

# Cisco Security Agent Kernel-only Protection Configuration Example

Document ID: 68251

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Obtain Full Administrative Rights**

**Configure**

**Verify**

**Troubleshoot**

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

This document demonstrates how to remediate certain interoperability issues with applications that run along with Cisco Security Agent 4.5. The Cisco Security Agent functions as an effective host intrusion prevention mechanism by monitoring local file systems and system components. Therefore, any malicious system processes are immediately detected and disabled.

Occasionally, an application might appear to not function properly with the Cisco Security Agent installed. The symptoms are that the application does not launch, or the application launches and then suddenly exits. Also, there are no events in the event log and the problem is not resolved when the agent is placed into testmode.

This document explains how to create this exception in order to allow specifically trusted applications to continue to function without compromising the level of security provided by unhooking COM and buffer overflow protection only for these applications.

## Prerequisites

### Requirements

Ensure that you meet this requirement before you attempt this configuration:

- Ensure that you have full administrative access rights to the Cisco Secure Agent MC. This allows you to view all application classes. See the Obtain Full Administrative Rights section of this document for more instruction.

### Components Used

The information in this document is based on Cisco Security Agent 4.5.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

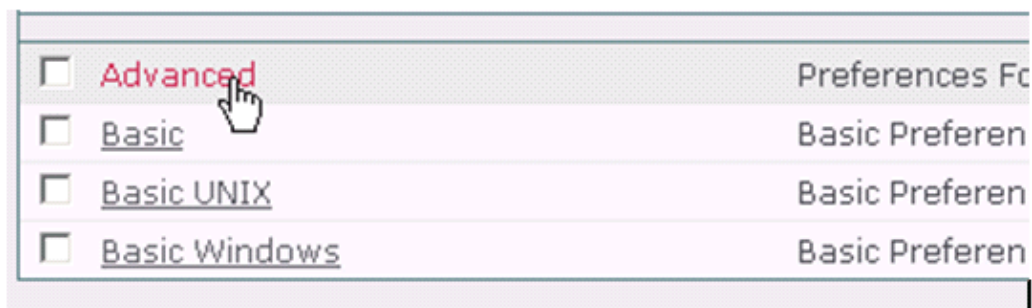
## Obtain Full Administrative Rights

Complete these steps to obtain full administrative rights.

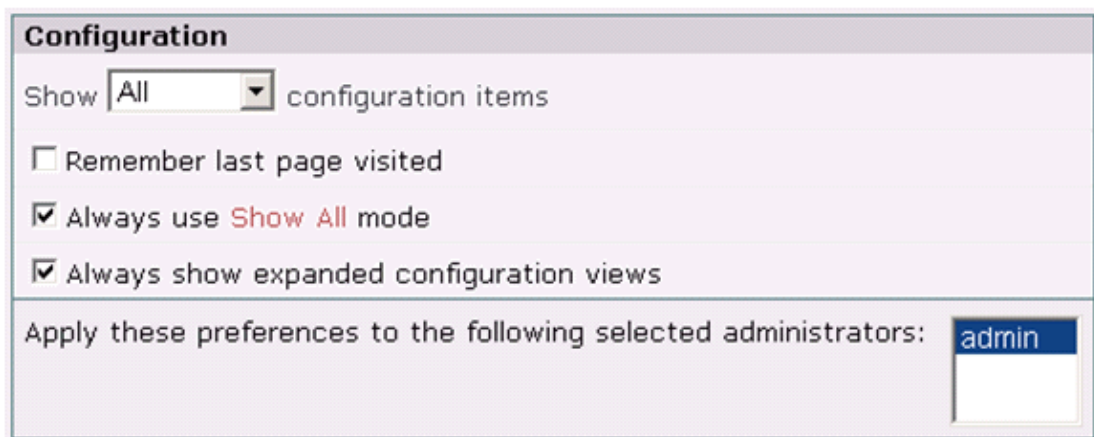
1. Select **Maintenance > Admin Preferences**.



2. Click **Advanced**.



3. Highlight **admin** for Apply these preferences to the following selected administrators.



4. Click **Save**.

## Configure

Complete these steps to configure an exception for a specific application to run alongside Cisco Security Agent.

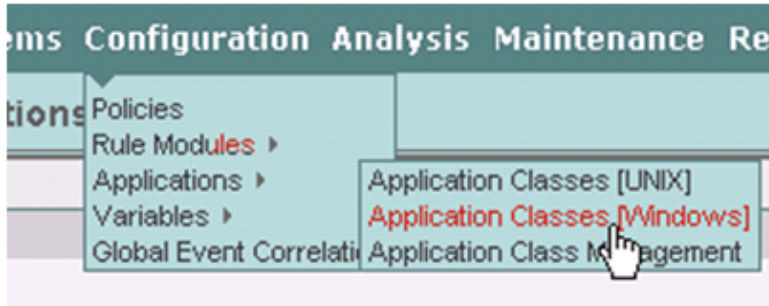
1. Create a new application class.
2. Create a new rule module.

3. Create a new policy.
4. Create a new group.
5. Link the hosts to the new group.
6. Generate rules.
7. Poll for new rules.

### Step 1: Create a New Application Class

Complete these steps:

1. Select **Configuration > Applications > Application Classes [Windows]** on your Cisco Secure Agent MC and click **New**.



2. Specify a name and description for this application class.

This name and description should reflect the application for which you create the exception.

3. Select the Operating System type that the application is to run on and check **Display only in Show All mode**.

4. Leave the default **when created from one of the following executables** radio button selected in order to specify this as a static application class.
5. Specify all the executables that pertain to the application you are running.

**Add process to application class**

when created from one of the following executables:

`**\xyz.exe`

[Insert File Set](#)

[double-click variable to view]

when dynamically defined by policy rules

---

**Remove process from application class**

After  seconds

---

**This application class includes**

Only this process

This process and all its descendents

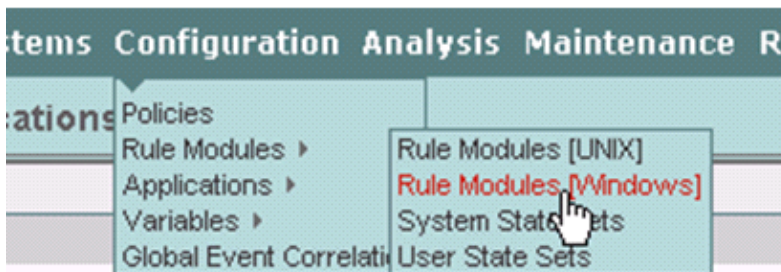
Only descendents of this process

6. Click **Save**.

## Step 2: Create a New Rule Module

Complete these steps:

1. Select **Configuration > Rule Modules > Rule Modules [Windows]** and click **New**.



2. Specify a name and description for this rule module.

**Name**

XYZ Rule Module

---

**Description**

Rule module for creating exception for XYZ executable

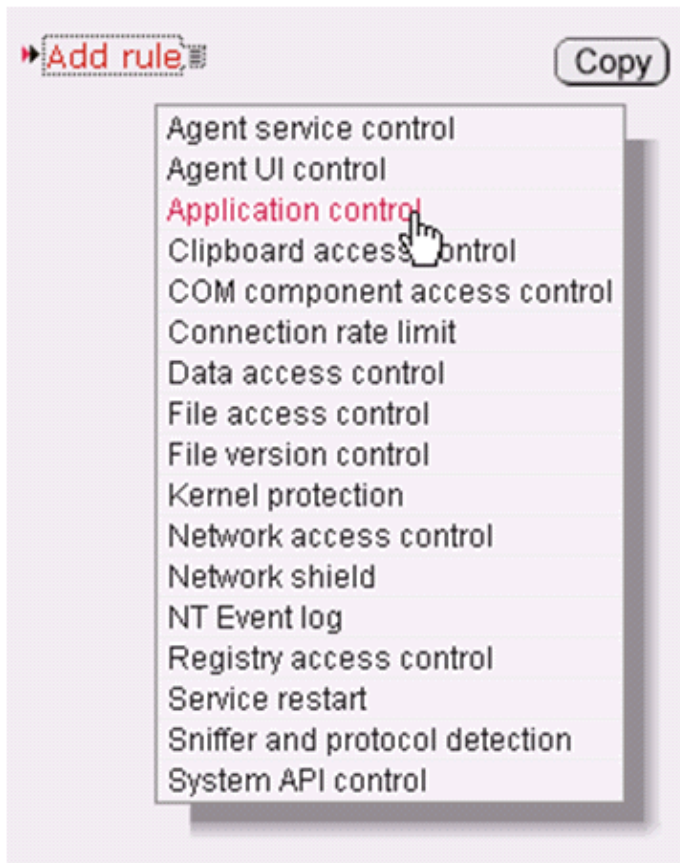
Detailed

3. Leave the rest at the default settings and click **Save**.

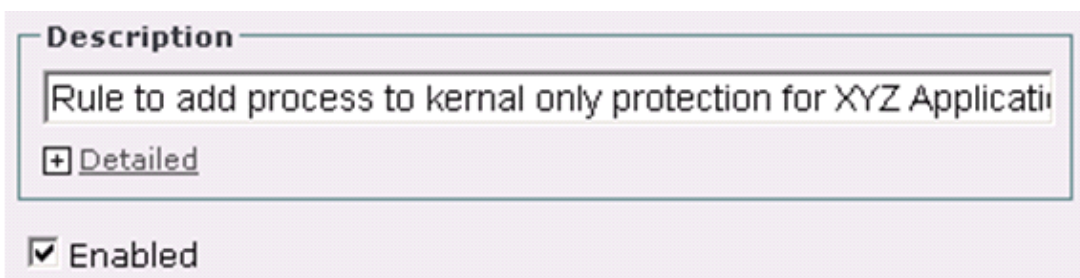
4. Click **Modify rules**.



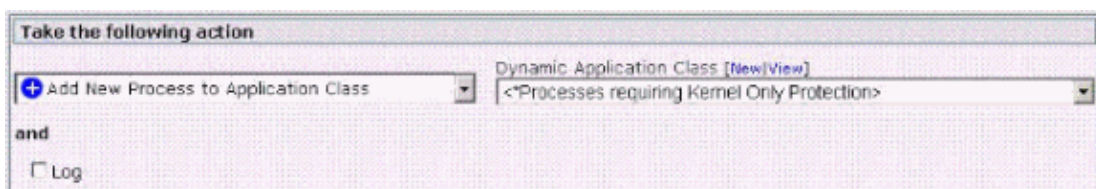
5. Click **Add rule** and select **Application Control**.



6. Specify a name and description for this rule module and check **Enabled**.



7. Add the processes generated to the <Processes requiring Kernel Only Protection> application class.



The applications attempt to run:

**when**

An enforcement action of the following type  Terminate  Deny  Allow occurs

**and**

Current applications in any of the following selected classes:

- <All Applications>
- <\*Authorized rootkit>
- <\*Installation Applications>
- <\*Processes Communicating with Untrusted Hosts>
- <\*Processes Copying Untrusted Content>

But not in any of the following selected classes:

- <none>
- <\*Authorized rootkit>
- <\*Installation Applications>
- <\*Processes Communicating with Untrusted Hosts>
- <\*Processes Copying Untrusted Content>

**attempt to run**

New applications in any of the following selected classes:

- XYZ Application
- User Invoked applications
- User Invoked applications [V4.5 r565]
- Virus scanner - all applications (McAfee) [V4.5 r565]
- Virus scanner - all applications (Norton) [V4.5 r565]

But not in any of the following selected classes:

- <none>
- <\*Authorized rootkit>
- <\*Installation Applications>
- <\*Processes Communicating with Untrusted Hosts>
- <\*Processes Copying Untrusted Content>

8. Click **Save**.

### Step 3: Create a New Policy

Complete these steps:

1. Select **Configuration > Policies** and click **New**.
2. Specify a name and description for this policy.

**Name**

XYZ Policy

**Description**

Policy for XYZ exception

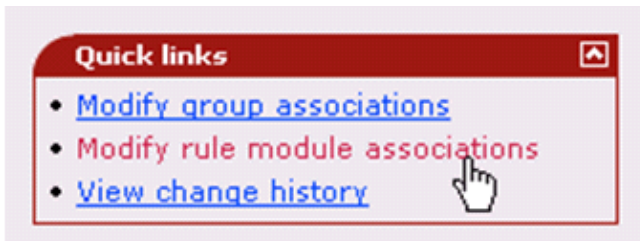
Detailed

3. Select **Windows** as the Target Architecture.

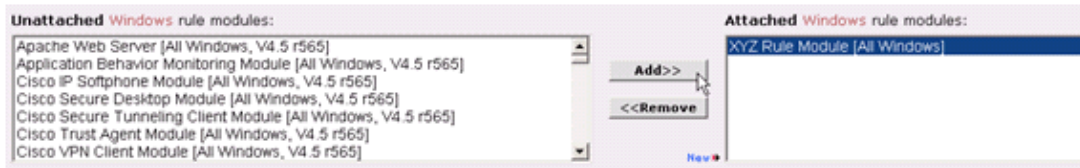
**Target Architectures**

<input type="checkbox"/>	Linux	[0 modules]
<input type="checkbox"/>	Solaris	[0 modules]
<input checked="" type="checkbox"/>	Windows	[0 modules]

4. Click **Save**.
5. Click **Modify rule module associations**.



6. On the window on the left hand side, locate the new rule module you just created and click **Add** to populate the right hand window.



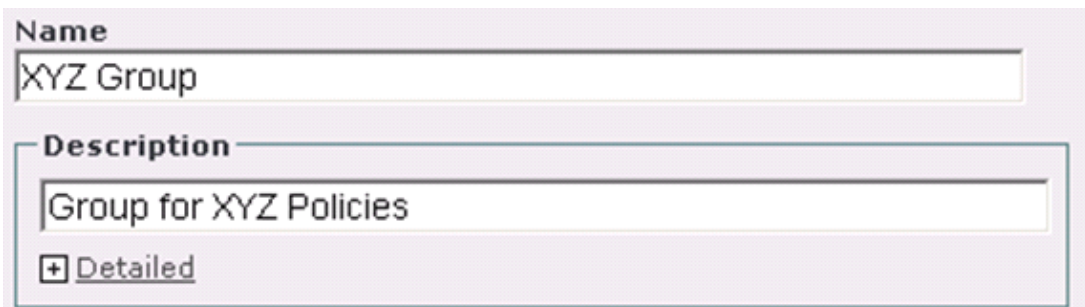
#### Step 4: Create a New Group

Complete these steps:

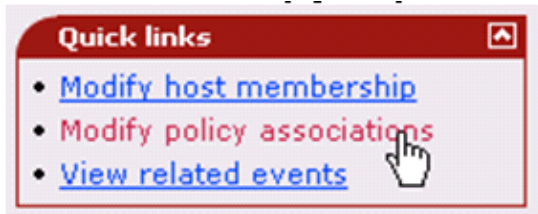
1. Select **Systems > Groups** and click **New**.
2. Select **Windows** as your Target Architecture.



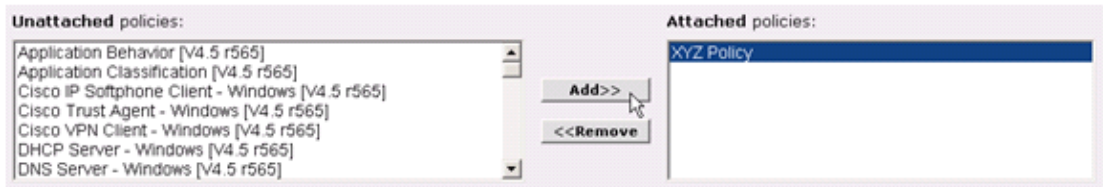
3. Specify a name and description for this group.



4. Leave the rest of the configuration at the default values.
5. Click **Save**.
6. Click **Modify policy associations**.



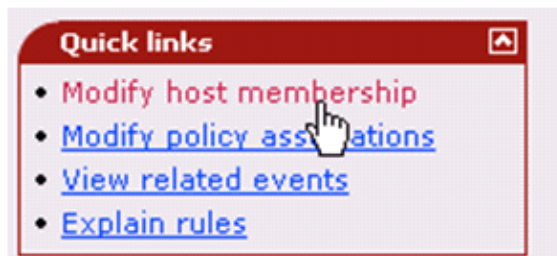
7. On the window on the left hand side, locate the new policy you created and click **Add** to populate the right hand window.



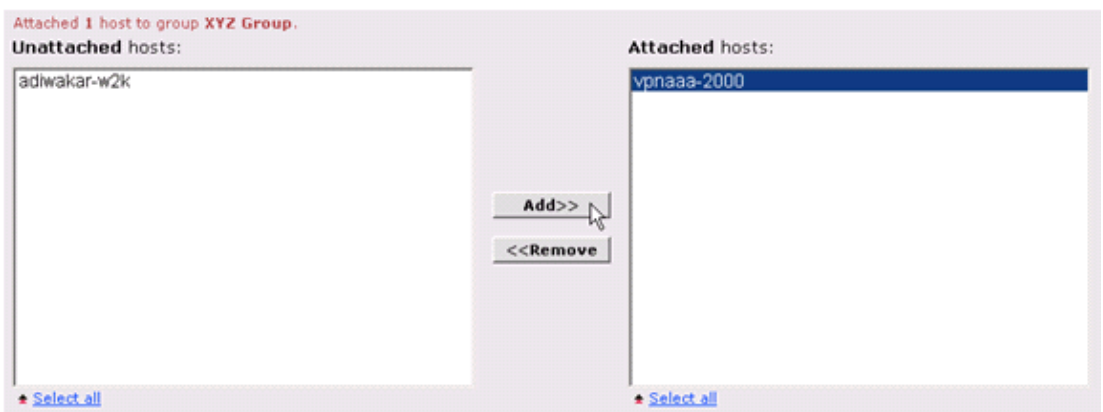
### Step 5: Link the Hosts to a New Group

Complete these steps:

1. Select **Systems > Groups** and locate the group you created under the set of Windows groups.
2. Click **Modify host membership**.



3. On the window on the left hand side, locate any hosts that are running the application for which you are creating the kernel exception and click **Add** to populate the right hand window. Optionally, you can do a Bulk transfer to facilitate the addition of your host membership to this group.



### Step 6: Generate Rules

Complete these steps:

1. Click **Generate Rules**.
2. Click **Generate**.

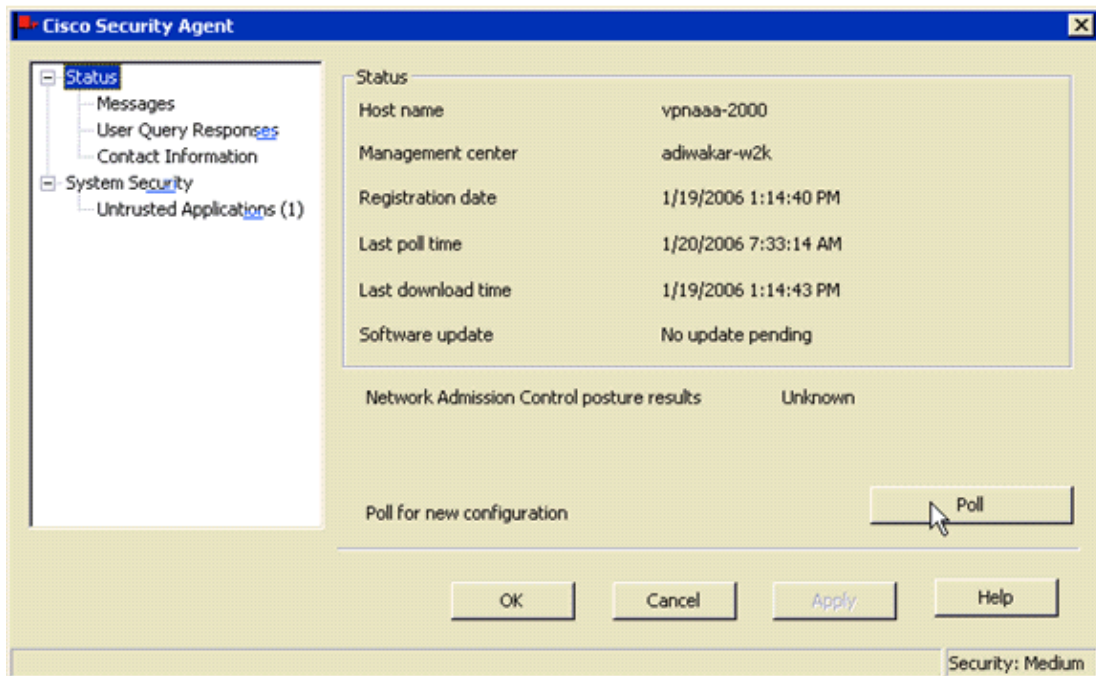
## Step 7: Poll for New Rules

Complete these steps:

1. Access the physical machine from which you are running the application for upon completion of the rule generation.

In this example, go to the machine which has trouble running XYZ.exe.

2. Double click on the Cisco Security Agent flag located in your system tray, or select **Start > Programs > Cisco Security Agent > Cisco Security Agent**.
3. Highlight **Status** in the navigation tree in the left hand panel and click **Poll**.
4. Verify that the last poll time is properly updated.



## Verify

Invoke the application. It should now run concurrently with the Cisco Security Agent.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General

## Related Information

- **Cisco Security Agent Product Support**
  - **Technical Support & Documentation – Cisco Systems**
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 26, 2006

Document ID: 68251

---