränkt. Wenn der Schalter „Untergeordnete Elemente

einbeziehen“ für bestimmte Elemente aktiviert ist, werden alle Unterentitäten (aktuelle und zukünftige) automatisch einbezogen.



Der Schritt für den Entitätszugriff in der Rollenverwaltung: der Vollzugriff ist ausgeschaltet und einzelne Standorte sind im Baum ausgewählt, wodurch die Rolle auf diese Entitäten beschränkt wird.

Warnung: Bei der Auswahl von Entitäten ohne „Untergeordnete Elemente einbeziehen“ werden nur die aktuell vorhandenen und manuell ausgewählten Elemente einbezogen. Später hinzugefügte neue Geräte sind NICHT automatisch zugänglich. Erwägen Sie immer die Verwendung von „Untergeordnete Elemente einbeziehen“, um Ihre Entitätszuweisungen zukunftssicher zu machen. Beispiel: Sie weisen Benutzer X Standort A zu, der derzeit über 1 Gerät verfügt. Wenn später unter Standort A ein neues Gerät hinzugefügt wird und „Kinder einbeziehen“ deaktiviert wurde, wird Benutzer X weiterhin nur das ursprüngliche Gerät sehen. Sie müssten manuell zu „Entitätszugriff bearbeiten“ gehen und das neue Gerät für diesen Benutzer hinzufügen.

Klicken Sie auf „Senden“, um die Rolle zu erstellen.

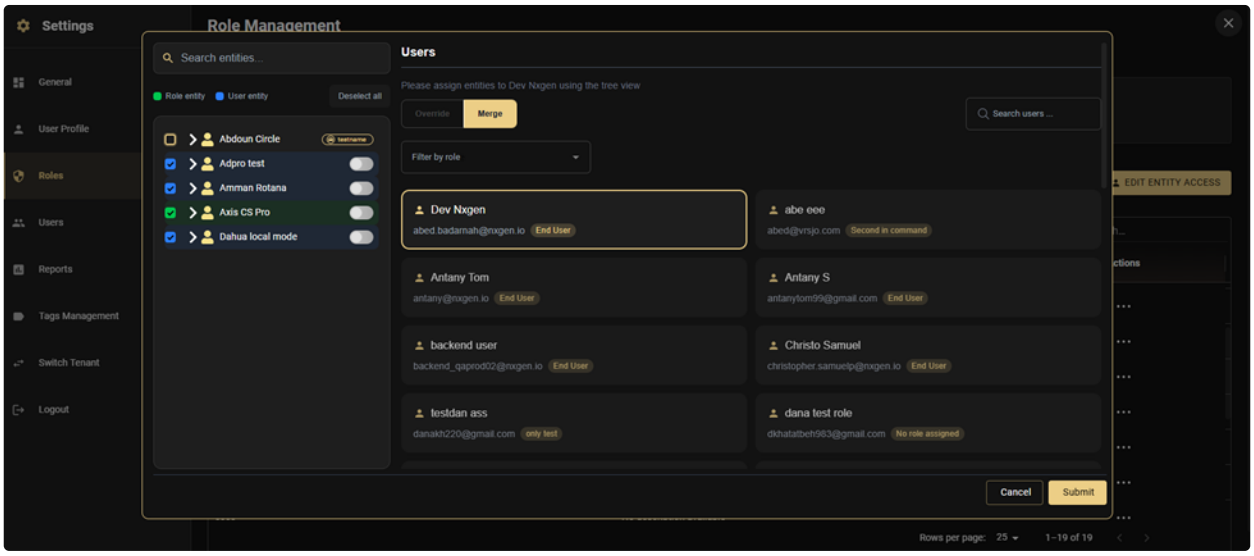
Entitätszugriff bearbeiten (Entitätsverwaltung pro Benutzer)

Navigation: Einstellungen → Rollen → Entitätszugriff bearbeiten

Dies ist die Schlüsselfunktion, die es Ihnen ermöglicht, den Entitätszugriff für einzelne Benutzer anzupassen, ohne separate Rollen zu erstellen. Denken Sie daran: Der Entitätszugriff bestimmt, WO ein Benutzer agieren kann, und nicht, was er tun kann. Privilegien ergeben sich immer aus der Rolle.

Die Benutzeroberfläche ist in zwei Bereiche unterteilt:

- Linkes Feld: Entitätsbaum mit den Registerkarten „Rollenentität“, „Benutzerentität“ und „Verbunden mit“.
- Rechtes Feld: Benutzerliste mit Registerkarten für Suche, Rollenfilterung und Überschreibungs-/Zusammenführungsmodus



Der Schritt Users in der Rollenverwaltung mit ausgewähltem Merge statt Override, sodass die Rolle zu den bereits zugewiesenen Entitäten hinzukommt.

So passen Sie den Entitätszugriff eines Benutzers an

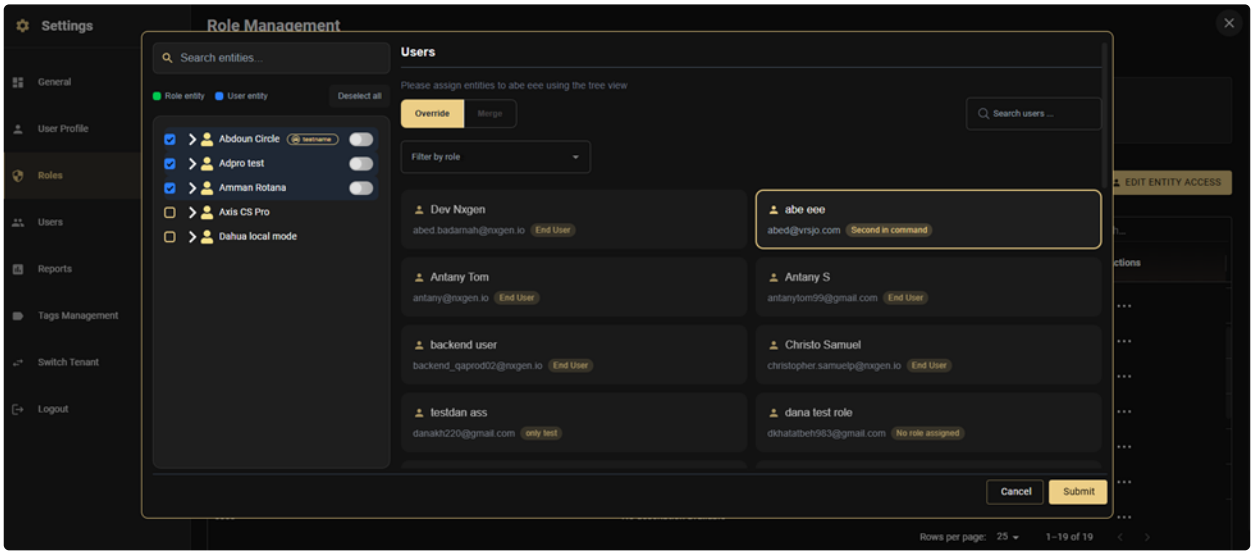
1. Klicken Sie auf der Seite „Rollenverwaltung“ auf „Entitätszugriff bearbeiten“.
2. Wählen Sie im rechten Bereich einen Benutzer aus, indem Sie auf seine Karte klicken
3. Wählen Sie den Modus: Überschreiben oder Zusammenführen
4. Verwenden Sie den Entitätsbaum auf der linken Seite, um Entitäten für diesen bestimmten Benutzer auszuwählen oder die Auswahl aufzuheben

5. Aktivieren Sie „Untergeordnete Elemente einbeziehen“ für Entitäten, bei denen Sie alle aktuellen und zukünftigen Unterentitäten einbeziehen möchten. Dies ist von entscheidender Bedeutung, um sicherzustellen, dass alle neu hinzugefügten Kameras, Geräte oder Sensoren unter einer übergeordneten Entität automatisch in die Entitätszugriffsliste des Benutzers aufgenommen werden, ohne dass manuelle Aktualisierungen erforderlich sind. Beispiel: Sie weisen Benutzer X Standort A zu, der derzeit über 1 Gerät verfügt. Am nächsten Tag wird unter Standort A ein neues Gerät hinzugefügt (jetzt insgesamt 2 Geräte). Wenn „Kinder einbeziehen“ für Standort A deaktiviert wurde, sieht Benutzer X weiterhin nur das ursprüngliche Gerät und hat KEINEN Zugriff auf das neu hinzugefügte Gerät. Wenn „Kinder einbeziehen“ aktiviert wurde, sieht Benutzer X automatisch beide Geräte – eine manuelle Aktualisierung ist nicht erforderlich.
6. Klicken Sie auf „Senden“, um die Änderungen zu speichern

Überschreiben vs. Zusammenführen

Override-Modus: Die benutzerdefinierte Entitätsauswahl des Benutzers ERSETZT die Standardeinstellungen auf Rollenebene. Was auch immer Sie für diesen Benutzer auswählen, hat Vorrang vor dem, was die Rolle bereitstellt. Verwenden Sie diese Option, wenn Sie die vollständige Kontrolle über den Entitätszugriff eines bestimmten Benutzers wünschen.

Zusammenführungsmodus: Die ausgewählten Entitäten werden zusätzlich zu den vorhandenen Entitätszuweisungen der Rolle HINZUGEFÜGT. Der Benutzer erhält sowohl die Entitäten auf Rollenebene als auch die zusätzlichen Entitäten auf Benutzerebene. Verwenden Sie dies, um den Zugriff eines Benutzers über das hinaus zu erweitern, was die Rolle bietet.



Der Schritt Users in der Rollenverwaltung: links der Entitätsbaum, rechts die Personen, die der Rolle zugewiesen werden können, darüber die Optionen Override und Merge.

Sie können die Benutzerliste auch nach Rolle filtern, indem Sie das Dropdown-Menü oben im rechten Bereich verwenden, um den Entitätszugriff für alle Benutzer einer bestimmten Rolle einfacher zu verwalten.

Tipp: Verwenden Sie das Dropdown-Menü „Nach Rolle filtern“, um schnell alle Benutzer zu finden, die einer bestimmten Rolle zugewiesen sind, und ihren Entitätszugriff in großen Mengen anzupassen.

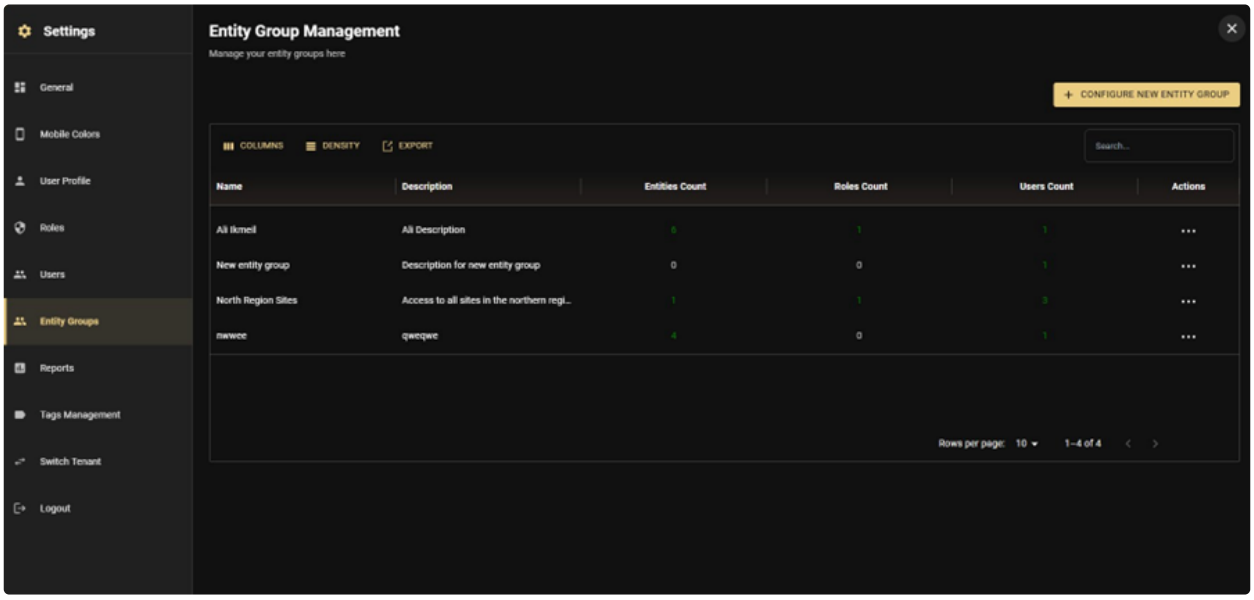
Entitätsgruppen verwalten

Navigation: Einstellungen → Entitätsgruppen

Entitätsgruppen sind gespeicherte, wiederverwendbare Sammlungen von Entitäten (Kunden, Standorte, Geräte und Sensoren), die als Vorlagen dienen. Anstatt jedes Mal, wenn Sie eine Rolle konfigurieren oder Benutzerzugriff zuweisen, dieselben Entitäten manuell auszuwählen, definieren Sie die Gruppe einmal und wenden sie bei Bedarf an. Stellen Sie sich eine Entitätsgruppe als eine benannte Verknüpfung für einen bestimmten Satz von Entitäten vor.

Entitätsgruppen: Definieren Sie die Gruppe einmal und wählen Sie sie dann nach Namen aus, wenn Sie einer Rolle oder einem Benutzer Entitätszugriff zuweisen. Jede dieser Gruppe zugewiesene Rolle oder jeder Benutzer erhält automatisch die richtigen Entitäten.

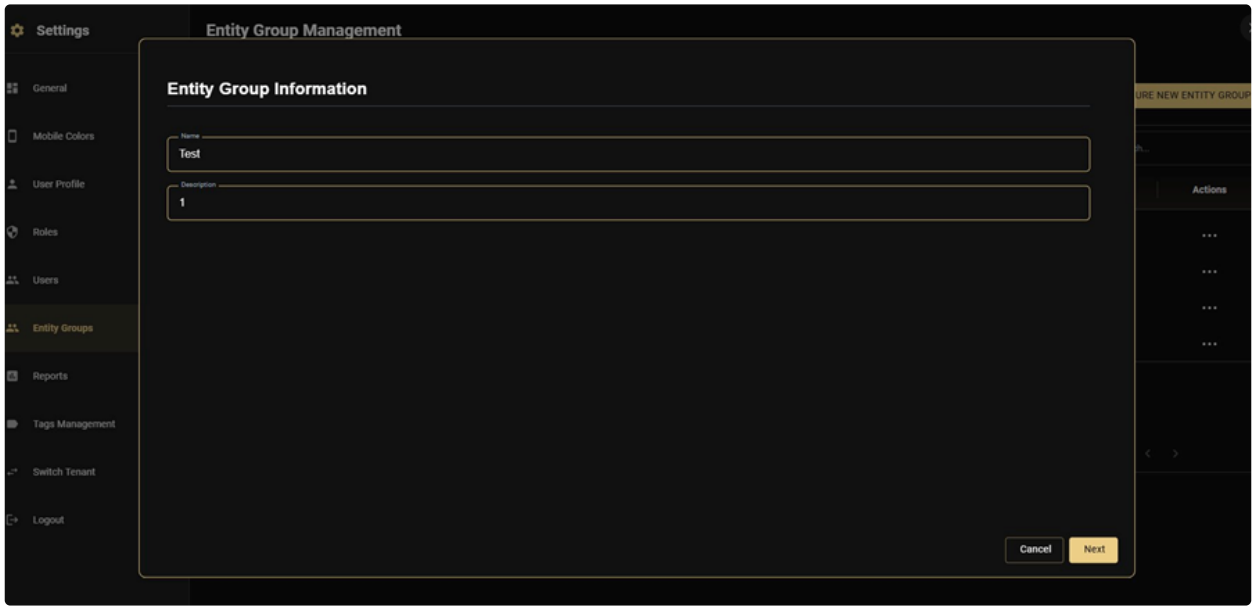
Auf der Seite „Entitätsgruppen“ werden alle vorhandenen Gruppen in einer Tabelle mit Name, Beschreibung, Anzahl der Entitäten, Anzahl der Rollen und Anzahl der Benutzer aufgeführt. Von hier aus können Sie über die Schaltfläche „Neue Entitätsgruppe konfigurieren“ neue Gruppen suchen, exportieren und konfigurieren.



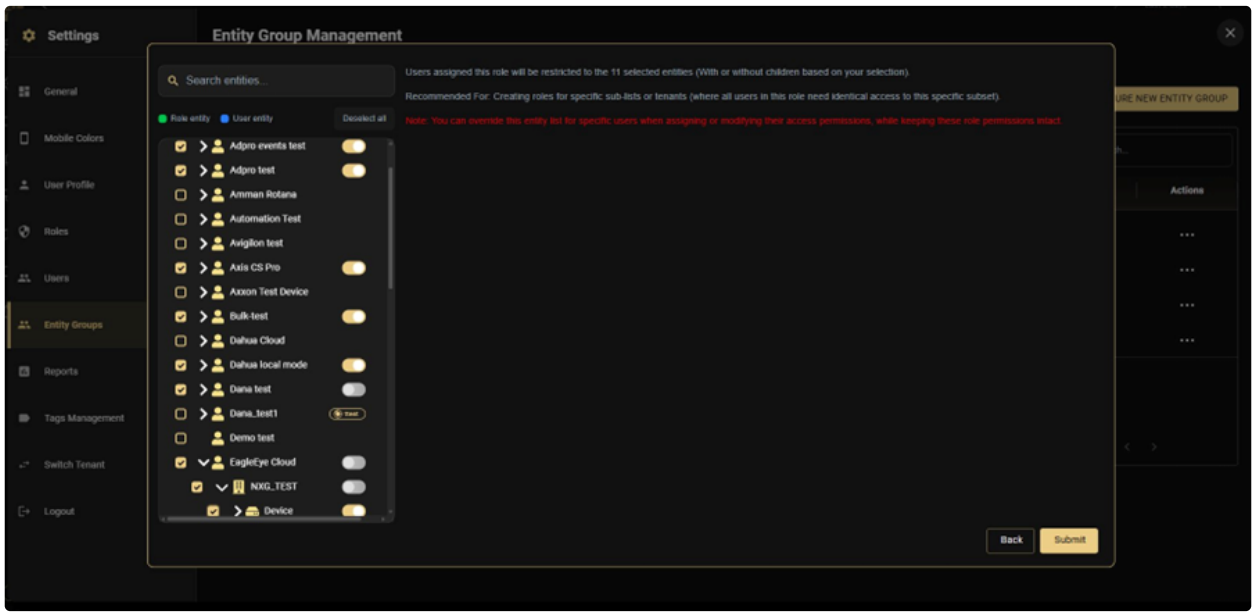
Erstellen einer Entitätsgruppe

Klicken Sie auf „Neue Entitätsgruppe konfigurieren“, um den zweistufigen Erstellungsassistenten zu öffnen.

Schritt 1 – Gruppeninformationen: Geben Sie einen Namen und optional eine Beschreibung für die Gruppe ein und klicken Sie dann auf Weiter.



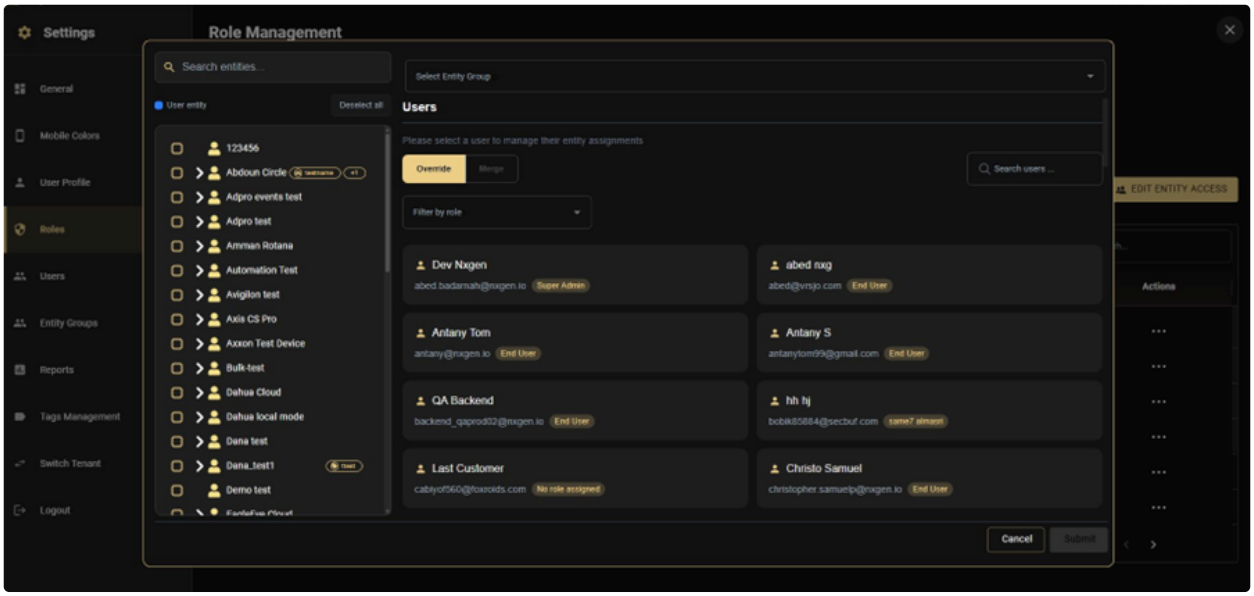
Schritt 2 – Entitäten auswählen: Verwenden Sie den Entitätsbaum, um die Kunden, Standorte, Geräte oder Sensoren zu überprüfen, die in diese Gruppe aufgenommen werden sollen. Verwenden Sie den Schalter „Untergeordnete Elemente einbeziehen“ neben einer beliebigen Entität, um automatisch alle aktuellen und zukünftigen untergeordneten Entitäten darunter einzuschließen. Eine Zusammenfassung auf der rechten Seite zeigt, wie viele Entitäten ausgewählt sind und welche Rollen und Benutzer derzeit betroffen sind. Klicken Sie auf „Senden“, um die Gruppe zu speichern.



Zuweisen einer Entitätsgruppe zu einer Rolle oder einem Benutzer

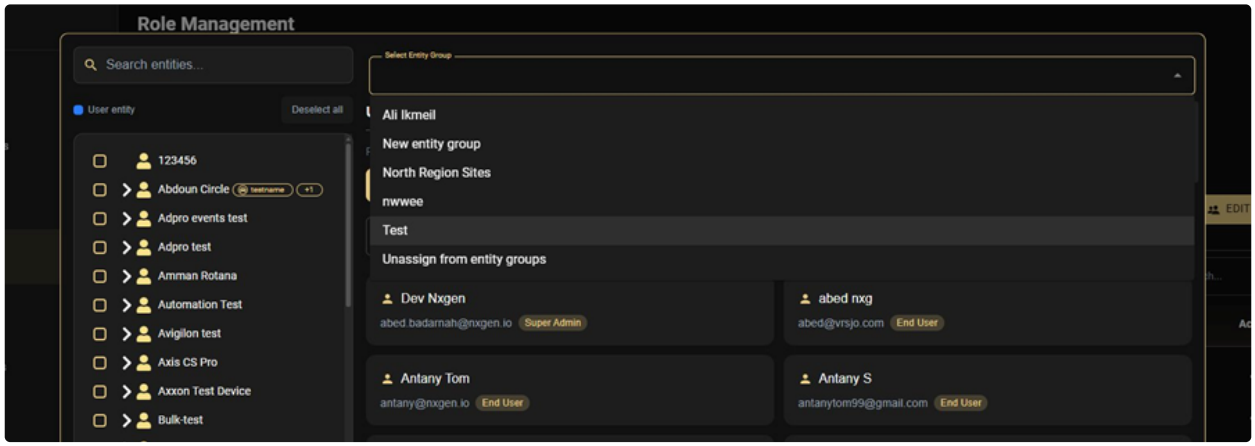
Entitätsgruppen können an zwei Stellen angewendet werden:

- Während der Rollenentitätszuweisung (Schritt 4 der Rollenerstellung/-bearbeitung): Verwenden Sie im Entitätsauswahlbildschirm das Dropdown-Menü „Entitätsgruppe auswählen“, um eine gespeicherte Gruppe anzuwenden. Alle Elemente in dieser Gruppe werden sofort in die Auswahl geladen. Alle Benutzer der Rolle erben diese Entitäten.



Der Schritt Users in der Rollenverwaltung mit ausgewähltem Override: links der Entitätsbaum, rechts die zuzuweisenden Personen, jeweils mit ihrer bereits bestehenden Rolle gekennzeichnet.

- In Entitätszugriff bearbeiten (pro Benutzer): Nachdem Sie im Bereich „Entitätszugriff bearbeiten“ einen Benutzer ausgewählt haben, verwenden Sie oben das Dropdown-Menü „Entitätsgruppe auswählen“, um schnell die Entitäten einer Gruppe für diesen Benutzer zu laden. Die Einstellung „Override“ oder „Merge“-Modus gilt weiterhin – die Gruppe füllt lediglich die Entitätsauswahl vorab aus.



Tipp: Entitätsgruppen sind besonders nützlich, wenn mehrere Rollen oder Benutzer Zugriff auf denselben Satz von Websites oder Kunden benötigen. Erstellen Sie die Gruppe einmal und wenden Sie sie dann auf so viele Rollen und Benutzer wie nötig an. Sollte sich die Entitätsliste jemals ändern, aktualisieren Sie die Gruppe an einer Stelle und alle zugewiesenen Rollen und Benutzer spiegeln die Änderung automatisch wider.

Bearbeiten einer Rolle

Navigation: Einstellungen → Rollen → [Rollenname] → Bearbeiten (über das Menü „Aktionen“)

Der Bearbeitungsablauf verwendet dieselbe Assistentenoberfläche wie die Rollenerstellung. Ändern Sie einen beliebigen Schritt – Rolleninformationen, Benutzer, Modulberechtigungen oder Entitätszuweisungen – und speichern Sie ihn dann. Änderungen wirken sich sofort auf alle Benutzer mit dieser Rolle aus.

Warnung: Das Entfernen des Modulzugriffs oder von Entitäten kann die Arbeitsabläufe der Benutzer stören. Überprüfen Sie, wer diese Rolle hat, bevor Sie wesentliche Änderungen vornehmen.

Löschen einer Rolle

Navigation: Einstellungen → Rollen → [Rollenname] → Löschen (über das Menü „Aktionen“)

Das System warnt, wenn der Rolle derzeit Benutzer zugewiesen sind, und listet betroffene Benutzer auf. Systemrollen (Admin, Super Admin) können nicht gelöscht werden.

Best Practices

Beispiel 1: Zwei regionale Administratoren, eine Rolle

Szenario: Sie haben zwei regionale Administratoren, die identische Berechtigungen benötigen (vollständige Überwachung, Alarmsteuerung, Videoexport), aber Administrator A verwaltet Nordost-Kunden, während Administrator B Südost-Kunden verwaltet. Bisher waren hierfür zwei getrennte Rollen erforderlich. Jetzt brauchen Sie nur noch einen.

Schritt 1 – Erstellen Sie die Rolle ohne Standardentitätszugriff:

1. Gehen Sie zu Einstellungen → Rollen → Neue Rolle konfigurieren
2. Rolleninformationen: Name = „Regionaler Administrator“, Beschreibung = „Vollständige Überwachung und Alarmsteuerung für die zugewiesene Region“
3. Benutzer: Wählen Sie sowohl Admin A als auch Admin B aus dem Benutzerraster aus
4. Modulberechtigungen: Aktivieren Sie Dashboard, Video Viewer, Alarm Manager, Karte mit den gewünschten Funktionen
5. Entitätszuweisung: Lassen Sie „Vollzugriff für alle Entitäten“ AUS und wählen Sie KEINE Entitäten aus. Klicken Sie auf Senden.

Schritt 2 – Entitätszugriff pro Benutzer zuweisen:

- Gehen Sie zu Einstellungen → Rollen → Entitätszugriff bearbeiten
- Wählen Sie „Administrator A“ → „Zusammenführen“ auswählen → „Alle Kunden im Nordosten überprüfen“ (mit aktivierter Option „Kinder einschließen“) → „Senden“.
- Wählen Sie „Admin B“ → „Zusammenführen“ auswählen → „Alle südöstlichen Kunden überprüfen“ (mit aktivierter Option „Kinder einschließen“) → „Senden“.

Ergebnis: Beide Administratoren haben genau dieselbe Rolle und dieselben Berechtigungen, aber Administrator A sieht nur Kunden im Nordosten, während Administrator B nur Kunden im Südosten

sieht. Eine Rolle statt zwei. Wenn unter den ihnen zugewiesenen Kunden neue Standorte oder Geräte hinzugefügt werden, werden diese dank „Untergeordnete Elemente einschließen“ automatisch einbezogen.

Beispiel 2: Nur-Ansicht-Operator

Szenario: Bediener, die während ihrer Schicht nur Kameras sehen sollten – kein Videoexport, keine Alarmsteuerung, nur Live-Anzeige und Wiedergabe für bestimmte Standorte.

Konfiguration:

- Einstellungen → Rollen → Neue Rolle konfigurieren
- Rolleninformationen: Name = „Nur-Anzeige-Operator“
- Benutzer: Wählen Sie die Operatoren aus, die diese Rolle benötigen
- Modulberechtigungen: Nur Dashboard (nur Ansicht) und Video Viewer (mit Live-Ansicht und Wiedergabe) aktivieren. Lassen Sie alle anderen Module deaktiviert.
- Entitätszuweisung: Wählen Sie bestimmte Sites aus, die diese Operatoren im Entitätsbaum abdecken, wobei „Untergeordnete Elemente einbeziehen“ aktiviert ist

Operatoren können Kameras beobachten, aber kein Filmmaterial exportieren, auf die Konfiguration zugreifen oder Alarme steuern. Perfekt für Einsteiger oder Überwachungsdienste von Drittanbietern.

Beispiel 3: Installationsprogramm mit standortspezifischem Zugriff

Szenario: Ein Feldinstallateur benötigt Zugriff auf einen bestimmten Kundenstandort, um Geräte zu verwalten und Sensoren zu konfigurieren. Sie sollten nur die Entitäten sehen, die für ihre aktuelle Aufgabe relevant sind.

Konfiguration:

- Erstellen Sie die Rolle „Installer“ (oder verwenden Sie die Standard-Installer-Rolle).

- Modulberechtigungen: Konfiguration aktivieren (Geräte, Sensoren, Netzwerkeinstellungen), Video Viewer (Live-Ansicht zum Testen)
- Entitätszuweisung: Kein standardmäßiger Entitätszugriff
- Entitätszugriff bearbeiten: Wählen Sie den Installationsbenutzer aus → Zusammenführen → Wählen Sie nur die spezifische Site aus, an der er arbeitet, wobei „Kinder einbeziehen“ aktiviert ist

Der Installateur kann nur den spezifischen Standort und alle seine Geräte/Sensoren sehen und verwalten. Wenn an diesem Standort ein neues Gerät installiert wird, ist es automatisch zugänglich. Wenn die Aufgabe erledigt ist, entfernen Sie den Entitätszugriff oder weisen Sie ihn der nächsten Site neu zu.

Beispiel 4: Mobile App-Zugriff für Außendiensttechniker

Szenario: Außendiensttechniker benötigen mobilen App-Zugriff auf die von ihnen betreuten Standorte, mit Kameraanzeige und Alarmsteuerung.

Konfiguration:

- Erstellen Sie die Rolle „Außendiensttechniker“ über den Rollenassistenten
- Modulberechtigungen: Video-Viewer (Live-Ansicht), Alarm-Manager (Scharf/Unscharf), Karte (Live-Stream-Ansicht) aktivieren.
- Entitätszuweisung: Kein standardmäßiger Entitätszugriff. Verwenden Sie „Entitätszugriff bearbeiten“, um jedem Techniker seinen Servicebereich mit aktivierter Option „Kinder einschließen“ zuzuweisen.

Verhalten der mobilen App: Der Techniker meldet sich bei der mobilen GCXONE-App an und sieht nur die individuell zugewiesenen Standorte. Sie können Live-Kameras ansehen und von ihrem Telefon aus aktivieren/deaktivieren. Berechtigungsänderungen werden innerhalb von 5 Sekunden auf Mobilgeräte angewendet. Es ist nicht erforderlich, mobile Berechtigungen separat zu verwalten oder individuelle Rollen zu erstellen.

Verwandte Ressourcen

- Informationen zum Verständnis der Entitätshierarchie finden Sie unter Organisations- und Hierarchie-Setup
- Informationen zum Verwalten von Benutzern finden Sie unter Benutzerverwaltung
- Informationen zu Überwachungsprotokollen finden Sie unter Prüfung
- Informationen zur Kontaktaufnahme mit dem Support finden Sie unter Kontaktieren Sie den Support