ZENworks Endpoint Security Management - Wireless Access Control

December 2016

This document provides test scenarios that show you how to use ZENworks Endpoint Security Management to ensure that users, regardless of their location, connect only to secure wireless networks.

1 Preventing Devices from Connecting to Unsecure Wireless Networks

As a ZENworks administrator, you want to ensure that your mobile users don’t connect to wireless networks that are not secure. The best way to do this is to create a Wi-Fi policy that establishes the minimum level of security (WEP, WPA, or WPA2) that wireless network must provide, and then assign that policy to your **Unknown** security location.

The following steps use predefined policies to create a scenario that shows you how Wi-Fi policies can be used to filter out unsecure wireless networks. The final step helps you assign the appropriate Wi-Fi policy to your **Unknown** location if you so choose.

1 Import the Location Assignment policy and Wi-Fi policies:

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

- `Location-Assignment.xml`
- `Wireless-Minimum-WiFi-Security-WPA.xml`
- `Wireless-Minimum-WiFi-Security-WPA2.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 "Wireless - Minimum Wi-Fi Security WPA" policykey.txt Wireless-Minimum-WiFi-Security-WPA.xml
```

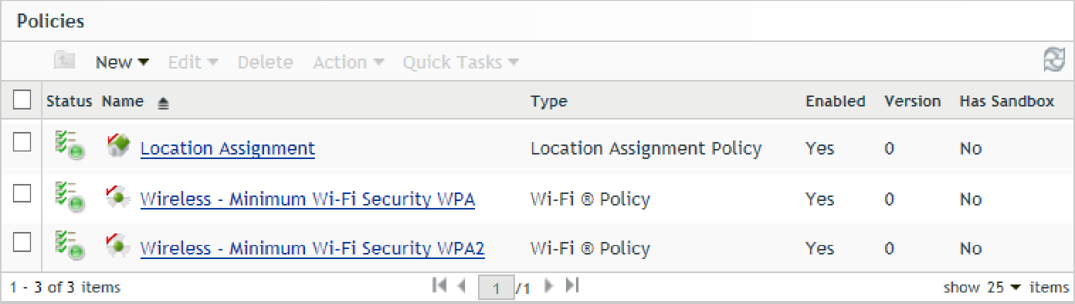
```
zman epi "Wireless - Minimum Wi-Fi Security WPA2" policykey.txt Wireless-Minimum-WiFi-Security-WPA2.xml
```

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 three imported policies.



Policies

□	Status	Name	Type	Enabled	Version	Has Sandbox
□		Location Assignment	Location Assignment Policy	Yes	0	No
□		Wireless - Minimum Wi-Fi Security WPA	Wi-Fi ® Policy	Yes	0	No
□		Wireless - Minimum Wi-Fi Security WPA2	Wi-Fi ® Policy	Yes	0	No

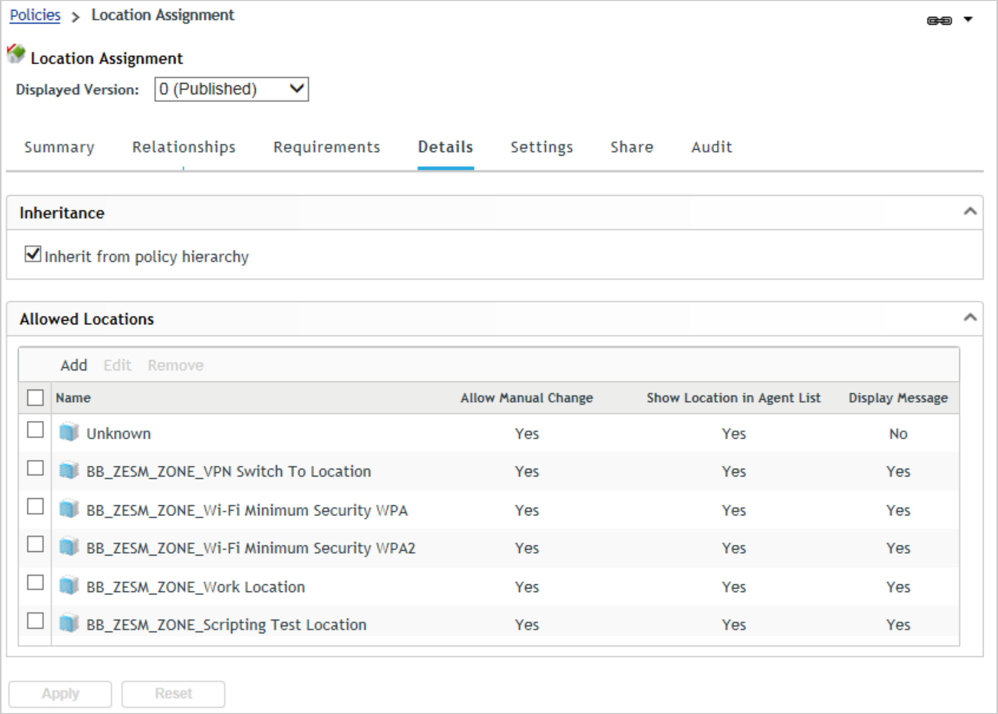
1 - 3 of 3 items   1 /1   show 25 items

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 Wi-Fi locations are used. The other locations are used with the test scenarios for other policies (VPN 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.



Policies > Location Assignment

Location Assignment

Displayed Version: 0 (Published)

Inheritance

☑ Inherit from policy hierarchy

Allowed Locations

□	Name	Allow Manual Change	Show Location in Agent List	Display Message
□	Unknown	Yes	Yes	No
□	BB_ZESM_ZONE_VPN Switch To Location	Yes	Yes	Yes
□	BB_ZESM_ZONE_Wi-Fi Minimum Security WPA	Yes	Yes	Yes
□	BB_ZESM_ZONE_Wi-Fi Minimum Security WPA2	Yes	Yes	Yes
□	BB_ZESM_ZONE_Work Location	Yes	Yes	Yes
□	BB_ZESM_ZONE_Scripting Test Location	Yes	Yes	Yes

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

3 Assign the Location Assignment and Wi-Fi policies to a device that has a wireless network card:

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

- **Location Assignment**
- **Wireless - Minimum Wi-Fi Security WPA**
- **Wireless - Minimum Wi-Fi Security WPA2**

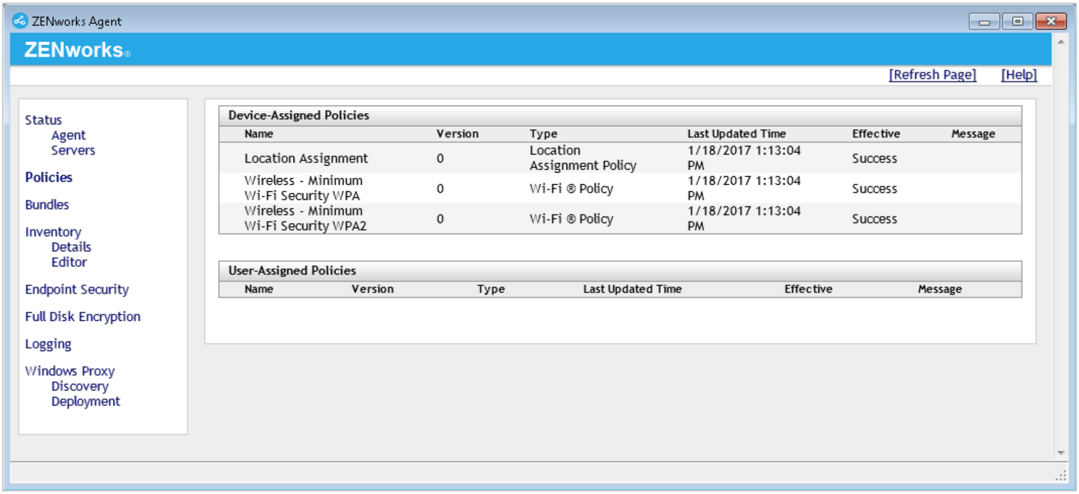
3b Click **Action** > **Assign to Device**, then follow the prompts to assign the policies to the appropriate device.

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

4 Test the policies on the assigned device:

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

4b When the device finishes refreshing, right-click the ZENworks icon, and select **Technical Application** to display the ZENworks Agent, then click **Policies** and make sure the **Location Assignment**, **Wireless - Minimum Wi-Fi Security WPA**, and **Wireless - Minimum Wi-Fi Security WPA2** policies were successfully applied.



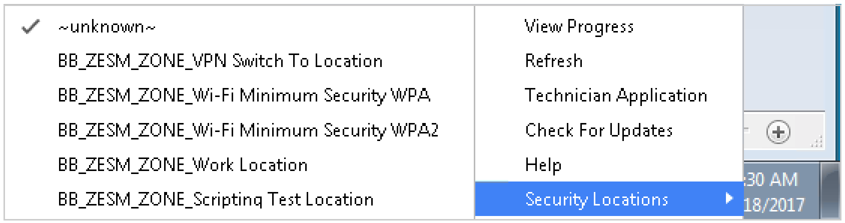
Device-Assigned Policies

Name	Version	Type	Last Updated Time	Effective	Message
Location Assignment	0	Location Assignment Policy	1/18/2017 1:13:04 PM	Success	
Wireless - Minimum Wi-Fi Security WPA	0	Wi-Fi ® Policy	1/18/2017 1:13:04 PM	Success	
Wireless - Minimum Wi-Fi Security WPA2	0	Wi-Fi ® Policy	1/18/2017 1:13:04 PM	Success	

User-Assigned Policies

Name	Version	Type	Last Updated Time	Effective	Message

4c Right-click the ZENworks icon, and select **Security Location** > **~unknown~** to change the device's location to the Unknown location.


✓ ~unknown~
BB_ZESM_ZONE_VPN Switch To Location
BB_ZESM_ZONE_Wi-Fi Minimum Security WPA
BB_ZESM_ZONE_Wi-Fi Minimum Security WPA2
BB_ZESM_ZONE_Work Location
BB_ZESM_ZONE_Scripting Test Location
View Progress
Refresh
Technician Application
Check For Updates
Help
Security Locations
:30 AM
18/2017

4d View your detected wireless networks.

The list of wireless networks hopefully includes unsecure, WPA, and WPA2 networks.

4e Change the security location to the **BB_ZESM_ZONE_Wi-Fi Minimum Security WPA** location, wait a minute, then view the list of detected wireless networks again.

The **BB_ZESM_ZONE_Wi-Fi Minimum Security WPA** location applies the **Wireless - Wi-Fi Minimum Security WPA** policy. The policy requires a wireless network to provide a minimum security level of WPA encryption, which results in all unsecured wireless networks being filtered from the list.

4f Change the security location to the **BB_ZESM_ZONE_Wi-Fi Minimum Security WPA2** location, wait a minute, then view the list of detected wireless networks again.

The **BB_ZESM_ZONE_Wi-Fi Minimum Security WPA2** location applies the **Wireless - Wi-Fi Minimum Security WPA2** policy. The policy requires a wireless network to provide a minimum security level of WPA2 encryption, which results in all unsecured wireless networks being filtered from the list. The WPA wireless networks are not filtered from the list because differentiation between WPA and WPA2 is not made until the device attempts to connect to the wireless network. At that point, if the security level is WPA, the connection fails and the wireless network disappears from the list, leaving only the WPA2 secured networks.

5 To assign a Wi-Fi policy to your **Unknown** location in order to enforce a minimum security level in that location:

5a In ZENworks Control Center, click **Policies** to display the **Policies** list.

5b If you want to use WPA as the minimum security level, click the **Wireless - Minimum Wi-Fi Security WPA** policy, then click **Details**.

or

If you want to use WPA2 as the minimum security level, click the **Wireless - Minimum Wi-Fi Security WPA2** policy, then click the **Details** tab.

5c On the **Details** page, do the following:

5c1 In the **Location Assignments** panel, remove the locations used for the scenario and add the **Unknown** location.

5c2 In the **Minimum Security Level** section, modify the message if desired.

5c3 Click **Apply** to save your changes.

5d Click the **Relationships** tab and assign the policy to the devices and users you want it to apply to.

5e Close the Wi-Fi policy.

5f Make sure that the users and devices you assigned the Wi-Fi policy to also have a Location Assignment policy assigned to them that includes the **Unknown** location.

2 Allowing Access to Approved Wireless Network Access Points (SSIDs) Only

As a ZENworks administrator, you want to ensure that users at work only connect to your corporate wireless network and that all other wireless networks are disallowed.

The following steps help you import a predefined W-Fi policy and Location Assignment policy that limits wireless network access to two approved Access Points (SSIDs) when the device in a *Work* location.

1 Import the Wi-Fi policy and Location Assignment policy:

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

- `Location-Assignment.xml`
- `Wireless-Work-WiFi-SSID-Filtering.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 "Wireless - Work Wi-Fi SSID Filtering" policykey.txt Wireless-Work-WiFi-SSID-Filtering.xml
```

The following message is displayed if the policy is successfully imported:

```
Successfully created the object "Wireless - Work Wi-Fi SSID Filtering" in "/Policies".
```

1c If you completed the Preventing Devices from Connecting to Unsecure Wireless Networks scenario, you can skip this step. Otherwise, run the following command to import the Location Assignment policy, entering your ZENworks administrator username and password when prompted:

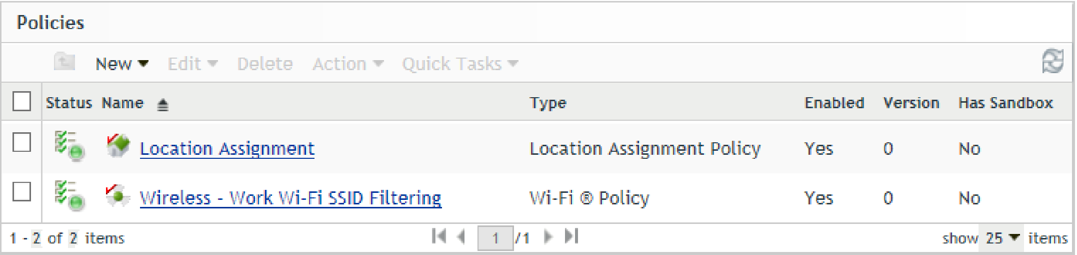
```
zman epi "Location Assignment" policykey.txt Location-Assignment.xml
```

The following message is displayed if the 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.



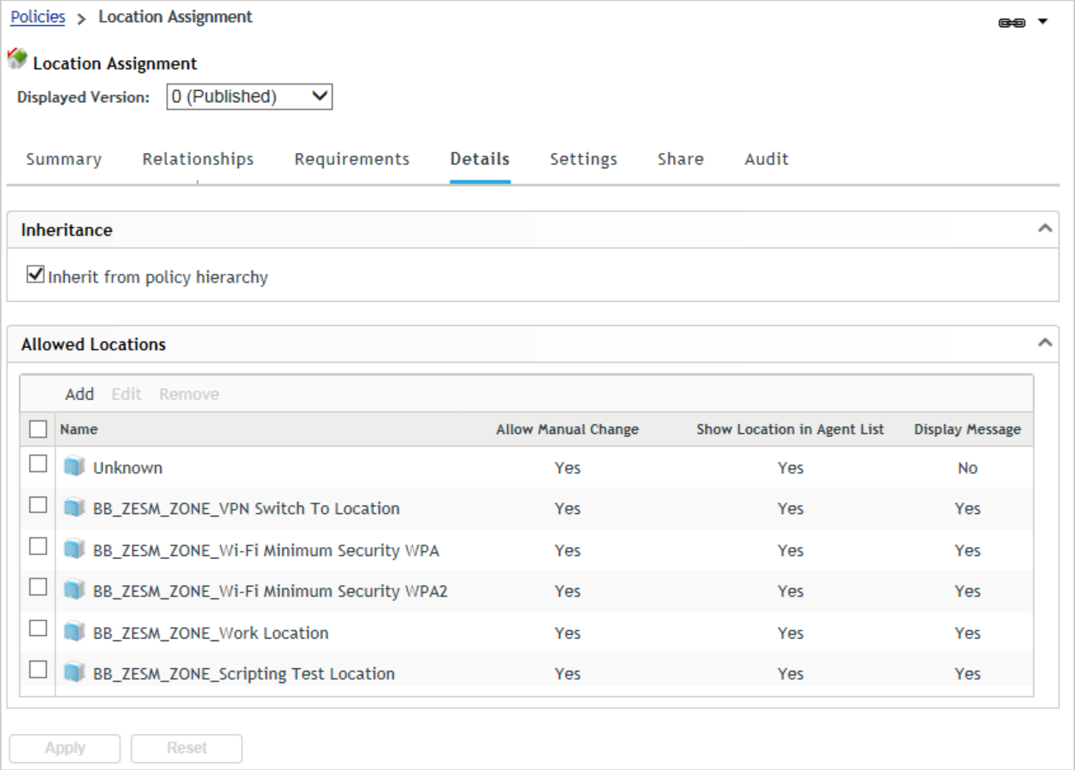
□	Status	Name	Type	Enabled	Version	Has Sandbox
□		Location Assignment	Location Assignment Policy	Yes	0	No
□		Wireless - Work Wi-Fi SSID Filtering	Wi-Fi ® Policy	Yes	0	No

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 Work location is used. The other locations are used with the test scenarios for other policies (VPN and Scripting).

The Work location does not include any network environments, which means that the only way a device can switch to the location is for the device's user to manually change to the location. For this reason, the 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.



Location Assignment

Displayed Version: 0 (Published)

Inheritance

☑ Inherit from policy hierarchy

Allowed Locations

□	Name	Allow Manual Change	Show Location in Agent List	Display Message
□	Unknown	Yes	Yes	No
□	BB_ZESM_ZONE_VPN Switch To Location	Yes	Yes	Yes
□	BB_ZESM_ZONE_Wi-Fi Minimum Security WPA	Yes	Yes	Yes
□	BB_ZESM_ZONE_Wi-Fi Minimum Security WPA2	Yes	Yes	Yes
□	BB_ZESM_ZONE_Work Location	Yes	Yes	Yes
□	BB_ZESM_ZONE_Scripting Test Location	Yes	Yes	Yes

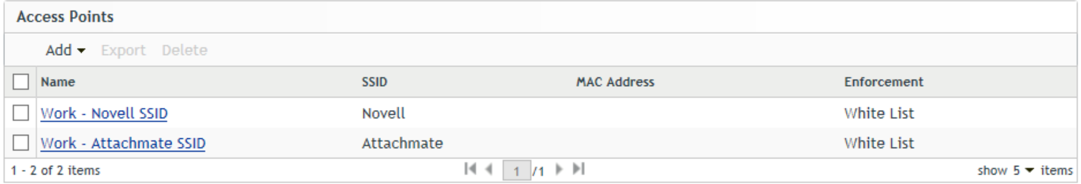
2c Return to the **Policies** list.

3 Modify the **Wireless - Work Wi-Fi SSID Filtering** policy to add the SSIDs for your “Work” location:

3a Click the **Wireless - Work Wi-Fi SSID Filtering** policy, then click its **Details** tab.

The Access Points list is used to explicitly approve (whitelist) or prohibit (blacklist) Access Point SSIDs. If the list doesn’t include any Access Points, all Access Points are approved. As soon as one Access Point is added, the list becomes an explicit list and only explicitly approved Access Points are allowed.

In the **Wireless - Work Wi-Fi SSID Filtering** policy you imported, there are two explicitly approved (whitelisted) Access Points, which means that all other Access Points are prohibited.



Access Points

□	Name	SSID	MAC Address	Enforcement
□	Work - Novell SSID	Novell		White List
□	Work - Attachmate SSID	Attachmate		White List

1 - 2 of 2 items

3b Edit the list to define real Access Points for your “Work” location, referring to the sample entries as needed. Add only the Access Points you want to allow users to connect to in that location.

3c Click **Apply** to save your changes.

3d Click **Publish** to publish the changed policy.

4 Assign the two policies to a device that has a wireless network card:

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

- **Location Assignment**
- **Wireless - Work Wi-Fi SSID Filtering**

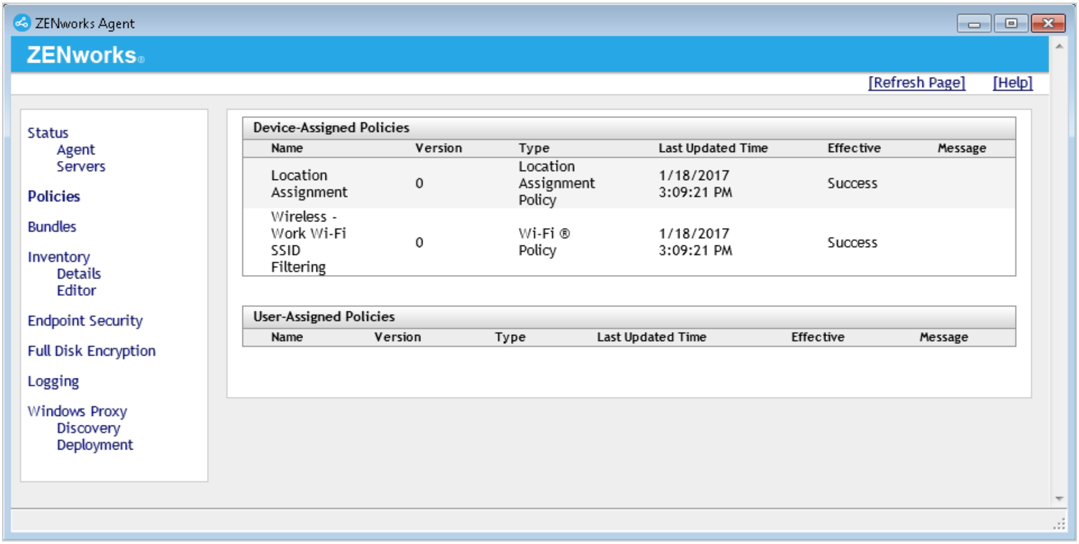
4b Click **Action** > **Assign to Device**, then follow the prompts to assign the policies to the appropriate device.

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

5 Test the policies on the assigned device:

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

5b When the device finishes refreshing, right-click the ZENworks icon, and select **Technical Application** to display the ZENworks Agent, then click **Policies** and make sure the **Location Assignment** and **Wireless - Work Wi-Fi SSID Filtering** policies have been successfully applied.



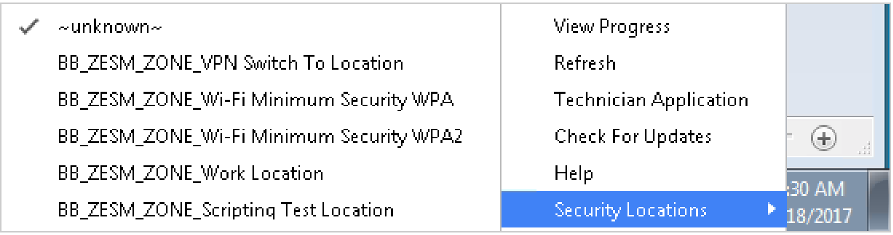
Device-Assigned Policies

Name	Version	Type	Last Updated Time	Effective	Message
Location Assignment	0	Location Assignment Policy	1/18/2017 3:09:21 PM	Success	
Wireless - Work Wi-Fi SSID Filtering	0	Wi-Fi ® Policy	1/18/2017 3:09:21 PM	Success	

User-Assigned Policies

Name	Version	Type	Last Updated Time	Effective	Message

5c Right-click the ZENworks icon > click **Security Location** > click **~unknown~** to change the device's location to the Unknown location.


✓ ~unknown~
BB_ZESM_ZONE_VPN Switch To Location
BB_ZESM_ZONE_Wi-Fi Minimum Security WPA
BB_ZESM_ZONE_Wi-Fi Minimum Security WPA2
BB_ZESM_ZONE_Work Location
BB_ZESM_ZONE_Scripting Test Location
View Progress
Refresh
Technician Application
Check For Updates
Help
Security Locations
:30 AM
18/2017

5d View your detected wireless networks.

The list of wireless networks hopefully includes multiple networks.

5e Change the security location to the **BB_ZESM_ZONE_Work Location**, wait a minute, then view the list of detected wireless networks again.

The **BB_ZESM_ZONE_Work Location** applies the **Wireless - Work Wi-Fi SSID Filtering** policy. The policy allows only those wireless networks you explicitly whitelisted through their Access Point SSIDs. This results in all non-approved wireless networks being filtered from the list.

3 Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.