

Sending Commands Through the Symantec Endpoint Protection Manager

<https://campus.barracuda.com/doc/84313238/>

You can send commands to Symantec Endpoint Protection Manager and clients from within the Symantec Endpoint Protection service module. When commanding is authenticated, the following functionality is enabled:

- on the site-level dashboard, in the Symantec Endpoint Protection Manager area, a Run Live Update link allows you to connect to the Manager to run an update against all endpoints at the site.
- on the device-level dashboard, a Client Management section appears that allows you to run scans and update content on the device.



For this functionality to appear in the service module, you must follow a few steps to authorize communication between Service Center and the Symantec Endpoint Protection Manager.

Authorizing Communication with Symantec Endpoint Protection Manager

Before you begin, you must obtain the following Symantec Endpoint Protection Manager credentials:

- the Endpoint Protection Manager URL, Client ID, and Client Secret that were created for Barracuda Managed Workplace.
- the user name, password, and Endpoint Protection domain to log in to the Endpoint Protection Manager.

If you do not have these credentials, contact your Symantec Endpoint Protection administrator.

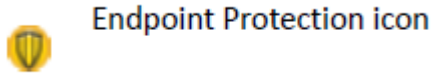
1. In Service Center, click Status and then click Service Modules.
2. Click Symantec Endpoint Protection on the right sidebar.
3. Click the gear icon .
4. In the corresponding fields, provide the following:
 - Symantec Endpoint Protection Manager URL
 - Client ID
 - Client Secret
5. Click Save.
6. A key icon  now appears on the Multi-Site Overview dashboard. Click the key icon.
7. Log in to the Symantec Endpoint Protection Manager by typing the user name, password, and if required the Endpoint Protection domain in the corresponding fields.



Providing Site Level Credentials

The Endpoint Protection Manager URL, Client ID, and Client Secret entered at the multi-site level are

used for all sites managed by the Endpoint Protection Manager. Optionally, you can override these authentication parameters at the site level for sites managed by a different Endpoint Protection Manager.

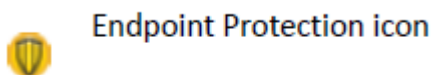
1. On the Central Dashboard, click the Endpoint Protection icon for a site:



2. Click the gear icon .
3. Clear the Inherited From Parent check box. 
4. Enter the Endpoint Protection Manager URL in the corresponding field.
5. Click Save.
6. Click the key icon.
7. Log in to the Symantec Endpoint Protection Manager by typing the user name, password, and if required the Endpoint Protection domain in the corresponding fields.
8. Click Log On.
9. On the Authorization page, click the Authorize button.
10. On the Web Service Application Registration page, make note of the Client ID and Client Secret assigned to the Symantec Endpoint Protection service module.
11. Log out of the Symantec Endpoint Protection Manager.
12. Click Close.
13. Click the gear icon .
14. Enter the new Client ID and Client Secret in the corresponding fields.
15. Click Save.

To Run Live Updates at a Site

1. On the Central Dashboard, click the Endpoint Protection icon for a site:



2. In the Symantec Endpoint Protection Manager area, click the Run LiveUpdate link.
3. A notification message appears at the top of the screen when the LiveUpdate session has successfully started. Click the red X to close the message.

To Scan or Update an Endpoint

1. From the Endpoint Protection site dashboard, in the Network Health Summary section, click one of the endpoint links.
2. From the device list, click the name of the device you want to run commands against.
3. In the Client Management area, click one of the following links:
 - Run Full Scan
 - Run Active Scan
 - Run Custom can

- Update Content
- Update Content and Scan

Figures

1. Symantec - 2.png
2. Symantec - 3.png
3. - 1.png
4. Symantec - 2.png
5. Symantec - 2.png
6. - 1.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.