COMODO
Creating Trust Online®

Comodo
Endpoint Security Manager
Windows Phone Console

Software Version 2.0

Administrator Guide

Version Guide 2.0.111114

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1.Comodo Endpoint Security Manager - Windows Phone Console - Introduction

The mobile console for the Comodo ESM server provides views of the statuses of antivirus updates, policy compliance and malware detections for all endpoints protected by Comodo Internet Security antivirus and firewall software and managed by Comodo Endpoint Security Manager 2.0 Business Edition. It is used to monitor system status, computer properties and offers an ability to resolve the most common day-to-day issues.

Guide Structure

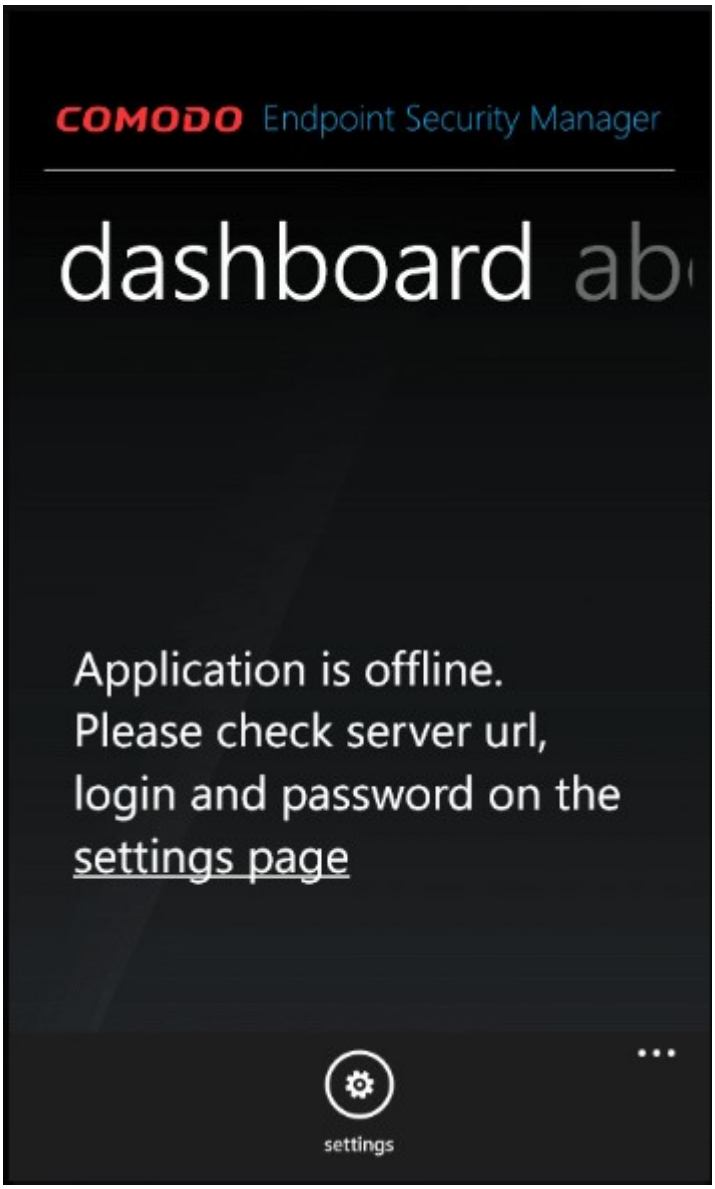
This guide is intended to take you through the mobile console for the Comodo ESM server and is broken down into the following main sections.

- **Startup Screen** - Allows you to the current running status of the CESM Service.
- **Settings Page** - Contains connection, application and notification settings required for the application to operate.
- **Dashboard Page** - Features a set of highly configurable, dynamic tiles that let system administrators create the control panel of their choice.
- **Computers Page** - Plays a key role in the ESM Administrative Console interface by providing system administrators with the ability to import, view and manage networked computers.
- **About Page** - Get the information on client version, server version and license information.
- **Reports** - Generate highly informative, graphical summaries of the security and status of managed endpoints.

2.Startup Screen

To start the application, double click on the setup file. On the first launch, by default, the application will not be connected to the server and must be **configured**. Once configured, a “Connecting…” screen will be displayed, followed by the **Dashboard Pane**, at which point you will be able to view the status of all managed endpoints.

The un-configured Dashboard contains a hint about lack of server host name and user credentials along with a link to the settings page. You can access the 'Settings' page by tapping this link or by tapping '. . .' to reveal the 'settings' button in the application bar.

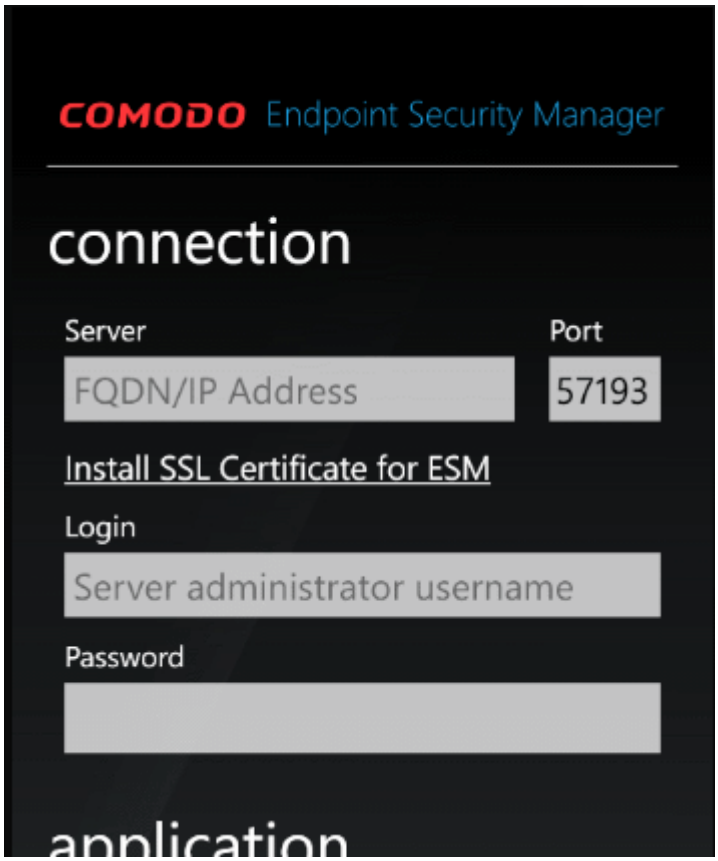


After the server host name/IP address and administrator credentials (the same username and password used to access the ESM server from a browser-based console) are provided, the application will try to automatically connect every time upon launch.

3.Settings Page

The settings page contains connection, application and notification settings required for the application to operate. There are two ways that you can configure access to the ESM server:

- Enter the fully qualified host name or an IP address of the server.
- Enter an Internet accessible IP address.



Note: The certificate is used to create an SSL connection between the phone and the server. It has associated host names or IP addresses that are listed in the configuration tool. The certificate file itself can be installed using any server host name, but the SSL connection can be established only using host names that are listed in the ESM server configuration tool.

- Click 'Save' to save your settings and initiate the connection with the ESM server. While the application is connected...

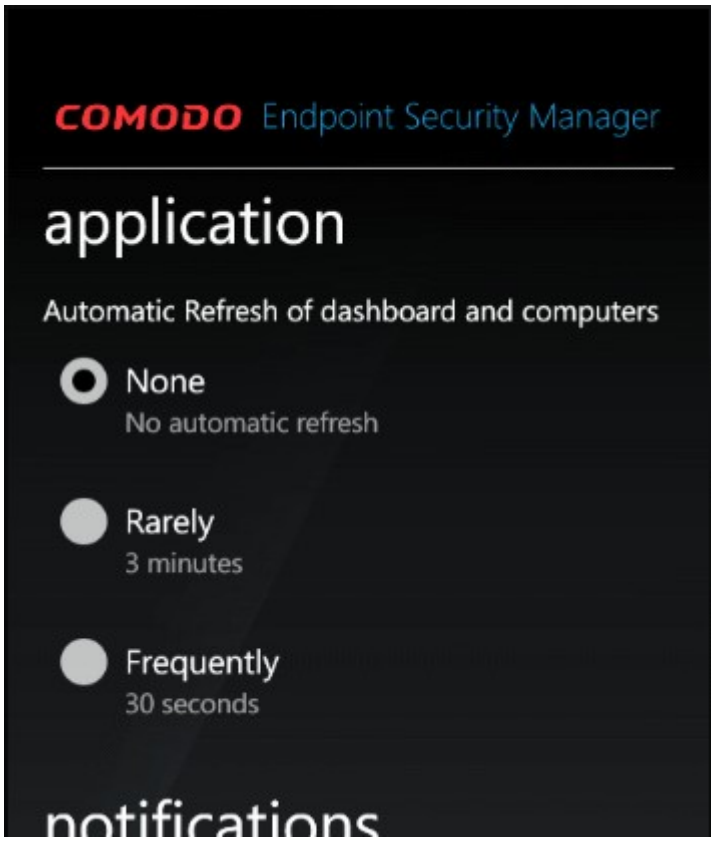
Note: Only Internet-accessible fully-qualified host names or IP addresses will be able resolved by the Windows Phone 7 correctly.

- Leave the default server http port number as 57193, if it wasn't changed in the Configuration Tool. Otherwise enter the correct http port. The application will automatically discover the secure https port.
- Tap on the "Install SSL certificate for ESM" link if the server does not have a valid public certificate. If the configured server address and port are correct (and the server is online) then the phone's web browser will open, and the message "Tap to open the file CesmSvc.cer" will appear.
    - Tap the icon to install the certificate. After it is successfully installed click the phone's hardware 'Back' button to return to the ESM application.
- Enter ESM server administrator user name and password in the 'Login' and 'Password' fields. This is the same credentials used to manage the server in the browser-based console.
- The application is now ready for connection with the server. Tap the 'Save' button to connect.

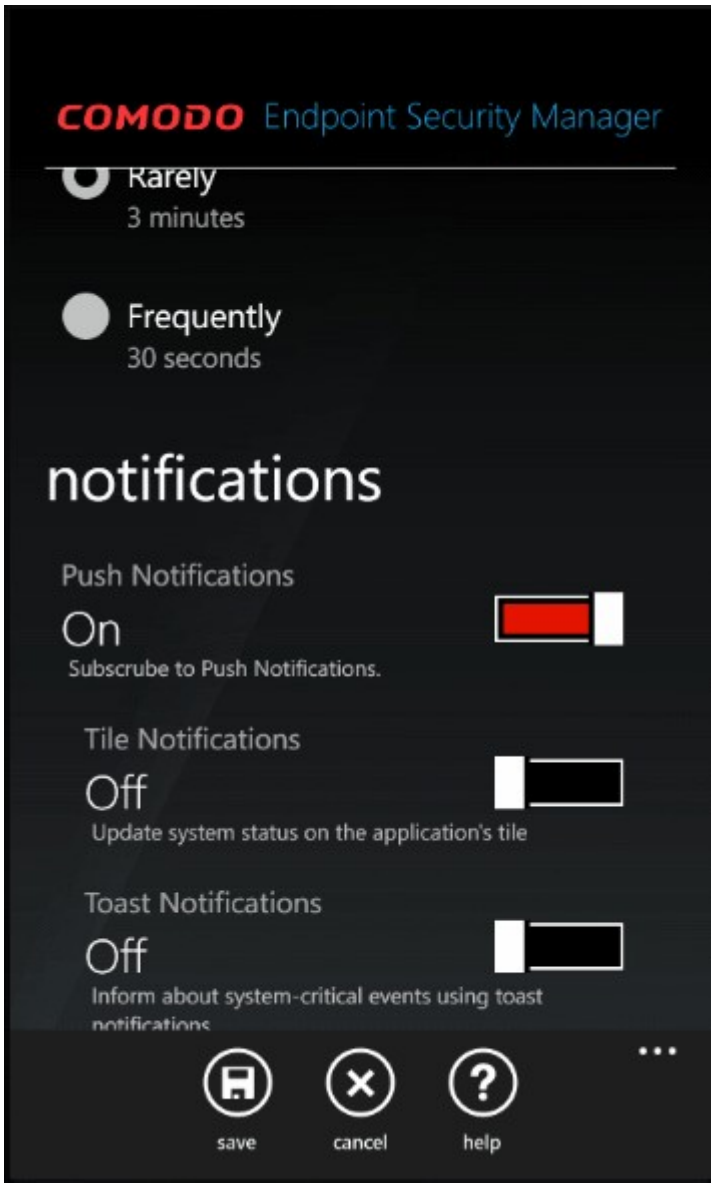
After successful connection, the settings will be saved and the dashboard will appear.

Additional settings:

- Automatic refresh - Set the rate at which dashboard data and computer list are to be refreshed while connected.



- Push Notifications - Use Windows Phone 7 Notification system to notify you about server events even when the application is closed.
    - Tile Notifications - Notify about system issues on the application tile. Note: application tile must be pinned to phone's start screen.
    - Toast Notifications - Notify about system issues using pop-up messages (like voicemail and text messages you receive on your phone).



While the application is connected to the ESM server the main screen consists of three pages: **Dashboard**, **Computers** and **About**.

4.Dashboard Page

The dashboard consists of four indicators:

- Outdated
- Malware Found
- Non-Compliant
- Online

'Outdated', 'Malware Found', 'Non-Compliant' indicators represent the number of issues in the network. They turn red if the number of identified issues is larger than zero.

Each of the indicators on the Dashboard is clickable and lead to corresponding detailed reports.

- **Outdated** - Shows the number of endpoints with outdated virus signature database. Clicking this tile will open the antivirus updates report from which you can update the relevant machines (the 'Update' button at the bottom of the screen enable automatic update of any and all outdated machines).
- **Malware Found** - Shows the total number of viruses identified on all managed endpoints. Clicking this tile will open a summary screen that lists the names of the malware found and the affected endpoints (the 'run a scan' button enables to automatically kick off a scan on infected endpoints).
- **Non-Compliant** - Represents a summary of endpoints that are not compliant with their assigned security policy. If the endpoint is in 'Remote Mode' then non-compliance is 'auto-corrected' by CESM as soon as it is detected (it will push the correct policy back onto the machine). If the endpoint is in 'Local Mode' then it will retain non-compliant status until the administrator switches back to remote mode (or clicks the Reapply button at the bottom of the screen). The endpoints applied with 'Locally Configured' policy will always be retained in Compliant status as CESM does not enforce any policy compliance on to them.
- **Online** - Shows a summary of endpoints that are currently online and connected to CESM locally or via the Internet.

To refresh the data, click the ellipsis (...) button.

5.Computers

The 'Computers' page can be accessed by swiping left from the dashboard page. It provides you with the list of computers with their properties:

- Status - Agent status (Online/Offline), CIS (Comodo Internet Security) administration mode (Remote/Local).
- IP Address - IP Address of the endpoint.
- Local Policy (or Internet Policy) - Shows the name of local (or Internet) policy applied to the computer.
- Policy Status - Shows OK or Non-Compliant depending upon its security policy compliance
- Group - Shows the name of the group to which this endpoint belongs.

Press any endpoint listed on the computers screen to run the **Computer Details report** showing additional information about the endpoint.

Press and hold a computer in the list to open a menu of options that includes:

- 'Run a Scan' to force a scan on the endpoint
- 'Update Antivirus Database' to force an update of the virus definitions
- 'Force Remote Mode' to return a computer in local administration mode to be remotely managed.

Additional properties appear when a virus scan or AV base update is running.

- AV Scan: Status of the antivirus scan performed on the endpoint.
- AV Update: Status of the antivirus database update process on the endpoint.

The following buttons on the application bar can be accessed by tapping '. . .' to perform additional operations:

- Refresh button - Refreshes the computers list immediately.
- Settings button – Navigates to the **settings page**.
- Select button – Lets you select computers in the list using checkboxes that appear on the left side of the screen. If any computers are selected this way then AV scanning or AV database update can be launched. In that case 'Run a scan' and 'Update antivirus database' menu items appear in the application bar (below the buttons).
- Search – Opens a search textbox. You can search an endpoint by entering keywords e.g. computer name, group name or online status.

6.About Page

The About page, accessible by swiping left from the Computers page, displays client version, server version and license information when application is connected to the server.

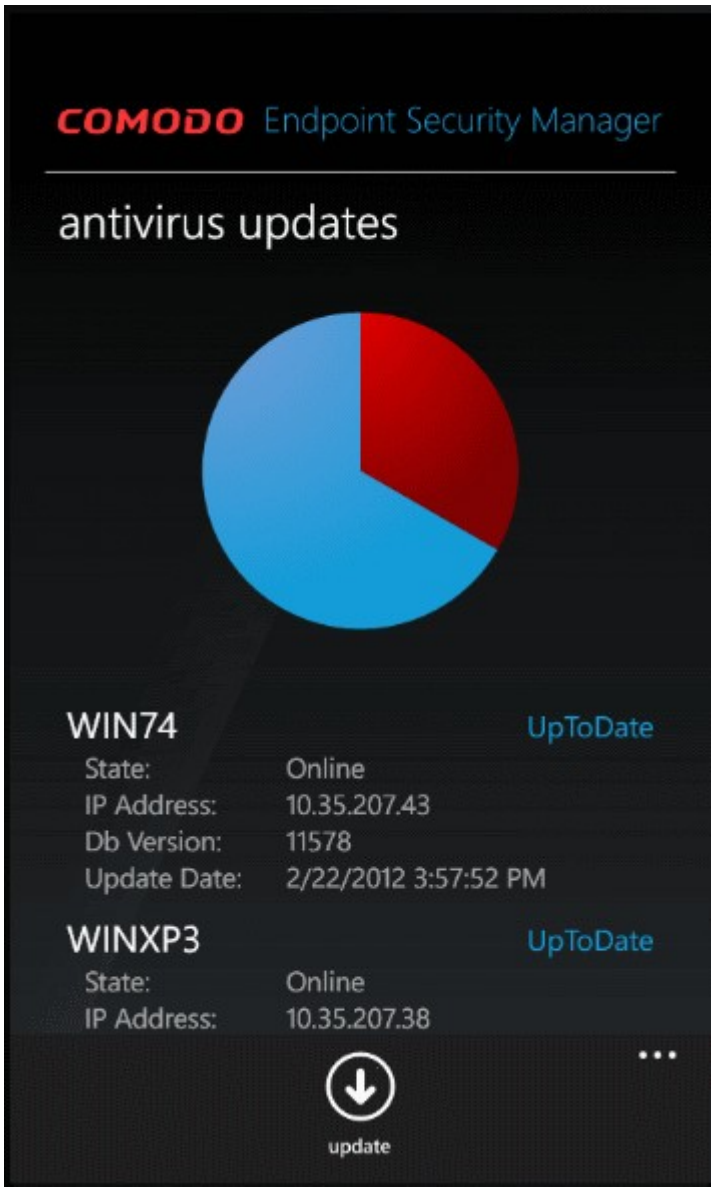
The page also contains links to the online help and the Comodo **support forums** are provided, which will open in the phone's Internet Explorer browser when clicked.

7.Reports

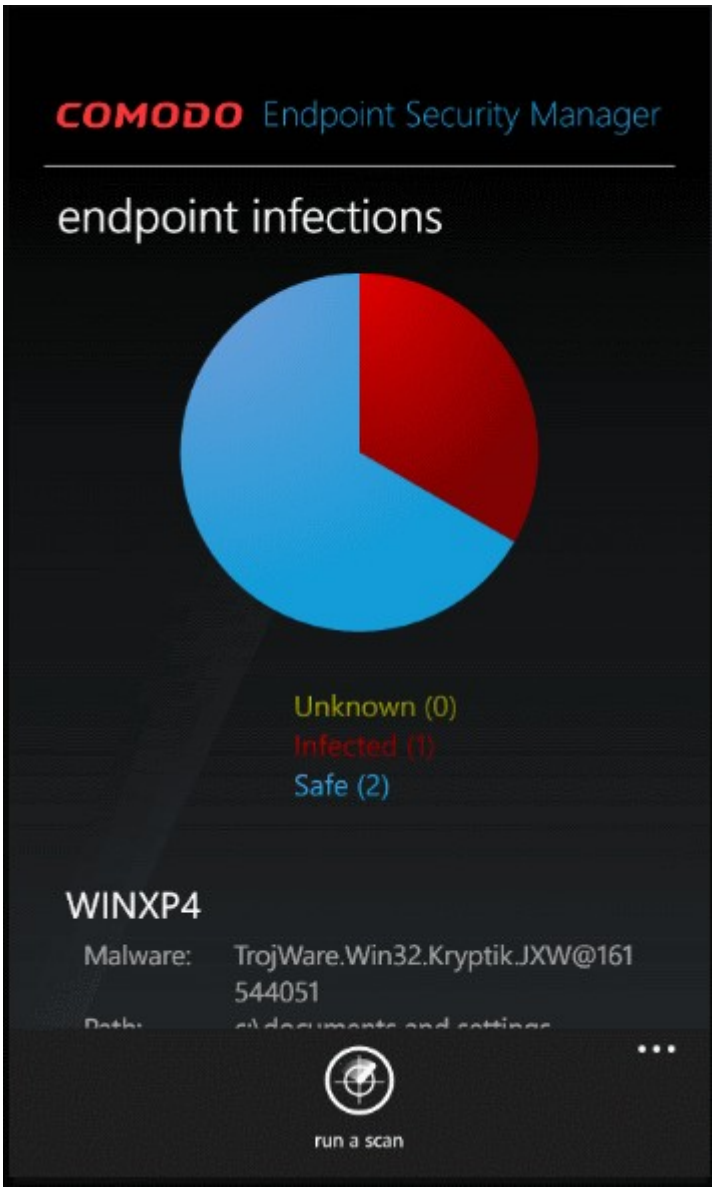
Reports can be accessed in several ways. The common way is to click on **dashboard page** items 'Outdated', 'Malware Found', 'Non-Compliant' and 'Online'. They lead to '**Antivirus updates**', '**Endpoint infections**', '**Policy compliance**' and '**Computer details**' reports accordingly.

The '**Computer details**' report for a specific endpoint can also be accessed by clicking on that endpoint in the 'Computers' page. Reports that represent issues in the system have a remediation button in the application bar, which is displayed by tapping the ellipsis (…).

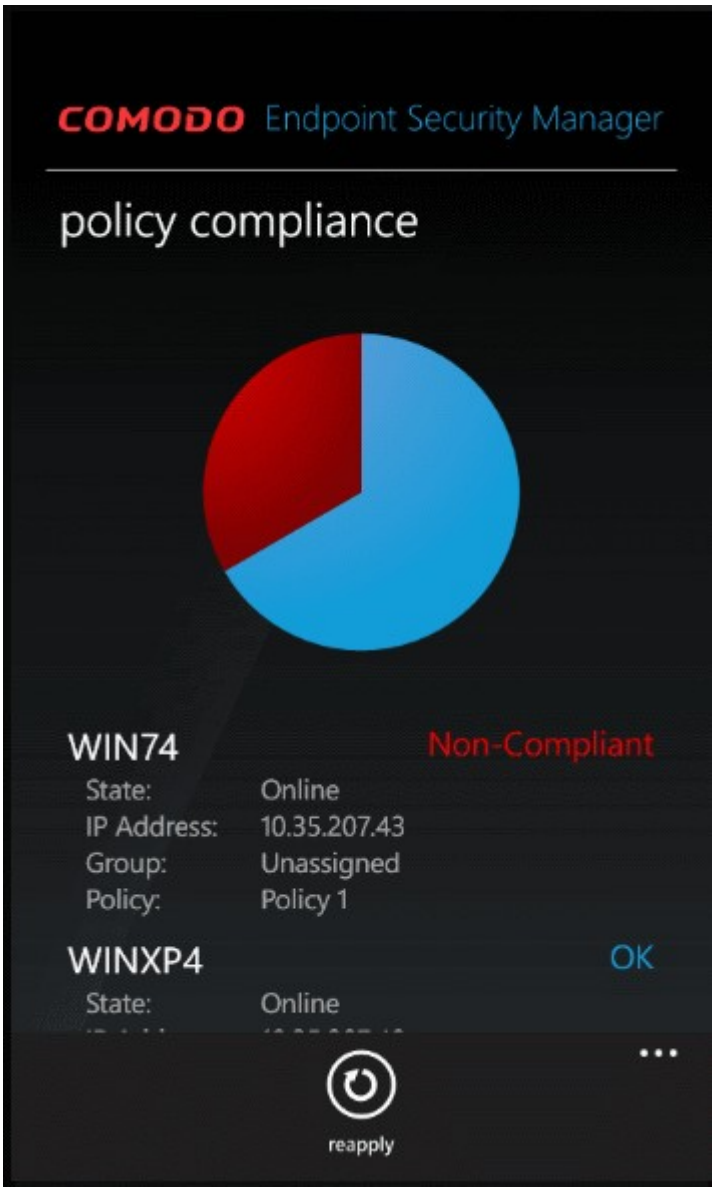
- 'Update' button in the antivirus updates report updates AV databases on all endpoints marked in the report as 'outdated'.



- 'Run a scan' button in the endpoint infections report initializes an automatic system scan on infected endpoints.



- 'Reapply' button in the policy compliance report enforces policy on the non-compliant endpoints by reapplying their currently defined policy.


COMODO Endpoint Security Manager
policy compliance
WIN74
Non-Compliant
State: Online
IP Address: 10.35.207.43
Group: Unassigned
Policy: Policy 1
WINXP4
OK
State: Online
reapply

About Comodo

Comodo® is a leading brand in Internet security. With US Headquarters in New Jersey and global resources in UK, China, India, Ukraine, and Romania, Comodo provides businesses and consumers worldwide with security and trust services, including digital certificates, PCI scanning, desktop security, and remote PC support. Securing online transactions for over 200,000 businesses, and with more than 35 million desktop security software installations, including an award-winning firewall and antivirus software, Comodo is Creating Trust Online®.

To learn more, visit Comodo's website: **www.comodo.com**.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com/**