# ZENworks Endpoint Security Management - VPN Enforcement

December 2016

This document provides test scenarios that show you how to use ZENworks Endpoint Security Management to initiate a VPN session when a device is in an unknown location and also lock down the firewall to block all network traffic except for VPN server traffic.

# 1 Prompting a User to Initiate a VPN Session When in an Unknown Location

As the ZENworks administrator, you want mobile users to use VPN when they are in unsecure locations. The following steps help you import a predefined VPN Enforcement policy that prompts users to start a VPN session whenever their device is in the default Unknown location.

**1** Import the Firewall policy:

**1a** Copy the following files to a directory on the ZENworks Primary Server:

- `Location-Assignment.xml`
- `VPN-Session-Prompt.xml`
- `policykey.txt`

When you click a filename, the file will either be opened, saved, or you will be prompted to open or save it. You need to save the file. If it opens, click **File** > **Save**.

If you downloaded the Endpoint Security Resource Kit, you can copy the files from the `PolicyExamples` directory.

**1b** On the Primary Server, open a command prompt, change to the directory where you copied the files, then run the following commands one at a time, entering your ZENworks administrator username and password when prompted:

```
zman epi "Location Assignment" policykey.txt Location-Assignment.xml
```

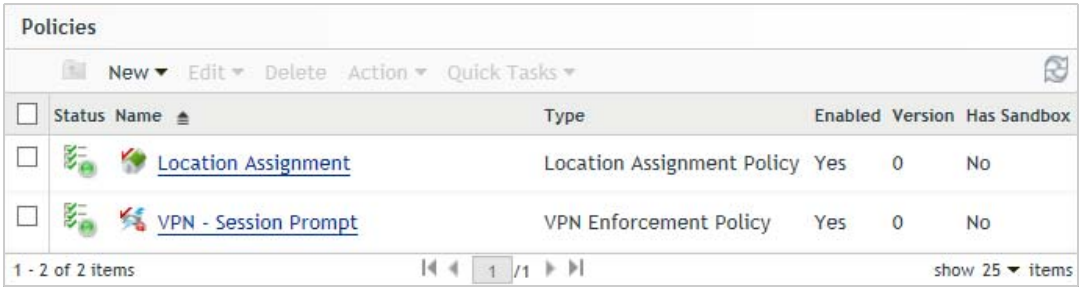
```
zman epi "VPN - Session Prompt" policykey.txt VPN-Session-Prompt.xml
```

A message similar to the following is displayed when a policy is successfully imported:

```
Successfully created the object "Location Assignment" in "/Policies".
```

**2** Validate the policy import:

**2a** In ZENworks Control Center, click **Policies** to display the **Policies** list with the two imported policies.

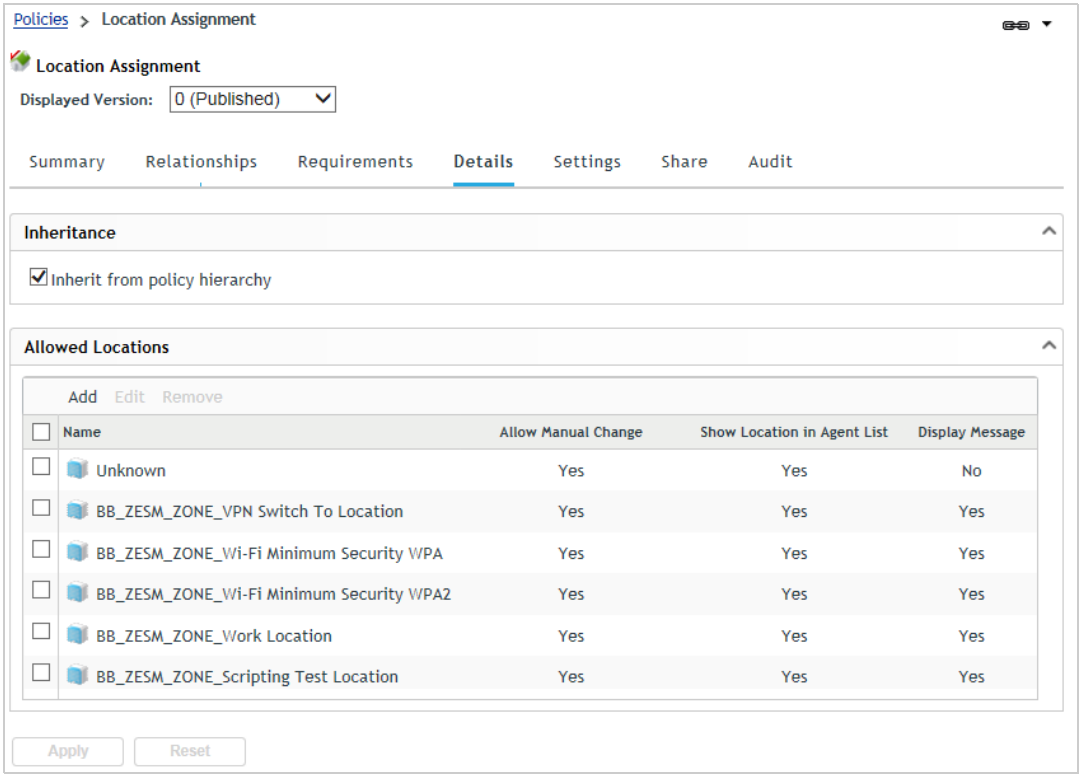



**2b** Click the **Location Assignment** policy, then click its **Details** tab.

There are six locations included in the policy: the standard **Unknown** location and five locations that start with **BB_ZESM_ZONE**. The **BB_ZESM_ZONE** locations were imported with the policy and added as locations in your zone. If you go to the **Locations** page (**Configuration** > **Locations**), you will see them listed.

For this test scenario, only the **Unknown** and **BB_ZESM_ZONE_VPN Switch to Location** locations are used. The other locations are used with the test scenarios for other policies (Wireless, USB, and Scripting).

The locations do not include any network environments, which means that the only way a device can switch to one of the locations is for the device's user to manually change to the location. For this reason, each location is configured to appear in the **Security Locations** list (available when right-clicking the ZENworks icon on the device) and to allow the user to manually change to the location.



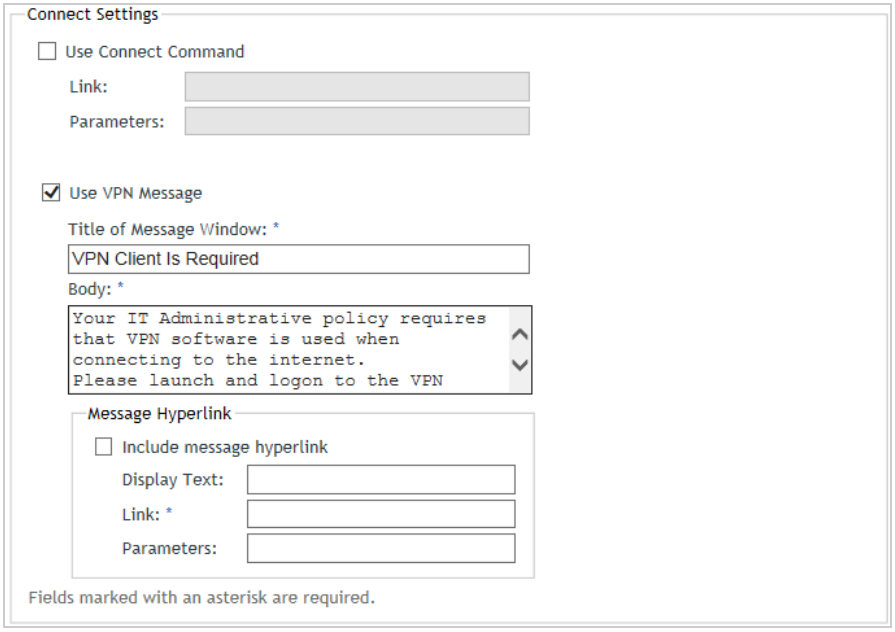

**2c** Return to the **Policies** list.

**3** View the **VPN - Session Prompt** policy to see how it is configured:

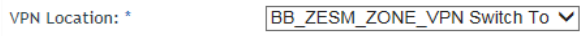
**3a** Click the **VPN - Session Prompt** policy, then click its **Details** tab.

The **Trigger Locations** list includes the **Unknown** location. This causes the policy to be launched whenever the device moves into the **Unknown** location.


The **Connect Settings** panel contains the message that will be displayed prompting the user to initiate a VPN session:




The **VPN Location** displays the switch-to-location. This location can be configured with other policies you want enforced (such as the restrictive Firewall policy explained in the next scenario, Enforcing a Restrictive Firewall During the VPN Session) while the device remains in the VPN location. For this scenario, the VPN location (**BB_ZESM_ZONE_VPN Switch to Location**) does not have any policies that it applies.




**3b** Return to the **Policies** list.

**4** Assign the Location Assignment and VPN policies to a device:

**4a** In the **Policies** list, select the check boxes next to the following policies:

- **Location Assignment**
- **VPN - Session Prompt**

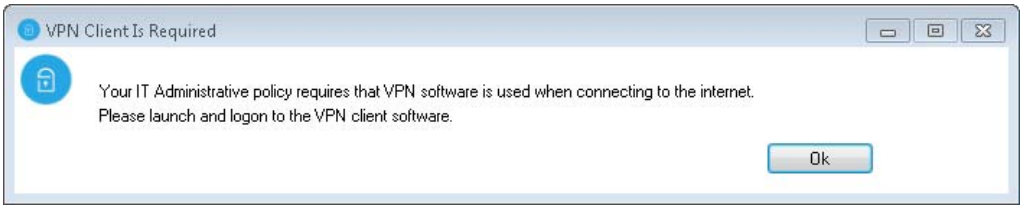
**4b** Click **Action** > **Assign to Device**, then follow the prompts to assign the policies to the appropriate device.

When prompted for the policy conflict method, you can leave it set to **User Precedence**.

**5** Test the VPN policy on the assigned device:

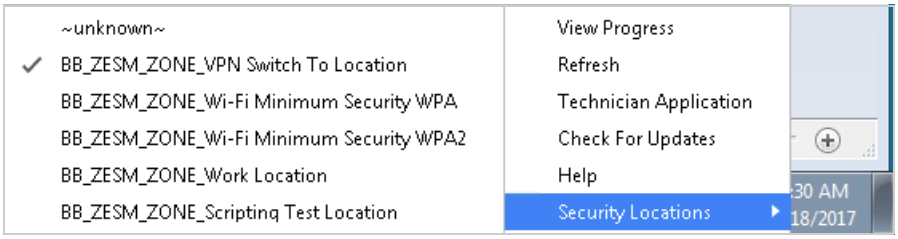
**5a** On the device, right-click the ZENworks icon, then click **Refresh** to retrieve the new policies.

When the device finishes refreshing and the policies are applied, the location is set to the **Unknown** location. The **Unknown** location applies the **VPN - Session Prompt** policy, which causes the location to be switched to the **BB_ZESM_ZONE_VPN Switch to Location** and the following prompt to be displayed:




**5b** Click **OK** to dismiss the prompt.

**5c** Right-click the ZENworks icon > click **Security Location** to see the device is in the **BB_ZESM_ZONE_VPN Switch to Location**.




**6** For the purpose of this test scenario, you need to unassign the **VPN - Session Prompt** policy from the device (in ZENworks Control Center) to exit the **BB_ZESM_ZONE_VPN Switch to Location** on the device.

# 2 Enforcing a Restrictive Firewall During the VPN Session

This scenario assumes that you have already completed the Prompting a User to Initiate a VPN Session When in an Unknown Location scenario. This scenario builds on that scenario, so if you have not completed it, do so before continuing.

As the ZENworks administrator, when a user is in a location that requires a VPN session you want to ensure that all network traffic is passed through the VPN server.

The following steps help you import a predefined restrictive Firewall policy that is enforced whenever the device switches to the VPN location.

**1** Import the Firewall policy:

**1a** Copy the following files to a directory on the ZENworks Primary Server:

- `VPN-Firewall.xml`
- `policykey.txt`

When you click a filename, the file will either be opened, saved, or you will be prompted to open or save it. You need to save the file. If it opens, click **File** > **Save**.

If you downloaded the Endpoint Security Resource Kit, you can copy the files from the `PolicyExamples` directory.

**1b** On the Primary Server, open a command prompt, change to the directory where you copied the files, then run the following command, entering your ZENworks administrator username and password when prompted:

```
zman epi "Firewall - Restrictive VPN" policykey.txt VPN-Firewall.xml
```

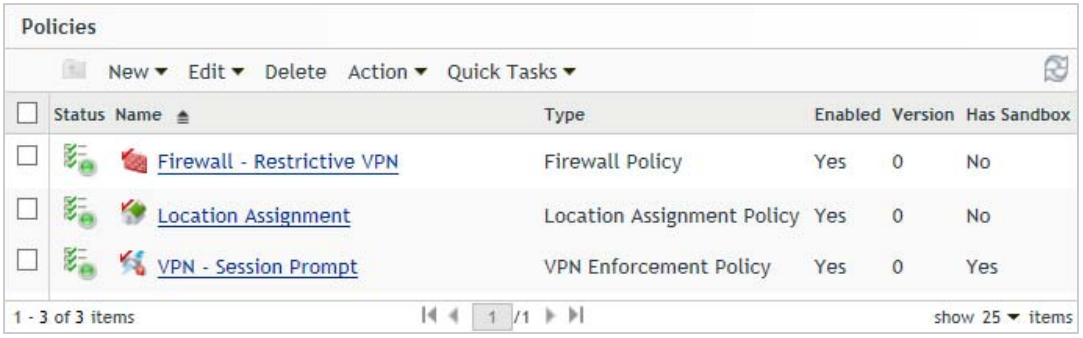
A message similar to the following is displayed when a policy is successfully imported:

```
Successfully created the object "Firewall - Restrictive VPN" in "/
Policies".
```

2 Validate the policy import and modify the Firewall policy as needed:

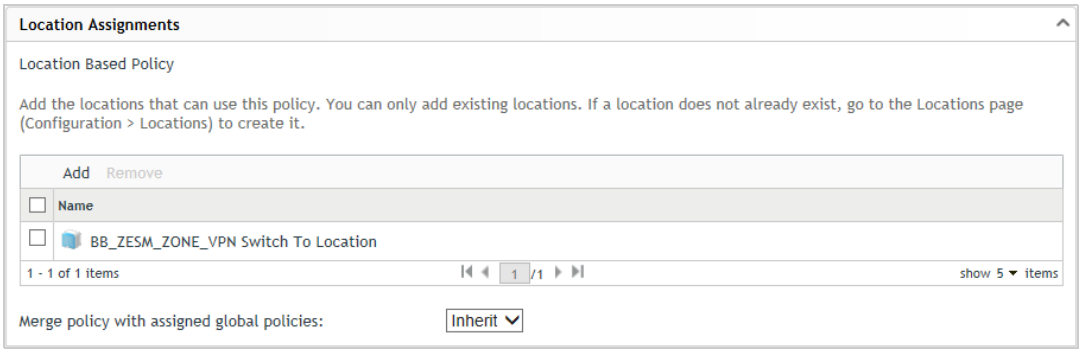
**2a** In ZENworks Control Center, click **Policies** to display the **Policies** list with the imported policies.

The **Firewall - Restrictive VPN** policy is listed along with the **Location Assignment** and **VPN - Session Prompt** policies that were imported as part of the Prompting a User to Initiate a VPN Session When in an Unknown Location scenario.

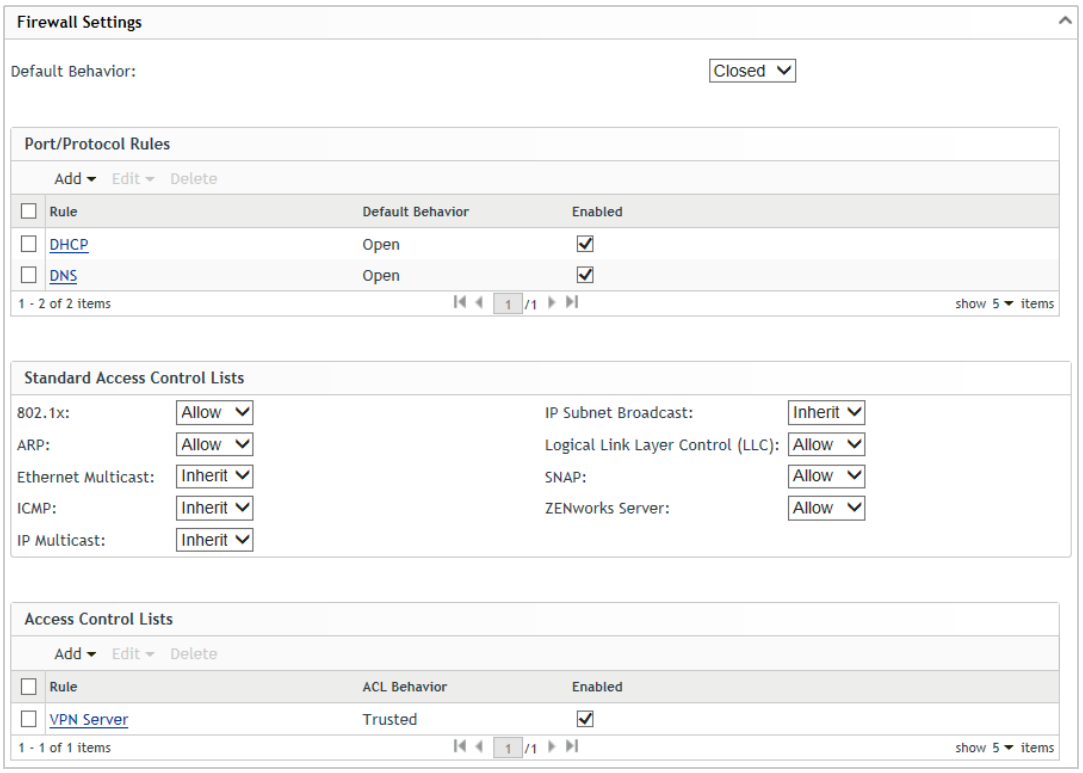



**2b** Click the **Firewall - Restrictive VPN** policy, then click the **Details** tab.

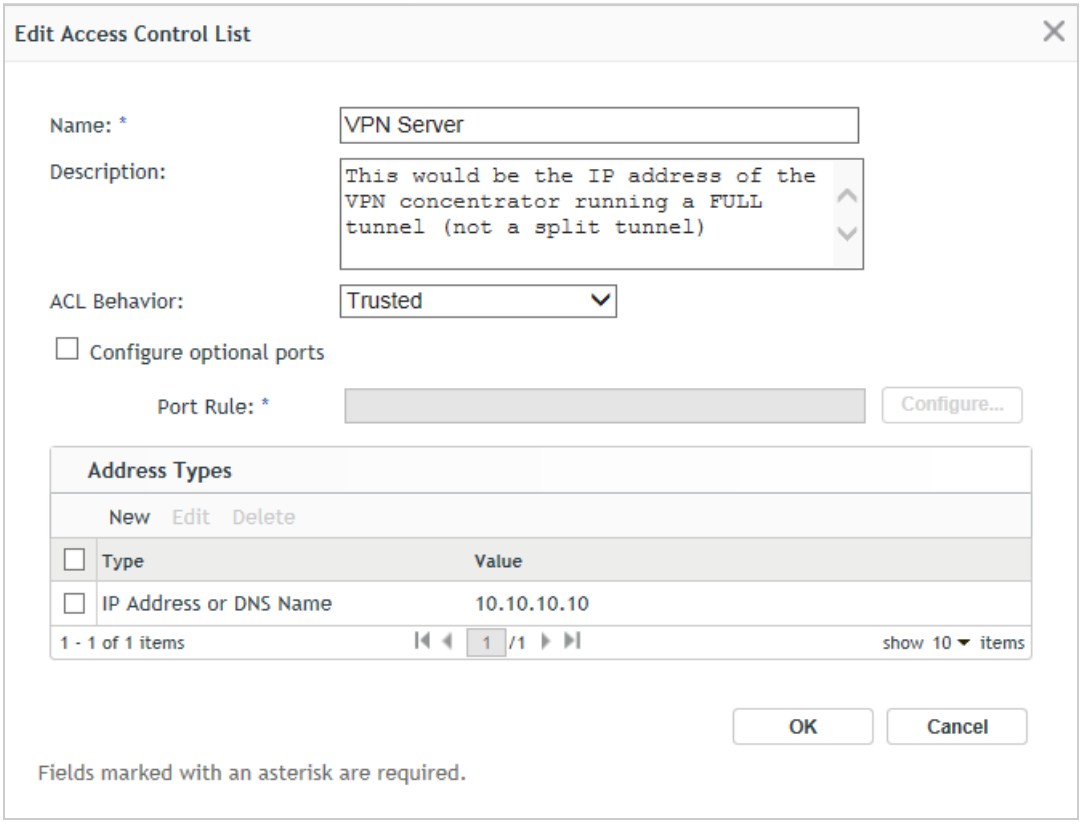
Notice that this location-based policy is configured to be available in the VPN location:




The **Default Behavior** for the firewall is **Closed**, which means that any ports, protocols, and addresses that need to be open must be explicitly defined. In this case, DHCP and DNS are open and several standard ACLs are allowed. In addition, the VPN server is added as a trusted ACL. The combination of these settings allow network traffic to the VPN server address but block all other addresses.




**2c** Click **VPN Server** to display the Edit Access Control List dialog box.




**2d** In the **Address Types** list, change the address to your VPN server address.

**2e** Click **OK** to save the address change.

**2f** Click **Apply** to save the policy.

**2g** Return to the **Policies** list.

**3** Assign the Location Assignment, VPN, and Firewall policies to a device:

**3a** In the **Policies** list, select the check boxes next to the following policies:

- **Location Assignment**
- **VPN - Session Prompt**
- **Firewall - Restrictive VPN**

**3b** Click **Action** > **Assign to Device**, then follow the prompts to assign the policies to the appropriate device.

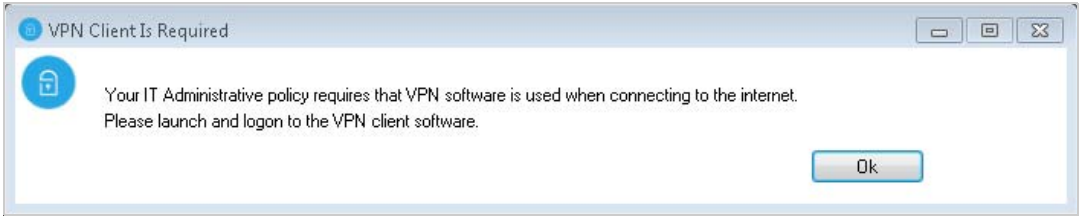
If the **Location Assignment** and **VPN - Session Prompt VPN** policies are already assigned to the device because of a previous scenario, you are prompted whether or not you want to replace the assignments. You can keep the current assignments.

When prompted for the policy conflict method, you can leave it set to **User Precedence**.

**4** Test the Firewall policy on the assigned device:

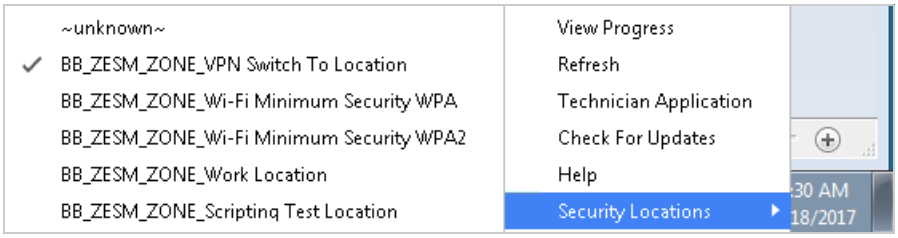
**4a** On the device, right-click the ZENworks icon, then click **Refresh** to retrieve the new policies.

When the device finishes refreshing and the policies are applied, the location is set to the **Unknown** location. The **Unknown** location applies the **VPN - Session Prompt** policy, which causes the location to be switched to the **BB_ZESM_ZONE_VPN Switch to Location** and the following prompt to be displayed:




**4b** Click **OK** to dismiss the prompt.

**4c** Right-click the ZENworks icon > click **Security Location** to see that the device is in the **BB_ZESM_ZONE_VPN Switch to Location**.




**5** Open a command prompt and ping your VPN server address to verify that it is accessible.

The policy also allows access to ZENworks Servers so that the ZENworks Agent can continue to communicate with the system. You can ping a ZENworks Server to verify if desired.

**6** Use your normal administrative tools to verify that all other network traffic is blocked.

7 For the purpose of this test scenario, you need to unassign the **VPN - Session Prompt** policy from the device (in ZENworks Control Center) to exit the **BB_ZESM_ZONE_VPN Switch to Location** on the device.

# 3 Launching a VPN Client to Initiate a VPN Session When in an Unknown Location

This scenario assumes that you have already completed the Prompting a User to Initiate a VPN Session When in an Unknown Location and Enforcing a Restrictive Firewall During the VPN Session scenarios. This scenario builds on those scenarios, so if you have not completed them, do so before continuing.

As the ZENworks administrator, when a user is in a location that requires a VPN session you want to automatically launch the VPN client for the user and then ensure that only network traffic through the VPN session is allowed.

The following steps help you import a predefined VPN policy that launches a VPN client when a device is in the default **Unknown** location. The Firewall policy used in Enforcing a Restrictive Firewall During the VPN Session is also applied to block all network access that is not through the VPN server.

1 Import the VPN policy:

**1a** Copy the following files to a directory on the ZENworks Primary Server:

- `VPN-Session-Launch.xml`
- `policykey.txt`

When you click a filename, the file will either be opened, saved, or you will be prompted to open or save it. You need to save the file. If it opens, click **File** > **Save**.

If you downloaded the Endpoint Security Resource Kit, you can copy the files from the `PolicyExamples` directory.

**1b** On the Primary Server, open a command prompt, change to the directory where you copied the files, then run the following command, entering your ZENworks administrator username and password when prompted:

```
zman epi "VPN - Session Launch" policykey.txt VPN-Session-Launch.xml
```

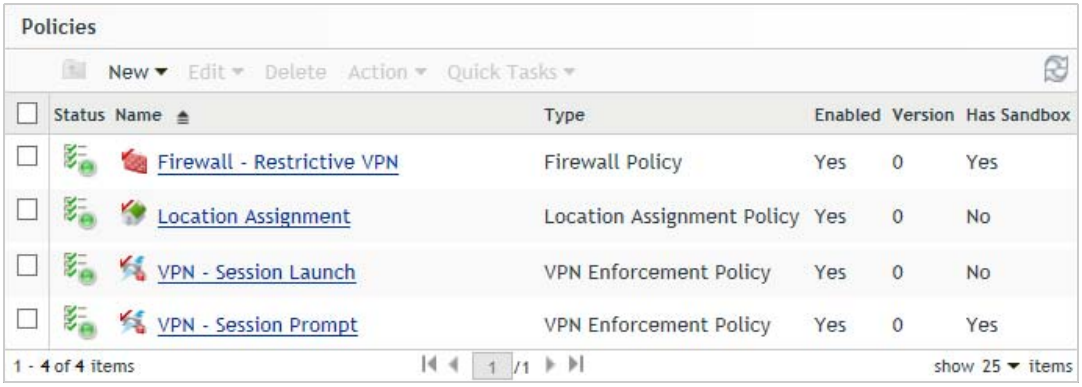
A message similar to the following is displayed when a policy is successfully imported:

```
Successfully created the object "VPN - Session Launch" in "/Policies".
```

2 Validate the policy import and modify the VPN policy as needed:

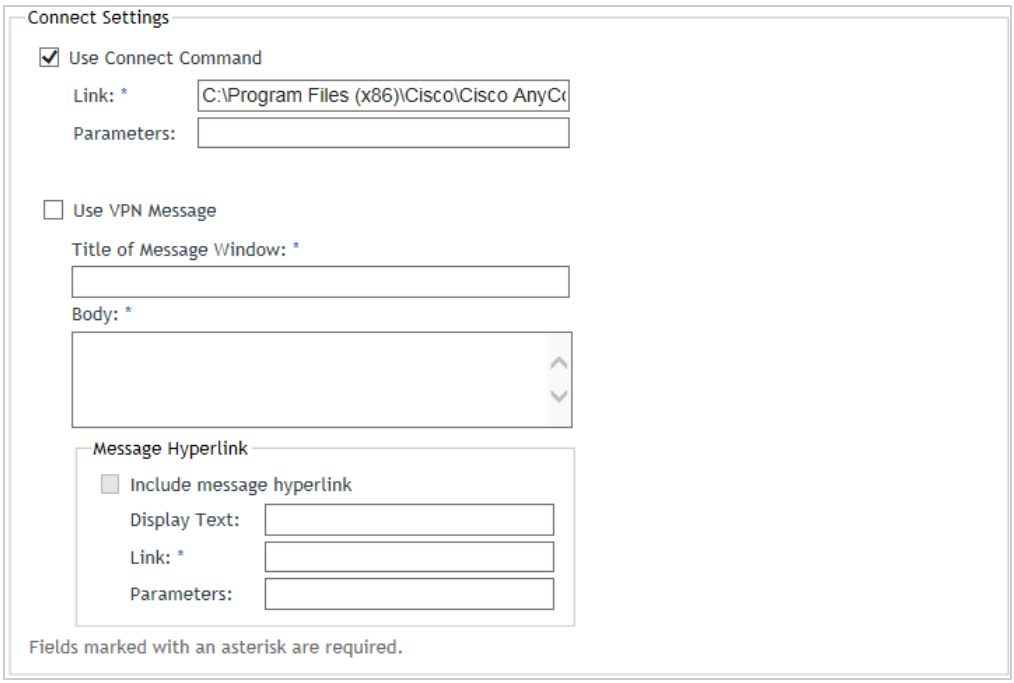
**2a** In ZENworks Control Center, click **Policies** to display the **Policies** list with the imported policies.

The **VPN- Session Launch** policy is listed along with the **Location Assignment**, **VPN - Session Prompt**, and **Firewall - Restrictive VPN** policies that were imported as part of the previous scenarios.




**2b** Click the **VPN - Session Launch** policy, then click the **Details** tab.

The policy is configured the same as the **VPN - Session Prompt** policy with the exception that a connect command is used instead of a VPN message prompt. The connect command launches a VPN client. The user must then log in using the client.




**2c** In the **Link** field, enter the command needed to launch your VPN client.

**2d** Click **Apply** to save the policy.

**2e** Return to the **Policies** list.

**3** Assign the Location Assignment, VPN, and Firewall policies to a device:

**3a** In the **Policies** list, select the check boxes next to the following policies:

- **Location Assignment**
- **VPN - Session Launch**
- **Firewall - Restrictive VPN**

**3b** Click **Action** > **Assign to Device**, then follow the prompts to assign the policies to the appropriate device.

If the **Location Assignment** and **Firewall - Restrictive VPN** policies are already assigned to the device, you are prompted whether or not you want to replace the assignments. You can keep the current assignments.

When prompted for the policy conflict method, you can leave it set to **User Last**.

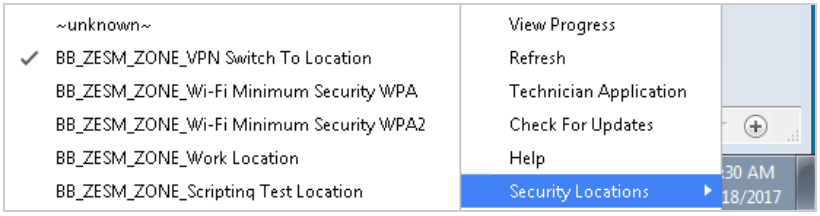
**3c** If the **VPN - Session Prompt** policy is assigned to the device (from the previous scenarios), remove the policy assignment from the device. To do so, click the policy, click **Relationships**, then remove the device from the **Device Assignments** list.

**4** Test the policy on the assigned device:

**4a** On the device, right-click the ZENworks icon, then click **Refresh** to retrieve the new policies.

When the device finishes refreshing and the policies are applied, the location is set to the **Unknown** location. The **Unknown** location applies the **VPN - Session Launch** policy, which causes the location to be switched to the **BB_ZESM_ZONE_VPN Switch to Location** and the VPN client to be launched.

**4b** Right-click the ZENworks icon > click **Security Location** to see that the device is in the **BB_ZESM_ZONE_VPN Switch to Location**.




**4c** For the purpose of this test scenario, you need to unassign the **VPN - Session Launch** policy from the device (in ZENworks Control Center) to exit the **BB_ZESM_ZONE_VPN Switch to Location** on the device.

# 4 Legal Notice