



Application Note

Onsight Device Certificate Management

ONSIGHT DEVICE CERTIFICATE MANAGEMENT.....	3
Supported Certificate Formats:	3
Stores List	3
Importing Certificates:	3
CERTIFICATE PACKAGES USING ONSIGHT MANAGEMENT SUITE.....	5
ONSIGHT DEVICE SIP REGISTRATION - SIP-TLS CHECK LIST:	5
ONSIGHT DEVICE WIRELESS NETWORK - EAP-TLS CHECK LIST:	6
ONSIGHT DEVICE WIRELESS NETWORK - PEAP CHECK LIST:.....	6
TROUBLESHOOTING	7

Onsight Device Certificate Management

X.509 Certificates are used to authenticate the identity of a User or Computer on a network. The Onsight Device supports using X.509 certificates for the following:

- 802.1X Wireless Network User Authentication e.g. TLS
- Server Authentication e.g. TLS or PEAP
- SIP-TLS encryption e.g. SIP Proxy Server registration
- Cisco Presence Server Authentication

Supported Certificate Formats:

- Certificates: .cer – contains certificate information with public a public key but not a private key. This is a generic extension that denotes a certificate. Server, Root Certificate Authority (CA), and Intermediate CA certificates can be in this format. It is commonly a plain text file and can be PEM, DER or Base 64 format. You can import these formats into the Windows certificate store.
- Public-Key Cryptography Standards (PKCS #12): .pfx, .p12 – stores private keys with accompanying public key certificates, protected with a password based symmetric key. This format is generally only seen with a Client Certificate.
- Private Keys: .pvk – private key for a User certificate.

Stores List

Certificates can be imported into the following three logical stores:

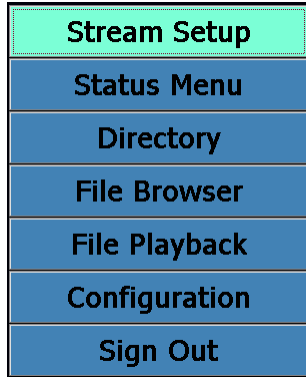
- My Certificates: contains individual certificates for users.
- Trusted Authorities: contains certificates from Trusted Root authorities.
- Other Authorities: stores all other certificate types, e.g. intermediate CA authorities.

IMPORTANT: When using certificates the Onsight Device date and time must be accurate to allow successful authentication of the certificate.

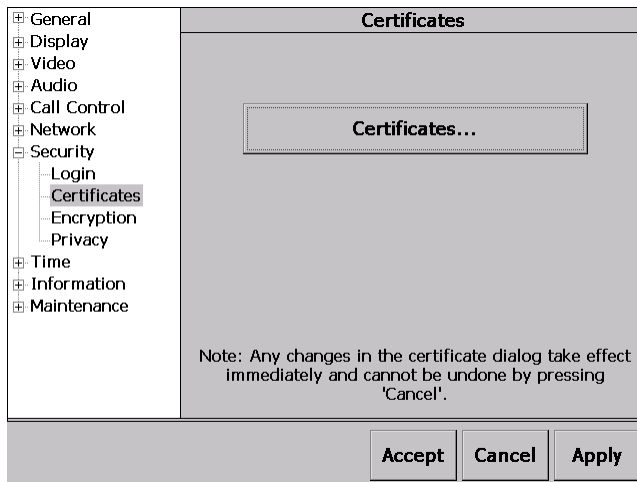
Importing Certificates:

- Copy the certificate you wish to install onto the Root directory of an SD card e.g. 'siphost.cer'.
- Insert the SD card into the Onsight Device.
- Login to the Onsight Device and proceed...

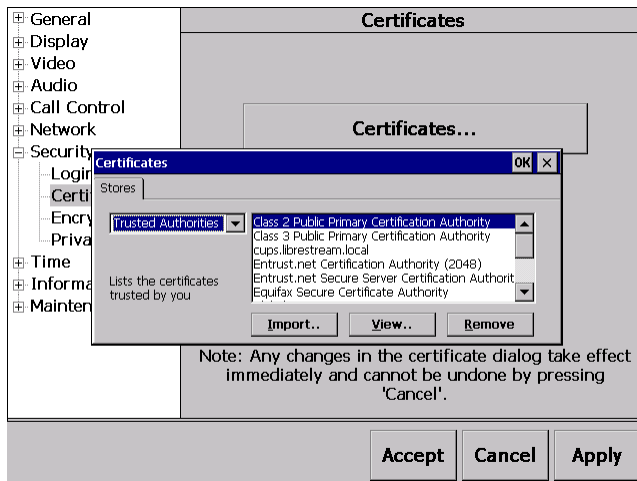
1. Go to the Main Menu and select Configuration.



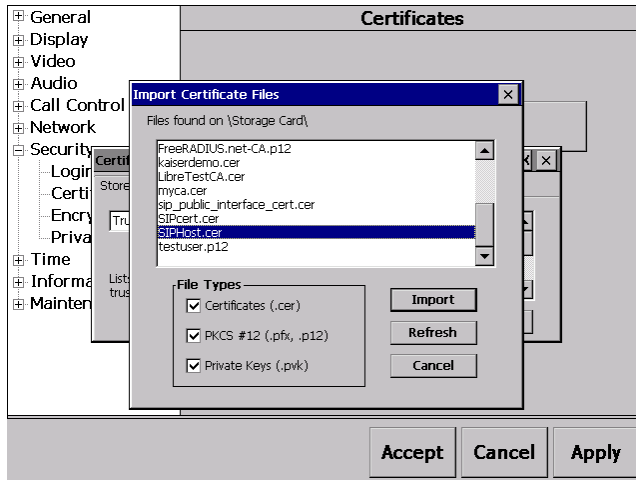
2. Go to Security\Certificates and Press 'Certificates...' button.



3. Press 'Import...' button.



4. Select the certificate to import and press 'Import' button. Note: you may be prompted to enter a password if the certificate is password protected.



Certificate Packages using Onsight Management Suite

Librestream's Onsight Management Suite can be used to manage your Onsight Mobile Devices and install certificates by creating certificate packages which are installed during a Software Update Job.

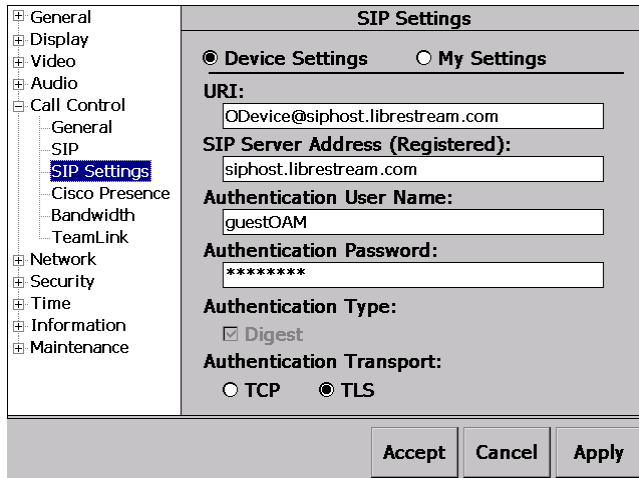
The Onsight Management Suite Administrator creates a Certificate package which includes the certificate types supported by the Onsight Device. This package is then added to a Software Update Job that is pushed out to the devices when they connect to the Onsight Management Web Service.

Each certificate is assigned to a Certificate Store and can be installed for use by all Users or a selected User only.

Consult the Onsight Management Suite User Manual for details on creating Certificate and Software Update Packages.

Onsight Device SIP Registration - SIP-TLS Check List:

- Confirm the correct date and time is set on the Onsight Device
- Install required X.509 certificates:
 - SIP Server Certificate e.g. siphost.cert
- Set the Authentication Transport to 'TLS'



Onsight Device Wireless Network - EAP-TLS Check List:

- Confirm the correct date and time is set on the Onsight Device
- Install required X.509 certificates:
 - User Certificate
 - Server
 - Certificate Authority Root (if necessary)
- Correct WiFi security settings are entered on the Onsight Mobile
 - Encryption: TKIP or AES
 - Authentication: WPA or WPA2
 - EAP type: TLS
 - Enter the *user name* of the Certificate under Configuration\Network\Wireless\Advanced\Wireless Network Properties\Properties\Authentication Settings\User Information
 - Press 'Select' and tap on the correct Certificate to use for Authentication

Onsight Device Wireless Network - PEAP Check List:

- Confirm the correct date and time is set on the Onsight Mobile
- Enter PEAP *user name* and *password* under Configuration\Network\Wireless\Advanced\Wireless Network Properties\Properties\Authentication Settings\User Information
- Verify the 'Validate Server' check box is correctly set on the User Information page
 - If you are not validating the identity of the server uncheck 'Validate Server'.
 - If you are validating the identity of the server check 'Validate Server' and install the certificate for the server on the Onsight Device.
 - Install required X.509 certificates:
 - Server
 - Certificate Authority Root (if necessary)

- Correct WiFi security settings are entered on the Onsite Device.
 - Encryption: TKIP or AES
 - Authentication: WPA or WPA2
 - EAP type: PEAP

Troubleshooting

1. After following the setup steps the device still can't Authenticate:
 - a. Is the user locked out because of too many authentication attempts?
 - i. Time outs can occur during authentication attempts. E.g. Cisco Access Point controllers have an 'identity-request-timeout' this can be modified to increase the timeout to prevent lockouts. If a user hasn't entered the username/password correctly and has to re-enter information the timeout can cause a lockout to occur.
 - ii. Fix: Reset the PEAP user account at the RADIUS Server.
2. The username and password were entered in the correct location but the Network Information Dialog still prompts me for user name/password information.
 - a. A typo may have occurred when entering the information.
 - i. Press the 'Advanced' button on the Wireless Information tab. Delete the SSID you are trying to connect to from the 'Preferred Networks' list. Press 'OK'.
 - ii. Re-enter the information for the connection to the SSID including PEAP username/password information.
3. Has the date and time been reset?
 - a. If the battery was allowed to drain the date and time may have been reset, check that the date and time are accurate.