
Ecora Auditor Professional

System Requirements for Version 4.5

January 2008

Table of Contents

1.	Generic Requirements For All Modules.....	4
1.1.	Auditor Console — Installation System	4
1.2.	Database Considerations.....	5
1.3.	Optional — Distribution	5
2.	Active Directory Module.....	6
2.1.	Auditor Console — Installation System	6
2.2.	Target Systems.....	6
2.3.	Supported/Reported.....	6
3.	Check Point Module.....	7
3.1.	Target Systems.....	7
3.2.	Supported/Reported.....	7
4.	Cisco Module	8
4.1.	Target Systems.....	8
4.2.	Supported/Reported.....	8
5.	Cisco PIX Module	9
5.1.	Target Systems.....	9
5.2.	Supported/Reported.....	9
6.	Citrix Module.....	10
6.1.	Target Systems.....	10
6.2.	Supported/Reported.....	10
7.	IBM DB2 Module.....	11
7.1.	Auditor Console — Installation System	11
7.2.	Target Systems.....	11
7.3.	Supported/Reported.....	11
8.	Domino Module.....	12
8.1.	Auditor Console — Installation System	12
8.2.	Target Systems.....	12
8.3.	Supported/Reported.....	12
9.	Exchange Module.....	13
9.1.	Auditor Console — Installation System	13
9.2.	Target Systems.....	13
9.3.	Supported/Reported.....	13
10.	MS IIS Module.....	14
10.1.	Auditor Console — Installation System	14
10.2.	Target Systems.....	14
10.3.	Supported/Reported.....	14
11.	MS SQL Module.....	15
11.1.	Auditor Console — Installation System	15
11.2.	Target Systems.....	15
11.3.	Supported/Reported.....	15
12.	Novell Module.....	16
12.1.	Auditor Console — Installation System	16
12.2.	Target Systems.....	16
12.3.	Supported/Reported.....	16
13.	Oracle Module	17
13.1.	Target Systems.....	17
13.2.	Supported/Reported.....	17
14.	Unix Module	18
14.1.	Target Systems.....	18
14.2.	Supported/Reported.....	18
15.	VMware Module	19
15.1.	Auditor Console — Installation System	19

15.2.	Target Systems.....	19
15.3.	Supported/Reported.....	19
16.	Windows Module.....	20
16.1.	Auditor Software — Installation System.....	20
16.2.	Target Systems.....	20
16.3.	Supported/Reported.....	20
17.	Ecora Compliance Center (ECC).....	21
17.1.	Installation System.....	21
18.	Ecora Executive Dashboard.....	22
18.1.	Installation System.....	22
18.2.	Database Considerations.....	22
19.	Auditor Agent.....	24
19.1.	Installation Systems.....	24

1. Generic Requirements For All Modules

1.1. 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 1.1
- 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.

1.2. 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).

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

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

1.3. Optional — Distribution

- For web-based distribution of reports, a Microsoft IIS web server with file access to the web server content regions is needed.
- See separate requirements for Ecora Compliance Center (ECC).
- See separate requirements for Ecora Executive Dashboard.

2. Active Directory Module

2.1. 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.

2.2. 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.

2.3. Supported/Reported

- Active Directory 2000, 2003

3. Check Point Module

3.1. 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.)

3.2. Supported/Reported

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

4. Cisco Module

4.1. Target Systems

- RPC Service
- Routers & Layer 3 Switching Devices/Modules (RSM, RSFC, MSFC) running Cisco IOS® version 11.x or higher
- 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

4.2. Supported/Reported

- Cisco IOS® version 11.x or higher

5. Cisco PIX Module

5.1. Target Systems

- RPC Service
- PIX firewalls running Cisco PIX OS version 2.0-6.3
- 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

5.2. Supported/Reported

- Cisco PIX OS version 2.0-6.3

6. Citrix Module

6.1. Target Systems

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

6.2. Supported/Reported

- Citrix MetaFrame XP SP2, Citrix Presentation Server 3.0, 4.0

7. IBM DB2 Module

7.1. Auditor Console — Installation System

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

7.2. 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

7.3. Supported/Reported

- IBM DB2 UDB v8.1 and higher

8. Domino Module

8.1. Auditor Console — Installation System

- Lotus Notes 4.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)

8.2. Target Systems

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

8.3. Supported/Reported

- IBM Lotus Domino Server 4.x, R5x, 6.x or 7.x

9. Exchange Module

9.1. Auditor Console — Installation System

- NetBIOS (over TCP/IP) protocol support
- Exchange Administrative permissions are required
- Exchange 5.5 only:
 - Exchange Administrator 5.5 must be installed
 - 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
 - If Outlook 2003 is installed, Exchange Administrator 5.5 must be installed from the Exchange 2000 or 2003 CD
- Exchange 2000/2003 only:
 - Exchange System Manager
 - 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
 - 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

9.2. Target Systems

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

9.3. Supported/Reported

- Exchange 5.5
- Exchange 2000
- Exchange 2003

10. MS IIS Module

10.1. Auditor Console — Installation System

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

10.2. 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)

10.3. Supported/Reported

- IIS 4, 5, 5.1, 6, 7

11. MS SQL Module

11.1. Auditor Console — Installation System

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

11.2. Target Systems

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

11.3. Supported/Reported

- MS-SQL server 7.x, 2000, 2005

12. Novell Module

12.1. Auditor Console — Installation System

- Novell NetWare client version 4.6 or higher

12.2. 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

12.3. Supported/Reported

- Novell NetWare server 4, 5, 6

13. Oracle Module

Auditor Console — Installation System

- Oracle client version 8i, 9i or 10g with Oracle Networking components installed

Note: Oracle client version 8i for reporting 8i databases and 9i for reporting 9i databases, 10g for reporting 10g.

13.1. Target Systems

- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- Oracle instance
- Database user account with the following:
 - **8i:**
CONNECT - role
or
SELECT_ANY_TABLE - system privilege
 - **9i:**
CONNECT - role
or
SELECT ANY DICTIONARY - system privilege
 - **10g:**
CONNECT - role
or
SELECT ANY DICTIONARY - system privilege

13.2. Supported/Reported

- Oracle instances (7.3.x, 8.0.x, 8i, 9i) running on any operating system (i.e. Sun Solaris, IBM AIX, and HPUX)
- Oracle 10g compatible

14. Unix Module

14.1. 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

14.2. Supported/Reported

- Solaris 2.5.1 - 10
- HPUX 10.20, 11, 11i
- AIX 4.3 or higher
- Red Hat Enterprise Linux 2.1, 3.0, 4.0, 7.0 (AS/EW/WS)
- Red Hat Linux 7.0 or higher
- Novel SuSE Enterprise Linux 9 or higher

15. VMware Module

15.1. Auditor Console — Installation System

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

15.2. Target Systems

- VMware VmCOM Scripting API

15.3. Supported/Reported

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

16. Windows Module

16.1. Auditor Software — Installation System

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

16.2. Target Systems

- Remote Registry Service enabled
- RPC 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.

16.3. Supported/Reported

- Microsoft NT 4.0 SP4 or higher
- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows 2003
- Microsoft Windows Vista

17. Ecora Compliance Center (ECC)

17.1. 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 or Windows 2003 Server 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

18. Ecora Executive Dashboard

18.1. 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
- MSDE engine version 8 accessible
- 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.

- ~60MB free disk space available for MSDE installation

Note: Additional space for saved measurements will 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

18.2. Database Considerations

- Microsoft SQL Server 2000SP4 or higher for the database
 - MSDE is a free Microsoft database with a 2GB 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).
 - Resource: Microsoft's requirements for SQL are available at:
<http://www.microsoft.com/sql/prodinfo/sysreqs/default.mspx>
- MSDE (or MS SQL server) 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.

19. Auditor Agent

19.1. Installation Systems

- Microsoft Windows 2000, Windows XP, Windows 2003
- 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 1.1
- TCP port that is manually specified by the user at install time must be open for outbound connections.