

Milestone Systems

XProtect® Access 2020 R2

Bedienungsanleitung für Administratoren



Inhalt

Copyright, Marken und Verzichtserklärung	3
Übersicht	4
XProtect Access (erklärt)	4
Lizenzierung	5
XProtect Access Lizenzen	5
Konfiguration	6
Konfigurieren eines integrierten Zugangskontrollsystems	6
Assistent zur Zugangskontrollintegration	6
Integration des Zugangskontrollsystems erstellen	7
Verbindung zum Zugangskontrollsystem	7
Zugewiesene Kameras	7
Zusammenfassung	7
Zugangskontrolleigenschaften	8
Registerkarte „Allgemeine Einstellungen“ (Zugangskontrolle)	8
Registerkarte „Türen und zugehörige Kameras“ (Zugangskontrolle)	9
Registerkarte Zugangskontrollereignisse (Zugangskontrolle)	10
Registerkarte „Zugangsanforderungsbenachrichtigung“ (Zugangskontrolle)	11
Registerkarte „Karteninhaber“ (Zugangskontrolle)	13
Konfiguration von Zugangsanfragen	14

Copyright, Marken und Verzichtserklärung

Copyright © 2020 Milestone Systems A/S

Marken

XProtect ist eine eingetragene Marke von Milestone Systems A/S.

Microsoft und Windows sind eingetragene Marken der Microsoft Corporation. App Store ist eine Dienstleistungsmarke von Apple Inc. Android ist eine Handelsmarke von Google Inc.

Alle anderen in diesem Dokument genannten Marken sind Marken ihrer jeweiligen Eigentümer.

Haftungsausschluss

Dieses Dokument dient ausschließlich zur allgemeinen Information und es wurde mit Sorgfalt erstellt.

Der Empfänger ist für jegliche durch die Nutzung dieser Informationen entstehenden Risiken verantwortlich, und kein Teil dieser Informationen darf als Garantie ausgelegt werden.

Milestone Systems A/S behält sich das Recht vor, ohne vorherige Ankündigung Änderungen vorzunehmen.

Alle Personen- und Unternehmensnamen in den Beispielen dieses Dokuments sind fiktiv. Jede Ähnlichkeit mit tatsächlichen Firmen oder Personen, ob lebend oder verstorben, ist rein zufällig und nicht beabsichtigt.

Das Produkt kann Software anderer Hersteller verwenden, für die bestimmte Bedingungen gelten können. In diesem Fall finden Sie weitere Informationen in der Datei `3rd_party_software_terms_and_conditions.txt`, die sich im Installationsordner Ihres Milestone Systems befindet.

Übersicht

XProtect Access (erklärt)



Zur Nutzung von XProtect Access müssen Sie eine Basislizenz erworben haben, die Ihnen den Zugriff auf diese Funktion innerhalb Ihres XProtect-Systems erlaubt. Zudem benötigen Sie für jede Tür, die Sie kontrollieren möchten, eine Zugriffskontrolltür-Lizenz.



Sie können XProtect Access zusammen mit Zugangskontrollsystemen anderer Anbieter verwenden, sofern diese über ein anbieterspezifisches Plug-in für XProtect Access verfügen.

Die Funktion der Zugangskontrollintegration führt neue Funktionalität ein, die eine einfache Integration der Zugangskontrollsysteme von Kunden mit XProtect ermöglichen. Sie erhalten:

- Eine allgemeine Bedienoberfläche für Anwender für mehrere Zugangskontrollsysteme in XProtect Smart Client
- Schnellere und bessere Integration der Zugangskontrollsysteme
- Mehr Funktionalität für den Anwender (siehe unten)

In XProtect Smart Client erhält der Anwender:

- Live-Überwachung von Ereignissen an Zugangspunkten
- Anwendergestützter Zutritt für Zugangsanforderung
- Karten-Integration
- Alarmdefinitionen für Ereignisse bezogen auf die Zugangskontrolle
- Untersuchung von Ereignissen am Zugangspunkt
- Zentralisierte Übersicht und Kontrolle von Türstatus
- Kartenhalter-Informationen und -Verwaltung

Das **Auditprotokoll** protokolliert die Befehle, die jeder Benutzer im Zugangskontrollsystem von XProtect Smart Client ausführt.

Abgesehen von einer XProtect Access-Basislizenz, müssen Sie ein händlerspezifisches Integrations-Plug-In auf dem Event-Server installieren, bevor Sie eine Integration beginnen können .

Lizenzierung

XProtect Access Lizenzen

XProtect Access erfordert die folgenden Lizenzen für die Zugangskontrolle:

- Eine **Basislizenz** für XProtect Access, die eine unbegrenzte Anzahl von Zugangsservern abdeckt
- Eine **Zugangskontroll-Türlizenz** pro Tür, die Sie in XProtect Access integrieren und steuern möchten. **Zwei** Zugangskontroll-Türlizenzen sind in der Basislizenz von XProtect Access enthalten. Alle Türlizenzen werden automatisch bei der Installation Ihres XProtect Access-Produkts mitinstalliert. Allerdings sind die installierten Türlizenzen standardmäßig deaktiviert. Sie müssen daher die Türen aktivieren, wenn Sie diese benutzen möchten. Sie können nur so viele Türen aktivieren, wie Sie Lizenzen besitzen

Beispiel: Sie haben fünf Zugangskontroll-Türlizenzen und Sie haben 10 Türen hinzugefügt. Sobald Sie fünf Türen hinzugefügt haben, können Sie keine weiteren auswählen. Sie müssen einige Ihrer Türen entfernen, bevor Sie weitere hinzufügen können.

Um Informationen über den aktuellen Status Ihrer Zugangskontroll-Türlizenzen zu erhalten, erweitern Sie den Knoten **Zugangskontrolle**.

Wenden Sie sich Ihren Anbieter, wenn Sie zusätzliche Basislizenzen oder Türlizenzen für XProtect Access erwerben möchten.

Konfiguration

Konfigurieren eines integrierten Zugangskontrollsystems

Voraussetzungen

- Sie haben die erforderlichen XProtect Access-Lizenzen erworben.
 - Sie haben das Integrations-Plug-In für Ihr Zugangskontrollsystem auf dem Event-Server installiert
1. Fügen Sie das integrierte Zugangskontrollsystem zu Ihrem XProtect-System hinzu. Siehe Assistent zur Zugangskontrollintegration auf Seite 6. Der Assistent führt Sie durch die grundlegendsten Schritte.
 2. Bestimmen Sie zusätzliche Eigenschaften für die Integration des Zugangskontrollsystems, vor allem könnten Zugangskontrollereignisse eine Aufzeichnung von Ereignissen vom Zugangskontrollsystem erfordern, dessen Ereigniskategorien XProtect wiedererkennt. Siehe Zugangskontrolleigenschaften auf Seite 8.
 3. Sie müssen eine Rolle mit Berechtigung zur Nutzung der Zugangskontrollfunktionen in XProtect Smart Client erstellen. Siehe die Registerkarte Zugangskontrolle (siehe die Registerkarte Zugangskontrolle (Rollen) im *XProtect Management Client Administrator-Handbuch*).
 4. Sie müssen außerdem diese Rolle einem Smart Client-Profil zuweisen. Siehe Smart Client Eigenschaften von Profil im *XProtect Management Client Administrator-Handbuch*.
 5. Das System legt eine Standard-Regel fest, die Ihnen Zugangsanforderungenbenachrichtigungen auf dem XProtect Smart Client-Bildschirm anzeigt, falls der Zugang verweigert wird. Sie können Benachrichtigungen für Zugangsanforderungen hinzufügen und modifizieren. Siehe hierzu Zugangsanforderungen-Benachrichtigungen (Eigenschaften) (siehe Registerkarte Registerkarte „Zugangsanforderungenbenachrichtigung“ (Zugangskontrolle) auf Seite 11).
 6. Sie können zusätzliche Regeln auf Grundlage von Aktionen und Ereignissen aus dem Zugangskontrollsystem erstellen. Siehe Aktionen und Stopp-Aktionen (Erklärung) und Ereignisübersicht im *XProtect Management Client Administrator-Handbuch*.
 7. Bei Bedarf können Sie die übergreifenden Zugangskontrolleinstellungen unter **Optionen** > **Zugangskontrolleinstellungen** ändern. Siehe die Registerkarte Zugangskontrolleinstellungen (siehe Konfigurieren eines integrierten Zugangskontrollsystems im *XProtect Management Client Administrator-Handbuch*).

Assistent zur Zugangskontrollintegration

Der Assistent für die **Zugangskontrollintegration** führt durch eine schrittweise Konfiguration der initialen Integration mit einem Zugangskontrollsystem. Verwenden Sie den Assistenten, um die grundlegendsten Konfigurationsaufgaben durchzuführen. Sie können danach eine detailliertere Konfiguration durchführen.

Bevor Sie den Assistenten für die Zugangskontrollintegration starten, sollten Sie sicherstellen, dass Sie das Integrations-Plug-in auf dem Event-Server installiert haben.

Einige der auszufüllenden Felder und ihre Standardwerte werden aus dem Integrations-Plug-in übernommen. Daher könnte das Aussehen des Assistenten abweichen, je nach Zugangskontrollsystem, welches Sie integrieren.

Klicken Sie mit der rechten Maustaste auf die **Zugangskontrolle** in der Knotenstruktur und klicken Sie auf **Neu erstellen**, um den Assistenten zu starten.

Integration des Zugangskontrollsystems erstellen

Geben Sie den Namen ein und geben Sie die Verbindungsdetails für das Zugangskontrollsystem an, das Sie hinzufügen wollen. Die von Ihnen festzulegenden Parameter sind vom Systemtyp abhängig, bestehen aber typischerweise in der Netzwerkadresse des Zugangskontrollsystemservers und einem Benutzernamen und Passwort eines Zugangskontrolladministrators.

Das Videomanagementsystem verwendet den spezifischen Benutzernamen und Passwort, um sich im Zugangskontrollsystem anzumelden und die komplette Konfiguration aufzurufen.

Das Integrations-Plug-in bestimmt zudem sekundäre Parameter, die nicht im Assistenten aufgeführt werden, aber unter **Allgemeine Einstellungen** nach der Integration geändert werden können. Die Standardwerte der Parameter werden vom Plug-in oder dem XProtect-System angegeben.

Verbindung zum Zugangskontrollsystem

Nachdem das Plug-in erfolgreich integriert wurde, erscheint eine Zusammenfassung der Konfiguration des Zugangskontrollsystems. Überprüfen Sie die Liste, um sicherzustellen, dass alle Elemente integriert wurden, bevor Sie zum nächsten Schritt des Assistenten fortfahren.

Zugewiesene Kameras

Ordnen Sie Zugangspunkte im Zugangskontrollsystem den Kameras im XProtect-System zu, um zugehöriges Video des Ereignissen von den Türen zu zeigen.

Sie können mehrere Kameras einem Zugangspunkt zuordnen. Die XProtect Smart Client-Benutzer können dann Videos von allen Kameras ansehen, wenn sie z. B. Ereignisse untersuchen.

Die XProtect Smart Client-Benutzer können zudem eine der Kameras hinzufügen, wenn sie Ansichtselemente des **Zugangsmonitors** konfigurieren.

Lizenzierte Türen sind standardmäßig aktiviert. Wählen Sie das Kontrollkästchen ab, um eine Tür zu deaktivieren und so eine Lizenz einer Zugangskontrolltür freizugeben.

Zusammenfassung

Ihre Zugangskontrollsystemintegration wurde erfolgreich in XProtect mit den Standardeinstellungen des Integrations-Plug-ins erstellt. Client-Benutzer müssen sich bei XProtect Smart Client anmelden, um das neue Zugangskontrollsystem zu sehen und zu nutzen.

Sie können die Konfiguration bei Bedarf ergänzen.

Zugangskontrolleigenschaften

Registerkarte „Allgemeine Einstellungen“ (Zugangskontrolle)

Name	Beschreibung
Aktivieren	<p>Systeme sind standardmäßig aktiviert, d. h. sie sind für Benutzer mit ausreichenden Rechten in XProtect Smart Client sichtbar und das XProtect-System erhält Zugangskontrollereignisse.</p> <p>Sie können ein System beispielsweise während der Wartung deaktivieren, um unnötige Alarme zu vermeiden.</p>
Name	<p>Der Name der Zugangskontrollintegration, wie in der Management-Anwendung und den Clients angezeigt. Sie können den bestehenden Namen mit einem Neuen überschreiben.</p>
Beschreibung	<p>Geben Sie eine Beschreibung für die Zugangskontrollintegration ein. Dies ist optional.</p>
Integrations-Plug-in	<p>Zeigt den Typ des Zugangskontrollsystems an, welches während der initialen Integration ausgewählt wurde.</p>
Letzte Konfiguration aktualisieren	<p>Zeigt Datum und Zeit der letzten Konfiguration, die vom Zugangskontrollsystem importiert wurde.</p>
Konfiguration aktualisieren	<p>Klicken Sie auf die Schaltfläche, wenn Sie die im Zugangskontrollsystem in XProtect vorgenommene Konfigurationsänderungen anzeigen lassen wollen (zum Beispiel wenn Sie eine Tür hinzugefügt oder entfernt haben).</p> <p>Eine Zusammenfassung der Konfigurationsänderungen des Zugangskontrollsystems erscheint. Überprüfen Sie die Liste, um sicherzustellen, dass Ihr Zugangskontrollsystem korrekt widerspiegelt wird, bevor Sie die neue Konfiguration anwenden.</p>
Anwenderanmeldung erforderlich	<p>Erlauben Sie ein zusätzliches Log-in für Client-Benutzer, wenn das Zugangskontrollsystem differenzierte Benutzerberechtigungen unterstützt. Wenn sie diese Option aktivieren, steht Ihnen das Zugangskontrollsystem im XProtect Mobile-Client nicht zur Verfügung.</p> <p>Diese Option ist nur sichtbar, wenn das Integrations-Plug-in differenzierte Benutzerrechte unterstützt.</p>

Die Bezeichnung und der Inhalt der folgenden Felder wurde aus dem Integrations-Plug-in importiert. Unten finden Sie einige Beispiele typischer Felder:

Name	Beschreibung
Adresse	Geben Sie die Adresse des Hostservers des integrierten Zugangskontrollsystems ein.
Port	Bestimmen Sie die Portnummer auf dem Server, der mit dem Zugangskontrollsystem verbunden ist.
Benutzername	Geben sie den Namen des Benutzers ein, wie im Zugangskontrollsystem festgelegt, der als Administrator des integrierten Systems in XProtect fungieren soll.
Passwort	Bestimmen Sie das Passwort des Benutzers.

Registerkarte „Türen und zugehörige Kameras“ (Zugangskontrolle)

Diese Registerkarte stellt Zuordnungen zwischen Zugangspunkten von Türen und Kameras, Mikrofonen oder Lautsprechern her. Sie können Kameras als Teil des Integrationsassistenten verknüpfen, eine spätere Änderung ist aber jederzeit möglich. Zuordnungen zu Mikrofonen und Lautsprechern sind durch die zugehörigen Mikrofone und Lautsprecher an der Kamera eingeschlossen.


Name	Beschreibung
Türen	<p>Listet die verfügbaren Zugangspunkte der Türen auf, die im Zugangskontrollsystem festgelegt sind; nach Türen gruppiert.</p> <p>Zur einfacheren Navigation der relevanten Türen, können Sie mittels einer Dropdown-Liste oberhalb der Türen in Ihrem Zugangskontrollsystem filtern.</p> <p>Aktiviert: Lizenzierte Türen sind standardmäßig aktiviert. Sie können eine Tür deaktivieren, um eine Lizenz freizugeben.</p> <p>Lizenz: Zeigt, falls eine Tür lizenziert ist oder ob die Lizenz abgelaufen ist. Das Feld ist leer, wenn die Tür deaktiviert ist.</p> <p>Entfernen: Klicken Sie auf Entfernen, um eine Kamera aus einem Zugangspunkt zu entfernen. Wenn Sie alle Kameras entfernen, wird das Kontrollkästchen für zugehörige Kameras automatisch abgewählt.</p>

Name	Beschreibung
Kameras	Listet alle im XProtect-System konfigurierten Kameras auf. Wählen Sie eine Kamera aus der Liste aus und ziehen Sie diese per Drag & Drop zum gewünschten Zugangspunkt, um diese beiden miteinander zu verknüpfen.

Registerkarte Zugangskontrollereignisse (Zugangskontrolle)

Ereigniskategorien erlauben es Ihnen, Ereignisse zu gruppieren. Die Konfiguration von Ereigniskategorien betrifft das Verhalten der Zugangskontrolle im XProtect-System und erlaubt es Ihnen beispielsweise einen Alarm einzustellen, der einen einzelnen Alarm in mehreren Ereignistypen auslöst.


Name	Beschreibung
Zugangskontrollereignis	Listet die Zugangskontrollereignisse auf, die vom Zugangskontrollsystem importiert wurden. Das Integrations-Plug-in steuert die standardmäßige Aktivierung und Deaktivierung von Ereignissen. Sie können Ereignisse jederzeit nach der Integration deaktivieren oder aktivieren. Sobald ein Ereignis aktiviert ist, wird es in der XProtect Ereignisdatenbank gespeichert und steht beispielsweise dem Filtern im XProtect Smart Client zur Verfügung.
Quellentyp	Zeigt die Zugangskontrolleinheit, die das Zugangskontrollereignis auslösen kann.
Ereigniskategorie	Weisen Sie keine, eine oder mehrere Ereigniskategorien den Zugangskontrollereignissen zu. Das System ordnet automatisch zugehörige Ereigniskategorien zu den Ereignissen während der Integration zu. Dies aktiviert ein Standard-Setup im XProtect-System. Sie können die Zuordnung zu jeder Zeit ändern. Integrierte Ereigniskategorien sind: <ul style="list-style-type: none"> • Zugang verweigert • Zugang gewährt • Zugangsanforderung • Alarm

Name	Beschreibung
	<ul style="list-style-type: none"> • Fehler • Warnung <p>Ereignisse und Ereigniskategorien, die vom Integrations-Plug-in festgelegt werden, erscheinen ebenfalls, allerdings können Sie auch Ihre eigenen Ereigniskategorien festlegen; siehe Benutzerdefinierte Kategorien.</p> <div style="border: 1px solid #ccc; background-color: #f9e79f; padding: 10px; margin-top: 10px;">  <p>Wenn Sie die Ereigniskategorien in XProtect Corporate ändern, stellen Sie sicher, dass die bestehenden Zugangskontrollregeln weiterhin funktionieren.</p> </div>
Benutzerdefinierte Kategorien	<p>Erlaubt es Ihnen benutzerdefinierte Ereigniskategorien zu erstellen, zu ändern oder zu löschen.</p> <p>Sie können Ereigniskategorien erstellen, wenn die integrierten Kategorien nicht Ihren Anforderungen entsprechen, bspw. in Verbindung mit der Festlegung von auslösenden Ereignissen für Zugangskontrollaktionen.</p> <p>Die Kategorien werden global für alle Integrationssystem zum XProtect-System hinzugefügt. Sie erlauben die Einrichtung von systemübergreifender Steuerung, z. B. bei Alarmdefinitionen.</p> <p>Wenn Sie eine benutzerdefinierte Ereigniskategorie löschen, erhalten Sie eine Warnung, falls diese von einer Integration verwendet wird. Sollten Sie diese dennoch löschen, funktionieren keine der Konfigurationen in dieser Kategorie (z. B. Zugangskontrollaktionen) mehr.</p>

Registerkarte „Zugangsanforderungsbenachrichtigung“ (Zugangskontrolle)

Sie können Zugangsanforderungsbenachrichtigungen festlegen, die auf der XProtect Smart Client-Anzeige erscheinen sollen, wenn ein Ereignis auftritt.

Name	Beschreibung
Name	Geben Sie einen Namen für die Zugangsanforderungsbenachrichtigung ein.

Name	Beschreibung
<p>Zugangsanforderungsbenedachrichtigung hinzufügen</p>	<p>Klicken Sie, um Zugangsanforderungsbenedachrichtigungen hinzufügen und festzulegen.</p> <p>Klicken Sie auf das X an der rechten Seite, um eine Benedachrichtigung zu löschen.</p> <div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;">  <p>Wenn ein Benutzer von XProtect Smart Client sich in den übergeordneten Standort in einer Milestone Federated Architecture-Hierarchie einloggt, erscheinen Zugangsanforderungsbenedachrichtigungen des untergeordneten Standorts ebenfalls in XProtect Smart Client.</p> </div>
<p>Details der Zugangsanforderungsbenedachrichtigung</p>	<p>Bestimmt, welche Kameras, Mikrofone oder Lautsprecher in den Zugangsanforderungsbenedachrichtigungen erscheint, wenn ein gewisses Ereignis auslöst. Bestimmt auch den Alarmton wenn die Benedachrichtigung aufpoppt.</p>
<p>Befehl hinzufügen</p>	<p>Wählen Sie aus, welche Befehle als Schaltflächen im Dialogfenster der Zugangsanforderungsbenedachrichtigung in XProtect Smart Client zur Verfügung stehen sollen.</p> <p>Zugehörige Zugangsanfragebefehle:</p> <ul style="list-style-type: none"> • Aktiviert alle Befehle in Bezug auf Zugangsanforderungsoperationen, die in der Quelleinheit verfügbar sind. Zum Beispiel, Tür öffnen <p>Alle zugehörigen Befehle:</p> <ul style="list-style-type: none"> • Aktiviert alle Befehle in der Quelleinheit <p>Zugangskontrollbefehl:</p> <ul style="list-style-type: none"> • Aktiviert einen ausgewählten Zugangskontrollbefehl <p>Systembefehl:</p> <ul style="list-style-type: none"> • Aktiviert ein Befehl, der im XProtect-System voreingestellt ist <p>Klicken Sie auf das X an der rechten Seite, um ein Befehl zu löschen.</p>

Registerkarte „Karteneinhaber“ (Zugangskontrolle)

Verwenden Sie die Registerkarte **Karteneinhaber**, um Informationen über Karteneinhaber im Zugangskontrollsystem zu überprüfen.

Name	Beschreibung
Karteneinhaber suchen	Geben Sie die Buchstaben des Namens eines Karteneinhabers ein und, sofern dieser existiert, erscheint er in der Liste.
Name	Listet die Namen der Karteneinhaber auf, die aus dem Zugangskontrollsystem abgerufen wurden.
Typ	Listet den Karteneinhabertypen auf, zum Beispiel: <ul style="list-style-type: none"> • Mitarbeiter • Wache • Gast

Wenn Ihr Zugangskontrollsystem das Hinzufügen/Löschen von Bildern im XProtect-System unterstützt, können Sie den Karteneinhaber Bilder hinzufügen. Dies ist besonders nützlich, wenn Ihr Zugangskontrollsystem keine Bilder der Karteneinhaber einschließt.

Name	Beschreibung
Bild auswählen	Legen Sie den Dateipfad für ein Bild des Karteneinhabers fest. Diese Schaltfläche ist nicht sichtbar, wenn das Zugangskontrollsystem die Bilder verwaltet. Erlaubte Dateiformate sind: .bmp, .png, und .jpg. Bilder werden an die maximale Ansichtsgröße angepasst. Milestone empfiehlt, dass Sie ein quadratisches Bild verwenden.
Bild löschen	Klicken Sie, um das Bild zu löschen. Wenn das Zugangskontrollsystem ein Bild hatte, wird dieses Bild nach der Löschung angezeigt.

Konfiguration von Zugangsanfragen

Es gibt verschiedene Typen von Zugangskontrollereignissen, beispielsweise **Zugang verweigert** und **Zugang gewährt**. Zum Aktivieren von Zugangsanfragenachrichten müssen Sie den Ereignistyp mit der Ereigniskategorie **Zugangsanfrage** verbinden. Als Standard ist **Zugang verweigert** mit **Zugangsanfrage** verbunden: Zugangsanfragenachrichten werden nur gesendet, wenn jemandem der Zugang verweigert wird. Um diese Einstellung zu ändern, folgen Sie den Schritten in diesem Thema.

Anforderungen: Sie müssen Benachrichtigungen über die Rollen der Client-Benutzer aktivieren. Um dieses für die Rolle zu tun, klicken Sie auf die Registerkarte **Zugangskontrolle**, wählen Sie **Zugangskontrolle** und wählen Sie dann das Kontrollkästchen **Benachrichtigungen empfangen**.

Schritte:

1. Klicken Sie im Fenster **Standort-Navigation** auf **Zugangskontrolle**.
2. Suchen Sie auf der Registerkarte **Zugangskontrollereignisse** in der Spalte **Zugangskontrollereignis** den Ereignistyp, den Sie bearbeiten wollen.
3. Zur Deaktivierung von Zugangsanfragen für einen Ereignistyp klicken Sie auf die Spalte **Ereigniskategorie** wählen Sie das Kontrollkästchen **Zugangsanfrage** und leeren Sie es.
4. Zur Aktivierung von Zugangsanfragen für einen Ereignistyp klicken Sie in der Spalte **Ereigniskategorie** auf das Kontrollkästchen **Zugangsanfrage** und wählen Sie dies aus.
5. Speichern Sie die Änderungen.



helpfeedback@milestone.dk

Über Milestone

Milestone Systems ist ein weltweit führender Anbieter von Open-Platform-Videomanagementsoftware – Technologie, die Unternehmen hilft für Sicherheit zu sorgen, Ressourcen zu schützen und die Wirtschaftlichkeit zu erhöhen. Milestone Systems ist die Basis einer Open Platform Community, die die Zusammenarbeit und Innovation bei der Entwicklung und dem Einsatz von Netzwerkvideotechnologie vorantreibt und für zuverlässige, individuell anpassbare Lösungen sorgt, die sich an über 150.000 Standorten auf der ganzen Welt bewährt haben. Milestone Systems wurde 1998 gegründet und ist ein eigenständiges Unternehmen der Canon Group. Weitere Informationen erhalten Sie unter <https://www.milestonesys.com/>.

