App C Using SSL Encryption with AppTransaction Xpert

AppTransaction Xpert supports SSL encryption for authentication to, and communication between, Capture Manager and capture agents. This appendix describes how to create certificates using OpenSSL on Windows; these certificates enable you and other users to capture data in AppTransaction Xpert using level-2 encryptions. This appendix also describes how to create a local Certificate Authority (CA).

The workflow described in this document relies on:

- openssl.exe, which is part of the OpenSSL distribution
- *op_cert.bat*, which is a helper batch file. This batch file wraps openssl.exe. You should customize the top portion of *op_cert.bat* with information that is specific to your environment, including specifying your organization name and the certificate expiration durations.

  This file and additional documentation are available on Riverbed Splash. To obtain the batch file, go to Riverbed Splash and search for “Generate certificates for use with SSL encryption for AppTransaction Xpert capture agents”.

Background

AppTransaction Xpert captures Anonymous (level 1) encryption by default. You can also specify Certificate Authentication (level 2) encryption, which requires that Capture Manager and the capture agents have a signed certificate from a trusted party.

It is recommended that you create certificates using a local Certificate Authority (CA) within your organization; this avoids the fees associated with third-party certificates. Many organizations already have local Certificate Authorities.

If you do not already have a local Certificate Authority, this document describes how to set up and use a local Certificate Authority using OpenSSL, which is open-source and widely used. See Creating SSL Certificates on Windows: Workflow Description.

Creating SSL Certificates on Windows: Workflow Description

The following sections outline the general steps:

- Step 1: Install SSL on your Certificate Authority (CA) Machine
- Step 2: Generate the Configuration File and Certificate Authority Keys
- Step 3: Generate the Capture Manager Certificate
- Step 4: Deploy the Certificate Files

Step 1: Install SSL on your Certificate Authority (CA) Machine

Procedure C-1 Installing SSL on a Certificate Authority (CA) Machine

1. Choose a machine to be your certificate authority (CA).
2. Download and install a binary distribution of OpenSSL onto the CA machine. This includes a command-line program **`openssl.exe`**, which is used to create certificates.

   The OpenSSL website maintains the official list of binary downloads for OpenSSL. To download an SLL installer for windows, go to the following URL:

   http://www.openssl.org/related/binaries.html
3. Install all SSL files in one directory (for example, c:\openssl) on the CA machine.

End of Procedure C-1

Step 2: Generate the Configuration File and Certificate Authority Keys

Procedure C-2 Creating Certificate Authority Keys

1. Open a command prompt window and go to the directory where the SSL executable files are installed.
2. Optionally, modify the *op_cert* batch file to change the expiration date of the certificates. Capture Manager private key has a default expiration of 90 days; the other certificates are valid for 10 years. (The country, state, locality, and organization in the batch file appear in the certificates, but have no effect on the security or setup.)
3. Run **`op_cert dsaparam`**.

   This command creates the *dsaparam.pem* file, which will be used to create the other certificates.

4 Run **`op_cert gencakey`**.

This command prompts for a passphrase three times. It will ask you for the passphrase for the CA private key. This should be a secure password. This command creates the following two files:

Table C-1 Files Created by the "op_cert dsaparam" Command

Item	Description
ca.pem	Public key of the certificate authority. This file goes on the manager and the agent.
casign.pem	Private key of the certificate authority. This file is used to sign *cert.pem* and *ca.pem*. This file should be kept only on the CA machine, and should be kept secure.

End of Procedure C-2

Step 3: Generate the Capture Manager Certificate

Procedure C-3 Generating a Capture Manager Certificate

1 Run **`op_cert genmanager`**.

This command prompts for a passphrase twice. When Capture Manager in level-2 mode is started, the user must enter this passphrase.

The command then prompts for a passphrase for the file casign.pem, which is the passphrase to the CA's private key specified in step 4 of Procedure C-2. This operation creates the following file:

Table C-2 File Created by the "op_cert genmanager" Command

Item	Description
cert.pem	Private key for Capture Manager. Goes on Capture Manager.

End of Procedure C-3

Step 4: Deploy the Certificate Files

Procedure C-4 Deploying Certificates

1. Install the capture agent on the agent machine.
2. On the agent machine, copy the file ca.pem in the capture agent directory. (The Windows default is C:\Program Files\opnet\AppCapture<*rel_num*>). The agent automatically uses level-2 encryption the next time a client machine tries to connect to it.
3. Copy the files ca.pem and cert.pem into your <*user_home*>\op_admin\ace_import_configs directory.
4. Exit and restart AppTransaction Xpert, and open Capture Manager. (From the AppTransaction Xpert System window, choose File > Capture Manager).

   ➥ A dialog box prompts for the passphrase used to create the certificate in step 4 of Procedure C-2.
5. Enter the passphrase and click OK. (If you click Cancel, Capture Manager still opens, but not using level 2 security.)
6. Start a capture with the new agent that you set up in this step. In the Capture Agents treeview of Capture Manager, the agent icon should show a padlock with a "2" in it, indicating that you are capturing using level-2 security.

End of Procedure C-4

Additional Information about Capture Agents and Encryption

For more information about the security functionality of capture agents, see Capture Encryption.

Note—This document is intended to assist AppTransaction Xpert users, but a definitive guide to the entirety of SSL is beyond the scope of this help system. Many organizations already have security teams that are familiar with SSL. For additional details about SSL itself, the O'Reilly book "Network Security with OpenSSL" by John Viega provides first an overview and then details of SSL. You can read the introductory chapter online (http://www.oreilly.com/catalog/openssl). There are numerous other books about SSL, and of course many articles about SSL are available on the Internet.