Exposing ECOP for Access from the Public Network

Introduction

This document describes the technical considerations and some technical operations required to expose ECOP to public access. This exposure will allow the ECOP UI to be used from the Internet using things like public computers, wireless tablets, laptops, and smart phones. While this can be inherently insecure, if done properly the data stored by ECOP will be safe while still being globally accessible.

As stated in our other documentation, ECOP data is not, by design, accessible outside of the network on which it is installed. This decision was made very early in the design process to ensure the safety of this sensitive information. By following the steps outlined in this document, the consumer is making an 'opt-in' decision to potentially expose their data to the world at large.

What Gets Exposed

The user-facing portion of ECOP is essentially just a web site running on a standalone web server. When allowing access to ECOP from the Internet, it is access to this web server that is being granted. To do this there are several steps. Some are required simply to make it work, some are required to make it as secure as possible.

In order to make it work, the local firewall must allow access from the public side of the network into the private side. This process is known by different names such as 'port forwarding', 'port mapping', or 'port nat'. This action is performed on the local network's firewall, which in a residential setting is most likely a wireless access point, a DSL modem, or possibly a cable router. The specific equipment to target will vary depending on the local network and the policies of the Internet service provider for that network. It is obvious that administrative access to this device is required to make these changes, so that's the first thing that needs to be figured out.

Open It Up

There are a couple of considerations that need to be made when setting up public access. The first is that the ECOP should have a static private address. To do this requires administering the ECOP

machine from a terminal session and should have been done during the standard installation procedure. To set up the port mapping you must know this address; you may also be able to use a host name depending on your DHCP setup and your firewall's capabilities. It is impossible for this document to cover the possibilities related to private DNS services.

The second is if any other services on the network are also being mapped into the private network. If so, and they include another web server listening on port 443 (the standard HTTPS port), then an alternative public port will need to be chosen for use with ECOP. Even in that case, the private ports utilized by ECOP can most likely stay the same, depending on the capabilities of the firewall in question.

Once the private static IP address and the public port have been determined, utilize the firewall administration UI to set up a mapping from the public port to the private address of ECOP on port 443. After this step is performed correctly, ECOP UI should be accessible from outside the private network by using a URL in the format of https://<public IP address>/ecop.ui/Main.htm. In the event that an optional port was needed for the public side, then the URL will have the format of https://<public IP address>:<public port>/ecop.ui/Main.htm.

Once a test of this URL succeeds, we can possibly make it easier to share and remember the public URL for the private ECOP by using a public domain name rather than a public IP address. If the private network in question has a static IP address, this is not such a big deal. However, most residential Internet connections utilize dynamic IP addressing, which means that the public IP address can and will change over time. This can make it impossible to locate the ECOP from the public side without checking information from the private side (IE: if it changes while the user is not home, then access will be impossible until the new public address is learned).

One way to alleviate this issue with dynamic addressing is to utilize dynamic domain name service (DDNS), of which there are several free options such as no-ip.com, dyndns.com, and others, as well as paid DDNS services. Many vendors of gateway devices have added a DDNS option to their equipment to make exposing private services to the public Internet easier and keep network administration in one location. We leave further investigation of DDNS to the user, and encourage you to ask questions at AP&C Support Email should the need arise.

Exposing ECOP for Access from the Public Network

Locked Down

Once communications to the ECOP are established from the Internet, the configuration is essentially done since the standard ECOP configuration is to only allow secure HTTP. Consumers should know that, ECOP user authentication is performed using Basic Authentication, which by itself does not protect user names and passwords. The best way to do that is to use secure HTTP (HTTPS) to encrypt communications between the public client and the private ECOP server. This also protects any other information shared by the web site and it is for these reasons that we chose to disallow access to ECOP using standard HTTP.

Consumers should also know that the running ECOP web server has its own self-signed certificate which allows it to act as an HTTPS server. This certificate is generated for the ECOP machine on which it is installed, and will expire 10 years after it is created, then it will need to be renewed.

Because it is generated by the ECOP machine itself it cannot be sourced to a trusted certificate authority, such as Versign. This means that you will get warnings from browsers about the 'scariness' of the certificate and the server providing it. You may install the certificate as a trusted host in your browser to avoid these warnings.

One other hint when locking down ECOP for the Internet is to change any default passwords, and possibly user names, before opening it up. This will keep our well-known default configurations from being an open doorway to private systems.

Wrap It Up

By following these procedures, it is possible for consumers to protect their sensitive power usage patterns and other data while still being able to access it from anywhere in the world. If there are any problems or questions with these procedures please do not hesitate to contact us at AP&C Support Email.

