Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Version of this Document
Download the latest version of this document

To learn more, visit the Check Point Support Center

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 May 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Endpoint Security Web Remote Help SDK

This guide is intended for administrators and application developers who want to use the Endpoint Security external APIs to give third party applications the ability to perform actions related to Endpoint Security management.

It assumes that you have read the *Endpoint Security Administration Guide* and that you have a good understanding of the Endpoint Security product.

The Endpoint Security external APIs let you:

- Perform remote password change or one-time logon for devices encrypted with Full Disk Encryption.
- Perform remote password change for devices encrypted with Media Encryption.

**Prerequisites**

- A release that supports the Web Remote Help SDK must be installed on the Endpoint Security Management Server or on a dedicated Remote Help Server.
- Endpoint Remote Help Server must be enabled on the primary Endpoint Security Management Server or on a dedicated Remote Help Server.
- A Web Remote Help Account must be configured.

For complete instructions on how to activate a Remote Help Server and create Web Remote Help Accounts, see the *Endpoint Security Administration Guide*.

**Service URL**

The service is available by sending a SOAP request to:

https://<Endpoint Remote Help Server IP>/webrh/services/webRHSDK

**Full Disk Encryption Remote Help**

Full Disk Encryption Remote Help is done in two steps and provides these Remote Help options:

- One-Time Logon - Lets users perform one-time logon in Pre-boot.
- Remote Password Change - Lets users change their Pre-boot passwords.

The unique identifier of the Full Disk Encryption module is:

{11D0FF26-D3AC-4FD1-BF36-435F43290C9C}
Remote Help is done in two steps:

1. Step 1 performs login with the information provided in the request using the username, device name, or device id. If the device name and device id were not provided, the last device the user logged into is used.
   Upon success, the first response is returned in the response.

2. In addition to login, which is performed in the same way as in previous step, Step 2 reads the challenge and Remote Help type from the request fields.
   Upon success, the second response is returned in the response.

**Step 1 Request**

The first step requires the information below and upon success it generates the input for the **Response one** field in the Full Disk Encryption client Pre-boot window.

**Step 1 Request Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webrh_user_name</td>
<td>User name for authenticating to Endpoint Security Web Remote Help. Must be of a Web Remote Help account on Endpoint Security Management Server.</td>
</tr>
<tr>
<td>rhbounduser</td>
<td>The name of the Full Disk Encryption user being helped in this format: &lt;domain name&gt;&lt;user name&gt;.</td>
</tr>
<tr>
<td>rhdevicename</td>
<td>The name of the device being accessed with Remote Help. Optional field.</td>
</tr>
<tr>
<td>rhdeviceid</td>
<td>The ID of the device being accessed with Remote Help. Optional field.</td>
</tr>
</tbody>
</table>

**Note** - If device name and device ID are not provided, the last device the user logged into will be used.

**Step 1 Request Structure**

```xml
<REQUEST>
  <WEBRHUSERNAME>webrh_user_name</WEBRHUSERNAME>
  <WEBRHPASSWORD>webrh_password</WEBRHPASSWORD>
  <MODULE guid="{11D0FF26-D3AC-4FD1-BF36-435F43290C9C}"
    <REMOTEHELPINPUT>
      <VERSION>1</VERSION>
      <STEP>1</STEP>
      <USERNAME>rhbounduser</USERNAME>
      <DEVICENAME>rhdevicename</DEVICENAME>
      <DEVICEID>rhdeviceid</DEVICEID>
    </REMOTEHELPINPUT>
  </MODULE>
</REQUEST>
```
To build a step 1 request:

1. Use the XML structure above and fill in the actual values.
2. Flatten the XML to a single line:
   
   ```xml
   <REQUEST><WEBRHUSERNAME>webrh_user_name</WEBRHUSERNAME>…</MODULE></REQUEST>
   ```
3. Escape XML characters and place the result in the `bstrInput` field, in this SOAP message structure:

   ```xml
   <soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/
   xmlns:v1="http://uepm.checkpoint.com/ws/webRHSDK/v1/">
   <soapenv:Header/>
   <soapenv:Body>
   <v1:GetResponseIn>
   <bstrInput>Your XML goes here</bstrInput>
   </v1:GetResponseIn>
   </soapenv:Body>
   </soapenv:Envelope>
   ```

**Step 1 Response**

**Step 1 Response Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>returnValue</td>
<td>An integer value. All return values other than zero are treated as a failure [see error table].</td>
</tr>
<tr>
<td>bstrOutput</td>
<td>The string that should be entered in the <strong>Response one</strong> field in the Full Disk Encryption client Pre-boot window.</td>
</tr>
</tbody>
</table>

**Step 1 Response Example**

```xml
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Body>
  <ns2:GetResponseOut xmlns:ns2="http://uepm.checkpoint.com/ws/webRHSDK/v1/">
   <returnValue>0</returnValue>
   <bstrOutput>6664134953</bstrOutput>
  </ns2:GetResponseOut>
 </soap:Body>
</soap:Envelope>
```

**Step 2 Request**

The second step requires the information below and upon success it generates the input for the **Response two** field in the Full Disk Encryption client Pre-boot window.
Step 1 Request Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webrh_user_name</td>
<td>User name for authenticating to Endpoint Security Web Remote Help. Must be of a Web Remote Help account on Endpoint Security Management Server.</td>
</tr>
<tr>
<td>rhbounduser</td>
<td>The name of the Full Disk Encryption user being helped in this format: &lt;domain name&gt;&lt;user name&gt;.</td>
</tr>
<tr>
<td>rhchallenge</td>
<td>The challenge generated in Full Disk Encryption Pre-boot after typing in response one.</td>
</tr>
<tr>
<td>remotehelptype</td>
<td>The type of Remote Help given: password change or one-time login. Valid values of the element are PASSWORDCHANGE and ONETIMELOGON.</td>
</tr>
</tbody>
</table>

Step 2 Request Structure

```xml
<REQUEST>
  <WEBRHUSERNAME>webrh_user_name</WEBRHUSERNAME>
  <WEBRHPASSWORD>webrh_password</WEBRHPASSWORD>
  <MODULE guid="{11D0FF26-D3AC-4FD1-BF36-435F43290C9C}"
    <REMOTEHELPINPUT>
      <VERSION>1</VERSION>
      <STEP>2</STEP>
      <USERNAME>rhbounduser</USERNAME>
      <CHALLENGE>rhchallenge</CHALLENGE>
      <REMOTEHELPTYPE>remotehelptype</REMOTEHELPTYPE>
    </REMOTEHELPINPUT>
  </MODULE>
</REQUEST>
```

To build a step 2 request:

Follow the steps in “To build a step 1 request”.

Step 2 Response

Step 2 Response Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>returnValue</td>
<td>An integer value. All return values other than zero will be treated as a failure (see error table).</td>
</tr>
<tr>
<td>bstrOutput</td>
<td>The string that should be entered in the <strong>Response two</strong> field in the Full Disk Encryption client Pre-boot window.</td>
</tr>
</tbody>
</table>
Step 2 Response Example

```xml
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:GetResponseOut xmlns:ns2="http://uepm.checkpoint.com/ws/webRHS DK/v1/">
      <returnValue>0</returnValue>
      <bstrOutput>1655380792521104802268618900</bstrOutput>
    </ns2:GetResponseOut>
  </soap:Body>
</soap:Envelope>
```

Media Encryption Remote Help

Media Encryption Remote Help lets users change the offline access password for an encrypted device.

The unique identifier of the Media Encryption module is:

{22A7A4AC-3A28-4A7E-AEA6-252EFB8BA318}

Request

The request requires the information below and upon success it generates the input for the Response field in the Endpoint Security client or the Media Encryption Offline Utility.

Step 1 Request Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webrh_user_name</td>
<td>User name for authenticating to Endpoint Security Web Remote Help.</td>
</tr>
<tr>
<td></td>
<td>Must be of a Web Remote Help account on Endpoint Security Management Server.</td>
</tr>
<tr>
<td>rhbounduser</td>
<td>The name of the device owner being helped in this format: &lt;domain name&gt;&lt;user name&gt;.</td>
</tr>
<tr>
<td>rhchallenge</td>
<td>The challenge generated by the Endpoint Security client or the Media Encryption Offline Utility without spaces.</td>
</tr>
</tbody>
</table>

Request Structure

```xml
<REQUEST>
  <WEBRHUSERNAME>webrh_user_name</WEBRHUSERNAME>
  <WEBRHPASSWORD>webrh_password</WEBRHPASSWORD>
  <MODULE guid="{22A7A4AC-3A28-4A7E-AEA6-252EFB8BA318}"
    <REMOTEHELPINPUT>
      <VERSION>1</VERSION>
      <USERNAME>rhbounduser</USERNAME>
      <CHALLENGE>rhchallenge</CHALLENGE>
    </REMOTEHELPINPUT>
  </MODULE>
</REQUEST>
```
To build a request:

1. Use the XML structure above and fill in the actual values.
2. Flatten the XML to a single line:
   <REQUEST><WEBRHUSERNAME>webrh_user_name</WEBRHUSERNAME>…</MODULE></REQUEST>
3. Escape XML characters and place the result in the bstrInput field, in this SOAP message structure:
   <soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/
   xmlns:v1="http://uepm.checkpoint.com/ws/webRHSK/v1/"
   <soapenv:Header/>
   <soapenv:Body>
     <v1:GetResponseIn>
       <bstrInput>Your XML goes here</bstrInput>
     </v1:GetResponseIn>
   </soapenv:Body>
</soapenv:Envelope>

Response

Response Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>returnValue</td>
<td>An integer value. All return values other than zero are treated as a failure (see error table).</td>
</tr>
<tr>
<td>bstrOutput</td>
<td>The string that should be entered in the Response field in the Endpoint Security client or Media Encryption Offline Utility.</td>
</tr>
</tbody>
</table>

Response Example

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:GetResponseOut xmlns:ns2="http://uepm.checkpoint.com/ws/webRHSK/v1/">
      <returnValue>0</returnValue>
      <bstrOutput>bd1475ca1a57fddbad99596fd7aac0b2d</bstrOutput>
    </ns2:GetResponseOut>
  </soap:Body>
</soap:Envelope>
## Remote Help Error Codes

<table>
<thead>
<tr>
<th>Error code</th>
<th>Error description</th>
</tr>
</thead>
<tbody>
<tr>
<td>102</td>
<td>Invalid XML in input</td>
</tr>
<tr>
<td>105</td>
<td>Failed to get authentication level of user</td>
</tr>
<tr>
<td>108</td>
<td>Failure during authentication</td>
</tr>
<tr>
<td>111</td>
<td>Invalid module tag in XML</td>
</tr>
<tr>
<td>303</td>
<td>Invalid Remote Help input</td>
</tr>
<tr>
<td>304</td>
<td>Device name was not found</td>
</tr>
<tr>
<td>311</td>
<td>Invalid Remote Help type given. Valid values are PASSWORDCHANGE and ONETIMELOGIN</td>
</tr>
<tr>
<td>312</td>
<td>Invalid challenge contents</td>
</tr>
<tr>
<td>313</td>
<td>No user name in request</td>
</tr>
<tr>
<td>315</td>
<td>Invalid step, valid values are 1 and 2</td>
</tr>
<tr>
<td>316</td>
<td>Failed to generate response (Internal error)</td>
</tr>
<tr>
<td>317</td>
<td>Unsupported Remote Help version</td>
</tr>
<tr>
<td>500</td>
<td>Internal error</td>
</tr>
<tr>
<td>501</td>
<td>Service not available</td>
</tr>
</tbody>
</table>