Installing a Browser Security Certificate for PowerChute Business Edition Agent

The PowerChute Business Edition Agent has a "self-signed" security certificate. This means that when you access your Agent installation, your browser will display warnings about the validity and security of the Agent site.

It is possible to proceed by ignoring the warnings, however we recommend installing the certificate as shown in the sections below.

Installing an Agent security certificate for Firefox

1. After installing the PowerChute Agent, launch it. Firefox displays the following warning:

![Image of Firefox warning](image)

2. Click on Advanced to see this:

```
localhost:6547 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
The certificate is only valid for the following names:
  WTIEMVSE029562L.eur.gad.schneider-electric.com, WTIEMVSE029562L, 192.168.122.1, 192.168.122.1,
  10.216.224.41, 10.216.224.41, 192.168.192.1, 192.168.192.1, 127.0.0.1, localhost

Error code: SEC_ERROR_UNKNOWN_ISSUER
```

3. Click Add Exception to see this:
4. Click **Confirm Security Exception** to add your PowerChute Agent to the browser's list of trusted sites.

**Installing an Agent security certificate for Internet Explorer (IE)**

1. After installing the PowerChute Agent, launch it. The following is displayed:

There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).
- More information
2. Choose **Continue to this website (not recommended)**. You should see:

![Certificate Error Dialog](image)

3. You must first add the IP address or domain name as a trusted site in Internet Explorer before you can add the certificate.

4. To the right of the address bar, click on **Certificate Error**. This dialog displays:

   ![Untrusted Certificate Dialog](image)

   **Untrusted Certificate**

   The security certificate presented by this website was not issued by a trusted certificate authority.

   This problem might indicate an attempt to fool you or intercept any data you send to the server.

   We recommend that you close this webpage.

   **About certificate errors**

   ![View certificates button](image)
5. Click **View certificates** to view this:

6. Click **Install Certificate**. The Wizard dialog displays:

7. Choose **Place all certificates in the following store** and select Browse.
8. Select **Trusted Root Certification Authorities** and click OK. (It is possible that you might have to check “show physical stores”, and then “Local Computer” under Trusted Root
9. Click **Finish** at Completing the Certificate Import Wizard.
10. Click **Yes** at the Security Warning dialog, shown below.

Security Warning

⚠️ You are about to install a certificate from a certification authority (CA) claiming to represent:

```
192.168.192.130
```

Windows cannot validate that the certificate is actually from "192.168.192.130". You should confirm its origin by contacting "192.168.192.130". The following number will assist you in this process:

Thumbprint (sha1): A4609A65 D724002E 2B50C3F3 4590DFD28 C6E2EC8

**Warning:**
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

---

11. You should see this confirmation box below, click **OK** to finish.

Certificate Import Wizard

![Certificate Import Wizard]

**The import was successful.**

---

12. The Certificate dialog might still be open (see step 4 above). Click **OK** to close it.
13. Restart Internet Explorer to complete the installation of the security certificate.
Installing an Agent security certificate for Chrome

After installing the PowerChute Agent, launch it. Chrome displays the following warning:

![Warning Message]

Your connection is not private

Attackers might be trying to steal your information from localhost (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

ADVANCED

Back to safety

Currently, Chrome does not have a way of installing a certificate from a URL. But as Chrome relies on the Windows certificate store, the method described directly above in Installing an Agent security certificate for Internet Explorer (IE) works for Chrome also.

Launch the IE browser and follow those steps. Then restart Chrome and it will recognize the security certificate as being installed. The warning for PowerChute Agent will not display again.

Installing an Agent security certificate for Microsoft Edge

1. After installing the PowerChute Agent, launch it, and Edge displays the following warning:

![Warning Message]

There’s a problem with this website’s security certificate

This might mean that someone’s trying to fool you or steal any info you send to the server. You should close this site immediately.

☐ Go to my homepage instead

✉ Continue to this webpage (not recommended)
2. Choose **Continue to this webpage (not recommended)**. You should see:

3. Follow the steps outlined in **Installing an Agent security certificate for Internet Explorer (IE)**.

4. Restart Edge to confirm that the security certificate is installed. The warning will no longer be displayed.