

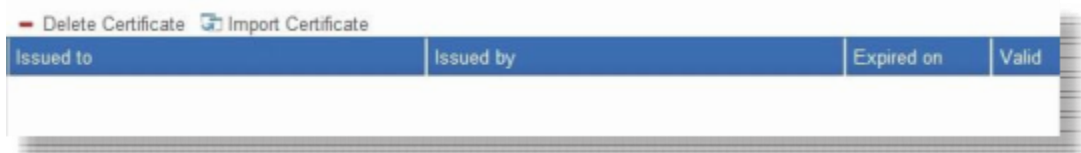
3.2.8 Managing Certificates of Remote Computers

Thin clients are simple endpoint devices for accessing services from remote computers. To ensure connection security between thin clients and remote computers, certificates of remote computers where desktop virtualization services are delivered may be required in order to verify the identify of remote computers. You could import security certificates of remote computers, and then push certificates remotely to multiple thin clients with the help of Atrust Device Manager.

Importing Certificates of Remote Computers

To import the certificate of a remote computer, please do the following:

1. On **System** tab, click **Deployment > Certificate**.
2. The Certificate list appears in Management area.



Issued to	Issued by	Expired on	Valid
-----------	-----------	------------	-------



NOTE

- If you never imported certificate files into Atrust Device Manager, the Certificate list will be empty as shown above.

3. Click **Import Certificate** on the top of the list.
4. The Import Certificate window appears.



NOTE

- Atrust Device Manager supports both PEM (Privacy Enhanced Mail) and DER (Distinguished Encoding Rules) format certificates.
- The upper limit of imported certificates is 16.

5. Click **Browse** to locate the desired certificate file, and then click **Open** to confirm.

NOTE

- Atrust Device Manager will automatically perform file check to ensure there is no duplicate in the Certificate list.

6. Click **Import** to continue.



7. On completion, the imported certificate appears as an entry in the Certificate list.

Issued to	Issued by	Expired on	Valid
Go Daddy Secure Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	2031-05-03	Valid


NOTE

- While pushing certificates to thin clients, all certificates in the Certificate list will be imported to selected clients. For instructions on how to push certificates to clients, please refer to section "3.4.18 Pushing Certificates of Remote Computers to Clients" on page 86.

Deleting Certificates of Remote Computers

To delete the certificate of a remote computer, please do the following:

1. On **System** tab, click **Deployment > Certificate**.
2. The Certificate list appears in Management area.
3. Click to select the desired certificate.



NOTE


- To delete more than one certificate, Ctrl-click to select multiple entries.

4. Click **Delete Certificate** on the top of the Certificate list.
5. The Delete Certificate window appears prompting for confirmation.
6. Click **Delete** to confirm.
7. The selected certificate is removed from the Certificate list.

3.2.9 Configuring Deployment Settings

You can deploy, maintain, and upgrade your thin clients from a computer with Atrust Device Manager. All required files (firmware, snapshot, or package files) can come from the same computer where your Atrust Device Manager is installed, or another computer with needed files.

Deployment Configuration			
Option	Description	Required Actions	See Page
Use Internal Server	Using updates and snapshots from the same computer	<ul style="list-style-type: none"> • Import or copy all required files to the same computer where your Atrust Device Manager is installed • Default settings; no configuration need to be done 	Page 34
Use External Server	Using updates and snapshots from another computer	<ul style="list-style-type: none"> • Import or copy all required files to another computer where an instance of Atrust Device Manager is installed • Configure settings to get all needed files from another computer 	Page 35 Page 35



NOTE

- In Atrust Device Manager, the local updates and snapshots are used by default.

Maintaining or Deploying Clients with Updates or Snapshots from the Same Computer

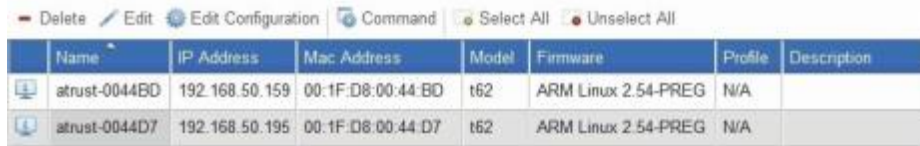
To maintain or deploy clients with updates or snapshots from the same computer, please do the following:

1. On **System** tab, click **Deployment > Deploy Server**.
2. The Deploy Settings pane appears in Management area.

3.4.18 Pushing Certificates of Remote Computers to Clients

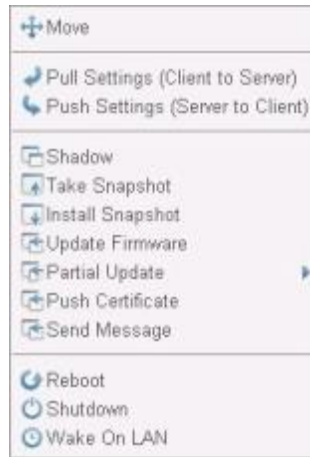
To push certificates of remote computers to a thin client, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

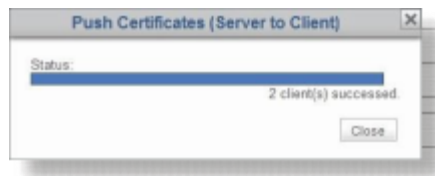


Name	IP Address	Mac Address	Model	Firmware	Profile	Description
atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.54-PREG	N/A	
atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.54-PREG	N/A	

3. Click to select the desired client, and then click **Command** on the top of the Client list.
4. The Command menu appears.



5. Click to select **Push Certificate**.
6. A window appears prompting for confirmation.
7. Click **OK** to confirm.
8. The Push Certificates window appears showing the progress and result of pushing certificates.



9. After completion, click **Close** to exit.