Comment gérer les certificats sur le contrôleur

Guide utilisateur

06/2019

EIO0000003898.00

www.schneider-electric.com

Le présent document comprend des descriptions générales et/ou des caractéristiques techniques des produits mentionnés. Il ne peut pas être utilisé pour définir ou déterminer l'adéquation ou la fiabilité de ces produits pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur ou intégrateur de réaliser l'analyse de risques complète et appropriée, l'évaluation et le test des produits pour ce qui est de l'application à utiliser et de l'exécution de cette application. Ni la société Schneider Electric ni aucune de ses sociétés affiliées ou filiales ne peuvent être tenues pour responsables de la mauvaise utilisation des informations contenues dans le présent document. Si vous avez des suggestions, des améliorations ou des corrections à apporter à cette publication, veuillez nous en informer.

Toutes les réglementations locales, régionales et nationales pertinentes doivent être respectées lors de l'installation et de l'utilisation de ce produit. Pour des raisons de sécurité et afin de garantir la conformité aux données système documentées, seul le fabricant est habilité à effectuer des réparations sur les composants.

Lorsque des équipements sont utilisés pour des applications présentant des exigences techniques de sécurité, suivez les instructions appropriées.

La non-utilisation du logiciel Schneider Electric ou d'un logiciel approuvé avec nos produits matériels peut entraîner des blessures, des dommages ou un fonctionnement incorrect.

Le non-respect de cette consigne peut entraîner des lésions corporelles ou des dommages matériels.

Table des matières

Consignes de sécurité

Informations importantes

AVIS

Lisez attentivement ces instructions et examinez le matériel pour vous familiariser avec l'appareil avant de tenter de l'installer, de le faire fonctionner, de le réparer ou d'assurer sa maintenance. Les messages spéciaux suivants que vous trouverez dans cette documentation ou sur l'appareil ont pour but de vous mettre en garde contre des risques potentiels ou d'attirer votre attention sur des informations qui clarifient ou simplifient une procédure.

La présence de ce symbole sur une étiquette “Danger“ ou “Avertissement“ signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.

Ce symbole est le symbole d'alerte de sécurité. Il vous avertit d'un risque de blessures corporelles. Respectez scrupuleusement les consignes de sécurité associées à ce symbole pour éviter de vous blesser ou de mettre votre vie en danger.

⚠ DANGER

DANGER signale un risque qui, en cas de non-respect des consignes de sécurité, **provoque** la mort ou des blessures graves.

⚠ AVERTISSEMENT

AVERTISSEMENT signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** la mort ou des blessures graves.

⚠ ATTENTION

ATTENTION signale un risque qui, en cas de non-respect des consignes de sécurité, **peut provoquer** des blessures légères ou moyennement graves.

AVIS

AVIS indique des pratiques n'entraînant pas de risques corporels.

REMARQUE IMPORTANTE

L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

AVANT DE COMMENCER

N'utilisez pas ce produit sur les machines non pourvues de protection efficace du point de fonctionnement. L'absence de ce type de protection sur une machine présente un risque de blessures graves pour l'opérateur.

⚠ AVERTISSEMENT

EQUIPEMENT NON PROTEGE

- N'utilisez pas ce logiciel ni les automatismes associés sur des appareils non équipés de protection du point de fonctionnement.
- N'accédez pas aux machines pendant leur fonctionnement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cet automatisme et le logiciel associé permettent de commander des processus industriels divers. Le type ou le modèle d'automatisme approprié pour chaque application dépendra de facteurs tels que la fonction de commande requise, le degré de protection exigé, les méthodes de production, des conditions inhabituelles, la législation, etc. Dans certaines applications, plusieurs processeurs seront nécessaires, notamment lorsque la redondance de sauvegarde est requise.

Vous seul, en tant que constructeur de machine ou intégrateur de système, pouvez connaître toutes les conditions et facteurs présents lors de la configuration, de l'exploitation et de la maintenance de la machine, et êtes donc en mesure de déterminer les équipements automatisés, ainsi que les sécurités et verrouillages associés qui peuvent être utilisés correctement. Lors du choix de l'automatisme et du système de commande, ainsi que du logiciel associé pour une application particulière, vous devez respecter les normes et réglementations locales et nationales en vigueur. Le document National Safety Council's Accident Prevention Manual (reconnu aux Etats-Unis) fournit également de nombreuses informations utiles.

Dans certaines applications, telles que les machines d'emballage, une protection supplémentaire, comme celle du point de fonctionnement, doit être fournie pour l'opérateur. Elle est nécessaire si les mains ou d'autres parties du corps de l'opérateur peuvent entrer dans la zone de point de pincement ou d'autres zones dangereuses, risquant ainsi de provoquer des blessures graves. Les produits logiciels seuls, ne peuvent en aucun cas protéger les opérateurs contre d'éventuelles blessures. C'est pourquoi le logiciel ne doit pas remplacer la protection de point de fonctionnement ou s'y substituer.

Avant de mettre l'équipement en service, assurez-vous que les dispositifs de sécurité et de verrouillage mécaniques et/ou électriques appropriés liés à la protection du point de fonctionnement ont été installés et sont opérationnels. Tous les dispositifs de sécurité et de verrouillage liés à la protection du point de fonctionnement doivent être coordonnés avec la programmation des équipements et logiciels d'automatisation associés.

NOTE : La coordination des dispositifs de sécurité et de verrouillage mécaniques/électriques du point de fonctionnement n'entre pas dans le cadre de cette bibliothèque de blocs fonction, du Guide utilisateur système ou de toute autre mise en œuvre référencée dans la documentation.

DEMARRAGE ET TEST

Avant toute utilisation de l'équipement de commande électrique et des automatismes en vue d'un fonctionnement normal après installation, un technicien qualifié doit procéder à un test de démarrage afin de vérifier que l'équipement fonctionne correctement. Il est essentiel de planifier une telle vérification et d'accorder suffisamment de temps pour la réalisation de ce test dans sa totalité.

⚠ AVERTISSEMENT

RISQUES INHERENTS AU FONCTIONNEMENT DE L'EQUIPEMENT

- Assurez-vous que toutes les procédures d'installation et de configuration ont été respectées.
- Avant de réaliser les tests de fonctionnement, retirez tous les blocs ou autres cales temporaires utilisés pour le transport de tous les dispositifs composant le système.
- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Effectuez tous les tests de démarrage recommandés dans la documentation de l'équipement. Conservez toute la documentation de l'équipement pour référence ultérieure.

Les tests logiciels doivent être réalisés à la fois en environnement simulé et réel.

Vérifiez que le système entier est exempt de tout court-circuit et mise à la terre temporaire non installée conformément aux réglementations locales (conformément au National Electrical Code des Etats-Unis, par exemple). Si des tests diélectriques sont nécessaires, suivez les recommandations figurant dans la documentation de l'équipement afin d'éviter de l'endommager accidentellement.

Avant de mettre l'équipement sous tension :

- Enlevez les outils, les instruments de mesure et les débris éventuels présents sur l'équipement.
- Fermez le capot du boîtier de l'équipement.
- Retirez toutes les mises à la terre temporaires des câbles d'alimentation entrants.
- Effectuez tous les tests de démarrage recommandés par le fabricant.

FONCTIONNEMENT ET REGLAGES

Les précautions suivantes sont extraites du document NEMA Standards Publication ICS 7.1-1995 (la version anglaise prévaut) :

- Malgré le soin apporté à la conception et à la fabrication de l'équipement ou au choix et à l'évaluation des composants, des risques subsistent en cas d'utilisation inappropriée de l'équipement.
- Il arrive parfois que l'équipement soit déréglé accidentellement, entraînant ainsi un fonctionnement non satisfaisant ou non sécurisé. Respectez toujours les instructions du fabricant pour effectuer les réglages fonctionnels. Les personnes ayant accès à ces réglages doivent connaître les instructions du fabricant de l'équipement et les machines utilisées avec l'équipement électrique.
- Seuls ces réglages fonctionnels, requis par l'opérateur, doivent lui être accessibles. L'accès aux autres commandes doit être limité afin d'empêcher les changements non autorisés des caractéristiques de fonctionnement.

A propos de ce manuel

Présentation

Objectif du document

Ce document explique comment gérer les certificats qui doivent être utilisés pour une communication TCP sécurisée au niveau de l'application.

Champ d'application

Ce document a été actualisé pour le lancement d'EcoStruxure™ Machine Expert V1.1.

Documents associés

Titre du document	Référence
Modicon M262 Logic/Motion Controller - Guide de référence du matériel	*EIO0000003659 (ENG);* *EIO0000003660 (FRE);* *EIO0000003661 (GER);* *EIO0000003662 (SPA);* *EIO0000003663 (ITA);* *EIO0000003664 (CHS)*
EcoStruxure Machine Expert - Guide de programmation	*EIO0000002854 (ENG)* ; *EIO0000002855 (FRE)* ; *EIO0000002856 (GER)* ; *EIO0000002858 (SPA)* ; *EIO0000002857 (ITA)* ; *EIO0000002859 (CHS)*

Information spécifique au produit

⚠ AVERTISSEMENT

PERTE DE CONTROLE

- Le concepteur d'un système de commande doit envisager les modes de défaillance possibles des chemins de commande et, pour certaines fonctions de commande critiques, prévoir un moyen d'atteindre un état sécurisé en cas de défaillance d'un chemin, et après cette défaillance. Par exemple, l'arrêt d'urgence, l'arrêt en cas de surcourse, la coupure de courant et le redémarrage sont des fonctions de contrôle cruciales.
- Des canaux de commande séparés ou redondants doivent être prévus pour les fonctions de commande critique.
- Les liaisons de communication peuvent faire partie des canaux de commande du système. Soyez particulièrement attentif aux implications des retards de transmission imprévus ou des pannes de liaison.
- Respectez toutes les réglementations de prévention des accidents ainsi que les consignes de sécurité locales.[1]
- Chaque implémentation de cet équipement doit être testée individuellement et entièrement pour s'assurer du fonctionnement correct avant la mise en service.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

[1] Pour plus d'informations, consultez le document NEMA ICS 1.1 (dernière édition), « Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control » (Directives de sécurité pour l'application, l'installation et la maintenance de commande statique) et le document NEMA ICS 7.1 (dernière édition), « Safety Standards for Construction and Guide for Selection, Installation, and Operation of Adjustable-Speed Drive Systems » (Normes de sécurité relatives à la construction et manuel de sélection, installation et opération de variateurs de vitesse) ou son équivalent en vigueur dans votre pays.

⚠ AVERTISSEMENT

FONCTIONNEMENT IMPREVU DE L'EQUIPEMENT

- N'utilisez que le logiciel approuvé par Schneider Electric pour faire fonctionner cet équipement.
- Mettez à jour votre programme d'application chaque fois que vous modifiez la configuration matérielle physique.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Terminologie utilisée dans les normes

Les termes techniques, la terminologie, les symboles et les descriptions correspondantes employés dans ce manuel ou figurant dans ou sur les produits proviennent généralement des normes internationales.

Dans les domaines des systèmes de sécurité fonctionnelle, des variateurs et de l'automatisme en général, les termes employés sont *sécurité*, *fonction de sécurité*, *état sécurisé*, *défaut*, *réinitialisation du défaut*, *dysfonctionnement*, *panne*, *erreur*, *message d'erreur*, *dangereux*, etc.

Entre autres, les normes concernées sont les suivantes :

Norme	Description
IEC 61131-2:2007	Automates programmables - Partie 2 : exigences et essais des équipements
ISO 13849-1:2015	Sécurité des machines : parties des systèmes de commande relatives à la sécurité. Principes généraux de conception
EN 61496-1:2013	Sécurité des machines : équipements de protection électro-sensibles. Partie 1 : Prescriptions générales et essais
ISO 12100:2010	Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque
EN 60204-1:2006	Sécurité des machines - Équipement électrique des machines - Partie 1 : règles générales
ISO 14119:2013	Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix
ISO 13850:2015	Sécurité des machines - Fonction d'arrêt d'urgence - Principes de conception
IEC 62061:2015	Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmable relatifs à la sécurité
IEC 61508-1:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité : prescriptions générales.
IEC 61508-2:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité : exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.
IEC 61508-3:2010	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité : exigences concernant les logiciels.
IEC 61784-3:2016	Réseaux de communication industriels - Profils - Partie 3 : Bus de terrain de sécurité fonctionnelle - Règles générales et définitions de profils.
2006/42/EC	Directive Machines
2014/30/EU	Directive sur la compatibilité électromagnétique
2014/35/EU	Directive sur les basses tensions

De plus, des termes peuvent être utilisés dans le présent document car ils proviennent d'autres normes telles que :

Norme	Description
Série IEC 60034	Machines électriques rotatives
Série IEC 61800	Entraînements électriques de puissance à vitesse variable
Série IEC 61158	Communications numériques pour les systèmes de mesure et de commande – Bus de terrain utilisés dans les systèmes de commande industriels

Enfin, le terme *zone de fonctionnement* utilisé dans le contexte de la description de dangers spécifiques a la même signification que les termes *zone dangereuse* ou *zone de danger* employés dans la *directive Machines* (*2006/42/EC*) et la norme *ISO 12100:2010*.

NOTE : Les normes susmentionnées peuvent s'appliquer ou pas aux produits cités dans la présente documentation. Pour plus d'informations sur chacune des normes applicables aux produits décrits dans le présent document, consultez les tableaux de caractéristiques de ces références de produit.

Applications mettant en œuvre une communication TCP sécurisée

Bibliothèques de communication

EcoStruxure Machine Expert propose des bibliothèques compatibles avec la communication sécurisée via TLS (Transport Layer Security). Ces bibliothèques offre une fonctionnalité de client et/ou serveur, comme indiqué dans le tableau suivant :

Bibliothèque	Fonctionnalité offerte :
TcpUdpCommunication	• Client TCP • Serveur TCP
HttpHandling	Client HTTP/HTTPS
MqttHandling	Client MQTT / secured MQTT
EmailHandling	• Client SMTP/SMTPS • Client POP3/POP3S

Les clients ou le serveur peuvent être configurés de manière à utiliser le protocole TLS pour la communication cryptée.

La prise en charge ou non d'une connexion utilisant le protocole TLS dépend du contrôleur sur lequel le bloc fonction correspondant est utilisé. Reportez-vous au manuel de votre contrôleur pour vérifier si les communications TCP qui utilisent le protocole TLS sont prises en charge.

Certificats

Dans le contexte de TLS, les certificats peuvent être utilisés pour vérifier l'identité des partenaires de communication. Ces certificats sont envoyés durant l'établissement d'une connexion (transfert TLS). Le client n'est pas tenu d'envoyer de certificat, sauf si le serveur en fait la demande. Par contre, le serveur envoie systématiquement son certificat. Une connexion ne peut être établie avec le partenaire de communication que si le résultat de la vérification du certificat est positif.

Vérification des certificats

Les bibliothèques EcoStruxure Machine Expert prenant en charge la connexion sécurisée via TLS fournissent le paramètre `etCertVerifyMode`, qui permet de sélectionner le mode de vérification du certificat envoyé par le partenaire de communication lors du transfert TLS.

Modes pris en charge :

Mode `etCertVerifyMode`	Description
`TrustedOnly`	Le partenaire de communication doit fournir un certificat. Ce certificat doit être déclaré comme approuvé.

Mode `etCertVerifyMode`	Description
`AllCertificates`	Le partenaire de communication doit fournir un certificat. Ce certificat n'est pas vérifié.
`NotVerified`	Le partenaire de communication n'est pas tenu de fournir un certificat.

Si le client ou le serveur est configuré pour vérifier le certificat du serveur en mode `TrustedOnly`, il est nécessaire de gérer manuellement les certificats sur votre contrôleur. Vous pouvez effectuer cette opération à l'aide de l'éditeur **Security Screen** dans EcoStruxure Machine Expert Logic Builder. La procédure à suivre est décrite dans la section suivante.

NOTE : `TrustedOnly` est le seul mode permettant d'authentifier le partenaire de communication.

Gestion des certificats sur le contrôleur

Présentation

Si le client ou le serveur est configuré pour vérifier le certificat du partenaire de communication en mode `TrustedOnly`, le certificat correspondant doit être déclaré comme approuvé et disponible sur le contrôleur. Vous pouvez gérer les certificats sur votre contrôleur à l'aide de l'éditeur **Security Screen** dans EcoStruxure Machine Expert Logic Builder.

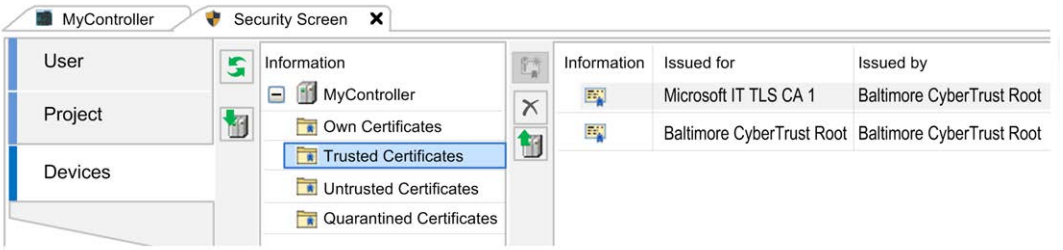
Editeur Security Screen

L'éditeur **Security Screen** est accessible dans EcoStruxure Machine Expert Logic Builder via la commande **Affichage → Security Screen**. L'onglet **Devices** de l'éditeur **Security Screen** permet d'accéder aux dossiers dédiés à la gestion des certificats sur le contrôleur connecté.

Cliquez sur le bouton  pour afficher ces onglets et leur contenu.

Voici les dossiers disponibles pour le Modicon M262 Logic/Motion Controller, par exemple :

- **Own Certificates** : certificats détenus par le contrôleur et qui servent pour les services associés à cet équipement.
- **Trusted Certificates** : certificats délivrés par une source de certification de confiance.
- **Untrusted Certificates** : certificats que vous avez déclarés comme non approuvés.
- **Quarantined Certificates** : certificats qui ne remplissent pas les critères des autres catégories.

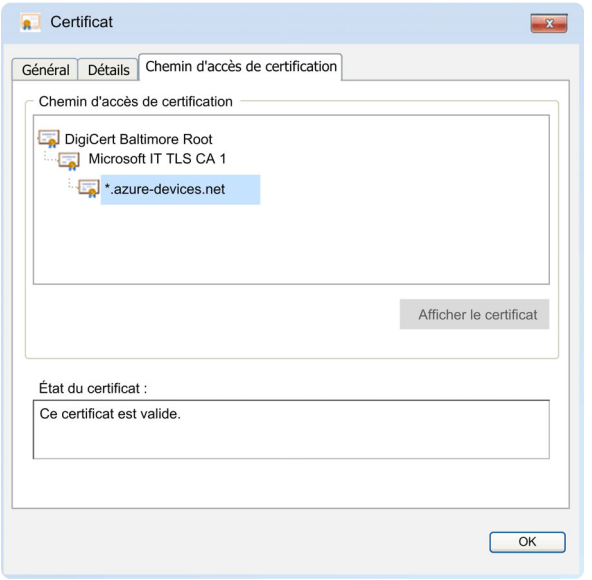


Pour qu'un certificat puisse être vérifié en mode `TrustedOnly`, le ou les certificats correspondants doivent être disponibles dans le dossier **Trusted Certificates**.

Déclaration d'un certificat comme approuvé

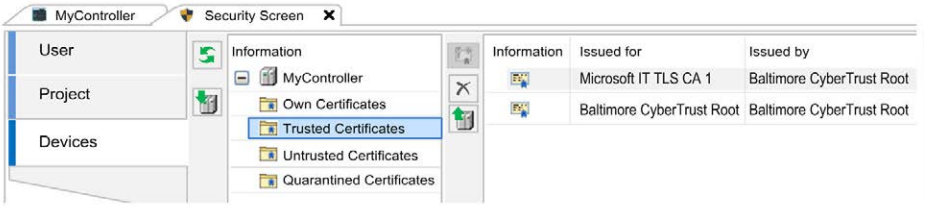
Pour déclarer un certificat comme approuvé sur votre contrôleur, procédez comme suit :

Étape	Action	Commentaire
1	Enregistrez sur le PC exécutant EcoStruxure Machine Expert le certificat de l'équipement ou du logiciel qui vous a été remis par le fabricant.	Si le fabricant de l'équipement ou du logiciel ne vous a pas envoyé de certificat, établissez une connexion tel que décrit au paragraphe *Obtention d'un certificat inconnu* *(voir page 18)*.
2	Double-cliquez sur le certificat. **Résultat** : la boîte de dialogue **Certificat** s'ouvre.	–
3	Examinez attentivement le certificat dans l'onglet **Général** avant de le déclarer ou pas comme approuvé.	–

Étape	Action	Commentaire
4	Sélectionnez l'onglet **Chemin d'accès de certification**, et vérifiez si le dossier contient une ou plusieurs entrées. 	Si une seule entrée apparaît dans l'onglet **Chemin d'accès de certification**, le certificat est auto-signé (comme c'est le cas avec le Modicon M262 Logic/Motion Controller). Vous pouvez alors ignorer les deux étapes suivantes, et passer à l'étape 7. Si une arborescence apparaît dans l'onglet **Chemin d'accès de certification**, le certificat a été signé par une autorité de certification (CA, Certificate Authority). Vous pouvez passer aux étapes suivantes qui concernent les certificats CA.
5	Si le certificat a été signé par une autorité de certification, vérifiez chaque certificat dans l'arborescence de l'onglet **Chemin d'accès de certification**, y compris celui en racine.	–
6	Sélectionnez un certificat dans l'onglet **Chemin d'accès de certification**, puis cliquez sur le bouton **Afficher le certificat**. Répétez l'opération pour chaque certificat. **Résultat** : le certificat sélectionné s'ouvre dans une nouvelle boîte de dialogue.	–
7	Sélectionnez l'onglet **Détails**, puis cliquez sur le bouton **Copier dans un fichier...** pour enregistrer le certificat sur le PC.	–
8	Téléchargez, dans le dossier **Trusted Certificates** de votre contrôleur, les fichiers de certificat enregistrés.	Consultez le paragraphe *Téléchargement de certificats déclarés comme approuvés sur le contrôleur (voir page 17)*.

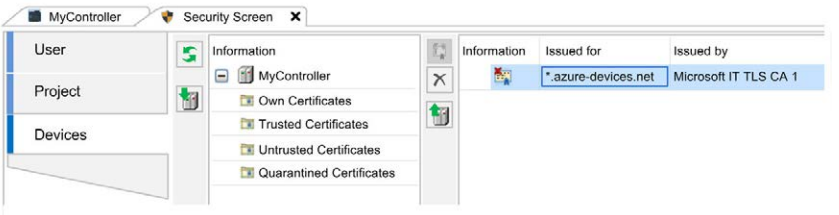
Téléchargement de certificats sur le contrôleur

Procédez comme suit pour enregistrer, dans le dossier **Trusted Certificates** du contrôleur, des certificats déclarés comme approuvés :

Étape	Action
1	Dans EcoStruxure Machine Expert Logic Builder, ouvrez l'éditeur **Security Screen** à partir du menu **Affichage**.
2	Dans l'éditeur **Security Screen**, sélectionnez l'onglet **Devices**.
3	Cliquez sur le bouton **Refresh the list of available devices and their certificate stores**. **Résultat** : l'écran est mis à jour en fonction des informations en provenance du contrôleur connecté.
4	Sélectionnez le dossier **Trusted Certificates**, puis cliquez sur le bouton **Download**.
5	Dans la boîte de dialogue **Ouvrir**, accédez au dossier contenant le ou les fichiers de certificat enregistrés sur le PC exécutant EcoStruxure Machine Expert.
6	Sélectionnez le ou les fichiers de certificat, puis cliquez sur le bouton **Ouvrir**. **Résultat** : les certificats sont téléchargés sur le contrôleur et apparaissent sur la droite de l'éditeur **Security Screen** en tant que contenu du dossier **Trusted Certificates**. 

Obtention d'un certificat inconnu

Lorsque le certificat d'un partenaire de communication n'est pas disponible et ne peut être obtenu auprès du fabricant ni d'une autre source, procédez comme suit :

Étape	Action	Informations complémentaires
1	Etablissez une connexion sécurisée entre le client et le serveur, en définissant le paramètre `etCertVerifyMod` sur `TrustedOnly` : ● Si votre application met en œuvre un client, établissez la connexion avec le serveur. ● Si votre application met en œuvre un serveur, ouvrez celui-ci et acceptez la connexion entrante en provenance du client. **Résultats** : ● Etant donné que le certificat reçu du serveur ou du client est inconnu, il est impossible d'établir la connexion. ● Le certificat inconnu est enregistré dans le dossier **Quarantined Certificates** sur votre contrôleur.	● Si votre application de contrôleur met en œuvre un client, le résultat `ConnectionFailed` indique que le certificat reçu du serveur est inconnu. ● Si votre application de contrôleur met en œuvre un serveur, le résultat `TlsError` indique que le certificat reçu du client est inconnu. **NOTE :** si le dossier est vide, le partenaire de communication n'a pas envoyé son certificat. Vérifiez la configuration du client ou du serveur distant pour savoir si vous allez recevoir un certificat.
2	Dans EcoStruxure Machine Expert Logic Builder, ouvrez l'éditeur **Security Screen**, puis cliquez sur le bouton **Refresh the list of available devices and their certificate stores**.	–
3	Sélectionnez le dossier **Quarantined Certificates**.	–
4	Sélectionnez le certificat dans la liste sur la droite de l'éditeur **Security Screen**, puis cliquez sur le bouton **Upload the selected certificate from the device and save it to your PC**. 	
5	Dans la boîte de dialogue **Enregistrer sous**, accédez au dossier dans lequel vous souhaitez enregistrer le ou les fichiers de certificat sur le PC exécutant EcoStruxure Machine Expert, puis cliquez sur le bouton **Enregistrer**.	–

Étape	Action	Informations complémentaires
6	Vérifiez le ou les certificats et déclarez-les ou pas comme approuvés, tel que décrit dans le paragraphe sur l'*obtention de certificats approuvés* *(voir page 15)*.	–
7	Téléchargez sur le contrôleur le ou les certificats déclarés comme approuvés *(voir page 17)*.	–

Remarques à propos de l'utilisation de certificats

Remarques

Tenez compte des remarques suivantes si vous utilisez des certificats pour des communications sécurisées :

- Les certificats ayant une période de validité limitée, il convient de les gérer et de les mettre à jour régulièrement, et ce tout au long du cycle de vie de votre machine ou de votre système de contrôle.
- L'horloge du contrôleur permet de vérifier si le certificat est encore valide. Aussi, vérifiez régulièrement qu'elle est synchronisée avec l'heure UTC (Universal Time Coordinated). Pour cela, consultez l'onglet **Services** dans la configuration du contrôleur.
- Une autre méthode pour déclarer des certificats comme non approuvés consiste à les enregistrer dans le dossier **Untrusted Certificates** du contrôleur.