CHAPTER 7

CSA for Mobile Client Security

A secure unified network, featuring both wired and wireless access, requires an integrated, defense-in-depth approach to security, including comprehensive endpoint security that is critical to effective threat detection and mitigation, and policy enforcement.

This chapter outlines the role of Cisco Security Agent (CSA) in mobile client endpoint security and provides an overview of the security features it offers to address the threats they encounter and to enforce policy according to their location. Implementation guidelines to assist in the design and deployment of these features are also provided.

Software implementation, screenshots, and behavior referenced in this chapter are based on the releases listed in Test Bed Hardware and Software, page 7-56. It is assumed that the reader is already familiar with CSA.

Note This chapter addresses only CSA features specific to mobile client security.

CSA Overview

CSA is the first endpoint security solution that combines zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated day-zero attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.

CSA provides numerous benefits including the following:

- Zero-update protection reduces emergency patching in response to vulnerability announcements, minimizing patch-related downtime and IT expenses
- Visibility and control of sensitive data protects against loss from both user actions and targeted malware
- Signature-based anti-virus protection to identify and remove known malware
- Pre-defined compliance and acceptable use policies allow for efficient management, reporting, and auditing of activities
- Industry-leading network and endpoint security integration and collaboration, including Cisco Network Access Control (NAC), Cisco network IPS devices and Cisco Security Monitoring, Analysis, and Response System (CS-MARS)
- Centralized policy management offering behavioral policies, data loss prevention, and antivirus protection fully integrated into a single configuration and reporting interface

CSA Solution Components

The CSA solution consists of the following components:

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

  The Management Center runs as a standalone application performing configuration, management, and reporting for all Cisco Security Agents in a centralized manner.

- Cisco Security Agents

  Host-based agents deployed on desktops and servers to enforce the defined security and general use policies. These agents are managed and report to the CSA MC but each agent operates autonomously and enforces the security policy even if communication with the CSA Management Center is not possible. These agents are supported on a range of desktop and server platforms and operating systems.

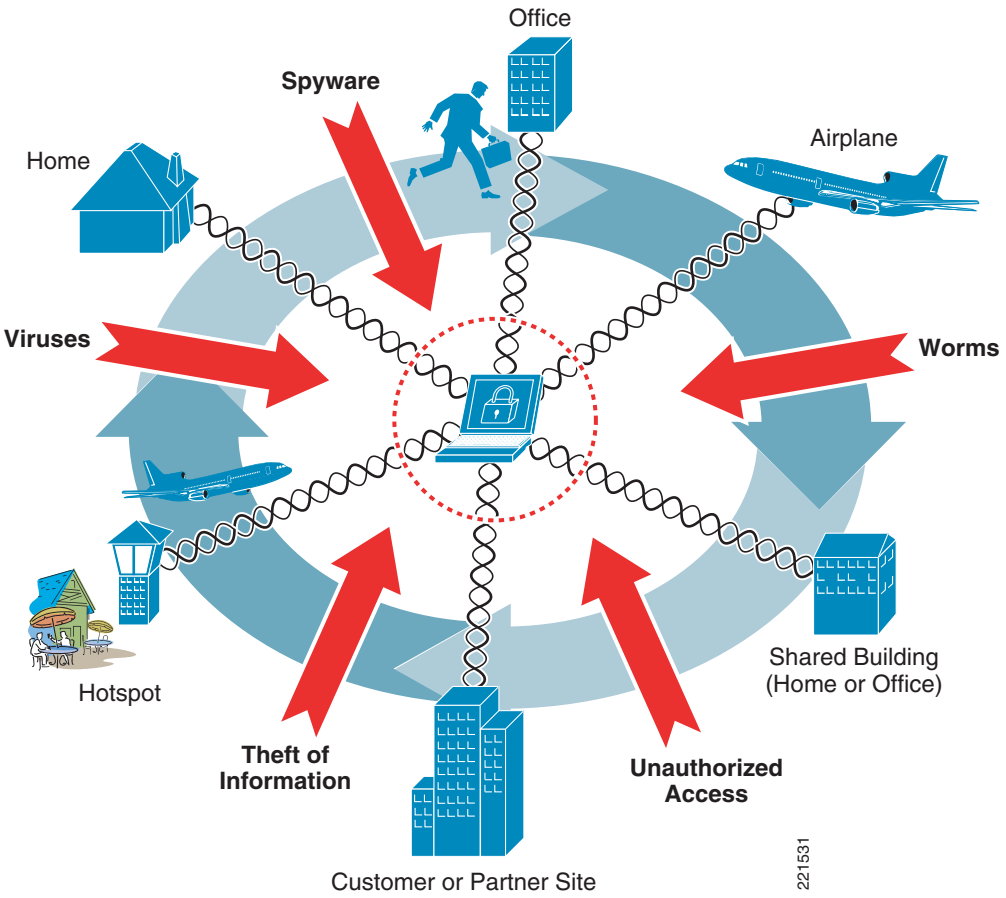
For more information on the CSA product, platform, and features, refer to the product pages referenced in Reference Documents, page 7-56.

CSA for Mobile Client Security Overview

CSA for General Client Protection

Both mobile and fixed clients and servers are exposed to a range of security threats, including viruses, worms, botnets, spyware, theft of information, and unauthorized access. CSA offers comprehensive endpoint security that defends clients and servers from these attacks, providing zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent, as well as offering the ability to enforce acceptable-use and compliance policies. (See Figure 7-1.)

Figure 7-1 General Security Threats Encountered by a Client or Server

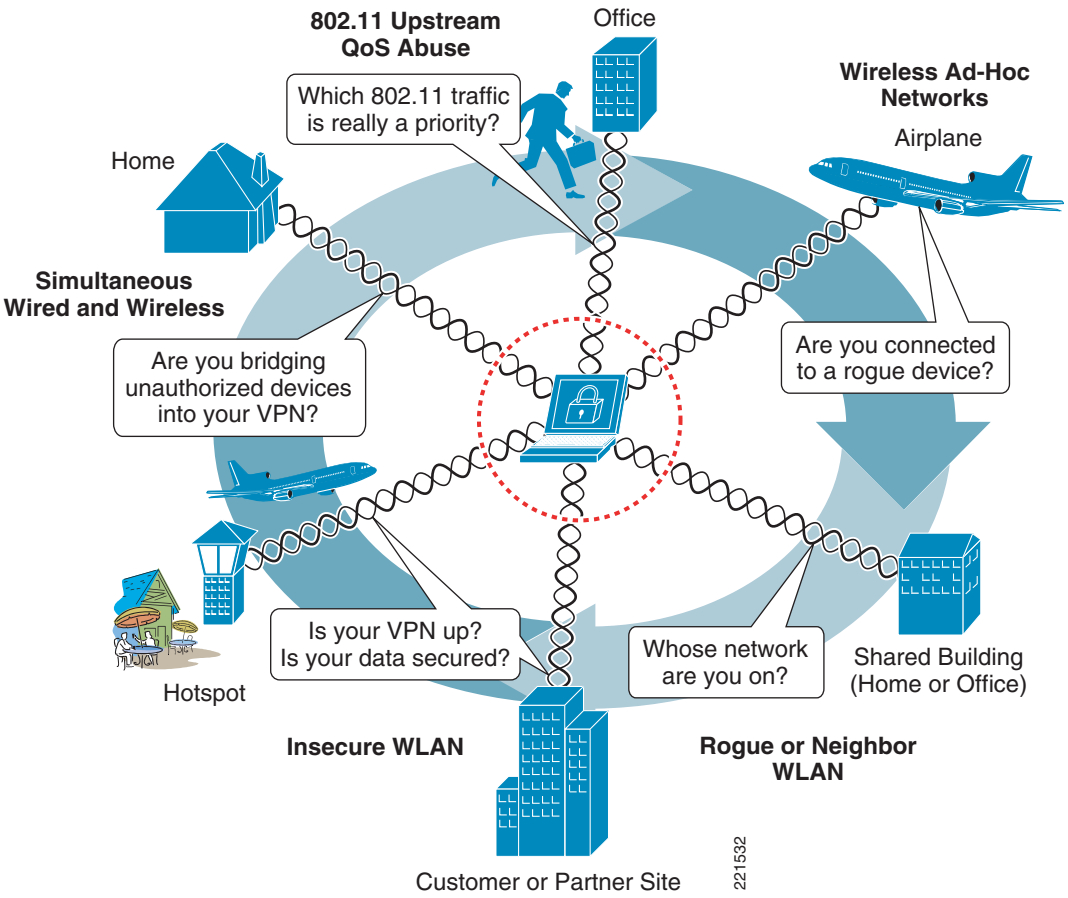


Endpoint security is a critical element of an integrated, defense-in-depth approach to security, protecting both the client or server itself, and the corporate network to which it connects.

CSA for Mobile Client Protection

A mobile client typically associates, knowingly or unknowingly, to a range of different networks, wired or wireless, including a corporate network, hotspots, a home network, partner networks, wireless ad-hoc networks and rogue networks. As such, it is exposed to additional security threats. (See Figure 7-2.)

Figure 7-2 Additional Security Threats Encountered by a Mobile Client



CSA offers the ability to extend general endpoint protection to address the typical threats encountered by a mobile client and adapt the security policy being enforced according to their current location.

Table 7-1 lists a summary of the typical, additional security threats encountered by a mobile client, the risks they pose, and the CSA security features that can be used to mitigate them. Each of these areas is addressed in more detail in subsequent sections.

Table 7-1 Typical Mobile Client Security Threats and CSA Mitigation Features

Mobile Client 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

Table 7-1 Typical Mobile Client Security Threats and CSA Mitigation Features (continued)

Connection to non-corporate, insecure, unauthorized, rogue, or incorrect network	• 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	• Force use of VPN when roaming predefined rule module[1] • Location-aware policy enforcement to enforce stricter controls when on non-corporate network[1]
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 policies for mobile clients should be used to complement and extend general CSA security policies, which should already be enforced for general endpoint protection of both fixed and mobile clients and servers, as outlined in the previous section.

CSA and Complementary Cisco Security Features

The Cisco Unified Wireless and Cisco security portfolios feature a number of complementary security features that support an integrated, defense-in-depth approach to security. For example, two of the mobile client security threats addressed by CSA can be detected and mitigated through complementary or alternative features, as outlined below.

Wireless Ad-hoc Connections

CSA addresses the threat posed by wireless ad-hoc connections from a client endpoint perspective, protecting a client hosting this type of connection no matter which location the client may be in at any time.

To complement this, the wireless IDS/IPS features of the Cisco WLAN Controller (WLC) address this threat from the network-side, providing threat detection and mitigation of wireless ad-hoc and rogue networks.

Leveraging both these features enables a more comprehensive approach to security: CSA protecting the client in all environments and WLC providing visibility and control of such activity on the corporate network.

For more information on the wireless IDS/IPS features of the Cisco WLC, refer to Reference Documents, page 7-56.

Simultaneous Wired and Wireless Connections

CSA addresses the threat posed by simultaneous wired and wireless connections by restricting traffic over the wireless network if an Ethernet port is active.

Cisco offers an alternative client-based approach to address this threat with the Cisco Secure Services Client (CSSC). CSSC is a software client that manages the user identity, device identity and network access protocols required for secure access to both wired and wireless networks. One of its features includes the ability to block wireless access if a wired port is active. Its primary role, however, is to provide an 802.1X supplicant for wired and wireless networks, offering the centralized management of local network access profiles that enforce the use of appropriate authentication and encryption parameters.

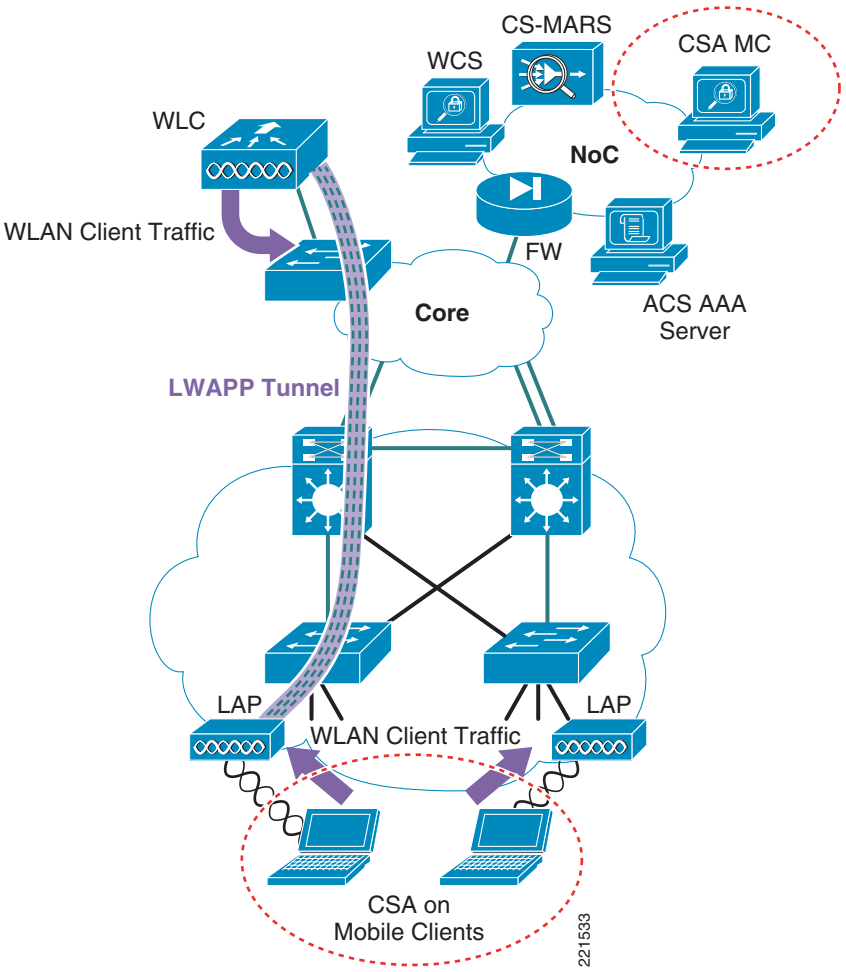
These two products both feature the ability to address simultaneous wired and wireless connections but the full feature sets and roles of each product perform very different but complementary roles in network security: CSA providing rich endpoint protection, data loss prevention and anti-virus, CSSC providing a strong authentication framework for secure access.

For more information on CSSC, refer to Reference Documents, page 7-56.

CSA Integration with the Cisco Unified Wireless Network

Integration of CSA within the Cisco Unified Wireless Network architecture involves CSA deployment on clients and deployment of a Cisco Management Center for Cisco Security Agents (CSA MC). (See Figure 7-3.)

Figure 7-3 CSA Integration within the Cisco Unified Wireless Network Architecture

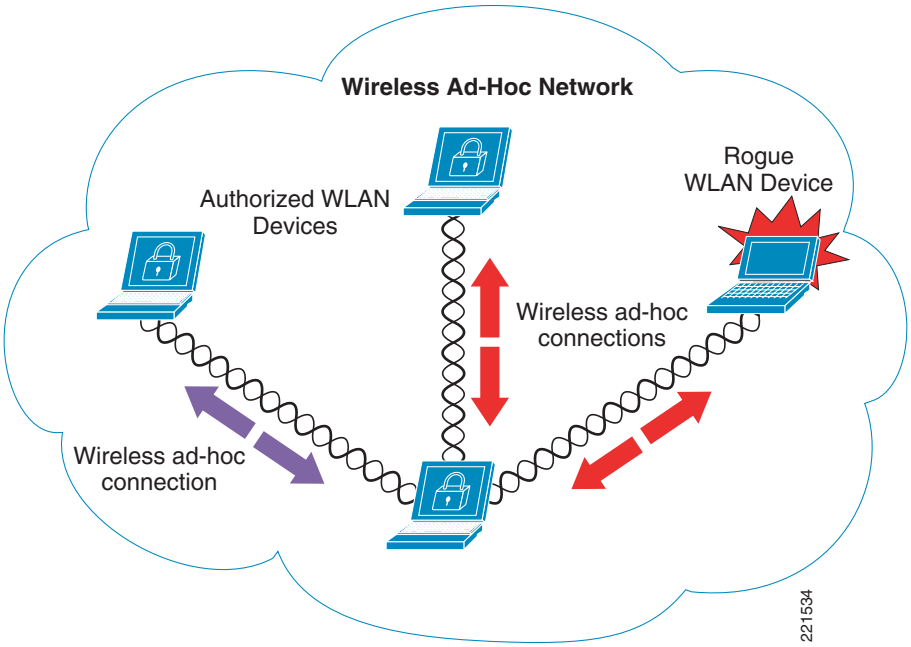


Wireless Ad-Hoc Connections

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 7-4.)

Figure 7-4 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 more information on this vulnerability and its exploitation, refer to Reference Documents, page 7-56.

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.

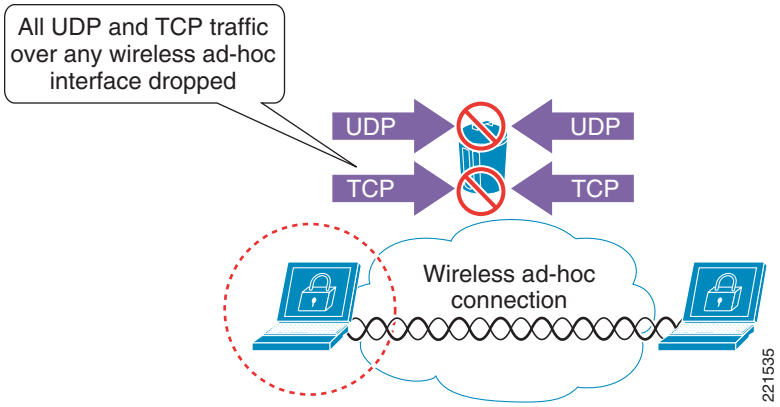
Pre-Defined Rule Module Operation

The default behavior of the predefined wireless ad-hoc Windows rule module can be summarized as follows:

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

(See Figure 7-5.)

Figure 7-5 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:

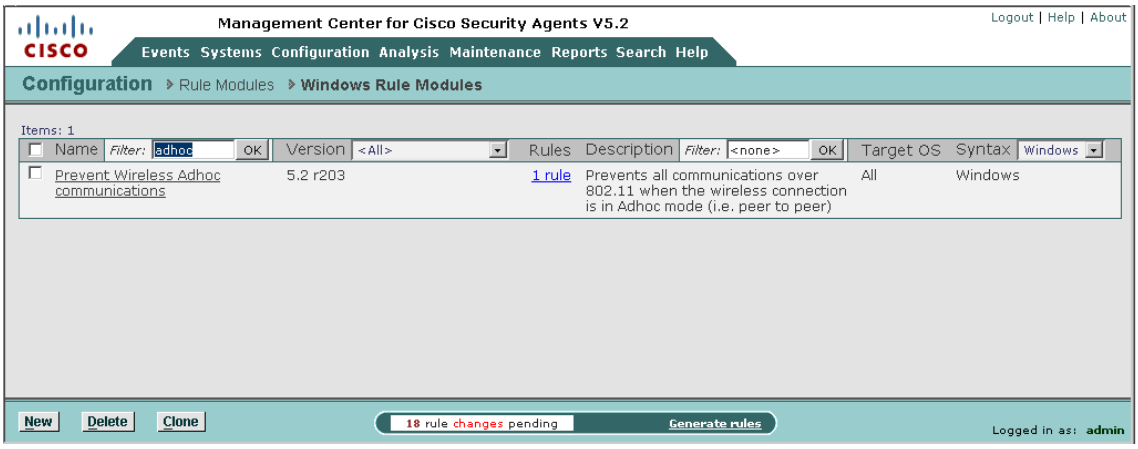
- UDP or TCP traffic detected on an active wireless ad-hoc connection invokes the rule module. This is true regardless of whether any other network connections are active or not.
- All UDP and TCP traffic routed over a wireless ad-hoc connection is dropped.
- Traffic on a non-wireless ad-hoc connection 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 Configuration

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

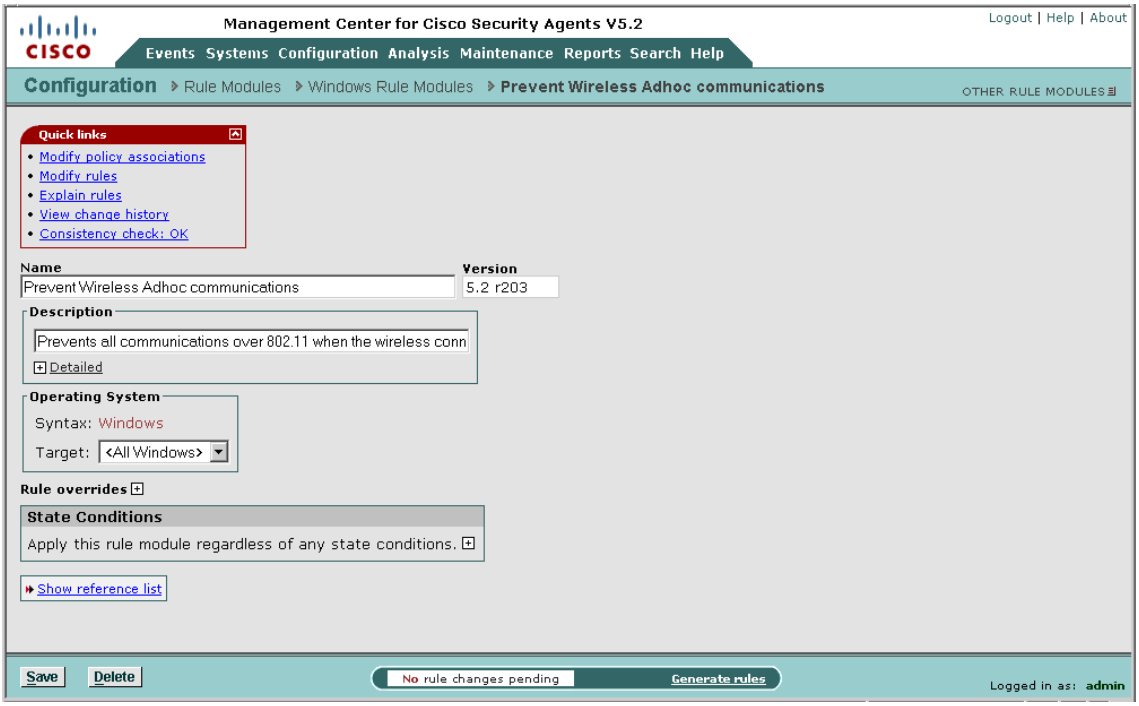
It can be located on the CSA MC by browsing to **Configuration -> Rule Modules -> Rule Modules [Windows]**. Define a filter with the name **adhoc** to locate it quickly. (See Figure 7-6.)

Figure 7-6 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 7-7.)

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



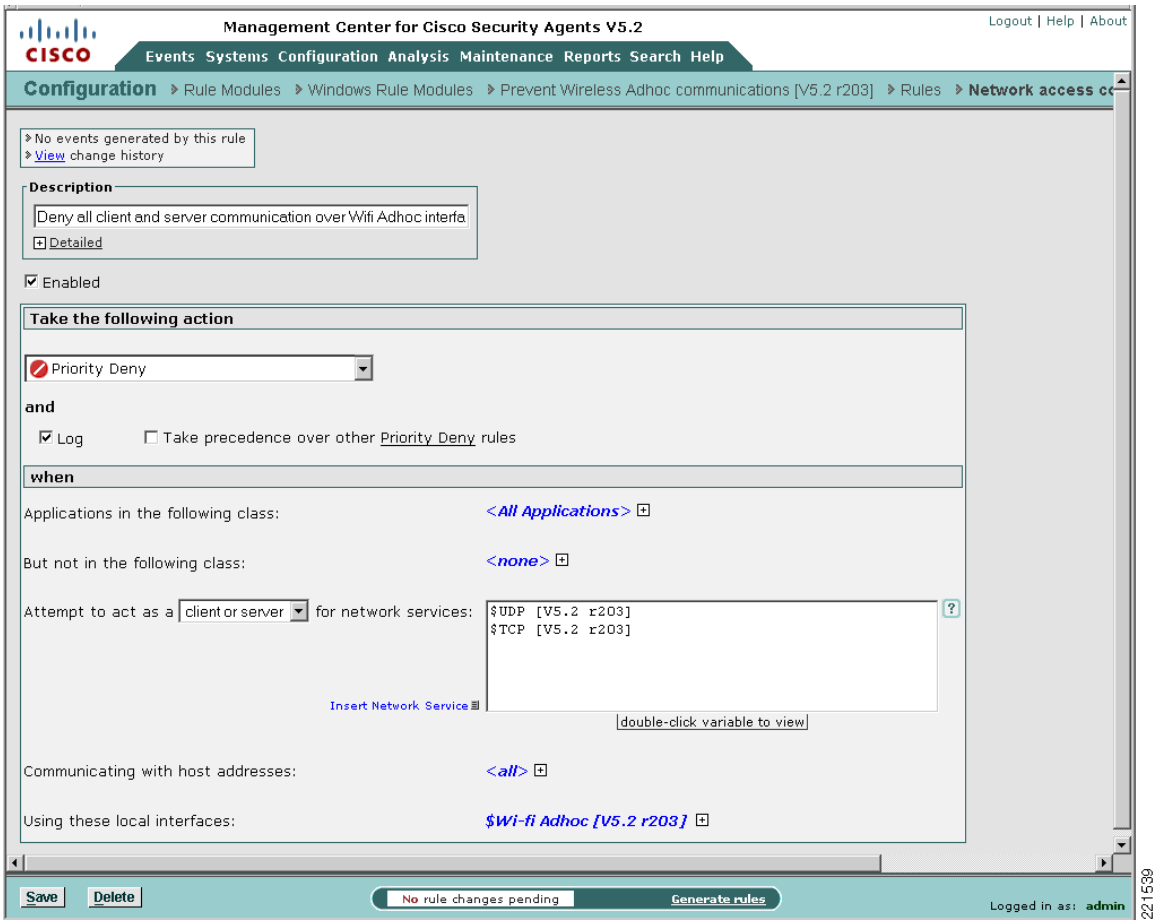
Click the **Modify** rules link to present the associated rule. (See Figure 7-8.) This may also be accessed directly from the rule module listing by clicking the **1 rule** link.

Figure 7-8 Rule Associated with the Pre-defined Wireless Ad-hoc Windows Rule Module

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

Click the rule name to display the detailed configuration of the rule. (See Figure 7-9.)

Figure 7-9 Pre-defined Wireless Ad-hoc Rule Configuration



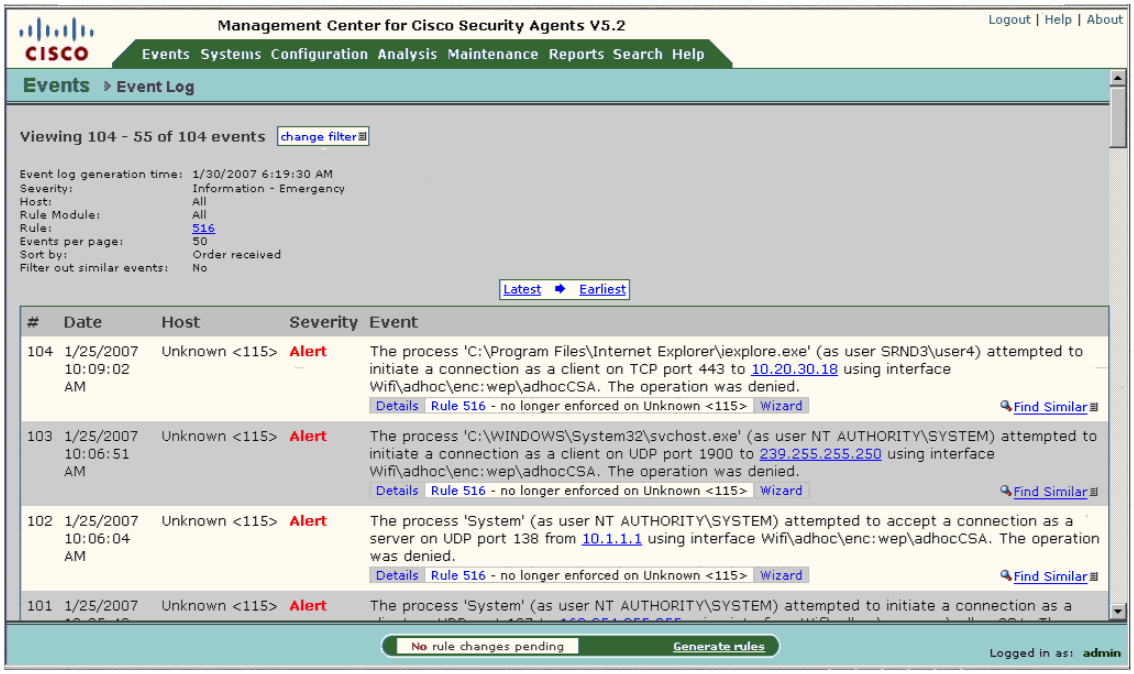
This shows the detailed configuration of the rule whereby any UDP or TCP traffic over a wireless ad-hoc connection is denied, regardless of the application or IP address.

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 7-10.

Figure 7-10 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.

The sample development of a customized rule module is presented in Sample Development of a Customized Rule Module, page 7-47.

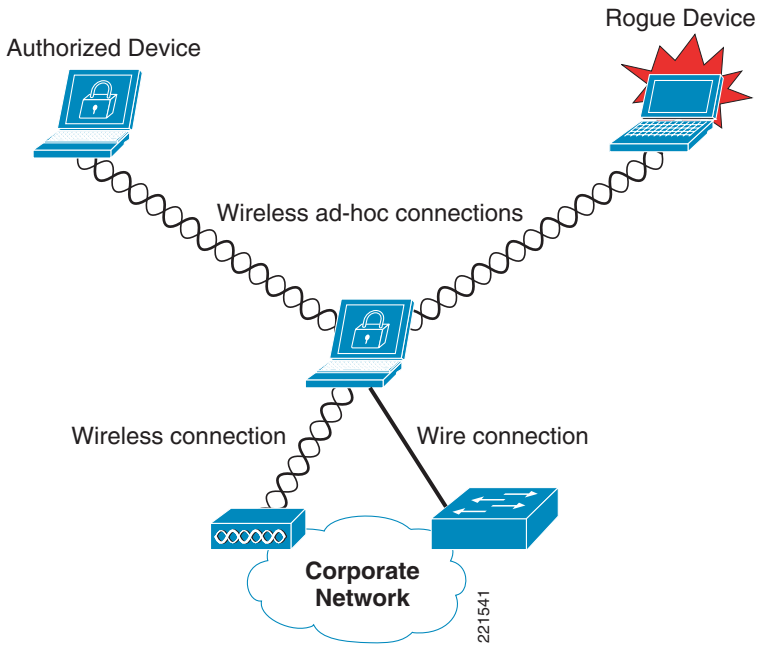
Note The business requirements and security policy of each individual customer vary and must be reviewed and applied on a per-case basis before deployment.

Simultaneous Wired and Wireless Connections

Simultaneous wired and wireless connections occur 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, or a wireless ad-hoc network. (See Figure 7-11.)

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 7-11 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 pre-defined rule module encompasses all 802.11 wireless connections, including 802.11 a/b/g/n, open, ad-hoc, and secure 802.11 wireless connections. Non-802.11 wireless connections, such as those to 3G networks, are not included but customized rules can be created to do so.

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

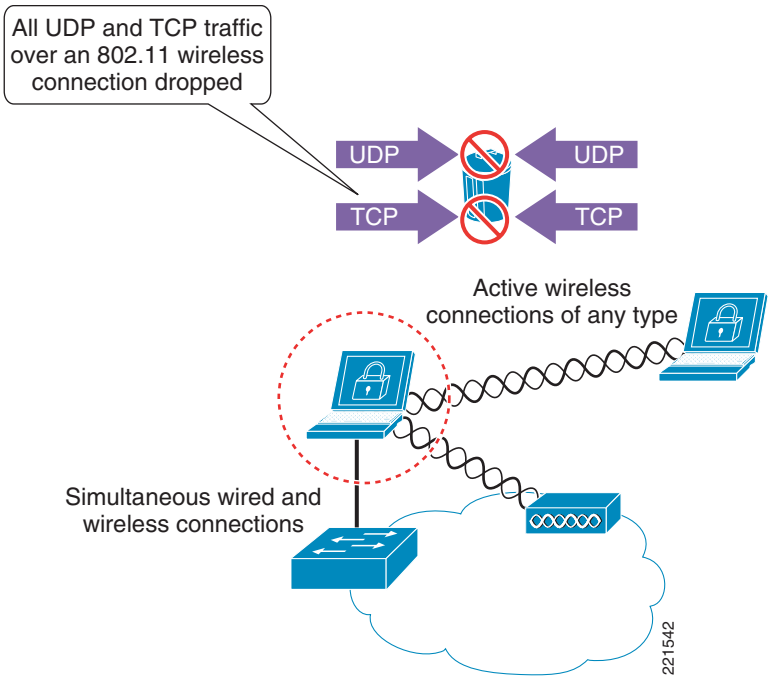
If CSSC is deployed on endpoints, the simultaneous wired and wireless feature of this client can be leveraged as an alternative means of blocking this threat.

Pre-Defined Rule Module Operation

The default behavior of the pre-defined simultaneous wired and wireless Windows rule module (see Figure 7-12) can be summarized as follows:

If an Ethernet connection is active, all UDP or TCP traffic over any active 802.11 wireless connection is denied, regardless of the application or IP address.

Figure 7-12 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:

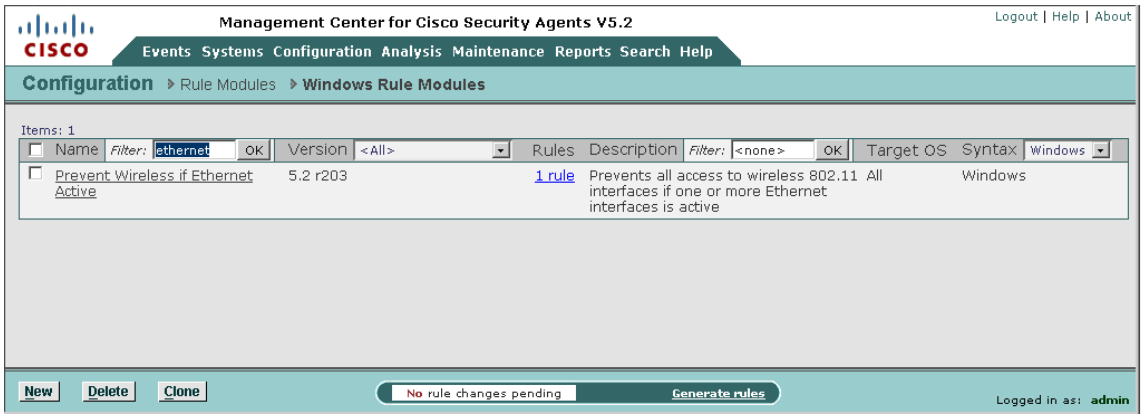
- If an Ethernet connection is active, UDP or TCP traffic detected on any active 802.11 wireless connection invokes the rule module. This is true regardless of the type of 802.11 connection, including open, ad-hoc, and secure wireless connections.
- All UDP and TCP traffic routed over any 802.11 wireless connection is dropped.
- Traffic on a non-802.11 wireless connection is not affected by this rule module.
- No user query is performed.
- A message is logged.
- When no Ethernet connection is active, the rule module is revoked.
- No logging occurs after revocation of a rule module..

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**.

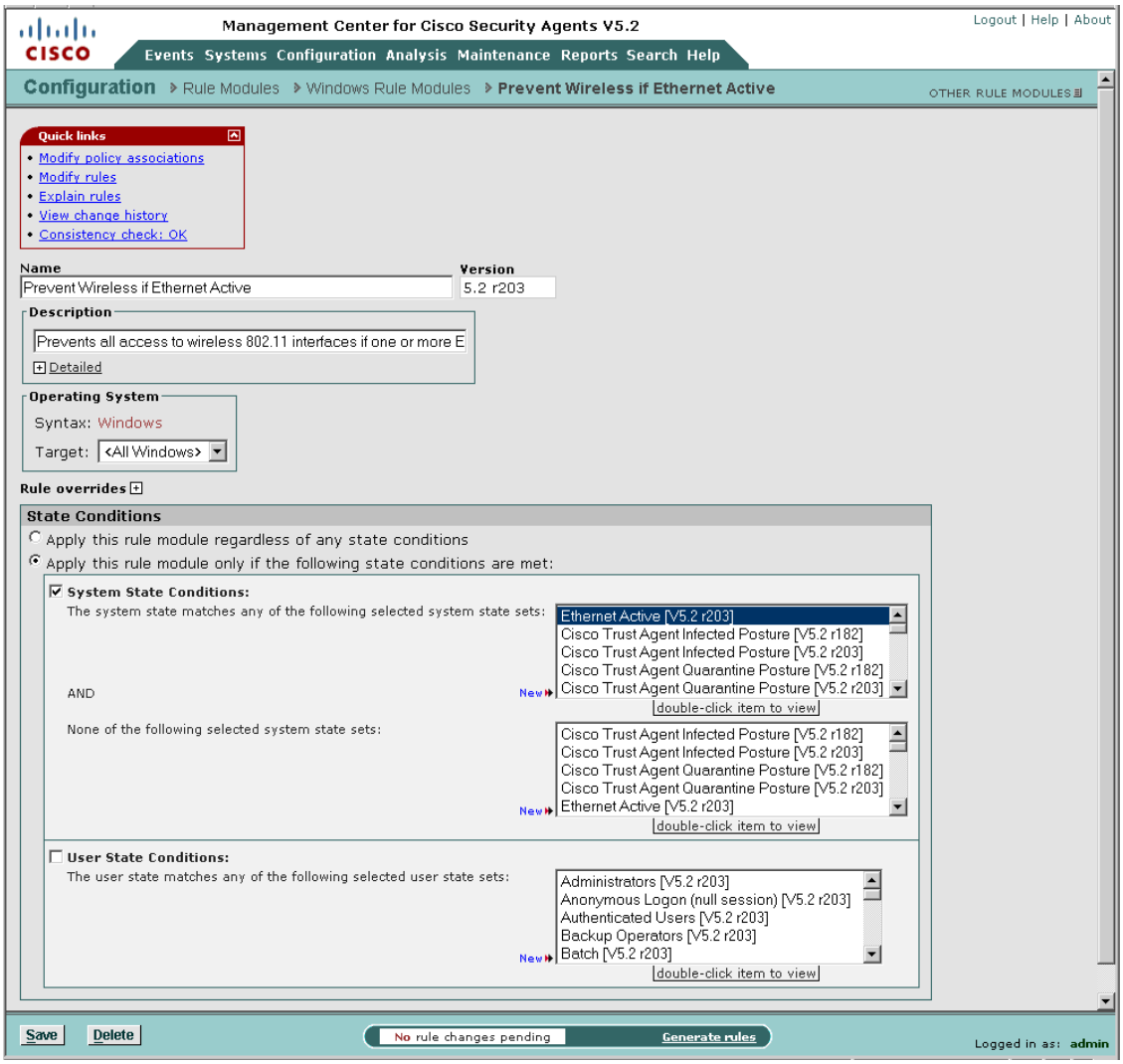
It can be located on the CSA MC by browsing to **Configuration** -> **Rule Modules** -> **Rule Modules [Windows]**. (See Figure 7-13.) Define a filter with the name **ethernet** to locate it quickly.

Figure 7-13 Pre-defined Simultaneous Wired and Wireless Windows Rule Module Listing



Click the name of the rule module to present the description, operating system, and state conditions associated with this rule module. (See Figure 7-14.)

Figure 7-14 Pre-defined Simultaneous Wired and Wireless Windows Rule Module Configuration

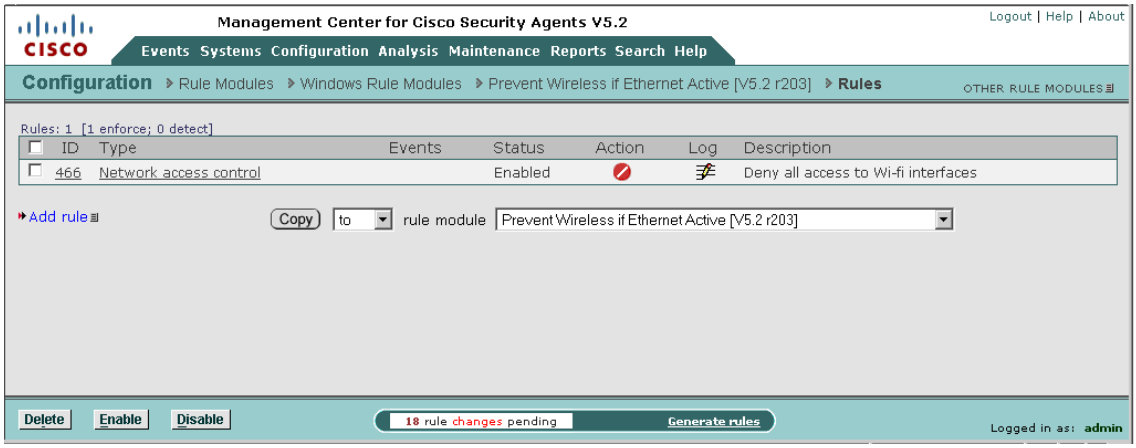


This shows the state condition that exists for this rule, whereby the Ethernet interface must be active for the rule be invoked.

Click the **Modify** rules link to present the rule summary. (See Figure 7-15.)

This may also be accessed directly from the rule module listing by clicking the **1 rule** link. (See Figure 7-13.)

Figure 7-15 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.

Click the rule name to present the detailed configuration of the rule. (See Figure 7-16.)

Figure 7-16 Pre-defined Simultaneous Wired and Wireless Rule Configuration

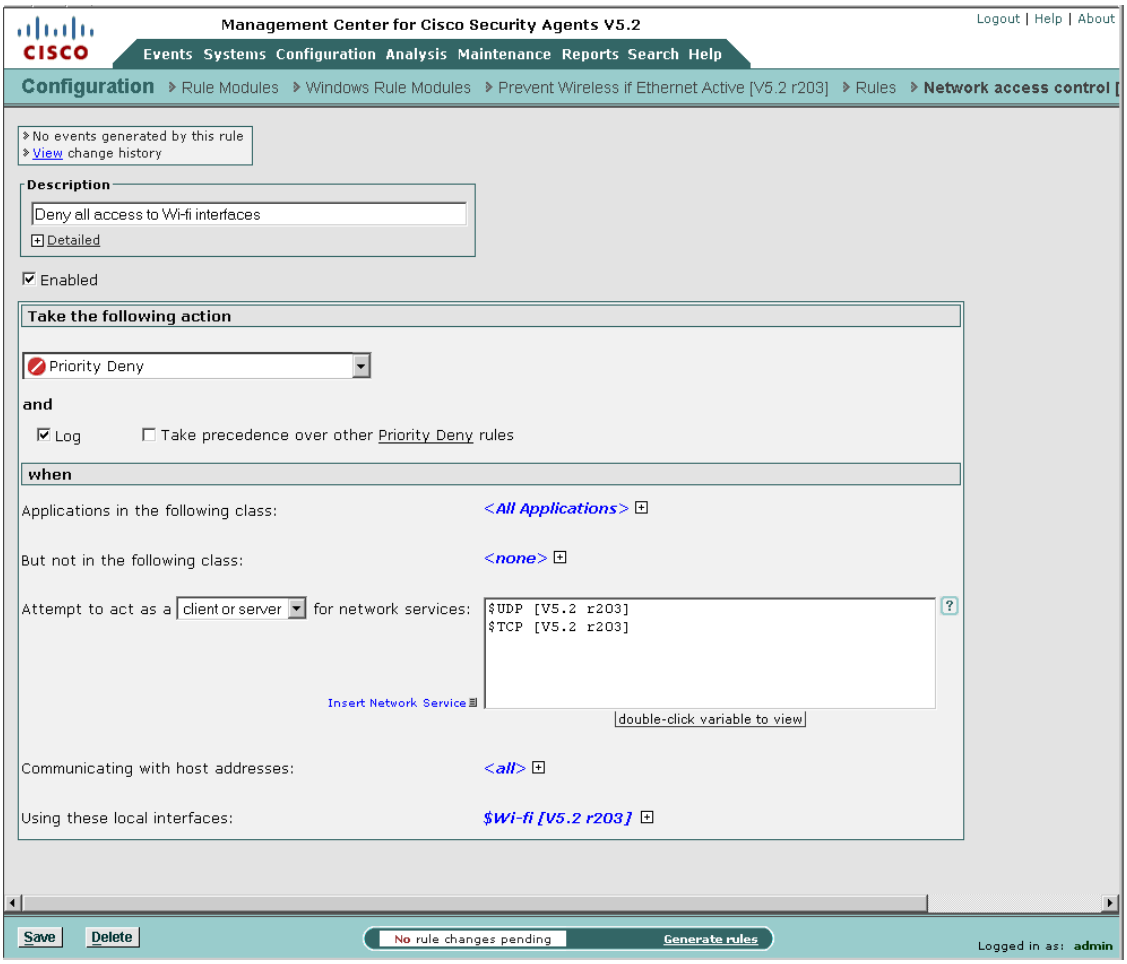


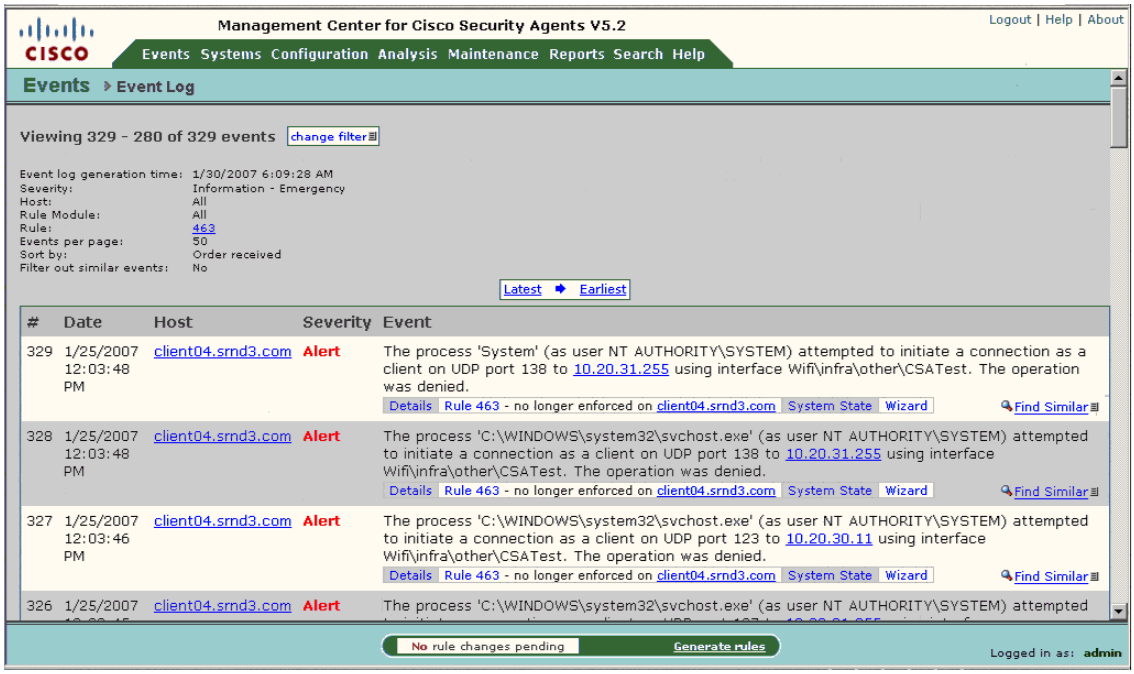
Figure 7-16 shows the detailed configuration of the rule, whereby if an Ethernet connection is active, all UDP or TCP traffic over any active 802.11 wireless connection is denied, regardless of the application or IP address.

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 7-17.

Figure 7-17 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 802.11 wireless connection is to the corporate WLAN but deny traffic to other WLANs. See Location-Aware Policy Enforcement, page 7-22 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.

The sample development of a customized rule module is presented in Sample Development of a Customized Rule Module, page 7-47.

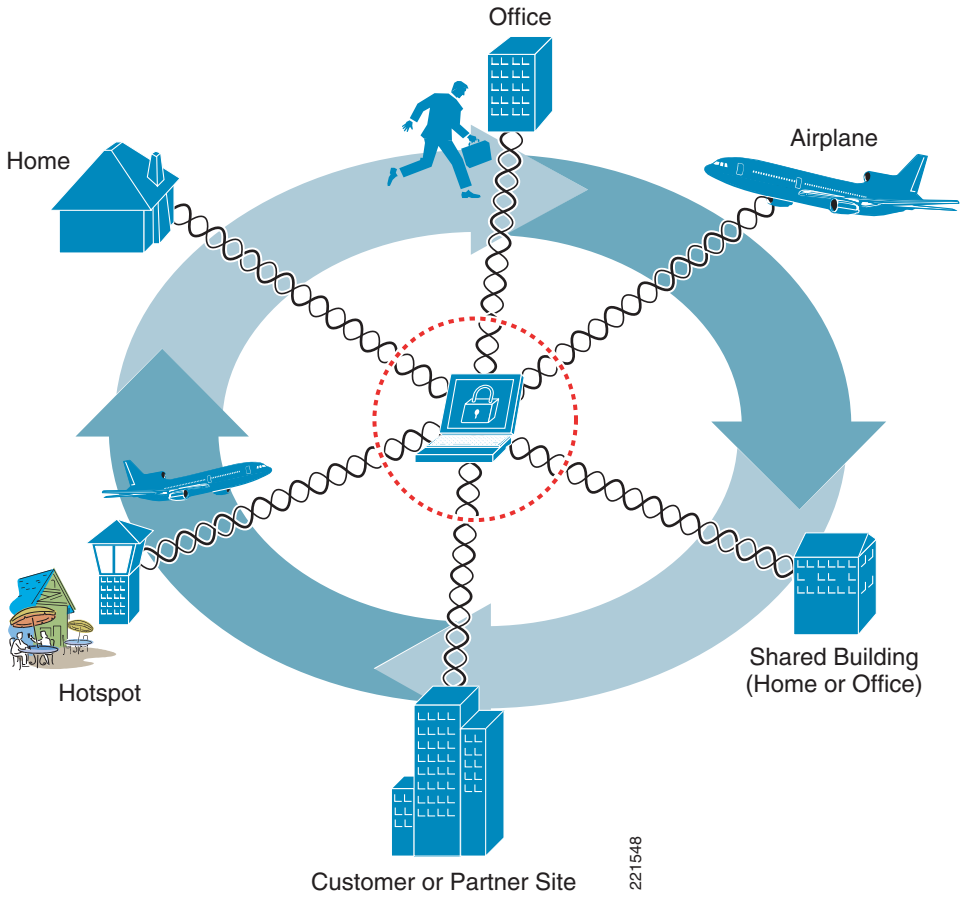
Note The business requirements and security policy of each individual customer vary and must be reviewed and applied on a per-case basis before deployment.

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 mobile client is connected, based on the perceived security risk associated with their location (see Figure 7-18). A mobile client may connect to a range of different networks, including the following:

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

Figure 7-18 Possible Locations and Networks to which a Mobile Client May Connect



Mobile Client Security Threat Exposure

Mobile clients connect to different networks in different locations and are thus exposed to additional security risks for some of the following reasons (see Figure 7-19):

- 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.

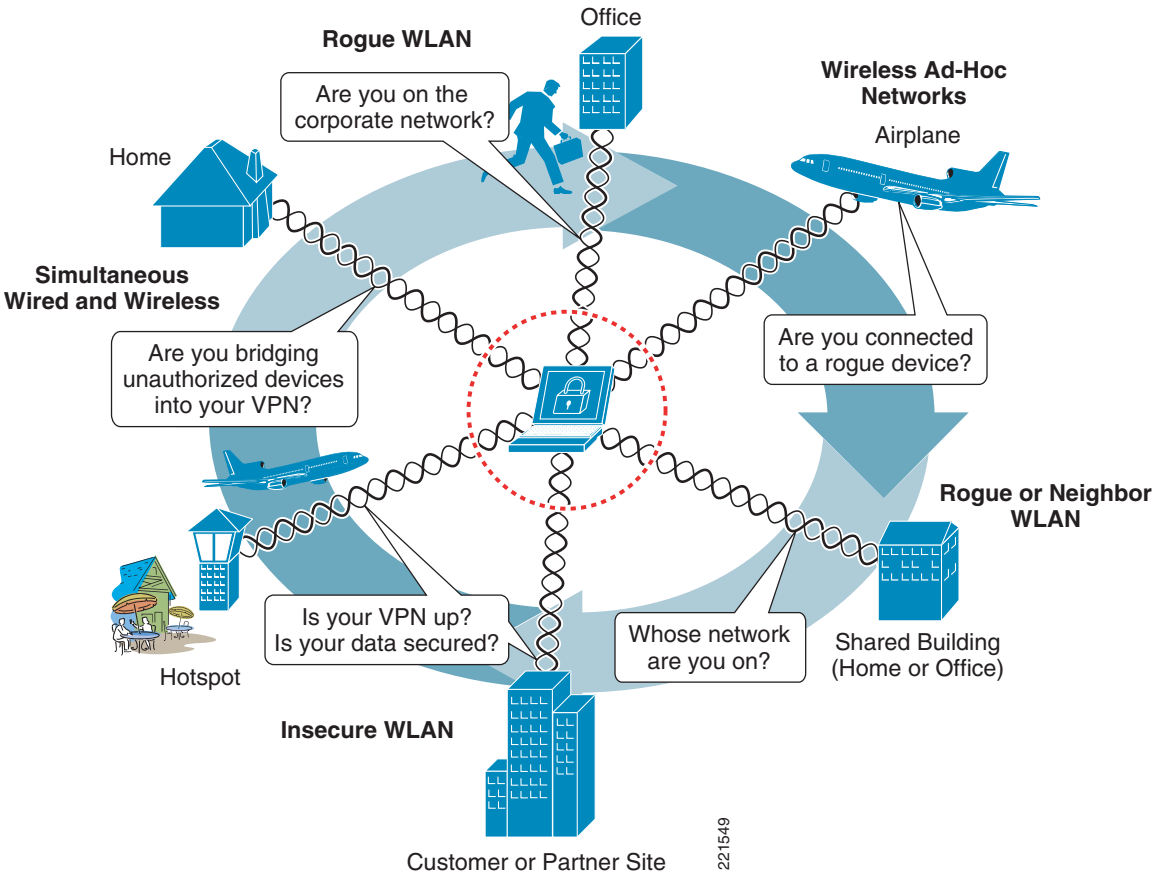
- Lack of user awareness of an active WLAN connection

  The end user of a mobile 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 7-19 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 mobile client. This enables the security protection measures to be adapted according to the risks associated with a particular location and the appropriate security policies enforced. For instance, when a mobile client is connected to a non-corporate network, stricter controls could be enforced to lock down the host and the user could be forced to initiate a VPN connection back to the corporate site.

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, refer to CSA Force VPN When Roaming Pre-Defined Rule Module, page 7-31.

In order to complement the deployment of CSA, CSSC should be considered to enforce the required authentication and encryption parameters for each authorized network profile, as well as to enable the automatic activation of a VPN connection when required. For more information on CSSC, refer to the product documentation (see Reference Documents, page 7-56).

Location-Aware Policy Enforcement Operation

CSA currently enables the location of a mobile 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.

Location-Aware Policy Enforcement Configuration

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

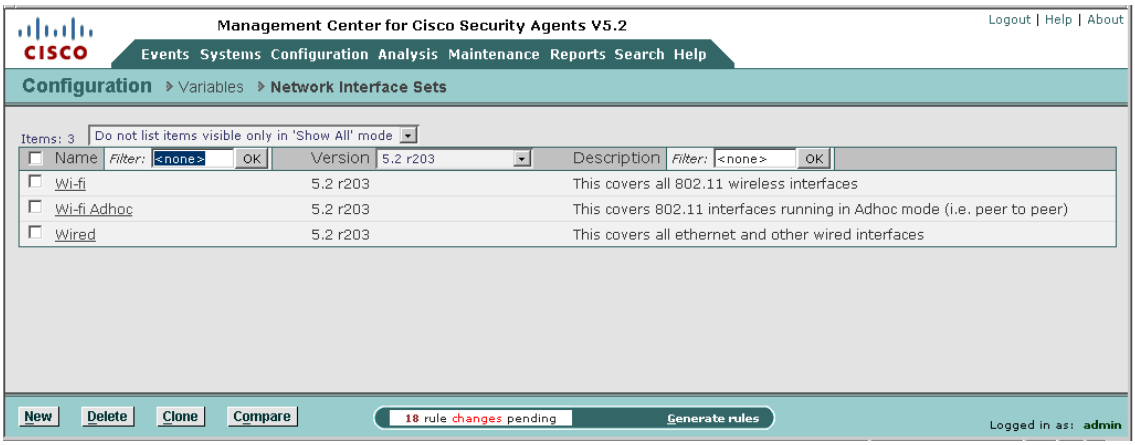
- Define the qualifying network interface sets.
- Define the qualifying system state conditions.
- Define a location-specific rule module.

- 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 7-20.)

Figure 7-20 Pre-defined Network Interface Sets



Clicking the name of a network interface set presents its description and associated configuration parameters. (See Figure 7-21.)

Figure 7-21 Pre-defined Wi-Fi Network Interface Set

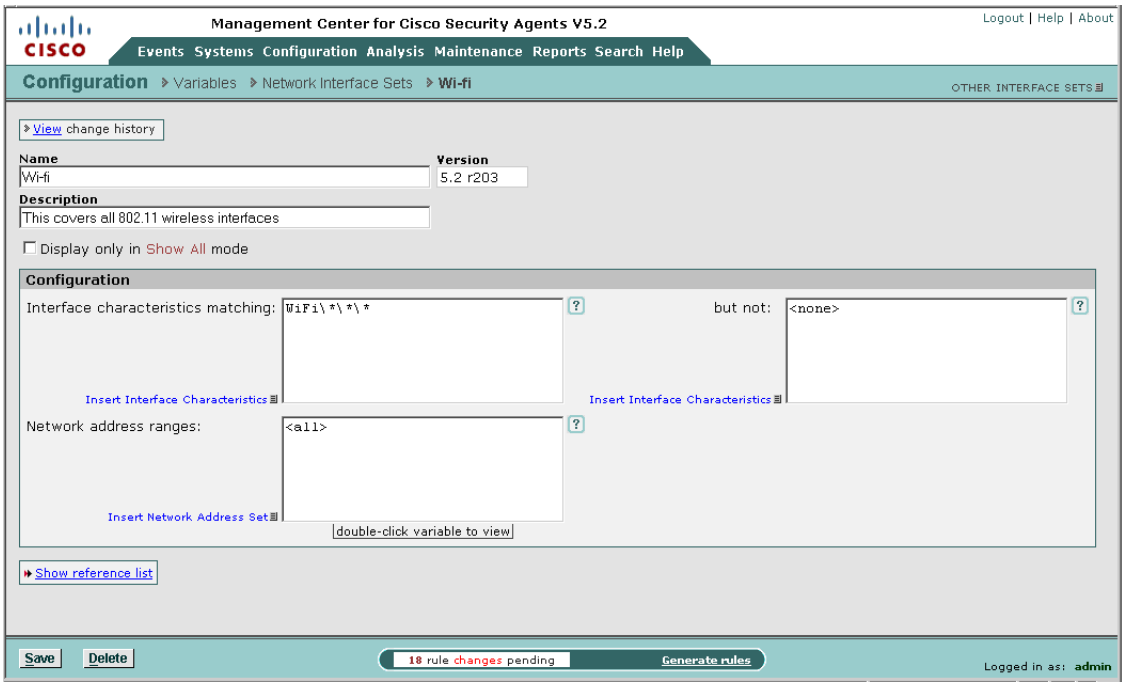


Figure 7-21 shows the pre-defined Wi-Fi network interface set that incorporates all wireless connections, regardless of mode, encryption, or SSID, as indicated by the wildcards in the interface characteristics definition “WiFi***”.

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 7-22):

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

Figure 7-22 Configurable Wi-Fi Parameters and Sample Definition of a Corporate WLAN

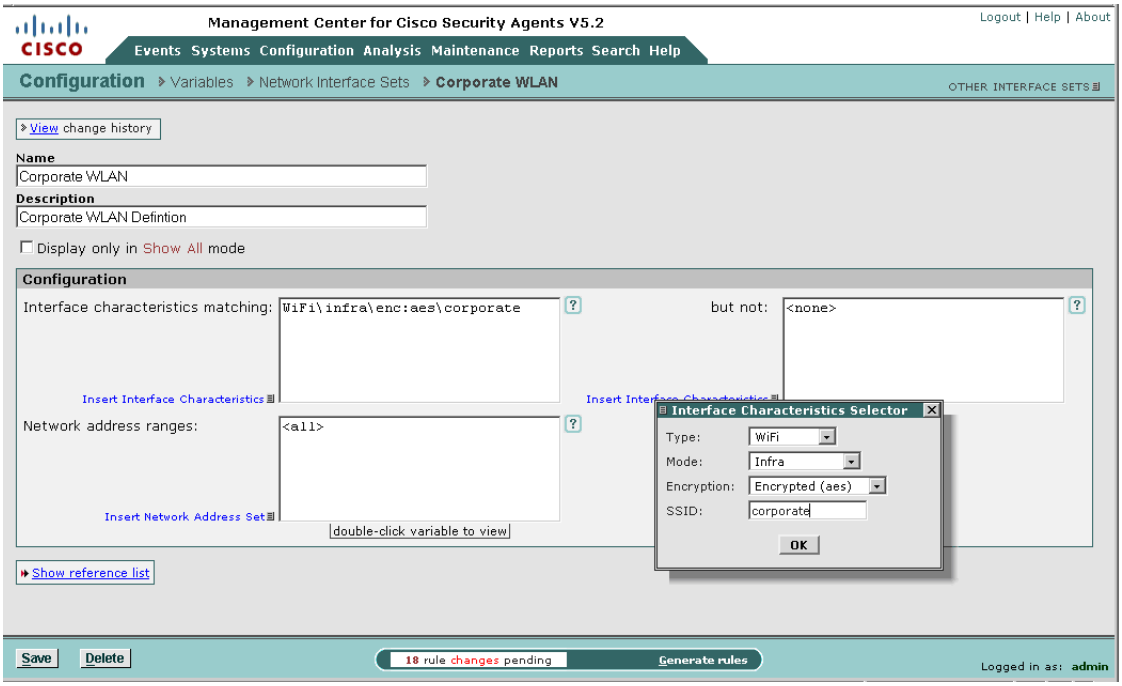
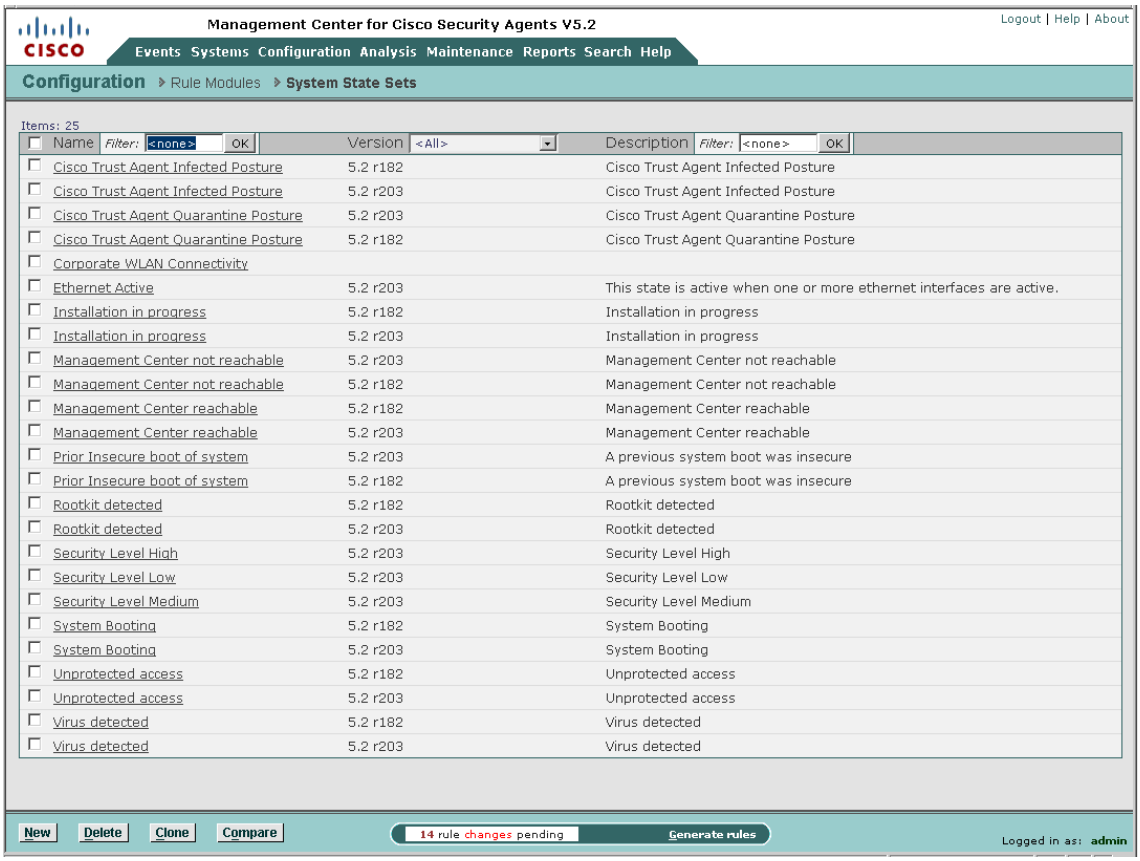


Figure 7-22 shows the network interface characteristics that can be defined for wireless connections, including mode, encryption, and SSID. Figure 7-22 also shows how a corporate WLAN can be defined.

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 7-23.)

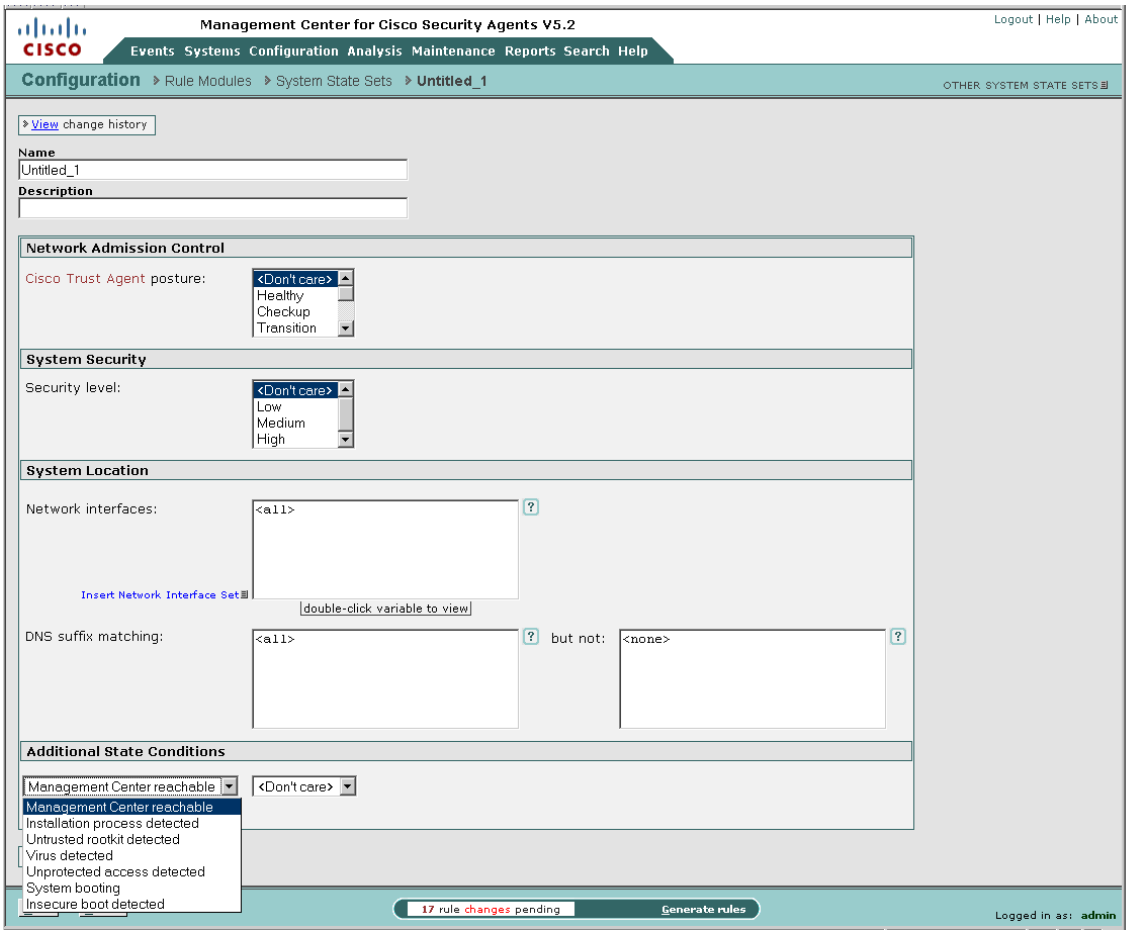
Figure 7-23 Pre-defined System State Sets



New system state sets can be created based on a number of parameters, including the following (see Figure 7-24):

- 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 7-24 Configurable Parameters for Custom System State Sets

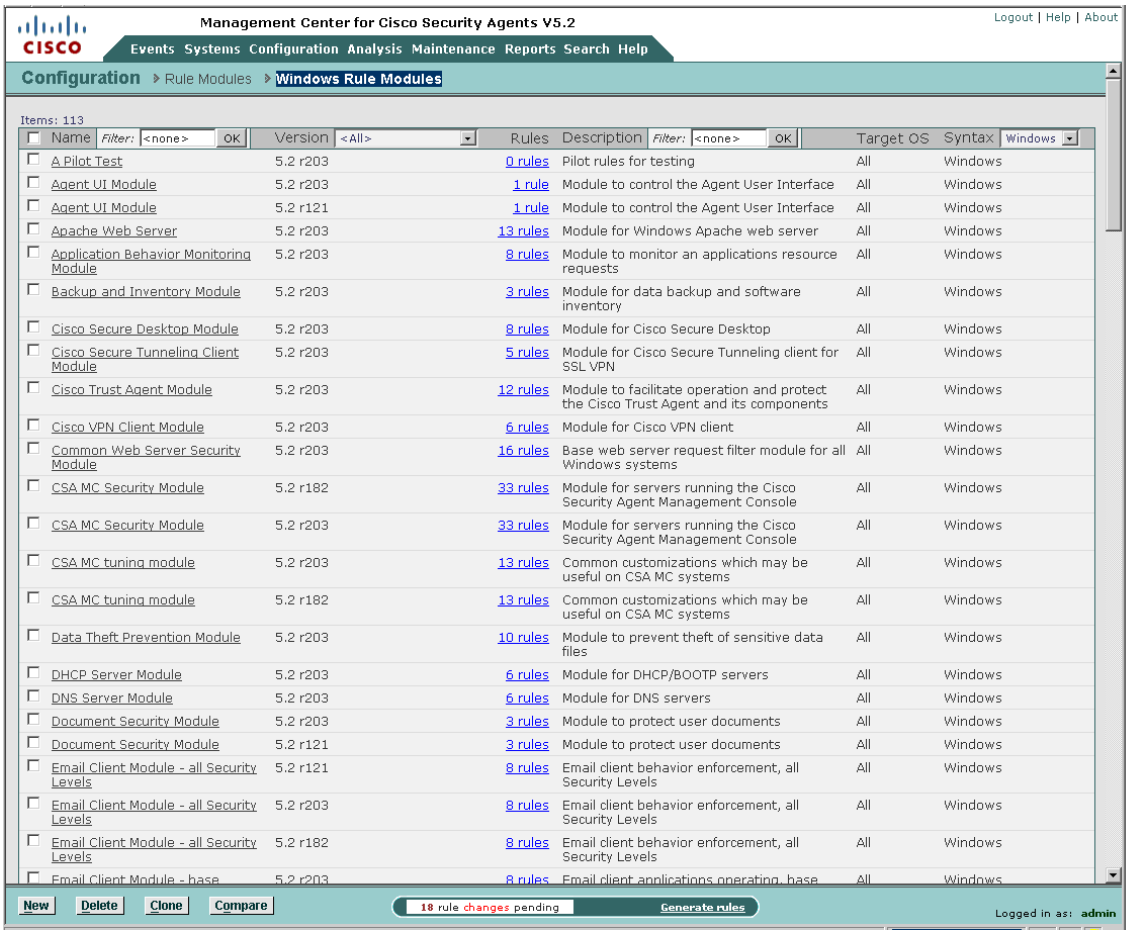


Viewing and Defining Location-Aware Rule Modules

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 7-25.)

Figure 7-25 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 7-31 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**.

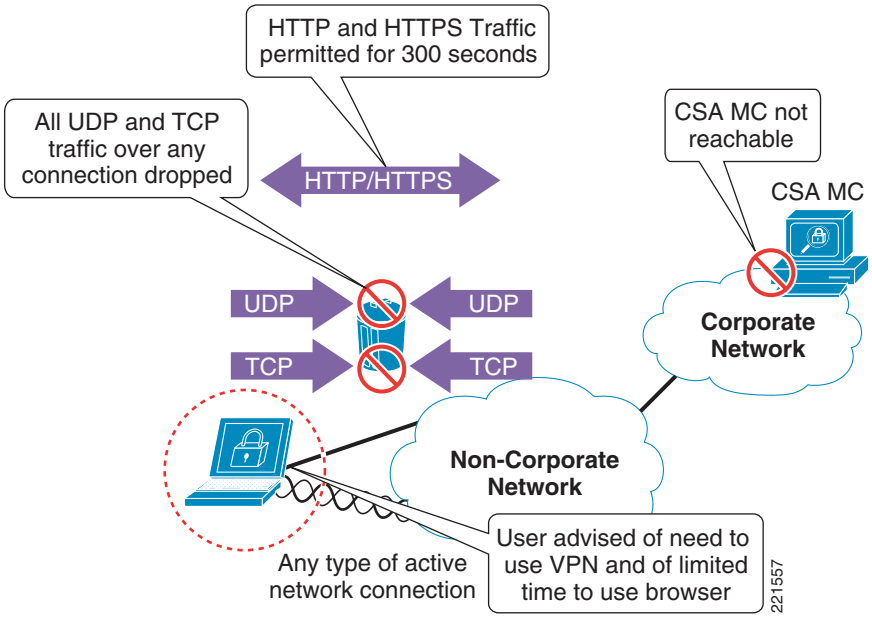
In a roaming scenario, enforcement of this rule module can be used to enforce security policy and protect the client itself, local data, and data in transit when on insecure, non-corporate networks.

Pre-Defined Rule Module Operation

The default behavior of the pre-defined force VPN when roaming Windows rule module (see Figure 7-26) 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 7-26 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 connection invokes the rule module. This is true regardless of the type of connection being used.
- All UDP and TCP traffic routed over any connection is dropped, except HTTP or HTTPS traffic.
- HTTP or HTTPS traffic is permitted for a period of 300 seconds.

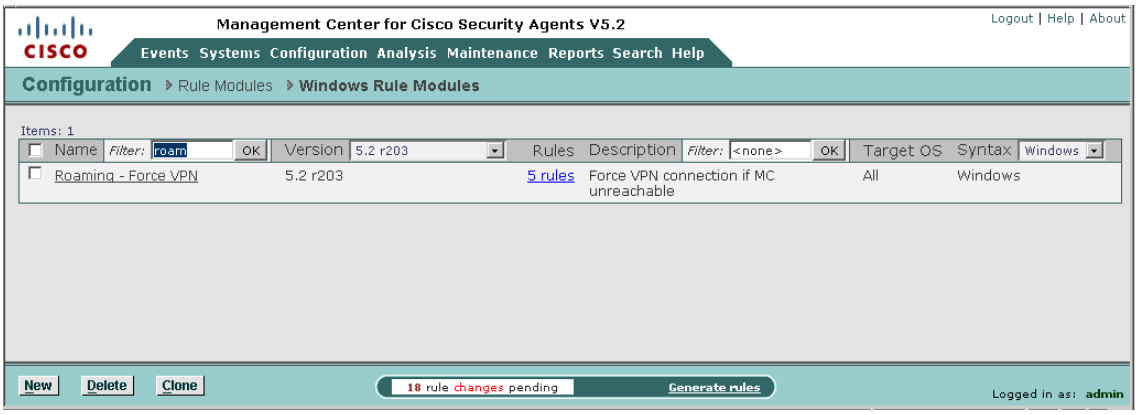
- A user query is presented, advising the user that they are not connected to the corporate network, that they must use the VPN client to gain access, and that they have limited time to use their browser to connect to a hotspot.
- A message is logged.
- If the CSA MC remains unreachable after expiration 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 Configuration

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

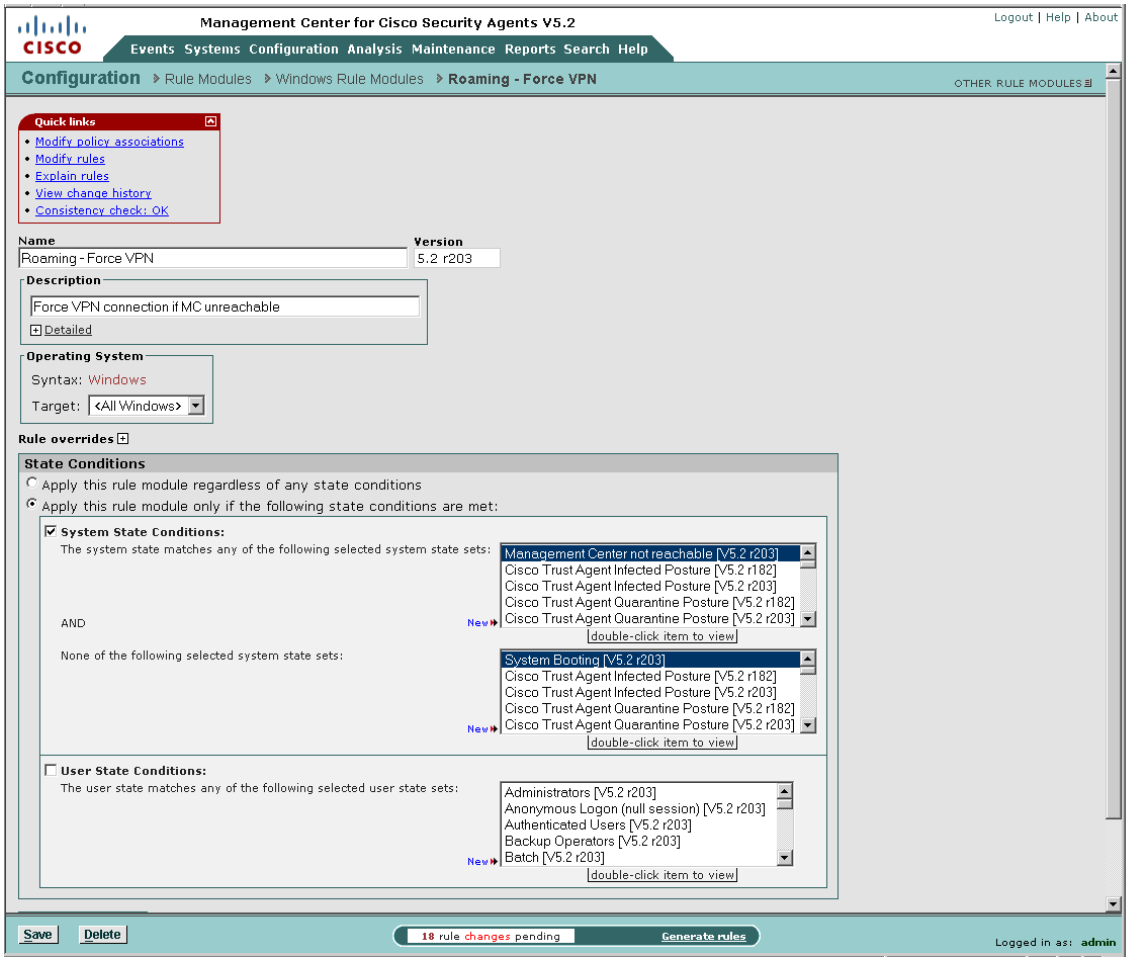
It can be located on the CSA MC by browsing to **Configuration -> Rule Modules -> Rule Modules [Windows]**. (See Figure 7-27.) Define a filter with the name **roam** to locate it quickly.

Figure 7-27 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 7-28.)

Figure 7-28 Pre-Defined Force VPN When Roaming Windows Rule Module Definition

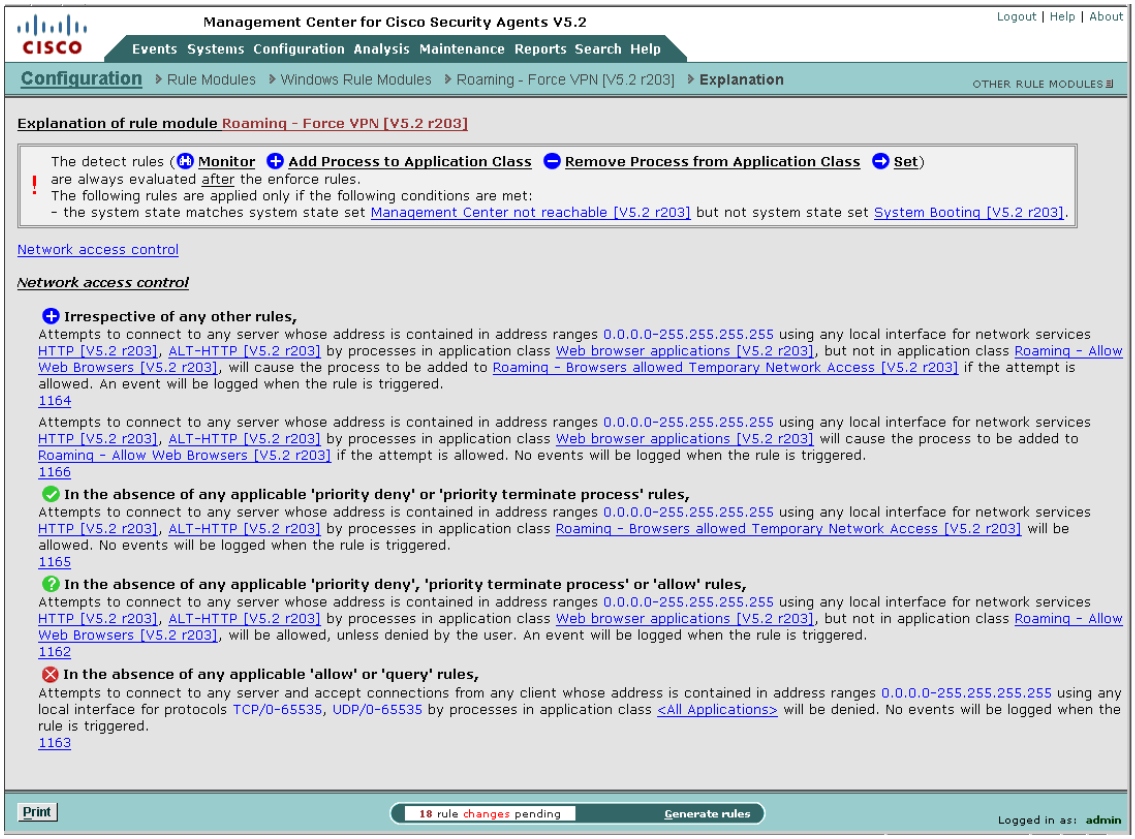


Note that the state conditions for this pre-defined rule module require the following conditions to be met for the rule to be invoked:

- Management Center not reachable
- System not booting

Clicking the **Explain rules** link presents an explanation of the rules and their associated actions. (See Figure 7-29.)

Figure 7-29 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 7-30.)

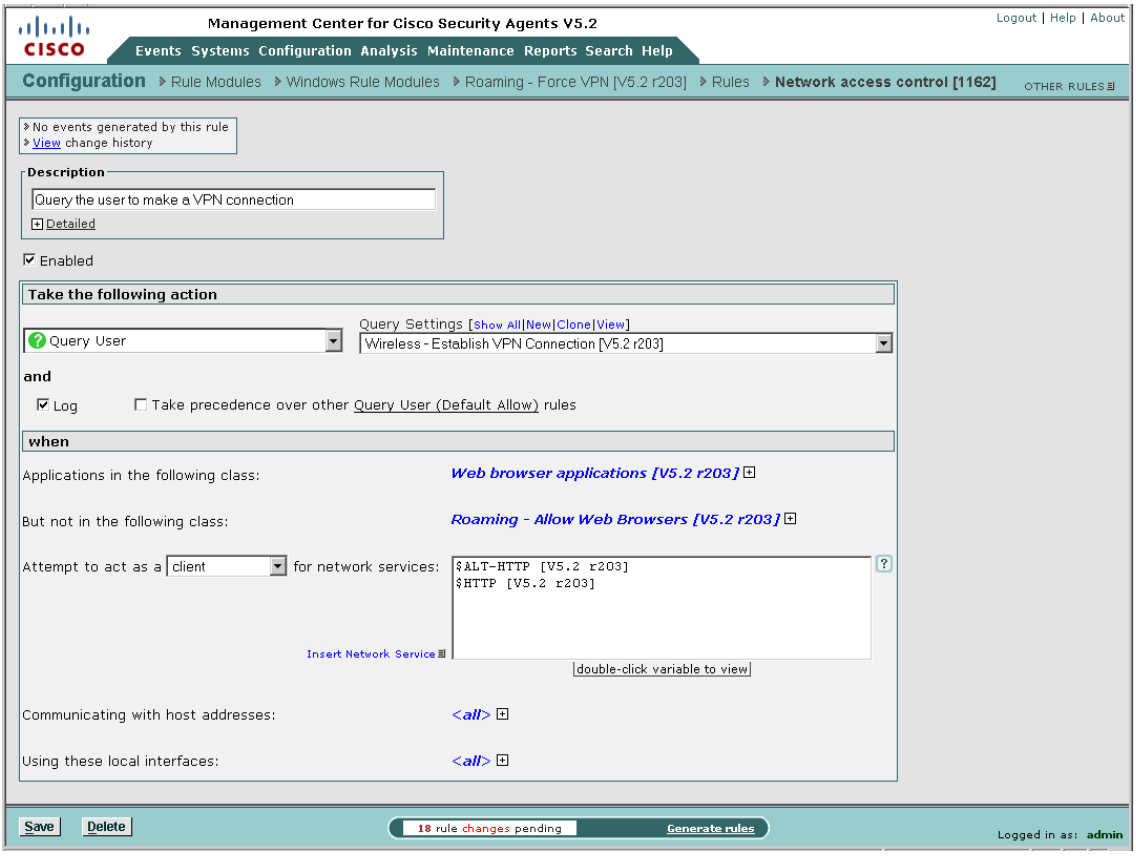
The rules may also be accessed directly from the rule module listing by clicking the **5 rules** link. (See Figure 7-27.)

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

Figure 7-30 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 7-31.)

Figure 7-31 Pre-Defined Network Access Control Rule to Query the User to Make a VPN Connection



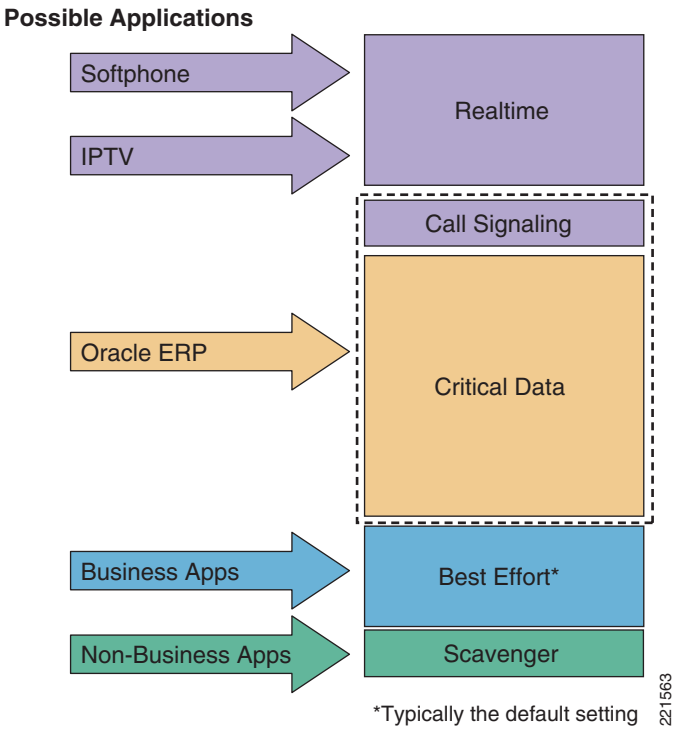
Upstream QoS Marking Policy Enforcement

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 7-32):

- 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 7-32 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.

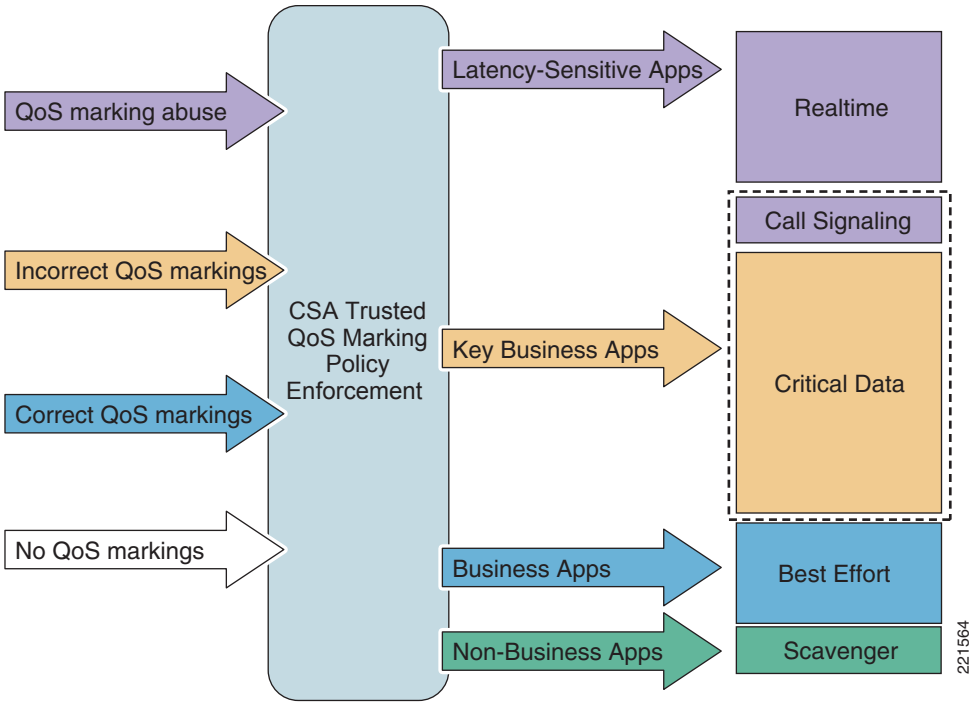
- Lack of QoS support in legacy applications

  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 7-33.)

Figure 7-33 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.

For more information on the CSA Trusted QoS feature, refer to the document listed in the CSA section of Reference Documents, page 7-56.

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 7-2.

Table 7-2 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.

Implementation of the CSA Trusted QoS feature is not covered in detail in this document. For more information on implementing this feature, refer to the document listed in the CSA section of Reference Documents, page 7-56.

CSA Wireless Security Policy Reporting

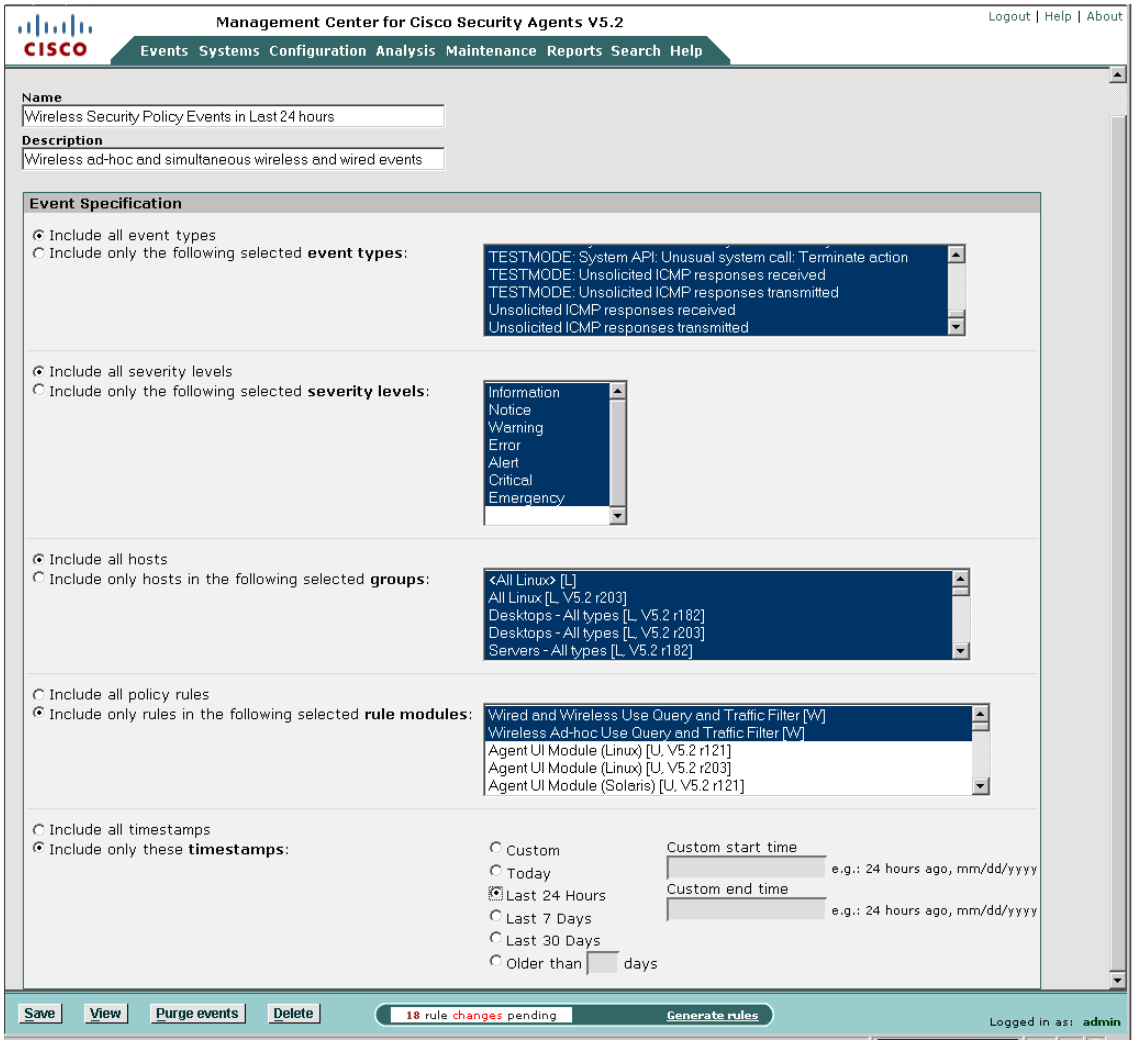
CSA Management Center Reports

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.

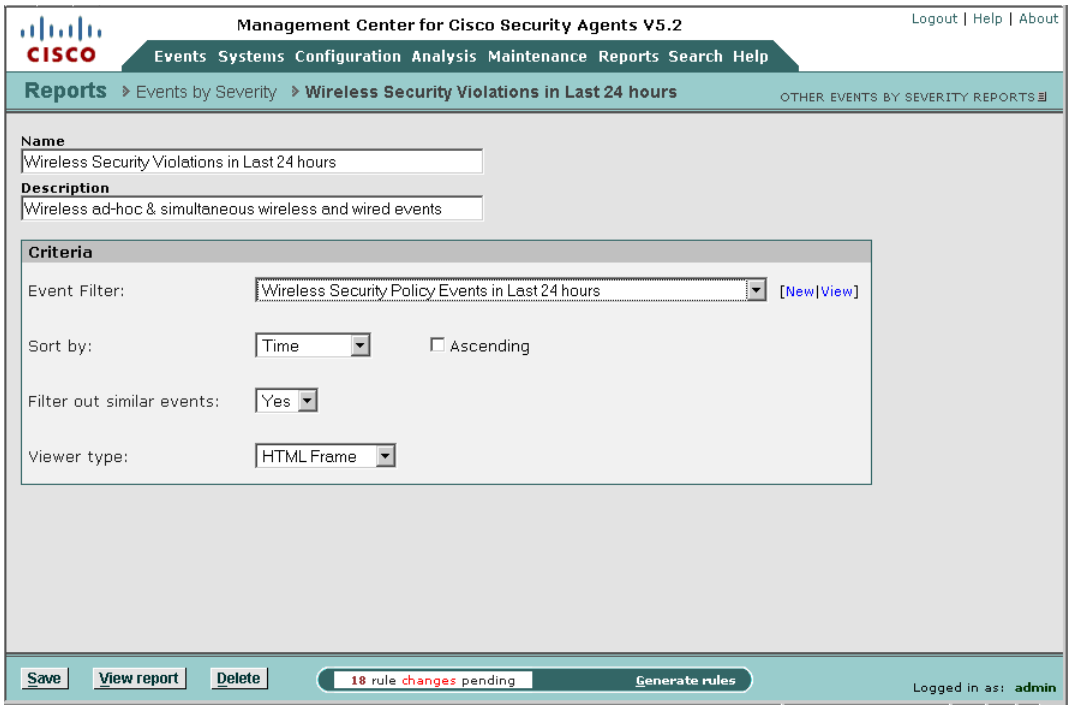
Step 1 Define an event set for the wireless-specific policies of interest and the time period required. Browse to **Events** -> **Event Sets** and create a new event set including only the wireless-specific rule modules and set the timestamps; for example, to the last 24 hours. (See Figure 7-34.)

Figure 7-34 Creation of a Wireless-Specific Event Set Based on Wireless-Specific Policies



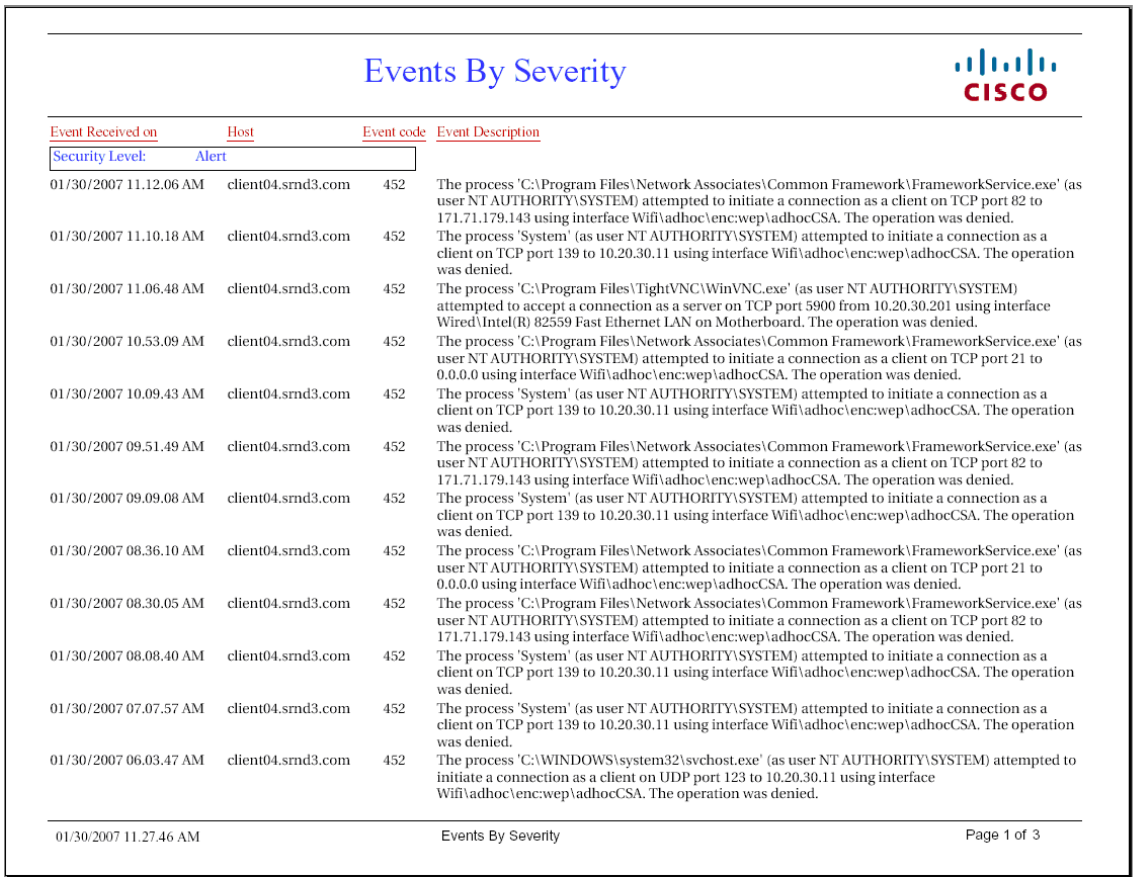
Step 2 Create and define a report on events by severity or by group, depending on the required format, using the newly defined event set as the event filter. Browse to **Reports** -> **Event Severity** and create a new report with the event filter set to the newly created wireless-specific event set. (See Figure 7-35.)

Figure 7-35 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 7-36.) This can be useful for traceback when an incident occurs.

Figure 7-36 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 CS-MARS platform is supported by CSA delivering SNMP alerts to CS-MARS. For information on configuring host-based IDS and IPS devices, see the CS-MARS user guide listed in Reference Documents, page 7-56.

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

General Guidelines for CSA Mobile Client Security

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

- Deploy CSA for general client endpoint protection.
- Consider additional CSA policies to address threats encountered by mobile clients, 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 network access profiles according to security policy, including WLAN profiles, authentication and encryption parameters.

Customers are recommended to do the following:

- Develop customized CSA policies that enforce the defined corporate security policies.
- Carefully review the operational considerations outlined for each rule module in relation to their particular environment before deployment.
- Ensure that WLAN policy violation events are regularly monitored and reviewed as part of the overall security policy.

Additional Information

CSA Pre-Defined Rule Module Operational Considerations

Wireless Ad-Hoc Connections

Cisco recommends that customers wishing to implement wireless ad-hoc policy enforcement consider the following operational aspects of the CSA 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 connection cease to function upon the rule module being invoked because the return IP address is that of the wireless adapter hosting the wireless ad-hoc connection, which is now being filtered. Sessions need to be re-established through a non-wireless ad-hoc connection.

  - ICMP pings that route over a wireless ad-hoc connection 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.
  - Outgoing ICMP continues to function over a wireless ad-hoc connection, even if a CSA Network Shield rule module is enforced. This may present some confusion to end users because the wireless ad-hoc connection is active and connected, and ICMP pings continue to function, but the connection appears 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.

- Client routing table
  - The routing table is not updated upon the rule module being enforced, because all wireless ad-hoc connections remain connected and active.
  - If a wireless ad-hoc connection 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. All traffic to that destination is dropped, even if an alternative route exists over an alternative, non-wireless ad-hoc connection.
  - Ensure that operational staff are aware that some applications (UDP and TCP-based) may fail if a preferred route exists over a wireless connection on which the policy is being enforced.
- Complementary Features
  - Client-side mitigation of wireless ad-hoc connections and rogue access points should be complemented with network-side detection and mitigation, in order to provide defense-in-depth. This can be achieved on a Cisco Unified Wireless Network using the rogue AP security features of the WLC. For more information, refer to the WLC documentation (see Reference Documents, page 7-56).

Simultaneous Wired and Wireless Connections

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

- Wireless connection status
  - New 802.11 wireless connections continue to be initiated and accepted even if an Ethernet interface is active.
  - Established 802.11 wireless connections remain active and connected despite an Ethernet interface being active.
  - End users continue to see 802.11 wireless connections as active and connected.
- Traffic filtering
  - Only UDP and TCP traffic over an 802.11 wireless 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 an 802.11 wireless connection, before simultaneously connecting a wired interface, cease to function upon the rule module being invoked because the return IP address is that of the wireless adapter, which is now being filtered. Sessions either need to be re-established through a non-802.11 wireless connection or the Ethernet connection de-activated to revoke the rule module.

  - ICMP pings that route over an 802.11 wireless connection are not filtered by this rule module and remain a threat. Incoming ICMP packets can be filtered by enforcing a CSA Network Shield rule module.
  - Outgoing ICMP continues to function over an 802.11 wireless connection, even if a CSA Network Shield rule module is enforced. This may present some confusion to end users because the wireless connection is active and connected, and ICMP pings continue to function, but the connection appears 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.
- Client routing table
  - The routing table is not updated upon the rule module being enforced, because all 802.11 wireless connections remain connected and active.
  - If an 802.11 wireless connection 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. All traffic to that destination is dropped, even if an alternative route exists over an alternative, non-802.11 wireless connection.
  - Ensure that operational staff are aware that some applications (UDP and TCP-based) may fail if a preferred route exists over a wireless connection on which policy is being enforced.
- Non-802.11 Wireless Interfaces
  - The pre-defined rule module applies to all 802.11 wireless connections, including 802.11 a/b/g/n networks. The pre-defined rule module does not address non-802.11 wireless connections, such as those to 3G networks, but customized rules can be created to do so.
- Alternative Implementation
  - If CSSC is deployed, the simultaneous wired and wireless feature of this client can be leveraged as an alternative means of blocking this threat.

Force VPN When Roaming

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.
  - 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 interface is active and connected, and ICMP pings continue to function, but the connection appears 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.
- Complementary Features
  - If CSSC is deployed, the VPN activation feature of this client can be leveraged to enhance the user experience and facilitate VPN connectivity.

Sample Development of a Customized Rule Module

This section illustrates how a customized rule module can be developed. A customized simultaneous wired and wireless rule module will be used as an example. The customized rule module will:

- Upon simultaneous wired and wireless connections being detected, present a customized user query 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.

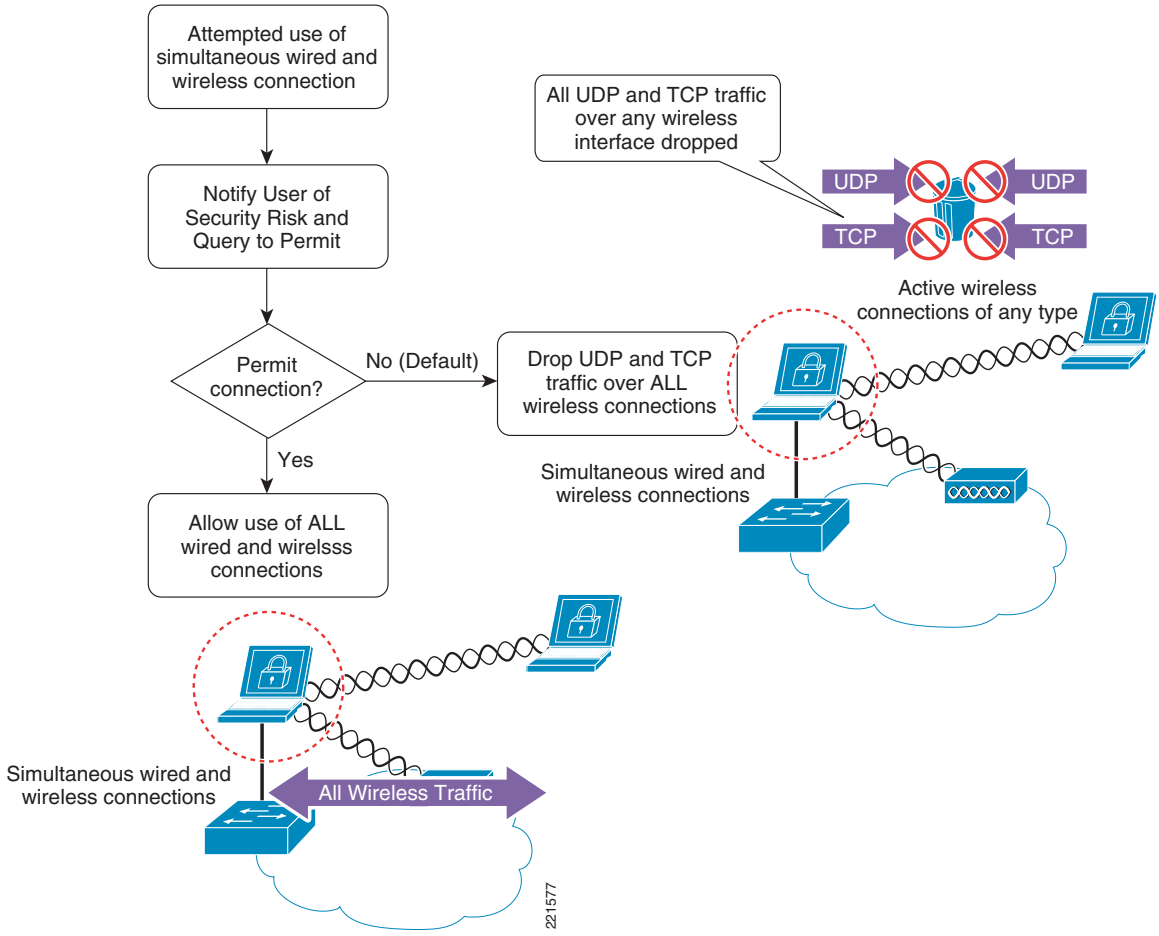
Response caching can be enabled to minimize user disruption.

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

Sample Customized Rule Module Operation

The operation of this customized simultaneous wired and wireless rule module is shown in Figure 7-37.

Figure 7-37 Sample Customized Simultaneous Wired and Wireless Rule Module Operation



Sample customized rule module operation is as follows:

- Upon an attempt to send UDP or TCP traffic over an active 802.11 wireless connection when an Ethernet connection is active, the customized rule module is invoked.
- Traffic on a non-802.11 wireless connection is not affected by this rule module.
- User query is presented, stating the security policy.
- User is presented with the option to permit or deny the action.
- Default action is a deny.
- All UDP and TCP traffic routed over any 802.11 wireless connection is dropped.
- A message is logged.

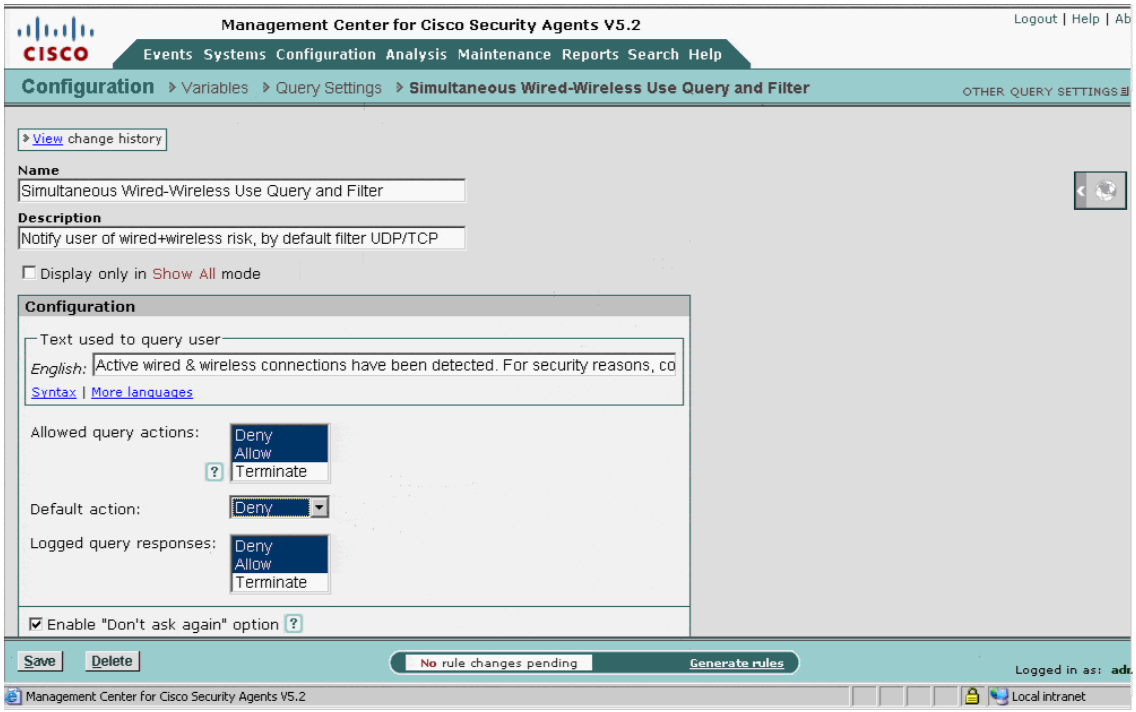
Sample Customized Rule Module Definition

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.

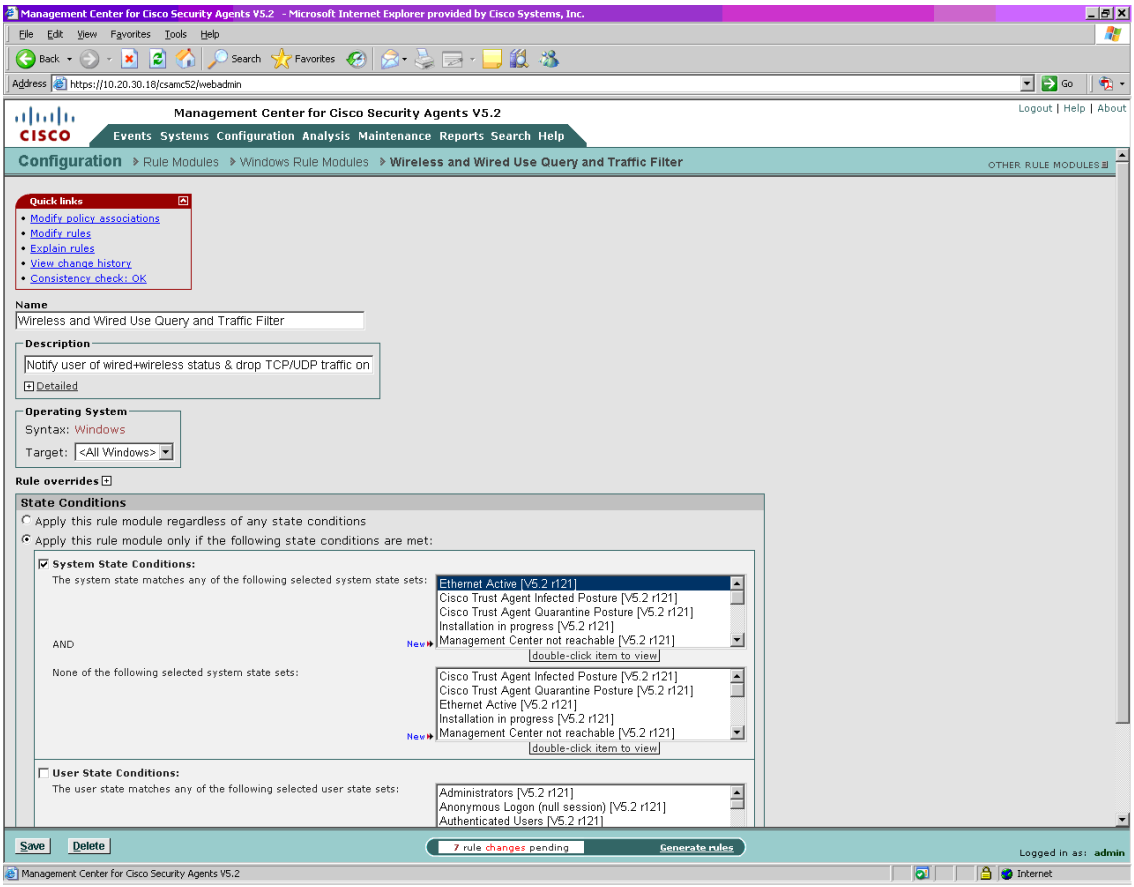
Step 2 Configure the query to present the user with a choice of actions but, by default, enforce a deny action. (See Figure 7-38.)

Figure 7-38 New Query Setting Variable Definition for Sample Customized Simultaneous Wired and Wireless Rule Module



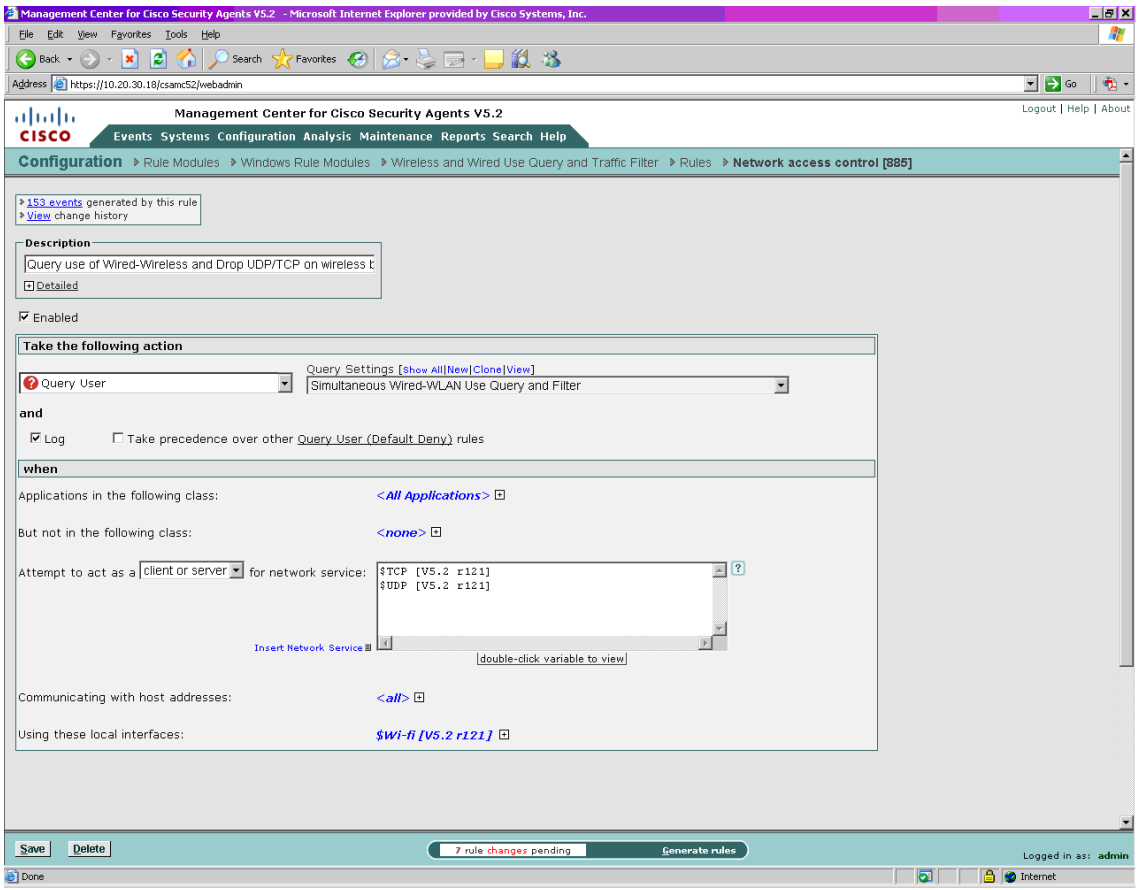
Step 3 Locate the pre-defined simultaneous wired and wireless Windows rule module, clone it, and rename it. (See Figure 7-39.)

Figure 7-39 New Sample Customized Simultaneous Wired and Wireless Rule Module



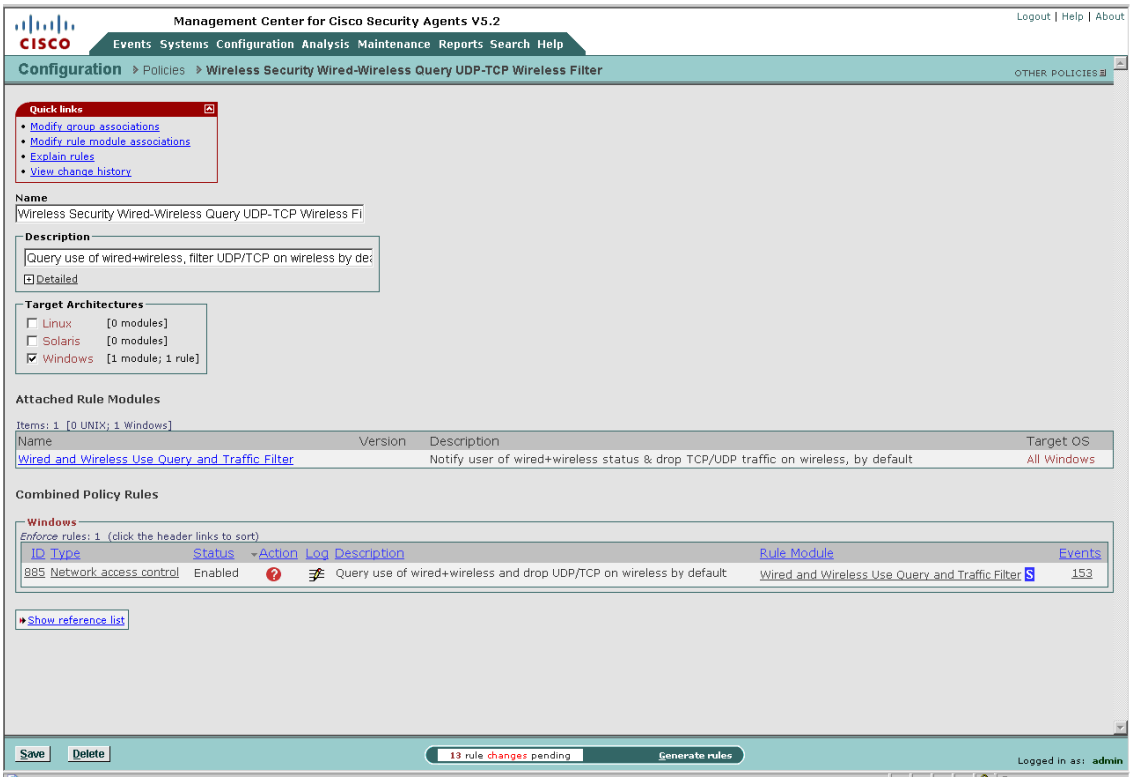
Step 4 Modify the rules associated with this newly customized simultaneous wired and wireless rule module to query the user and apply the new query setting. (See Figure 7-40.)

Figure 7-40 Application of New Query Setting to Sample Customized Simultaneous Wired and Wireless Rule Module



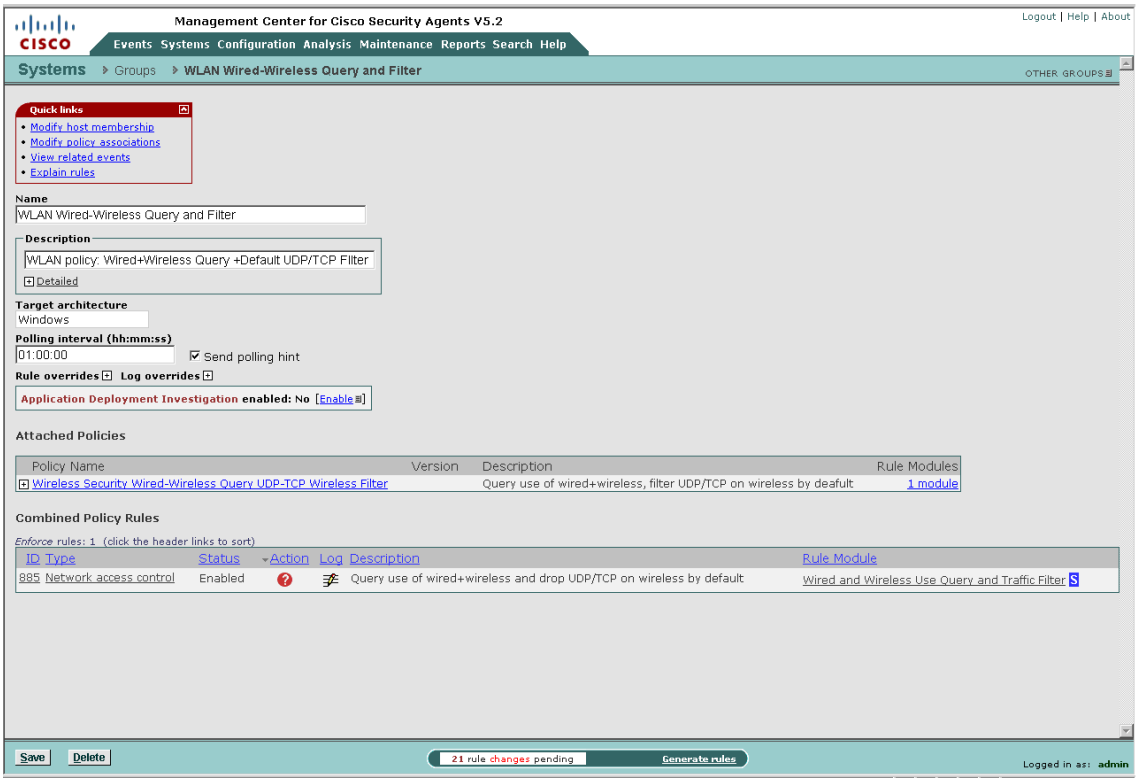
Step 5 Either associate the new rule module with a current policy or create a new policy (See Figure 7-41.)

Figure 7-41 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 7-42.)

Figure 7-42 Association of the Sample Customized Simultaneous Wired and Wireless Policy with a Group

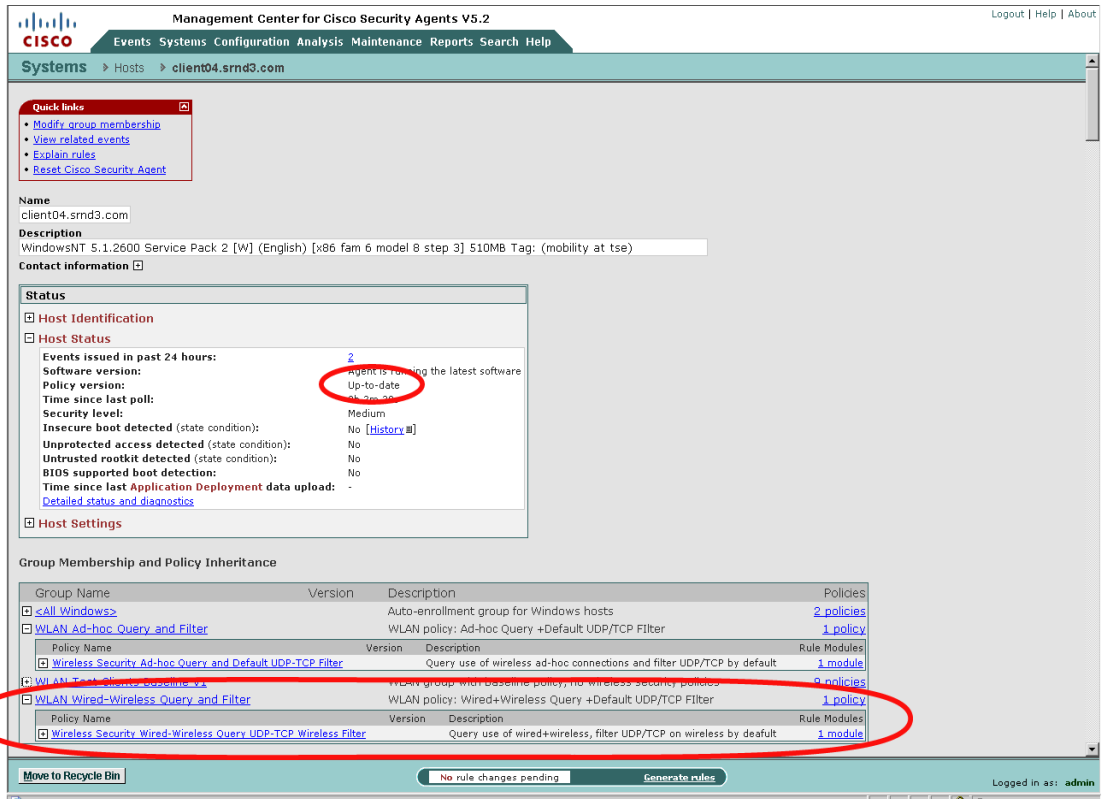


Step 7 If a new group has been created, ensure that host membership is updated to enforce the policy on appropriate hosts.

Step 8 Generate the rules to apply all changes.

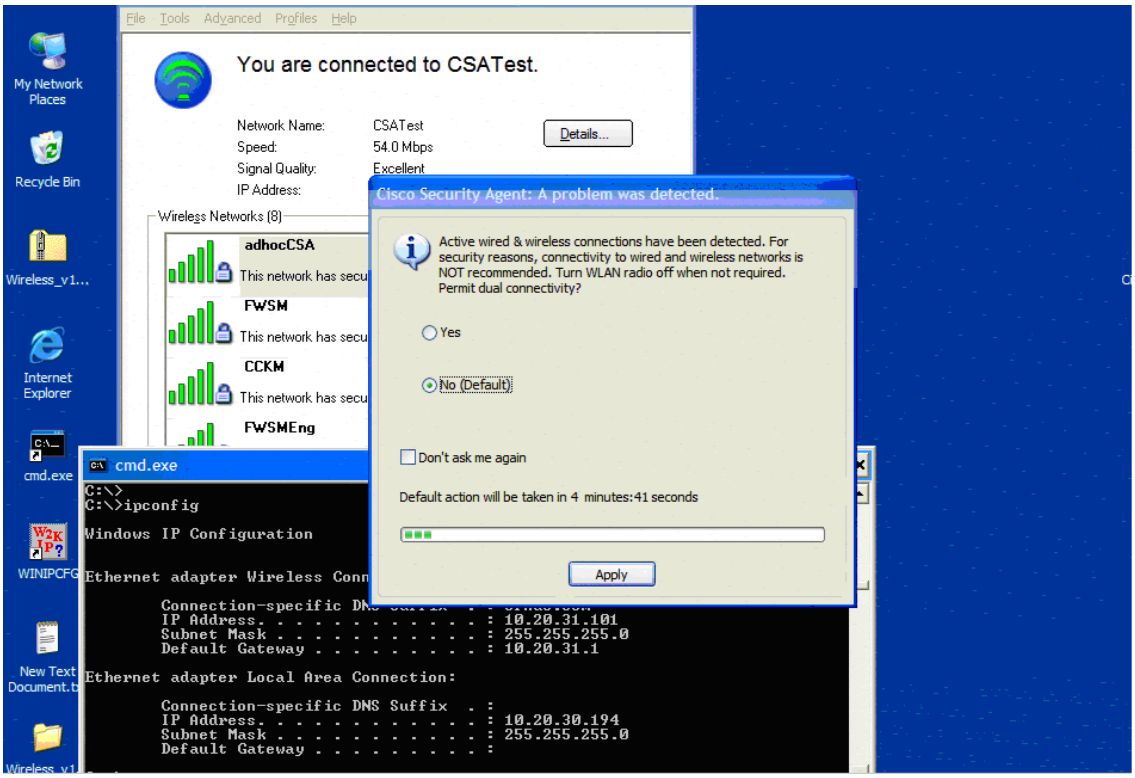
Step 9 Verify that a host is running up-to-date policies before checking operation of the new customized rule module. (See Figure 7-43.)

Figure 7-43 Host Detail Showing Policy Status and Group Membership



Step 10 Attempt to use an 802.11 wireless connection on a host with an active Ethernet connection to check the new customized rule module. (See Figure 7-44.)

Figure 7-44 End User Notification upon Enforcement of Sample Customized Simultaneous Wired and Wireless Rule Module

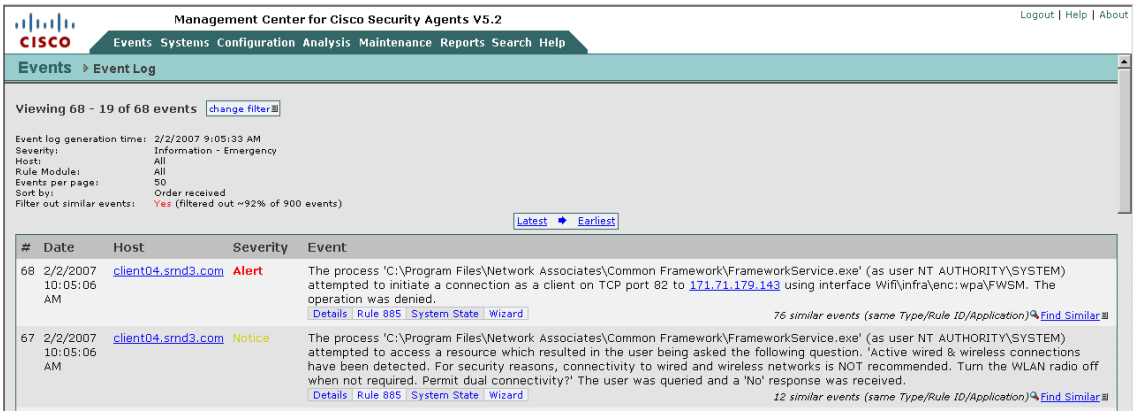


Sample Customized Rule Module Logging

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 7-45.)

Figure 7-45 CSA MC Event Log Generated by Sample Customized Simultaneous Wired and Wireless Rule Module



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 7-3.

Table 7-3 Test Bed Hardware and Software

CSA	Software	V5.2.0.203
	CSA MC Platform	Microsoft Windows 2003 Enterprise Edition Service Pack 1
Mobile Client	Operating system	Microsoft Windows XP Professional Service Pack 2
	Wireless client	CSSC v5.1.0.39
	Wireless adapter	Intel PRO/Wireless 2915ABG Driver Version 9.0.4.26

Reference Documents

Cisco Security Agent (CSA)

- CSA product site

  http://www.cisco.com/go/csa/
- CSA Trusted QoS
  - Implementing Trusted Endpoint Quality of Service Marking

    http://www.cisco.com/application/pdf/en/us/guest/products/ps6786/c1225/ccmigration_09186a00805b6a81.pdf

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

- Rogue AP and Wireless Ad-hoc Monitoring

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808d9330.pdf

CS MARS

- CS MARS User Guides

  http://www.cisco.com/en/US/products/ps6241/products_user_guide_list.html

Wireless Ad-hoc Vulnerability

- 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

- Wi-Fi Planet article "*The Windows Ad-Hoc Exploit*" outlining how the Windows ad-hoc behaviour may be exploited

  http://www.wi-fiplanet.com/news/article.php/3578271