Deploying Certificates Over the Air

Certificate Manager / SecurePlus Extensions

June 2010

Contents

Introduction

With the introduction of the Wavelink Certificate Manager, capabilities were added to Avalanche to allow it to deploy 802.1 X Certificate-based authentications to mobile devices. Furthermore, coupled with user authentication, a device is able to tie sets of credentials to individual certificates, thereby allowing users to authenticate to the network using a certificate issued to them.

The first version of the Certificate Manager facilities made use of CE Secure (AKA SecurePlus) as its client. In essence, the certificate facilities were a natural evolution of CE Secure's device-side user authentication facilities.

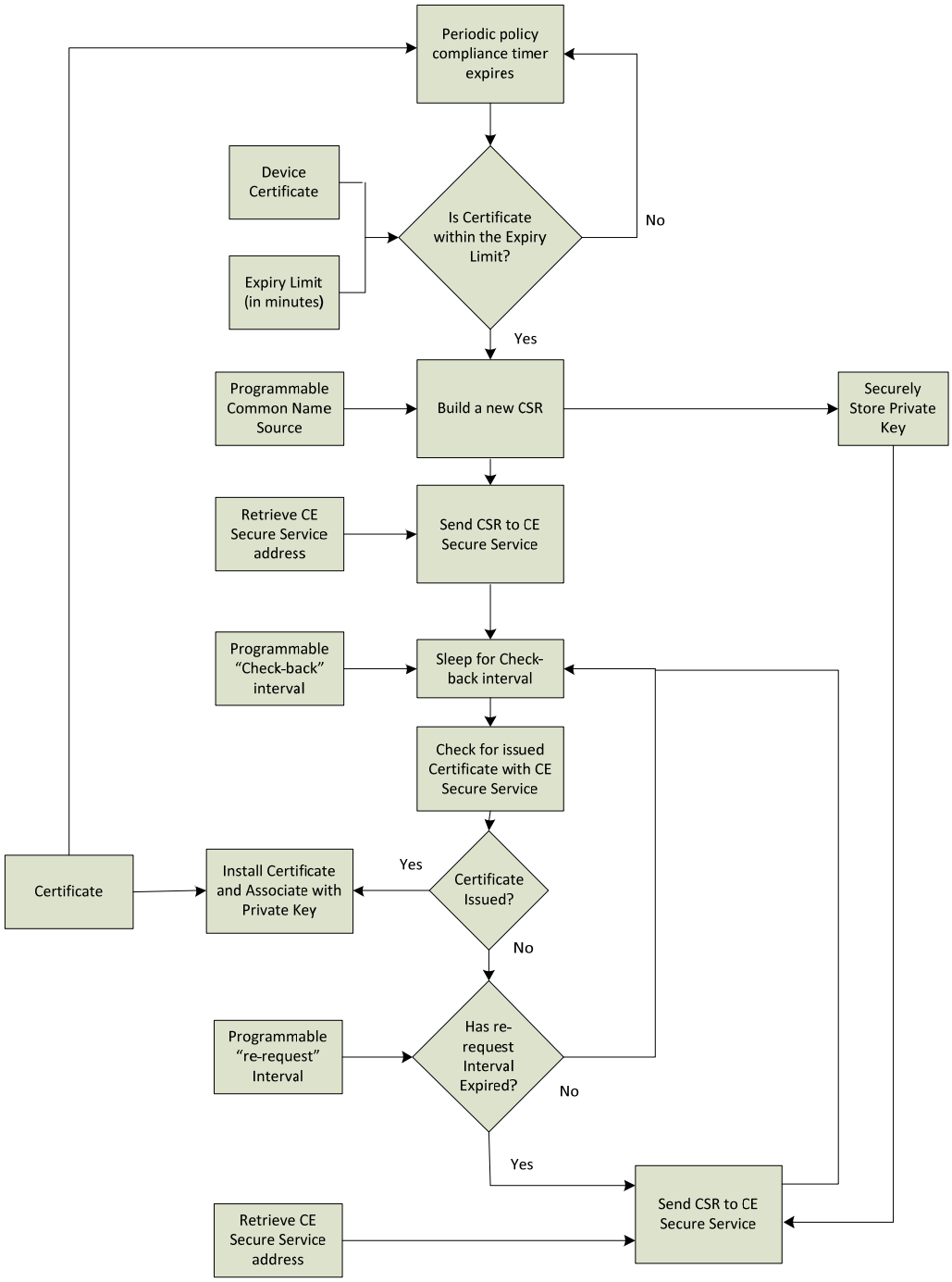
Installation of the certificates is performed via the ActiveSync cradle. The process involved the generation of a Certificate Signing Request by the device coupled with an issued certificate loading procedure.

The extensions described in this document cover the next phase in the lifecycle of certificate management – namely the automatic issuance of new Certificate Signing Requests over the air to a secure point, followed by the automatic installation of certificates to mobile devices once they are issued.

SecurePlus Extensions for Over the Air (OTA) Certificate Renewal

The design of the SecurePlus client has been changed to allow the client to automatically request new certificates when they are within a timeframe to expire. Once the client is inside of this timeframe, the client communicates back to the CE Secure Service.

The process followed by the client is as follows:



As it can be seen, there are a number of parameters which may be configured in order to determine how the client behaves. These are:

Expiry Limit	This is the time limit set by the administrator as being the amount of time left on a certificate at which point a new CSR should be issued.
Programmable Common Name Source	New CSRs will be issued and stored on the CE Secure Service host. The Common Name inside the CSRs may contain any Avalanche property. This property must be specified.
Programmable Check-back interval	The amount of time the client will wait until it checks in to retrieve an issued certificate.
Programmable re-request interval	In the case that a CSR becomes missing, the client can be programmed to issue a new CSR if no certificate is issued after this specified period of time.

In addition to these parameters, the CE Secure Service also allows for the following parameters to be configured:

Programmable CSR filenames	In order to easily identify CSRs, the filename can be programmed to contain device-side Avalanche properties, such as TerminalID, IP address or any other property, including custom properties.
CSR Directory	CSRs may be placed in any directory on the CE Secure Service host for which it has read/write permissions.
Issued Certificate Directory	Certificates may be placed in any directory on the CE Secure Service host for which it has read/write permissions.

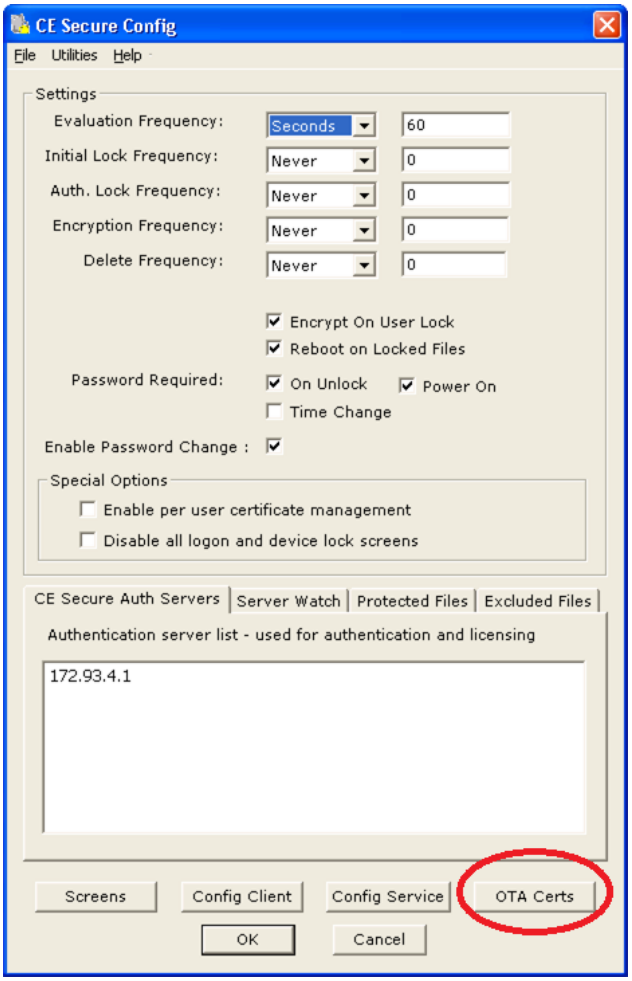
Using the OTA Certificates Facility

Assuming the installation is currently using CE Secure perform the following:

1. Uninstall the existing CE Secure Service
2. Disable the CE Secure package.
3. Do not deploy.

Next, install the new CE Secure OTA package and configure the parameters for:

4. Licensing Server
5. Authentication Server List
6. Server watch (if any)
7. Protected files (if any)
8. Excluded files (if any)
9. Configure the client (using the Config Client button).



Now choose a directory for CSRs and Issued Certificates.

Create these directories and ensure that the CE Secure Service has permissions to read and write to those directories.

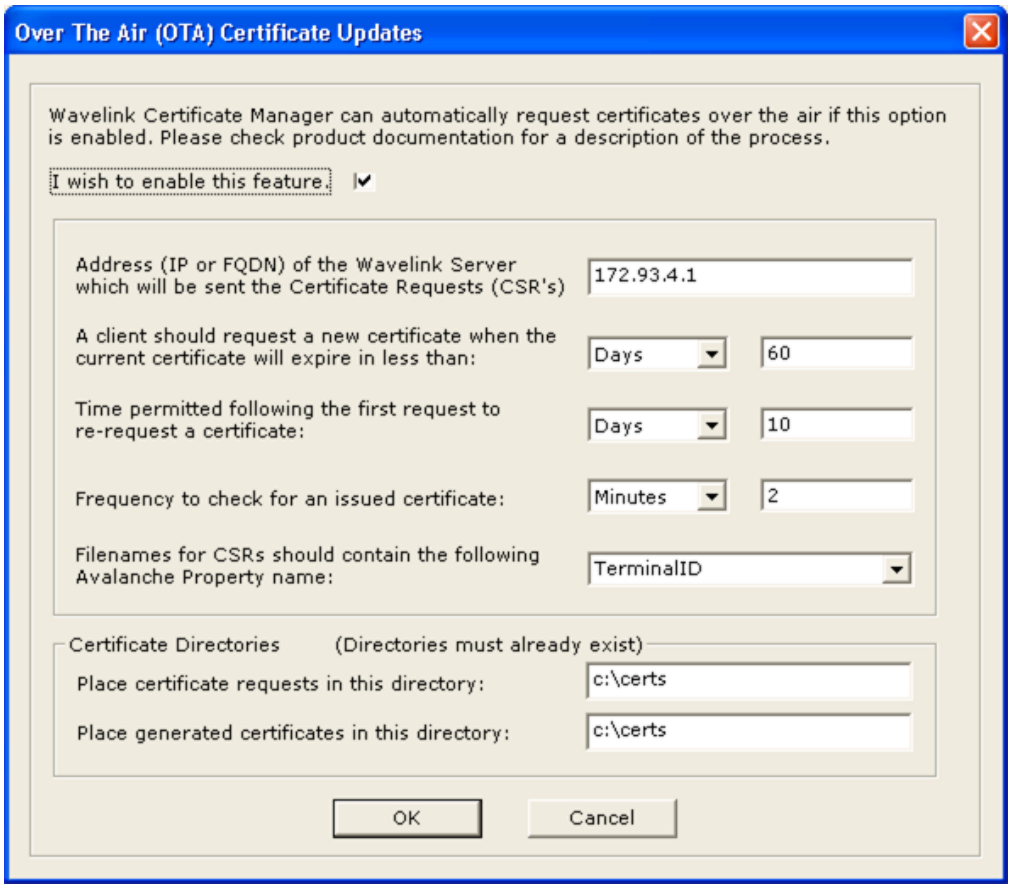
Also select whether per user certificate management is to be used. Please be aware that at this time, only device certificates may be renewed over the air.

Per user certificate renewal over the air will be addressed in a future release.

Now select the OTA Certs button to be taken to the OTA configuration section of CE Secure.

Over the Air Certificates Configuration

Once the OTA Certs button is selected, the following pop-up menu will be displayed.

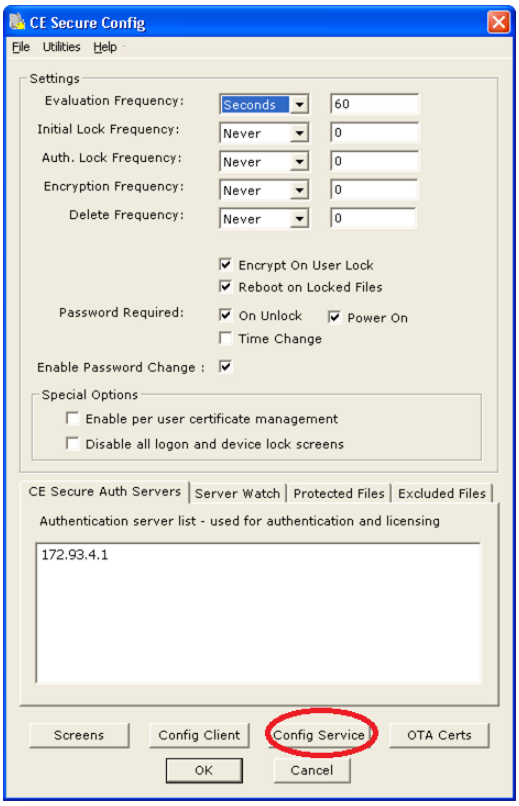


To avoid any ambiguity, each option has a full English description of its function. The client must be given the name of the CE Secure Service to use, together with the parameters outlined earlier.

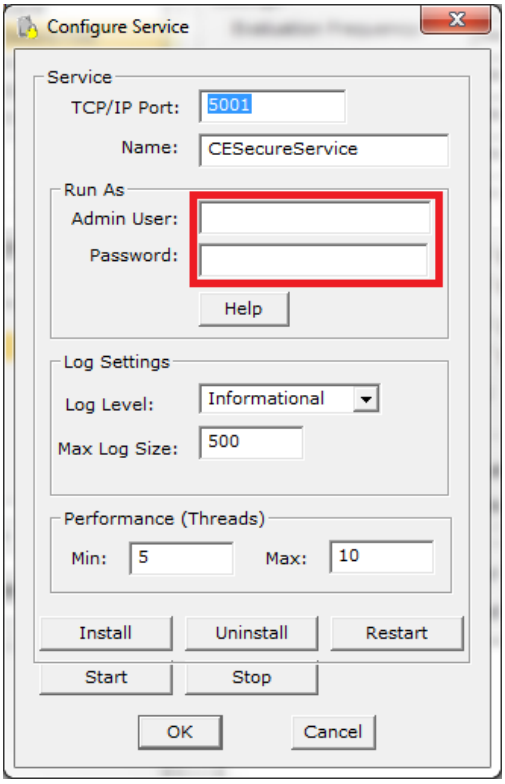
Once the parameters have been configured click OK.

The CE Secure Service now needs to be installed using the parameters which have just been configured.

To do this select the Config Service button.



Once this is performed, the following is displayed:



It is critical with this page to ensure the right credentials are provided to install the CE Secure Service.

If no credentials are provided, then the CE Secure Service will install using the local service account. For most installations, this will be adequate.

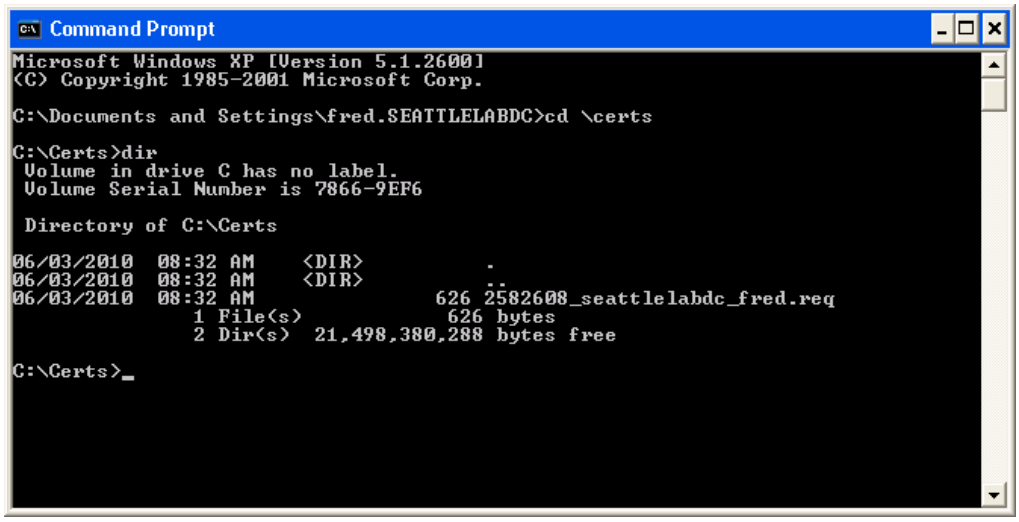
However, if CE Secure is installed onto a domain and the CE Secure client is to honor and allow passwords to be changed upon expiration, then the credentials will need to have administrative privilege on the domain.

Once the credentials have been entered, the service may be installed and run by selecting the Install option followed by the Start option.

Avalanche Package Installation onto the Client

Once the package is delivered to the mobile devices, via the Universal Update, the CE Secure client will automatically be updated. It will also invoke the policy compliance check shown in the flowchart. If this check determines that a new certificate is to be issued, then a new CSR using the parameters above will be placed in the "c:\certs" directory as shown in the dialog.

The following example shows the directory once a certificate request is issued using the TerminalID as part of the filename and Common Name of "fred":



As it can be seen, the TerminalID is 2582608, the Common Name is seattlelabdc _fred.

Any Common Name containing a backslash is translated into an underscore ("_") for the purpose of naming the CSR in the file system.

The Common Name itself is automatically generated using the Common Name which is associated with the certificate which is currently in use to authenticate the device.

This base-64 encoded PKCS#10 formatted CSR should now be passed to a CA for certificate issuance. The mobile terminal has the private key for this CSR securely stored.

Once the certificate has been issued, it should be placed into the directory using the name naming convention, but with a .CER extension.

Please be aware that the naming convention of <Avalanche Property>_CommonName.CER must result in a unique filename per device.

The client will then automatically find the appropriate filename and install the certificate and associate it with its local private key.

Troubleshooting

The most common problem encountered when using the Certificate Manager with CE Secure is authentication issues. The CE Secure service does have a diagnostic interface which may be invoked in order to establish the cause of such problems. To use it, ensure that Telnet is installed. A basic Telnet client for Windows is included with XP, Vista and Windows 7 (although for the latter two, it must be separately installed).

To invoke the diagnostic interface, do the following:

1. Invoke the Windows Command Line Interface (cmd.exe).
2. Type:
   telnet <IP address of CE Secure service> 5001
3. A prompt will appear as follows:
   CE Secure v2
4. Type:
   logon <username> <password> <domain>
5. The system will respond with either:
   SUCCESS
   FAILURE

If there is a long delay followed by FAILURE, this can indicate that the CE Secure service was unable to contact the domain authentication services. This can happen if the trust relationship between the PC hosting the CE Secure service and the domain fails. To establish whether this is the cause, go to the Users part of the control panel and attempt to add a domain user to the local machine. If that fails, it will indicate whether it was a domain trust issue.