Milestone – lares 4.0

Integrazione
Plugin Milestone e centrali lares 4.0
Procedure di aggiornamento
a partire dalla ver. 2.1.X
della lares 4.0

Questo documento descrive le procedure di aggiornamento delle centrali della famiglia lares 4.0 e del componente di integrazione della piattaforma XProtect di Milestone, necessarie per garantire la corretta compatibilità tra i due sistemi a partire dalla versione 2.1.X della lares 4.0. Il documento include sia le istruzioni per l'aggiornamento delle centrali, sia le istruzioni per l'adeguamento della componente integrata della piattaforma, che consiste nell'installazione del pacchetto *.msi e nella registrazione del certificato radice, al fine di consentire l'utilizzo del Protocollo Cifrato (TLS).

Indice

Introduzione 3
Procedura di aggiornamento lares 4.0 4
Istruzioni per l'aggiornamento della lares 4.0 5
Aggiornamento del Plugin Milestone 6
Registrazione Certificato Radice 6

Introduzione

A partire dalla versione 2.1.X delle centrali lares 4.0, la comunicazione con la piattaforma XProtect di Milestone richiede l'aggiornamento del componente di integrazione, al fine di mantenere la compatibilità tra i sistemi e consentire l'utilizzo del Protocollo Cifrato (TLS). Tale aggiornamento prevede l'installazione di un nuovo plugin e la registrazione del certificato radice.

Questo documento descrive le **procedure di aggiornamento** delle centrali della famiglia lares 4.0 e del componente di integrazione della piattaforma XProtect di Milestone, necessarie **per garantire la corretta compatibilità** tra i due sistemi a partire dalla versione 2.1.X. Il documento include sia le istruzioni per l'aggiornamento delle centrali, sia le istruzioni per l'adeguamento della componente integrata della piattaforma, che consiste nell'installazione del pacchetto *.msi e nella registrazione del certificato radice, al fine di consentire l'utilizzo del Protocollo Cifrato (TLS).

Procedura di aggiornamento lares 4.0

In occasione del rinnovo della certificazione SBSC (**SSF 1014 Edizione 6**, specifica per il mercato svedese) abbiamo recepito i più recenti requisiti di sicurezza che innalzano i già elevati criteri di integrità e stabilità complessiva del sistema, estendendoli ed applicandoli a tutte le centrali lares 4.0.

La piattaforma lares-S è stata allineata allo standard **SSF 1120-1 (IoT Connected Devices)**, richiamato dalla normativa **SSF 1014 Edizione 6**.

Lo standard SSF 1120-1 è **derivato dalla normativa europea ETSI EN 303 645** e ne recepisce i requisiti fondamentali in materia di cybersecurity per dispositivi IoT connessi a Internet.

L'adeguamento a questi standard ha comportato una serie di aggiornamenti software e firmware finalizzati a:

- Rafforzamento della protezione da attacchi informatici
- Migliore sicurezza dei dati e delle comunicazioni cifrate
- Gestione più sicura delle chiavi crittografiche
- Maggiore affidabilità e integrità degli aggiornamenti firmware

Per poter utilizzare i miglioramenti introdotti nel sistema, occorre aggiornare il firmware della centrale. L'aggiornamento della centrale richiede 2 step obbligatori:

- **Aggiornamento alla versione 2.0.27**
- **Aggiornamento alla versione 2.1.35**

Nota: A partire da questa versione 2.1.35, i file di aggiornamento cambiano estensione: *.cose al posto di *.ksa.

IMPORTANTE: Durante la procedura di aggiornamento è necessario che la centrale abbia accesso ad internet!

Istruzioni per l'aggiornamento della lares 4.0

Prima di iniziare

1. Collegare momentaneamente la centrale ad Internet. Non è necessaria la registrazione della centrale a SecureWeb.
2. Scaricare dal sito www.kseniasecureweb.com i pacchetti di aggiornamento:
   - cumulative update – v. 2.0.27 : file: lares4_update.ksa
   - cumulative update – v. 2.1.35 : file: lares4_update.cose

Step 1 – Aggiornamento alla versione 2.0.27

1. Accedi al web server di centrale
2. Clicca su "Carica file di aggiornamento" e seleziona il file: **lares4_update.ksa**
3. Attendi il completamento dell'installazione ed il riavvio della centrale.
4. Accedi nuovamente al web server di centrale e verifica che la versione installata sia **2.0.27**.Il browser dovrebbe richiedere di riaccettare il certificato.

Step 2 – Aggiornamento alla versione 2.1.35

1. Clicca nuovamente su "Carica file di aggiornamento" e seleziona il file: **lares4_update.cose**
2. Attendi il completamento dell'installazione ed il riavvio della centrale.
3. Accedi nuovamente al web server di centrale e verifica che la versione installata sia **2.1.35**. Se l'aggiornamento non è andato a buon fine, ripetere il caricamento del file di aggiornamento.
4. Una volta installata la versione 2.1.35, la centrale può essere scollegata da Internet. **I futuri aggiornamenti potranno essere installati con la centrale offline**.

NOTA IMPORTANTE!
Verificare e aggiornare le regole del firewall perché permettano alla centrale di raggiungere:

a. Porta remota: 9443
b. Protocollo: TCP
c. URL: api.kseniasecureweb.com/*

Aggiornamento del Plugin Milestone

Scaricare il pacchetto "**MIP_plugin_lares4.0**" da **DOWNLOAD DEGLI AGGIORNAMENTI: da WWW.KSENIASECUREWEB.COM , accedere alla cartella Documentazione e software -> Milestone**

e procedere con l'installazione nel modo consueto; il file compresso "**MIP_plugin_lares4.0**" contiene, oltre al file di installazione del plugin "KS_Installer.msi", il Certificato Radice da installare come descritto nel capitolo successivo.

Il Plugin dispone di una propria procedura di installazione che crea la specifica cartella di destinazione, copiandoci all'interno tutti i file necessari al corretto funzionamento.

La cartella di destinazione proposta è C:\Programmi\Milestone\MIPPlugins\KS; la cartella finale KS può essere modificata in fase di installazione stessa, sebbene sia consigliato utilizzare il nome proposto.

In caso di aggiornamenti la procedura provvederà alla rimozione della vecchia versione prima di installare la nuova.

Registrazione Certificato Radice

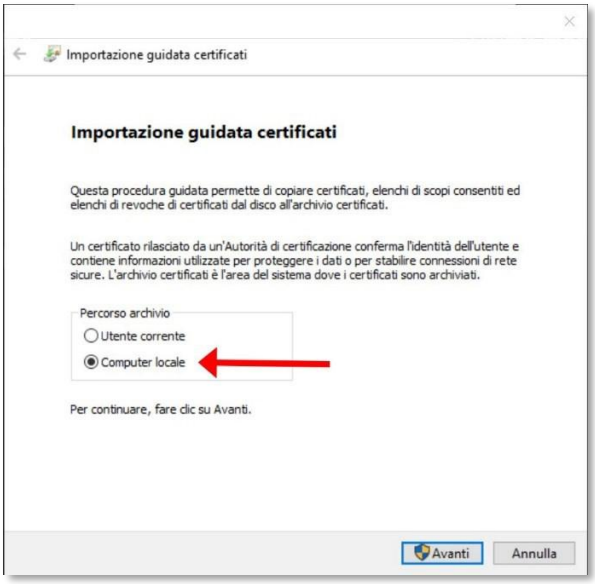
Affinché la verifica della Catena di Certificati funzioni correttamente è necessario che il Certificato Radice sia registrato nello Store "Computer locale" del Server e non in quello definito "Utente corrente" che rappresenta il default.

Di seguito i passaggi della registrazione:

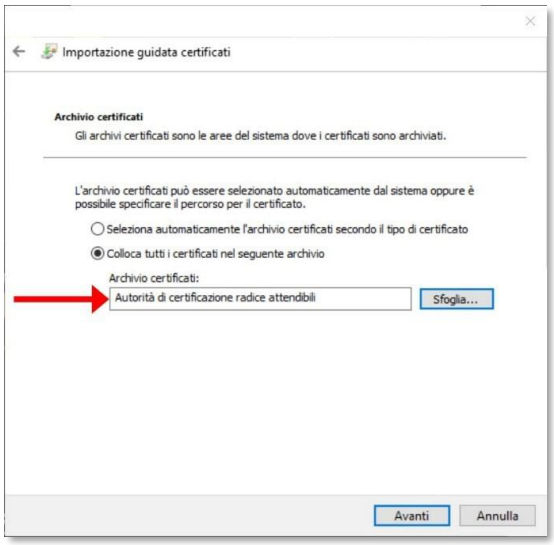
1. Eseguire doppio click sul file **Certificato Radice KS-Root-CA-R1-cert.crt** appena scaricato, quindi cliccare sul bottone “Installa certificato…”



2. Selezione dello Store “Computer locale”



3. Selezione archivio “Autorità di certificazione radice attendibili”



4. Completamento dell’operazione

