

Superior KeyPad Outdoor Fibra

Kabelgebundenes Bedienteil mit Authentifizierung über Pass, Tag, Smartphone und Codes. Für den Innen- und Außenbereich.

Spaces steuern – bei Wind und Wetter

Entdecken Sie die Allwetterlösung für Sicherheit und Automatisierung. Schalten Sie das Sicherheitssystem scharf oder unscharf, aktivieren Sie den Nachtmodus, verwalten Sie Gruppen und führen Sie Szenarien mit nur einem Bedienteil aus. Nutzen Sie klassische ZugangsCodes oder berührungslose Technologien. Das ultraflache Gehäuse passt überall hin und verfügt über große, handschuhfreundliche mechanische Tasten. Das robuste Gehäuse wurde so entwickelt, dass es selbst extremen Bedingungen standhält und auch nach Stößen oder Beschädigungen voll funktionsfähig bleibt. Ein kompromisslos sicheres Bedienteil, das Eindringlingen keine Chance lässt.

Hauptmerkmale

Unterstützung von Transpondern Pass-Karten und Tag-Schlüsselanhänger mit DESFire®-Technologie	BedrohungsCodes wenn ein Benutzer gezwungen wird, ein System zu deaktivieren	Vier Arten von ZugangsCodes • Bedienteil-Code • persönliche Codes • Codes für nicht registrierte Benutzer • Einsatzteam-Code	Große mechanische Tasten schnelle Reaktion, selbst bei der Bedienung mit Handschuhen oder Fäustlingen
Berührungslose Steuerung über Smartphone mit Bluetooth Low Energy (BLE)	Zwei Betriebsmodi: Sicherheit Automatisierung Einfacher Moduswechsel durch langes Drücken der OK-Taste	Schutz gegen das Erraten von Codes	Bypass-Modus Das Bedienteil startet eine Eingangsverzögerung, um die Unscharfschaltung zu bestätigen
Eingebaute Paniktaste	IP66 Schutz vor Staub, Wasser und extremen Temperaturen	IK08 Schutz gegen Schläge und Erschütterungen	Bis zu 2000 m (6550 ft) kabelgebundene Kommunikation¹ mit einer Ajax Hub-Zentrale oder einem Modul zur Verlängerung der Fibra-Buslinie
Fernaktualisierung der Firmware	Fernsteuerung und -konfiguration	Sabotagealarm das Gehäuse hat zwei Sabotagekontakte	60 dB-Summer für akustische Signale informiert über Alarme, Scharf-/Unscharfschaltung, Eingangs-/Ausgangsverzögerung, Türöffnung und andere Ereignisse
Fibra Kabelverbindung	Edelstahlgehäuse in drei Farben		
Verbindung mit anderen Fibra Geräten auf der Leitung	Detaillierte Push-Benachrichtigungen Ajax Zuhause: Hinterhof scharf durch John Ajax Büro: Nachtmodus aktiviert durch Ann	Sehr geringer Stromverbrauch	Konformität Grade 3 (EN 50131) PD 6662:2017 ANSI/SIA CP-01-2019 INCERT SSF

In einem Ajax System können Geräte aus allen Produktkategorien kombiniert werden:
Einbruchschutz (sowohl Superior als auch Baseline), **Videoüberwachung**, **Brandschutz und Sicherheit** oder **Komfort und Automatisierung**. Stellen Sie das System zusammen, das Ihren Anforderungen entspricht, und steuern Sie es über eine einzige Schnittstelle.

Dies ist ein Gerät der **Superior Produktlinie**. Nur akkreditierte Partner von Ajax Systems dürfen Superior Produkte installieren, verkaufen und warten.

In jeder Umgebung einsatzbereit

	Lagerhaus	Büro	Produktionsstätte	Privatwohnung
--	-----------	------	-------------------	---------------

Ein Gerät, drei Aufgaben

Anlagesteuerung	Steuerung von Automatisierungsgeräten	Akustische Signale und LED-Anzeige
Verwalten Sie die Sicherheit eines gesamten Objekts, einzelner Gruppen oder aktivieren Sie den Nachtmodus – alles mit nur einem Gerät. Zudem verfügt es über eine individuell konfigurierbare Funktionstaste, die als Paniktaste oder zur Stummschaltung des Feueralarms genutzt werden kann. KeyPad Outdoor kann auch im Bypass-Modus betrieben werden, bei dem eine Eingangsverzögerung aktiviert wird. Dies gibt dem Benutzer Zeit, das System über das Hauptbedienfeld zu deaktivieren, z. B. mit einem zusätzlichen Ajax Bedienteil, das im Innenbereich installiert ist.	Das Bedienteil kann ein oder mehrere Automatisierungsgeräte wie Schalter, Relais, Stecker, Steckdosen oder Absperrventile steuern. So kann der Benutzer beispielsweise das Garagentor öffnen und die Außenbeleuchtung einschalten, wenn er nach Hause kommt (oder das Garagentor schließen und die Beleuchtung ausschalten, wenn er die Garage verlässt). Ein einziger Druck auf die OK-Taste genügt, um ein Szenario zu starten. Die Hintergrundbeleuchtung der Tasten zeigt den Status der Automatisierungsgeräte an ² : Rot steht für ausgeschaltet, Grün für eingeschaltet.	Das handschuhfreundliche Bedienteil verfügt über hinterleuchtete Ziffern, die dauerhaft lesbar bleiben. Der integrierte Summer informiert über Alarme, Türöffnungen (Türglocke), Scharf-/Unscharfschaltungen sowie Eingangs- und Ausgangsverzögerungen. Sowohl die Helligkeit der LEDs als auch die Lautstärke des Summers lassen sich bequem über die Ajax Apps anpassen.
• Sicherheitsmanagement für das Gesamtsystem oder einzelne Gruppen • Nachtmodus-Aktivierung • Bypass-Modus zur Auslösung einer Eingangsverzögerung zur Bestätigung der Unscharfschaltung	• Steuerung von Automatisierungsgeräten mit einem Tastendruck auf die OK-Taste • Statusanzeige eines Automatisierungsgerätes durch Hintergrundbeleuchtung	• Akustische Signalisierung von Alarmen und Ereignissen • Mechanische Tasten mit hinterleuchteten, nicht verblassenden Ziffern • Anpassbare Lautstärke und einstellbare LED-Helligkeit

Schnelle und sichere Authentifizierung

Das Bedienteil bietet drei einfache Nutzungsmöglichkeiten, sodass die Benutzer flexibel wählen können, was am besten zu ihnen passt. Die Ajax Apps zeigen alle Ereignisse an, einschließlich Benutzeraktivitäten und Authentifizierungsdetails.

Pass-Karte und Tag-Schlüsselanhänger

Mit einem Ajax Pass oder Tag kann das System mit einer einfachen Handbewegung scharf oder unscharf geschaltet werden: Halten Sie einfach den Transponder an den Kartenleser. Jede Nutzung eines Transponders wird im Ereignisprotokoll der Ajax App aufgezeichnet. Der Administrator kann Transponder jederzeit widerrufen, einschränken oder vorübergehend sperren. Außerdem

können Administratoren die Benutzerrechte ändern, indem sie den Zugang zu bestimmten Gruppen gewähren oder einschränken.

Die Tastatur ist mit der DESFire®-Technologie ausgestattet, einer kontaktlosen Lösung zur Benutzeridentifikation mittels Karte oder Schlüsselanhänger. DESFire® basiert auf dem internationalen Standard ISO 14443 und bietet eine umfassende 128-Bit-Verschlüsselung sowie Kopierschutz. Diese Technologie wird auch in Verkehrs- und Logistiksystemen europäischer Hauptstädte sowie bei Zutrittssystemen der NASA eingesetzt.

Smartphone

Lassen Sie sich vom Systemadministrator Zugriffsrechte erteilen und autorisieren Sie Ihr Smartphone über die Ajax Apps zur kontaktlosen Steuerung des Bedienteils via Bluetooth Low Energy (BLE).

BLE (Bluetooth Low Energy) ist ein Funkprotokoll, das es ermöglicht, ein Bedienteil mit einem Smartphone anstelle von Transpondern zu steuern. Die Datenübertragung zwischen Smartphone und Bedienteil erfolgt verschlüsselt. Das System enthält Maßnahmen gegen Spoofing, um unbefugten Zugriff durch Eindringlinge zu verhindern. KeyPad Outdoor Fibra unterstützt iOS- und Android-Smartphones mit BLE 4.2 oder höher.

Zugangscode

Das Bedienteil unterstützt mehrere Arten von Zugangscode:

- **Bedienteil-Code (einer pro Bedienteil):** Ein allgemeiner Code für das Bedienteil.
- **Persönliche Codes:** Individuelle Zugangscode, die von jedem Systembenutzer in seiner Ajax App persönlich konfiguriert werden.
- **Codes für nicht registrierte Benutzer:** Codes, die von einem Administrator für Reinigungspersonal oder Immobilienmakler erstellt werden, die keine Ajax Konten haben. Diese Benutzer können das Bedienteil nutzen, haben jedoch keinen Zugriff auf Systeminformationen.
- **Einsatzteam-Code:** Ein Zugangscode, der von einem Verwalter konfiguriert wird, um den Einsatzkräften nach einem Alarm Zugang zu den Räumlichkeiten zu gewähren, wenn der Eigentümer nicht zu Hause ist. Der Code wird nur nach einem Alarm aktiviert und ist für einen bestimmten Zeitraum gültig.

Transponder

Pass und Tag sind mit originalen DESFire®-Chips ausgestattet. Sie erfüllen die gleiche Funktion, sind jedoch in unterschiedlichen Gehäusen erhältlich. Ein Tag oder Pass kann bis zu 13 Sicherheitssysteme steuern. Die Transponder werden separat in Sets zu 3, 10 oder 100 Stück angeboten.

Pass Kontaktlose Karte zur Steuerung der Sicherheitsmodi	Tag Kontaktloser Schlüsselanhänger zur Steuerung der Sicherheitsmodi
--	--

Kontrolle des Fernzugriffs

Ändern Sie Zugangsrechte und Codes in Echtzeit über die Ajax Apps. Verlorene Transponder und kompromittierte Codes können innerhalb von Minuten aus der Ferne geändert werden, ohne dass ein Installateur das Objekt besuchen muss.

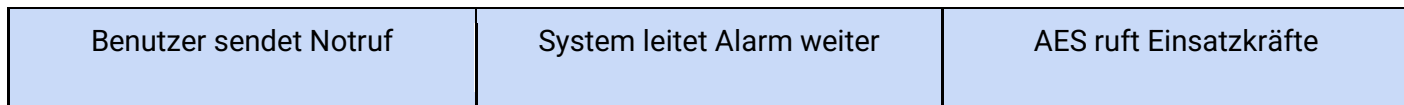
- Möglichkeit, Codes aus der Ferne zu ändern
- Möglichkeit, die Zugangsrechte der Benutzer aus der Ferne zu ändern
- Fernsperrung von Karten, Schlüsselanhängern und Smartphones

Zugang für nicht registrierte Benutzer

Durch eine einfache Zuweisung in den Hub-Einstellungen kann ein PRO einen temporären Zugangscode für Büroangestellte, Mitarbeiter von Reinigungsfirmen oder andere verifizierte Besucher erstellen.

- Benachrichtigungen über das Hinzufügen, Entfernen oder Deaktivieren von Codes
- Eindeutiger Name und ID-Nummer zur Identifizierung des Benutzers
- Bis zu 99 Codes für nicht registrierte Benutzer

Effektive Hilfe im Notfall



Das Bedienteil ist mit einer Paniktaste ausgestattet, die bei Betätigung einen Alarm auslöst. Diese kann so konfiguriert werden, dass der Benutzer einen Notruf sendet, Sirenen aktiviert oder ein Automatisierungsszenario startet. Wenn der Benutzer gezwungen ist, Einbrechern Zutritt zu gewähren, kann er einen Bedrohungscode verwenden, um eine Unscharfschaltung vorzutäuschen: Das Bedienteil simuliert eine normale Unscharfschaltung und sendet sofort einen Alarm an den Sicherheitsdienst, um diesen über den Notfall zu informieren. In der Zwischenzeit bleiben die Ajax Apps und die im Objekt installierten Sirenen stumm, um den Benutzer nicht zu gefährden.

- Panikknopf zur Benachrichtigung im Alarmfall
- Bedrohungscode zur Simulation der Unscharfschaltung

Entdecken Sie zukunftsichere Hardware

Wetterfestes IP66-Gehäuse mit Schlagfestigkeit IK08

hält extremen Bedingungen wie Regen, Schnee und direkter Sonneneinstrahlung stand

Große mechanische Tasten

für einfachen und schnellen Zugriff, auch mit Handschuhen oder Fäustlingen

LED-Hintergrundbeleuchtung

zeigt die Sicherheitsmodi, die Ausführung von Szenarien, den Moduswechsel und andere Befehle an

DESFire®- und BLE-Lesegerät

für kontaktlosen Zugang mit Tag, Pass oder Smartphone

60 dB-Summer

informiert über Alarmer, Scharf-/Unscharfschaltung, Eingangs-/Ausgangsverzögerung, Türöffnung und andere Ereignisse

SmartBracket-Montageplatte

ermöglicht die Installation des Bedienteils, ohne das Gehäuse zu zerlegen

Abnehmbare Klemmleiste

vereinfacht die Verkabelung

Zwei Sabotagekontakte

benachrichtigen bei Versuchen, das Bedienteil von der Wand oder der Montageplatte zu entfernen

Befestigungsschraube

sichert das Bedienteil an der Montageplatte

Einzigartige Kabeltechnologie

Das Ajax System verwendet das firmeneigene Protokoll Fibra für eine sichere und bidirektionale Funkkommunikation.

Verschlüsselung und Geräteauthentifizierung während jeder Kommunikationssitzung schützen vor Sabotage, Manipulation und Datendiebstahl. Die Fibra Leitungen sind multifunktional und ermöglichen den Anschluss verschiedener Geräte: Sirenen, Bedienteile und Melder mit Fotoverifizierung.

- Bis zu 2000 m (6550 ft) kabelgebundene Kommunikation¹ mit einer Hub-Zentrale oder einem Modul, das die Fibra Leitung verlängert
- Eine Leitung für verschiedene Gerätetypen
- Störungsfreie Bildübertragung über Fibra Leitung
- Schutz vor Sabotage und Signalfälschung

Energieeffizienz geht vor

Die Fibra Kommunikation ist äußerst energieeffizient: Das Bedienteil verbraucht maximal nur bis zu 0,6 W. Fibra arbeitet nach dem

TDMA-Prinzip. Jedes Gerät hat eine kurze Zeit, um Daten mit einer Hub-Zentrale auszutauschen, die restliche Zeit ist das Kommunikationsmodul inaktiv. Dadurch wird der Stromverbrauch deutlich reduziert und gleichzeitig werden Störungen minimiert – selbst bei gleichzeitiger Kommunikation mehrerer Geräte.

- Stromverbrauch von bis zu 0,6 W
- TDMA- und Energiesparmodus

Erweiterte Systemüberwachung

Das Bedienteil ist Teil des Ajax Ökosystems und somit ein echtes IoT-Gerät. Jedes Element dieses Ökosystems wird kontinuierlich überwacht. Das Bedienteil tauscht Daten mit einer Hub-Zentrale über das Fibra Protokoll aus. Die Hub-Zentrale nutzt die bidirektionale Kommunikation mit der Ajax Cloud, um die Ajax Apps mit Echtzeitinformationen zu versorgen. Das Ajax System überprüft den Gerätestatus jede Minute. Wenn ein Bedienteil ein Problem hat, erhalten Sie eine Benachrichtigung.

- IoT-Gerät
- Einstellung des Ping-Intervalls in den Einstellungen der Hub-Zentrale
- Direkte Wartungsmeldungen

Sabotagealarm Das Gehäuse des Geräts ist mit zwei Sabotagekontakten ausgestattet, die anzeigen, wenn das Bedienteil von der Oberfläche oder der Montageplatte entfernt wird. Zusätzlich ist das Bedienteil mit einer Befestigungsschraube an der Unterseite des Gehäuses gesichert, um den Widerstand gegen Demontageversuche zu erhöhen.	Schutz gegen das Erraten von Codes Das System sperrt das Bedienfeld nach drei erfolglosen Versuchen für eine bestimmte Zeit und meldet den Vorfall sofort, sodass Unbefugte den Zugangscode nicht erraten können.	Kopierschutz für Transponder Das Bedienteil reagiert nur auf Transponder, die über Ajax Apps autorisiert wurden. Die DESFire®-Chips in Karten und Schlüsselanhängern entsprechen dem internationalen Standard ISO 14443 und kombinieren eine umfassende 128-Bit-Verschlüsselung mit einem Kopierschutz. Das BLE-Lesegerät reagiert einfach nicht auf ein Smartphone, wenn es nicht über Ajax Apps autorisiert wurde.
Robustes Gehäuse Das Bedienteil hat die Schutzart IP66 und hält Temperaturen von –25 °C bis +60 °C (von –13 °F bis 140 °F) stand. Es funktioniert zuverlässig bei Regen und Schnee. Die mechanischen Tasten verblassen nicht, wodurch es unmöglich wird, die am häufigsten verwendeten Ziffern zu erkennen und den Code zu ermitteln. Das Gehäuse erfüllt die Anforderungen der Stoßfestigkeitsklasse IK08 und bleibt auch bei Stößen oder Beschädigungen stabil.	Authentifizierung zum Schutz vor Signalmanipulationen Jede Kommunikationssitzung zwischen der Hub-Zentrale und dem Gerät beginnt mit einer Authentifizierung: Das System überprüft eindeutige Parameter des Geräts. Wenn ein Parameter die Prüfung nicht besteht, werden alle Befehle von diesem Gerät von der Hub-Zentrale ignoriert.	Erkennung eines Kommunikationsausfalls Das Gerät tauscht regelmäßig Daten mit der Hub-Zentrale aus. Selbst bei Verwendung des minimalen Abfrageintervalls (drei Datenpakete alle 12 Sekunden) dauert es nur 36 Sekunden, um einen Kommunikationsausfall zu erkennen und den Sicherheitsdienst und den Benutzer über den Vorfall zu informieren.
Schutz gegen Kurzschluss Das System erkennt sofort einen Kurzschluss in der Leitung und alarmiert den Sicherheitsdienst und den Benutzer. Nach Behebung des Problems müssen die Sicherungen nicht ausgetauscht werden: Das	Datenverschlüsselung Alle Daten, die das System speichert und überträgt, sind durch Blockverschlüsselung mit einem dynamischen Schlüssel geschützt. Die Verschlüsselung macht es extrem schwierig, das Gerät zu manipulieren und die	Detaillierte Push-Benachrichtigungen Das Ajax-System informiert über Alarme und Ereignisse mit sofortigen Benachrichtigungen: Sicherheitsdienste und Benutzer erhalten genaue Informationen darüber, welches Gerät wann und wo ausgelöst wurde.

System stellt den Betrieb automatisch wieder her.	Daten zu ersetzen oder zu stehlen.	
Regelmäßige Abfrage Das Gerät tauscht regelmäßig Daten mit der Hub-Zentrale aus. Das System überwacht den Status jedes Geräts und meldet Störungen oder Kommunikationsfehler.		

Fibra Leitungsschutz des nächsten Niveaus

Lernen Sie LineProtect kennen, ein Modul, das Ajax Hub-Zentralen und die daran angeschlossenen kabelgebundenen Geräte vor Sabotage schützt, wenn ein Eindringling einen Kurzschluss verursacht, 110/230 V~ anlegt oder einen Elektroschocker benutzt.

PRO ist König

Der Mythos, dass kabelgebundene Systeme schwierig zu installieren sind, ist widerlegt. Ajax ist es gelungen, den teuren, zeitaufwändigen und staubigen Installations- und Wartungsprozess so weit wie möglich zu vereinfachen, indem für jeden Arbeitsschritt die besten Werkzeuge entwickelt wurden. Das Gerät muss während der Installation nicht auseinandergenommen werden. Benutzerfreundliche Ajax Apps helfen dabei, das Gerät schnell in das System zu integrieren und es jederzeit aus der Ferne neu zu konfigurieren. Keine Programmierung erforderlich: Alles ist sofort verfügbar.

Rechner der Fibra Stromversorgung

Das Online-Tool liefert Sicherheitstechnikern detaillierte Daten über den Stromverbrauch von Geräten und ermöglicht so eine einfache Einschätzung des Verkabelungsprojekts vor der Installation. Es unterstützt die Projektplanung in Echtzeit, identifiziert potenzielle Schwachstellen und schlägt sofort passende Lösungen vor. Die Ergebnisse können anschließend als PDF-Datei heruntergeladen werden.

Installation

Mit der SmartBracket Montageplatte kann das Gerät einfach an einer Wand befestigt werden. Der Montagesatz enthält alle notwendigen Befestigungselemente. Das Gerät muss nicht zerlegt werden: Die Klemmleiste befindet sich außerhalb des Gehäuses hinter dem SmartBracket, so dass die Hardware bei der Installation nicht beschädigt wird. Die Klemmleiste ist abnehmbar, was den gesamten Prozess vereinfacht. Eine eingebaute Wasserwaage hilft dem Fachmann bei der perfekten Ausrichtung. Löcher zum Fixieren der Kabel mit Kabelbindern im Inneren des SmartBracket dienen der besseren Organisation der Kabel.

- Das Gehäuse des Geräts muss nicht zerlegt werden
- Abnehmbare Klemmleiste
- Alle erforderlichen Befestigungsmittel sind im Montagesatz enthalten
- Schraube zur Befestigung des Gerätes an einer Montageplatte

Einrichtung

Das Gerät wird automatisch mit einer Hub-Zentrale gekoppelt, indem die Fibra Leitung gescannt wird. Diese Funktion ist in den Desktop- oder mobilen PRO Apps verfügbar. Der Installateur muss dem Gerät lediglich einen Namen geben und es einem Raum und einer Sicherheitsgruppe zuordnen. Alternativ kann das Gerät auch durch Scannen des QR-Codes oder durch manuelle Eingabe der Geräte-ID hinzugefügt werden.

- Scannen des QR-Codes oder der Fibra Leitung, um das Gerät mit einer Hub-Zentrale zu verbinden
- Geräteidentifikation durch Auslösen des Gerätes oder Blinken der LED
- Optimale Standardeinstellungen für die wichtigsten Anforderungen

Konfiguration

Intuitive Ajax Apps ermöglichen die Fernkonfiguration und den Zugriff auf alle Geräteinformationen von überall aus – über ein Smartphone oder einen Computer mit Internetzugang. Ein Installateur kann Einstellungen aus der Ferne ändern und Dienste sofort bereitstellen, ohne das Objekt besuchen zu müssen.

- Konfigurieren und Testen aus der Ferne oder vor Ort
- Apps für iOS, Android, macOS und Windows
- Konten für Unternehmen und Installateure

Überwachung

Ein Ajax System überträgt Alarme an die Überwachungs-App **PRO Desktop** oder an eine dritte NSL. Der Sicherheitsdienst erhält Alarmmeldungen in weniger als einer Sekunde. Diese enthalten alle notwendigen Informationen: den Namen des Geräts, den Zeitpunkt des Ereignisses und sogar den genauen Raum, in dem sich das Gerät befindet. Der Sicherheitsdienst erhält zudem eine Foto- oder Videobestätigung, die den Grund des Alarms darstellt.

- Volle Adressierbarkeit der angeschlossenen Geräte
- Sofortige In-App-Benachrichtigungen
- Alarm- und Ereignisüberwachung über PRO Desktop oder andere Überwachungssoftware

¹ Kabelgebundene Ajax Geräte haben eine Kommunikationsreichweite von bis zu 2000 m (6550 ft) ohne Modul zur Leitungsverlängerung, wenn U/UTP Cat.5 Twisted-Pair-Kabel verwendet werden. Andere Kabel können abweichende Werte aufweisen. Bitte verwenden Sie den Rechner der Fibra Stromversorgung, um das Projekt des kabelgebundenen Systems vor der Installation zu überprüfen.

² Wenn das Bedienteil ein Szenario steuert, an dem mehrere Automatisierungsgeräte beteiligt sind, kann der Status des Geräts oder des Szenarios nicht durch die OK-Taste angezeigt werden. Stattdessen signalisiert das Bedienteil durch einen kurzen Signalton, wenn die eingestellte Aktion abgeschlossen ist.