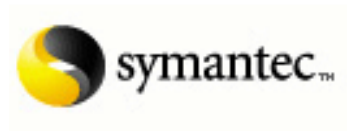
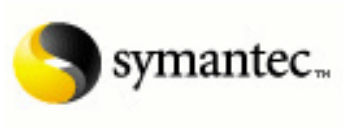
Enterprise Support Utilities Group

SylinkReplacer



SylinkReplacer
Enterprise Support Utilities Group

Table of Contents



SylinkReplacer
Enterprise Support Utilities Group

Disclaimer

Symantec Complimentary Software Tool License Agreement

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THIS COMPLIMENTARY SOFTWARE TOOL AS PART OF THE SOFTWARE AND DOCUMENTATION (THE "PRODUCT") WITH WHICH THIS SOFTWARE TOOL WAS DELIVERED, OR WITH WHICH THIS SOFTWARE TOOL IS INTENDED TO FUNCTION, TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE PRODUCT (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT (THE "AGREEMENT"). THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BEFORE YOU CLICK ON THE "I ACCEPT" OR "CONTINUE" BUTTON OR OTHERWISE INDICATE ASSENT FOR CONTINUING THE DOWNLOAD PROCESS, PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH CASE YOU SHOULD CLICK THE "CANCEL" OR OTHER SIMILAR BUTTON, AND NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE TOOL. BY CLICKING ON THE "I ACCEPT," "CONTINUE" OR OTHER SIMILAR BUTTON AND DOWNLOADING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

License Grant

The complimentary software tool that accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain limited rights to use the Software after Your acceptance of this license. Your rights and obligations with respect to the use of this Software are as follows:

You may:

(i) Use one copy of the Software and any accompanying documentation for Your internal purposes in conjunction with the Product; and

(ii) Make one copy of the Software and documentation for archival purposes.

You may not:

(i) use the Software on any computing systems other than Your own;

(ii) Sublicense, rent or lease any portion of the Software; or

(iii) Reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software.

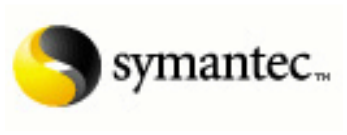
Warranty Disclaimer

THE SOFTWARE IS PROVIDED “AS IS,” EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ANY OTHER WARRANTY, WHETHER EXPRESSED OR IMPLIED. THIS SOFTWARE IS PROVIDED GRATUITOUSLY AND, ACCORDINGLY, SYMANTEC SHALL NOT BE LIABLE UNDER ANY THEORY FOR ANY DAMAGES SUFFERED BY YOU OR ANY USER OF THE SOFTWARE. SYMANTEC WILL NOT PROVIDE TECHNICAL SUPPORT FOR THIS SOFTWARE AND WILL NOT ISSUE UPDATES, UPGRADES, OR ENHANCEMENTS TO THIS SOFTWARE.

Disclaimer of Damages

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE OF SUCH DAMAGES.



US GOVERNMENT RESTRICTED RIGHTS LEGEND

All Symantec products and documentation are commercial in nature. The software and software documentation ar e "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sec tions of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

Export Regulation

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

General Terms

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Sy mantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. This Agreement may only be modified by a License

SylinkReplacer
Enterprise Support Utilities Group

Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Proposal

Symantec Enterprise Support Technicians and Engineers requested a method to recover from a disaster in case the “Disaster Recovery” prerequisites have not been followed or if the client needs to report to a different SEPM (Symantec Endpoint Protection Manager) without uninstalling and reinstalling the client software.

Solution

In response, the Enterprise Support Utilities Group created ‘SylinkReplacer’. SylinkReplacer is a GUI based tool that provides interactive screens that allows a user to move clients, re-establish communication between a client and SEPM or change unmanaged clients to be managed by dropping Sylink.xml from the SEPM on the client.

Prerequisites

SEP clients: 11.0 or higher

Preferably “Domain administrator” privilege for the logged in user account.

Windows Xp or higher (on the computer where the tool is being run from (Not for SEP clients)).

ICMP (Ping specifically) needs to be enabled for discovery to function. (NOTE: RTM/STM versions have ICMP disabled by default)

SylinkReplacer Help

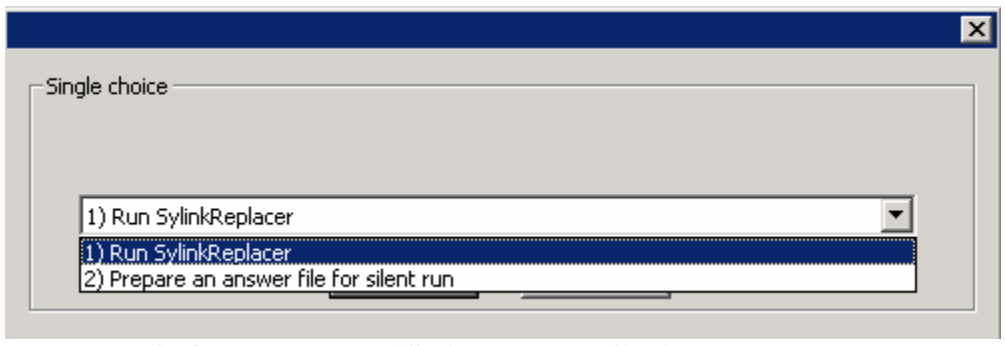
Instructions for use:

Execute the SylinkReplacer.bat and follow the onscreen instructions.
Please note that the DOS window should not be closed during any course of action while the tool is running.

The first prompt will be as shown below. You may select "Run SylinkReplacer" to run the tool in verbose mode (prompting for each action).

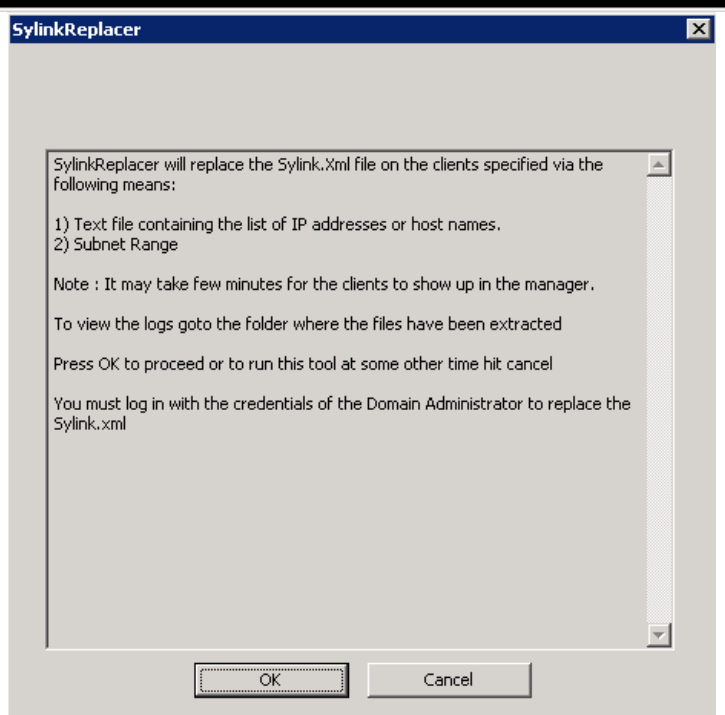
NOTE: To run the tool silently, one must first "Prepare an answer file for silent run". After a silent run file has been created the tool will run silently on its next run using the information specified in the silent run file created earlier. A silent run will allow the user to cancel within the first 15 seconds.

1) The subsequent steps will describe the operations if "Run SylinkReplacer" has been selected.

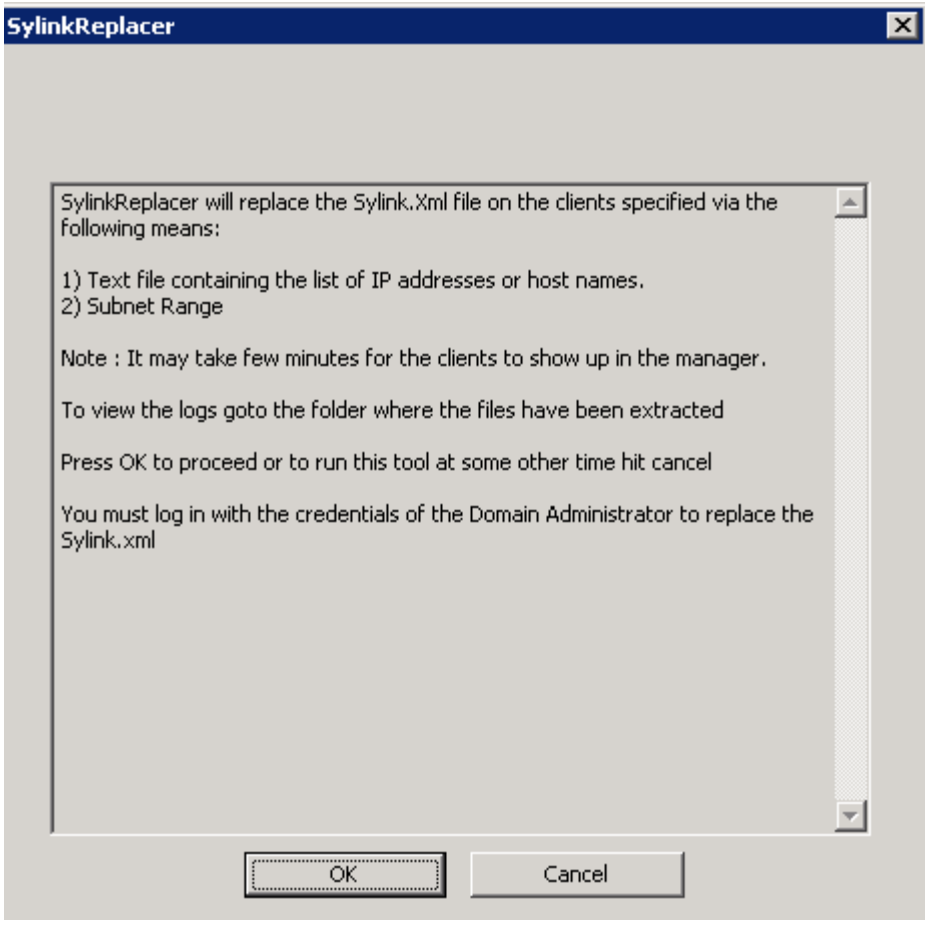


The directory under the root of c:\ by the name "SylinkReplacer" will be created, where the tools content will be extracted.

The logged in user account will be checked next. It is mandatory that the user be a member of the "domain admins" or else the tool will fail.

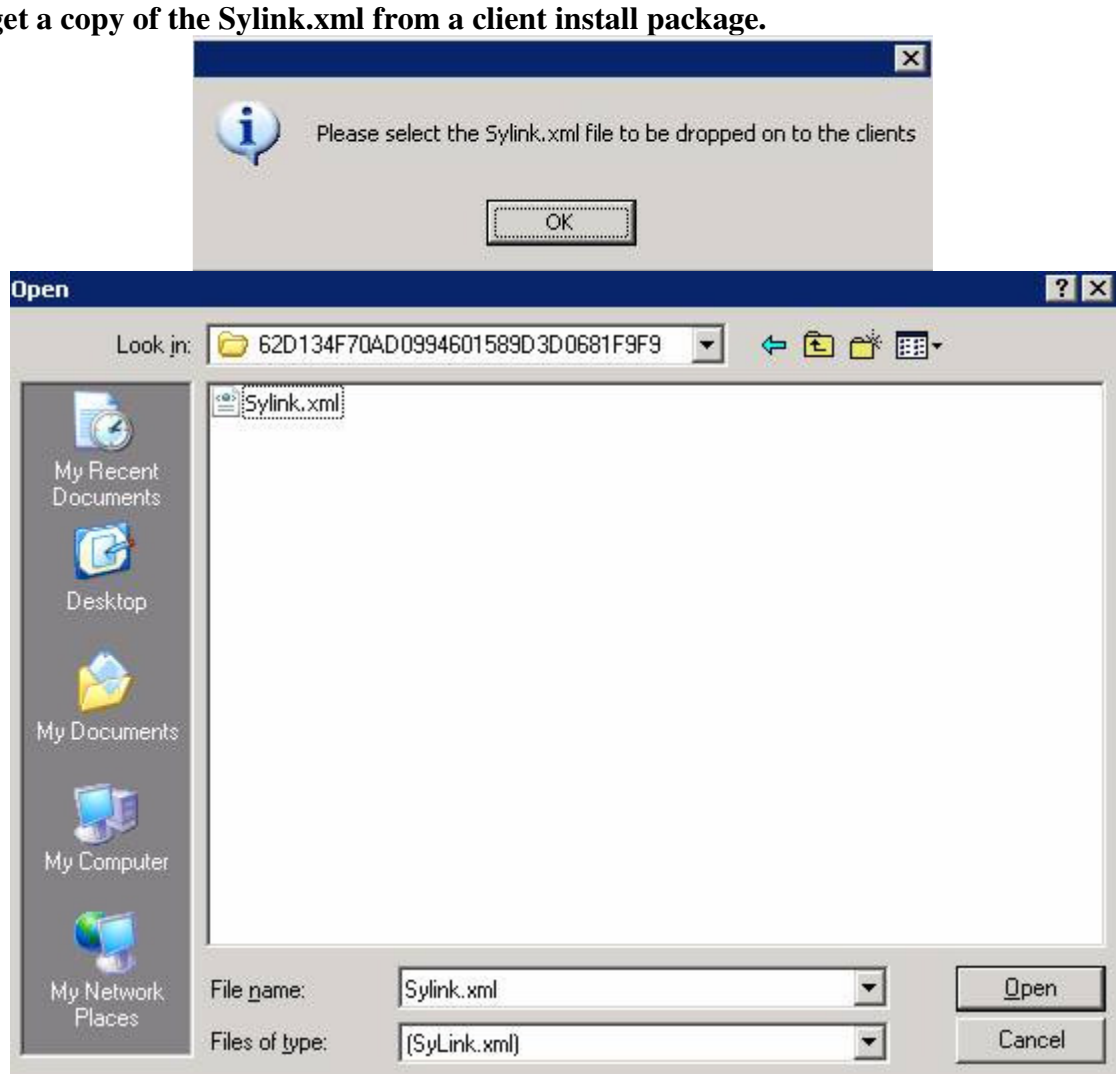


The next screen explains the SylinkReplacer tool, if the user presses "cancel" the extracted files will be cleaned up and the code will exit.



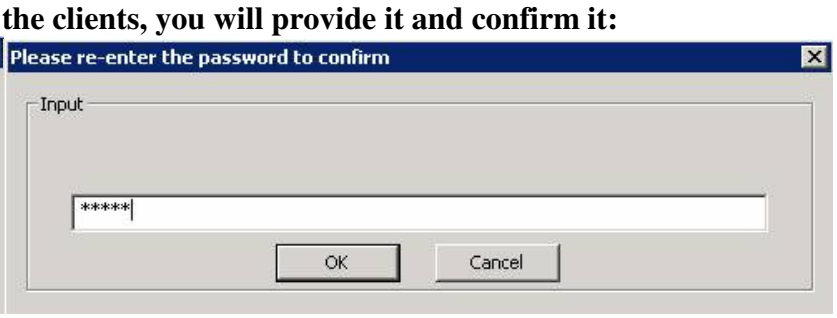
Pressing "OK" it will continue on to the next screen for confirmation of running the SylinkReplacer tool.

2) The user is prompted to select the "Sylink.xml" file which will be the new sylink.xml copied over to the clients. This can be selected by navigating to the C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\ "alpha numeric folder for the group." The folder that the group is designated to can be found by opening up the LSProfile.xml in the same "Alpha Numeric" folder or by logging in to the "Symantec Endpoint Protection Manager" and navigating to Clients > details tab where under the "Policy serial Number" the first four characters are for the group which is reflected in the agent folder as well.
You may also get a copy of the Sylink.xml from a client install package.

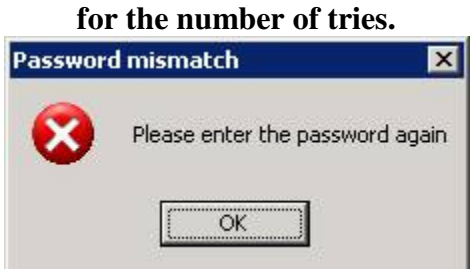


3) Next you will be prompted whether or not SMC ("Symantec management Client") requires a password to stop.

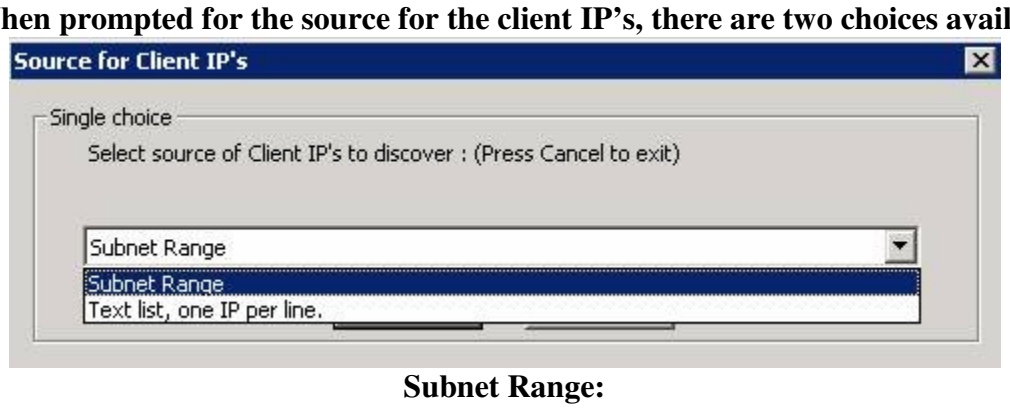
If you have a password to stop the service on the clients, you will provide it and confirm it:



If the password and the confirmed password do not match, it must be re-entered. There are no lockout attempts for the number of tries.

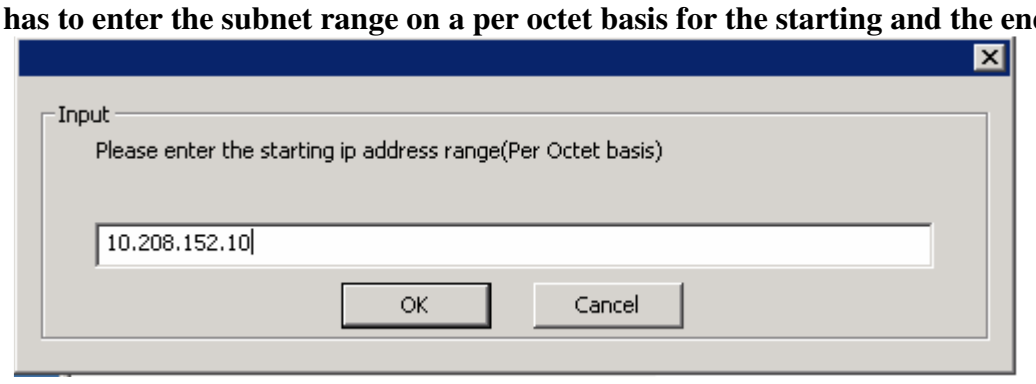


4) When prompted for the source for the client IP's, there are two choices available.

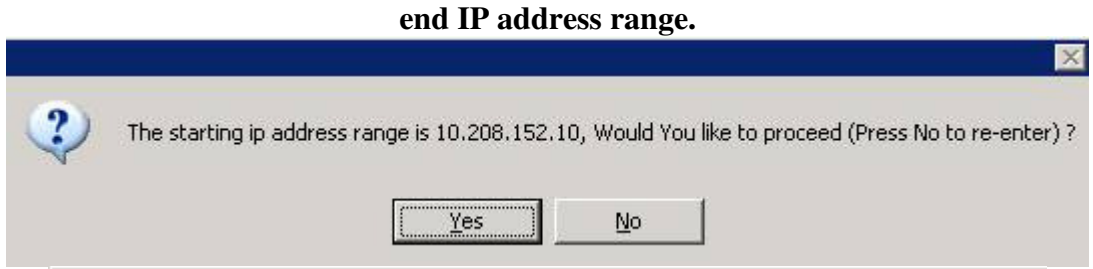


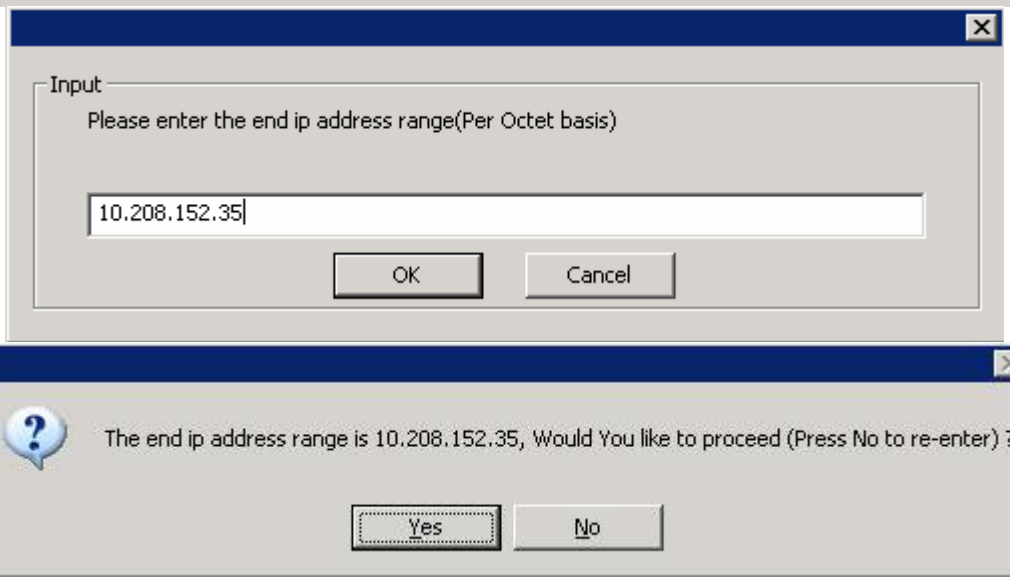
Subnet Range:

4a) The user has to enter the subnet range on a per octet basis for the starting and the end IP address.



If the starting IP address range needs to be corrected, Hit "No" on the next screen or else hit "Yes" to enter the end IP address range.



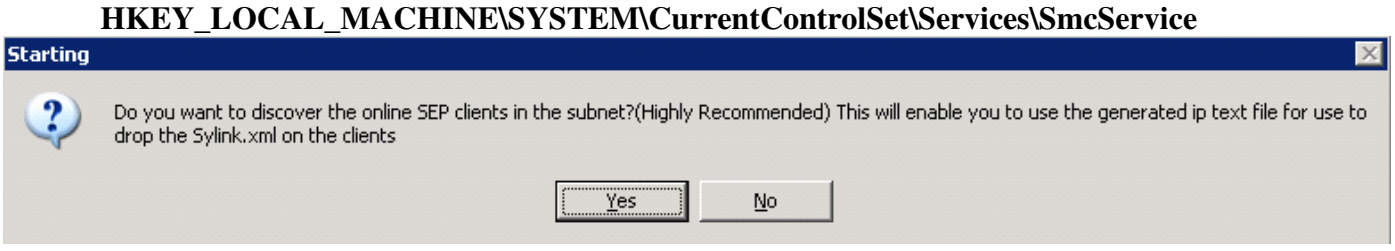


4b) Text List, One per line:

This is a text file containing a list of IP addresses of the clients that are to have the sylink replaced.

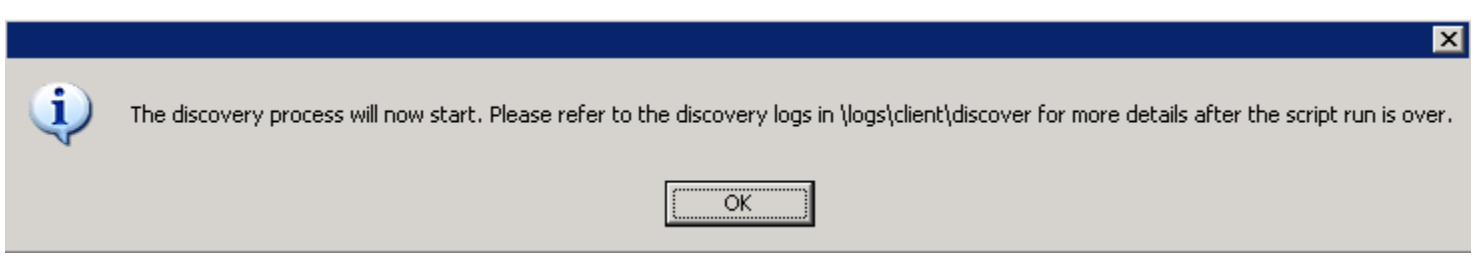
It is highly recommended to discover the clients before dropping the "Sylink.xml" on them to save time and improve accuracy. This will also help you to determine if there are permission issues related to the logged in domain admin account with respect to the client in question. The user should have at least read access to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SmcService

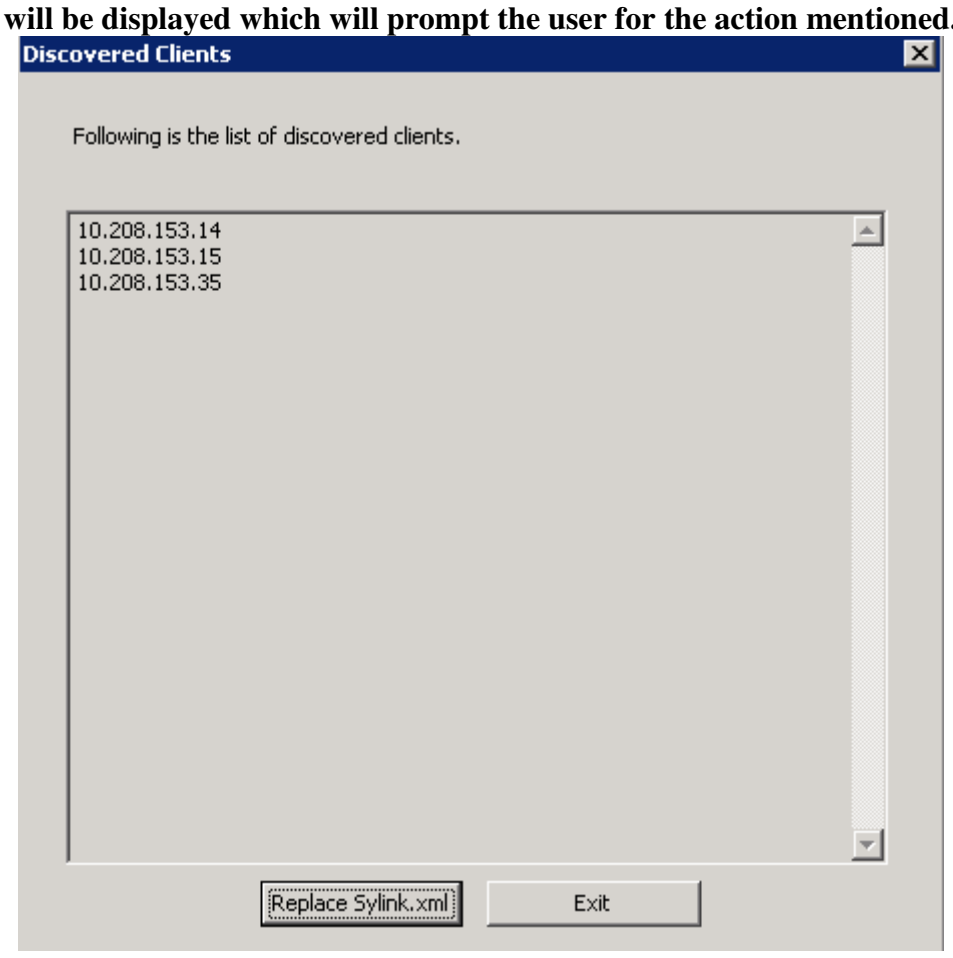


If discovery is selected but no "Symantec Endpoint Protection" clients have been discovered, the following two messages will be displayed:

On hitting "OK", the discovery for the "Symantec Endpoint protection" clients will start.

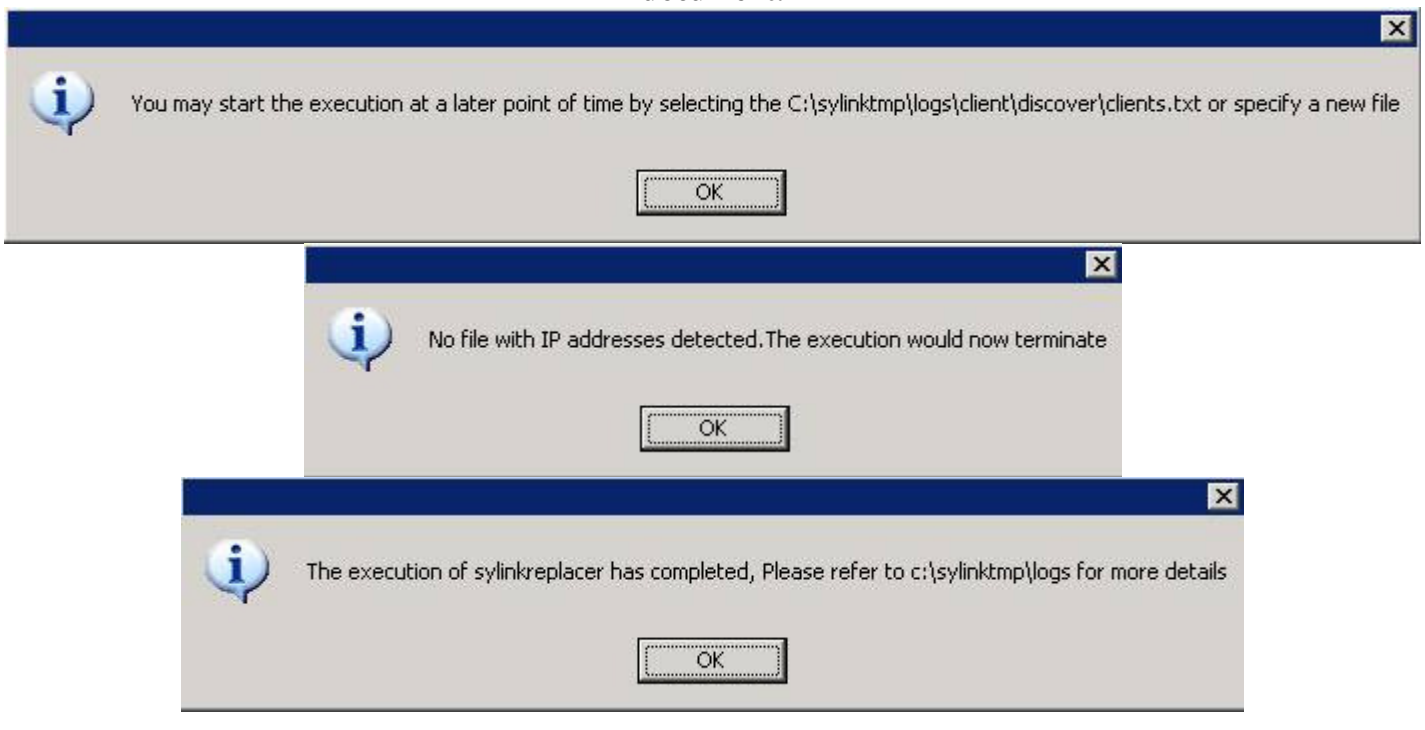


Do not close the DOS window during any course of action. Once the discovery is complete the following message will be displayed which will prompt the user for the action mentioned.



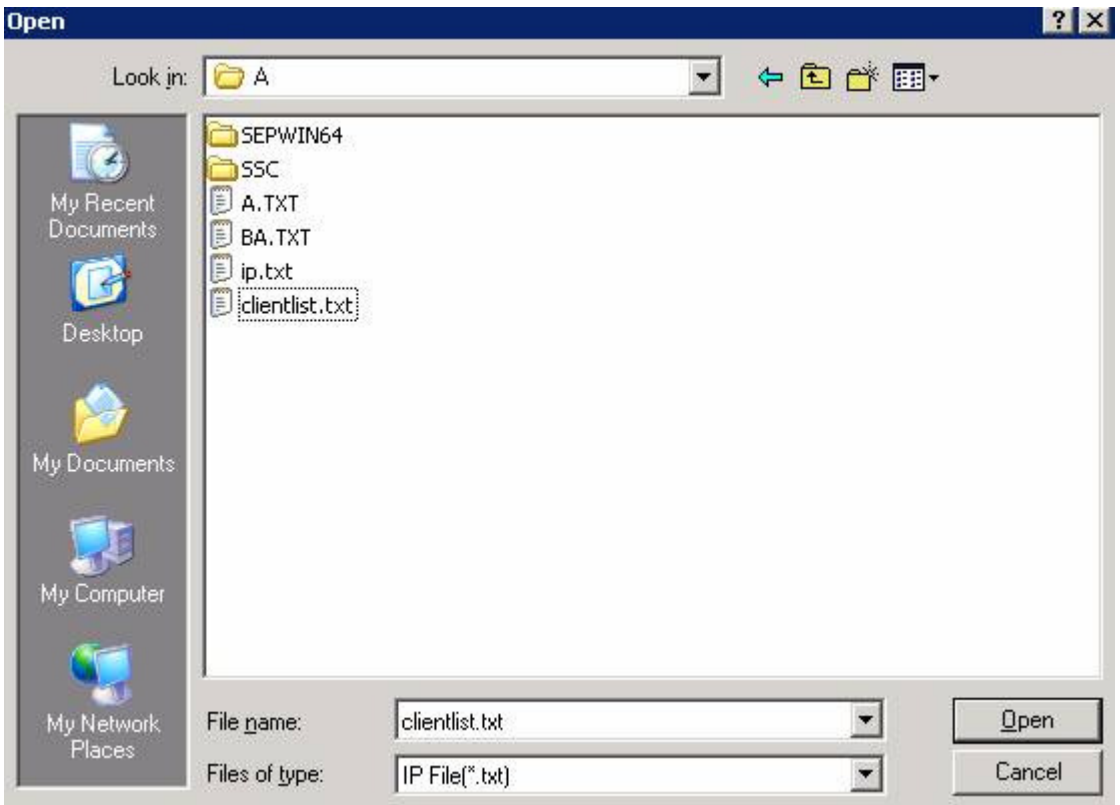
5a) If "Replace Sylink.xml" is hit, the execution for the discovered clients will start immediately

5b) If "Exit" is hit, the execution will be cancelled and the user will be able to use the generated IP file for the actual clients at a later stage. For more information about the log files, Please refer to the Second section of this document.



Please allow some time to pass if "Replace Sylink.xml" button has been chosen, as the sylink.xml replacement is being performed on the discovered clients.

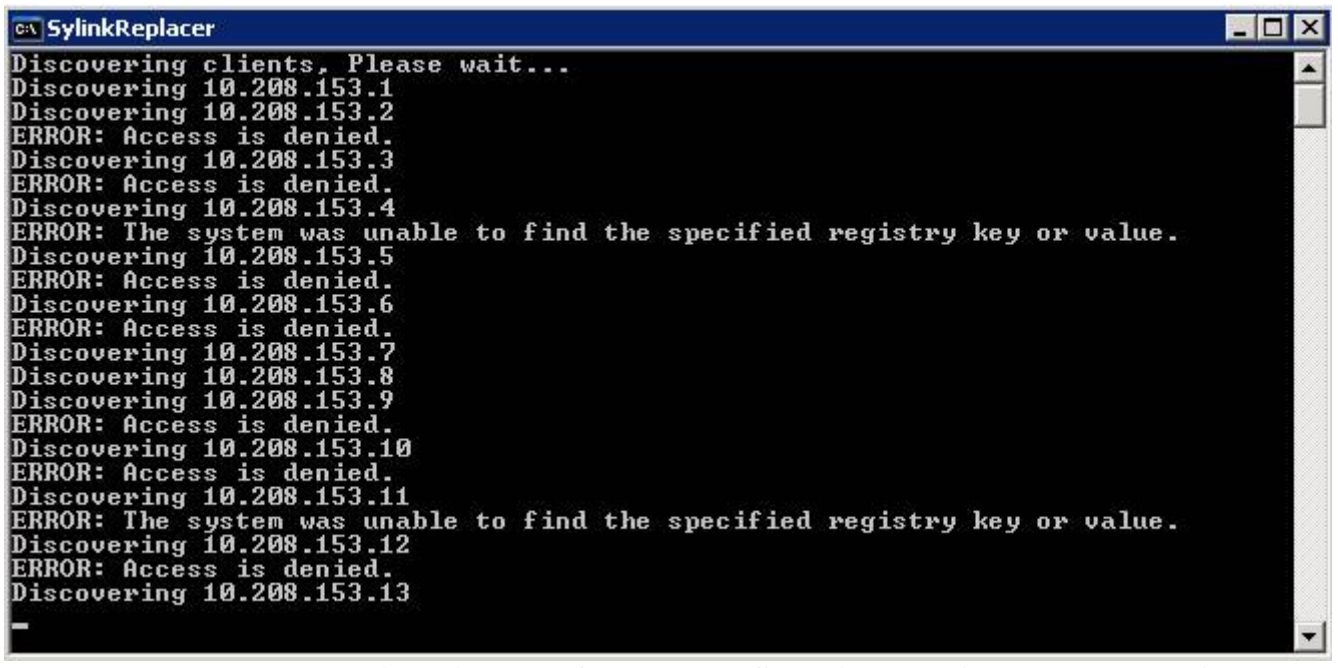
6) Text list, one IP per line: The user has to select the text file that has either been prepared previously by discovering the clients or a self prepared list of IP addresses with the clients IP addresses on a per line basis.



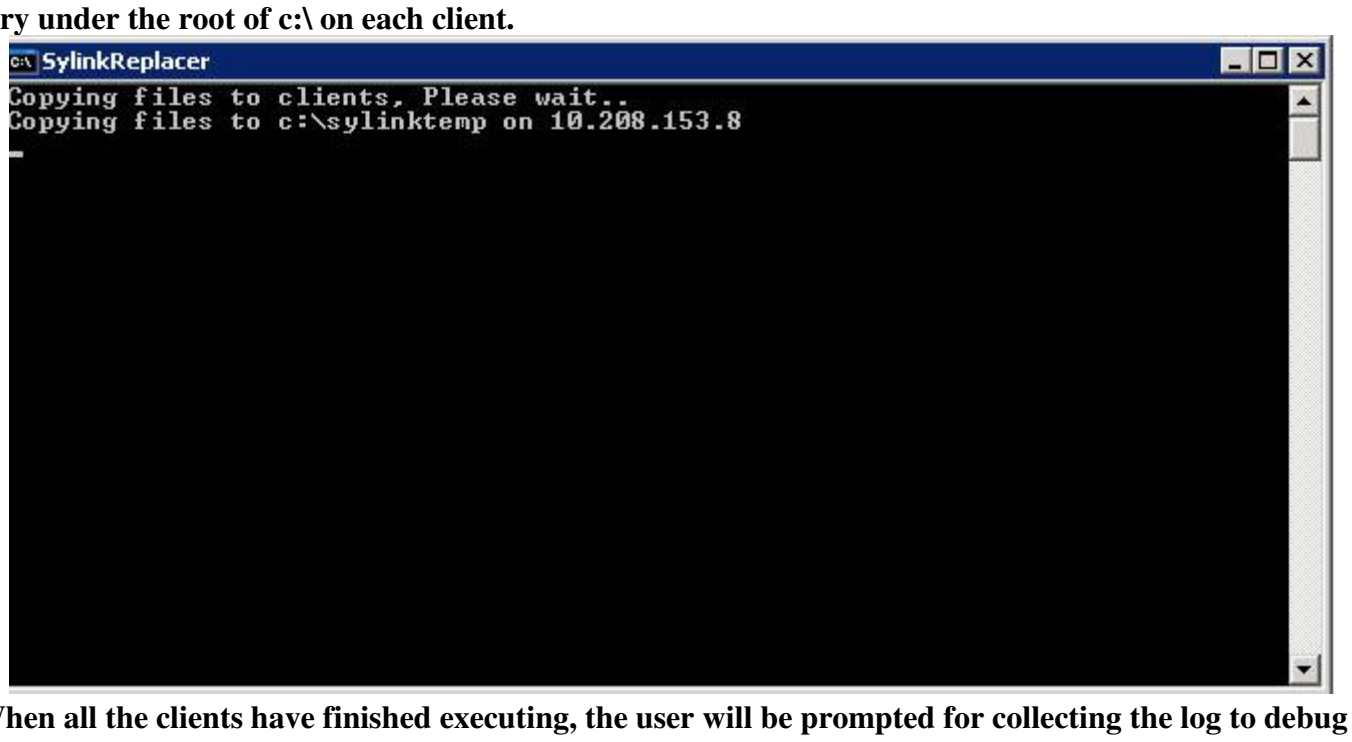
For the discovery, the following screen will be displayed.

***If you see "ERROR: Access is denied", It is likely a permissions issue. If you are logged in as a member of the "Domain admins" group, you should visit the client or try to remotely connect to the registry. The clients under this category will be logged under the NON_CLIENTS.LOG**

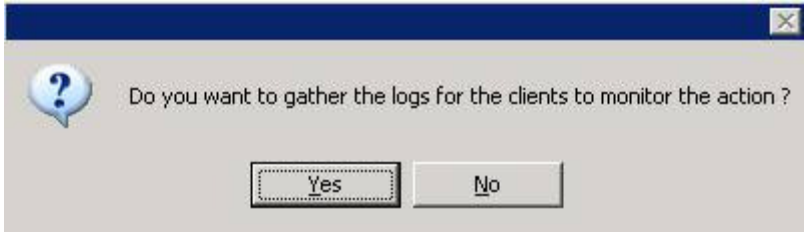
*** If you see "ERROR: The system was unable to find the specified registry key or value", it is likely that the permissions are not effective on the key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SmcService or the workstation in question does not have the "Symantec Endpoint Client" installed on it. This will also be logged under the NON_CLIENTS.LOG.**



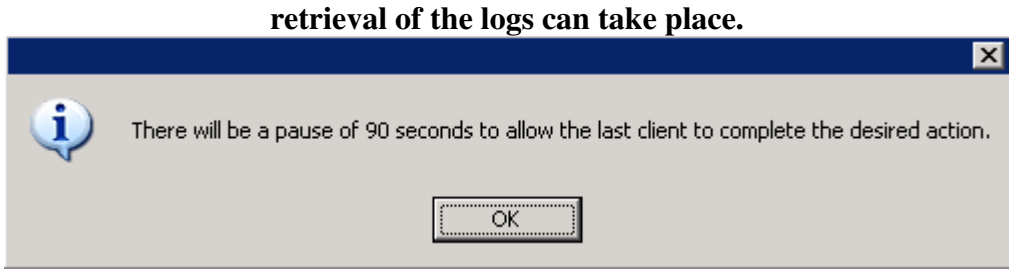
Once that has been done the execution will be performed. The files will be copied over to the sylinktemp directory under the root of c:\ on each client.

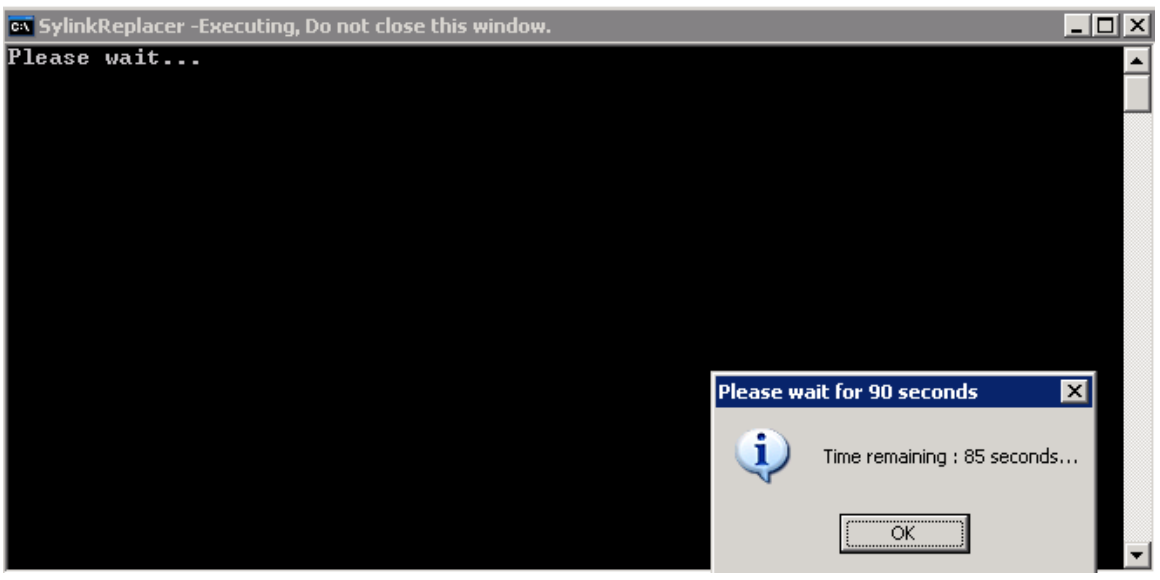


7) When all the clients have finished executing, the user will be prompted for collecting the log to debug and troubleshoot the probable causes if a client hasn't received the new "Sylink.xml" file. (Highly recommended)

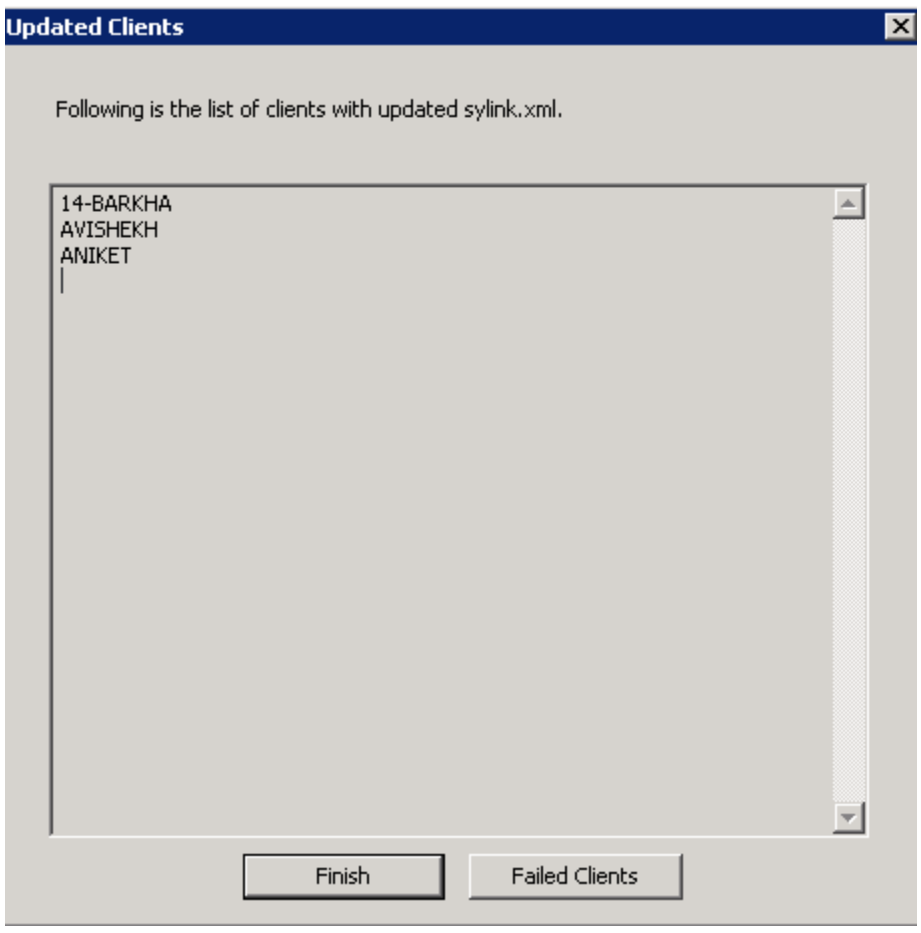


It will take some time (around 90 seconds) to allow the code on the client to be executed completely, before retrieval of the logs can take place.

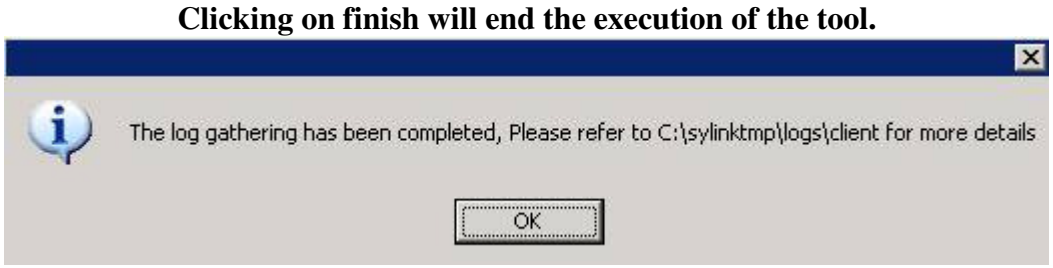




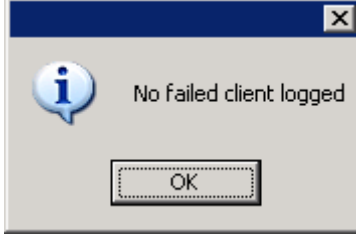
Once this stage is complete, the log files generated on the client side are copied over to Extracted folder\logs\client. This will be further discussed in the LOG ANALYSIS section of this document.



Clicking on finish will end the execution of the tool.



Clicking on "failed Clients" will display the hostnames of the clients on which the Sylink.xml failed to update. This can be debugged with the help of the logs generated. If all clients have been successful in getting the Sylink.xml, then the following message would be displayed.



LOG ANALYSIS

The only place where the logs are stored on the client side is at the Extracted folder\logs.

The log files explained below are for the administrative purposes described:

Extracted folder\logs\server

1) **auth.log: This is the log file generated during the time of logged in user account checking. An example of the contents of auth.log file is below:**

Current User: Administrator
Member of:
Everyone
Administrators
Users
REMOTE INTERACTIVE LOGON
INTERACTIVE
Authenticated Users
This Organization
NTLM Authentication

User account is NOT a member of Domain Admins.

This is an indication that the SylinkReplacer tool will not succeed as the logged in user account is not a member of the "Domain Admins" group. If none or very few clients are successful in obtaining the new "Sylink.xml" file, then the user should rectify the permissions issue.

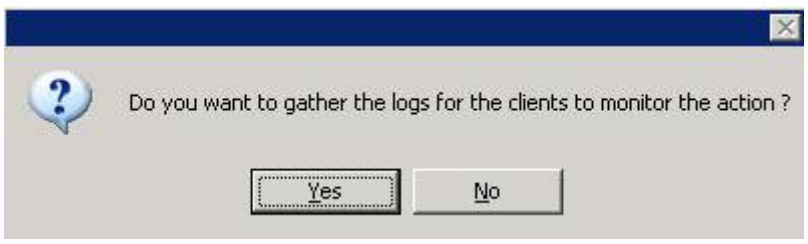
2) **Deploy.log: This log file contains the IP address of all the clients on which the sylink.xml and other files needed for execution have been pushed, regardless of whether it was/will be successful or not.**

3) **Init.txt: This text file is a reference for the user of the action(s) selected during the time of choosing the discovery or execution and will contain either of the following entries**

User selected "Text list, one IP per line."
User selected "Subnet Range"

Extracted folder\logs\client

One or more of the following files may be present in this directory, depending on the action performed on the client side. The log files in the root of "Extracted folder\logs\client" are a result of gathering the log files from the client side after the execution has been completed. This is optional and dependant on your selection when prompted.



If "No" has been hit during the time of run, there will be no file under this directory other than the "discovery" directory.

1) **SUCCESS.LOG: Contains the host names of the clients for which the "Sylink.xml" file has been replaced successfully.**

2) **NO_SEP_INSTALL.Log: Contains the host names of the clients in which "Symantec Endpoint Protection" client is not installed. This file will be present only when the discovery has not been selected as an option.**

3) **SMC_STOP_FAIL.LOG: Contains the host names of the clients in which the "Symantec Management Client" service refused to stop within reasonable amount of time or error out. This file is present when an incorrect password has been supplied to stop the service if password is required. The other reason could be that the client installation has become corrupt and needs to be troubleshot or the client is timing out due to resource issues.**

4) **SYLINK_COPY_FAIL.LOG: Contains the host names of the clients for which the old "Sylink.xml" could not be replaced with the new one.**

5) **SMC_START_FAIL.LOG: Contains the host names of the clients for which the "Symantec Management Client" service could not be started after the completion of the execution. If the "Sylink.xml" file is not copied over as well, then this host would also be mentioned in one or more of these log files.**

6) **FAILED_LUMPSOME.LOG : This file contains the list of all the clients included with in the NO_SEP_INSTALL.Log, SMC_STOP_FAIL.LOG, SYLINK_COPY_FAIL.LOG, SMC_START_FAIL.LOG.**

Extracted folder\logs\client\discover

This folder will be empty unless discovery has been chosen during the time of execution.

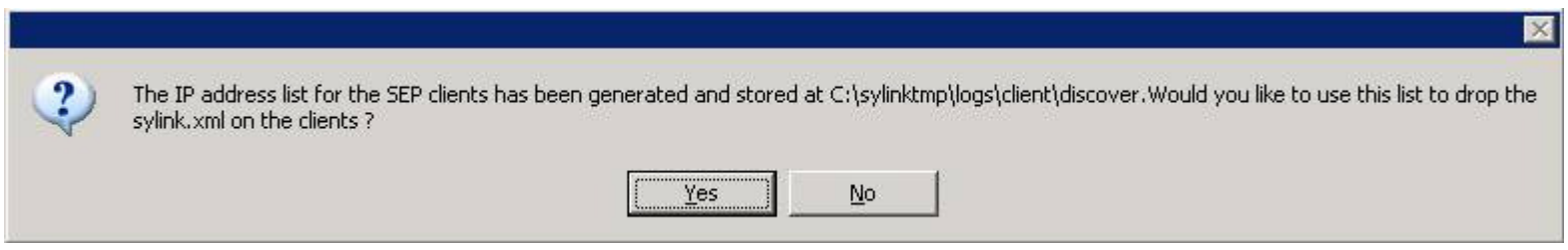
The various log files under this folder denote the network behavior of the clients at that particular time.

1) **Clients.txt: Contains the IP address list of all the hosts that have been determined to be a Symantec Endpoint Protection Client.**

2) **No_Ping.log: Contains the IP address list of all the clients that have not responded to the ping request and are assumed to be offline or otherwise unreachable.**

3) **Non_clients.txt: This file contains the IP address list of all the clients that are either not running Symantec Endpoint Protection Client or the user does not have proper permissions on the registry key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SmcService". Since the permissions on this registry key are inherited from the top of the branch HKEY_LOCAL_MACHINE, it's recommended to connect remotely to the registry of the computers where the access is denied and go downward from HKEY_LOCAL_MACHINE to SmcService to debug where the permissions issue is.**

4) **Exec_now.txt: This file contains the information about two actions. If the user has selected to discover the online clients and drop the "Sylink.xml" on them then the following underlined text will be contained within this file, *Discover and drop chosen* Whereas if the user has selected to discover the online clients but not to drop the "Sylink.xml" file on them then the following underlined text would be contained within this file *Discover and no drop chosen.* This log file is synonymous with the following action depending on the users selection.**

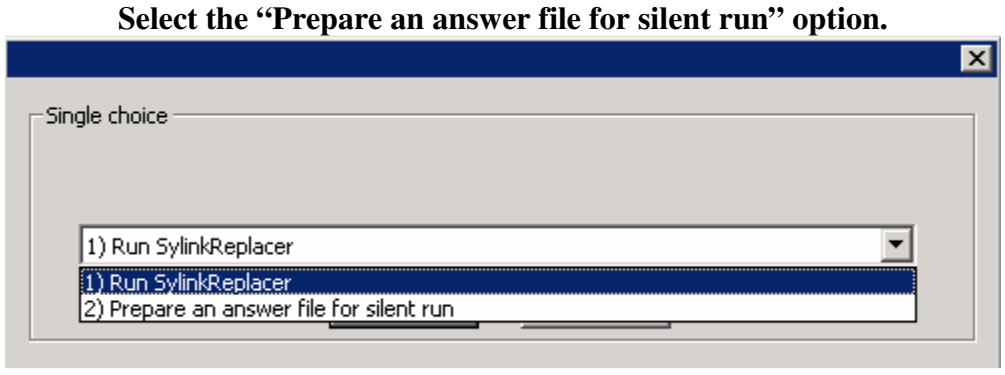


SylinkReplacerSilent Help

Instructions for use:

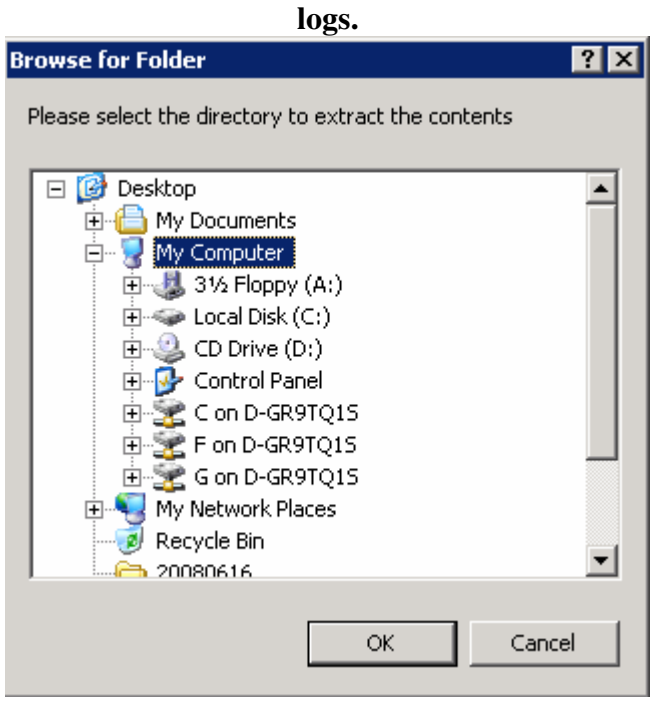
1) **Prepare the answer file for use**

Select the "Prepare an answer file for silent run" option.



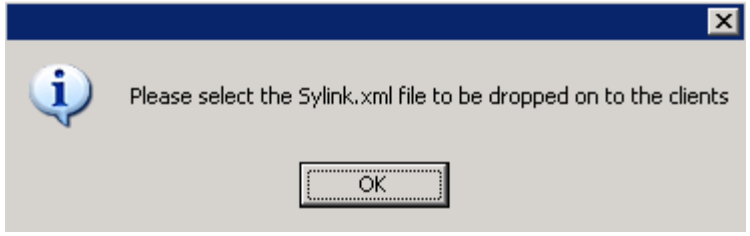
2) **Select the directory to extract the contents**

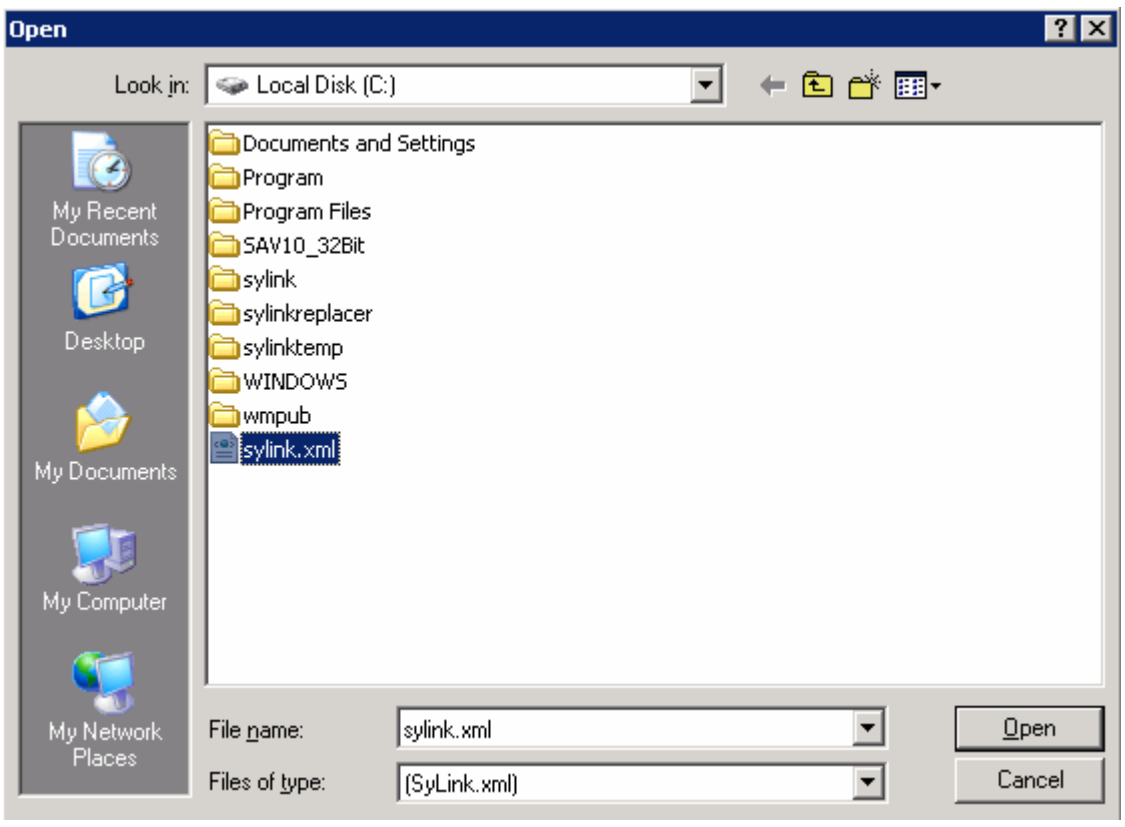
This will be the directory where the files required for the silent run will be copied over and the location for the logs.



3) **Select the Sylink.xml**

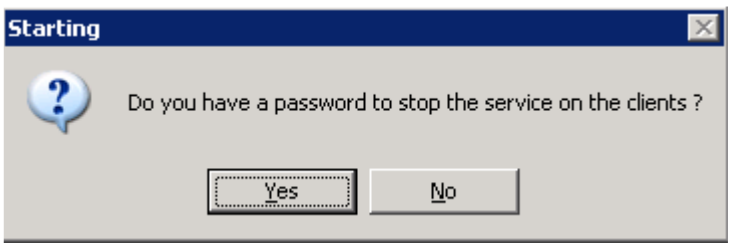
Select the Sylink.xml file, which needs to be replaced on the clients.

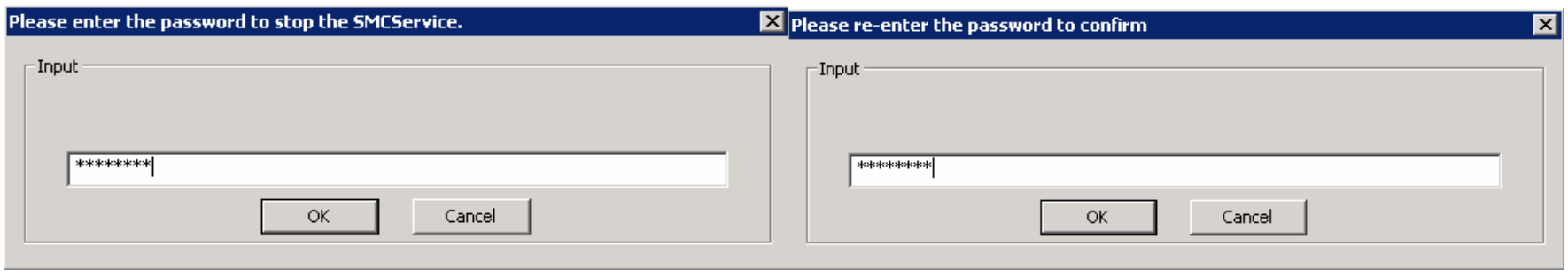




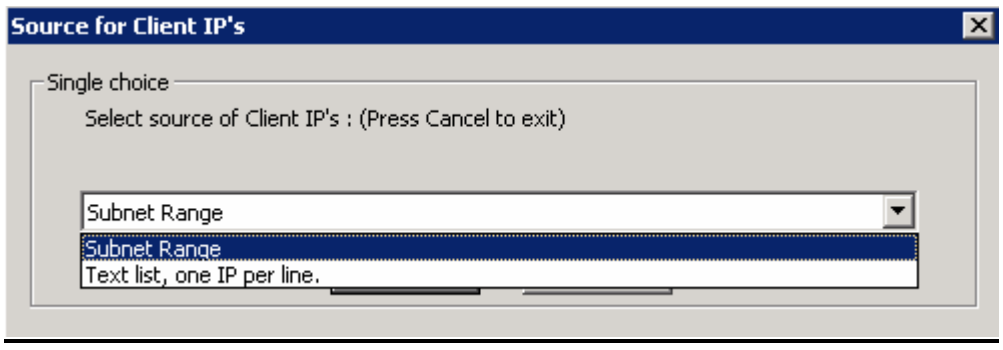
4) Enter the password to stop the SMCService(if applicable)

In case a password has been set to stop the SMCService, it has to be entered and confirmed in the illustrated dialog box.

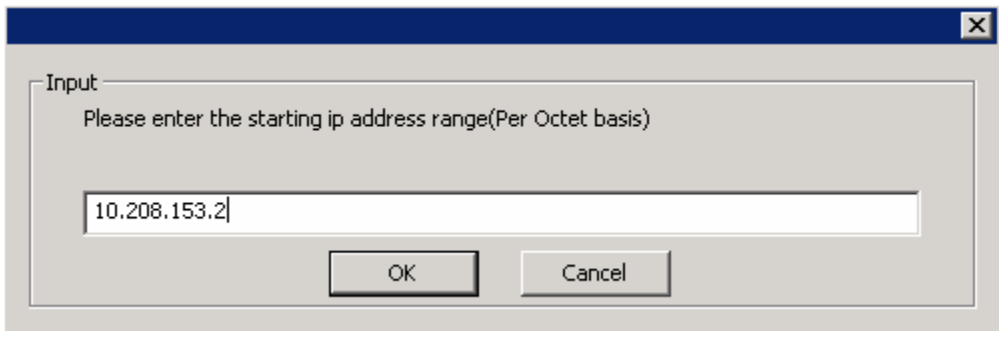


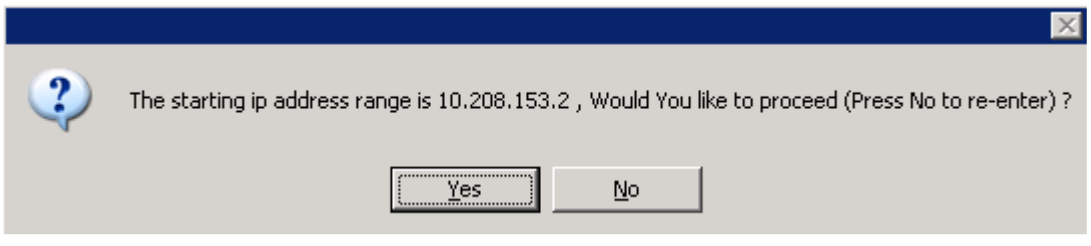


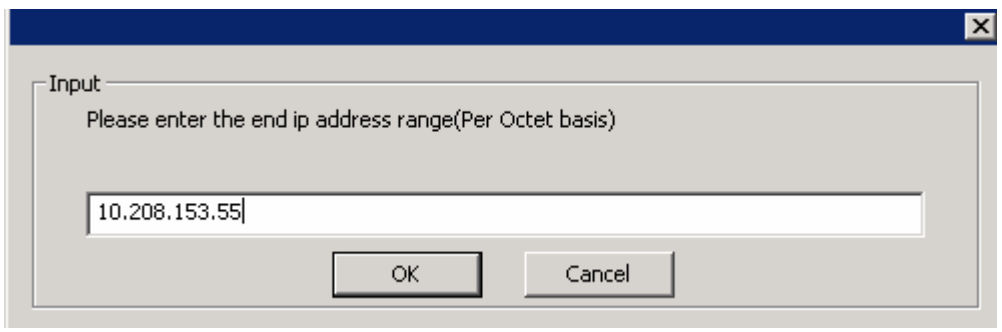
5) The source for the clients has to be determined.

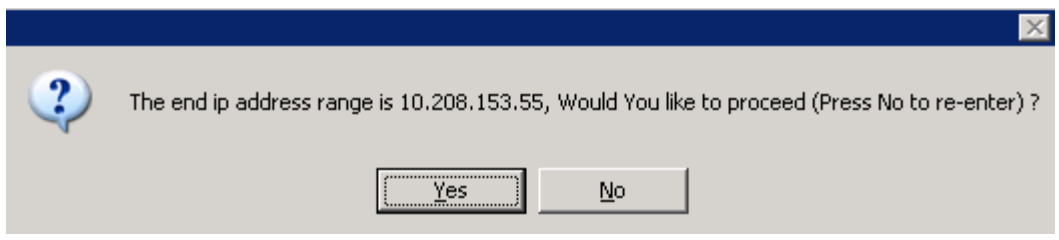


If the subnet range has been specified then the starting and the end IP address range has to be supplied.



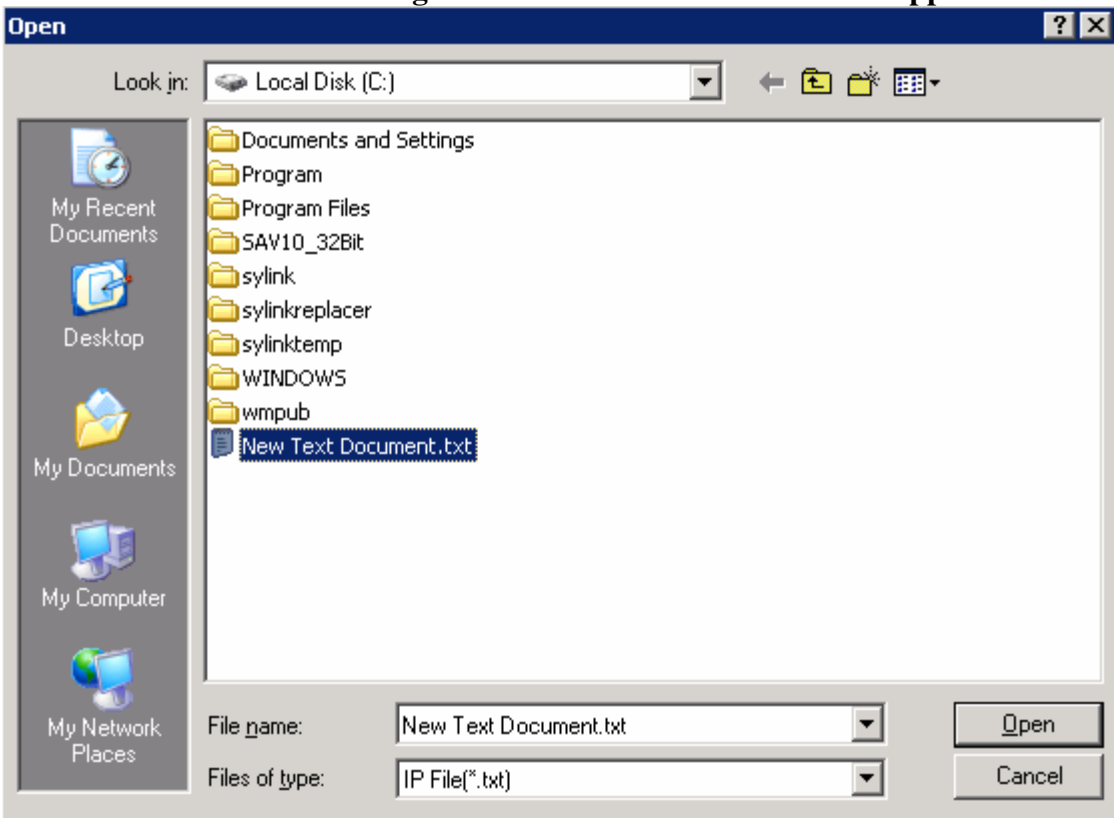






For the text file with list of IP addresses:

The text file containing the list of IP addresses has to be supplied.



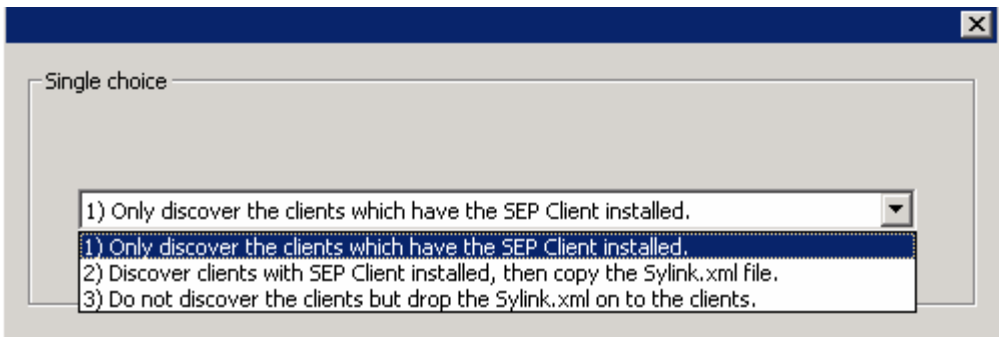
6) Select the mode of operation

There are three choices available:

6a) Only discover the clients which have the SEP client installed: To be aware of the SEP clients in the environment and use the list in the further run if desired.

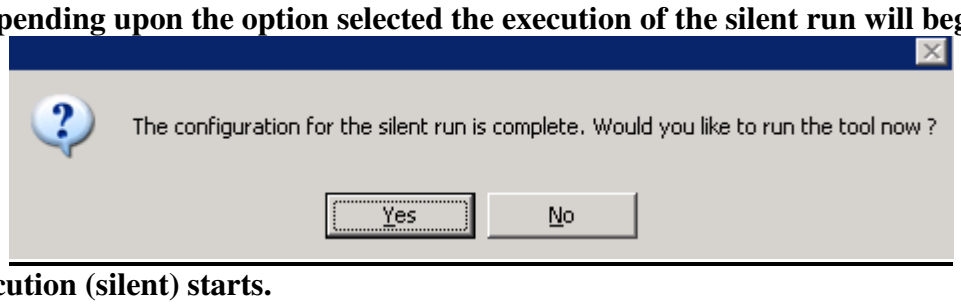
6b) Discover Clients with SEP installed, then copy the Sylink.xml file: To discover the SEP clients in the environment and then drop the Sylink.xml file on the clients that have been recorded.

6c) Do not discover the clients but drop the Sylink.xml on to the clients: To drop(replace) the sylink.xml file on the clients without checking if the machine has SEP client installed on it.(recommended to be used only if there are problems with the registry permissions in the environment.)



7) Configuration Complete

Depending upon the option selected the execution of the silent run will begin.



If "yes" has been selected then the execution (silent) starts.
If "no" is selected, the run is delayed until the next time the sylinkreplacer.exe is executed.

Execution of the Silent Run

Once the "answer file" has been prepared on the next run there will be a pause of 15 seconds and if there is no user intervention then the silent run will start automatically depending on the options selected during the silent run.
To prepare a new answer file, delete the c:\sylinkreplacer\silent\SylinkSilent.Settings and run the tool again to prepare the answer file.

SylinkReplacer Troubleshooting

ESUG Executables

TestSec.exe

This application is used to verify the logged in user account privileges.

ESUGUnEn.exe

This application is used to stop a process without user interaction.

ESUGSleep.exe

This application provides a delay for processing inside the batch files.

ESUGReg.exe

This application is used to read the registry, find out the location of the SMC.exe, and the client installation location.

ESUGDlgControl.exe

This application is used to provide the user interface for the SylinkReplacer tool.

ESUGRegEx.exe

This application is used to run regular expressions and verify the authenticity of the entered I.P. address.

Text File

SylinkReplacer.txt

This text file displays the EULA to the user running the tool.

Executable batch files

call.bat (Invoked File by SylinkReplacer.exe)

This file gets invoked when the contents are extracted to the directory C:\sylinkreplacer. Depending on the user's choice of "Preparing the answer file" or running the tool, this will consequent call one of the files (sylinkreplacersilent.bat or sylinkreplacermain.bat).

Silent Run

sylinkreplacersilent.bat

This file gets invoked if the answer file has been prepared and the 10 second delay completes. Depending upon the prepared answer file, the execution is carried out.

discoversilent.bat

This file is invoked when silent run is chosen. It is only invoked if the text file of IP addresses has been specified instead of the subnet range. It discovers the clients to see if the client is installed on the machine by checking the registry key "HKLM\SYSTEM\CurrentControlSet\Services\SmcService" if it exists on the client.

subdropsilent.bat

This file is invoked when silent run is chosen. It is only invoked if the subnet range has been specified instead of the text file of IP addresses. It copies over the files to the client side and starts the "SylinkReplacer" service that it creates. It will then deletes the service once the app2.bat on the client side is invoked. The files copied over on the client are app2.bat, Sylink.Xml, esugsleep.exe, esugreg.exe and password.txt (in case a password to stop the service is specified).

subdiscoversilent.bat

This file is invoked when silent run is chosen. It is only invoked if the subnet range has been specified instead of the text file of IP addresses. It discovers the clients to see if the client is installed on the machine by checking the registry key "HKLM\SYSTEM\CurrentControlSet\Services\SmcService" if it exists on the client.

dropsilent.bat

This file is invoked when silent run is chosen. It is only invoked if the text file of IP addresses has been specified instead of the subnet range. Like the subdropsilent.bat it also copies over the files needed for execution on the client, creates the "SylinkReplacer" service, starts it and then deletes it. The files copied over on the client are app2.bat, Sylink.Xml, esugsleep.exe, esugreg.exe and password.txt (in case a password to stop the service is specified).

gathersilent.bat

This is the file that's invoked when silent run is the option. It gathers together the logs from the clients under %windir%\system32\ESUG.

Verbose Run

SylinkReplacermain.bat

This file creates the directories needed for logs i.e. C:\Sylinkreplacer\ logs, C:\Sylinkreplacer\ logs\server, C:\Sylinkreplacer\ logs\client and C:\Sylinkreplacer\ logs\discover.

sylinkreplacer.bat

This is the file that is called by the SylinkReplacermain.bat for the further execution. It checks the account privileges and gathers the rest of the information needed for execution as per the user's choice.

app.bat

This file is executed to copy over the files needed for execution on the client side. It copies over the files to the client side and starts the "SylinkReplacer" service that it creates and then deletes the service once the app2.bat on the client side is invoked. The files copied over on the client are app2.bat, Sylink.Xml, esugsleep.exe, esugreg.exe and password.txt (in case a password to stop the service is specified.)

app1.bat

This file is invoked when the discovery has been specified. This is only invoked if the subnet range has been specified instead of the text file of IP addresses. It discovers the clients to see if the client is installed on the machine by checking the registry key "HKLM\SYSTEM\CurrentControlSet\Services\SmcService" if it exists on the client.

app3.bat

This file is invoked when the discovery option has not been specified. It pings the clients and tries to copy over the files on the "c:\sylinktemp" directory on the client. It copies over the files to the client side and starts the "SylinkReplacer" service that it creates and then deletes the service once the app2.bat on the client side is invoked. The files copied over on the client are app2.bat, Sylink.Xml, esugsleep.exe, esugreg.exe and password.txt (in case a password to stop the service is specified.)

app5.bat

This file gets invoked when the text file with IP addresses is specified. . It discovers the clients to see if the client is installed on the machine by checking the registry key "HKLM\SYSTEM\CurrentControlSet\Services\SmcService" if it exists on the client.

app6.bat

This file gets invoked for the log gathering. It gathers the logs from the clients under %windir%\system32\ESUG.

Client Side

app2.bat

This is the file that gets executed on the client side to replace the Sylink.xml file. The helper files along with app2.bat on the client side are Sylink.Xml, esugsleep.exe, esugreg.exe and password.txt (in case a password to stop the service is specified.)

Sylink.xml

This is the file that eventually replaces the original Sylink.xml

Esugsleep.exe
This application provides a delay for processing inside the batch files.

esugreg.exe

This application is used to read the registry, find out the location of the SMC.exe, and the client installation location.

password.txt

This file contains the password in case it is needed to stop the SMCService on the client.

General:

-All the files in the C:\Sylinktemp on the client side are deleted along with the folder once the execution is complete and the logging is done in the directory %windor%\system32\ESUG.
-On the computer where the tool is being run the c:\sylinkreplacer will not get deleted unless manually done.
-If the silent run option has to be removed, the answer file located in C:\sylinkreplacer\silent by the name SylinkSilent.Settings has to be deleted manually.
-It is highly recommended to run the tool with the credentials of the "Domain admin."
-This tool is designed for a domain, but can be used in a workgroup if there is a universal admin account used.
-For the discovery process it is mandatory for the user executing the tool to have at least "read" permissions on the registry key "HKLM\SYSTEM\CurrentControlSet\Services\SmcService" on the client side.

Frequently Asked Questions (FAQ):

Question: What are the best practices for running the tool?
Answer: The logged in user should be a member of the "Domain admins" group and should have at least "Read" privileges to the registry key "HKLM\SYSTEM\CurrentControlSet\Services\SmcService" on the client side in case of discovery.

Question: Is it mandatory to have the c$ on the clients?
Answer: Yes, It is mandatory to have the c$ on the client and c:\ on the server.

Question: Why does the tool appear to run properly when executed from a windows 2000 machine but not replace the Sylink.xml on the clients?
Answer: This is due to the fact that the tool uses the built in sc.exe command to create a temporary service which by default is not part of the Windows 2000(available in windows 2000 server resource kit)

Question: In what environments should the discovery not be selected?
Answer: It is highly recommended to run the discovery but in case there is a known problem with the registry permissions, this option can be omitted.

Question: How can the 10 second wait be omitted after preparing the answer file?
Answer: The best and the easiest way is to delete the sylinksilent.settings file located in c:\sylinkreplacer\silent directory. This will return the tool to it's default "verbose" mode.

Question: What is the use of preparing the silent file?
Answer: The silent file could be used for ease with the "Task Scheduler" to replace the Sylink.xml on the clients that are not online at the moment or out of the environment. A task can be setup that points to sylinkreplacer.exe once the answer file has been prepared to replace the sylink.xml on those clients.

Question: Will this tool work on windows 2000 clients?
Answer: Yes, it will replace the Sylink.xml on 2000 and higher clients.

Question: Why are all or some of my clients not being discovered?
Answer: ICMP (Ping specifically) needs to be enabled for discovery to function. (NOTE: RTM/STM versions have ICMP disabled by default)