

AXIS A1610-B Network Door Controller

Manuel d'utilisation

AXIS A1610-B Network Door Controller

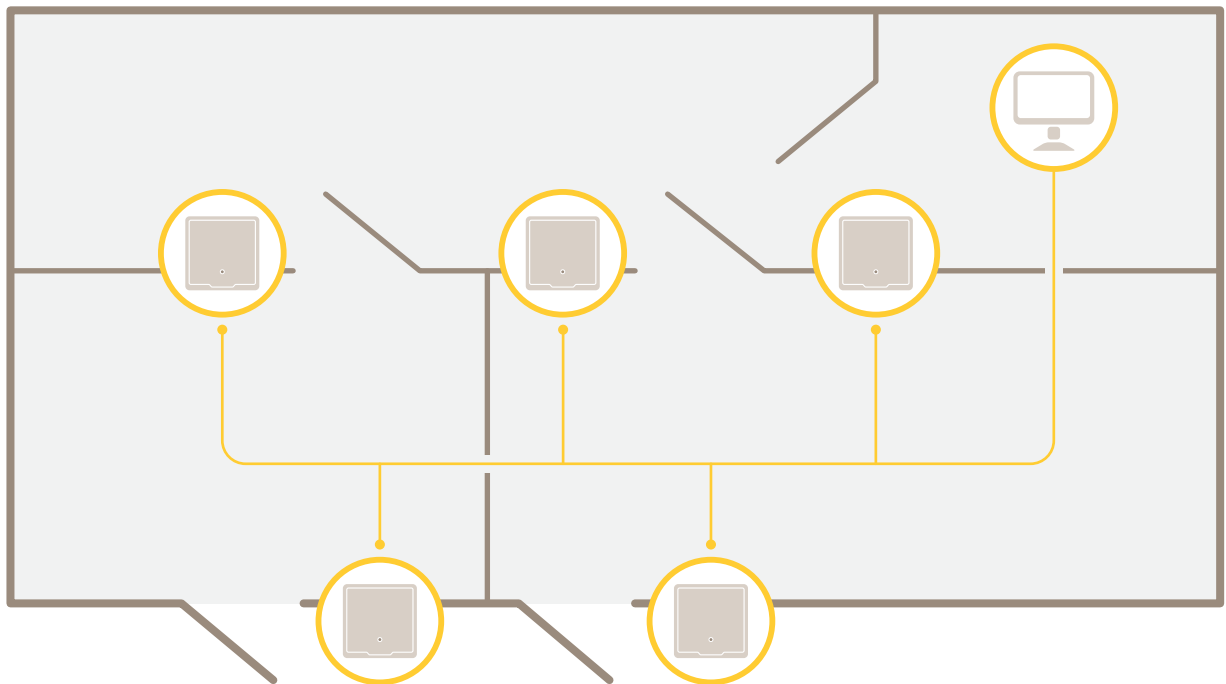
Table des matières

Présentation de la solution	3
Premiers pas	5
Trouver le périphérique sur le réseau	5
Ouvrir l'interface web du périphérique	5
Définition d'un nouveau mot de passe pour le compte root	5
Mots de passe sécurisés	5
Vérifiez que personne n'a saboté le firmware.	6
Vue d'ensemble de l'interface web	6
Configurer votre périphérique	7
Interface du périphérique	8
Statut	8
Contrôle d'accès	9
Système	9
Maintenance	19
En savoir plus	20
Sécurité	20
Caractéristiques	21
Vue d'ensemble du produit	21
Voyants DEL	21
Boutons	22
Connecteurs	22
Dépannage	29
Réinitialiser les paramètres par défaut	29
Options du firmware	29
Vérifier la version du firmware actuel	29
Mettre à niveau le firmware	29
Problèmes techniques, indications et solutions	30
Facteurs ayant un impact sur la performance	31
Contacter l'assistance	31

AXIS A1610-B Network Door Controller

Présentation de la solution

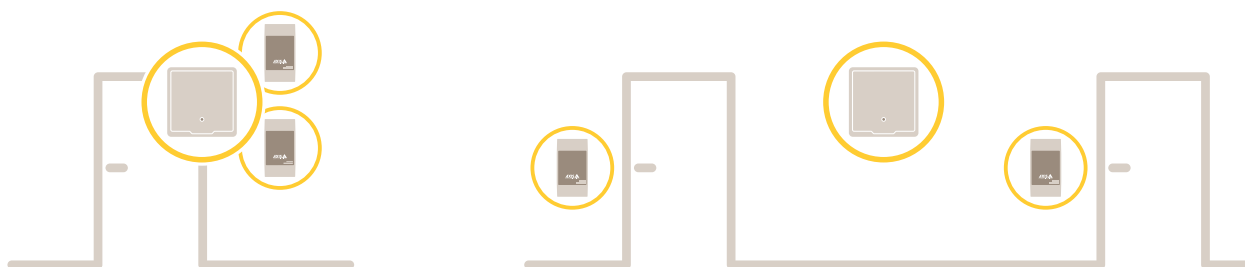
Présentation de la solution



Le contrôleur de porte réseau peut facilement être connecté et alimenté par votre réseau IP existant sans câblage spécial.

AXIS A1610-B Network Door Controller

Présentation de la solution



Chaque contrôleur de porte réseau est un périphérique intelligent qui se monte facilement à proximité d'une porte. Il peut alimenter et contrôler jusqu'à deux lecteurs.

AXIS A1610-B Network Door Controller

Premiers pas

Premiers pas

Trouver le périphérique sur le réseau

Pour trouver les périphériques Axis présents sur le réseau et leur attribuer des adresses IP sous Windows®, utilisez AXIS IP Utility ou AXIS Device Manager. Ces applications sont gratuites et peuvent être téléchargées via axis.com/support.

Pour plus d'informations sur la détection et l'assignation d'adresses IP, accédez à *Comment assigner une adresse IP et accéder à votre périphérique*.

Prise en charge du navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

	Chrome™	Firefox®	Edge™	Safari®
Windows®	recommandé	recommandé	✓	
macOS®	recommandé	recommandé	✓	✓
Linux®	recommandé	recommandé	✓	
Autres systèmes d'exploitation	✓	✓	✓	✓*

*Pour utiliser l'interface Web AXIS OS avec iOS 15 ou iPadOS 15, accédez à **Settings > Safari > Advanced > Experimental Features** (Paramètres > Safari > Avancé > Fonctionnalités expérimentales) et désactivez *NSURLSession Websocket*.

Si vous avez besoin de plus d'informations sur les navigateurs recommandés, consultez le *portail AXIS OS*.

Ouvrir l'interface web du périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis.
Si vous ne connaissez pas l'adresse IP, utilisez AXIS IP Utility ou AXIS Device Manager pour identifier le périphérique sur le réseau.
2. Saisissez le nom d'utilisateur et le mot de passe. Si vous accédez au périphérique pour la première fois, vous devez définir le mot de passe root. Voir *Définition d'un nouveau mot de passe pour le compte root à la page 5*.

Définition d'un nouveau mot de passe pour le compte root

Le nom d'utilisateur administrateur par défaut est `root`. Il n'existe pas de mot de passe par défaut pour le compte root. Vous définissez un mot de passe la première fois que vous vous connectez au périphérique.

1. Saisissez un mot de passe. Suivez les instructions sur les mots de passe sécurisés. Voir *Mots de passe sécurisés à la page 5*.
2. Ressaisissez le mot de passe pour le confirmer.
3. Cliquez sur **Add user (Ajouter un utilisateur)**.

Important

Si vous perdez le mot de passe pour le compte root, accédez à *Réinitialiser les paramètres par défaut à la page 29* et suivez les instructions.

AXIS A1610-B Network Door Controller

Premiers pas

Mots de passe sécurisés

Important

Les périphériques Axis envoient le mot de passe initial en texte clair sur le réseau. Pour protéger votre appareil après la première connexion, configurez une connexion HTTPS sécurisée et cryptée, puis modifiez le mot de passe.

Le mot de passe de l'appareil est la principale protection de vos données et services. Les périphériques Axis n'imposent pas de stratégie de mot de passe, car ils peuvent être utilisés dans différents types d'installations.

Pour protéger vos données, nous vous recommandons vivement de respecter les consignes suivantes :

- Utilisez un mot de passe comportant au moins 8 caractères, de préférence créé par un générateur de mots de passe.
- Prenez garde à ce que le mot de passe ne soit dévoilé à personne.
- Changez le mot de passe à intervalles réguliers, au moins une fois par an.

Vérifiez que personne n'a saboté le firmware.

Pour vous assurer que le périphérique dispose de son firmware Axis d'origine ou pour prendre le contrôle total du périphérique après une attaque de sécurité :

1. Réinitialisez les paramètres par défaut. Voir *Réinitialiser les paramètres par défaut à la page 29*.

Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.

2. Configurez et installez le périphérique.

Vue d'ensemble de l'interface web

Cette vidéo vous donne un aperçu de l'interface web du périphérique.



Pour regarder cette vidéo, accédez à la version Web de ce document.

help.axis.com/?&pid=81250§ion=web-interface-overview

Interface web des périphériques Axis

AXIS A1610-B Network Door Controller

Configurer votre périphérique

Configurer votre périphérique

Pour savoir comment configurer votre périphérique, consultez le *manuel d'utilisation d'AXIS Camera Station* ou des solutions tierces.


AXIS A1610-B Network Door Controller


Interface du périphérique


Interface du périphérique


Pour accéder à l'interface du périphérique, saisissez l'adresse IP de ce dernier dans un navigateur Web.


Remarque




La prise en charge des fonctionnalités et des paramètres décrits dans cette section varie d'un périphérique à l'autre. Cette icône  indique que la fonction ou le paramètre n'est disponible que sur certains périphériques.



 Affichez ou masquez le menu principal.


 Accédez à l'aide du produit.

 Changez la langue.

 Définissez un thème clair ou foncé.

   Le menu utilisateur contient :

- les informations sur l'utilisateur connecté.
-  **Changer d'utilisateur** : déconnectez l'utilisateur actuel et connectez un nouvel utilisateur.
-  **Se déconnecter** : déconnectez l'utilisateur actuel.

 Le menu contextuel contient :

- **Analytics data (Données d'analyse)** : acceptez de partager les données de navigateur non personnelles.
- **Feedback (Commentaires)** : partagez vos commentaires pour nous aider à améliorer votre expérience utilisateur.
- **Legal (Informations légales)** : affichez les informations sur les cookies et les licences.
- **About (À propos)** : affichez les informations sur le périphérique, dont la version du firmware et le numéro de série.
- **Ancienne interface du périphérique** : Définissez l'interface du périphérique sur l'interface périphérique existant.

Statut

État de la synchronisation horaire

Affiche les informations de synchronisation NTP, notamment si le périphérique est synchronisé avec un serveur NTP et le temps restant jusqu'à la prochaine synchronisation.

Paramètres NTP : Cliquez pour accéder à la page Date and time (Date et heure) où vous pouvez modifier les paramètres NTP.

Infos sur les périphériques

Affiche les informations sur le périphérique, dont la version du firmware et le numéro de série.

Mettre à niveau le firmware : Cliquez pour accéder à la page de maintenance où vous pouvez mettre à niveau le firmware.

AXIS A1610-B Network Door Controller

Interface du périphérique

Contrôle d'accès

Alarmes

Device motion (Mouvement du périphérique) : déclenche une alarme dans le système lorsque le mouvement du périphérique du contrôleur de porte est détecté.

Casing open (Boîtier ouvert) : déclenche une alarme dans le système lorsque le boîtier ouvert du contrôleur de porte est détecté. Désactiver ce réglage pour les contrôleurs de porte compacts.

External tamper (Sabotage externe) : déclenche une alarme dans le système lorsqu'un sabotage externe est détecté. Par exemple, lorsque l'armoire externe est ouverte ou fermée.

- **Entrée supervisée** : Activez le moniteur de l'état d'entrée et configurez les résistances de fin de ligne.
 - Pour utiliser la première connexion parallèle, sélectionnez **Première connexion parallèle avec une résistance parallèle de 22 K Ω et une résistance série de 4,7 K Ω** .
 - Pour utiliser la première connexion série, sélectionnez **Première connexion série** et sélectionnez une valeur de résistance dans la liste déroulante **Valeurs des résistances**.

Périphériques

Mettre à niveau les lecteurs : Cliquez pour mettre à niveau les lecteurs vers une nouvelle version du firmware. Seuls les lecteurs pris en charge peuvent être mis à niveau lorsqu'ils sont en ligne.

Système

Date et heure

Le format de l'heure dépend des paramètres de langue du navigateur Web.

Remarque

Nous vous conseillons de synchroniser la date et l'heure du périphérique avec un serveur NTP.

Synchronization (Synchronisation) : sélectionnez une option pour synchroniser la date et l'heure du périphérique.

- **Automatic date and time (manual NTS KE servers) (Date et heure automatiques (serveurs NTS KE manuels))**
Synchronisez avec les serveurs d'établissement de clés NTP sécurisés connectés au serveur DHCP.
 - **Serveurs NTS KE manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
- **Automatic date and time (NTP servers using DHCP) (Date et heure automatiques (serveurs NTP utilisant DHCP))** : synchronisez avec les serveurs NTP connectés au serveur DHCP.
 - **Serveurs NTP de secours** : saisissez l'adresse IP d'un ou de deux serveurs de secours.
- **Automatic date and time (serveurs NTP manuels) (Date et heure automatiques (serveur NTP manuel))** : synchronisez avec les serveurs NTP de votre choix.
 - **Serveurs NTP manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
- **Custom date and time (Date et heure personnalisées)** : réglez manuellement la date et l'heure. Cliquez sur **Get from system (Récupérer du système)** pour récupérer les paramètres de date et d'heure une fois de votre ordinateur ou de votre périphérique mobile.

Time zone (Fuseau horaire) : sélectionnez le fuseau horaire à utiliser. L'heure est automatiquement réglée pour l'heure d'été et l'heure standard.

Remarque

Le système utilise les paramètres de date et heure dans tous les enregistrements, journaux et paramètres système.

AXIS A1610-B Network Door Controller

Interface du périphérique

Réseau

IPv4

Assign IPv4 automatically (Assigner IPv4 automatiquement) : Sélectionnez cette option pour laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement. Nous recommandons l'IP automatique (DHCP) pour la plupart des réseaux.

Adresse IP : Saisissez une adresse IP unique pour le périphérique. Des adresses IP statiques peuvent être affectées au hasard dans des réseaux isolés, à condition que chaque adresse soit unique. Pour éviter les conflits, nous vous recommandons de contacter votre administrateur réseau avant d'attribuer une adresse IP statique.

Masque de sous-réseau : Saisissez le masque de sous-réseau pour définir les adresses à l'intérieur du réseau local. Toute adresse en dehors du réseau local passe par le routeur.

Routeur : Saisissez l'adresse IP du routeur par défaut (passerelle) utilisé pour connecter les appareils qui sont reliés à différents réseaux et segments de réseaux.

L'adresse IP statique est la solution de secours si le protocole DHCP n'est pas disponible: Sélectionnez si vous souhaitez ajouter une adresse IP statique à utiliser comme secours si DHCP n'est pas disponible et que vous ne pouvez pas attribuer une adresse IP automatiquement.

IPv6

Assigner IPv6 automatiquement : Sélectionnez cette option pour activer IPv6 et laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement.

Nom d'hôte

Attribuer un nom d'hôte automatiquement : Sélectionnez cette option pour laisser le routeur réseau attribuer un nom d'hôte au périphérique automatiquement.

Nom d'hôte : Saisissez manuellement le nom d'hôte afin de l'utiliser comme autre façon d'accéder au périphérique. Le nom d'hôte est utilisé dans le rapport de serveur et dans le journal système. Les caractères autorisés sont les suivants : A-Z, a-z, 0-9 et -.

Serveurs DNS

Affecter DNS automatiquement : Sélectionnez cette option pour laisser le serveur DHCP assigner automatiquement des domaines de recherche et des adresses de serveur DNS au périphérique. Nous recommandons le DNS automatique (DHCP) pour la plupart des réseaux.

Domaines de recherche : Lorsque vous utilisez un nom d'hôte qui n'est pas entièrement qualifié, cliquez sur **Ajouter un domaine de recherche (Add search domain)** et saisissez un domaine dans lequel rechercher le nom d'hôte utilisé par le périphérique.

Serveurs DNS : Cliquez sur **Add DNS server (Serveur DNS principal)** et saisissez l'adresse IP du serveur DNS. Cela assure la conversion de noms d'hôte en adresses IP sur votre réseau.

HTTP et HTTPS

AXIS A1610-B Network Door Controller

Interface du périphérique

Autoriser l'accès via : Sélectionnez cette option si un utilisateur est autorisé à se connecter au périphérique via HTTP,HTTPS, ou les deux protocoles HTTP et HTTPS.

Le protocole HTTPS permet le cryptage des demandes de consultation de pages des utilisateurs, ainsi que des pages envoyées en réponse par le serveur Web. L'échange crypté des informations est régi par l'utilisation d'un certificat HTTPS, garantissant l'authenticité du serveur.

Pour utiliser HTTPS sur le périphérique, vous devez installer un certificat HTTPS. Accédez à **System > Security (Système > Sécurité)** pour créer et installer des certificats.

Remarque

Si vous affichez des pages Web cryptées via HTTPS, il se peut que vos performances baissent, en particulier lorsque vous faites une requête de page pour la première fois.

Port HTTP : Entrez le port HTTP à utiliser. Le port 80 ou tout port de la plage 1024-65535 sont autorisés. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

Port HTTPS : Entrez le port HTTPS à utiliser. Le port 443 ou tout port de la plage 1024-65535 sont autorisés. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

Certificate (Certificat) : Sélectionnez un certificat pour activer HTTPS pour le périphérique.

Protocoles de détection réseau

Bonjour® : Activez cette option pour effectuer une détection automatique sur le réseau.

Bonjour name (Nom Bonjour) : Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

UPnP® : Activez cette option pour effectuer une détection automatique sur le réseau.

UPnP name (Nom UPnP) : Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

WS-Discovery : Activez cette option pour effectuer une détection automatique sur le réseau.

Connexion Cloud en un clic

One-Click Cloud Connect (O3C) associé à un service O3C fournit un accès Internet simple et sécurisé à des vidéos en direct et enregistrées accessibles depuis n'importe quel lieu. Pour plus d'informations, voir axis.com/end-to-end-solutions/hosted-services.

Autoriser O3C :

- **One-click (Un clic) :** Le paramètre par défaut. Maintenez le bouton de commande enfoncé sur le périphérique pour établir une connexion avec un service O3C via Internet. Vous devez enregistrer le périphérique auprès du service O3C dans les 24 heures après avoir appuyé sur le bouton de commande. Sinon, le périphérique se déconnecte du service O3C. Une fois l'enregistrement du périphérique effectué, **Always (Toujours)** est activé et le périphérique reste connecté au service O3C.
- **Always (Toujours) :** Le périphérique tente en permanence d'établir une connexion avec un service O3C via Internet. Une fois inscrit, le périphérique reste connecté au service O3C. Utilisez cette option si le bouton de commande du périphérique est hors de portée.
- **No (Non) :** Désactive le service O3C.

Proxy settings (Paramètres proxy) : si besoin, saisissez les paramètres proxy à connecter au serveur proxy.

Host (Hôte) : Saisissez l'adresse du serveur proxy.

Port : Saisissez le numéro du port utilisé pour l'accès.

Identifiant et Mot de passe : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour le serveur proxy.

AXIS A1610-B Network Door Controller

Interface du périphérique

Authentication method (Méthode d'authentification) :

- **Base** : Cette méthode est le schéma d'authentification le plus compatible pour HTTP. Elle est moins sécurisée que la méthode **Digest**, car elle envoie le nom d'utilisateur et le mot de passe non cryptés au serveur.
- **Digest** : Cette méthode est plus sécurisée car elle transfère toujours le mot de passe crypté à travers le réseau.
- **Auto** : Cette option permet au périphérique de sélectionner la méthode d'authentification selon les méthodes prises en charge. Elle donne priorité à la méthode **Digest** sur la méthode **Basic (Base)**.

Clé d'authentification propriétaire (OAK) : Cliquez sur **Get key (Récupérer la clé)** pour récupérer la clé d'authentification du propriétaire. Cela n'est possible que si le périphérique est connecté à Internet sans pare-feu ni proxy.

SNMP :

Le protocole SNMP (Simple Network Management Protocol) autorise la gestion à distance des périphériques réseau.

SNMP : : Sélectionnez la version de SNMP à utiliser.

- **v1 et v2c** :
 - **Communauté en lecture** : Saisissez le nom de la communauté disposant d'un accès en lecture seule à tous les objets SNMP pris en charge. La valeur par défaut est **public**.
 - **Communauté en écriture** : Saisissez le nom de la communauté disposant d'un accès en lecture/écriture seule à tous les objets SNMP pris en charge (à l'exception des objets en lecture seule). La valeur par défaut est **écriture**.
 - **Activer les dérouterments** : Activez cette option pour activer les rapports de dérouterment. Le périphérique utilise les dérouterments pour envoyer des messages à un système de gestion concernant des événements importants ou des changements de statut. Dans l'interface du périphérique, vous pouvez configurer des dérouterments pour SNMP v1 et v2c. Les dérouterments sont automatiquement désactivés si vous passez à SNMP v3 ou si vous désactivez SNMP. Si vous utilisez SNMP v3, vous pouvez configurer les dérouterments via l'application de gestion SNMP v3.
 - **Adresse de dérouterment** : Entrez l'adresse IP ou le nom d'hôte du serveur de gestion.
 - **Communauté de dérouterment** : saisissez la communauté à utiliser lors de l'envoi d'un message de dérouterment au système de gestion.
 - **Dérouterments** :
 - **Démarrage à froid** : Envoie un message de dérouterment au démarrage du périphérique.
 - **Démarrage à chaud** : Envoie un message de dérouterment lorsque vous modifiez un paramètre SNMP.
 - **Lien vers le haut** : Envoie un message d'interruption lorsqu'un lien change du bas vers le haut.
 - **Échec de l'authentification** : Envoie un message de dérouterment en cas d'échec d'une tentative d'authentification.

Remarque

Tous les dérouterments Axis Video MIB sont activés lorsque vous activez les dérouterments SNMP v1 et v2c. Pour plus d'informations, reportez-vous à *AXIS OS Portal* > *SNMP*.

- **v3** : SNMP v3 est une version plus sécurisée qui fournit un cryptage et mots de passe sécurisés. Pour utiliser SNMP v3, nous vous recommandons d'activer HTTPS, car le mot de passe est envoyé via ce protocole. Cela empêche également les tiers non autorisés d'accéder aux dérouterments v1 et v2c SNMP non cryptés. Si vous utilisez SNMP v3, vous pouvez configurer les dérouterments via l'application de gestion SNMP v3.
 - **Mot de passe pour le compte « initial »** : Entrez le mot de passe SNMP du compte nommé « initial ». Bien que le mot de passe puisse être envoyé sans activer le protocole HTTPS, nous ne le recommandons pas. Le mot de passe SNMP v3 ne peut être configuré qu'une fois, et de préférence seulement lorsque le protocole HTTPS est activé. Une fois le mot de passe configuré, le champ de mot de passe ne s'affiche plus. Pour reconfigurer le mot de passe, vous devez réinitialiser le périphérique aux paramètres des valeurs par défaut.

Connected clients (Clients connectés)

View details (Afficher les détails) : cliquez pour afficher tous les clients connectés au périphérique.

Sécurité

Certificats

AXIS A1610-B Network Door Controller

Interface du périphérique

Les certificats servent à authentifier les périphériques d'un réseau. Le périphérique prend en charge deux types de certificats :

- **Certificats serveur/client**
Un certificat serveur/client valide l'identité du périphérique et peut être auto-signé ou émis par une autorité de certification (CA). Un certificat auto-signé offre une protection limitée et peut être utilisé avant l'obtention d'un certificat CA émis.
- **Certificats CA**
Un certificat CA permet d'authentifier un certificat d'homologue, par exemple pour valider l'identité d'un serveur d'authentification lorsque le périphérique se connecte à un réseau protégé par IEEE 802.1X. Le périphérique dispose de plusieurs certificats CA préinstallés.

Les formats suivants sont pris en charge :

- Formats de certificats : .PEM, .CER et .PFX
- Formats de clés privées : PKCS#1 et PKCS#12

Important

Si vous réinitialisez le périphérique aux valeurs par défaut, tous les certificats sont supprimés. Les certificats CA préinstallés sont réinstallés.



Filtrez les certificats dans la liste.



Add certificate (Ajouter un certificat) : cliquez pour ajouter un certificat.



Le menu contextuel contient :

- **Certificate information (Informations sur le certificat)** : affichez les propriétés d'un certificat installé.
- **Delete certificate (Supprimer certificat)** : supprimez le certificat.
- **Create certificate signing request (Créer une demande de signature du certificat)** : créez une demande de signature du certificat pour l'envoyer à une autorité d'enregistrement afin de demander un certificat d'identité numérique.

Norme IEEE 802.1x

La norme IEEE 802.1x est une norme IEEE servant au contrôle de l'admission au réseau basé sur les ports en fournissant une authentification sécurisée des périphériques réseau câblés et sans fil. IEEE 802.1x repose sur le protocole EAP (Extensible Authentication Protocol).

Pour accéder à un réseau protégé par IEEE 802.1x, les périphériques réseau doivent s'authentifier. L'authentification est réalisée par un serveur d'authentification, généralement un serveur RADIUS (par exemple le Service d'Authentification Internet de Microsoft et FreeRADIUS).

Certificats

Lorsqu'il est configuré sans certificat CA, la validation du certificat du serveur est désactivée et le périphérique essaie de s'authentifier indépendamment du réseau auquel il est connecté.

En cas d'utilisation d'un certificat, lors de l'implémentation Axis, le périphérique et le serveur d'authentification s'authentifient avec des certificats numériques à l'aide de EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Pour permettre au périphérique d'accéder à un réseau protégé par des certificats, un certificat client signé doit être installé sur le périphérique.

Certificat client : Sélectionnez un certificat client pour utiliser IEEE 802.1x. Le serveur d'authentification utilise le certificat CA pour valider l'identité du client.

Certificat CA : Sélectionnez un certificat CA pour valider l'identité du serveur d'authentification. Si aucun certificat n'est sélectionné, le périphérique essaie de s'authentifier indépendamment du réseau auquel il est connecté.

EAP identity (Identité EAP) : Saisissez l'option Identity (Identité) de l'utilisateur associée au certificat du client.

AXIS A1610-B Network Door Controller

Interface du périphérique

EAPOL version (Version EAPOL) : sélectionnez la version EAPOL utilisée dans votre commutateur réseau.

Utiliser IEEE 802.1x : Sélectionnez cette option pour utiliser le protocole IEEE 802.1x.

Empêcher les attaques par force brute

Blocage : Activez cette option pour bloquer les attaques par force brute. Une attaque par force brute utilise l'essai-erreur pour deviner les informations de connexion ou les clés de cryptage.

Période de blocage : Saisissez le nombre de secondes pour bloquer une attaque par force brute.

Conditions de blocage : Saisissez le nombre d'échecs d'authentification autorisés par seconde avant le démarrage du blocage. Vous pouvez définir le nombre d'échecs autorisés à la fois au niveau de la page et au niveau du périphérique.

Filtre d'adresse IP

Utiliser un filtre : Sélectionnez cette option pour filtrer les adresses IP autorisées à accéder au périphérique.

Politique : Choisissez cette option pour **Allow (Autoriser)** l'accès ou **Deny (Refuser)** l'accès pour certaines adresses IP.

Adresses : Saisissez les numéros IP qui sont autorisés ou non à accéder au périphérique. Vous pouvez également utiliser le format CIDR.

Certificat de firmware avec signature personnalisée

Pour installer le firmware de test ou tout autre firmware personnalisé d'Axis sur le périphérique, vous avez besoin d'un certificat de firmware avec signature personnalisée. Le certificat vérifie que le firmware est approuvé à la fois par le propriétaire du périphérique et par Axis. Le firmware ne peut être exécuté que sur un périphérique précis, identifié par son numéro de série unique et son ID de puce. Seul Axis, qui détient la clé pour les signer, peut créer des certificats de firmware avec signature personnalisée.

Cliquez sur **Install (Installer)** pour installer le certificat. Vous devez installer le certificat avant d'installer le firmware.

Utilisateurs



Add user (Ajouter un utilisateur) : cliquez pour ajouter un nouvel utilisateur. Vous pouvez ajouter jusqu'à 100 utilisateurs.

Nom d'utilisateur : saisissez un nom d'utilisateur unique.

New password (Nouveau mot de passe) : saisissez un mot de passe pour l'utilisateur. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans les mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

Repeat password (Répéter le mot de passe) : saisissez à nouveau le même mot de passe.

Role (Rôle) :

- **Administrator (Administrateur)** : accès sans restriction à tous les paramètres. Les administrateurs peuvent également ajouter, mettre à jour et supprimer les autres utilisateurs.
- **Operator (Opérateur)** : accès à tous les paramètres à l'exception de :
 - tous les paramètres **System (Système)**.
 - Ajout d'applications.
- **Viewer (Observateur)** : n'a pas le droit de modifier les paramètres.



Le menu contextuel contient :

Update user (Mettre à jour l'utilisateur) : modifiez les propriétés de l'utilisateur.

Delete user (Supprimer l'utilisateur) : supprimez l'utilisateur. Vous ne pouvez pas supprimer l'utilisateur racine.

AXIS A1610-B Network Door Controller

Interface du périphérique

MQTT

MQTT (message queuing telemetry transport) est un protocole de messagerie standard pour l'Internet des objets (IoT). Conçu pour simplifier l'intégration IoT, il est utilisé dans de nombreux secteurs pour connecter des périphériques distants avec une empreinte de code réduite et une bande passante réseau minimale. Le client MQTT du firmware des périphériques Axis peut simplifier l'intégration des données et des événements produits sur le périphérique dans les systèmes qui ne sont pas des systèmes de gestion vidéo (VMS).

Configurez le périphérique en tant que client MQTT. La communication MQTT est basée sur deux entités, les clients et le courtier. Les clients peuvent envoyer et recevoir des messages. Le courtier est responsable de l'acheminement des messages entre les clients.

Pour en savoir plus sur MQTT, accédez à *AXIS OS Portal*.

ALPN

ALPN est une extension TLS/SSL qui permet de choisir un protocole d'application au cours de la phase handshake de la connexion entre le client et le serveur. Cela permet d'activer le trafic MQTT sur le même port que celui utilisé pour d'autres protocoles, tels que HTTP. Dans certains cas, il n'y a pas de port dédié ouvert pour la communication MQTT. Une solution consiste alors à utiliser ALPN pour négocier l'utilisation de MQTT comme protocole d'application sur un port standard, autorisé par les pare-feu.

MQTT client (Client MQTT)

Connexion : Activez ou désactivez le client MQTT.

Status (Statut) : Affiche le statut actuel du client MQTT.

Courtier

Host (Hôte) : Saisissez le nom d'hôte ou l'adresse IP du serveur MQTT.

Protocol (Protocole) : Sélectionnez le protocole à utiliser.

Port (Port) : Saisissez le numéro de port.

- 1883 est la valeur par défaut pour MQTT sur TCP.
- 8883 est la valeur par défaut pour MQTT sur SSL.
- 80 est la valeur par défaut pour MQTT sur WebSocket.
- 443 est la valeur par défaut pour MQTT sur WebSocket Secure.

Protocole ALPN : Saisissez le nom du protocole ALPN fourni par votre fournisseur MQTT. Cela ne s'applique qu'aux normes MQTT sur SSL et MQTT sur WebSocket Secure.

Nom d'utilisateur : Saisissez le nom d'utilisateur utilisé par le client pour accéder au serveur.

Mot de passe : Saisissez un mot de passe pour le nom d'utilisateur.

Client ID (Identifiant client) : Entrez un identifiant client. L'identifiant client est envoyé au serveur lorsque le client s'y connecte.

Clean session (Nettoyer la session) : Contrôle le comportement lors de la connexion et de la déconnexion. Lorsque cette option est sélectionnée, les informations d'état sont supprimées lors de la connexion et de la déconnexion.

Keep alive interval (Intervalle Keep Alive) : L'intervalle Keep Alive permet au client de détecter quand le serveur n'est plus disponible sans devoir observer le long délai d'attente TCP/IP.

Timeout (Délai d'attente) : Intervalle de temps en secondes pour permettre l'établissement d'une connexion. Valeur par défaut : 60

Préfixe de rubrique du périphérique : Utilisé dans les valeurs par défaut pour le sujet contenu dans le message de connexion et le message LWT sur l'onglet MQTT client (Client MQTT), et dans les conditions de publication sur l'onglet MQTT publication (Publication MQTT).

Reconnect automatically (Reconnexion automatique) : Spécifie si le client doit se reconnecter automatiquement en cas de déconnexion.

Connect message (Message de connexion)

AXIS A1610-B Network Door Controller

Interface du périphérique

Spécifie si un message doit être envoyé lorsqu'une connexion est établie.

Send message (Envoyer message) : Activez cette option pour envoyer des messages.

Use default (Utiliser les valeurs par défaut) : Désactivez cette option pour saisir votre propre message par défaut.

Topic (Rubrique) : Saisissez la rubrique du message par défaut.

Payload (Charge utile) : Saisissez le contenu du message par défaut.

Conserver : Sélectionnez cette option pour conserver l'état du client sur cette **Rubrique**.

QoS : Modifiez la couche QoS pour le flux de paquets.

Message Dernière Volonté et Testament

Last Will Testament (LWT) permet à un client de fournir un testament avec ses identifiants lors de sa connexion au courtier. Si le client se déconnecte incorrectement plus tard (peut-être en raison d'une défaillance de sa source d'alimentation), il peut laisser le courtier délivrer un message aux autres clients. Ce message LWT présente la même forme qu'un message ordinaire. Il est acheminé par le même mécanisme.

Send message (Envoyer message) : Activez cette option pour envoyer des messages.

Use default (Utiliser les valeurs par défaut) : Désactivez cette option pour saisir votre propre message par défaut.

Topic (Rubrique) : Saisissez la rubrique du message par défaut.

Payload (Charge utile) : Saisissez le contenu du message par défaut.

Conserver : Sélectionnez cette option pour conserver l'état du client sur cette **Rubrique**.

QoS : Modifiez la couche QoS pour le flux de paquets.

MQTT publication (Publication MQTT)

Utiliser le préfixe de rubrique par défaut : Sélectionnez cette option pour utiliser le préfixe de rubrique par défaut, défini dans la rubrique du périphérique dans l'onglet **MQTT client (Client MQTT)**.

Inclure le nom de rubrique : Sélectionnez cette option pour inclure la rubrique qui décrit l'état dans la rubrique MQTT.

Inclure les espaces de noms de rubrique : Sélectionnez cette option pour inclure des espaces de noms de rubrique ONVIF dans la rubrique MQTT.

Inclure le numéro de série : Sélectionnez cette option pour inclure le numéro de série du périphérique dans la charge utile MQTT.



Add condition (Ajouter condition) : Cliquez pour ajouter une condition.

Retain (Conserver) : Définit les messages MQTT qui sont envoyés et conservés.

- **Aucun** : Envoyer tous les messages comme non conservés.
- **Property (Propriété)** : Envoyer seulement les messages avec état comme conservés.
- **All (Tout)** : Envoyer les messages avec état et sans état, comme conservés.

QoS : Sélectionnez le niveau souhaité pour la publication MQTT.

Abonnements MQTT

AXIS A1610-B Network Door Controller

Interface du périphérique



Ajouter abonnement (Add subscription) : Cliquez pour ajouter un nouvel abonnement MQTT.

Subscription filter (Filtre d'abonnements) : Saisissez le sujet MQTT auquel vous souhaitez vous abonner.

Use device topic prefix (Utiliser le préfixe de rubrique du périphérique) : Ajoutez le filtre d'abonnement comme préfixe au sujet MQTT.

Subscription type (Type d'abonnement) :

- **Stateless (Sans état)** : Sélectionnez cette option pour convertir les messages MQTT en message sans état.
- **Stateful (Avec état)** : Sélectionnez cette option pour convertir les messages MQTT dans une condition. La charge utile est utilisée comme état.

QoS : Sélectionnez le niveau souhaité pour l'abonnement MQTT.

Accessoires



Ports d'E/S



Utilisez une entrée numérique pour connecter les périphériques externes pouvant basculer entre un circuit ouvert et un circuit fermé, tels que les capteurs infrarouge passifs, les contacts de porte ou de fenêtre et les détecteurs de bris de verre.

Utilisez une sortie numérique pour connecter des dispositifs externes, comme des relais ou des voyants. Vous pouvez activer les périphériques connectés par l'interface de programmation VAPIX® ou par l'interface du périphérique.

Port

Nom : modifiez le texte pour renommer le port.


Sens :  indique que le port est un port d'entrée.  indique qu'il s'agit d'un port de sortie. Si le port est configurable, vous pouvez cliquer sur les icônes pour modifier entre l'entrée et la sortie.

État normal : Cliquez sur  open circuit (circuit ouvert), et  pour closed circuit (circuit fermé).

État actuel : Indique l'état actuel du port. L'entrée ou la sortie est activée lorsque l'état actuel diffère de l'état normal. Une entrée sur le périphérique a un circuit ouvert lorsqu'elle est déconnectée ou lorsque la tension est supérieure à 1 V DC.

Remarque

Lors du redémarrage, le circuit de sortie est ouvert. Lorsque le redémarrage est terminé, le circuit repasse à la position normale. Si vous modifiez un paramètre sur cette page, les circuits de sortie repassent à leurs positions normales quels que soient les déclencheurs actifs.

Supervisé  : Activez cette option pour pouvoir détecter et déclencher des actions si quelqu'un touche aux périphériques d'E/S numériques. En plus de détecter si une entrée est ouverte ou fermée, vous pouvez également détecter si quelqu'un l'a altérée (c'est-à-dire coupée ou court-circuitée). La supervision de la connexion nécessite des composants supplémentaires (résistances de fin de ligne) dans la boucle d'E/S externe.

Journaux

Rapports et journaux

AXIS A1610-B Network Door Controller

Interface du périphérique

Reports (Rapports)

- **View the device server report (Afficher le rapport du serveur de périphériques)** : cliquez pour afficher les informations sur l'état du produit dans une fenêtre contextuelle. Le journal d'accès est automatiquement intégré au rapport de serveur.
- **Download the device server report (Télécharger le rapport du serveur de périphériques)** : cliquez pour télécharger le rapport de serveur. Il crée un fichier .zip qui contient un fichier texte du rapport de serveur complet au format UTF-8 et une capture d'image de la vidéo en direct actuelle. Joignez toujours le fichier .zip du rapport de serveur lorsque vous contactez le support.
- **Download the crash report (Télécharger le rapport d'incident)** : cliquez pour télécharger une archive avec des informations détaillées sur l'état du serveur. Le rapport d'incident contient les informations figurant dans le rapport de serveur et les informations de débogage détaillées. Ce rapport peut aussi contenir des informations sensibles comme le suivi réseau. L'opération de génération du rapport peut prendre plusieurs minutes.

Journaux

- **View the system log (Afficher le journal système)** : cliquez pour afficher les informations sur les événements système tels que le démarrage du périphérique, les avertissements et les messages critiques.
- **View the access log (Afficher le journal d'accès)** : cliquez pour afficher tous les échecs d'accès au périphérique, par exemple si un mot de passe erroné a été utilisé.

Suivi réseau

Important

Un fichier de suivi réseau peut contenir des informations sensibles, comme des certificats ou des mots de passe.

Un fichier de suivi réseau contribue à dépanner les problèmes en enregistrant l'activité sur le réseau.

Trace time (Durée du suivi) : Sélectionnez la durée du suivi en secondes ou en minutes, puis cliquez sur **Download (Télécharger)**.

Journal système distant

Syslog est une norme de journalisation des messages. Elle permet de séparer le logiciel qui génère les messages, le système qui les stocke et le logiciel qui les signale et les analyse. Chaque message est étiqueté avec un code de fonction qui donne le type de logiciel générant le message et le niveau de gravité assigné.



Server (Serveur) : cliquez pour ajouter un nouvel serveur.

Host (Hôte) : saisissez le nom d'hôte ou l'adresse IP du serveur.

Format (Format) : sélectionnez le format du message Syslog à utiliser.

- RFC 3164
- RFC 5424

Protocole : Sélectionnez le protocole et le port à utiliser :

- UDP (Le port par défaut est 514)
- TCP (Le port par défaut est 601)
- TLS (Le port par défaut est 6514)

Severity (Gravité) : sélectionnez les messages à envoyer lorsqu'ils sont déclenchés.

CA certificate set (Initialisation du certificat CA) : affichez les paramètres actuels ou ajoutez un certificat.

AXIS A1610-B Network Door Controller

Interface du périphérique

Maintenance

Restart (Redémarrer) : redémarrez le périphérique. Cela n'affecte aucun des paramètres actuels. Les applications en cours d'exécution redémarrent automatiquement.

Restore (Restaurer) : la *plupart* des paramètres sont rétablis aux valeurs par défaut. Ensuite, vous devez reconfigurer le périphérique et les applications, réinstaller toutes les applications qui ne sont pas préinstallées et recréer les événements et les préreglages PTZ.

Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

- le protocole Boot (DHCP ou statique) ;
- l'adresse IP statique ;
- le routeur par défaut ;
- le masque de sous-réseau ;
- les réglages 802.1X ;
- les réglages O3C.

Factory default (Valeurs par défaut) : *tous* les paramètres sont rétablis aux valeurs par défaut. Réinitialisez ensuite l'adresse IP pour rendre le périphérique accessible.

Remarque

Tous les firmwares des périphériques Axis sont signés numériquement pour garantir que seuls les firmwares vérifiés sont installés sur le périphérique. Cela permet d'accroître le niveau minimal de cybersécurité globale des périphériques Axis. Pour plus d'informations, lire le livre blanc « Signed firmware, secure boot, and security of private keys » (Firmware signé, démarrage sécurisé et sécurité des clés privées) sur axis.com.

Firmware upgrade (Mise à niveau du firmware) : mettez à niveau vers une nouvelle version du firmware. Les nouvelles versions du firmware peuvent contenir des fonctionnalités améliorées, des résolutions de bogues et de nouvelles fonctions. Nous vous conseillons de toujours utiliser la version la plus récente. Pour télécharger la dernière version, accédez à axis.com/support.

Lors de la mise à niveau, vous avez le choix entre trois options :

- **Standard upgrade (Mise à niveau standard)** : mettez à niveau vers la nouvelle version du firmware.
- **Factory default (Valeurs par défaut)** : mettez à niveau et remettez tous les paramètres sur les valeurs par défaut. Si vous choisissez cette option, il est impossible de revenir à la version précédente du firmware après la mise à niveau.
- **AutoRollback (Restauration automatique)** : mettez à niveau et confirmez la mise à niveau dans la durée définie. Si vous ne confirmez pas, le périphérique revient à la version précédente du firmware.

Firmware rollback (Restauration du firmware) : revenez à la version du firmware précédemment installée.

AXIS A1610-B Network Door Controller

En savoir plus

En savoir plus

Sécurité

Firmware signé

Le firmware signé est mis en œuvre par le fournisseur du logiciel, qui signe l'image du firmware avec une clé privée. Lorsque cette signature est associée à un firmware, le périphérique valide le firmware avant d'accepter de l'installer. Si le périphérique détecte que l'intégrité du firmware est compromise, la mise à niveau du firmware est rejetée.

Démarrage sécurisé

Le démarrage sécurisé est un processus de démarrage constitué d'une chaîne ininterrompue de logiciels validés par cryptographie, commençant dans la mémoire immuable (ROM de démarrage). Basé sur l'utilisation d'un firmware signé, le démarrage sécurisé garantit qu'un périphérique ne peut démarrer qu'avec le firmware autorisé.

Axis Edge Vault

Axis Edge Vault offre une plate-forme de cybersécurité matérielle qui protège les périphériques Axis. Elle garantit leur identité et leur intégrité, et protège vos informations sensibles contre tout accès non autorisé. Elle s'appuie sur de solides bases de modules de calcul cryptographique (élément sécurisé et TPM) et de sécurité SoC (TEE et amorçage sécurisé), associés à une expertise en termes de sécurité des périphériques edge.

Identifiant de périphérique Axis

Il est essentiel de pouvoir vérifier l'origine du dispositif pour établir la confiance concernant son identité. Pendant la production, les dispositifs compatibles avec Axis Edge Vault reçoivent un certificat d'ID des dispositifs Axis conformes à la norme IEEE 802.1AR, fourni en usine. Cela fonctionne comme un passeport pour prouver l'origine du dispositif. L'ID du dispositif est stocké en toute sécurité et de manière permanente dans le secure keystore sous la forme d'un certificat signé par un certificat racine Axis. L'ID du dispositif peut être utilisé par l'infrastructure informatique du client pour l'intégration automatique et l'identification sécurisée des dispositifs.

Pour en savoir plus sur Axis Edge Vault et les fonctionnalités de cybersécurité des périphériques Axis, accédez à axis.com/learning/white-papers et lancez une recherche sur la cybersécurité.

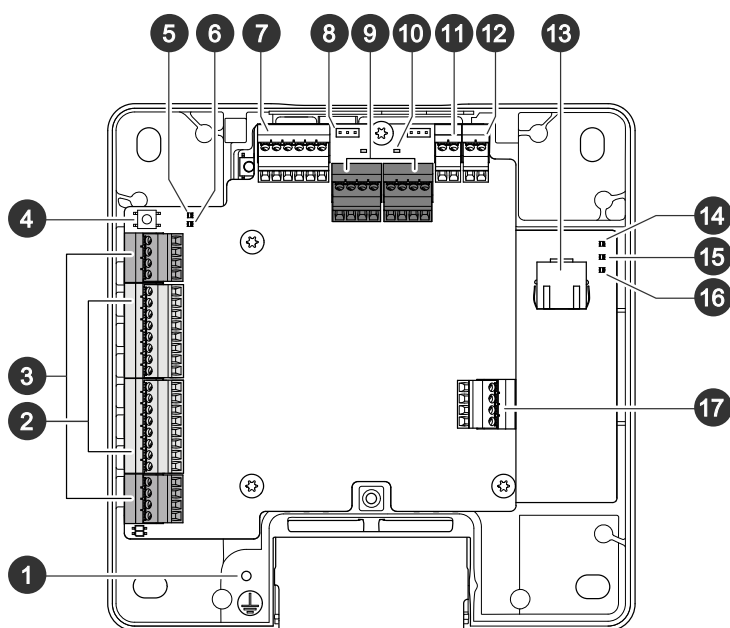
AXIS A1610-B Network Door Controller

Caractéristiques

Caractéristiques

Le texte portant la mention UL s'applique uniquement aux installations UL 294.

Vue d'ensemble du produit



- 1 Position de mise à la terre
- 2 Connecteur du lecteur, x 2
- 3 Connecteur de porte, x 2
- 4 Bouton de commande
- 5 Voyant de surintensités du relais
- 6 Voyant de surintensités du lecteur
- 7 Connecteur auxiliaire
- 8 Cavalier de relais, x 2
- 9 Connecteur relais, x 2
- 10 Voyant de relais, x 2
- 11 Entrée d'alimentation de secours 12 V
- 12 Connecteur d'alimentation
- 13 Connecteur réseau
- 14 LED d'alimentation
- 15 LED d'état
- 16 Voyant réseau
- 17 Connecteur externe

AXIS A1610-B Network Door Controller

Caractéristiques

Voyants DEL

Voyant DEL	Couleur	Indication
Réseau	Vert	Fixe en cas de connexion à un réseau de 100 Mbit/s. Clignote en cas d'activité réseau.
	Orange	Fixe en cas de connexion à un réseau de 10 Mbits/s. Clignote en cas d'activité réseau.
	Éteint	Pas de connexion réseau.
État	Vert	Vert fixe en cas de fonctionnement normal.
	Orange	Fixe pendant le démarrage et lors de la restauration des paramètres.
	Rouge	Clignote lentement en cas d'échec de la mise à niveau.
Alimentation	Vert	Fonctionnement normal.
	Orange	Le voyant vert/orange clignote pendant la mise à niveau du firmware.
Surintensités relais	Rouge	Fixe si court-circuité ou si des surintensités ont été détectées.
	Éteint	Fonctionnement normal.
Surintensités du lecteur	Rouge	Fixe si court-circuité ou si des surintensités ont été détectées.
	Éteint	Fonctionnement normal.
Relais	Vert	Relais actif. ¹
	Éteint	Relais inactif.

1. Relais actif lorsque COM est connecté à NO.

Remarque

- Vous pouvez configurer le voyant d'état pour qu'il clignote lorsqu'un événement est actif.
- Le voyant d'état peut clignoter pendant l'identification de l'appareil. Accédez à **Setup > Additional Controller Configuration > System Options > Maintenance (Configuration > Configuration du contrôleur supplémentaire > Options du système > Maintenance)**.

Boutons

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. *Réinitialiser les paramètres par défaut à la page 29*.

Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45 avec alimentation par Ethernet Plus (PoE+).

UL : L'alimentation par Ethernet (PoE) doit disposer d'un injecteur à alimentation limitée POE IEEE 802.3af/802.3at Type 1 Classe 3 ou PoE+ IEEE 802.3at Type 2 Classe 4 homologué UL 294 fournissant 44 à 57 V CC, 15,4 W/30 W. L'alimentation par Ethernet (PoE) a été évaluée par l'UL avec AXIS T8133 Midspan 30 W 1-port.

Connecteur du lecteur

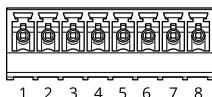
Deux blocs terminaux à 8 broches prenant en charge les protocoles RS485 et Wiegand pour la communication avec le lecteur.

AXIS A1610-B Network Door Controller

Caractéristiques

Les valeurs de sortie d'alimentation spécifiées sont partagées entre les deux ports du lecteur. Cela signifie que 500 mA à 12 V CC sont réservés pour tous les lecteurs connectés au contrôleur de porte.

Sélectionnez le protocole à utiliser dans la page Web du produit.



Configuré pour RS485

Fonction	Broche	Note	Caractéristiques
Masse du CC (GND)	1		0 V CC
Sortie CC (+12 V)	2	Permet d'alimenter le lecteur.	12 V CC, 500 mA max. combinés pour tous les lecteurs
RX/TX	3-4	Full-duplex : RX. Half-duplex : RX/TX.	
TX	5-6	Duplex intégral : TX.	
Configurable (entrée ou sortie)	7-8	Entrée numérique : connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à maxi. 30 V CC
		Sortie numérique : en cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

Important

- Lorsque le lecteur est alimenté par le contrôleur, la longueur de câble qualifiée maximale est de 200 m (656 pi).
- Lorsque le lecteur n'est pas alimenté par le contrôleur, la longueur de câble qualifiée maximale pour les données du lecteur est de 1 000 m (3280,8 pieds) si le câble respecte les exigences suivantes : 1 paire torsadée avec blindage, AWG 20-16.

Configuré pour Wiegand

Fonction	Broche	Note	Caractéristiques
Masse CC (GND)	1		0 V CC
Sortie CC (+12 V)	2	Permet d'alimenter le lecteur.	12 V CC, max 500 mA combinés pour tous les lecteurs
D0	3		
D1	4		
0	5-6	Sortie numérique, drain ouvert	

AXIS A1610-B Network Door Controller

Caractéristiques

Configurable (entrée ou sortie)	7-8	Entrée numérique : connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à maxi. 30 V CC
		Sortie numérique : en cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

Important

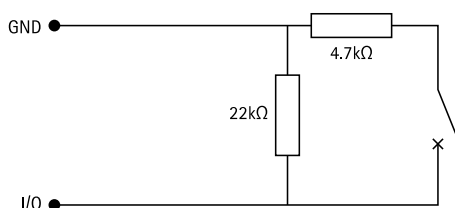
- Lorsque le lecteur est alimenté par le contrôleur, la longueur de câble qualifiée maximale est de 150 m (500 pi).
- Lorsque le lecteur n'est pas alimenté par le contrôleur, la longueur de câble qualifiée maximale pour les données du lecteur est de 150 m (500 pieds) si le câble respecte l'exigence suivante : AWG 20-16.

Entrées supervisées

Pour utiliser des entrées supervisées, installez des résistances de fin de ligne en suivant le schéma ci-dessous.

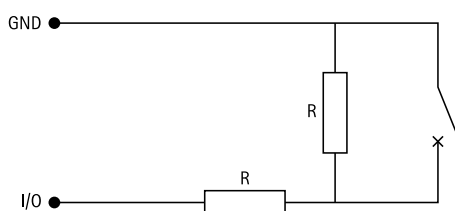
Première connexion parallèle

Les valeurs des résistances doivent être de 4,7 k Ω et de 22 k Ω .



Première connexion série

Les valeurs de résistance doivent être les mêmes et les valeurs possibles sont : 1 k Ω , 2,2 k Ω , 4,7 k Ω et 10 k Ω .



Remarque

Il est conseillé d'utiliser des câbles torsadés et blindés. Connectez le blindage à 0 V CC.

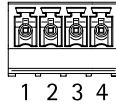
Connecteur de porte

Deux blocs terminaux à 4 broches pour les périphériques de contrôle des portes (entrée numérique).

Un moniteur de porte prend en charge la surveillance avec des résistances de fin de ligne. Si la connexion est interrompue, une alarme est déclenchée. Pour utiliser des entrées supervisées, installez des résistances de fin de ligne. Utilisez le schéma de connexion pour les entrées supervisées. Voir *Entrées supervisées* à la page 24.

AXIS A1610-B Network Door Controller

Caractéristiques



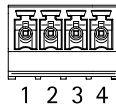
Fonction	Broche	Notes	Caractéristiques
Masse du CC	1, 3		0 V CC
Entrée	2, 4	Pour la communication avec le moniteur de porte. Entrée numérique ou entrée supervisée : permet de raccorder respectivement à la broche 1 ou 3 pour activer ou laisser flotter (déconnectée) pour désactiver.	0 à 30 V CC max.

Important

La longueur de câble qualifiée maximale est de 200 m (656 pi) si le câble respecte l'exigence suivante : AWG 24.

Connecteur relais

Deux blocs terminaux à 4 broches pour les relais de forme C peuvent être utilisés, par exemple, pour commander un verrou ou une interface d'une barrière.



Fonction	Broche	Notes	Caractéristiques
Masse du CC (GND)	1		0 V CC
NO	2	Normalement ouvert. Pour la connexion des périphériques relais. Connectez un verrou à sécurité intégrée entre NO et la terre CC. Les deux broches du relais sont isolées du reste des circuits si les cavaliers ne sont pas utilisés.	Courant maxi. = 2 A par relais Tension maxi. = 30 V CC
COM	3	Courant	
NC	4	Normalement fermé. Pour la connexion des périphériques relais. Connectez un verrou à sécurité intrinsèque entre NC et la terre CC. Les deux broches du relais sont isolées du reste des circuits si les cavaliers ne sont pas utilisés.	

Cavalier d'alimentation de relais

Lorsque le cavalier d'alimentation de relais est monté, il connecte du 12 V CC ou du 24 V CC à la broche de relais COM.

Il peut servir à connecter un verrou entre la terre GND et les broches NO ou GND et NC.

Source d'alimentation	Puissance max. à 12 V CC ¹	Puissance max. à 24 V CC ¹
CC IN	1 800 mA	750 mA
PoE	900 mA	410 mA

1. L'alimentation est partagée entre les deux relais et les E/S AUX 12 V CC.

REMARQUE

Si le verrou n'est pas polarisé, nous vous recommandons d'ajouter une diode flyback externe.

AXIS A1610-B Network Door Controller

Caractéristiques

Connecteur auxiliaire

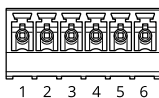
Utilisez le connecteur auxiliaire avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie CC), le connecteur auxiliaire fournit une interface aux éléments suivants :

Entrée numérique – Pour connecter des dispositifs pouvant passer d'un circuit ouvert à un circuit fermé, par exemple capteurs infrarouge passifs, contacts de porte/fenêtre et détecteurs de bris de verre.

Entrée supervisée – Permet la détection de sabotage sur une entrée numérique.

Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les appareils connectés peuvent être activés par l'interface de programmation VAPIX® ou à partir de la page Web du produit.

Bloc terminal à 6 broches

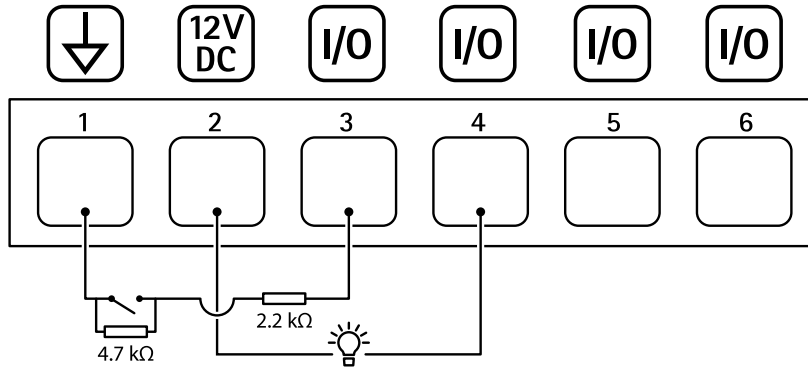


Fonction	Broche	Notes	Caractéristiques
Masse CC	1		0 V CC
Sortie CC	2	Peut servir à alimenter le matériel auxiliaire. Remarque : Cette broche ne peut être utilisée que comme sortie d'alimentation et sur le côté sécurisé car elle partage l'alimentation avec les relais.	12 V CC Charge max. = 50 mA pour chaque E/S
Configurable (entrée ou sortie)	3-6	Entrée numérique ou entrée supervisée – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Pour utiliser une entrée supervisée, installez des résistances de fin de ligne. Consultez le schéma de connexion pour plus d'informations sur la connexion des résistances.	0 à 30 V CC max
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension. Chaque E/S est capable de fournir une charge externe de 12 V CC, 50 mA (max.) si une sortie interne de 12 V CC (broche 2) est utilisée. Lorsque des connexions	0 à 30 V CC max., drain ouvert, 100 mA

AXIS A1610-B Network Door Controller

Caractéristiques

	à drain ouvert sont utilisées avec une alimentation externe, les E/S peuvent gérer l'alimentation CC de 0 – 30 V CC, 100 mA.	
--	--	--

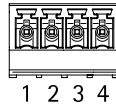


- 1 Masse du CC
- 2 Sortie CC 12 V, 50 mA max.
- 3 E/S configurée comme entrée supervisée
- 4 Entrée/sortie configurée comme sortie
- 5 E/S configurable
- 6 E/S configurable

Connecteur externe

Bloc terminal à 4 broches pour périphériques externes, par exemple détecteurs d'incendie ou de bris de verre.

UL : Le connecteur n'a pas été évalué par l'UL pour les alarmes anti-vol/anti-incendie.



Fonction	Broche	Remarques	Caractéristiques
Masse du CC	1, 3		0 V CC
Configurable (entrée ou sortie)	2, 4	Entrée numérique : vous pouvez la connecter à la broche 1 ou 3 pour l'activer ou la laisser flottante (non connectée) pour la désactiver.	0 à 30 V CC max.
		Sortie numérique : vous pouvez la connecter à la broche 1 ou 3 pour l'activer ou la laisser flottante (non connectée) pour la désactiver. Si utilisée avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge afin de protéger contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

Connecteur d'alimentation

Bloc terminal à 2 broches pour l'entrée d'alimentation CC. Utilisez une source d'alimentation limitée (LPS) conforme aux exigences de Très basse tension de sécurité (TBTS) dont la puissance de sortie nominale est limitée à ≤ 100 W ou dont le courant de sortie nominal est limité à ≤ 5 A.

AXIS A1610-B Network Door Controller

Caractéristiques



Fonction	Broche	Remarque	Caractéristiques
0 V cc (-)	1		0 V CC
Entrée CC	2	Pour alimenter le contrôleur lorsque l'alimentation par Ethernet n'est pas utilisée. Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation.	10,5-28 V CC, max. 36 W

UL : puissance CC fournie par une alimentation électrique UL 294, UL 293 ou UL 603, selon l'application, avec des puissances appropriées.

Entrée d'alimentation de secours 12 V

Pour une solution de sauvegarde à l'aide d'une batterie avec chargeur intégré. Entrée 12 V CC.

UL : Le connecteur n'a pas été évalué par l'UL.

Important

Lorsque l'entrée de la batterie est utilisée, un fusible externe à action retardée 3 A doit être connecté en série.



Fonction	Broche	Notes	Caractéristiques
0 V CC (-)	1		0 V CC
Entrée batterie	2	Pour alimenter le contrôleur de porte lorsque les autres sources d'alimentation ne sont pas disponibles. Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation de la batterie. Pour la connexion au système UPS uniquement.	11 à 13,7 V CC, 36 W max.

AXIS A1610-B Network Door Controller

Dépannage

Dépannage

Réinitialiser les paramètres par défaut

Important

La restauration des paramètres d'usine par défaut doit être utilisée avec prudence. Cette opération restaure tous les paramètres par défaut, y compris l'adresse IP.

Pour réinitialiser l'appareil aux paramètres d'usine par défaut :

1. Déconnectez l'alimentation de l'appareil.
2. Maintenez le bouton de commande enfoncé en remettant l'appareil sous tension. Cf. *Vue d'ensemble du produit à la page 21*.
3. Appuyez sur le bouton de commande pendant 25 secondes jusqu'à ce que le voyant d'état passe à l'orange une seconde fois.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état passe au vert. Les paramètres d'usine par défaut de l'appareil ont été rétablis. En l'absence d'un serveur DHCP sur le réseau, l'adresse IP par défaut est 192.168.0.90.
5. Utilisez les outils d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au produit.

Vous pouvez également rétablir les paramètres d'usine par défaut via l'interface web du périphérique. Accédez à **Maintenance > Valeurs par défaut** et cliquez sur **Par défaut**.

Options du firmware

Axis permet de gérer le firmware du produit conformément au support actif ou au support à long terme (LTS). Le support actif permet d'avoir continuellement accès à toutes les fonctions les plus récentes du produit, tandis que le support à long terme offre une plateforme fixe avec des versions périodiques axées principalement sur les résolutions de bogues et les mises à jour de sécurité.

Il est recommandé d'utiliser le firmware du support actif si vous souhaitez accéder aux fonctions les plus récentes ou si vous utilisez des offres système Solution Complète d'Axis. Le support à long terme est recommandé si vous utilisez des intégrations tierces, qui ne sont pas continuellement validées par rapport au dernier support actif. Avec le support à long terme, les produits peuvent assurer la cybersécurité sans introduire de modification fonctionnelle ni affecter les intégrations existantes. Pour plus d'informations sur la stratégie du firmware du produit Axis, consultez axis.com/support/firmware.

Vérifier la version du firmware actuel

Le firmware est le logiciel qui détermine les fonctionnalités des périphériques réseau. Lorsque vous devez résoudre un problème, nous vous recommandons de commencer par vérifier la version actuelle du firmware. En effet, il est possible que la toute dernière version du firmware contienne un correctif pouvant résoudre votre problème.

Pour vérifier le firmware actuel :

1. Accédez à l'interface web du périphérique > **Statut**.
2. Consultez la version du firmware sous **Informations sur les périphériques**.

Mettre à niveau le firmware

Important

- Les paramètres préconfigurés et personnalisés sont enregistrés lors de la mise à niveau du firmware (à condition qu'il s'agisse de fonctions disponibles dans le nouveau firmware), mais Axis Communications AB n'offre aucune garantie à ce sujet.
- Assurez-vous que le périphérique reste connecté à la source d'alimentation pendant toute la durée du processus de mise à niveau.

AXIS A1610-B Network Door Controller

Dépannage

Remarque

La mise à niveau vers le dernier firmware de la piste active permet au périphérique de bénéficier des dernières fonctionnalités disponibles. Lisez toujours les consignes de mise à niveau et les notes de version disponibles avec chaque nouvelle version avant de procéder à la mise à niveau du firmware. Pour obtenir le dernier firmware et les notes de version, rendez-vous sur axis.com/support/firmware.

Remarque

En raison de la mise à jour de la base de données des utilisateurs, des groupes, des informations de connexion et d'autres données après la mise à jour d'un firmware, le premier démarrage peut prendre quelques minutes. Le temps requis dépend du volume de données.

1. Téléchargez le fichier de firmware sur votre ordinateur. Celui-ci est disponible gratuitement sur axis.com/support/firmware.
2. Connectez-vous au périphérique en tant qu'administrateur.
3. Accédez à **Maintenance > Firmware upgrade (Mise à niveau du firmware)** et cliquez sur **Upgrade (Mettre à niveau)**.

Une fois la mise à niveau terminée, le produit redémarre automatiquement.

4. Une fois le produit redémarré, videz le cache du navigateur Web.

Problèmes techniques, indications et solutions

Si vous ne trouvez pas les informations dont vous avez besoin ici, consultez la section consacrée au dépannage sur la page axis.com/support.

Problèmes de mise à niveau du firmware

Échec de la mise à niveau du firmware	Si la mise à niveau du firmware échoue, le périphérique recharge le firmware précédent. Le problème provient généralement du chargement d'un fichier de firmware incorrect. Vérifiez que le nom du fichier de firmware correspond à votre périphérique, puis réessayez.
Problèmes après la mise à niveau du firmware	Si vous rencontrez des problèmes après une mise à niveau du firmware, revenez à la version installée précédemment à partir de la page Maintenance .

Problème de configuration de l'adresse IP

Le périphérique se trouve sur un sous-réseau différent.	Si l'adresse IP du périphérique et l'adresse IP de l'ordinateur utilisé pour accéder au périphérique se trouvent sur des sous-réseaux différents, vous ne pourrez pas configurer l'adresse IP. Contactez votre administrateur réseau pour obtenir une adresse IP.
L'adresse IP est utilisée par un autre périphérique.	Déconnectez le périphérique Axis du réseau. Exécutez la commande ping (dans la fenêtre de commande/DOS, saisissez <code>ping</code> et l'adresse IP du périphérique) : <ul style="list-style-type: none">• Si vous recevez : <code>Reply from <IP address>: bytes=32; time=10...</code>, cela peut signifier que l'adresse IP est déjà utilisée par un autre périphérique sur le réseau. Obtenez une nouvelle adresse IP auprès de l'administrateur réseau, puis réinstallez le périphérique.• Si vous recevez : <code>Request timed out</code>, cela signifie que l'adresse IP est disponible pour une utilisation avec le périphérique Axis. Vérifiez tous les câbles et réinstallez le périphérique.
Conflit d'adresse IP possible avec un autre périphérique sur le même sous-réseau	L'adresse IP statique du périphérique Axis est utilisée avant la configuration d'une adresse dynamique par le serveur DHCP. Cela signifie que des problèmes d'accès au périphérique sont possibles si un autre périphérique utilise la même adresse IP statique par défaut.

AXIS A1610-B Network Door Controller

Dépannage

Impossible d'accéder au périphérique à partir d'un navigateur Web

Connexion impossible	<p>Lorsque le protocole HTTPS est activé, assurez-vous que le protocole correct (HTTP ou HTTPS) est utilisé lors des tentatives de connexion. Vous devrez peut-être entrer manuellement <code>http</code> ou <code>https</code> dans le champ d'adresse du navigateur.</p> <p>Si vous perdez le mot de passe du nom d'utilisateur <code>root</code>, les paramètres d'usine par défaut du périphérique devront être rétablis. Voir <i>Réinitialiser les paramètres par défaut</i> à la page 29.</p>
L'adresse IP a été modifiée par DHCP.	<p>Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et peuvent changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau. Identifiez le périphérique à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré).</p> <p>Si nécessaire, une adresse IP statique peut être attribuée manuellement. Pour plus d'instructions, consultez la page axis.com/support.</p>
Erreur de certification avec IEEE 802.1X	<p>Pour que l'authentification fonctionne correctement, la date et l'heure du périphérique Axis doivent être synchronisées avec un serveur NTP. Accédez à System > Date and time (Système > Date et heure).</p>

Le périphérique est accessible localement, mais pas en externe.

Pour accéder au périphérique en externe, nous vous recommandons d'utiliser l'une des applications pour Windows® suivantes :

- **AXIS Companion** : application gratuite, idéale pour les petits systèmes ayant des besoins de surveillance de base.
- **AXIS Camera Station** : version d'essai gratuite de 30 jours, application idéale pour les systèmes de petite taille et de taille moyenne.

Pour obtenir des instructions et des téléchargements, accédez à axis.com/vms.

Connexion impossible via le port 8883 avec MQTT sur SSL

Le pare-feu bloque le trafic via le port 8883, car ce dernier est considéré comme non sécurisé.	<p>Dans certains cas, le serveur/courtier ne fournit pas de port spécifique pour la communication MQTT. Il peut toujours être possible d'utiliser MQTT sur un port qui sert normalement pour le trafic HTTP/HTTPS.</p> <ul style="list-style-type: none">• Si le serveur/courtier prend en charge WebSocket/WebSocket Secure (WS/WSS), généralement sur le port 443, utilisez plutôt ce protocole. Vérifiez auprès du fournisseur de serveur/courtier si WS/WSS est pris en charge, ainsi que le port et le chemin d'accès de la base à utiliser.• Si le serveur/courtier prend en charge ALPN, l'utilisation de MQTT peut être négociée sur un port ouvert, tel que le port 443. Vérifiez auprès de votre serveur/courtier si ALPN est pris en charge et quels protocole ET port ALPN utiliser.
---	---

Facteurs ayant un impact sur la performance

Les principaux facteurs à prendre en compte sont les suivants :

- Une utilisation intensive du réseau en raison de l'inadéquation des infrastructures affecte la bande passante.

Contactez l'assistance

Contactez le service d'assistance sur la page axis.com/support.

