XpressConnect Enrollment System

Pre-Deployment Checklist

Software Release 4.2

December 2015

Summary: This document describes the items to consider when integrating the Enrollment System with the other systems in your local network.
Document Type: Planning
Audience: Network Administrator

XpressConnect Enrollment System Pre-Deployment Checklist

Software Release 4.2

December 2015

Pre-Deployment Checklist

This document describes how to prepare for your Enrollment System implementation call with Cloudpath support.

Please provide the Cloudpath implementation team with the following information about your network. In addition, review the Information the Customer Should Consider section to help you get the most out of your implementation call.

Information Required From Customer

For local deployments, Cloudpath requires the following information from the customer:

- Which brand of AP/Controller are you using?
- Do you plan to use the onboard PKI or an external certificate store?
- Do you plan to use the onboard RADIUS server or an external RADIUS server (NPS)?
- Are you using NAC in your network?
- Do you plan to use replication in your network?
- If yes, which configuration do you expect to use?

  -Master-Master

  -Hub and spoke

- Do you have a load balancer? If yes, which vendor?

Information the Customer Should Consider

Before we implement the Enrollment System in your network, you should consider the following network configurations:

- Your secure network must be set up for WPA2-Enterprise.
- Set up both the open and secure SSID on the Controller before the implementation call. Note: If your network is set up for PEAP, we can change it to TLS when we implement the Enrollment System.
- You should have knowledge about how to configure a captive portal on your wireless controller(s).

  -The open SSID typically has pre-authentication ACLs defined, which permit access to the VM. The LAN controller is configured to point to the Enrollment System VM as an external captive portal.

- The WPA2-Enterprise SSID should be setup to delegate authentication to the onboard AAA server or your existing AAA.

-If using an existing AAA server, it requires layer 3 access to the Enrollment System VM to verify certificate status (optional).

- If using Active Directory, you need the AD domain information (plus any subdomains) and the IP address of the AD server. AD groups should be set up before the implementation call.

  -The ES/VM should have layer 3 access to Active Directory.

- A web server certificate is required for HTTPS. The system can be configured prior to the WWW server certificate being installed, but it should be installed before attempting to enroll end-users.

  -The WWW certificate may be a wildcard certificate (*.company.com) or a named certificate (test.company.com).

  -The WWW certificate must match the DNS name used by the end-users to enroll.

  -To request a WWW certificate, you may need to provide a Certificate Signing Request (CSR). If so, you can download a CSR from the ES after the system is set up.

- If using NPS, set up the NPS server role and a RADIUS server. Note: The new RADIUS server certificates and root CA can be uploaded after ES is configured.
- If using a pre-existing RADIUS server, you need the IP address and access to the RADIUS server-signed certificates.
- If using an existing CA, and you would like to use ES as an intermediates CA to issue client certificates, you need the public and private key of the existing CA to upload into the Enrollment System.
- If using the ES as a proxy for an existing CA (Microsoft CA or Custom External CA) you need the CA URL and CA chain for the remote CA.
- DNS should be configured for Enrollment System and other components appropriate for your network.
- The initial firewall configuration should be set up to allow Internet access for following:

  -Access from ES -> xpc.cloudpath.net (TCP 80/443-HTTP/HTTPS)

  -Access from ES -> dist.cloudpath.net (used for ES updates TCP 80/443-HTTP/HTTPS)

  -Access from ES -> NTP (UDP 123) Note: 0.centos.pool.ntp.org on the standard NTP port (123). This can be configured to point to a local server during system setup, if you prefer.

- You should have some idea about your deployment scheme for employees, partners, contractors and guests. For example, some use cases might be:

  -Employee, IT asset, internal network, AD group

  -Employee, BYOD, internal network, AD group, BYOD use policy

  -Employee, BYOD, Internet-only, OAuth, short term

  -Sponsored Guest, BYOD, Internet-only, short term

  -Contractor, IT asset, internal network, limited access

Initial Setup Call

If you are setting up an account for a hosted deployment (onboard.cloudpath.net) or for a local VMware server, you can request an initial setup appointment with our implementation team. A typical implementation call lasts 1-2 hours.

Before the implementation call, you should review the Customer Checklist and Deployment Guide. If deploying to a local VMware server, be sure to download the OVA file prior to the setup call.

During the implementation call, we can help you with:

- Discussion about what you are trying to achieve
- Initial product setup
- Workflow basics
- If time permits, other configuration issues.
- Our goal is to get you up and running quickly so that you have adequate time to evaluate our product.

Who Should Be Involved in the Initial Setup Call

The ES implementation touches different aspects of your environment. Therefore, you might want to involve other members of your network team.

- The ES is installed as a virtual appliance. If you have a VM team, they should be contacted regarding the ES deployment.
- The open and secure SSIDs are set up on the wireless controller. The person/team that manages this aspect of your network should be available for making adjustments to the wireless controller.
- The ES can be set up to authenticate users to an Active Directory or LDAP server. Typically, you do not need to make adjustments to the authentication server. However, if there are issues connecting to the secure network, this person/team might be required.
- If you plan to use the onboard RADIUS server, which we recommend, you do not need the RADIUS server team. However, if you plan to use NPS or another external RADIUS server, this person/team should attend the setup meeting as user certificates are authenticated to the RADIUS server.
- After the initial setup, the Enrollment System provides a list of the inbound and outbound traffic of your XpressConnect Enrollment System. Firewall updates may be required for getting the ES up and running in your network.

Deployment Testing

Ideally, you should have devices on hand, for each operating system that you plan to support, for deployment testing. While the enrollment workflow behaves the same on each device, the Wizard application behaves slightly different on each operating system. With Android, this issue is compounded by the fact that each vendor can make modifications to the Android operating system, causing the application, in some cases, to behave slightly different between models.

Review the End-User Experience documentation for your supported OSes.