

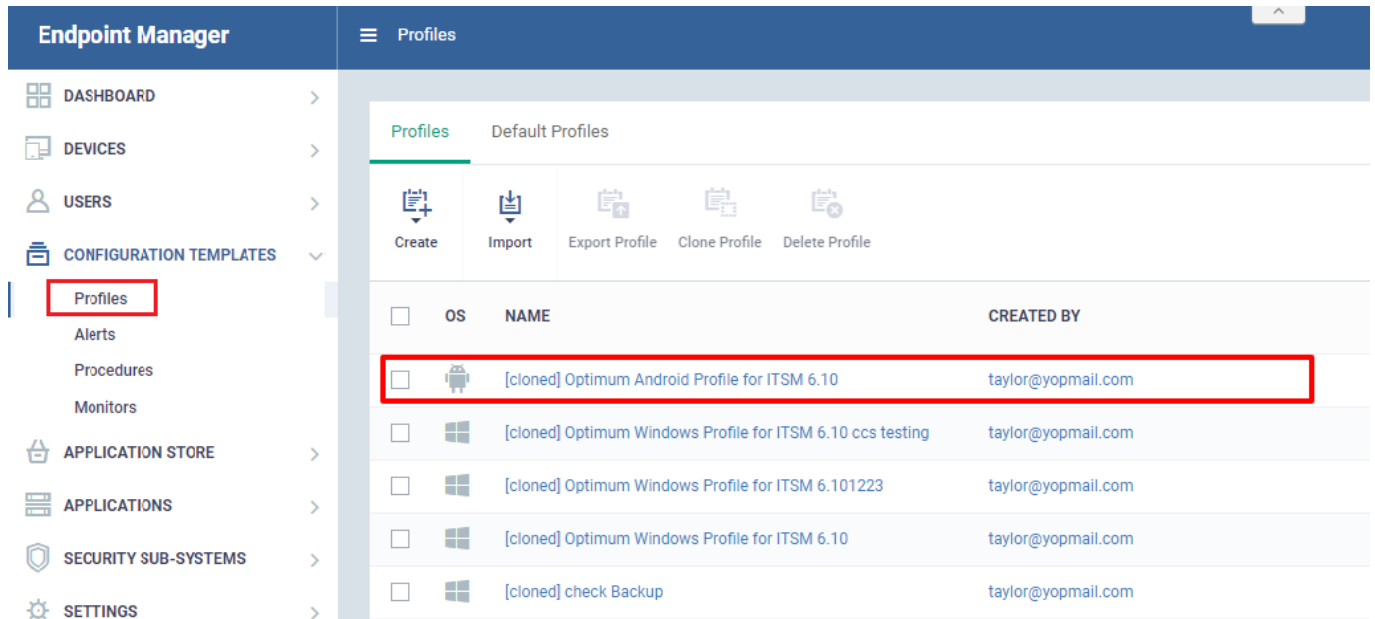
How to allow Citrix application in Comodo Firewall

Step[1]: Login into Endpoint Manager.

Goto **CONFIGURATION TEMPLATES** → **Profiles** , and select the profile you want to configure.

Step[2]: Please select profile associated with device or group which requires **Firewall** Configuration

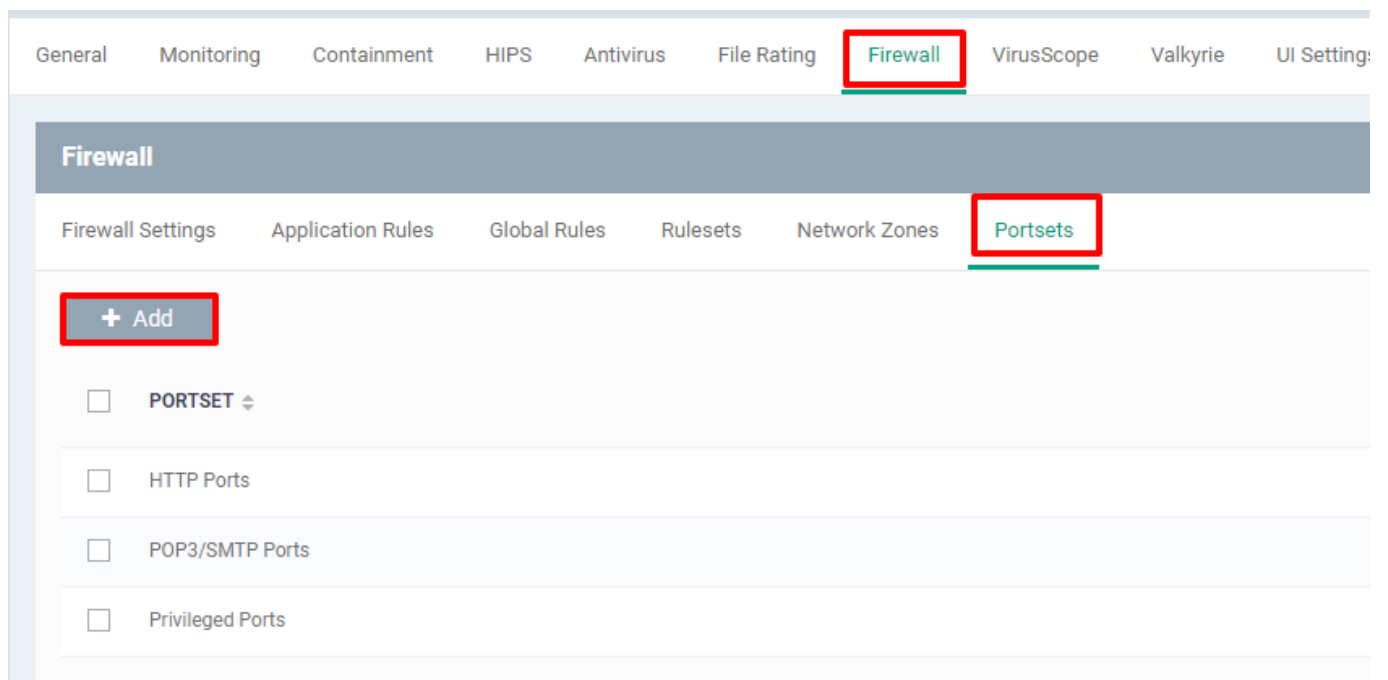
For Example:Optimum Windows Profile for 6.10 is associated with device DESKTOP-J45HD05



Step[3]:Add Firewall port sets for Citrix

In Firewall, Add the Port numbers in Portsets. So that we can use it to allow Citrix application in through Firewall global rules.

1) Goto **Firewall** → **Portsets** → **Add**, It directs you to **Portset** dialog box.



II) Name the **Portset** as required

For Example: "Citrix Ports" and click "Add"

Portset

Name

PORTS
<input type="checkbox"/>

III) Add the port numbers for Citrix one by one

For Example- Port Number for Citrix are **80, 443, 1494, 2598, 2512, 2513** and then click "OK"

Port

Exclude (i.e. NOT the choice below)

Any

A single port

A port range -

Portset

Name

Citrix Ports

+ Add

<input type="checkbox"/>	PORTS	
<input type="checkbox"/>	80	
<input type="checkbox"/>	443	
<input type="checkbox"/>	1494	
<input type="checkbox"/>	2598	
<input type="checkbox"/>	2512	
<input type="checkbox"/>	2513	

OK Cancel

IV) Check whether the **Name** you added is available in the portset and then click **Save**.

For Example: **Citrix Ports** is available

Firewall Save Delete

Firewall Settings Application Rules Global Rules Rulesets Network Zones Portsets

+ Add

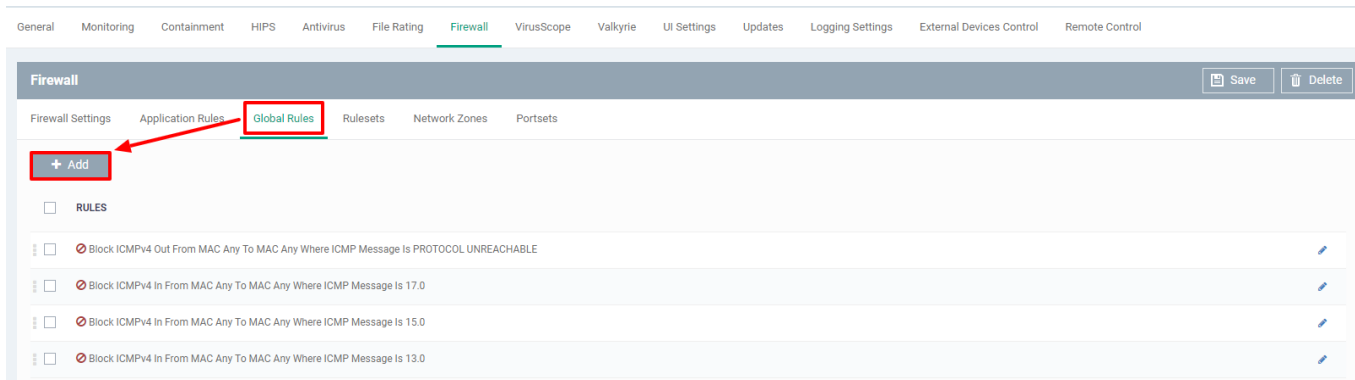
<input type="checkbox"/>	PORTSET ▾	
<input type="checkbox"/>	HTTP Ports	
<input type="checkbox"/>	POP3/SMTP Ports	
<input type="checkbox"/>	Privileged Ports	
<input type="checkbox"/>	My Portset	
<input type="checkbox"/>	Citrix Ports	

Step[4]: Add Global rules to allow Citrix ports

In Firewall, Add the Global Rules .So that we can use it to allow Citrix application in through Firewall global rules.

By selecting Destination Port, Citrix Application will be allowed by Firewall only by those Port numbers added.

1)Goto "**Global Rules**" and click "**Add**" , it will direct to a **Firewall rule** dialog box



II) In Firewall Rule,

Enable the Check box "**Log as Firewall event if this rule is fired**".

Action: This is to allow or block the application action.

By default, the **Action** will be "**Allow**"

Protocol: There are some protocols which need to be selected based on the application.

By default: It will be "**TCP or UDP**"

Direction: It tells about the direction In, Out or Both

By default: It will be "**In or Out**"

Description: Add any description.

For Example: Description is "**Allow Citrix**".

Then Click "**Destination Port**".

Firewall Rule

Action: Allow Log as Firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description: Allow Citrix

Source Address Destination Address Source Port **Destination Port**

Exclude (i.e. NOT the choice below)

Type: Any

OK Cancel

III) In destination port, select desired **Type** and add the **Portset** you created and click "OK"

For Example: Select **Type** as "A set of ports" and **Portset** as "Citrix ports" which is created and click **OK**.

Firewall Rule

Action: Allow Log as Firewall event if this rule is fired

Protocol: TCP or UDP

Direction: In or Out

Description: Allow Citrix

Source Address Destination Address Source Port Destination Port

Exclude (i.e. NOT the choice below)

Type: A set of ports

Portset: Citrix Ports

OK Cancel