

Symantec Endpoint Protection

Version 12.1

Migration Whitepaper

Version 1.1



Table of Contents

What is covered in this Whitepaper	3
Before Migrating	3
Migration.....	5
LiveUpdate Administrator (LUA)	5
Enforcers.....	5
SEPM.....	5
Group Update Providers (GUPs).....	18

What is covered in this Whitepaper

This whitepaper is intended for those that are migrating to version 12.1 of the Symantec Endpoint Protection Manager (SEPM). This whitepaper will provide guidelines and considerations for activities before, during and post migration.

These guidelines are meant to supplement to your knowledge of Symantec Endpoint Protection Technologies. For information about what is new with Symantec Endpoint Protection 12.1 please refer to the following URL

if you are lacking general knowledge of Symantec Endpoint Protection it is strongly recommended that you engage Symantec Consulting services for additional support.

Although migration from earlier Symantec Endpoint Protection versions is possible, this whitepaper will focus on migration from Symantec Endpoint Protection version 11.x to Symantec Endpoint Protection 12.1

Areas Covered:

- LiveUpdate Administrator (LUA)
- Enforcer Migration
- Replication
- Migrating Symantec Endpoint Protection 11
- Group Update Providers (GUPs)

Before Migrating

Before migrating it is important to understand what impact the process will have to your production systems. Please note the following:

- Symantec Endpoint Protection Managers
 - Perform a database backup for each site
 - Inventory your policy managers
 - Review the system requirements for SEP 12.1 and confirm that your systems still meet the hardware and software requirements
 - Ensure that you have enough disk space for the migration
 - The SEP 12.1 SEPM upgrade installer requires 3 times the current database size (sem5.db) if upgrading from pre-12.1 SEPM with the embedded database only
 - Obtain an up to date architecture inventory of your production systems
 - Know how many SEPMs you will be migrating
 - Which sites are replicating

Notes:

- SEP 11.x management software cannot manage SEP 12.1. If you plan to use both in your environment, you will need two separate management programs, one for SEP 11 policy managers and one for SEP 12.1 policy managers.
- LiveUpdate Administrator
 - Where are they and how many are deployed?
 - Obtain a copy of LUA version 2.3
- Enforcers
 - It will be necessary to shut down the SEPM service during the migration period
 - Understand that Enforcers need SEPM to authenticate client GUIDs, plan accordingly. See the Implementation guide about how to set 'local authentication' while the SEPM is migrating.
 - Command for enabling Local Authentication
 - Enforcer(advanced) local-auth enable
 - In order to have the Enforcers functional after migration you will need to have a new version of the SNAC.XML file. This file is typically located on the SNAC DVD distribution disc
- Licensing
 - With the introduction of Symantec Endpoint Protection 12.1 Licensing is enforced. Be sure to have a valid license file or license code from Sales / Enterprise Support
- Client Software Settings
 - Be advised that when you are ready to migrate your clients to 12.1, these clients will require a reboot to install the new drivers.
 - 11.x clients will report and will be managed by SEPM 12.1
 - Immediate migration of your clients is not necessary
 - Transitioning to 12.1 client software should proceed after proper testing is done with a cross section of your user base

Migration

LiveUpdate Administrator (LUA)

Update your LUA servers to version 2.3. This version has been updated to include content updates for 12.1 SEPM and Clients. Performing this step will ensure that your clients and SEPMs will receive 12.1 content once you've upgraded them, especially if your SEPMs retrieve content updates from LUA directly.

Enforcers

In the section 'Before Migration' you were informed that any Enforcers would not be able to authenticate clients during the migration down time.

For the reason stated above you will need to disable SEPM/Client Authentication and enable 'Local Authentication' for each Enforcer appliance. See the command below for this function and refer to the Enforcer documentation if unsure you are able to perform this task.

- Command to Enable Authentication on the Enforcer
 - i. Enforcer(advanced) local-auth enable

Note: At the end of the migration you will be reminded to disable 'Local Authentication'.

SEPM

Note: Please review the section "[Before Migrating](#)" before performing the following steps.

Items to cover:

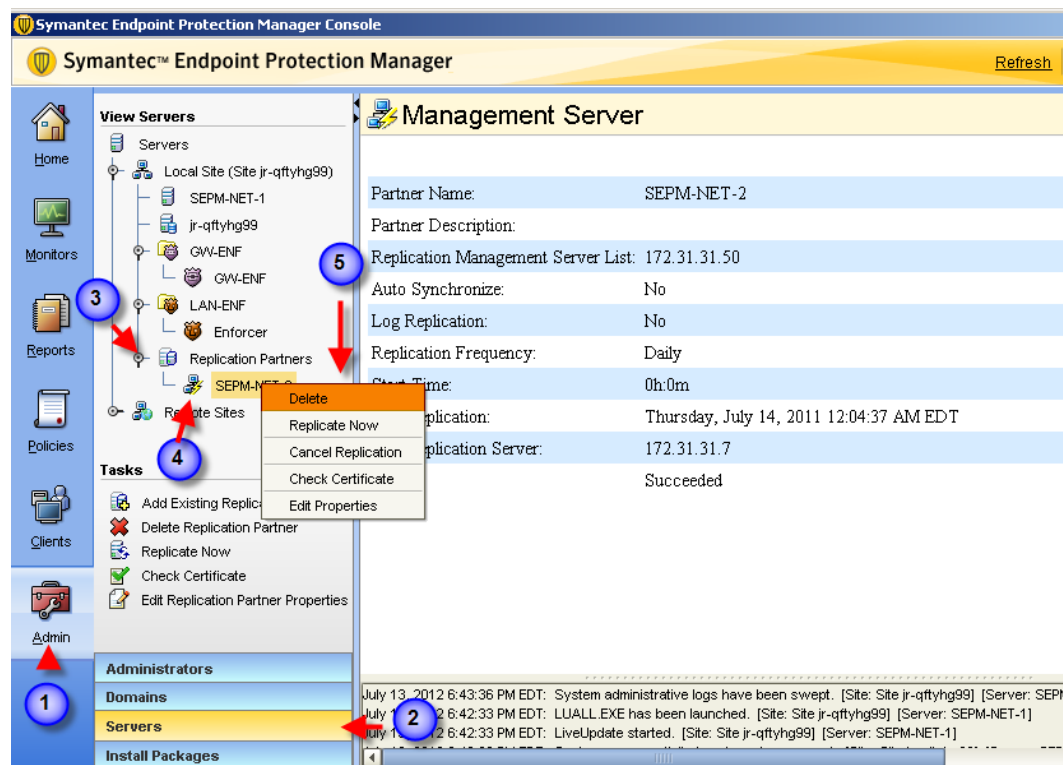
- SEPM upgrade from existing SEPM (v11.0)
 - Using existing embedded database
 - Use existing SQL server used by SEP 11

Outline of Procedures

- Disable Replication
- Backup Your Database
- Stop SEPM Services for each Policy Manager Installed
- Upgrade each Policy Manager
- Upgrade each Policy Manager at each other site
- Enable Replication
- Disable 'Local Authentication' on Enforcers
- Upgrade clients to 12.1

Disable Replication

1. Log into the SEPM at one of your sites and Click on the '**Admin**' tab
2. Select **Servers**
3. Expand the '**Replication Partners**' listing
4. Select a partner
5. Right Click and Delete



Database Backup

During the migration you will be prompted to back up your database. At this stage you can perform a database backup manually through the SEPM database function and this will prepare you for migration, otherwise you will need to perform a backup during the migration process as stated above.

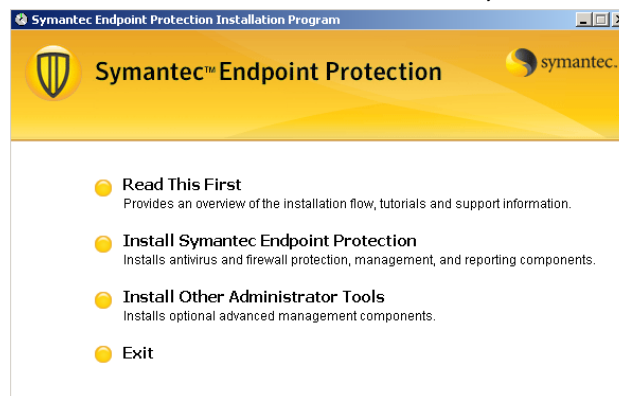
Stopping the SEPM Service

1. Stop SEPM Services on Policy Manager
 - a. Via services or the command line with:

C:\>net stop "Symantec Endpoint Protection Manager"

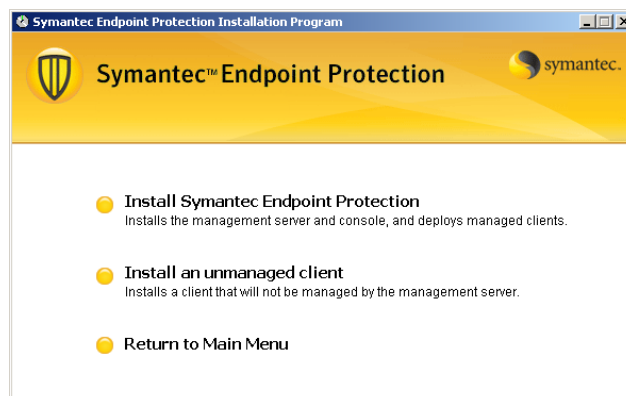
Upgrading the SEPM

1. Locate and run the 'setup.exe' located in the root folder of the DVD distribution
2. On the first welcome screen click "Install Symantec Endpoint Protection".

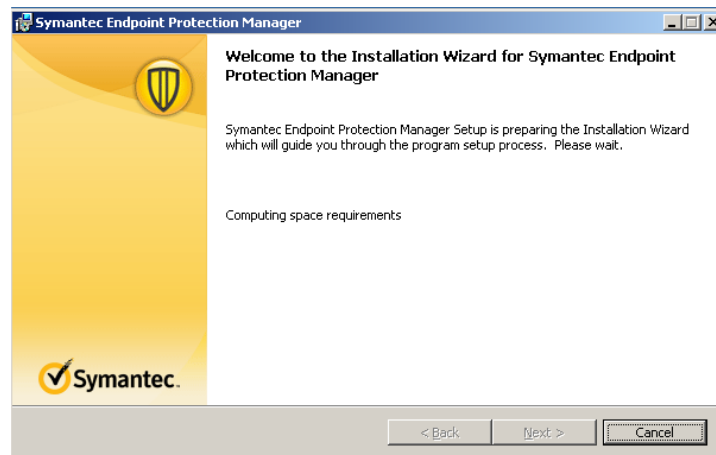


Note: Please Review the Release Notes included with the DVD via the 'Read This First' selection

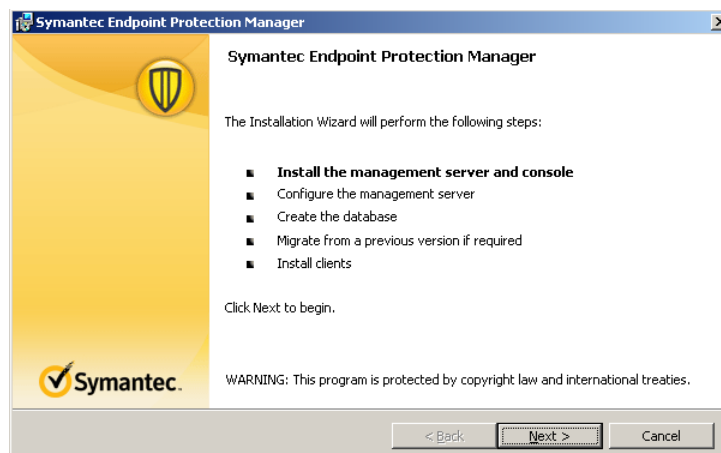
3. On the next screen click "Install Symantec Endpoint Protection" This will install the SEPM 12.1 software.



System Requirements will be checked.



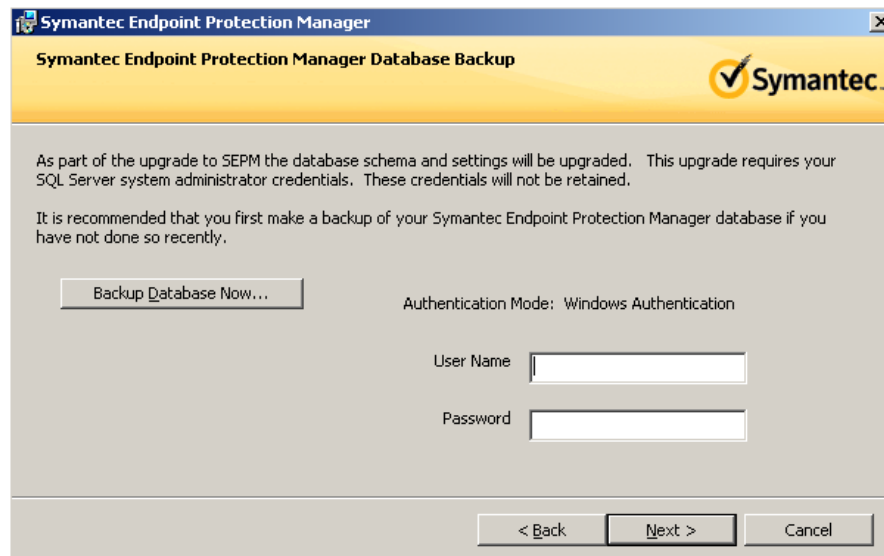
4. Click "Next"



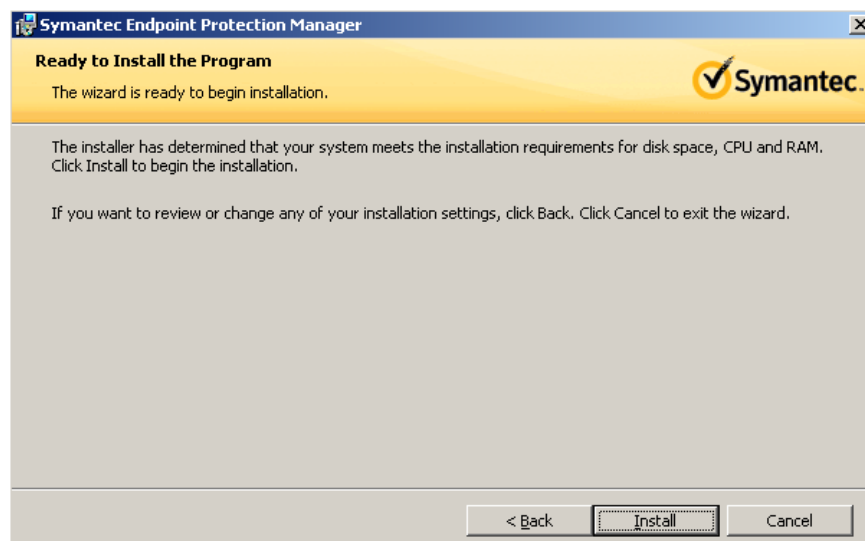
you then see the following read and confirm then click "Next" again



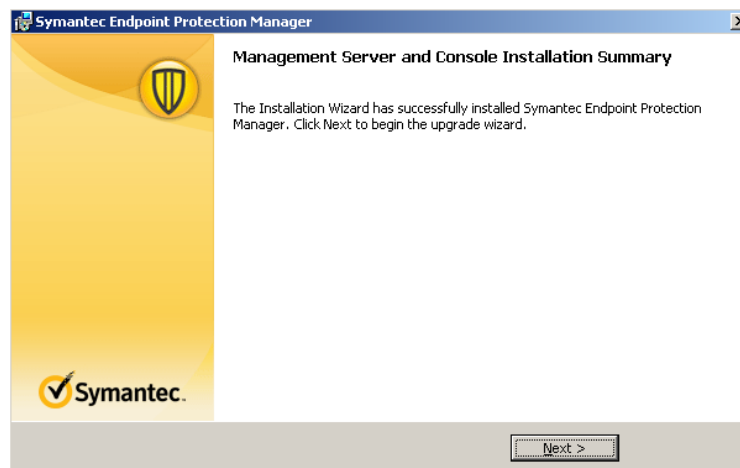
5. Select “I accept the terms in the license agreement” and click “Next.”
6. As mentioned earlier, you now have the opportunity to perform a ‘Database Backup’. Additionally you will need to enter the credentials of the database. Enter the credentials and click on ‘Next’.



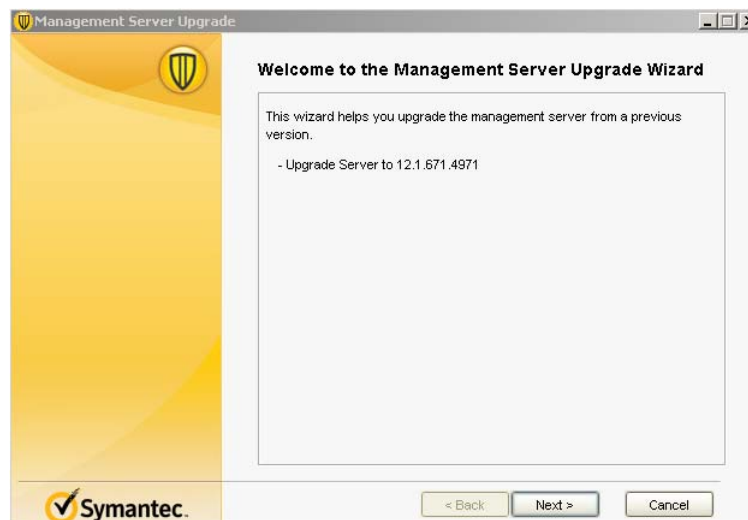
7. Checkpoint - When ready click on ‘Install’.



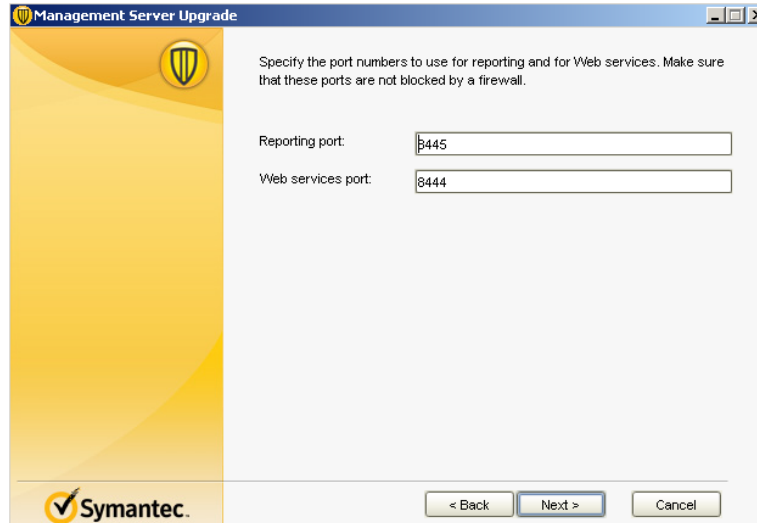
8. Click 'Next' to start the 'Upgrade Wizard'



9. Upgrade Wizard Start Screen Appears, click 'Next'

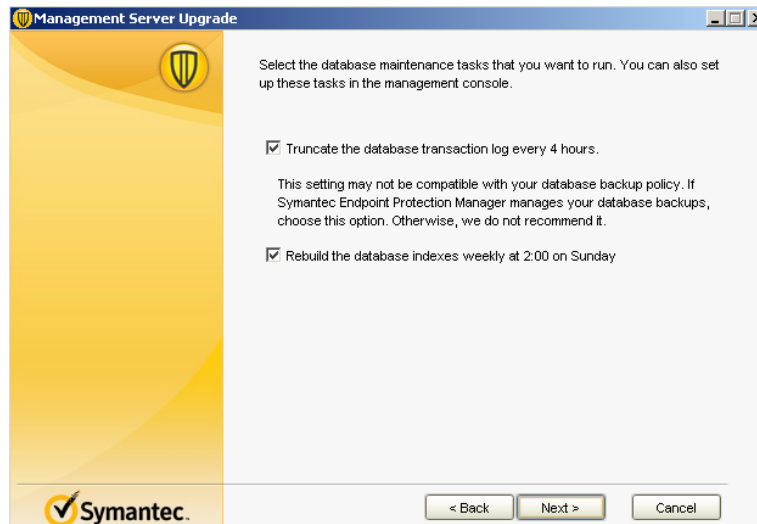


10. Reporting and Web Services Ports. Please review the documentation if you have any questions about these ports. If no changes are required click 'Next'



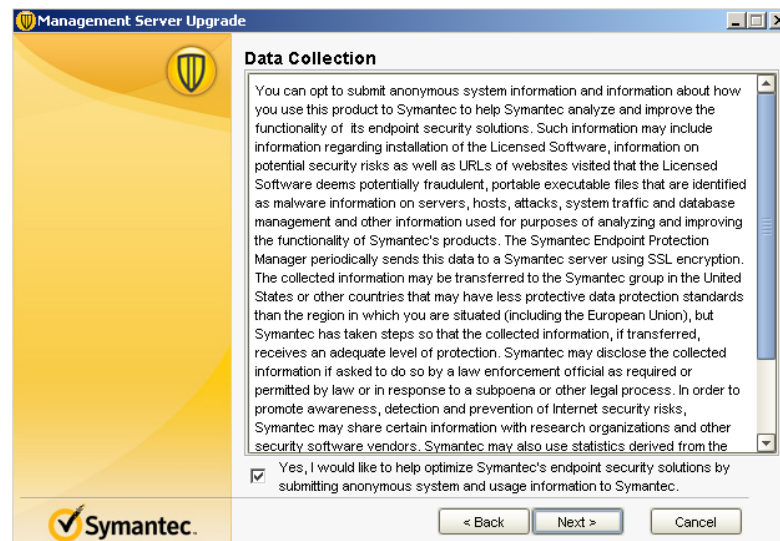
The dialog box is titled "Management Server Upgrade" and features the Symantec logo on the left. The main text reads: "Specify the port numbers to use for reporting and for Web services. Make sure that these ports are not blocked by a firewall." Below this, there are two input fields: "Reporting port:" with the value "8445" and "Web services port:" with the value "8444". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

11. Database Maintenance Options (New!) – An administrator can now have control over these database maintenance tasks. If the administrator wants to have their database team perform these tasks then uncheck these settings. If not certain about these you can change the settings within the SEPM console post migration. Click 'Next'.

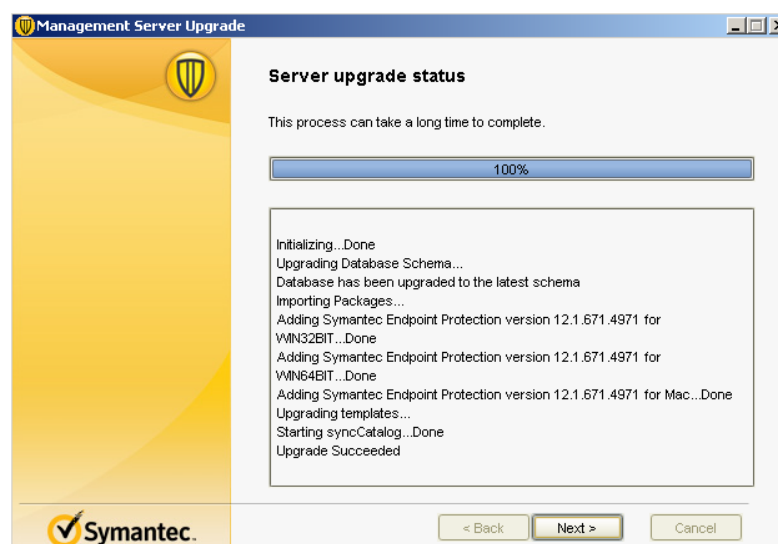


The dialog box is titled "Management Server Upgrade" and features the Symantec logo on the left. The main text reads: "Select the database maintenance tasks that you want to run. You can also set up these tasks in the management console." Below this, there are two checked options: "Truncate the database transaction log every 4 hours." and "Rebuild the database indexes weekly at 2:00 on Sunday". A note states: "This setting may not be compatible with your database backup policy. If Symantec Endpoint Protection Manager manages your database backups, choose this option. Otherwise, we do not recommend it." At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

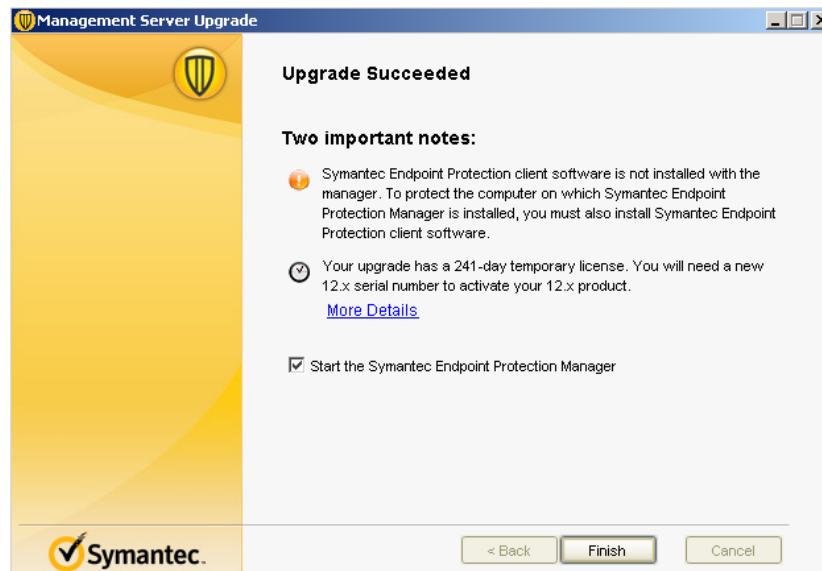
12. Data Collection - You can opt to submit anonymous system information and information about how you use this product to Symantec to help Symantec analyze and improve the functionality of its endpoint security solutions. Make your selection and click on 'Next'



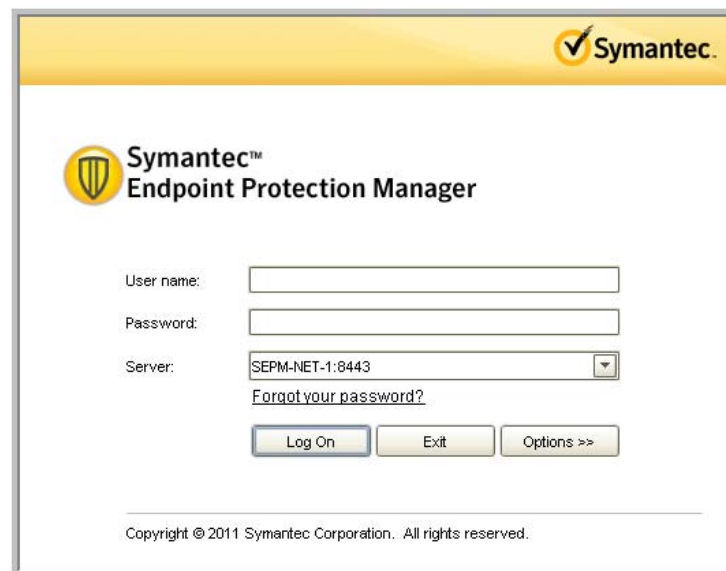
13. Server Upgrade Status. Note that the database schema has changed with this version of SEPM. Click on 'Next'



14. Upgrade Success – Please review the important notes, especially about your license period. Your license or SLF file can be imported from the main menu by selecting ‘Admin’ and then ‘Licenses’. Additional details on importing your license file can be found within the documentation. Click on ‘Finish’



15. Login Screen Presented



Note: SEPM Version 12.1 supports both 11.x and 12.1 clients. Have a migration plan of testing and implementation of the new 12.1 features that include a cross section of your client population.

Disable Local Authentication on Enforcers

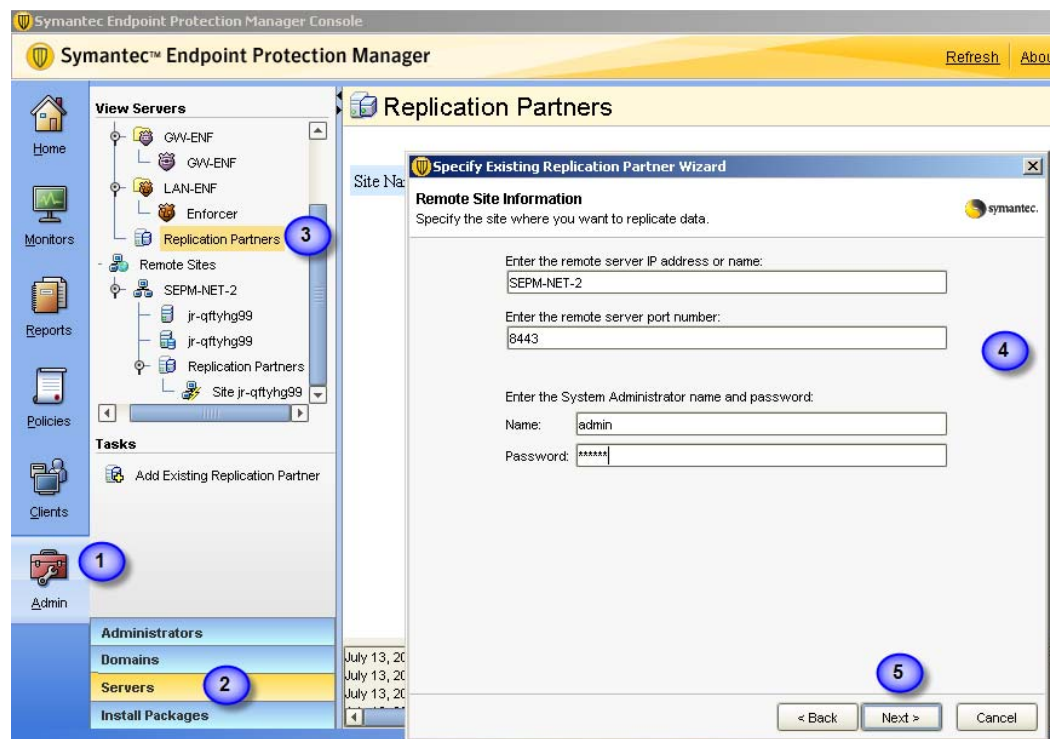
At this point assuming you have finished the steps above for the migration of the SEPMs in your environment. It is now time to re-enable the authentication mechanism on each of your Enforcers. See the command below for this function and refer to the Enforcer documentation if unsure you are able to perform this task.

- Command to Disable Local Authentication on the Enforcer
 - i. Enforcer(advanced) local-auth disable

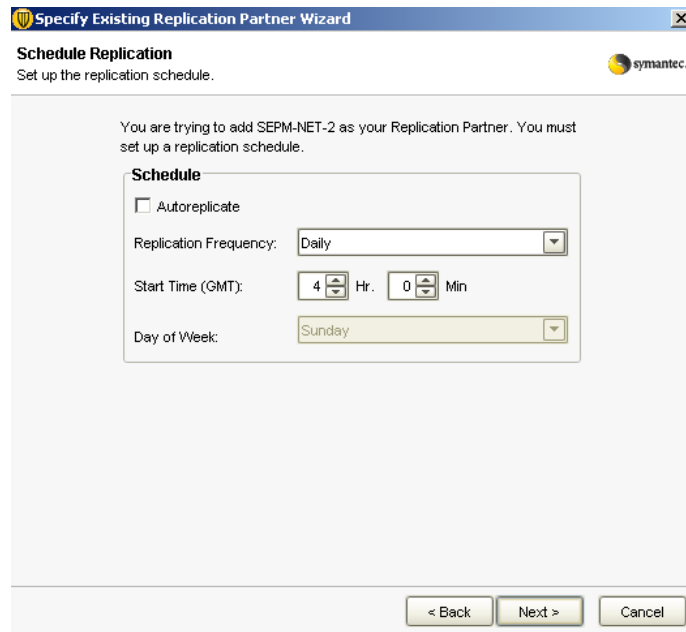
Enabling Replication

We've disabled replication for the migration process. The migration process is now complete so we must return and add our replication partners.

1. Login and click on the **Admin** Tab
2. Select Servers
3. Right Click and select 'Add Replication Partner'
4. Fill in the appropriate information
5. Click on 'Next'



6. Fill in scheduling information



Specify Existing Replication Partner Wizard

Schedule Replication
Set up the replication schedule.

You are trying to add SEPM-NET-2 as your Replication Partner. You must set up a replication schedule.

Schedule

☐ Autoreplicate

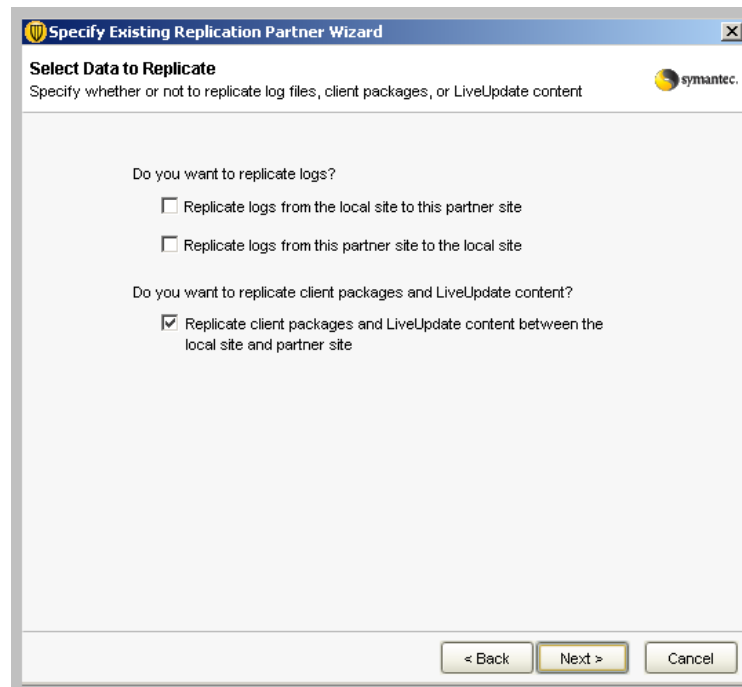
Replication Frequency: Daily

Start Time (GMT): 4 Hr. 0 Min

Day of Week: Sunday

< Back Next > Cancel

7. Select Data for Replication



Specify Existing Replication Partner Wizard

Select Data to Replicate
Specify whether or not to replicate log files, client packages, or LiveUpdate content

Do you want to replicate logs?

☐ Replicate logs from the local site to this partner site

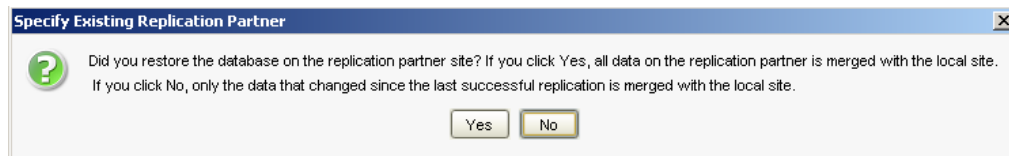
☐ Replicate logs from this partner site to the local site

Do you want to replicate client packages and LiveUpdate content?

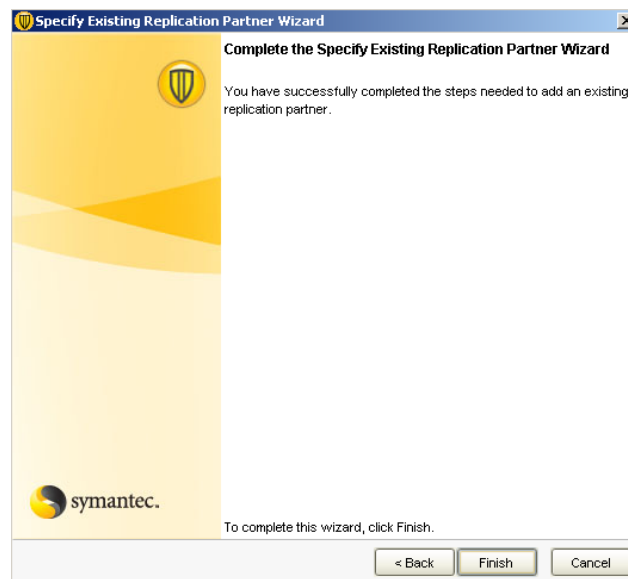
☒ Replicate client packages and LiveUpdate content between the local site and partner site

< Back Next > Cancel

8. You will then be prompted with the message below. Selecting 'No' will replicated only the delta from the last replication (recommended selection)

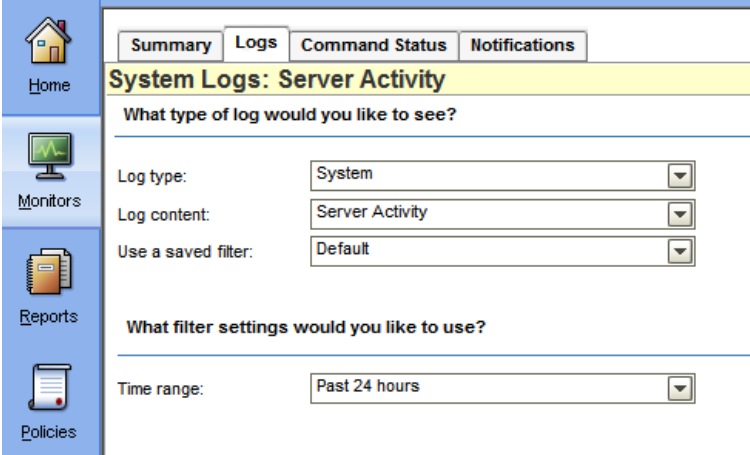


9. Click finish to complete



10. Verify Replication is successful. Depending on your individual situation you may want to wait for the schedule to activate a replication process or initiate a replication process 'on-demand'. The following screenshots show how to verify the status of replication.

The logs for the System/Server activity is where you should start. Click on Monitors and then select the 'Logs' tab.



Summary Logs Command Status Notifications

System Logs: Server Activity

What type of log would you like to see?

Log type: System

Log content: Server Activity

Use a saved filter: Default

What filter settings would you like to use?

Time range: Past 24 hours

Following this you should be able to view entries similar to the ones shown below.

 Export  Details					
Time	Event Type	Site	Server	Severity	Description
07/14/2011 10:29:58	Retrieval of local changed data for remote site finished successfully	Site jr-qfthyg99	SEPM-NET-1	Info	Retrieval of local changed data for replication requested by remote server 172.31.31.50 finished successfully!
07/14/2011 10:29:46	Retrieval of local changed data for remote site started	Site jr-qfthyg99	SEPM-NET-1	Info	Retrieval of local changed data for replication requested by remote server 172.31.31.50 started.
07/14/2011 10:29:45	Replication finished successfully	Site jr-qfthyg99	SEPM-NET-1	Info	Replication from remote site SEPM-NET-2 to local site Site jr-qfthyg99 finished successfully
07/14/2011 10:29:34	Replication data is received	Site jr-qfthyg99	SEPM-NET-1	Info	Replication data from remote site SEPM-NET-2 is received by local site Site jr-qfthyg99
07/14/2011 10:29:20	Certificate matched	Site jr-qfthyg99	SEPM-NET-1	Info	Got a valid Certificate.
07/14/2011 10:29:20	Replication from remote site started	Site jr-qfthyg99	SEPM-NET-1	Info	Replication from remote site SEPM-NET-2 to local site Site jr-qfthyg99 being initiated
07/14/2011 10:27:54	Certificate matched	Site jr-qfthyg99	SEPM-NET-1	Info	Got a valid Certificate.

Group Update Providers (GUPs)

Group update providers will continue to deliver content to 11.x clients. As a consequence of reporting into the newly migrated SEPM running 12.1, these GUPs are now capable of delivering 12.1 content as well. The GUPs will be updated as these clients are upgraded to 12.1.

Virtualized Environments

A Best Practice Whitepaper entitled “Best_Practices_v1.00.pdf” can be found at the following location.

https://symqforpartners.com/sites/sdrk/es/Service%20Offering%20Library/Supplement_SEP_Virtualization_Best_Practices_v1.00.pdf