DOMOTICA LABS WIKI - http://www.domoticalabs.com/dokuwiki/

HTTPS e Certificati SSL

Configurare Certificati SSL

<u>Dalla versione</u> **1.3.0** in poi, iKon è in grado di generare certificati SSL corretti per un accesso più sicuro. Per poter sfruttare appieno questa nuova funzionalità, è necessario effettuare una breve operazione su ciascun client che desidera accedere ai prodotti <u>Domotica Labs</u>.

L'operazione è molto semplice, differisce leggermente a seconda del sistema operativo che si sta usando e consiste semplicemente nell'indicare Domotica Labs come una sorgente affidabile di certificati SSL <u>sia sul browser che su Java</u>.

Se un client non è configurato, accedendo ad un iKon in HTTPS, in alto a sinistra nella barra degli indirizzi verrà mostrato un lucchetto "aperto" e verranno continuamente mostrati dei messaggi di "Warning" ad ogni accesso.

92.168.0.193/ikon/n

HOME

🕂 IKON

In caso contrario, se il client considera Domotica Labs come una sorgente affidabile di certificati, si mostrerà un lucchetto verde.







Last update:	ikap fage potwork selved http://www.domoticalabe.com/dokuwiki/doku.php?id=ikap.fage.potwork.celvelverv=1426071807
2015/03/11 11:03	

Per configurare Domotica Labs come una sorgente affidabile di certificati è sufficiente effettuare le seguenti operazioni:

Java

Questa operazione è necessaria solo se si desidera accedere in HTTPS ad iKon con il modulo **VoIP licenziato**, ed evitare messaggi di "warning" generati da Java.

- Scaricare il certificato di CA (Certification Authority) di Domotica Labs dal seguente indirizzo: certificato CA.
- Avviare il "Pannello di Controllo Java", selezionare l'etichetta "Sicurezza" e premere il bottone "Gestisci Certificati"



• Selezionare la linguetta "Utente"

- Selezionare il Tipo di certificato "CA Firmataria"
- Premere il bottone "Importa"

\$	Pannello di controllo Java	-		
Generale Aggiorna Java	Sicurezza Avanzate			
Abilitare il contenuto Jav	a nel browser			
	Certificati			x
Tipo certificato: CA firmat Utente Sistema	taria			•
Rilasciato a	Rilasciato da			
Domotica Labs	Domotica Labs			^
				×
Impo	orta Esporta Rimuovi Dettagli			
			Chiu	ıdi
	OK Annu	lla	Ap	plica

- Selezionare il file certificato CA appena scaricato.
- Ripete l'operazione per tutti gli utenti della macchina coinvolti dall'uso della domotica

Windows - Chrome e IE

- Rammentare che IE non è ufficialmente supportato. Nulla vieta tuttavia di provare ad utilizzarlo per navigare un iKon configurato con Chrome.
- Accedere a Windows con un utente di amministrazione.
- Scaricare il certificato di CA (Certification Authority) di Domotica Labs dal seguente indirizzo: certificato CA.
- Fare un doppio-click sul file scaricato.
- Concedere al sistema di aprire il file nel caso si presenti un messaggio di warning.

		Apri file - Avviso di sicurezza	×
Aprire il	file?		
	Nome:	D:\tmp\rootCA.Dlabs.crt	
	Autore:	Autore sconosciuto	
	Tipo:	Certificato di sicurezza	
	Da:	D:\tmp\rootCA.Dlabs.crt	
And And	a cempre prim	Apri Annulla	
- AVVIS	a sempre prin	a di apiri e questo nie	
۲	l file scaricat può danneg attendibile, r	i da Internet possono essere utili, ma questo tipo di file giare il computer. Se l'origine non è considerata non aprire il software. <u>Quali rischi si corrono</u>	

• Premere sul pulsante "Installa certificato".

	Certificato ×
Gen	erale Dettagli Percorso certificazione
	Informazioni sul certificato
	Scopo certificato: • Criteri di rilascio • Criteri di applicazione
-	Rilasciato a: Domotica Labs
	Rilasciato da: Domotica Labs
	Valido dal 01/07/2014 al 08/02/2020
Ulter	Installa certificato Dichiarazione emittente
	ОК

• Selezionare di voler installare il certificato sul "Computer Locale" (nulla vieta di installare il certificato solo sull'utente corrente; tuttavia deve esser chiaro che, accedendo con un utente

differente, Windows non considererà più Domotica Labs come una sorgente affidabile di certificati) e poi premere "Avanti".

	×
📀 🍠 Importazione guidata certificati	
Importazione guidata certificati	
Questa procedura guidata permette di copiare certificati, elenchi di scopi consentiti ed elenchi di revoche di certificati dal disco all'archivio certificati.	
Un certificato rilasciato da un'Autorità di certificazione conferma l'identità dell'utente e contiene informazioni utilizzate per proteggere i dati o per stabilire connessioni di rete sicure. L'archivio certificati è l'area del sistema dove i certificati sono archiviati.	
Percorso archivio	
O Utente corrente O Computer locale	
Per continuare, scegliere Avanti.	
Annu	lla

• Selezionare di voler collocare il certificato in un archivio specifico e poi premere "Sfoglia".

	X
📀 🍠 Importazione guidata certificati	
Archivio certificati	
Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati.	
	_
L'archivio certificati può essere selezionato automaticamente dal sistema oppure è	
possibile specificare il percorso per il certificato.	
Seleziona automaticamente l'archivio certificati secondo il tipo di certificato	
Colloca tutti i certificati nel seguente archivio	
Archivio certificati:	
Sfoglia	
Ulteriori informazioni suoli archivi di certificati	
ercher internazioni dagli <u>erchint er caronade</u>	
Avanti Annulla	

• Selezionare l'archivio "Autorità di certificazione di radice attendibile" e poi premere "Ok".

Archivio certifi Gli archivi (Selezione archivio certificati	Piati.
L'archivio c possibile sr	Selezionare l'archivio certificati da utilizzare.	oppure è
) Sele	Autorità di certificazione radice attendibi	rtificato
Ard	Autorita di certificazione intermedie Autori attendibili Certificati non disponibili nell'elenco locale	Sfoglia
	Mostra archivi fisici	
Ulteriori informa	zioni sugli <u>archivi di certificati</u>	

• Dopodichè premere "Avanti".

 ✓ Importazione guidata certificati Archivio certificati Gi archivi certificati sono le aree del sistema dove i certificati sono archiviati. L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificati secondo il tipo di certificato ✓ Seleziona automaticamente l'archivio certificati secondo il tipo di certificato ✓ Colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili ✓ Sfoglia 		×
Archivio certificati Gi archivio certificati sono le aree del sistema dove i certificati sono archiviati. L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificati secondo il tipo di certificato Seleziona automaticamente l'archivio certificati secondo il tipo di certificato O colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili Sfoglia	📀 🍠 Importazione guidata certificati	
Achivio certificati sono le aree del sistema dove i certificati sono archiviati. L'archivio certificati può essere selezionato automaticamente dal sistema oppure è sossibile specificare il percorso per il certificati secondo il tipo di certificato Image: Imag		
Archivio certificati Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati. L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato. Seleziona automaticamente l'archivio certificati secondo il tipo di certificato © Colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili Sfoglia		
Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati. L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato. Seleziona automaticamente l'archivio certificati secondo il tipo di certificato Colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili Ulteriori informazioni sugli <u>archivi di certificati</u>	Archivio certificati	
L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato. Seleziona automaticamente l'archivio certificati secondo il tipo di certificato Colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili Sfoglia Ulteriori informazioni sugli <u>archivi di certificati</u>	Gli archivi certificati sono le aree del sistema dove i certificati sono archiviati.	
L'archivio certificati può essere selezionato automaticamente dal sistema oppure è possibile specificare il percorso per il certificato. © Seleziona automaticamente l'archivio certificati secondo il tipo di certificato © Colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili Sfoglia Ulteriori informazioni sugli <u>archivi di certificati</u>		
 Seleziona automaticamente l'archivio certificati secondo il tipo di certificato Colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili Sfoglia Ulteriori informazioni sugli archivi di certificati 	L'archivio certificati può essere selezionato automaticamente dal sistema oppu possibile specificare il percorso per il certificato.	re è
 Colloca tutti i certificati nel seguente archivio Archivio certificati: Autorità di certificazione radice attendibili Sfoglia Ulteriori informazioni sugli archivi di certificati 	Seleziona automaticamente l'archivio certificati secondo il tipo di certifica	ato
Archivio certificati: Autorità di certificazione radice attendibili Sfoglia Ulteriori informazioni sugli <u>archivi di certificati</u>	 Colloca tutti i certificati nel seguente archivio 	
Autorità di certificazione radice attendibili Sfoglia Ulteriori informazioni sugli archivi di certificati	Archivio certificati:	
Ulteriori informazioni sugli <u>archivi di certificati</u>	Autorità di certificazione radice attendibili Sfog	lia
Ulteriori informazioni sugli <u>archivi di certificati</u>		
Ulteriori informazioni sugli <u>archivi di certificati</u>		
Ulteriori informazioni sugli <u>archivi di certificati</u>		
Ulteriori informazioni sugli <u>archivi di certificati</u>		
Ulteriori informazioni sugli <u>archivi di certificati</u>		
	Ulteriori informazioni sugli <u>archivi di certificati</u>	
Avanti Annulla	Avanti	Annulla

• Premere "Fine" per completare l'installazione.

completai	nento dell'Impo	rtazione guidata certificati
Scegliendo Fine,	il certificato verrà importa	ato.
Impostazioni sele	zionate:	
Archivio certific	ati selezionato dall'utente	Autorità di certificazione radice attendibili Certificato
Contended		

Windows - Firefox

- Rammentare che Firefox non è ufficialmente supportato. Nulla vieta tuttavia di provare ad utilizzarlo per navigare un iKon configurato con Chrome.
- Scaricare il certificato di CA (Certification Authority) di Domotica Labs dal seguente indirizzo: certificato CA.
- Accedere alle "Opzioni" di Firefox dal menù principale del browser
- Premere sull'etichetta "Certificati" e poi su "Mostra Certificati"

			Opzior	ni			X
Commit	E-h-d-	页				0	şõ;
Generale	Schede	Contenuti	Applicazioni	Privacy	Sicurezza	Sync	Avanzate
Generale Co	ondivision	e dati Rete A	ggiornament	Certificati)		
Quando u	ın sito web	richiede il ce	tificato persona	le:			
○ <u>S</u> elezi	onane uno	automaticam	nente 💿 <u>C</u> hie	di ogni vol	ta		
Mostra	ertificati	Verifica	Dispositivi	di sicurezza	a		
Mostra	crunedd	<u>v</u> enneu	Dispositivi	an sicurezzi			
			-				
				ОК	Annul	la	2

• Premere su "Autorità" e poi su "Importa"

2024/09/21 (02:46			11/17				HTTPS e	e Certificati SSI
	Generale	e Schede	正 页 Contenuti	Applicazioni	Privacy	Sicurezza	Sync (C)	्रिं Avanzate	
8				Gestione ce	rtificati				1 ×
Certific	ati personali o presenti cert	Persone Ser ificati su file	ver Autorità che identifica	Altro	utorità di ce	ertificazione:			
Nor	me certificato			Disposi	tivo di sicu	rezza			E\$
⊿ (c)) 2005 TÜRKTI	RUST Bilgi İle	tişim ve Bilişiı	m Güv					^
	TÜRKTRUST E	Elektronik Ser	tifika Hizmet	Sağla Builtin (Object Toke	en			
▲A-	Trust Ges. f. S	icherheitssys	teme im elek	tr. Dat					
	A-Trust-nQua	al-03		Builtin (Object Toke	en			
I A(C Camerfirma	S.A.							
	Chambers of	Commerce R	oot - 2008	Builtin (Object Toke	en			
	Global Cham	bersign Root	- 2008	Builtin (Object Toke	en			
I A(C Camerfirma	SA CIF A8274	43287						~
Vis	ualizza	<u>M</u> odifica atte	ndibilità	Impo <u>r</u> ta	Esp <u>o</u> rta	<u>E</u> limin	a o consid	era inattendibil	e
								C	Ж
				F					
					OK	A	-	2	

- Selezionare il certificato di CA di Domotica Labs appena scaricato.
- Al termine dell'operazione, nella lista dei certificati delle "Autorità" apparirà la voce Domotica Labs

Windows XP o Windows 2000 o Windows 7 Embedded - Chrome e IE

Usare Microsoft Management Console (MMC) (Vedi tutorial.)

Apple MAC

- Scaricare il certificato di CA (Certification Authority) di Domotica Labs dal seguente indirizzo: certificato CA.
- Fare doppio click sul certificato appena scaricato
- Aggiungere il certificato al portachiavi di "Sistema" (nulla vieta di installare il certificato solo al portachiavi di "login"; tuttavia deve esser chiaro che, accedendo con un utente differente, Windows non considererà più Domotica Labs come una sorgente affidabile di certificati)

Certificate Standard	Desideri aggiungere il/i certificato/i dal documento "rootCA.Dlabs.crt" su un portachiavi?
	l nuovi certificati principali dovrebbero essere aggiunti al portachiavi di login per l'utente attuale o al portachiavi di sistem se devono essere condivisi da tutti gli utenti di questo computer
	Portachiavi: Sistema
<u></u>	

Apple iPhone/iPad

Metodo 1

- Aprire Safari sul dispositivo su cui si vuole installare il certificato
- Inserire l'indirizzo relativo al certificato CA
- Sul dispositivo si aprirà una finestra di conferma come la seguente
- Cliccare sul pulsante in alto a destra "Installa" e si aprirà una ulteriore schermata di conferma
- Cliccare di nuovo sul pulsante "Installa"
- A questo punto il certificato è installato e dovreste vedere una schermata con una spunta verde, come la seguente
- Cliccare sul pulsante "Fine" per terminare la procedura

NB: una volta installato il certificato è buona norma chiudere tutti browser (anche dal background), fare una pulizia delle cache e riavviarli.

Metodo 2

- Scaricare, se necessario, il software iPhone configuration utility
- Scaricare il certificato di CA (Certification Authority) di Domotica Labs dal seguente indirizzo: certificato CA.
- Avviare iPhone configuration utility
- Sotto la voce "Libreria", selezionare "Profili di configurazione"

File Modifica Vista Finestra Aiuto	Utilit
LIBRERIA	Nome
Dispositivi	
🗛 Applicazioni	
Profili di fornitura	
Profili di configurazione	
DISPOSITIVI	

- Scegli se creare o importare un profilo di configurazione:
 - Importa profilo esistente (soluzione base):
 - Scaricare il seguente profilo pregenerato e scompattarlo.
 - Premere "File", poi "Aggiungi alla libreria" e selezionare il profilo appena scaricato e scompattato.
 - $\circ~$ Nuovo profilo di configurazione (soluzione avanzata):
 - premere "Nuovo" in alto a sinistra
 - Sotto "Generale" riempire i dati obbligatori
 - Sotto "Credenziali" aggiungere il certificato CA di Domotica Labs
- Connettere fisicamente iPhone al PC/MAC
- Selezione il tuo iPhone/iPad nella sezione "Dispositivi" e poi seleziona la linguetta "Profili di configurazione"; infine premi il pulsante "Installa" accanto al profilo di configurazione appena creato/importato.

File Modifica Vista Finestra Aiuto	Utility Configurazione iPhone	
Aggiungi Condividi Esporta		Nascondi Q
LIBRERIA	Riepilogo Profili di configurazione Profili di fornitura Applicazion Gestisci promi or comgurazione	ni Console
💼 Profili di fornitura	Nome Identificatore	Installa
Profili di configurazione	Domotica Labs - Certification Authority com.domoticalabs.CAroot	Installa
hone		

• Sul dispositivo iPhone/iPad apparirà una finestra di conferma; premi il bottone "installa" e segui la procedura premendo i pulsanti "installa".

Last update: 2015/03/11 11:03 ikon:faqs:network:ssl:ssl http://www.domoticalabs.com/dokuwiki/doku.php?id=ikon:faqs:network:ssl:ssl&rev=1426071807



• Al termine dalla procedura verrà mostrato il certificato installato



Android Mobile

Per poter installare un certificato su un qualsiasi disposivito Android è necessario aver configurato almeno un a protezione al dispositivo (ad esempio: il PIN). Nel caso non si sia configurata alcuna protezione il dispositivo Android richiederà prima di configurarla.

- Accedere con il browser all'indirizzo: certificato CA.
- Accettare di voler installare il certificato e seguire la procedura descritta dal dispositivo.

UNIX Debian

- Scaricare il certificato di CA (Certification Authority) di Domotica Labs dal seguente indirizzo: certificato CA.
- Eseguire i seguenti comandi:

apt-get install libnss3-tools

```
certutil -d sql:/mnt/storage/RWdlabs/guest/.pki/nssdb -A -t TC -n
"rootCA.Dlabs" -i rootCA.Dlabs.crt
```

```
sudo mkdir /usr/share/ca-certificates/extra
```

```
sudo cp foo.crt /usr/share/ca-certificates/extra/foo.crt
```

```
sudo dpkg-reconfigure ca-certificates
```

Configurare dominio di accesso remoto

Se si desidera accedere ai prodotti Domotica Labs in HTTPS da remoto, è necessario anche configurare il "**Dominio di accesso remoto**" nella pagina di configurazione di "**Rete**".

Il dominio è quella parte compresa tra il protocollo e la porta di accesso.

Ad esempio: se l'accesso da remoto è "*https:***example.dyndns.org**:4123" il dominio di accesso remoto è: "**example.dyndns.org**"

Rigenerare Certificati SSL

Ogni prodotto Domotica Labs, provvede a rigenerare automaticamente, in piena autonomia, i certificati per l'accesso HTTPS.

I certificati vengono rigenerati **solo** se il prodotto ha **accesso ad internet**. In caso contrario l'operazione termina senza errori ma non produce alcun risultato lasciando i certificati originali intatti.

La rigenerazione dei certificati avviene quando:

- Viene aggiornato il software
- Viene configurato un **nuovo IP**
- Viene configurato un **nuovo dominio di accesso** remoto
- Viene utilizzato il pulsante "Rigenera certificati" sotto il menù di "sistema" → "manutenzione"

Nel caso si rigenerino i certificati a mano attraverso il menù di **manutenzione**, è necessario premere il pulsante "**Riavvi servizi Web**" dopo l'operazione di rigenerazione.

Non si vedono alcuni contenuti

Quando si accede in HTTPS è possibile che non si riescano a vedere contenuti di rete non sicuri a cui iKon accede in HTTP (Ad esempio: le telecamere locali). Su chrome è necessario sbloccare il lucchetto in alto a destra nella barra degli indirizzi:



Avast 2015

Avast 2015, attraverso il servizio "Mail Shield", tende ad intromettersi nel sistema di certificazione SSL e decide, in piena autonomia, che i certificati Domotica Labs non sono attendibili. Questo significa che, anche se si è configurato correttamente tutto, il "lucchetto" della pagina web in HTTPS rimane comunque "rosso".

Per controllare se Avast si sta intromettendo nel sistema basta premere sul pulsante del "Lucchetto"

e confrontarlo con il seguente screenshot:

Certificat	e ×
General Details Certification Path	
Certifice#traged1	
	<u>V</u> iew Certificate
Certificate <u>s</u> tatus:	
This certificate is OK.	
	ОК

Le soluzioni sono le seguenti:

- Disattivare il "Mail Shield" di Avast 2015
- Disattivare la configurazione "esamina traffico di rete crittografato SSL" andando in: Protezione esplorazione WEB → ONLINE SHIELD → IMPOSTAZIONE AVANZATA.

From: http://www.domoticalabs.com/dokuwiki/ - DOMOTICA LABS WIKI	
Permanent link: http://www.domoticalabs.com/dokuwiki/doku.php?id=ikon:faqs:network:ssl:ssl&rev=1426071807	K
Last update: 2015/03/11 11:03	