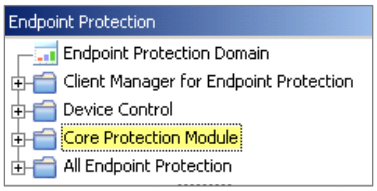
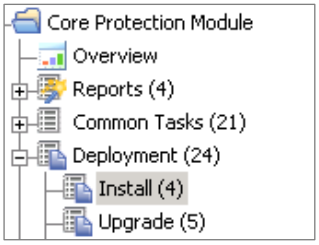
1. Once you subscribe to the Core Protection Module site, click on the *Endpoint Protection* domain in the domain panel to access the Core Protection Module navigation tree.



2. Run the **Install Server Components** task on the BigFix Server to install the CPM server components necessary for providing pattern updates to CPM endpoints. Click the **Deployment** node in the Navigation Tree, then click *Install CPM Server*.



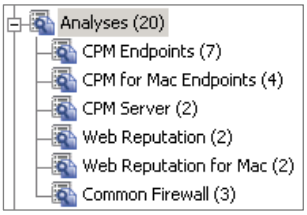
3. Use the **CPM Endpoint Deploy** task under the **Deployment / Install** nodes in the navigation tree to target and deploy CPM to relevant computers.

   Note: There are software and hardware requirements for the installation of CPM components. If computers do not appear applicable for deployment tasks, check the *Ineligible for Install* Fixlets in the Troubleshooting node of the navigation tree to determine potential conflicts.

   Note: To resolve computers relevant to the Ineligible for Install conflicting products Fixlet, use the Uninstall tasks located under Deployment/Uninstall in the navigation tree.

4. Deploy the **Set ActiveUpdate Server Pattern Update Interval** task located under the **Deployment / Install** nodes of the navigation tree. Set this action to run as a policy with periodic re-applicability behavior. Under the Execute tab in the Take Action dialog, select *Never Expire*, *Run Once an Hour*, *On Failure Retry 99 times* and *Reapply an unlimited number of times.*

5. Next, **Activate Analyses**. Click the **Analyses** node in the navigation tree and select analyses *by type,* or select them all at once from the List Panel on the right side of the Console. Right-click on all analyses and select *Activate*.

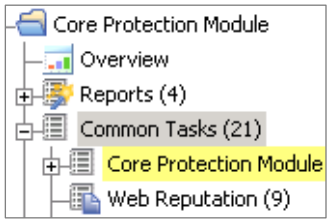


6. CPM's new **Automatic Updates** feature allows you to automatically deliver and apply pattern file updates to your endpoints whenever new patterns are made available by Trend Micro. Check the CPM *User's Guide* for detailed information.

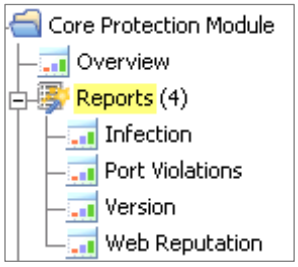
7. Use the **Configuration Wizards** located under the **Configuration** node in the navigation tree to customize your CPM settings:

   - **Global Settings wizard** - configures global scan, virus and spyware settings
   - **Active Update Server Settings wizard** - updates settings from Trend's "cloud" server
   - **Common Firewall wizard** – enables Common Firewall and configure firewall rules
   - **On-Demand Scan Settings wizard -** configures on-demand scan settings
   - **Real-Time Scan Settings wizard -** configures real-time scan settings
   - **Spyware White List wizard** - configures spyware whitelist settings
   - **Web Reputation wizard** – manages your blacklist and whitelist policies and templates

8. Select **Core Protection Module** under the **Common Tasks** node in the navigation tree to start or stop an On-Demand Scan or to upload quarantine or log files to the server.



9. Use the **Reports** node of the navigation tree to view your overall deployment status - **Overview, Infection, Port Violations, Version,** and **Web Reputation**.



10. Use **Web Reports** to view the Top 25 Spyware/Virus reports, endpoint health status, or to configure email notifications. To get to Web Reports, click the *Tools* pull-down menu at the top of the Console and select *Launch Web Reports.*