RSA Security Analytics

Security Analytics v10.3 Windows Legacy Collection Installation Instructions

Contents

Window Legacy Collection **2**

SA Legacy Windows Collector Setup Requirements **3**

Create a Non-Admin Domain User **4**

Task 1 - Create Non-Admin Domain User on the Domain Controller 5
Task 2 - Set Event Log Security on Domain Controller 6
Task 3 - Add Non-Admin Domain User to WMI and DCOMCNFG on Each Windows Legacy Event Source 8
Task 4 - Add Non-Admin Domain User to Local Administrators and Remote Desktop Users Groups on Windows 2008 Server 13

Install the SA Legacy Windows Collector **14**

Window Legacy Collection

The Security Analytics (SA) 10.3 Log Collector introduces Windows Legacy collection. With this feature, you can collect event data from:

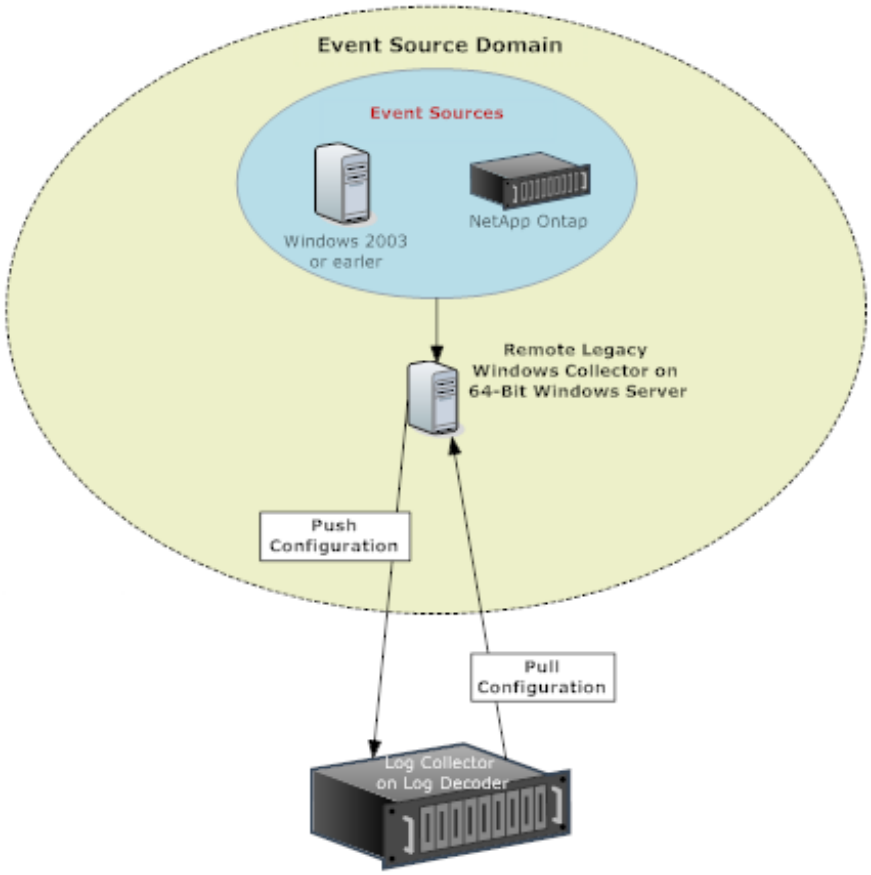
- Windows 2003 and earlier event sources
- NetApp ONTAP appliance evt files

SA Legacy Windows Collector Setup Requirements

To set up the SA Legacy Windows Collector, you need:

- Any physical or virtual Windows 2008 64-Bit Server located in the same domain as your Windows 2003 event sources.
- A minimum of 20% free disk space. For example, you need at least 20 GB of free space if your system drive is 100 GB in size.
- A non-admin domain user (see Create a Non-Admin Domain User) that has access to the event sources in the domain.
- To include the non-admin domain user in both the Local Administrator Group and the Remote Desktop User Group on Windows legacy collector system.

Note: Installing the Windows legacy collector on a Domain controller may affect the performance of the system.



Create a Non-Admin Domain User

You must complete the following tasks to create a non-admin domain user for the **SA Legacy Windows Collector.**

Task 1 - Create a non-admin domain user (for example, **sauser**) on the Domain Controller.

Task 2 - Set Event Log Security on the Domain Controller.

Task 3 - Add a non-admin domain user to **WMI** and **DCOMCNFG** management on each Windows 2003 or earlier event source from which you want to collect event data.

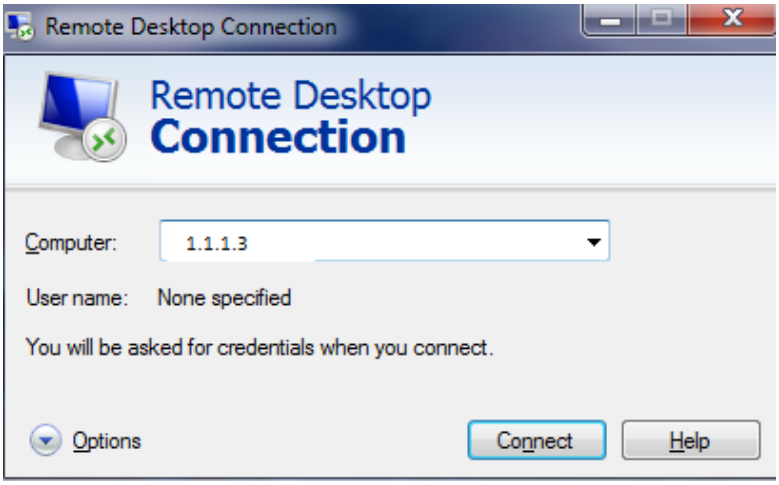
Task 4 - Add non-admin domain user (for example, **sauser**) to the Local Administrators group and Remote Desktop Users group on Windows 2008 server.

Note: You need to add a non-admin domain user in the **Local Administrators** group only on the Windows 2008 server on which the SA Legacy Windows Collection Service is installed. You do not need to add it to all event source machines.

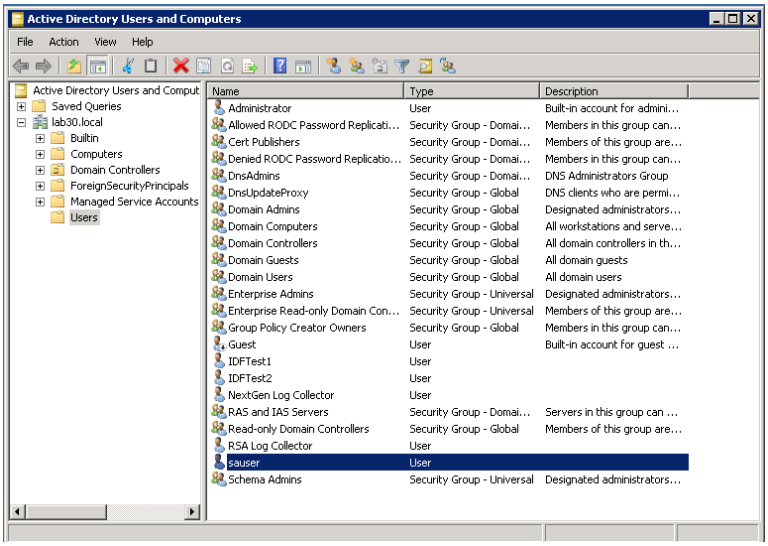
Task 1 - Create Non-Admin Domain User on the Domain Controller

To create the SA domain user (for example, **sauser**) on the Domain Controller:

1. Log into the Domain Controller.



2. On Domain Controller create a non-admin domain user (for example, **sauser**).



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

Task 2 - Set Event Log Security on Domain Controller

To set Event Log Security on the Domain Controller:

1. Log on the Domain Controller.
2. Use a text editor such as Notepad to open the **Sceregvl.inf** in the **%Windir%\Inf** folder.
3. Add the following lines to the **[Register Registry Values]** section:

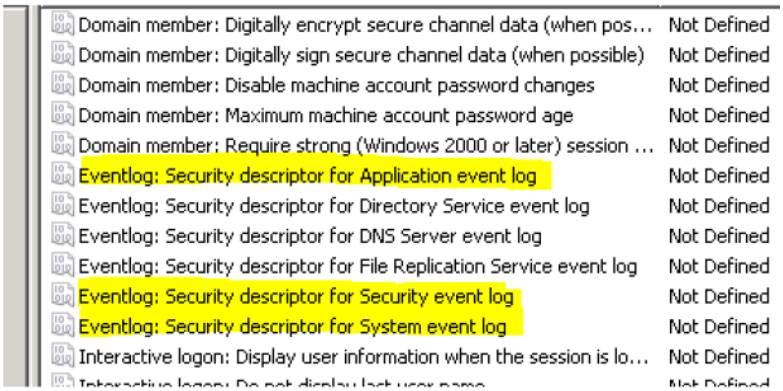
```
MACHINE\System\CurrentControlSet\Services\Eventlog\Application\CustomSD,1,%AppCustomSD
%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\Security\CustomSD,1,%SecCustomSD%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\System\CustomSD,1,%SysCustomSD%,2
MACHINE\System\CurrentControlSet\Services\Eventlog\Directory
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 **Sceregvl.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 pane, right click, and select **Enforce**.
    e. Under **Security Filtering**, click **Add**.
    f. Under **Select User**, **Computer and Group**, type **Domain Computers**, click on **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 **Eventing** settings in the right pane.



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

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:

1. Run 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
   ```

If the security policy Settings 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)`

- 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;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;; 0x1;;;`***SID***.

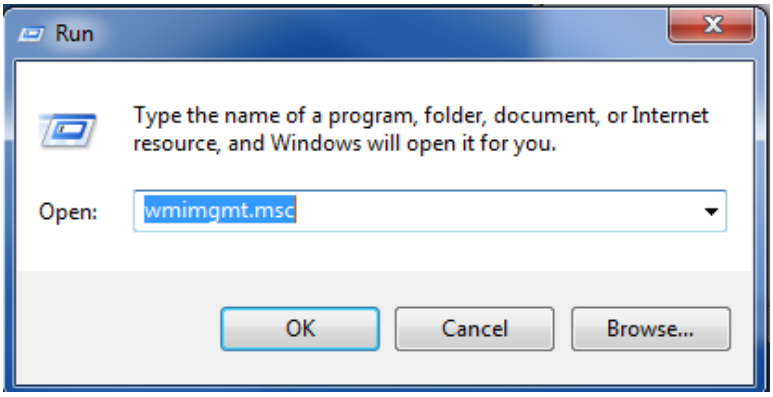
  For example:
  `O:BAG:SYD:(D;;0xf0007;;;AN)(D;;0xf0007;;;BG)(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x7;;;SO)(A;;0x3;;;IU)(A;;0x3;;;SU)(A;;0x3;;;S-1-5-3)(A;; 0x1;;;S-1-5-21-3244245077-2111152846-3233386924-1114)`

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

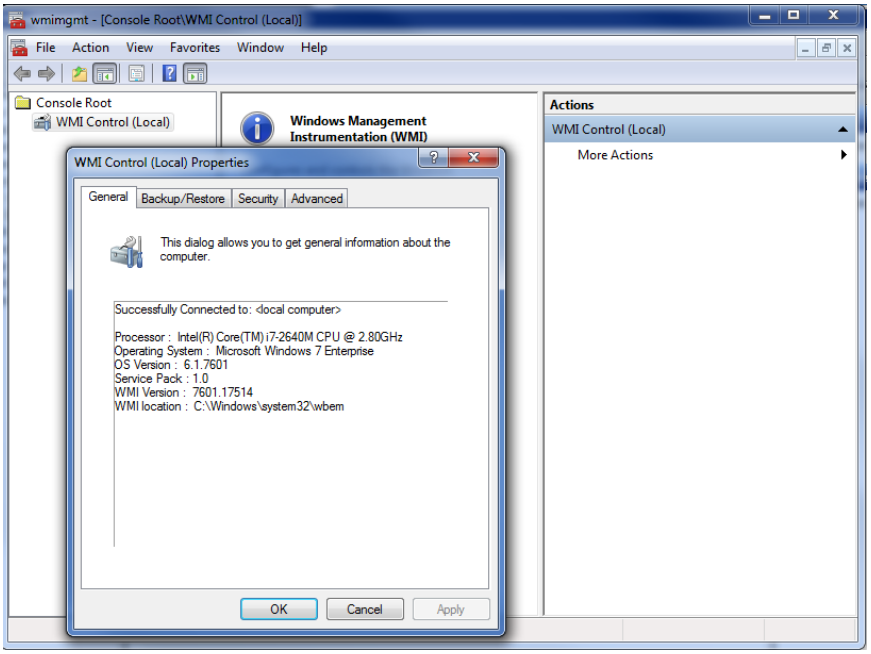
Task 3 - Add Non-Admin Domain User to WMI and DCOMCNFG on Each Windows Legacy Event Source

To add the SA user (for example, **sauser**) to the WMI and DCOMCNFG management on each Windows 2003 or earlier event source:

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

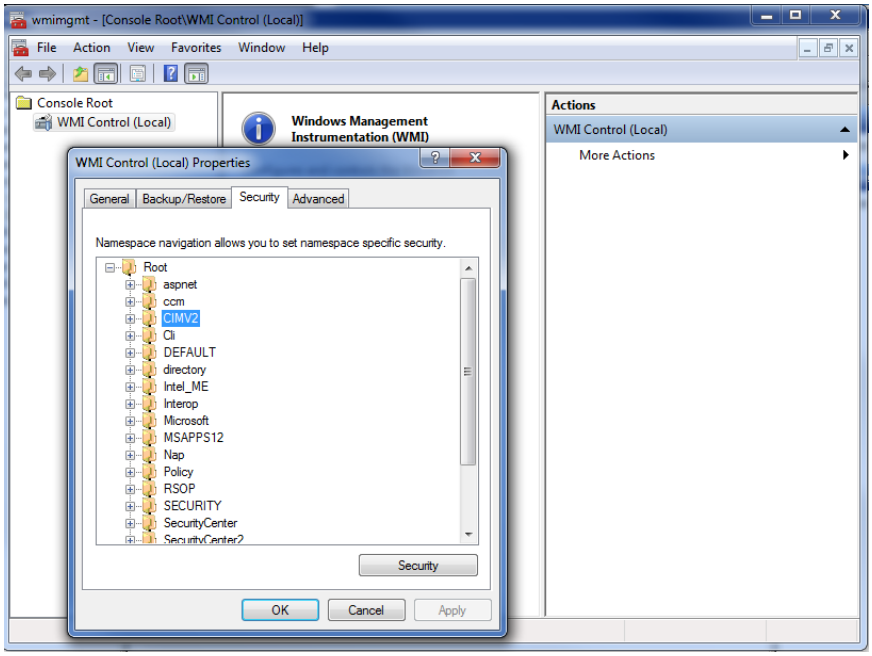


3. Add the SA user under **wmi \root\CIMV2** security option.
   a. Right click **WMI Control** and click **Properties**.



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

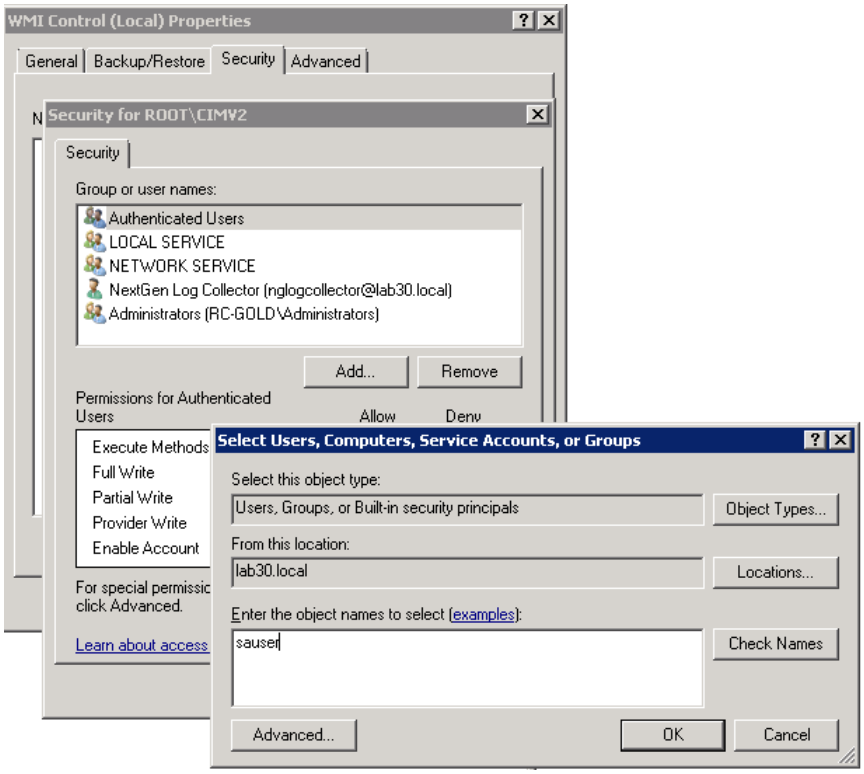
c. Click Security.

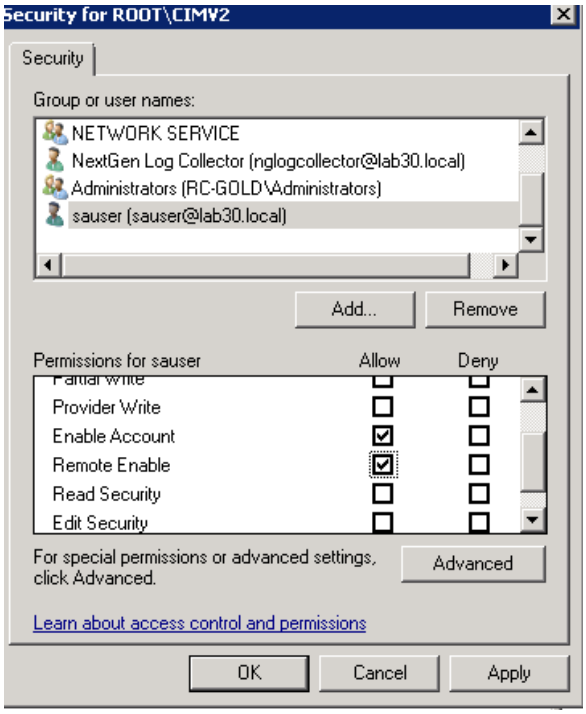


d. In the **Group or user names** section, click **Add**... to create a user.

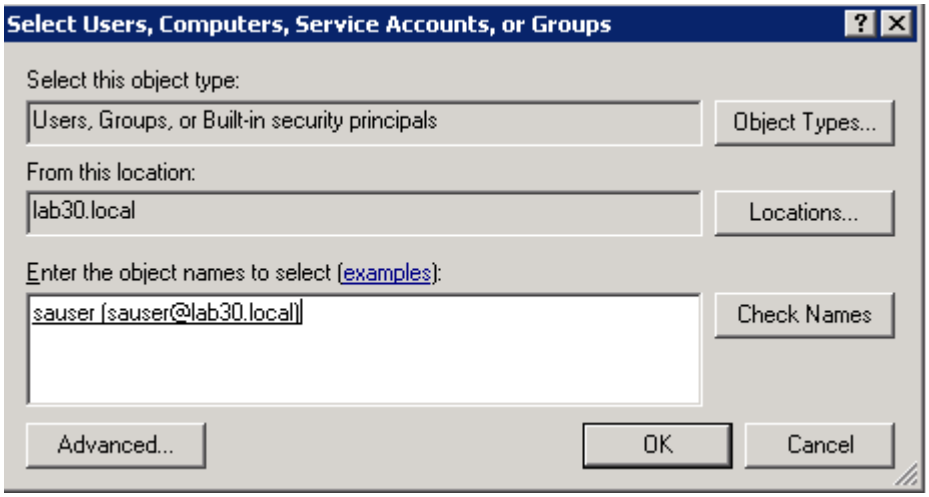
e. Select the **Enable Account** and **Remote Enable** permissions for that user.

f. Enter the user (for example, **sauser**).





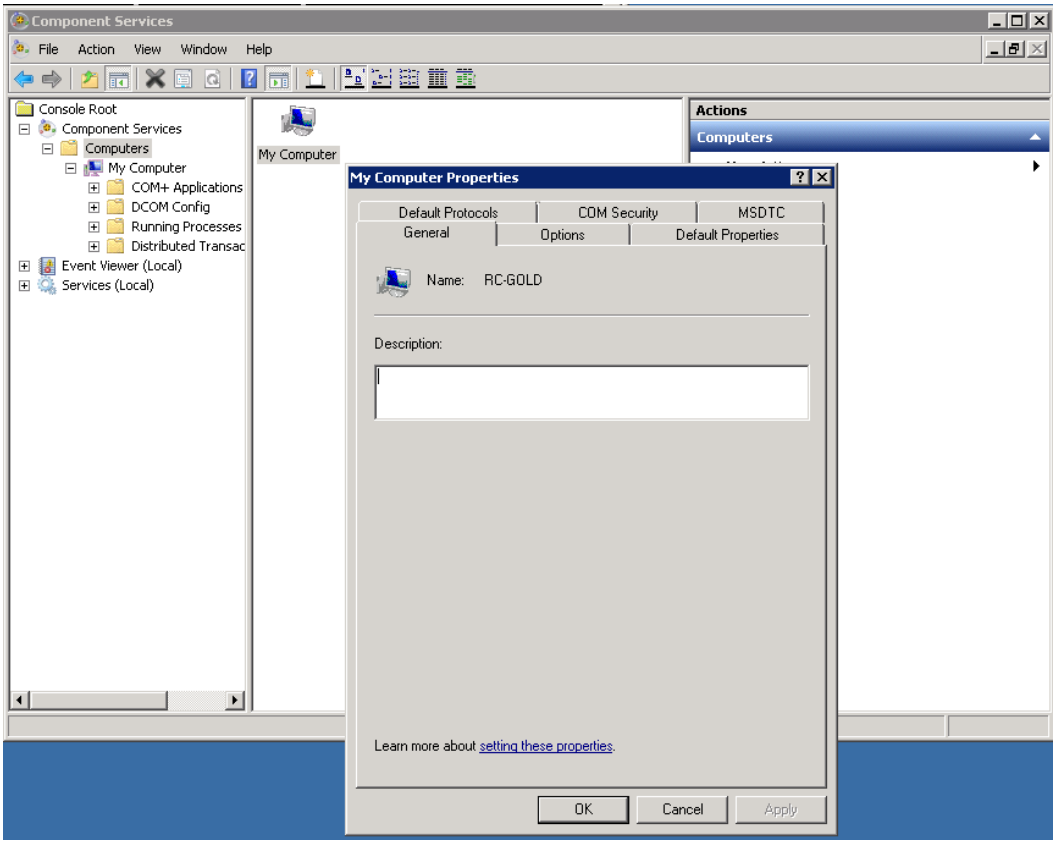
g. Click **Check Names** to verify that the new user was added correctly.



h. Click **Apply**, **OK**, and **OK**.

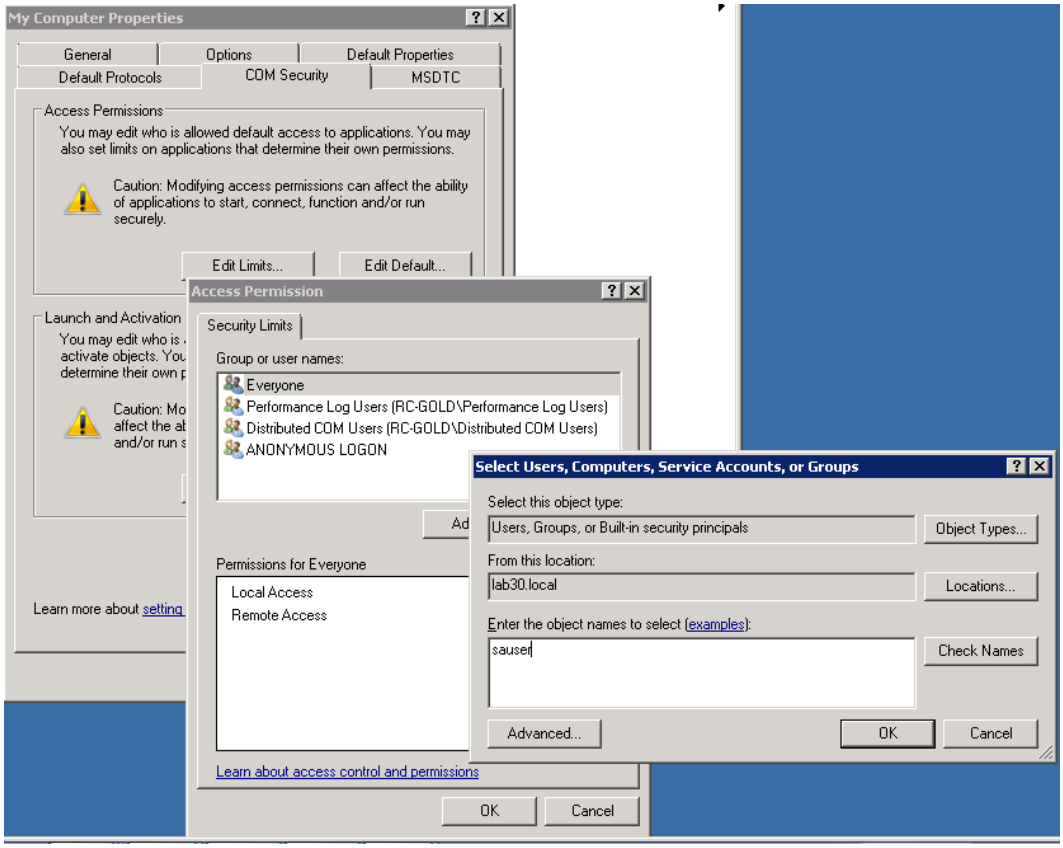
4. Add a user under **DCOMCNFG**:
   a. Run **dcomcnfg**.
   b. Click **Root** > **Component Services** > **Computers** > **My Computer**.

c. Right click **My Computer** and click **properties**.



5. Under **Access Permissions:**
   a. Click **Edit Limits**
   b. Add the SA 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 SA 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.

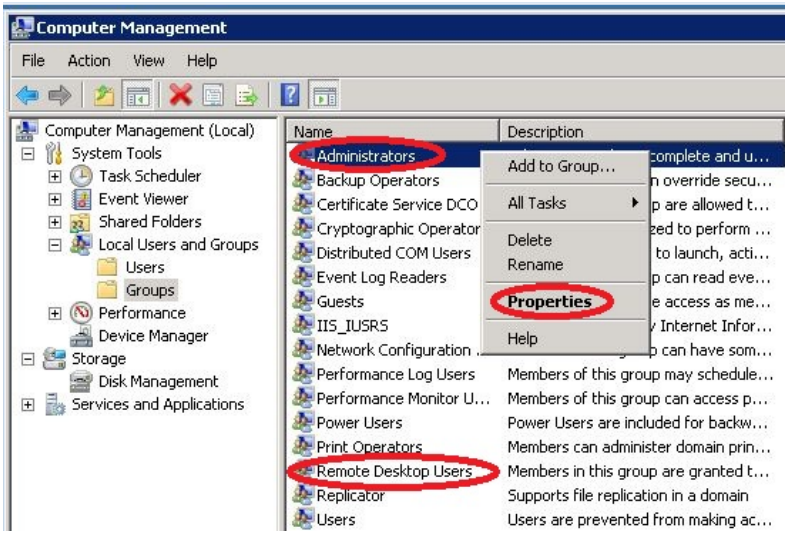


Task 4 - Add Non-Admin Domain User to Local Administrators and Remote Desktop Users Groups on Windows 2008 Server

Note: You only need to add non-admin domain user in the **Local Administrators** group on the Windows 2008 server on which the SA Legacy Windows Collection Service is installed. You do not need to add it to all eventsource machines.

To add a non-admin user (for example, **sauser**) to local **Administrators** and **Remote Desktop Users** groups:

1. Log in as a local administrator to windows 2008 server.
2. Click **Start** >**Administrative Tools**>**Computer Management**.
3. Click **Local Users and Groups**.
4. Click **Groups**.
5. Add a non-admin user (for example, **sauser**) to the local **Administrator** group:
    a. Click **Administrators**.
    b. Add a non-admin user (for example, **sauser**) to the local **Administrator** group.
6. Add a non-admin user (for example, **sauser**) to the local **Remote Desktop Users** group:
    a. From **Administrative Tools**>**Computer Management>Local Users and Groups>Groups**, click **Remote Desktop Users**.
    b. Add a non-admin user (for example, **sauser**) to the local **Remote Desktop Users** group.



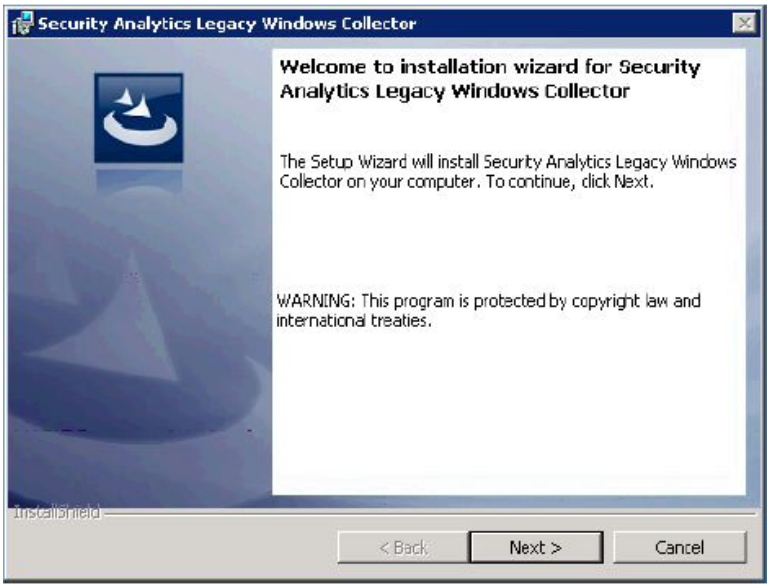
Install the SA Legacy Windows Collector

To install the SA Legacy Windows Collector on a Windows 2008 server:

1. Download the **SALegacyWindowsCollector-*version-number*.exe** from SecurCare Online (SCOL).
2. Log on to a Windows 2008 machine using a non-admin domain user (or local administrator).
   Please refer to Create a Non-Admin Domain User if you need instructions on how to create a non-admin domain user.
3. Copy the **SALegacyWindowsCollector-*version-number*.exe** to the Windows 2008 server.
4. Right click on the **SALegacyWindowsCollector-*version-number*.exe** and select **Run As Administrator**.

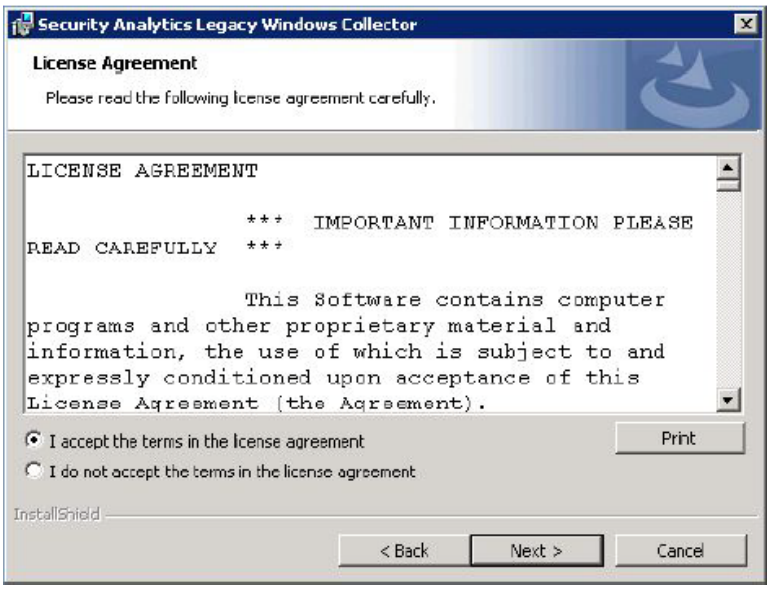
   The **Preparing to Install….** page of installation wizard displays.

After the installation program extracts SA Legacy Windows Collector installation files, the **Welcome…** page is displayed.



5. Click **Next**.

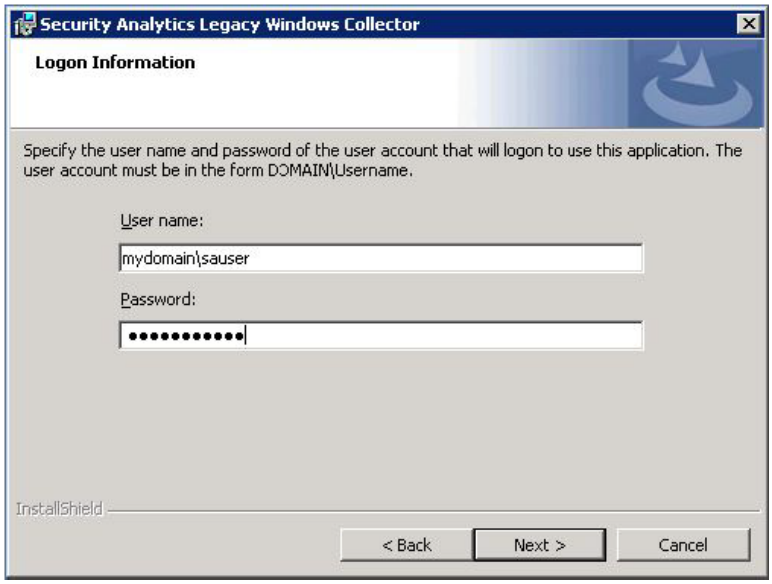
   The **License Agreement** page is displayed.



6. Read the License agreement carefully, select the **I accept the terms in the license agreement** radio button, and click **Next**.

The **Logon Information** page is displayed.

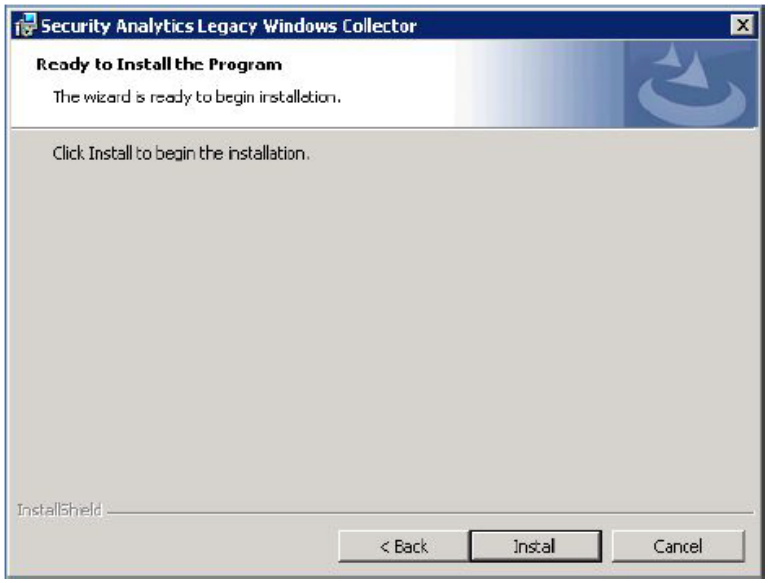
Note:	The example in this procedure uses the non-admin domain user "**sauser**" for a windows domain called "**mydomain**" along with the corresponding password for the user.



7. Enter a user name and password and click **Next**.

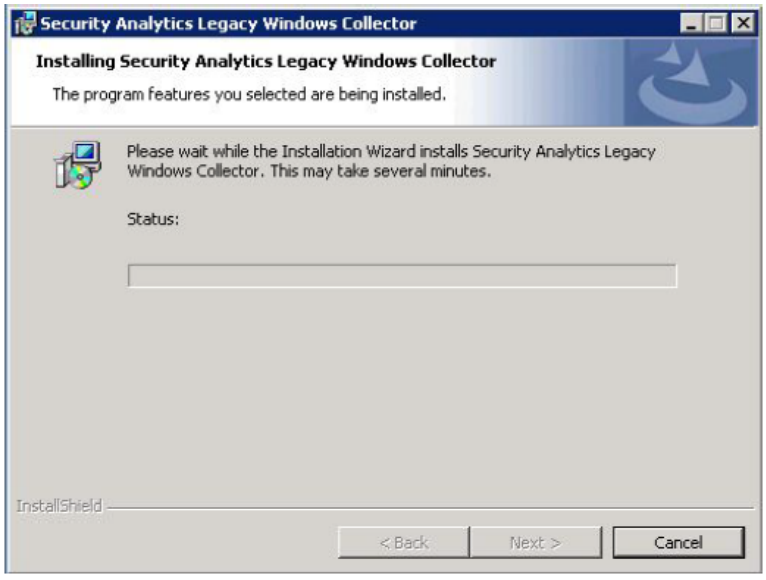
The **Ready to Install the Program** page displays.

Note: If the credentials are not valid, **Invalid credentials message** is displayed.



8. Click **Install**.

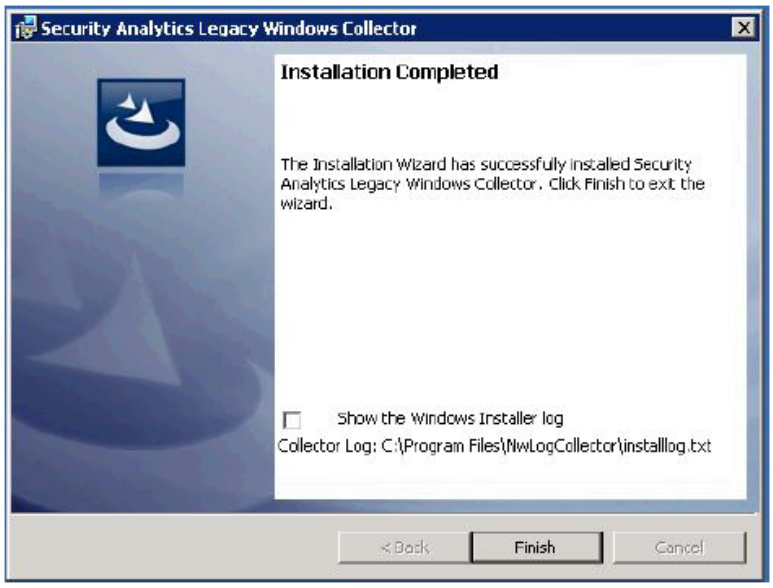
The **Installing SA Legacy Windows Collector** page displays.



After the installation completes, the **Next** button becomes active.

9. Click **Next**.

   The **Installation Completed** page is displayed.



10. (Optional) If you want to review a log of the Installation, select the **Show the Windows Installer log** check box.
11. Click **Finish**.

Note: Refer to the following log files if you need to troubleshoot problems:

- **%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log**
- **%systemDrive%\Program Files\NwLogCollector\installlog.txt**
