**IP400 Series Phones Fail to Connect to CAS**

**SCENARIO**

IP400 series phones are failing to connect to the Connect Server's CAS connection.  The phones will register to their controlling switch, but functions such as Directory or Visual Voicemail return a Failed to Connect to Server error.

**SYMPTOMS**

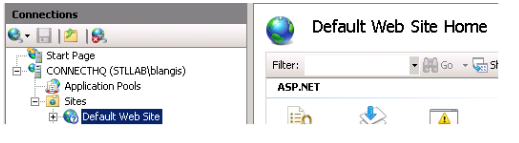
IP400 series phones are failing to connect to the Connect Server's CAS connection.  They will register to their controlling switch, but functions such as History, Directory or Visual Voicemail return a Failed to Connect to Server error.

**CAUSE**

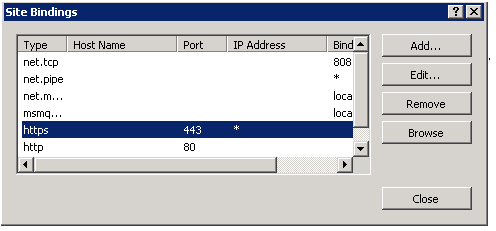
**Reason 1**  
  
  
Reviewing the IIS logs on the HQ server a search for the IP address of the IP phones will show a 403 error returned when the phone attempts to access the HQ server:  
  
This can be caused by a certificate that is not self-signed, such as an Intermediate CA certificate, which has been imported into the Local Computer --> Trusted Root Certification Authorities certificate store on the Mitel Connect server.  
  
2016-12-21 15:01:37 10.169.24.10 POST /shoreauth/certauth - 443 - 10.169.24.139 Mozilla/5.0 - **403**16 2148204809 730  
2016-12-21 15:01:37 10.169.24.10 POST /shoreauth/certauth - 443 - 10.169.24.139 Mozilla/5.0 - **403**16 2148204809 1  
2016-12-21 15:01:37 10.169.24.10 POST /shoreauth/certauth - 443 - 10.169.24.139 Mozilla/5.0 - **403**16 2148204809 1  
  
In the same IIS log the sc-win32-status field shows the status of 2148204809 which translates to error code 0x800b0109, which is defined as CERT\_E\_UNTRUSTEDROOT.  
  
2016-12-21 15:01:37 10.169.24.10 POST /shoreauth/certauth - 443 - 10.169.24.139 Mozilla/5.0 - 403 16 **2148204809** 730  
2016-12-21 15:01:37 10.169.24.10 POST /shoreauth/certauth - 443 - 10.169.24.139 Mozilla/5.0 - 403 16 **2148204809** 1  
2016-12-21 15:01:37 10.169.24.10 POST /shoreauth/certauth - 443 - 10.169.24.139 Mozilla/5.0 - 403 16 **2148204809** 1  
  
This information is explained in Microsoft KB 2802568 at URL [**https://support.microsoft.com/en-us/kb/2802568**](https://support.microsoft.com/en-us/kb/2802568)  
  
**OR**  
  
This can also be caused by the HW root CA missing in the Trusted root store.  
  
**Reason 2**  
This can be caused by a mismatch in the IIS binding when compared to the keystore. This will generally be shown by a "SSL handshake error" or a "Certificate Authority Invalid" error message in the phone logs.  
  
**Reason 3**  
The phone cannot reach the HQ server when using its FQDN. The phone logs will show:  
  
2018-12-03T10:40:16.156-07:00 P105709FW16424D2D8B p8[240]: 342246.5 pri 0000,sl 01165,sf src/networkaccessmanager.cpp,msg [0x45bff490] NetworkAccessManager::handleRequestFinished: ERROR ON REPLY qreply (0x156a980), reply (0x169f010), id (0x15), cancelled (0): on url: [**https://example.fqdn.com/shoreauth/certauth**](https://example.fqdn.com/shoreauth/certauth), error code = 3, **Host not found**  
  
**Reason 4**  
  
There have been modifications to the TLS versions or Cipher suites supported on the HQ server.  
See the **Resolution** section below.

**MORE INFORMATION**

**RESOLUTION**

**Reason 1**  
  
a) To resolve this issue the incorrectly imported certificate must be identified and removed from the Local Computer --> Trusted Root Certification Authorities certificate store on the Mitel Connect server.  Once the certificate has been removed, restart the Connect Server's World Wide Web Publishing Service.  
  
You can identify if there are unwanted certificates in the root store by running the below command from an administrative powershell prompt and removing the certificates listed in the resulting c:\computer\_filtered.txt file.  
  
Get-Childitem cert:\LocalMachine\root -Recurse | Where-Object {$\_.Issuer -ne $\_.Subject} | Format-List \* | Out-File "c:\computer\_filtered.txt"  
  
**OR**  
  
b) Install the Mitel HW root Certificate in to the Trusted Root Certificate store.  
  
Navigate to Shoreline Data\Keystore\certs  
Double click the Mitel\_mfg\_ca.crt and the certificate should open. If it does not, right click and select "open with" and select "crypto shell extensions"  
In the resulting window click on "Install Certificate" and hit next.  
Select "Place all certificates in the following store" and select browse.  
Highlight the "Trusted Root Certificate Authorities" store and select ok.   
Click next and complete the certificate installation and test.  
  
**Reason 2**  
  
We will need to compare the certificates bound to IIS and the keystore. To do this:  
  
1) Browse to your Shoreline Data directory. The default location is c:\Shoreline data.  
2) Browse to shoreline data\keystore\certs  
3) Double click the [**server.crt**](http://server.crt/) file and click on the details pane, scroll to the bottom of the window and select the "thumbprint". **Make note of this**and close the certificate window.  
              (note: if the default program for certificate files has been changed, you will want to right click the file and select open with and select "crypto shell extensions")+  
  
4) Open IIS Manager and expand the server and sites connection and select "Default Web Site"

5) On the right hand side Actions pane, select "Bindings"  
6) Select the HTTPS port 443 binding and select "Edit"



7) Select "View" on the Edit Site Binding Page, this will open the certificate window.  
8) Go to the details pane and compare the thumbprint to the thumbprint you noted in step 3. They should be the same.   
9) If the thumbprints are different, select the appropriate certificate out of the drop down list in the Edit Site Binding window. You can verify that it is the correct certificate by selecting it from the list, clicking on view and comparing the thumbprint before making any changes.  
10) Click OK and close. Test CAS features.  
  
  
**Reason 3 - DNS**  
  
Verify the DNS configuration for the A record of the HQ server. The hostname (FQDN) needs to match its IP Address.  
Verify the phones have a DNS server. This can be done from phone logs. Phone logs can be searched for "Host not found" , this would indicate a DNS problem.  
  
**Reason 4 - Cipher suites**  
  
Ensure that TLS version 1.0 is enabled on the server. This can be done using IIS crypto, or the registry.   
[**https://www.nartac.com/Products/IISCrypto**](https://www.nartac.com/Products/IISCrypto)  
**Note:**any changes made here require a reboot.

**WORKAROUND**

**Workaround for Reason 1 a)**  
As a work-around the following procedure can be followed to allow connectivity while the certificate store is investigated.  As always, ***use care when modifying a server's registry settings***.  
  
1. Open regedit   
2. Navigate to HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL  
3. Create a new 32 bit D-Word entry named ClientAuthTrustMode  
4. Put 2 in the data field  
5. Restart the server's World Wide Web Publishing Service  
  
Once the services return to service, retest and verify the IP400 series phones now have CAS connectivity.