Administrator Guide

Thirtyseven4 Exchange Protection 4.0

Thirtyseven4, LLC.
http://www.thirtyseven4.com

Copyright Information

All Rights Reserved.

Trademarks

End-User License Agreement

By using or installing any software product created by Thirtyseven4, L.L.C. an Ohio limited liability company having a principal place of business at P.O. Box 1642, Medina, Ohio 44258 (hereafter referred to as “Company”) including software components, source code, object code, and the corresponding documentation herein referred to as “Software”), you (herein referred to as “User”), are agreeing to be bound by the terms and conditions of this Agreement.

1. License Grant and Restrictions

In consideration for the license fee paid at time of purchase and subject to the conditions set forth in this Agreement, Company grants to User, a non-exclusive, non-sublicensable, non-assignable, non-transferable, worldwide right to use the Software.

User may only use the Software on one single computer. User may install the Software on a network, provided User have a licensed copy of the Software for each and every computer that can access the Software on the network.

User may not resell, rent, lease, distribute or transfer the Software in any way.

2. Fees

In consideration for use of the Software, User has agreed to pay Company the amount set forth on www.thirtyseven4.com, Company’s primary website, or the amount agreed to in writing between User and Company. USER EXPRESSLY ACKNOWLEDGES THAT PRIOR TO SUBMITTING ANY PAYMENT TO COMPANY OR USING THE SOFTWARE, THAT USER HAS REVIEWED AND AGREED TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

3. Ownership

The Software and all intellectual property rights, including collateral and/or derivative rights associated therewith are the property of Company. Should any of rights relating to the forgoing become vested in User or a third party by User's use of the Software, User shall immediately transfer and/or take all steps necessary, and without compensation to Company, to insure that all right, title and interest in the same vest fully and completely in Company.

The Software and any accompanying materials are copyrighted and contain proprietary information. Unauthorized copying of the Software or accompanying materials even if modified, merged, or included with other software, or of any documentation or written materials, is expressly forbidden. However, User may make one (1) copy of the Software solely for backup purposes provided all proper legal notices are reproduced in their entirety on the backup copy. Company reserves all rights not specifically granted to User.

The Software and documentation are licensed, not sold, to User. User may not rent, lease, display or distribute copies of the Software to others except under the conditions of this Agreement.

4. Termination

This Agreement is effective until terminated. This Agreement will terminate immediately and automatically without notice from Company for failure to comply with any provision contained herein or if the funds paid for the license are refunded or are not received.

Company also may terminate this Agreement with or without cause at any time by providing notice to User of its intent to Terminate. Should Company elect to terminate this Agreement under this provision and Customer has not violated any provision of this Agreement, Company shall refund any fees paid by User to Company during the twelve months that preceded the termination.

User agrees that if User desire to terminate this Agreement, that Company shall determine in its sole and absolute discretion whether or not to refund part or all of any fee paid by User for the Software. Therefore, User expressly acknowledges that User has no right to any refund.

Upon termination, User shall destroy the Software and all copies, in part and in whole, including modified copies, if any.

5. Warranties and Indemnities

Although efforts have been made to assure that the Software is date compliant, correct, reliable, and technically accurate, the Software is licensed to User “as is” and without warranties as to performance of merchantability, fitness for a particular purpose or use, or any other warranties whether expressed or implied. User assumes all risks when using it.

EXCEPT AS OTHERWISE EXPRESSLY STATED HEREIN, THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, AS TO THE VALUE, CONDITION, DESIGN, FUNCTIONING OF THE SOFTWARE, OR ANY USE OF THE SOFTWARE, MERCHANTABILITY, FITNESS FOR ANY PURPOSE OR USE OF THE SOFTWARE, FREEDOM FROM INFRINGEMENT OR ANY OTHER REPRESENTATION OR WARRANTY WHATSOEVER WITH RESPECT TO THE SOFTWARE. COMPANY SHALL NOT BE LIABLE TO ANY USER OF THE SOFTWARE, FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, LIABILITY, LOSS OR DAMAGE CAUSED OR ALLEGED TO HAVE BEEN CAUSED BY THE SOFTWARE, EVEN IF COMPANY WAS A AWARE OF THE POTENTIAL FOR SUCH DAMAGES AND LOSS TO OCCUR.

USER SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS COMPANY, ITS LICENSORS, DEALERS, INDEPENDENT CONTRACTORS, SHAREHOLDERS, DIRECTORS, EMPLOYEES, OFFICERS, AFFILIATES AND AGENTS, AND THE RESPECTIVE SHAREHOLDERS, DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES AND AGENTS OF EACH OF THE FOREGOING, FROM AND AGAINST ANY AND ALL CLAIMS, ACTIONS, JUDGMENTS, LIABILITIES, COSTS AND EXPENSES (INCLUDING LEGAL FEES) RELATING TO OR ARISING FROM

THE USE OR DISTRIBUTION OF USER APPLICATIONS OR SERVICES PROVIDED BY USER (INCLUDING, BUT NOT LIMITED TO, CLAIMS RELATING TO LIABILITY FOR INFRINGEMENT OF PROPRIETARY RIGHTS, INTELLECTUAL PROPERTY RIGHTS, U.S. EXPORT AND IMPORT LAWS, DEFECTIVE PRODUCTS, OR PRODUCT LIABILITY CLAIMS).

User expressly acknowledges that any modification of the Software, whether or not permitted, is beyond the control of Company, and as such, such modification shall void any warranties, express or implied, under this Agreement.

6. Controlling Law and Severability

This Agreement shall be governed by and construed in accordance with the laws of the United States and the State of Ohio, as applied to agreements entered into and to be performed entirely within Ohio between Ohio residents. The federal and state courts of the State of Ohio, County of Medina, shall have exclusive jurisdiction and venue over any dispute, proceeding or action arising out of or in connection with this Agreement or User’s use of the Software. If venue is appropriate in federal court and that federal court is not located in Medina County, User and Company agree to litigate any disputes in a federal court located in Cuyahoga County, Ohio. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement shall be enforced to the maximum extent permissible so as to affect the intent of the arties, and the remainder of this Agreement shall continue in full force and effect.

7. Non-Binding Mediation

Company and User agree to submit the dispute to non-binding mediation before resorting to litigation. Mediation shall occur in Medina, Ohio before a single mediator jointly selected by the parties. The parties agree to each pay one-half of the mediator’s fee. Company and User agree to waive any possible arbitration claims unless Company and User later agree to arbitrate this dispute following mediation, wherein such arbitration shall be binding and incur in lieu of litigation.

8. Limitation of Liability and Fees

COMPANY'S TOTAL LIABILITY, INCLUDING ANY DAMAGES, SHALL NOT EXCEED THE TOTAL AMOUNT USER PAID TO COMPANY. SHOULD COMPANY BE FORCED TO MEDIATE, ARBITRATE, OR LITIGATE ANY DISPUTE AGAINST USER AND SHOULD COMPANY PREVAIL IN SUCH DISPUTE, USER SHALL REIMBURSE COMPANY FOR ALL OF ITS ATTORNEY FEES AND COSTS ASSOCIATED WITH THE ENTIRE DISPUTE, INCLUDING FEES OR COSTS INCURRED PRIOR TO ANY CLAIM BEING FILED AND ALL OF COMPANY'S COSTS, INCLUDING ATTORNEY'S FEES, ASSOCIATED WITH THE MEDIATION, ARBITRATION, OR LITIGATION.

9. Non-Waiver

The failure by Company at any time to enforce any of the provisions of this Agreement or any right or remedy available hereunder or at law or in equity, or to exercise any option herein provided, shall not constitute a waiver of such provision, right, remedy or option or in any way affect the validity of this Agreement. The waiver of any default by Company shall not be deemed a continuing waiver, but shall apply solely to the instance to which such waiver is directed.

10. Successors; Assigns

This Agreement shall be binding on and inure to the benefit of the parties and their respective successors and permitted assigns. Except as provided for herein, this Agreement may not be assigned by User without the prior written consent of Company.

11. Use of Site Image

User grants a perpetual, world-wide, royalty-free license to Company to use and publish one or more screen shot captures of any User web sites using the Software, User's trademarks, logos or names and/or otherwise list User as a licensee of Company; provided, however, no such license shall be granted to Company if User sends an e-mail to Company stating objecting to such license within ten (10) days of receiving the Software.

12. Complete Agreement

This Agreement constitutes the complete agreement between the User and the Company. No amendment or modification may be made to this Agreement except in writing signed by User and Company.

Please contact us with any questions or concerns regarding this Agreement.

About the Document

This User Guide covers all the information about how to install and use Thirtyseven4 Exchange Protection in the easiest possible ways. We have ensured that the details provided in this guide are up-to-date with the latest developments in the software.

The following list describes the conventions that we have followed to prepare this document.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down box, dialog, button names, hyperlinks, and so on.
	This symbol indicates additional information or important information about the topic being discussed.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.

Thirtyseven4 Exchange Protection Highlights

Thirtyseven4 Exchange Protection 4.0 (TSEP) provides effective protection against malware and spams. TSEP is easy-to-use administration console that you can customize as per your requirements, apply protection rules for content filtering, AntiSpam, and monitor features and reports.

Some of the important features of TSEP include:

Virus Scan
The robust virus scanning engine of Thirtyseven4 Exchange Protection detects viruses and other infections. For better management of virus identification, virus scanning may be initiated at any of the following levels: Transport Scan and Edge Transport Scan. This helps you receive the emails in a more secured environment.

AntiSpam
AntiSpam provides you the facility to set rules for protection for all inbound and outbound mails. You may set strict rules for spam emails, or go on a normal way depending on your requirement or the types of emails you receive frequently. When you set the AntiSpam feature, all inbound and outbound messages are filtered by the AntiSpam agent and metadata is added by which you easily identify whether the messages are spams.

Content Filtering
Content Filtering filters all emails based on various filtering criteria such as sender or sender's domain, keywords in the subject line, file type and file name and words or phrases in the body text so every suspicious email is effectively identified and filtered.

Schedule Scan
TSEP helps you define a scan schedule so that the mailboxes and public folders are scanned automatically at the scheduled time. You can define multiple schedules so the scanning is initiated at your convenience. Additionally, you can scan your mailbox manually as well if you prefer by using Store Scan.

Notification
TSEP sends notification regularly to keep the administrators updated about the virus infections and policy breaches in the emails. Notifications are the messages about all important system events such as license getting expired, password is change and so on, so that you can take the appropriate actions on time and avoid any mishap.

Quarantine
Quarantine is a folder where suspicious emails are placed. If you have selected quarantine as an action to be taken for reasons such as a virus or spam is found or content filtering criteria are met, the suspicious emails are placed in the quarantine folder. Organizations need to preserve email communications for legal and other organizational policy compliance and the quarantine folder comes as a rescue to the valuable email communication across the board. All suspicious messages are quarantined so you can look all the emails manually and check whether you need them. If you need them you can restore otherwise you can remove them.

Reports
The Reports feature provides a detailed view of all the actions and events that TSEP keeps on taking regularly. This is helpful as it provides you the option to save and download the reports for future references, and see what actions have been taken.

For more information about Thirtyseven4 Exchange Protection, visit http://www.thirtyseven4.com.

Contents

Chapter 1. Getting Started

Thirtyseven4 Exchange Protection (TSEP) is simple to install and easy to use. During installation, read each installation screen carefully, and follow the instructions.

Prerequisites

Pre-Installation

Multiple Exchange security products installed on a single system may result in system malfunction. If any other Exchange security software is installed on your system, you need to remove it before proceeding with the Thirtyseven4 Exchange Protection installation.

Please ensure the following before installing Thirtyseven4 Exchange Protection (TSEP) on your system.

- x64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T).
- x64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform.
- 1500-MB disk space for TSEP. This space exclude the disk space required for items such as quarantined messages and attachments, reports, and log data.
- Microsoft Internet Information Services (IIS) Manager (Only for TSEP Console or Complete installation).
- .NET Framework 3.5.
- Monitor that supports 1024 x 786 resolution at highest (32 bit) colors or later.
- Microsoft SQL Server 2008 R2 / SQL Server 2012 Express (with Management Studio) should be installed in Mixed Mode Authentication.

Post-Installation

After installing SQL Server, ensure the following:

- SQL Server service is running
- SQL Server Browser service is running
- Add Firewall exception for SQLServer (Default port - 1433 TCP)
- Add Firewall exception for SQLBrowser (Default port - 1434 UDP)

Note: SQLServer and SQLBrowser ports may vary depending on your system.

Firewall Exception for Node Update

To update the Thirtyseven4 Exchange Protection nodes, add the Exchange Protection Service port in the firewall exception.

Add Firewall exception for ExchgProtService (Port Range: 51101 - 51105 TCP)

Note: On Windows Server 2003 operating system, check on which port Exchange Protection Service is running and add the firewall exception accordingly.

System Requirements

To use Thirtyseven4 Exchange Protection, your system should meet the following minimum requirements.

Operating Systems

- Microsoft Windows Server 2008 x 64 R2 Standard Edition
- Microsoft Windows Server 2008 x 64 R2 Enterprise Edition
- Microsoft Windows Server 2012 Standard
- Microsoft Windows Server 2012 Datacenter

Exchange Platforms

- Microsoft Exchange Server 2013

Supported Exchange platforms for Edge Role

- Microsoft Exchange Server 2010 Service Pack 3
- Microsoft Exchange Server 2007 Service Pack 3 (Rollup 10 and later)

Browser Compatibility

- Internet Explorer (IE) 8.0 and later
- Firefox 3.6 and later
- Google Chrome 10 and later

Email Clients

- Microsoft Outlook client
- Outlook Web Access(OWA)
- Exchange ActiveSync
- POP3 and IMAP4

Other Requirements:

- Internet connection to receive updates.
- The requirements provided are minimum system requirements. Thirtyseven4 recommends your system has higher configuration than the minimum requirements to obtain best results.
- To check for the latest system requirements, visit http://www.thirtyseven4.com.

Deployment Plan of TSEP

TSEP should be deployed in compliance with the following guidelines.

Scenario 1: TSEP Environment with Exchange Edge Transport

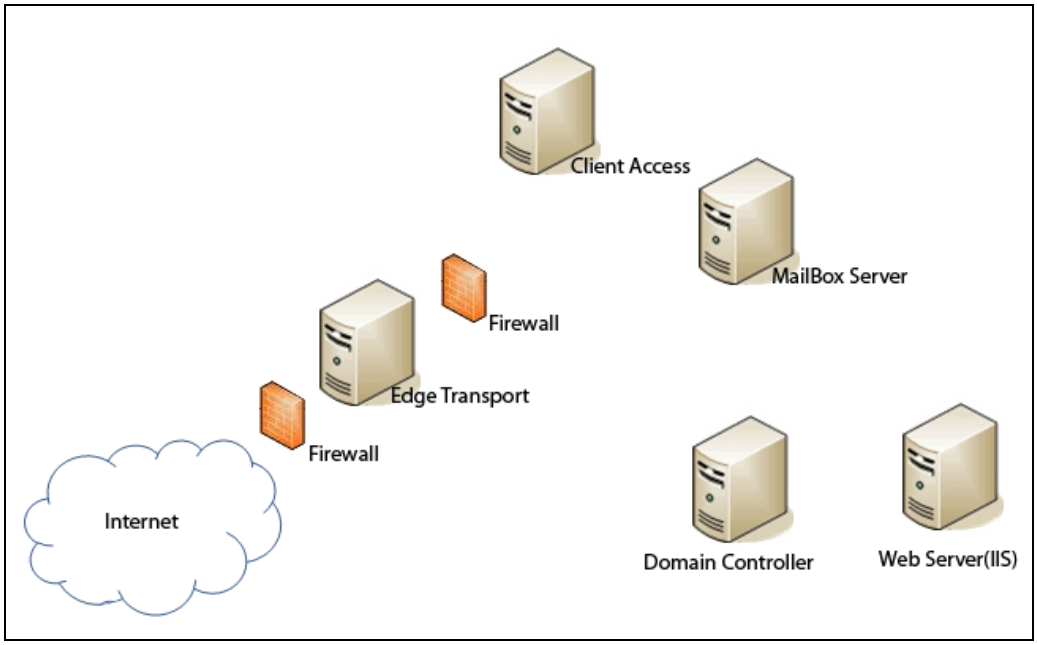


Figure 1: TSEP installation where Exchange Edge Transport is present.

In this scenario, Exchange Edge Transport role is placed to face the Internet and the remaining Exchange roles are installed on separate systems.

Deploying TSEP with Exchange Edge Transport

Make sure that SQL Server 2008 R2 or SQL Server 2012 is installed in the Exchange environment as Thirtyseven4 Exchange Protection uses SQL Server 2008 R2 or SQL Server 2012 for maintaining the configuration and reports during and after the installation.

1. Install TSEP web console on the system where IIS Web Server is installed.
2. Install TSEP components on the Exchange Nodes such as Edge and Mailbox.

For detailed information about how to install TSEP, see Installing TSEP in the following section.

Scenario 2: TSEP Environment with Exchange Mailbox role

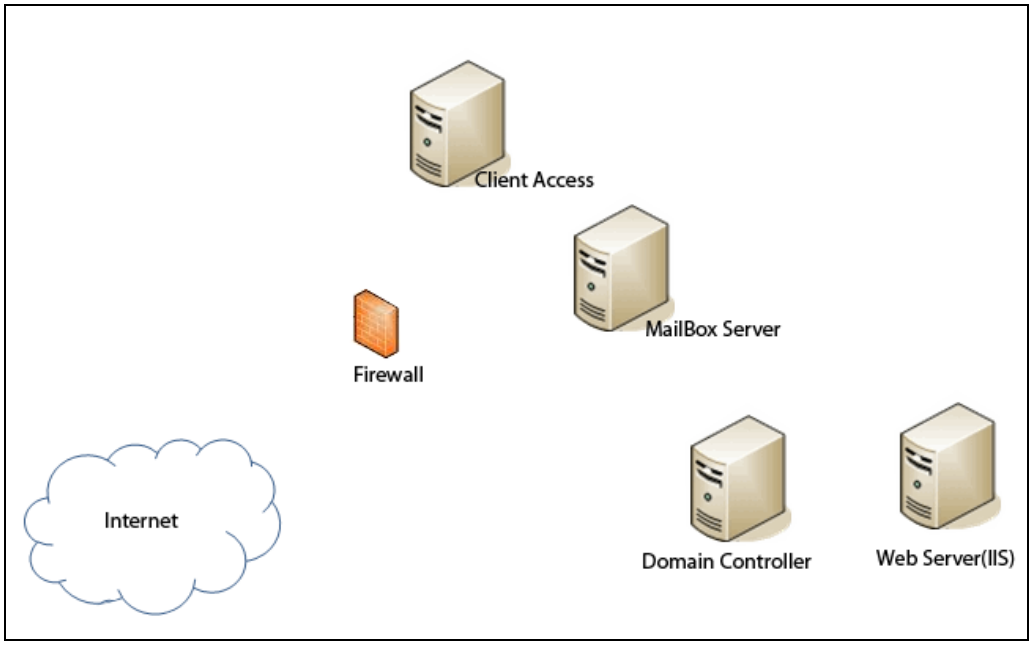


Figure 2: TSEP installation where Exchange Mailbox and Client Access roles are present on same system.

In this scenario, Exchange Mailbox role is placed to face the Internet and the remaining Exchange roles are installed on separate systems.

Deploying TSEP with Exchange Mailbox role

Make sure the SQL Server 2008 R2 or SQL Server 2012 is installed in the Exchange environment as Thirtyseven4 Exchange Protection uses SQL Server 2008 R2 or SQL Server 2012 for maintaining the configuration and reports during and after the installation.

1. Install TSEP web console on the system where IIS Web Server is installed.
2. Install TSEP component on the Exchange Mailbox Server.

For detailed information about how to install TSEP, see Installing TSEP in the following section.

Note: If you have installed multiple Exchange Mailbox servers, you have to install TSEP component on all Mailbox servers.

Scenario 3: TSEP Environment with DAG Mailbox Server

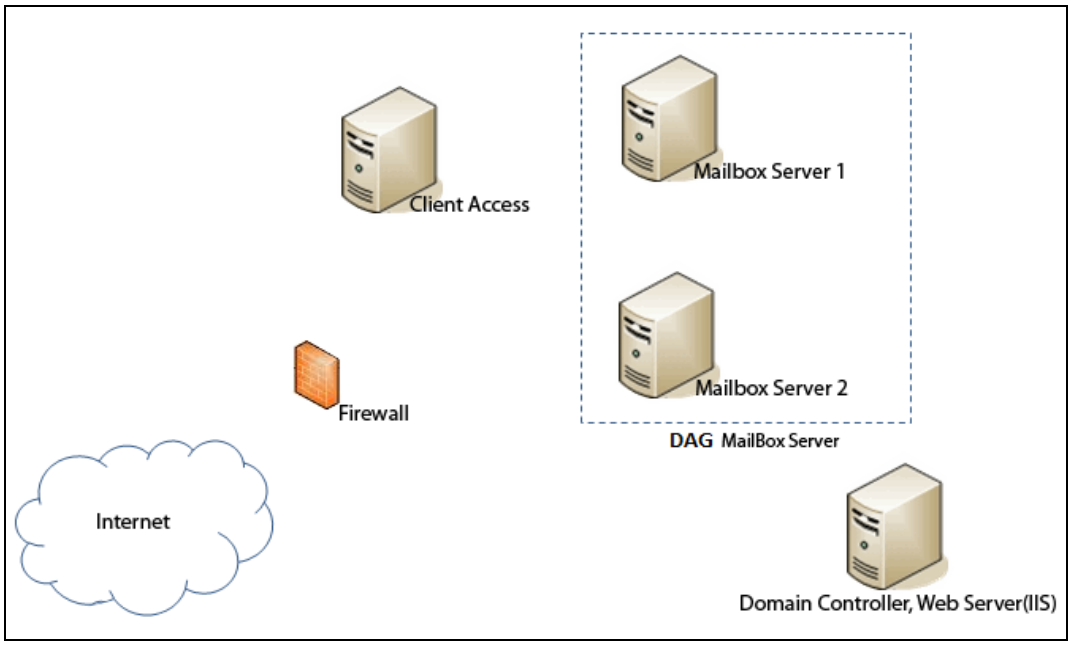


Figure 3: TSEP installation where DAG Mailbox Server is present.

This Exchange environment is similar to the environment scenario 2 but this environment includes the DAG mailbox server.

Deploying with DAG Mailbox server

Make sure that SQL Server 2008 R2 or SQL Server 2012 is installed in the Exchange environment as Thirtyseven4 Exchange Protection uses SQL Server 2008 R2 or SQL Server 2012 for maintaining the configuration and reports during and after the installation.

1. Install TSEP web console on the system where IIS Web Server is installed.
2. Install TSEP components on the Exchange DAG Nodes.

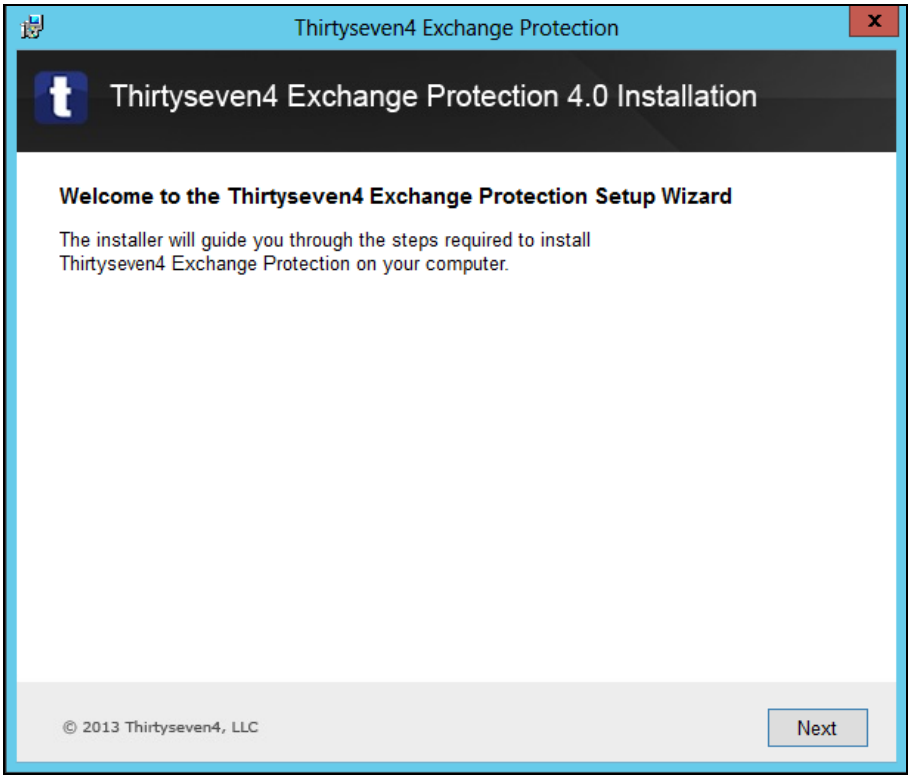
For detailed information about how to install TSEP, see Installing TSEP in the following section.

Installing TSEP

To install Thirtyseven4 Exchange Protection on your system, follow these steps:

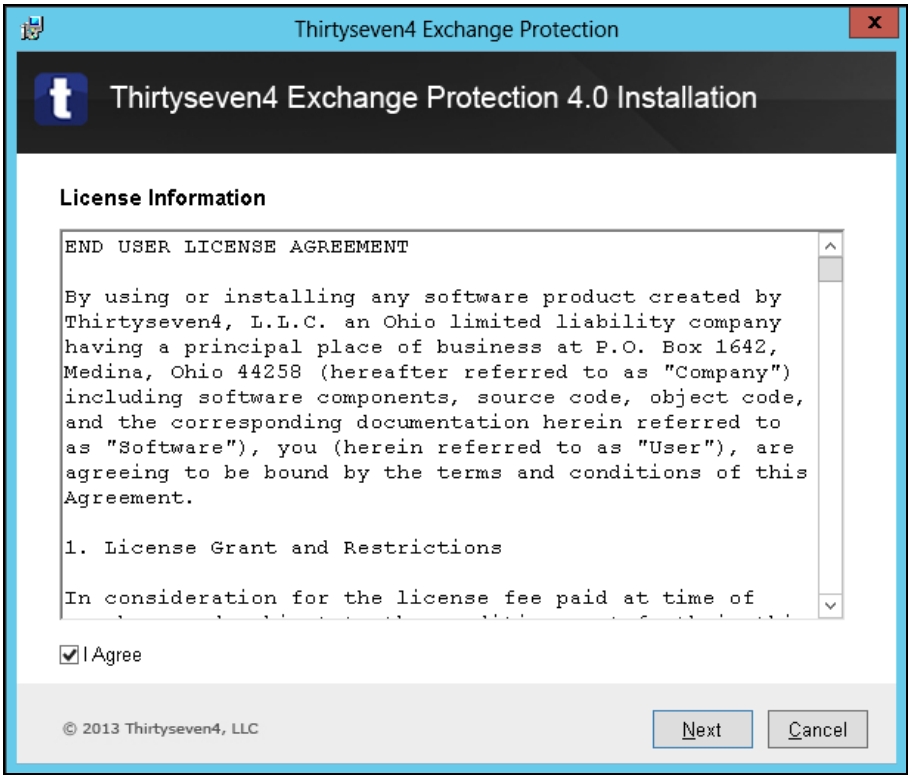
1. Insert the installation CD/DVD into the drive.
2. Click **Thirtyseven4 Exchange Protection.pkg** to launch the installer.

   The Welcome to Thirtyseven4 Exchange Protection Setup Wizard appears.



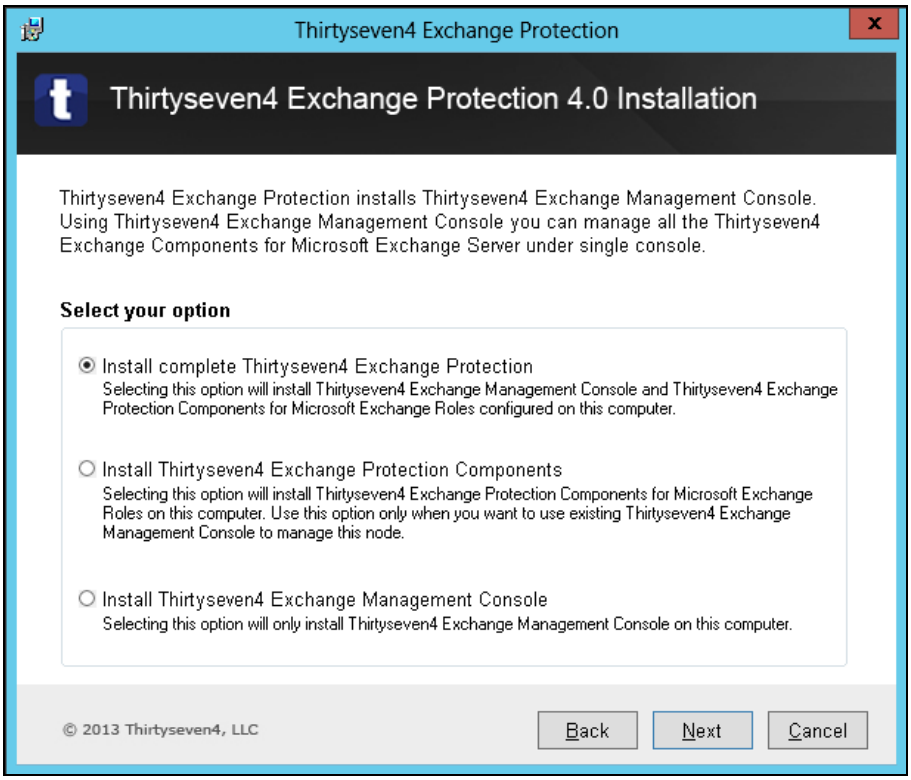
3. Click **Next** to continue.

   The user license agreement page appears.



4. Select the **I Agree** check box, and then click **Next**.

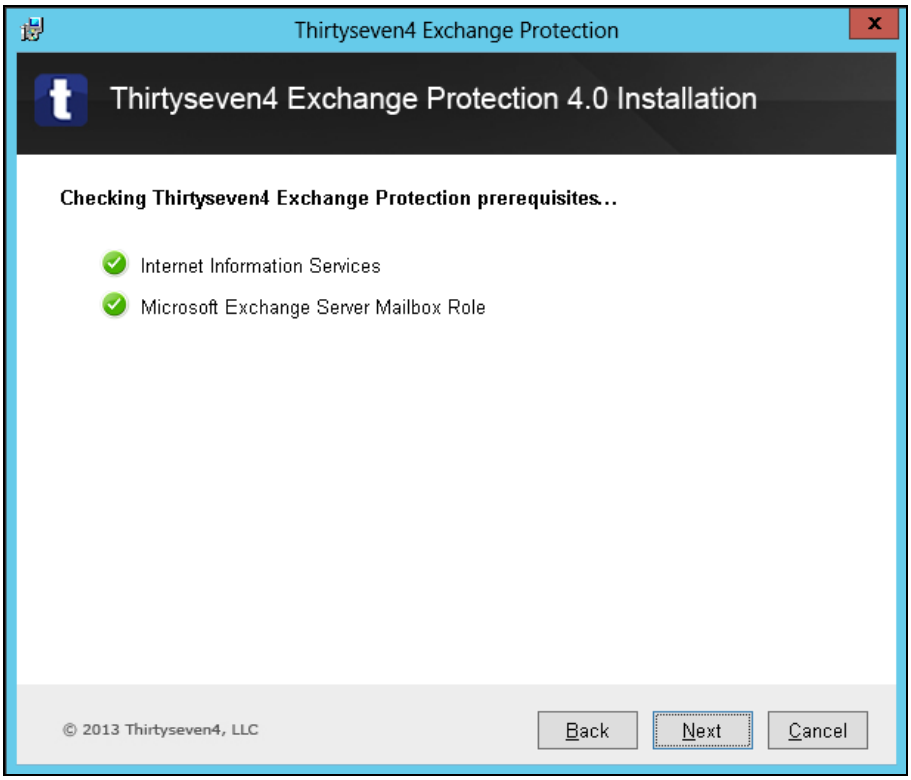
   *The **Select your option** screen appears with three installation options: Complete Thirtyseven4 Exchange Protection, Thirtyseven4 Exchange Protection Components, and Thirtyseven4 Exchange Management Console. Complete Thirtyseven4 Exchange Protection installs both Thirtyseven4 Exchange Protection Components and Thirtyseven4 Exchange Management Console components, while the other two are individual components.*



5. Select one of the options that you want to install, and then click **Next**.

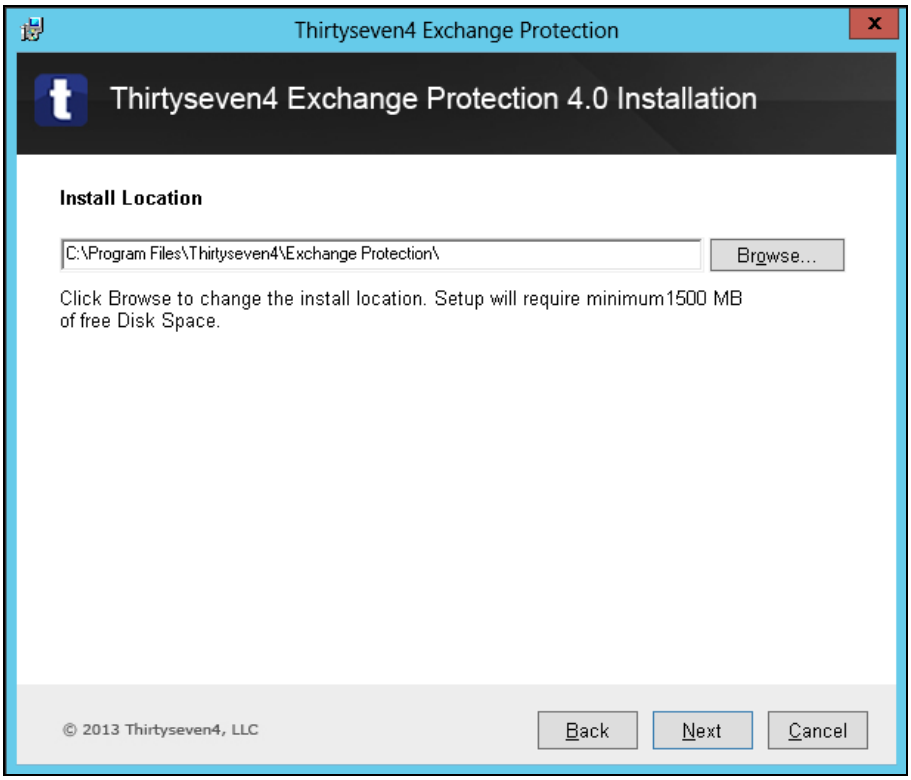
   Note: In this installation example, Complete Thirtyseven4 Exchange Protection is selected that is also a default selection. Screen displays for other application types are similar with minor variance.

   When installing a component, prerequisites for the relevant component are displayed.



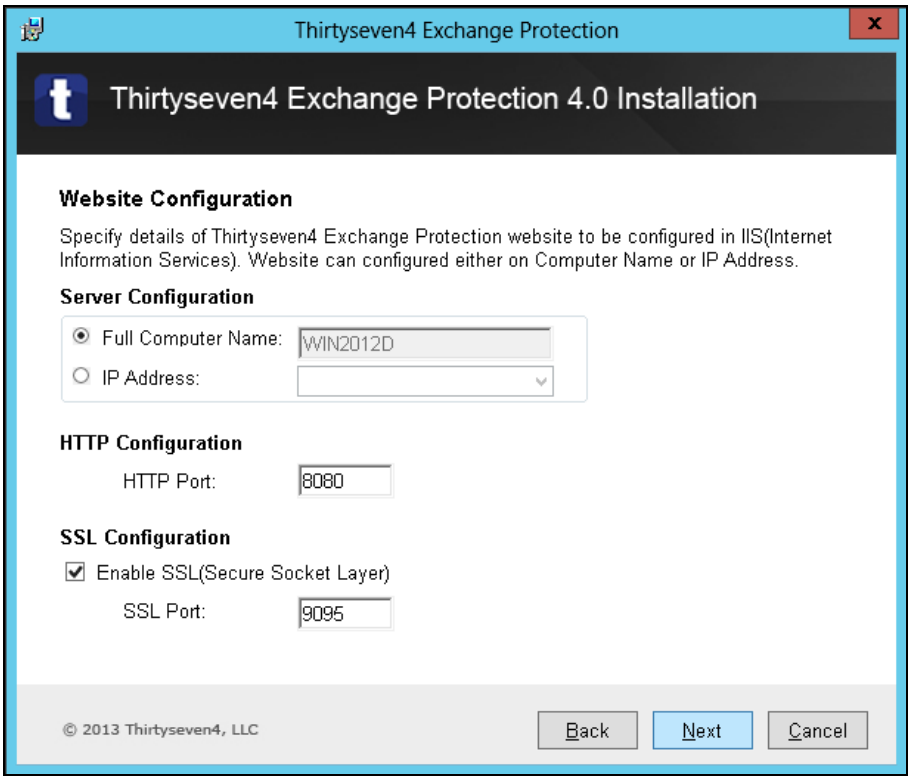
6. Click **Next** to continue.

   The default installation location appears that you may change if required.



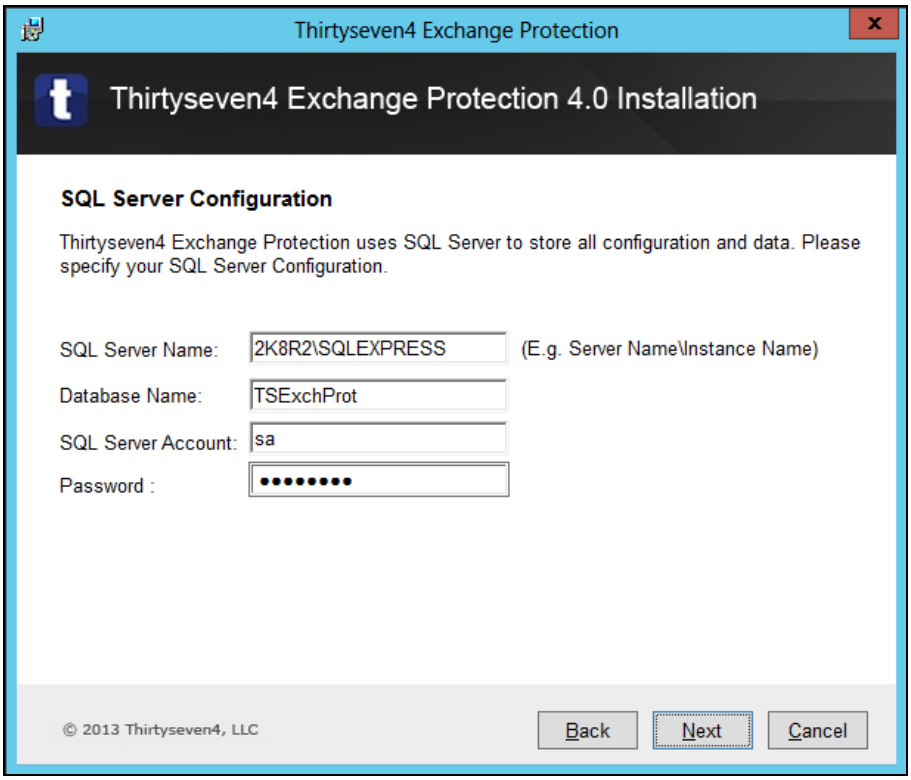
7. Click **Next** to continue.

   The Website Configuration screen appears.



8. Select the Computer Name or IP Address, enter HTTP Port, and SSL Port. The application URL will be based on the configuration you do here. The URL would combine the server configuration and either of the HTTP Port or SSL Port configuration whichever will be available.
9. Click **Next** to continue.

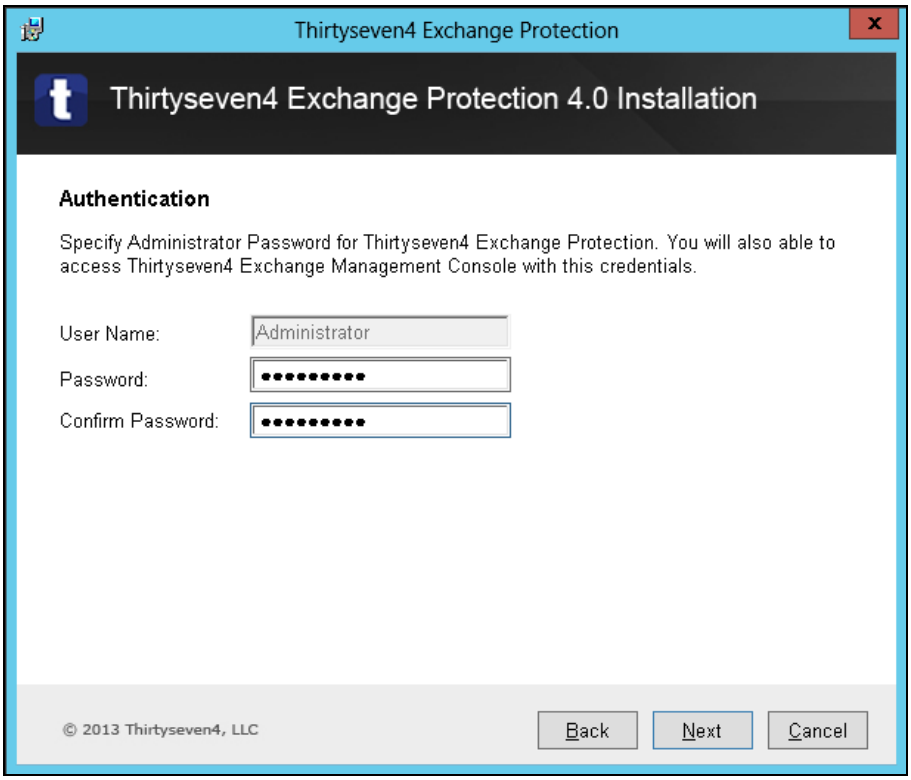
   The SQL Server Configuration screen appears.



10. Enter the SQL Server Name, Database Name, SQL Server Account, and Password in the relevant fields, and then click **Next**.

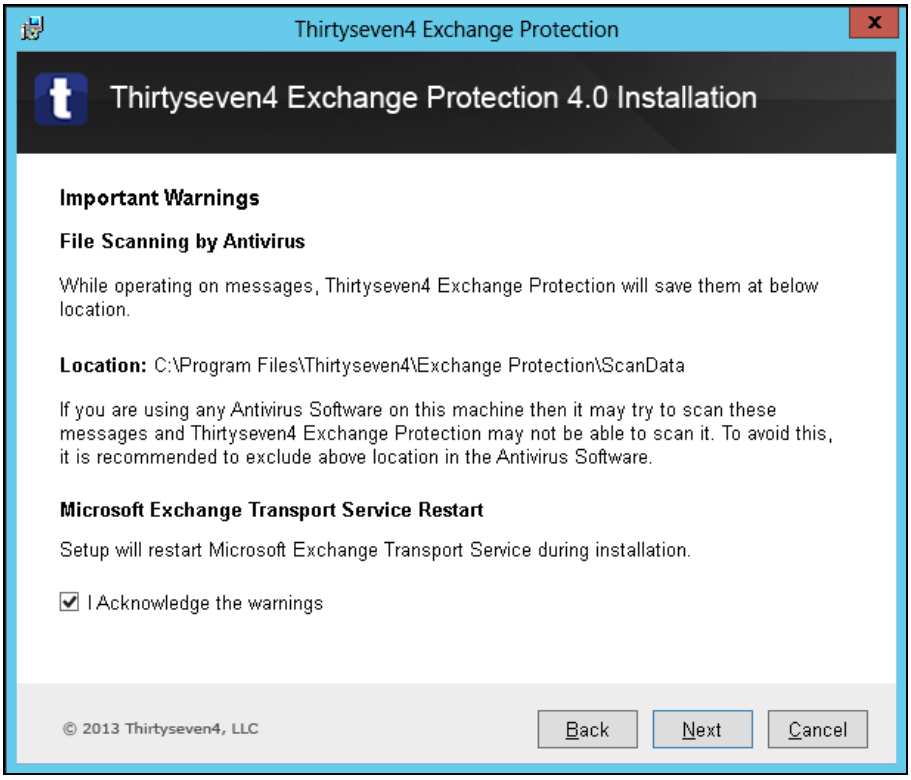
    SQL Server name is displayed automatically in the relevant fields if SQL Server is installed on the same server or you can use SQL Server installed on other system.

    The Authentication screen appears.



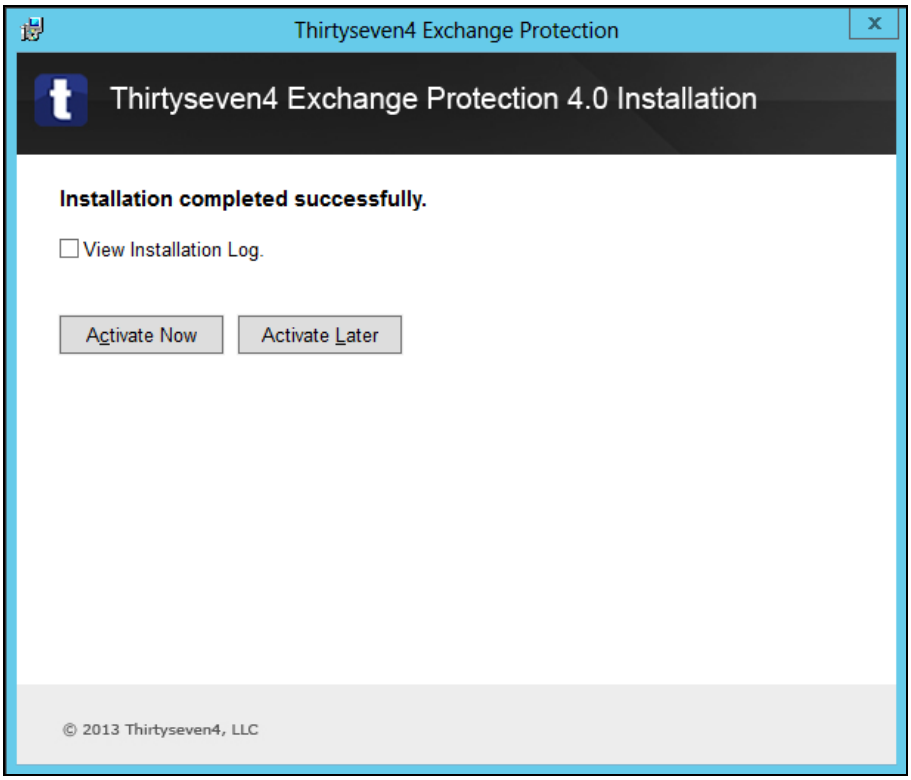
11. Enter your credentials and then click **Next**.

The Important Warnings screen appears that displays the installation location and acknowledgement.



12. Select the **I Acknowledge the warnings** check box, and then click **Next**.

    Installation starts. When installation is complete a message is displayed.



- Make sure that the user doing the installation is a domain user with administrative privileges on the system on which TSEP is being installed.
- You can install TSEP Management Console outside domain also. However, you need to have Server 2003 & IIS 6.0 and later for this.

.

Post Installation Task

TSEP sends email notifications to keep the users updated about virus incidents, policy breaches in the emails, system events such as license getting expired, password change and so on. Email notifications are also important to the administrators who prefer to have the updates delivered directly to their mailbox instead of continually checking the logs for various activities.

Note: In these scenarios, you can also configure third party SMTP Host in TSEP SMTP Host Settings for sending Notification.

SMTP Server Configuration

To configure SMTP Virtual Server on Windows Server 2003 operating system, follow these steps:

1. Select **Start > Control Panel**.
2. Double-click the **Add** or **Remove Programs** option.

   The Add or Remove Programs dialogue appears.
3. In the left pane, click the **Add/Remove Windows Components** option.

   The Windows Components Wizard dialogue appears.
4. In the Components list, click **Application Server**, and then click **Details**.

   The Internet Information Services dialogue appears.
5. In the Subcomponents of Application Server list, click **Internet Information Services (IIS)**, and then click **Details**.
6. In the Subcomponents of Internet Information Services (IIS) list, select the **SMTP Service** check box, and then click **OK**.
7. Click **Next**.

   A prompt may appear for the Windows Server 2003 family CD or the network path for installation.
8. Click **Finish**.
9. Go to IIS Manager, expand the local computer, expand the Default SMTP Virtual Server option, and then right-click the component that you want to configure.
10. Click **Properties**.

    On the **property** pages, make changes in the default settings as per your requirement.

Note:

i. To configure SMTP Virtual Server on Windows Server 2008 operating system, install SMTP Server feature using server manager.

ii. While configuring SMTP Virtual Server, make sure that the port number assigned to the SMTP Virtual Server is not being used by any other application or component.

iii. While configuring SMTP Virtual Server in TSEP console, make sure that anonymous permissions are set to receive connectors both at Transport sever and Edge server.

Activating TSEP

Once Thirtyseven4 Exchange Protection is installed on your computer, you can activate the product anytime you prefer. However, you are recommended to activate the product immediately after installation so that you can use all the features without any interruption.

To activate Thirtyseven4 Exchange Protection, follow these steps:

1. Select **Start > Programs > Thirtyseven4 Exchange Protection 4.0 > Activate Thirtyseven4 Exchange Protection**.

   The Registration Wizard appears.

   The wizard searches for whether your computer is connected to the Internet. For activating your product you need Internet connection.

2. Enter the 20-digit Product Key and click **Next**.

   The Registration Information page appears.

3. Enter relevant information in the **Purchased from** and **Register for** text boxes, and then click **Next**.

   The Educational/Company Information page appears.

4. Provide user information in the relevant text boxes and select your choices in the **Country**, **State** and **City** lists. In case your State/Province and City are not available in the list, you can type your locations in the respective text-boxes, and the click **Next**.

   *A confirmation screen appears with the details entered in the preceding step. If any modifications are needed, click **Back** to go to the previous screen and make the required changes, and then click **Next**.*

   Your product is activated successfully. The date when your license expires is displayed.

5. Click **Finish** to close the Registration Wizard.

Note: To activate the TSEP license, you are required to connect your system to the Internet. The activation wizard uses direct connection if available. If direct connection is not available, the web browser proxy is used and if the web browser proxy is not available, the proxy settings wizard appears with a message about it.

Renewing License Through Registration Wizard

With License Renewal, you can renew your license whenever you need once you have activated your license. You can renew your license within four months from the date your current license has expired.

To renew Thirtyseven4 Exchange Protection, follow these steps:

1. Select **Start > Programs > Thirtyseven4 Exchange Protection 4.0 > Activate Thirtyseven4 Exchange Protection**.

   The Registration Wizard appears.

   The wizard searches for whether your computer is connected to the Internet. For renewing your product you need Internet connection.

2. Enter the 20-digit Product Key and click **Next**.

   If your current license has expired, the renewal screen displays a message about it. You can renew your license by purchasing a renewal key.

3. Enter the renewal key and then click **Next**.

   The Registration Information page appears.

4. Enter relevant information in the **Purchased from** and **Register for** text boxes, and then click **Next**.

   *A confirmation screen appears with the details entered in the preceding step. If any modifications are needed, click **Back** to go to the previous screen and make the required changes, and then click **Next**.*

   Your license is renewed successfully. The date when your license expires is displayed.

5. To close the Registration Wizard, click **Finish**.

Logging in to TSEP

Access the URL of the Thirtyseven4 Exchange Protection (TSEP) application and then enter your credentials to log in.

As you log in to the application the Dashboard appears, which is also the Home screen. Here you see the status whether any of the Virus Scan, AntiSpam, Content Filtering, and Automatic Update features is enabled or disabled and the summary of Virus Scan, AntiSpam, and Content Filtering about how many emails have been scanned and whether there are any infected emails.

The summary gets updated continuously.

Managed Servers: Helps you check the details of all the servers that are being managed under TSEP. To see the details, click **View Details**.

Threat Meter: Displays the intensity of threats detected in your organization.

Alert: An alert is displayed here about an event that demands your action. Click **Show All** to see all the alerts. (The **Show All** link is displayed only if multiple alerts are available) You can take appropriate action to fix the issue. However, alert is displayed only if there is any event.

Status: Indicates the current status of the features, which of them are enabled and which are disabled.

Note: All those features that are enabled are displayed in green color, while those disabled are displayed in red color.

Summary: Summary is a brief report of clean and infected inbound, outbound, and internal emails.

String	Description
Inbound	All incoming emails are known as inbound emails.
Outbound	All outgoing emails are known as outbound emails.
Internal	All emails within the same domain are known as internal emails.
Store	These are the emails from Mailbox Stores.

Note: You cannot log in to console if TSEP is not activated.

Uninstalling TSEP

Uninstalling Thirtyseven4 Exchange Protection exposes your system and your valuable data to virus threats. However, before uninstalling TSEP Console or Complete TSEP, ensure that all the TSEP components on other systems are already uninstalled.

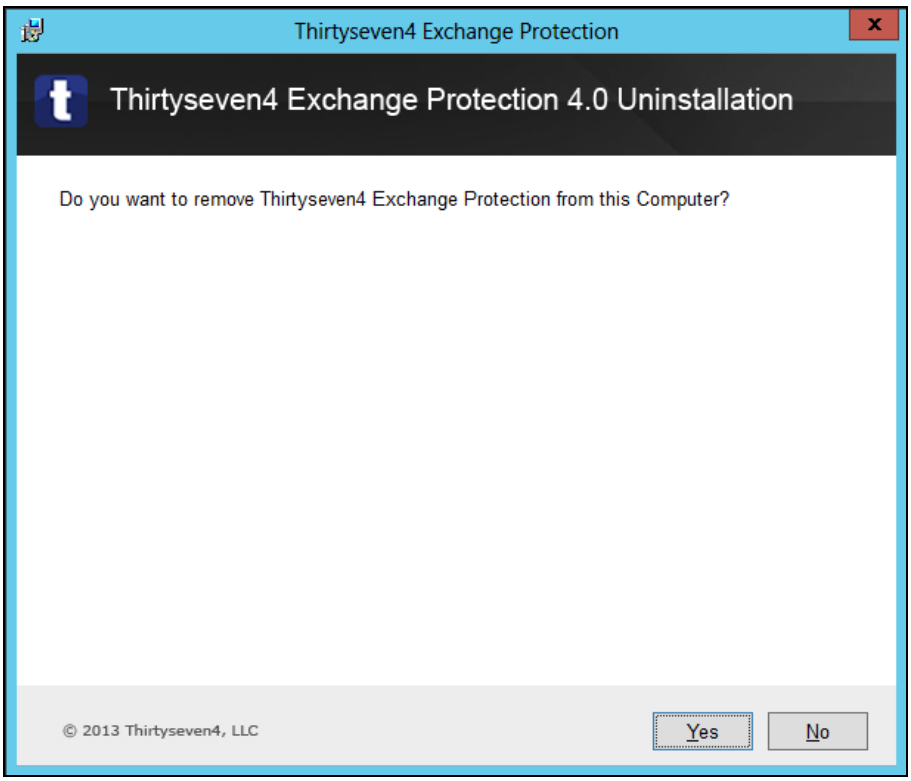
To remove Thirtyseven4 Exchange Protection 4.0, follow these steps:

1. Select **Start > Programs > Thirtyseven4 Exchange Protection 4.0 > Uninstall Thirtyseven4 Exchange Protection 4.0**.

   Alternatively, you can select **Start > Programs > Control Panel > Add or Remove Programs > Thirtyseven4 Exchange Protection**.

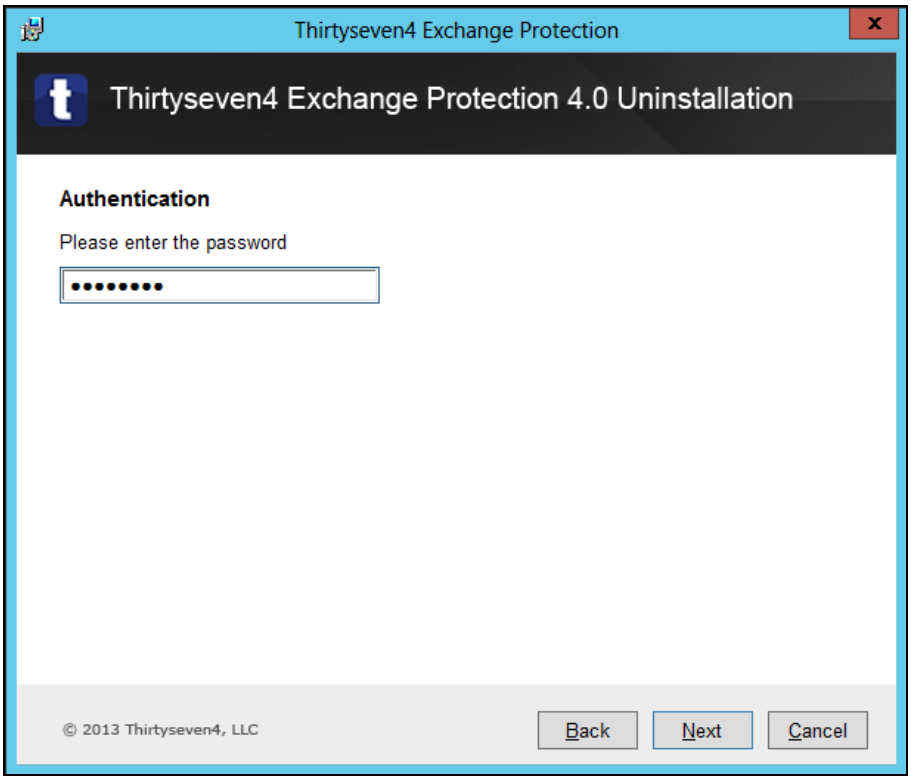
   The path **Start > Programs > Thirtyseven4 Exchange Protection 4.0** is available only if Complete Thirtyseven4 Exchange Protection 4.0 or Manager Console is installed on your computer and not other components.

The confirmation screen appears.



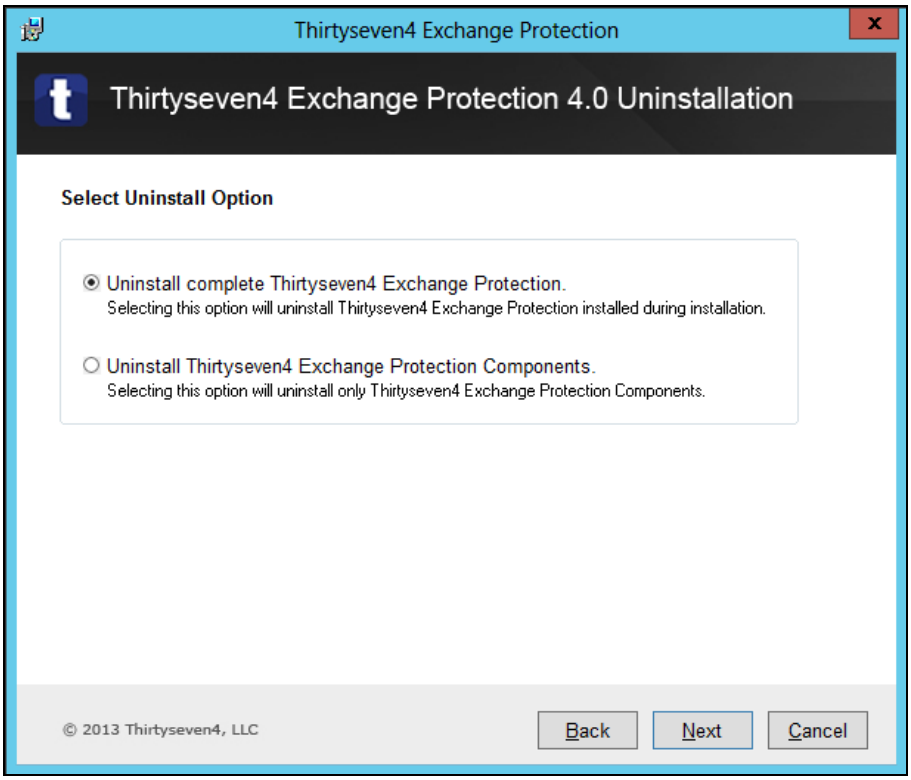
2. Click **Yes** to continue with the uninstallation.

   The Authentication screen appears.



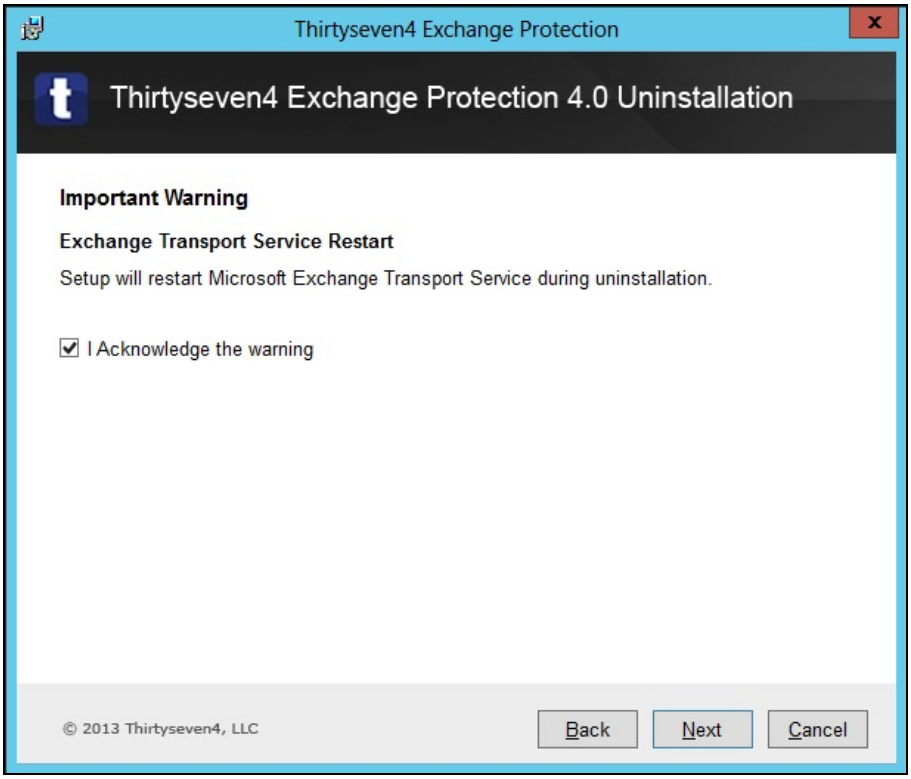
3. Provide your credentials, and then click **Next**.

   The Select Uninstall Option screen appears displaying the options for the components installed on your computer.



Note: In this uninstallation example, the Uninstall complete Thirtyseven4 Exchange Protection option is selected that is also a default selection. Screen displays for other application types are similar with minor variance.

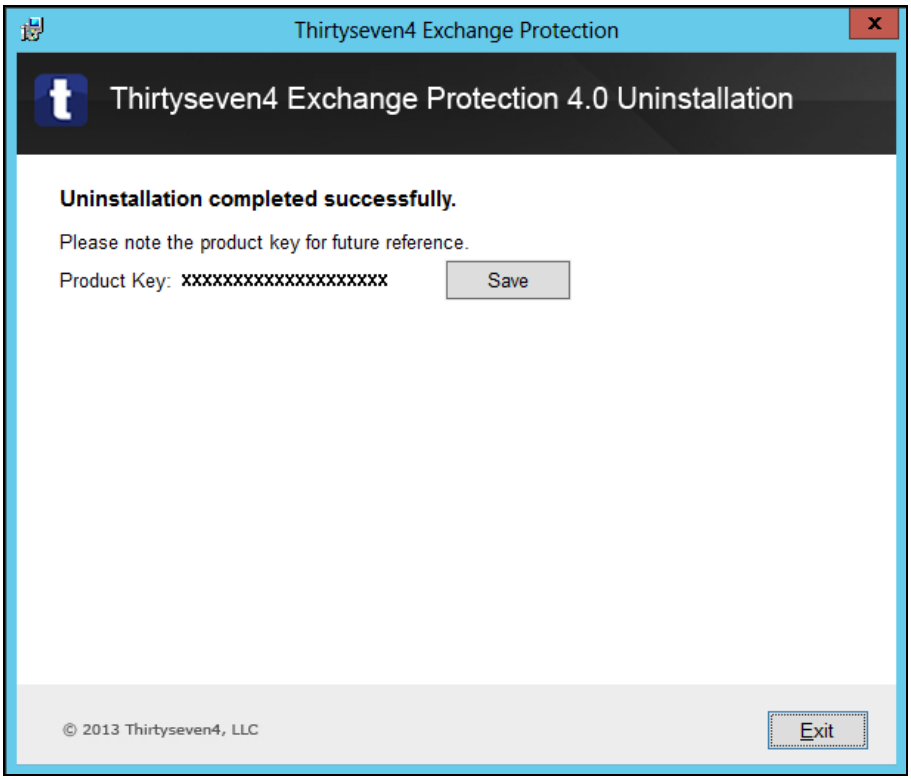
4. Select the component of Thirtyseven4 Exchange Protection that you want to remove, and then click **Next**.



The Important Warnings screen appears which displays the message that Microsoft Exchange Transport Service will restart during uninstallation (only if the TSEP Mailbox or Edge components are being uninstalled).

5. Select the **I Acknowledge the warnings** check box, and then click **Next**.

   *Uninstallation starts. When uninstallation is complete, a message is displayed. If Complete Thirtyseven4 Exchange Protection is uninstalled, then the product key is also displayed so that you can note down or save the key by clicking the **Save** button for future reference.*



6. To close the wizard, click **Exit**.

Chapter 2.

Settings

With Settings, you can configure settings for various features such as virus scan, AntiSpam, content filtering, store scan, schedule scan, notifications and so on.

Virus Scan

With Virus Scan you can configure scan settings for Transport Scan and Edge Transport Scan.

Transport Scan: The emails and attachments are scanned in transit at Transport Scan.

Edge Transport Scan: The emails and attachments are scanned in transit at Edge Transport Scan.

Configuring Transport Scan

With Transport Scan, you can configure the Virus Scanning feature for emails and attachments at Transport scan.

To configure Transport Scan, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Virus Scan** tab.
3. On the Virus Scan screen, click the **Transport Scan** tab.
4. Select the **Enable Transport Scan** check box if you want to scan your emails and attachments at Transport.

   The Settings details are activated.
5. Select either or both of the following:
   - Scan with DNAScan Technology
   - Scan archive files
6. Select the scan level for the **Archive Scan Level** option. Also, select the types of archives that are to be scanned from the archives list.

   You can set the scan level up to 5. However the default level is set to 2.
7. Select the **Exclude Extension** check box to enter the file extensions that you want to exclude from being scanned. Then enter the file extensions manually in the list. This is helpful when you are sure not to scan certain file extensions.

8. Select the **Attach disclaimer to outbound mails** check box if you want to attach the disclaimer to all outbound emails. You can write your disclaimer as per your company's policies. However, a disclaimer message is displayed by default.
9. Under **Action on Virus Found**, select one of the actions to be taken when a virus is found in the email or attachments from the following:
    - Repair, replace with virus information if unsuccessful
    - Repair, delete entire mail if unsuccessful
    - Repair, quarantine entire mail if unsuccessful
    - Delete entire mail
    - Quarantine entire mail
10. To save your settings, click **Save**. You can revert to the default setting whenever you prefer by clicking the **Default** button.

Scan with DNAScan Technology

DNAScan is an indigenous technology of Thirtyseven4 that is used to detect and eliminate new and unknown malicious threats. DNAScan technology successfully traps suspected files with very less false alarms.

Scan archive files

With **Scan archive files**, you can scan archive files. You can scan files of various archive file types that are listed in the **Select type of archives to be scanned** list.

Archive Scan level

With Archive Scan Level, you can scan the archive files till five levels deep inside the archive files so to ensure no files are left out from being scanned. The default scanning is set to level 2. You may increase the archive scan level which may though affect the scanning speed. However, password protected files are not scanned.

Configuring Edge Transport Scan

With Edge Transport Scan, you can configure the Virus Scanning feature for emails and attachments at edge transport scan.

To configure Edge Transport Scan, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Virus Scan** tab.
3. On the Virus Scan screen, click the **Edge Transport Scan** tab.

4. Select the **Edge Transport Scan** check box if you want to scan your emails and attachments at edge transport scan.

   The Settings details are activated.

5. Select either or both of the following:
   - Scan with DNAScan Technology
   - Scan archive files
6. Select the **Exclude Extension** check box to enter the file extensions that you want to exclude from being scanned. Then enter the file extensions manually in the list. This is helpful when you are sure not to scan certain file extensions.
7. Select the **Attach disclaimer to outbound mails** check box if you want to attach the disclaimer to all outbound emails. You can write your disclaimer as per your company's policies.
8. Select an action to be taken under **Action on Virus Found**, when a virus is found in the email or attachments.
9. To save your settings, click **Save**. You can revert to the default setting whenever you prefer by clicking the **Default** button.

Note:

- The TSEP Transport Agent on Edge gets lowest priority by default due to which the following problems may occur:
  - If Microsoft **Attachment Filtering Agent** has higher priority than the TSEP transport agent, the emails having attachments get filtered by Attachment filtering agent and may not be passed to the TSEP Virus Scan engine for scanning.
  - If Microsoft **Content Filtering Agent** has higher priority than the TSEP transport agent, the emails may not be passed to the TSEP cloud-based AntiSpam engine for verification.

    To get rid of the above problems, it is recommended that you should set the priority of the TSEP scan agent to 4 on Edge server using the following power shell command.

    - Open the "Exchange Management shell" on Edge server.
    - Execute the command:

      "Set-Transport agent – identity "ExchgProtEdgeScanAgent" – priority 4"

      Exit the Exchange Management shell and restart the Microsoft Exchange Transport service.

- On Mailbox Server if Malware Agent is installed then mails will not be scanned by TSEP Transport agent.

  To get rid of this problem use following powershell commands

  - Open the “Exchange Management shell” on Mailbox Server.
  - Execute the command: “Get-TransportAgent”
  - If in results it shows “Malware Agent” then execute following command
  - Disable-TransportAgent -identity “Malware Agent”

More on Virus Scan (AVStamp)

TSEP comes with additional feature that is AVStamp. Because of AVStamp, the emails that are once scanned are not scanned again by any other TSEP component having the same virus database date and thus helps you utilize the optimum system resources.

If two systems have different virus database dates, the emails scanned at the component having previous database date will be scanned again at the component having later database date but the vice versa is not carried out.

AntiSpam

With AntiSpam, you can set protection rules for spams, so that all spam emails are filtered and your mailbox is protected. However, only inbound and outbound emails are scanned for spam using cloud-based service, while internal emails are not scanned for spam.

Configuring AntiSpam

To configure AntiSpam, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **AntiSpam** tab.
3. Select the **Enable Spam Protection** check box.

   The Setting details for spam protection are activated.
4. Under **Spam Protection Level**, select one of the spam protection levels:
   - Low
   - Moderate
   - High

5. Select the **Enable Black List** check box to activate the black list. If you activate Black List, you should add email IDs or domains so that the AntiSpam protection rule is implemented on the domains listed in the Black List.
6. Select the **Enable White List** check box to activate the white list. If you activate White List, you should add email IDs or domains so that the AntiSpam protection rule is not implemented on the domains listed in the White List.

Note: Make sure that you do not enter the same email ID in both Black List and White List.

7. Select one of the following messages to scan for spam:
   - Scan inbound mails for spam
   - Scan inbound and outbound mails for spam
8. Select an action to be taken if virus is found under **Action on Spam Mail** from the following:
   - Delete
   - Quarantine
   - Tag Subject and Deliver
9. Enter the tag in the **Tag Subject with Text** text box. Tag Subject with Text is enabled only if you select Tag Subject and Deliver under **Action on Spam Mail**.
10. To save your settings, click **Save**.

Content Filtering

With Content Filtering, you can create and manage content filtering criteria that help you filter both inbound and outbound email communications. You can filter messages based on all or any combinations of the following factors:

- file types and file names
- keywords in subject line
- word or phrases in the message body
- sender or senders domain

Configuring Content Filtering

To configure Content Filtering, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Content Filtering** tab.

   A list of filters is displayed (if you have added any).
3. Click **Add** to add a new filtering criterion.
4. In the **Name** text box, type a filter name.
5. Select the **Enable Filter** check box.

   The Setting details for filter are activated.
6. Set any of the following: File Type and File Name, Keywords in subject line, Words or Phrases in message body, Sender or Senders Domain, Exclusion.
7. Under **Apply this filter at**, select any of the following filter types check boxes:
   - Store Scan
   - Schedule Scan
   - Edge Transport Scan
   - Transport Scan
8. Select one of the following filtering criteria, under **Filter messages if**:
   - All filtering criteria meet: messages will be filtered only if all filtering criteria from File Type and File Name, keywords in subject line and Words or Phrases in message body meet.
   - Any of the filtering criteria meet: messages will be filtered if any one of filtering criteria from File Type and File Name, keywords in subject line and Words or Phrases in message body meet.
9. Select one of the options for **Action to be taken if content filtering rule matches** from the following:
   - Replace with policy breach information
   - Delete
   - Quarantine
10. To save your settings, click **Save**.

Various Conditions for Filtering Content

TSEP provides various conditions for filtering content for all internal, inbound, and outbound emails so to filter the emails for better security.

File Type and File Name

With File Type and File Name, you can set the file types and file names that you do not want to receive through emails. This is helpful when you are sure you do not want certain file types or file names.

You can apply filtering criteria in the following ways:

1. Click the **File Type and File Name** tab.
2. Under **Select File Types**, select file types.

   To select file type, expand the file type node, all the file types are displayed.
3. In the **Enter File Extension** list, enter file extensions.

   This is helpful when you want to block a file type and it is not available in the list.
4. Enter file name in the File Name.

   This is helpful when you want to block a certain file name. .

Keywords in subject line

With Keywords in subject line, you can add keywords for the subject line so all internal, inbound, and outbound emails are filtered for such keywords. If such keywords are found in the email subject lines, they are blocked. This is helpful when you find emails with certain keywords that are either useless or you do not intend to receive, such as Lottery Winning Notice, Bumper Prize Offer or so.

You can apply filtering criteria in the following ways:

1. Click the **Keywords in subject line** tab.
2. In the **Enter Keywords** text box, type the keywords for filtering content.
3. Click **Add** to enter the keywords in the list.

Words or Phrases in message body

With Words or Phrases in message body, you can add words or phrases for the body messages so all internal, inbound, and outbound emails are filtered for such words and phrases. If such words or phrases are found in the email body , they are blocked. This is helpful when you find emails with certain words or phrases that are either useless or you do not intend to receive, such as Lottery Winning Notice, Bumper Prize Offer, Your Bank Details, Update Your Account Details or so.

You can apply filtering criteria in the following ways:

1. Click the **Words or Phrases message body** tab.
2. In the **Enter Word or Phrases** text box, type words or phrases for filtering content.
3. Click **Add** to enter the words or phrases in the list.

Sender or Sender's Domain

With Sender or Sender's Domain, you can apply the content filtering rule on the emails to be received from a particular sender or sender's domain. The filter criteria apply only on the configured sender or sender's domain while there is no impact on the other senders or domains. You can apply the filtering criteria in the following ways:

You can apply the filtering criteria in the following ways:

1. Click the **Sender or Sender's Domain** tab.
2. In the **Enter Sender's Email ID or Domain** text box, type the sender's email ID or domain for filtering content.
3. Click **Add** to enter the email IDs or domains in the list.

Note: Domain can be added in the format: *@abc.com

Exclusion

With Exclusion, you have the option to exclude particular recipients from the filtering rule. The filter criteria are not applied on the email IDs that are listed in the Exclusion list.

You can apply the filtering criteria in the following ways:

1. Click the **Exclusion** tab.
2. In the **Enter Recipients Email IDs**, type the recipients email IDs for filtering content.
3. Click **Add** to enter the email IDs in the list.

Note: Edge Transport Scan involves scanning of inbound and outbound emails. While Transport Scan involves scanning of inbound, outbound, and internal emails.

More on Content Filtering Scanning Flow

The following is the sequence in which the content filtering engine filters and validates the email content.

- Sender domain – The filter criteria check the sender/domain first in the one-to-many format that is one sender to a list of senders. The filter criteria apply if the sender is configured in the restriction.
- Exclusion List – The filter criteria check all the recipients with the excluded IDs in the many-to-many format. If all the recipients are enlisted in the Exclusion List, the filtering criteria do not apply. If some or none recipients are found excluded, the filter criteria apply
- Subject Line – The filtering criteria check for the keywords in the subject line of the emails.
- Message body – The filtering criteria check for the keywords in the message body.
- Custom File Names and Extensions – The filtering criteria check if the attachments have certain file names/extensions that match with the file names/extensions enlisted in the Custom File Names and Extensions category.

Schedule Scan

With Schedule Scan, you can define when to begin scanning of your mailbox and public folder automatically. You can schedule multiple number of scan schedules so that you can initiate scanning of your mailbox and public folder at the time convenient to you. This supplements other automatic protection features to ensure that your mailbox remains virus free.

You can set schedule frequency that additionally refines your request to schedule scanning on certain days. Further you can also schedule the task to repeat at specific intervals.

Configuring Schedule Scan

To configure Schedule Scan, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Schedule Scan** tab.
3. Click **New** to go to the Configure Schedule Scan screen.
4. In the **Name** text box, enter a schedule name.
5. Select the **Enable Schedule** check box.

   Setting details for schedule scan are activated.

6. Set Scan Frequency from the following:
   - Daily: Select the Daily option if you want to initiate scanning of your mailbox daily.
   - Weekly: Select the Weekly option if you want to initiate scanning of your mailbox on a certain day of the week. When you select the Weekly option, the Day drop-down list is activated where you can select a day of the week.
   - Monthly: Select the Monthly option if you want to initiate scanning of your mailbox on a certain day of the month. When you select the Monthly option, the Day drop-down list is activated where you can select a day of the month.
7. Set scan time and scan priority under **Start At**.
8. Set scan occurrence under **Repeat Scan**. Enter how often the scanning should be started.
9. Select any of the following **Message Settings**:
   - Select the **Scan messages from last days** check box and set the number of days.
   - Select the Scan messages having attachments only check box.
   - Select the Scan unscanned messages only check box.
10. Select the mail stores on which you want to apply the schedule scan under **Mailbox Stores** using either of the following scan options:
    - **Entire Scan**: Helps you scan the mailbox stores and/or public folders of all the servers. This scan may take time and may also slows down the system considerably.
    - **Custom Scan**: Helps you customize your scanning option for particular mailboxes and/or public folders.. This takes less time. If you select Custom Scan, some additional settings appear that are as follows:
      - Under **Select Sever**, select a server whose mailboxes and/or public folders you want to scan.
      - Under **Scan Options**, you can include or exclude mailbox stores and/or public folders for scanning:
        - If you want to scan only the selected mailbox stores or public folders, select **Scan selected mailbox stores**.
        - If you want to exclude some mailbox stores or public folders from being scanned, select **Scan all mailbox stores except the excluded mailbox stores**.
      - Enter the name of a mailbox store or a public folder and then click **Add** to add it in the respective list.

11. To save your settings, click **Save**.
12. Click **Settings**.

    Clicking Settings redirects you to configuring Virus Scan for further settings.

Note: Please note that if you create public folders in Exchange Server after the installation of Thirtyseven4 Exchange Protection, such folders cannot be scanned though they appear in Mailbox Stores list of Store Scan and Schedule Scan.

To scan such folders successfully, you have to follow these steps:

1. Open command prompt.
2. Go to the installation directory of Thirtyseven4 Exchange Protection.
3. Execute “userutil.exe” with parameter -p

Example for command:

```
C:\Program Files\Thirtyseven4\Exchange Protection> userutil.exe -p
```

Notification

With Notification, you can manage notifications to be sent on occurrence of certain events. You can set notification rules for various activities.

TSEP sends notification in the following ways:

- TSEP Complete/Console installed on Mailbox/Edge Component: Detects the Exchange SMTP Host settings and delivers the notification to the configured Email IDs. If you want to send notification through any third party SMTP host, you may configure an SMTP host. The notification will be sent through the third party SMTP host henceforth.
- TSEP Complete/Console installed on Domain machine or Client Access machine: The notification is sent through the third party SMTP host, which may be Exchange SMTP host or any third party host. In case any third party SMTP host is not configured it detects the IIS Virtual SMTP Host settings to deliver the notification to the configured Email IDs.

Configuring Notification

To configure Notification, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Notification** tab.

3. Select the **Enable SMTP Host** check box, if you want to send notification emails through other SMTP Host.

   The Configure button is activated. However, this is not a mandatory option.

   Configure any of the following: Virus Scan, Virus Outbreak, Content Filtering, System Messages, Consolidated Notification.

4. To save your settings, click **Save**.

Configuring SMTP

If you have hosted a different SMTP on your machine, follow the procedures for configuring the SMTP host of your system.

To configure SMTP, follow these steps:

1. On the Notification page, select the **Enable SMTP Host** check box.

   The Configure button is activated.

2. Click **Configure**.

   The Configure SMTP Host screen appears.

3. Enter Server, Port, and login credentials (if applicable) in relevant fields, and then click **Save** to save your settings.

   Server and port are mandatory fields.

Note: While configuring SMTP Virtual Server, make sure that the port number assigned to. SMTP Virtual Server is not used by any other application or component.

To know about how to configure SMTP Server, see Configuring SMTP Server, p - 39.

Configuring Virus Scan

With Virus Scan, you can configure notifications to be sent on detection of virus incident.

1. On the Notification page, click the **Virus Scan** tab.
2. Select the **Enable Notifications for Virus Scan** check box, if you want to receive notification when a virus is detected.

   Notification message details are activated.

3. Type the subject and the message for the notification.
4. In the **Notification From Email Address** text box, enter an email address to get notification from.

5. In the **Notify Administrator** list, enter email addresses.

   Here you can enter multiple email addresses. However, separate the multiple email IDs by semicolon.

6. Select an appropriate option for whether the notification email is to be sent to internal or external sender or recipient from **Notify Senders**, and **Notify Recipients** check boxes respectively.

Configuring Virus Outbreak

With Virus Outbreak, you can configure notifications to be sent on virus outbreak.

1. On the Notification page, click the **Virus Outbreak** tab.
2. Select the **Trigger Virus outbreak if** check box, if you want to receive notification when there is a virus outbreak.

   Notification message details are activated.

3. Set number of virus incidents detected in a certain span of time.

   This helps you set the criticality of virus incidents for outbreak.

4. Type the subject and the message for the notification.
5. Enter an email address to get notification from in the **Notification From Email Address** text box.
6. Enter email addresses in the **Notify Administrator** list.

   Here you can enter multiple email addresses. However, separate the multiple email IDs by semicolon.

Configuring Content Filtering

With Content Filtering, you can configure notifications to be sent on violation of content filtering rules.

1. On the Notification page, click the **Content Filtering** tab.
2. Select the **Enable Notifications for Content Filtering** check box, if you want to receive notification when there is a violation of content filtering rules.

   Notification message details are activated.

3. Type the subject and the message for the notification.
4. In the **Notification From Email Address** text box, enter an email address to get notification from.
5. Enter email addresses in the **Notify Administrator** list.

   Here you can enter multiple email addresses. However, separate the multiple email IDs by semicolon.

6. Select an appropriate option for whether the notification email is to be sent to internal or external sender or recipient from **Notify Senders**, and **Notify Recipients** check boxes respectively.

Configuring System Messages

With System Messages, you can configure notifications to be sent for system events such as license is getting expired, password is changed, and update notification and so on.

1. On the Notification page, click the **System Messages** tab.
2. Select the **Enable System Notification** check box, if you want to receive notification when you need messages for any updates.

   Notification message details are activated.
3. Select the events for which you want to receive notifications.
4. In the **Notification From Email Address** text box, enter an email address to get notification from.
5. Enter email addresses in the **Notify Administrator** list.

   Here you can enter multiple email addresses. However, separate the multiple email IDs by semicolon.

Configuring Consolidated Notification

With Consolidated Notification, you can configure consolidated notification to be sent of the entire day. This notification contains a summary of all exchange protection activities of past 24 hours.

1. On the Notification page, click the **Consolidated Notification** tab.
2. Select the **Enable consolidated notification** check box, if you want to receive a consolidated notification.

   Notification message details are activated.
3. Set time of the day when you want to receive the consolidated notification.
4. Type the subject and the message for the notification.
5. In the **Notification From Email Address** text box, enter an email address to get notification from.
6. Enter email addresses in the **Notify Administrator** list.

   Here you can enter multiple email addresses. However, separate the multiple emails by semicolon.

Configuring SMTP Server

Simple Mail Transfer Protocol (SMTP) is an Internet-based one-to-many mail communication system through Transmission Control Protocol/Internet Protocol (TCP/IP) networks using port 25. SMTP may be used both for sending and receiving mails using email servers and email transfer agents. However, the client mail applications use SMTP only to relay messages, while to receive messages they use either the Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP4) or a proprietary system such as Microsoft Exchange.

For more details about SMTP server, see Post Installation Task in "Chapter 1: Getting Started", p - 16.

To configure SMTP Virtual Server, follow these steps:

1. Select **Start > Control Panel**.
2. Double-click the **Add or Remove Programs** option.

   The Add or Remove Programs dialogue appears.
3. In the left pane, click the **Add/Remove Windows Components** option.

   The Windows Components Wizard dialogue appears.
4. In the Components list, click **Application Server**, and then click **Details**.

   The Internet Information Services dialogue appears.
5. In the Subcomponents of Application Server list, click **Internet Information Services (IIS)**, and then click **Details**.
6. In the Subcomponents of Internet Information Services (IIS) list, select the **SMTP Service** check box, and then click **OK**.
7. Click **Next**.

   A prompt may appear for the Windows Server 2003 family CD or the network path for installation.
8. Click **Finish**.

Note:

Upon successful installation of the SMTP service, a default configuration setting of SMTP server is created, along with a message storage folder in ***LocalDrive*:\Inetpub\Mailroot**.

If you set up the SMTP service for the first time, you may need to configure global settings for a SMTP virtual server and for individual components of the virtual server.

To configure global SMTP settings, follow these steps:

1. Go to IIS Manager and expand the local computer. Right-click the **Default SMTP Virtual Server** option and then click **Properties**.
2. On the property pages, make changes in the default settings as per your requirement.

To configure SMTP virtual server components settings, follow these steps:

1. Go to IIS Manager and expand the local computer. Expand the **Default SMTP Virtual Server** option and then right-click the component that you want to configure.
2. Click **Properties**.
3. On the property pages, make changes in the default settings as per your requirement.

Automatic Update

With Automatic Update, you can set rules to receive updates automatically.

Configuring Automatic Update

To configure Automatic Update, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Automatic Update** tab.
3. Select the server and click the **Edit** button to change automatic update settings.

   The Automatic Update configuration screen appears.
4. Under Settings, select the **Enable Automatic Update** check box.
5. If Enable Automatic Update option is selected, the Node server will download the updates from the selected update mode automatically whenever the new updates are available on update server. Select one of the Update Mode options to get the updates.

   Download from Thirtyseven4 Exchange Management Console: Helps to update the node server from Thirtyseven4 Management Console.

   Download from Internet: Helps to update the node server from Internet (Thirtyseven4 Update Server). For this, your system should be connected to the Internet.
6. To save your setting, click **Save**.

Quarantine

With Quarantine, you can configure quarantine settings. Quarantine is a folder where suspicious files are placed so that your mailbox is clean and protected.

Configuring Quarantine

To configure Quarantine, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Quarantine** tab.
3. Click the **Edit** button to change the quarantine settings.

   The Quarantine setting screen appears.
4. Set the maximum size limit of the quarantine folder.

   By default Maximum Quarantine disk space is set to 5% of free disk space available before installation.
4. Set the number of days when the files placed in the quarantine folder should be removed.
5. Give the path where the files should be quarantined.

   The default path is displayed which you can change if required.
6. To save your setting, click **Save**.

Reports

With Reports, you can configure report settings and define when the reports should be removed.

Configuring Reports

To configure Reports, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Reports** tab.
3. Set the number of days when the reports should be removed.
4. To save your setting, click **Save**.

Logs

With Logs, you can configure log settings and define when the logs should be removed.

Configuring Logs

To configure Logs, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Settings**.
2. Click the **Logs** tab.
3. Set the criticality level of the log.
4. Set the number of days when the Logs and Event logs should be deleted.
5. To save your setting, click **Save**.

Note: Logs and Event logs are two different entities.

Chapter 3. Store Scan

With Store Scan, you can configure rules for scanning mailbox stores for Viruses and Content Filtering Policy breaches.

Store Scan

With Store Scan, also known as mailbox scan or on-demand scan, you can configure rules for scanning mailbox stores for Viruses and Content Filtering Policy breaches. The settings configured for Content Filtering for scanning is also applied during Store Scan. This helps you initiate the scanning of mailboxes and public folders manually when required.

Note: After installing TSEP on the mailbox server, a user with special permissions is created in Active Directory by default that is used to perform Store Scan.

Configuring Store Scan

To configure Store Scan, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Store Scan**.
2. Select any of the following **Message Settings** options:
   - Scan messages from last…days
   - Scan messages having attachments only
   - Scan unscanned messages only
3. Select one of the scanning options from the following:
   - Entire Scan: To scan the mailbox stores and/or public folders on all the servers.
   - Custom Scan: To scan only selected mailbox stores and/or public folders.
4. Under **Mailbox Stores**, select the mailbox stores on which you want to apply the rules for scanning.

   If you select the parent mailbox store, all the child mailbox stores are selected.
5. Click **Scan** to begin scanning.

   *You can stop the scanning process when you prefer so by clicking **Stop Scan**.*
6. Click **Settings** to proceed to further settings for Store Scan.

   The Store Scan Settings screen appears. You can configure settings for Store Scan.

Entire Scan

With Entire Scan, you can scan the mailbox stores and/or public folders of all the servers. This scan may take time and slow down the system considerably.

Custom Scan

With Custom Scan you can customize your scanning for particular mailboxes and/or public folders.

This takes less time. If you select Custom Scan, some additional settings appear that are as follows:

1. Under **Select Sever**, select a server whose mailboxes and/or public folders you want to scan..
2. Under **Scan Options**, you can include or exclude mailbox stores and/or public folders for scanning:
    - If you want to scan only the selected mailbox stores and/or public folders , select **Scan selected mailbox stores**.
    - If you want to exclude some mailbox stores and/or public folders from being scanned, select **Scan all mailbox stores except the excluded mailbox stores**.
3. Enter the name of a mailbox store and/or a public folder and then click **Add** to add it in the respective list .
4. To begin scanning, click **Scan**.

Store Scan Settings

With Store Scan Settings, you can configure further settings about how to scan and what files should be scanned.

To configure Store Scan Settings, follow these steps:

1. On the Store Scan page, click the **Settings** button.

    The Store Scan Settings page appears.
2. Select either or both of the following:
    - Scan with DNAScan Technology
    - Scan archive files
3. Select the archive scan level till which you want to scan the mailbox.

    You can set up to level 5 while the default level is set to 2.
4. From the archive files list, select the archive file types to scan.
5. Select the **Exclude Extension** check box to enter file types that you want to exclude from being scanned. Then enter file extensions manually in the list. This is helpful when you are sure not to scan certain file extensions.

6. Under **Action on Virus Found**, select an action to be taken when virus is found. The actions that you take include the following:
    - Repair, replace with virus information if unsuccessful
    - Repair, delete entire mail if unsuccessful
    - Repair, quarantine entire mail if unsuccessful
    - Delete entire mail
    - Quarantine entire mail
7. To save your settings, click **Save**.

Note: Please note that if you create public folders in Exchange Server after the installation of Thirtyseven4 Exchange Protection, such folders cannot be scanned though they appear in Mailbox Stores list of Store Scan and Schedule Scan.

To scan such folders successfully, you have to follow these steps:

5. Open command prompt.
6. Go to the installation directory of Thirtyseven4 Exchange Protection.
7. Execute “userutil.exe” with parameter -p

Example for command:

```
C:\Program Files\Thirtyseven4\Exchange Protection> userutil.exe -p
```

Chapter 4.

Admin

With Admin, you can administer various activities such as quarantine files, event logs, you can import and export settings, and so on.

Quarantine

With Quarantine, you can view and manage quarantine files.

Viewing Quarantine

To view Quarantine, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Quarantine** tab.
3. Select your search criteria under **Search Quarantined Items**.
4. Click **Search** to search the quarantined items as per your search criteria.

   You can view the details of a quarantined item and remove it as per your requirement.

   You can also send a quarantined item to either the recipients and/or anyone you prefer.
5. Select a quarantined item, and then click **View Details** to see the details.
6. Select a quarantined item, and then click **Delete** to remove the item.
7. Select a quarantined item, and then click **Deliver**.

   Clicking Deliver redirects you to the Deliver Messages screen.
8. Select the **Deliver messages to its original recipients** check box, if you want to send messages to the recipients.
9. Select the **Deliver messages to following Email IDs** check box and then enter the email addresses in the list.
10. Click **Deliver** to send the messages.

Event Log

With Event Log, you can view and manage all the event logs.

Viewing Event Logs

To view Event Logs, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Event Log** tab.

   The Event Log list is displayed.

   You can delete all the event logs or export them for future reference. While exporting, the events are downloaded at the Downloads folder on your system.

Update

With Update, you can manage the Update Manager and node servers. The Update Manager downloads the updates from Thirtyseven4 Update Server and saves it to the central location. Other servers managed under this Management Console can pick the updates instead of downloading from the Internet.

Configuring Update Manager

To configure Update Manager, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Update** tab.
3. Click the **Update Manager** tab.
4. Select the **Enable Automatic Update** check box, if you want to pick up the updates automatically whenever the updates are available on Thirtyseven4 Update Server.
5. Select the **Take backup of old updates before downloading new update** check box, if you want to have a backup of previous updates before taking new updates.
6. Click **Update Now** to download the updates immediately.
7. To save your setting, click **Save**.
8. Click the **Rollback** button to revert to the previous state of updates.

Note: The Update Manager can also be configured following the same process through Thirtyseven4 Update Manager. (Start > Programs > Thirtyseven4 Exchange Protection 4.0 > Update Manager).

With Update Now, you can update the servers immediately to the latest virus definition. To configure Update Now, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Update** tab.
3. Click the **Update Now** tab.
4. Select the server name from where you want to take the updates.
5. To update immediately, click **Update Now**.

Export

With Export, you can export various settings so you can import the settings later. This is helpful when you want to remove Thirtyseven4 Exchange Protection for a time. Once you reinstall the application, you can simply import the settings and the application will start working with all previous settings.

Exporting Settings

To export Settings, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Export** tab.
3. Select the settings to export.
4. Click **Export** to export the settings.

   The settings are exported in .xml format.

   *The exported file (**ExportSettingsXml**) is saved at the following path: **Thirtyseven4 > Exchange Protection > Web > ExportSettingsXml.** It is also saved at the Downloads location of your system.. You can import the settings from the same path later if required.*

Import

With Import, you can import the settings that you might have exported. Once you import the settings, they will be applied to all the features. However you can change the settings as you require.

Importing Settings

To import Settings, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Import** tab.

3. Click **Browse** to select the file that you want to import.
4. Click **Next** to go to the Import Settings details screen.
5. Select the settings that you want to import.
6. Click **Import**.

   The selected settings are imported successfully.

Internal Domains

With Internal Domains, you can configure internal domains. The domain names that you configure here will be used to identify internal mails.

Configuring Internal Domains

To configure Internal Domains, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Internal Domains** tab.
3. Enter the domain name in Internal Domains list, and then click **Add**.

   However, the current domain on which Microsoft Exchange is installed, is added in the internal domain list by default.
4. Click **Save** to save your setting.

Change Password

With Change Password, you can change your password whenever you require so.

Changing Password

To change Password, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Change Password** tab.
3. Enter your existing password in the **Enter Old Password** text box.
4. Enter your new password in the **Enter New Password** text box.
5. Enter your new password in the **Confirm New Password** text box.
6. Click **Save** to save your setting.

Internet

With Internet, you can configure Internet settings in case you want to use proxy server.

Configuring Internet

To configure Internet, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Admin**.
2. Click the **Internet** tab.
3. Select the **Enable proxy settings** check box.
4. Enter the server, port, and user credentials in relevant fields.
5. Click **Save** to save your setting.

   The Internet setting is applied to AntiSpam, Update, and License. If the Internet setting is configured in the application, it uses the Internet settings configured in the application and if the Internet setting is not configured, it uses direct connection if available.

Chapter 5.

Reports

With Reports, you can generate reports for various activities such as virus scan, AntiSpam, content filtering, updates, and delete reports that are not required. The reports can be displayed both in tabular and line chart formats. Reports for tabular format can be generated for any duration while those for the line chart the reports can be generated for the duration of 45 days only.

Virus Scan

With Virus Scan, you can generate reports on virus scanning.

Generating Reports on Virus Scan

To generate reports on Virus Scan, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Reports**.
2. Click the **Virus Scan** tab.
3. Select the start and end dates.
4. Select the level, messages, and report type.
5. Click **Generate** to generate report.

Scan Level: Includes Transport Scan, Edge Transport Scan, Store Scan, and Schedule Scan.

Messages: Includes Inbound, Outbound, Internal, and Store.

Report Type: Includes Line Chart and Tabular.

AntiSpam

With AntiSpam, you can generate reports on AntiSpam.

Generating Reports on AntiSpam

To generate reports on AntiSpam, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Reports**.
2. Click the **AntiSpam** tab.
3. Select the start and end dates.

4. Select the level, messages, and report type.
5. Click **Generate** to generate report.

Content Filtering

With Content Filtering, you can generate reports on Content Filtering.

Generating Reports on Content Filtering

To generate reports on Content Filtering, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Reports**.
2. Click the **Content Filtering** tab.
3. Select the start and end dates.
4. Select the level, messages, and report type.
5. Click **Generate** to generate report.

Update

With Update, you can generate reports on Update.

Generating Reports on Update

To generate reports on Update, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Reports**.
2. Click the **Update** tab.
3. Select the start and end dates.
4. Select the option to generate report for, and server names.
5. Click **Generate** to generate report.
6. Click **View Details** to view the details of a report.
7. Click **Export** if you want to export the generated reports.

Report for: Includes Automatic Update.

Managed Server Name: Includes all the managed server names.

Delete Reports

With Delete Reports, you can manage how you want to delete the reports. You can delete the reports both automatically and manually.

Deleting Reports

To delete reports, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **Reports**.
2. Click the **Delete Reports** tab.
3. Select the number of days to delete reports automatically.
4. Select the reports under **Select Reports** that you want to delete manually.
5. Click **Delete** to delete the reports.

Chapter 6.

License

With License, you can check the product license status, add new user license, renew your license, update license information, and fill the license order form.

Status

With Status, you can check the current license status.

Viewing License Status

To view the status of your license, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **License**.
2. Click the **Status** tab.

   The License Manager screen appears displaying the license information.

License Addition

With License Addition, you can add new mailbox license.

Adding License

To add a new mailbox license, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **License**.
2. Click the **License Addition** tab.
3. Enter the additional mailbox license key to support more number of mailbox in your license in the **Additional Key** text box.
4. Click **Submit** to submit the additional license key.

License Renewal

With License Renewal, you can renew your license anytime after activation till four months after the expiry of your current license.

Renewing Your License

To renew your license, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **License**.
2. Click the **License Renewal** tab.
3. Enter renewal key to renew your license in the **Renewal Key** text box.
4. Click **Submit** to submit the renewal key.

License Sync

With License Sync, you can update the license information. Whenever there is any change in License Information such as Expiry Date is changed in case of direct renewal done by a vendor, you can update the License Information as per Thirtyseven4 License Server manually.

Updating License Information

To update license information, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **License**.
2. Click the **License Sync** tab.
3. Click **Update License Information**.

   Your license is updated.

License Order Form

With License Order Form, you can place order for additional license, or can renew your existing license through email.

Ordering Additional/Renewal License Key

To order for new license, follow these steps:

1. On the Thirtyseven4 Exchange Protection Dashboard, click **License**.
2. Click the **License Order Form** tab.
3. Select **Additional license for existing license** if you want to add new mailbox license.
4. Enter the number of additional mailbox.
5. Select **Renewal license for existing license** if you want to renew your license.

6. Click **Create** to generate an order form.

   The License Order Form screen appears.

7. Click **Print** to take the print of your order form, or click **Send Mail** to send the order through email.

Chapter 7.

Technical Support

Courteous and dedicated customer service is our top priority and defines our business relationships. Thirtyseven4 offers Web-based support (Knowledgebase, Frequently Asked Questions (FAQ)), Live-Chat support, E-mail support, and Telephone support.

Support

The Support menu provides you with various support facilities. The Support menu redirects you to the relevant support systems such as Web Support (Visit FAQ), Email Support, and Phone Support.

To seek support, follow these steps:

- On the Thirtyseven4 Exchange Protection Dashboard, click the **Support** menu.

  The Support screen with the following Support options appears.

  - Web Support (Visit FAQ) – Frequently Asked Questions (or FAQ) offer answers to the most common and frequently asked questions related to the Thirtyseven4 Exchange Protection features.
  - Email Support – Email Support helps you submit your queries and issues online.
  - Phone Support – Phone Support helps you call the support team at the given contact numbers about your issues and queries.

Web Support

If you have a query, you are recommended to check with our FAQ at least once before you resort to using other means of support systems. It is possible that you may find an answer to your queries in FAQ.

Email Support

With email support, you can register your queries online instantly so as the turnaround time on your queries is as low as possible.

Phone Support

You can also call us directly for your queries. Thirtyseven4, LLC. provides technical support between 8:00 AM and 5:00 PM EST (Eastern Standard time).

Thirtyseven4 users in the United States can call us at the support number: 1-877-374-7581.

Help

In the Help menu, you can find the online Help that helps you understand how to use and configure various features of Thirtyseven4 Exchange Protection.

To access Help, follow these steps:

- On the Thirtyseven4 Exchange Protection Dashboard, click the **Help** menu.

