Control Wifi access using Group Policy

Users can create a Group Policy setting that blocks workstations connected to any Wi-Fi network outside the specified network.

In this article we will learn how to prevent users from accessing another Wifi network, a method to create a secure Group Policy for Wifi networks and a Group Policy method to protect the network from termites. threats from inside and outside the network.

Windows operating system does not limit the process of installing virtual access points. An access point is a hardware device built into the system that is not controlled by Windows. However, users can create a Group Policy setting that blocks workstations connected to any Wi-Fi network outside the specified network.

The need of using Group Policy to control Wifi network access

The types of settings included in Group Policy perform two functions. First, they prevent users from installing virtual access points. So what is the problem when installing a virtual access point if you are not allowed to connect to it? Remember, although users can still install a virtual access point and use this virtual access point to connect to the network, in such cases, the settings in the Group Policy that you have deployed will not block that user from connecting because the settings in that Group Policy are only valid for Active Directory domains, pages or sub-levels. Since the user's system is not connected to Active Directory, no Group Policy settings will be applied. However, you can set up network security to only allow domain members to have access to network resources. The combination of these elements will prevent users from installing virtual access points.

These settings in Group Policy will also prevent users from randomly connecting to other Wifi networks. In most systems users can see other companies' Wi-Fi networks (to a certain extent), preventing users from connecting to these networks has two main benefits. Firstly, if you can block users from randomly connecting to a non-corporate network, you can minimize access issues for users because if they connect to the wrong network they will encounter error messages when accessing. certain types of resources.
Second, more importantly, when users connect to a network they are vulnerable to security threats that may exist in that network.

Create a Group Policy with limited access

Next we will create a Group Policy that limits users who are allowed to connect to the Wifi network. First, you need to know that the settings in Group Policy are to limit access to wireless networks that are not integrated in Windows. To be able to use these settings you will have to expand the Active Directory schema.

To expand the Active Directory schema for the Wireless Group Policy of Windows Vista we first need to create the file 802.11Schema.ldf. Perform the following actions:

1. From the Windows screen, go to the **Start** menu **| Programs | Accessories | Notepad** .

2. Select the content of the file *802.11Schema.ldf* at the bottom.
3. Copy this area and paste it into the Notepad window.
4. Go to **File and** choose **Save As** and save to the appropriate folder. Enter *802.11Schema.ldf* for the **File** name field, in **Save as type** select **All files** , and select **ANSI** for **Encoding** . After selecting, click **Save** .

Then use the Ldifde tool to extend the Active Directory schema. Perform the following actions:

1. If necessary, copy the file *802.11Schema.ldf* to a folder on the Domain Controller using Windows Server 2003 or Windows Server 2003 R2.

1. On this Domain Controller, go to **Start** , type *cmd* in the **Run** box, and click **OK** .

1. Open the folder containing the file *802.11Schema.ldf* .

1. In the Command Prompt window, run the following command:

   ldifde -i -v -k -f 802.11Schema.ldf -c DC = X Dist_Name_of_AD_Domain

   In it, **Dist_Name_of_AD_Domain** is the distinguished name of the Active Directory domain whose schema is being edited. For example, if the Active Directory domain name is *wcoast.microsoft.com* , the distinguished name will be **DC = wcoast, DC = microsoft, DC = com** .

   The file *802.11Schema.ldf* uses the string **DC = X** to display the distinguished name of the Active Directory domain. The **-c** option replaces the string **DC = X** with the string **DC = X** similar to the Active Directory domain when the *802.11Schema.ldf* file is imported.

   For example, if the domain name is *quantrimang.com* , the command syntax will be:

   ldifde -i -v -k -f 802.11Schema.ldf -c DC = X DC = quantrimang, DC = com

The *Ldifde.exe* tool uses the instructions in the *802.11Schema.ldf* file to edit the Active Directory schema to contain the additional values ??and attributes needed to store improvements to Wireless Group Policy settings that are hosted by the client. Wireless Windows Vista support.

The contents of the *802.11Schema.ldf* file *are* as follows:

```
# ------------------------------------------------ ----------------------
# Copyright (c) 2006 Microsoft Corporation
#
# MODULE: 802.11Schema.ldf
# ------------------------------------------------ ----------------------
# ------------------------------------------------ ----------------------
# define schemas for these attributes:
# ms-net-ieee-80211-GP-PolicyGUID
```

 # ms-net-ieee-80211-GP-PolicyData
 # ms-net-ieee-80211-GP-PolicyReserved
 # ---------- ----------
dn: CN = ms-net-ieee-80211-GP-PolicyGUID, CN = Schema, CN = Configuration, DC = X
changetype: ntdsSchemaAdd
objectClass: attributeSchema
ldapDisplayName: ms-net-ieee-80211-GP-PolicyGUID
adminDisplayName: ms-net-ieee-80211-GP-PolicyGUID
adminDescription: This attribute contains a GUID which identifies a specific 802.11 group policy ??i t??ng trên mi?n.
attributeId: 1.2.840.113556.1.4.1951
Attribute: 2.5.5.12
omSyntax: 64
isSingleValued: TRUE
systemOnly: FALSE
searchFlags: 0
rangeUpper: 64
schemaIdGuid :: YnBpNa8ei0SsHjiOC + T97g ==
showInAdvancedViewOnly: TRUE
systemFlags: 16
dn: CN = ms-net-ieee-80211-GP-PolicyData, CN = Schema, CN = Configuration, DC = X
changetype: ntdsSchemaAdd
objectClass: attributeSchema
ldapDisplayName: ms-net-ieee-80211-GP-PolicyData
adminDisplayName: ms-net-ieee-80211-GP-PolicyData
adminDescription: This attribute contains all of settings and d? li?u c?u hình m?t c?u hình cho 802.11 wireless networks.
AttributeId: 1.2.840.113556.1.4.1952
Attribute: 2.5.5.12
omSyntax: 64
isSingleValued: TRUE
systemOnly: FALSE
searchFlags: 0
rangeUpper: 4194304
schemaIdGuid :: pZUUnHZNjkaZHhQzsKZ4VQ ==
showInAdvancedViewOnly: TRUE
systemFlags: 16
dn: CN = ms-net-ieee-80211-GP-PolicyReserved, CN = Schema, CN = Configuration, DC = X
changetype: ntdsSchemaAdd
objectClass: attributeSchema
ldapDisplayName: ms-net-ieee-80211-GP-PolicyReserved
adminDisplayName: ms-net-ieee-80211-GP-PolicyReserved
adminDescription: Reserved for future use
AttributeId: 1.2.840.113556.1.4.1953
attributeSyntax: 2.5.5.10
omSyntax: 4
isSingleValued: TRUE
systemOnly: FALSE

searchFlags: 0
rangeUpper: 4194304
schemaIdGuid :: LsZpD44I9U + lOukjzsB8Cg ==
showInAdvancedViewOnly: TRUE
systemFlags: 16
 # ---------- ----------
 # Reload the schema schema to pick up altered classes and attributes
 # ---------- ----------
dn:
changetype: ntdsSchemaModify
add: schemaUpdateNow
schemaUpdateNow: 1
-
 # ---------- ----------
 # define schemas for giá tr? Parent:
 # ms-net-ieee-80211-GroupPolicy
 # ---------- ----------
dn: CN = ms-net-ieee-80211-GroupPolicy, CN = Schema, CN = Configuration, DC = X
changetype: ntdsSchemaAdd
objectClass: classSchema
ldapDisplayName: ms-net-ieee-80211-GroupPolicy
adminDisplayName: ms-net-ieee-80211-GroupPolicy
adminDescription: This class represents 802.11 wireless network group policy object. T?p tin này ch?a m?t xác ??nh và xác ??nh d? li?u xác th?c ?? th?c hi?n máy ?nh wireless 802.11.
governsId: 1.2.840.113556.1.5.251
objectClassCategory: 1
rdnAttId: 2.5.4.3
subClassOf: 2.5.6.0
systemMayContain: 1.2.840.113556.1.4.1953
systemMayContain: 1.2.840.113556.1.4.1952
systemMayContain: 1.2.840.113556.1.4.1951
systemPossSuperiors: 1.2.840.113556.1.3.30
systemPossSuperiors: 1.2.840.113556.1.3.23
systemPossSuperiors: 2.5.6.6
schemaIdGuid :: Yxi4HCK4eUOeol / 3vcY4bQ ==
defaultSecurityDescriptor: D: (A ;; RPWPCRCCDCLCLORCWOWDSDDTSW ;;; DA) (A ;; RPWPCRCCDCLCLORCWOWDSDDTSW ;;; SY) (A ;; RPLCLORC ;;; AU)
showInAdvancedViewOnly: TRUE
defaultHidingValue: TRUE
systemOnly: FALSE
defaultObjectCategory: CN = ms-net-ieee-80211-GroupPolicy, CN = Schema, CN = Configuration, DC = X
systemFlags: 16
 # ---------- ----------
 # Reload the schema schema to pick up altered classes and attributes
 # ---------- ----------
dn:
changetype: ntdsSchemaModify

add: schemaUpdateNow
schemaUpdateNow: 1
-

Once you have expanded the Active Directory schema, open the domain security policy, then on the **Group Policy Object Editor** open **Computer Configuration | Windows Settings | Security Settings** . When you expand **Security Settings** you will see that it now contains a **Wireless Network** node **(IEE802.11)** as shown in Figure 1.

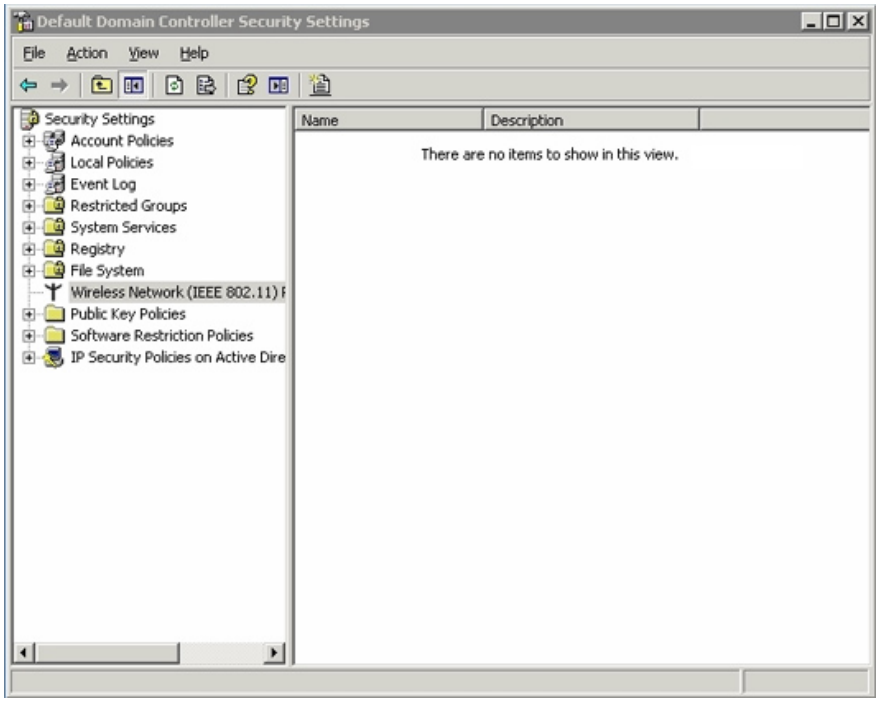

Figure 1: Group Policy Object Editor allows you to edit Wifi security settings.

Since no Wireless Policy exists by default, we will have to create a Group Policy. Right-click **Wireless network (802.11)** and select the **Create Wireless Network Policy** command from the context menu. Windows will then launch the **Wireless Network Policy** wizard. Click **Next** to bypass the **Welcome** page of this wizard, next you will see a page asking for the name and description for the Policy being created. After entering, click **Next** and **Finish** . Now Windows will open the newly created Policy property page.

On the **General** tab of the properties page, you can check the types of Wifi networks that the workstation is allowed to connect to, and you can select the *use Windows* checkbox *to automatically configure network settings for wireless clients* (use Windows to configure Automatic network settings for Wifi workstations).

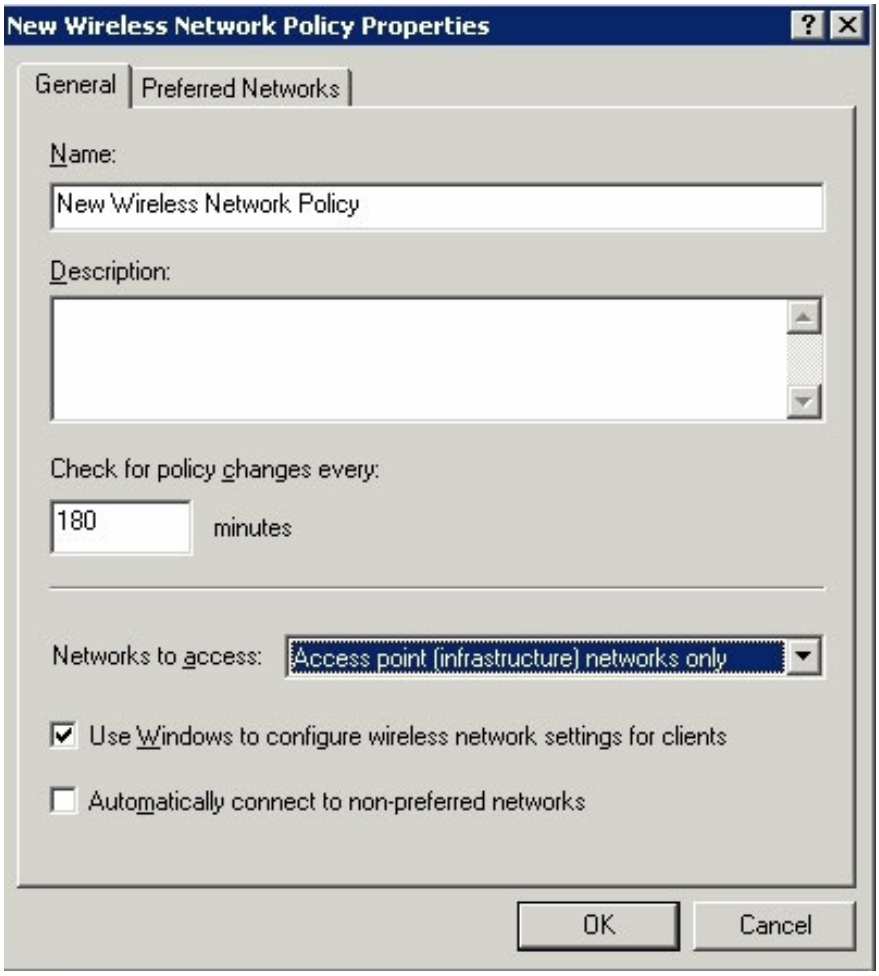

Figure 2: Network configuration Wifi workstation is allowed to connect to.

Tab **Preferred Networks** , in Figure 3, allows you to specify a list of priority networks that you want the Windows system to connect to.

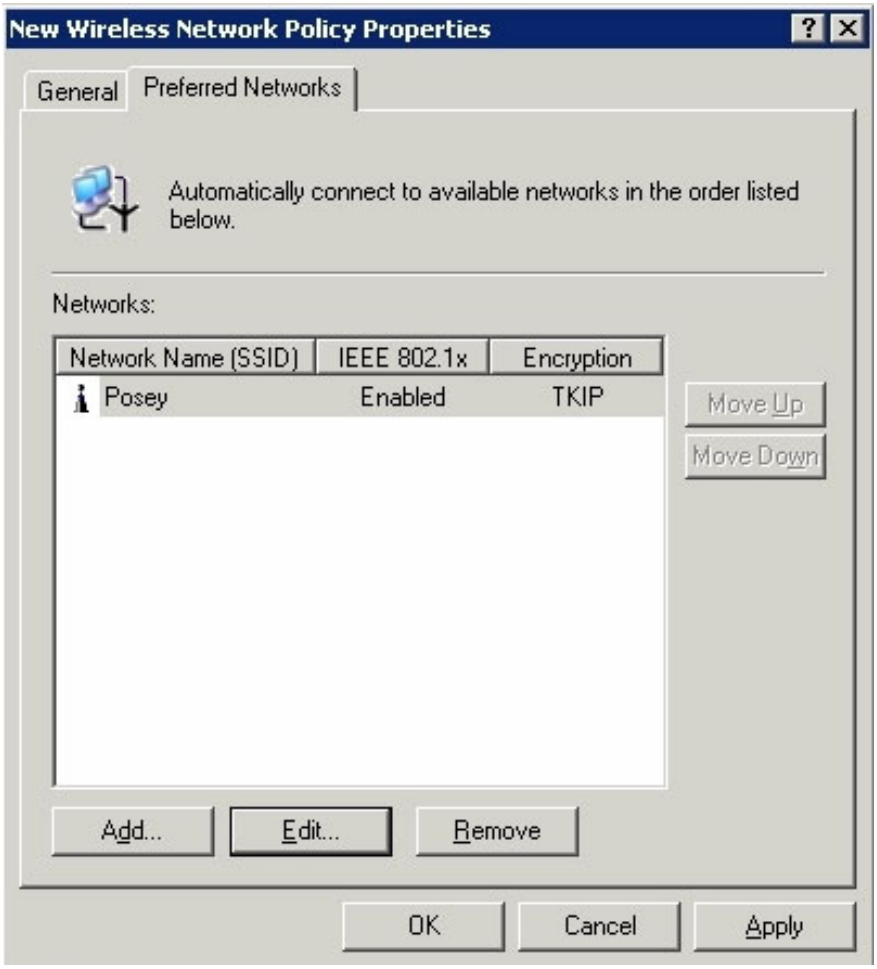

Figure 3: Select the preferred network in the Preferred Networks tab.

All of these settings may apply to Windows XP-based computers. However, there are some settings that can only be applied to Windows Vista and Windows Server 2008 workstations. These settings allow you to specify exactly which Wifi networks the workstation is allowed to access. You can access Vista-specific settings by opening a default domain policy using a Windows Vista or Windows Server 2008 machine.