SOPHOS

Security made simple.

SafeGuard Enterprise

Professional Services – Deployment Preparation Guide

This document is a reference guide to assist with providing a consolidated overview for Sophos customers when working with Sophos Professional Services for implementation of the SafeGuard Enterprise solution

Table of Contents

Introduction 3
Software Download 3
System Requirements 3
SafeGuard Enterprise Management Center 3
SafeGuard Enterprise Server and WebHelpDesk 3
SafeGuard Enterprise Client 4
Microsoft SQL Server 4
Active Directory 4
Group(s) 4
Service Accounts 4
Anti-Virus Software Exclusions/Exceptions of SGN LocalCache Folders 4
Connectivity Requirements 5
DMZ SGN Server 5
Securing transport connections with SSL (Recommended / Best Practice) 5
Pre-engagement Checklist 5

Introduction

This document will assist in the preparation for installation of Sophos SafeGuard Enterprise solution. The following information is based on Safeguard Enterprise version 7.0. Please ensure ALL tasks in the guide are completed PRIOR to your actual Professional Services engagement day.

Please note: The SafeGuard Enterprise Server and WebHelpDesk components **MUST** be installed on a dedicated server. Any programs running on the same server may disrupt its operation or function. This includes additional IIS features not required by the SafeGuard Enterprise products.

Any conflicting third-party installations may impede performance or introduce irresolvable issues with either the third-party software, the SafeGuard Enterprise Solution or both. Troubleshooting these conflicts will be billed against the Service hours and may prevent the full execution of the Scope of Work.

Please forward any questions to ProfessionalServices@sophos.com pertaining to the preparation task descripted below

In addition to this preparation guide, review of the current SafeGuard Enterprise Release Notes is recommended for more detailed hardware and system requirements.

http://www.sophos.com/en-us/support/knowledgebase/112776.aspx

Software Download

If order to download the software, please review the following knowledge article for instructions on creating a MySophos account.

http://www.sophos.com/en-us/support/knowledgebase/111195.aspx

System Requirements

Please refer to the following knowledge article for complete list of all supported platforms and system requirements for all Safeguard Enterprise Components.

http://www.sophos.com/en-us/support/knowledgebase/118646.aspx

SafeGuard Enterprise Management Center

The SafeGuard Management Center application is used to perform all administrative tasks for the Safeguard Enterprise environment. This software package can be installed on more than one system depending on your specific requirements and what IT personnel need access.

A dedicated server is NOT required for this software package. This software is typically installed on a Safeguard Enterprise Server.

SafeGuard Enterprise Server and WebHelpDesk

The SafeGuard Enterprise Server is responsible for communicating with the SafeGuard Enterprise Clients. The SafeGuard Enterprise WebHelpDesk is a web portal that can be used by your Help Desk organization to assist end user who have forgotten their password.

The requirements for these two software packages are the same and are typically installed on the same Windows server. Only one instance of the WebHelpDesk is required, so if multiple SafeGuard Enterprise Servers are installed, one will be chosen to host the solution.

SafeGuard Enterprise Client

Client machines should be prepared and ready for testing before the engagement begins. Please refer to sighed SoW for guidelines on number for machines that should be available for testing. If possible, different models should be used to represent what is deployed within your production environment. If a 'production' client is to be used during initial testing, be sure a backup of the machine is completed before installation.

Microsoft SQL Server

A Microsoft SQL Server is required for the SafeGuard Enterprise environment. This can be an existing SQL server or a new SQL server installed for the Safeguard solution.

Please note: If Microsoft SQL Express is used, please make sure to also install the Microsoft SQL Management Studio as it will be required to configure authentication permissions to the 'SafeGuard' database

The database used by the SafeGuard Enterprise solution is either created during the installation and configuration of the SafeGuard Management Center or via SQL scripts provided within the software download. Please read below to see the requirements for each method

Management Center

- This is the default method used to create the 'SafeGuard' database and is used in most installations and can be completed during the Professional Services engagement.
- Requires "db_create" rights be granted to Windows account used to install and configure the SafeGuard Enterprise environment. Once the database is created, these rights can be altered.

SQL Scripts

- This method is used when the SQL DBA would rather not have an application create a database within the corporate SQL infrastructure.
  - CreateDatabase.sql
  - CreateTables.sql – Be sure to run this against the newly create 'SafeGuard' database.

Active Directory

Group(s)

SGN Admins – Any user that requires access to the SafeGuard Management Center will need to be placed in this group. This group will need to be given 'db_datareader' and 'db_datawriter' to the newly created 'SafeGuard' database.

Service Accounts

A service account is used for both AD synchronization and SafeGuard Server authentication to the SQL database. This account doesn't need any special rights within AD, but should have a non-expiring password. Please record this password as it will be needed several times during the initial SafeGuard setup.

Anti-Virus Software Exclusions/Exceptions of SGN LocalCache Folders

Add Safeguard LocalCache and its backup into your company AV exceptions list. This is required and will prevent your AV product from damaging this sensitive area of our client. Make this a file and folder exception.

- For Windows 7 and Windows 8.x
  - C:\ProgramData\Utimaco\SafeGuard Enterprise

Connectivity Requirements

SafeGuard Enterprise Client

- Connect to server via HTTPS, port 443 (HTTP, port 80 is available but nor recommended)
- Non-standard ports can be used if required

SafeGuard Enterprise Management Center

- Connects to SQL database via port 1433/TCP & 1434/UDP
  Non-standard ports can be used if required
- Active Directory (Port 389/TCP, Port 636 SLDAP, Port 1025/TCP (RPC),
  135/TCP (end-point mapper - RPC).

The SGN Server must be able to connect to

- Connects to SQL database via port 1433/TCP & 1434/UDP
  Non-standard ports can be used if required

DMZ SGN Server

If a requirement exists for managing machines that are not on the corporate network, and those clients do not ordinarily VPN into the corporate network, it is recommended to establish an Internet facing SGN server within the company DMZ. Network communication from the client to the SGN server within the DMZ is recommended to use SSL using default port 443. Communication is required from the DMZ SGN server to the SGN database server. This communication ordinarily uses SQL authentication and requires TCP ports 1433, UDP 1434 be open between the DMZ Server and the SQL Server. Further details on this sort of setup should be discussed with your assigned Professional Services Engineer in advance of your scheduled engagement date and time.

Securing transport connections with SSL (Recommended / Best Practice)

Sophos strongly recommends using SSL-encrypted communication between SGN Client workstations and the SGN Server for use in **any system** except demo or test setups. If, for some reason, this is not possible and proprietary SGN encryption must be used, there is an upper limit of 1000 client workstations that connect to a single server instance. When using SSL, the necessary settings have to be configured manually in the SGN Management Center to enable this functionality.

SSL certs can either be issued by an internal CA on your network, purchased from a third party or can be self-signed. If using self-signed certificate you must create a GPO to place this self-signed cert into the trusted Root Authority of ALL of your domain machines that will be encrypted or the cert will not work. If you decide to purchase a cert from a third party, you can use a cert purchased specifically for this machine or use a wild card cert.

Pre-engagement Checklist

- ○ Create a "MySophos" Account
- ○ Download SafeGuard Enterprise Software
- ○ SGN Server – Review requirements and ensure Windows Server is available and is fully patched
- ○ Certificate – Obtain certificate for SSL communications
- ○ Ensure SQL Management Studio is available for the SQL Server being used for this installation
- ○ Have client machines available for testing

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

10.14RG.na.simpl