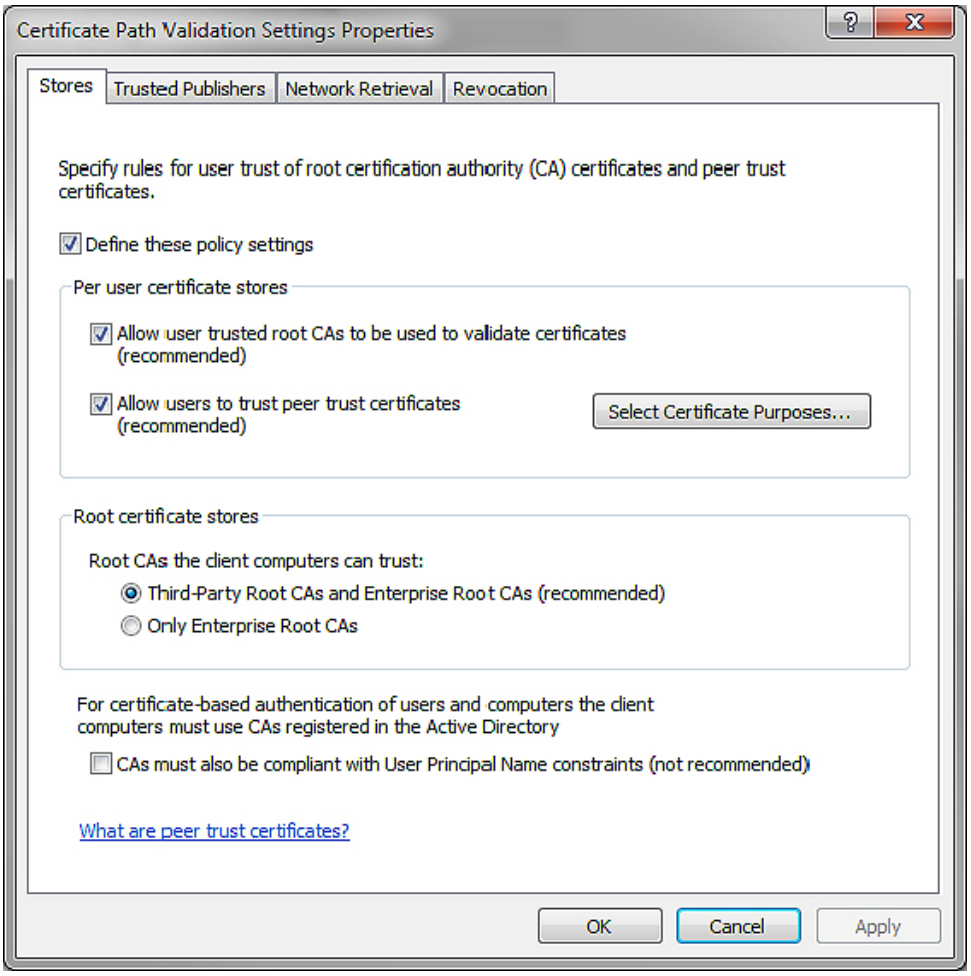
Cybersecurity consideration for the PXDBP

For added security, you should always disable HTTP access and enable HTTPS access for the Dashboard. To use HTTPS to connect to the PXDBP, you will need to download the certificate file from the PXDBP. (instructions for this are below).

Enabling user management of root certificates

The process for either enabling this on a local machine or setting a group policy is outlined in the following Microsoft Technet Article: https://technet.microsoft.com/en-us/library/Cc754841.aspx.

Essentially, you're going to enable the users to allow trusted root CAs to be used to validate certificates and to trust peer trust certificates. You will do this through MMC. If you are changing the local policy, you will have policy settings for certificate stores set as is shown in the following figure.



Powering Business Worldwide

1. Set either the local machine policy to allow users to manage certificates or, if multiple people in your organization will access the PXDBP, set a group policy. You may need assistance from your IT organization to set a group policy.
2. Both enabling user management for certificates and installing a certificate require administrative privileges for the PC. If you don't have such privileges, you may need to contact your IT organization for assistance before proceeding.

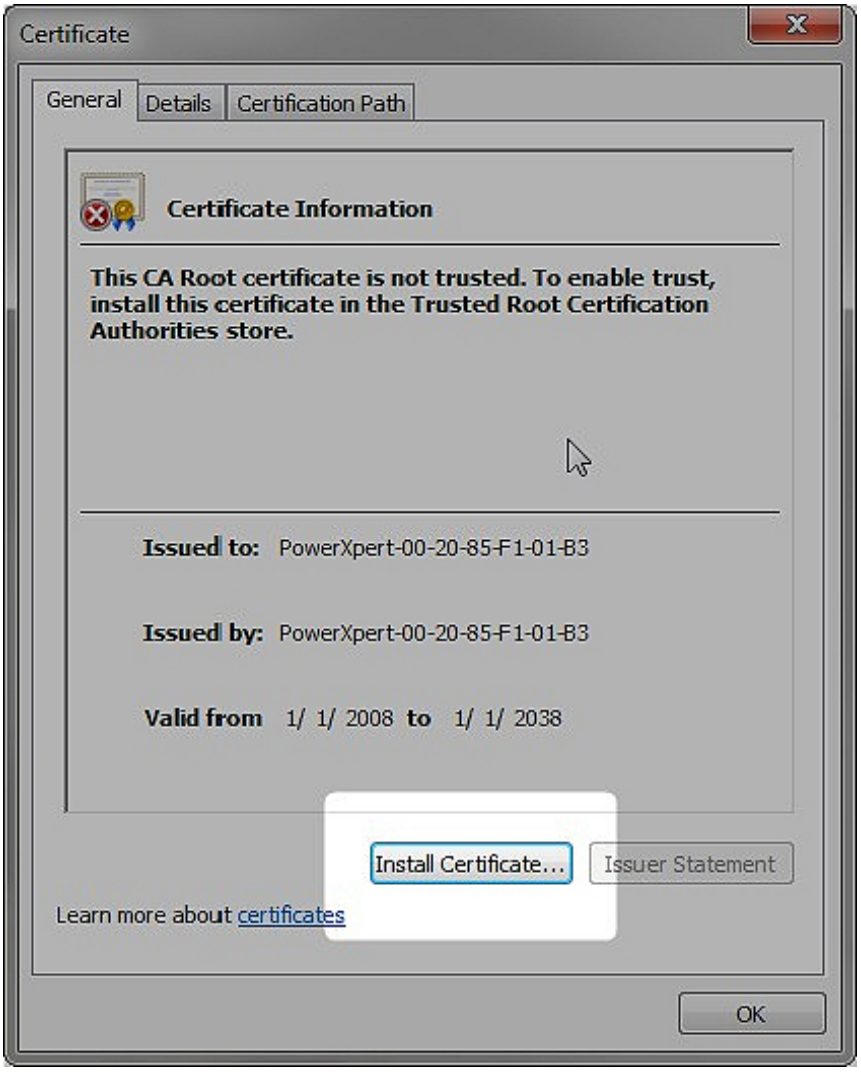
Downloading the certificate file from the PXDBP

1. Point Google Chrome to the IP address of the PXDBP followed by /ca.html. For example: http://192.168.1.1/ca.html.
2. Click the Root CA Certificate link. The browser will download the certificate.

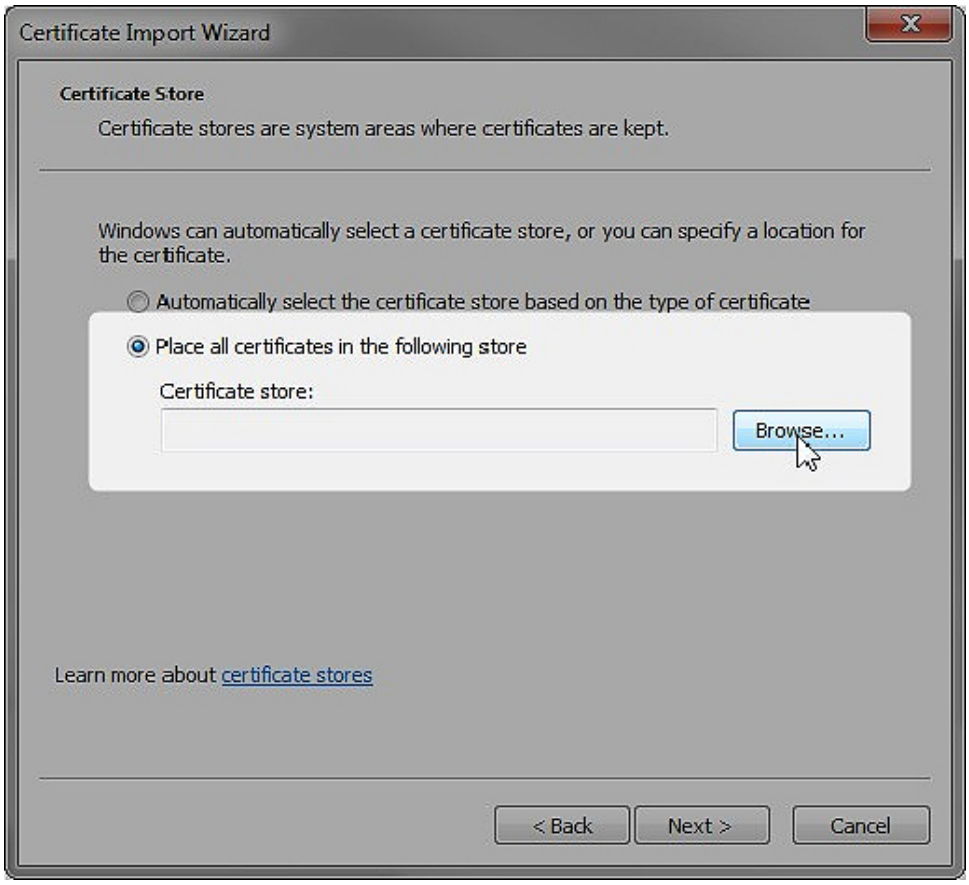
Note that the certificate uses SHA-256 as its cryptographic hash function to avoid incompatibility problems with various browsers.

Installing the certificate

1. Double-click the certificate file. This will launch the certificate installation wizard.
2. Click Install certificate.

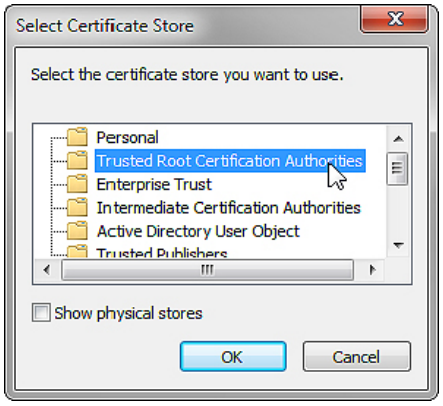


3. On the Welcome dialog box, click Next.
4. Select Place all certificates in the following store and then click Browse.

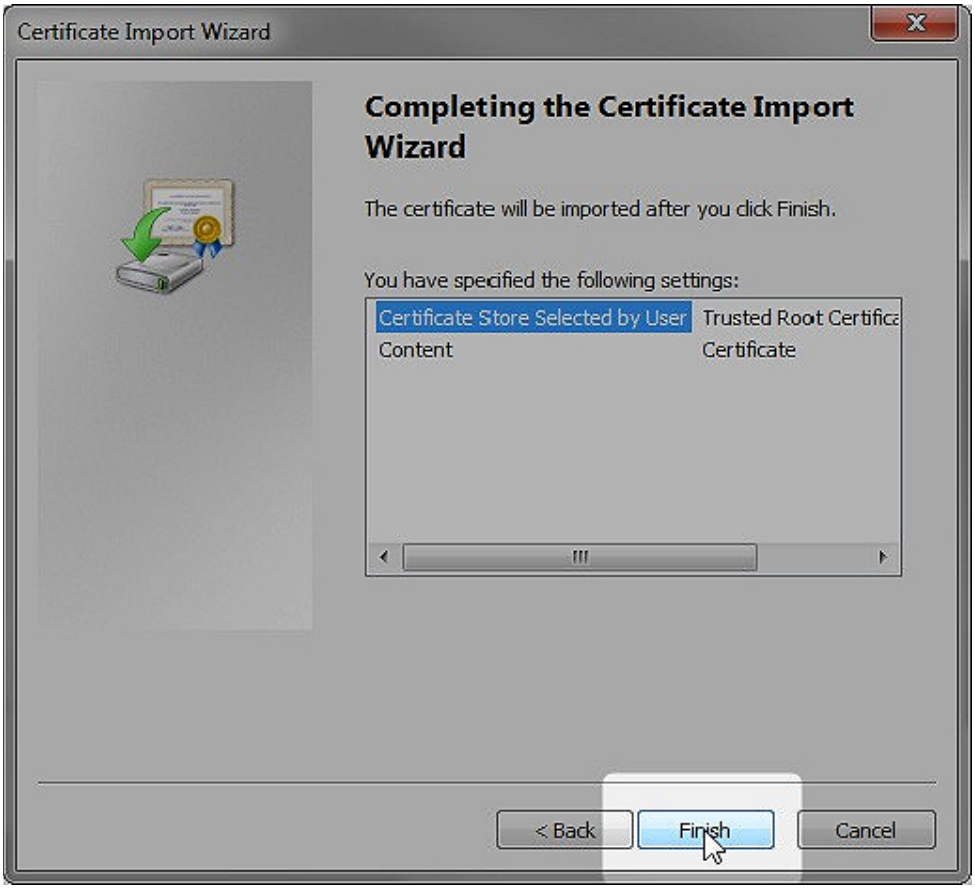


5. Select Trusted Root Certification Authorities from the list, then click OK.

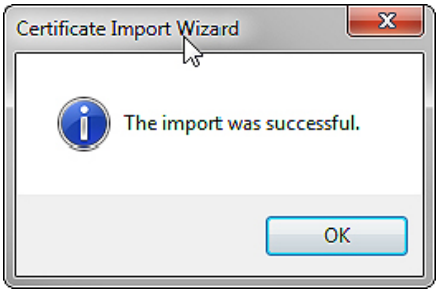
Trusted Root Certification Authorities store is not the default store that the certificate installation wizard will choose, which is why you may need permission to manage certificates.



6. On the Completing the Certificate Import Wizard dialog box, click Finish.



7. You should see an alert box stating that the import was successful. Click OK.



8. Close and restart the browser.

You can now access the PXDBP using the HTTPS protocol (for example, https://192.168.1.1/).

Ports in use

For web-based communications with the PXDBP, TCP Ports 80 (HTTP) and 443 (HTTPS) are enabled by default. For special situations, you may elect to disable one or the other. However, disabling both prevents any web access to the PXDBP and is not recommended. You may also choose to change the assigned port number for either.

The following ports and protocols are disabled by default. You must elect to enable them and may choose to change the assigned port number.

Port number	Protocol/use	TCP/UDP
502	Modbus TCP	TCP
5150	EMINT Mode - INCOM 1	UDP
5151	EMINT Mode - INCOM 2	UDP
5152	EMINT Mode - INCOM 3	UDP
26501	Modbus (COM1 Pass-thru)	TCP
26502	Modbus (COM2 Pass-thru)	TCP
26503	Modbus (Ethernet Pass-thru)	TCP
47808	BACnet/IP	UDP

The following ports are open and necessary for proper PXDBP operation:

Port number	Protocol/use	TCP/UDP
7011	Eaton's Mercury Websockets	TCP
7012	Eaton's Mercury Websockets – Secure via TLS	TCP

These ports cannot be disabled or their port numbers changed.

Browser specific notes

- If you use HTTPS with Internet Explorer 10 you must enable TLS version 1.2 support in the browser. The PXDBP does not support SSL version 3.
- Restart your browser after loading the certificate to avoid any problems caused by the browser caching data.

Settings

Network tab - controlling access to various protocol servers

BACnet/IP

Under BACnet/IP, you should only enable those services that you will be using. Leave everything else disabled. For those services that you do enable, make sure that you also enable Trusted Hosts for each and then maintain the minimum number of trusted hostnames/IP addresses that you need. Note that you must have Trusted Hosts enabled in order to save any trusted host machine names/IP addresses you've added.

Modbus TCP server configuration

Unless you have a specific need to enable Write Commands, make sure that this is Disabled.

SNMP

Unless you require SNMP features, it is recommended that you leave the overall support turned off by unchecking SNMP support in the Access Control section of the Network Access tab.

Users tab, e-mail server

You should, if possible, require TLS when communicating with an e-mail server. Also, limit the recipient list to those who truly need this information.

Passwords

One of the first things that you should do is to change the passwords for both the Admin and User accounts. You can change these on the Users tab under the settings section. When in edit mode, the Users tab in settings lets you change passwords, add and delete users, and assign roles.

When changing passwords, follow good security practices including, but not limited to:

- Passwords should be in excess of seven characters.
- Passwords should contain at least one capital letter, number, and special character.

Global Password Policy settings are configurable in the Dashboard, allowing security administrators to define the complexity, length, reuse and expiration rules for passwords of all users of the Dashboard.

Individually, User Password Management features allows security administrators to further define password rules on a per-user basis. Additionally, accounts can be locked and unlocked as necessary.

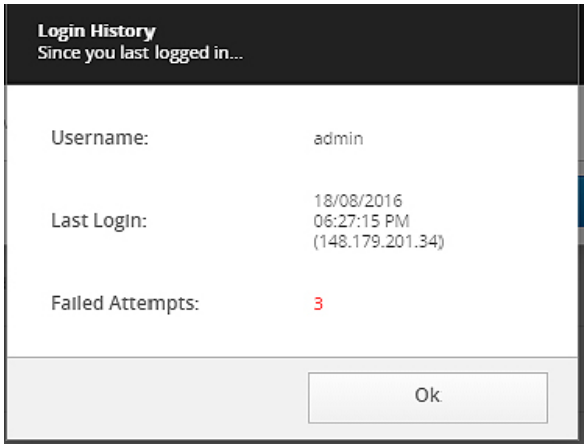
The Global Password Policy and User Password Management features are further documented in the User Guide(Help Reveal panel –> Quick Start Guide)

You can verify who has accessed the Dashboard through the logs present on the Logs tab under Settings. Using the show and sort option, you can view the logs on screen. You can also download all logs file by clicking on Export button present in action bar. The Session log may be of particular interest as it lists login attempts and failures. For more information about the various logs, Please visit the Settings Logs tab.

Eaton recommends that all products should be installed on a secure network. For more information on how to secure this product in your environment please refer to the whitepaper "Cybersecurity considerations for electrical distribution systems" at http://www.eaton.com/Eaton/ProductsServices/Electrical/ThoughtLeadership/WhitePapers/index.htm.

Last login notification and history

The DashBoard will warn you of previously failed login attempts. Any time there has been at least one failed login attempt, you will be greeted with a warning message on your next successful login.



Failed login attempt warning

Browser session time-out

You can use the Session Timeout (on the Safety tab Under Settings) to impose a time-out to automatically log out a browser session. This time-out applies to all user accounts. The Session Timeout value is the number of minutes during which no browser activity is detected. Once the specified number of minutes of account inactivity is reached, the current browser session will be logged out. A value of zero disables the time-out function.

Browser time-out setting

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

The information, recommendations, descriptions and safety notations in this document are based on Eaton Corporation's ("Eaton") experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined in appropriate Eaton selling policies or other contractual agreement between Eaton and the purchaser.

THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES.

In no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability or other-wise for any special, indirect, incidental or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations and descriptions contained herein. The information contained in this manual is subject to change without notice.

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

Printed in USA
Publication No. MN152012EN / TBG 1365
June 2017

Powering Business Worldwide