

Cloudmark Server Edition

*Installation and
Administration Guide*



© 2001-2007 Cloudmark, Inc. All rights reserved. Cloudmark, the Cloudmark logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Cloudmark Inc. and its subsidiaries in the United States and in foreign countries. Other brands and products are trademarks of their respective holders. All product information is subject to change without notice.

All examples with names, company names or companies that appear in this guide are fictitious and do not refer to, or portray, in name or substance, any actual names, organizations, entities or institutions. Any resemblance to any real person, organization, entity or institution is purely coincidental.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Cloudmark, Inc. Cloudmark makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Cloudmark shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance or use of this manual or examples herein.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine readable form without prior consent in writing from:

Cloudmark, Inc. 128 King Street, 2nd Floor, San Francisco, CA 94107 USA

Cloudmark Europe, Ltd. Carmelite, 50 Victoria Embankment, Blackfriars, London EC4Y 0DX UK

Cloudmark Server Edition version 2.1

Last modified: December 13, 2007



Contents

CHAPTER 1	<i>Introduction</i>	.1
	What's New in Version 2.1b	.2
	What is the Cloudmark Global Threat Network?	.3
	How Cloudmark Server Edition works.	.4
	Where to find more information.	.4
CHAPTER 2	<i>Installing Cloudmark Server Edition</i>	.7
	System requirements	.7
	System requirements for CSE Server.	.7
	System requirements for the Administration Console	.8
	Client-side system requirements	.9
	Before you install	.9
	Setting up a Windows user account for CSE	.9
	Creating a new user for CSE	10
	Adding the CSE user to the appropriate groups.	12
	Granting Exchange Server administrative rights to the CSE user account	13
	Granting administrative rights on Exchange 2000 or 2003	14
	Granting administrative rights on Exchange 2007	15
	Installing Cloudmark Server Edition	16
	Installing the Administration Console separately.	21
	Uninstalling CSE	21
	Upgrading CSE	22
CHAPTER 3	<i>Using the Administration Console</i>	25
	Launching the Administration Console	25
	Starting and stopping the CSE service	27

- Connecting to and disconnecting from CSE servers **.28**
- Configuring global options **.30**
 - Enabling mail checking* **30**
 - Enabling mail checking for new users* **30**
 - Enabling mail checking for public folders* **32**
 - Enabling mail checking for local messages* **32**
 - Disabling or enabling user feedback* **33**
 - Enabling troubleshooting event logs* **34**
 - Configuring spam-filtering actions* **34**
 - Configuring spam folder names* **35**
 - Specifying spam-filtering actions for users* **36**
 - Specifying spam-filtering actions for public folders* **37**
 - Configuring options for empty messages* **37**
 - Configuring scheduled mailbox rescanning* **38**
 - Configuring connections* **39**
 - Managing whitelists* **40**
 - Adding and modifying whitelist entries* **40**
 - Importing and exporting a whitelist* **42**
 - Removing whitelist entries* **43**
- Viewing and exporting spam statistics **.44**
 - Viewing the Statistics tab* **44**
 - Viewing the Scanning Statistics graph* **45**
 - Generating monthly statistics reports* **46**
 - Exporting a comma-delimited statistics file* **47**
 - Real-time performance monitoring* **48**
- Selectively enabling and disabling spam checking **.49**
 - Selectively enabling and disabling spam checking for users* **50**
 - Selectively enabling and disabling spam checking for public folders* **51**
 - Assigning ownership of a public folder to the CSE user* **51**
 - Enabling spam checking for a public folder* **52**
 - Disabling spam checking for a public folder* **53**
- Selectively disabling or enabling user feedback **.53**
- Selectively rescanning mailboxes **.54**
- Accessing My Cloudmark **.55**
- Managing subscriptions **.56**
 - Purchasing a subscription after the trial period* **56**
 - Adding subscriptions* **56**

	<i>Renewing subscriptions</i>	56
CHAPTER 4	<i>Configuring CSE for Mobile Spam Filtering</i>	57
	Configuring Microsoft Exchange ActiveSync for CSE	57
	Configuring Blackberry Enterprise Server (BES) for CSE	59
	<i>Configuring BES 3.6 and below</i>	59
	<i>Configuring BES 4.1.3 and above</i>	59
	Configuring GoodLink for CSE	60
CHAPTER 5	<i>Command-Line Interface</i>	61
	Usage	61
	Examples	62
APPENDIX A	<i>Troubleshooting</i>	63
	Errors starting CSE.	63
	Errors stopping CSE	64
	Errors opening the Administration Console	64
	CSE runtime errors.	64
APPENDIX B	<i>Logs</i>	65
	Event log messages	65
	Error log messages	66
APPENDIX C	<i>Trial Evaluation</i>	67
	<i>Index</i>	69

Introduction

Cloudmark Server Edition (CSE) is a server-side spam-filtering application that stops spam, phishing, and email-borne viruses by connecting your Microsoft Exchange Server to the Cloudmark Global Threat Network. It includes the CSE Administration Console—a Microsoft Management Console (MMC) snap-in—that can be installed on the CSE server and one or more administrative desktop computers. CSE does not require client-side software or configuration of end-users' computers.

This *Installation and Administration Guide* shows you how to add spam-filtering functionality to your email infrastructure, in the following chapters:

- Chapter 2, "Installing Cloudmark Server Edition", provides instructions for preparing a Windows server for installation of CSE, which are followed by instructions for installing the CSE software.
- Chapter 3, "Using the Administration Console", shows how to use the CSE Administration Console to access CSE functions, such as configuring spam handling policies, enabling spam-filtering for end-users, and more.
- Chapter 4, "Configuring CSE for Mobile Spam Filtering", explains how to configure your server for effective spam filtering for your users' mobile devices.
- Appendix A, "Troubleshooting", contains CSE troubleshooting information, specifically for running the CSE service and using the Administration Console.
- Appendix B, "Logs", describes all events that are logged to the Windows Event Log.
- Appendix C, "Trial Evaluation", describes CSE's trial evaluation period and provides instructions for purchasing subscriptions to CSE after it expires.

In order to use this guide, you should possess a working knowledge of Microsoft Windows Server 2000 or 2003 and Microsoft Exchange Server 2000, 2003, or 2007.

Additionally, the *User's Quick Reference Guide* is included with the software. You can distribute this guide to your end users to educate them about how CSE blocks spam and how to get the most from its features.

The remainder of this chapter provides a conceptual overview of Cloudmark Server Edition.

What's New in Version 2.1b

- mailbox rescan
Daily rescanning can be scheduled server-wide or performed on-demand for individual users. See “Selectively rescanning mailboxes” on page 54 and “Configuring scheduled mailbox rescanning” on page 38.
- graphical reporting
Hourly graphical reports can be displayed, and a comma-delimited report is produced each month for export to other applications. See “Viewing and exporting spam statistics” on page 44.
- whitelist import and export
Whitelists can now be shared between CSE installations by exporting from or importing to CSE. See “Importing and exporting a whitelist” on page 42.
- performance monitoring
The Performance console in Windows Server can be used to monitor CSE's performance. See “Real-time performance monitoring” on page 48.
- automatic notification of software updates
The Administration Console now displays a notification when a new version of CSE is available. See “Upgrading CSE” on page 22.
- ability to disable user feedback
User feedback is submitted to Cloudmark automatically to achieve the best possible accuracy. You can disable or enable this option globally or selectively. See “Disabling or enabling user feedback” on page 33 and “Selectively disabling or enabling user feedback” on page 53.
- spam-filtering options for empty messages
Empty messages are normally treated as spam. See “Configuring options for empty messages” on page 37.
- command-line interface
A command-line tool is provided to perform user management operations. See Chapter 5, “Command-Line Interface”.

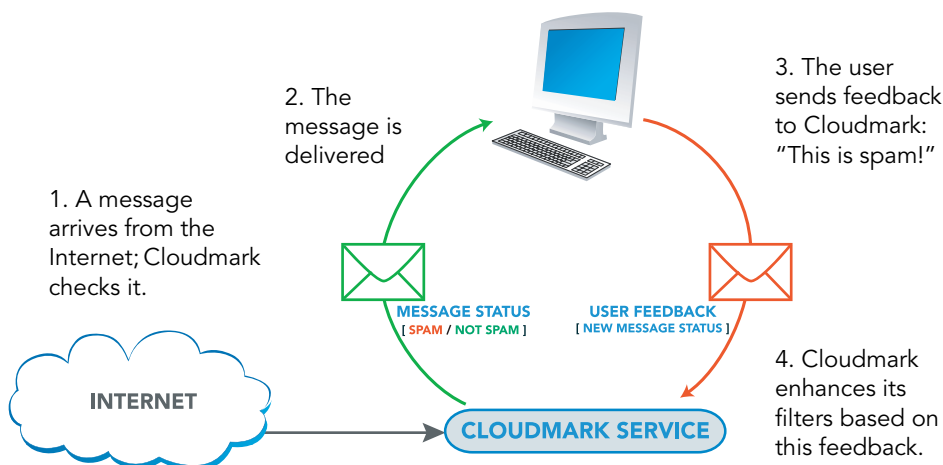
What is the Cloudmark Global Threat Network?

The Cloudmark Global Threat Network consists of over a million email users, all sending feedback to Cloudmark about which messages are spam or phishing and which ones are legitimate. This information helps everyone in the network.

When a user drags a message out of the Inbox and into the Spam folder, Cloudmark compares this feedback with feedback from other users. If other users in the network also consider the message to be spam or fraud, then similar messages are automatically blocked in the future, for all users in the network.

Likewise, if a user drags a message out of the Spam folder, Cloudmark compares this feedback with that of other users. If they agree, the message is unblocked throughout the Cloudmark network.

Figure 1 Cloudmark Global Threat Network



With so many users providing feedback, spam messages generally do not appear in your end users' Inbox folders. Instead, CSE diverts them to the spam folder. CSE automatically creates a spam folder in each user's mailbox.

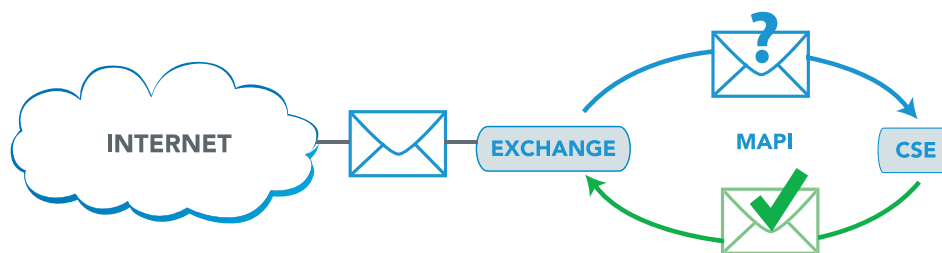
The *User's Quick Reference Guide* includes instructions for users who want to participate in the Cloudmark Global Threat Network. Distribute this guide to your users to educate them about spam and how to use the spam folder.

How Cloudmark Server Edition works

CSE communicates with the Microsoft Exchange Server through the Microsoft Messaging Application Programming Interface (MAPI) to receive notifications when messages arrive and to perform various pre-concerted actions on messages that are determined to be spam.

Figure 2, below, shows how CSE works with Exchange Server and the Cloudmark Global Threat Network to filter spam.

Figure 2 How Cloudmark Server Edition filters email



1. Email arrives at the Exchange Server.
2. CSE computes a unique fingerprint—which does not contain message content and cannot be decoded—for each message.
3. CSE sends the fingerprints to the Cloudmark Global Threat Network for evaluation.
4. The Cloudmark Global Threat Network sends a response to the CSE server indicating whether the message is spam or legitimate.
5. Depending on how you’ve configured CSE, it either tags the message as spam, moves it to a designated spam folder, or deletes it.

Cloudmark Server Edition does not block the regular flow of messages, so its operation has no impact on throughput.

Where to find more information

There are several online resources available to support users of Cloudmark Server Edition:

- CSE support site
<http://www.cloudmark.com/server/support>
 The support site provides the latest FAQs and technical documentation for CSE.

- Cloudmark store

<https://store.cloudmark.com>

The online store lets you purchase additional subscriptions and renew existing ones.

- My Cloudmark

<https://my.cloudmark.com>

My Cloudmark allows you to view your subscriptions, change your contact information and more. My Cloudmark is also accessible on the Administration Console, as described in “Accessing My Cloudmark” on page 55.

Installing Cloudmark Server Edition

This chapter provides hardware and software requirements and installation instructions for Cloudmark Server Edition and the Cloudmark Server Edition Administration Console:

- “System requirements” below
- “Before you install” on page 9
- “Installing Cloudmark Server Edition” on page 16
- “Installing the Administration Console separately” on page 21
- “Uninstalling CSE” on page 21
- “Upgrading CSE” on page 22

System requirements

- “System requirements for CSE Server” below
- “System requirements for the Administration Console” on page 8
- “Client-side system requirements” on page 9

System requirements for CSE Server

The following table lists minimum and recommended software and hardware requirements for Cloudmark Server Edition software.

Table 1 CSE system requirements

Component	Minimum Requirements
Processor	Intel Pentium or compatible, 733 megahertz (MHz) or higher
Memory	256 megabytes (MB) RAM; 512 MB recommended

Table 1 CSE system requirements

Component	Minimum Requirements
Operating system	Microsoft Windows Server 2000 or 2003; Microsoft Windows Small Business Server 2000 or 2003, with the latest service packs installed
Mail server	Microsoft Exchange Server 2000, 2003, or 2007, with the latest service packs
Hard disk	20 MB for CSE software; 200 MB on the primary hard drive
Activation code	Issued by either Cloudmark or your vendor when you acquired the CSE software

You can install Cloudmark Server Edition on the same server as the Microsoft Exchange Server or on a separate server. If you plan to install Cloudmark Server Edition on a server other than the Microsoft Exchange Server (recommended for large deployments) or on Exchange 2007, you must install Extended MAPI. You can obtain Extended MAPI by installing Outlook 2000 or higher with the latest service packs and setting up an email account with it, or by downloading from Microsoft's Web site:

```
http://www.microsoft.com/downloads/
details.aspx?familyid=E17E7F31-079A-43A9-BFF2-
0A110307611E&displaylang=en
```

! *CSE will install—but not run—on a mapped network drive.*

System requirements for the Administration Console

The following table lists minimum and recommended software and hardware requirements for computers running the Cloudmark Server Edition Administration Console.

Table 2 Administration Console system requirements

Component	Minimum Requirements
Processor	Intel Pentium or compatible, 733 megahertz (MHz) or higher
Memory	128 megabytes (MB) RAM
Operating system	Microsoft Windows 2000 Professional; Microsoft Windows Server 2000 or 2003; Microsoft Windows Small Business Server 2000 or 2003; Microsoft Windows XP Professional, with the latest service packs installed
Hard disk	5 MB

To launch the Administration Console, you must be logged on as a user that is a member of Domain Admins group.

Client-side system requirements

CSE filters email independent of the mail client. All email clients are supported for filtering.

For the end-user feedback feature, the following clients are supported:

- Outlook 2000 or higher (configured in Exchange mode)
- Outlook Web Access

You can learn more about the user feedback feature in the *Cloudmark Server Edition User's Quick Reference Guide*. Distribute the guide to your end users to inform them about this feature.

! *The feedback feature is not compatible with IMAP or POP3.*

Before you install

You must perform these tasks before installing CSE or the Administration Console:

- “Setting up a Windows user account for CSE” below
- “Granting Exchange Server administrative rights to the CSE user account” on page 13

Setting up a Windows user account for CSE

There are two steps for setting up the Windows user account for CSE:

- “Creating a new user for CSE” below
- “Adding the CSE user to the appropriate groups” on page 12

Creating a new user for CSE

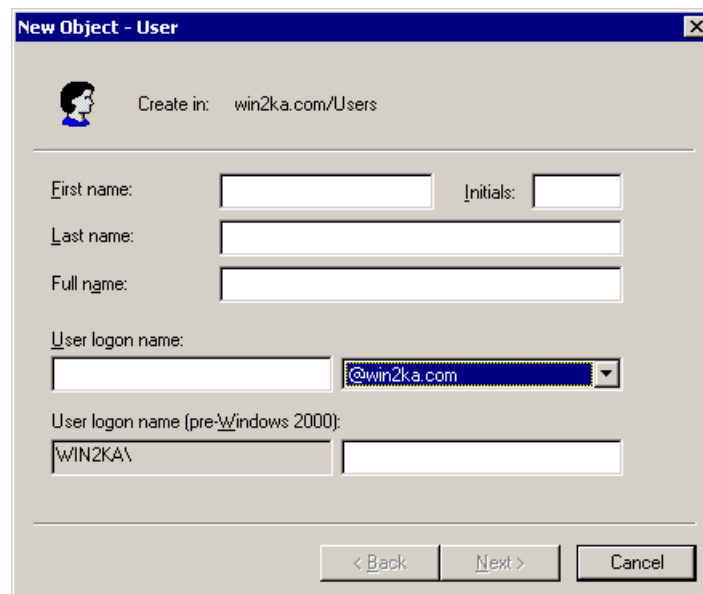
TO CREATE A NEW USER FOR CSE

- 1 From the Start menu, select Programs > Administrative Tools > Active Directory Users and Computers.

The Active Directory Users and Computers window appears.

- 2 From the Action menu, select New > User.

The New Object - User window appears:



The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: win2ka.com/Users'. Below that are several input fields: 'First name:' with an empty text box and 'Initials:' with an empty text box; 'Last name:' with an empty text box; 'Full name:' with an empty text box; 'User logon name:' with an empty text box and a dropdown menu showing '@win2ka.com'; and 'User logon name (pre-Windows 2000):' with a text box containing 'WIN2KA\' and an empty text box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

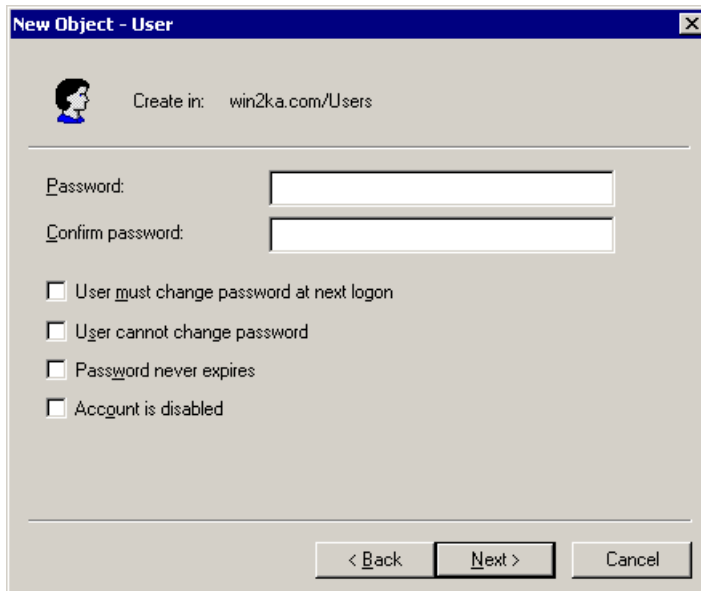
- 3 Enter information for the new CSE user:

- first name
- last name
- full name, if different from first name plus last name
- logon name

It is suggested that you choose names that indicate that this is the CSE user, usually CSEAdmin.

4 Click Next.

The password screen appears:



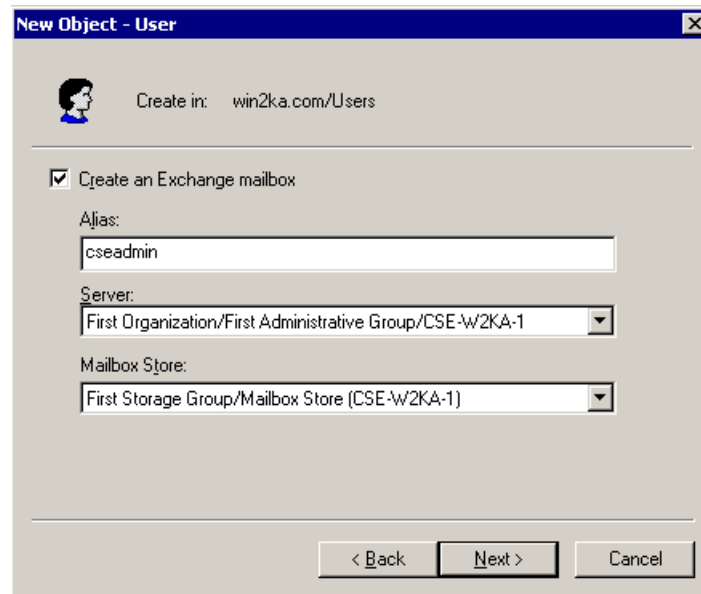
The screenshot shows a Windows-style dialog box titled "New Object - User". At the top left is a small user icon, and to its right is the text "Create in: win2ka.com/Users". Below this is a horizontal line. Underneath the line are two text input fields. The first is labeled "Password:" and the second is labeled "Confirm password:". Below the input fields are four checkboxes, each with a label: "User must change password at next logon", "User cannot change password", "Password never expires", and "Account is disabled". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

5 Enter the new user's password, twice.**6** Select "Password never expires".

This prevents the server from suddenly failing to start due to an expired password.

! *Do not select "User must change password at next logon" or "Account is disabled". These options are not compatible with CSE.*

7 Click Next.



- 8 Verify that “Create an Exchange mailbox” and the correct server and mailbox store are all selected.
- 9 Click Next.
The next screen displays the information you entered.
- 10 If the information you entered is correct, click Finish.

! *Exchange 2003 users only: Never enable the Hide from Exchange address list option (located in the Exchanged Advance tab of the User Properties window) for the CSE user account. This option prevents CSE from functioning.*

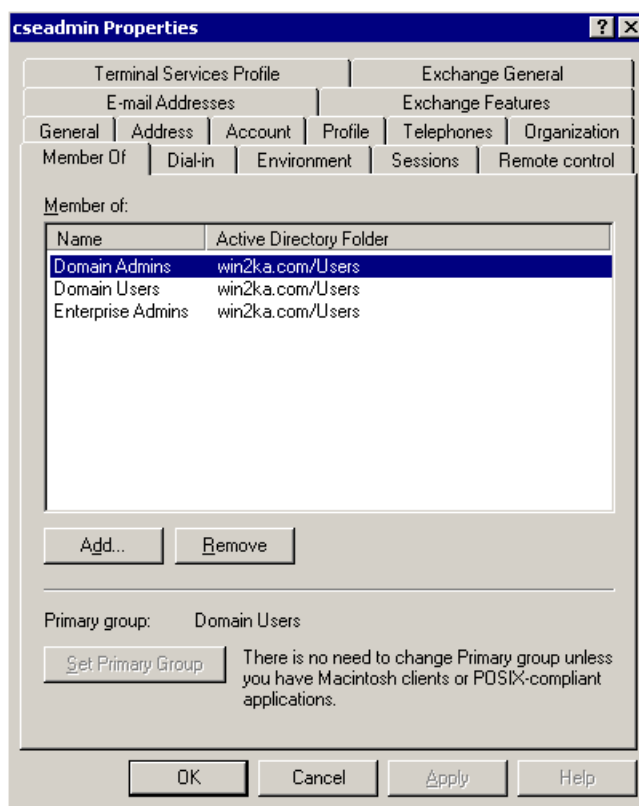
Adding the CSE user to the appropriate groups

This procedure varies, depending on whether CSE is running on a domain controller. Follow the procedure below.

TO ADD THE CSE USER

- 1 From the Start menu, select Programs > Administrative Tools > Active Directory Users and Computers.
The Active Directory Users and Computers window appears.
- 2 In the Users list, double-click the CSE user.
The Properties window appears.

3 Click the Member Of tab:



4 Click Add.

The Select Groups window appears.

5 Select the Domain Admin group.

6 Click Add.

7 Click OK in the Select Groups window.

8 Click OK in the Properties window.

Granting Exchange Server administrative rights to the CSE user account

The CSE user account must have administrative rights to the Exchange Server. This section provides instructions for doing this with different versions of Exchange:

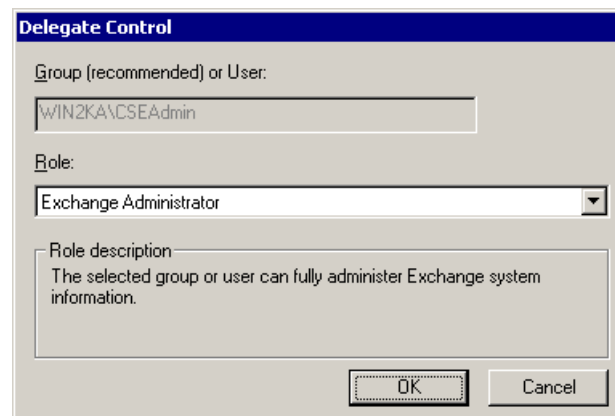
- “Granting administrative rights on Exchange 2000 or 2003” below
- “Granting administrative rights on Exchange 2007” on page 15

Granting administrative rights on Exchange 2000 or 2003

TO GRANT EXCHANGE SERVER ADMINISTRATIVE RIGHTS TO THE CSE USER ACCOUNT

- 1 From the Start menu, select Programs > Microsoft Exchange > System Manager.
- 2 Right-click the name of the Exchange server to display the pop-up menu.
- 3 Select Delegate Control to launch the Exchange Administration Delegation Wizard.
- 4 Click Next.
- 5 On the Users or Groups page, click Add.

The Delegate Control window appears:



- 6 In the Group or User text box, specify the name of the CSE user account.
- 7 From the Role list, select Exchange Administrator.
- 8 Click OK.
- 9 Click Next.
- 10 Click Finish to exit the wizard.

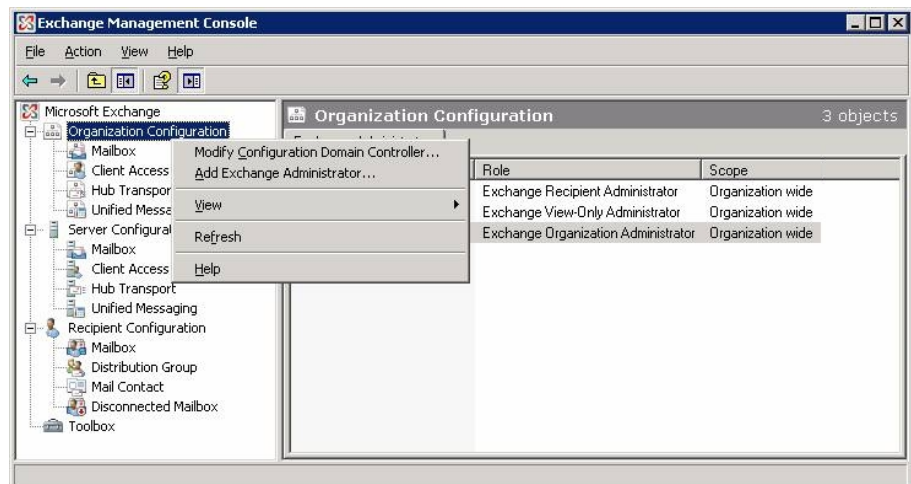
When you exit the wizard, a dialog box notifies you that, to fully administer an Exchange server, the CSE user account must be an administrator of the local machine.

- 11 Click OK to dismiss this prompt.

Granting administrative rights on Exchange 2007

TO GRANT EXCHANGE SERVER ADMINISTRATIVE RIGHTS TO THE CSE USER ACCOUNT

- 1 Launch the Exchange Management Console.
- 2 Right-click on Organization Configuration to open the pop-up menu:



3 Select Add Exchange Administrator....

The Add Exchange Administrator wizard appears:



- 4 Enter the username of the CSE user.
- 5 Select “Exchange Organization Administrator role”.
- 6 Click the Add button.
- 7 When the Add Exchange Administrator wizard finishes adding the CSE user, click Finish.

Installing Cloudmark Server Edition

The installer program is available on a CDROM or by downloading it from Cloudmark or a vendor. It installs CSE and the Administration Console. You must install at least one instance of the Administration Console in order to operate CSE. One instance of the Administration Console can control multiple instances of CSE.

If you are using Exchange 2007, be sure to install Extended MAPI first. You can download and install the MAPI/CDO component for Exchange 2007 from Microsoft. From the Microsoft Download Center, search for the file ExchangeMapiCdo.EXE. Alternatively, you can install Microsoft Outlook on the Exchange Server.

If you are installing CSE on a different computer than the Exchange Server, then you must install Extended MAPI on both the CSE host and the Exchange host.

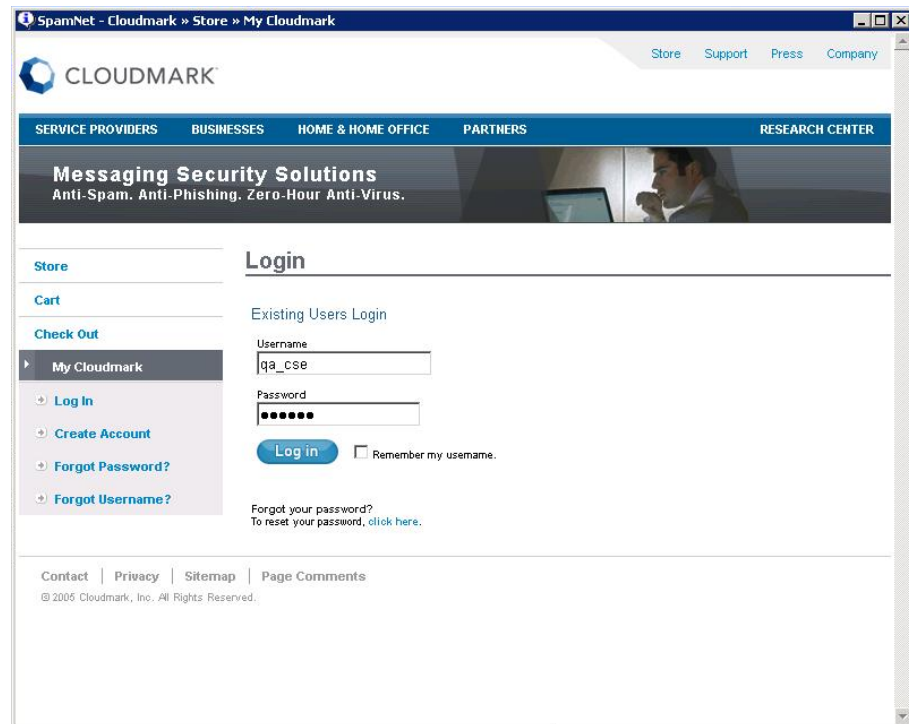
! *If you are upgrading a previous version, be sure to stop the service and close any open MMC or Services Administration windows before running the new installer.*

TO INSTALL CSE SOFTWARE

- 1** Log on to the Windows server with a Windows user account with domain administrator privileges.
- 2** Double-click the CSE installer.
The installation wizard appears.
- 3** Click Next.
- 4** Read the terms and conditions of the license agreement.
If you agree with them, click I Accept.
- 5** On the Select Features screen, choose the software components to install: Cloudmark Server Edition, the Administration Console, or both.
- 6** Click Next.
- 7** Enter your CSE activation code.

8 Click Next.

The My Cloudmark window appears, prompting you to log in or create a new account:

**9** Enter your credentials.**10** Click Log In.

My Cloudmark confirms your product activation.

11 Click Continue.

The installer program reappears.

12 Click Next.**13** Click Next to accept the default installation location, or select a different one.

! *CSE will not run on a mapped network drive.*

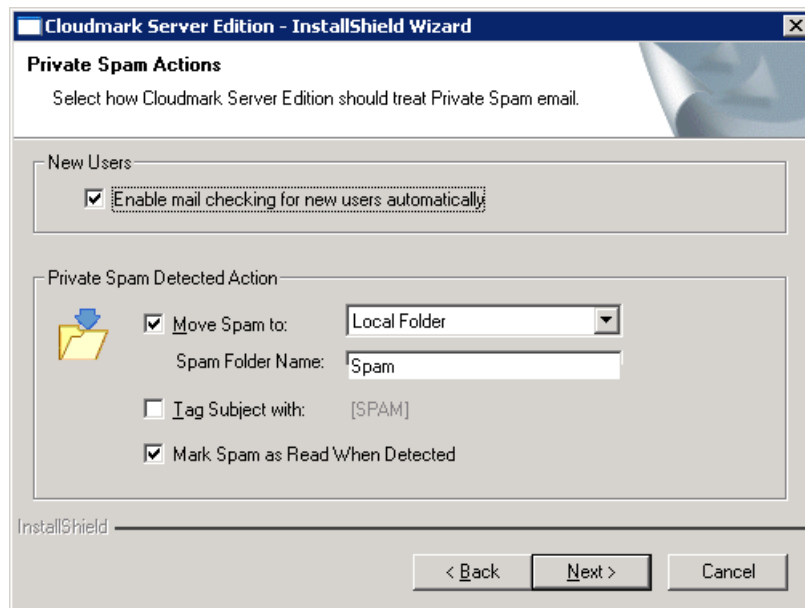
14 Enter the machine name of your Exchange Server.**15** Enter the username and password of the Windows user account you created for the CSE service.

- 16** Enter the domain of this server, without the top-level domain such as .com or .net.

For example, if your domain is domain.com, enter “domain”.

- 17** Click Next.

The Private Spam Actions window appears. Private spam includes spam, phishing, and email-borne viruses sent to a user’s private mailbox.



- 18** Optionally, select “Enable mail checking for new users automatically”.

This initially enables spam filtering for all users on this server. Thereafter, spam filtering is also enabled for any new users you add. You can disable this option later; see “Enabling mail checking for new users” on page 30.

- 19** Select the action CSE should apply to spam messages when delivering to the recipient:

- Move Spam to

This option moves spam to the user’s local spam folder by default, or to another local or public folder that you name. If the spam folder does not exist, it is created automatically in the user’s mailbox. To create a folder for spam with a different name, enter a new name next to this option.

! *Feedback will not be sent to Cloudmark if you select the Junk E-mail folder or the Deleted Items folder.*

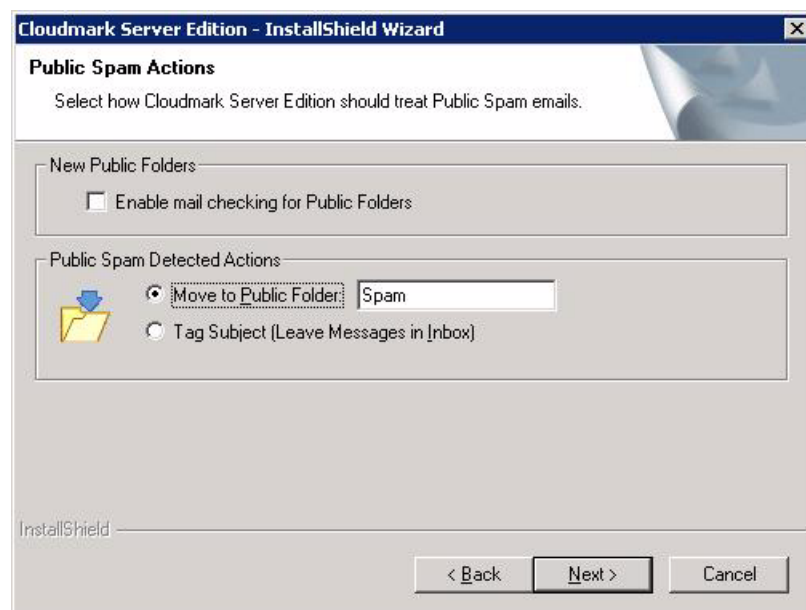
- Tag Subject

This option places a [SPAM] tag in the subject line of suspected spam messages but does not move them.

Regardless of which option you choose, you can mark spam as read by selecting Mark Spam as Read When Detected. You can change these options later; see “Enabling mail checking” on page 30.

20 Click Next.

The Public Spam Actions window appears. Public spam includes spam, phishing, and email-borne viruses sent to a public folder.



21 Optionally, select “Enable mail checking for Public Folders”.

22 Select the action that CSE should take when it detects spam being delivered to a public folder:

- Move to Public Folder

The default public folder for spam is called Spam. Enter a different folder name if desired. If you select this option, see “Assigning ownership of a public folder to the CSE user” on page 51.

- Tag Subject (Leave Messages in Inbox)

This option places a [SPAM] tag in the subject line of suspected spam messages but does not move them.

23 Click Next.

24 Enter the HTTP proxy support settings (if any).

! *HTTP proxy authentication is not supported.*

25 Click Next.

26 Determine which port to use to connect to the Cloudmark Network—either port 2703 or 80—and select the corresponding option.

By default, port 2703 is used. This is the preferred option because it is faster than port 80. If you cannot open this port on your firewall, use port 80.

27 If your server is unable to resolve IP addresses, browse to the following knowledgebase article to obtain an alternate discovery server IP address:

`http://www.cloudmark.com/server/kb/?article=kb-cee-afdsjkle`

Select the Enable DNS Proxy Support check box and type the IP address in the text box.

28 Click Next to review your installation wizard settings.

29 If they are correct, click Next again; otherwise, click Back to make changes.

The wizard installs the CSE software components you selected.

30 Click Finish to exit the wizard when installation is complete.

Installing the Administration Console separately

Optionally, the CSE Administration Console can be installed on another computer besides the Exchange Server, using the CSE installation wizard.

To install the Administration Console separately, follow the instructions in “Installing Cloudmark Server Edition” on page 16. When you reach step 5, select the Cloudmark Server Edition Administration Console as the only software component to install.

Uninstalling CSE

You can remove CSE using the Add/Remove Programs Control Panel.

TO REMOVE THE CSE PROGRAM

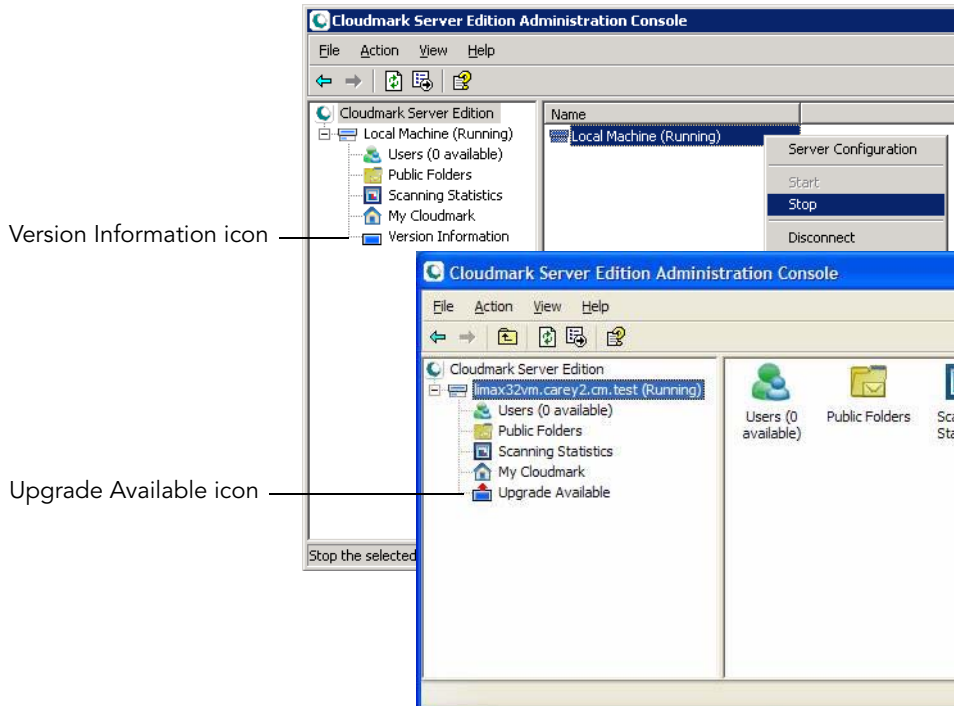
- 1 Close all open Microsoft Management Consoles.
This includes the Services Administration Tool.
- 2 Open the Windows Control Panel.
- 3 Open the Add/Remove Programs control panel.
- 4 From the program list, select CSE.
- 5 Click Remove.

The uninstaller launches, removing the CSE program.

Upgrading CSE

CSE's Administration Console notifies you automatically whenever a new version of CSE is available. When a new version is released, the Version Information icon changes to the Upgrade Available icon:

Figure 1 Automatic upgrade notification



Click the Upgrade Available icon to open the CSE download page on the Cloudmark Web site in your default browser. After downloading the upgrade, follow the instructions in “Installing Cloudmark Server Edition” on page 16.

Using the Administration Console

All Cloudmark Server Edition administration functions are performed using the Administration Console, a MMC snap-in that allows you to configure how CSE handles spam and more.

This chapter explains how to perform the following tasks:

- “Launching the Administration Console” below
- “Starting and stopping the CSE service” on page 27
- “Connecting to and disconnecting from CSE servers” on page 28
- “Configuring global options” on page 30
- “Viewing and exporting spam statistics” on page 44
- “Selectively enabling and disabling spam checking” on page 49
- “Selectively disabling or enabling user feedback” on page 53
- “Selectively rescanning mailboxes” on page 54
- “Accessing My Cloudmark” on page 55
- “Managing subscriptions” on page 56

Launching the Administration Console

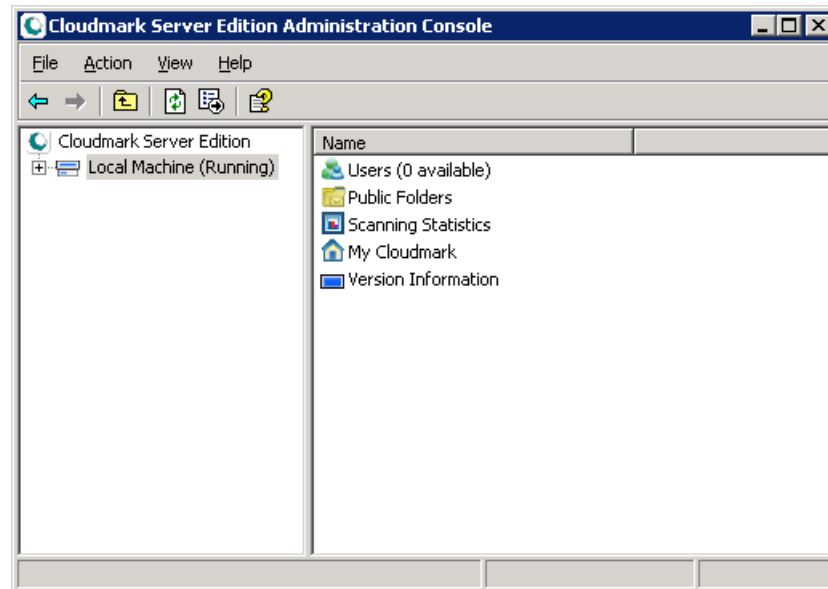
Normally, you run the Administration Console as a member of the Domain Admins group, as explained in the procedure below. See the procedures that follow it for instructions on running it as a member of another group.

TO LAUNCH THE ADMINISTRATION CONSOLE

- 1 Make sure you are logged in as a member of the Domain Admins group.

- 2 In the Start menu, select Programs, then Cloudmark Server Edition, then Cloudmark Server Edition Administration Console.

The Cloudmark Admin Console appears:



If you are logged in as a user belonging to a different group, you can still run the Administration Console by selecting Cloudmark Server Edition > Administration Console in the Start menu and following the instructions for your operating system below:

TO LAUNCH THE ADMINISTRATION CONSOLE IN ANOTHER GROUP ON WINDOWS 2000

- 1 In the Start menu, navigate to Programs, then Cloudmark Server Edition, then Cloudmark Server Edition Administration Console. (Do not click Administration Console yet.)
- 2 Right-click Administration Console.
- 3 In the pop-up menu that appears, select Run As....
- 4 Enter the username and password of the Windows user account that you set up for CSE.

TO LAUNCH THE ADMINISTRATION CONSOLE IN ANOTHER GROUP ON WINDOWS XP

- 1 In the Start menu, navigate to Programs, then Cloudmark Server Edition, then Cloudmark Server Edition Administration Console. (Do not click Administration Console yet.)

- 2 Right-click Administration Console.
- 3 In the pop-up menu that appears, select Properties.
- 4 On the Shortcut tab, click the Advanced button.
- 5 Select the “Run with different credentials” check box.
- 6 Click OK.
- 7 Click OK again.

After you apply this change, you will be prompted to choose a user every time you click the menu item.

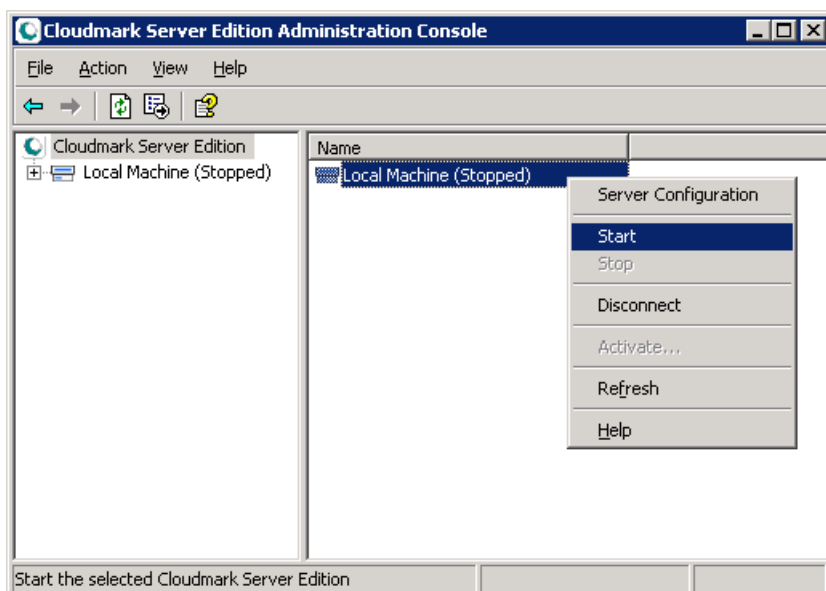
The remaining sections of this chapter explain how to use the Administration Console.

Starting and stopping the CSE service

If you get an error attempting to start or stop the Cloudmark Server Edition service, refer to Appendix A, "Troubleshooting".

TO START CSE

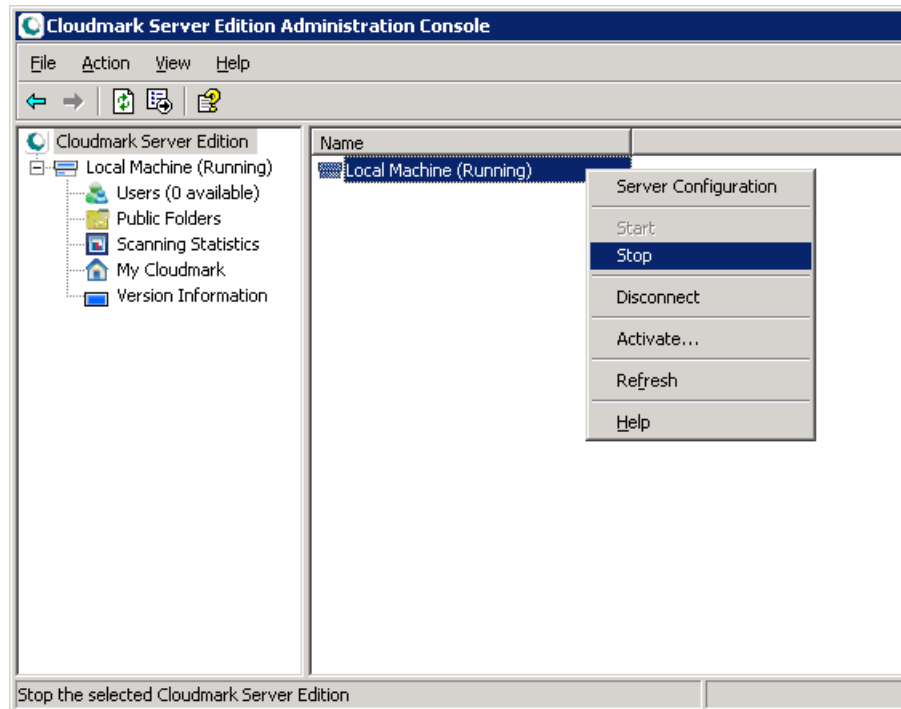
- 1 In the left pane of the Administration Console, expand the Cloudmark Server Edition folder.
- 2 Right-click the name of the CSE server to display the pop-up menu:



- 3 Select Start.

TO STOP CSE

- 1 In the left pane of the Administration Console, expand the Cloudmark Server Edition folder.
- 2 Right-click the name of the CSE server to display the pop-up menu:



- 3 Select Stop.

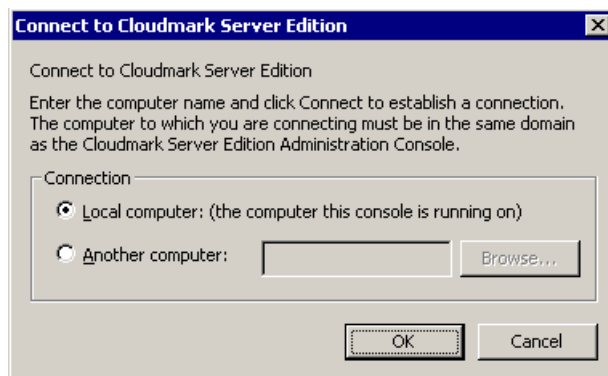
Connecting to and disconnecting from CSE servers

The Administration Console automatically connects to the CSE server you specified during installation; however, you can connect to another CSE server in the same domain.

TO CONNECT TO ANOTHER CSE SERVER IN THE SAME DOMAIN

- 1 In the left pane of the Administration Console, right-click Cloudmark Server Edition.
- 2 Click Connect.

The Connect window appears:



- 3 Choose whether to connect to a server running on the local computer or a server running elsewhere in the domain:
 - To connect to a CSE server running on the local computer, click Local computer.
 - To connect to another CSE in the domain, click Another computer, then enter the name or IP address of the computer. Click Browse to find the CSE server on the network.
- 4 Click OK.

The Administration Console is now connected to the specified CSE server.

TO DISCONNECT FROM A CSE SERVER

- 1 In the left pane of the Administration Console, right-click the name of the server from which you want to disconnect.
- 2 Click Disconnect.

Configuring global options

You can configure global options using the Server Configuration window of the Administration Console.

TO OPEN THE SERVER CONFIGURATION WINDOW

- 1 In the left pane of the Administration Console, right-click a CSE server to display the pop-up menu.
- 2 Click Server Configuration.

The Server Configuration window appears.

You can perform the following configuration tasks in this window:

- “Enabling mail checking” below
- “Disabling or enabling user feedback” on page 33
- “Enabling troubleshooting event logs” on page 34
- “Configuring spam-filtering actions” on page 34
- “Configuring scheduled mailbox rescanning” on page 38
- “Configuring connections” on page 39
- “Managing whitelists” on page 40

Enabling mail checking

The General tab of the Server Configuration window allows you to specify how CSE automatically checks mail. You can perform the following spam-handling configuration tasks in this tab:

- “Enabling mail checking for new users” below
- “Enabling mail checking for public folders” on page 32
- “Enabling mail checking for local messages” on page 32

To enable or disable mail checking selectively instead of globally, see “Selectively enabling and disabling spam checking” on page 49.

Enabling mail checking for new users

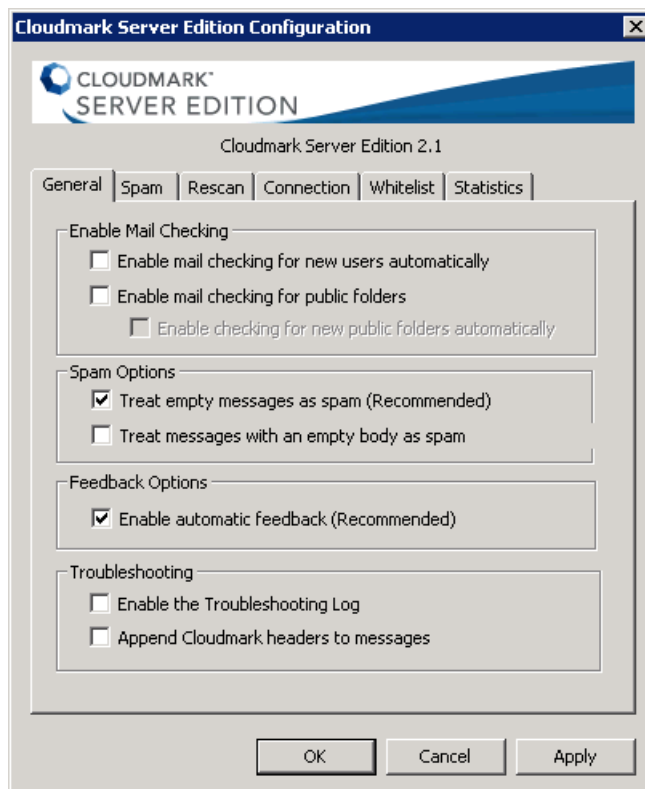
Mail checking can be selectively enabled or disabled for existing users; see “Selectively enabling and disabling spam checking” on page 49. You can also set

the default mail-checking option (either enabled or disabled) that will be applied to new users when they are added to the server, as explained below.

TO ENABLE AUTOMATIC SPAM FILTERING FOR NEW USERS

- 1 Open the Server Configuration window.

The General tab is displayed by default:



- 2 In the Enable Mail Checking area of the tab, select “Enable mail checking for new users automatically”.
- 3 Click OK.

With this option selected, spam filtering will be enabled for each new user you add to the system. If you prefer to enable and disable spam filtering selectively, see “Selectively enabling and disabling spam checking” on page 49.

! *If you enable this option before the first time that you run CSE, all users are enabled for spam filtering.*

Enabling mail checking for public folders

By enabling this option, you allow CSE to look for public folders and display them in the Administration Console. If you disable this option, public folders will not appear in the Administration Console.

If you also want CSE to filter spam from public folders, you must

- enable this option *and*
- selectively enable spam checking for public folders, as explained in “Selectively enabling and disabling spam checking for public folders” on page 51.

TO ENABLE AUTOMATIC MAIL CHECKING FOR PUBLIC FOLDERS

- 1 Open the Server Configuration window.
- 2 In the Enable Mail Checking area of the General tab, select “Enable mail checking for public folders”.
Public folders are now displayed in the Administration Console and can be selectively enabled or disabled for spam filtering.
- 3 Optionally, select “Enable checking for new public folders automatically”.
Any public folders that are created from now on will automatically be checked.
- 4 Click OK.

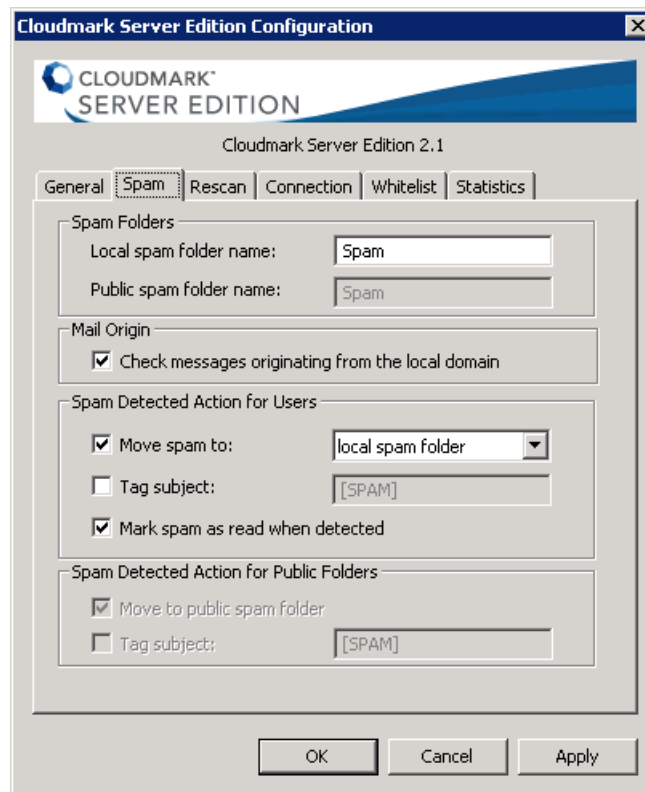
Enabling mail checking for local messages

By default, messages originating from the local domain are not checked for spam. You may choose to enable this option.

TO ENABLE AUTOMATIC MAIL CHECKING FOR LOCAL MESSAGES

- 1 Open the Server Configuration window.

- 2 Click the Spam tab:



- 3 In the Mail Origin area, select “Check messages originating from the local domain”.
- 4 Click OK.

Disabling or enabling user feedback

User feedback occurs when a user contests CSE’s automatic filtering by moving messages into or out of the local spam folder. Information about contested messages is automatically sent to the Cloudmark service, where it may influence future filtering of similar messages.

By default, feedback is enabled for all users. This is the recommended setting to achieve the best accuracy. You can disable this option in the Server Configuration window. You can also disable or enable feedback selectively for individual users; see “Selectively disabling or enabling user feedback” on page 53.

For more information about how users submit feedback, see the *Cloudmark Server Edition User's Quick Reference Guide*, designed for distribution to your end users.

HOW TO DISABLE USER FEEDBACK

- 1 Open the Server Configuration window.
The General tab is displayed by default.
- 2 Remove the check mark from the “Enable automatic feedback” option.
You can re-enable this option by selecting it again.

Enabling troubleshooting event logs

Troubleshooting event logs help you determine the cause of problems you may encounter with CSE and is needed by Cloudmark when contacting technical support. The log file is written to:

Program Files\Cloudmark\Cloudmark Server Edition\log\cloudmark.log

TO ENABLE TROUBLESHOOTING EVENT LOGGING

- 1 Open the Server Configuration window.
- 2 In the Troubleshooting area of the General tab, select “Enable troubleshooting log”.
- 3 Optionally, select “Append Cloudmark headers to messages”.
This option provides more useful information with which Cloudmark can improve its accuracy.
- 4 Click OK.

Configuring spam-filtering actions

The Spam tab of the Server Configuration window allows you to configure the actions that CSE takes when it detects spam or fraud messages.

- “Configuring spam folder names” below
- “Specifying spam-filtering actions for users” on page 36
- “Specifying spam-filtering actions for public folders” on page 37

Configuring spam folder names

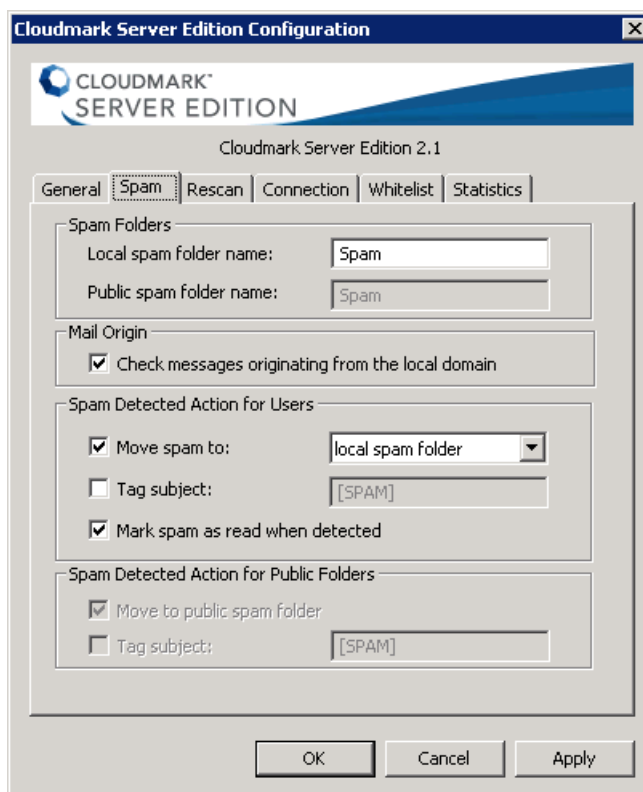
This topic provides instructions for configuring the names of the designated folders for spam, phishing, and email-borne viruses. CSE can automatically move spam and phishing to either of these configured folders, as explained in the following topics:

- “Specifying spam-filtering actions for users” below
- “Specifying spam-filtering actions for public folders” on page 37

Both the local folder and the public folder are available to users as feedback folders; that is, users can drag spam and phishing messages into either of these folders in order to automatically send feedback to the Cloudmark Global Threat Network.

TO CONFIGURE SPAM FOLDER NAMES

- 1 Open the Server Configuration window.
- 2 Click the Spam tab:



- 3 In the “Local spam folder name” field, enter the name of the local spam folder. This folder will be automatically created in users’ local mailboxes.

- 4 In the Public spam folder Name field, enter the name of the public spam folder.
This folder will be automatically created as a public folder.
- 5 Click OK.

Specifying spam-filtering actions for users

You can configure the action that CSE takes when it automatically detects a spam or phishing message being delivered to a user's mailbox.

TO CONFIGURE SPAM-FILTERING ACTIONS FOR USERS

- 1 Open the Server Configuration window.
- 2 Click the Spam tab.
- 3 In the Spam Detected Action for Users area, select one of these actions:
 - **Move Spam to**
This option moves spam to the user's local spam folder by default, or to another local or public folder that you name. If the spam folder does not exist, it is created automatically in the user's mailbox. To create a folder for spam with a different name, enter a new name next to this option.

! *Feedback will not be sent to Cloudmark if you select the Junk E-mail folder or the Deleted Items folder.*

 - **Tag Subject**
Places the text you specify in the text box adjacent to the Tag Subject option to the beginning of the message subject line and then delivers the message to the user's Inbox. The default tag is "[SPAM]."

! *Because Outlook and Outlook Express run message rules before CSE filters messages, rules will not run on messages tagged by CSE.*

- 4 Optionally, you can also select "Mark Spam as Read when detected".
This option marks spam as read when it is delivered.
- 5 Click OK.

Specifying spam-filtering actions for public folders

The Spam Detected Action for Public Folders area allows you to specify the action that CSE automatically takes when it detect spam or fraud being delivered to a public folder.

TO CONFIGURE SPAM-FILTERING ACTIONS FOR PUBLIC FOLDERS

- 1 Open the Server Configuration window.
- 2 Click the Spam tab.
- 3 In the Spam Detected Action for Public Folders area, select one of these actions:
 - Move to public spam folder
This option moves spam to a public spam folder. The name of this folder is configured in the spam folders area of this tab, as explained in “Configuring spam folder names” on page 35.
 - Tag Subject
This option inserts the specified text at the beginning of the message subject line, then delivers the message as usual. The default tag is “[SPAM].”
- 4 Click OK.

Configuring options for empty messages

Empty messages are commonly used by spammers to perform directory harvesting. By default, messages with empty Subject and Body fields are treated as spam. However, legitimate users may wish to send short messages in the Subject field while leaving the body of the message empty. CSE provides the ability to specify how you wish to handle these messages.

HOW TO CONFIGURE OPTIONS FOR EMPTY MESSAGES

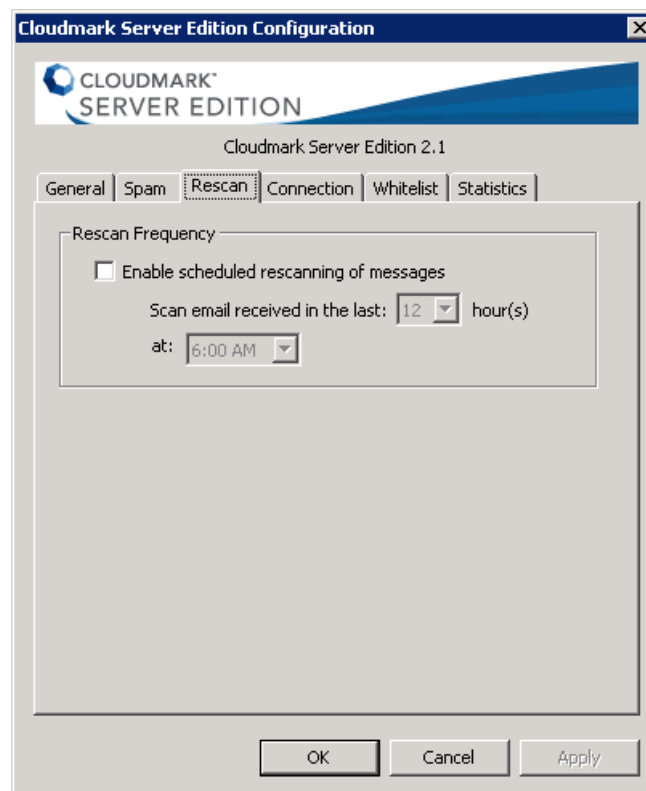
- 1 Open the Server Configuration window.
The General tab is displayed by default.
 - When you select “Treat empty messages as spam”, messages with empty Subject and Body fields are automatically treated as spam. This is the default configuration.
 - When you select “Treat messages with an empty body as spam”, messages with empty Body fields are treated as spam even if the Subject field is not empty. This option is not enabled by default.

Configuring scheduled mailbox rescanning

In the case of a very new spam, phishing, or virus attack, it may take some time for sufficient user feedback to accumulate in order to begin automatically blocking the attack. For this reason, it is advantageous to rescan mailboxes in order to take advantage of the latest user feedback. CSE provides an option to schedule an automatic rescan of all mailboxes on a server.

HOW TO CONFIGURE AUTOMATIC MAILBOX RESCANNING

- 1 Open the Server Configuration window.
- 2 Click the Rescan tab:



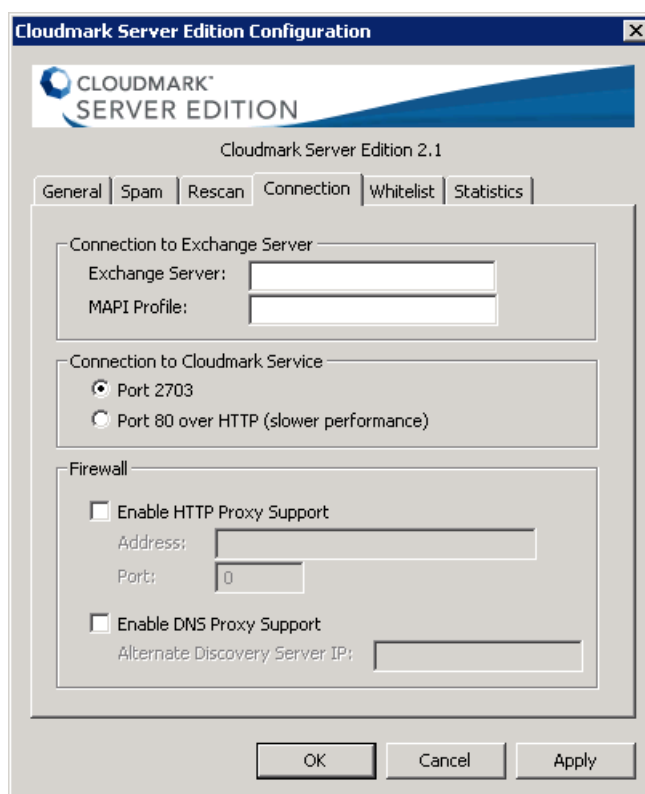
- 3 Select "Enable scheduled rescanning of messages".
- 4 Select the maximum age of messages to rescan.
The default age is 12 hours. This is usually sufficient to rescan all messages received during inactive periods, such as overnight.
- 5 Select the time at which to rescan.

Configuring connections

The Connection tab is where you enter the settings that connect CSE service to the Cloudmark service.

TO CONFIGURE THE CONNECTION TAB

- 1 Open the Server Configuration window.
- 2 Click the Connection tab:



- 3 In the Connection to Exchange Server area of the tab, enter the following information:
 - In the Exchange Server field, enter the IP address or hostname of the Exchange server to which to connect.
 - In the MAPI Profile field, enter the name of the MAPI profile to use for this connection. (By default this is automatically filled in as CloudmarkSE_profile.)

- 4 In the Connection to Cloudmark Service area, make sure that Port 2703 is selected.

This is the recommended setting and will yield the fastest connection speeds. If this port is not available to you, select “Port 80 over HTTP” instead.

- 5 In the Firewall area, enter firewall proxy settings, if any.

- Enable HTTP Proxy Support

Check this box if you use an HTTP proxy on your network and use port 80 as your Connection to Cloudmark Services.

Specify an IP address or hostname in the Address field and a port number in the Port field. The native Cloudmark Global Threat Network protocol is encapsulated in HTTP requests to comply with the HTTP 1.0 specification.

- Enable DNS Proxy Support

It is normally not necessary to enable DNS proxy support because Cloudmark Server Edition automatically switches to IP-based discovery mode to connect to the Cloudmark Global Threat Network.

If you experience “Unable to connect” errors, check Enable DNS Proxy Support and type in an Alternate Discovery Server IP address in the text box. The IP address is available here:

<http://www.cloudmark.com/server/kb/?article=kb-cee-afdsjkle>

- 6 Click OK.

Managing whitelists

On the Whitelist tab, you can create and edit a list of email addresses and domains which are exempt from spam filtering. CSE will not filter messages that are sent from these sources. You can do the following on the Whitelist tab:

- “Adding and modifying whitelist entries” below
- “Importing and exporting a whitelist” on page 42
- “Removing whitelist entries” on page 43

Adding and modifying whitelist entries

TO ADD AN ITEM TO THE WHITELIST

- 1 Open the Server Configuration window.

2 Click the Whitelist tab:**3** Click the Add button.

The Whitelist - Add window appears.

4 Enter one of the following:

- an email address
For example:
`janedoe@domain.com`
- a hostname
For example:
`mail.domain.com`
- a full or partial domain name
For example:
`domain.cx`
or
`cx`

- an IP address
For example:
64.236.16.20
- a partial IP address in CIDR format
For example:
127.0.0/24

! CSE's *whitelist* feature does not support wildcards.

- 5 Click OK.

TO MODIFY A WHITELIST ITEM

- 1 Open the Server Configuration window.
- 2 Click the Whitelist tab.
- 3 Select the whitelist item in the Email Addresses table.
- 4 Click the Edit button.
- 5 Edit the item as desired.
- 6 Click OK.

Importing and exporting a whitelist

In order to share whitelists between multiple servers, you can import and export whitelists.

TO IMPORT A WHITELIST

- 1 Open the Server Configuration window.
- 2 Click the Whitelist tab.
- 3 Click the Import button.
- 4 Navigate to the location of the whitelist file to import.

The whitelist file must be a text file containing email addresses, hostnames, domain names, and full or partial IP addresses (in CIDR format), one entry per line.

- 5 Click Open.

If there are already entries in your whitelist, a prompt appears, asking you to specify whether you want to append the new entries to the existing whitelist or overwrite the existing whitelist.

- 6 Click Append or Overwrite.

The imported entries now appear in the Whitelist tab.

TO EXPORT A WHITELIST

- 1 Open the Server Configuration window.
- 2 Click the Whitelist tab.
- 3 Click the Export button.
- 4 Navigate to the location where you want to save the whitelist and enter a filename.
- 5 Click Save.

Removing whitelist entries

TO REMOVE A WHITELIST ITEM

- 1 Open the Server Configuration window.
- 2 Click the Whitelist tab.
- 3 Select the whitelist item in the Email Addresses table.
- 4 Click the Remove button.
- 5 To clear the entire whitelist, click Remove All.
- 6 Click OK.

TO EMPTY THE WHITELIST

- 1 Open the Server Configuration window.
- 2 Click the Whitelist tab.

A prompt appears, asking you to verify that you want to remove all entries in the whitelist.

! *This operation cannot be undone.*

- 3 Click OK to close the prompt.
The whitelist entries disappear.
- 4 Click OK to close the whitelist window.

Viewing and exporting spam statistics

There are three ways to access statistics about CSE's spam-filtering activity:

- “Viewing the Statistics tab” below
- “Viewing the Scanning Statistics graph” on page 45
- “Generating monthly statistics reports” on page 46
- “Exporting a comma-delimited statistics file” on page 47
- “Real-time performance monitoring” on page 48

Viewing the Statistics tab

The Statistics area of the General tab shows the following data:

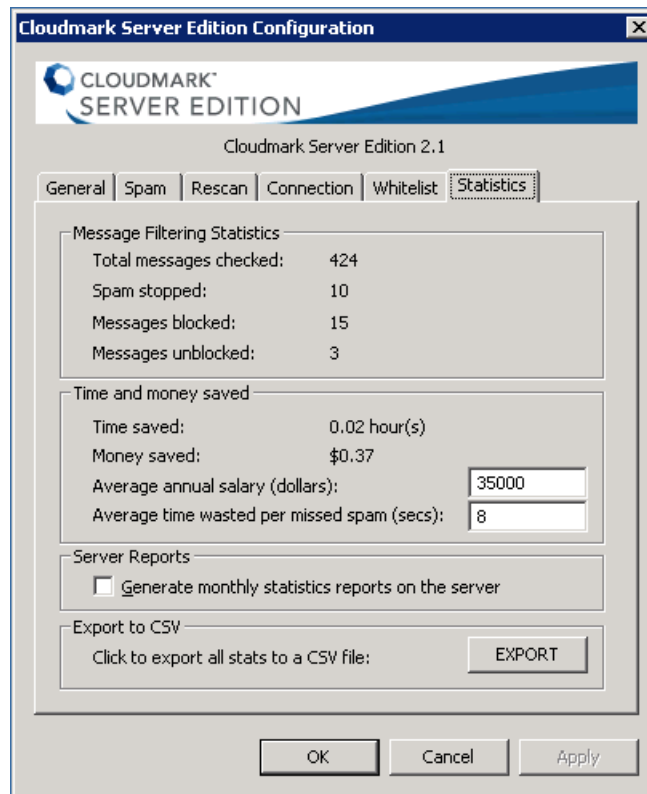
- how many messages were checked
- how much spam was caught
- how many messages were manually blocked by users
- how many messages were manually unblocked by users
- estimated time and money saved

Time saved is calculated by dividing the average amount of time spent on each spam message by the amount of spam that was filtered. Money saved is calculated by the average amount of money spent per hour on spam (based on an average salary) multiplied by the time saved. You can change the variables used to calculate these figures by entering new ones in the text fields.

TO VIEW THE STATISTICS TAB

- 1** Open the Server Configuration window.

2 Click the Statistics tab:



Viewing the Scanning Statistics graph

The Scanning Statistics graph provides a 65-day graphical view of CSE's spam-filtering activities, including the following:

- messages scanned
- messages caught automatically
- messages blocked by users
- messages unblocked by users

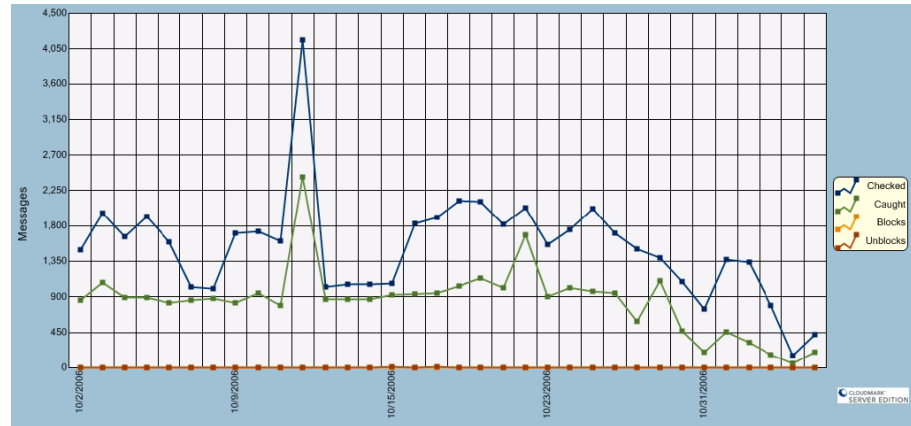
The statistics in this graph are updated hourly. Additional statistics can be captured on a monthly basis. See "Generating monthly statistics reports" on page 46.

HOW TO VIEW THE SCANNING STATISTICS GRAPH

- 1 In left pane of the Administration Console window, click the plus sign (+) next to the server whose statistics you want to view.

2 Click Scanning Statistics.

The Scanning Statistics graph appears in the right pane:



Generating monthly statistics reports

CSE can automatically generate graphical reports on the first day of each month for the previous month. These monthly reports are saved in the same directory as the log files, usually C:\Program Files\Cloudmark\Cloudmark Server Edition\log.

When you enable automatic generation of monthly statistics reports, the following graphical reports are generated at the end of each month:

Table 1 Monthly statistics reports

Report	Filename	Description
accuracy	cse-YYYY-MM-Accuracy.jpg	The accuracy graph depicts the percentage of email abuse that was detected automatically by CSE. All other abuse was detected through user feedback.
blocks	cse-YYYY-MM-Blocks.jpg	This graph displays the number of messages that were blocked by users.
stats	cse-YYYY-MM-Stats.jpg	This is the one-month equivalent of the five-day graph displayed in the Administration Console. It includes the number of messages checked, automatically caught, and blocked or unblocked by users.

Table 1 Monthly statistics reports

Report	Filename	Description
unblockrate	cse-YYYY-MM-UnblockRate.jpg	The unblock rate is the percentage of “false positives”, that is, automatically-filtered spam and phishing messages which were later reported by users as legitimate. A high unblock rate indicates a problem; contact Cloudmark if this occurs.
unblocks	cse-YYYY-MM-Unblocks.jpg	This graph provides a simple count of the number of false positives reported by users.

Additionally, a comma-delimited statistics file is generated with the following filename format:

```
export-<yyyy>-<mm>.csv
```

For example, the monthly statistics report for September 2007 is `export-2007-09.csv`.

HOW TO GENERATE MONTHLY STATISTICS REPORTS

- 1 Open the Server Configuration window.
- 2 Click the Statistics tab.
- 3 Select “Generate monthly statistics reports on the server”.
- 4 Click OK.

Exporting a comma-delimited statistics file

You can export all statistics for all users on the server, on demand, to a text file in CSV format.

HOW TO EXPORT A STATISTICS FILE

- 1 Open the Server Configuration window.
- 2 Click the Statistics tab.
- 3 Click the Export button.
- 4 Navigate to the location where you want to save the file and enter a filename.
- 5 Click Save.

Real-time performance monitoring

In addition to the hourly and monthly statistics available in the Administration Console, you can use the Performance console (“perfmon”) in Windows Server.

The system setting “Language for non-Unicode programs” must be set to the default language of the operating system in order for the CSE performance counters to be available to perfmon. This setting is located in the “Regional and Language Options” control panel.

HOW TO ADD CSE COUNTERS TO THE PERFORMANCE CONSOLE

- 1 From the Start menu, select All Programs > Administrative Tools > Performance.

If you are running CSE on a 64-bit operating system, run the following instead:

```
mmc.exe /32 perfmon.msc
```

- 2 Click the Add  button.

The Add Counters window appears:



- From the Performance Object list, select Cloudmark Server Edition.

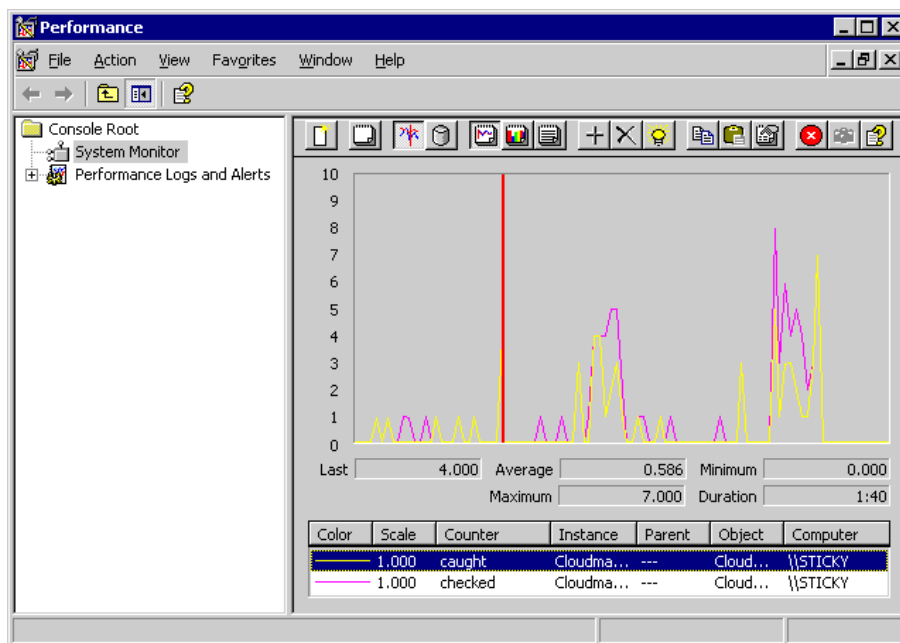
Four performance counters appear:

Table 2 Performance counters

Counter	Description
caught	Spam and phishing messages automatically blocked by CSE
checked	Messages scanned by CSE
reported	Spam and phishing messages blocked by end users
revoked	Legitimate messages unblocked by end users

- Select All Counters, or select one or more counters from the list.
- Click Add.
- Click Close.

The CSE performance counters now appear in the Performance console:



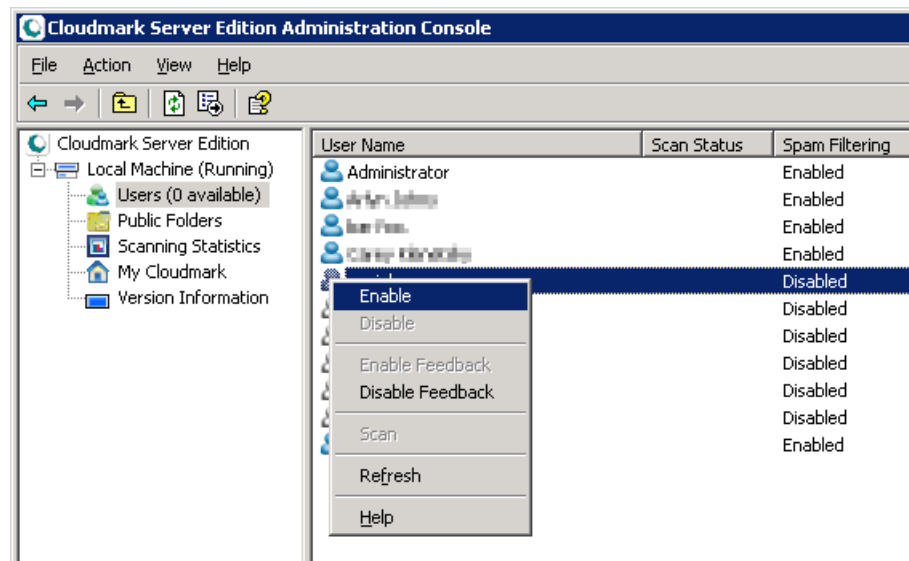
Selectively enabling and disabling spam checking

You can enable and disable spam-checking for individual users or groups of users, and for public folders. To automatically enable or disable spam-checking for new users and public folders, see “Enabling mail checking” on page 30.

Selectively enabling and disabling spam checking for users

TO ENABLE SPAM-CHECKING FOR A USER OR GROUP

- 1 In the left pane of the Administration Console, expand the CSE server.
- 2 Click the Users folder.
The list of users appears in the right pane.
- 3 Select one or more users.
- 4 Right-click the selection to display the pop-up menu:



- 5 Select Enable.
The selected users are now marked “Enabled”.

TO DISABLE SPAM-CHECKING FOR A USER OR GROUP

- 1 In the left pane of the Administration Console, expand the CSE server.
- 2 Click Users.
The list of users appears in the right pane.
- 3 Select one or more users.
- 4 Right-click the selection to display the pop-up menu.
- 5 Click Disable.
The selected users are now marked “Disabled”.

Selectively enabling and disabling spam checking for public folders

In order to control spam-checking for a public folder, the CSE user must be the owner of the public folder. The following topics explain how to manage public folders with CSE:

- “Assigning ownership of a public folder to the CSE user” below
- “Enabling spam checking for a public folder” on page 52
- “Disabling spam checking for a public folder” on page 53

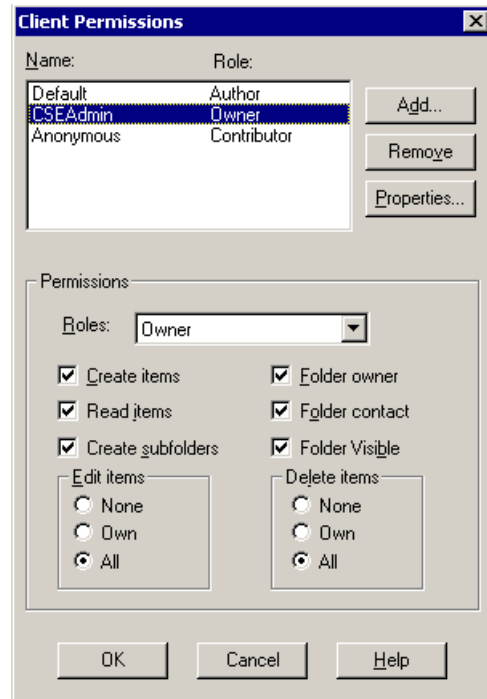
Assigning ownership of a public folder to the CSE user

TO ASSIGN OWNERSHIP OF A PUBLIC FOLDER TO THE CSE USER

- 1** From the Start menu, select Programs > Microsoft Exchange > System Manager.
The System Manager appears.
- 2** In the left pane, select the Folders item.
- 3** In the right pane, right-click the public folder for which you want to control spam filtering.
A menu appears.
- 4** Select Properties.
The Properties window appears.
- 5** Click the Permissions tab.

- 6 Click the Client Permissions button.

The Client Permissions window appears:



- 7 Click the Add... button.

The Select Users, Computers, or Groups window appears.

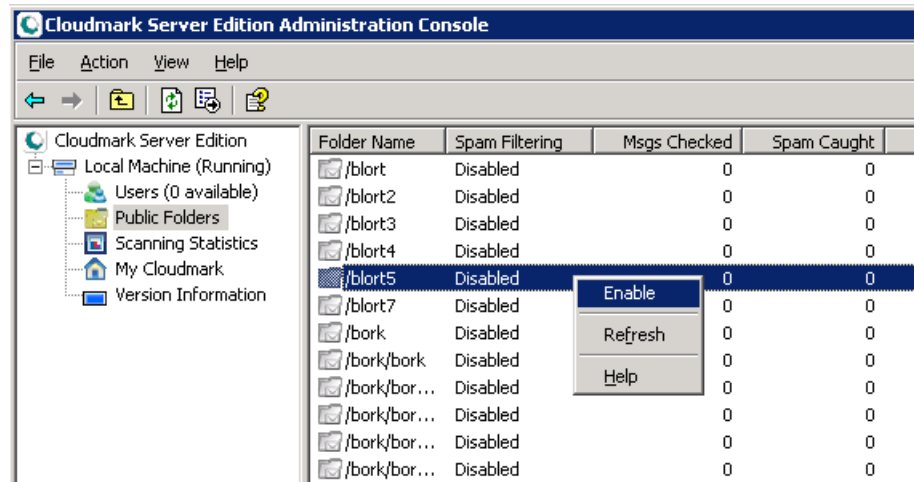
- 8 Select the CSE user you created when you installed the server.
- 9 Click OK.
- 10 In the Roles field, select Owner.
- 11 Make sure that all possible permissions are selected in the Permissions area.
- 12 Click OK.
- 13 Click OK to close the Properties window.

Enabling spam checking for a public folder

TO ENABLE SPAM CHECKING FOR A PUBLIC FOLDER

- 1 In the left pane of the Administration Console, expand the CSE server.
- 2 Click Public Folders.
The list of public folders appears in the right pane.
- 3 Select one or more public folders.

- 4 Right-click the selection to display the pop-up menu:



- 5 Click Enable.

The selected public folders are now marked “Enabled”.

Disabling spam checking for a public folder

TO DISABLE SPAM CHECKING FOR A PUBLIC FOLDER

- 1 In the left pane of the Administration Console, expand the CSE server.
- 2 Click the Public Folders folder.
The list of public folders appears in the right pane.
- 3 Select one or more public folders.
- 4 Right-click the selection to display the pop-up menu.
- 5 Click Disable.

The selected public folders are now marked “Disabled”.

Selectively disabling or enabling user feedback

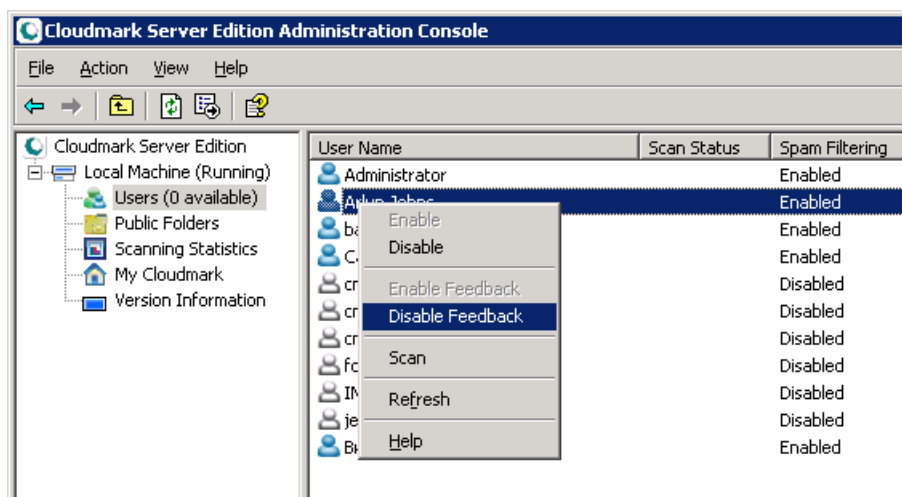
User feedback occurs when a user contests CSE’s automatic filtering by moving messages into or out of the local spam folder. Information about contested messages is automatically sent to the Cloudmark service, where it may influence future filtering of similar messages.

By default, feedback is enabled for all users. This is the recommended setting to achieve the best accuracy. You can change this global setting by following the instructions in “Disabling or enabling user feedback” on page 33. In some cases, you may wish to selectively disable feedback for specific users, as explained below.

For more information about how users submit feedback, see the *Cloudmark Server Edition User’s Quick Reference Guide*, designed for distribution to your end users.

HOW TO DISABLE FEEDBACK FOR A USER

- 1 In the left pane of the Administration Console, expand the CSE server.
- 2 Click the Users folder.
The list of users appears in the right pane.
- 3 Select one or more users.
- 4 Right-click the selection to display the pop-up menu:



- 5 Select Disable Feedback.
You can re-enable feedback for this user by selecting Enable Feedback.

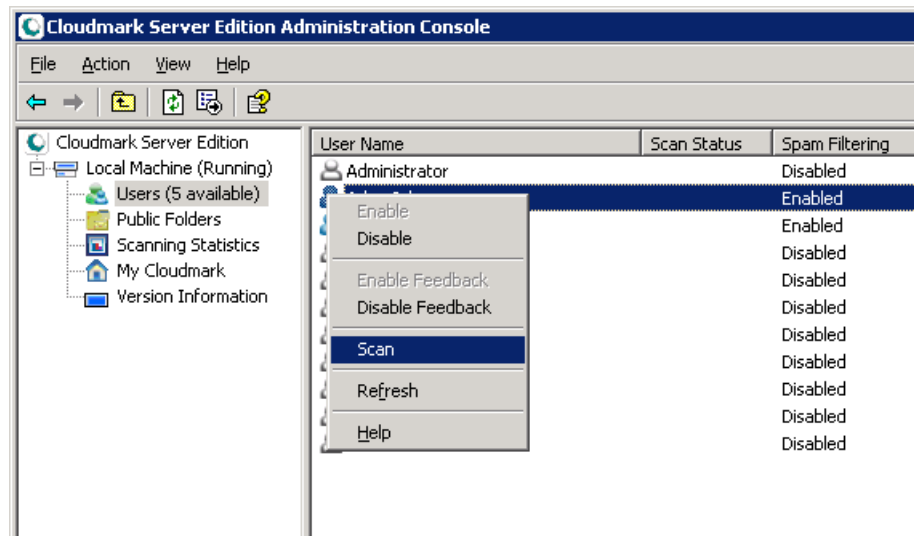
Selectively rescanning mailboxes

A mailbox can be rescanned on demand.

HOW TO RESCAN A MAILBOX

- 1 In the left pane of the Administration Console, expand the CSE server.
- 2 Click Users.

The list of users appears in the right pane.
- 3 Select one or more users.
- 4 Right-click the selection to display the pop-up menu:



- 5 Select Scan.

The Scan Status column now shows a status of “Pending” for this mailbox, then “Scanning” when scanning begins. The Scan Status column is empty when scanning is complete.

Accessing My Cloudmark

My Cloudmark is your interface to your Cloudmark account. Here you can view your statistics, change your account information or password, and view or update your subscription. You can also download software and technical documentation. My Cloudmark is secure; your account information is received only by Cloudmark.

There are two ways to access My Cloudmark:

- In the Administration Console, click My Cloudmark.
- Use your web browser to go to <https://my.cloudmark.com>.

Managing subscriptions

After your initial trial period, you must purchase a subscription to the Cloudmark Service for each CSE end user.

- “Purchasing a subscription after the trial period” below
- “Adding subscriptions” on page 56
- “Renewing subscriptions” on page 56

Purchasing a subscription after the trial period

Cloudmark notifies you before your CSE trial period expires, you are notified by Cloudmark, allowing you sufficient time to complete your evaluation and address any issues you may have. You can also use the Administration Console to view the number of days remaining in your trial period.

Once the trial period ends, click Purchase on the Administration Console. You are then directed to Cloudmark’s or your vendor’s web site to purchase a subscription.

Adding subscriptions

To add a subscription, right-click the name of the CSE server you want to activate the subscription on, and then click Activate. Enter your activation code obtained from either Cloudmark or your vendor.

Renewing subscriptions

If you have existing subscriptions, you can purchase additional subscriptions or renew existing ones from the My Cloudmark page (described in “Accessing My Cloudmark” on page 55).

Configuring CSE for Mobile Spam Filtering

There is a short delay between the time at which a spam message arrives at the Exchange server and the time at which it is filtered out of the mailbox by CSE.

- For mobile devices that receive messages by “server push” technology, the server should be configured to delay the push so that spam can be filtered before messages are delivered to the device.
- For mobile devices that receive messages by “client pull” technology, server configuration is not relevant. These devices can be configured to check for new messages at an interval that will generally accommodate spam filtering. On rare occasions, spam message may arrive at or about the moment at which the mobile device pulls new messages. In this case, the spam messages may be delivered to the device, unfiltered.

This chapter explains how to perform server-side configuration to introduce a message synchronization delay for mobile devices using server push technology. This delay allows CSE to filter spam before messages are delivered to mobile devices.

- “Configuring Microsoft Exchange ActiveSync for CSE” below
- “Configuring Blackberry Enterprise Server (BES) for CSE” on page 59
- “Configuring GoodLink for CSE” on page 60

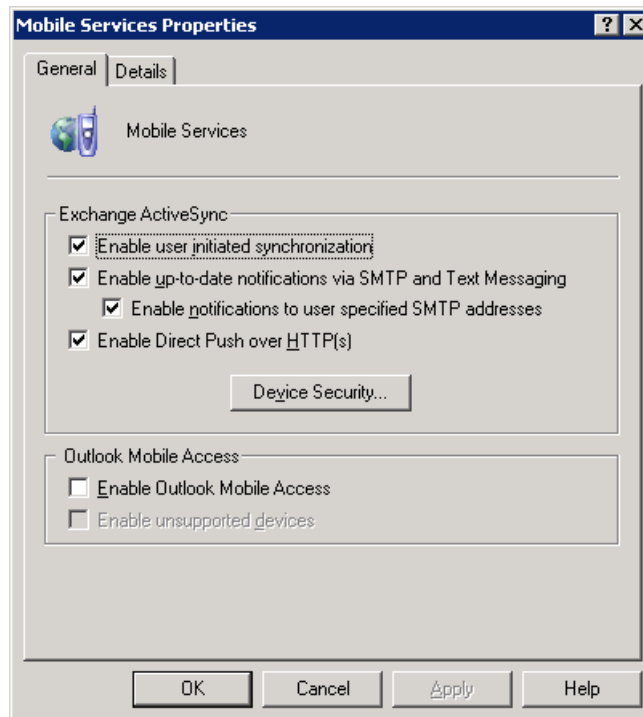
Configuring Microsoft Exchange ActiveSync for CSE

Although ActiveSync uses server push technology, the synchronization interval is set by the client device and not the server. This topic explains how to enable ActiveSync on the server side.

TO ENABLE EXCHANGE ACTIVESYNC

- 1 On the Exchange server, start the System Manager.
- 2 Expand the Global Settings folder.
- 3 Right-click Mobile Services.
- 4 Select Properties.

The Mobile Services Properties dialog appears:



- 5 Select "Enable user initiated synchronization".
- 6 Optionally, enable other Exchange ActiveSync features as appropriate for your organization.

For more information about these features, see the Microsoft Exchange Server documentation, available at <http://www.microsoft.com/>.

- 7 Click OK.

Configuring Blackberry Enterprise Server (BES) for CSE

When using CSE and Exchange in conjunction with Blackberry Enterprise Server, you can configure a 45-second synchronization delay in order to allow CSE to filter spam before messages are delivered to users' Blackberry devices.

Configuring BES 3.6 and below

TO CONFIGURE BES 3.6 AND BELOW

- 1 On the BES server, run Regedit.
- 2 Navigate to the following key:
`HKEY_LOCAL_MACHINE > SOFTWARE > Research In Motion > BlackBerry Enterprise Server > Servers > <ServerName>`
For example, <ServerName> might be "BESSERVER".
- 3 Locate the following DWORD value:
`ProcessMailDelay`
If this value does not exist, create it.
- 4 Set the value of ProcessMailDelay to 45 (or your preferred value).
- 5 Save the new value.
- 6 Restart BES.

Configuring BES 4.1.3 and above

TO CONFIGURE BES 4.0 AND ABOVE

- 1 On the BES server, run Regedit.
- 2 Browse to the following key:
`HKEY_LOCAL_MACHINE > SOFTWARE > Research In Motion > BlackBerry Enterprise Server > Agents`
- 3 Locate the following DWORD value:
`ProcessMailDelay`
If ProcessMailDelay does not exist, create it.
- 4 Set the value of ProcessMailDelay to 45 (or your preferred value).
- 5 Save the new value.
- 6 Restart BES.

Configuring GoodLink for CSE

GoodLink does not provide a method for configuring a delay in mail synchronization. Spam messages may initially appear on users' mobile devices. However, these spam messages disappear after CSE performs spam filtering, when the mobile device re-synchronizes with the GoodLink server.

Command-Line Interface

CSE includes a command-line tool called `csecmd` for managing CSE users. It can perform the following operations:

- list the users on a CSE installation
- enable or disable spam filtering per user
- enable or disable spam reporting per user
- scan a user's mailbox
- display the CSE version

Usage

Invoke `csecmd` as follows:

```
csecmd [/enable] [/disable] [/list] [-host:<host>]
[-port:<port>] [-user:<email>]
```

Table 1 *Command-line options*

Option	Description
<code>/enable</code>	enable a user for spam filtering (requires <code>-user:</code>)
<code>/disable</code>	disable a user for spam filtering (requires <code>-user:</code>)
<code>/enablefb</code>	enable feedback reporting for a user (requires <code>-user:</code>)
<code>/disablefb</code>	disable feedback reporting for a user (requires <code>-user:</code>)
<code>/scan</code>	scan a user's mailbox for spam (requires <code>-user:</code>)
<code>/list</code>	display all users that cse knows about
<code>/version</code>	display the version of cse
<code>-user:<email></code>	specify a user's email address to act upon

Table 1 *Command-line options*

Option	Description
-host:<host>	specify a remote host that CSE is running on (default: localhost)
-port:<port>	specify an alternate admin port that CSE is listening on (default: 9371)

csecmd will exit with zero on success and non-zero on error. The success or failure of the operation can be determined by examining the %ERRORLEVEL% environment variable.

Examples

For the following examples, CSE is running on stick.confused.cm.test. There is no need to specify a host parameter if csecmd is running on the local CSE server.

```
>csecmd /list -host:stick.confused.cm.test
Administrator@confused.cm.test:enabled
arly@confused.cm.test:enabled
barfoo@confused.cm.test:disabled
cmsink@confused.cm.test:enabled
cmsink2@confused.cm.test:disabled
cmsink3@confused.cm.test:disabled
foobar@confused.cm.test:enabled
imap@confused.cm.test:disabled
jesse@confused.cm.test:disabled
>csecmd /enable -user:barfoo@confused.cm.test -
host:stick.confused.cm.test
failed to enable user: barfoo@confused.cm.test
>echo %ERRORLEVEL%
1
>csecmd /disable -user:foobar@confused.cm.test -
host:stick.confused.cm.test
foobar@confused.cm.test disabled
>echo %ERRORLEVEL%
0
>csecmd /enable -user:barfoo@confused.cm.test -
host:stick.confused.cm.test
barfoo@confused.cm.test enabled
>echo %ERRORLEVEL%
0
```

Troubleshooting

This appendix contains troubleshooting information for starting and stopping the CSE service and the Administration Console, as well as correcting errors that occur while running the service.

Errors starting CSE

If you are unable to start Cloudmark Server Edition from the Administration Console, try to start it manually using the Services tool (Control Panel, Administrative Tools). On the tool, locate and right-click the Cloudmark Server Edition service and then click Start.

If the service still does not start, verify that the CSE user account information is set up correctly.

! *The Services tool can be used to grant “Log on as a service” rights, as well.*

TO VERIFY CSE USER ACCOUNT INFORMATION AND SETUP USING THE SERVICES TOOL

- 1** On the Services tool, right-click the Cloudmark Server Edition service and then click Properties.
- 2** On the Log On tab, verify that "This account" is the CSE administrator user and that the password is correct.
- 3** Select This account and then type the CSE user account name and password if it is incorrect. Click OK.

- 4 If a prompt informs you that the CSE user account is granted “Log on as a service” rights, click OK.

You should now be able to start Cloudmark Server Edition from the Cloudmark Server Edition Administration Console or from the Services tool.

Errors stopping CSE

If you are unable to stop CSE, use the Task Manager to end the cloudmarkse.exe process.

Errors opening the Administration Console

If you receive an error message when trying to open the Cloudmark Server Edition Administrative Console, ensure that the CSE user account is a member of the Domain Admins group, as described in “Setting up a Windows user account for CSE” on page 9.

CSE runtime errors

If CSE stops unexpectedly or displays abnormal behavior when running and you are using Exchange 2003, make sure the Hide from Exchange address lists option is disabled. This option is located in the Exchange Advanced tab of the User Properties window in the Active Directory Users and Computers tool.

If spam is not being moved to public folders designated for spam, check for the following log message:

```
WARN: Failed to open message [MAPI_E_NO_ACCESS]
ERROR: [xid=7] newmail: failed to open message
```

If this error appears, public folder permissions are not set correctly. See “Assigning ownership of a public folder to the CSE user” on page 51.

Logs

Event log messages

The following table lists the event log messages that Cloudmark Server Edition can output to the Windows Event Log.

Table 1 *Event log messages*

Event Log Message	Description
Cloudmark Server Edition has started	INFO – Indicates that the service has successfully started and Cloudmark Server Edition will now begin to initialize.
Cloudmark Server Edition has shutdown	INFO – Indicates that the service has been stopped.
Cloudmark Server Edition failed to connect to the Exchange server	WARNING – Indicates that there was a connection error attempting to connect to the Microsoft Exchange server. Cloudmark Server Edition will try again.
Cloudmark Server Edition failed to connect to the SpamNet Network	WARNING – Indicates that there was a connection error attempting to connect to the Cloudmark Global Threat Network. Cloudmark Server Edition will try again.
Check that a mailbox has been created for the Cloudmark Server Edition service account	ERROR – could prevent Cloudmark Server Edition from properly connecting to the Microsoft Exchange server. Verify that the user that the Cloudmark Server Edition service runs as has a mailbox on the Exchange server.
Cloudmark Server Edition exceeded user limit	ERROR – An attempt has been made to enable more users than the license allows.
Cloudmark Server Edition failed to startup	ERROR – Cloudmark Server Edition could not start. Refer to Appendix A, "Troubleshooting" for more instructions.
Cloudmark Server Edition failed to initialize	Fatal error that is followed by shutdown.

Error log messages

The following table lists installation and operation error messages and possible causes. Make a note of the error messages and associated error codes you receive before contacting Cloudmark Technical Support (<http://www.cloudmark.com/support/exchangeedition>).

Table 2 *Error log messages*

Error Message	Possible Causes
An error occurred attempting to load the settings for the Cloudmark Server Edition at the computer name specified. Ensure that you have a connection to the server, the appropriate administrative privileges and that Cloudmark Server Edition is installed correctly on the server.	This error is likely caused either by a connection problem or by incorrect permissions. Verify that the computer you are on is on the same network as Cloudmark Server Edition and is able to access it. Verify that you have given a correct computer name to connect to. Verify that all permissions are set correctly, as specified in "System requirements for CSE Server" on page 7.
The Cloudmark Server Edition Administration Console failed to start the Cloudmark Server Edition service.	Refer to Appendix A, "Troubleshooting", for steps to resolve issues starting or stopping the service.
You must have administrative permissions on Cloudmark Server Edition in order to Start or Stop the Cloudmark Server Edition service.	Verify that all permissions are set correctly, as specified in "System requirements for CSE Server" on page 7.
The Cloudmark Server Edition service is in an unknown state. Check for additional status in the Services management console on the server.	Refer to Appendix A, "Troubleshooting", for steps to resolve issues starting or stopping the service.

Trial Evaluation

Cloudmark offers a free trial evaluation period. You start your trial period when installing the product by selecting the appropriate option, as described in “Installing Cloudmark Server Edition” on page 16.

When the evaluation period ends, spam filtering is immediately disabled. An entry is logged in the Windows Event Log, indicating the end of the trial period, as well. An email is then sent to postmaster that provides purchasing information for Cloudmark Server Edition.

You can purchase a subscription to Cloudmark Server Edition by clicking Purchase in the Administration Console, which directs you to either the Cloudmark web site or your vendor, depending on who issued your activation code. When purchased, Cloudmark Server Edition is reactivated without the need to install and configure new software, or remove any existing software first.

Index

A

- accuracy 33, 46, 54
- ActiveSync 57
- Administration Console 1, 25
 - installing 21
 - launching 25
 - requirements 8
 - troubleshooting 64
- alternate discovery server 21, 40

B

- Blackberry Enterprise Server (BES) 59

C

- Cloudmark Collaborative Security Network 1, 3, 4
- command line interface 61
- command-line interface 2
- configuration 30
- connections
 - Admin Console to CSE 29
 - to Cloudmark 39
- csecmd 61

D

- disconnecting 29
- DNS proxy 40

E

- empty messages 37
- errors 64
- Exchange 2007 8, 15, 17
- Extended MAPI 8

F

- false positives 47

- feedback 9, 35, 46
 - enabling and disabling 33, 53
- filtering
 - automatic 30
 - empty messages 2
 - enabling and disabling 19, 61
 - for mobile devices 57
 - selective 49
- folders
 - public 20
 - spam folder 19, 36

G

- GoodLink 60

H

- HTTP proxy 21, 40

I

- IMAP 9
- installation 7, 16

L

- languages 48
- logs 65
 - enabling 34

M

- MAPI
 - profiles 39
- Microsoft Exchange 8, 15, 17
 - ActiveSync 57
- Microsoft Management Console (MMC) 1, 17
- Microsoft Messaging Application Programming Interface (MAPI) 4
- Microsoft Outlook 8, 9, 36
- Microsoft Outlook Express 36

Microsoft Outlook Web Access 9
mobile messaging 57
monitoring 2, 48
My Cloudmark 5, 18
 accessing 55

P

perfmon 48
performance 2, 48
Performance console 48
POP3 9
public folders 19, 20, 32, 36, 37, 51
 new 32

R

reports 2
 graphical 46
 monthly 46
requirements 7
rescanning 2
 on demand 54

S

scanning 2
 on demand 61
 statistics 45
spam
 action 36, 37
 actions 19
 spam-checking

 automatic 30
 mobile messaging 57
 selective 49
 statistics 44
 tagging 20
spam folder 19, 36
starting CSE 27
 errors 63
statistics 44
 comma-delimited 47
 graphical 45
 hourly 45
stopping CSE 28
 errors 64
subscriptions 56

T

trial evaluation 67
troubleshooting 63
troubleshooting logs 34

U

user feedback 2, 19, 35, 36
 enabling and disabling 61
 statistics 45, 46, 49

W

whitelists 2, 40
 exporting 42
 importing 42