CSA for WLAN Security

A Cisco Secure Wireless Network offers customers an integrated, defense-in-depth approach to WLAN security, and includes WLAN threat detection and mitigation, as well as policy enforcement.

This guide outlines the role of Cisco Security Agent (CSA) in WLAN threat detection and mitigation, as well as in policy enforcement, and provides an overview of the security features it offers for a WLAN, along with implementation guidelines to assist in its design and deployment in production networks.

More information on end-to-end integrated WLAN security, along with references to documents that outline current guidelines for securing a WLAN, can be found in Appendix B—Sample Customized Wireless Ad-Hoc Rule Module, page 49.

Software implementation, screenshots, and behavior referenced in this chapter are based on CSA v5.2.0.203 FCS software release. It is assumed that readers are already familiar with both CSA and the Cisco Unified Wireless Network.

Note Note that this guide addresses only CSA features specific to WLAN security.

Contents

CSA for WLAN Security Overview 3
- CSA for General Client Protection 3
- CSA for WLAN-Specific Scenarios 4
- CSA and Complementary WLAN Security Features 6
- CSA Integration with the Cisco Unified Wireless Network 6

Wireless Ad-Hoc Connections 7
- Wireless Ad-hoc Networks—Security Concerns 7
- CSA Wireless Ad-Hoc Connections Pre-Defined Rule Module 8
  - Pre-Defined Rule Module Operation 8
  - Pre-Defined Rule Module Operational Considerations 9
  - Pre-Defined Rule Module Configuration 10

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Pre-Defined Rule Module Logging 12
Wireless Ad-Hoc Rule Customization 13
Simultaneous Wired and Wireless Connections 14
Simultaneous Wired and Wireless Connections—Security Concerns 15
CSA Simultaneous Wired and Wireless Connections Pre-Defined Rule Module 15
Pre-Defined Rule Module Operation 15
Pre-Defined Rule Module Operational Considerations 16
Pre-Defined Rule Module Configuration 17
Pre-Defined Rule Module Logging 21
Simultaneous Wired and Wireless Rule Customization 22
Location-Aware Policy Enforcement 23
Security Risks Addressed by Location-Aware Policy Enforcement 24
CSA Location-Aware Policy Enforcement 25
Location-Aware Policy Enforcement Operation 25
Location-Aware Policy Enforcement Configuration 28
General Location-Aware Policy Enforcement Configuration Notes 33
CSA Force VPN When Roaming Pre-Defined Rule Module 34
Pre-Defined Rule Module Operation 34
Pre-Defined Rule Module Operational Considerations 35
Pre-Defined Rule Module Configuration 36
Upstream QoS Marking Policy Enforcement 40
Benefits of Upstream QoS Marking 41
Benefits of Upstream QoS Marking on a WLAN 42
Challenges of Upstream QoS Marking on a WLAN 42
CSA Trusted QoS Marking 42
Benefits of CSA Trusted QoS Marking on a WLAN Client 44
Basic Guidelines for Deploying CSA Trusted QoS Marking 44
CSA Wireless Security Policy Reporting 44
CSA Management Center Reports 44
Third-Party Integration 47
Overall Deployment Guidelines for CSA Integrated WLAN Security 48
Appendix A—CSA Overview 48
CSA Solution Components 49
Appendix B—Sample Customized Wireless Ad-Hoc Rule Module 49
Sample Customized Rule Module Operation 50
Sample Customized Rule Module Definition 51
Sample Customized Rule Module Logging 57
Appendix C—Sample Customized Simultaneous Wired and Wireless Rule Module 58
Sample Customized Rule Module Operation 59

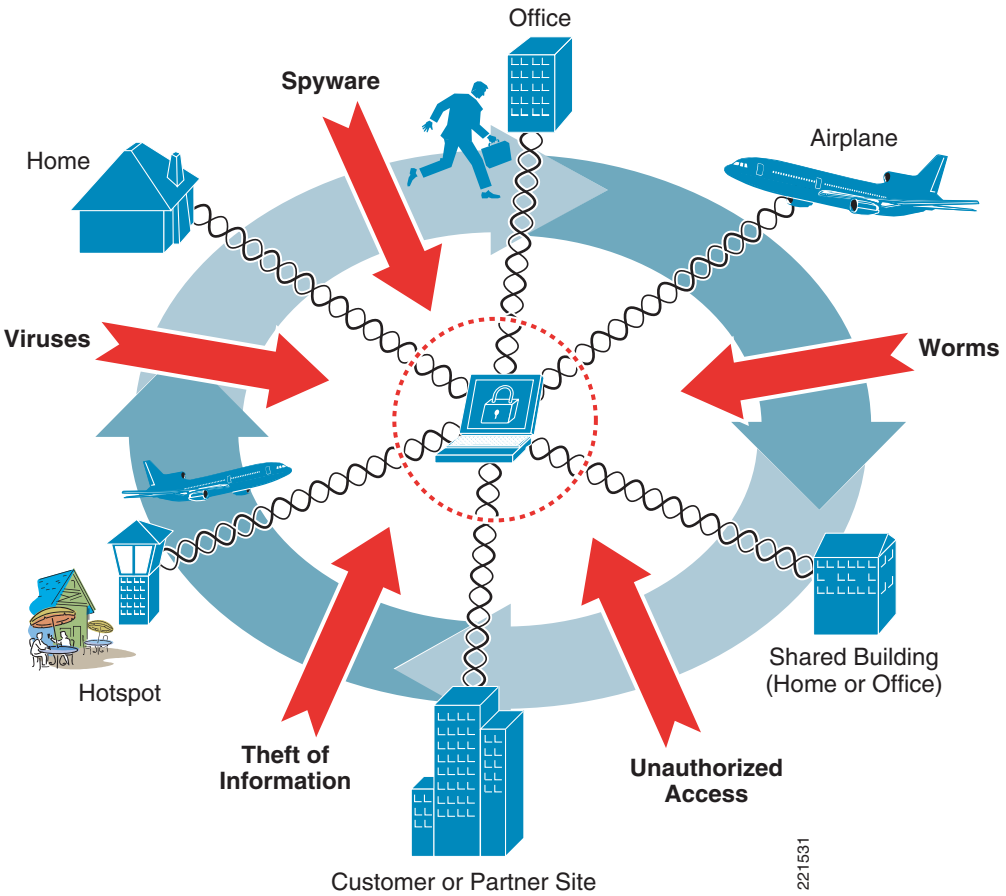
Sample Customized Rule Module Definition 60
Sample Customized Rule Module Logging 66
Appendix D—Test Bed Hardware and Software 67
Appendix E—References 67

CSA for WLAN Security Overview

CSA for General Client Protection

A WLAN client typically associates, knowingly or unknowingly, to a range of different networks such as a corporate network, Wi-Fi hotspots, a home network, partner networks, wireless ad-hoc networks, rogue networks, and so on. As such, it is exposed to security threats that may not be experienced by clients solely connected to a corporate network (see Figure 1). These threats may subsequently be transferred to the corporate network when a client returns to the office.

Figure 1 Exposure to General Security Threats of a Mobile Client



CSA offers the ability to protect a wired or wireless endpoint from many threats, including viruses, worms, botnets, spyware, theft of information, and unauthorized access. CSA provides this endpoint protection by identifying and preventing malicious or unauthorized behavior. This role is generally referred to as Host-based Intrusion Protection Solution (HIPS).

This is a critical element of endpoint security that protects both the host itself and the corporate network to which it connects.

These general endpoint protection policies may also be extended by leveraging the wireless-specific security policies introduced in CSA v5.2.

A brief overview of CSA is available in Appendix D—Test Bed Hardware and Software, page 67. Detailed information is available on the product sites, as listed in Appendix B—Sample Customized Wireless Ad-Hoc Rule Module, page 49.

CSA for WLAN-Specific Scenarios

CSA v5.2 extended the critical HIPS and policy enforcement features offered by CSA to include wireless-specific policies. These policies can be deployed to extend endpoint protection and tailor it to the particular type of wireless network to which a WLAN client may be connected, such as a corporate network, Wi-Fi hotspot, home network, rogue network, and so on. (See Figure 2.)

Figure 2 WLAN-Specific Security Risks Addressed by CSA

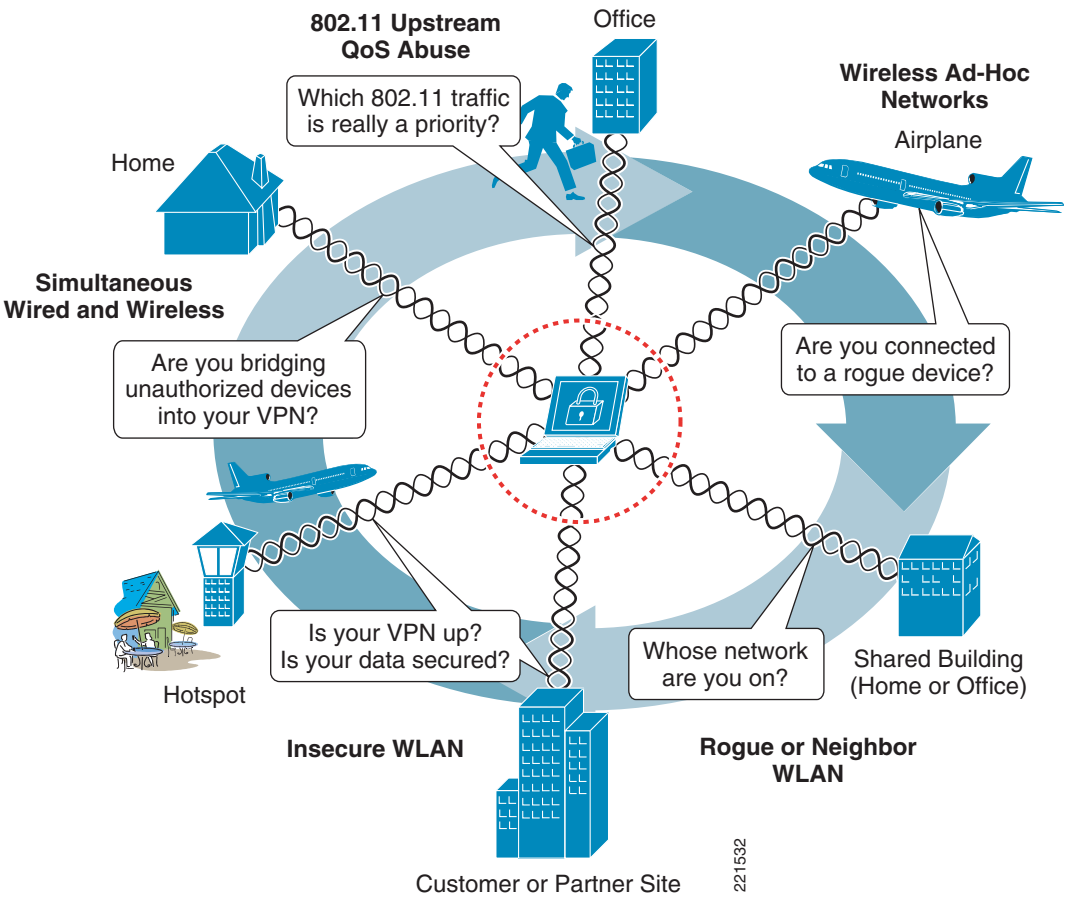


Table 1 lists a summary of the key WLAN-specific security threats that CSA can be used to mitigate, along with the CSA wireless security features to enable them. Each of these areas is addressed in more detail in subsequent sections.

Table 1 Key WLAN-Specific Security Threats and CSA Mitigation Features

WLAN-specific Security Threat	Security Concern	CSA Feature
Wireless ad-hoc connections	• Typically an insecure, unauthenticated, unencrypted connection • High risk of connectivity to unauthorized or rogue device	• Wireless ad-hoc pre-defined rule module[1] • Restricts wireless ad-hoc traffic
Simultaneous wired and wireless connections	• Risk of bridging traffic from insecure wireless networks or rogue devices to a wired network • Bypasses standard network security measures	• Simultaneous wired and wireless pre-defined rule module[1] • Restricts wireless traffic if Ethernet active
Connection to non-corporate, insecure, unauthorized, rogue, or incorrect WLAN	• Strong authentication or encryption may not be in use, if at all • Risk of sniffing, MITM, rogue network connectivity, and so on • Increased risk of theft of information	• Location-aware policy enforcement including pre-defined rule module to force use of VPN when roaming, plus ability to restrict permitted SSIDs[1] • May enforce stronger security policy when on insecure and non-corporate networks
802.11 upstream QoS abuse and lack of support	• Traffic QoS marking violations can be abused to attempt DoS attacks, bandwidth hogging, priority queue jumping, and so on • Many legacy devices and applications lack support for QoS marking	• Trusted QoS Markings[2] • Upstream QoS policy enforcement by marking or re-marking DiffServ settings on packets sent from the client

1. CSA location-aware policy enforcement was introduced in CSA v5.2 and includes pre-defined rule modules to address wireless ad-hoc and simultaneous wired and wireless connections, to force VPN use when roaming, as well as the ability to restrict the SSIDs to which a client may connect.
2. The CSA Trusted QoS Marking feature was introduced in CSA v5.0.

Note CSA wireless-specific policies should be used to complement and extend general CSA security policies, which should already be enforced for general endpoint protection of wired and wireless clients and servers, as outlined in the previous section.

CSA and Complementary WLAN Security Features

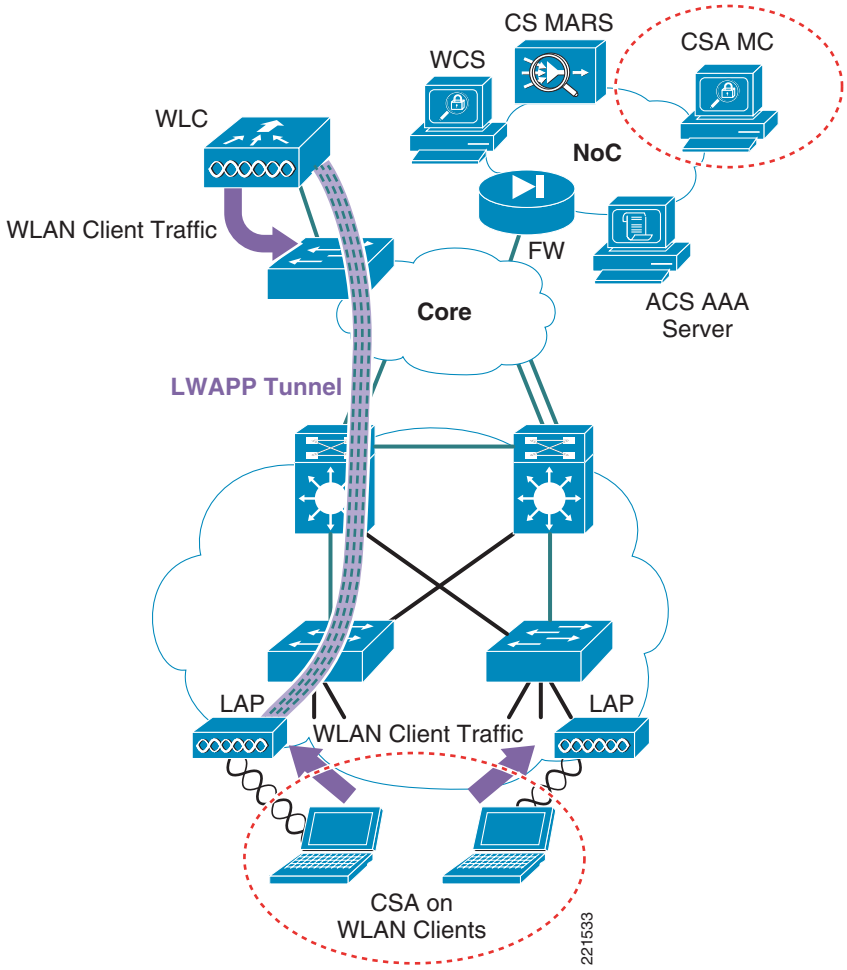
The Cisco Secure Wireless Network features a number of complementary security features that support its integrated, defense-in-depth approach. Some of the WLAN security threats addressed by CSA, as outlined in Table 1, can be detected and mitigated on the network-side through complementary features of the Cisco Secure Wireless Network. For instance, the wireless IDS/IPS features of the Cisco WLAN Controller (WLC) provide threat detection and mitigation of wireless ad-hoc and rogue networks.

CSA is complementary to these network-side security features of the Cisco Secure Wireless Network, addressing these threats from a client endpoint perspective, no matter to which WLAN the client may be connected. Features such as these are key to creating an integrated, defense-in-depth approach to security.

CSA Integration with the Cisco Unified Wireless Network

Integration of CSA within the Cisco Secure Wireless Network architecture involves CSA deployment on WLAN clients and deployment of a Cisco Management Center for Cisco Security Agents (CSA MC). (See Figure 3.)

Figure 3 CSA Integration within the Cisco Secure Wireless Network Architecture

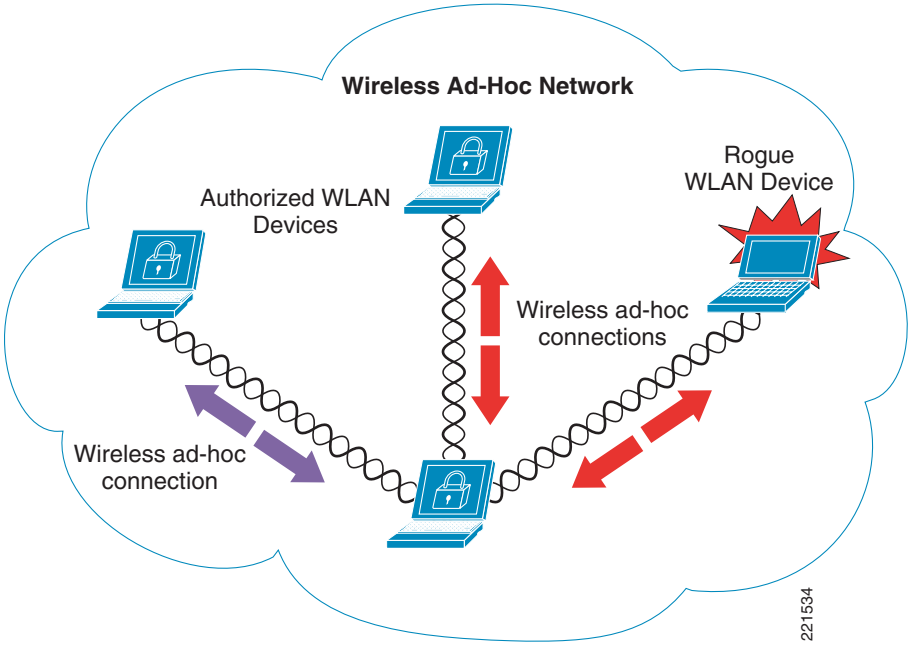


Wireless Ad-Hoc Connections

A wireless ad-hoc network is when two or more wireless nodes communicate directly on a peer-to-peer basis with no wireless network infrastructure. This is also referred to as an independent basic service set (IBSS).

Wireless ad-hoc networks are typically formed on a temporary basis to rapidly enable communication between hosts, such as to exchange files during a spontaneous meeting or between hosts at home. (See Figure 4.)

Figure 4 Sample Wireless Ad-hoc Network



Wireless Ad-hoc Networks—Security Concerns

Wireless ad-hoc connections are generally considered a security risk for the following reasons:

- Typically little or no security

  In general, wireless ad-hoc connections are implemented with very little security; no authentication, no access control, no encryption, and so on. Consequently, this represents a security risk even between authorized devices, as well as to the client itself, data being transferred, and any clients or networks that are connected to it.

- Endpoint at significant risk of connecting to a rogue device

  Endpoints are at risk of connecting to a rogue device because of the lack of security typically associated with a wireless ad-hoc connection.

- Endpoint at significant risk of insecure connectivity even with an authorized device

  This is an inherent risk because of the lack of security typically associated with a wireless ad-hoc connection.

- Risk of bridging a rogue wireless ad-hoc device into a secure, wired network

Simultaneous use of a wireless ad-hoc and a wired connection may enable bridging of a rogue device into a wired network.

- Microsoft Windows native WLAN client vulnerability

  When a wireless ad-hoc profile is configured, the default behavior of Microsoft Wireless Auto Configuration creates a significant risk of connectivity to a rogue device, particularly because a user may not even be aware that an 802.11 radio is enabled. The Microsoft Wireless Auto Configuration feature corresponds to the Wireless Configuration service in Windows Server 2003 and the Wireless Zero Configuration service in Windows XP.

  For links to more detailed information on Microsoft Wireless Auto Configuration behavior and an article outlining an exploit for this vulnerability, see Appendix B—Sample Customized Wireless Ad-Hoc Rule Module, page 49.

CSA Wireless Ad-Hoc Connections Pre-Defined Rule Module

CSA v5.2 introduced a pre-defined Windows rule module to address wireless ad-hoc connections, which is called “Prevent Wireless Adhoc communications”.

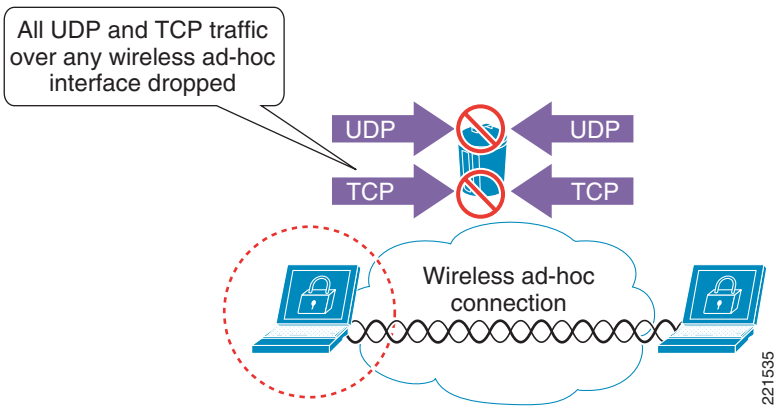
This rule module can be enforced to provide endpoint threat protection against wireless ad-hoc connections.

Pre-Defined Rule Module Operation

The default behavior of the pre-defined wireless ad-hoc Windows rule module (see Figure 5) can be summarized as follows:

If a wireless ad-hoc connection is active, all UDP or TCP traffic over any active wireless ad-hoc interface is denied, regardless of the application or IP address.

Figure 5 CSA Pre-defined Wireless Ad-hoc Windows Rule Module Operation



The default behavior of the pre-defined wireless ad-hoc Windows rule module is as follows:

- UDP or TCP traffic detected on an active wireless ad-hoc interface invokes the rule module. This is true regardless of whether any other network connections are active or not.
- All UDP and TCP traffic routed over a wireless ad-hoc interface is dropped.
- Traffic on a non-wireless ad-hoc interface is not affected by this rule module.
- No user query is performed.

- A message is logged.
- When no wireless ad-hoc connections are active, the rule module is revoked.
- No logging occurs after revocation of a rule module.

Pre-Defined Rule Module Operational Considerations

Cisco recommends that customers wishing to implement wireless ad-hoc policy enforcement consider the following operational aspects of the pre-defined wireless ad-hoc rule module:

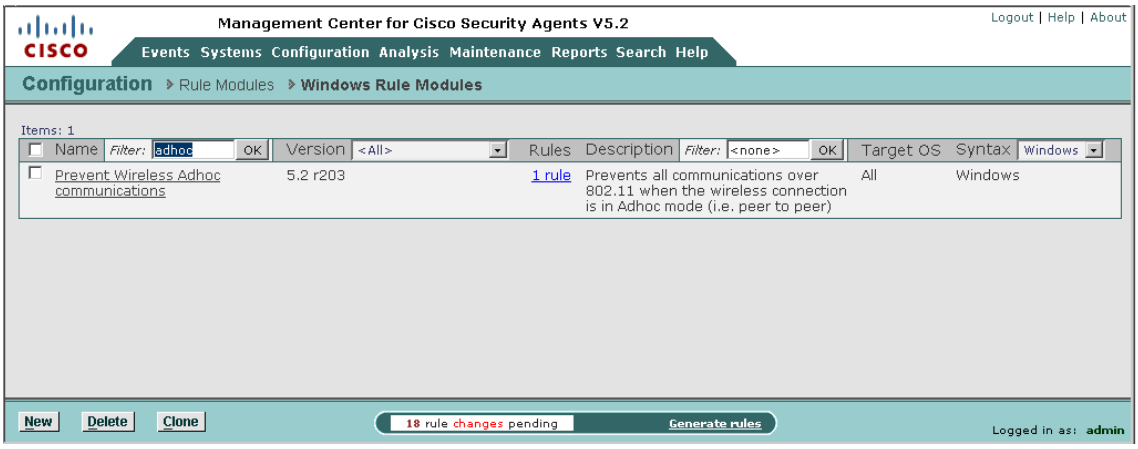
- Wireless ad-hoc connection status
  - New wireless ad-hoc connections continue to be initiated and accepted.
  - Established wireless ad-hoc connections remain active, connected, and a security risk.
  - End users continue to see wireless ad-hoc connections as active and connected.
- Traffic filtering
  - Only UDP and TCP traffic over a wireless ad-hoc connection is dropped.
  - Ensure that additional CSA security measures are in place to protect clients from non-UDP and non-TCP attacks.
  - Sessions based on UDP or TCP that are already established over a wireless ad-hoc interface cease to function upon the rule module being invoked because the return IP address is that of the wireless ad-hoc IP address, which is now being filtered. Sessions need to be re-established through a non-wireless ad-hoc interface.
  - ICMP pings that route over a wireless ad-hoc interface are not filtered by default by this rule module and remain a threat.
  - Incoming ICMP packets can be filtered by enforcing a CSA Network Shield rule module.
  - It is not currently possible to enforce the filtering of outgoing ICMP packets.
  - Outgoing ICMP continues to function over wireless ad-hoc interfaces, even if a CSA Network Shield rule module is enforced. This may present some confusion to end users because the wireless ad-hoc interfaces are active and connected, and ICMP pings continue to function, but connections appear to “not be working properly”.
  - Ensure that operational staff are aware that an outgoing ICMP ping from a client continues to work even when the rule module is being enforced.
- Routing table
  - The routing table is not updated upon the rule module being enforced, because all wireless ad-hoc interfaces remain connected and active.
  - If a wireless ad-hoc interface has routing precedence for a particular destination host IP or network, all UDP and TCP transactions with a route to or via this destination cease to function upon the rule module being invoked.
  - If the preferred route for a destination is over a wireless ad-hoc interface, all traffic to that destination is dropped, even if an alternative route exists over an alternative, non-wireless ad-hoc interface, because wireless ad-hoc interfaces remain active.
  - Ensure that operational staff are aware that some applications (UDP and TCP-based) may fail if a preferred route exists over a wireless interface on which the policy is being enforced.
- Wireless ad-hoc connections should be monitored on the network-side as an integral part of WLAN threat detection and mitigation on a corporate network. This can be achieved on a Cisco Unified Wireless Network using the wireless IDS/IPS features of the WLC.

Pre-Defined Rule Module Configuration

The pre-defined wireless ad-hoc rule module is a Windows rule module with the name “Prevent Wireless Adhoc communications”.

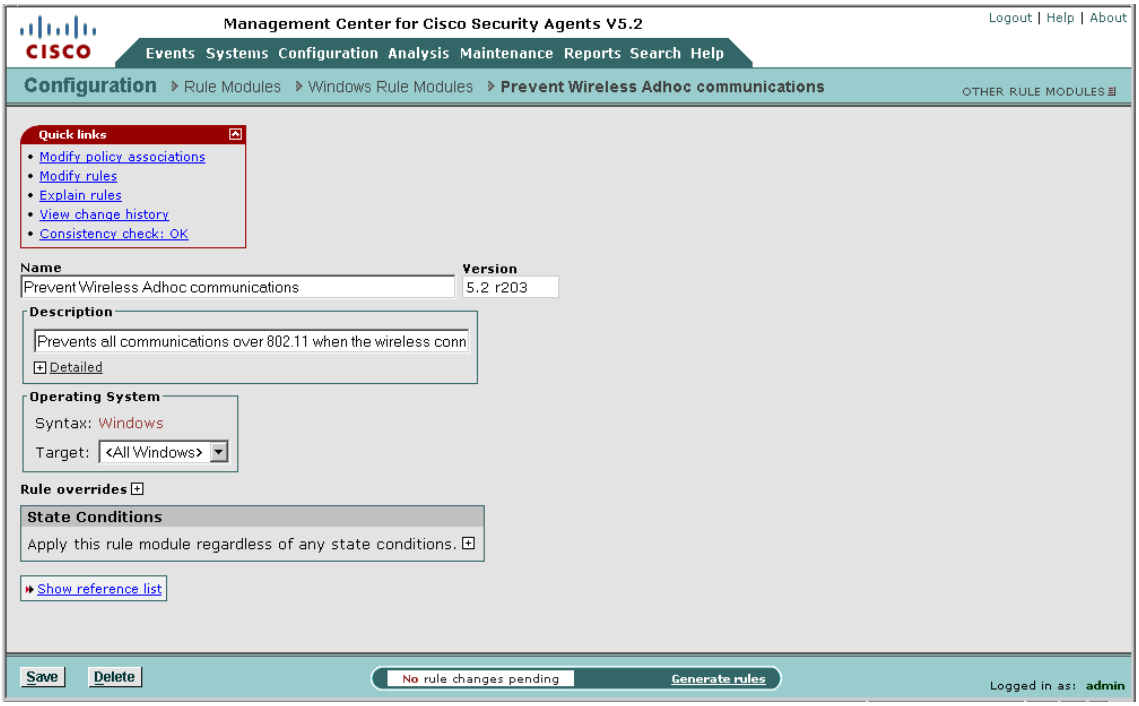
It can be located on the CSA MC by browsing to Configuration -> Rule Modules -> Rule Modules [Windows]. Defining a filter with the name “adhoc” allows it to be quickly located. (See Figure 6.)

Figure 6 Pre-defined Wireless Ad-hoc Windows Rule Module Listing



Clicking the name of the rule module presents the description, operating system, and state conditions associated with this rule module. (See Figure 7.)

Figure 7 Pre-defined Wireless Ad-hoc Windows Rule Module Definition



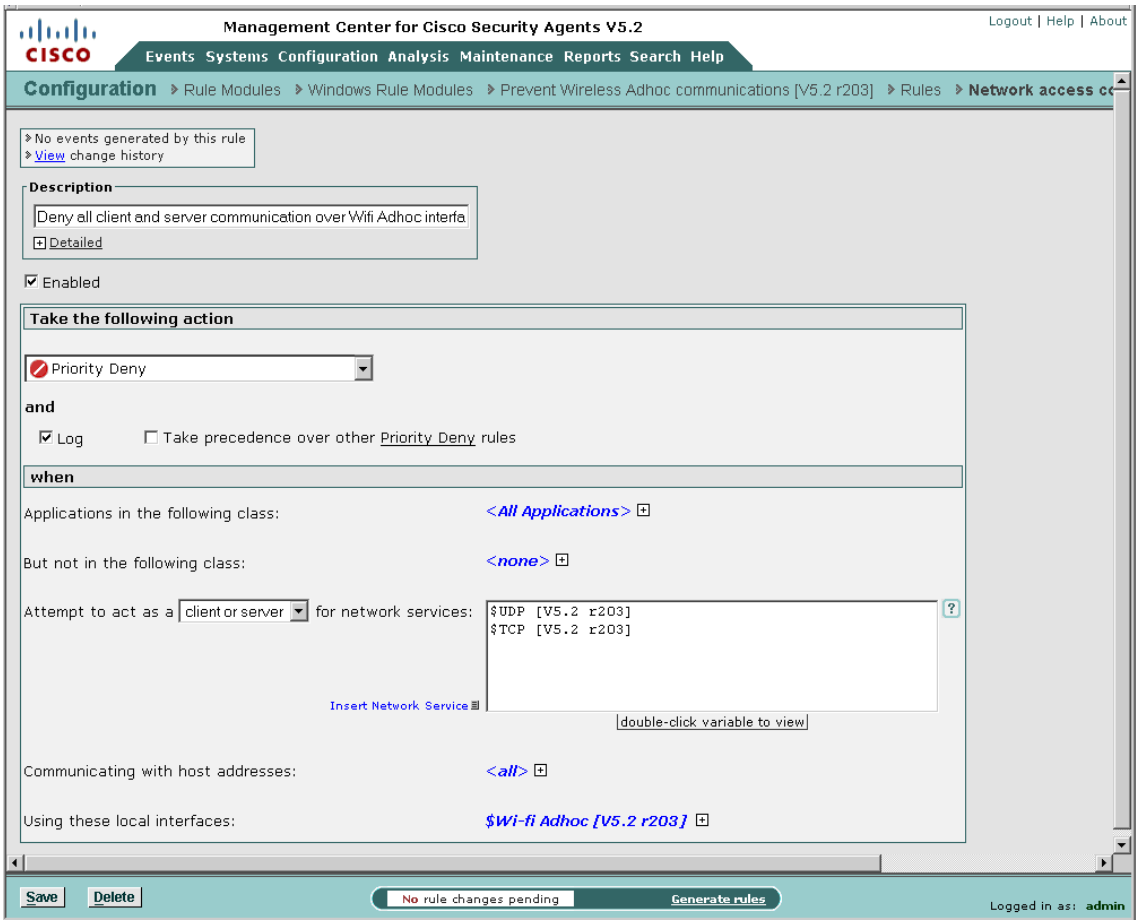
Clicking the Modify rules link presents the associated rule. (See Figure 8.) This may also be accessed directly from the rule module listing by clicking the “1 rule” link.

Figure 8 Rule Associated with the Pre-defined Wireless Ad-hoc Windows Rule Module

Note The rule numbers vary depending on the particular system being used.

Clicking the rule name presents the detailed configuration of the rule. (See Figure 9.)

Figure 9 Pre-defined Wireless Ad-hoc Rule Configuration



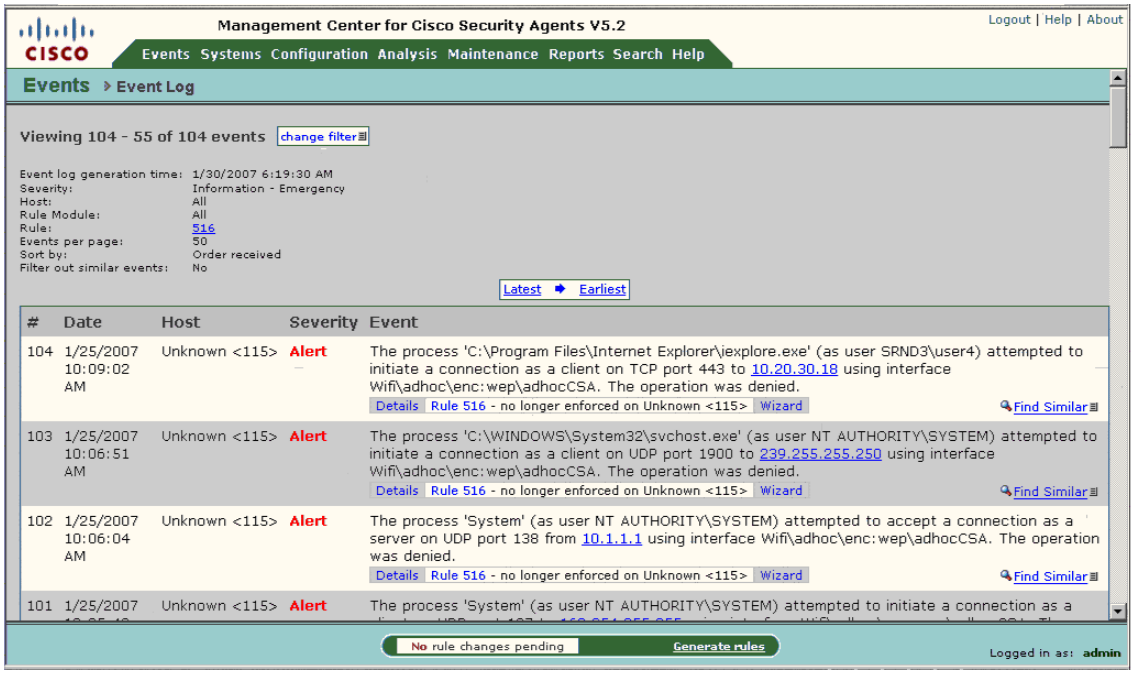
This shows the detailed configuration of the rule whereby any UDP or TCP traffic over a wireless ad-hoc interface is denied, regardless of the application or IP address.

Pre-Defined Rule Module Logging

The pre-defined wireless ad-hoc Windows rule module has event logging enabled by default.

An alert is generated for each unique instance that the rule module is triggered. By default, an event log entry is created only once per hour for the same scenario. A sample log entry is shown in Figure 10.

Figure 10 CSA MC Event Log Generated by Pre-defined Wireless Ad-hoc Windows Rule Module



Wireless Ad-Hoc Rule Customization

Customers wishing to implement wireless ad-hoc policy enforcement may wish to consider the following options for a customized wireless ad-hoc rule module:

- Customized user query as a rule action—A customized wireless ad-hoc rule module can be developed that presents a user query, notifying the end user of the risks associated with a wireless ad-hoc connection to educate them on the security risks.
- Customized rule module in test mode—A customized wireless ad-hoc rule module can be deployed in test mode to enable administrators to gain visibility into wireless ad-hoc connection events without changing the end-user experience.

A sample customized wireless ad-hoc rule featuring a customized user query as a rule action, along with configuration steps, is presented in Appendix B—Sample Customized Wireless Ad-Hoc Rule Module, page 49.

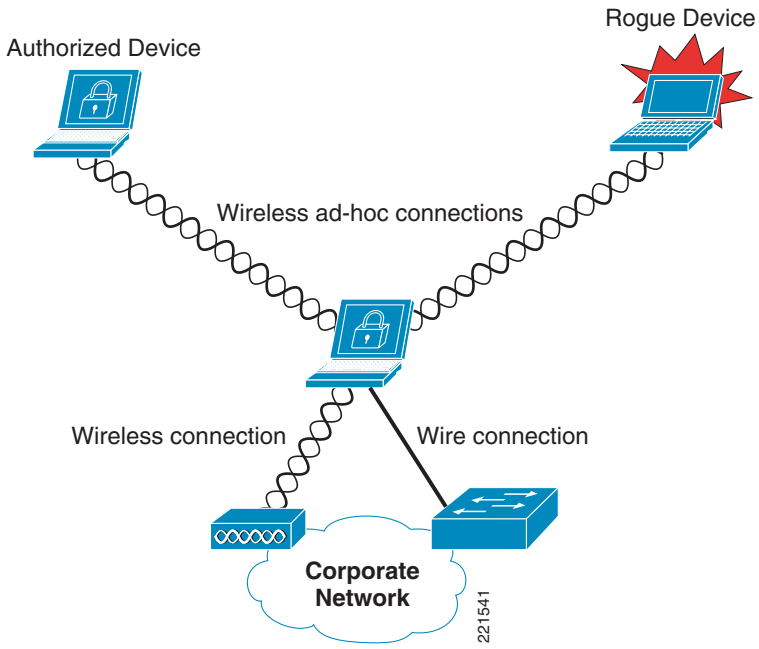
Note The business requirements and security policy of each individual customer vary and must be reviewed and applied on a per-case basis before deployment.

Simultaneous Wired and Wireless Connections

Simultaneous wired and wireless connections are when a client has an active connection on a wired network (typically, over Ethernet), as well as an active wireless connection, such as to an open WLAN, a secure WLAN, a wireless ad-hoc network, or any other type of wireless connection. (See Figure 11.)

This is commonly encountered when users connect to a WLAN while in a meeting, and then return to their desk, connecting back into their docking station.

Figure 11 Simultaneous Wired and Wireless Connections



Simultaneous Wired and Wireless Connections—Security Concerns

Simultaneous wired and wireless connections are typically considered a security risk for the following reasons:

- Risk of bridging a rogue device into a secure, wired network

  Simultaneous use of a wired and a wireless connection may enable bridging of a rogue device into the wired network.

- Risk of bridging an authorized device into the wired network

  Simultaneous use of a wired and a wireless connection may enable bridging of an authorized device into the wired network, thereby bypassing network security measures and policies.

- Lack of end-user awareness

  Users often unwittingly leave their 802.11 radio enabled. Depending on the wireless profiles configured on a client, this may create an opportunity for a rogue device to wirelessly connect to the client and bridge onto the wired network using an insecure or wireless ad-hoc profile. This commonly occurs when a user uses a non-corporate WLAN, such as a public hotspot, an unauthenticated home WLAN, or insecure partner site; and, some time later, connects to a wired network, such as the corporate LAN.

CSA Simultaneous Wired and Wireless Connections Pre-Defined Rule Module

CSA v5.2 introduced a pre-defined rule module to address simultaneous wired and wireless connections, which is called “Prevent Wireless if Ethernet active”.

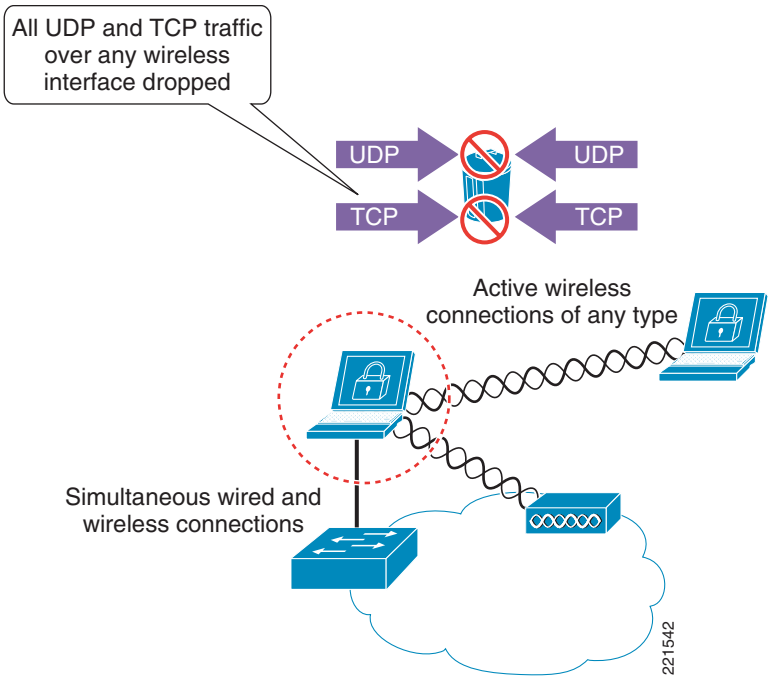
This rule module can be enforced to provide general network policy enforcement, protecting the network infrastructure and resources as well as the clients themselves.

Pre-Defined Rule Module Operation

The default behavior of the pre-defined simultaneous wired and wireless Windows rule module (see Figure 12) can be summarized as follows:

If an Ethernet connection is active, all UDP or TCP traffic over any active wireless interface is denied, regardless of the application or IP address.

Figure 12 CSA Pre-defined Simultaneous Wired and Wireless Windows Rule Module Operation



The pre-defined simultaneous wired and wireless Windows rule module involves the following elements:

1. If an Ethernet connection is active, UDP or TCP traffic detected on any active wireless interface invokes the rule module. This is true regardless of the type of wireless connection, including open, ad-hoc, and secure wireless connections.
2. All UDP and TCP traffic routed over any wireless interface is dropped.
3. Traffic on a non-wireless interface is not affected by this rule module.
4. No user query is performed.
5. A message is logged.
6. When no Ethernet connection is active, the rule module is revoked.
7. No logging occurs after revocation of a rule module.

Pre-Defined Rule Module Operational Considerations

Cisco recommends that customers wishing to implement wireless ad-hoc policy enforcement consider the following operational aspects of the pre-defined simultaneous wired and wireless ad-hoc rule module:

- Wireless connection status
  - New wireless connections continue to be initiated and accepted even if an Ethernet interface is active.
  - Established wireless connections remain active and connected despite an Ethernet interface being active.
  - End users continue to see wireless connections as active and connected.
- Traffic filtering

  - Only UDP and TCP traffic over a wireless interface is dropped.
  - Ensure that additional CSA security measures are in place to protect clients from non-UDP and non-TCP attacks.
  - Sessions based on UDP or TCP that are already established over a wireless interface, before simultaneously connecting to a wired interface, cease to function upon the rule module being invoked because the return IP address is that of the wireless IP address, which is now being filtered. Sessions need to be re-established through a non-wireless interface.
  - ICMP pings that route over a wireless interface are not filtered by default by this rule module and remain a threat.
  - Incoming ICMP packets can be filtered by enforcing a CSA Network Shield rule module.
  - It is not currently possible to enforce the filtering of outgoing ICMP packets.
  - Outgoing ICMP continues to function over wireless interfaces, even if a CSA Network Shield rule module is enforced. This may present some confusion to end users because the wireless interfaces are active and connected, and ICMP pings continue to function, but connections appear to “not be working properly”.
  - Ensure that the operational staff is aware that an outgoing ICMP ping from a client continues to work even when the rule module is being enforced.

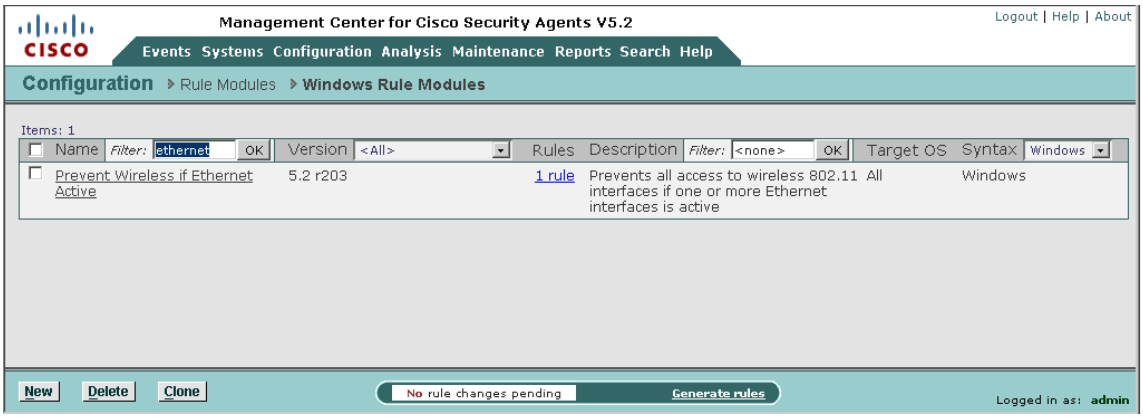
- Routing table
  - The routing table is not updated upon the rule module being enforced, because all wireless interfaces remain connected and active.
  - If a wireless interface has routing precedence for a particular destination host IP or network, all UDP and TCP transactions with a route to or via this destination cease to function upon the rule module being invoked.
  - If the preferred route for a destination is over a wireless interface, all traffic to that destination is dropped, even if an alternative route exists over an alternative, non-wireless interface, because wireless interfaces remain active.
  - Ensure that operational staff are aware that some applications (UDP and TCP-based) may fail if a preferred route exists over a wireless interface on which policy is being enforced.
- Wireless ad-hoc connections should be monitored on the network side as an integral part of WLAN threat detection and mitigation on a corporate network. This can be achieved on a Cisco Unified Wireless Network using the wireless IDS/IPS features of the WLC.

Pre-Defined Rule Module Configuration

The pre-defined simultaneous wired and wireless rule module is a Windows rule module with the name “Prevent Wireless if Ethernet active”.

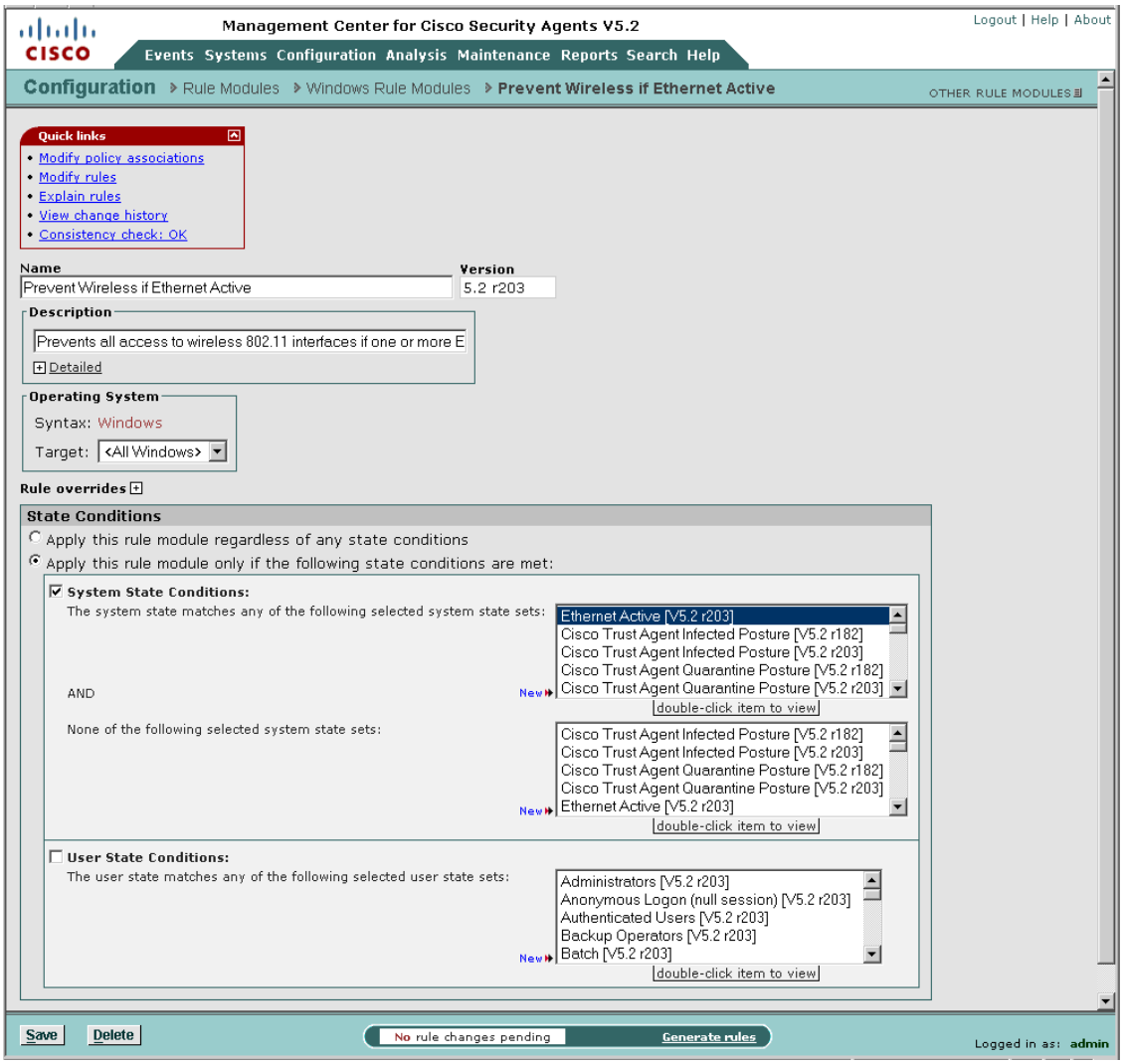
It can be located on the CSA MC by browsing to Configuration -> Rule Modules -> Rule Modules [Windows]. (See Figure 13.) Defining a filter with the name “ethernet” allows it to be quickly located.

Figure 13 Pre-defined Simultaneous Wired and Wireless Windows Rule Module Listing



Clicking the name of the rule module presents the description, operating system, and state conditions associated with this rule module. (See Figure 14.)

Figure 14 Pre-defined Simultaneous Wired and Wireless Windows Rule Module Configuration

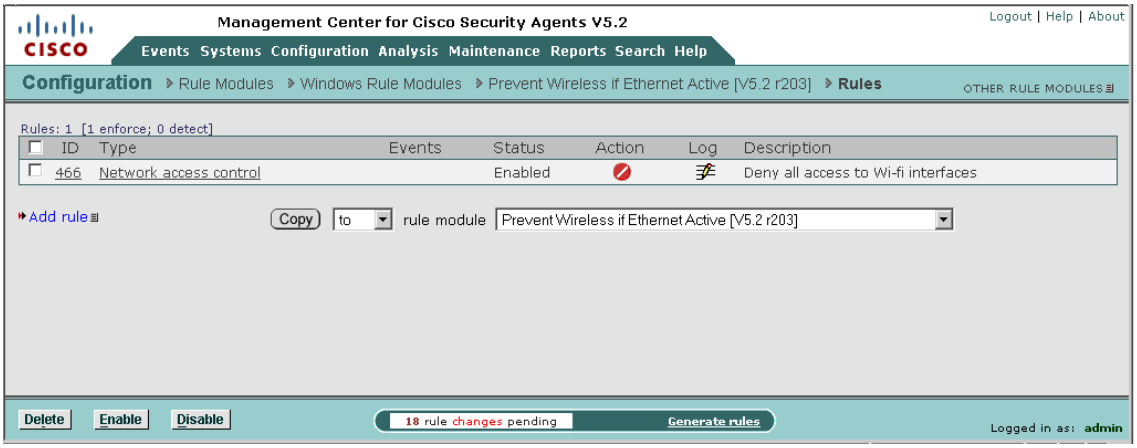


This shows the state condition that exists for this rule, whereby the Ethernet interface must be active for the rule be invoked.

Clicking the Modify rules link presents the rule summary. (See Figure 15.)

This may also be accessed directly from the rule module listing by clicking the “1 rule” link. (See Figure 13.)

Figure 15 Rule Associated with the Pre-defined Simultaneous Wired and Wireless Windows Rule Module



Note The rule numbers vary depending on the particular system being used.

Clicking the rule name presents the detailed configuration of the rule. (See Figure 16.)

Figure 16 Pre-defined Simultaneous Wired and Wireless Rule Configuration

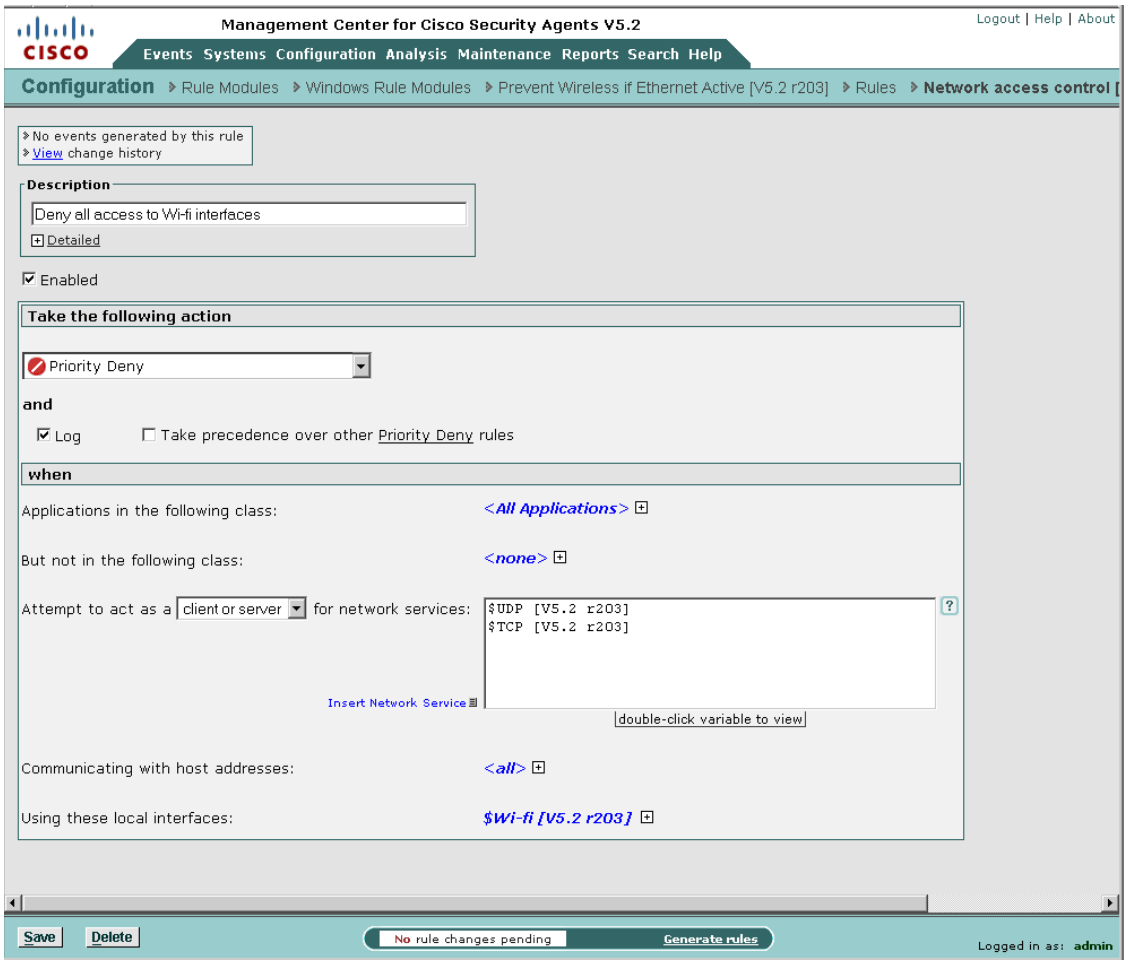


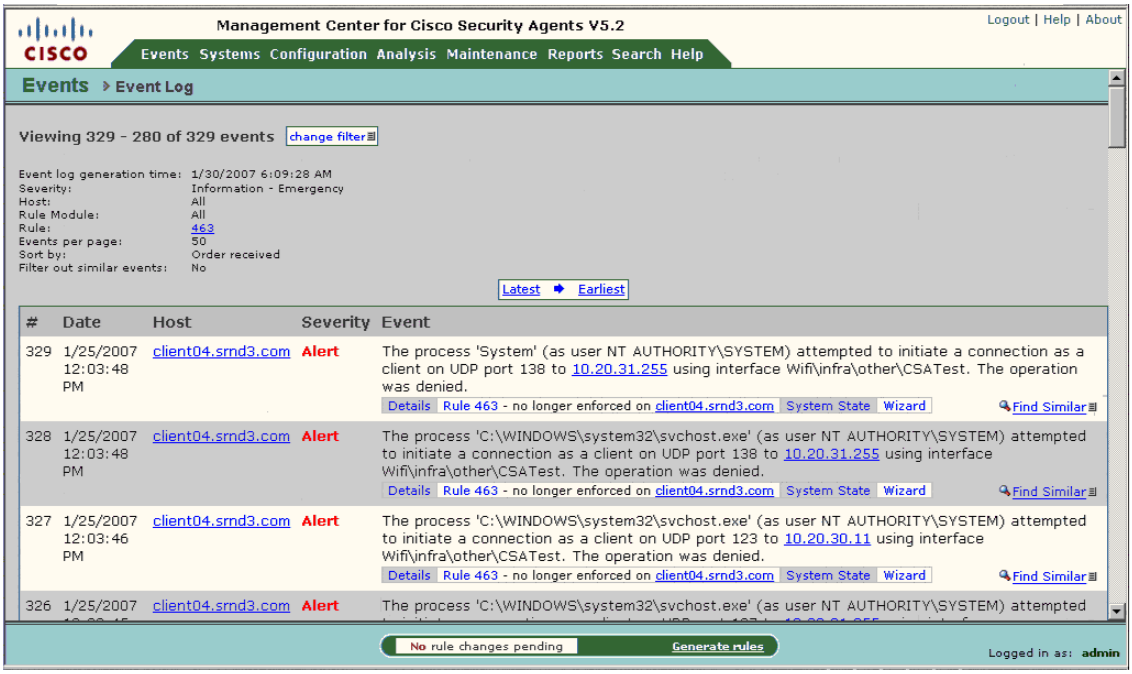
Figure 16 shows the detailed configuration of the rule, whereby if an Ethernet connection is active, all UDP or TCP traffic over all active wireless interface is denied, regardless of the application or IP address.

Pre-Defined Rule Module Logging

The pre-defined simultaneous wired and wireless Windows rule module has event logging enabled by default.

An alert is generated for each unique instance that the rule module is triggered. By default, an event log entry is created only once per hour for the same scenario. A sample log entry is shown in Figure 17.

Figure 17 CSA MC Event Log Generated by Pre-defined Simultaneous Wired and Wireless Rule Module



Simultaneous Wired and Wireless Rule Customization

Customers wishing to implement simultaneous wired and wireless policy enforcement may wish to consider the following options for a customized simultaneous wired and wireless rule module:

- Customized user query as a rule action—A customized simultaneous wired and wireless rule module can be developed that presents a user query, notifying the end user of the risks associated with simultaneous wired and wireless connections to educate them on the security risks.
- Customized rule module based on location—A customized simultaneous wired and wireless rule module can be developed to permit simultaneous wired and wireless connections if the wireless connection is to the corporate WLAN but deny traffic to other WLANs. See Location-Aware Policy Enforcement, page 23 for more information on this topic.
- Customized rule module in test mode—A customized simultaneous wired and wireless rule module can be deployed in test mode to enable administrators to gain visibility into simultaneous wired and wireless events without changing the end-user experience.

A sample customized simultaneous wired and wireless rule featuring a customized user query as a rule action, along with configuration steps, is presented in Appendix C—Sample Customized Simultaneous Wired and Wireless Rule Module, page 58.

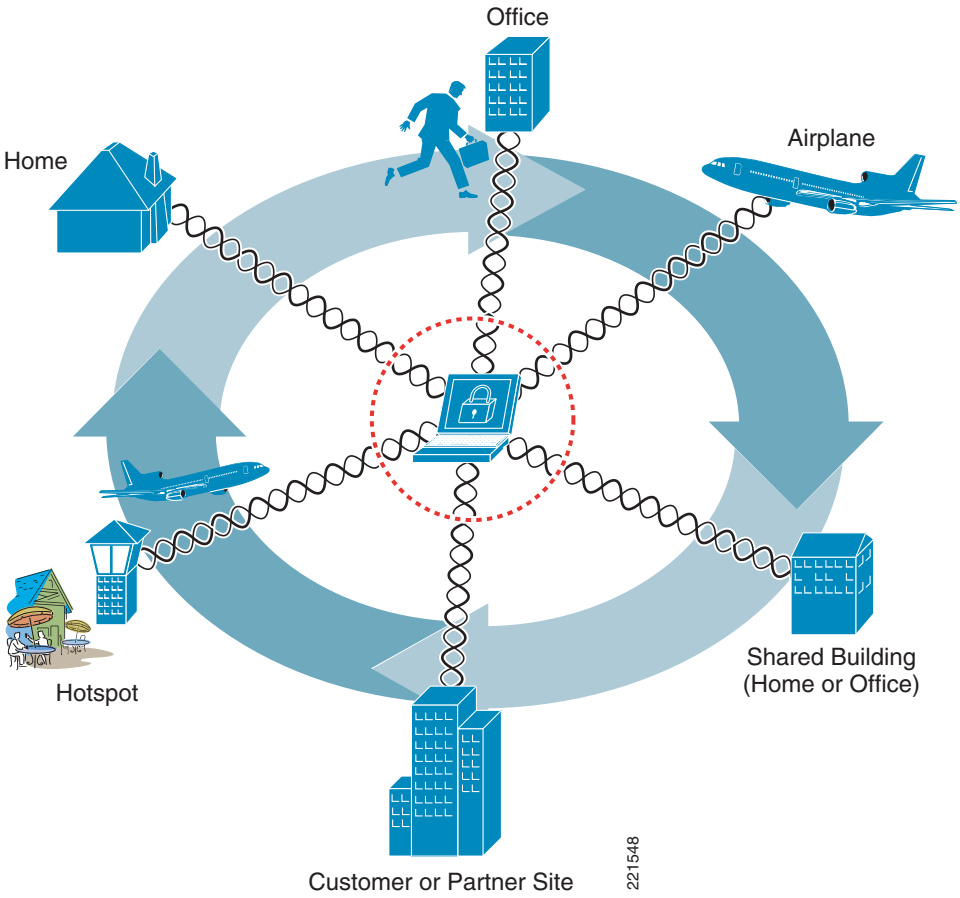
Note The business requirements and security policy of each individual customer vary and must be reviewed and applied on a per-case basis before deployment.

Location-Aware Policy Enforcement

Location-aware policy enforcement refers to the ability to enforce different or additional security policies according to the network to which a client is connected, based on the perceived security risk associated with each location (see Figure 18). A roaming WLAN client may connect to the following common locations and networks:

- Corporate office
- Home
- Hotspots
- Customer or partner sites

Figure 18 Possible Locations and Networks to which a Roaming WLAN Client May Connect



Security Risks Addressed by Location-Aware Policy Enforcement

Clients that connect to different networks in different locations are considered to be exposed to greater security risks for the following reasons (see Figure 19):

- Exposure to networks with different security and protection levels

  Different locations present inherently different security risks. For instance, the security risks associated with wireless connectivity to an open, public hotspot are far greater than those associated with wired or wireless connectivity to a secure corporate network.

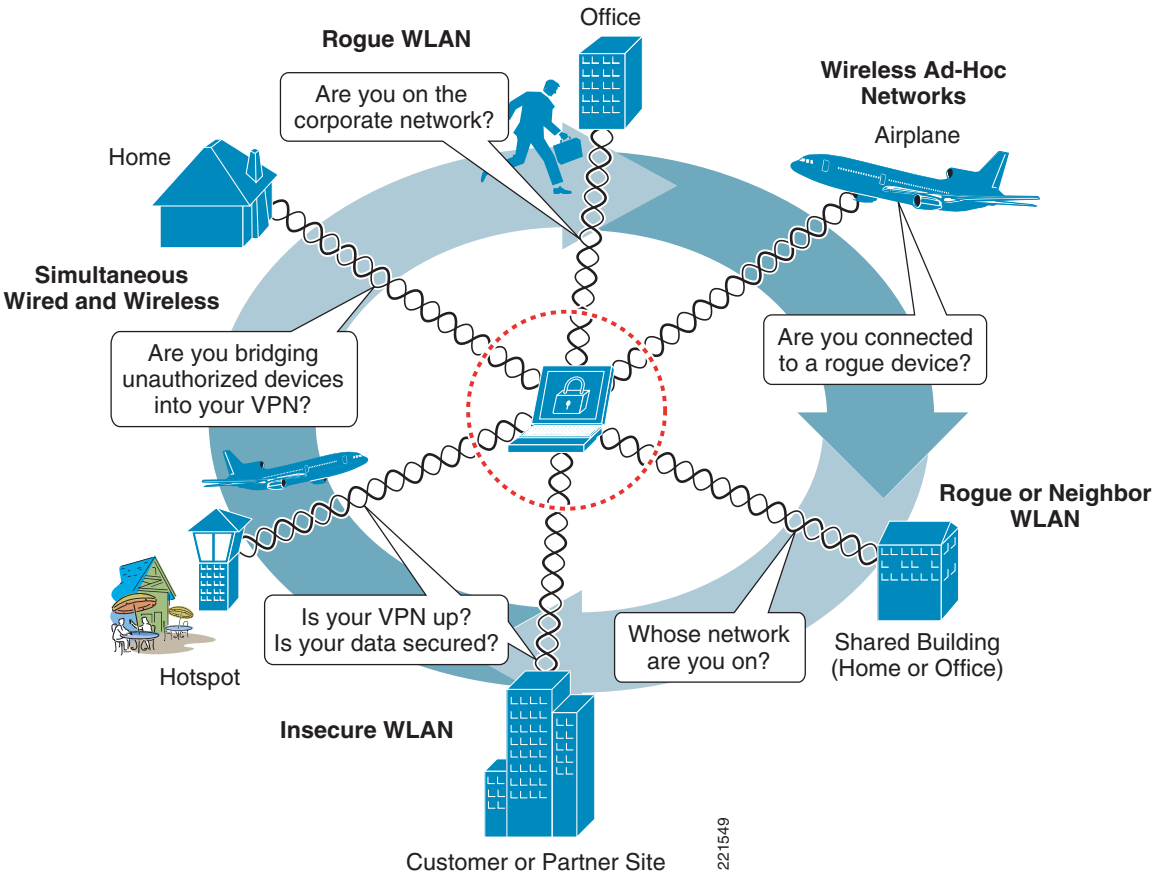
- Lack of user awareness of an active WLAN connection

  The end user of a WLAN client with multiple WLAN profiles may not always know to which, if any, WLAN they are connected. This may result in a user maliciously or unwittingly connecting to a rogue network.

  For instance, a user on a plane may use a hotspot or home network before boarding, then disconnect their VPN but not disable their 802.11 radio. If they use their laptop on the plane, they may unwittingly connect to a rogue network, operated by a fellow passenger, spoofing the hotspot or their home network.

  Similarly, a user in a shared building may think they are connected to the corporate WLAN but may, in fact, be connected to a neighbor WLAN.

Figure 19 Possible Security Concerns Associated with Connecting in Different Locations



CSA Location-Aware Policy Enforcement

CSA offers the ability to enforce different security policies based on the location of a client. This enables the security protection measures enforced to be adapted according to the security risks to which a client may be exposed in any particular location.

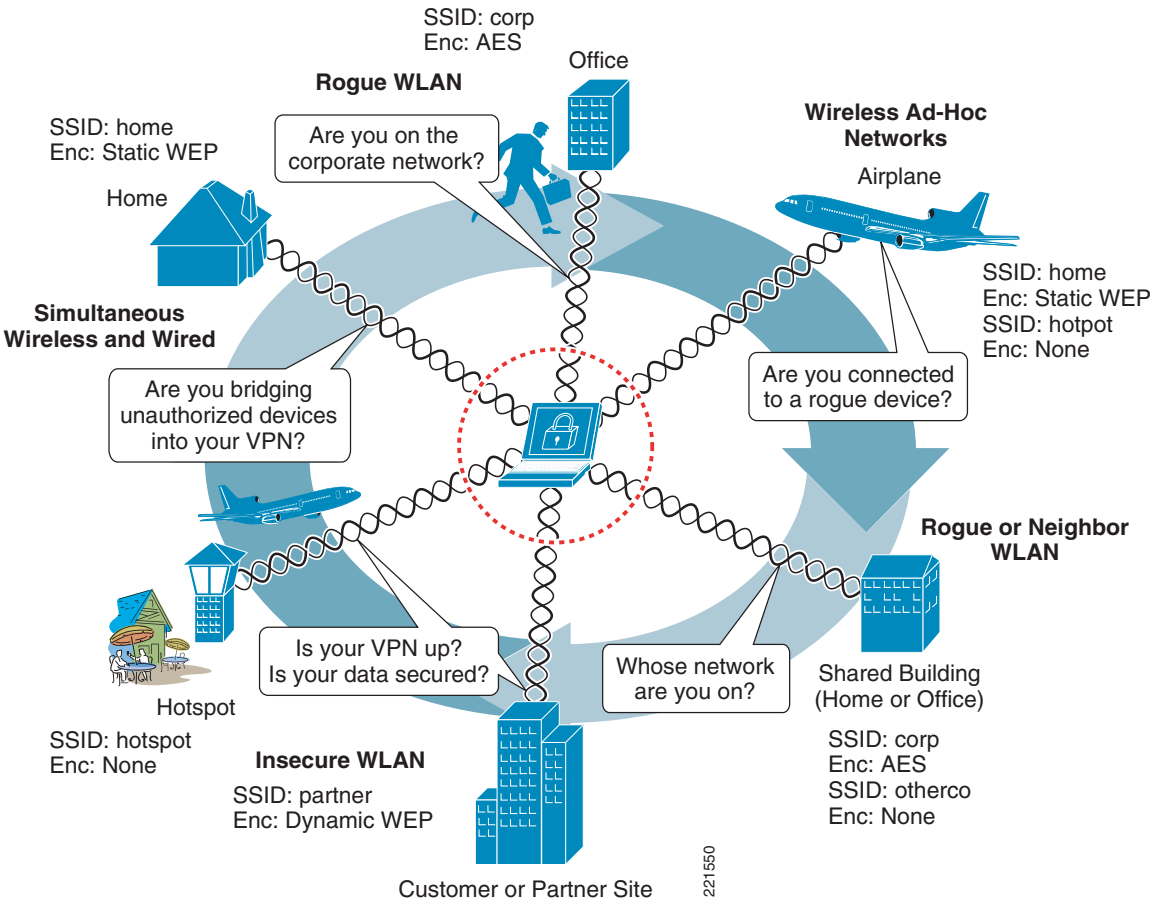
Location-Aware Policy Enforcement Operation

CSA currently enables the location of a client to be determined based on the following criteria:

- System state conditions, including the following:
  - Ethernet active
  - CSA MC reachability
  - Cisco Trust Agent posture
  - Network interface sets
  - DNS server suffix; for example, cisco.com
  - System security level
- Network interface set characteristics, including the following:
  - Network connection type; for example, wired, Wi-Fi, Bluetooth, PPP
  - WLAN mode of infrastructure or ad-hoc
  - Wireless SSID
  - Wireless encryption type; for example, AES, WEP, TKIP
  - Network address range

After CSA identifies the location of a client, the particular security policies to be enforced in that location are determined by the associated CSA policy rules. A CSA location-aware policy may leverage any of the standard CSA features, using pre-defined or custom rules, to adapt the security measures enforced on the client to the security risks associated with the location and network to which a client is currently connected. (See Figure 20.)

Figure 20 Possible Location-Aware Policy Enforcement



CSA v5.2 also introduced a pre-defined location-aware Windows rule module called "Roaming - Force VPN". This rule module leverages system state conditions and interface sets to apply rules that force the use of VPN if a client is out of the office. For more details, see CSA Force VPN When Roaming Pre-Defined Rule Module, page 34.

Table 2 shows sample locations, the criteria that can be leveraged to identify them, and possible policies that they may be used to enforce.

Table 2 Sample Location-Aware Policy Enforcement

Location	Location Identification			Sample Location-Aware Policy
	Corporate Connectivity[1]	Connection Type		
		Ethernet	WLAN	
Office	Yes	Yes	No	Standard security policy[2]
	Yes	No	Corporate[3]	
	Yes	Yes	Corporate[3]	
	Yes	Yes	Non-corporate	Rogue network policy Extension of standard security policy to include: • Drop all traffic on any wireless interface as rogue or insecure connection being bridged to secure wired network[4]
Home Hotspot Customer Partner	Yes	Yes	Non-corporate	
	No	Yes	No	Out-of-office policy Extension of standard security policy to include: • Lock down client, restrict access to confidential files and applications • May use pre-defined Roaming - Force VPN rule module to drop all traffic except HTTP/HTTPS until VPN connected Standard security policy applied once VPN connected[5]
	No	No	Non-corporate	
	Yes	No	Non-corporate	
	N/A	N/A	Ad-hoc	Wireless ad-hoc policy Extension of standard security policy to include: • Drop all traffic on any wireless ad-hoc interface[6]
Airplane	N/A	N/A	Ad-hoc	

1. Corporate Connectivity identified by ability to reach the CSA MC.
2. This sample standard security policy permits simultaneous wired and wireless connections if the wireless connection is to the corporate WLAN.
3. Corporate WLAN identified based on the corporate SSID AND encryption type. It is assumed that a corporate WLAN is enforcing strong authentication and encryption; for example, WPA2 with AES.
   Note that SSID alone is not sufficient to identify a WLAN, because a rogue network can easily be set up with the same SSID.
4. See Simultaneous Wired and Wireless Connections, page 14 for more information on this scenario and the CSA pre-defined Windows rule module.
5. Determined based on the ability to reach the CSA MC.
6. See Wireless Ad-Hoc Connections, page 7 for more information on this scenario and the CSA pre-defined Windows rule module.

In addition to the deployment of CSA, WLAN client features should be used to enforce the required authentication and encryption parameters for each authorized WLAN profile. The Cisco Secure Services Client (SSC) is client software offering 802.1x support for both wired and wireless networks, enabling simplified management and secure access through user and device identity, and the associated network access protocols. See Appendix B—Sample Customized Wireless Ad-Hoc Rule Module, page 49 for more details on this product.

Location-Aware Policy Enforcement Configuration

The creation of location-aware policies involves the following general steps on a per-location basis:

- Define the qualifying network interface sets.
- Define the qualifying system state conditions.
- Define a location-specific rule module.
- Define and associate the location-specific rules.
- Associate the location-specific rule module with an existing or new policy.
- Ensure that hosts on which a location-specific policy is to be enforced are members of a group that includes the location-specific policy.

Viewing and Defining Network Interface Sets

Pre-defined network interface sets and the creation of new network interface sets can be accessed on the CSA MC page by browsing to Configuration -> Variables -> Network Interface Sets. (See Figure 21.)

Figure 21 Pre-defined Network Interface Sets

Clicking the name of a network interface set presents its description and associated configuration parameters. (See Figure 22.)

Figure 22 Pre-defined Wi-Fi Network Interface Set

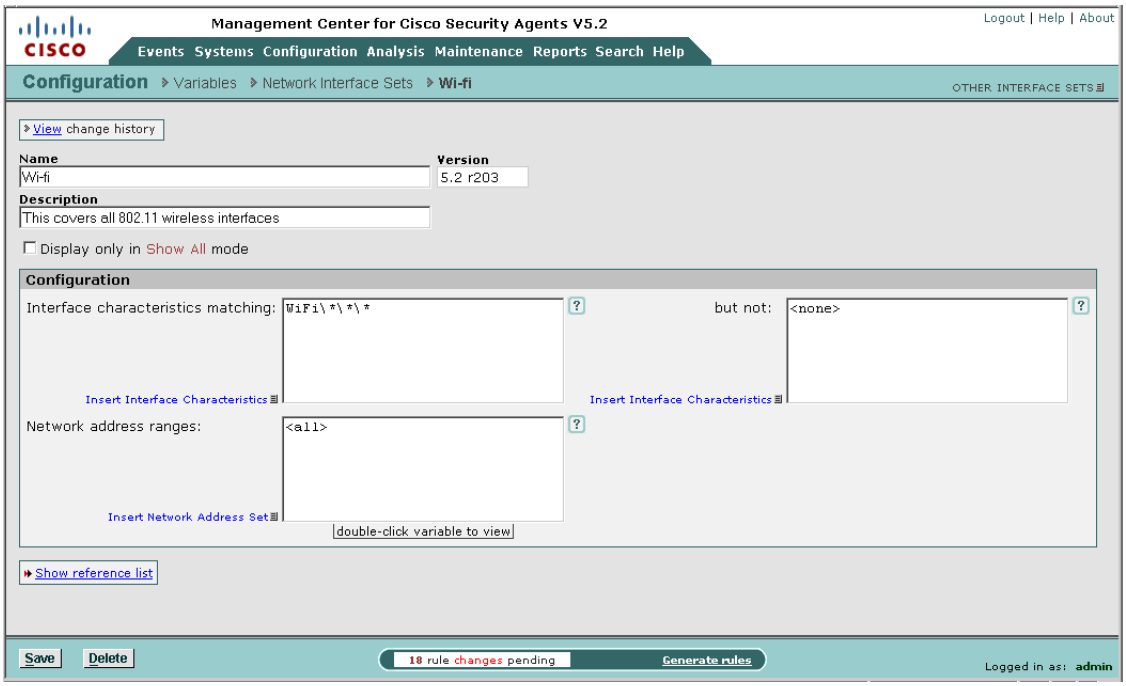


Figure 22 shows the pre-defined Wi-Fi network interface set that incorporates all wireless connections, regardless of mode, encryption, or SSID, as indicated by the wildcards in the interface characteristics definition “WiFi***”.

Network interface sets allow a number of parameters to be defined, depending on the type of connection. For instance, for a WLAN, parameters include the following (see Figure 23):

- Mode: infrastructure or ad-hoc
- Encryption; for example, WEP, AES, TKIP
- SSID

Figure 23 Configurable Wi-Fi Parameters and Sample Definition of a Corporate WLAN

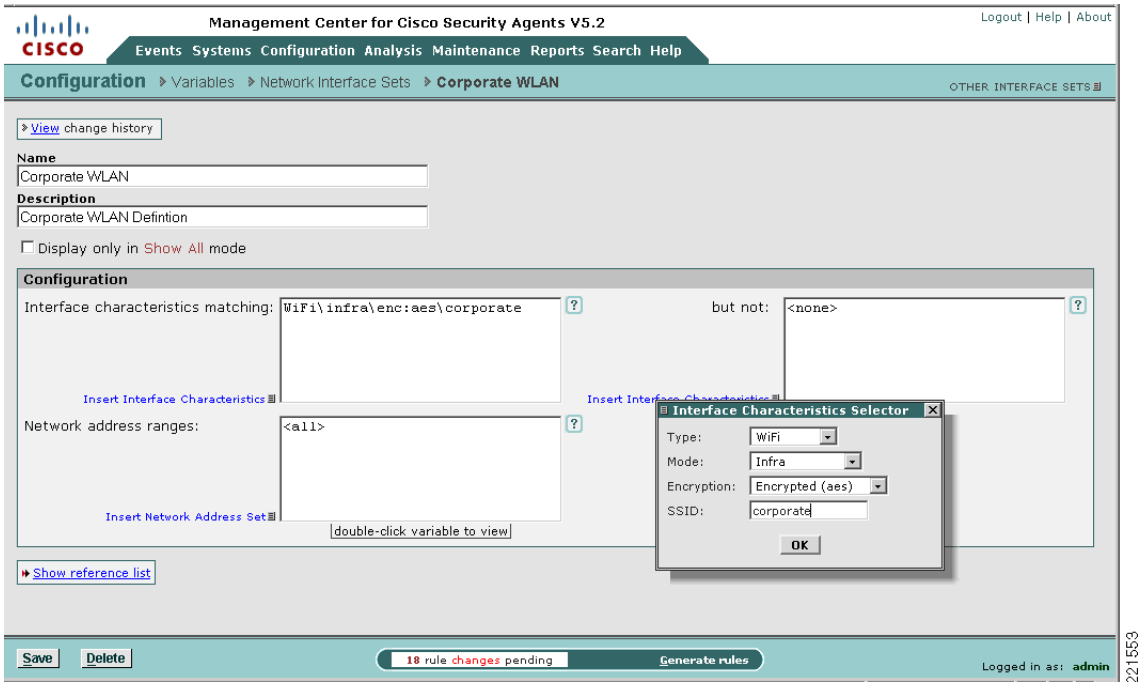
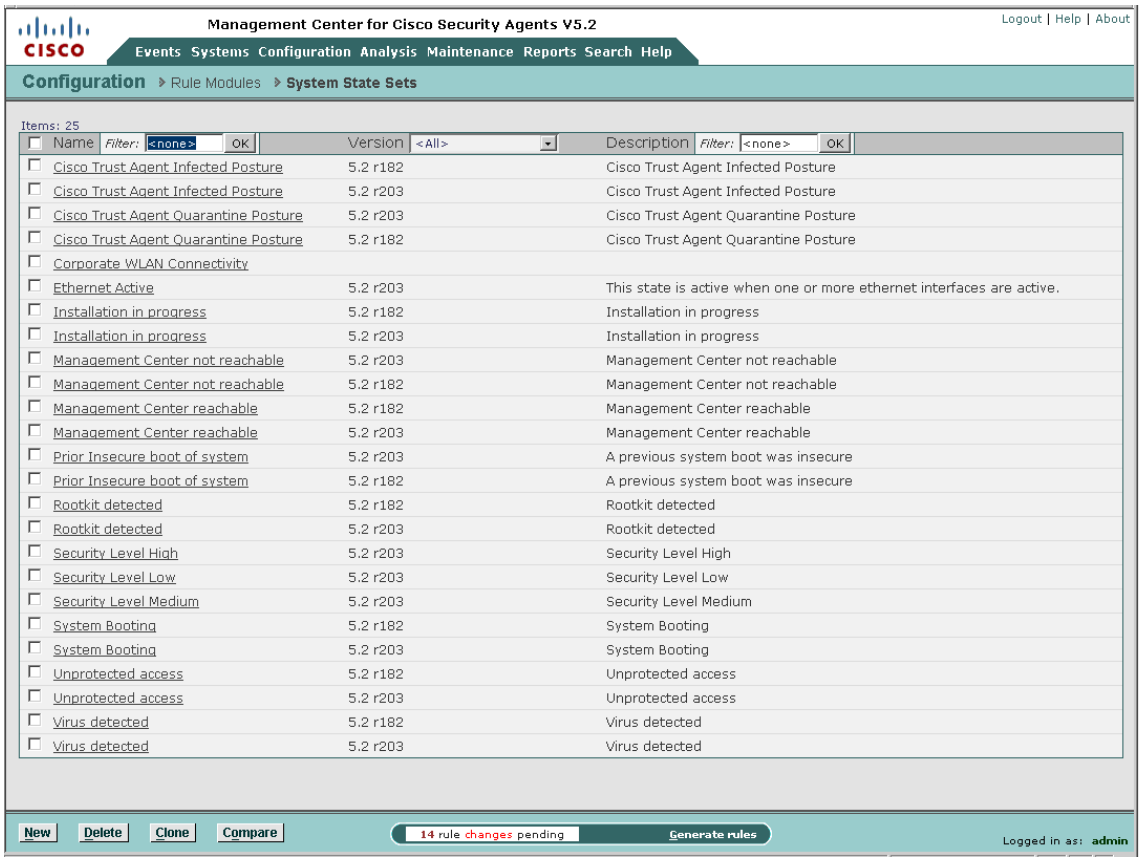


Figure 23 shows the network interface characteristics that can be defined for wireless connections, including mode, encryption, and SSID. Figure 23 also shows how a corporate WLAN can be defined.

Viewing and Defining System State Sets

Pre-defined system state sets and the creation of new system state sets can be accessed on the CSA MC by browsing to Configuration -> Rule Modules -> System State Sets. (See Figure 24.)

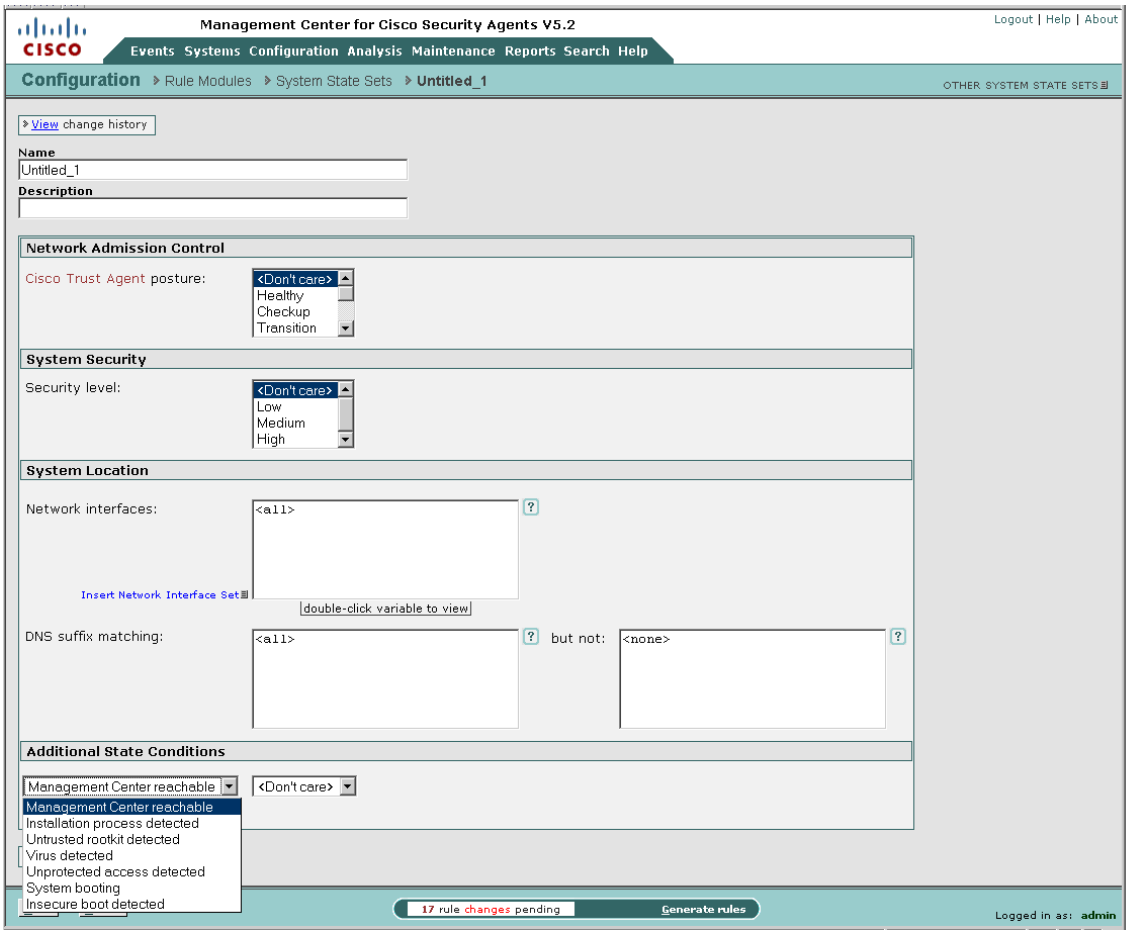
Figure 24 Pre-defined System State Sets



New system state sets can be created based on a number of parameters, including the following (see Figure 25):

- Cisco Trust Agent posture
- System security level
- System location, based on the following:
  - Network interface sets
  - DNS suffixes
- Additional state conditions, including Management Center reachability

Figure 25 Configurable Parameters for Custom System State Sets

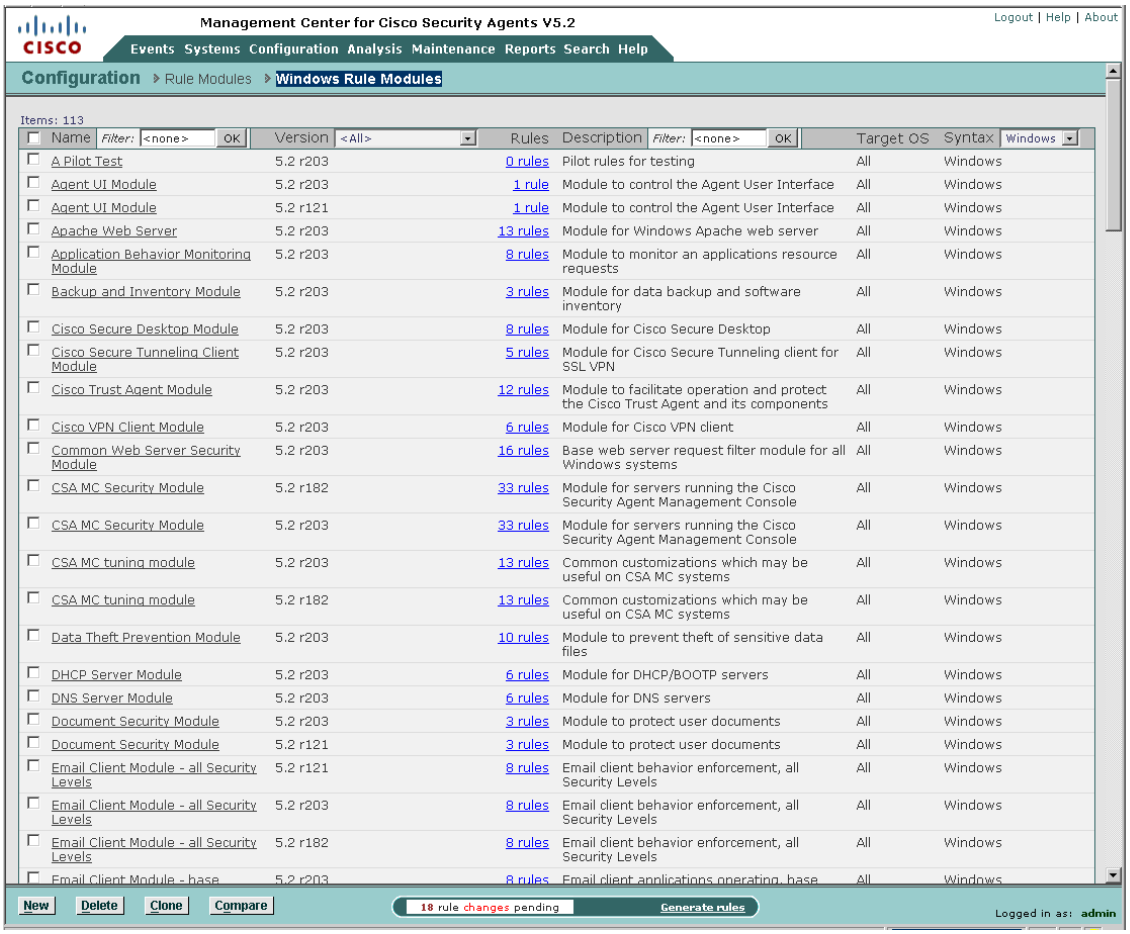


Viewing and Defining Location-Aware Rule Modules

Having defined the qualifying network interface and system state sets, a location-aware rule module can be created that leverages these sets to enforce particular rules according to the location.

Pre-defined Windows rule modules and the creation of a new Windows rule module can be accessed on the CSA MC page by browsing to Configuration -> Rule Modules -> Windows Rule Modules. (See Figure 26.)

Figure 26 Pre-defined Windows Rule Modules



The pre-defined Roaming - Force VPN Windows rule module is an example of how location-aware policy enforcement can be deployed. See CSA Force VPN When Roaming Pre-Defined Rule Module, page 34 for details.

General Location-Aware Policy Enforcement Configuration Notes

General location-aware policy enforcement configuration notes include the following:

- A network interface set can be defined with generic to very specific match characteristics; for example, a generic network interface set may include all wireless connections, and a specific network interface set may include only a particular WLAN profile, with a particular SSID and encryption type.
- A network interface set can include exceptions, such as a particular WLAN profile.
- A single network interface set can include multiple connection type characteristics; for example, a corporate network interface set can be defined with wired and WLAN characteristics.
- A system state condition is not required for rules associated with a particular network interface set to be applied.
- If system state conditions are defined, the rule module is invoked only if the system state conditions are met.

- Multiple qualifying system state conditions can be defined; for example, Ethernet active *and* Management Center not reachable.
- Per general CSA implementation requirements, for a policy to be applied on a host, the host must be a member of a group that includes the policy to be enforced.
- CSA group membership is additive, so a host can be a member of multiple groups.

CSA Force VPN When Roaming Pre-Defined Rule Module

CSA v5.2 introduced a pre-defined Windows rule module to force connectivity to the corporate network if a network connection is active. This rule module is called "Roaming - Force VPN".

In a roaming scenario, enforcement of this rule module can be used to protect the client itself, local data, and data in transit when on insecure, non-corporate networks.

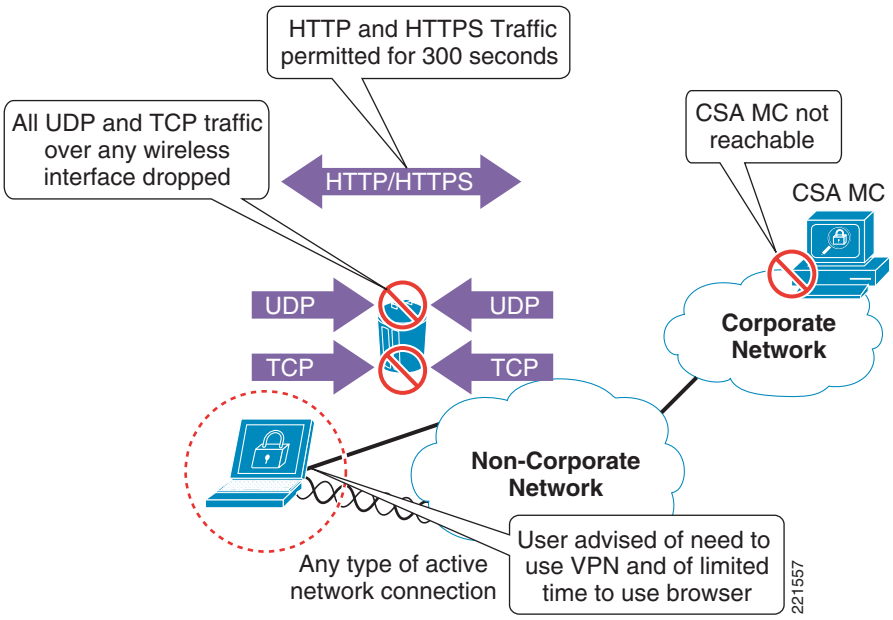
The rule module leverages the system state "CSA Management Center reachable" to determine whether a client is connected to the corporate network.

Pre-Defined Rule Module Operation

The default behavior of the pre-defined force VPN when roaming Windows rule module (see Figure 27) can be summarized as follows:

> If the CSA MC is not reachable and a network interface is active, all UDP or TCP traffic over any active interface is denied, regardless of the application or IP address, with the exception of web traffic, which is permitted for 300 seconds.

Figure 27 CSA Pre-defined Force VPN When Roaming Windows Rule Module Operation



The pre-defined force VPN when roaming Windows rule module involves the following elements:

- If the CSA MC is not reachable and the system is not booting, UDP or TCP traffic on any active interface invokes the rule module. This is true regardless of the type of interface being used.

- All UDP and TCP traffic routed over any interface is dropped, except HTTP or HTTPS traffic.
- HTTP or HTTPS traffic is permitted for a period of 300 seconds.
- A user query is presented, advising the user that they are not connected to the corporate network, that they must use the VPN client to gain access, and that they have limited time to use their browser to connect to a hotspot.
- A message is logged.
- If the CSA MC remains unreachable after expiration of the 300 seconds, all UDP or TCP traffic, including HTTP and HTTPS, is dropped.
- Upon the CSA MC becoming reachable, the rule module is revoked.
- No logging occurs upon revocation of a rule module.

Pre-Defined Rule Module Operational Considerations

Cisco recommends that customers wishing to deploy this pre-defined rule module to enforce connectivity to the corporate network when a client has an active interface consider the following aspects:

- Non-corporate network connectivity
  - All access to non-corporate networks is permitted only through the corporate network.
  - Local client connectivity to non-corporate networks is blocked upon this rule module being enforced.
- Timing considerations
  - By default, a user has only 300 seconds to establish local connectivity to a non-corporate network and establish VPN connectivity to the corporate network. This may require the user to connect, authenticate, subscribe, and enter billing information for a hotspot, then initiate, connect, and authenticate to the VPN.
- Network connection status
  - Network connections remain active even if the rule module is invoked and the timeout exceeded; however, traffic is dropped.
  - Network connections continue to be established and activated even if the rule module is invoked and the timeout exceeded.
  - End users continue to see network connections as active and connected, but UDP and TCP traffic is not passed.
- Traffic filtering
  - Only UDP and TCP traffic is dropped.
  - Ensure that additional CSA security measures are in place to protect clients from non-UDP and non-TCP attacks.
  - ICMP pings are not filtered by default by this rule module, and remain a threat.
  - Incoming ICMP packets can be filtered by enforcing a CSA Network Shield rule module.
  - It is not currently possible to enforce the filtering of outgoing ICMP packets.
  - Outgoing ICMP continues to function, even if a CSA Network Shield rule module is enforced. This may present some confusion to end users because the network interfaces are active and connected, and ICMP pings continue to function, but connections appear to “not be working properly”.

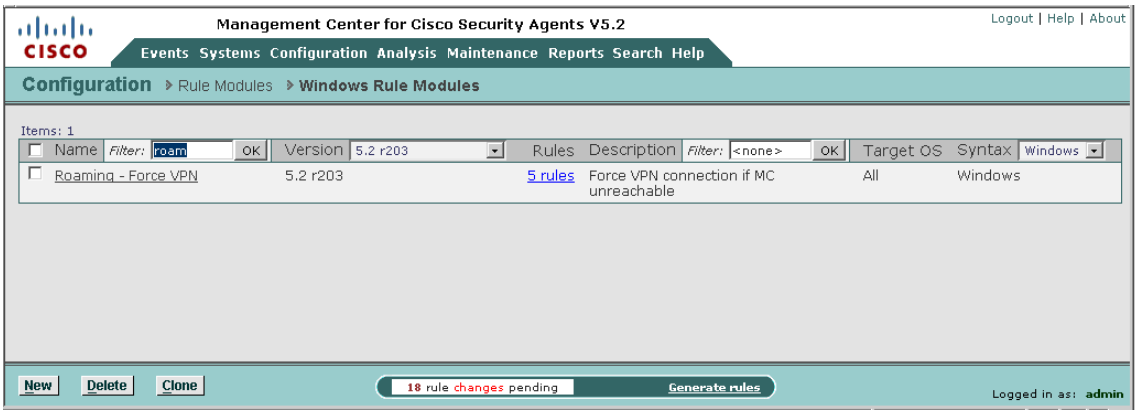
– Ensure that operational staff are aware that an outgoing ICMP ping from a client continues to work, even when the rule module is being enforced.

Pre-Defined Rule Module Configuration

The pre-defined Windows rule module to force connectivity to a corporate network is called “Roaming - Force VPN”.

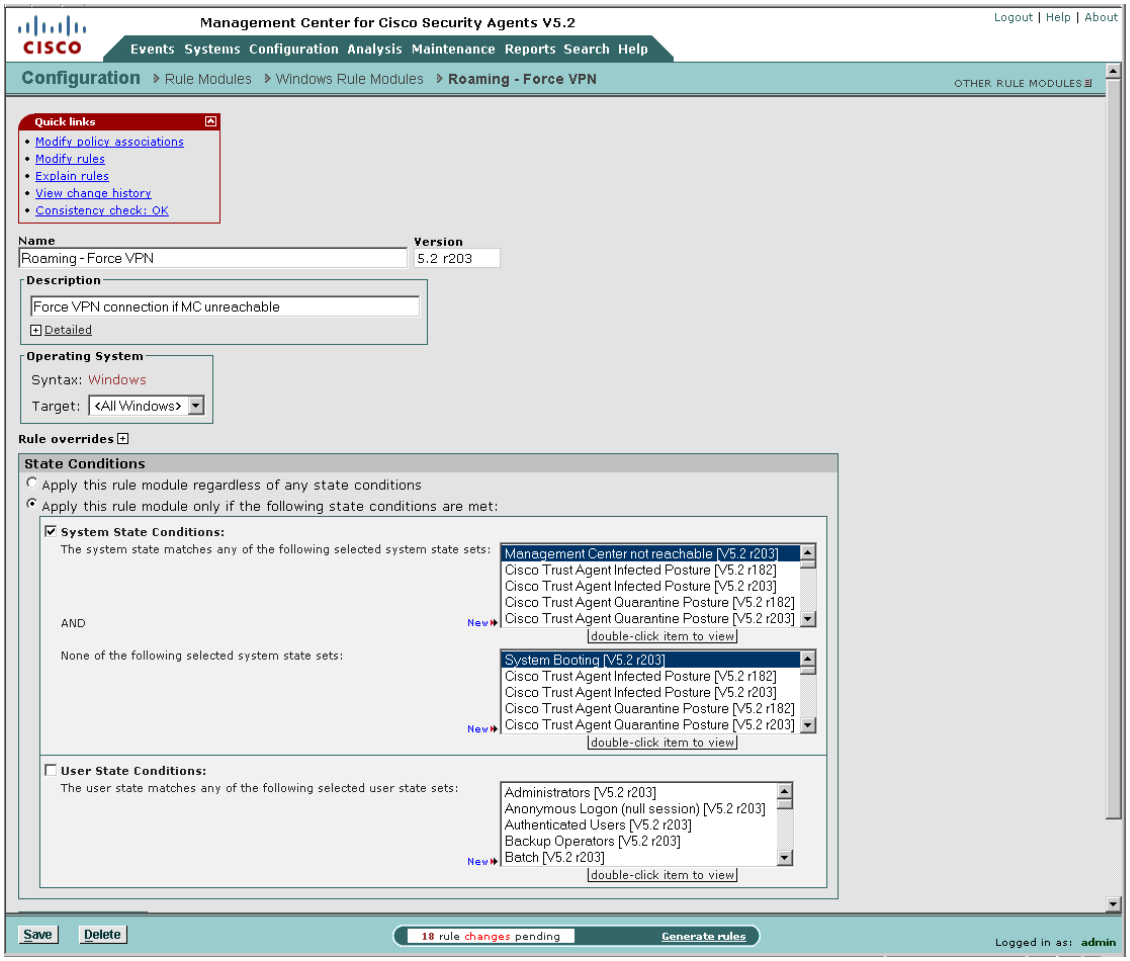
It can be located on the CSA MC by browsing to Configuration -> Rule Modules -> Rule Modules [Windows]. (See Figure 28.) Defining a filter with the name “roam” allows it to be quickly located.

Figure 28 Pre-Defined Force VPN When Roaming Windows Rule Module Listing



Clicking the name of the rule module presents the description, operating system, and state conditions associated with this rule module. (See Figure 29.)

Figure 29 Pre-Defined Force VPN When Roaming Windows Rule Module Definition

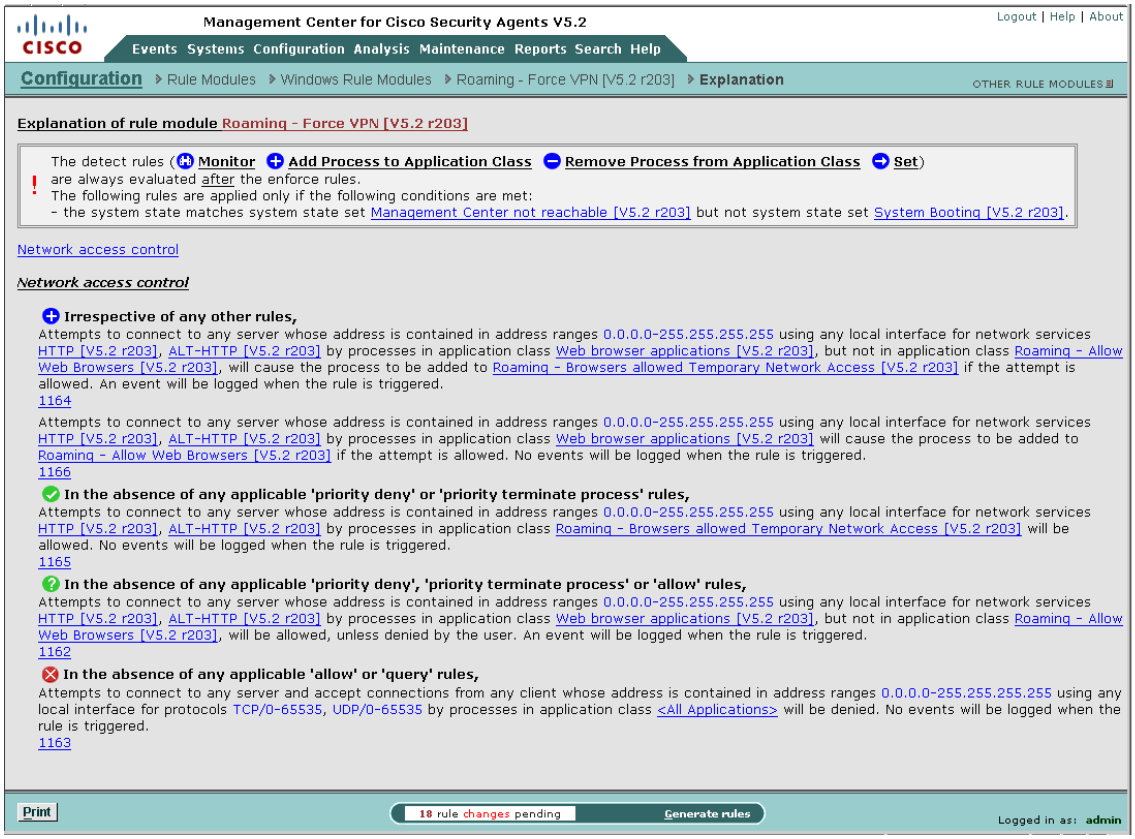


Note that the state conditions for this pre-defined rule module require the following conditions to be met for the rule to be invoked:

- Management Center not reachable
- System not booting

Clicking the Explain rules link presents an explanation of the rules and their associated actions. (See Figure 30.)

Figure 30 Explanation of the Rules Associated with Force VPN When Roaming Windows Rule Module



Alternately, clicking the Modify rules link of the rule module definition screen lists the associated rule. (See Figure 31.)

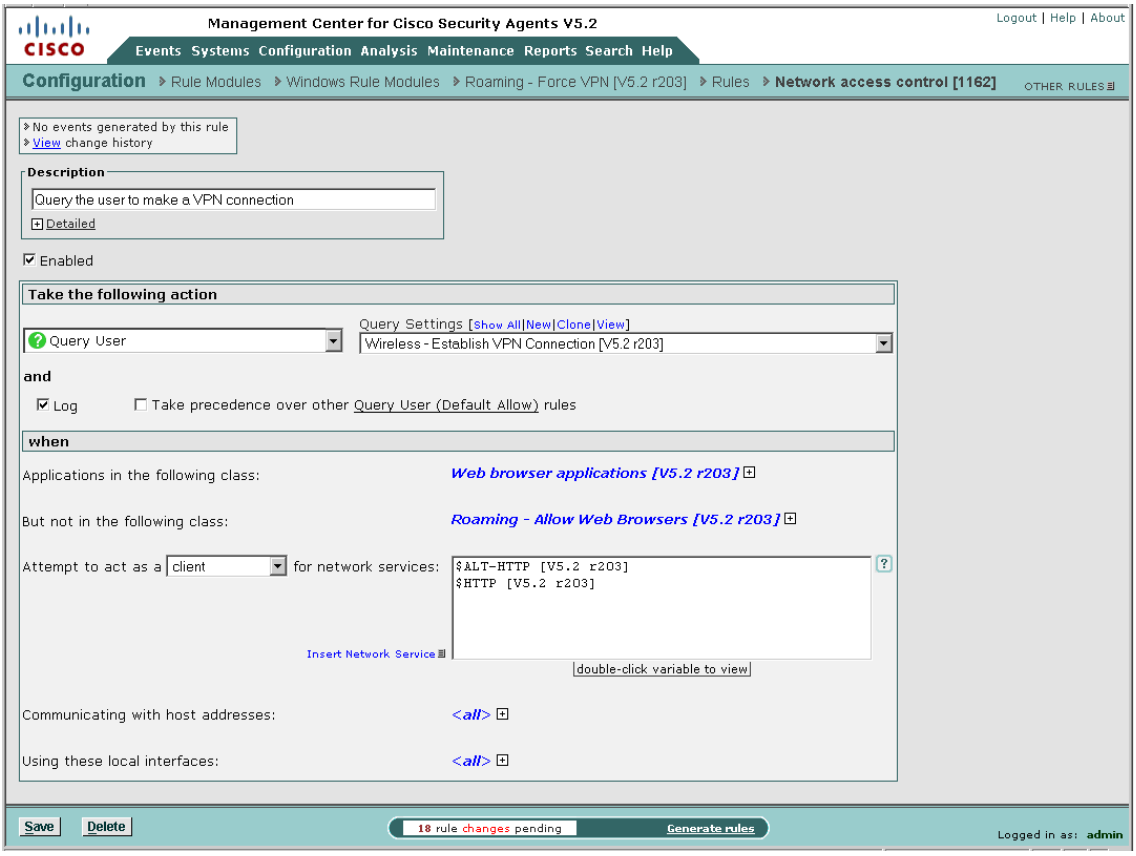
The rules may also be accessed directly from the rule module listing by clicking the “5 rules” link. (See Figure 28.)

Note The rule numbers vary depending on the particular system being used.

Figure 31 Rules Associated with the Force VPN When Roaming Windows Rule Module

Clicking a particular rule name presents the detailed configuration of that rule. (See Figure 32.)

Figure 32 Pre-Defined Network Access Control Rule to Query the User to Make a VPN Connection



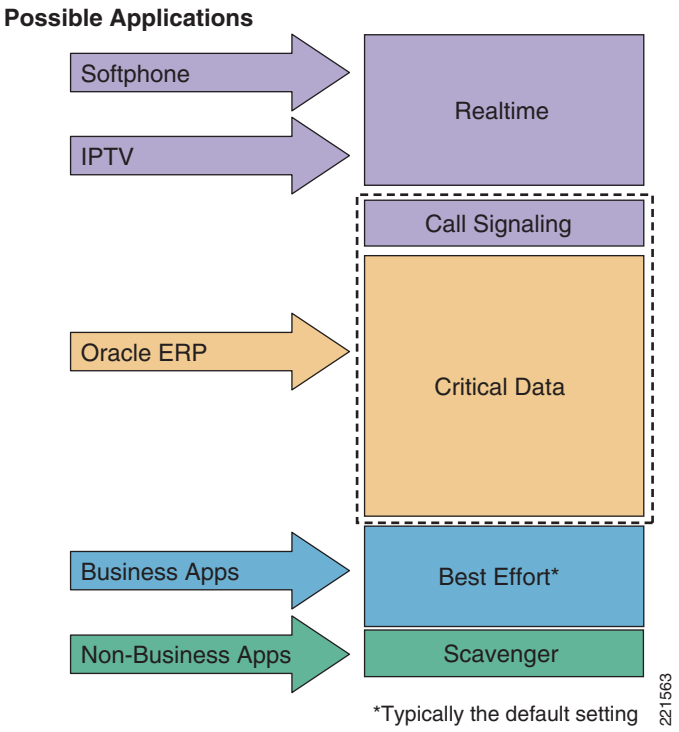
Upstream QoS Marking Policy Enforcement

QoS marking policy enforcement refers to the ability to set or re-mark the QoS parameters of application flows sourced from a host. These markings can be used by upstream devices in a network to classify the packets and apply the appropriate QoS service policies.

The goal of QoS marking is to separate application flows into different service classes so that they can be handled according to their particular network requirements and business priorities. Common service classes include the following (see Figure 33):

- Latency sensitive applications; for example, voice over IP (VoIP)
- Network control traffic
- Business-critical applications
- General user traffic; for example, e-mail, web
- Non-business traffic

Figure 33 Sample Application of a Four or Five Class QoS Model



This model is applicable to enterprise or campus networks that implement the DiffServ architecture.

Benefits of Upstream QoS Marking

From a general networking standpoint, upstream QoS marking offers two major benefits:

- Network and service availability—The preservation of network and service availability is a key element of network security, particularly for latency-sensitive business applications such as VoIP, which are susceptible to loss, delay, and jitter. This is particularly important on congested or limited bandwidth links, as well as during network incidents such as link or site outages that can be caused by general failures, DoS attacks, or worm outbreaks.

  QoS marking can be used to prioritize different service classes according to business needs, thereby preserving and prioritizing critical business applications under all network conditions.

- Operational cost management—QoS markings may also be used to ensure that only the necessary bandwidth is deployed, particularly in the case of expensive, limited bandwidth links such as WAN links. This can be achieved by handling different service classes according to policy, thereby minimizing operational costs.

Benefits of Upstream QoS Marking on a WLAN

Upstream QoS marking on a WLAN offers significant benefits because 802.11 bandwidth is a shared medium that is often under contention.

Upstream QoS marking on a WLAN endpoint enables 802.11 traffic to be classified and prioritized according to application needs. In a mixed application environment, this enables high priority applications, such as latency-sensitive VoIP applications, to be given higher priority access to the 802.11 medium, thereby preserving service availability.

Challenges of Upstream QoS Marking on a WLAN

Upstream QoS marking offers significant benefits on a WLAN, but enabling QoS also presents challenges such as the following:

- QoS marking abuse or misuse

  802.11e and Wi-Fi Multimedia (WMM)-capable devices have the ability to mark upstream packets with QoS classifications, but these self-appraised markings may not always be trusted and are subject to abuse, either because of unintentional higher markings or because of intended abuse, perhaps by compromised hosts. Consequently, these settings can be used to attempt DoS attacks on both the 802.11 RF medium and the network infrastructure, as well as general QoS marking abuse, such as priority queue jumping.

- Lack of QoS support on legacy devices

  Legacy, non-802.11e, and non-WMM devices do not support upstream QoS marking. Consequently, traffic from these devices is not classified or prioritized and is typically handled on a best-effort basis on the WLAN.

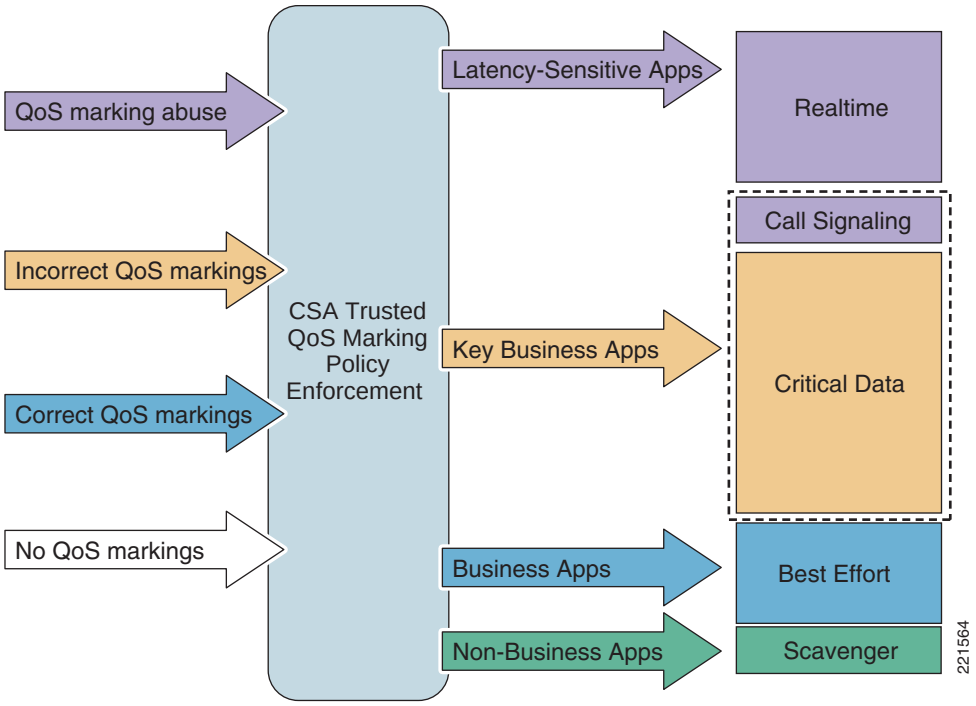
- Lack of QoS support in legacy applications

  Many applications do not support QoS functionality. Consequently, traffic from these applications is not classified or prioritized and is typically handled on a best-effort basis on the WLAN.

CSA Trusted QoS Marking

CSA v5.0 introduced the ability to apply upstream QoS markings to host application flows on the endpoint. Consequently, CSA can be used to ensure that all upstream traffic leaving a host has QoS markings set according to network policy. (See Figure 34.)

Figure 34 CSA Trusted QoS Marking for Policy Enforcement



The QoS markings set by CSA are Differentiated Services Code Point (DSCP) values and are defined as CSA policy rules. This provides administrators with centralized, granular control that can be defined as follows:

- Per protocol
- Per port range
- Per application per-port per-protocol

The DSCP values are mapped into Layer 2 class of service (CoS) values for transmission over the 802.11 RF medium. This mapping is performed by the client.

In addition, Cisco NAC may also be deployed to ensure that CSA is installed and running on a client, thereby ensuring that QoS markings are being appropriately set and validated on an endpoint.

The CSA Trusted QoS feature is not covered in detail in this document. More details on this feature, and in particular its implementation within a Cisco Unified Wireless Network, can be found in Appendix B—Sample Customized Wireless Ad-Hoc Rule Module, page 49.

Benefits of CSA Trusted QoS Marking on a WLAN Client

CSA Trusted QoS Marking enables the typical challenges presented by implementing upstream QoS on 802.11 networks to be addressed, as outlined in Table 3.

Table 3 Common QoS Challenges

Common Challenges of QoS on a WLAN	CSA Trusted QoS Marking Enforcement
QoS marking abuse or misuse	Overrides incorrectly defined upstream QoS markings
Lack of QoS support on legacy devices	Enables upstream QoS markings on legacy devices without QoS support
Lack of QoS support in legacy applications	Enables upstream QoS markings on legacy applications without QoS support

The enforcement of CSA Trusted QoS Markings thus ensures that QoS markings are applied to all packets sent by a client, and that they are set in accordance with the network policy. This enables the accurate classification and prioritization of applications, which is particularly critical in a mixed environment consisting of multiple applications and a range of endpoint devices and platforms.

This can be complemented by re-classifying and re-marking the packets at the access switch behind the WLC to ensure that any anomalies are corrected.

Basic Guidelines for Deploying CSA Trusted QoS Marking

To enforce upstream QoS markings on all packets leaving a client, Cisco recommends that CSA Trusted QoS Marking be deployed on all clients. This can be deployed in two stages:

1. Define a default QoS rule module to mark all traffic as best effort.
2. Define additional rule modules to apply the appropriate QoS markings to identified mission-critical applications such as VoIP.

CSA Wireless Security Policy Reporting

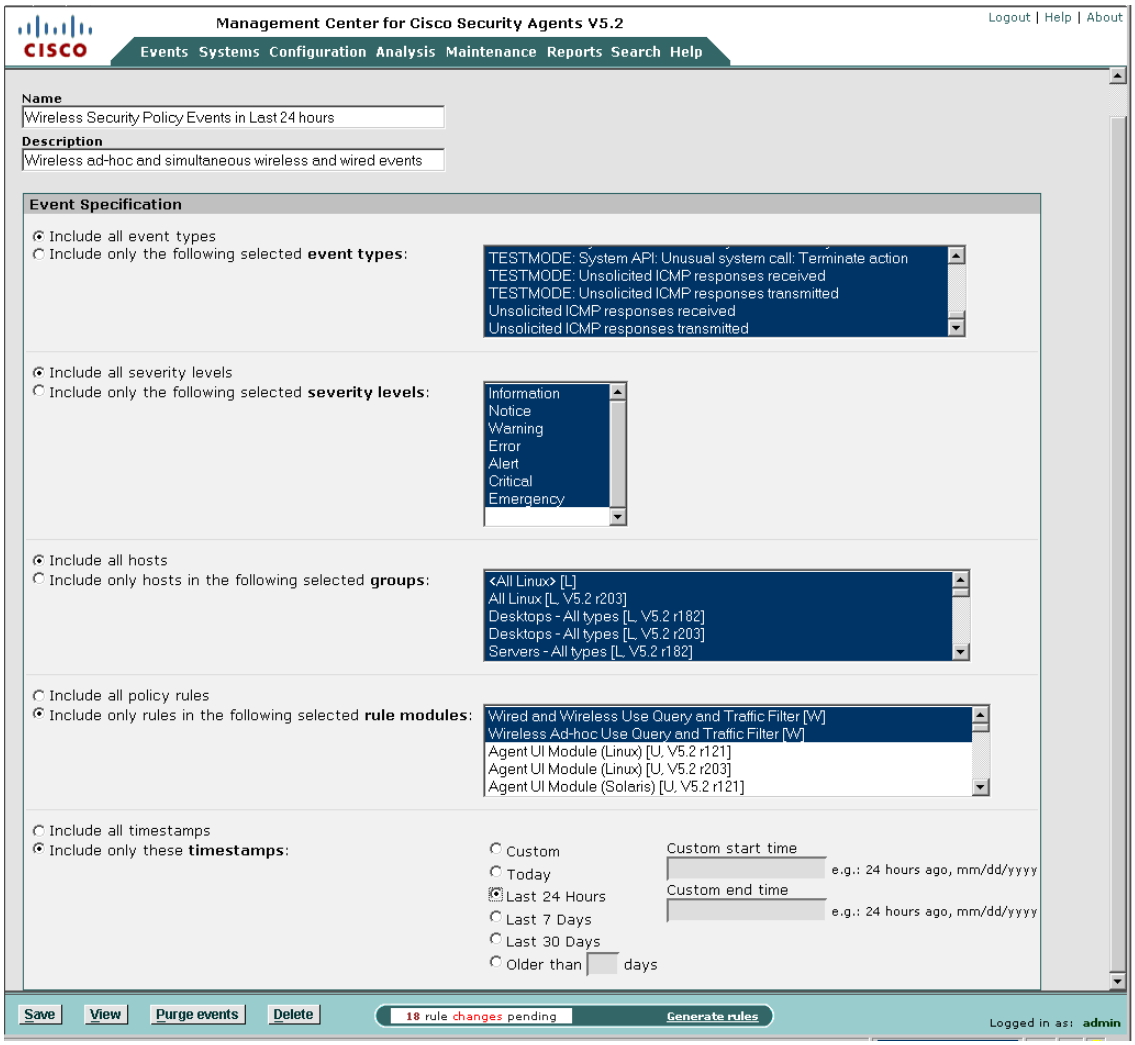
CSA Management Center Reports

CSA MC offers built-in report generation that can be used to view events based on a severity, group, host, or policy.

One wireless-specific report that may be useful is a list of wireless policy violation events over a certain time period. If the wireless rules have been configured in one or more separate WLAN policies, this type of report can easily be generated by performing the following steps.

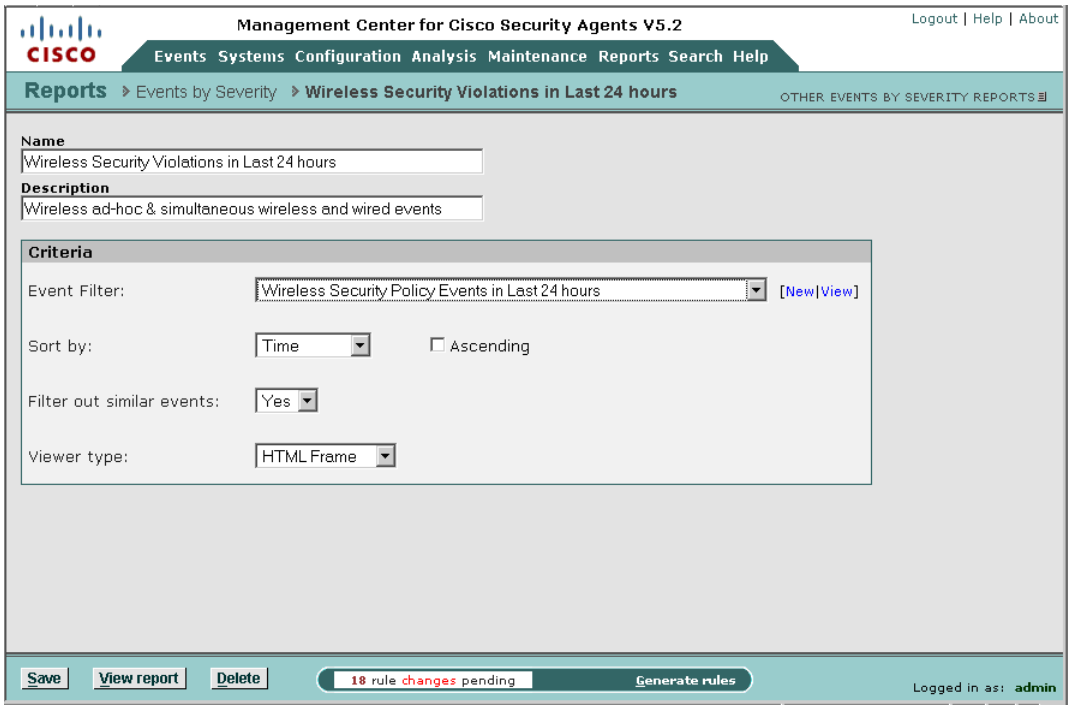
Step 1 Define an event set for the wireless-specific policies of interest and the time period required. Browse to Events -> Event Sets and create a new event set including only the wireless-specific rule modules and set the timestamps; for example, to the last 24 hours. (See Figure 35.)

Figure 35 Creation of a Wireless-Specific Event Set Based on Wireless-Specific Policies



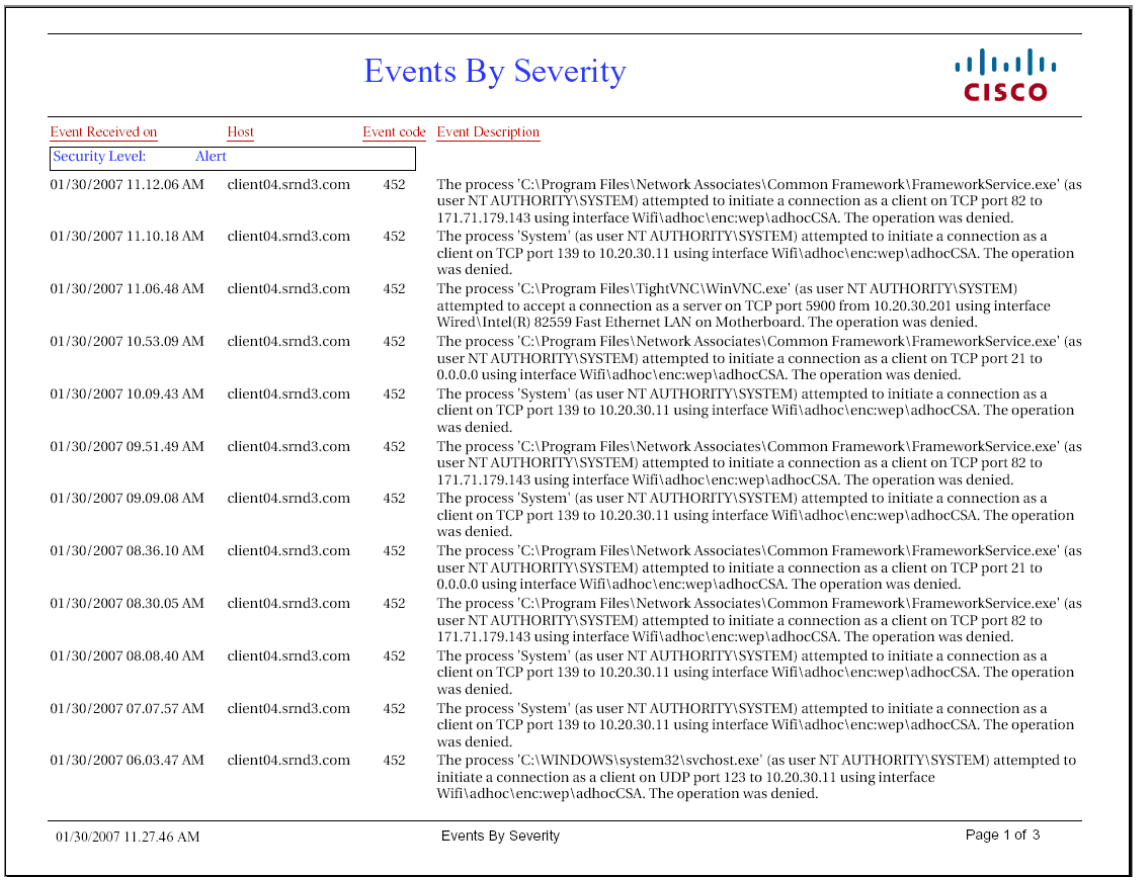
Step 2 Create and define a report on events by severity or by group, depending on the required format, using the newly defined event set as the event filter. Browse to Reports -> Event Severity and create a new report with the event filter set to the newly created wireless-specific event set. (See Figure 36.)

Figure 36 Sample Report Definition for Wireless Policy Events by Severity



Note A report on events by severity allows the events to be sorted by host. (See Figure 37.) This can be useful for traceback when an incident occurs.

Figure 37 Sample Report for Wireless Policy Events by Severity



Events By Severity

Event Received on	Host	Event code	Event Description
Security Level: Alert			
01/30/2007 11.12.06 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 82 to 171.71.179.143 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 11.10.18 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 11.06.48 AM	client04.srnd3.com	452	The process 'C:\Program Files\TightVNC\WinVNC.exe' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 5900 from 10.20.30.201 using interface Wired\Intel(R) 82559 Fast Ethernet LAN on Motherboard. The operation was denied.
01/30/2007 10.53.09 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 21 to 0.0.0.0 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 10.09.43 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 09.51.49 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 82 to 171.71.179.143 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 09.09.08 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 08.36.10 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 21 to 0.0.0.0 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 08.30.05 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 82 to 171.71.179.143 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 08.08.40 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 07.07.57 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 06.03.47 AM	client04.srnd3.com	452	The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on UDP port 123 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.

Third-Party Integration

In addition to internal reports, CSA MC offers third-party application integration through the following:

- SQL server view access to the CSA MC event database
- SNMP delivery of alerts
- Flat file logging of alerts
- E-mail delivery of alerts

Integration of CSA with the Cisco Security Monitoring, Analysis and Response System (CS MARS) platform is supported by CSA delivering SNMP alerts to CS MARS. See the CS MARS user guide for detailed information on configuring host-based IDS and IPS devices, as listed in Appendix B—Sample Customized Wireless Ad-Hoc Rule Module, page 49.

Note E-mail delivery of alerts should be used with caution to avoid creation of a possible DoS attack on the e-mail server.

Overall Deployment Guidelines for CSA Integrated WLAN Security

Overall deployment guidelines on the integration of CSA for WLAN security include the following:

- Deploy CSA for general client endpoint protection.
- Consider CSA wireless-specific policies including the following:
  - Wireless ad-hoc policy enforcement
  - Simultaneous wired and wireless policy enforcement
  - Location-aware policy enforcement
  - Upstream QoS marking
    - At a minimum, define a default QoS rule module to mark all traffic as best effort.
- Consider Cisco Secure Services Client (CSSC) to enforce authentication and encryption parameters.

Customers are recommended to do the following:

- Carefully review the operational considerations outlined for each rule module in relation to their particular environment before deployment.
- Consider customization of pre-defined rules to possibly address some of the operational considerations and impact.
- Ensure that WLAN policy violation events are regularly monitored and reviewed as part of the overall security policy.

Appendix A—CSA Overview

Cisco Security Agent (CSA) provides endpoint threat protection for servers and desktop systems by identifying and preventing malicious or unauthorized behavior. This role is generally referred to as Host-based Intrusion Protection Solution (HIPS). This is a critical element of endpoint security, providing protection against many threats, including viruses, worms, botnets, spyware, theft of information, and unauthorized access.

Cisco Security Agent benefits include the following:

- Intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation
- Zero-day attack protection for known and unknown attacks
- Protection against entire classes of attacks, including port scans, buffer overflows, Trojan horses, malformed packets, malicious HTML requests, and e-mail worms
- Application-specific protection for web servers and databases
- Enforcement of corporate policy to address undesirable behavior such as the use of unauthorized applications, music download, theft of information, and so on, plus policy compliance
- Enterprise-scalable architecture; up to 100,000 agents per manager
- Integrated solution architecture with Cisco Clean Access to provide network access control
- Integration with Cisco VPN devices to provide endpoint security for IP security (IPsec) and Secure Sockets Layer (SSL) VPN deployments

CSA Solution Components

The CSA solution consists of the following:

- Cisco Security Agents

  Host-based agents deployed on desktops and servers to enforce defined security and general use policies. These agents report to the CSA MC using HTTP and 128-bit SSL. A range of platforms and operating systems are supported.

- Cisco Management Center for Cisco Security Agents (CSA MC)

  The Management Center runs as a standalone application performing configuration, management, and reporting of Cisco Security Agents. CSA MC v5.2 is supported only on Windows 2003 R2 Server.

For more detailed information on the CSA product, platform, and features, see the product pages referenced in Appendix D—Test Bed Hardware and Software, page 67.

Appendix B—Sample Customized Wireless Ad-Hoc Rule Module

This sample customized wireless ad-hoc rule module includes the following modification:

Customized user query as a rule action

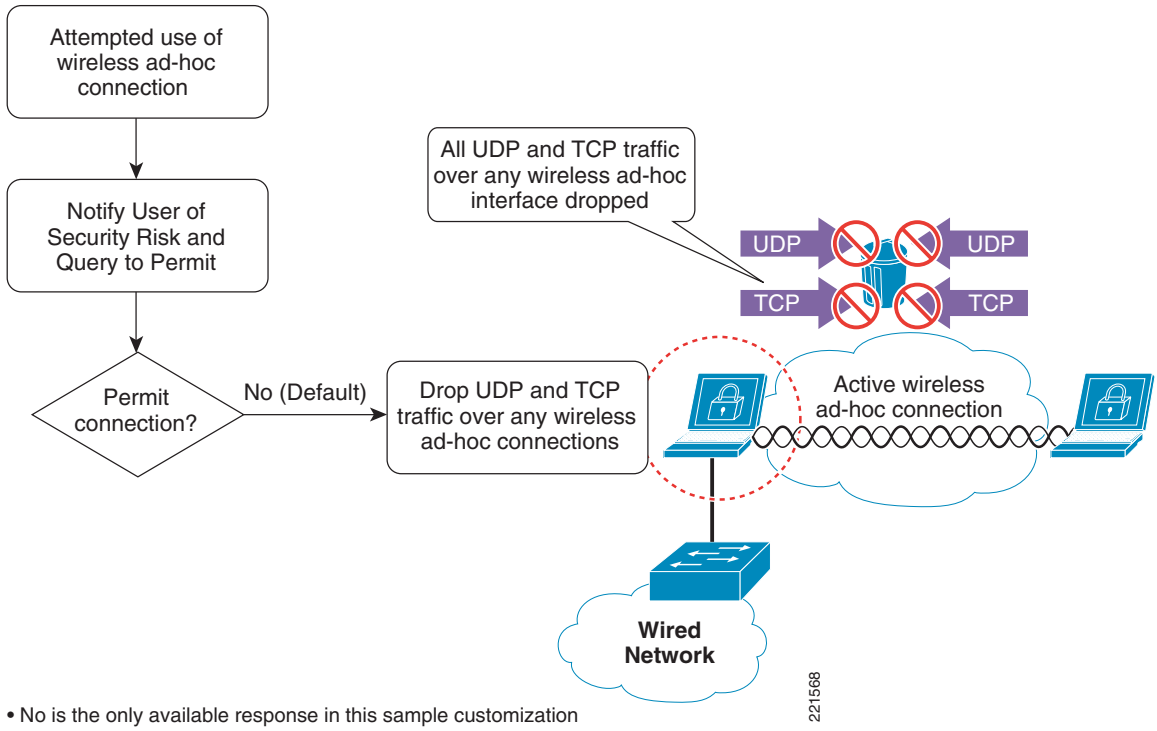
This customization can be used to educate users on the security risk of a wireless ad-hoc connection by presenting a user query, notifying an end user of the associated security risk but maintaining a deny only action. This can assist with improving awareness of the security policy as well as reducing the number of support calls.

Response caching can be enabled to minimize user disruption.

Sample Customized Rule Module Operation

The operation of this customized wireless ad-hoc rule module is shown in Figure 38.

Figure 38 Sample Customized Wireless Ad-hoc Rule Module Operation



• No is the only available response in this sample customization

This sample customized rule module operation is as follows:

- Upon an attempt to send UDP or TCP traffic over an active wireless ad-hoc interface, the customized rule module is invoked. This is true regardless of whether any other network connections are active or not.
- Traffic on a non-wireless ad-hoc interface is not affected by this rule module.
- User query is presented, stating the security policy.
- User is presented with deny as the only available action.
- Default action is a deny.
- All UDP and TCP traffic routed over any wireless ad-hoc interface is dropped.
- A message is logged.

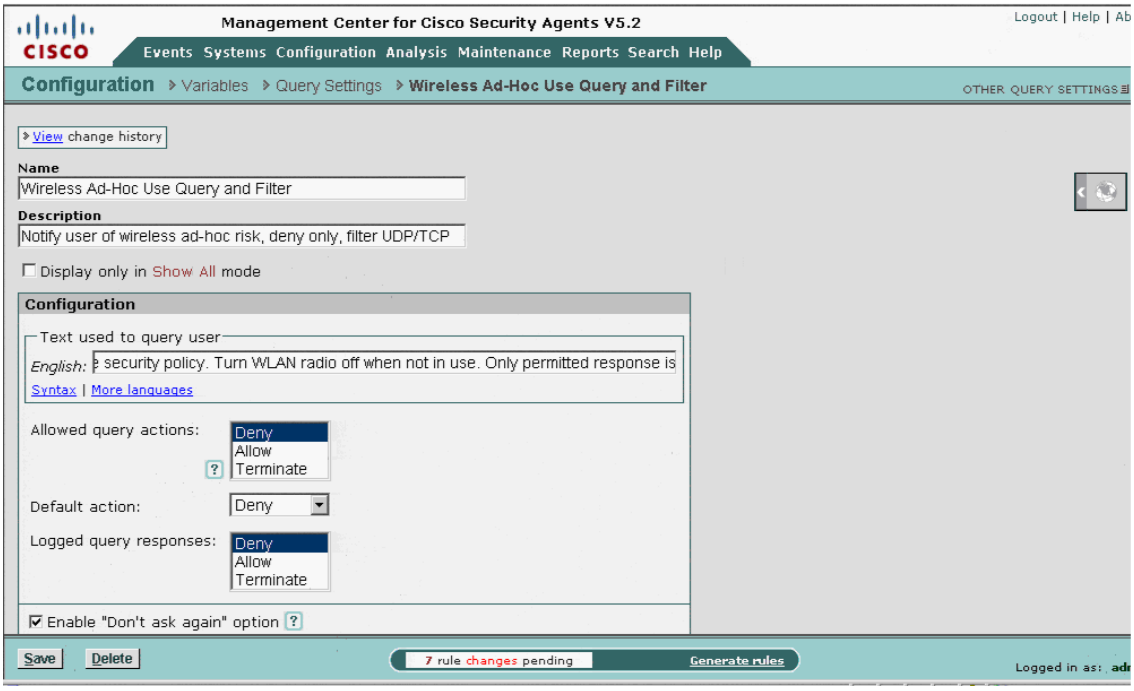
Sample Customized Rule Module Definition

Configuration of a customized wireless ad-hoc rule module, including user query and notification, is shown in the following steps, along with sample screenshots of the key stages.

Step 1 Create a new query setting variable to notify the end user of the event by going to Configuration -> Variables -> Query Settings. Click the **New** button in the bottom of the window.

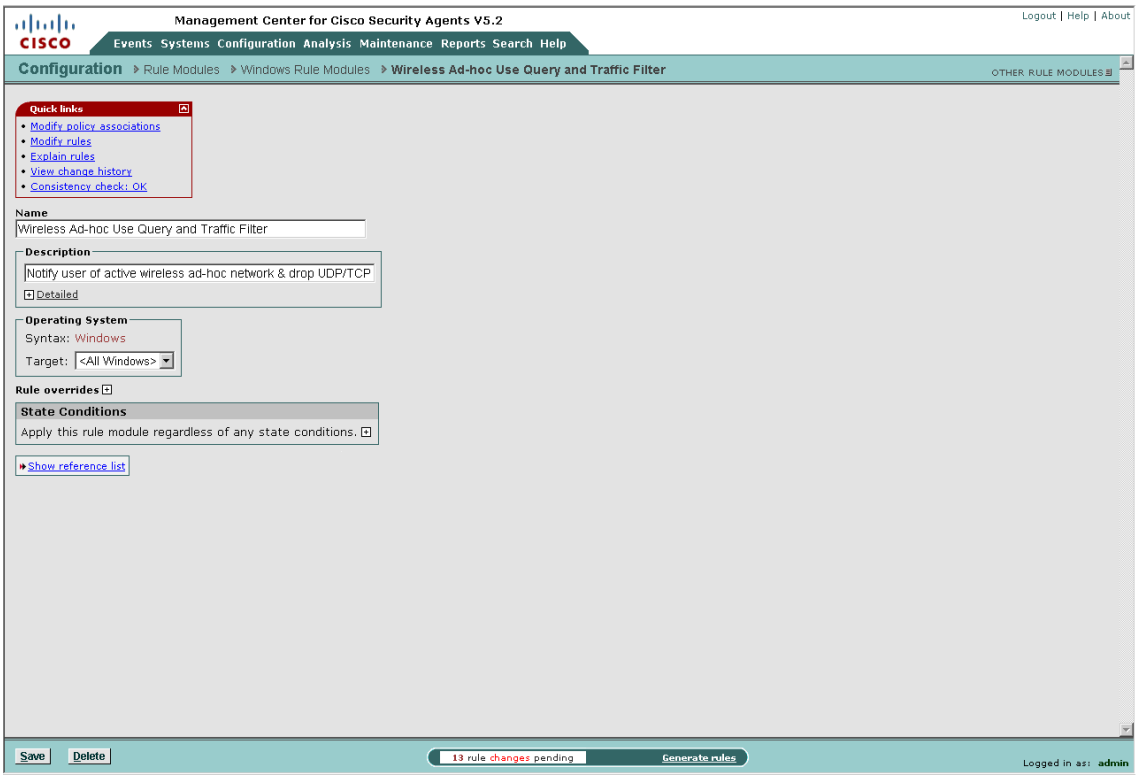
Step 2 Configure the query to present the user only with deny as an action option, set the default action to deny, log a deny response, and enable the **Don't ask again** option. (See Figure 39.)

Figure 39 New Query Setting Variable Definition for Sample Customized Wireless Ad-hoc Rule Module



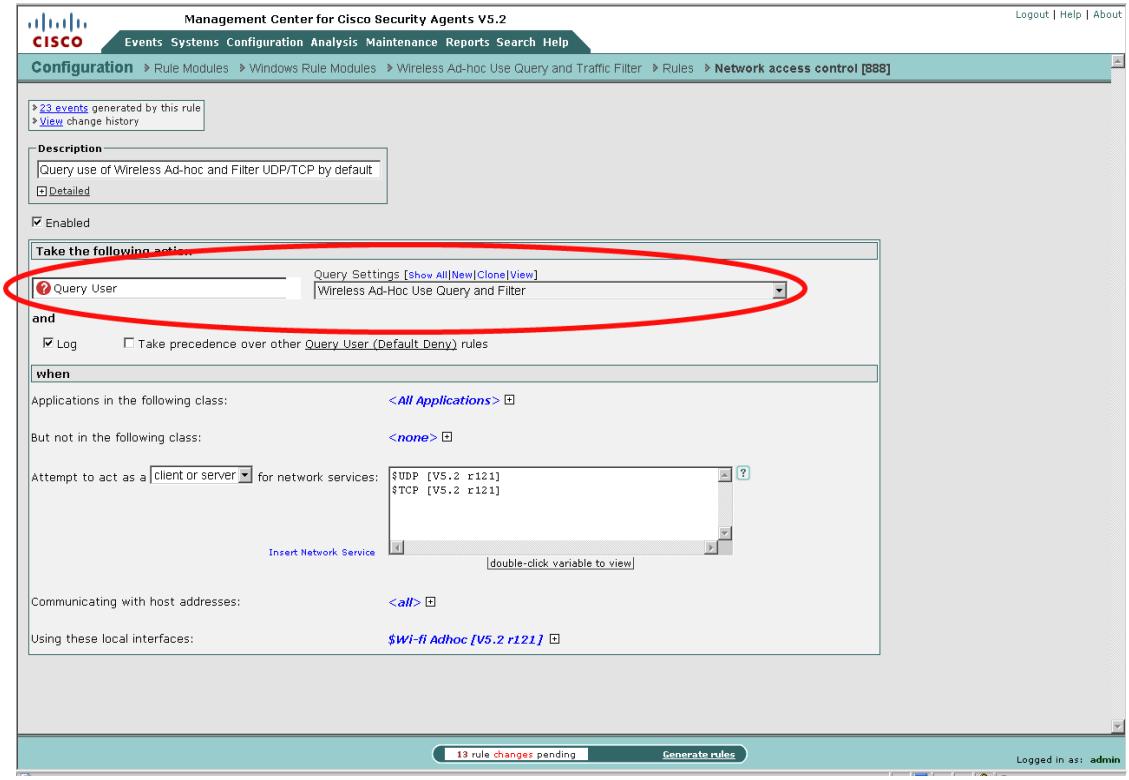
Step 3 Locate the pre-defined wireless ad-hoc Windows rule module, clone it, and rename it. (See Figure 40.)

Figure 40 New Sample Customized Wireless Ad-hoc Rule Module



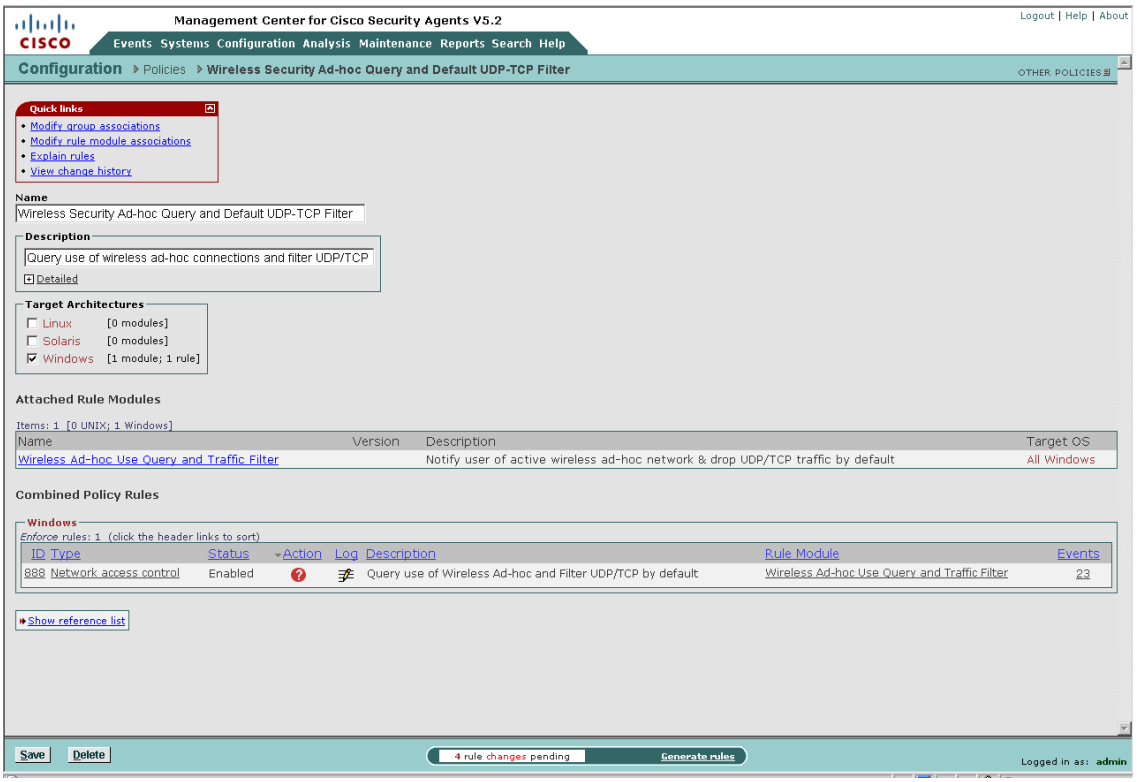
Step 4 Modify the rules associated with this newly customized wireless ad-hoc rule module to query the user and apply the new query setting. (See Figure 41.)

Figure 41 Application of New Query Setting to Sample Customized Wireless Ad-hoc Rule Module



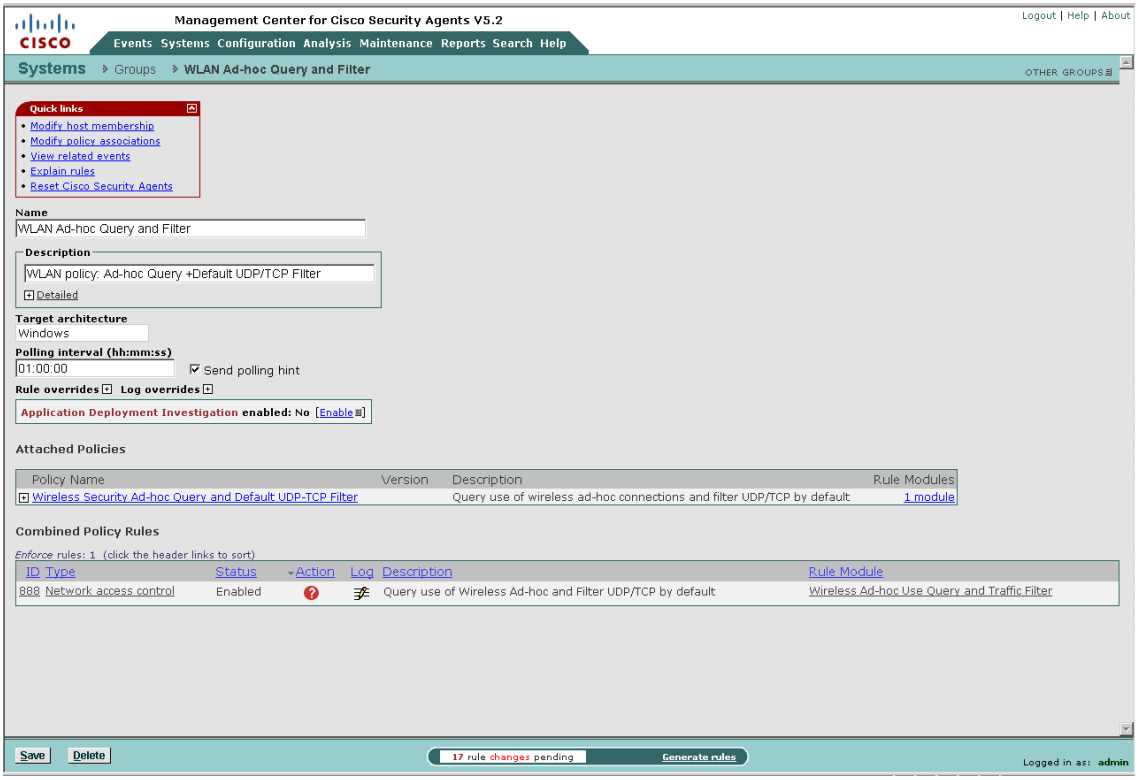
Step 5 Associate the new rule module with either a current policy or create a new policy. (See Figure 42.)

Figure 42 Association of the Sample Customized Wireless Ad-hoc Rule Module with a Policy



Step 6 Associate the updated or new policy with either a current group or create a new group. (See Figure 43.)

Figure 43 Association of the Sample Customized Wireless Ad-hoc Policy with a Group

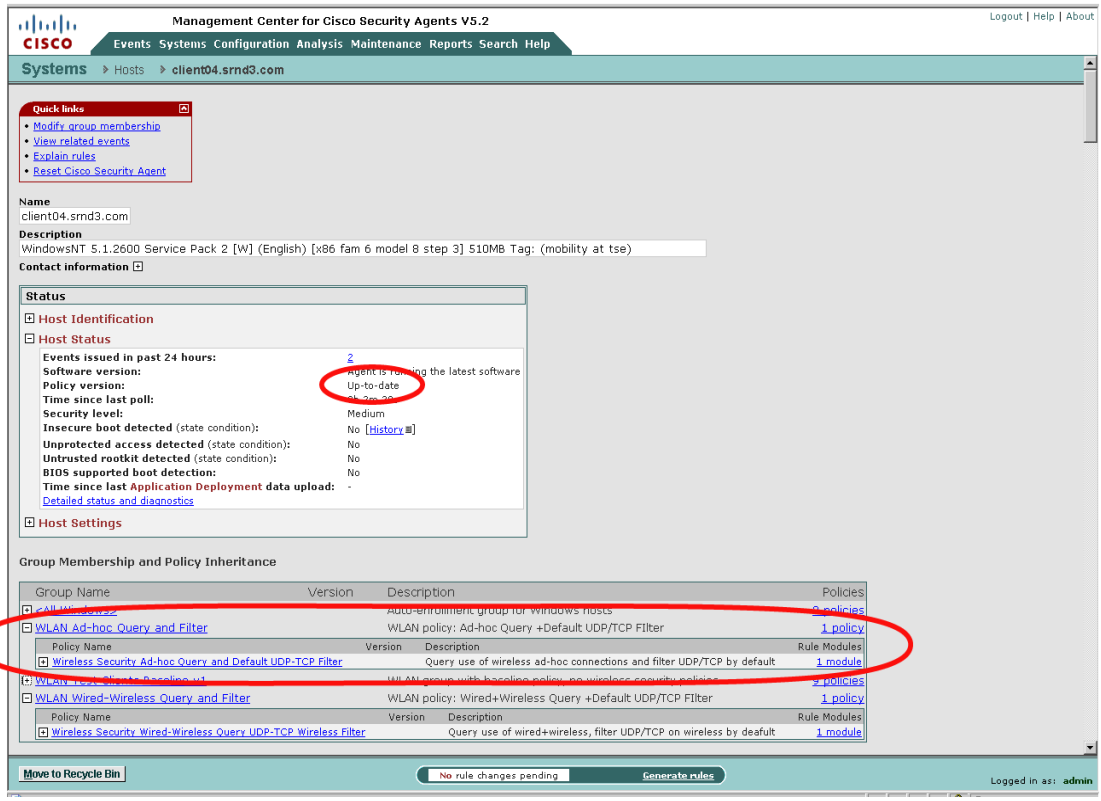


Step 7 If a new group has been created, ensure that host membership is updated to enforce the policy on appropriate hosts.

Step 8 Generate the rules to apply all changes.

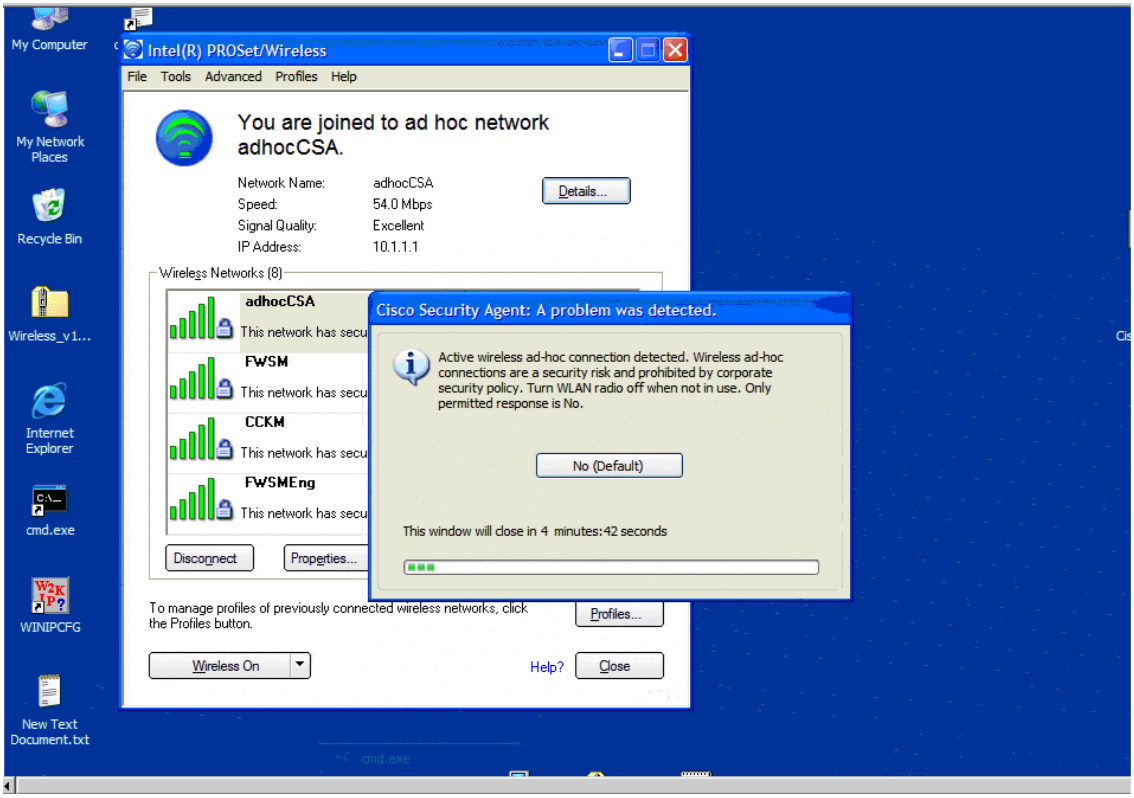
Step 9 Verify that a host is running up-to-date policies before checking operation of the new customized rule module. (See Figure 44.)

Figure 44 Host Detail Showing Policy Status and Group Membership



Step 10 Attempt to use a wireless ad-hoc connection on a host to check the new customized rule. (See Figure 45.)

Figure 45 End User Notification upon Enforcement of Sample Customized Wireless Ad-hoc Rule



Sample Customized Rule Module Logging

If event logging is enabled for a customized rule module configured with a user query action, a Notice event is generated upon the user being presented with the notification window.

An alert event is subsequently generated each time the rule module is triggered by the same behavior within the next one-hour window, indicating that the blocking is still being triggered but that the user is not being queried.

By default, user query is performed only once per hour for each particular type of behavior, even if the "Don't ask again" action is not enabled. (See Figure 46.)

Figure 46 CSA MC Event Log Generated by Sample Customized Wireless Ad-hoc Rule

Appendix C—Sample Customized Simultaneous Wired and Wireless Rule Module

The steps involved to create a customized simultaneous wired and wireless rule module are outlined below.

This sample customized simultaneous wired and wireless rule module includes the following modification:

Customized user query as a rule action with user option to permit or deny

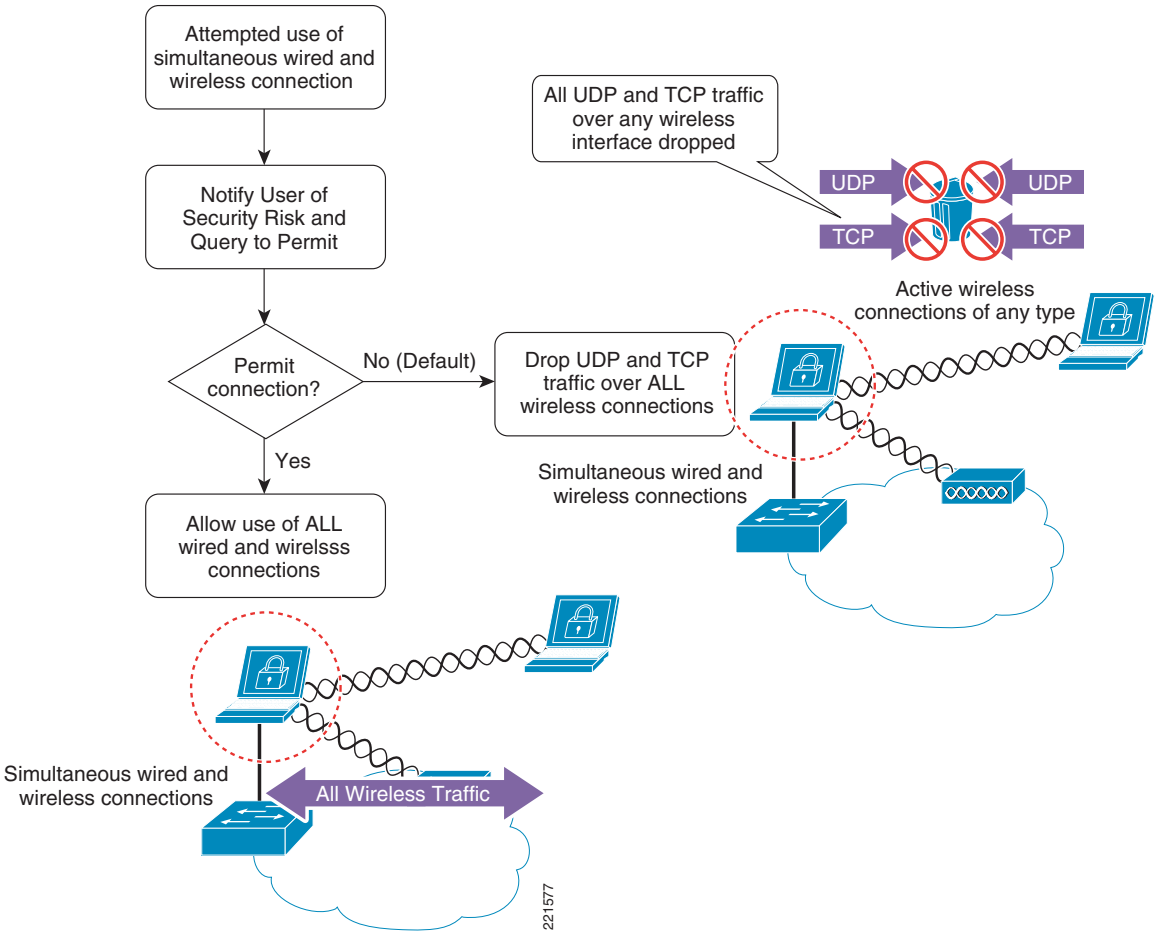
This customization can be used to educate users on the security risk of simultaneous wired and wireless connections by presenting a user query and notifying an end user of the associated security risk. This may assist with improving awareness of the security policy as well as reducing the number of support calls. The user can be given the option to permit or deny simultaneous wired and wireless connections, with the default action being deny.

Response caching can be enabled to minimize user disruption.

Sample Customized Rule Module Operation

The operation of this customized simultaneous wired and wireless rule module is shown in Figure 47.

Figure 47 Sample Customized Simultaneous Wired and Wireless Rule Module Operation



Sample customized rule module operation is as follows:

1. Upon an attempt to send UDP or TCP traffic over an active wireless interface when an Ethernet interface is active, the customized rule module is invoked.
2. Traffic on a non-wireless interface is not affected by this rule module.
3. User query is presented, stating the security policy.
4. User is presented with the option to permit or deny the action.
5. Default action is a deny.
6. All UDP and TCP traffic routed over any wireless interface is dropped.
7. A message is logged.

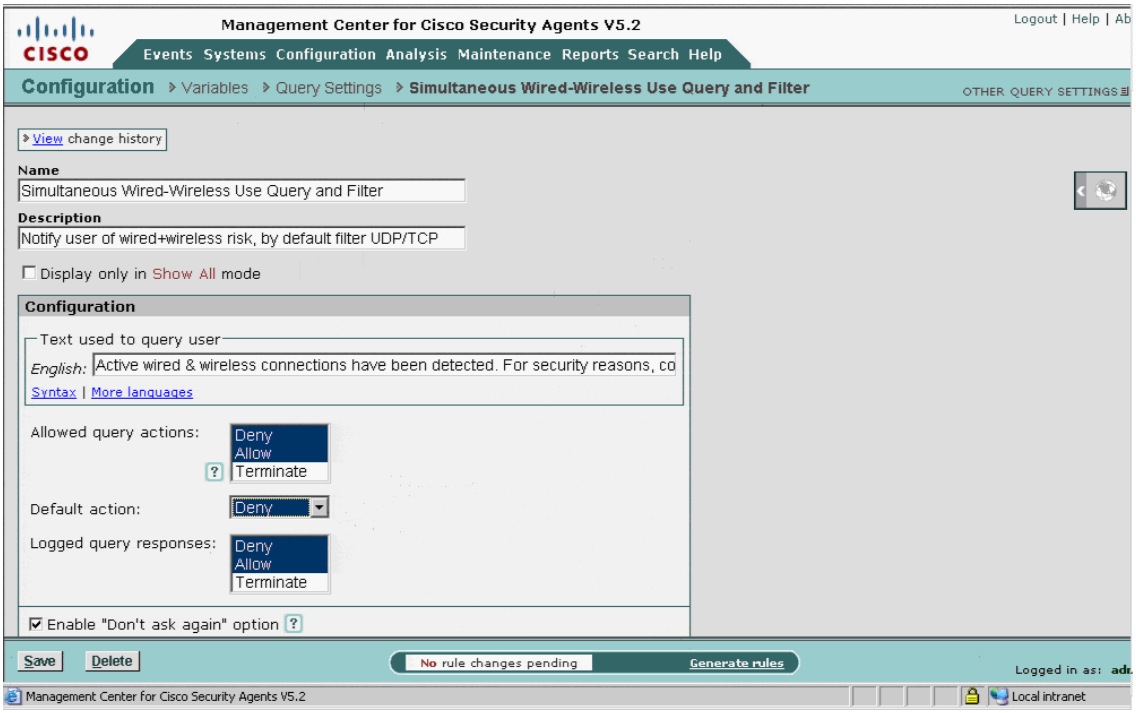
Sample Customized Rule Module Definition

Configuration of a customized simultaneous wired and wireless rule module, including user query and notification, is shown in the following steps, along with sample screenshots of the key stages.

Step 1 Create a new query setting variable to notify the end user of the event, using Configuration -> Variables -> Query Settings. Click the **New** button in the bottom of the window.

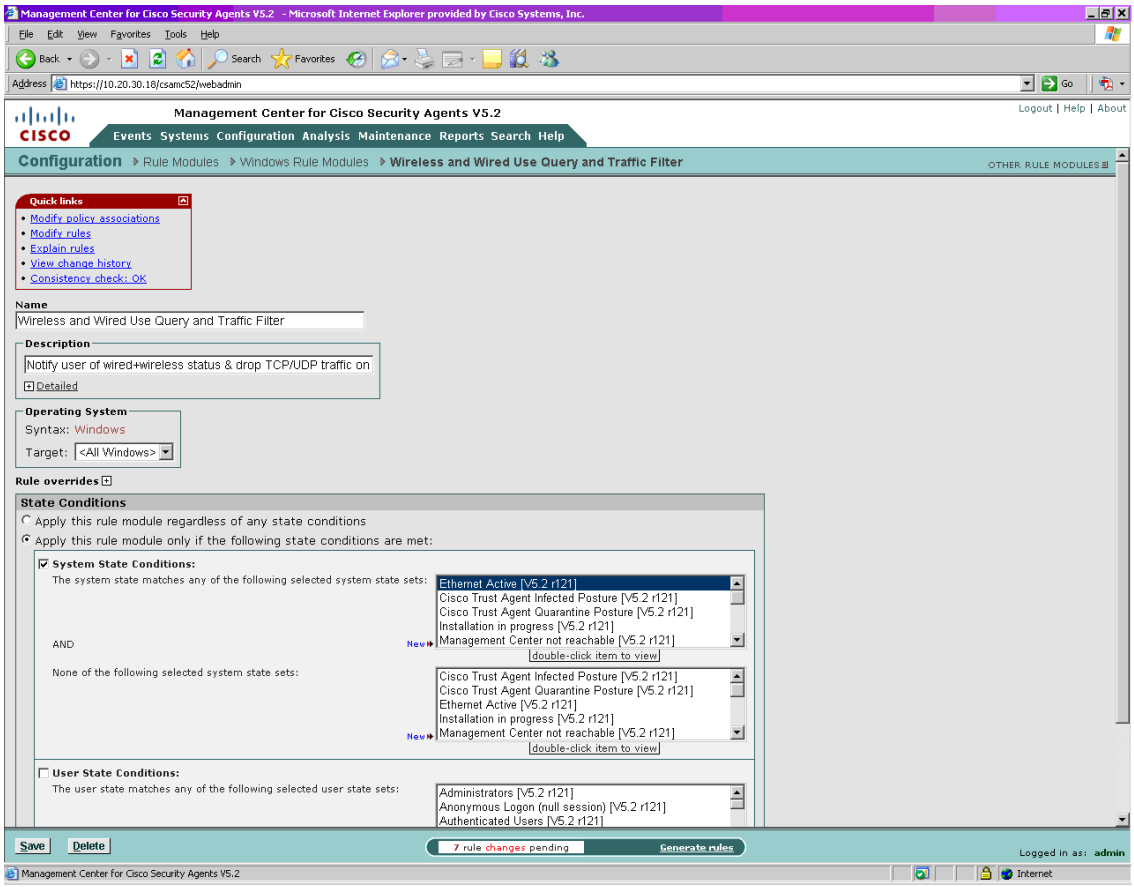
Step 2 Configure the query to present the user with a choice of actions but, by default, enforce a deny action. (See Figure 48.)

Figure 48 New Query Setting Variable Definition for Sample Customized Simultaneous Wired and Wireless Rule Module



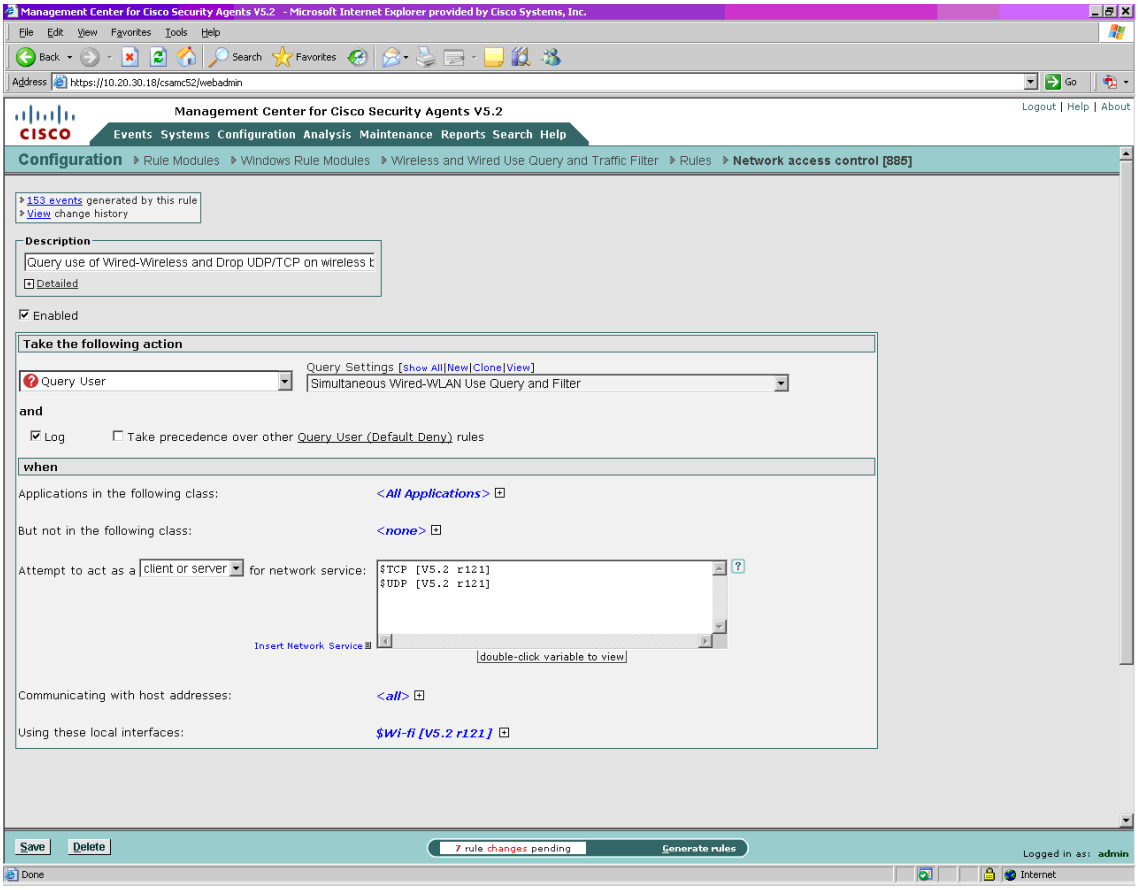
Step 3 Locate the pre-defined simultaneous wired and wireless Windows rule module, clone it, and rename it. (See Figure 49.)

Figure 49 New Sample Customized Simultaneous Wired and Wireless Rule Module



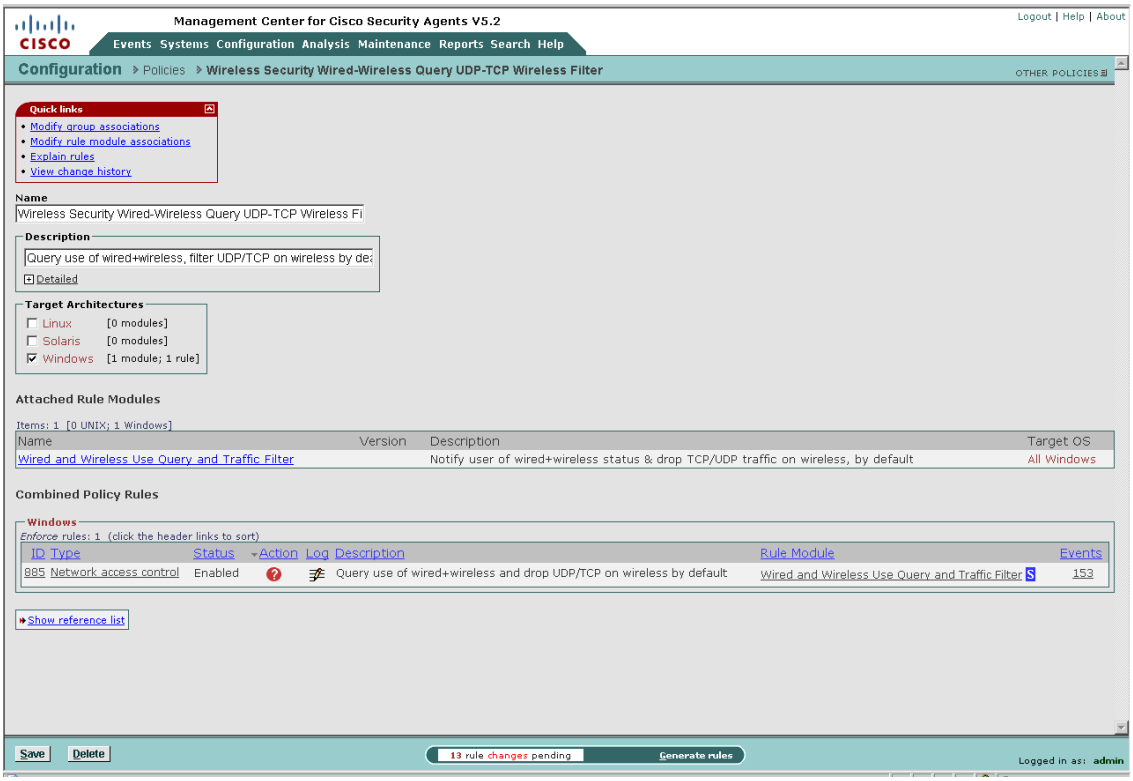
Step 4 Modify the rules associated with this newly customized simultaneous wired and wireless rule module to query the user and apply the new query setting. (See Figure 50.)

Figure 50 Application of New Query Setting to Sample Customized Simultaneous Wired and Wireless Rule Module



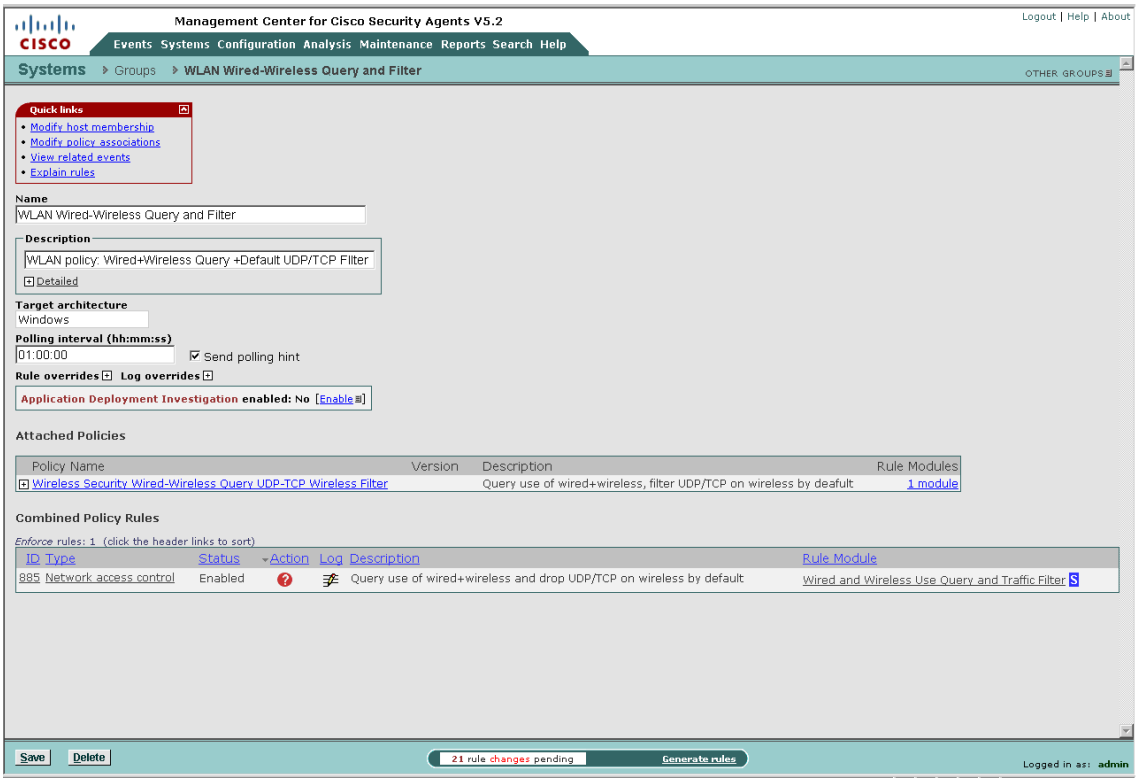
Step 5 Either associate the new rule module with a current policy or create a new policy (See Figure 51.)

Figure 51 Association of the Sample Customized Simultaneous Wired and Wireless Rule Module with a Policy



Step 6 Either associate the updated or new policy with a current group or create a new group. (See Figure 52.)

Figure 52 Association of the Sample Customized Simultaneous Wired and Wireless Policy with a Group

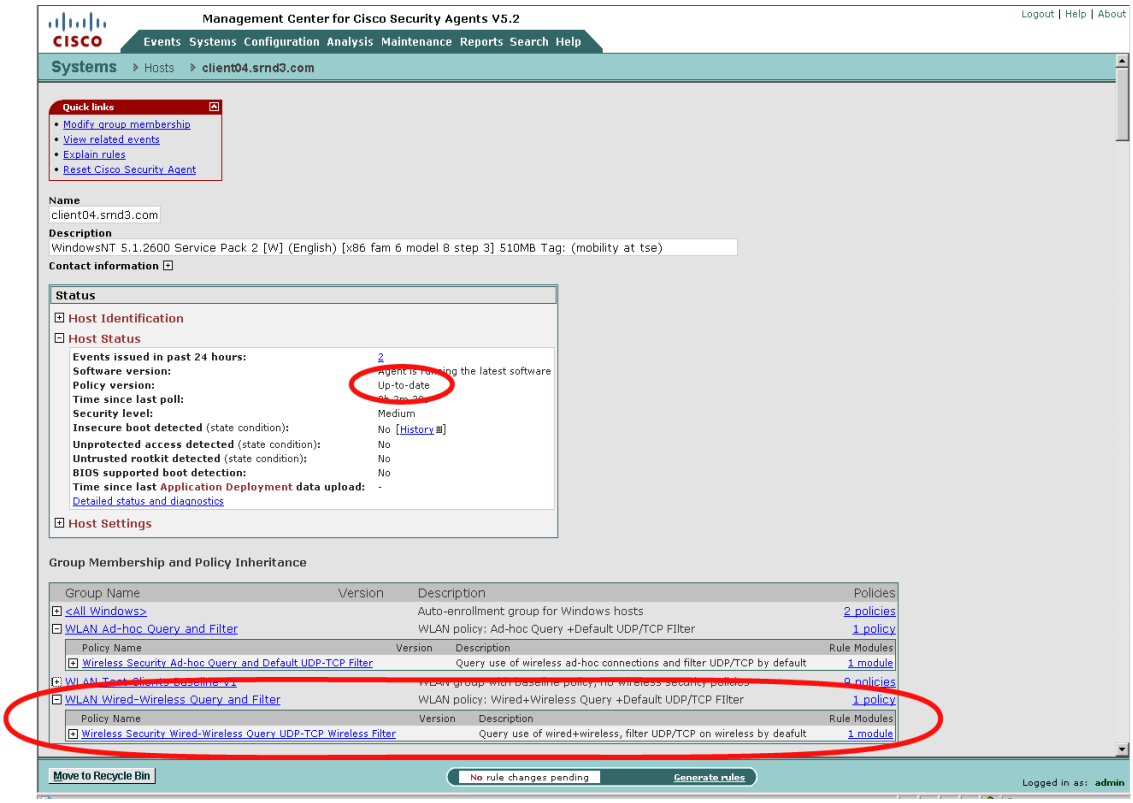


Step 7 If a new group has been created, ensure that host membership is updated to enforce the policy on appropriate hosts.

Step 8 Generate the rules to apply all changes.

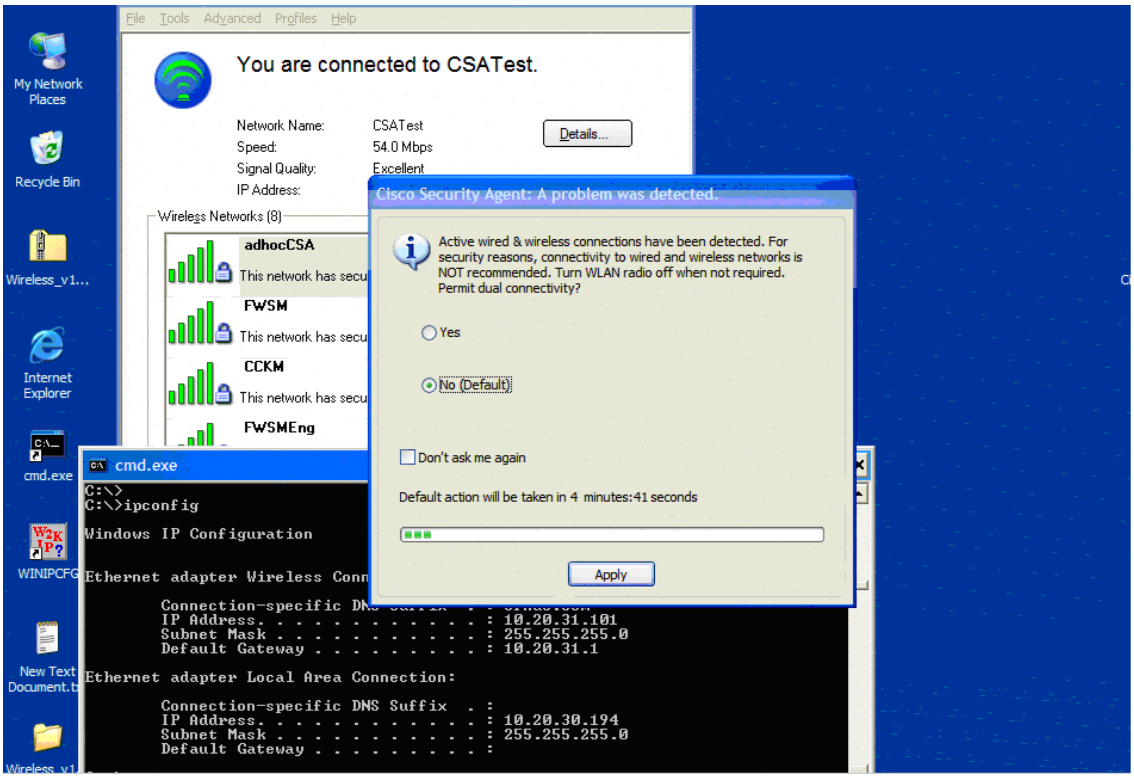
Step 9 Verify that a host is running up-to-date policies before checking operation of the new customized rule module. (See Figure 53.)

Figure 53 Host Detail Showing Policy Status and Group Membership



Step 10 Attempt to use a wireless connection on a host with an active Ethernet connection to check the new customized rule module. (See Figure 54.)

Figure 54 End User Notification upon Enforcement of Sample Customized Simultaneous Wired and Wireless Rule Module



Sample Customized Rule Module Logging

If event logging is enabled for a customized rule module configured with a user query action, a Notice event is generated upon the user being presented with the notification window.

An alert event is subsequently generated each time the rule module is triggered by the same behavior within the next one-hour window, indicating that the blocking is still being triggered but that the user is not being queried. By default, user query is performed only once per hour for each particular type of behavior, even if the "Don't ask again" action is not enabled. (See Figure 55.)

Figure 55 CSA MC Event Log Generated by Sample Customized Simultaneous Wired and Wireless Rule Module

Appendix D—Test Bed Hardware and Software

The key platforms and their software configurations used to perform the testing completed to support this documentation are shown in Table 4.

Table 4 Test Bed Hardware and Software

CSA Software	V5.2.0.203
Operating system	Microsoft Windows XP Service Pack 2
Wireless client	Intel PROSet/Wireless Software 10.5.1.0 CSSC v4.1.1
Wireless adapter	Intel PRO/Wireless 2915ABG Driver Version 9.0.4.26

Appendix E—References

- Cisco Security Agent (CSA)
  - CSA product site— http://www.cisco.com/go/csa/
  - CSA v5.2 documentation— http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_release_note09186a0080813a6d.html
- Cisco Secure Services Client (CSSC)
  - Cisco Secure Services Client (CSSC)— http://www.cisco.com/en/US/products/ps7034/index.html
- Cisco Unified Wireless
  - Cisco Wireless Portfolio—http://www.cisco.com/en/US/products/hw/wireless/index.html

  - Wireless Network Security—
    http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking_solutions_package.html

- CS MARS
  - CS MARS user guides—
    http://www.cisco.com/en/US/products/ps6241/products_user_guide_list.html
- Trusted QoS

  Implementing Trusted Endpoint Quality of Service Marking—
  http://www.cisco.com/application/pdf/en/us/guest/products/ps6786/c1225/ccmigration_09186a00805b6a81.pdf
- Windows Wireless Auto Configuration
  - Microsoft article outlining the behavior of Wireless Auto Configuration, creating the ad-hoc vulnerability—
    http://technet2.microsoft.com/WindowsServer/en/library/370b019f-711f-4d5a-8b1e-4289db0bcafd1033.mspx?mfr=true
  - Article “The Windows Ad-Hoc Exploit” outlining how the Windows ad-hoc behavior can be exploited—http://www.wi-fiplanet.com/news/article.php/3578271