Upgrading and Migrating to a SEP14.x Environment Using Replication

This document provides a detailed method using the SEP Configuration Wizard, with replication, to upgrade to the latest version of Symantec Endpoint Protection (SEP) and create an entirely new environment that is a duplicate of the previous environment.

**Important**
Actual client migration should take place as soon as possible after the SEP14 site has been successfully created. Depending on your environment size it may take several weeks to complete.

Make no changes to the Groups or Policies on either the old site or new site after the new site has been established. Doing so will cause issues when migrating clients because the old site and new site will be different after making changes.

The goals of the SEP upgrade in this document are listed below:

- Duplicate the existing production SEPM configurations in the upgraded 14.x SEPM environment.
- Certificates are automatically transferred to the 14.x SEPM.
- Existing Sylink.xml files are automatically updated across both environments to include the SEP14.x SEPM information.
- Duplicate all the policies of the existing production 12.x SEPM production environment in the upgraded 14.x SEPM environment, *without having to recreate them manually*.
- Migrate SEP clients seamlessly from the existing production 12.x SEPMs to the upgraded 14.x SEPM environment in a controlled process.
- The new upgraded 14.x SEP environment will be completely separate from the existing production environment when the entire upgrade process is complete.
- The previous existing production SEP 12.x environment will still exist and be able to manage SEP client versions not compatible with the SEP14.x environment.
OVERVIEW OF CREATING A NEW SEP14 ENVIRONMENT USING REPLICATION WITH AN EXISTING SEP12 ENVIRONMENT

**Important**

Replication between **SEP12 Site 2 & SEP12 Site 3** is broken after the **SEP12 Site 3** has been created.

**-DO NOT DELETE ANYTHING UNDER REMOTE SITES WHEN BREAKING REPLICATION-**

**MSL CONNECTIONS BETWEEN BOTH SEPM ENVIRONMENTS MUST BE MAINTAINED**

---

**Current SEP12.x Environment**

- **Site 1**
  - SEPM 1
  - (SEP12.1.RU6 MP8)

- **Site 2**
  - SEPM 2
  - (SEP12.1.RU6 MP8)

**New SEP14.x Environment**

- **Site 3**
  - SEP12.1-Temp SEP12
  - (Upgraded to SEP14.01 after created)

- **Site 4**
  - SEPM 2
  - (SEP14.x)

---

A temporary (SEP12.x Site 3) is created through replication with SEP12 Site 2.

Site 3 is now upgraded to SEP14.x.

Site 4 (SEP14.x) Created through Replication with Site 3.

---

All SEP12.x clients will be migrated to the New SEP14.x environment using MSL lists automatically generated during the replication site installations.
STEP 1
Beginning the Installation & Upgrade process of the SEP14 Site

The process starts with creating a new site with the same SEPM version currently in use in the SEP12.x Production Site (SEP will only replicate between the same SEP versions).

Replication is selected to create the database of this new site which will then become a SEP14.x version SEPM.

References in screen captures to port assignments are for example only. Use the port assignments that are in use in the current production environment. (Screen captures in this document are only to provide a visual idea of the process)

Start the SEP12.x SEPM install. When the Configuration Wizard portion of the install starts Select “Install an Additional Site” to be able to use replication with the old production environment to build the new environment’s site database.

![Management Server Configuration Wizard](image)

Once all configuration parameters have been competed the replication/site install will begin. Replication will create the new database which will be used for the SEP14.x Site. This may take a long time to complete because the entire SEP12.x production database is being replicated including content, install packages, policies, and logs.

Important: You must wait for the process to compete. At times it may appear to not be functioning. Do not attempt to monitor or interfere with this process.
Step 2

Breaking Replication between Sites

**WARNING:** It is important to understand that when breaking replication:
YOU MUST NOT DELETE ANY ENTRIES UNDER THE “REMOTE SITES” HEADING

The replication process automatically adds SEP14.x Site SEPM information to the MSL lists on all sites. To break replication and still maintain access between sites only do what is shown below.

*(Replication must be broken from sides (both partners)*

SEP14 Site- Delete Replication Partner Only as shown below.

**DO NOT Delete the Remote Sites.**

SEP12 Prod Site- Delete Replication Partner Only as shown below. **DO NOT Delete the Remote Sites.**

Once replication is broke you now have 2 separate SEP environments, however they can still communicate with each other. You are ready to upgrade the new site to SEP14.x.
Step 3
Upgrading the new site to version SEP14.x

Upgrade time is dependent on the size of the database. Content and install packages that have been transferred in creating the SEP14.x site database through replication will make the database full size.

Warning: Prior to upgrading to SEP14.x verify the new database does not contain any broken links or any other issues using the DBvalidator program located in the SEP Manager Tools folder. Once the database has passed verification you can proceed to upgrade.

How to use the Database Validation tool (DBValidator.bat)

Upgrading
Start the installation and it will default to “Upgrade the Management Server”.

The 1st SEP14.x SEPM has been upgraded and is complete.
Re-verify database is clean after the upgrade is complete with DBvalidator.
Adding additional SEPMs to the SEP14.x Site
Prior to adding each additional SEP14.x SEPM to the new SEP14.x Site, verify the database is still clean using the DBvalidator program located in the SEP Manager Tools folder.
Once the database has been verified you can proceed to add the next SEPM.
When all additional SEPMS have been added verify the database is clean with DBvalidator one last time prior to beginning the client migration.
SEP Client Migration Process

SEP Client Migration

*Client migration will take time for all SEP clients to obtain pre-migration policy changes*

1. The MSL lists will be used to perform the client migration. Both environments currently have the information required to perform the client migration from the SEP12.x Production site to the new SEP14.x site.
   
   **Do not remove the Remote Partners from either site until the migration is complete and has been verified.**

2. **Disable Secure Client Communications** across all groups in the SEP12.x Production environment and the SEP14.x new environment a minimum of 1 to 2 weeks prior to the SEP Client migration (this allows as many SEP clients as possible have time to receive the change). When it is determined that as many SEP clients as possible have migrated to the SEP14.x SEPM environment the **Secure Client Communications** can be re-enabled.

3. **Disable Tamper Protection** on all SEP clients in the SEP12.x Production environment and the SEP14.x new environment prior to the SEP Client migration. Disabling Tamper Protection will allow remote access by Technical Support personnel to correct any issues these SEP clients may have that is preventing them from moving to the new SEP14.x environment.

**SEP12.x Production Site Pre-Client Migration**

Disable **Secure Client Communications & Tamper Protection** from the highest level in your group structure.

If there are groups that have **Policy Inheritance Disabled** and have **Secure Communication & Tamper Protection ENABLED** – those groups will have to be configured individually to disable Secure Communications & Tamper Protection.

Check each client group to verify **Secure Communication & Tamper Protection** has been disabled.
All clients in the SEP12.x Production environment must have Secure Communication & Tamper Protection **DISABLED** prior to performing the migration.

See SEP12.x example below:

Example: Group Test 1 has Policy Inheritance Disabled

Select “General Settings” and verify all Groups and Sub-Groups have Secure Communications & Tamper Protection Disabled
Disabling Secure Client Communications in the SEP14.x Environment

Verify Groups & Sub-Groups have Secure Client Communication & Tamper Protection Disabled
How To Verify Secure Communications & Tamper Protection are Disabled on the SEP12.x Client

Verify Tamper Protection Is Disabled - Open SEP Client GUI and select “Change Settings”

Select “Client Management”

Verify Tamper Protection is disabled on the Tamper Protection tab
Verifying Client Secure Communications is disabled on a SEP12.x client

Locate the Sylink.xml file located here:

/ProgramData/Symantec/Symantec Endpoint Protection/[numbered SEP version]/Data/Config/

Open Sylink.xml file in your web browser by double-clicking it.

Check `VerifySignatures="0"`

Note the Sylink.xml references both the SEP12.x Production Site and the new SEP14.x Site

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServerSettings NameSpace="rpc" DomainId="51908FF0A7A1F220D20B3FDC67F331">
  <CommConf NameSpace="rpc">
    <AgentCommunicationSetting NameSpace="rpc" AllowClientUploadCriticalEventImmediately="1" RememberCurrentPolicyMode="1" RememberCurrentGroup="1" RandomizationEnabled="1" RandomizationRange="1800" DisableDownloadProfile="0" Kcs="AB05F6BCE19171B43C09E5C62DBF357" UploadCmdStateHeartbeatSeconds="1800" UploadOpStateHeartbeatSeconds="1800" UploadILogHeartbeatSeconds="300" ReconnectionMode="PULL" UploadLearnedApp="0" AlwaysConnect="3"/>
    <ServerList NameSpace="rpc" Name="Default Management server List for SEP12 Prod">
      <Server NameSpace="rpc" Name="Priority1">
        <ServerPriorityBlock NameSpace="rpc" Name="Priority1">
          <Server NameSpace="rpc" VerifySignatures="0" Address="1" />
          <Server NameSpace="rpc" VerifySignatures="0" Address="W2K8R2-Svr1" />
        </ServerPriorityBlock>
      </Server>
      <Server NameSpace="rpc" Name="Priority2">
        <ServerPriorityBlock NameSpace="rpc" Name="Priority2">
          <Server NameSpace="rpc" VerifySignatures="0" Address="W2K8R2-Svr2" />
        </ServerPriorityBlock>
      </Server>
    </ServerList>
  </CommConf>
</ServerSettings>
```

Note that both sites are listed in the sylink.xml above.
Client Migration with Management Server List (MSL)

The changes below are an example of what the MSL configuration will look like on both sites after replication. The only difference between them are which site SEPMs are the Priority 1.

SEP12.x Prod Site

SEP14.x Site

(Set as the Default MSLs through replication)

| Priority 1 | 10.122.31.34:8014 | SEP12.x SEPM |
| Priority 2 | 10.122.31.36:8014 | SEP14.x SEPM |

| Priority 1 | 10.122.31.35:8014 | SEP14.x SEPM |
| Priority 2 | 10.122.31.34:8014 | SEP12.x SEPM |

Adjusting the default MSL lists to make SEP12.x Production Site clients migrate to the SEP14.x Site

The SEP12.x Site MSL must have the **SEP14.x site in the Priority 1 position** and the **SEP12.x site in the Priority 2 position**.

*(this will allow SEP12.x client to move to the SEP14.x site, but still be able to access the SEP12.x site if the client is unable to register or the SEP14.x site does not respond)*

Modify the SEP12.x Production Site MSL List as shown below:

| Priority 1 | 10.122.31.35:8014 | SEP14.x SEPM |
| Priority 2 | 10.122.31.34:8014 | SEP12.x SEPM |

- To make SEP12.x clients that migrate successfully to SEP14.x remain there, the MSL list only contains the SEP14.x site information.

Modify the SEP14.x Production Site MSL List as shown below:

| Priority 1 | 10.122.31.35:8014 | SEP14.x SEPM |
| Priority 2 | 10.122.31.34:8014 | SEP14.x SEPM |
IMPORTANT

Both sites will have a large number of MSL lists. All MSL lists on both sites have to be reviewed to verify the SEP14.x SEPMs are the only site listed in the Priority 1 position when ready to start the migration. Adjust each Groups MSL list only when ready to migrate that group.

The migration should be performed in a controlled staged manner – group by group – to allow time to manage any issues that may be encountered and to limit over loading resources on the both sites.

“Assign” the SEP14.x Site MSL to a specific Group or Groups on the SEP12.x site to control and monitor the migration flow.

The example below is only migrating the “Test 1” Group.
Verifying Clients have migrated.

Prior to migrating, the clients in the SEP12.x Production Group “Test 1” are displayed on the SEP12 Site .x Site as “Online”, but in the SEP14.x as “On the Remote Site”.

After the client heartbeats in, updates its policy and moves it will display as “Online” on the SEP14.x Site. Refresh the site page to see the changes. It may take several minutes for the change to take place depending on your SEP client Heartbeat setting.
After a SEP client migrates to the SEP14.x Site it will display as “Offline” on the SEP12.x Production Site.

The migration should be performed in a controlled staged manner – group by group – to allow time to manage any issues that may be encountered and to limit over loading resources on the both sites.

Any clients that are unable to rejoin their previous group may/will migrate to the Default Group.

Clients that do not receive the updated policy to move (MSL) will have to be investigated separately.

**Note:**
Use the “How to Verify Secure Communications & Tamper Protection are Disabled on the SEP Client” section above to determine if the changes in policy updated the client.
Client Migration is Complete

When the client migration is determined to be complete and as many clients as possible have migrated the Remote Partners can be deleted. This will completely separate the SEP12.x site from the SEP14.x Site.

SEP14.x Site

From the “Servers” tab on the SEP14.x site highlight the “Remote Site” and delete the remote SEP12.x site.

The MSL used for the client migration should be deleted automatically but verify it has been removed.

The MSL in use on the SEP14.x site should now only contain the SEP14.x Site information and the clients will no longer be aware of the SEP12.x Site. Verify the MSL changes.
SEP12 Site

Prior to removing the Remote Site, assign a new MSL list to all groups that does not contain any references to the SEP14.x Site.

Delete the Remote Site

The sites are now separate and the SEP clients belong to the SEP14.x Site.

Verify all MSL lists on the SEP14.x Site for accuracy.