

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Microsoft Windows Legacy

Last Modified: Friday, September 8, 2017

### Event Source Product Information:

**Vendor:** [Microsoft](#)

**Event Source:** Windows

**Versions:** Microsoft Windows Server versions 2003 and earlier

### RSA Product Information::

**Supported On:** NetWitness Suite 10.0 and later

**Collection Method:** Windows Legacy

**Event Source Log Parser:** winevent\_nic

**Event Source Class.Subclass:** Host.Windows

The RSA NetWitness Suite Legacy Windows collection collects event data from multiple Windows Event Source domains.

It supports collection from:

- Windows 2003 and earlier event sources
- NetApp ONTAP host evt files

You must complete these tasks to configure Windows Legacy collection:

- I. [Create a Non-Admin Domain User for Each Domain](#)
- II. [Configure Legacy Collection on RSA NetWitness Suite](#)

**Prerequisite:**

Before configuring a Windows Legacy event source, you must install the RSA NetWitness<sup>®</sup> Suite Legacy Windows Collector. Search the [RSA Link NetWitness Suite](#) space for "Legacy Windows Collection Update" and select the version that corresponds to your NetWitness version.

## Create a Non-Admin Domain User for Each Domain

---

This section provides an overview of the end-to-end sequential configuration procedure for the Windows Legacy Collection protocol with a checklist that contains each configuration step.

### Context

Configuration steps for the Windows Legacy collection protocol must occur in the specific sequence listed in the table below.

### Create Non-Admin Domain User Checklist

**Note:** The steps in this list are in the order in which you must complete them.

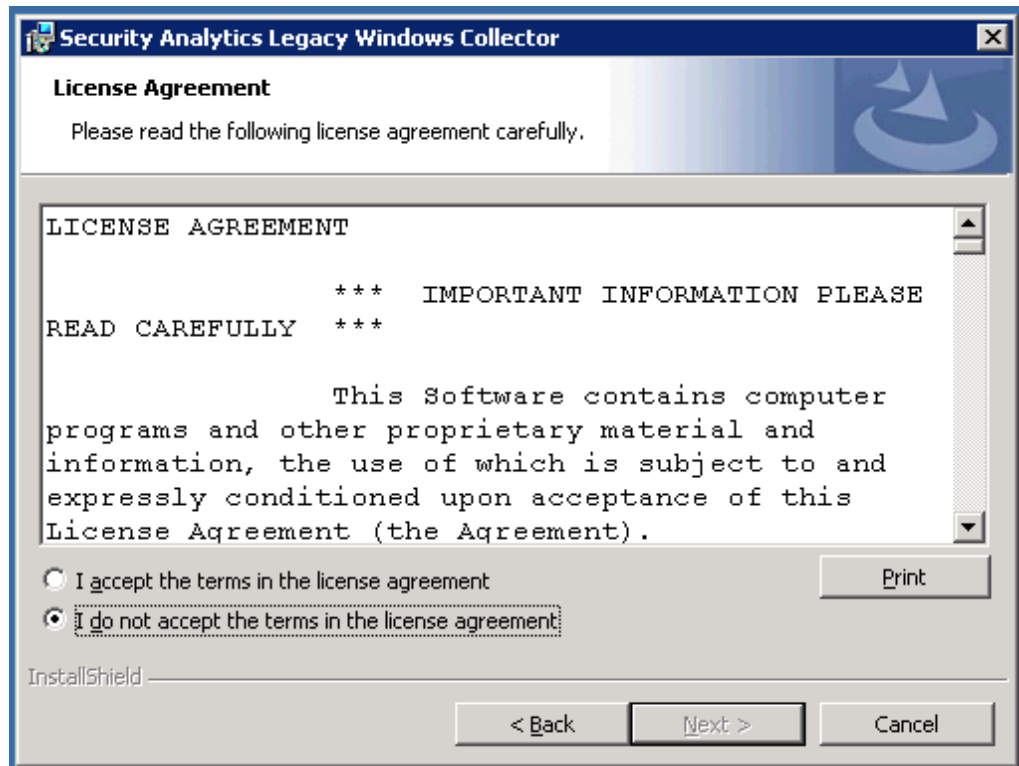
Step	Description
1	<a href="#">Step 1 - Create a Non-Admin Domain User</a> (for example, <b>sauser</b> ) on the domain controller for each domain.
2	<a href="#">Step 2 - Set Event Log Security</a> on the domain controller for each domain.
3	<a href="#">Step 3 - (Conditional) Disable Remote Registry Access Method</a>

**Note:** In the local Security policy on a Windows 2000 event source, you must assign the **Manage auditing and security log user** right that gives a non admin user access to the **Event log**.

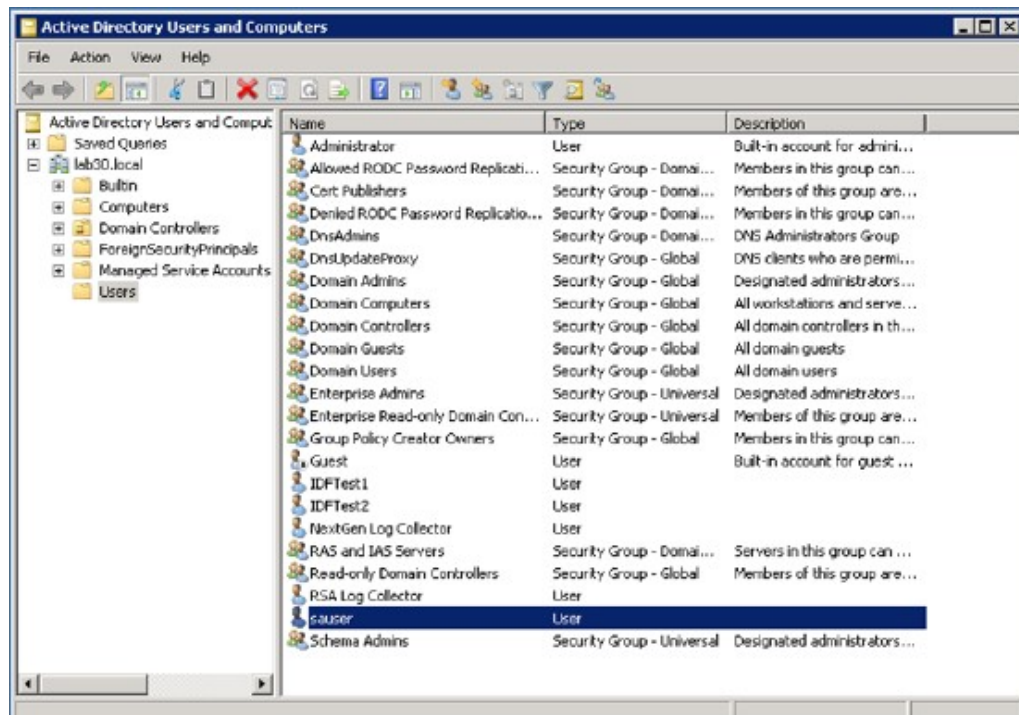
### Step 1 - Create a Non-Admin Domain User

To create the RSA NetWitness® Suite domain user (for example, **sauser**) on the domain controller for each domain:

1. Log on to the domain controller.



2. Create a non-admin domain user (for example, sauser).



3. Add the new user to the remote desktop user groups.

## Step 2 - Set Event Log Security

This section tells you how to set event log security on the domain controller for a domain.

### To set event log security on the domain controller for a domain:

1. Log on the Domain Controller.
2. Use a text editor such as Notepad to open the **Sceregl.inf** in the **%Windir%\Inf** folder.

3. Add the following lines to the [Register Registry Values] section:

```
MACHINE\System\CurrentControlSet\Services\Eventlog\Application\
CustomSD,1,%AppCustomSD%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\
Security\CustomSD,1,%SecCustomSD%,2
MACHINE\System\CurrentControlSet\Services\
Eventlog\System\CustomSD,1,%SysCustomSD%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\Directory
Service\CustomSD,1,%DSCustomSD%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\DNS
Server\CustomSD,1,%DNSCustomSD%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\File
Replication Service\ CustomSD,1,%FRSCustomSD%,2
```

4. Add the following lines to the [Strings] section:

```
AppCustomSD="Eventlog: Security descriptor for Application event
log" SecCustomSD="Eventlog: Security descriptor for Security
event log" SysCustomSD="Eventlog: Security descriptor for System
event log"
DSCustomSD="Eventlog: Security descriptor for Directory Service
event log" DNSCustomSD="Eventlog: Security descriptor for DNS
Server event log" FRSCustomSD="Eventlog: Security descriptor for
File Replication Service event log"
```

5. Save the changes you made to the **Sceregl.inf** file, and run the **regsvr32 scecli.dll** command.
6. Click **Start > Administrator Tools > Group Policy Management** and complete the following steps:
  - a. Expand the **Domains** tree, right click on the domain, and select the **Create a GPO in this domain, and link it here** option.

- b. Specify a name for the GPO policy and click **OK**.
  - c. Select the newly created GPO policy.
  - d. Select the domain in the right panel, right click, and select **Enforce**.
  - e. Under **Security Filtering**, click **Add**.
  - f. Under **Select User, Computer and Group**, type **Domain Computers**, click **Check Names**, and click **OK**.
7. Right-click on the newly created GPO policy and click Edit.
  8. Double-click the following branches to expand them:
    - Computer Configuration
    - Windows Settings
    - Security Settings
    - Local Policies
    - Security Options
  9. Find the new **Eventlog** settings in the right panel.



The screenshot shows a list of Group Policy Objects (GPOs) in the right-hand pane of the Group Policy Object Editor. The list includes various security settings, with several Eventlog security descriptors highlighted in yellow. The highlighted items are:

Eventlog: Security descriptor for Application event log	Not Defined
Eventlog: Security descriptor for Directory Service event log	Not Defined
Eventlog: Security descriptor for DNS Server event log	Not Defined
Eventlog: Security descriptor for File Replication Service event log	Not Defined
Eventlog: Security descriptor for Security event log	Not Defined
Eventlog: Security descriptor for System event log	Not Defined

10. In right panel, double-click Event log: Security descriptor for Application event log and add SDDL string.

**Note:** Note: In the following steps, the **SID** (for example, S-1-5-21-3244245077-2111152846-3233386924-1114) is the SID for a particular non-admin domain user (for example, **sauser**). If you need to retrieve the SID, see [Retrieve the SID](#) below.

Depending on whether the security policy Settings box is empty or not, do one of the following:

- **Box is not empty:** append the following string to the value in the box: (A;; 0x1;;;SID).

For example:

```
(A;; 0x1;;;S-1-5-21-3244245077-2111152846-3233386924-1114)
```

- **Box is empty:** insert the following string in the box:

```
O:BAG:SYD: (D;;0xf0007;;;AN) (D;;0xf0007;;;BG) (A;;0xf0007;;;SY) (A;;0x7;;;BA) (A;;0x7;;;SO) (A;;0x3;;;IU) (A; 0x1;;;SID)
```

For example:

```
O:BAG:SYD: (D;;0xf0007;;;AN) (D;;0xf0007;;;BG) (A;;0xf0007;;;SY) (A;;0x7;;;BA) (A;;0x7;;;SO) (A;;0x3;;;IU) (A; 0x1;;;S-1-5-21-3244245077-2111152846-3233386924-1114)
```

11. Repeat step 9 and 10 for **Event log: Security descriptor for Security event log** and **Event log: Security descriptor for System event log**.

## Retrieve the SID

### To retrieve the SID:

1. run the following command in PowerShell. Make sure that you change the user name accordingly (for example, change the user name to **sauser**).

```
([System.Security.Principal.NTAccount]'sauser').translate ([system.security.principal.securityidentifier]) | Format-List
```

2. Copy value field:

```
BinaryLength: 28
AccountDomainSid : S-1-5-21-3244245077-2111152846-3233386924
Value: S-1-5-21-3244245077-2111152846-3233386924-1114
```

## Step 3 - (Conditional) Disable Remote Registry Access Method

The Remote Registry Access Method is enabled by default when you set up a Legacy Windows event source in RSA NetWitness® Suite. If you want to disable this method, you must uncheck the **Use Remote Registry Initialization** parameter.

For details on completing this procedure, see the "Configure Remote Registry Access" topic in the *Windows Legacy and NetApp Collection Configuration Guide* in the RSA NetWitness® Suite help.

### To disable the Remote Registry Access Method:

1. Uncheck the **Use Remote Registry Initialization** parameter.
2. Add the RSA NetWitness® Suite user (for example, **sauser**) to the WMI and DCOMCNFG management on each Windows 2003 or earlier event source.
3. Add the Local Security Policy on each Windows 2000 event source.

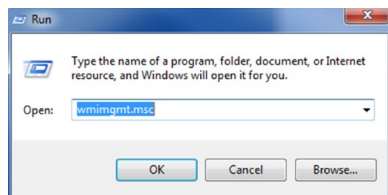
You need to add non-admin domain user to WMI and DCOMCNFG on each Legacy Event Source. See the appropriate section, depending on the version of your event source:

- [Add Non-Admin Domain User on Windows 2003 Event Source](#)
- [Add Non-Admin Domain User on Windows 2000 Event Source](#)

### Add Non-Admin Domain User on Windows 2003 Event Source

#### To add the RSA NetWitness® Suite user to the WMI and DCOMCNFG management on each Windows 2003 event source:

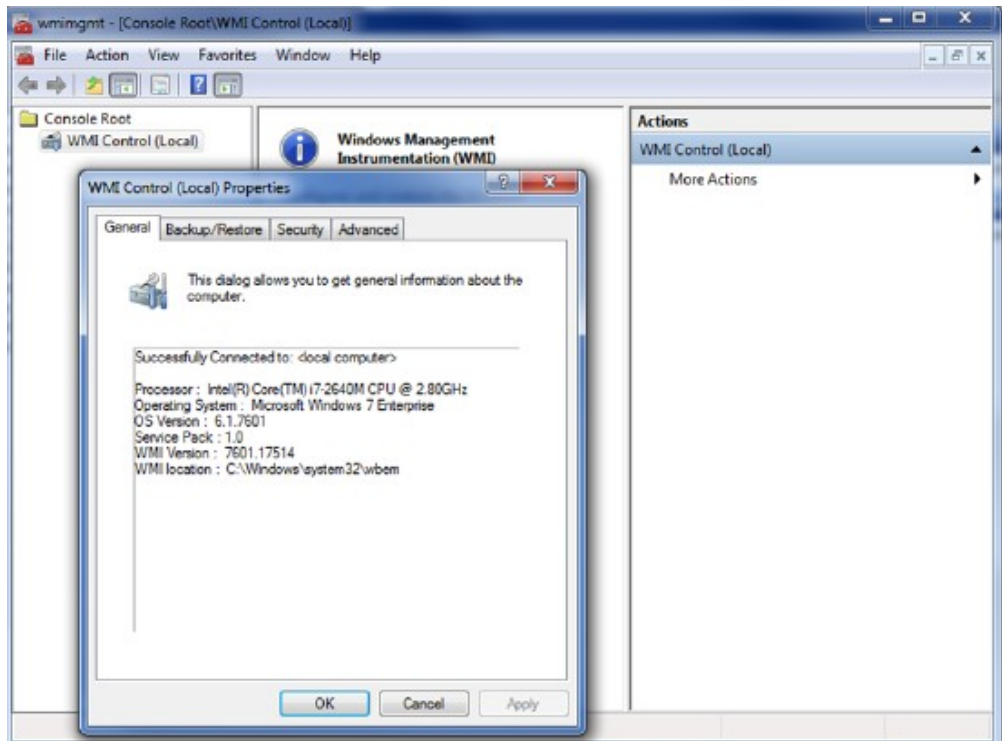
1. Log on the event source.
2. Run **wmimgmt.msc**.




3. Add the RSA NetWitness® Suite user under **wmi\root\CIMV2** security option.

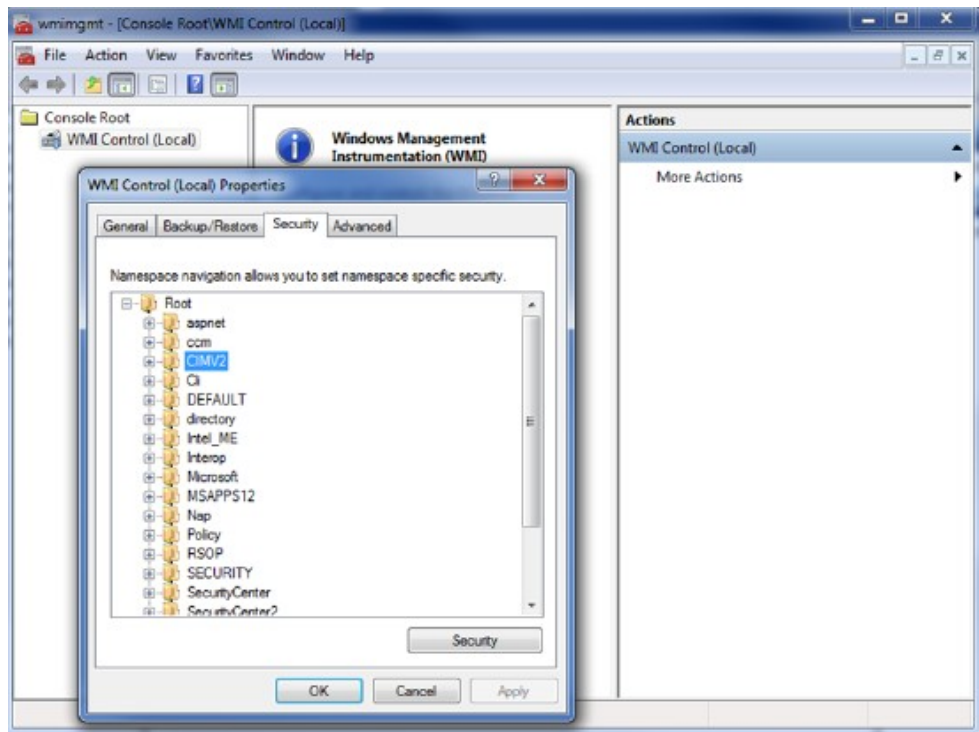


- a. Right-click WMI Control and click Properties.

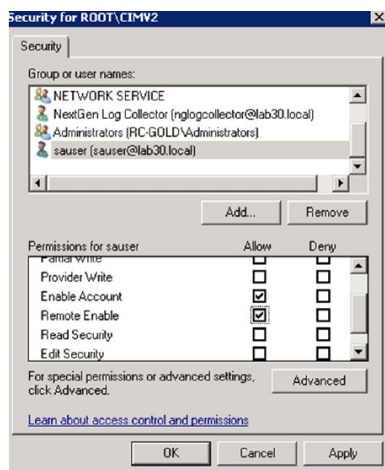
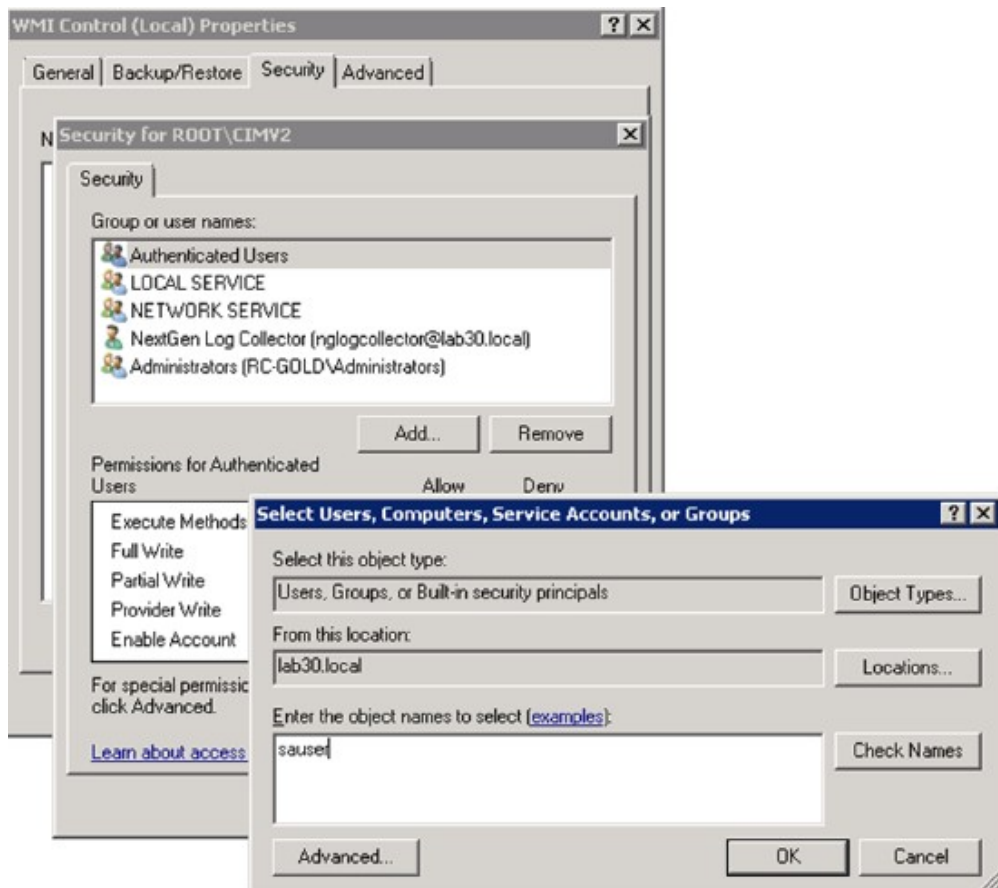


- b. Click Security tab and click on **Root\CIMV2**.

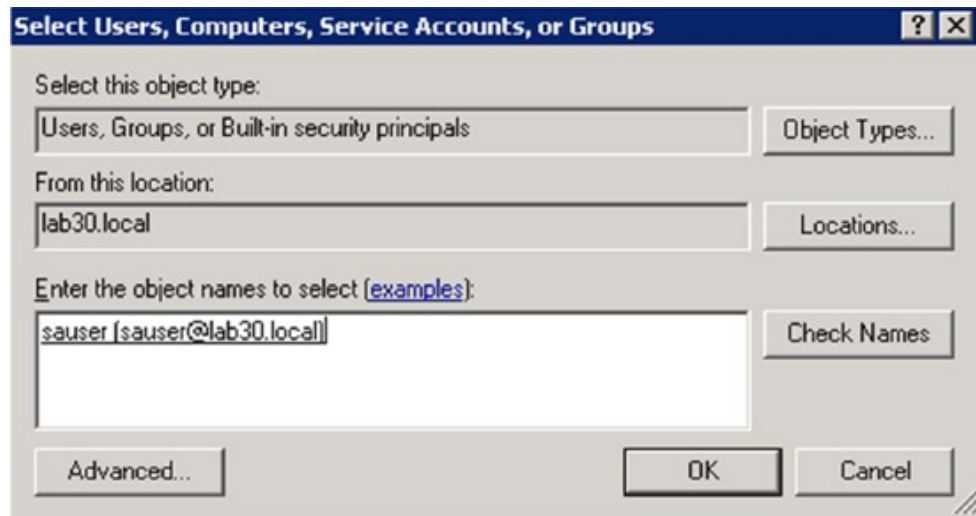
- c. Click .



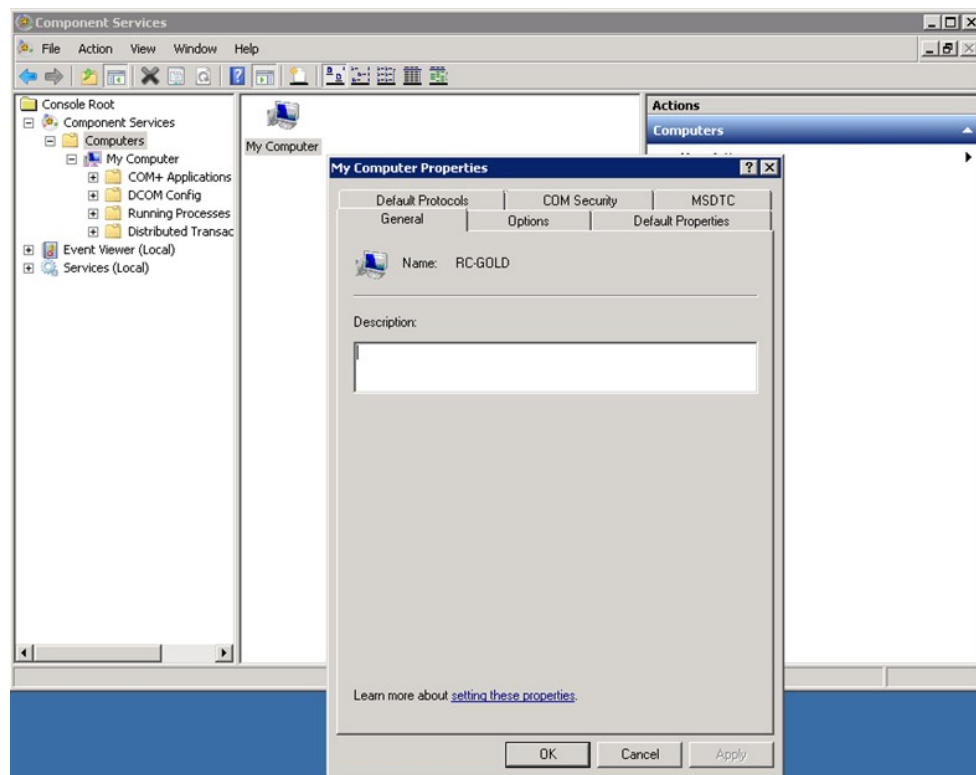
- d. In the Group or user names section, click Add... to create a user.
- e. Select the Enable Account and Remote Enable permissions for that user.
- f. Enter the user (for example, **sauser**).



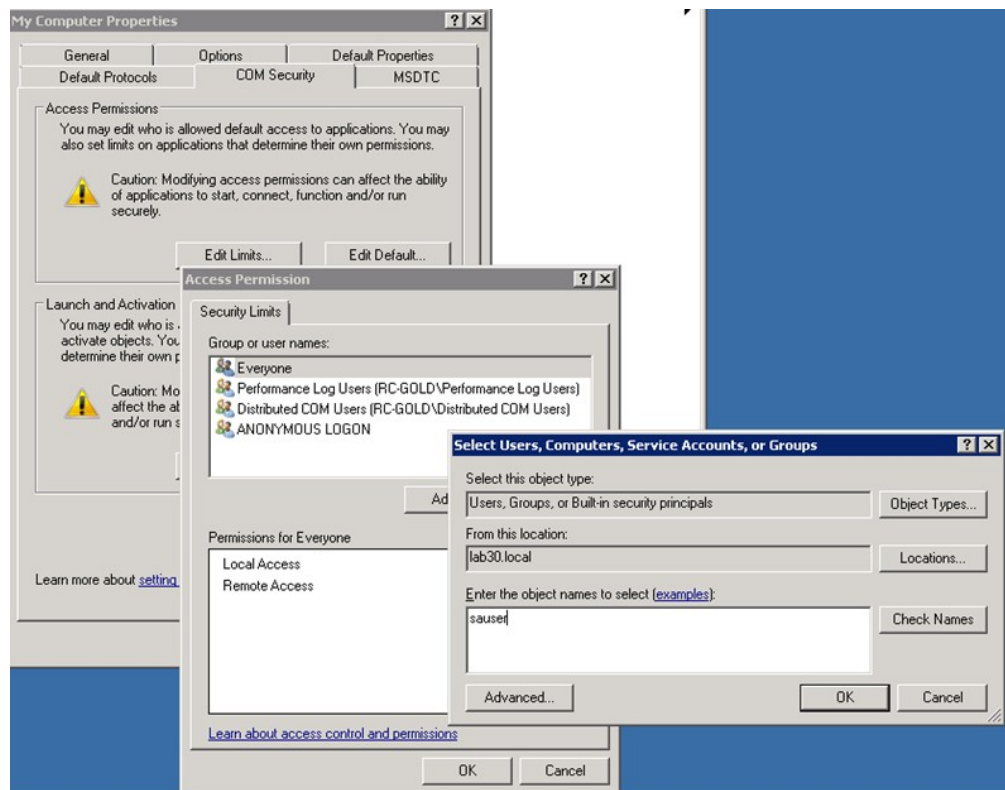
- g. Click Check Names to verify that the new user was added correctly.



- h. Click **Apply**, **OK**, and **OK**.
4. Add a user under **DCOMCNFG**:
  - a. Run **dcomcnfg**.
  - b. Click **Root > Component Services > Computers > My Computer**.
  - c. Right click **My Computer** and click **properties**.



5. Under **Access Permissions**:
  - a. Click **Edit Limits**.
  - b. Add the RSA NetWitness Suite user (for example, **sauser**).
  - c. Enable the **Local Access** and **Remote Access** permissions.
  - d. Click **OK**.
6. Under **Launch and Access Permissions**:
  - a. Click **Edit Limits**.
  - b. Add the RSA NetWitness Suite user (for example, **sauser**).
  - c. Enable **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** permissions.
  - d. Click **OK** and click **OK** again to close the properties box.



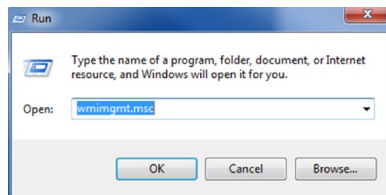
### Add Non-Admin Domain User on Windows 2000 Event Source

For Windows 2000 Event Sources, you need to perform the following procedures:

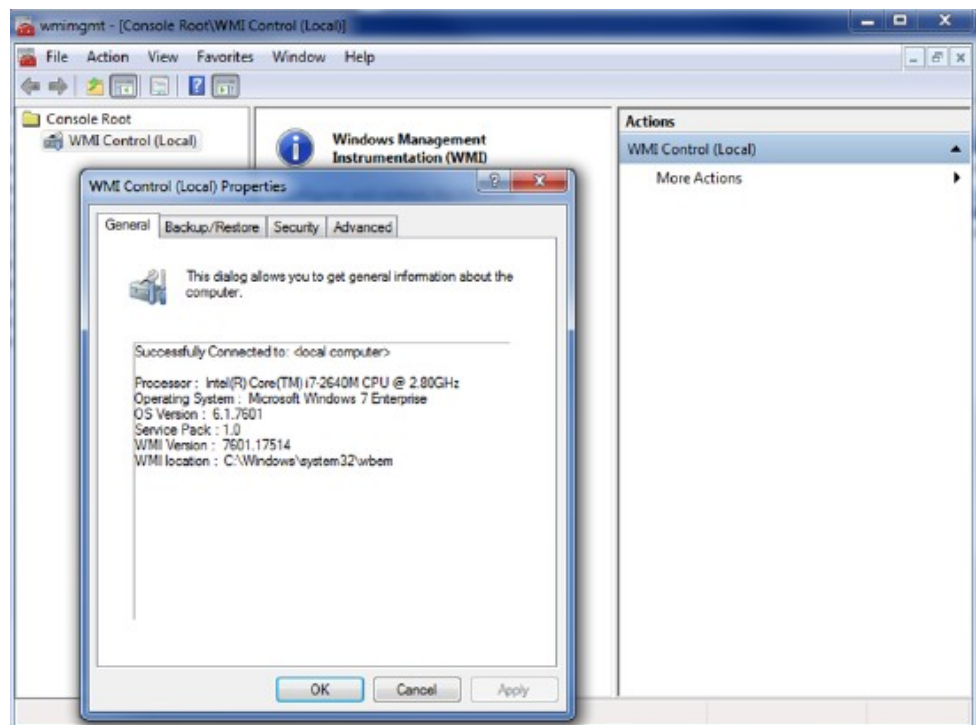
- I. Add the **sauser** to WMI and DCOMCNFG Management
- II. Add Local Security Policy

**To add the RSA NetWitness® Suite user to the WMI and DCOMCNFG management on each Windows 2000 event source:**

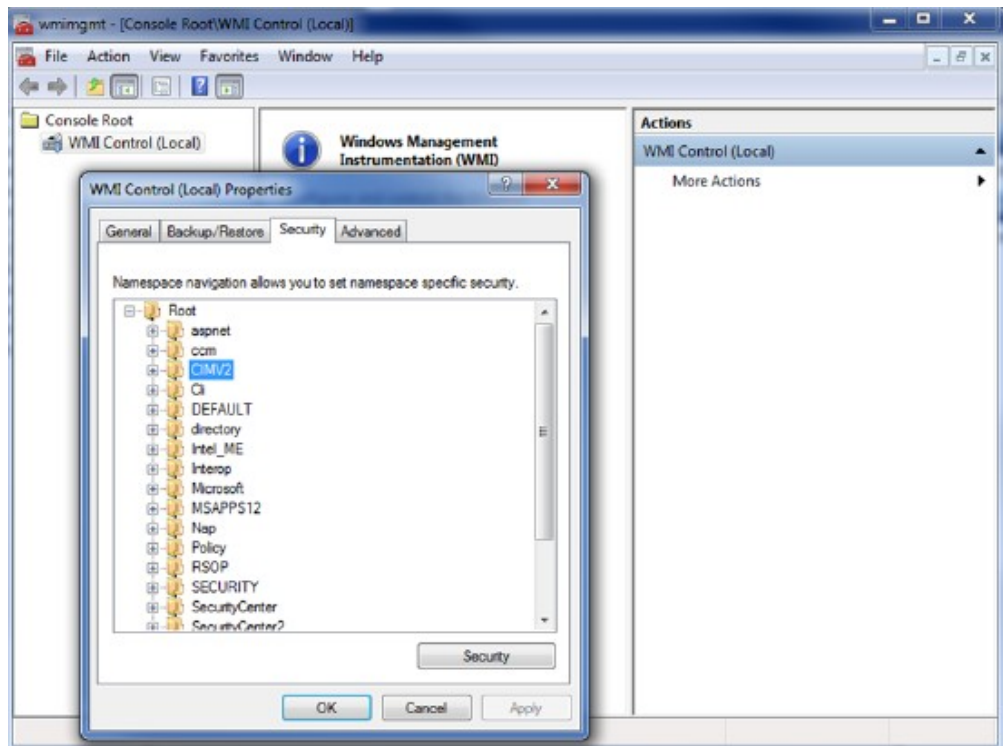
1. Log on to the event source.
2. Run **wmimgmt.msc**.



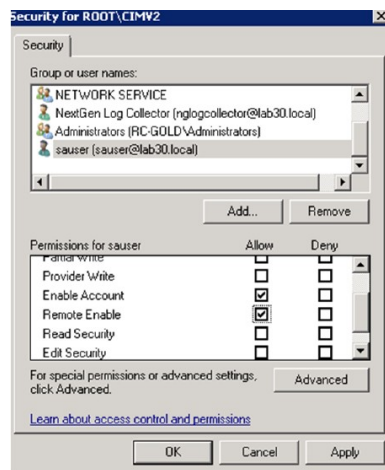
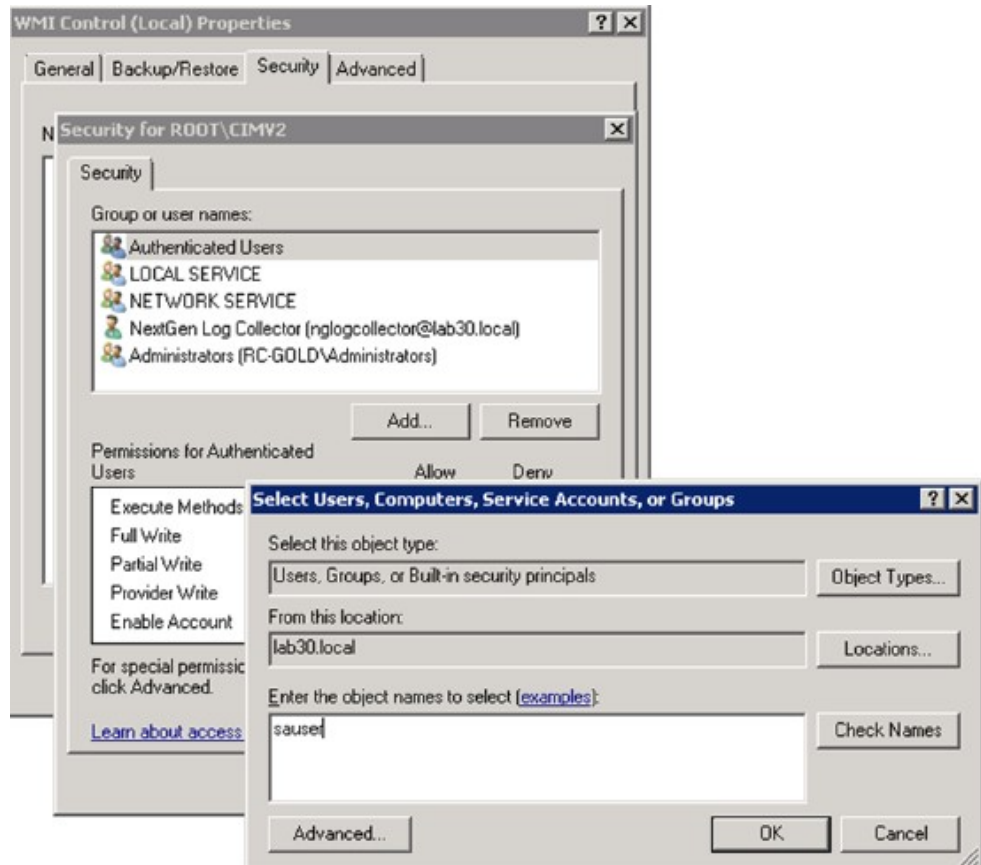
3. Add the RSA NetWitness Suite user under **wmi \root\CIMV2** security option.
  - a. Right click **WMI Control** and click **Properties**.



- b. Select the **Security** tab and click **Root\CIMV2**.
- c. Click .

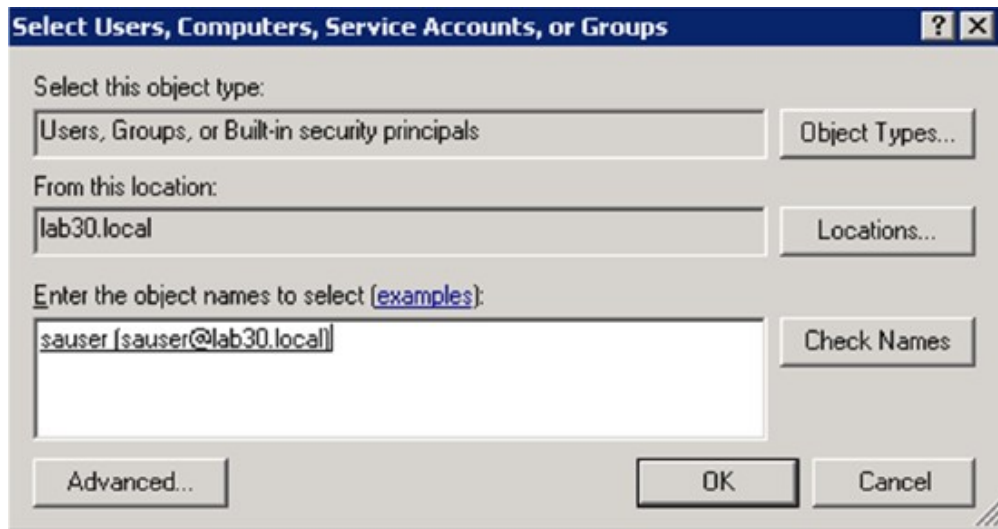


- d. In the **Group or user names** section, click **Add...** to create a user.
- e. Select the **Enable Account** and **Remote Enable** permissions for that user.
- f. Enter the user (for example, **sauser**).

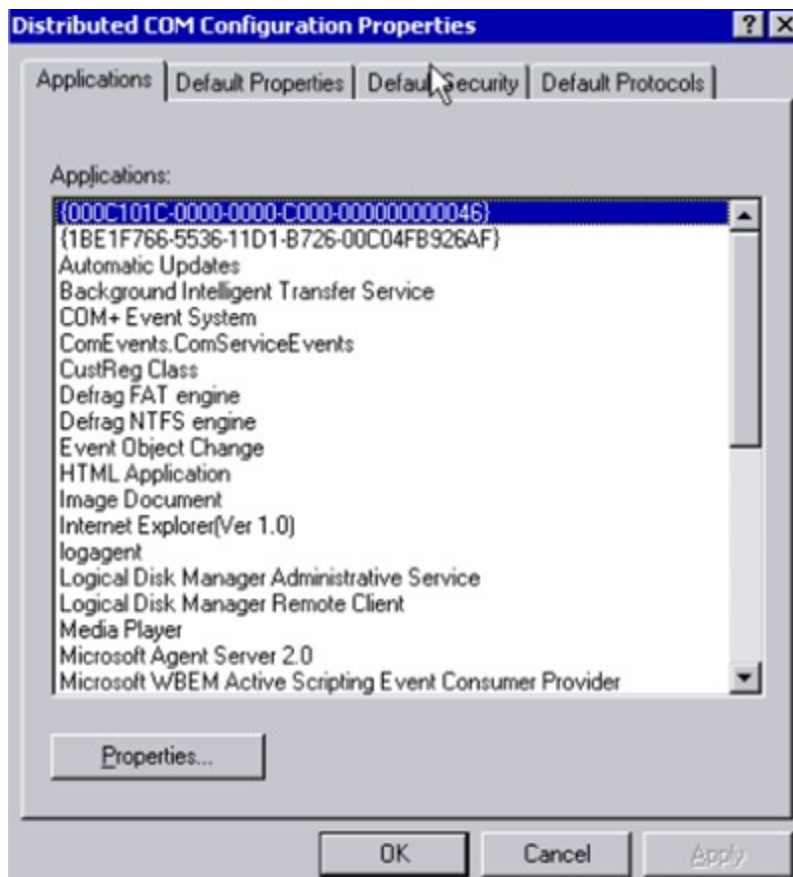


- g. Click **Check Names** to verify that the new user was added correctly.





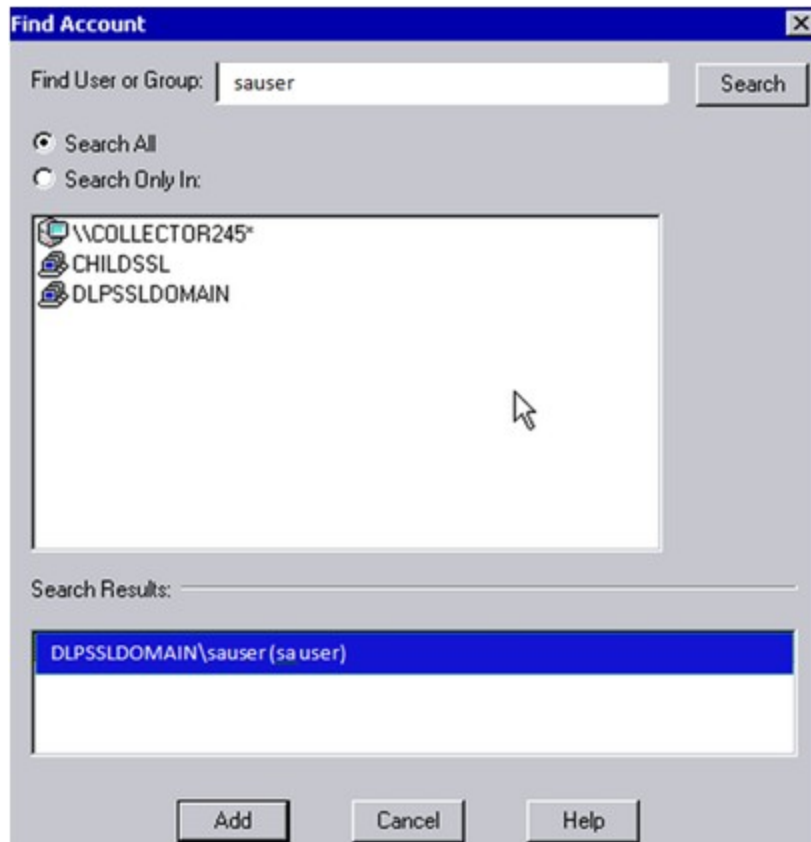
- h. Click **Apply**, **OK**, and **OK**.
- 4. Run **dcomcnfg** to add a user under **DCOMCNFG**.



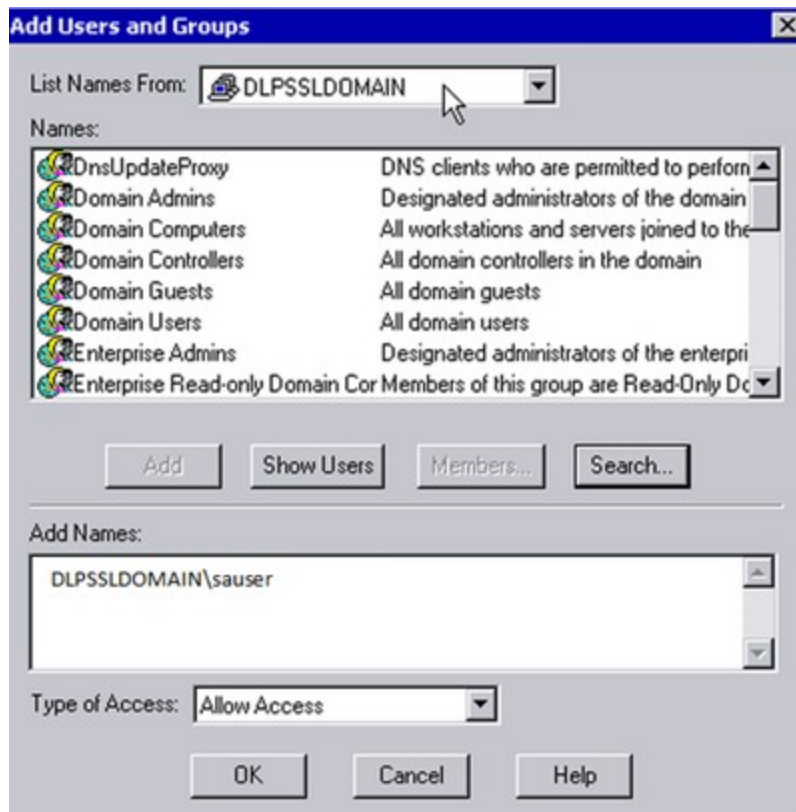
- 5. Select **Default Security** tab.



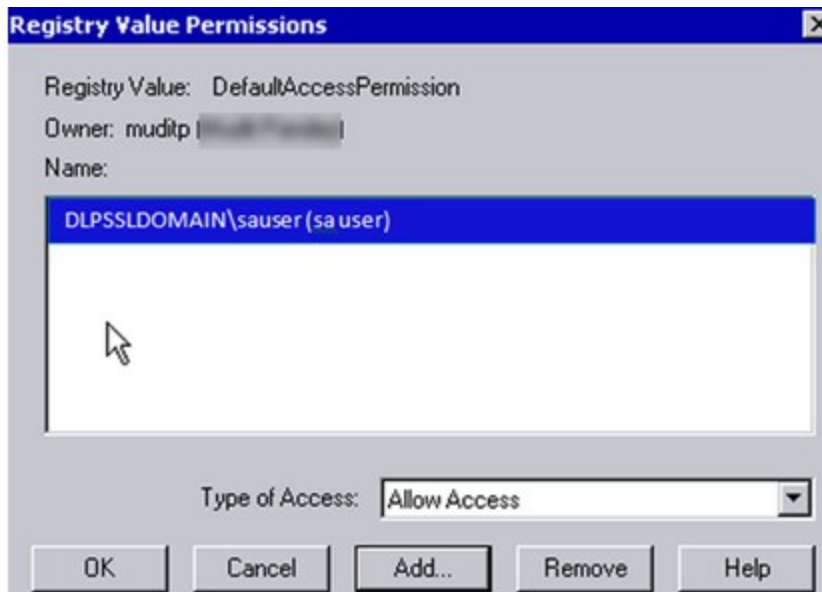
6. Click **Edit Permissions**.
7. Find **sauser**.



8. Click **Add**, select **Allow Access** in the **Type of Access** field from the drop-down list, and click **OK**.



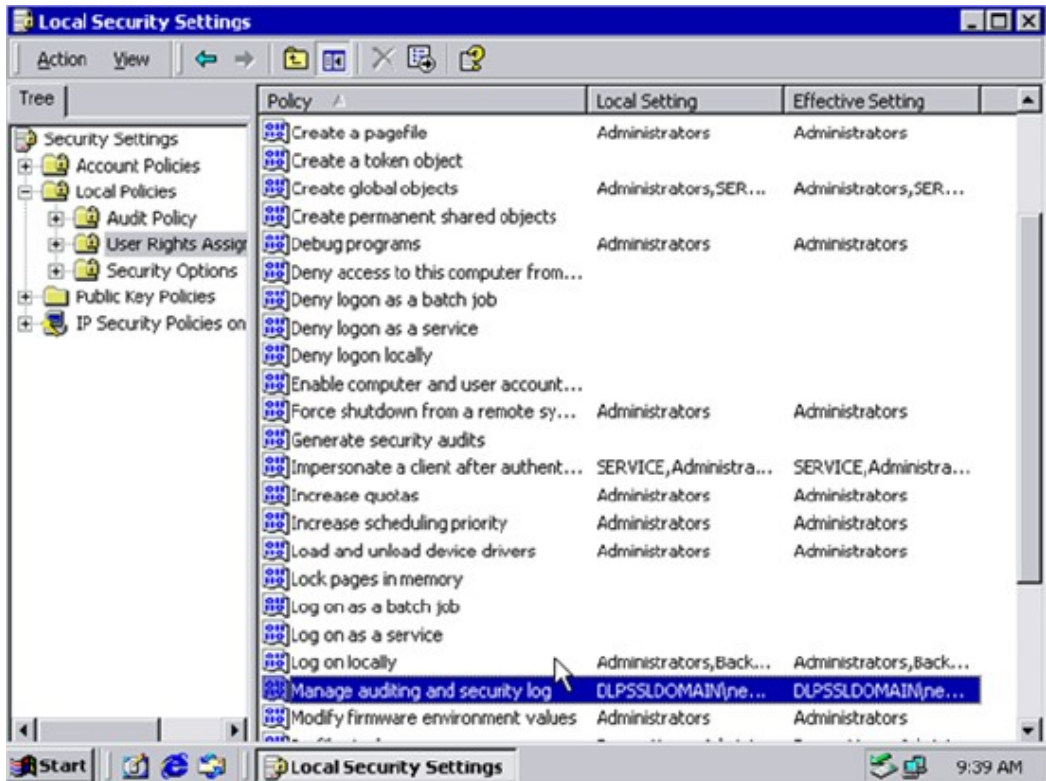
The Registry Value Permission page is displayed.



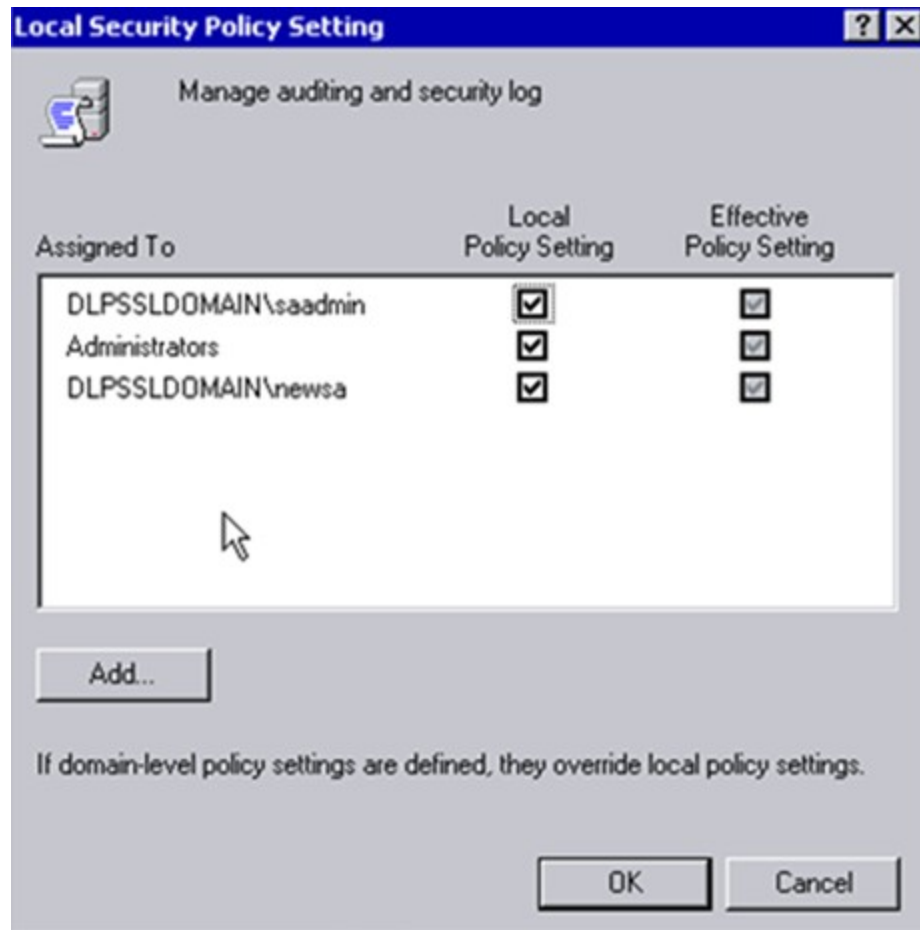
9. Click **OK**.

**To add the Local Security Policy on each Windows 2000 event source:**

1. In a command prompt, run the `secpol.msc` command.  
The Local Security Settings window is displayed.
2. In the **Local Policies** folder, select the **User Rights Assignment** folder.

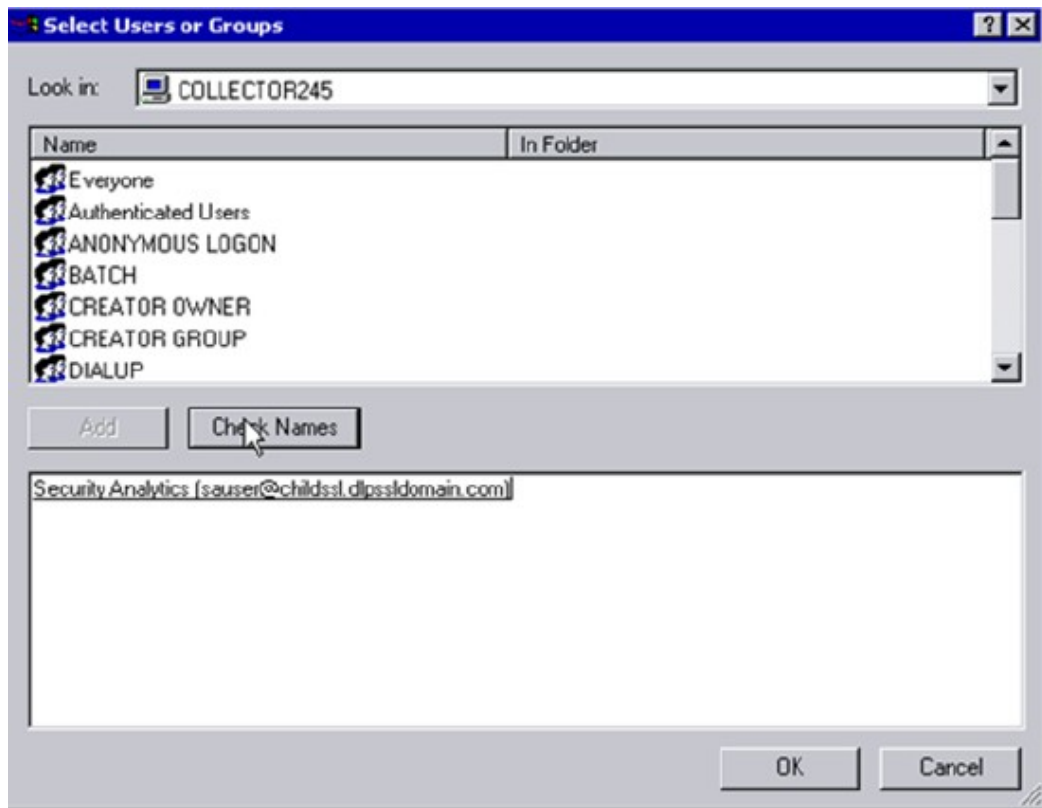


3. Select **Manage auditing and security log**, right click, and select **Security**.  
The Local Security Policy Setting dialog is displayed.
4. Click **Add**.



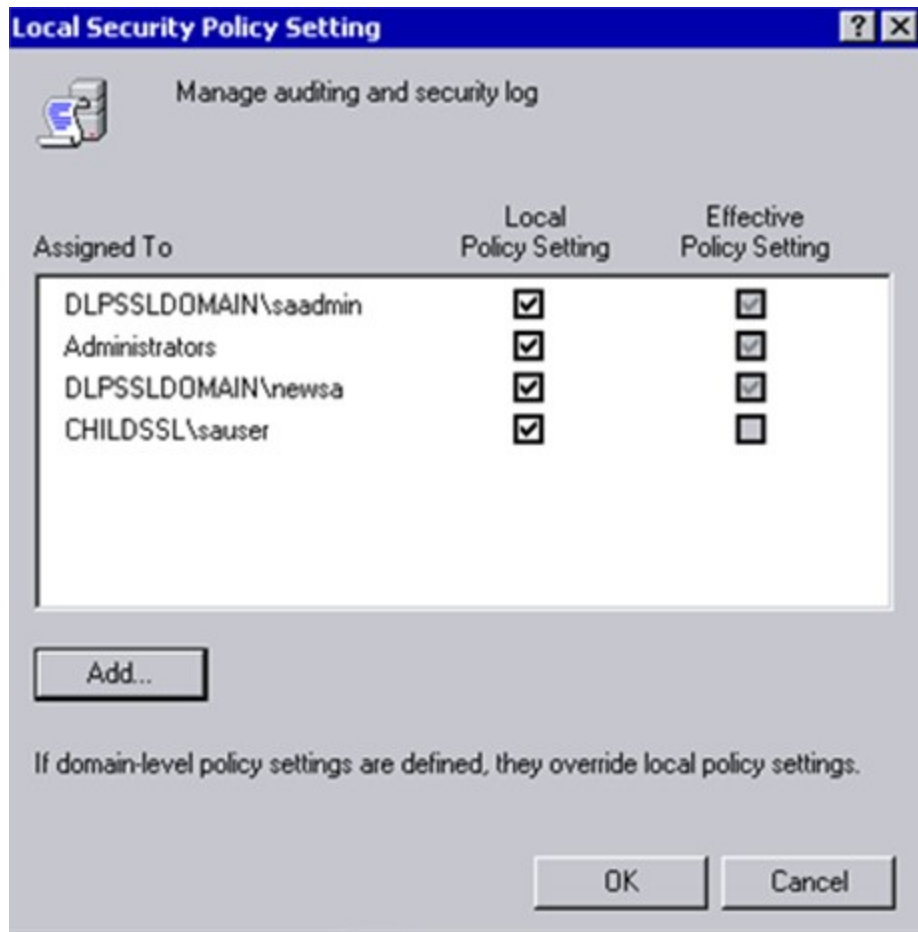
The Select Users or Groups dialog is displayed.

5. Enter the non admin username [for example, **NetWitness (sauser@childssl.dlpssldomain.com)**] and click **Check Names**.



The Local Security Policy Setting dialog is displayed.

6. Click **OK** twice to update the local security policy setting.








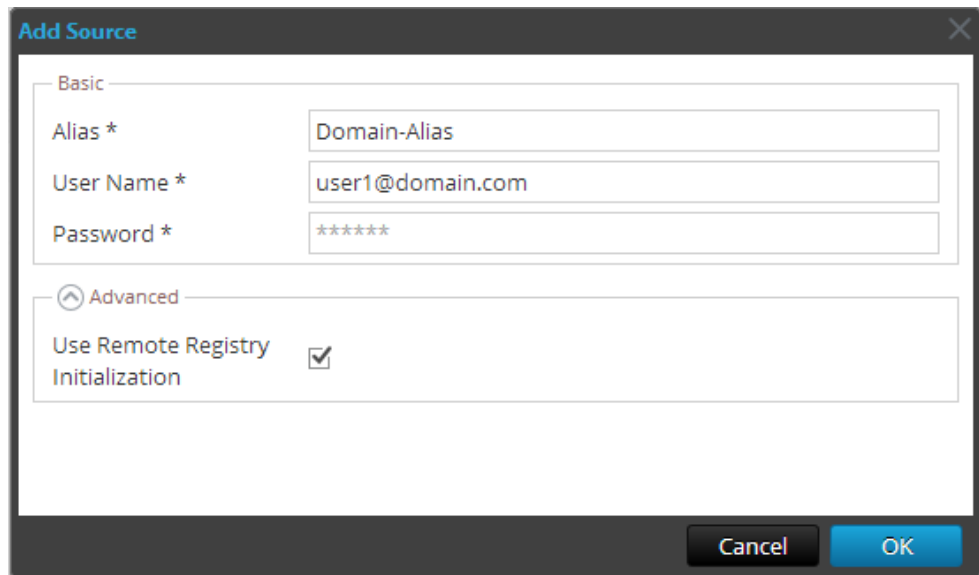
## Configure Legacy Collection on RSA NetWitness Suite

---

This section describes the procedures you need to follow in RSA NetWitness Suite to complete the Windows Legacy event source configuration.

### Add a Windows Legacy Event Source

1. Access the Services view by selecting **Admin > Services** from the NetWitness menu.
2. In the **Services** grid, select a **Windows Legacy Log Collector** service.
3. Under Actions, select   > **View > Config** to display the Log Collection configuration parameter tabs.
4. Click the **Event Sources** tab.
5. In the **Event Sources** tab, select one of the following options from the drop-down menu.
  - Windows Legacy/Windows.
  - Windows Legacy/NetApp.
6. Configure the alias:
  - a. Click  in the **Event Categories** panel toolbar.  
The **Add Source** dialog is displayed.
  - b. Specify values for the parameters and click **OK**.



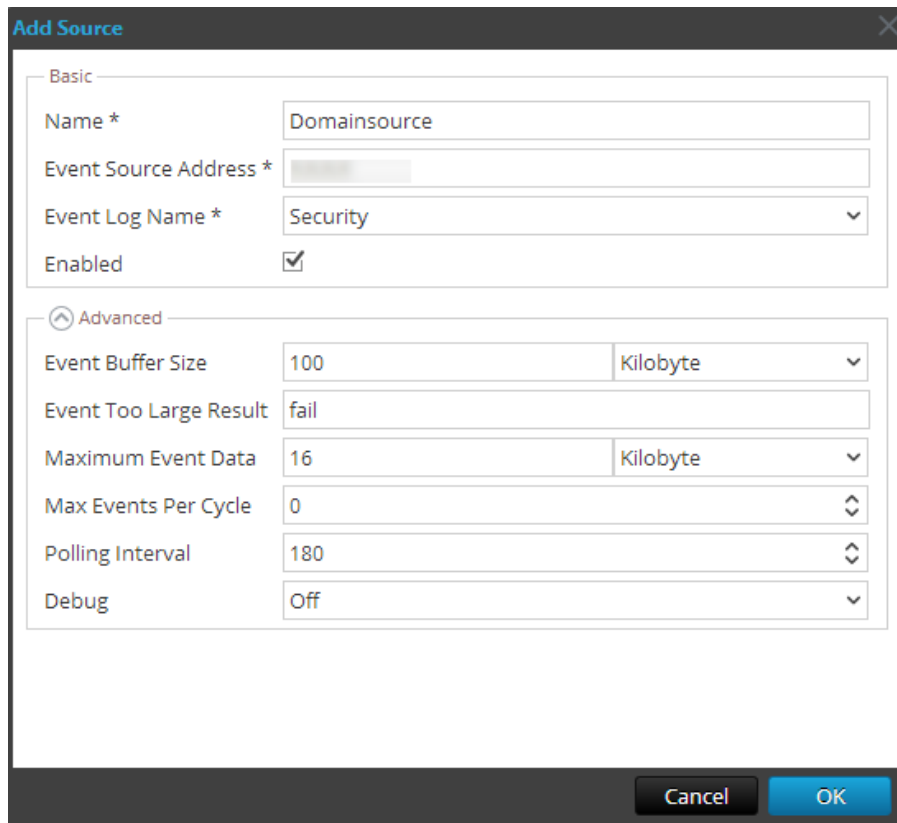
**Note:** Enter the credentials you created during [Step 1 - Create a Non-Admin Domain User](#).

**Note:** By default, **Remote Registry Initialization** is selected. For details, see [Remote Registry Access](#) below.

The newly added windows event source type is displayed in the **Event Categories** panel.

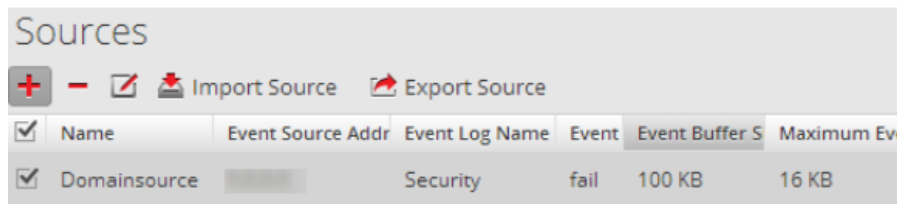
7. Add the event source:
  - a. Select the new alias in the **Event Categories** panel and click **+** in the **Source** panel toolbar.

The **Add Source** dialog is displayed.
  - b. Specify values for the event source parameters and click **OK**.



For details, see [Windows Legacy Configuration Parameters](#) below.

The newly added Windows event source is displayed in the **Event Categories** panel.



## Remote Registry Access

Windows Legacy Collector performs an initial verification of the event source before collecting data. By default, Windows Legacy Collector uses Windows Management Instrumentation (WMI) method to perform this initial verification. If you enable Remote registry access method, Windows Legacy Collector performs a remote registry query to verify the event source.

## Windows Legacy Configuration Parameters

The following table describes the parameters for a Windows Legacy event source.

Feature	Description
<b>Basic</b>	
Name*	The name of the event source. Valid value is a name in the [_a-zA-Z] [_a-zA-Z0-9]* range. You can use a dash "-" as part of the name.
Event Source Address*	IP address of the event source. Valid value is an IPv4 address, IPv6 address, or a hostname including a fully qualified domain name. NetWitness defaults to <b>127.0.0.1</b> .  The Log Collector converts the hostname to lower-case letters to prevent duplicate entries.
Event Log Name	The name of the event log from which to collect event data (for example, <b>System</b> , <b>Application</b> , or <b>Security</b> ). The following are examples of some of these channels: <ul style="list-style-type: none"> <li>• <b>System</b> - applications that run under system service accounts (installed system services), drivers, or a component or application that has events that relate to the health of the system.</li> <li>• <b>Application</b> - all user-level applications. This channel is unsecured and it is open to any application. If an application has extensive information, you should define an application-specific channel for it.</li> <li>• <b>Security</b> - the Windows Audit Log (event log) used exclusively for the Windows Local Security Authority.</li> </ul>
Enabled	Select this checkbox to collect from this event source. If you do not check this checkbox, the Log Collector does not collect events from this event source.

Feature	Description
Event Directory Path	<p>NetApp <b>.evt or .evtx</b> files directory path. This must be the UNC path. The NetApp generates event data and saves it in <b>.evt or .evtx</b> files in a shareable directory on the NetApp appliance.</p> <ul style="list-style-type: none"> <li>• In each polling cycle, the Log Collector browses the configured NetApp shared path for the <b>.evt</b> files that you identified with the <b>Event Directory Path</b> and <b>Event File Prefix</b> parameters. The Log Collector: <ul style="list-style-type: none"> <li>◦ sorts files that match the <b>event-file-prefix.YYMMDDhhmmss.evt</b> format in ascending order.</li> <li>◦ uses the timestamp of the last file processed to determine the files that still need processing. If the Log Collector finds a partially processed file, it skips the events already processed.</li> </ul> </li> <li>• In each polling cycle, the Log Collector browses the configured NetApp shared path for the <b>.evtx</b> files that you identified with the <b>Event Directory Path</b> and <b>Event File Prefix</b> parameters. The Log Collector : <ul style="list-style-type: none"> <li>◦ sorts files that match the <b>event-file-prefix.YYMMDDhhmmssms.evtx</b> format in ascending order.</li> <li>◦ uses the timestamp of the last file processed to determine the files that still need processing. If the Log Collector finds a partially processed file, it skips the events already processed.</li> </ul> </li> </ul>
Event File Prefix	Prefix of the <b>.evt</b> files (for example, <b>adtlog</b> .) saved in the <b>Event Directory Path</b> .
<b>Advanced</b>	
Event Buffer Size	<p>Maximum size of the data the Log Collector pulls from the event source for each request.</p> <p>Valid value is a number in <b>0 to 511</b> Kilobytes range. You specify this value in <b>Kilobytes</b>.</p>

Feature	Description
Event Too Large Result	Tells the Log Collector what to do if an event is too large for the event buffer.
Maximum Event Data	<p>Maximum size of event data to include in the output. Valid value is a number in <b>0</b> to <b>511Kilobytes</b> range. You specify this value in <b>Kilobytes</b> or <b>Megabytes</b>.</p> <ul style="list-style-type: none"> <li>• 1 Kilobyte - 100 Megabytes</li> <li>• 0 = do not include event data in the output.</li> </ul>
Max Events Per Cycle	The maximum number of events per polling cycle (how many events collected per polling cycle).
Polling Interval	<p>Interval (amount of time in seconds) between each poll. The default value is <b>180</b>.</p> <p>For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.</p>

Feature	Description
Debug	<p><b>Caution:</b> Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector .</p> <p>Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>Off</b> = (default) disabled</li> <li>• <b>On</b> = enabled</li> <li>• <b>Verbose</b> = enabled in verbose mode - adds thread information and source context information to the messages.</li> </ul> <p>This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). Limit the number of event sources for which you use Verbose debugging to minimize performance impact.</p>
Cancel	Closes the dialog without adding the Windows Legacy event source.
OK	Adds the current parameter values as a new event source.

Copyright © 2017 EMC Corporation. All Rights Reserved.

## Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.