Installing the Cisco Context Directory Agent

The Cisco Context Directory Agent (CDA) is a software application that is packaged as an ISO image. You can download it from Cisco.com. You must install it on a dedicated X86 machine or a virtual machine on VMware ESX server and configure it with consumer devices and Active Directory domain controllers.

This chapter contains the following:

Requirements

This section contains the following topics:

Supported Operating Systems

CDA is installed on the Cisco Linux OS it is bundled with.When installing the CDA ISO image on a standalone machine or on a VMWare server, Linux is installed as the OS and CDA is an application running on top of it.

Related Topics:

- Hardware Requirements, page 2-2
- Connectivity Requirements, page 2-3
- Active Directory Requirements for Successful Connection with CDA, page 2-4

Supported Active Directory Versions

CDA supports the following Active Directory versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012

Hardware Requirements

The CDA machine must be a separate, dedicated appliance or VMware.

In all cases, a CDA machine must meet the standard hardware and VMWare specifications listed in Table 2-1.

Table 2-1 Standard/Performance Hardware Requirements for a Standalone Appliance or a VMWare with Equivalent Resources

Component	Specification
CPU	Intel Xeon 2.66 GHz Q9400 (Quad Core)
System memory	4 GB of SDRAM
Hard disk space	250 GB
NIC	1 NIC or virtual NIC

Table 2-2 lists the minimum hardware requirements for installing CDA on a VMWare.

Table 2-2 Minimum Hardware Requirements for a VMWare

Component	Specification
CPU	2 Virtual Processors
System memory	2 GB of SDRAM
Hard disk space	120 GB
NIC	1 virtual NIC

Related Topics:

- Supported Operating Systems, page 2-1
- Connectivity Requirements, page 2-3
- Active Directory Requirements for Successful Connection with CDA, page 2-4

Connectivity Requirements

For CDA to function properly, it must be able to communicate freely with all the consumer devices, Active Directory domain controller machines from which it should receive logs, and target syslog servers that are configured with it. If log forwarding is being employed, then connectivity is required only between CDA and the aggregating domain controller machines, there is no need to provide connectivity between all domain controller machines and CDA in a centralized log forwarding deployment.

If Windows Firewall (or any other comparable third-party firewall software) is running on any of the Active Directory domain controller machines, then the firewall software on each of these endpoints must be configured with the necessary exceptions to allow this communication to flow freely.

This section uses the Windows Firewall as an example and details the exceptions that must be defined on any of the endpoints that might be running Windows Firewall.

For any other comparable third-party firewall software, refer to that vendor's documentation on how to configure the corresponding exceptions.

Windows Firewall Exceptions to be Configured on Each Separate Active Directory Domain Controller Machine

For each separate Active Directory domain controller machine that is configured on the CDA machine using the GUI, if Windows Firewall is enabled on that separate domain controller machine, then you must define a Windows Firewall exception on that particular domain controller machine that will allow the necessary WMI-related communication.

If that domain controller machine is running Windows Server 2008 or Windows Server 2008 R2, then you can configure this WMI-related exception using the following Windows command line (written in a single line):

```
netsh advfirewall firewall set rule group=”Windows Management Instrumentation (WMI)" new enable=yes
```

If that domain controller machine is running Windows Server 2003 or Windows Server 2003 R2 (with SP1 or later installed), then you can configure this WMI-related exception using the following Windows command line (written in a single line):

```
netsh firewall set service RemoteAdmin enable
```

Related Topics:

- Supported Operating Systems, page 2-1
- Hardware Requirements, page 2-2
- Active Directory Requirements for Successful Connection with CDA, page 2-4

List of Open Ports

Table 2-3 lists some of the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports that CDA uses for communication with consumer devices. These ports are open by default on CDA.

Table 2-3 List of Default Open Ports on CDA

Port No.	Protocol	Service	Purpose
22	TCP	The Secure Shell (SSH) Protocol	CDA SSH CLI Administration
80	TCP	HTTP (Web GUI, redirected to HTTPS)	CDA GUI Administration interface (for redirect only)

Table 2-3 List of Default Open Ports on CDA

Port No.	Protocol	Service	Purpose
123	UDP	NTP	Time server
443	TCP	HTTPS (Secure web GUI)	CDA GUI Administration interface
1645	UDP	RADIUS	CDA and device consumer (ASA/WSA) interface
1646	UDP	RADIUS	CDA and device consumer (ASA/WSA) interface
1812	UDP	RADIUS	CDA and device consumer (ASA/WSA) interface
1813	UDP	RADIUS Accounting	CDA and device consumer (ASA/WSA) interface
514	UDP	Syslog	CDA and ISE/ACS interface
1468	TCP	Syslog	CDA and ISE/ACS interface
6514	SSL	SSL Syslog	CDA and ISE/ACS interface

The ports mentioned in Table 2-3 should be open to establish proper communication between CDA and ASA or WSA.

The following ports are open for internal communication between CDA processes, but blocked for access from outside the appliance by the Linux firewall:

- 8005
- 8009
- 8020
- 8090
- 8091
- 8092
- 8093

Active Directory Requirements for Successful Connection with CDA

CDA leverages Active Directory login audit events generated by the Active Directory domain controller to gather user logins information. In order for CDA to work appropriately, CDA needs to be able to connect to Active Directory and fetch the user logins information.

The following steps should be performed on the Active Directory domain controller:

1. Make sure the Active Directory version is supported (refer to Supported Active Directory Versions) and there is network connectivity between Active Directory domain controller and CDA (refer to Connectivity Requirements)
2. Make sure relevant Microsoft patches are installed on the Active Directory domain controllers. Active Directory domain controller machines runs Windows Server 2008 or Windows Server 2008 R2 and must have the appropriate Microsoft hotfixes installed.

   The following patches for Windows Server 2008 are required:

a. http://support.microsoft.com/kb/958124

This patch fixes a memory leak in Microsoft's WMI, which prevents CDA to establish successful connection with the domain controller (CDA administrator can experience it in CDA Active Directory domain controller GUI page, where the status need to be "up" once the connection establishes successfully).

b. http://support.microsoft.com/kb/973995

This patch fixes different memory leak in Microsoft's WMI, which sporadically prevents the Active Directory domain controller from writing the necessary user login events to the Security Log of the domain controller. As result CDA may not get all user login events from this domain controller.

The following patches for Windows Server 2008 R2 are required (unless SP1 is installed):

a. http://support.microsoft.com/kb/981314

This patch fixes memory leak in Microsoft's WMI, which sporadically prevents the Active Directory domain controller from writing the necessary user login events to the Security Log of the domain controller. As result CDA may not get all user login events from this domain controller.

3. Make sure the Active Directory logs the user login events in the Windows Security Log.

Verify that the settings of the "Audit Policy" (part of the "Group Policy Management" settings) allows successful logons to generate the necessary events in the Windows Security Log (this is the default Windows setting, but you must explicitly ensure that this setting is correct). See Setting the Audit Policy, page 2-7.

4. You must have an Active Directory user with sufficient permissions to be used by CDA to connect to the Active Directory. In CDA patch 2, you can choose whether this user is member of the Active Directory domain admin group or not. Follow the following instructions to define permissions either for admin domain group user or none admin domain group user:

- Permissions Required when an Active Directory User is a Member of the Domain Admin Group, page 2-7
- Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group, page 2-8

5. The Active Directory user used by CDA can be authenticated either by NTLMv1 or NTLMv2. You need to verify that the Active Directory NTLM settings are aligned with CDA NTLM settings to ensure successful authenticated connection between CDA and the Active Directory Domain Controller. Figure 2-1 illustrates all Microsoft NTLM options. In case CDA is set to NTLMv2, all six options described in Figure 2-1 are supported. In case CDA is set to support NTLMv1, only the first five options are supported. This is also summarized in Table 2-4.

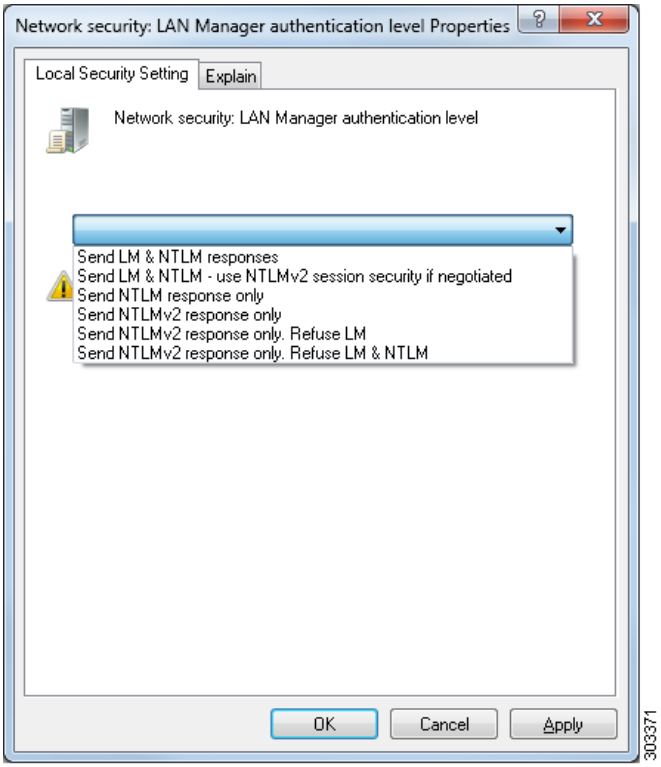
Table 2-4 Supported Authentication Types Based on CDA and AD NTLM Version Settings

CDA NTLM setting options / Active Directory (AD) NTLM setting options	NTLMv1	NTLMv2
Send LM & NTLM responses	connection is allowed	connection is allowed
Send LM & NTLM - use NTLMv2 session security if negotiated	connection is allowed	connection is allowed
Send NTLM response only	connection is allowed	connection is allowed
Send NTLMv2 response only	connection is allowed	connection is allowed

Table 2-4 Supported Authentication Types Based on CDA and AD NTLM Version Settings

CDA NTLM setting options / Active Directory (AD) NTLM setting options	NTLMv1	NTLMv2
Send NTLMv2 response only. Refuse LM	connection is allowed	connection is allowed
Send NTLMv2 response only. Refuse LM & NTLM	connection is refused	connection is allowed

Figure 2-1 MS NTLM Authentication Type Options



6. Make sure that you have created a firewall rule to allow traffic to dllhost.exe on Active Directory domain controllers.

Related Topics:

- Supported Operating Systems, page 2-1
- Hardware Requirements, page 2-2
- Connectivity Requirements, page 2-3

Setting the Audit Policy

Ensure that the "Audit Policy" (part of the "Group Policy Management" settings) allows successful logons to generate the necessary events in the Windows Security Log of that AD domain controller machine (this is the default Windows setting, but you must explicitly ensure that this setting is correct).

Step 1 Choose **Start > Programs > Administrative Tools > Group Policy Management**.

Step 2 Navigate under Domains to the relevant domain and expand the navigation tree.

Step 3 Choose Default Domain Controller Policy, right click and choose **Edit**.

The Group Policy Management Editor appears.

Step 4 Choose **Default Domain Controllers Policy > Computer Configuration > Policies > Windows Settings > Security Settings**.

- For Windows Server 2003 or Windows Server 2008 (non-R2), choose **Local Policies > Audit Policy**. For the two Policy items, **Audit Account Logon Events** and **Audit Logon Events**, ensure that the corresponding **Policy Setting** for each of these either directly or indirectly includes the **Success** condition. To include the **Success** condition indirectly, the Policy Setting must be set to **Not Defined**, indicating that the effective value will be inherited from a higher level domain, and the Policy Setting for that higher level domain must be configured to explicitly include the **Success** condition.
- For Windows Server 2008 R2 and Windows 2012, choose **Advanced Audit Policy Configuration > Audit Policies > Account Logon**. For the two Policy items, **Audit Kerberos Authentication Service** and **Audit Kerberos Service Ticket Operations**, ensure that the corresponding **Policy Setting** for each of these either directly or indirectly includes the **Success** condition as described above.

Step 5 If any **Audit Policy** item settings have been changed, you should then run "**gpupdate /force**" to force the new settings to take effect.

Permissions Required when an Active Directory User is a Member of the Domain Admin Group

No special permission is required for the following Active Directory versions:

- Windows 2003
- Windows 2003R2
- Windows 2008

For Windows 2008 R2 and Windows 2012, the Domain Admin group does not have full control on certain registry keys in the Windows operating system by default. In order to get the CDA to work, Active Directory admin must give the Active Directory user Full Control permissions on the following registry keys:

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

In order to grant full control, the Active Directory admin must first take ownership of the key. To do this:

Step 1 Go to the Owner tab by right clicking the key.

Step 2 Click **Permissions**.

Step 3 Click **Advanced**.

Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group

The following are the permissions required when an Active Directory user is not part of the Domain Admin group but of the Domain Users group:

- Required Registry Changes, page 2-8
- Permissions to Use DCOM on the Domain Controller, page 2-8
- Permissions to the WMI Root\CIMv2 Name Space, page 2-10
- Access to Read the Security Event Log of the Active Directory Domain Controller, page 2-11

These permissions are valid for all the following Active Directory versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012

Required Registry Changes

For CDA to work with a Domain User, certain registry keys should be added manually. These registry changes are required to establish a valid connection between CDA and domain controllers to retrieve the users login authentication events. CDA does not require installation of an agent on the domain controllers or on a machine in the domain.

The changes are described in the following registry script. The Active Directory admin can also copy and paste this into a text file with a .reg extension and double click it to make the registry changes. For adding registry keys as described below, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

Make sure that you include two spaces in the value of the key “DllSurrogate”.

You should keep the empty lines as shown in the script above, including an empty line at the end of the file.

Permissions to Use DCOM on the Domain Controller

The Active Directory user must have permissions to use DCOM (remote COM) on the Domain Controller. You can do this by using the **dcomcnfg** tool.

Step 1 Run the **dcomcnfg** tool from the command line.

Step 2 Expand Component Services.

Step 3 Expand Computers and click on My Computer.

Step 4 Select Action from the menu bar, click on properties and click on COM Security.

Step 5 Make sure that the CDA account for both Access and Launch has Allow permissions. The Active Directory user should be added to all the four options (Edit Limits and Edit Default for both Access Permissions and Launch and Activation Permissions). See Figure 2-2.

Step 6 Allow all Local and Remote access for both Access Permissions and Launch and Activation Permissions.

Figure 2-2 My Computer Properties

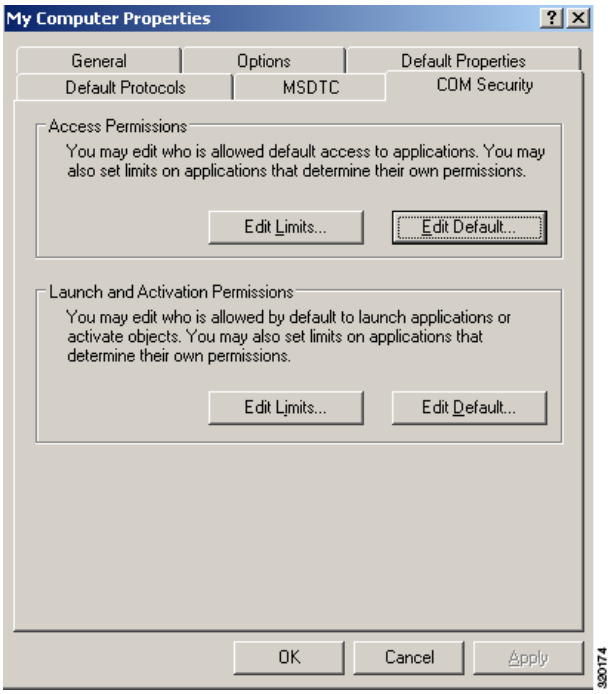


Figure 2-3 Local and Remote Access for Access Permissions

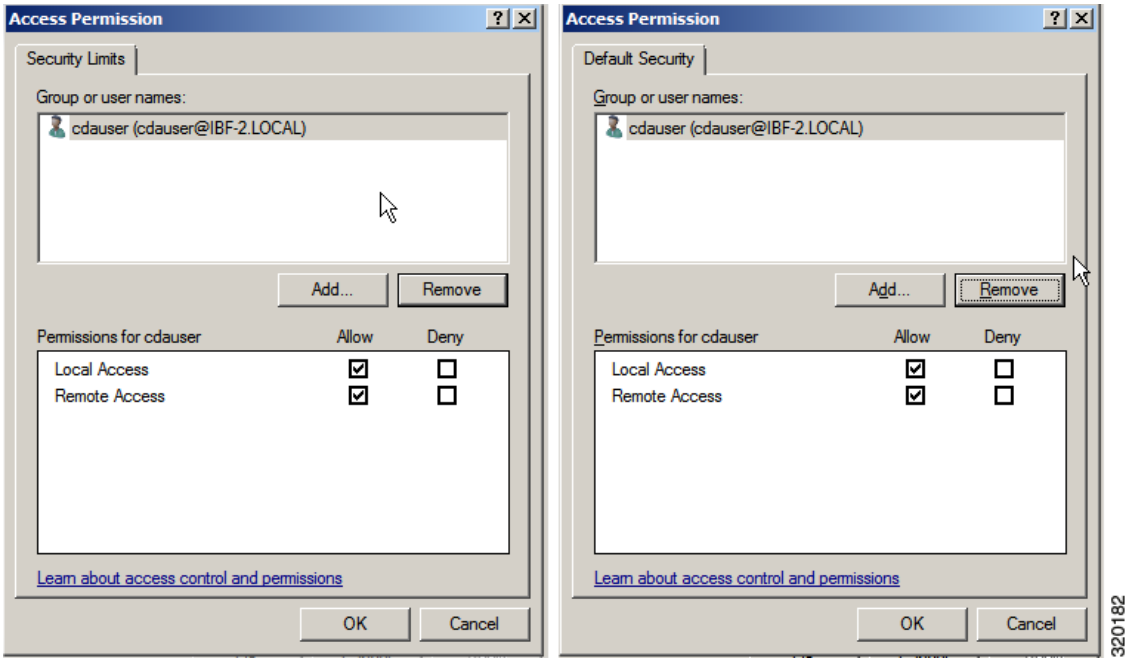
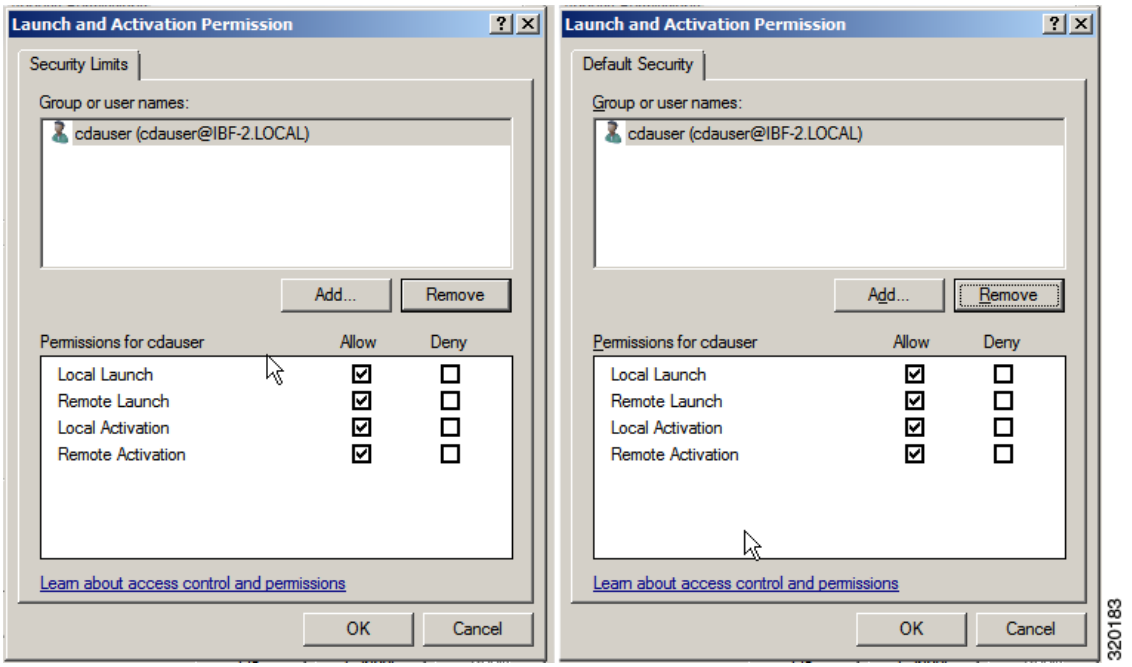


Figure 2-4 Local and Remote Access for Launch and Activation Permissions



Permissions to the WMI Root\CIMv2 Name Space

The Active Directory users do not have the Execute Methods and Remote Enable permissions by default. These can be granted by using the wmimgmt.msc MMC console.

Step 1 Click **Start > Run** and type wmimgmt.msc.

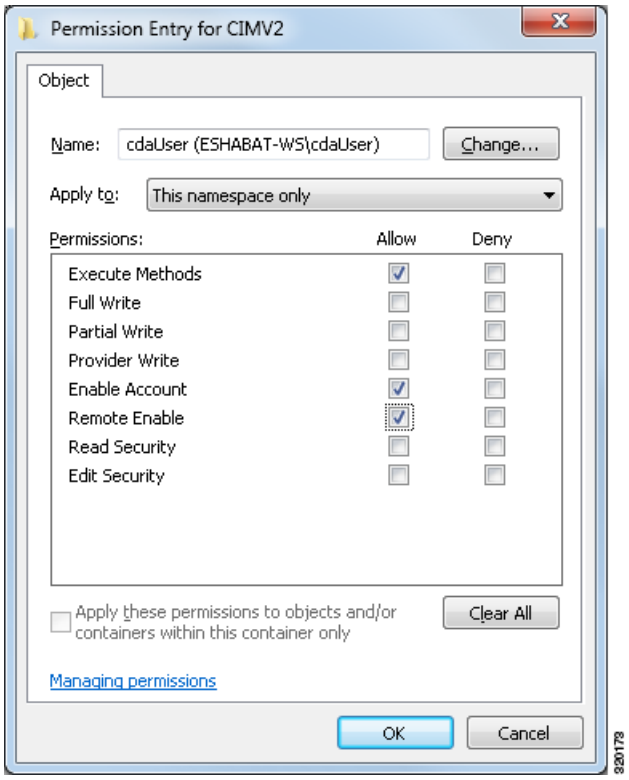
Step 2 Right-click WMI Control and click **Properties**.

Step 3 Under the Security tab expand Root and choose CIMV2.

Step 4 Click Security.

Step 5 Add the Active Directory user and give the required permissions as shown in Figure 2-5

Figure 2-5 Required Permissions for WMI Root\CIMv2 Name Space



Access to Read the Security Event Log of the Active Directory Domain Controller

On Windows 2008 and later, this can be done by adding the user to a group called Event Log Readers.

On all older versions of Windows, this can be done by editing a registry key in the following way:

Step 1 Find the SID for the account in order to delegate access to the Security event logs.

Step 2 Use the following command from the command line, as shown in Figure 2-6 to list all the SID accounts:

```
wmic useraccount get name,sid
```

You can also use the following for a specific username and domain:

```
wmic useraccount where name="cdaUser" get domain,name,sid
```

Step 3 Find the SID open Registry Editor and browse to the following location:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog

Step 4 Click on Security and double click CustomDS. See Figure 2-7.

For example, to allow read access to the cda_agent account (SID - S-1-5-21-1742827456-3351963980-3809373604-1107), enter (A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)

Step 5 Restart the WMI service on the DC. You can restart the WMI services in the following two ways:

a. Run the following command from the CLI,

```
net stop winmgmt
net start winmgmt.
```

b. Run Services.msc (This opens the Windows Services Management window)

In the Windows Services Management window, locate "Windows Management Instrumentation" service, right click and select Restart.

Figure 2-6 List All the SID Accounts

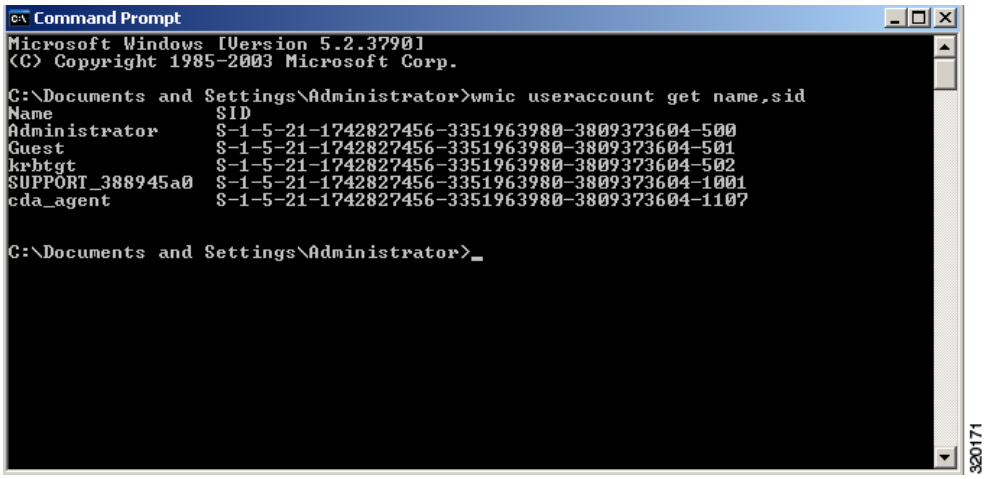
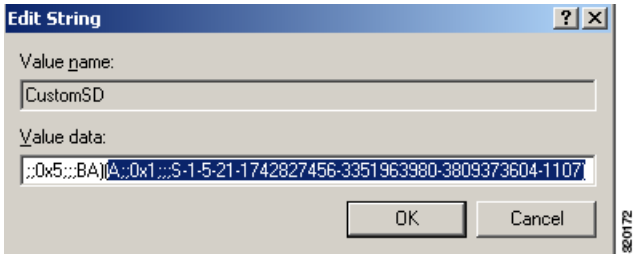


Figure 2-7 Edit CustomSD String



Installing Context Directory Agent

Context Directory Agent is packaged as an ISO image. You can download the package from Cisco.com and install it on a dedicated X86 machine or a VMWare ESX server.

CDA supports VMWare ESX versions 4.0, 4.1, and 5.0.

If you are installing CDA on a VMWare:

- You must select **Use Guest OS as Linux CentOS 4/5 32 bit**. Misconfiguration of the guest OS might result in very low performance.
- You must select LSI Logic Parallel as the SCSI controller.
- VMWare tools are automatically installed.

To install the Context Directory Agent, complete the following steps:

Step 1 Download the CDA ISO image, *cda-1.0.0.xxx.i386.iso* and save it in your local repository.

Step 2 Burn the ISO image on a DVD.

Step 3 Insert the DVD, choose the option to install the image from the optical drive.

The CDA package installation begins. After the installation is complete, the machine is rebooted. The following prompt is displayed when the boot sequence is completed:

```
*******************************************
Please type 'setup' to configure the appliance
*******************************************
```

The boot sequence takes about two minutes to complete.

Step 4 At the prompt, enter 'setup' to start the Setup program. You are prompted to enter networking parameters and first credentials.

The following illustrates a sample Setup program and default prompts:

```
localhost.localdomain login: setup
Press 'Ctrl-C' to abort setup
Enter Hostname[]: cda-server
Enter IP Address []: 192.168.10.10
Enter IP netmask []: 255.255.255.0
Enter IP default gateway []: 192.168.10.100
Enter default DNS domain []: cisco.com
Enter primary nameserver []: 200.150.200.150
Enter secondary nameserver? Y/N: n
Enter primary NTP server [time.nist.gov]: clock.cisco.com
Enter secondary NTP server? Y/N: n
Enter system timezone [UTC]: UTC
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up the network interface...
Pinging the gateway...
Pinging the primary nameserver...
```

```
Do not use 'Ctrl-C' from this point on...
Installing applications...
Installing cda...
Pre install
Post Install

Application bundle (cda) installed successfully
=== Initial setup for application: cda ===
Generating configuration...
Rebooting...
```

Step 5 Install the CDA patch 2. See Installing Context Directory Agent 1.0, Patch 2, page 2-14.

Step 6 You can log in to the CDA CLI after the machine is rebooted and verify the package installation. The following illustrates a sample verification procedure:

```
# login: admin
/admin# show application
<name> <description>
cda Cisco Context Directory Agent
/admin# show application status cda

CDA application server is running PID:2840
```

Step 7 You can now log in to the CDA user interface and start configuring your CDA.

Note The username and password specified during the initial setup program can be used for both the CLI and the GUI. If you change the GUI password using the user interface, the CLI password does not change and vice versa.

Related Topics:

- Supported Operating Systems, page 2-1
- Hardware Requirements, page 2-2
- Connectivity Requirements, page 2-3
- Active Directory Requirements for Successful Connection with CDA, page 2-4

Installing Context Directory Agent 1.0, Patch 2

You can download and install CDA 1.0, patch 2 from Cisco.com.

Step 1 Create a repository which will allow you to upload the patch into CDA. Refer to "repository" section on page 4-112 for instructions on how to create a repository.

Step 2 Download the CDA patch 2 to the repository created.

Step 3 Install the CDA patch 2, as described in "patch install" section on page 4-28.

Step 4 Verify that the patch is installed as follow:

```
/admin# sh application version cda

Cisco Application Deployment Engine OS Release:
ADE-OS Build Version:
ADE-OS System Architecture: i368

Copyright (c) 2005-2011 by Cisco Systems, Inc.
All right reserved.
Hostname: pmbu-ibf--pip08

Version information of installed applications
---------------------------------------------

Cisco Context Directory Agent
---------------------------------------------
Version      : 1.0.0.011
Build Date   : Tue May  8 15:34:26 2012
Install Date : Tue Jan 17 08:53:18 2014

Cisco Context Directory Agent
---------------------------------------------
Version      : 2
Build number : NA
Install Date : Mon Feb 3 09:35:09 2014
```

Migrating from AD Agent to CDA

CDA is compatible with AD agent. If AD Agent is already deployed in the network, you can replace it by CDA with a similar corresponding configuration, without requiring software changes or upgrades in other components of the Identity Based Firewall solution—Active Directory servers and Identity consumer devices (ASA/WSA).

Before you transition from AD Agent to CDA, take a note of the following AD Agent configuration details:

- General configuration options:

  Use the AD agent command **adacfg options list**
- Syslog servers, including IP Address and facility:

  Use the AD agent command **adacfg syslog list**
- Connected Active Directory DC list, including username, password, host and domain FQDNs:

  Use the AD agent command **adacfg dc list** (does not show the password.)
- Consumer devices (or subnets), including IP Address/subnet, shared secret:

  Use the AD agent command **adacfg client list** (does not show the shared secret.)

See the *Installation and Setup Guide for the Active Directory Agent, Release 1.0* for all the syntax and output examples for the above commands.

Install and configure CDA to correspond to your existing AD Agent application.

- Optionally configure the Active Directory General Settings. AD monitoring in the CDA is the equivalent of **dcStatusTime** in AD agent (note that the 10 seconds default in CDA is different from the 60 seconds default in AD agent.)

  History in CDA is the equivalent of **dcHistoryTime** in AD agent (note the 10 minutes default in CDA is different than the 24 hours default in AD Agent)

  User logon expiration period in CDA is the equivalent of **userLogonTTL** in AD agent (here the 24 hours default remains the same).
- Set the security policy on the DC machines. The differences between the AD agent and CDA with respect to Active Directory security policy setting is applicable only for Windows 2008R2 servers. For CDA, set the account permission on Microsoft Windows 2008 R2 server as described in Step 2 of "Adding and Editing Active Directory Servers" section on page 6.
- Optionally, configure the Log Level setting in CDA to correspond to **logLevel** in AD Agent.
- Optionally, add any syslog servers from **adacfg syslog list** to CDA.
- Add all Active Directory Servers from **adacfg dc list** to CDA.
- Add all Identity Consumers from **adacfg client list** to CDA.

If you are replacing the AD agent server with the CDA server, using the same hostname/IP Address, no changes are required in the consumer device (ASA/WSA) configuration, and consumer devices automatically connect to the CDA to retrieve identify mapping information.

If it is otherwise and you are newly adding a CDA server in your deployment, you have to update the configuration on the consumer device, to point to the new CDA server. For more information, refer to the ASA and WSA documentation on Cisco.com.