McAfee® Endpoint Encryption Enterprise Best Practices Guide

November 2009

Contents

Introduction

Purpose of this Guide

When planning a large rollout of Endpoint Encryption v5, it is important to understand the process of scaling the back end Object Directory and the associated Endpoint Encryption Communications Server processes to meet requirements. This guide outlines the considerations around Endpoint Encryption 5 implementation and suggests possible solutions.

The guide also discusses considerations on optimization and maintenance before and after its implementation.

It also assumes the reader has some knowledge of enterprise systems (configuration and management) and some knowledge of Endpoint Encryption components (Endpoint Encryption Manager v5.x, Endpoint Encryption for PC v5.x and other McAfee Endpoint Encryption components) that will benefit from good practice and Object Directory optimization (see below).

This guide is a collation of the professional opinions of Endpoint Encryption certified engineers, and not the exact science. Because every implementation is unique, it is critical to understand both the product and the environment in which it is being used, before arriving at any decision on implementation strategy. Calculations and figures in this guide are based on field evidence and not theoretical system testing and are our "best advice" at the time of writing.

We recommend you to discuss your requirements with your McAfee representative. McAfee has wide experience in deploying real world implementations.

Thanks to all the authors who have contributed towards this guide.

Relevant Products

This guide discusses configuration and maintenance of the back end server components, Endpoint Encryption Manager v5.x and its Object Directory together, which manage and govern the following version 5 client components of Endpoint Encryption:

- Endpoint Encryption for PC (EEPC)
- Endpoint Encryption for Files and Folders (EEFF)
- Endpoint Encryption for Mobile (EEMO)
- Endpoint Encryption for Removable Media (EERM)

Other components that may benefit indirectly:

- Endpoint Encryption Scripting Tool
- Endpoint Encryption Reporting Tool
- Endpoint Encryption Object Directory Backup

However, the vast majority of the guide is concerned with Endpoint Encryption for PC as optimizations of the Manager and Object Directory will make the most impact on this component.

Solution Architecture

Design Philosophy

McAfee Endpoint Encryption is a client/server application designed to be implemented with a simple, single server architecture. This single server hosts an encrypted database known as the Object Directory, and runs services to allow connections to the database from both the Encrypted Endpoints and the Management Center applications. Communication with the database occurs in a secure way (detailed descriptions are provided in the Management Center Administration Guide). This single server can host all components of the Management Center, even in enterprise environments.

While it is most common to implement the product with a single server, there are also other options. The components are modular and are installed in a distributed way. For example, the Web Helpdesk component can be installed on a dedicated web server while the rest of the components are on a separate Endpoint Encryption Server. However, the majority of our implementations are done with a single server because this is usually the best approach.

NOTE: This guide has all recommendations, assuming a single server approach.

When reading the following sections - even though our recommendation may be to use a single server with Direct Attached Storage (DAS), a virtual server with NAS based storage is usable and will have some advantages in your environment for small numbers of endpoints or with limited sync events and limited users per client. However, we advise against using such implementations and recommend you discuss your requirements with McAfee before implementation.

If the performance of the McAfee solution is below the acceptable limits, migrating towards our recommendations is sure to lend improvement.

Server Configuration

Basic Server Requirements

The Endpoint Encryption Communications Server process runs under Microsoft Windows 2000/2003. Currently some customers report that it works well under Windows 2008, however McAfee has not officially certified this. Please see the McAfee KnowledgeBase article KB53698 for current information on supported environments.

The performance required depends primarily upon the number of concurrent connections an enterprise can experience and the number of concurrent object creation events. Real world implementations suggest the following minimum and recommended configurations.

Note the term "Object Directory" used throughout this guide refers to the database or store for users, endpoints and other settings, and files for Endpoint Encryption management.

Recommended Server Hardware	
20-2000 users/systems Minimum single server configuration • Dedicated Server • 2 GHz Dual core processor • 2 GB Ram • 4 GB free hard disk, RAID1 • 100 Mb Network *Virtual or Shared Server can be used for low numbers. Please see Virtual Server section in this guide.* ***Virtual hardware has to be of higher specification if resources are shared. See Page 11.***	2000-5000 users/systems Recommended single server configuration • Dedicated Server • 2.4 GHz 2 Dual or 1 Quad core processor • 4 GB Ram • 4 GB free hard disk, RAID5 • 100 Mb Network
5000-50,000 users/systems Recommended single server configuration • Dedicated Server • 3 GHz 2 Dual / 1 Quad core processor • 4 GB RAM • RAID5 10 K RPM Direct-attached Storage, 100 GB • Gigabit or 3x 100 Mb Network	50,000-150,000 users/systems Recommended single server configuration • Dedicated Server • 3.0 GHz or higher 2 Quad / 4 Dual core (8 cores). • 6 GB RAM • RAID5 Direct-attached Storage. 15 K RPM. 250 GB • Gigabit or 4x 100Mb Network
Mentioned RAID refers to hardware RAID, not software. Enable caching on RAID if possible, but ensure suitable UPS power is available. Migrating an environment between hardware platforms is simple so it is possible to start with a minimal configuration and later extend it to a higher configuration in accordance with performance monitoring and capacity planning. **NOTE**: These may vary depending on other configuration settings.	

Server Redundancy

It is risky to have a single physical server for your enterprise, even if you take regular backups. We recommend you to take steps to expedite recovery from an outage in accordance with an established Business Continuity and Disaster Recovery (BCDR) plan.

Hot Backup Databases

Increase the redundancy of the system by replicating the Endpoint Encryption Object Directory to a second physical server. A dedicated replication tool "Object Directory Backup" which is optimized to follow the change log of an Endpoint Encryption v5 Object Directory is supplied with the product suite.

In this case set up a resilient system using two physical boxes, both hosting Endpoint Encryption Servers – one hosting the master ODB and the other having a hot backup. In case the master server fails, the Endpoint Encryption Server on the second backup box can be restarted in "master" mode. Then rebuild or replace the affected machine and create a new master.

The ODB Backup utility can also be used to make regular backups of the ODB, giving further recovery options in case of a disaster. This method however, requires manual interaction to start the failover.

A HotBackup document discussing this scenario is available.

Clustering

Fully automated failovers for applications usually employ a cluster server environment. Although the McAfee Endpoint Encryption Object Directory and Manager can run on a cluster, we recommend against using 'shared' resources where possible. As per McAfee KB53698, Windows Cluster environment has not been fully tested at this time in engineering.

Load Balancing

Given the best configuration is usually a single high performance server with DAS then the least optimal way to perform clustering is to put the Object Directory on a network share (NAS) and then install the Management Center on two servers which access the share simultaneously.

NOTE: The latter will function, but it will be significantly detrimental to server performance.

You should note that if you use special load balancing switches to split network load, you should set them to allow each client active connection to occur with the same switch throughout the sync event (and not split/distribute each packet during a single sync).

Making remote connections to the database is slower than local connections, so this design is often too slow to work effectively.

If DAS is not used and there are issues such as performance, object corruption (especially as object numbers in the McAfee Endpoint Encryption Object Directory increase) McAfee support will recommend moving to DAS and high performance dedicated server.

If a SAN is the only option available, please note SAN arrays can prioritize the connections to the physical box in what is known as Tier levels. Tier 1 is the highest priority, Tier 3 is the lowest. McAfee Endpoint Encryption needs optimal disk access so would need Tier 1 priority with dedicated LUNS to provide the highest speed connection. This is necessary for full and prompt service synchronization requests and administration. This avoids corrupted databases, objects, clients and slow administration performance. Running on SAN is not recommended, but if it must be done, then the connection must be Tier 1.

Server and Object Directory Optimisation

Endpoint to Server Communication - Network Load Estimation

Endpoint Encryption network traffic is the easiest to consider in terms of “synchronization events”. Each time a system starts it tries to connect to a designated EEPC database communication server and update its profile. It may also (depending upon configuration) try to connect periodically. In large deployments, the first step in estimating the network load caused by Endpoint Encryption is to estimate the peak number of concurrent synchronization events. This is related to the user working practices. For example, if 2000 users switch their systems on at 9 A.M, the “9 A.M.” effect can be diluted by setting optional boot sync delay and offset times to spread the load across, for example one hour.

Once peak flow is estimated, double it to give some safety, then work on an estimate of 7 KB per user per sync (this is a very high approximation based on total update of the user every two sync events). A typical Windows server, in our experience, can accept 100 connections per second per server, with a default maximum wait time of 30 seconds for pending connections.

The maximum capability of a single Communications Server, taking the capacity of the network to be 100 Mbps (1 million bits per second) is 20 synchronizations of data a second. A Windows server OS can establish connections about every 10ms, and can handle unlimited connections (although eventually it will run out of clock cycles and memory).

Once established, a connection can take an unlimited amount of time to finish, though the default timeout on establishing a connection is 30 seconds. If there are more than 100 attempted connections per second, the queue cannot be longer than 3,000 connections.

The default settings of the Communication Server limit the queue to 200 entries (a balance between taking connections and processing connections). After that point, the connections are refused. This is a reasonable “real world” setting. As long as the profile of the system is set to retry the connection after, for example, four hours, there is no loss of function. Setting the queue length to more than 1500 can result in poor performance from the server as it tries to service so many connections.

In real terms we can say that as a general maximum case, the Endpoint Encryption Server is limited to 100 connections per second, with a sustained load. Saturation in our experience is reached when there is more than 1400 synchronization events per minute (1200 accepted and processed, 200 queued). Achieving this load in the real world requires a massive, badly planned and configured population of systems. Current customers with 40000 + installations rarely exceed the 200 current connection points, most of which are administrators performing configuration changes.

The operating system or disk controller caches most of Endpoint Encryption’s database, so eventually the common files will be supplied from RAM rather than across the connection to the database host, or, from disk. Using the compressed version of the database can improve performance by a small amount, however, it is useful when corporate backup software has difficulty archiving the database.

This rough calculation tells us that we need one Endpoint Encryption Server per 1400 events a minute minimum; however, experiencing the system in action will give true feedback. It is often the case that modern hardware outperforms paper estimations.

Estimating the Size of the Object Directory

The base size of an Endpoint Encryption 5.x Object Directory is around 150 MB. Because you add new users and systems, the ODB grows accordingly. It also grows in size as systems synchronize and upload audit information.

An Object Directory with 5000 users and 5000 systems could be expected to grow as follows:

Typical Growth of 5000 user/machine Object Directory		
Day	**Data Size**	**Approx Disk Space Used**
1	83 MB	143 MB
5	89 MB	143 MB
20	204 MB	403 MB
50	396 MB	745 MB
100	747 MB	1050 MB
365	2455 MB	3900 MB

Users and systems are the most prevalent object types in a large database. Typically, on creation, these types of objects take 4000 bytes. A day's audit adds around an additional 700 bytes of data per object. Although these figures are very small, because of wasted space on the Object Directory Server's hard disk, the actual disk size occupied by the Object Directory can be 4x or more larger.

Virtual Servers

McAfee Endpoint Encryption Manager can be run from a Virtual Server for lower numbers of Endpoints. McAfee recommends physically dedicated hardware for high numbers of Endpoints.

Performance of virtual systems is dependent on many factors that can significantly affect the overall product performance when compared to physically dedicated hardware. High-speed access to the data within the Object Directory is required and must be carefully considered and evaluated in a Virtual Server Environment.

Current testing of Virtual Servers running EEPC operates within a set numbers of database objects. McAfee's experience shows that performances issue arising from the use of Virtual Servers is a result of:

- Lack of resources dedicated to the virtual server.
- Dynamically assigned resources to the virtual server which starves it of the necessary performance during peak periods.
- Slow or reduced disk access, resulting in a slower access to the Object Directory.

McAfee supports the use of Virtual Servers running the administrative functionality of EEPC provided the appropriate resources are fully dedicated to the Virtual Server at all times. If performance problems are experienced, the resources available to the Virtual Server need to be increased. Please refer to the recommended server specifications as the minimum resources fully assigned to the Virtual Server at all times. These resources apply to the specific image, and not to the overall resources of the host.
Customers need to follow the recommendations of McAfee Support and raise a support ticket for the issues related to a Virtual Server. These recommendations can vary from tweaking of server and machine settings as specified in this guide all the way to moving the EEPC management environment to physical hardware as a last resort if necessary.

By engaging McAfee professional services, they will assist you in adequately scoping your deployment hardware needs and can recommend a best practices approach.

As the technology is evolving and better VM farms are coming online, virtual hardware support for greater numbers should be possible. Please see McAfee KB 65747 for more information.

This will be reviewed for the next major release (version 6.0 ePO integrated).

Global Deployments

The single server approach works well as long as the endpoints can make and sustain a TCP/IP connection to the server. Depending on the quality of the WAN link, some global deployments will require multiple servers. Each of these is essentially its own environment, with its own Object Directory. Many customers have one server in each region: one for North America, one for Europe and Africa, and one for Asia. To determine, if this multi server strategy is necessary, it is better to include endpoints from all regions in the pilot phase.

Optimisation Actions

NOTE: These are generic recommendations based on experience but not always be suitable for your entire specific environment. For database maintenance and performance, it is always recommended you engage McAfee professional services prior to implementing these suggestions.

The Object Directory is small in size, but contains a high number of files. For example, a typical 10,000 node deployment has 1.7 million files in its Object Directory. For optimal performance, we must configure the operating system and the hardware to provide fast access to lots of small files.

Optimisation Actions Overview

McAfee generally recommends the following actions (*most of which are described in more detail later*):

• Optimize hard disks for I/O performance. As above, 15 K RPM disks are the best. The disks should be in a RAID 5 array with a controller, with the maximum amount of cache available. UPS backup is recommended. See chapters above.

• Use DAS rather than a network location SAN/NAS. See chapters above.

• Enable indexing of the Object Directory with dbcfg.ini.

• Keep number of objects per group to a minimum within the object directory and minimize number of users assigned to clients. Also less aggressive sync policy for clients can ease server load.

• Reduce the TCP/IP KeepAliveTime to five minutes.

• Disable NTFS Last Access Update with a registry change.

• Increase the size of the NTFS Master File Table (MFT) with a registry change.

• Optimize backups.

• Exclude the Object Directory and the associated services from virus scans.

• Set Windows server performances settings to background services and system cache.

• Manage Audits.

• Use Hard Drive controller caching.

• Use good network connections to Object Directory servers.

• Store the Object Directory (usually stored in SBDATA folder) on a separate drive or partition to the OS.

• Don’t allow the database to be shared.

• Check that every administrator goes through the EEPC Database server, not direct through local connection.

• Limit the use of the ‘Find’ function in 20K+ databases during normal working hours as it can slow access.

• Clear object items from deleted items, regularly when not needed.

• Increase max connections in SBServer.ini (in some cases).

Name Indexing (DBCFG.INI)

Name indexing should be enabled on all databases especially those with over 1000 endpoints or users. It will be noticeably faster and improve performance.

To do this, create a basic text file called DBCFG.INI; file and copy it to the SBDATA folder (assuming default location for Object Directory) and edit as below:

Warnings

- Do not use Single File mode as shown in the options below. It can be used for small databases but not recommended as it can be much slower.
- The Find function does not use the name cache and therefore searches the complete database sequentially.

DBCFG.INI

Sections are added defined by [] with the options in each section added as below.

[NameIndex]

Enabled=Yes

This must be set to "Yes" for the name index/caching to be used by programs running for this directory.

LockTimeout=3000

This option controls how long the process will retry access to the index file if it is locked. You can decrease this value if the administrator experiences long waiting times during installation, for example – 1000, however, only in databases smaller than 5000 systems, otherwise you find the number by multiplying the number of users or systems in the database by 0.6.

Example: If the number of users in the database is 10,000, the Locktimeout should be 6000.
The default value is 3000.
The value is in 100ths of a second.
In case of multiple servers, the timeout can exceed due to many simultaneous connections. In that case the value needs to be increased to 30000.

LockSleep=10

This option controls how long the process will sleep (wait) before re-trying opening a locked file. The value is in 1000ths of a second. In case of multiple servers, the locksleep might need to be increased due to many lock timeouts. In that case the value needs to be increased to 100 or even 1000.

HashCount=16

This option controls how many "buckets" the hash of the name is split into. It should be between 1 and 256 (default 16). Generally, a good value can be calculated by taking the square root of the number of users. However, for optimal performance this value should be tuned by testing.

MinEntrySize=16

This is the minimum space to allocate per object name in the index file. The default of 16 is a good value if the names do not exceed 16 characters. You do not need to specify the value if the names do not exceed 16 characters.

LifeTime=86400

The time (in seconds) for which the index will be used before it is automatically re-created if somebody logs on to the database. The default is 30 minutes but is never recommended. A value of zero means that it never expires automatically, and the value of 86400 means one day.

A value of zero gives you full control but this setting needs a separate process to recreate the index. This could be a simple batch file that runs overnight - removes the index files and forces a recreate. This can sometimes produce the best result and performance.

Recreation of the index files will take performance. It will cause the logon to be delayed for quite some time dependant on database size and performance, and can cause issues if the creation of systems occurs during this rebuild time. Therefore, depending on the size of the database, it is recommended this process is set to run very early in the morning. For example, remove name* files in SBDATA 00000001 and 00000002 folders especially through a script early morning 2 A.M. Following that, run an admin logon using the command line tool (SBADMCL) and perform a command such as **getcounts** through script to rebuild the cache early, before the systems synchronize.

You can use a batch files for this, one example is called RecreateCache.bat. Examples of scripts are in the optional EEPC Tools download, or, available from your McAfee representative.

[Attribs]

SingleFile=No

If this is set to Yes, the attributes for objects will be placed into a single file instead of each one having their own file. Not generally used although it simplifies and speeds up backup, this will make the database twice as slow!

AutoConvert=No

If this is set to Yes and SingleFile is also set to Yes, then attributes are automatically converted to a single file when the object is opened for writing. Otherwise, only new objects will have their attributes in a single file. **NOTE**: Attributes are not converted until they are opened for writing. Again, this can produce fewer files per object to aid backups but is slightly less resilient to failure.

[Tracking]

ObjectChanges=No

Object change tracking for the backup tool might decrease the performance of the database by about 100% thus it is not recommended to use this in big environments.

Group sizes

The size of a user group or systems group should not be too big. A user group of 5000 can take 20 seconds or more to open even on a fast server. We recommend keeping the size under 2000. Optimally 1000 or less will work well in many cases for faster access to groups on any server.

Also assigning large group of users directly to a client can have performance implications (network/server performance, slow client boot up and sync times and installation processes) so smaller groups are better. Users can be assigned individually too. The fewer users assigned the better from a security perspective. See *User Objects – General Performance Tips* section later.

TCP/IP KeepAliveTime Reduction

Reduce this setting on all EEPC servers from two hours (the default) to five minutes. The server will require a restart. Once this is done, if an endpoint client loses the connection with the server, the server will release the lock after approximately 5 minutes. This will also prevent broken remote sbadmcl connections from locking the scripting user account for 2 hours.

Procedure

1. Open **Regedit**
2. Go to: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters**
3. Open or create the **Dword KeepAliveTime**
4. Change the value to **300000** in decimals (Time in milliseconds)

Extra info

The **KeepAliveTime** setting controls how often keep-alive packets are sent in milliseconds (300,000 is recommended). It controls how often TCP sends a keep-alive packet to verify that an idle connection is still intact. If the remote computer is still reachable, it acknowledges the keep-alive packet.
MS KB article: http://support.microsoft.com/default.aspx?scid=kb;en-us;324270#EQACAAA

Key: Tcpip\Parameters
Value Type: REG_DWORD (Time in milliseconds)
Valid Range: 1-0xFFFFFFFF
Default: 7,200,000 (two hours)

NOTE: A similar setting KeepAliveInterval has a default 1000 (= 1 second), this setting is correct so do not change this.

Last Access Time Stamp (NtfsDisableLastAccessUpdate)

With large databases, it is possible that some groups may become overpopulated. When a large group is opened (for example one with over 5000 users), it can take some time to open. To reduce hard disk read and write time, a registry setting can be set to prevent the Last Access time stamp from being updated on every file access. The performance boost will be about 50%! A restart is needed after the change.

Procedure

1. Open **regedit.**
2. Go to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem.**
3. Create a new DWORD value, or modify the existing value, named "**NtfsDisableLastAccessUpdate**" and set it to "**1**".

Microsoft article: http://technet2.microsoft.com/WindowsServer/en/library/80dc5066-7f13-4ac3-8da8-48ebd60b44471033.mspx?mfr=true

Windows Server as a File Server

Tune Microsoft Windows 2003 server to be a file server.
See the Microsoft article http://support.microsoft.com/kb/174619 about this.

Theory

Increase NTFS MFT (Master File Table, used to be FAT) to 50% of the disk space. The result is that small files are being stored in the MFT and not as separate files in the NTFS. This helps a lot because we have thousands of small files.
Procedure

1. Open **Regedit**.
2. Go to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem**.
3. In the right pane, look for the Dword named **NtfsMftZoneReservation.**
4. If exists change the Dword to **4.**
5. If not exists, create a new DWORD **NtfsMftZoneReservation** in the registry and set its value to **4.**

EXTRA INFO

The default value for this key is **1**. This is good for a drive that will contain relatively a few large files. Other options include:

2—Medium file allocation
3—Larger file allocation
4—Maximum file allocation

Unfortunately, Microsoft doesn't give any clear guidelines as to what distinguishes Medium from Larger and Maximum levels of files. Suffice it to say, if you plan to store lots of files on your workstation, you may want to consider a value of **3** or **4** instead of the default value of **1**.

Object Directory Backup Tool Setup

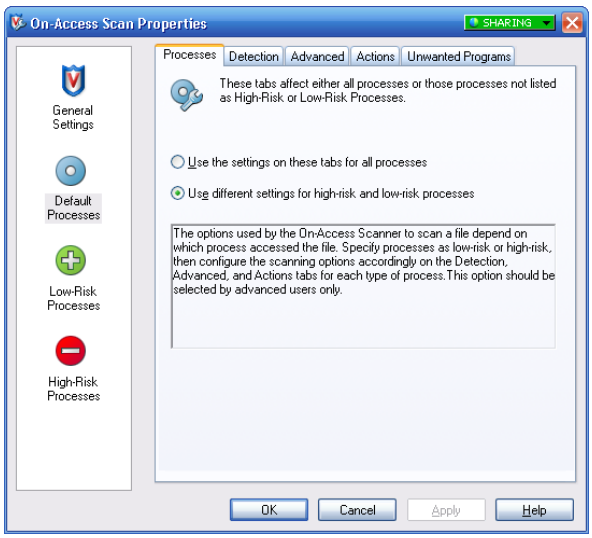
If you set up your Object Directory backup tool, make sure it is not running too many times a day because the in between time will be too short. This will cause the tool to run constantly causing overload. Do not use the object change tracker in big database. It will decrease the database speed about 100%!

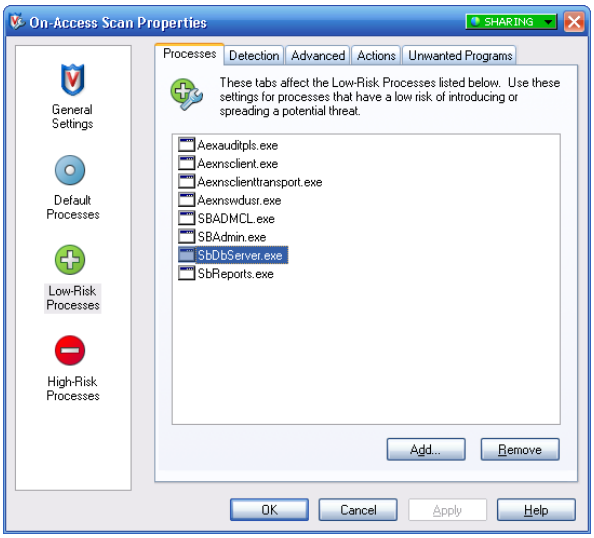
Anti-Virus Scanner

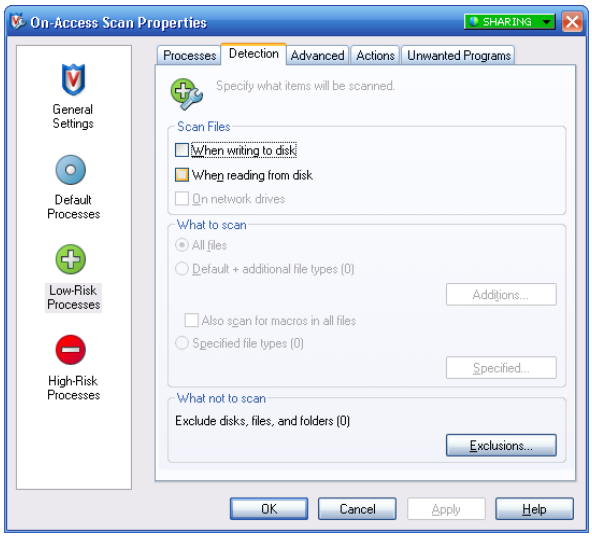
It is not necessary to use a virus scanner on the database (SBDATA). Most of the data is encrypted, so there is nothing to be scanned and scanning will reduce much of the performance. Switch off any scanning of the SBDATA on the EEPC Database server. Also, exclude the SbDbServer executable from scanning.

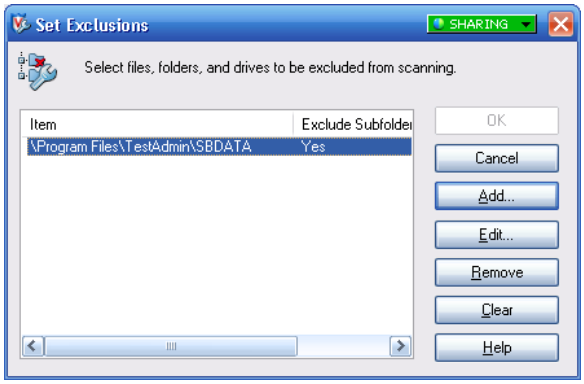
Also if your Anti Virus program has high-risk/low-risk process detection marking all the EEM/EEPC main executables on the server as low risk and disable scanning on reads / writes may help further (see screen shots).

Example setup using McAfee VSE 8.5:









Windows Performance

By default the Windows performance settings are set to 'Applications'. However, testing should define the best setting. The recommended settings under Control Panel, System, Advanced, performance are:

- Let Windows choose what's best for my computer

Under Advanced:

- Background services
- System cache

Opening a test group with more than the recommended number of objects (for example 5000) can be a good test using the EEPC server connection (not through a local connection). Another test is to create and delete 100 users and systems using the command line tool SBADMCL through a test batch file.

Managing Audits

The audit of the users and systems can slow down the database. It is recommended you schedule EEPC command line tool **SBADMCL** to cleanup machine audit and the user audit. See Endpoint Encryption Object Directory Maintenance section below.

File Cache on Raid Hard Drive Controller

Let the Object Directory host server have the largest possible file cache on the RAID Hard Drive controller. This Hardware device will increase the file-access speed dramatically.

NOTE: if cache is enabled on RAID controllers, use UPS backup for power failure protection, because a power failure can lead to a data loss as writes may be still held in cache.

Connection Speed

The speed between the remote servers and the file servers is crucial. Make those connections dedicated high speed connections, e.g. Gigabit Ethernet or Fibre. It is usually recommended you have a single server located on the same dedicated server, rather than multiple EEPC Database servers connecting in from remote server systems.

Object Directory Physical Location

Consideration should be made to the location of the Object Directory.

The default final folder for the Endpoint Encryption Object Directory is in a folder called SBDATA. If possible, use a separate fixed drive or partition to the OS for example, OS and application on C: database on D:. This is usually decided at the time of initial installation and can be modified at another time.

Object Directory Access

Check that every administrator that needs to log on to the Object Directory goes through the Endpoint Encryption Database server, not direct through local connection. Where possible, do not allow the database to be shared.

Searching for Objects

Limit the use of the **Find** function in 20K+ databases during normal working hours as it can slow access for other systems and user objects. Another alternative is to work on a recent copy of the Object Directory to perform searches, and once the location is found, they can be navigated to directly in the live Object Directory.

Clearing Deleted Objects

Clear objects from **Deleted Items** regularly when not needed. Deleted items are folders containing old deleted users, systems, and other objects and are found through the **System** tab in the Endpoint Encryption Manager. These objects can slow searches down. If these objects are needed for auditing, they will need to be retained by first backing up the whole database (SBDATA folder) and then storing, dated, carefully for that purpose. Then empty the deleted items from the current live database to help speed of access. See the more detailed *Object Directory Maintenance* section below.

SBSERVER.INI

This file is found in the main installation folder for your Endpoint Encryption Manager. It can be used to adjust the maximum number of connections the Endpoint Encryption server will accept and the behavior when the maximum is reached.

SBServer ini contents:
[Connections]
Max=200
AcceptAtMax=No

The default settings are usually fine for most implementations but Max=200 can be set to a higher value depending on the number of incoming connections. This should only be changed if the server has a high specification and is recommended by a McAfee Endpoint Encryption consultant. In addition, this would need to be tested to determine if this improves sync events and server load. (Please see *Endpoint Encryption Manager Administration Guide* supplied with Endpoint Encryption Manager for further details on SBServer.ini).

Object Directory Maintenance

Maintenance Introduction

To keep the database clean and healthy, maintenance is required on a regular basis. This maintenance can be done manually using the Endpoint Encryption Manager, or, with the EEPC command Line Tool (SBADMCL), which is the preferred way for larger Object Directories.

This guide describes the processes needed for maintenance. It is written for Endpoint Encryption administrators.

NOTE: These are generic recommendations based on experience but not always be suitable for your specific environment. For database maintenance and performance, it is always recommended to engage McAfee Professional services prior to implementing any of these suggestions. It is possible on already installed environments to have a McAfee professional perform consultancy and provide a "health check" on the setup and performance settings of the Object Directory

Environment

This guide applies to McAfee Endpoint Encryption V5 and up, however many steps in this guide can be applied to V4 (build 4770).

Audit maintenance

Audit can grow unlimited in the database. This can slow down the database dramatically. The Endpoint Encryption administrator has to make sure that the audit is cleaned up every year or every half year depending on the database performance. For more information on the command line tool SBADMCL.exe or its commands please see the *Endpoint Encryption Scripting Tool User Guide,* which is found in most normal installations of the Endpoint Encryption Manager.

Extracting and Clearing Audit from the Database

The audit from users and systems needs to be cleared at least once a year for smaller implementations and frequently for larger deployments because it grows fast. Heavily used objects such as an administrator's account or user object frequently used by a script are likely to be common large audit creators.

The need to clear audits can vary depending on configuration, usage and requirements. However, the Security Management team should decide when to clear the audit. In later versions of the tool, the **ClearDaysOld** command was added. This option gives the administrator the possibility to clear audits that are, for example, 90 days and older. This option must be used instead of the **Clear** option, because the **Clear** option will override the **ClearDaysOld** option if used together.

The audit will always be exported before it is deleted. This will give the administrator the possibility to look back at older audits using Microsoft Excel or similar tools.

Clearing the Audit

SBADMCL is usually run from the directory where the Endpoint Encryption Manager is installed. An admin account with high-level credentials will be needed for the script.

Some of the commands needed below are database intensive processes, so run these command during non working hours only, or, do it in more controlled sessions (one group at a time for example) during daytime if the groups are small.

To export and then clear ALL user audits use this command:

SBADMCL –Command:DumpUserAudit –Adminuser:Admin –Adminpwd:mypassword –File:c:\dump\Dumpuser.txt –Group:* –clear

To export and then clear ALL machine audits use this command:

SBADMCL –Command:DumpMachineAudit –Adminuser:Admin –Adminpwd:mypassword –File:c:\dump\DumpMachine.txt –Group:* –clear

To export and clear ALL user audits 90 days and older use this command:

SBADMCL -Command:DumpUserAudit -Adminuser:Admin -Adminpwd:mypassword -Group:* -File:c:\Dump\DuUserAu90.txt -ClearDaysold:90

To export and clear ALL machine audits 90 days and older use this command:

SBADMCL –Command:DumpMachineAudit –Adminuser:"Admin" –Adminpwd:"mypassword" –File:DuMachAu90.txt –Group:* –ClearDaysOld:90

For further analysis of the Audit see the *Advice on handling audit* document.

To export and clear from a specific group add the group name instead of *

Deleted Items Cleanup

As mentioned previously clearing objects from **Deleted Items** (found through the **System** tab in McAfee Endpoint Encryption Manager) can aid Object Directory access speed. When the deleted items are emptied, the actual physical folder for the object within the Object Directory is renamed. The extension of the folder is renamed from .RMV to .WPE. With a very large database, these empty/removed folders can sometimes slow down searches.

In a test lab, try removing .WPE folders and test search speeds. If an improvement is found, it may be worth repeating on the live Object Directory. Always ensure tests and full backups are performed before any procedure.

Checking for Database Corruption

Why does the database get corrupted?

Corruptions can be caused by failed installations and bad sectors on endpoint systems or unsupported procedures, disconnected network links to the Object Directory* or failing drives and so on.

Poor or slow access to the Object Directory can cause a slow or intermittent access to the database. This can cause the Object Directory to corrupt during database operations. Endpoint installations can fail and cause corruption. In addition, as a consequence, corrupted objects can cause a corrupted index, and to complete the circle this can also cause corrupted objects themselves. Slowness of the disk access can be a problem when using shared resources SAN or NAS connections rather than DAS.

See the document **Server and Object Directory Optimization** section above for detailed information about the performance settings.

*More robust in v5 Release 5701 onwards.

Orphaned Objects

To begin a cleanup, the database starts with what are known as “Orphaned” objects.

These are objects that exist in the Object Directory; they are **not** visible in the Endpoint Encryption Manager GUI.

From the Endpoint Encryption Manager console, you can run **Group scan** found under **Groups** menu. The preferred method though is to use the command line tool as the process can be automated.

The second step is to use the cleanup commands. These will try to fix the objects or delete them if they cannot be fixed. The cleanup commands use a cautious approach when deleting objects, so an object might not be deleted even if it is unusable.

In such a scenario the **DumpMachineDesc** command should be redirected to a file such as DumpMachine.log to dump the objects that do not respond properly. The broken objects in the DumpMachine.log can be deleted from the database. If the normal deletion process does not work, use Microsoft Windows Explorer to browse to the actual location in the database and delete the physical folder. Note: make sure you have a full backup of SBDATA before doing this.

Restore Commands

To restore orphaned user objects back into a group, use this command:

SBADMCL -Command:RestoreUsers -Adminuser:Admin -Adminpwd:mypassword -Group:"Orphaned Users" -Database:"Customer database"

Where “Orphaned Users” is a user group you have made to hold them (or can be another group).

To restore orphaned machine objects back into a group, use this command:

SBADMCL -Command:RestoreMachines -Adminuser:Admin -Adminpwd:mypassword -Group:"Orphaned Machines" -Database:"Customer database"

Please note that these commands are database intensive processes, so run these commands during non working hours only, or, do it per group during daytime if the groups are small.

Cleanup Commands

These two processes have to be done per group, so could be done during daytime if the groups are small. It could be automated running through a CSV file with user groups.

To cleanup corrupted User objects use this command:

SBADMCL -Command:CleanupUserGroup -Adminuser:Admin -Adminpwd:mypassword -Group:”My Laptop Users” -Database:"Customer database"

To cleanup corrupted Machine objects use this command:

SBADMCL -Command:CleanupMachineGroup -Adminuser:Admin -Adminpwd:mypassword -Group:” EndPoint Encryption Machines” -Database:"Customer database"

Dump Machine Description

If objects seem to hang the Manager when opened, then attempt to dump the machine description to find which objects are actually corrupted.

Use the DumpMachineDesc command:

SBADMCL -Command:DumpMachineDesc -Adminuser:Admini -Adminpwd:mypassword -Group:”EndPoint Encryption Machines” -Database:"Customer database" -File:c:\temp\DuMaDesc.txt >>DumpMaDesc.log

The log will show which systems are actually not responding.

The broken objects in the DumpMaDesc.log can be deleted from the database. If the normal deletion doesn’t work, use Windows Explorer to browse to the actual location in the database and delete the physical folder.

In extreme situations if the object was essential (very important encrypted endpoint client for example) it may be possible to restore the object manually from a known working backup. Given this is not “normal” procedure - we recommend you engage McAfee Professional services or take guidance from a McAfee Endpoint Encryption support engineer. This process must to be done per group and can therefore be performed during daytime if the groups are small.

User Objects - General Performance Tips

EEPC can support thousands of users per group and per machine. That said, for performance and security reasons, it is strongly recommended the numbers be kept to a minimum; assign fewer users to systems limiting to those who really need access. For example, a number of setups from customers have some administration/IT support users as well as individual users assigned to clients providing better security and performance.

If enough care is taken and adequate planning is made, performance and security can be increased considerably. Adding all users from large groups to all systems - without basic planning - is a bad idea. Adding thousands of users is possible; however, this will use more storage space and cause synchronization events to take much longer because each user is checked for updates during a synchronization. In addition, this can tie up the Object Directory server spending many extra seconds or minutes servicing each client.

EEPC has excellent password synchronization across all the endpoint clients a user is assigned to. It is therefore logical that adding thousands of users to each machine will add many more synchronization events across the enterprise. This will put further strain on servers and networks.

To ease the strain, you can configure the resync properties to a less aggressive setting (from Endpoint Encryption Manager see Machine Properties, Sync tab, Automatically resynchronize every x minutes option). Change to several hours rather than the default 60 minutes, especially if you have many users assigned. Set it to 240 minutes (4 hours) or 480 minutes (8 hours), or longer, depending on anticipated load and requirements for security policy updates or audit gathering.

Many large deployments successfully use only the base sync event on boot up. Some also use the resync option set to just less than a day, for example, 1200 (20 hours) to force at least one daily sync. This will ensure policy changes are applied; it will catch any unattended systems or those users who do not wish to restart often and ensure they do supply audit information.

General Advice

Default Product settings (for maximum compatibility).

Installing the Endpoint Encryption Manager (EEM) using the default settings will usually ensure maximum compatibility.

Endpoint Encryption Machines

For Endpoint Encryption Machine Groups and therefore individual Machines, the default settings in "Properties" would usually provide the most compatibility.

Some of the extra options that may help in certain situations (usually as advised by McAfee Support or Professional Services) can be used but could cause extra issues if used globally, or without careful thought.

Below are some settings that are not enabled by default. These could cause potential issues if not used correctly.

GENERAL:

- **Enable Boot disk compatibility**
  Some machines have BIOS code which mounts USB disks as physical drives. This can cause Windows to hang after EEPC has finished authorization. This should remain at the default setting, disabled (not selected), unless you have a specific issue with USB drives or have been advised by McAfee Support.

- **Reject Suspend/Hibernate Requests** - This option stops the machine from entering hibernation mode. Note: this option is not supported in Vista.

  With later versions of EEPC v5.x this should normally be left disabled, to allow normal operation of hibernation which is fully encrypted and protected by EEPC.

- **Always enable pre-boot USB support**

  This should remain at the default setting, disabled (not selected), unless you have issues with USB devices with EEPC at preboot, or, have been advised to try this option. It should not normally be enabled and also not used if the BIOS's USB legacy support is also enabled.

FILES:

Some compatibility options are available as special optional file groups that could be assigned to machines to support extra features, hardware, languages, or to work around 3rd party issues.

With a standard install of EEM and EEPC for example, using the defaults, the file groups commonly assigned to the default Machine Group are:

EEPC5x Theme213: Endpoint Encryption for PC McAfee Theme EEPC5x: Endpoint Encryption 5.2.2 Client Files (example shown from v5.2.2, names may vary).

These would normally work well for most machines – usually together with one of the language groups assigned, for example "EEPC52 LANG: English United Kingdom/USA (Preboot, keyboard, Windows)". Many

of the other groups should not be used unless there is a specific reason. These usually include “EEPC52 OPTION:” or similar at the start of the name (example from EEPC v5.2.2).

Some of the optional compatibility file groups that should not be assigned to machines unless a specific issue is being addressed:

- “EEPC52 OPTION: Exclude Sector 59 for NEC Compatibility”
- “EEPC52 OPTION: Tests for Computrace presence”
- “EEPC52 OPTION: Update MBR for Endpoint Encryption for PC compatibility”
- “EEPC52 OPTION: Update number of sides reported in the OS boot sector”
- “EEPC52 OPTION: WACOM Active Tablet Pen Driver”

Things to avoid

Alternative supported method follows each item.

- **Do not assign multiple Theme file groups**

  Assign the Theme you require.

- **Avoid using SafeTech via bootable USB stick.** Although the function it is available, the BIOS on many laptops causes the USB stick (at boot-up) to appear as a fixed drive and therefore swaps with the fixed disk after booting from it. It can cause recovery problems with Remove or Emergency Boot, for example.

  Alternatively, use with a floppy disk drive or bootable CD (make an ISO from the floppy disk to make a bootable CD).

- **Avoid making multiple fundamental changes to clients at once**. For example, changing the encryption state and upgrading EEPC clients at the same time will cause problems.

  Do one major thing at a time, allow clients to sync and perform the change, then make the second change.

- **Do not assign multiple unnecessary file groups as a “catch all” for all possible hardware/software combinations.**

  Instead, try to group machines carefully and assign only the necessary file groups for their specific requirements.

- **Do not use the file group “EEPC52 OPTION: Update MBR for Endpoint Encryption for PC compatibility” together with “EEPC52 OPTION: Update number of sides reported in the OS boot sector” – they are not compatible**;

  Instead, use one or the other, but only if specifically needed or recommended by McAfee Support.

- **When using smartcard readers and tokens, avoid assigning many or all of the Reader or Token file groups together.**

  Whilst they can be used together, more compatibility and easier troubleshooting is ensured using just the specific token or reader files required for a group of machines.

- **Using $autoboot$ user assigned to machines permanently for convenience to bypass pre boot logon as a normal everyday operational client – there is NO security in doing this.**

  This results in end users never seeing the pre-boot authentication screen. There are several perceived benefits to this approach:

  - No user training
  - No helpdesk calls for password resets
  - No administrative work to map users to machines
  - Most auditors simply require that you prove encryption, not strong authentication

  However, there is one **major** risk to this approach that should outweigh all the perceived benefits: **the data is not secure**. If an unauthorised user wanted the data from the drive, they would simply press the power button and get to the Windows GINA. From there, there a number of known attacks to access Windows.

  Instead, secure your data by removing $autoboot$ users when not needed (for example, after rolling out a Windows update). Force an authentication to encrypted data.

- **Using one $autoboot$ user for too many machines.**

  Instead use more autoboot users to reduce the multiple connections and load on the autoboot user object in the database.

  Autoboot user is just like a normal user object in the database. So if the account is accessed by too many endpoints at once, its object could become locked on the server causing errors with the object or client.

  As a rule of thumb, do not allow more than 100 machines to use a single autoboot account. This can vary wildly depending on server load, configuration and optimisation. Of course, if concurrency is high and the server is often busy, reduce this number much more. One tool that can help is the AutoDomain power tool. This can add and remove individual autoboot users to machines if necessary for deployment. AutoDomain is not covered by this document.

  Also, add backup autoboot accounts. Then, if the autoboot account is removed from the endpoint by accident - and there is a backup account in place - the user can remain blissfully unaware. The boot code will look through all autoboot users until it finds one to use.

  So add more than one for example :
  $autoboot$0001, $autoboot$0002, $autoboot$0003 etc.

  Note: at least version 5.2 or above is required for this to work.

  For further information on using Autoboot users or the AutoDomain power tool contact McAfee representatives who can arrange McAfee Professional Services to assist.