

The logo for Ecora, featuring the word "ecora" in a white, lowercase, sans-serif font on a dark blue background.

# **Ecora Auditor System Requirements**

**Auditor Professional v4.5 Service Pack 2**

**Copyright 2008**

Ecora, Ecora Auditor Professional, Ecora Auditor Basic, Auditor Professional Executive Dashboard, Ecora Patch Manager, ecora.com, and the names of Ecora products referenced herein are either trademarks and/or service marks or registered trademarks of Ecora Corporation.

Cisco, Cisco Systems, Cisco IOS, and CiscoLink are registered trademarks of Cisco Systems, Inc. or its affiliates in the US or certain other countries.

Lotus is a registered trademark and Domino and Notes are registration-pending trademarks of Lotus Development Corporation.

SQL Server, Visio, and BackOffice are either trademarks or registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation.

Sun, Sun Microsystems, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the US and other countries.

Novell and Cambridge Technology Partners are registered trademarks of Novell, Inc. in the United States and other countries.

Other product, operating system, application, and company names mentioned herein may be trademarks and/or service marks of their respective owners.

---

## Table of Contents

<b>Generic Requirements for All Modules .....</b>	<b>6</b>
Auditor Console — Installation System .....	6
Database Considerations .....	7
SQL Server.....	7
Oracle.....	7
Optional — Distribution .....	8
<b>Active Directory Module .....</b>	<b>9</b>
Auditor Console — Installation System .....	9
Target Systems.....	9
Supported/Reported .....	9
<b>Check Point Module .....</b>	<b>10</b>
Target Systems.....	10
Supported/Reported .....	10
<b>Cisco Module .....</b>	<b>11</b>
Target Systems.....	11
Supported/Reported .....	11
<b>Cisco PIX Module .....</b>	<b>12</b>
Target Systems.....	12
Supported/Reported .....	12
<b>Citrix Module .....</b>	<b>13</b>
Target Systems.....	13
Supported/Reported .....	13
<b>IBM DB2 Module.....</b>	<b>14</b>
Auditor Console — Installation System .....	14
Target Systems.....	14
Supported/Reported .....	14
<b>Domino Module.....</b>	<b>15</b>
Auditor Console — Installation System .....	15
Target Systems.....	15
Supported/Reported .....	15
<b>Exchange Module.....</b>	<b>16</b>
Auditor Console — Installation System .....	16

---

---

Target Systems.....	16
Supported/Reported .....	16
<b>MS IIS Module .....</b>	<b>17</b>
Auditor Console — Installation System .....	17
Target Systems.....	17
Supported/Reported .....	17
<b>MS SQL Module .....</b>	<b>18</b>
Auditor Console — Installation System .....	18
Target Systems.....	18
Supported/Reported .....	18
<b>Novell Module.....</b>	<b>19</b>
Auditor Console — Installation System .....	19
Target Systems.....	19
Supported/Reported .....	19
<b>Oracle Module.....</b>	<b>20</b>
Auditor Console — Installation System .....	20
Target Systems.....	20
Supported/Reported .....	20
<b>SAN/NAS Collector.....</b>	<b>21</b>
Auditor Console — Installation System .....	21
Target Systems.....	21
Supported/Reported .....	21
<b>Unix Module .....</b>	<b>22</b>
Auditor Console — Installation System .....	22
Target Systems.....	22
Supported/Reported .....	22
<b>VMware Module .....</b>	<b>23</b>
Auditor Console — Installation System .....	23
Target Systems.....	23
Supported/Reported .....	23
<b>Windows Module .....</b>	<b>24</b>
Auditor Software — Installation System.....	24
Target Systems.....	24

---

---

Supported/Reported .....	24
<b>Ecora Compliance Center (ECC) .....</b>	<b>25</b>
Installation System .....	25
Database Considerations .....	25
<b>Ecora Executive Dashboard .....</b>	<b>26</b>
Installation System .....	26
Database Considerations .....	26
SQL Server .....	26
Oracle .....	27
<b>Auditor Agent .....</b>	<b>28</b>
Windows .....	28
Installation Systems .....	28
Unix .....	28
Installation Systems .....	28
Installation System .....	29
Supported .....	29

## Generic Requirements for All Modules

### Auditor Console — Installation System

- Microsoft Windows 2000, Windows XP, Windows 2003, Windows Vista
- Pentium IV 1.7GHz or higher

**Recommendations:**

- 50 systems or fewer, 1.7 GHz or faster processor
- 50-100 systems, 2.0 GHz or faster processor
- 100 systems or more, 2.5 GHz or faster processor

- 1GB RAM or greater

**Recommendations:**

- 50 systems or fewer, 1GB RAM
- 50-100 systems, 2GB RAM
- 100 systems or more, 4GB RAM or more
- If hosting SQL database, 4GB RAM or more

**Note:** In addition to CPU speed and available RAM, network traffic and resource utilization (such as how many other application are running on the installed system) also affect performance.

- Screen resolution of 1024 x 768 or higher
- Microsoft .NET 2.0
- Swap file of 2GB or more (or twice the RAM, whichever is higher)
- ~200MB free disk space available to install software (100MB to run)
- Sufficient disk space for collected configuration data and generated reports (on installation system or storage system):

**Disk usage per system:**

- ~3MB per system per collection
- ~1MB per system reported by full configuration report

**Note:** Disk usage values are conditional on enabled/disabled collection options and system type.

- Microsoft Internet Explorer 6.0 or higher
- MDAC 2.7 or higher
- Microsoft Installer (MSI)
- Remote Registry Service should be up and running
- On a Windows Vista machine, either User Account Control has to be turned off for a current user account (even if the user account has Administrative rights), or else the Run this program as an administrator check box on the Compatibility tab of the Shortcut Properties dialog box must be checked.

- To view .CSV files, MS Excel or another spreadsheet program capable of displaying comma-delimited files must be installed.
- To view .PDF files, Adobe Reader or another program that reads PDFs.
- To use SNMP alerts, an SNMP manager (v2c traps) must be available on the network.
- To use email (SMTP) alerts, a mail server must be available on the network.
- To use NetSend alerts, Windows Messenger Service must be running.
- To use syslog alerts, there must be a machine configured with a syslog daemon running

## Database Considerations

### SQL Server

- Microsoft SQL Server (2000 SP4, 2005) or MSDE for the data repository.
- Microsoft's requirements for SQL are available at:
  - o <http://www.microsoft.com/sql/prodinfo/sysreqs/default.mspx>
  - o ~60MB free disk space available, if you are installing MSDE

**Note:** MSDE is a free Microsoft database with a 2.0GB data limit, making it a viable option for testing the database functionality in small environments. MSDE can be upgraded to SQL Server at any time (without any data loss).

- o Sufficient disk space for collected data:
- o Disk usage per system:
- o ~3MB of database space per system per collection

**Note:** Microsoft requires twice the database size available for the transaction log during delete actions.

### Oracle

- Oracle Database (9i, 10g, 11g Standard, Enterprise or Express edition) for the data repository.
  - o Oracle Database 10 G Express Edition is a free to deploy small-footprint (~120MB) entry-level database with a 4Gb data space limitation, available at:
  - o <http://www.oracle.com/technology/software/products/database/xe/htdocs/102xewinsoft.html>
- Sufficient free disk space for collected data:
  - o ~80MB of server disk space per Auditor module for the pre-created database objects.
  - o ~3MB of server disk space per system per collection
- Oracle client software supplied with the server distribution must be installed on the Auditor console with Oracle Network Utilities and Oracle Call Interface options turned on. The latest versions of Oracle ODBC drivers are also available at:
  - o <http://www.oracle.com/technology/software/tech/windows/odbc/index.html>

## Optional — Distribution

- For web-based distribution of reports, a Microsoft IIS web server with file access to the web server content regions is needed.

---

## Active Directory Module

### Auditor Console — Installation System

- NetBIOS protocol support (unless the installation machine is a member of an Active Directory forest)
- For initial domain controller discovery:
  - If NetBIOS is enabled — The computer with Auditor software installed may be a member of any domain (as long as the user has permissions to the Active Directory domain controller).
  - If NetBIOS is disabled on the domain controller or the computer with Auditor software installed:
    - 1. The computer with Auditor software installed must be a member of the Active Directory domain.
    - 2. The DNS settings on the computer with Auditor software installed must point to a DNS server within the Active Directory domain; otherwise a Domain Disabled message will result.

Domain Disabled – This message indicates that the Auditor software cannot find a domain controller in the Active Directory domain. Please verify that all system requirements above are met.

### Target Systems

- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- NetBIOS (over TCP/IP) protocol support or AD
- Domain, Local, or Enterprise Administrator permissions for all the domains containing systems you want to collect

**Note:** To report on machines in WorkGroups, you must have an administrator account on all machines to be reported that matches the login/password of the domain administrator account of the domain in which the machine with the software is installed.

### Supported/Reported

- Active Directory 2000, 2003

---

## Check Point Module

### Target Systems

- Read permissions for collection
- Remote registration of OPSEC applications should be allowed on the SmartCenter server
- Administrator permissions for registering OPSEC application
- Requirements on the Smart Center Server
  - Add host name (Host Name or IP address of the computer where Auditor is installed) to GUI clients tab in the Check Point Configuration Utility
  - Allow remote registration of OPSEC products must be checked on the Policy\Global Settings\OPSEC node in Check Point SmartDashboard. (If SmartDashboard is not used, then remote registration of OPSEC products should be manually registered in the config file).
  - Save changes and close SmartDashboard and Configuration utilities.
- Instructions for adding Check Point Smart Center servers to Auditor software for collection.

From the Data collection dialog box:

1. Click New.
2. On the Server tab, specify the Smart Center server name, administrator name and password.
3. Make sure SmartDashboard is closed; then, on the OPSEC Application tab, click the Initialize button. Then, in the Communication dialog box, specify the administrator name and password. (After successful registration, all boxes on OPSEC Application tab will be filled automatically.)

### Supported/Reported

- Check Point VPN-1/Firewall-1 NGX R60, R65

## Cisco Module

### Target Systems

- RPC Service
- Routers & Layer 3 Switching Devices/Modules (RSM, RSFC, MSFC) running Cisco IOS® version 12.2, 12.3
- Access to Privileged EXEC Mode or a security level with access to the following commands: show version, show running-config, and show startup-config on all devices to be documented

### Supported/Reported

- Cisco IOS® versions 12.x

---

## Cisco PIX Module

### Target Systems

- RPC Service
- PIX firewalls running Cisco PIX OS version 5.x, 6.x, ASA 7.x
- Access to Privileged EXEC Mode or a security level with access to the following commands: show version, show running-config, and show startup-config on all devices to be documented

### Supported/Reported

- Cisco PIX OS version 5.x, 6.x, ASA 7.x

## Citrix Module

### Target Systems

- Remote Registry Service must be enabled
- RPC Service
- Server Service
- Citrix MetaFrame XP SP3 or higher
- View-only administrator rights

### Supported/Reported

- Citrix MetaFrame XP SP3, Citrix Presentation Server 3.0, 4.0, 4.5

---

## IBM DB2 Module

### Auditor Console — Installation System

- NetBIOS (over TCP/IP) protocol support
- DB2 Administration Client v.8.1.7 (or higher) with OLE DB Client support

### Target Systems

- View-only administrator rights
- DAS (DB2 Administration Server) service should be up and running
- Following TCP ports should be open for both incoming and outbound requests:
  - 523 – utilized by DAS service
  - 50000, 50001, 50002, 50003 etc. (could differ, as it depends on the total number of DB2 instances being executed simultaneously and their settings) – if a TCP/IP connection is used
  - 137-139 – if a NETBIOS connection is used

### Supported/Reported

- IBM DB2 UDB v8.1 and higher

---

## Domino Module

### Auditor Console — Installation System

- Lotus Notes 4.6.x client or higher (you will be prompted for a Notes client password)
- Lotus Notes program directory in the path statement

**Note:** If you have to edit your path statement, restart the client machine before attempting to collect data.

- Read Access to the Domino Directory (Address Book)

### Target Systems

- Read Access to the Domino Directory (Address Book)
- Remote Registry Service enabled
- RPC Service
- Server Service enabled

### Supported/Reported

- IBM Lotus Domino Server 4.6.x, R5x, 6.x or 7.x

---

## Exchange Module

### Auditor Console — Installation System

- NetBIOS (over TCP/IP) protocol support
- Exchange Administrative permissions are required
- Outlook 2000 or above is required for additional mailbox or public folder information
- The Outlook profile must have local admin privileges and an Exchange mailbox with Exchange administrative rights for additional mailbox or public folder information
- Exchange 5.5 only:
  - Exchange Administrator 5.5 must be installed
  - If Outlook 2003 is installed, Exchange Administrator 5.5 must be installed from the Exchange 2000 or 2003 CD
- Exchange 2000/2003/2007 only:
  - Exchange System Manager
  - If Outlook 2000 is installed, the public folder attributes Deleted Items and Size of Items are not collected
  - If Outlook 2003 is installed, the Exchange System Manager is required to collect additional mailbox information

### Target Systems

- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- NetBIOS (over TCP/IP) protocol support

### Supported/Reported

- 5,5 (Gold, All SPs)
- 2000 (Gold, All SPs)
- 2003 (Gold, All SPs)
- 2007 (Gold, SP1)

---

## MS IIS Module

### Auditor Console — Installation System

- IIS common files
- NetBIOS (over TCP/IP) protocol support

### Target Systems

- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- NetBIOS (over TCP/IP) protocol support
- Operator rights to the IIS servers reported
- IIS Management Script and Tools installed (IIS 7.0 only)

### Supported/Reported

- IIS 4, 5, 5.1, 6, 7

---

## MS SQL Module

### Auditor Console — Installation System

- Microsoft SQL Client with net libraries (Named Pipes, TCP/IP etc.)
- SQL Database Administrator rights

### Target Systems

- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- Read rights on SQL servers

### Supported/Reported

- MS-SQL server 2000, 2005

## Novell Module

### Auditor Console — Installation System

- Novell NetWare client version 5.1, 6.0, 6.5 or higher

### Target Systems

- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- Console Operator access
- Supervisor rights to the portion of the NDS tree to report

### Supported/Reported

- Novell NetWare Server 5.1, 6.0, 6.5, Open Enterprise Server (V1, V2)

---

## Oracle Module

### Auditor Console — Installation System

- Oracle client version 9i, 10g, 11g with Oracle Networking components installed

**Note:** Oracle client version 9i for reporting 9i databases, 10g for reporting 10g database, 11g for reporting.

### Target Systems

- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- Oracle instance
- Database user account with the following:
  - CONNECT - role
  - or
  - SELECT ANY DICTIONARY - system privilege

### Supported/Reported

- Oracle instances (9i, 10g, 11g) running on any operating system (i.e. Sun Solaris, IBM AIX, and HPUX)

## **SAN/NAS Collector**

### **Auditor Console — Installation System**

- No specific pre-requisites
- SMI-S credentials for target device(s)

### **Target Systems**

- SMI-S provider installed and configured

### **Supported/Reported**

- Supports any SMI-S compliant device (Netapp and EMC tested)
- All “Block-Book” defined SMI-S Parameters

## Unix Module

### Auditor Console — Installation System

- Microsoft .Net 3.0 to support Agent Manager

### Target Systems

- Shell-level access to each target system using a standard user account
  - The user account startup must be non-interactive. No user input is required to get to a standard shell command line.
  - When the user account on the target system is a member of group sys, more configuration data can be reported.
  - When the root password is provided, the user account is used to make the initial connection and the /bin/su command is issued to become root. If the root password is not provided, only the data available to the user account can be reported. You can set up and use SUDO for collecting the data available to root.
- Each target system must support ssh (preferred) or telnet communications

### Supported/Reported

- Solaris 8, 9, 10
- HPUX 11, 11i
- AIX 4.3, 5.1, 5.3
- Red Hat Enterprise Linux 2.1, 3.0, 4.0, 5.0 (AS/EW/WS)
- Red Hat Linux 9
- Novel SuSE Enterprise Linux 9.x, 10.x
- openSUSE 10.2
- CENT OS 5.1
- Fedora 5, 6, 7, 8
- Linux Oracle EL 5

---

## VMware Module

### Auditor Console — Installation System

- VMware VmCOM Scripting API
- Read access to the VMware ESX Server

### Target Systems

- VMware VmCOM Scripting API

### Supported/Reported

- VMware Servers ESX 2.5, ESX 3.0.x, ESX 3.5

---

## Windows Module

### Auditor Software — Installation System

- NetBIOS (over TCP/IP) protocol support
- Microsoft .Net 3.0 to support Agent Manager
- To collect and report domain and system level information completely in one report:
  - Client for Microsoft Networks
  - RPC Service

### Target Systems

- Remote Registry Service enabled
- RPC Service
- WMI Service
- Server Service enabled
- File & Print sharing for Microsoft Networks protocol enabled
- NetBIOS (over TCP/IP) protocol support or Active Directory
- To collect and report domain and system level information completely in one report:
  - Client for Microsoft Networks
  - RPC Service
- Domain, Local, or Enterprise Administrator permissions for all the domains containing systems you want to collect

**Note:** To report on machines in WorkGroups, you must have an administrator account on all machines to be reported that matches the login/password of the domain administrator account of the domain in which the machine with the software is installed.

### Supported/Reported

- Windows XP (SP1, SP2, SP3)
- Windows 2000 (SP4)
- Windows 2003 (Gold, SP1, SP2)
- Windows Vista (Gold, SP1, 64bit SP1)
- Windows 2008 (Standard, Standard 64 bit, Enterprise, Enterprise 64 bit, DataCenter, DataCenter 64 bit)

---

## Ecora Compliance Center (ECC)

### Installation System

- 1800 MHz CPU or higher
- 512MB RAM or greater

**Note:** In addition to CPU speed and available RAM, network traffic and resource utilization (such as how many other applications are running on the installed system) also affect performance.

- Microsoft Windows 2000 Server SP4 or higher, Windows 2003 SP1 or higher
- MS IIS version 5.0 or higher
- MS .NET Framework 2.0
- Microsoft Installer (MSI)
- ~50MB free disk space available for the software

**Note:** Additional space for logs and saved reports might be required later.

- Valid user account with administrator access rights in the database instance on the target machine with Ecora Compliance Center installed.

**Note:** If Auditor installation is using a remote MS SQL database with Windows authentication, the respective domain account should be manually specified for the Ecora Compliance Center service (Log On as).

- Internet Explorer 6.0 SP1 or higher, Mozilla Firefox 2.0 or higher, or Opera 9.22 or higher
- Screen resolution of 1024 x 768 or higher

### Database Considerations

- Microsoft SQL Server (2000 SP4, 2005) or MSDE for the data repository.
- Microsoft's requirements for SQL are available at:
  - <http://www.microsoft.com/sql/prodinfo/sysreqs/default.mspx>
  - ~60MB free disk space available, if you are installing MSDE

**Note:** MSDE is a free Microsoft database with a 2.0GB data limit, making it a viable option for testing the database functionality in small environments. MSDE can be upgraded to SQL Server at any time (without any data loss).

---

## Ecora Executive Dashboard

### Installation System

- 1800 MHz CPU or higher
- 512MB RAM or greater

**Note:** In addition to CPU speed and available RAM, network traffic and resource utilization (such as how many other applications are running on the installed system) also affect performance.

- Microsoft Windows 2000 SP4 or higher, Windows 2003, Windows XP Professional
- MS IIS version 5.0 or higher
- MS .NET Framework 1.1
- MDAC 2.7 or higher
- Internet Explorer 6.0 or higher
- Microsoft Installer (MSI)
- ~200MB free disk space available for the software.

**Note:** Additional space for logs and saved reports might be required later.

- Valid user account with administrator access rights in the instance on the target machine where the web console is installed
- Screen resolution of 1024 x 768 or higher

### Database Considerations

#### SQL Server

- Microsoft SQL Server 2000SP4/MSDE or higher for the database
  - Resource: Microsoft's requirements for SQL are available at:
    - <http://www.microsoft.com/sql/prodinfo/sysreqs/default.msp>
- MS SQL/MSDE security considerations. User account for the Ecora Executive Dashboard must have db\_datareader, db\_datawriter, and db\_ddladmin roles for the Dashboard and Auditor databases.
  - To create a new database, the account must have dbcreator or sysadmin role.
  - Using a Windows account and Windows authentication mode, this account must have Logon as a service privilege on the computer. On Microsoft Windows 2000 systems, the account must also have Act as part of operating system privilege.
- Using a remote SQL engine, network access through named pipes and TCP/IP must be granted to the engine on that computer.
  - If the remote computer is protected by a firewall, the SQL engine must be allowed on the firewall.

---

## Oracle

- ❑ Oracle Database (9i, 10g, 11g Standard, Enterprise or Express edition).
  - Oracle Database 10 G Express Edition is a free to deploy small-footprint (~120MB) entry-level database with a 4Gb data space limitation, available at:
  - <http://www.oracle.com/technology/software/products/database/xe/htdocs/102xewinsoft.html>
- ❑ Oracle client software supplied with the server distribution must be installed on the Auditor console with Oracle Network Utilities and Oracle Call Interface options turned on. The latest versions of Oracle ODBC drivers are also available at:
  - <http://www.oracle.com/technology/software/tech/windows/odbc/index.html>

---

## Auditor Agent

### Windows

#### Installation Systems

- Microsoft Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 2008
- 1.7GHz CPU or better
- 512MB RAM or greater
- Swap file of 1GB or more (or twice the RAM, whichever is higher)
- ~50MB free disk space available to install software (and 50MB to run it)
- Sufficient disk space for collected configuration data:
- Disk usage:
  - ~1MB per collection

**Note:** Disk usage values are conditional on enabled/disabled collection options and system type.

- Microsoft .NET 2.0
- TCP port that is manually specified by the user at install time must be open for outbound connections.

### Unix

#### Installation Systems

- RedHat versions with kernel version 2.6 or later.\*
- Solaris version 10 (Intel and SPARC.)

\* Limited support for kernel version 2.4.2 available by request. Ask your account representative.

## ITSM Connector

### Installation System

- Ecora Auditor 4.5
- IIS 5 or later
- Microsoft .NET Framework 2.0
- Microsoft WSE 3.0
- If HP Service Desk 4.5 is the target ITSM application, then the JRE 1.4 or higher should be installed.

### Supported

- HP Service Desk 4.5 Service Pack 19 - 24
- Service-Now Fall 2007, Spring 2008
- BMC Service Desk Express 9.6
- BMC Remedy 6.3/CMDB 1.1
- BMC Remedy 7 (7.0, 7.1)/CMDB 2.0

## Ecora Contact Information

### Global Headquarters

Address: 2 International Drive  
Portsmouth, New Hampshire, 03801  
Phone: 603.436.1616  
877.923.2672 (main)  
603.436.1604 (fax)

### Boston Metro Office

One Burlington Business Center  
67 South Bedford Street  
Suite 301E  
Burlington, MA 01803

## Sales

### North America

Phone: 877.923.2672  
Fax: 603.436.1604  
Email: sales@ecora.com

### US Federal Programs, Projects, and Integrators

Phone: 603.334.3186  
Email: sales\_gov@ecora.com

### International Sales

Phone: +1 603 334 3141  
Email: Sales\_International@ecora.com

## Support

### Ecora Support Self-Service Web Portal

<https://na4.salesforce.com/sserv/login.jsp?orgId=00D300000006EBT>

### Phone Support

Monday – Friday, 8am – 8pm, EST  
1.603.436.1616  
1.877.92.ECORA (1.877.923.2672) Ecora Software