

Security Best Practices for Cisco Intelligent Contact Management Software Release 6.0(0)

July 28, 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (64387)
Fax: 408 526-4100

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0401R)

Security Best Practices for Cisco Intelligent Contact Management Software Release 6.0(0)

Copyright © 2004, Cisco Systems, Inc.

All rights reserved

Table of Contents

Introduction	5
Windows 2000 Server.....	7
Operating System Installation	7
Services	8
Accounts, Passwords and Policies.....	13
File System and Registry	14
File System	14
Registry.....	18
Hardening against Network Attacks	20
TCP/IP Stack Hardening	20
Harden the Winsock Interface Driver.....	21
Harden Network Browser Interface	21
Harden against Anonymous access	21
WMI Service Hardening.....	22
SNMP Service Hardening	22
Hardening against Application Attacks.....	23
Application Accounts	23
Toll Fraud Prevention	27
Application Security and Passwords	28
IPSec and NAT Support	30
Support for IPSec (IP Security) in Tunnel Mode	30
Support for NAT (Network Address Translation)	30
Active Directory	32
SQL Server	36
Internet Information Server	39
ServletExec (New Atlanta)	46
Sybase EAServer (Jaguar).....	47
Tomcat	51
Internet Explorer	53
Remote Administration	55
Windows Terminal Services	55
Telnet.....	56
pcAnywhere	58
VNC.....	60
Microsoft Security Updates.....	61
Microsoft Service Pack Policy.....	62
Anti-Virus	63
Guidelines and Recommendations	63
VirusScan Enterprise 7.0.....	65
Trend ServerProtect 5.5	71
Intrusion Prevention System – CSA.....	76
Baseline – MBSA	77
Auditing	80
Other Security Considerations	82
Syskey	82
Third-Party Security Providers.....	82
Third-Party Management Agents	82
Appendix.....	84
Hardening the RMS Listener	84
References	85
Cisco Contact Center Applications Documentation.....	85

Cisco Intelligent Contact Management (ICM) Software.....	85
Cisco ICM WebView.....	85
Cisco ICM CTI Object Server (CTI OS).....	85
Cisco Agent Desktop (CAD).....	86
Cisco ICM Web Collaboration Option - Collaboration Server.....	86
Cisco ICM Web Collaboration Option - Media Blender.....	87
Cisco ICM Web Collaboration Option - Dynamic Content Adapter.....	87
Cisco ICM Internet Service Node (ISN).....	88
Cisco Customer Response Solutions (CRS).....	88
Support Tools.....	88
Cisco Security Agent.....	88
Third-Party Documentation.....	88
Operating System Installation.....	88
Active Directory.....	89
File System.....	89
WMI.....	89
SQL Server.....	90
Internet Information Server.....	90
Internet Explorer.....	90
Terminal Services.....	90
Revision History.....	91
Obtaining Technical Assistance.....	92
Cisco Technical Support Website.....	92
Submitting a Service Request.....	92
Definitions of Service Request Severity.....	92

Introduction

This document describes security hardening configuration guidelines for Cisco ICM software Release 6.0(0) in the Microsoft Windows 2000 Server environment. The term "ICM software" includes: IP Contact Center (IPCC) Enterprise Edition and ICM Enterprise Edition. Optional ICM applications applying to these server configurations are also addressed here, with the exception of the following: Web Collaboration Option Collaboration Server, Media Blender, Dynamic Content Adapter and E-mail Manager Option. The References section of this document provides information and links to all available security related content in the contact center documentation portfolio. References throughout this document to "ICM/IPCC" will assume the aforementioned configurations. Any accompanying applications making up the customer's particular solution, whether Cisco provided – such as PSO applications – or provided by a Cisco partner, have not been approved for use with these security hardening recommendations. Special testing and qualification must be considered to ensure that recommended security configurations do not hinder the operation of those applications.

The configurations presented in this document represent parameters used internally within Cisco to test the applications. Other than the base Operating System and applications' installations, any deviation from this set cannot be guaranteed to provide a compatible operating environment. It is important to note recommendations contained in this document will not always be uniformly implemented; some implementations – as based on corporate policy, specific IT utilities (e.g., backup accounts) or other external guidelines – may modify or limit the application of these guidelines. Finally, some implementation details are omitted in the interest of keeping content condensed; refer to the references section for step by step instructions on how to accomplish a certain task in a particular section.

It is assumed that the target reader of this document is an experienced administrator familiar with security ramifications of the default Windows 2000 Server installation. It is further assumed that the reader is fully familiar with the applications making up the ICM/IPCC solution, as well as with the installation and administration of these systems. It is the intent of these best practices to additionally provide a consolidated view of securing the various third-party applications on which the Cisco contact center applications depend. Should vendor recommendations differ from these guidelines, following such recommendations may result in systems that are not protected from malicious attacks.

The recommendations contained herein are based in part on hardening guidelines published by Microsoft, such as those found in the *Windows 2000 Security Hardening Guide*,¹ as well as other third-party vendors' hardening recommendations. A number of recommendations are made fully consistent with supporting Microsoft guidelines; our intent is to further interpret and customize those guidelines as specifically applicable to the ICM/IPCC server products. Where exceptions or specific recommendations are made, we strive to present the underlying rationale for the deviation.

This document should be used in conjunction with the Planning and Staging Guides that are part of the ICM/IPCC documentation. It should further be used as a reference standard for all customers requiring verification that certain security configuration changes to the base operating system and contact center application servers have been certified for use with the ICM/IPCC applications. The average time to execute the majority of the steps outlined in the document is 1.5 hours for database and web servers and 1.25 hours for the rest of the servers.

An adequately secure server configuration requires a multi-layered approach to protecting systems from targeted attacks and the propagation of viruses. A first approach is to ensure that the servers hosting the Cisco contact center applications are physically secure. They must be located in data centers to which only authorized personnel are provided access. Another level of security is the network segmentation of the servers, which is not addressed in this document. All servers discussed in this document are not internet-facing machines and therefore should be protected behind a secure network.

¹ See References

The table below outlines the various nodes of the application and which sections of this guide apply to it.

Nodes	Sections Applicability	
<ul style="list-style-type: none"> • CAD Servers • CTI OS Server • CTI Server • Distributor • Logger • Peripheral Gateway (PG) • Router 	Operating System Installation Services Accounts, Passwords and Policies File System and Registry Hardening against Network Attacks	Internet Explorer Remote Administration Microsoft Security Updates Anti-Virus Auditing
<ul style="list-style-type: none"> • Logger • Distributor (AW, HDS) 	All the above plus: SQL Server	
<ul style="list-style-type: none"> • Distributor or with WebView 	All the above plus: Internet Information Server ServletExec (New Atlanta) Sybase EAServer (Jaguar)	
<ul style="list-style-type: none"> • Distributor or with Internet Script Editor 	All the above plus: Internet Information Server	
<ul style="list-style-type: none"> • Distributor or with Support Tools 	All the above plus: Tomcat	
<ul style="list-style-type: none"> • Listener 	Hardening the RMS Listener	
<ul style="list-style-type: none"> • Domain Controller 	Active Directory	

Windows 2000 Server

Operating System Installation

The Windows 2000 install process is itself vulnerable to several known exploits until the installation has been completed, and all applicable service packs and hot fixes have been applied. The information presented here is designed to prevent these problems. All information contained herein applies to Microsoft Windows 2000 Server installs.

To ensure secure system installs, a system should not be available on the network until all of the following criteria are met:

- System has strong local administrator password (see *Accounts, Passwords and Policies* section)
- System has been upgraded to Service Pack 4 or higher²
- *File System and Registry* hardening guidelines have been implemented
- Internet Explorer 6.0, with the latest service pack and security updates, has been installed
- If applicable, IIS and other non-necessary services have been disabled (see *Services* and *Internet Information Server* sections)

A common security measure is to avoid upgrading from Windows NT 4.0 to Windows 2000. It is preferable to always perform a clean install of Windows 2000 followed by an install of any application software. A system with a previous install may already have been compromised. All recommendations are based on a clean OS installation.

It may not always be possible to avoid upgrading from Windows NT 4.0. Several factors go into making an informed decision on when you should upgrade and when you should install on a fresh system. Among the possible considerations are the time required to migrate all data if the system supports a large database or other information.

In addition to the install instructions in the ICM Staging Guide, follow these hardening guidelines:

- 1) To ensure that the machines are not compromised during setup it is highly recommended that the system be disconnected from the network until setup is complete and the most recent compatible² service pack is installed.

Using the bootable Windows 2000 CD is the simplest and fastest method of installing Windows 2000.

If network connectivity is required for the setup process, create a small private domain that has not been compromised by security attacks, is not reachable from the public Internet, and is not reachable by systems infected with worms or viruses. An integrated Service Pack installation share is recommended for this method. Insure none of the systems on the private network have e-mail or IIS.

- 2) All disk partitions must be NTFS formatted. This is the only file system format available that provides ACL based security. Refer to the **ICM Staging Guide** (section Install Windows 2000 Server and

² Refer to the Bill of Materials for the compatible service pack for your product.

Service Packs) on configuring partitions, particularly for systems that support databases such as loggers.

- 3) Due to the high number of worms exploiting unsecured systems on most networks, it is highly recommended that systems requiring IIS disable this service until Service Pack 4 or higher is installed. Refer to the *Internet Information Server* section of this document for additional details.
- 4) After setup has completed, follow the guidelines in the *Accounts, Passwords and Policies* section to set local policies. Local policies should roughly follow domain policies. More details about which local security rights are required for the application created accounts and groups can be found in the *Application Accounts* section.
- 5) Rename the Administrator account to something less obvious. Make it ICMAAdmin or something similar. Ensure the Guest account is renamed and disabled.
- 6) Connect the system back to the corporate or lab network and reboot or re-logon.
- 7) Install [Internet Explorer 6.0](#) and apply all latest [service packs and critical updates](#).
- 8) Disable Windows Update (Start > Settings > Control Panel > Automatic Updates), uncheck the box that says Keep my computer up to date. Connect to Microsoft update web site <http://v4.windowsupdate.microsoft.com/en/default.asp> and apply all necessary Service Packs, Critical and Important updates. See *Microsoft Security Updates* section for more details from an operational perspective.
- 9) Subscribe to the Microsoft Security Notification Service. This is a free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products.

Services

Enable only essential services. The highlighted services are the ones we recommend changing, depending on the role of the server in the network infrastructure. Enabling or disabling some services will require a decision based on the functionality provided by the specified service.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Alerter	Automatic	Disabled	Notifies selected users and computers of administrative alerts. Unless this functionality is desired, it should be disabled.
Application Management	Manual	Disabled	This service can be disabled to prevent unauthorized installation of software.
Automatic Updates	Automatic	(see comment)	Provides the download and installation of critical Windows updates. This service can be disabled when automatic updates are not performed on the server or left unchanged if Software Update Services is used as described in the Security Updates section .

Service Name	Default Startup Type	Recommended Startup Type	Comment
Background Intelligent Transfer Service	Manual	(See comment)	Provides background file transfer mechanism and queue management, and it is used by Automatic Update to automatically download programs. This service can be disabled when automatic updates are not performed on the server.
ClipBook	Manual	Disabled	Enables the ClipBook Viewer to create and share "pages" of data to be reviewed by remote users.
COM+ Event System	Manual	(No change)	Provides automatic distribution of events to COM components.
Computer Browser	Automatic	Disabled No change: on servers with 9x/NT clients	Maintains the list of computers on the network, and supplies the list to clients that request the list. If you do not have Windows 9x and NT 4.0 clients that use this feature, set to Disabled.
DHCP Client	Automatic	(No change)	Updates DNS records using Dynamic update.
Distributed File System	Automatic	Disabled: Servers No change: Domain Controllers	Manages logical volumes that are distributed across a local area network or wide area network, and it is required for the Active Directory SYSVOL share.
Distributed Link Tracking Client	Automatic	Disabled	Maintains links between NTFS v5 file system files on the Domain Controllers and other servers in the domain.
Distributed Link Tracking Server	Manual	Disabled	Tracks information about files that are moved between NTFS v5 volumes throughout a domain.
DNS Client	Automatic	(No change)	Allows resolution of DNS names.
Event Log	Automatic	(No change)	Writes event log messages.
Fax Service	Manual	Disabled	Provides the ability to send and receive faxes through available fax resources.
File Replication Service	Manual	Disabled: Servers No change: Domain Controllers	Enables files to be automatically copied and maintained simultaneously on multiple computers, and it is used to replicate SYSVOL among all Domain Controllers.
Indexing Service	Manual	Disabled	Indexes content and properties of files on a server to provide rapid access to the file through a flexible querying language.
Internet Connection Sharing	Manual	Disabled	Provides network address translation, addressing, name resolution, and intrusion detection when connected through a dial-up or broadband connection.
Intersite Messaging	Disabled	(No change)	Required by SMTP replication in Active Directory, DFS, and Netlogon.
IPSEC Policy Agent	Automatic	(See comment)	Provides management and coordination of Internet Protocol security (IPSec) policies with the IPSec driver. If IPSec is not used, set the startup type to Manual.
Kerberos Key Distribution Center	Disabled: Servers Automatic: Domain Controllers	(No change)	Provides the ability for users to log on using the Kerberos V5 authentication protocol.

Service Name	Default Startup Type	Recommended Startup Type	Comment
License Logging Service	Automatic	(See comment)	Monitors and records client access licensing. This service can be disabled but it is preferable that the corporate licensing policy be followed.
Logical Disk Manager	Automatic	(No change)	Required to ensure that dynamic disk information is up to date.
Logical Disk Manager Administrative Service	Manual	(No change)	Required to perform disk administration.
Messenger	Automatic	Disabled	Transmits net sends and Alerter service messages between clients and servers. If your organization makes use of this feature, it may be left unchanged.
Net Logon	Manual	(No change)	Maintains a secure channel between the Domain Controller, other Domain Controllers, member servers, and workstations in the same domain and trusting domains.
Network Connections	Manual	(No change)	Manages objects in the Network Connections folder.
NetMeeting Remote Desktop Sharing	Manual	Disabled	Eliminates a potential security threat by allowing server remote administration through NetMeeting.
Network DDE	Manual	Disabled	Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the server. This service can be disabled when no DDE applications are running locally on the server.
Network DDE DSDM	Manual	Disabled	Used by Network DDE. This service can be disabled when Network DDE is disabled.
NTLM Security Support Provider	Manual	(No change)	Provides security to remote procedure call (RPC) programs that use transports other than named pipes, and enables users to log on using the NTLM authentication protocol.
Performance Logs and Alerts	Manual	(See comment)	Collects performance data for the server, writes the data to a log, or generates alerts. This service can be set to automatic when you want to log performance data or generate alerts without an administrator being logged on.
Plug and Play	Automatic	(No change)	Automatically recognizes and adapts to changes in the hardware with little or no user input.
Print Spooler	Automatic	Disabled No change: Administrative Workstations with WebView	Manages all local and network print queues, and controls all print jobs. Can be disabled on servers where no printing is required.
Protected Storage	Automatic	(No change)	Protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users.
QoS RSVP	Manual	(See comment)	Provides support for Quality of Service (QoS) Resource Reservation Protocol (RSVP) routing information. This service can be disabled when the ICM configuration is set to "Bypass Packet Scheduler" on a Router and PG.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Remote Access Auto Connection Manager	Manual	Disabled Automatic: RMS Listener with Modem support	Detects unsuccessful attempts to connect to a remote network or computer, and provides alternative methods for connection. This service can be disabled on servers where no virtual private network or dial-up connections are initiated.
Remote Access Connection Manager	Manual	Disabled Automatic: RMS Listener with Modem support	Manages VPN and dial-up connection from a server to the Internet or other remote networks. This service can be disabled on dedicated servers where no VPN or dial-up connections are initiated.
Remote Procedure Call (RPC)	Manual	(No change)	Serves as the RPC endpoint mapper for all applications and services that use RPC communications.
Remote Procedure Call (RPC) Locator	Automatic	(No change)	Enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database.
Remote Registry Service	Automatic	(No change)	Enables remote users to modify registry settings, provided that the remote users have the required permissions. By default, only Administrators and Backup Operators can access the registry remotely.
Removable Storage	Automatic	Disabled	Manages and catalogs removable media, and operates automated removable media devices, such as tape auto loaders. This service can be enabled when removable media devices are directly connected to the server.
Routing and Remote Access	Disabled	(No change)	Enables LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services.
RunAs Service	Automatic	Disabled	Allows you to run specific tools and programs with different privileges than your current logon provides. Only enable if required administratively.
Security Accounts Manager	Automatic	(No change)	A protected subsystem that manages user and group account information.
Server	Automatic	(No change)	Provides RPC support, file print, and named pipe sharing over the network.
Smart Card	Manual	Disabled	Manages and controls access to a smart card that is inserted into a smart card reader attached to a server.
Smart Card Helper	Manual	Disabled	Provides support for legacy, non-plug-and-play smart card readers.
System Event Notification	Automatic	(No change)	Monitors system events and notifies subscribers to the COM+ Event System of these events.
Task Scheduler	Automatic	(No change)	Provides the ability to schedule automated tasks. Note: This service is required by the ICM application and should not be disabled under any circumstance.
TCP/IP NetBIOS Helper Service	Automatic	(No change)	Provides support for the NetBIOS over TCP/IP (NetBT) service and network basic input/output system (NetBIOS) name resolution for clients.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Telephony	Manual	Disabled No change: Logger with Modem support	Provides Telephony API (TAPI) support of client programs that control telephony devices and IP-based voice connections. This service can be disabled on servers where TAPI is not used by applications.
Telnet	Manual	Disabled (see comment)	Enables a remote user to log on and run applications from a command line. Enable Telnet only when it is legitimately used for remote administration. Measures must be taken to secure Telnet as described in the Remote Administration section.
Terminal Services	Disabled	(See comment)	Allows multiple remote users to be connected interactively, and provides display of desktops and run applications. To reduce the surface area of attack, disable Terminal Services unless it is used for remote administration. Refer to Terminal Services section of this document.
Uninterruptible Power Supply	Automatic	(See comment)	Manages an uninterruptible power supply connected to the server by a serial port. This service can be safely disabled if the server is not connected to a UPS device.
Utility Manager	Manual	Disabled	Allows faster access to some accessibility tools, such as Magnifier and Narrator. Disable Utility Manager unless you require these special accessibility tools.
Windows Installer	Manual	(No change)	Adds, modifies, and removes applications that are provided as a Windows Installer (.msi) package.
Windows Management Instrumentation	Manual	(No change)	Provides a common interface and object model to access server management information through the WMI interface.
Windows Management Instrumentation Drivers	Manual	(No change)	Monitors all drivers and event trace providers that are configured to publish WMI or event trace information.
Windows Time	Manual	(No change)	Sets the server clock, and maintains date and time synchronization on all computers in the network.
Wireless Configuration	Manual	Disabled	Provides authenticated network access control using IEEE 802.1x for wired and wireless Ethernet networks.
Workstation	Automatic	(No change)	Creates and maintains client network connections to remote servers.

Accounts, Passwords and Policies

An effective password policy can help deter the use of old, obsolete, or guessed passwords. Windows uses policies to enforce specific behavior for passwords. Both local and domain policies must be set. Otherwise, an intrusion could occur by taking advantage of local passwords.

Minimum Criteria for Strong Passwords

- 1) Be at least 6 characters in length. 8 characters are preferable.
- 2) Must not contain any part of the user's account name
- 3) Must contain characters from at least three of the following five categories:
 - a. English upper case characters (A..Z)
 - b. English lower case characters (a..z)
 - c. Base 10 digits (0..9)
 - d. Non-alphanumeric characters, for example, !,\$#,%
 - e. Use the ALT key to generate accented or special symbols

Setting Local Password Policy

Use Start > Programs > Administrative Tools > Local Security Policies to set local policies.

Under Account Policies, Password Policy – set the following:

- 1) Enforce Password History, set to 6 passwords.
- 2) Maximum Password Age, keep at 42 days.
- 3) Minimum Password Age, keep default value of 0 (passwords can be changed immediately).
- 4) Enable Password complexity.
- 5) Store passwords using reversible encryption, keep as disabled for greater security.

Under Account Policies, Account Lockout Policy – set the following:

- 1) Account lockout duration. Default is not defined. Recommended value is 30 minutes.
- 2) Account lockout threshold. Default is 0 invalid login attempts. Recommended value is 5.
- 3) Reset account lockout counter after. Default is not defined. Keep unchanged.

Under Local Policies, User Rights Assignment, add Anonymous Logon to the following deny roles:

- 1) Deny logon as a batch job.
- 2) Deny logon as a service.
- 3) Deny logon locally.

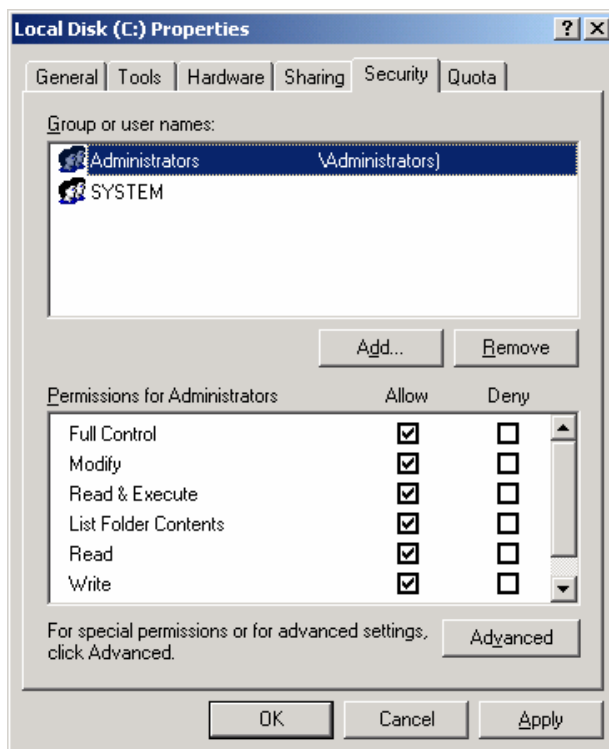
You must logout before changes take effect.

File System and Registry

File System

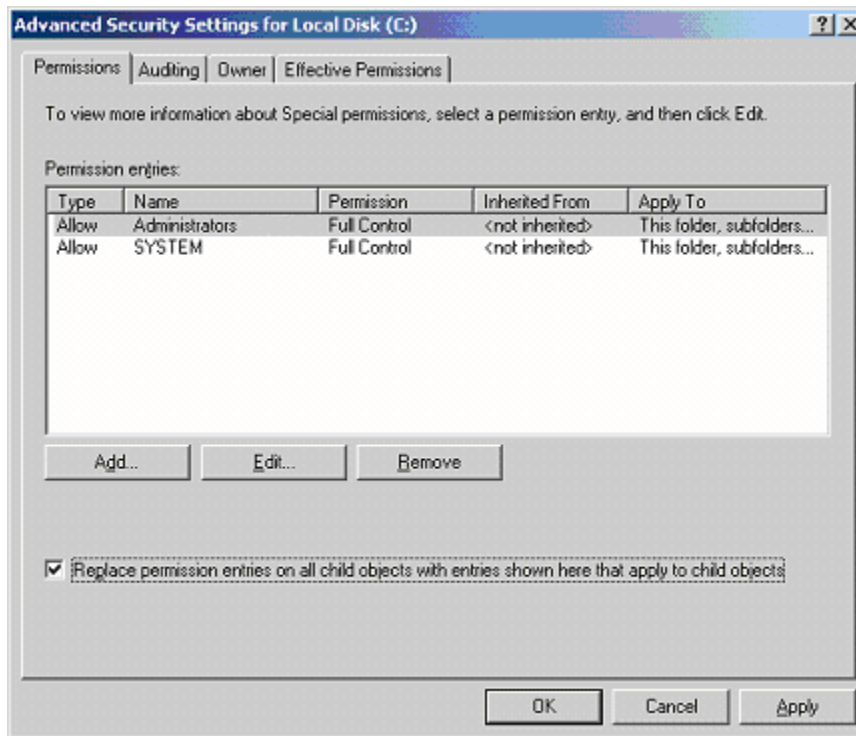
Top Hardening Suggestions:

- 1) It is assumed that the latest compatible service pack and security updates have been installed.
- 2) Convert all drives to NTFS.
- 3) At the drive root (e.g., C:) go the Security tab and remove the EVERYONE group account and any other unneeded accounts that might have been added such as <machine>\Users, etc.
- 4) In the security tab for the drive, add the <machine>\Administrators, Creator/Owner and SYSTEM group accounts and enable Full Control for those accounts.



- 5) Press the 'Advanced' button and select 'Reset permissions on all child objects and enable propagation of inheritable permissions' check box then select 'OK'. This will propagate the permission change to all subdirectories and files. Ignore any errors on locked files such as the system paging file.

Note: Propagation of permissions to all subdirectories only needs to be done during this step. All other permissions added later in this document will be automatically propagated.



- 6) Add auditing of failures for the Everyone account. In the Advanced Security Settings shown above, select the Auditing tab, Add the Everyone group, and select all Failure options.
- 7) Some additional accounts or account groups permissions are required. Some will be dictated by the system administrator. For example, allowing access to the *Backup Operators* group for backup and restore operations. Others are required for contact center application functionality as outlined in the next step. If you need to give read access to other accounts, use the <Machine>\Users group and set permissions for 'read only', adding accounts to that group as needed. *In General, avoid giving permissions globally across the complete partition. Narrow the scope down to the lowest subdirectories in the hierarchy.*

Note: ICM access security involves providing access to "Standard Users" and "WebView Only Users" as outlined in the Cisco ICM Software Security Guide. Standard Users are Windows user accounts who can access ICM applications and tools at an Administrative Workstation (AW) interactively. These users can also access ICM services over the Web using WebView in a Web browser.

Those user accounts or groups which require logon access to an AW will need to be given the appropriate permissions. The file system root ACL must provide at a minimum, specific user accounts or an ICMStandardUsers group with *Read & Execute* permissions.

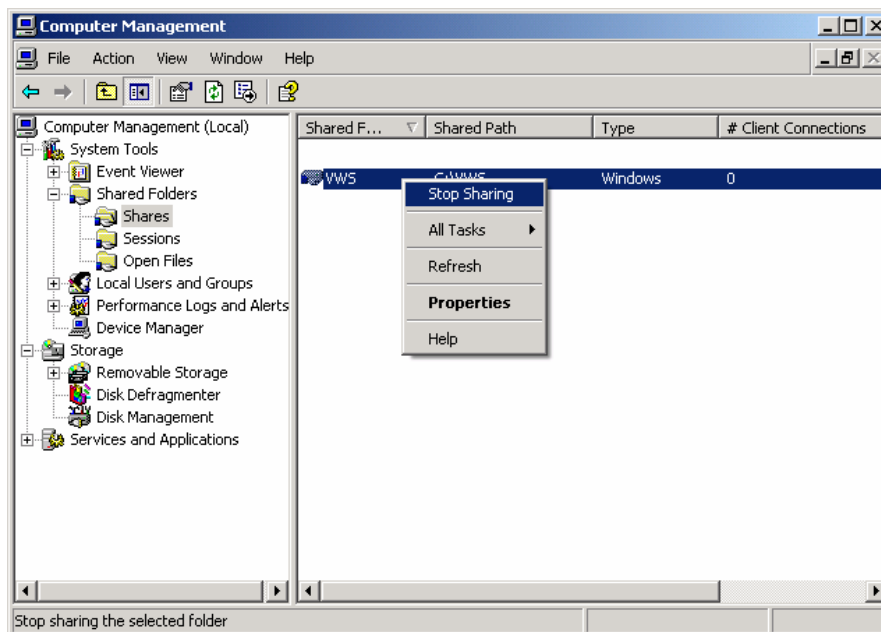
- 8) **After completing the steps outlined above, and after the ICM and SQL applications have been installed, some directory permissions must be given depending on the nodes being hardened. Refer to the details below and to the *Internet Information Server* and *SQL Server* sections of this document for additional required security implementation details.**

The following account groups need **file access permissions** on a Router node.

'DBagtWrite' and '<instance>DbagtRead': require read only access to the following directories as specified:

Router (sideA)	<ICM_Install_Drive>:\ICM<instance>\ra
Router (sideB)	<ICM_Install_Drive>:\ICM<instance>\rb

- 9) Remove all explicit and implicit file shares on systems that do not require it. RMS Listener requires explicit file shares. Refer to the product specific documentation for additional details.
- a. To remove explicit shares, go to Manage > Shared Folders > Shares and stop sharing each share that is not required.



- b. To remove implicit shares (e.g., Administrative shares) open the registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters and add a DWORD value named AutoShareServer and set to it '0' (zero).

Note: On a Domain Controller, the SYSVOL and NETLOGON shares must have the NTFS permissions for the physical directory set to match the logical share permissions.

- 10) If there is any sensitive contact center data, enable EFS, *Encrypted File System*, on directories that contain that data (database directories, etc.). EFS on Windows 2000 can only be bound to a single account. Make sure to enable EFS when logged on under the credentials that you want EFS to use (for example, <domain>\SQLServiceAcct).

Note: There is a performance impact when EFS is enabled. We do not recommend implementing EFS on high throughput systems.

- 11) Schedule the Windows Cipher process to run during maintenance windows to wipe all deleted records on any systems containing sensitive data that might have been erased. The scheduled command should be as follows: "Cipher /W:<drive letter:\>".

- 12) Other File System Hardening Considerations:

CAUTION: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Cisco cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk and make backups as appropriate.

- a. Disable Auto Generation of 8.3 Filenames.

CAUTION: This should not be done on a node that has or will have Support Tools Agent installed.

Under registry key (using regedt32):

HKLM\System\CurrentControlSet\Control\FileSystem

Note: if a value does not exist, create one.

Registry Value Entry	Format	Value (Decimal)
NtfsDisable8dot3NameCreation	DWORD	1

b. Removing OS/2 and POSIX Subsystems

Under this registry key delete the data contained in the following values along with the actual values (using regedt32):

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

Registry Value Entry
Optional
OS/2
POSIX

Note: The values can be deleted by doing a right click on the selected value and selecting 'Delete'.

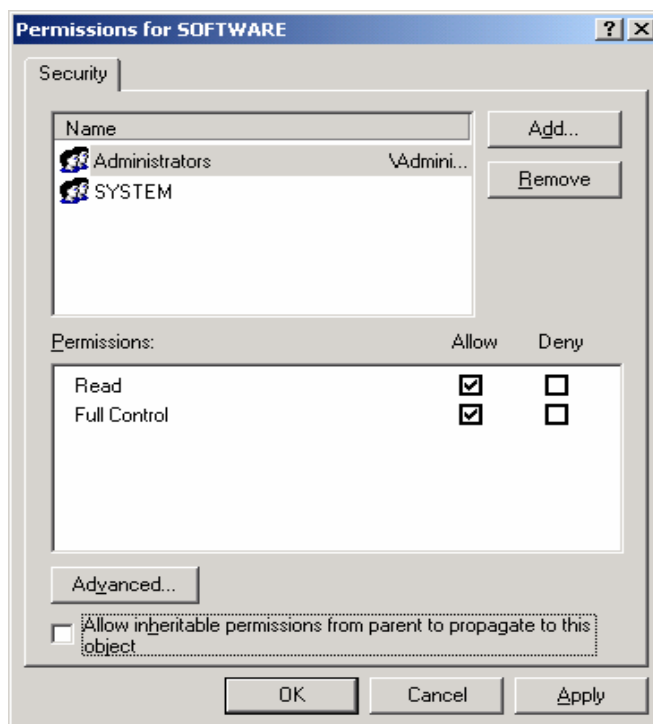
Refer to <http://support.microsoft.com/default.aspx?scid=kb:en-us:320869> for more details.

Registry

CAUTION: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Cisco cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk and make backups as appropriate.

- 1) It is assumed that the latest compatible service pack and security updates have been installed.
- 2) Launch RegEdt32.exe.
- 3) There is one root hive and two sub-hives that require security changes: HKEY_USERS, HKEY_LOCAL_MACHINE\Software and HKEY_LOCAL_MACHINE\System. **Do not** modify any other hives directly.
- 4) To edit permissions, click on each one of the three hives listed above and select Security > Permissions from the menu.
- 5) Uncheck the 'Allow inheritable permissions from parent to propagate to this object' checkbox if selected. Choose 'COPY' permissions if prompted.
- 6) Add the <machine>\Administrators and SYSTEM groups and set Full Control to both.
- 7) Remove all other groups and users from the list.
- 8) Press the 'Advanced' button and select 'Reset permissions on all child objects...' check box then select OK. This will propagate the permission change to all subkeys. When applying this change to the hive an error might occur indicating that permissions could not be changed on a subkey. This error can safely be ignored.

Note: Propagation of permissions to all subkeys only needs to be done during this step. All other permissions added later in this document will be automatically propagated.



- 9) Verify that the HKEY_LOCAL_MACHINE\Security and HKEY_LOCAL_MACHINE\SAM\SAM hives (Advanced Properties) have **SYSTEM** set to *Full Control* and **<machine>\Administrators** set to *Special Access, Write DAC and Read Control* only. No other accounts should have access to these two hives.
- 10) After completing the steps outlined above, and given the ICM application has already been installed, the following registry permissions must be given. Otherwise, the ICM Setup will apply these changes.

The following account group needs registry access on a Router node:

LocalCRPermon: requires read access to

HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM and
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

The following account group needs registry access on an AW (distributor) node:

<machine>\Users: requires read access to

HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM

- 11) **After completing the steps outlined above, and after the ICM and SQL applications have been installed, some registry permissions must be given depending on the nodes being hardened. Refer to the *Internet Information Server* and *SQL Server* sections of this document for more details on what registry permissions to set.**

Hardening against Network Attacks

TCP/IP Stack Hardening

Harden TCP/IP stack by making the following registry changes (using regedt32).

CAUTION: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Cisco cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk and make backups as appropriate.

Under registry key:

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

Note: If a value does not exist, create one.

Registry Value Entry	Format	Value (Decimal)
EnableICMPRedirect	DWORD	0
SynAttackProtect	DWORD	2
EnableDeadGWDetect	DWORD	0
EnablePMTUDiscovery†	DWORD	1
KeepAliveTime	DWORD	300000
DisableIPSourceRouting	DWORD	2
TcpMaxConnectResponseRetransmissions	DWORD	2
TcpMaxDataRetransmissions	DWORD	3
PerformRouterDiscovery	DWORD	0
TCPMaxPortsExhausted	DWORD	5

Note (†):

This table contains a setting which differs from Microsoft's security recommendations. The reason for this is explained below:

Per Microsoft "Windows 2000 TCP/IP Implementation Details":

`EnablePMTUDiscovery` – Completely enables or disables the PMTU discovery mechanism. When PMTU discovery is disabled, an MTU of 576 bytes is used for all non-local destination addresses.

By disabling MTU discovery we would force the use of an MTU which is much smaller than actually allowed by the link in most of the cases. This will cause wasted bandwidth, since header overhead will increase (payload per packet is decreased). This will require recalculation of bandwidth requirements, for example, in the case of remote PG to Central Controller communication. At the same time, it is very unlikely that a hacker will be able to completely take over the network infrastructure in order to capture a TCP session and generate an ICMP Destination unreachable packet to force communicating systems to lower MTU down to 1 byte.

Considering these two factors (increase in bandwidth needs and danger of hackers forcing systems to lower their MTU to 1 byte) we recommend keeping PMTU discovery enabled (default).

If you feel that you absolutely need to disable MTU discovery, you must first recalculate bandwidth needs for the links used, then increase available bandwidth, and only then disable MTU discovery. Testing may be necessary to assess the impact on throughput and performance.

Under registry key:

HKLM\System\CurrentControlSet\Services\Netbt\Parameters\

Note: If a value does not exist, create one.

Registry Value Entry	Format	Value (Decimal)
NoNameReleaseOnDemand	DWORD	1

Harden the Winsock Interface Driver

The ICM extensively uses Windows sockets interface and as a result the following hardening is recommended for Winsock interface drivers afd.sys:

Under registry key:

HKLM\System\CurrentControlSet\Services\AFD\Parameters\

Note: If a value does not exist, create one.

Registry Value Entry	Format	Value (Decimal)
DynamicBacklogGrowthDelta	DWORD	10
EnableDynamicBacklog	DWORD	1
MinimumDynamicBacklog	DWORD	20
MaximumDynamicBacklog	DWORD	20000

Harden Network Browser Interface

HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\

Note: If a value does not exist, create one.

Registry Value Entry	Format	Value (Decimal)
Hidden	DWORD	1
AutoShareServer	DWORD	0

Harden against Anonymous access

HKLM\System\CurrentControlSet\Control\LSA

Note: If a value does not exist, create one. A reboot is required for setting to take affect.

Registry Value Entry	Format	Value (Decimal)
RestrictAnonymous	DWORD	1

HKLM\System\CurrentControlSet\Services\LanManServer\Parameters

Note: If a value does not exist, create one.

Registry Value Entry	Format	Value (Decimal)
RestrictNullSessAccess	DWORD	1

WMI Service Hardening

Windows Management Instrumentation (WMI) is used to manage Windows systems. WMI security is an extension of the security subsystem built into Windows operating systems. WMI security includes: WMI namespace-level security; Distributed COM (DCOM) security; and Standard Windows OS security.

To configure the WMI namespace-level security:

- 1) Launch the %SYSTEMROOT%\System32\Wmimgmt.msc MMC control.
 - 2) Right click on the WMI Control icon and select properties.
 - 3) Select the 'Security' properties page.
 - 4) Select the 'Root' folder and press the 'Security' button.
 - 5) Remove EVERYONE from the selection list then press the 'OK' button.
- NOTE: Only <machine>\Administrators should have ALL rights.

DCOM security configuration should be performed in a manner that is consistent with your scripting environment. Refer to the [WMI security](#) documentation for additional details on using DCOM security.

Note: The WMI services are set to 'Manual' startup by default. These services are used by 3rd Party Management agents as well as Cisco Support Tools Node Agent to capture system data and should not be disabled unless specifically required.

SNMP Service Hardening

The SNMP protocol is inherently insecure, and it is strongly recommended that the SNMP and SNMP Trap Services simply be disabled. Read below for cases where the SNMP service should not be disabled.

Note: The SNMP service isn't installed by default on the Windows 2000 operating system unless the system was staged using one of the 3rd Party installation methods such as HP SmartStart or Dell OpenManage. The service is used for 3rd Party Management Agents as well as ICM and IPCC applications when configured for sending SNMP traps.

When used on ICM Enterprise and IPCC Enterprise hosts located on internal networks behind corporate firewalls, it is possible to enable the SNMP services when performing the additional hardening recommendations below.

- 1) Make sure that you change the default community name to a community name using a combination of upper- and lower-case characters.
- 2) Limit hosts that are allowed to connect to SNMP agent to only hosts running SNMP management platforms.
- 3) Enable sending of SNMP trap when authentication fails.

As an alternative that provides a much higher level of security, customers may choose to configure IPSec filters and an IPSec policy for SNMP traffic between an SNMP management station and SNMP agents. Follow Microsoft's recommendations on how to accomplish this. For more information on IPSec policy for SNMP traffic refer to Microsoft knowledge base article: Q324261.

Hardening against Application Attacks

Application Accounts

User Accounts

ICM products add local, domain and SQL Server user accounts and groups. These groups allow the software to manage their roles and rights, a critical element to maintaining the lowest possible security profile. These user accounts are usually created and managed by ICM Setup or the Configuration User List Tool. In some cases they are installed by ICMDDBA.

The table below captures all instances where ICM accounts are created and made members of various user groups. The ICM setup creates both domain and local accounts. For example, the domain account <instance>SQLUser is created as a Global Group and is made a member of <domain>DbagtWrite and <domain>LocalSQLUser groups. It is also made a member of LocalSQLUser in both the logger and distributor. In the table below, local groups are identified by the system on which they are created as <logger>, <distributor>, or <router>.

Domain Accounts

Account Name	Type	Members	Member Of	Installed By
<instance>SQLUser	Global Group	Added by User List	<domain>DbagtWrite <domain>LocalSQLUser <logger>\LocalSQLUser <distributor>LocalSQLUser <distributor>Power Users <distributor>Users	Logger Router Distributor
<instance>WVScript	Global Group	Added by User List	<distributor>LocalWVScript	Distributor
NTDomainOperators	Global Group	Added by User List	<domain>\Account Operators	Distributor
SQLAdmin	Global Group	<domain>\jag<distributor> <instance><side><logger>	<domain>DbagtWrite <domain>LocalSQLAdmin <logger>\LocalSQLAdmin <distributor>Users <distributor>LocalSQLAdmin <router>DbagtWrite	Logger Router Distributor
SQLAWAdmin	Global Group	<domain>\ <instance><distributor> <instance><side><distributor>	<domain>DbagtWrite <domain>LocalSQLAdmin <logger>\LocalSQLAdmin <distributor>LocalSQLAdmin <router>DbagtWrite	Logger Router Distributor
DbagtWrite	Global Group	<domain>\<instance>SQLUser <domain>SQLAdmin <domain>SQLAWAdmin	None	Router
ICRPerfmon	Global Group	None	<router>\LocalICRPerfmon	Router Distributor
jag<distributor>	Domain User	N/A	<domain>SQLAdmin <distributor>Administrators	Distributor
Account Operators	Local Group	<domain>NTDomainOperators	None	Operating System

<instance><distributor>	Domain User	N/A	<domain>\SQLAdmin <distributor>\Administrators	Distributor
<i>This account is used as the service logon account for the Cisco ICM Distributor service.</i>				
<instance><side><logger>	Domain User	N/A	<domain>\SQLAdmin <logger>\Administrators	Logger
<i>This account is used as the service logon account for the Cisco ICM Logger service.</i>				

Logger

Operating System Accounts

Account Name	Type	Members	Member Of	Installed By
LocalSQLAdmin	Local Group	<domain>\SQLAdmin <domain>\SQLAdmin	Logger SQL Login	Logger
LocalSQLUser	Local Group	<domain>\<instance>SQLUser	Logger SQL Login	Logger
Administrators	Local Group	<domain>\<instance><logger>	None	Logger assigns members to OS account

SQL Server Accounts

Account Name	Type	Members	Member Of	Installed By
<logger>\LocalSQLAdmin	SQL Login	None	System Administrators (sysadmin) Server Role	Logger setup
<logger>\LocalSQLUser	SQL Login	None	None	Logger setup
GeotelGroup	SQL AW DB Role	Added by User List	None	ICMDBA
GeoTelAdmin	SQL AW DB Role	None	None	ICMDBA
Sysadmin	SQL Server Role	<distributor>\LocalSQLAdmin	None	SQL Server

Operating System Assigned Permission Changes

Account Name	Change
LocalSQLAdmin	Security rights: <ul style="list-style-type: none"> • Access this computer from the network • Bypass traverse checking • Log on locally • Log on as a service • Act as part of the operating system
LocalSQLUser	Security rights: <ul style="list-style-type: none"> • Access this computer from the network • Bypass traverse checking • Log on locally • Log on as a service • Act as part of the operating system

Distributor and Client AW

Operating System Accounts

Account Name	Type	Members	Members Of	Installed By
Users	Local Group	<domain>\<instance>SQLUser <domain>\SQLAdmin	None	Distributor assigns members to OS account
Power Users	Local Group	<domain>\<instance>SQLUser	None	Distributor assigns members to OS account
Administrators	Local Group	<domain>\<instance><distributor> <domain>\jag<distributor>	None	Distributor assigns members to OS account
LocalSQLAdmin	Local Group	<domain>\SQLAdmin <domain>\SQLAWAdmin	Distributor SQL Login	Distributor
LocalSQLUser	Local Group	<domain>\<instance>SQLUser	Distributor SQL Login	Distributor
LocalWVScript	Local Group	<domain>\<instance>WVScript	None	Distributor

SQL Server Accounts

Account Name	Type	Members	Members Of	Installed By
<distributor>\LocalSQLAdmin	SQL Login	None	System Administrators (sysadmin) Server Role	Distributor
<distributor>\LocalSQLUser	SQL Login	None	None	Distributor
GeotelGroup	SQL AW DB Role	Added by User List	None	Distributor
GeoTelAdmin	SQL AW DB Role	None	None	Distributor
Sysadmin	SQL Server Role	<distributor>\LocalSQLAdmin	None	SQL Server

Operating System Assigned Permission Changes

Account Name	Change
Users	Access to the following registry keys: <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>
LocalSQLAdmin	Security rights: <ul style="list-style-type: none"> • Access this computer from the network • Bypass traverse checking • Log on locally • Log on as a service • Act as part of the operating system

LocalSQLUser	Security rights: <ul style="list-style-type: none"> • Access this computer from the network • Bypass traverse checking • Log on locally • Log on as a service • Act as part of the operating system
LocalWVScript	Security rights: <ul style="list-style-type: none"> • Bypass traverse checking • Log on locally

Router

Operating System Accounts

Account Name	Type	Members	Members Of	Installed By
DbagtWrite	Local Group	<domain>\<instance>SQLUser <domain>\SQLAdmin <domain>\SQLAWAdmin	None	Router
LocalICRPerfmon	Local Group	<domain>\ICRPerfmon	None	Router
<instance>DbagtRead	Local Group	None	None	Router

Operating System Assigned Permission Changes

Account Name	Change
LocalICRPerfmon	Access to the following registry keys: <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM • HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance> • HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services • HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Cisco ICM Router Security rights: <ul style="list-style-type: none"> • None
DbagtWrite	Access to the following NTFS file or directory objects <ul style="list-style-type: none"> • <icm install drive>:\icm\<instance>\ra • <icm install drive>:\icm\<instance>\ra\dbagt.acl Security rights: <ul style="list-style-type: none"> • Access this computer from the network • Bypass traverse checking • Log on locally • Log on as a service
<instance>DbagtRead	Access to the following NTFS file or directory objects <ul style="list-style-type: none"> • <icm install drive>:\icm\<instance>\ra • <icm install drive>:\icm\<instance>\ra\dbagt.acl Security rights: <ul style="list-style-type: none"> • Access this computer from the network • Bypass traverse checking • Log on locally • Log on as a service

Toll Fraud Prevention

Toll fraud is a serious issue in the Telecommunications Industry. The fraudulent use of telecommunications technology can be very expensive for a company, and it is essential that the Telecom Administrator take the necessary precautions to prevent this. For IPCC environments, resources are available on Cisco.com providing some basic information to lock down CallManager systems and to mitigate against toll fraud.

In ICM, the primary concern would be in using dynamic labels in the label node of an ICM script. If the dynamic label is constructed from information entered by a caller (such as with Run External Script), then it is possible to construct labels of the form.

9.....
9011....
etc.

These labels might cause the call to be sent to outside lines or even to international numbers. If the dial plans configured in the routing client would allow such numbers to go through, and the customer does not want such labels to be used, then the ICM script must check for valid labels before using them.

A simple example would be an ICM script that prompts the caller with "If you know your party's extension, enter it now", and then uses the digits entered blindly in a dynamic label node. It is possible that the call could be transferred anywhere. If this behavior is not desired, then either the ICM routing script or the routing client's dial plan must check for and disallow invalid numbers.

An example of an ICM script check might be an "If" node that use an expression such as

```
substr (Call.CallerEnteredDigits, 1, 1) = "9"
```

The "True" branch of this node would then branch back to ask the caller again. The false branch would allow the call to proceed. This is, of course, only an example. Each customer must decide what is allowed, or not, based on their own environment.

ICM does not normally just transfer calls to arbitrary phone numbers. Numbers have to be explicitly configured as legal destinations, or alternatively the ICM routing script can contain logic which causes the call to be transferred to a phone number which is contained in a script variable. It is possible for a script to be written in such a way that a caller enters a series of digits and the script treats it as a destination phone number and asks the routing client to transfer the call to that number. Our recommendation would be to add logic to such a script to make sure the requested destination phone number is reasonable.

Application Security and Passwords

This section identifies how passwords and call data are handled in ICM/IPCC products. ICM relies on network infrastructure security, including physical security, edge security, routers and firewalls. For performance reasons, ICM servers must trust each other. This eliminates the requirement to add extended encryption and authentication between servers.

ICM

- Passwords encoded as an MD5 hash between AW, PG, Router, and Logger.
- Passwords transferred and stored in the SQL Server database as an MD5 hash.
- Call Variables and Extended Call Variables are not encrypted.

Note: Call variables are stored in the application databases therefore there is a reliance on the security provided by Microsoft SQL Server. In some cases, customers may be storing sensitive information such as bank account numbers or personal identification numbers which can constitute a risk if confidentiality is a requirement. The passing of call variables across the various distributed components making up the ICM and IPCC solution is done via proprietary binary protocols. These variables may be written to binary log files or directed to text files when debugging the system. Following the file system hardening and system access control recommendations along with applying due diligence in distributing log files should ensure that this data is not compromised.

The next section of this document (IPSec and NAT Support) should provide for a way to protect the confidentiality of the data traveling across non trusted networks.

CTI and CTI OS

- Passwords always sent as clear text from the agent and supervisor desktops.

CAD

- Passwords always sent as clear text from the agent and supervisor desktops.
- Agent ID/Password also sent to LDAP server. Login uses base64 encoding.

In CAD 6.0(0), the passwords kept in LDAP are encrypted using an RSA RC4 algorithm that uses a 40 bit key.

Note: The path traversed by the communication between the agent desktop to the CTI OS, CTI or CAD Server should be secured. Typically, ICM and IPCC Enterprise deployments will have these applications sharing a security zone or spread across trusted zones. If agent desktop communication must cross the public internet, appropriate measures should be taken to secure that link to protect it from eavesdropping. A strong password management policy that requires passwords to be periodically changed is recommended.

The next section (IPSec and NAT Support) of this document should provide for a way to protect the confidentiality of the data traveling across non trusted networks.

WebView

- Username/password sent to IIS server from browser uses Base 64 Encoding. Qualification is underway to support SSL for WebView.

Internet Script Editor

- Internet Script Editor gets services from various processes on the ICM distributor. These services are exposed through the web server (IIS) so that Internet Script Editor can access them using HTTP or HTTPS. Username/password sent to ISE server uses Base 64 Encoding by default. For strong encryption, SSL must be enabled. The ISE client software allows for encrypted communication over an HTTPS connection on Port 443.

Support Tools

- Username/password sent to Support Tools HTTP Server from browser uses Base 64 Encoding. For strong encryption, SSL must be enabled for Support Tools HTTP Server. Please refer to the Cisco Support Tools User Guide for more details on Configuring Support Tools to use SSL.

IPSec and NAT Support

Support for IPSec (IP Security) in Tunnel Mode

Due to increased security concerns in the deployment of data and voice networks alike, ICM and IPCC Enterprise deployments now add support for IPSec between Central Controller sites and remote Peripheral (PG) sites as well as between call control servers and agent desktops. This secure network implementation implies a distributed model where the WAN connection is secured via IPSec tunnels. The testing undertaken in this release was limited to configuration of Cisco IOS™ IPSec in Tunnel Mode, meaning only the Cisco IP Routers (IPSec peers) between the two sites were part of the secure channel establishment. All data traffic is encrypted across the WAN link but un-encrypted on the local area networks. In tunnel mode, traffic flow confidentiality is ensured between IPSec peers which, in this case, are the IOS Routers connecting a central site to a remote site.

The qualified specifications for the IPSec configuration are as follow:

- **HMAC-SHA1 Authentication (ESP-SHA-HMAC)**
- **3DES Encryption (ESP-3DES)**

We recommend that hardware encryption be used in order to avoid a significant increase in IP Router CPU overhead and throughput impact. There are also some latency implications, so it's important to size the network infrastructure (network hardware and physical links) accordingly. There are also considerations that must be taken for QoS networks. The common recommendation is to classify and apply QoS features based on packet header information before traffic is tunnel encapsulated and/or encrypted.

More detailed resources on Cisco IOS IPSec functionality can be found at http://www.cisco.com/en/US/tech/tk583/tk372/tech_protocol_family_home.html

Support for NAT (Network Address Translation)

Release 6.0(0) officially adds support for deployment of Agent Desktops and IP Phones (IPCC) across NAT. Cisco has also tested locating remote Peripheral (PG) servers on a NAT network remote from the Central Controller servers (Routers and Loggers). The qualification of NAT support for Agent Desktops and PG servers was limited to a network infrastructure implementing Cisco IP Routers with NAT functionality.

Cisco IOS™ Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. As its name implies, Cisco IOS NAT translates IP addresses within private "internal" networks to "legal" IP addresses for transport over public "external" networks (such as the Internet). Incoming traffic is translated back for delivery within the inside network.

More detailed resources on how to configure NAT can be found at http://cisco.com/en/US/partner/tech/tk648/tk361/tk438/tech_protocol_home.html

More details on how to deploy IP Phones across NAT for IPCC deployments can be found at the following link: http://cisco.com/en/US/partner/products/sw/iosswrel/ps1834/products_feature_guide09186a008008052e.html.

Note: IPSec and NAT Transparency

The IPSec NAT Transparency feature introduces support for IP Security (IPSec) traffic to travel through Network Address Translation (NAT) or Port Address Translation (PAT) points in the network by addressing many known incompatibilities between NAT and IPSec. NAT Traversal is a feature that is auto detected by VPN devices. There are no configuration steps for a router running Cisco IOS Software Release 12.2(13)T and above. If both VPN devices are NAT-T capable, NAT Traversal is auto detected and auto negotiated.

Active Directory

Security Recommendations for Active Directory / DNS / Domain Controllers are taken from the Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I & II and various Microsoft knowledge base security articles. See references for a link to this reference guide.

Note: Cisco ICM Software Release 6.0(0) supports domain controllers running Windows Server 2003 in addition to Windows 2000. The applications, however, are only supported on Windows 2000 operating systems. While the recommendations for securing AD in Windows 2000 and Windows Server 2003 are similar, there are special considerations for the latter. See External Trusts section for details.

- General Domain Controller Security

- It is recommended that you do not run SQL Server on a Domain Controller. Domain Controllers contain sensitive data such as user account information, and they should not be used in another role. If you run a SQL Server database on a Domain Controller, you increase the complexity involved in securing the server and preventing attack.
- If possible, do not image or re-SID a Domain Controller (DC). DCs should be built from scratch when possible.
- Have more than 1 dedicated Domain Controller for fault tolerance.
- Hide the identity of the DCs. Change the name of the computer so that it does not indicate it is a Domain Controller (e.g., CORPDC1 is not a recommended name).
- Protect the Built-in Administrator account. Rename the account to something other than 'Administrator'.
- LDAP traffic is signed and sealed. This behavior is automatically turned on when applying SP3 to Windows 2000 Servers. (<http://www.microsoft.com/technet/columns/profwin/pw0203.asp>)
- Remove weak LanMan (LM) Hash from AD and SAM. Turn off the LM Hash by setting the following registry key on the DC:

Under registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Note: If a value does not exist, create one.

A Password reset is required in order for the change to take effect. (MSKB-Q299656)

Registry Value Entry	Format	Value (Decimal)
NoLMHash	DWORD	1

- Enable NTLM v2 Authentication for Windows 95/98/2000 and NT. (MSKB-Q239869)
- Make sure machines are up-to-date with the relevant Microsoft security updates.
- Make sure your account policies are properly configured: Prevent anonymous logon when not needed, enforce strong and complex passwords, with minimum characters, etc. Refer to *Accounts, Passwords and Policies* section.

- External Trusts

- Enable SID filtering while creating external trust between domains in isolated forests. (MSKB-Q289243) (**Caution: note the incompatibilities of SID filtering in MSKB-Q289243**)

- When setting up group membership, make sure that the administrative groups from one forest do not include accounts from the other forests. (Create a separate account(s) in each domain instead of having cross-domain accounts)
 - Users from other forests should not be included in any of the following groups:
 - Groups responsible for service management or groups that can manage the membership of service administrator groups.
 - Groups with administrative control over computers that store protected data.
 - Groups that have access to protected data, or groups responsible for the management of users or group objects that have access to protected data.
- **Windows Server 2003 only:**
 - Create forest trust relationships between Windows Server 2003 forests only when all forest administrators and all domain administrators are trusted individuals. (A forest functional level of Windows Server 2003 is required in both forests.)
 - Before creating an external trust between two domains in isolated forests, be sure that the two domains have a domain functional level of at least Windows 2000 native and that all domain controllers are running at least Windows 2000 Server SP4, so that SID filtering is enforced by default.
- **DNS Security**
 - Use AD integrated zones.
 - Allow Secure Dynamic Updates.
 - Protect the DNS cache on DCs
 - Properties > Advanced > Secure Cache against pollution
 - Separate internal and external DNS servers.
 - Restrict zone transfers.
 - If a firewall exists between DNS Servers or clients, open port 53 for DNS client queries. Refer to "How to Configure a Firewall for Domains and Trusts" at Microsoft KB Article 179442 for more details.
 - Monitor network activity for attacks.
 - Log DNS events and check logs periodically to identify potential breaches.
- **Replication**
 - Limit number of ports involved/opened when performing DC replication over RPC.
 - Ensure replication works when new sites or DCs are added (using dcdiag.exe, etc.).
 - If a firewall exists between Domain Controllers, open the appropriate firewall port for replication communication depending on whether IP, RPC, or SMTP is used. Refer to "How to Configure a Firewall for Domains and Trusts" at Microsoft KB Article 179442 for more details.
- **Securing Domain Master Roles**

Changes in forest-wide operations master roles (also known as flexible single master operations, or FSMO) are important to security because they affect the entire forest. Forest-wide operations master roles include the following:

 - Schema Master
 - Domain Naming Master
 - PDC Emulator
 - RID Master
 - Infrastructure Master

Because forest-wide operations master roles are assigned to specific domain controller computers, any unauthorized change in the operations master roles can be an indication of a breach in Active Directory security.

- Schema Master should be protected from any kind of access.
- Domain Naming Master should be kept under strong password policies.

- Restrict Access

- Restrict physical access to AD/DNS/DC.
- Only give access to the level that is required.
- Only Administrators having a good understanding of AD should have full administrative access.
- Only the Enterprise Admin should have access to the Schema.
- Allow only DNS Administrators Group to manage DNS services.
- Prohibit cached credentials from unlocking a DC console.

Under registry key:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Note: If a value does not exist, create one.

Registry Value Entry	Format	Value (Decimal)
ForceUnlockLogon	DWORD	1

- Use the "Trusted for Delegation" option wisely. This powerful configuration enables a machine to perform delegated authentication and operate any service on other machines in the domain.
- Disable Pre-Windows 2000 Compatible Access if possible.
- Use/enforce Smart Card logins for Administrators.
- Limit the number of members in security groups such as Enterprise Admins and Schema Admins.
- Prevent anonymous logon when not needed.

- Backup Best Practices

- Force full system backup of AD and all the respective domain controllers.
- Protect admin password used to restore AD DB from backup.
- Files to backup/protect are
 - ntds.dit – The database file
 - edb.chk – Checkpoint file
 - edb*.log – Transaction logs
 - res1.log and res2.log – Reserved Transaction log files
- Backup Registry prior to making registry changes.

- User Rights and access

- Anonymous Users: Disable access
- Everyone: Disable access
- Authenticated Users: Allow access
- Service Administrator: Control directory service configuration
- Data Administrators: Manage Organizational Units (OUs)

Note: On a Domain Controller, the SYSVOL and NETLOGON shares must have the NTFS permissions for the physical directory set to match the logical share permissions.

- **RAS (Remote Access Services)**

- o Leverage RAS policies such as validate CallerID.

- **Anti-Virus**

- o Exclude AD database and log files from being scanned. The files to be excluded and the registry values specifying their location are as below:

Exclude from Scan	HKLM\System\CurrentControlSet\Services\NTDS\Parameters
Ntds.dit	DSADatabaseFile
Edb*.log, Edb*.pat, Res.log, and Res2.log	DatabaseLogFilesPath
Temp.edb and Edb.chk	DSAWorkingDirectory
Ntds.pat	DSADatabaseFile

- o Exclude FRS database and log files from being scanned. The files to be excluded and the registry values specifying their locations are as below:

Exclude Files from Scan	HKLM\System\CurrentControlSet\Services\NtFrs\Parameters
Jet\sys\edb.chk, jet\ntfrs.jdb and jet\log*.log	WorkingDirectoryFile
Log*.log	DBLogFileDirectory
Exclude Folders from Scan	HKLM\System\CurrentControlSet\Services\NtFrs\Parameters\ReplicaSets\GUID
<i>replica_root</i>	ReplicaSetRoot
<i>staging_directory</i>	ReplicaSetStage
<i>preinstall_directory</i>	<i>replica_root</i> \DO_NOT_REMOVE_Ntfrs_Preinstall_Directory

- o If SYSVOL files are excluded from being scanned, then **enforce** script signing on DCs and administrative workstations. For more information on script signing, refer to the relevant Microsoft documentation (see references).

SQL Server

Top Hardening Suggestions:

- 1) Install latest applicable SQL Server service pack and security updates (SP3a or later)³.
- 2) Avoid running SQL Server on an Active Directory Domain Controller as outlined in the [AD section](#).
- 3) Set a strong password for the 'sa' account before installing the ICM software.
- 4) It is assumed that you have completed the [File System and Registry hardening](#) steps.
- 5) Limit privileges for SQL Server Service account, **MSSQLServer**.

Note: The following assumes the SQL Server has been installed prior with the service configured to run as the 'LocalSystem' Account (as specified in the ICM Staging Guide). It's possible these steps can be shortened if the SQL Server is installed initially to run using a least privileged account.

In addition, SQL Server can be configured to run using a local user account as opposed to a domain user account as specified below. A standard user account can be created using 'Local Users and Groups' and then configure SQL Server through Enterprise Manager to run the service under this least privileged account (see *SQL Server* referenced documentation).

- a. Create a Windows domain user account (e.g., <domain>\SQLServiceAcct>). This account should be added to Active Directory with default user privileges. Appropriate file system permissions (Modify) must be given to this user account for the \mssql\data directory to be able to create, expand or delete databases as needed by the 'icmdba' application.
- b. Configure [Security Account Delegation](#) in Active Directory (Users folder) for this account:
 - i. From the 'Account' property page, select 'Account is trusted for delegation'.
 - ii. Make sure 'Account is sensitive and cannot be delegated' is **NOT** selected.
- c. Configure [Security Account Delegation](#) in Active Directory (Computers folder) for each machine that has SQL (or MSDE) installed:
 - i. Select 'Trust computer for delegation' on the 'General' property page.
- d. Have a Domain Administrator configure [Security Account Delegation](#) using the **SetSPN** utility from the Windows 2000 resource kit to set a Service Principal Name as follows:
 - i. List the existing SPN for the machine by typing the following at a command prompt:

```
setspn -L <machine>
```

- ii. Delete any existing SPN for the MSSQLSvc entry by typing the following at a command prompt:

```
setspn -D "MSSQLSvc/<machine:port> <serviceaccountname>" <machine>
```

Note: The string inside quotes must match exactly what is seen in the List from step 1. The quotes must be used around the string.

- iii. Create a new SPN entry for the MSSQLSvc entry by typing the following at a command prompt:

```
setspn -A "MSSQLSvc/<machine:port> <serviceaccountname>" <machine>
```

³ Refer to the Bill of Materials for the compatible service pack for your product.

Example:

```
setspn -A "MSSQLSvc/CCLoggerA.cisco.com:1433 SQLServiceAccount"
CCLoggerA
```

Where:

"CCLoggerA.cisco.com" is the fully qualified domain name for the side A logger machine.

"SQLServiceAccount" is the domain account.

"1433" is the port used by SQL.

"CCLoggerA" is the target machine.

- e. Add the domain user account created in Step a. to the NTFS permissions for the Operating System and data partitions at the root level (e.g., C:\). Allow all permissions, **except** Full Control.
 - f. Finally, add this domain user account created in Step a. to the Registry permissions for the HKEY_LOCAL_MACHINE\Software, HKEY_LOCAL_MACHINE\System and HKEY_USERS hives, giving it Full Control.
 - g. From the SQL Server Enterprise Manager, configure the SQL Server service to run as the domain user account created in Step a. (e.g., <domain>\SQLServiceAcct>).
- 6) Disable SQL Server Agent Service, **SQLServerAgent**
- Note:** Applying SQL Server security updates or hotfixes may require that this service be enabled. It is recommended that this service should be reset to 'enabled' before performing the update. When the update has completed, stop the service and set it to back to 'disabled'.
- 7) Disable Distributed Transaction Coordinator, **MSDTC**
- Note:** The SQLServerAgent and MSDTC services may be used for 3rd Party Backup solutions therefore we recommend checking the Backup Agents' system requirements before disabling these services.
- 8) Use NTFS directory security with EFS for SQL Server data directories. EFS must be set while logged in under the account credentials that the SQL service will run under (e.g., <domain>\SQLServiceAcct>). From the Local Policy editor, temporarily grant 'logon locally' privileges to this account to enable EFS then remove this right after logging off. EFS should only be enabled if there is a concern with data theft as there will be a performance impact.
- Note:** In order to copy and send the data to other parties, it will be necessary to backup the database to a different directory that is not encrypted to ensure that the receiving party is able to read the data in the backup. This can be accomplished by exporting or backing up the database from the SQL Server Enterprise Manager.
- 9) Disable the SQL guest account.
- 10) Restrict **sysadmin** membership to your ICM administrators.
- 11) Block TCP port 1433 and UDP port 1434 at the firewall except for when the ICM distributor or administrative workstation is not in the same security zone as the ICM Logger.
- 12) Assign static ports to named instances of SQL (MSSQL\$<InstanceName>)
- 13) Protection by good housekeeping:
- a. Run the **KillPwd** utility to remove password data from setup files. Detailed instructions on how to run this utility can be found in KB Article Q263968 at <http://support.microsoft.com/default.aspx?scid=kb;en-us;263968>

- b. Delete or secure old setup files: Delete or archive the following files after installation: sqlstp.log, sqlsp.log, and setup.iss in the <systemdrive>:\Program Files\Microsoft SQL Server\MSSQL\Install folder for a default installation, and the <systemdrive>:\Program Files\Microsoft SQL Server\MSSQL\$<Instance Name>\Install folder for named instances.

If the current system is an upgrade from SQL Server 7.0, delete the following files: setup.iss in the %Windir% folder, and sqlsp.log in the Windows Temp folder.

- 14) Change the recovery actions of the Microsoft SQL Server service to restart after a failure.
- 15) Remove all sample databases, e.g., Pubs and Northwind.

Internet Information Server

Internet Information Server (IIS) is only required for two applications making up the ICM/IPCC solution targeted in this document, *WebView* and *Internet Script Editor*. The service should not be installed, or should be disabled, on any other node except for the Distributor as noted in the [Introduction](#). There are some exceptions in multi-media configuration of the solution. In this case, product documentation and system requirements must be followed.

WebView and IScript Editor

Top Hardening Suggestions:

- 1) IIS 5.0 is used as an intranet-only http server for the ICM product. It is expected that a firewall is deployed to protect external connections to the server.
- 2) Install the most recent compatible⁴ service pack and updates.
- 3) Disable the following non essential services:
 - File Transfer Service
 - E-mail Service
 - News Service

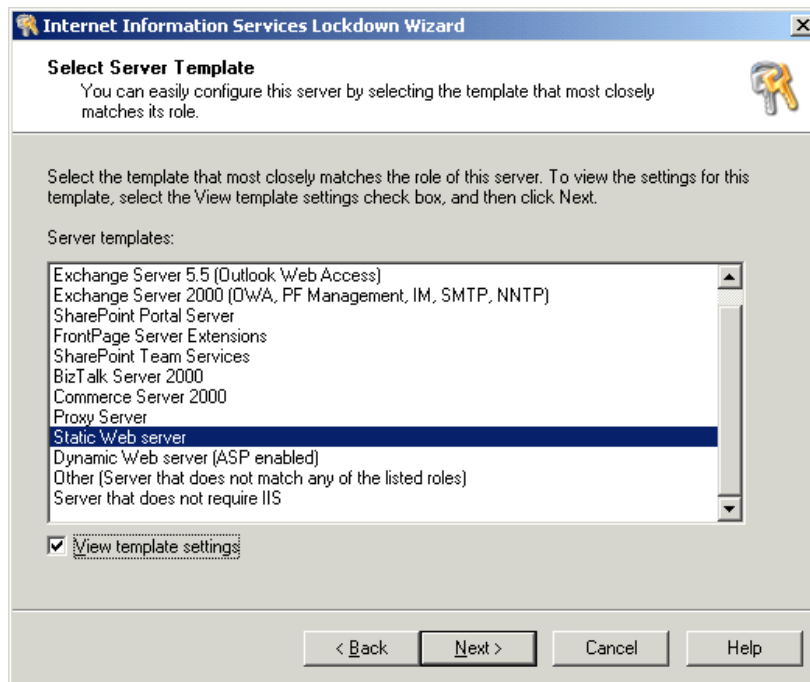
This can be accomplished using the IIS Lockdown tool as described below.

The following subcomponents of Internet Information Services (IIS) must be selected during the installation of the web server:

- Common Files
 - Internet Information Services Snap-In – for management purposes
 - Internet Services Manager (HTML) – for management purposes
 - World Wide Web Server
- 4) Complete the *File System and Registry* hardening steps before proceeding.

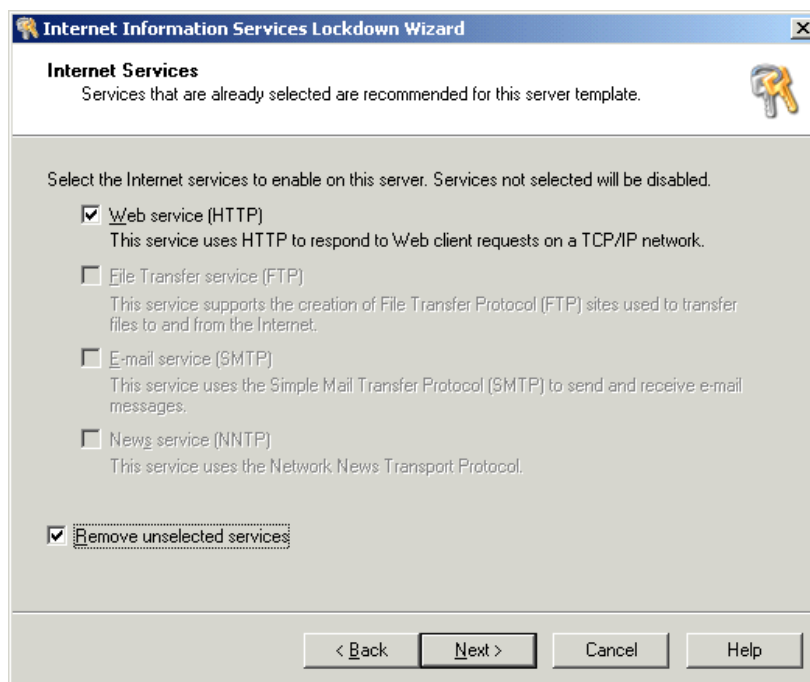
⁴ Refer to the Bill of Materials for the compatible service pack for your product.

- 5) Run the [IISLockDown](#) tool:
 - a. Select Static Web server template and select “View template settings” checkbox:

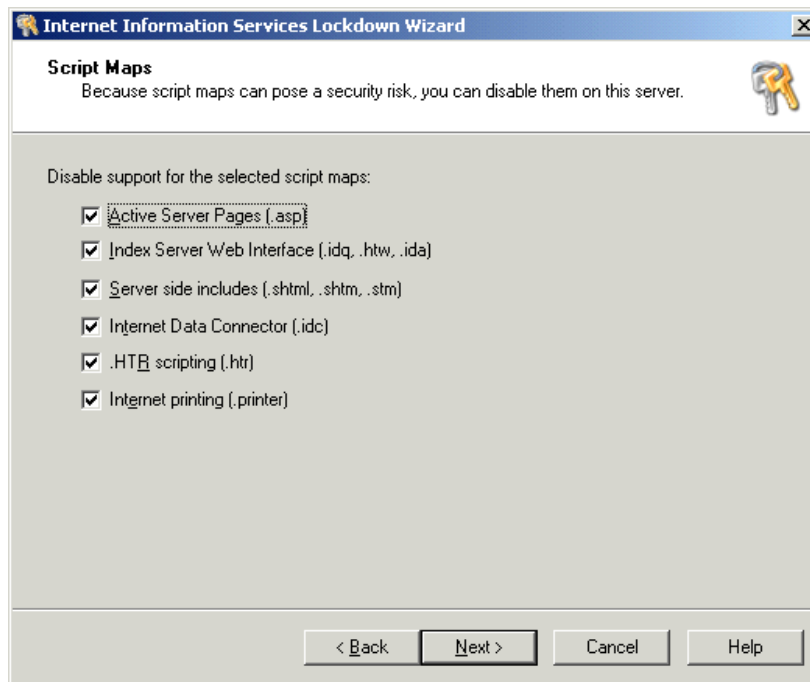


Note: On systems that **do not require** IIS you can use this tool to disable IIS by selecting the '*Server that does not require IIS*' template option.

- b. Disable all services except Web service:

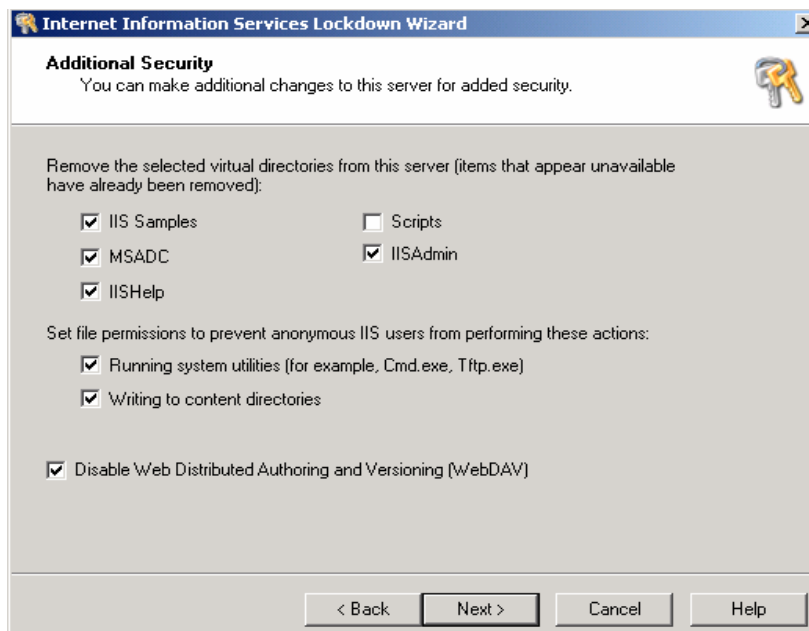


- c. Disable all unneeded script extensions:

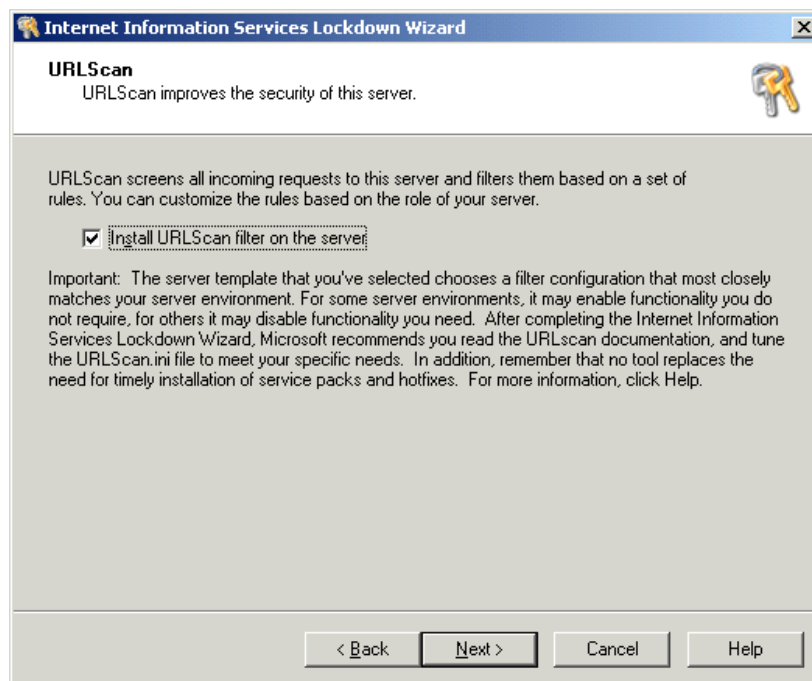


- d. Select all additional security options except for "Scripts":

Note that all selected virtual directories must be removed with the exception of the "Scripts" virtual directory.



- e. Install URLScan:



- 6) Click Finish to complete the wizard. Edit `<system_directory>\system32\inetsrv\urlscan\urlscan.ini` as follows:
- Change "AllowDotInPath=0" to "AllowDotInPath=1"
 - Add "POST" to the [AllowVerbs] section
 - Remove all entries under [DenyUrlSequences] section.

In addition to the above edits, the following additional changes are required depending on whether WebView or IScript Editor or both are going to be running on the computer.

WebView Only:

No additional changes are necessary.

IScript Editor Only:

- Change "UseAllowExtensions=0" to "UseAllowExtensions=1"
- Add these entries to [AllowExtensions]
 - .exe
 - .dll

WebView and IScript Editor:

- Change "UseAllowExtensions=0" to "UseAllowExtensions=1"
- Add these entries to [AllowExtensions]
 - .jhtml

- .jsp
- .AdminServlet
- .js
- .css
- .cab
- .psr
- .xml
- .zip
- .jar
- .
- .exe
- .dll

Note: This entry is a "dot"

7) Setting NTFS file permissions

This section assumes that you have already set the NTFS file permissions as specified in the *File System* section of this document. For instructions on how to set file permissions, refer to the *File System* section.

Set the NTFS permissions depending on whether only WebView or only IScript Editor or both are going to be running on the computer

a. WebView Only:

Add the "IUSR_<machine_name>", to have the following rights to these directories:

- Full Control for <icm_install_dir> (e.g. c:\icm)
- Read & Execute for <inetpub> (e.g. c:\inetpub)
- Full Control for <ServletExec_install_dir> (e.g. "C:\Program Files\New Atlanta")
- Read & Execute permission for <JDK directory> (e.g. c:\jdk1.3.1)
- Read permission for <EAServer directory> (e.g. "C:\Program Files\Sybase")
- Full Control for <EAServer directory>\EAServer\html\classes\com\cisco\atg

b. Internet Script Editor Only:

Add the "IWAM_<machine_name>" to have the following rights to these directories:

- Read & Execute permission for the Windows %SYSTEMROOT%\System32 directory
- Read & Execute permission for the Windows %SYSTEMROOT%\Registration directory

Add the <Machine>\Users to have the following rights to these directories:

- Read & Execute permission for the Windows %SYSTEMROOT%\System32 directory
- Read & Execute permission for the <icm_install_dir> e.g. c:\icm

c. WebView and Internet Script Editor:

Implement both of the "WebView Only" and "Internet Script Editor Only" sections above.

8) Setting Registry permissions

This section assumes that you have already set Registry permissions as specified in the [Registry Permissions](#) section of this document.

Use RegEdt32 to set the permissions depending on whether only WebView or only IScript Editor or both are going to be running on the computer

a. WebView Only:

Add the "IUSR_<machine_name>" account to have Read only rights to the HKEY_LOCAL_MACHINE\Software and HKEY_LOCAL_MACHINE\System hives.

b. Internet Script Editor Only:

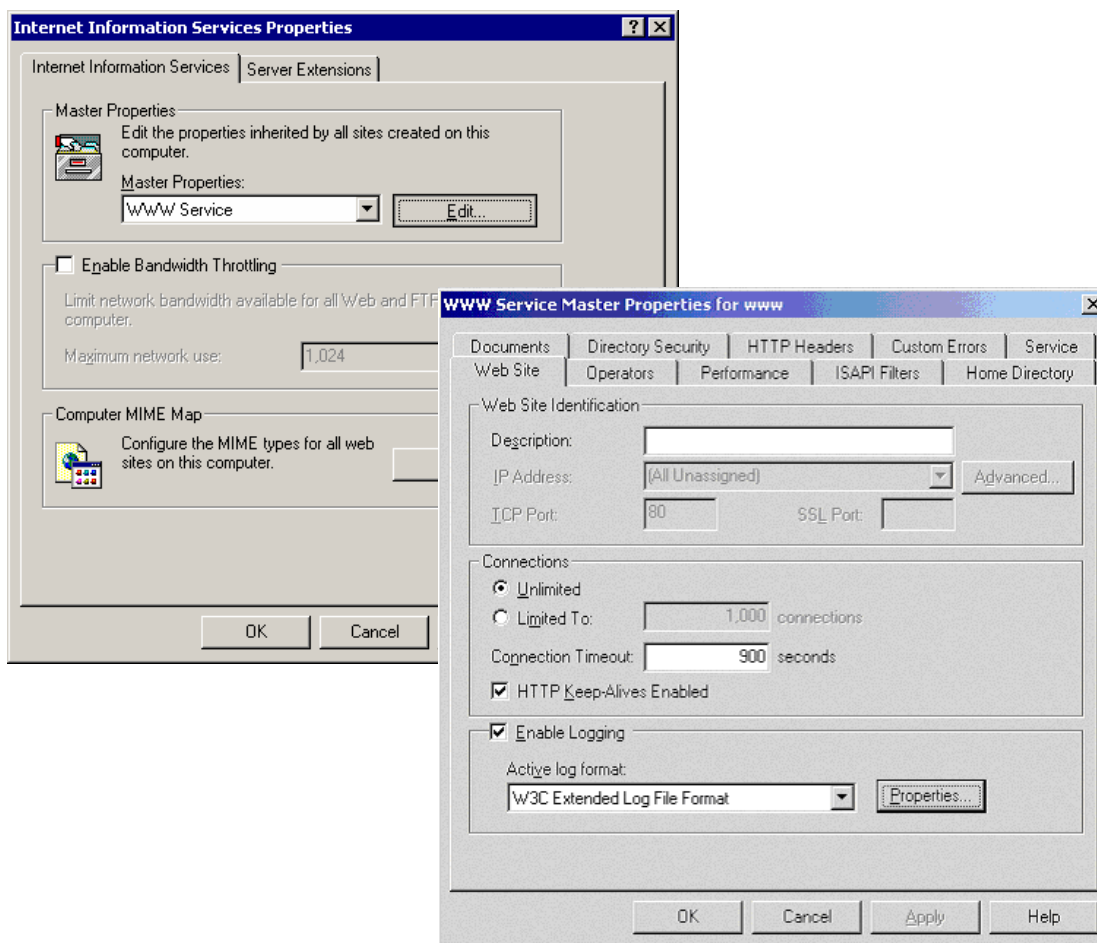
Add the "IWAM_<machine_name>" account to have Read only rights to the HKEY_LOCAL_MACHINE\Software and HKEY_LOCAL_MACHINE\System hives.

c. WebView and Internet Script Editor:

Implement both of the "WebView Only" and "IScript Editor Only" sections above.

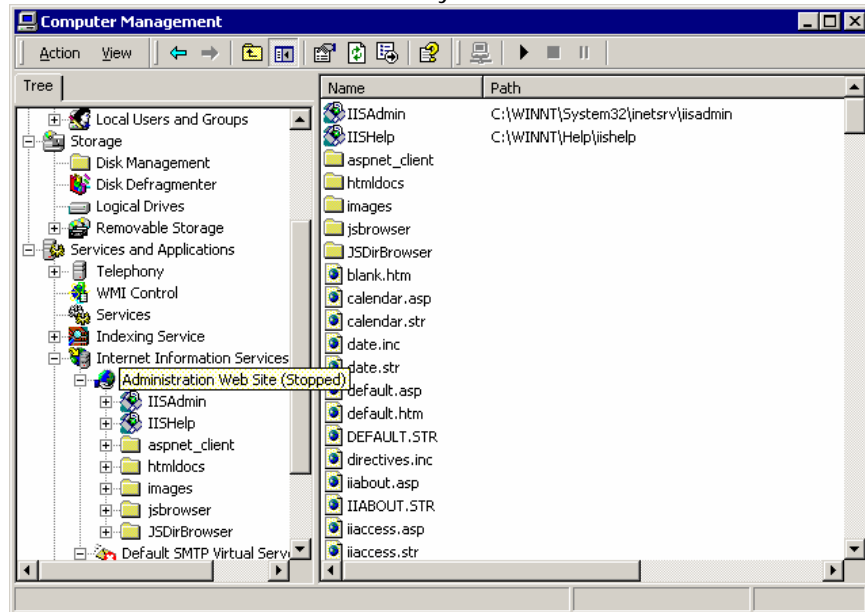
CAUTION: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Cisco cannot guarantee that you can solve problems that result from using the Registry Editor incorrectly. Use the Registry Editor at your own risk and make backups as appropriate.

- 9) Right click on "My Computer" and select Manage. Select Services and Applications > Internet Information Services. Right click on Internet Information Services and select Properties. Edit the Master Properties page for the 'WWW Service':



- a. Limit connections to 10 or the anticipated maximum concurrent number of users.

- b. Enable logging in extended-W3C format.
- c. Select logging properties > Extended properties and add 'Cookie', 'Referrer', and 'Win32 Status' checkboxes.
- d. Select the 'Home Directory' tab
 - i. Verify that 'Log visits' is enabled.
 - ii. In the 'Application Configuration' dialog box, click the 'App Options' tab, and then clear the 'Enable parent paths' check box.
- e. Select the HTTP Headers tab and remove any custom headers.



ServletExec (New Atlanta)

ServletExec is used by some ICM/IPCC Enterprise products such as WebView. Use these guidelines for hardening ServletExec with WebView **after** the installation of the ICM and Third-Party Tools:

Note: The Third-Party Tools and ICM/WebView for ICM Versions 5.0(0) and 6.0(0) contain the same versions of the middleware applications. However, the 6.0(0) installer will apply the first two hardening changes.

- 1) Removal of ServletExec's example servlets.

Deletion of these files from "<ServletExec_dir>\ServletExec ISAPI\Servlets":
<ServletExec_dir> is typically "C:\Program Files\New Atlanta"

AuthServlet.*
CookieServlet.*
DateServlet.*
EmailServlet.*
FilterServlet.*
ForwardServlet.*
IncludeServlet.*
JarServlet.*
PropertyServlet.*
SessionServlet.*
TestServlet.*

- 2) Removal of unused ServletExec servlets.

JIServlet
SSIServlet
TemplateServlet
UploadServlet

- 3) Limiting ServletExec administration to local machine only

If this default security setting needs to be changed, please follow these steps:

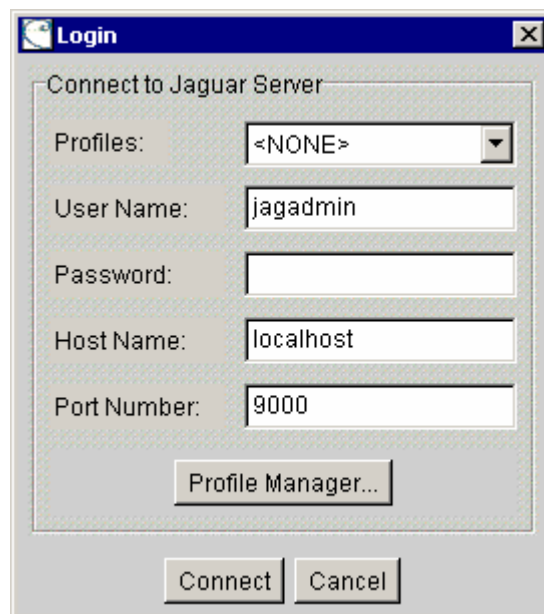
- a. Open Internet Explorer and go to http://<server_name>/servlet/admin
- b. Log on to ServletExec Admin Realm with User Name, Administrator and blank password
- c. Select "license & security" under "General".
In the "Allowed IPs:" field, replace "127.0.0.1" with the desired IP addresses. Use commas to separate multiple IP addresses; use the asterisk (*) wildcard character to denote a range of IPs.

Sybase EAServer (Jaguar)

Jaguar is used by some ICM/IPCC Enterprise products such as WebView. Use these guidelines for hardening Jaguar with WebView **after** the installation of the ICM and 3rd Party Tools:

Start Jaguar Manager

- Launch "Jaguar Manager" Application from Start > Program > Sybase > EAServer 4.1.1 > Jaguar Manager from the WebView Server Machine.
- Once the Jaguar Manager has started, click on Tools > Connect > Jaguar Manager.
- In the resulting dialog replace "localhost" in the "Host Name" field with the actual hostname or host IP address.
- Click 'Connect' button.



Changing Jaguar Password

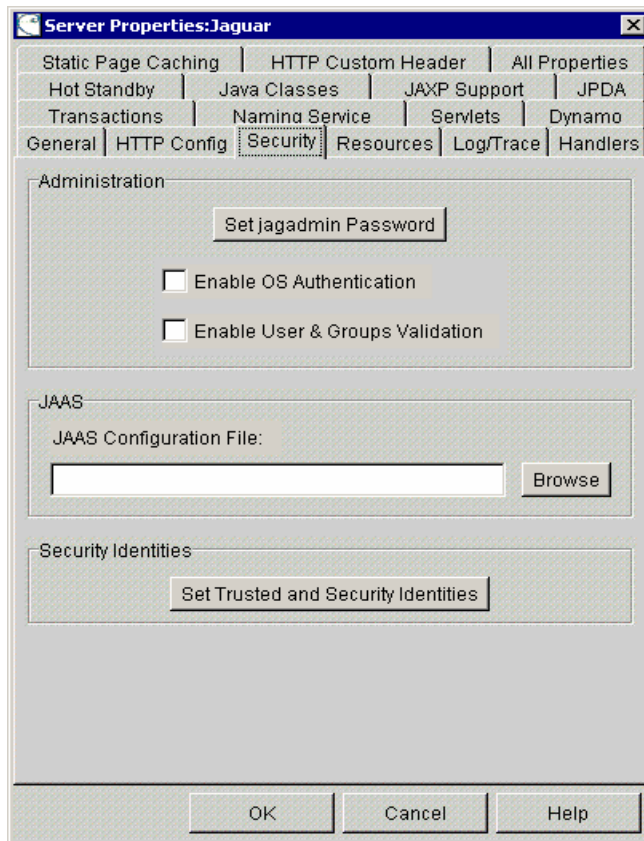
The password used to connect to the Jaguar service is changed in Jaguar Administration **and** in the jagconnection.properties file. The guidelines provided below to accomplish this are also provided in the reporting documentation (See WebView Installation Guide).

Note: If the password is changed, any subsequent reinstallation of ICM on a WebView server will prompt the user for the Jaguar Password.

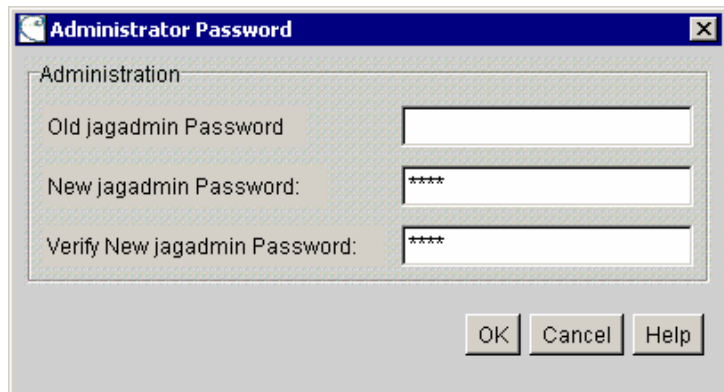
The 'jagadmin' password is modified in two steps:

1. Modify 'jagadmin' password on EAServer

- Using the tree on the left pane of Jaguar Manager, navigate to Jaguar Manager > Servers > Jaguar
- After selecting 'Jaguar' node, click on File->Server Properties... menu
- On the server properties dialog box, select 'Security' tab as shown below



- Click on 'Set jagadmin Password' button.
- On the 'Administrator Password' dialog box
 - Leave 'Old jagadmin Password' blank.
 - Enter new password in the 'New jagadmin Password' and 'Verify New jagadmin Password' fields.
- Click 'OK'



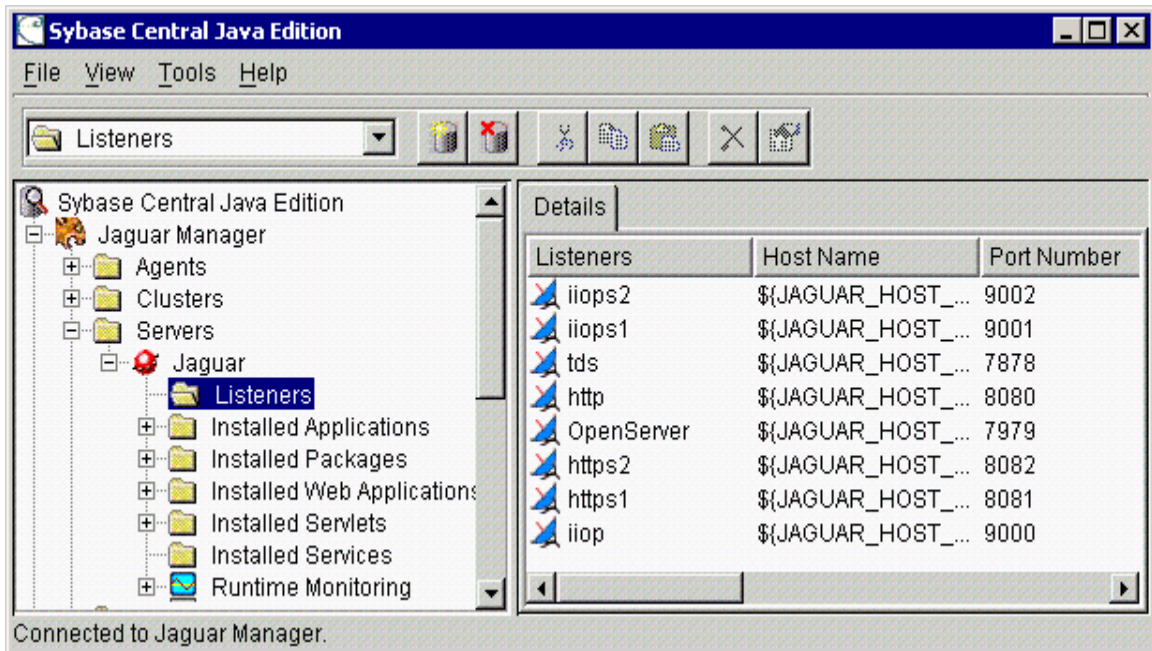
2. Modify 'jagadmin' password at WebView

- Using Windows Explorer, navigate to '<Sybase Home>\EAServer\html\classes\com\cisco\atg' directory (<Sybase Home> is typically 'C:\Program Files\Sybase').
- Open file 'jagconnection.properties' using Notepad or WordPad.
- Locate 'JAGCONNECT_JAGUAR_ADMIN_PWD' key in the properties file. By default it is blank.
- Enter the new jagadmin password from step 1 above in clear text. The modified key should look like 'JAGCONNECT_JAGUAR_ADMIN_PWD=<new password>'

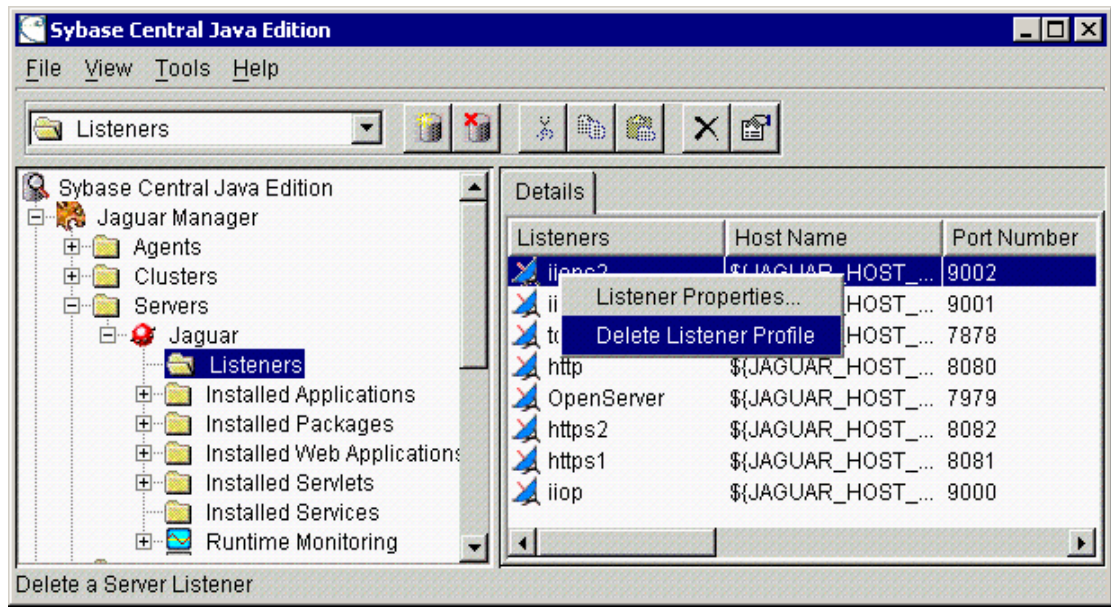
Note: The password entered in clear text gets encrypted when WebView runs for first time after the change.

Remove Unnecessary Listeners

- Using the tree on the left pane of Jaguar Manager, navigate to Jaguar Manager > Servers > Jaguar > Listeners
- This should list all the listeners in the right pane of Jaguar Manager as shown below



- Remove the following listeners by right clicking on each one of them and selecting "Delete Listener Profile":
 - Listeners to be removed
 - **Note:** Do not remove "iiop" Listener on Port Number 9000
 - iiops2
 - iiops1
 - tds
 - http
 - OpenServer
 - https2
 - https1



Note: The only listener remaining should be "iiop" listening on port 9000

Restart WebView/Services

- Close Jaguar Manager.
- Restart 'Jaguar' service from Windows Services panel.
- Restart 'IIS Admin' service from Windows Services panel (this will also restart 'World Wide Web' service automatically).

Tomcat

Tomcat is used by some ICM/IPCC Enterprise products, specifically the Support Tools Server, as its default web server. Use the following guidelines for hardening Tomcat.

Note: The Cisco Support Tools version 1.0(1) automatically applies the first two steps outlined here. After upgrading from Support Tools 1.0(0) to 1.0(1) or in the case of reinstallation, steps 3 and 4 will have to be repeated as the install process will overwrite the security changes.

- 1) Remove Tomcat's example applications.

Delete these directories from Tomcat (including sub-directories):

```
<supportTools_install_dir>\jakarta-tomcat-4.0.6\webapps\examples  
<supportTools_install_dir>\jakarta-tomcat-4.0.6\webapps\tomcat-docs  
<supportTools_install_dir>\jakarta-tomcat-4.0.6\webapps\webdav
```

- 2) Redirect `http://localhost:8188` to `http://localhost:8188/uiroot` to avoid Tomcat's default welcome page.

Replace the `index.html` in `<install_dir>\jakarta-tomcat-4.0.6\webapps\ROOT\index.html` with the following:

```
<html><head>  
<script>self.location.replace("/uiroot/index.jsp");</script>  
</head></html>
```

- 3) To protect username/password, use SSL for login. See Support Tools documentation for details on how to turn SSL on during login.
- 4) Restrict access via client IP address or host name.

Tomcat's "Remote Address Filter" enables one to specify a list of IP addresses (or regular expressions representing IP addresses) from which Tomcat will accept or deny requests.

To configure for IP restrictions, edit the file: `<supportTools_install_dir>\jakarta-tomcat-4.0.6\conf\server.xml`.

For example, the following will only allow access from the local machine (127.0.0.1) or IP addresses that begins with "161.44.79":

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"  
allow="127.0.0.1,161.44.79.*" />
```

Tomcat's "Remote Host Filter" enables one to specify a list of host names rather than IP addresses for restricted access.

For example the following will only allow access from `*.mycompany.com`

```
<Valve className="org.apache.catalina.valves.RemoteHostValve"  
allow="*.mycompany.com" />
```

Note: Use of the "Remote Host Filter" requires a reverse DNS lookup; therefore the DNS server with Reverse Lookup Zones must be setup and accessible from the server side.

These IP restriction lines should be placed below the following line in
< supportTools_install_dir >\jakarta-tomcat-4.0.6\conf\server.xml after installation.

```
<Valve className="org.apache.catalina.valves.AccessLogValve"  
directory="logs" prefix="localhost_access_log." suffix=".txt" pattern="common"  
/>
```

For more details on configuring the filters, see "Remote Address Filter" and "Remote Host Filter" at:

<http://jakarta.apache.org/tomcat/tomcat-4.0-doc/config/valve.html>

Internet Explorer

Using contact center servers for Internet browsing is not sound security practice because Internet browsing increases the exposure of your server to potential security attacks. Regardless of the browser you use, it is a good idea to restrict browsing on your server. To reduce the risk to your server of potential attacks from malicious Web-based content:

- Upgrade to Internet Explorer 6.0 and apply the latest service pack and security updates.
- Do not use servers for browsing general Web content.
- Use client computers to download files such as drivers and service packs.
- Do not view sites that you cannot confirm are secure.
- Use a limited user account instead of an administrator account for general Web browsing.
- Use Group Policy to keep unauthorized users from making inappropriate changes to browser security settings.

The following table highlights the recommended changes to default URL security zones.

URL Security Zone	Default Security Template in Windows 2000	Change to Match High Security Template
Internet	Medium	High
Local Intranet	Medium-low	Medium-low
Trusted Sites	Low	Medium
Restricted Sites	High	High

Each of these values can be changed on the **Security** tab of the **Internet Options** dialog box available from the **Tools** menu in Internet Explorer or from the Control Panel. When any of these values is changed, the **Restore Defaults** button allows users to revert the value to the secure default. To change:

- 1) Go to the **Tools > Internet Options** dialog
- 2) Select the **Security** tab
- 3) Select the **Zone** you want to change (for example, **Internet**)
- 4) Select **Custom Level...**
- 5) Change *Reset Custom Settings* to the new value (e.g., in the **Internet** zone, change **Medium** to **High**)
- 6) Select the **Reset** button to make the changes stick
- 7) Select **OK**
- 8) Repeat for the other Zones
- 9) Finally, click **OK** on Security tab to get out of the dialog

Note: If you go back and view the settings, you will see the *Reset Custom Settings* field populated with the Windows 2000 default value. This can be confusing, but the settings have been changed, as you can see if you closely examine each of the settings in the Settings list.

Advanced Settings

These settings should be made in Windows 2000 Server. To find these settings, select **Tools > Internet Options** and then select the **Advanced** tab.

Browsing:

- Enable Install On Demand (Internet Explorer): Not enabled
- Enable Install On Demand (Other): Not enabled
- Enable third-party browser extensions: Not enabled

Microsoft VM:

- JIT compiler for virtual machine enabled: Not enabled

Multimedia:

- Do not Display online content in the media bar: Enabled
- Play animations in web pages: Not enabled
- Play sounds in web pages: Not enabled
- Play videos in web pages: Not enabled

Security:

- Check for server certificate revocation: Enabled
- Check for signatures on downloaded programs: Enabled
- Do not save encrypted pages to disk: Enabled
- Empty Temporary Internet Files folder when browser is closed: Enabled

You should restart the browser after making these changes.

CAUTION: Any browsing from the servers that have undergone the above configuration changes will be blocked. In some cases, using Internet Explorer may be required on a PG to download, for example, the JTAPI plugin from a CallManager. This plugin must be installed on any computer that will host applications that access the CallManager via JTAPI. JTAPI is the standard programming interface for telephony applications written in the Java programming language. It may also be necessary to allow the servers to fetch security updates from a Windows Update Server, internal or external, depending on the patch management policy in use. In order to accommodate this safe browsing, we recommend that trusted sites are configured to allow reaching certain Web sites considered safe.

Please use the following steps to add a Web site to the Restricted Sites zone or Trusted Sites zone in Internet Explorer. Use a wild card to include all the domains in a specific domain.

1. Click Start, point to Settings, click Control Panel, and then double-click Internet.
2. Click the Security tab, click the Trusted Sites Zone or Restricted Sites Zone in the Zone box, and then click Add Sites.
3. Type an asterisk in place of the domain in a specific domain in the "Add this Web site to the zone" box. For example, you might type "http://*.microsoft.com" or "http://CallManager*" (without quotation marks).
4. Click OK, click OK, and then close Control Panel.

More details on how to use Security Zones in Internet Explorer can be found at [MSKB174360](#).

Remote Administration

Windows Terminal Services

Terminal Services permits users to remotely execute applications on Microsoft Windows 2000 Servers from a wide range of devices over virtually any type of network connection. It can be enabled to run in either Application Server or Remote Administration modes. ICM/IPCC only supports Remote Administration mode.

This section will only describe how to secure for remote administration access.

- 1) During Installation, select the **Permissions compatible with Windows 2000 server** option. This will restrict access to the registry and critical system files.
- 2) Do not select **Permissions compatible with Terminal Server 4.0 users** option. This is intended for legacy applications that may still require this type of open access.
- 3) After you install Terminal Services, ensure that the latest patches for Terminal Services are installed by visiting <http://windowsupdate.microsoft.com/> for an automated list of applicable patches or by visiting <http://www.microsoft.com/downloads/> to manually install the necessary updates. Although patches might have been applied after installing Windows 2000, it is important to apply the necessary patches that address specific vulnerabilities that might exist within Terminal Services.

Securing the RDP-TCP Connection

You can configure the properties of the terminal server's RDP-TCP connection to provide better protection. Run Terminal Services Configurator, select Connections, and then select RDP-TCP.

- 1) Restrict the number of client sessions that can remain active on the server.

From the Network Adapter tab, select Maximum connections and set the limit on the number of concurrent connections.

- 2) Set session time limits.

From the Sessions tab, check the first of three Override User Settings check box and set values for each of the following (all values are recommendations; use values that work best within your organization):

- a. End a disconnected session, 1 or 5 minutes.
 - b. Active session limit, 1 or 2 days.
 - c. Idle session limit, 30 minutes.
- 3) Set permissions for users and groups on the terminal server.

Use the Permissions tab to add users, groups and computers access limits and permissions. Click Add, select the user, group or computer name, and then set one of three basic permissions:

- a. Full Control (given to administrators and the system; allows logging onto the terminal server, modifying the connection parameters, connecting to a session, getting session info, resetting or ending a session, logging off other users, remotely controlling other users' sessions, sending messages to other users, and disconnecting sessions).
 - b. User Access (given to ordinary users; allows logging onto the terminal server, getting session info, connecting to a session or sending messages to other user sessions).
 - c. Guest Access (for restricted users; allows logging onto the terminal server).
- 4) Optionally, restrict reconnections of a disconnected session to the client computer from which the user originally connected.

From the Sessions tab, check the last of three Override User Settings check boxes and set Allow reconnection from previous client.

- 5) Optionally, configure encryption levels to High.

From the General tab, set Encryption level to High. Use this option only if there is a risk that communications can be eavesdropped.

Per-User Terminal Services Settings

You can configure a number of per-user terminal services settings for each user. Using Active Directory Users and Computers, right click on a user and then select properties

- 1) On the Terminal Services Profile tab, set a user's right to logon to terminal server by setting the Allow logon to terminal server checkbox. Optionally, create a profile and set a path to a terminal services home directory.
- 2) On the Sessions tab, set session active and idle time outs.
- 3) On the Remote Control tab, set whether a remote session can be remotely viewed and controlled by administrators and whether a user's permission is required.

Telnet

Windows 2000 Telnet Server allows Telnet clients to connect to a server, log onto that server, and run character-mode applications such as the ICM troubleshooting and tracing tools (dumplog, procmon, etc.). The Telnet server included with Windows 2000 supports a maximum of two Telnet clients at any given time. The Services for UNIX add-on pack supports a maximum of 63. This addition is not a tested or supported configuration on Windows servers running the ICM applications.

The Telnet service is set to manual by default. Unless intended to be used as an integral part of administering the server, it should be disabled. It is worth noting that Microsoft recommends making use of Windows Terminal Services instead of Telnet given the latter's all clear-text communication.

Authentication

You can use your local Windows 2000 user name and password or domain account information to access the Telnet server. The security scheme is integrated into Windows 2000 security. If you do not use the NTLM authentication option, the user name and password are sent to the Telnet server as plain text.

If you are using NTLM authentication (default), the client uses the Windows 2000 security context for authentication and the user is not prompted for a user name and password. The user name and password are encrypted.

Administration

If you are installing Telnet only to allow access to TAC or other customer support, it is recommended that clients install Cisco ICM Support Tools in place of Telnet service. Contact your partner or Cisco Sales for Cisco ICM Supports Tools.

The Microsoft recommended solution for restricting access to a Windows 2000-based computer through Telnet is to follow these steps as described in Article ID 250908. Telnet uses clear text passwords which is inherently unsafe.

Create a local user group, and then add the users that are to have access to the Windows 2000-based computer through Telnet. Follow these steps:

1. In Control Panel, double-click **Administrative Tools**, and then double-click **Computer Management**.
2. Expand **Local Users And Groups**, and then click **Groups**.
3. Click **Action**, and then click **New Group**.
4. In the **Group Name** box, type **TelnetClients**.
5. In the **Description** box, type a description of the group.
6. Click **Add**, and then add the users who are to have Telnet access to the computer.
7. Click **Create**, and then click **Close**.

Note: When there is a TelnetClients group, only users who are members of this group have Telnet access to the computer, unless those users are administrators of the computer. Members of the Administrators group will always have access via Telnet regardless of their membership, or lack thereof, in the TelnetClients group.

pcAnywhere

Note: The following discussion applies to all approved versions of pcAnywhere⁵.

Security is one of the most important considerations in implementing a remote control solution.

pcAnywhere addresses security in the following ways:

- 1) Restricting access to internal machines
- 2) Preventing unauthorized connections to a pcAnywhere host
- 3) Protecting the data stream during a remote control session
- 4) Preventing unauthorized changes to the installed product
- 5) Identifying security risks
- 6) Logging events during a remote control session

1) Restricting access to internal machines

One of the best ways to ensure security is to restrict connections from outside your organization. pcAnywhere is the only remote control product to provide the following two ways to accomplish this objective:

- Limiting connections to a specific TCP/IP address range
pcAnywhere hosts can be configured to only accept TCP/IP connections that fall within a specified range of addresses.
- Serialization
A feature that enables the embedding of a security code into the pcAnywhere host and remote objects created. This security code must be present on both ends for a connection to be made.

2) Preventing unauthorized connections to a pcAnywhere host

The first line of defense in creating a secure remote computing environment is to prevent unauthorized users from connecting to the host. pcAnywhere provides a number of security features to help you achieve this objective.

Authentication	Authentication is the process of taking a user's credentials and verifying them against a directory or access list to determine if the user is authorized to connect to the system.
Mandatory passwords	pcAnywhere now requires a password for all host sessions. This security feature prevents users from inadvertently launching an unprotected host session.
Callback security (for dial-up connections)	pcAnywhere lets dial-up users specify a call-back number for remote control sessions. In a normal pcAnywhere session, the remote connects to the host, and the session begins. When callback is enabled, the remote calls the host, but then the host drops the connection and calls back the remote at the specified phone number.

⁵ Refer to the Bill of Materials for the versions qualified and approved for your release of ICM.

Settings	Default	Change to	Description
Restrict connections after an end of session	No	(Optional)	With pcAnywhere, host users can prevent remote users from reconnecting to the host if the session is stopped due to a normal or abnormal end of session.
Wait for anyone and secure by	Yes	Yes	
	No	Yes (Lock computer)	

Security Options	Default	Change to	Description
Connection Options			
Prompt to confirm connection	No	(Optional)	This feature prompts the host user to acknowledge the remote caller and permit or reject the connection. By enabling this feature, users can know when someone is connecting to their host computer. This will depend on the remote administration policy of whether users must be physically present at the server being remotely accessed.
Login Options			
Make password case sensitive	No	Yes	Lets you use a combination of uppercase and lowercase letters in a password. This setting applies to pcAnywhere Authentication only.
Limit login attempts per call	3	3	pcAnywhere lets host users limit the number of times a remote user can attempt to login during a single session to protect against hacker attacks.
Limit time to complete login	3	1	Similarly, host users can limit the amount of time that a remote user has to complete a login to protect against hacker and denial of service attacks.
Session Options			
Disconnect if inactive	No	Yes (2 minutes)	Limits time of connection. pcAnywhere lets host users limit the amount of time that a remote caller can stay connected to the host to protect against denial of service attacks and improper use.

3) Protecting the data stream during a remote control session

Encryption prevents the data stream (including the authorization process) from being viewed using readily available tools.

pcAnywhere offers three levels of encryption:

- pcAnywhere encryption
- Symmetric encryption
- Public key encryption

Encryption Configuration

Security Options	Default	Change to	Description
Encryption			
Level	<None>	Symmetric	Lists the following encryption options: <u>None</u> : Sends data without encrypting it. <u>pcAnywhere encoding</u> : Scrambles the data using a mathematical algorithm so that it cannot be easily interpreted by a third party. <u>Symmetric</u> : Encrypts and decrypts data using a cryptographic key. <u>Public key</u> : Encrypts and decrypts data using a cryptographic key. Both the sender and recipient must have a digital certificate and an associated public/private key pair.
Deny lower encryption level	No	Yes	Refuses a connection with a computer that uses a lower level of encryption than the one you selected.
Encrypt user ID and password only	No	No	Encrypts only the remote user's identity during the authorization process. This option is less secure than encrypting an entire session.

4) Preventing unauthorized changes to the installed product

Integrity checking is a feature that, when enabled, verifies that the host and remote objects, DLL files, executables, and registry settings have not been changed since the initial installation. If pcAnywhere detects changes to these files on a computer, pcAnywhere will not run. This security feature guards against hacker attacks and employee changes that might hurt security.

5) Identifying security risks

Symantec's Remote Access Perimeter Scanner (RAPS) lets administrators scan their network and telephone lines to identify unprotected remote access hosts and plug security holes. This tool provides administrators with a way to access the vulnerability of their network in terms of remote access products. Using RAPS, you can automatically shut down an active pcAnywhere host that is not password protected and inform the user.

6) Logging events during a remote control session

You can log every file and program that is accessed during a remote control session for security and auditing purposes. Previous versions only tracked specific pcAnywhere tasks such as login attempts and activity within pcAnywhere. The centralized logging features in pcAnywhere let you log events to pcAnywhere log, NT Event Log (NT & Windows 2000 only), or an SNMP monitor.

VNC

SSH Server allows the use of VNC through an encrypted tunnel to create secure remote control sessions. However, this configuration is currently not supported. The performance impact of running an SSH server has not been determined. It will, however, be planned for future support.

Microsoft Security Updates

Automatically applying security and software update patches from third-party vendors is not without risk. Although the risk is generally small, subtle changes in functionality or additional layers of code may alter the overall performance of Contact center products.

ICM/IPCC customers are specifically cautioned to not automatically enable Microsoft Windows Update. The update schedule can conflict with other ICM/IPCC activity. Users should only apply those updates that are recommended by Cisco. However, customers can use Microsoft Software Update Service or similar patch management products to selectively approve Critical and Important patches that have been qualified by Cisco.

Cisco categorizes and qualifies third-party security updates as they are released by the manufacturer. While some updates clearly impact ICM/IPCC products, it is important to realize that not all updates are critical, important, or impact ICM/IPCC products. To help guide customers, updates are placed in one of these four categories:

1) Impacting

ICM/IPCC product impact testing is performed within a predefined window of when the security update is released by the third-party vendor. The security update must match the following conditions:

- The update is labeled by the vendor as Critical or Important or is otherwise of special interest
- It potentially affects some ICM/IPCC product component or functionality (or is basic to the OS and affects all operations for any software)
- It must apply to the latest ICM/IPCC specified Service Pack(s)

2) Not Impacting

ICM/IPCC products are not impacted by the security update and no further testing is performed. The security update must match the following conditions:

- The update is labeled by the vendor as Critical or Important or is otherwise of special interest
- It does not affect any ICM/IPCC component or functionality or any basic OS functionality
- It must apply to the latest ICM/IPCC specified Service Pack(s)

3) Deferred

Validation is typically deferred to the next Service Release, Maintenance Release, and subsequent Major/Minor Releases. The security update must match the following conditions:

- The update is labeled by the vendor as Moderate or Low
- It affects some ICM/IPCC component or functionality (or is basic to the OS and affects all operations for any software)

- It must apply to the latest ICM/IPCC specified Service Pack(s)

4) Not Applicable

The security update does not apply to any current ICM/IPCC product. No further qualification is required. The security update must match the following conditions:

- The security update does not apply to the latest ICM/IPCC Specified Service Pack(s), regardless of ICM/IPCC product applicability or vendor-rated severity.

All third-party qualification notices are sent as Field Notices.

Microsoft Service Pack Policy

Do not automatically apply Microsoft Service Packs for the Operating system or SQL Server. Cisco qualifies service packs through extensive testing and defines compatible service packs in each product's Bill of Materials.

Anti-Virus

Cisco recommends that only approved Anti-Virus (AV) software products be used⁶. Many of the default AV configuration settings can adversely affect product performance as a result of increased CPU load, memory, and disk usage by the Anti-Virus software program. Cisco tests specific configurations to maximize product performance.

Viruses can be unpredictable and Cisco cannot assume responsibility for consequences of virus attacks on mission-critical applications. Particular care should be taken for systems that use Microsoft Internet Information Server (IIS): Cisco Web Collaboration Option, Cisco Media Blender, Cisco E-Mail Manager Option, and Cisco WebView. In addition, your corporate Anti-Virus strategy should include specific provisions for any server positioned outside the corporate firewall or subject to frequent connections to the Public Internet.

Special considerations for configuring Anti-Virus applications on domain controllers can be found in the Active Directory section.

Guidelines and Recommendations

The general guidelines provided below can be applied to any AV application version in use. The next sections will outline specific configuration steps for Virus Scan Enterprise version 7.0 and Trend Micro ServerProtect version 5.5x.

- 1) The Anti-Virus software should not be set to run in an "automatic" or "background" mode where all incoming data or modified files are scanned in real time.
- 2) Full scans of systems by the Anti-Virus software should be set to run **only** during scheduled maintenance windows.
- 3) Anti-Virus software scanning engines and definition files should be updated on a regular basis, following your organization's current security/Anti-Virus policy.

ICM Maintenance Parameters

Before scheduling Anti-Virus software activity on Cisco ICM nodes, it is important to note a few parameters that control the application's activity at specific times. Anti-Virus software configuration settings should avoid scheduling "Daily Scans," "Automatic DAT Updates," and "Automatic Product Upgrades" during the times specified as described below.

Logger

Check the Schedule settings for the Purge and Update Statistics registry keys on the ICM Logger:

Logger registry keys:

[HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<inst>\
Logger<A/B>\Recovery\CurrentVersion\Purge\Schedule\Schedule](#)
Value Name: Schedule

⁶ Refer to the Bill of Materials for the application and version qualified and approved for your release of ICM.

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\Logger<A/B>\Recovery\CurrentVersion\UpdateStatistics\Schedule
Value Name: Schedule

Distributor

Check the Schedule settings for the Purge and Update Statistics registry keys on the Distributor nodes:

Distributor registry keys:

HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\CurrentVersion\Recovery\CurrentVersion\Purge\Schedule
Value Name: Schedule

HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\CurrentVersion\Recovery\CurrentVersion\UpdateStatistics\Schedule
Value Name: Schedule

Router/PG

On the ICM Router and Peripheral Gateway (PG), do not schedule Anti-Virus program tasks:

- During times of heavy or peak call load.
- At the half hour and hour marks, as ICM processes increase during those times.

All Nodes

Other scheduled ICM processes activities can be found on Windows 2000 servers by inspecting the Scheduled Tasks Folder. Scheduled Anti-Virus program activity should not conflict with those ICM scheduled activities.

File Exclusions

There are a number of binary files that are written to during the operation of ICM processes that have little risk of virus infection. Files with the following file extensions can be safely omitted from the drive and on-access scanning configuration of the Anti-Virus program:

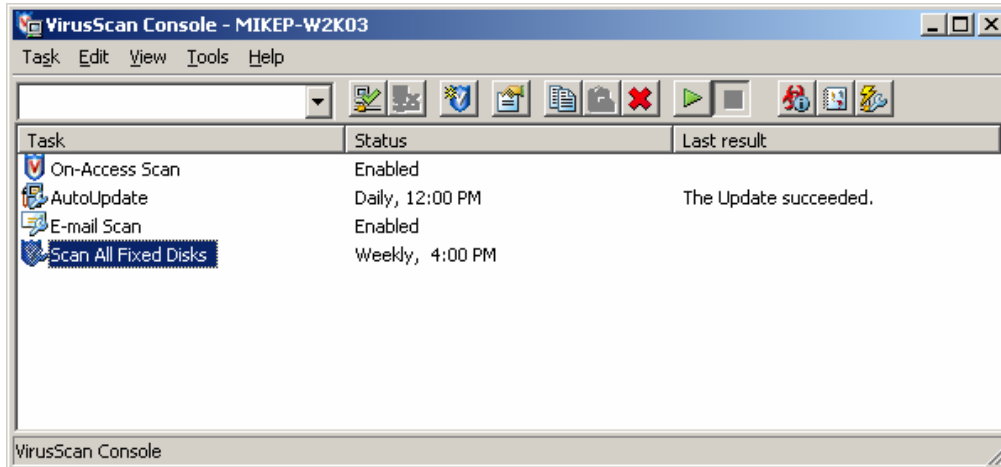
*.hst applies to PG

*.ems applies to ALL

VirusScan Enterprise 7.0

The following instructions apply to Network Associates' VSE 7.0 products.

- 1) Start Netshield Console: Start > Programs > Network Associates > VirusScan Console



- 2) Select Scan All Fixed Disks and press Enter

- 3) **Detection Tab:**

What to Scan

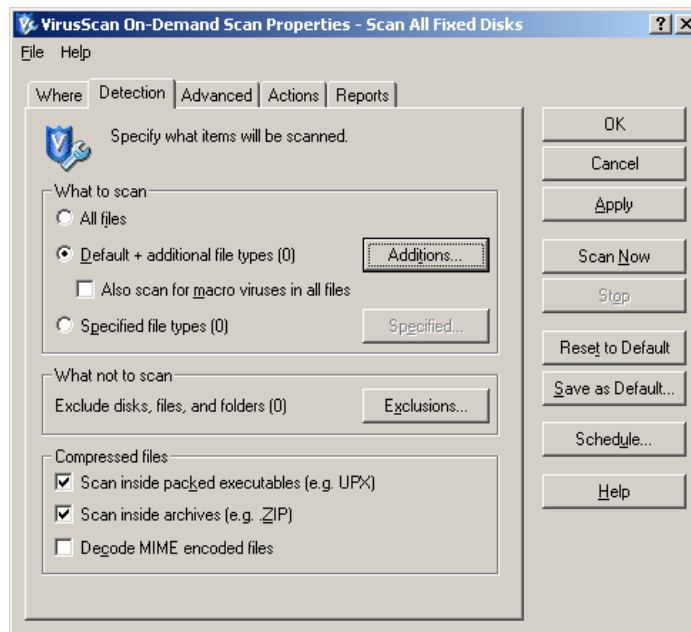
- Select, Default

What Not to Scan

- Select Exclusions, Add
- Add *.EMS files and add specific log directories under \icm
- Add *.HST files and add specific log directories under \icm

Compressed files

- Select, Scan inside packed executables
- Select, Scan inside archives (e.g., ZIP)



4) **Advanced Tab:**

Heuristics

- Select, Find unknown program viruses
- Select, Find unknown macro viruses

Non-Viruses

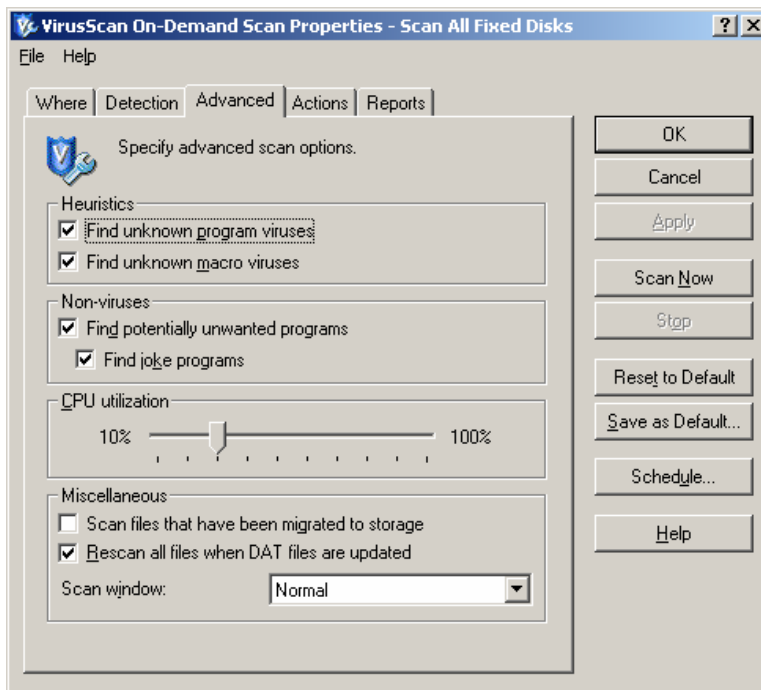
- Select, Find potentially unwanted programs
- Select, Find joke programs

CPU Utilization

- Select under 20%

Miscellaneous

- Select, Rescan all files when DAT files are updated



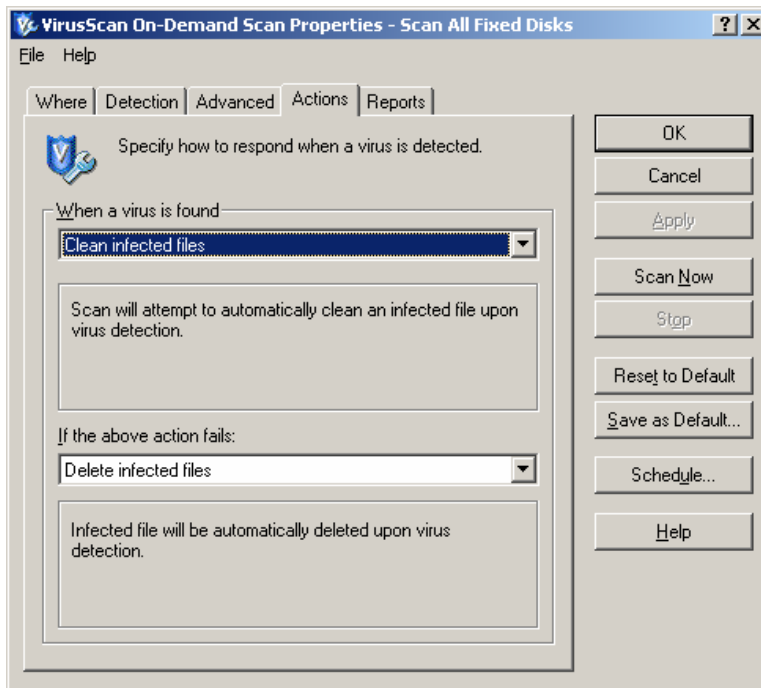
5) **Actions Tab:**

When a Virus is found

- Select, Clean infected files

If the above action fails

- Delete infected files

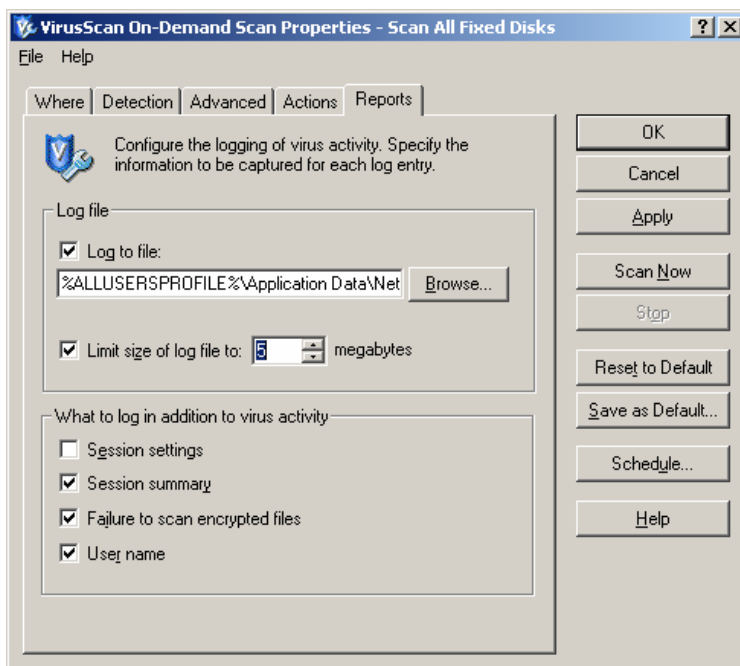


6) Reports Tab:

Log file

- Select, Log to file
- Select, Limit size of log file to 5 MB or greater recommended

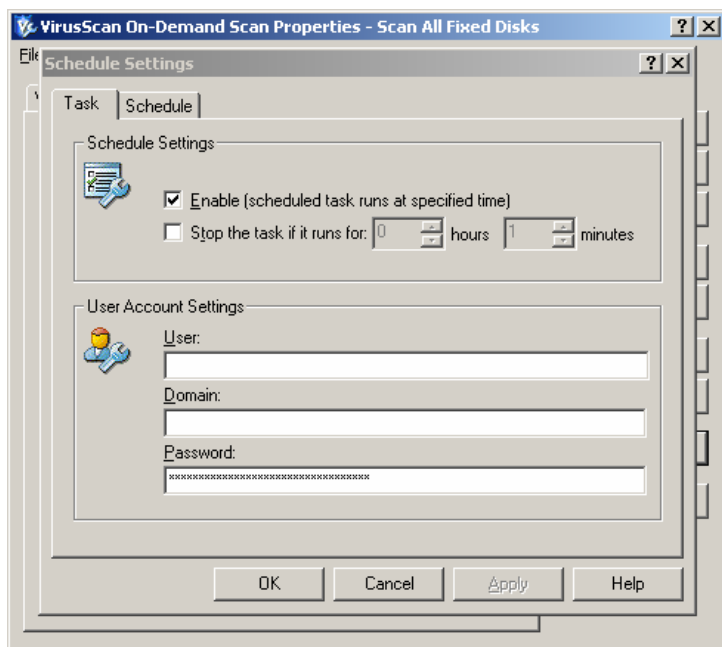
Set 'Apply' to apply changes



7) Schedule Button:

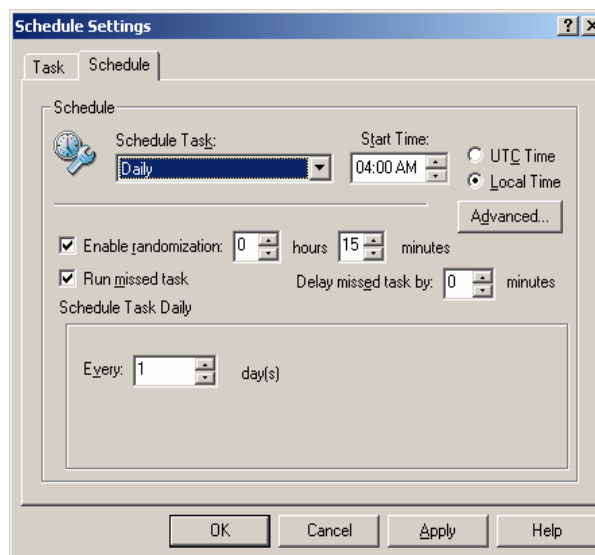
Task Tab:

- Select Enable scheduled task runs at specified time



Schedule Tab:

- Select a schedule that does not conflict with ICM maintenance
- Select Daily



Click Ok

8) AutoUpdate

AutoUpdate tasks update virus definitions (DAT files) and scan engines. Before scheduling the task, ensure that the AutoUpdate repository list is configured. You can use the AutoUpdate repository list to download the most recent dat file updates, scanning engine upgrades, HotFixes, and/or product upgrades. The AutoUpdate repository list specifies repositories and configuration information necessary to perform an update task.

8.a To add or edit a repository in the AutoUpdate repository list:

1. Open the VirusScan Console.
2. Select Tools > Edit AutoUpdate Repository List.
3. Select the Repositories tab. *The ftp repository is the default site. The http repository is the fallback site.*
4. To add or edit an AutoUpdate repository list, choose from the following:
 - o To add a repository, click Add to open the Repository Settings dialog box.
 - o To edit a repository, highlight it in the Repository Description list, then click Edit to open the Repository Settings dialog box.
5. In the Repository description box, enter the name or description for this repository.
6. In the Retrieve files from area, select the repository type or path from the following choices:
 - o **HTTP repository.** *This option is selected by default.* Use the http repository location you designate below as the repository from which you retrieve the update files.
 - o **FTP repository.** Use the ftp repository location you designate below as the repository from which you retrieve the update files.
 - o **UNC path.** Use the unc path you designate below as the repository from which you retrieve the update files.
 - o **Local path.** Use the local site you designate below as the repository from which you retrieve the update files.
7. In the Repository details area, the information you enter depends on the repository type or path you selected in the Retrieve files from area.
 - o If you selected **HTTP repository** or **FTP repository**:

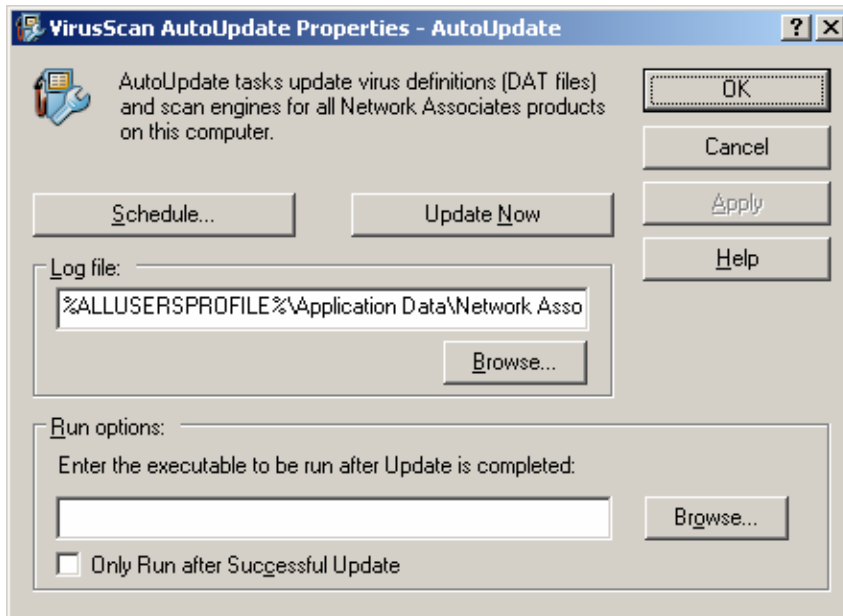
In the 'Repository details' area, enter the path to the repository you selected, the port number, and specify security credentials for accessing the repository.

- o URL. Enter the path to the http or ftp repository location as follows:
 1. **HTTP.** Enter the location for the http server and directory where the update files are located. The default McAfee http repository for dat file updates is located at: <http://download.nai.com/products/commonupdater>
 2. **FTP.** Enter the location for the ftp server and directory where the update files are located. The default McAfee ftp repository for dat file updates is located at: <ftp://ftp.nai.com/commonupdater>
- o Port. Enter the port number for the http or ftp server you selected.
- o 'Use authentication' or 'Use anonymous login'. *The title differs depending on whether you have selected HTTP path or FTP path.* Specify security credentials for accessing the repository. Next enter a 'User name' and 'Password', then 'Confirm password'.

Click 'OK' to save your changes and return to the 'AutoUpdate Repositories List' dialog box.

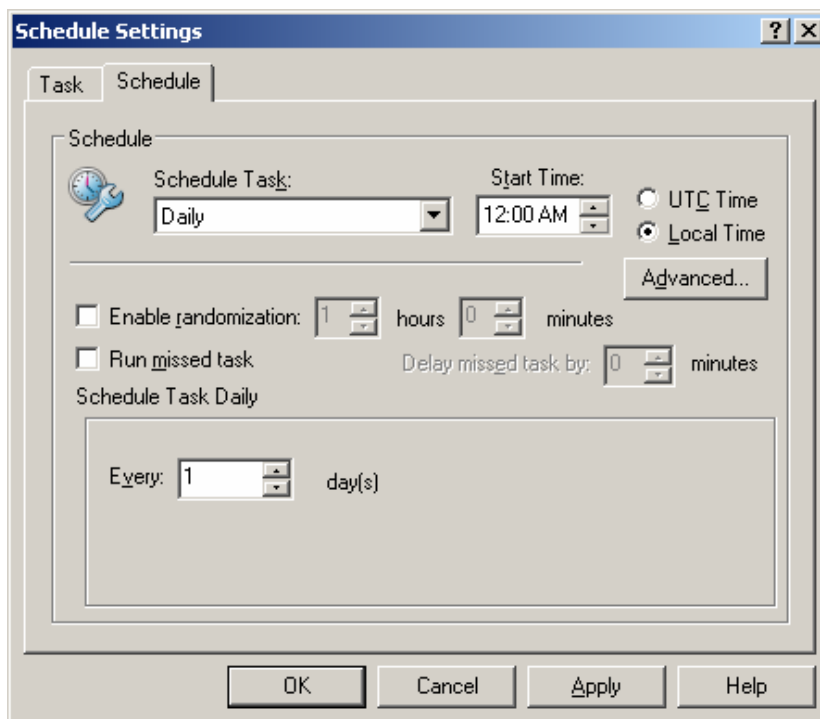
8.b To edit or add an AutoUpdate Task follow these steps:

Select the AutoUpdate Task in the console and press Enter (create the task if it doesn't exist).



Select 'Schedule'

Ensure the Task is enabled (on the Task tab) and click the Schedule tab



Configure the Schedule Task to start at a non-peak call routing time

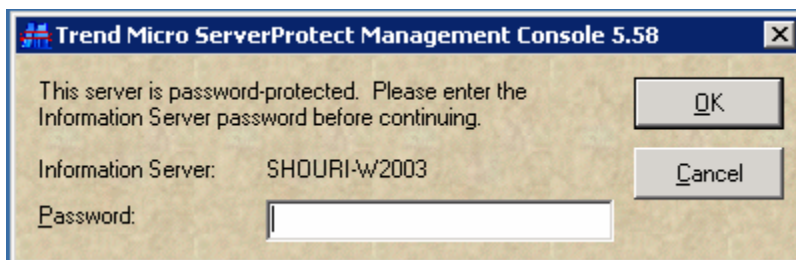
Trend ServerProtect 5.5

Trend Micro ServerProtect consists of a Management console, ServerProtect Information server and ServerProtect clients (called "Normal Servers"). The Management Console allows a password-protected logon to the ServerProtect Information Server.

The Information Server administers other ServerProtect clients using Remote Procedure Call (RPC) to connect to Windows 2000/NT servers. The management console allows the administrator to manage all the ServerProtect clients in a domain.

How to setup Virus scan Trend Micro ServerProtect

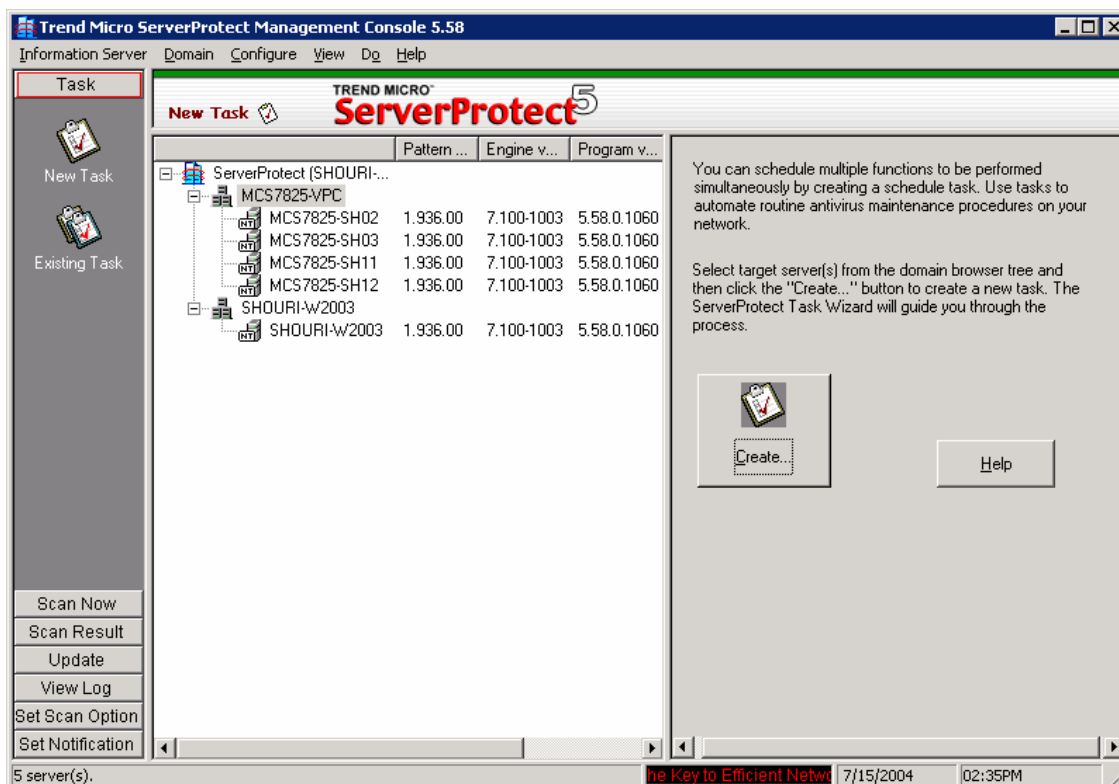
- 1) Start > Programs > Trend ServerProtect Management Console > ServerProtect Management Console



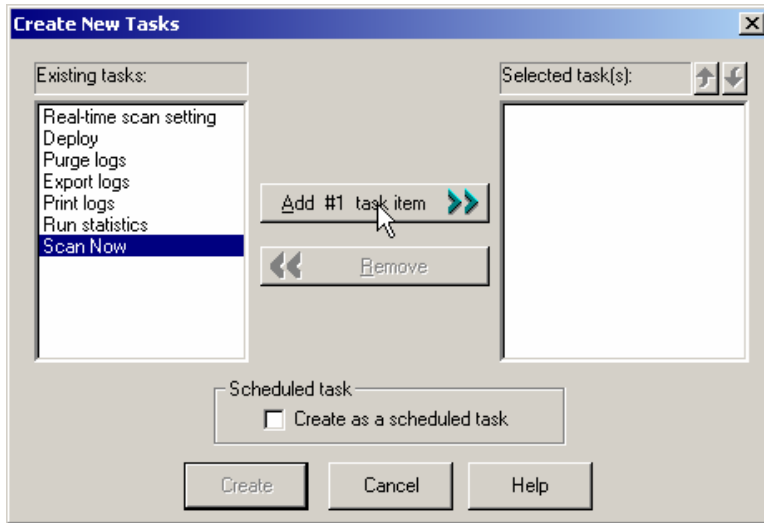
Enter the console password.

The Management console window appears as shown below. This management console has to be used to setup the Scan task on all the servers in the domain.

- 2) Select the domain from the domain browser tree. Click on the Create button in the right pane.



- 3) Select Scan Now and click on Add #1 task item.
Check the box "Create as a scheduled task". Click on Create button.

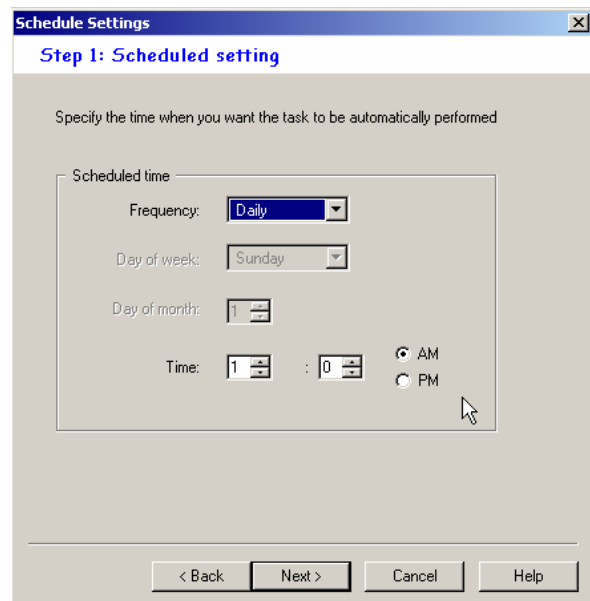


- 4) The Task Wizard appears as shown in figure below:



Click Next >

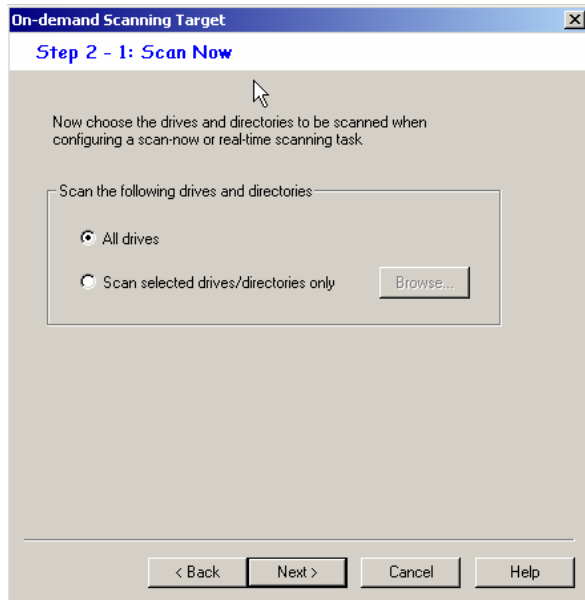
Step 1: Scheduled setting



Select the Frequency as Daily and a time that does not conflict with ICM maintenance.

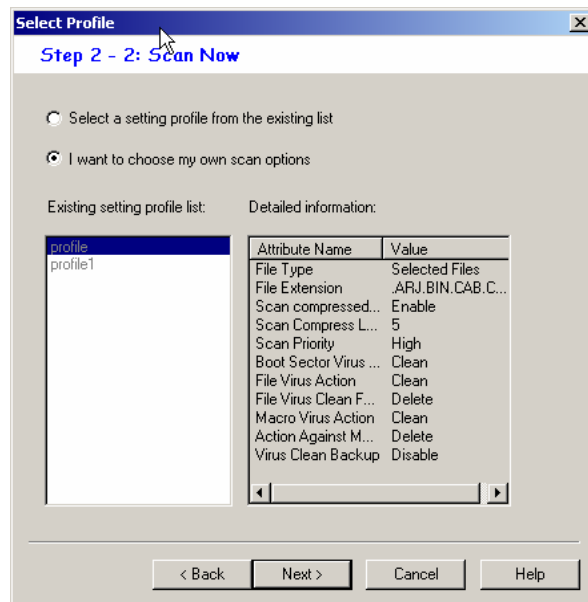
Click on Next >

Step 2 – 1: Scan Now



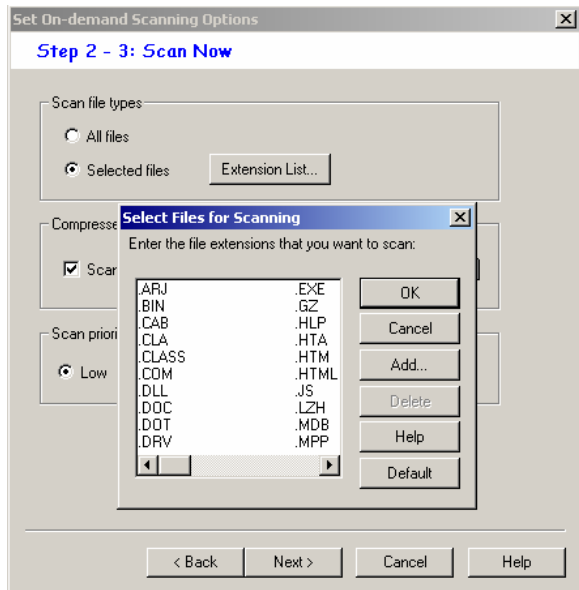
Select "All drives" and click Next >

Step 2 – 2

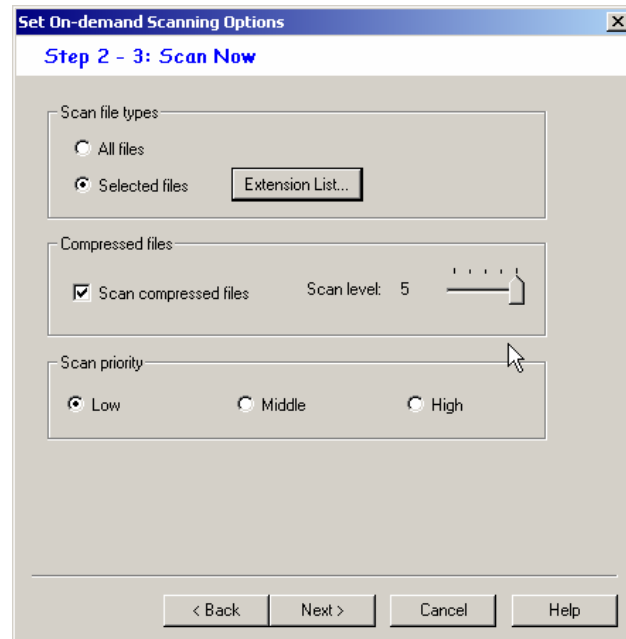


Select "I want to choose my own scan options" and click Next>

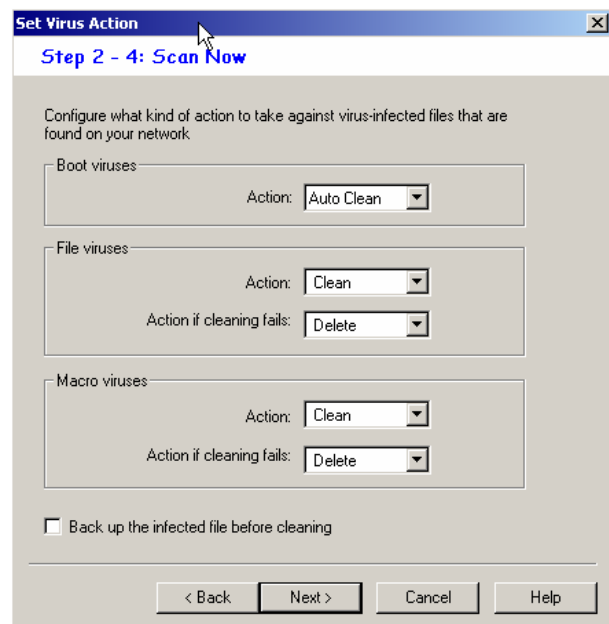
Step 2 – 3



Choose the option "Selected files" and open the Extension List window. Click on the Default button.



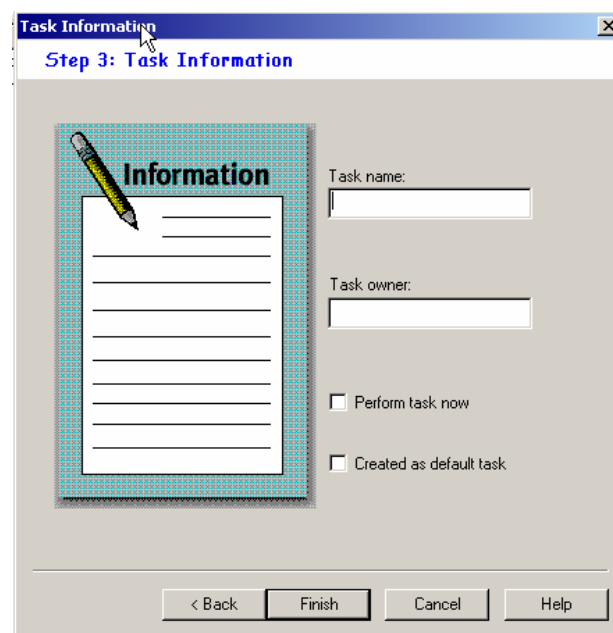
Check the box "Scan compressed files", set Scan level to 5 and Scan priority to Low. Click on Next >

Step 2 – 4

In the Set Virus Action window, select the 'Auto Clean' as Action for Boot, File and Macro viruses, and 'Delete' as Action if cleaning fails.

Click on Next button.

The Scan options and Virus list window appears. Click on Next again.

Step 3: Task Information

In the Task information window, you can enter the Task name and Task owner for reference. Check the box "Created as default task" option and click Finish

Setting File Exclusion List for Scan Task

In the left pane, select 'Set Scan Option', click on 'Exclusion List' and select the server in the middle pane. In the right pane, under the Excluded directory list, add the log directories under "icm\" to exclude on the right pane. Click Apply.

Updating the product, Engine and Virus Pattern file

Updating Trend Micro has two steps- Download and Deploy

The process involves downloading all the updates on to the Trend Server and then deploying it to the Normal servers.

A. Download

1. Select update on the Left Pane.
2. Click on update
3. Click on configure and verify that the download source is: -
" <http://serverprotect-t.activeupdate.trendmicro.com/activeupdate>"

4. Go to the schedule setting tab. Set the frequency as daily and select a time, which does not conflict with the ICM maintenance.

Note: Major release upgrades of the product have to be done manually to the local machine and then uploaded to Trend using the Download Now option.

B. Deploy

1. Select update on the Left Pane.
2. Click on update
3. Click on deploy now.
4. By default only the Pattern will be enabled for deployment. Enable both program and engine too for deployment.
5. Click on deploy for deploying the updates to the normal servers.
6. Deployment of updates can be configured as a scheduled job.
7. Click on configure under deploy.
8. Select new task
9. Add "Deploy" as the task item and enable "create as a schedule task"
10. Specify the frequency for deployment as Daily and select the time at least 1 hour after the download time.
11. Select virus pattern, scan engine and program for deployment.
12. Give a name and save the task

Intrusion Prevention System – CSA

The Cisco Security Agent (CSA) is a Cisco security product which provides Host Intrusion Detection and Prevention for servers. As high-visibility network security attacks like Code Red and the SQL Slammer worm have shown, traditional host and desktop security technologies are limited in their capability to combat the effects of new and evolving virus attacks. Unlike traditional signature-matching security technologies, the Cisco Security Agent analyzes virus behavior to provide robust protection with reduced operational costs. By identifying and preventing malicious behavior before it can occur, Cisco Security Agent removes potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications.

The Agent provides protection for Windows platforms based on rule sets or "policies" which have been tuned by an Administrator or developer for a given set of applications. These policies define which actions on the system are allowed or denied. The Cisco Security Agent checks any action using system resources by any program against the policy and blocks "denied" actions before any system resources are accessed and acted upon. Policies provide administrators with the ability to control access to system resources based on the following parameters:

- What resource is being accessed
- What operation is being invoked
- Which application is invoking the action

The resources in question may be either system resources or network Resources. CCBU has carefully tuned a policy for the Cisco Security Agent which will protect a host server without interfering with the normal operations of ICM applications.

The Cisco Security Agent can be used as either a "Standalone Agent" or a "Managed Agent". A Managed Agent reports all significant events back to a centralized "Management Center", which services Agents running on many servers simultaneously. The Management Center allows the administrator to monitor and protect many servers using one convenient Browser-based console. A Standalone Agent provides the same protection as a Managed Agent, but does not report events back to a central server. Rather, events are only logged locally on the host server.

Cisco is providing the "Standalone Agent" free of charge for use with Cisco ICM software. The Standalone Agent uses a static policy that cannot be changed or viewed by an administrator. We recommend that customers install the ICM Standalone Agent on any servers hosting ICM 6.0(0) applications.

The "Managed Agent" approach is appropriate for customers who need to use Third-party software not approved by Cisco for ICM 6.0(0) servers. These customers should purchase and install the CSA Management Center (CSA MC). They can then import the ICM policy into the Management Center and customize this policy to allow their Third-party applications to function properly with CSA. The ICM 6.0(0) policy for CSA can be downloaded from CCO.

CSA should not be viewed as providing complete security for servers hosting Cisco ICM software. Rather, it should be viewed as an additional line of defense which, when used with other standard defenses, such as virus scanning software, firewalls, and the hardening guidelines in this document, provides enhanced security for host servers.

For further information about the Cisco Security Agent, please refer to the document "**Installing Cisco Security Agent for Cisco Intelligent Contact Management Software, Release 6.0(0)**" available from CCO. More information on Cisco Security Agent is available at www.cisco.com/go/csa.









Baseline – MBSA

The Microsoft Baseline Security Analyzer (MBSA) evaluates your system's configurations and provides a report with specific recommendations to improve server security. MBSA v1.2 will recommend missing hotfixes and configuration changes related to both the core operating system and optional services such as IIS, SQL Server, and Internet Explorer. Use MBSA to identify vulnerabilities in your system's initial configuration, and run it regularly to find new vulnerabilities.

The recommendations provided in this document are in line with the baseline parameters the Security Analyzer uses to scan Windows machines. There are events which the MBSA reports which are deemed by Cisco to be permissible given the functionality of the application. The following are results from an MBSA security report on an ICM server. Some items were omitted as they related more to auditing or general policies. The recommendation is to review this table and any other event details before implementing a change.







Computer name: DOMAINMachine_Name
IP address: *.*.*.
Security report name: DOM - MACHINE (1-22-2004 1-55 PM)
Scan date: 1/22/2004 1:55 PM
Scanned with MBSA version: 1.2.3316.1
Security update database version: 2004.01.20.0
Office update database version: 11.0.0.6004
Security assessment: Severe Risk (One or more critical checks failed.)






Windows Scan Results Vulnerabilities

Score	Issue	Result
	Automatic Updates	Updates are automatically downloaded, but not automatically installed on this computer. This warning is acceptable depending on the Windows Automatic Update policy.
	Restrict Anonymous	Computer is running with RestrictAnonymous = 1. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security. This warning is acceptable. Setting a value of 2 will have adverse effect on Windows networking functionality. This setting is <u>not</u> supported.
	Administrators	More than 2 Administrators were found on this computer. This warning can be ignored given that the ICM application requires the addition of certain groups to the Local Administrators group, therefore triggering this event. It is recommended that you review the Result Details and remove any known unnecessary accounts.
	Password Expiration	Some user accounts (9 of 16) have non-expiring passwords. A similar warning will result if the default Domain Group Policy is left unchanged in terms of allowing the creation of accounts without expiration policies.
	Internet Connection Firewall	Internet Connection Firewall is not installed or configured properly, or is not available on this version of Windows.
	File System	All hard drives (1) are using the NTFS file system.
	Autologon	Autologon is not configured on this computer.
	Guest Account	The Guest account is disabled on this computer.

SQL Server Scan Results Instance (default)






Vulnerabilities

Score	Issue	Result
	Domain Controller Test	SQL Server and/or MSDE is running on a primary or backup domain controller. This warning is a result of not following the security recommendation outlined in this document to avoid running SQL Server on a domain controller. This is a security risk that <u>can</u> be remedied by removing the ICM applications requiring a database server from the DC.
	Sysadmins	More than 2 members of sysadmin role are present. This warning is acceptable. The ICM installation adds members to the sysadmin role and therefore this is a requirement of the application and should not be changed.
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are members of the local Administrators group or run as LocalSystem. This is the result of not implementing the least privileged account recommendation in the SQL Server section of this document. Microsoft recommends that SQL Server service is run under a different account than the default LocalSystem. This <u>can</u> be changed without negative impact to the application if the steps outlined in the SQL Server section are followed.
	Sysadmin role members	BUILTIN\Administrators group is part of sysadmin role. This is acceptable because the application adds certain groups to the local Administrators account on the server which require dbo access to the database.
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode). The recommendation is to <u>not</u> make changes to the SQL Server authentication mode as outlined here. The ICM application checks on initialization and requires that the authentication is set to "Mixed Mode". Note: This will be corrected in a future Service or Major release.
	Guest Account	The Guest account is enabled in 2 databases. This is the result of not removing the sample databases "Northwind" and "Pubs". The recommendation is to <u>remove</u> these databases or remove the Guest account access from these databases. To remove the Guest account access from databases <ol style="list-style-type: none"> 1. Click Start, point to Programs, point to Microsoft SQL Server, and then click Enterprise Manager. 2. Double-click Microsoft SQL Servers, and then double-click SQL Server Group. 3. Click the Databases folder, click the database that you want to secure, and then click users. 4. In the right pane, right-click Guest, and then click Delete.

	Exposed SQL Server/MSDE Password	The 'sa' password and SQL service account password are not exposed in text files.
	SQL Server/MSDE Account Password Test	No SQL user accounts have weak passwords.
	Registry Permissions	The Everyone group does not have more than Read access to the SQL Server and/or MSDE registry keys.
	CmdExec role	CmdExec is restricted to sysadmin only.
	Folder Permissions	Permissions on the SQL Server and/or MSDE installation folders are set properly.

Internet Information Services (IIS) Scan Results

Vulnerabilities

Score	Issue	Result
	MSADC and Scripts Virtual Directories	Scripts virtual directory was found under one or more web sites. This is an expected and acceptable warning. Scripts directory is needed for ServletExec ISAPI extension for WebView. It is not needed for ISE if ISE is running by itself without WebView.
	IIS Lockdown Tool	The IIS Lockdown tool has been run on the machine.
	Sample Applications	IIS sample applications are not installed.
	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present.
	Parent Paths	Parent paths are not enabled.

Auditing

Accounts

Auditing policies can be set to track significant events, such as account logon attempts. It helps to understand what events occurred on a system and in what time frame. Local auditing policies are always overwritten by Domain policies. The two sets of policies should be identical where possible. Local policies should also always be set.

Use Start > Programs > Administrative Tools > Local Security Policies to set local policies.

Under Audit Policy, set the following:

- 1) Audit account logon events, set Success and Failure
- 2) Audit account management, set Success and Failure
- 3) Audit directory service access, set Failure
- 4) Audit logon events, set Success and Failure
- 5) Audit object access, set Failure
- 6) Audit policy change, set Success and Failure
- 7) Audit privilege use, set Failure
- 8) Audit process tracking, set Failure
- 9) Audit system events, set Failure

Periodically, approximately once a week, view the Security Event log.

Go to Start> Programs > Administrative Tools > Event Viewer, select Security log, and check for any unusual activity such as Logon failures, or Logon success for unusual accounts.

SQL Server

Audit connections to SQL server [Auditing for SQL](#):

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/dbsql/sql2kaud.asp>

Active Directory Audit Policies

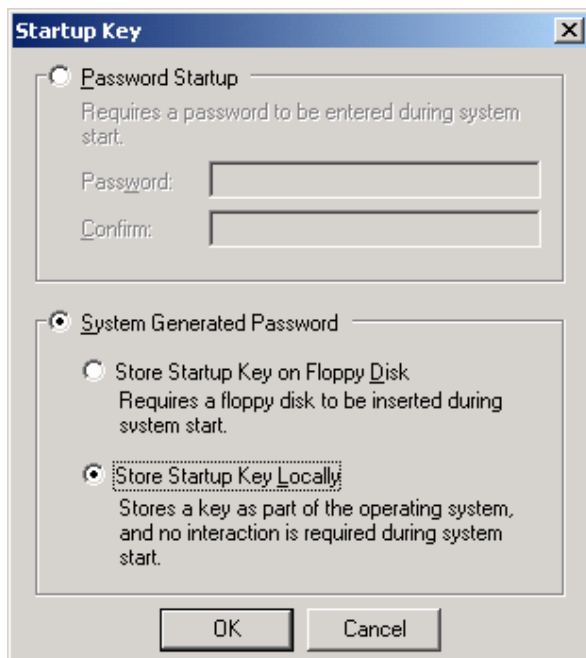
- Audit account management and logins, and monitor audit logs and proactively respond to audit findings.
- The following table contains the recommended and default DC Audit policies:

Policy	Default Setting	Recommended Setting	Comments
Audit account logon events	No auditing	Success and Failure	Account logon events are generated when a domain user account is authenticated on a Domain Controller.
Audit account management	Not defined	Success	Account management events are generated when security principal accounts are created, modified, or deleted.
Audit directory service access	No auditing	Success	Directory services access events are generated when an Active Directory object with a system access control list (SACL) is accessed.
Audit logon events	No auditing	Success and Failure	Logon events are generated when a domain user interactively logs onto a Domain Controller or when a network logon to a Domain Controller is performed to retrieve logon scripts and policies.
Audit object access	No auditing	(No change)	
Audit policy change	No auditing	Success	Policy change events are generated for changes to user rights assignment policies, audit policies, or trust policies.
Audit privilege use	No auditing	(No change)	
Audit process tracking	No auditing	(No change)	
Audit system events	No auditing	Success	System events are generated when a user restarts or shuts down the Domain Controller or when an event occurs that affects either the system security or the security log.

Other Security Considerations

Syskey

Syskey enables the encryption of the account databases. It is recommended that this utility is used to secure any local account database. The only option that can be implemented is the 'System Generated Password' using the 'Store Startup Key Locally' option as shown below:



Third-Party Security Providers

ICM software has been qualified with the Operating System implementations of NTLM, Kerberos V and IPSec security protocols. Third-party security provider implementations are not supported at this time.

Third-Party Management Agents

Server vendors such as HP and IBM include in their server operating systems installation agents to provide convenient manageability and server monitoring. For instance, HP's ProLiant Servers run "Insight Management Agents for Windows", while IBM includes the "IBM Director Agent". Among other things, these and other agents run on the systems and enable the gathering of detailed inventory information about servers, including operating system, memory, network adapters and hardware.

Cisco recommends that these agents only be used during off-peak hours or maintenance windows to reduce the risk of system resource usage. Cisco recommends that, when qualified, these agents should be installed and configured in a secure state (not on by default, in some cases) according to the vendors' security guidelines. The agents should be kept up-to-date as security vulnerabilities are plugged in newer releases.

CAUTION: It's important to note that these management agents should be configured in accordance to the Anti-Virus policy whereas polling or intrusive scans should not be executed during peak hours. Preferably, these should be scheduled during the system's maintenance window.

Note:

The installation of SNMP services is recommended by these 3rd Party Management Applications to take full advantage of the management capabilities provided with your servers. Failing to install or disabling SNMP prevents enterprise management applications such as Insight Manager from receiving hardware pre-failure alerts and disables certain application functions, such as advanced ProLiant status polling, inventory reporting, and version control in HP Insight Manager.

Some references:

Director 4.1 Installation and Configuration Guide (IBM Director Security)

ftp://ftp.pc.ibm.com/pub/pccbbs/pc_servers_pdf/dir41_install.pdf

HPInsight Management Agents User Guide

<ftp://ftp.compaq.com/pub/products/servers/management/imaug.pdf>

HP Software Security Customer Advisories

<http://h18013.www1.hp.com/products/servers/management/mgtsw-advisory.html>

Appendix

Hardening the RMS Listener

The RMS Listener receives data from remote Logger or SDDSN nodes using either a TCP/IP LAN connection or a RAS dial-up modem connection and NetBEUI. The data is transferred using a file copy process over this connection. As a result, a writeable file share must be configured on the RMS Listener.

- 1) It is assumed that you have followed the general hardening procedures in this document.
- 2) It is also assumed that you have two NTFS partitions, one for the OS and one for the remote data transfer.
- 3) The OS partition should be hardened to allow only <machine>\Administrators and SYSTEM accounts for file system and registry permissions as described earlier in this document.
- 4) Create a local group called <machine>\ListenerAccounts.
- 5) Create a local account for the duplex Listener to use to connect to this Listener with basic user rights (e.g., <machine>\ListenerAcct).
- 6) Add this account to the <machine>\ListenerAccounts group and remove this account from <machine>\Users group.
- 7) From the ListenCfg utility configure the other Listener to connect to this Listener using this account. **Note:** The domain would be the name of this machine. For example, if this is the side A Listener and the machine name was *ListenerSideA*, you would configure the side B Listener to connect to *ListenerSideA\ListenerAcct*.
- 8) For each customer system that will connect to the RMS Listener, create a local account with basic user rights (e.g., <machine>\Acme_ICMUser). **Note:** If remote access (modem) is used, this account will need dial-in permissions.
- 9) Add these customers to the local <machine>\ListenerAccounts group and remove these accounts from the <machine>\Users group.
- 10) No registry access is needed for this group.
- 11) Create the identical group and accounts on both Side A and Side B RMS Listener systems.
- 12) The root of the remote data partition (e.g., F:\) should be configured to allow the SYSTEM account Full Control.
- 13) At the root of the remote data partition (e.g., F:\), the <machine>\Administrators and <machine>\ListenerAccounts groups should have ONLY: 'List Folder Contents', 'Read' and 'Write' permissions. Do NOT give 'Full', 'Modify' or 'Read & Execute' rights. This will prevent inadvertent launching of a virus that might have been copied from a remote system to the RMS Listener.
- 14) The logical share to the remote data partition (e.g., 'FF') should be configured for Full Control with the <machine>\ListenerAccounts and SYSTEM accounts having access. Note that the NTFS permissions will further restrict the physical access to this share.
- 15) Enable Remote Access logging if a RAS connection via modem is used.
- 16) Configure the Domain and Backup domain in the Logger or SDDSN 'Phone Home' setup screen to use the Listener Side A and B machine names respectively.

Refer to the RMS documentation for additional information about configuration.

References

The references provided here span from product documentation highlighting security features in the product to online references of content from which the best practices covered in this document have been extracted. The authoritative sources for all third-party related content are the links provided in this section. These guidelines and best practices have been adhered to and presented to fit the requirements of the contact center applications covered in this document. Customers should follow the recommendations provided in this document in order to harden their contact center servers. If there is any deviation from the steps provided here, and where the sources get updated by the owning parties, Cisco cannot guarantee that applying the new recommendations will not impact the operation of the application. Proper testing and qualification and, where necessary, consultation with Cisco may be necessary to ensure that changes from the guidelines provided will be supported.

Cisco Contact Center Applications Documentation

The following refers mainly to security related content in the documentation for Cisco Intelligent Contact Management (ICM) 6.0(0) Software (and its options). The Cisco ICM Enterprise Edition and Cisco IP Contact Center Enterprise Edition, as well as the Cisco ICM CTI Object Server, documentation can be accessed from:

<http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/index.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/index.htm>

Cisco Intelligent Contact Management (ICM) Software

- ICM Partitioning is discussed in the *Cisco ICM Enterprise Edition Administration Guide*.
- Feature Control: This functionality can be used to restrict user access to certain ICM features; it is discussed in the *Cisco ICM Enterprise Edition Configuration Guide*, Chapter 3.

Cisco ICM WebView

The *Cisco ICM/IP Contact Center Enterprise Edition WebView Installation and Administration Guide* contains the following security related information:

- "Changing the Jaguar Admin Password"
- "Creating a WebView Administrator", "Supervisors and WebView Reports", and "Setting Up WebView Users" which describe login, domain, and password security for WebView users.
- "Supervisors and WebView Reports" also describes how a supervisor can only see the reports for his or her own agents.
- "WebView User's Password Expiration and Domain Security Settings" describes WebView (ICM) users as taking their security setting from the domain on which they are created. The domain also sets the expiration date on the password.

WebView online help:

Under saving reports: From the Security pull-down menu, select either Shared or Private. If you select Shared, all WebView users can access the report. If you select Private, only you can access the report. Under Viewing graphical reports and using the Job Scheduler is a discussion of the mechanics involved in order to allow viewing graphical reports and use of the Job Scheduler in a Microsoft Internet Explorer browser — which requires that all ActiveX Controls and plug-ins be enabled in the browser's Security Settings.

Cisco ICM CTI Object Server (CTI OS)

In the *Cisco ICM Software CTI OS System Manager's Guide*:

- Desktop Users: the section "Desktop User Accounts" contains instructions for configuring privileges for desktop users.
- SQL Server Login: the section "SQL User Login Configuration" contains instructions for configuring SQL user database access.

Cisco Agent Desktop (CAD)

Cisco Agent Desktop Documentation

<http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm46doc/ipccdoc/cadall/index.htm>

- Privileges: Required privileges of various kinds are discussed in the CAD Installation Guide and the CAD Administrator User's Guide.

Cisco ICM Web Collaboration Option - Collaboration Server

Cisco Collaboration Sever (CCS) Documentation

<http://www.cisco.com/univercd/cc/td/doc/product/icm/icm50/icmfam/icmweb/>

- **Passwords**

Admin Login, by default, is done over plain HTTP. There is a note on page 3 stating that if you have Secure Socket Layer (SSL), then you can use secure login through HTTPS.

As a side note, if you do not use secure administration, then all the administration that you do is sent plain text over the network. This could be things like agent usernames and passwords.

Passwords are also required for agents to login, which are done over normal HTTP by default.

- **Connections**

Collaboration Server supports the following connections

- 1) Connection to a SQL Database
- 2) Connection to ICM
- 3) Connection to Media Blender
- 4) Connection to DCA

- 1) Connection to a SQL Database**

CCS can connect to an ORACLE or MS SQL Server database. The connection is done through a JDBC Driver. For Oracle, the customer must download Oracle's JDBC driver. We include the Inet JDBC driver for connection to SQL Server. Security implications may exist for either driver.

- 2) Connection to ICM**

- a. RMI

CCS connects to the ICM Distributor AW by means of an RMI connection. By default this connection is unencrypted. You can, however, secure the RMI connection. Detailed documentation on how to do this is available in the CCS 5.0 Admin Guide, starting on page 29.

- b. ConAPI

CCS also connects to the ICM AW by means of ConAPI, which is built on top of the RMI driver. Again, this is not secure by default. You can secure ConAPI Communication. Details are available on page 43 of the CCS 5.0 Admin Guide.

3) Connection to Media Blender

Connection to Media Blender is done over BAPI, which communicates over an RMI connection. By default, this connection is not secure. Details on securing this connection are available in the CCS 5.0 Admin Guide, starting on page 31.

4) Connection to DCA

CCS > DCA communication is done over the messaging layer of the RMI connection. By default this connection is also unencrypted. Page 38 of the CCS 5.0 Admin Guide provides details on securing this connection.

- **Database Security Implications**

CCS connects to either a Microsoft SQL Server 2000 or Oracle 8i database. Any security deficiencies within the database will affect CCS.

The CCS Database stores information that may impact security, for example, see the following fields in the CCS 5.0 Database Guide:

ACD_TERMINAL_PASSWORD - Agent table
Password - CCL_Person table (Agent, encrypted)

The CCS administrator password is stored, encrypted, in the wserver.properties file.

Cisco ICM Web Collaboration Option - Media Blender

- SSL: There is information about Secure Socket Layer (SSL) in the Cisco Media Blender Administration Guide
<http://www.cisco.com/univercd/cc/td/doc/product/icm/icm50/icmfam/icmweb/icmmedbl/admin.pdf>
- Firewalls: There is a section on Configuring Communication through a Firewall in the Cisco Media Blender Installation Guide.
<http://www.cisco.com/univercd/cc/td/doc/product/icm/icm50/ipccfam/ipccweb/ipccmedb/install.pdf>

Cisco ICM Web Collaboration Option - Dynamic Content Adapter

The DCA 2.0(1) documentation set

<http://www.cisco.com/univercd/cc/td/doc/product/icm/icm50/icmfam/icmweb/icmdca/index.htm> contains the following security information:

- Creating users/passwords
- Deploying the DCA behind a firewall
- Limiting Access to the DCA Admin Tool
- How to use the IIS Lockdown Tool with the DCA
- DCA Session Security
- Enabling/disabling ports for the DCA
- Configuring the Collaboration Toolbar for SSL
- Configuring the DCA-CCS connection for SSL

Cisco ICM Internet Service Node (ISN)

- ISN Production Description (<http://www.cisco.com/univercd/cc/td/doc/product/icm/isn/isn21/isnprod.pdf>) page 2-1, the "Security" section.
- ISN Configuration and Administration Guide (<http://www.cisco.com/univercd/cc/td/doc/product/icm/isn/isn21/isncfg.pdf>) page 7-18, the "Anti-Virus Guidelines" section.

Cisco Customer Response Solutions (CRS)

- Cisco Secure Telnet: In the CRA Serviceability Guide there is a section on Cisco Secure Telnet http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_1/english/admn_app/service/service7.htm
- SNMP: In Chapter 3, the "Configuring the SNMP Trap Sender" section discusses configuring security settings for SNMP traps. http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_5/english/admn_app/gs35.pdf

Support Tools

The Cisco Support Tools documentation contains the following security information:

- Creating users/passwords
- Assigning user privileges
- Configuring Support Tools to use SSL
- Deploying Support Tools behind a firewall
- Using NTFS directory security to limit access to directories
- Enabling/disabling ports for Support Tools
- Limiting Support Tools access to the local network

Cisco Security Agent

- Installing CSA for ICM is part of the Cisco ICM 6.0(0) Documentation set: <http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/index.htm>
- Installing CSA for CRS document: http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_5/english/admn_app/csa_crs.pdf
- Installing CSA for ISN is part of the Cisco ISN documentation set: <http://www.cisco.com/univercd/cc/td/doc/product/icm/isn/>

Third-Party Documentation

Operating System Installation

- Windows 2000 Security Hardening Guide (Version 1.0 Published: May 15, 2003): <http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&displaylang=en>

- Microsoft Security Tool Kit: Installing and Securing a New Windows 2000 System (Accessed: December 2003):
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/w2knew.asp>
- Chapter 3 - Operating System Installation (Accessed: December 2003):
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/win2khg/03osinstl.asp>
- Glossary of Windows 2000 Services (Posted: July 31, 2001):
<http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp>
- Chapter 6 - Hardening the Base Windows 2000 Server (Accessed: December 2003):
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/06basewn.asp>
- Windows 2000 Service Packs:
<http://www.microsoft.com/windows2000/downloads/servicepacks/>

Active Directory

- Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I (Version 1.0 Published: December 4, 2003)
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D>
- Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II (Version 1.0 Published: May 22, 2003):
<http://www.microsoft.com/downloads/details.aspx?FamilyId=C0DBEB7E-D476-4498-9F6C-24974FB81F1E&displaylang=en>

File System

- Windows 2000 NTFS File System (Accessed: December 2003):
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/core/fncc_fil_orws.asp
- Encrypting File System for Windows 2000 (Accessed: December 2003):
<http://www.microsoft.com/windows2000/docs/encrypt.doc>

WMI

- WMI Security (Accessed: January, 20, 2004):
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/scrguide/sas_wmi_vzbp.asp
- WMI Security Settings (Accessed: January, 20, 2004):
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/scrguide/sas_wmi_kyrx.asp

SQL Server

- 10 Steps to Help Secure SQL Server 2000 (Updated: June 28, 2003):
<http://www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.asp>
- Microsoft SQL Server 2000 SP3 Security Features and Best Practices (Accessed: December 2003):
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sql/maintain/security/sp3sec/Default.asp>
- Security Account Delegation for SQL (Accessed: January 20, 2004):
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adminsql/ad_security_2gmm.asp
- The SetSPN utility download (Accessed: January 20, 2004):
<http://www.microsoft.com/downloads/details.aspx?FamilyID=5fd831fd-ab77-46a3-9cfe-ff01d29e5c46&displaylang=en>

Internet Information Server

- HOW TO: Configure the URLScan Tool (Accessed: December 2003):
<http://support.microsoft.com/default.aspx?kbid=326444>

Internet Explorer

- Enhanced Security Configuration for Internet Explorer (Accessed: December 2003):
http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/esc_changes.asp
- Internet Explorer Enhanced Security Configuration Changes the Browsing Experience (Accessed: December 2003):
<http://support.microsoft.com/default.aspx?scid=kb:en-us:815141>
- Managing Internet Explorer Enhanced Security Configuration (Version 1.0 Published: May 5, 2003):
<http://www.microsoft.com/downloads/details.aspx?familyid=d41b036c-e2e1-4960-99bb-9757f7e9e31b&displaylang=en>

Terminal Services

- Securing Windows 2000 Terminal Services (Accessed: December 2003):
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp>

Revision History

Revision	Date	Details
Revision 1.0	April 27, 2004	Initial Public Release
Revision 2.0	July 28, 2004	<ul style="list-style-type: none"> ▪ Introduction: Clarification and addition of CAD Servers. ▪ File System: <ol style="list-style-type: none"> 1. Removal of CAD Server requiring explicit file shares. This is due to architectural changes in CAD 6.0(1). 2. Added that EFS is not recommended for high throughput systems. ▪ WMI Service Hardening: Added note addressing the WMI services default startup type and dependencies. ▪ SNMP Service Hardening: Added note addressing the installation and dependencies of the SNMP services. ▪ Application Security and Passwords: Added note addressing the risk of call variables being not encrypted and edited the note for mitigating against CAD and CTI OS agent passwords being sent in clear text. ▪ IPSec and NAT Support: New section. ▪ SQL Server: Clarification and addition of least privileged service account configuration and permissions required. ▪ Anti-Virus – Trend ServerProtect: New section. ▪ Third Party Management Agent: Added note around effect of these agents on system performance and availability. ▪ VirusScan Enterprise 7.0: Added AutoUpdate configuration details.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.