

# How to create application rules of the firewall on windows profile

Application Rules - Allows the users to add or modify or remove Custom ruleset for [firewall](#) settings.

Step [1]: Go to Endpoint Manager > CONFIGURATION TEMPLATES > Profiles



Step [2]: Click Create icon and Choose the Create Windows Profile from the drop down menu

The screenshot shows the Endpoint Manager interface. On the left is a navigation menu with categories: DASHBOARD, DEVICES, USERS, CONFIGURATION TEMPLATES (expanded to show Profiles, Alerts, Procedures, Monitors), APPLICATION STORE, APPLICATIONS, SECURITY SUB-SYSTEMS, and SETTINGS. The main content area is titled 'Profiles' and has tabs for 'Profiles' and 'Default Profiles'. Below the tabs are five action buttons: 'Create' (highlighted with a red box), 'Import', 'Export Profile', 'Clone Profile', and 'Delete Profile'. A dropdown menu is open under the 'Create' button, listing options: 'Create Android Profile', 'Create iOS Profile', 'Create OS X Profile', and 'Create Windows Profile' (highlighted with a red box). Below the menu is a table of existing profiles.

	CREATED BY
Antivirus Settings	
Mac profile	
Standard Updates Management profile	
Profiles for updates	
Optimum Windows Profile for ITSM 6.2	admin
Optimum OSX Profile for ITSM 6.2	admin

Step [3]: Enter the Name, Description of the profile and Click the Create button

Create Windows ProfileClose

**Name \***

Advanced Profile for Firewall Settings

**Description**

this is the recommended profile for firewall protection

Create

Step [4]: Click Add Profile Section and Choose Firewall from the drop down

Endpoint Manager Profiles / Advanced Profile for Firewall Settings License Options

Add Profile Section

Export Profile

Clone Profile

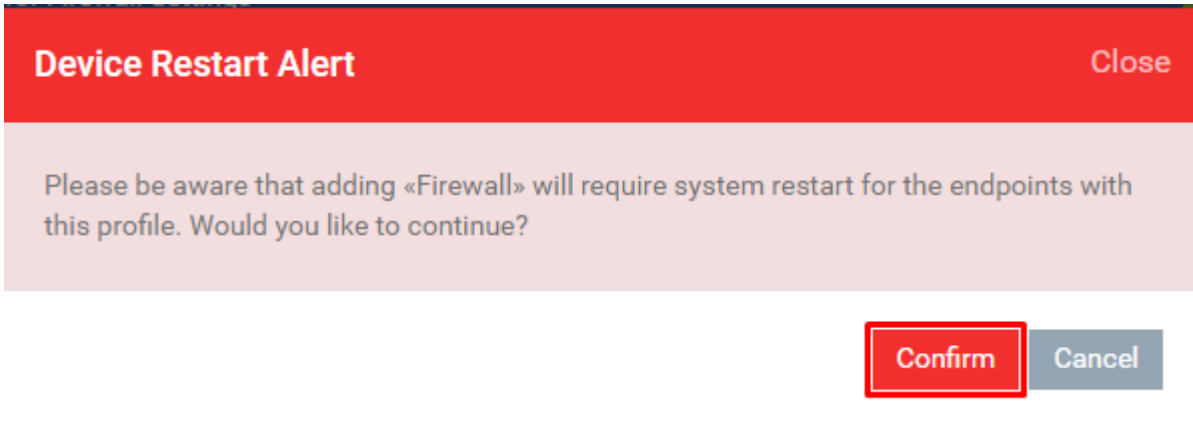
Delete Profile

Make Default

Advanced Profile for Firewall Settings

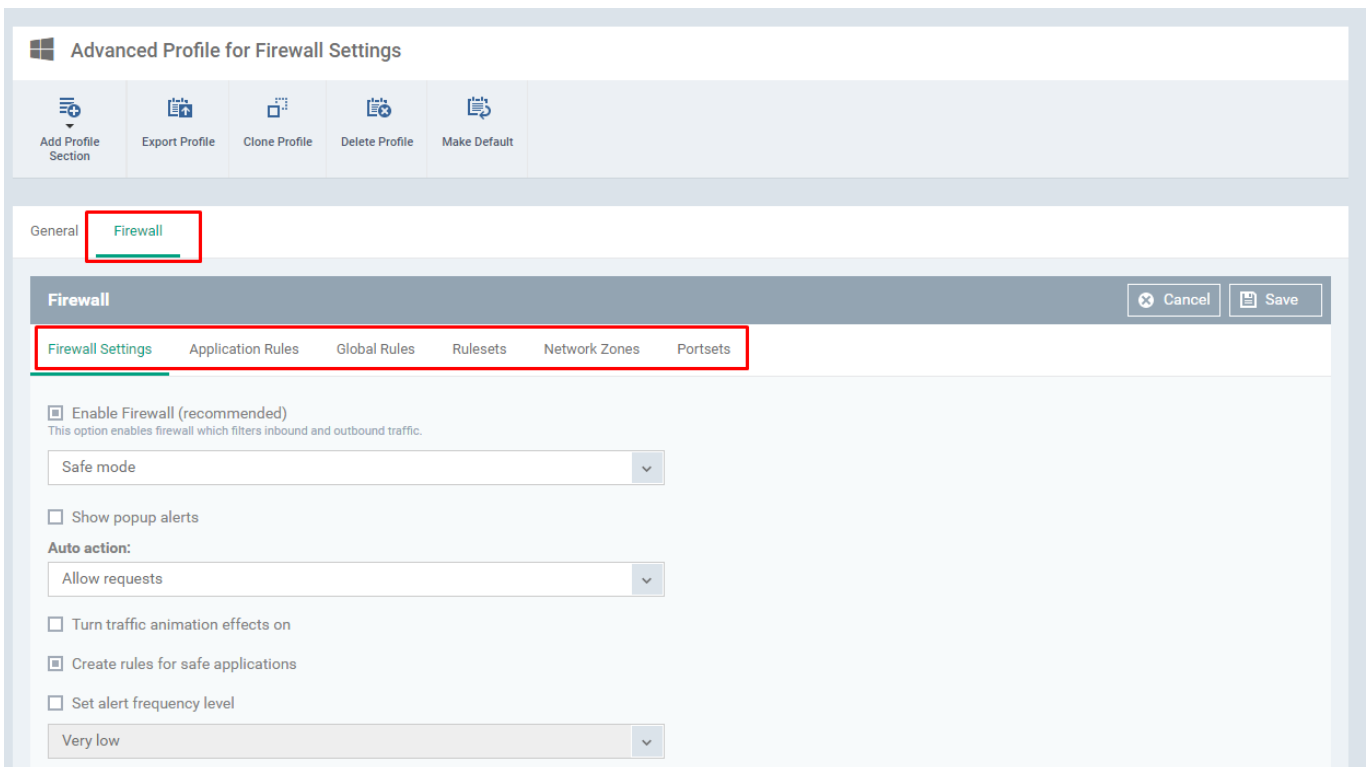
- Antivirus
- Updates
- File Rating
- Firewall
- HIPS
- Containment
- VirusScope
- Valkyrie
- Global Proxy
- Clients Proxy
- Agent Discovering Settings
- UI Settings
- Logging Settings
- Client Access Control
- External Devices Control
- Monitoring
- Procedures

Step [5]: Click the Confirm button

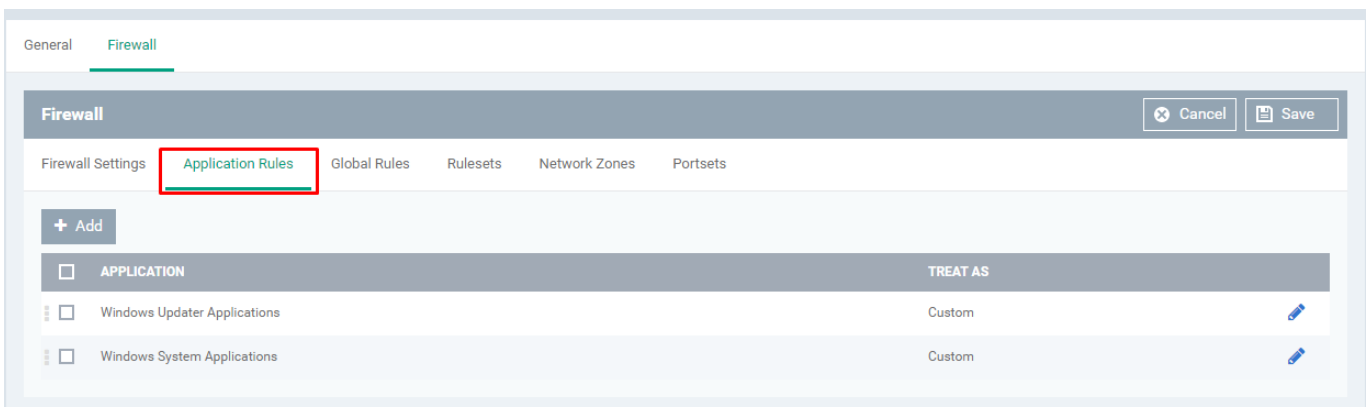


**Note:**

There are some necessary settings to be completed to continue further on advanced [firewall](#) profile such as



Step [6]: Select the tab Application Rules



Step [7]: Click Add button and Fill the form Application Rule, if you want to add more application rules, Otherwise leave the setting as in the beginning.

APPLICATION	TREAT AS
<input type="checkbox"/> Windows Updater Applications	Custom
<input type="checkbox"/> Windows System Applications	Custom

Step [8]: Choose the choice 'using existing target' or 'using new target'

Enter the name if you would like to create a new file group target.

**Application Rule**

Name:  Browse ...

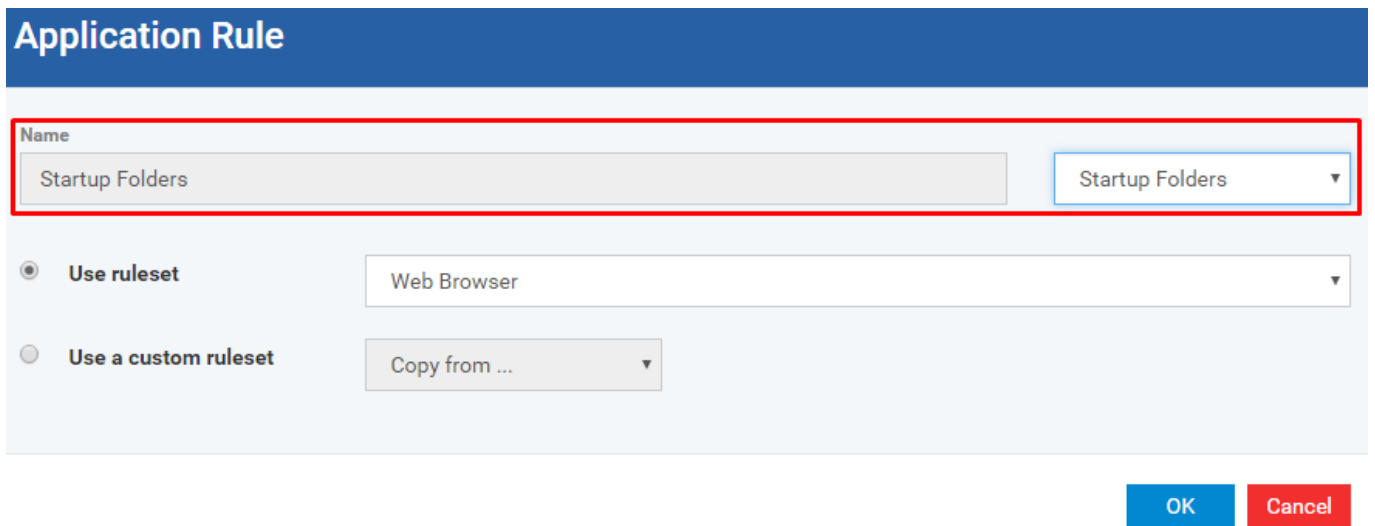
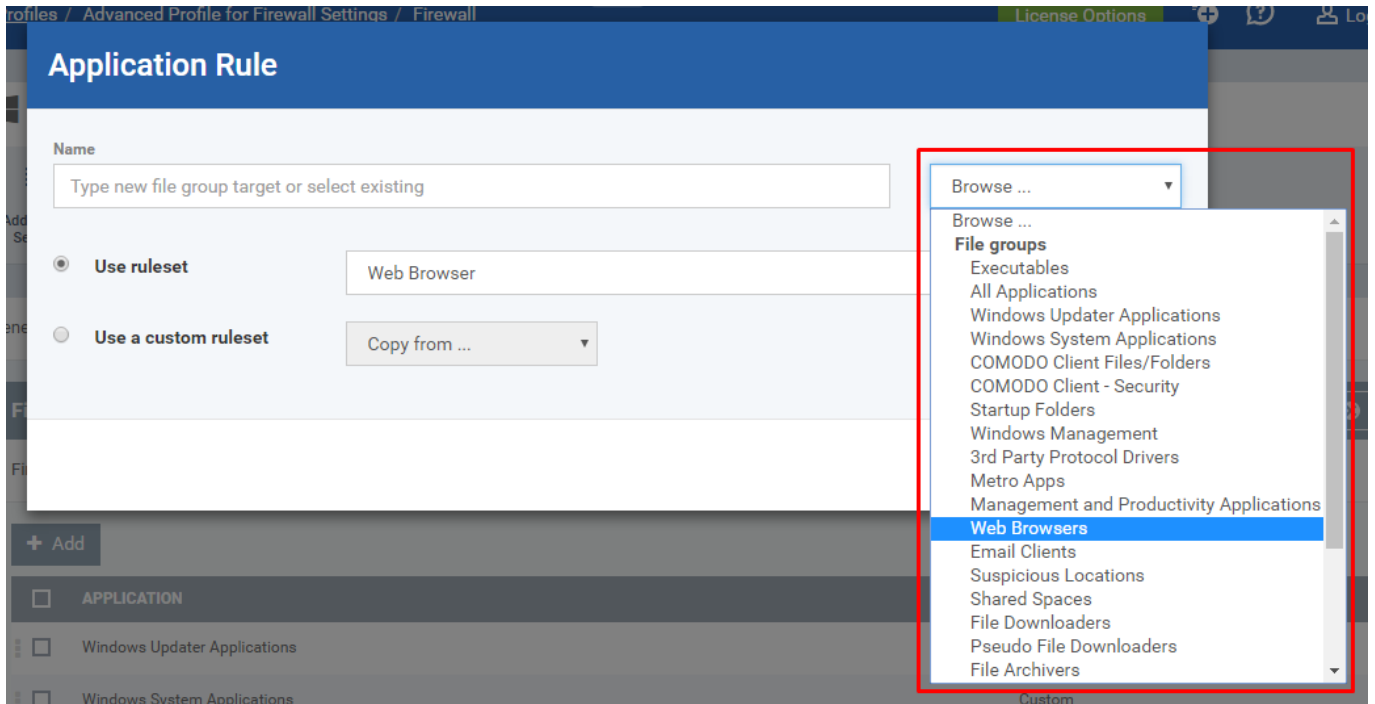
**Use ruleset** Web Browser

**Use a custom ruleset** Copy from ...

OK Cancel

Choose the choice 'using existing target' or 'using new target'

If you would like to use existing target then Click the drop down Browser and Choose the specific option from there



Step [9]: There are two possible options to continue further with adding new ruleset, Choose the option 'Use ruleset' or 'Use a custom ruleset' from the form

1. Use ruleset - predefined ruleset by Comodo
2. Use a custom ruleset - custom ruleset which can be set by the user (you)

If you would like to create a predefined ruleset,

Click the radio button 'Use ruleset'

## Application Rule

Name

Startup Folders

Startup Folders

Use ruleset

Use a custom ruleset

Web Browser

Web Browser

Email Client

Ftp Client

Allowed Application

Blocked Application

Outgoing Only

OK Cancel

Options:

1. Web Browser - all applications belongs to browse the internet, Example: IE, Firefox, Chrome, Opera, and etc.
2. Email Client - all applications belongs to email client interface, Example: Thunderbird, and etc.
3. FTP Client - all applications belongs to FTP interface, Example: FileZilla, and so on
4. Allowed Application - all applications which are set to be allowed
5. Blocked Application - all applications which are set to be blocked
6. Outgoing Only - all applications which are set to be allowed for outgoing connection

Choose application category from the drop down and click OK button

## Application Rule

Name

Startup Folders

Startup Folders

Use ruleset

Web Browser

Use a custom ruleset

Copy from ...

OK Cancel

If you would like to copy from the existing rulesets,

Click the radio button 'Use a custom ruleset' and Click 'Copy from...!' drop down

## Application Rule

Name  
Startup Folders Startup Folders

Use ruleset

Use a custom ruleset

+ Add Rule

RULES

Copy from ...  
Copy from ...  
Ruleset  
Another application

OK Cancel

Options:

1. Ruleset - Which helps to copy from desired existing predefined rulesets
2. Another Application - Which helps to copy from desired existing user-defined rulesets

If you want to use predefined Ruleset then Choose Ruleset from the 'Copy from...!' dropdown

## Application Rule

Name  
Startup Folders Startup Folders

Use ruleset

Use a custom ruleset

+ Add Rule

RULES

Ruleset

Please, select ...  
Please, select ...  
Web Browser  
Email Client  
Ftp Client  
Allowed Application  
Blocked Application  
Outgoing Only

OK Cancel

Choose desired predefined ruleset from the drop down. Example: Web Browser

# Application Rule

Name

Startup Folders

Startup Folders

Use ruleset

Use a custom ruleset

Copy from ...

+ Add Rule

RULES

- ✓ Allow Access to Loopback Zone
- ✓ Allow Outgoing HTTP Requests
- ✓ Allow Outgoing FTP Requests
- ✓ Allow Outgoing FTP-PASV Requests
- ✓ Allow Outgoing DNS Requests
- ⚠ Block and Log All Unmatching Requests

OK

Cancel

Explanation:

From the table, you can add or remove rules or you can modify a specific rule from the table

If you want to add rules then click Add Rule button

## Application Rule

Name

Startup Folders

Startup Folders

Use ruleset

Use a custom ruleset

Copy from ...

+ Add Rule

RULES

Allow Access to Loopback Zone

Allow Outgoing HTTP Requests

Allow Outgoing FTP Requests

Allow Outgoing FTP-PASV Requests

Allow Outgoing DNS Requests

Block and Log All Unmatching Requests

OK

Cancel

Fill the Firewall Rule form and Click OK button to submit

## Firewall Rule

Action

Allow

Log as Firewall event if this rule is fired

Protocol

TCP or UDP

Direction

In or Out

Description

this is for global rule set for TCP or UDP

Source Address

Destination Address

Source Port

Destination Port

Exclude (i.e. NOT the choice below)

Type

Any address

OK

Cancel

Explanation:

Action - Allows setting the action that firewall would take over the rule

1. Allow - If chosen, which allows the connection
2. Block - If chosen, which blocks the connection
3. Ask - If chosen, which asks you (user) to confirm the connection to be allowed or blocked

Log as Firewall event if this rule is fired - Can be enabled or disabled for logging the event into Firewall Events when it is triggered

Protocol - Allows setting the type of protocol for the rule

1. TCP - If chosen, the rule applied only for TCP connection
2. UDP - If chosen, the rule applied only for UDP connection
3. TCP or UDP - If chosen, the rule applied only for TCP or UDP connection
4. ICMP - If chosen, the rule applied only to ICMP connection
5. IP - If chosen, the rule applied only for IP connection

Direction - Allows setting the direction of the connection

1. In - Incoming connection
2. Out - Outgoing connection
3. In or Out - Either Incoming or Outgoing connection

Description - Allows describing the rule

Source Address - Allows you to apply the rule for the Address of the device that tries to access your endpoint

Destination Address - Allows you to apply the rule for the Address of the device that your endpoint tries to access it

# Firewall Rule

**Action**   Log as Firewall event if this rule is fired

**Protocol**

**Direction**

**Description**

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

Exclude (i.e. NOT the choice below)

**Type**

- Any address
- Any address**
- Host name
- IPv4 address range
- IPv4 single address
- IPv4 subnet mask
- IPv6 single address
- IPv6 subnet mask
- MAC address
- Network zone

Options:

Exclude - If enabled, allows to set up devices to be excluded from the rule

Exclude (i.e. NOT the choice below)

**Type**

Type - Types of the Address of the device

Any address - any devices

Exclude (i.e. NOT the choice below)

**Type**

Hostname - device that has the same name of hostname

**Type**

**Host**

IPv4 address range - device from the range of IP addresses

<b>Type</b>	IPv4 address range
<b>Start IP</b>	10.108.51.100
<b>End IP</b>	10.108.51.120

IPv4 single address - device from the same IP address

<b>Type</b>	IPv4 subnet mask
<b>IP</b>	10.108.51.100
<b>Mask</b>	255.255.255.0

IPv6 single address - device from the same IP address

<b>Type</b>	IPv6 single address
<b>IP</b>	2a02:1788:4ff:c330:2147:180c:29b:f9bf

IPv6 single address - device from the same IP address

<b>Type</b>	IPv6 subnet mask
<b>IP</b>	2a02:1788:4ff:c330:2147:180c:29b:f9bf
<b>Mask</b>	255.255.255.0

MAC address - device that has the same MAC address

<b>Type</b>	MAC address
<b>MAC address</b>	18:36:F3:98:4F:9A

Network zone - device that belongs the same network zone

<b>Type</b>	Network zone
<b>Network zone</b>	<ul style="list-style-type: none"> <li>Loopback Zone</li> <li style="background-color: #007bff; color: white;">Loopback Zone</li> </ul>

Source Port - Allows you to apply the rule for the port number or ranges of the device that tries to access your endpoint

Destination Port - Allows you to apply the rule for the port number or ranges of the device that your endpoint tries to access it

Options:

Exclude - If enabled, allows to set up the port number or range to be excluded from the rule

Exclude (i.e. NOT the choice below)

Type

- Any
- A port range
- A set of ports
- A single port
- Any

A port range - port from the range of ports

Type: A port range

Start port: 1

End port: 65535

A set of ports - port from the set of ports

Type: A set of ports

Portset

- HTTP Ports
- HTTP Ports
- POP3/SMTP Ports
- Privileged Ports

A single port - port which is same of the given port

Type: A single port

Port: 1

Any - any port

Type: Any

Check whether you have the specified rule and Click OK button

# Application Rule

Name

Startup Folders

Startup Folders

Use ruleset

Use a custom ruleset

Copy from ...

+ Add Rule

RULES

<input type="checkbox"/>	✓ Allow Access to Loopback Zone	
<input type="checkbox"/>	✓ Allow Outgoing HTTP Requests	
<input type="checkbox"/>	✓ Allow Outgoing FTP Requests	
<input type="checkbox"/>	✓ Allow Outgoing FTP-PASV Requests	
<input type="checkbox"/>	✓ Allow Outgoing DNS Requests	
<input type="checkbox"/>	⊘ Block and Log All Unmatching Requests	
<input type="checkbox"/>	✓ this is the rule to allow in or out connection form the specified device and from the specified port - protocol tcp or ip	

OK

Cancel

Step [10]: Check whether you have the application rule on Application Rules and Click Save button

Advanced Profile for Firewall Settings

Add Profile Section | Export Profile | Clone Profile | Delete Profile | Make Default

General | **Firewall**





Firewall Settings | **Application Rules** | Global Rules | Rulesets | Network Zones | Portsets

+ Add

APPLICATION	TREAT AS
<input type="checkbox"/> Windows Updater Applications	Custom
<input type="checkbox"/> Windows System Applications	Custom
<input type="checkbox"/> without ruleset and custom ruleset	Custom
<input type="checkbox"/> Startup Folders	Custom

Step [11]: Click Profiles menu and check whether the profile has been added to the table.

Profiles Default Profiles

-  Create
-  Import
-  Export Profile
-  Clone Profile
-  Delete Profile



<input type="checkbox"/>	OS	NAME	CREATED BY	CREATED	UPDATED AT
<input type="checkbox"/>	Windows	Malware scan	admin	2017/02/08 04:28:25 PM	2017/02/08 04:37:22 PM
<input type="checkbox"/>	Windows	<u>Advanced Profile for Firewall Settings</u>	admin	2017/02/08 04:20:22 PM	2017/02/09 05:18:13 PM
<input type="checkbox"/>	Windows	Check updates	admin	2017/02/07 07:20:18 PM	2017/02/07 07:20:18 PM
<input type="checkbox"/>	Windows	security updates	admin	2017/02/07 07:12:11 PM	2017/02/07 07:12:11 PM
<input type="checkbox"/>	Windows	Recommended Antivirus Settings	admin	2017/02/07 03:49:39 PM	2017/02/07 03:49:39 PM
<input type="checkbox"/>	Windows	Antivirus Settings	admin	2017/02/07 02:37:00 PM	2017/02/07 02:37:00 PM
<input type="checkbox"/>	Mac	Mac profile	admin	2017/02/06 08:27:55 PM	2017/02/06 08:27:55 PM
<input type="checkbox"/>	Windows	Standard Updates Management profile	admin	2017/01/31 03:42:25 PM	2017/01/31 07:17:18 PM
<input type="checkbox"/>	Windows	Profiles for updates	admin	2017/01/31 12:06:00 PM	2017/02/07 01:40:47 PM
<input type="checkbox"/>	Windows	Optimum Windows Profile for ITSM 6.2	admin	2016/09/10 01:33:00 PM	Not updated
<input type="checkbox"/>	OSX	Optimum OSX Profile for ITSM 6.2	admin	2016/06/26 12:02:00 PM	Not updated
<input type="checkbox"/>	Windows	Standard Windows Profile for ITSM 6.2	admin	2015/12/26 08:55:29 AM	Not updated
<input type="checkbox"/>	Windows	Hardened Windows Profile for ITSM 6.2	admin	2015/11/16 02:17:43 PM	Not updated
<input type="checkbox"/>	Android	Optimum Android Profile for ITSM 6.2	admin	2015/04/28 05:36:13 PM	Not updated