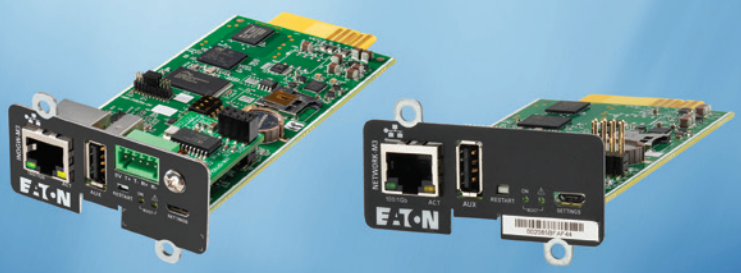
Application note



PKI automation with Certbot for Eaton connectivity devices

The Eaton Gigabit Network Cards and Industrial Gateway Cards are both cybersecure by design. They come with UL2900-1 and IEC 62443-4-2 cybersecurity certifications and are continuously reviewed by Eaton's Cybersecurity Center of Excellence to ensure they meet industry standards as well as our own state-of-the-art cybersecurity requirements.

One way Eaton has taken the lead in cybersecurity is its policy of using only encrypted, secure protocols by default. One of those protocols is HTTPS, over which you can securely access the web user interface or RESTful API. The one thing that we cannot provide out of the box is a signed certificate from a trusted certificate authority. We can only initially provide a self-signed certificate, which should be replaced by a certificate signed by a trusted certificate authority at the time of commissioning. Using the default self-signed certificate will result in receiving the following error as shown using a Chrome web browser. See Figure 1.

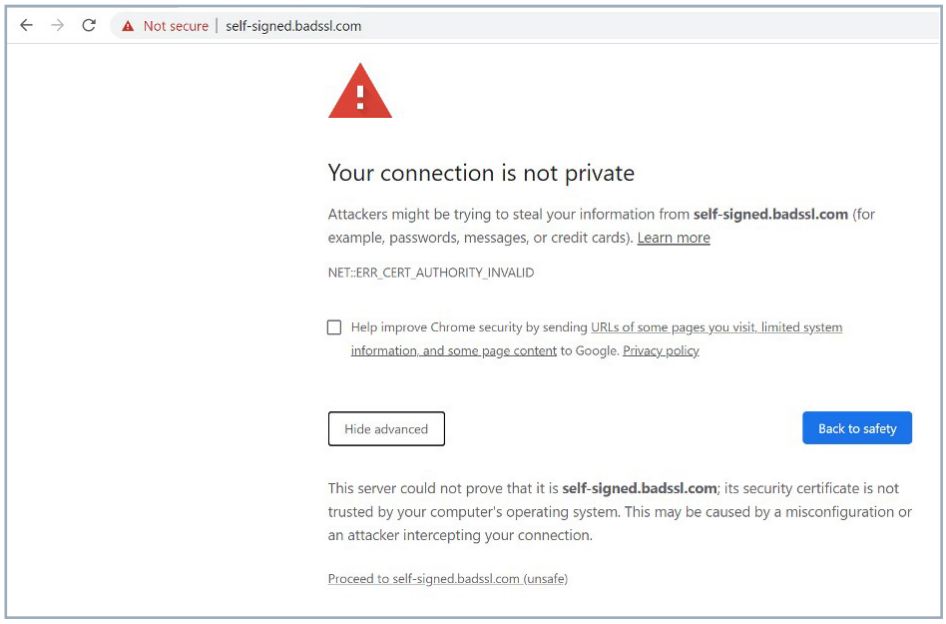


Figure 1: Insecure connection error

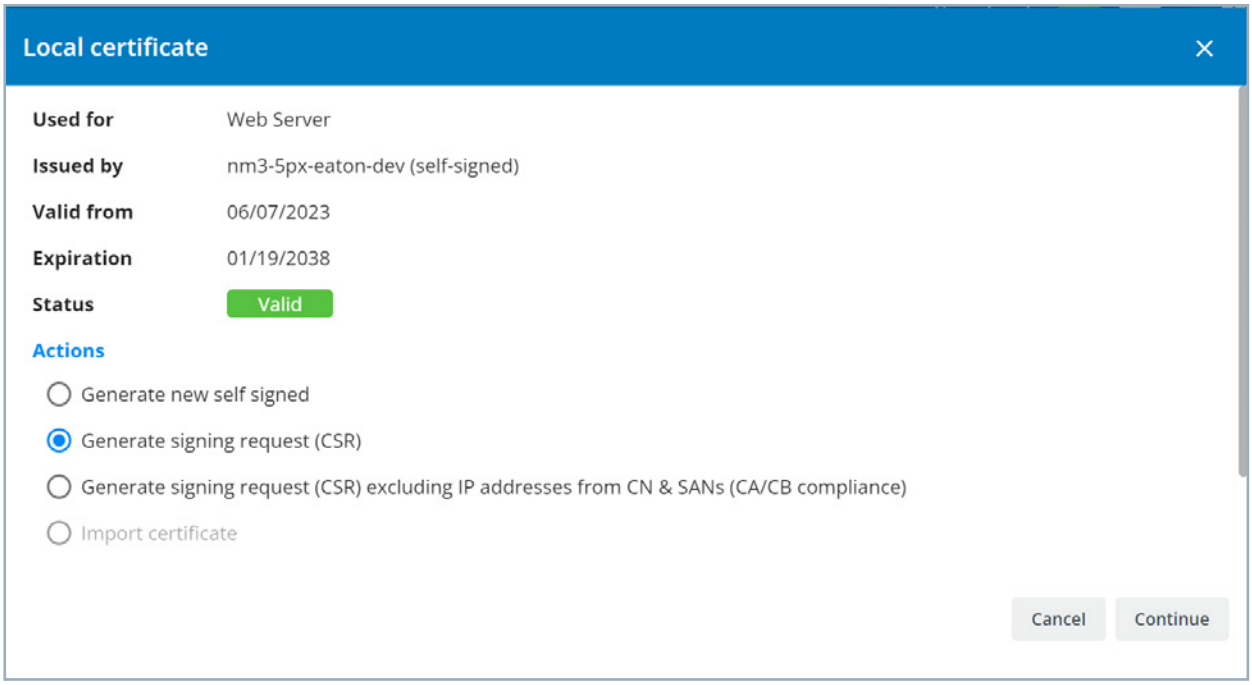
Users can click the "Advanced" button and then "Proceed to URL (unsafe)", but there are several reasons why this is not desirable beyond initial commissioning of the device. If the network card is exposed to the public internet with a self-signed certificate, the user could be vulnerable to potential cybersecurity attacks. Even on private or firewalled networks, it adds an extra step to log in, can promote bad browsing habits and requires RESTful API clients to operate in a less secure mode.

Many organizations have defined Public Key Infrastructure (PKI) that can provide certificates to securely access their devices using HTTPS. For those who don't have access to a PKI or don't want to pay a third party for a certificate, there is an alternative. Let's Encrypt is a free, automated and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG). Certbot is an open source application maintained by the Electronic Frontier Foundation that can automate the process of acquiring a signed certificate from Let's Encrypt. The following is a basic introduction to obtaining a free digital certificate. In order to use Certbot, you need a fully qualified domain name (FQDN) and the ability to add DNS records to your domain name server (DNS) in order to prove ownership of your domain.

Powering Business Worldwide

Configure your Issuer Information

Obtain a Certificate Signing Request



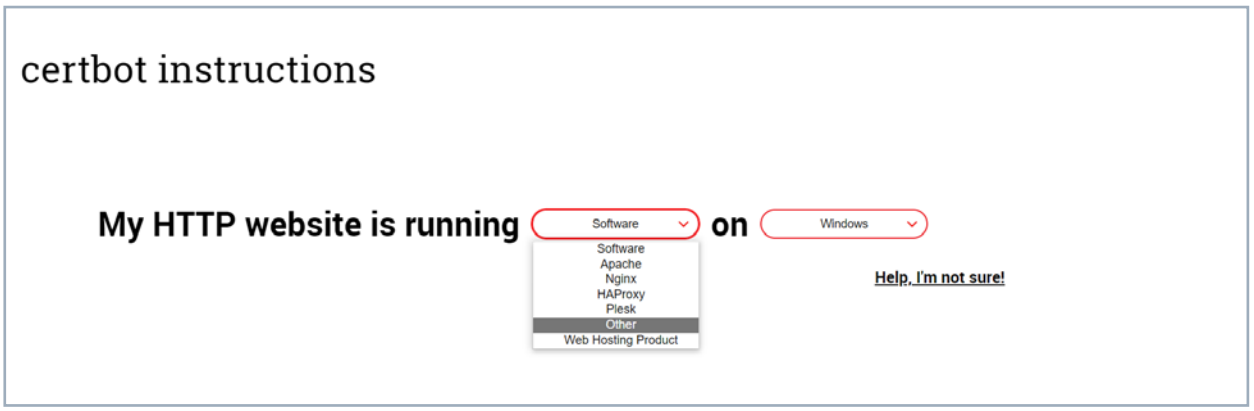
Use Certbot to obtain a signed certificate from Let's Encrypt

In order to use an ACME client to obtain a free certificate, you will need to demonstrate ownership of your FQDN through a DNS challenge. This means you must be able to add TXT records to your DNS server. Currently, this is the only supported way to obtain certificates for your Eaton Gigabit Network Card through Certbot. This method will not work unless you have access to your DNS server and have applied an FQDN to your network card.

Use the following link to obtain detailed instructions for this operation.

Certbot.eff.org/instructions

Select software as "Other" and the operating system you will use to install Certbot.
Below you can see Windows selected, but this may be different for each user.

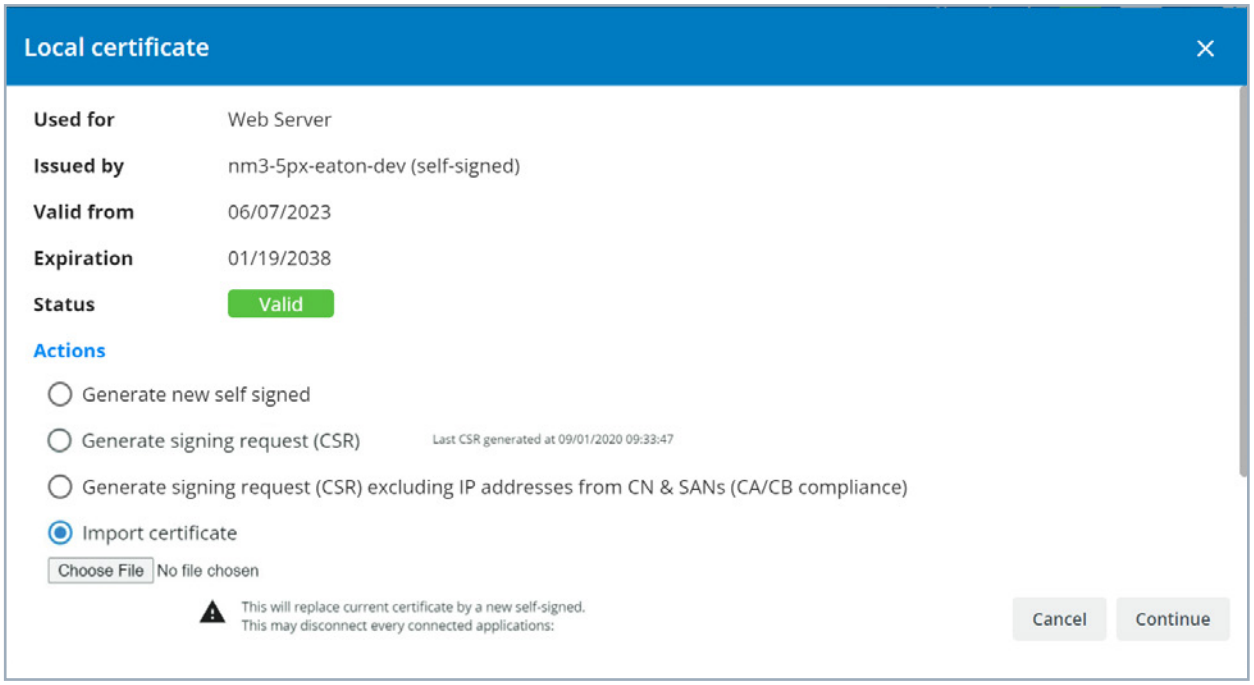


Once you have Certbot installed, you can run the following command.

$ certbot --manual --preferred-challenges dns certonly

Follow the interactive directions to receive your certificate.
Be aware that you will need to consider how to renew your certificate.
Eaton technical support does not support Certbot.

Upload new digital certificate



For more information visit: **Eaton.com/Network-M3**

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Pub. No. AP152012EN / GG / 23-04-195
July 2023

Follow us on social media to get the latest product and support information.

Powering Business Worldwide