Considerations Prior to Upgrading & Migrating to a SEPM 14.x Environment

1. Firewall access on the default TCP Port 8443 and 8014 is required to allow SEP Manager Communication between the SEP12 Production Site and the new SEP14 Site. Please check your own environment for which ports are in use.

2. Firewall access on TCP 1443 between the new SEP14 Site and the SQL Server that will be used to hold the SEP14 database.

3. The SEP14.x upgrade using replication may take several hours due to the size of the existing SEP12 Site database. Determining when to upgrade is important. Determine the lowest activity time period of the SEP12 Production Site to perform the upgrade process to SEP14 - Avoid the 12AM to 1AM time period which is when the system purges older data. If unavoidable, start the upgrade process at 1:30am when the purge is finished. Also, modify the SEP12 Production Site SEPM Liveupdate download schedule so it will not attempt any downloads during the replication phase of the SEP14 upgrade. (Liveupdate may/can break a replication process.

4. Copy the SEP14 installation package to every server that will become a SEP14 SEPM prior to starting.

5. SEP 14 requires “sa” logon account access to the SQL Server. Have access to the SQL Server “sa” logon and password or arrange for an SQL administrator to join and be part of the entire SEP14 upgrade process to enter SQL logons and passwords for you that may/will be required.

6. Permissions issues are the #1 cause of SEPM/SEP install failures that significantly increase the time required to complete the upgrade process.

   Complete access to the actual servers that will be used to create the SEP14 SEPMs is required. Due to the fact that Domain Administrator accounts may/will have additional GPO restrictions that can cause installation failures, Symantec strongly recommends that the person performing the upgrade process have access to the servers Local Administrator account and use it to perform the installations.

   If that is not possible, then a temporary user account should be created directly on these servers with membership to only the Local Administrators Group (do not add the USERS membership) and that account be used to perform the installations.

   When the installation is complete these temporary accounts are no longer required and can be removed.

7. Symantec recommends that during installations & upgrades that the SEPM “admin” account be used to logon to a SEPM. This SEPM account always has the highest privileges on a SEPM.

8. If SEPM servers have a logon time out due to inactivity it needs to be disabled prior to beginning the upgrade process.