# Unable to get local issuer certificate.

- Parallels Remote Application Server

# Symptoms

The **Unable to get local issuer certificate. <20>** error is observed when starting published apps:

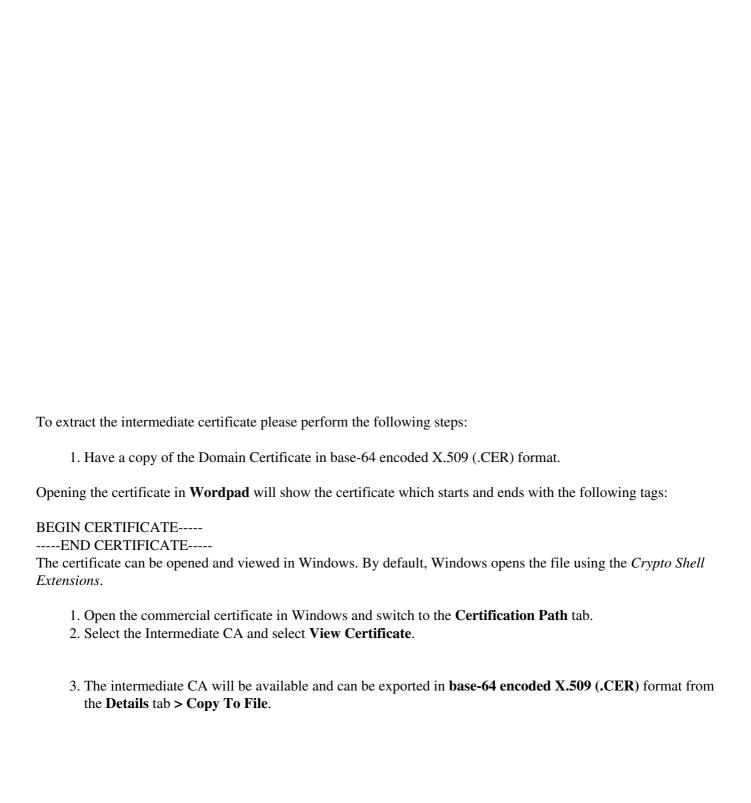The issue also might be observed when upgrading from previous RAS versions to v17.1 or later.

# Cause

Missing an associated intermediate certificate in the RAS console.

**NOTE:** It should be a one time issue due to a significant change in the way of storing certificates in the product starting from v17.1

# Resolution

1. Go to **RAS Console  Farm  Certificates**  Open certificate **Properties** from the context menu and switch to **Intermediate** Tab.

2. Check if it is empty, copy the intermediate certificate to this tab and apply the settings.

To extract the intermediate certificate please perform the following steps:

1. Have a copy of the Domain Certificate in base-64 encoded X.509 (.CER) format.

Opening the certificate in **Wordpad** will show the certificate which starts and ends with the following tags:

BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

The certificate can be opened and viewed in Windows. By default, Windows opens the file using the *Crypto Shell Extensions*.

1. Open the commercial certificate in Windows and switch to the **Certification Path** tab.
2. Select the Intermediate CA and select **View Certificate**.


3. The intermediate CA will be available and can be exported in **base-64 encoded X.509 (.CER)** format from the **Details** tab **> Copy To File**.

Opening the exported .cer file for the Intermediate CA in notepad will also show the following tags for the Intermediate CA certificate:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

    4. As a fix, one would need to put the Intermediate CA information in the domain certificate issued in notepad.

In notepad the certificate would have the following structure:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```
The top tag would pertain to the domain certificate, where as the bottom one would contain the Intermediate CA one.

**NOTE**: The Root CA does not require this operation as all supported Root CAs are listed in the trusted.pem files available on Client Installations as well as within the Remote Application Server installation directory.