ControlGuard

Endpoint Access Manager v3.1 Installation Guide

Table of Contents

Preface **3**

Components Overview **4**

Setup **5**

Hardware/Software Requirements 5

Endpoint Access Manager Installation 6

Starting Endpoint Access Manager Services 14

Uninstalling Endpoint Access Manager Server 14

Endpoint Access Manager Activation 15

Certification 18

Installing Endpoint Access Manager Agent 20

Unloading Endpoint Access Manager's Agent 26

Uninstalling Endpoint Access Manager's Agent 26

Index **27**

Preface

ControlGuard provides a comprehensive solution to internal security breaches such as unauthorized access to I/O devices. By defining the organization's access security policy, ControlGuard's software enables access control over a wide range of I/O devices at different levels.

ControlGuard's software enables easy deployment to all the computers and laptops in the network domain, automatic version update when newer versions are available, and access to up-to-date information about access to I/O resources and on line access authorization.

This manual specifies pre requirements and details the installation process of ControlGuard's software package components.

Components Overview

- Endpoint Access Manager

The Endpoint Access Manager (EAM) provides a comprehensive solution to internal security breaches such as unauthorized access to I/O devices. By defining the organization's access security policy, Endpoint Access Manager enables access control over a wide range of I/O devices at different levels.

The EAM software includes a centralized console, server and Report module. It also includes an Agent that is installed on every desktop, server or laptop in the network.

- Messaging

The Messaging product enables you to monitor system gathered information (device and forensic events) and filter it according to your needs. The software includes a console and server

- Live Update

The Live Update product enables you to manage Endpoint Access Manager (EAM) agents' upgrade processes, monitor currently installed versions and upgrade versions of multiple clients simultaneously. The software includes a console and server.

Setup

This section describes the pre requirements and installation process of the comprehensive ControlGuard package.

Note: The Live Update and Messaging servers must be installed on the same workstation as the EAM management server.

Hardware/Software Requirements

Endpoint Access Manager Server

- Any edition of Microsoft Windows 2003 Server running Microsoft Internet Information Server
- .NET Framework 1.1
- Any edition of Microsoft SQL Server (MSDE is provided on installation CD)
- Microsoft Data Access Components (MDAC) 2.63 or higher
- 200 MB free disk space

Endpoint Access Manager Console

- Any edition of Microsoft Windows 2000, XP Professional, or 2003
- Microsoft Internet Explorer 5.5 or higher
- .NET Framework 1.1
- 10 MB free disk space

Endpoint Access Manager Agent

- Any edition of Microsoft Windows 2000, XP Professional, or 2003
- 20 MB free disk space
- MSI Version 2 or higher
- .NET Framework 1.1 (installed automatically if not pre-installed)

Hardware (server)

- Minimum P-III 1000 MHz

- Minimum 256 MB RAM

Report Module

Endpoint Access Manager's platform provides a Graphic Analyzer and Report Generator of events taking place, alerts and "plug&play" media and devices.

To view reports, your system must meet the following requirements:

- Microsoft Internet Explorer 5.5 or higher
- For Windows Server 2003, asp.net is required.

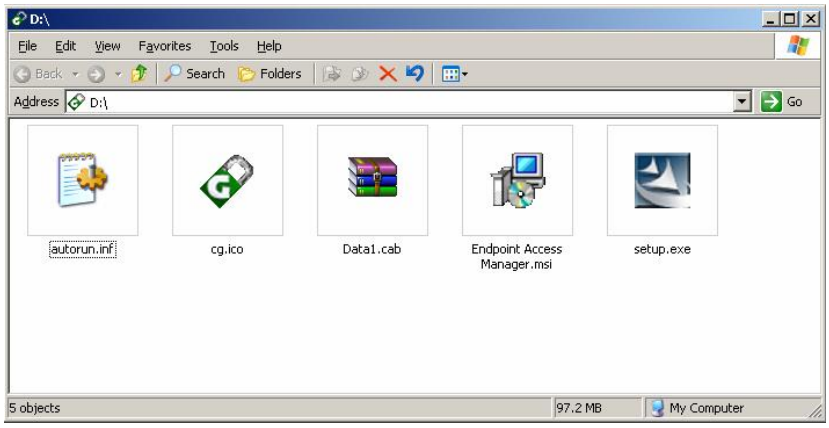
Note: If IIS is installed before installing .NET, run C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322\aspnet_regiis.exe-i in order to register required asp.net components.

Endpoint Access Manager Installation

The installation process described below allows you to install the complete Endpoint Access Manager package, including the Endpoint Access Manager, Messaging and Live Update. Alternatively, you can install only some of the components according to your network layout (e.g. servers on one management workstation, and consoles on different, remote workstations)

To begin installation:

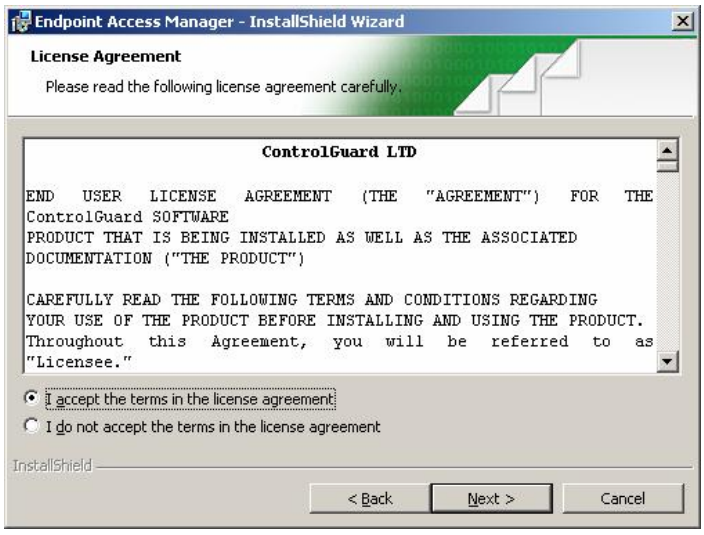
1. Insert the Endpoint Access Manager installation CD into the CD drive.



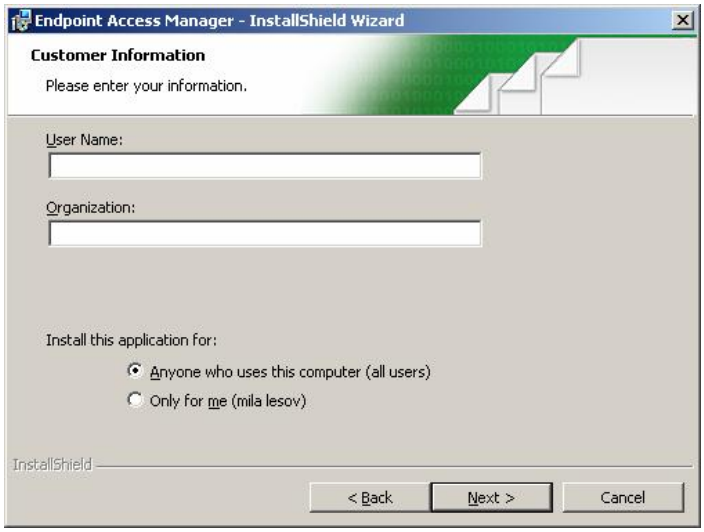
The installation CD contains the Endpoint Access Manager software and additional software required by Endpoint Access Manager to be installed if needed.

2. Double-click the ***setup.exe*** file.
3. On the Welcome screen, click **Next**.

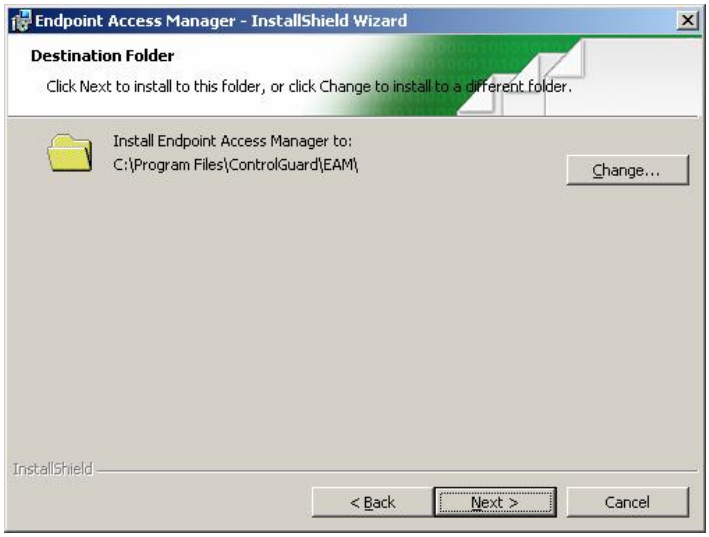
4. On the License Agreement screen, select the 'I accept' option, if you accept the license terms, and click **Next**.



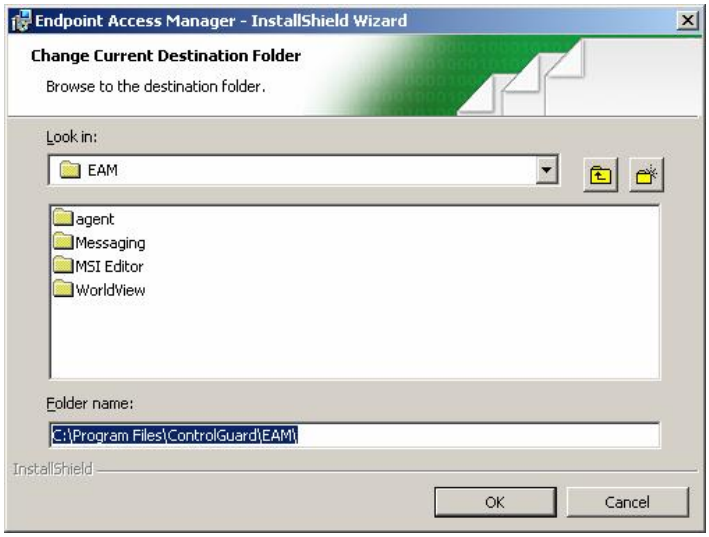
5. On the Customer Information screen, fill in User Name and Organization and select who will be allowed to use the application. Click **Next**.



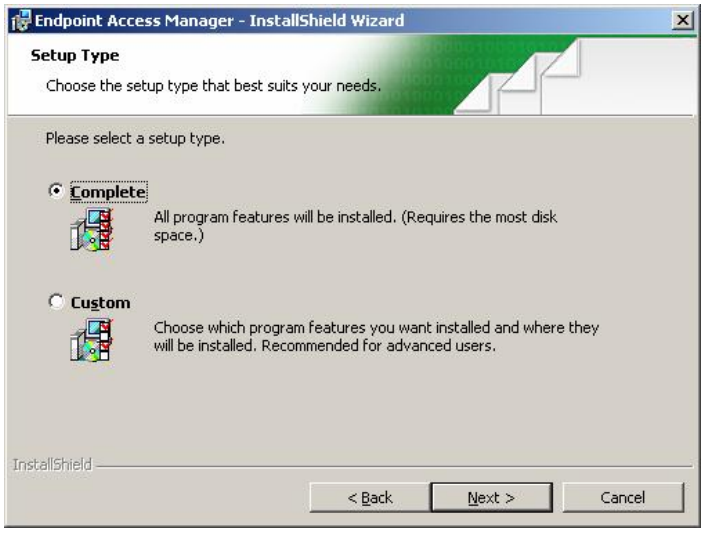
6. On the Destination Folder screen, set the name and path of the destination folder.



If you want to change the default destination folder, click **Change** and set the folder using the browser. Click **OK** and **Next**.



7. On the Setup Type screen you can choose **Complete** or **Custom** setup.



If you select the Complete Setup option, all software components (servers, consoles, MSDE) are installed on the workstation. To do so, select **Complete** and click **Next**. Skip to step 10.

Selecting the Custom Setup option allows you to select which components to install and where to install them. You may prefer to use Custom Setup in the following cases:

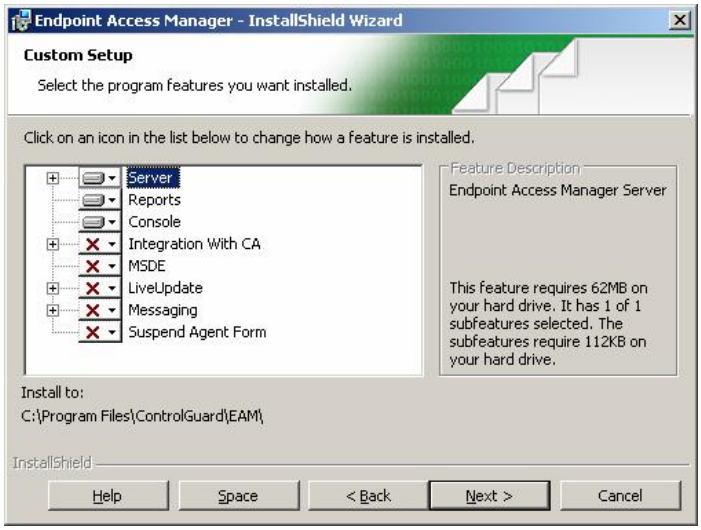
- If you already have MSSQL installed on your computer, and you want to avoid MSDE installation.

- If you want to install the consoles on a workstation other than the management (remote).

To perform a custom setup installation, select **Custom** and click **Next**.

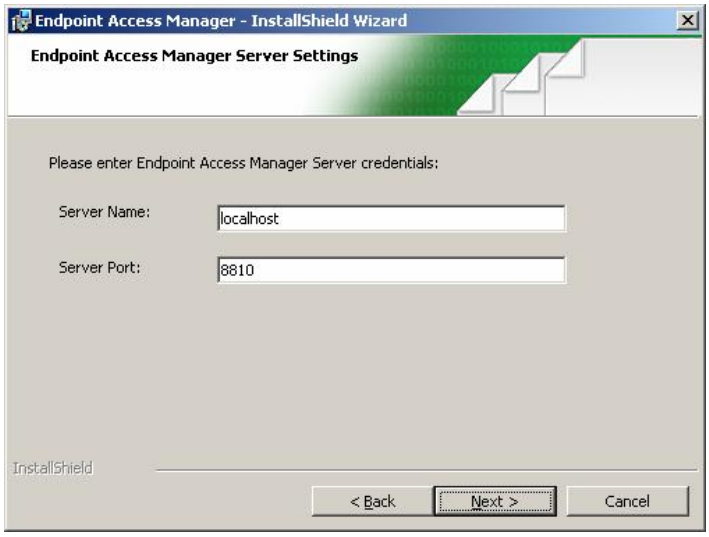
On the Custom Setup screen, select the components you need to install, and click **Next**.

Note: Custom installation does not install CA integration, MSDE, Live Update, Messaging, and Suspended Agent Form by default.

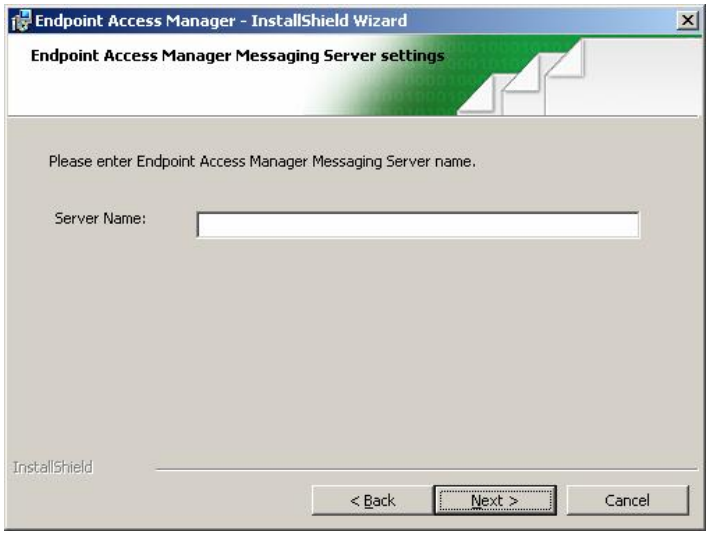


Since the Messaging and Live Update servers and the Suspend Agent Form must be installed on the same workstation as the EAM server, trying to select these servers without selecting the EAM server will result in a pop-up message asking you to select the EAM server as well.

8. If you want to install components other than the messaging console, skip to step 10. If you want to install the Messaging console on a remote workstation, you need to provide information about the servers and their location. On the Endpoint Access Manager Server, fill in the Endpoint Access Manager server's name and port fields and click **Next**.

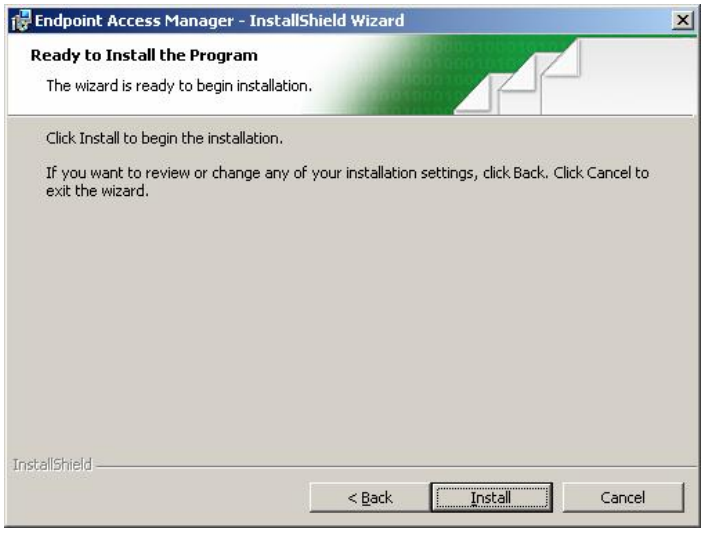


9. On the Messaging Server Setting screen, type in the name of the computer on which the Messaging server is installed. Click **Next**.



10. If you are not installing the EAM server, skip to step 11. On the Service Type screen, select the service type you want to install (Windows or Web service). Click **Next**.

11. Now you can install Endpoint Access Manager.



12. If IIS server is not installed, the following error message appears.

You need to install IIS server on your computer in order for the Endpoint Access Manager's reporting feature to work. If you want to use the reporting feature, click

Abort, install IIS server and reinstall Endpoint Access Manager. Otherwise, click **Ignore** and continue.

13. When the Endpoint Access Manager's installation process is complete, click **Finish**.

Note: The Endpoint Access Manager Server service is down when you complete the installation process. The service is started following Endpoint Access Manager's activation (see Endpoint Access Manager Activation, page 15).

Following installation, a new folder is created under the path you specified (see step 6 above), that includes the following:

- If you installed Live Update server, a folder titled LiveUpdate Server Service
- If you installed Live Update console, a folder titled LiveUpdate Console
- If you installed Messaging server or console, a folder titled Messaging

After you have completed the installation process, a message box appears, enabling you to proceed directly to Endpoint Access Manager's activation. You can choose to activate later by clicking **Cancel**. Clicking **OK** prompts you with the activation dialog box (see Endpoint Access Manager Activation, page 15).

Starting Endpoint Access Manager Services

If you selected to install Endpoint Access Manager as a web service, you can access the service via **Computer Management → Services and Applications → Internet Information Services Manager → Web Sites → ControlGuard**.

If you selected to install Endpoint Access Manager as a Windows service, you can access the service via **Start → Settings → Control Panel → Administrative Tools**. Double-click **Services** and select the Endpoint Access Manager Server service.

Note: Endpoint Access Manager Server service is started automatically following activation.

The Endpoint Access Manager Liveupdate and Messaging Server services are not active by default and need to be started following installation.

To start the LiveUpdate and Messaging server services:

1. Go to **Start → Settings → Control Panel →Administrative Tools**.
2. Double-click **Services**. To start the Live Update server service, select **Endpoint Access Manager Liveupdate Server** and click **Start.** To start the Messaging server service, select **Endpoint Access Manager Messaging Server** and click **Start**.

Uninstalling Endpoint Access Manager Server

To uninstall the Endpoint Access Manager product:

1. Go to **Start → Settings → Control Panel → Add or Remove Programs**.
2. Select **Endpoint Access Manager** and click **Remove.**

You can modify a previous installation process by adding or removing components from an installed product or in order to repair installation errors.

Note: If you remove the Endpoint Access Manager server, you will not be able to access the Messaging or Live Update servers.

To modify installation:

1. Go to **Start → Settings → Control Panel → Add or Remove Programs**.
2. Select **Endpoint Access Manager** and click **Change**.
3. Click **Next** to open the Program Maintenance screen.

4. Select the appropriate option and click **Next**.
5. If you selected **Repair**, click **Install** and **Finish,** to complete the process. If you selected **Modify**, return to step 7 of the installation process (page 9), to complete the installation process.

Endpoint Access Manager Activation

To use the Endpoint Access Manager, you first need to activate the installed server. You can select to activate a management or a regular server.

Activating a Management Server

To activate a management server:

1. Go to **Start → Programs → ControlGuard → Endpoint Access Manager → Activation**. The Endpoint Access Manager Activation dialog box appears:

2. Type in the activation code. (To obtain the activation code, contact the local distributor.)
3. Select **Management** as the server type you are activating and click **Activate**.

Endpoint Access Manager now starts to create the database. If you want to create a new database, click **Yes**. If you want to use the existing Endpoint Access Manager's database, click **No**.

4. If you are using an existing database, the Databse Settings dialog box appears, featuring the existing database parameters. Click **Back** to return to the main activation dialog box. Click **Save** to complete the activation process.

5. If you are creating a new database, you need to set the database configuration in the Database Settings dialog box. To return to the main activation dialog box, click **Back**.

Note: The Host and User fields are automatically generated.

The default authentication method is “SQL Server” and the default user and password are the SQL user “sa” and “controlguard”, respectively. During activation, you can change the authentication method to Windows authentication. If you change the Authentication Method to Windows, a message appears, indicating the necessary setting configuration (see Endpoint Access Manager User Manual, page 30).

6. Click **Create**. You have now completed the Endpoint Access Manager’s activation process. Following activation completion, the Endpoint Access Manager Server service is started.

Activating a Regular Server

To activate a regular (non-management server):

1. Go to **Start → Programs → ControlGuard → Endpoint Access Manager → Activation**. The Endpoint Access Manager Activation dialog box appears:

2. Type in the activation code. (To obtain the activation code, contact the local distributor.)
3. Select **Regular** as the server type you are activating and click **Activate**.

4. The Database Setting dialog box displays the existing database settings as defined for the management server. Click **Back** to return to the main activation dialog box. Click **Save** to continue**.**

5. On the Certification Settings dialog box, you need to specify a path for the server and agent certificate files. You can type in the path or browse using the ... button. Click **OK** to complete the activation process.

Certification

Following Endpoint Access Manager's activation, a server certificate file (serverCert) and an agent certificate file (agentCert) are created and stored in the Endpoint Access Manager's installation folder. These files are used for verification of the agents' and server's identities. The certificate is copied to all the computers on which an agent is installed. When the server contacts the agents, the agent and server's identities are verified using the certificates. If verification fails, the computer's name on the console's main screen turns purple, indicating a certification error.

The agent installation file (cgAgent.msi) is automatically updated with the server's certificate following activation, and does not need to be manually updated. If, for some reason, the file is not updated, you can copy the certificate file manually or use the EAM MSI tool (see below) to update cgAgent.msi with the certificate.

Manually Copying the Agent Certificate

To manually copy the agent's certificate to the agent's computer:

1. When you install an agent on a computer, copy the agentCert.crt file to system 32.
2. Reboot the computer. On reboot, the computer creates a registry entry for the agent certificate.

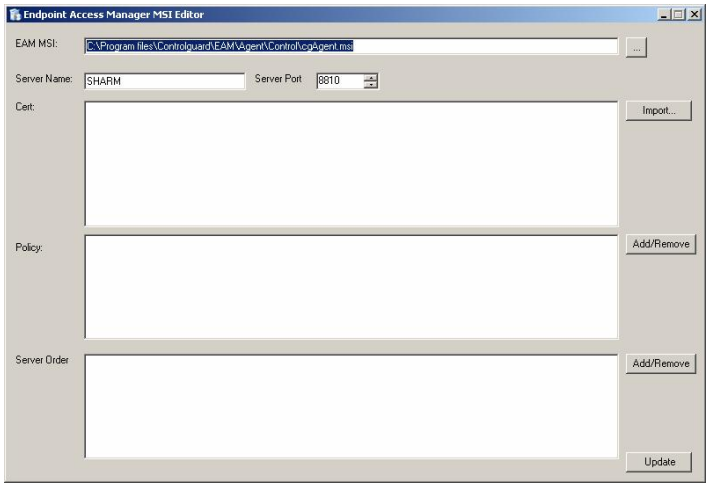
Using MSI Updater

Endpoint Access Manger's MSI tool enables to automatically update the agent's installation file (cgAgent.msi) with the certificate file.

Note: The MSI Updater tool enables you to sent defined policies to the installed agent. If no policies are defined yet, skip this step and use the tool to send the certificate.

To use the MSI Updater tool:

1. On the computer where the EAM Server is installed, go to the EAM server installation folder and double-click **MsiUpdater.exe** to open the EAM MSI Editor.



2. Set the EAM agent MSI path (i.e the path to the cgAgent.msi file), server name, and server port.
3. To import the certificate file, click **Import**. Set the path to the server's certificate file (serverCert.crt in the Endpoint Access Manager's installation folder) using the browser, and click **OK**. The server's certificate appears in the Cert window.
4. If no policies are defined yet, skip this step. To select ACLs, click the **Add/Remove** button to the right of the Policy window. The defined policies list appears in the Policy window. Select the policies you want to be sent to the agent, using Ctrl+click and Shift+click.
5. For agents' version 3.1 and up, you can set the order of the servers to which the agent sends its report. Use the **Add/Remove** button to the right of the Server Order window to add the servers in the desired order.
6. Click **Update**. A message indicates the agent's installation file is updated.

Installing Endpoint Access Manager Agent

Before you install an Endpoint Access Manager agent, you need to determine what kind of agent to install. Endpoint Access Manager provides two types of agents (both types can be either control or monitor agents):

- Linked agent: to be installed on computers where .Net is not installed. When you install a linked agent, Net 1.1 is installed on your computer as well. To install a linked agent, use either C:\Program Files\ControlGuard\EAM\agent\Control or C:\Program Files\ControlGuard\EAM\agent\Monitor depending on the required agent functionality. A linked agent is installed by default during remote installation via the console.
- Unlinked agent: to be installed on computers where .Net is already installed. To install an unlinked agent use either C:\Program Files\ControlGuard\EAM\unlinkedagent\Control or C:\Program Files\ControlGuard\EAM\unlinkedagent\Monitor, depending on the required

agent functionality. If you want to remotely install an unlinked agent via the console, you need to perform the following steps before installing the agent:

1. Rename the Control and Monitor folders, located under C:\Program Files\ControlGuard\EAM\agent (e.g. rename Control_linked and Monitor_linked respectively).
2. Copy the Control and Monitor folders, located under C:\Program Files\ControlGuard\EAM\unlinkedagent to C:\Program Files\ControlGuard\EAM\agent.

You can install the Endpoint Access Manager agent on the workstations in your network using any of the methods described below.

Note: Regardless of the installation method you use, reboot the workstation after installation.

Manual Installation

Before manually installing an agent you need to choose the type of agent to install, a control (protecting) agent or a monitoring (passive) agent.

To manually install the Endpoint Access Manager agent:

1. Go to the library in which Endpoint Access Manager is installed. To install a protecting agent, use the path <ControlGuard installation folder>\EAM\agent\Control or <ControlGuard installation folder>\EAM\unlinkedagent\Control. To install a monitoring agent, use the path <ControlGuard installation folder>\EAM\agent\Monitor or <ControlGuard installation folder>\EAM\unlinked agent\Monitor.
2. Double-click cgAgent.msi or drag and drop cgAgent.msi to the **Start Menu** → **Run** and run it.

   Example:

   "C:\Program Files\ControlGuard\EAM\agent\Control\cgAgent.msi"

   During the installation process, you need to enter the server name. The server name parameter defines the Endpoint Access Manager server and is mandatory.

Alternatively, you can run cgAgent.msi with the SERVERNAME=cgservername parameter. For example:

"C:\Program Files\ControlGuard\EAM\agent\Control\cgAgent.msi" SERVERNAME=cgservername

When you run cgAgent.msi with the server name parameter, the parameter you enter appears in the Server Setting screen during the installation process.

You can define optional parameters to configure the agent as described below:

BLUE (TRUE/FALSE) – allows offline use of BlueTooth. The default value is FALSE.

WIFI (TRUE/FALSE) – allows offline use of WIFI. The default value is FALSE.

MODEM (TRUE/FALSE) – allows offline use of the modem. The default value is FALSE.

AGENTPORT – defines the agent listening port. The default value is 7710.

SERVERPORT – defines the server listening port. The default value is 8810.

3. On the Welcome screen, click **Next**.

Figure 0-1 Endpoint Access Manager Agent Install Wizard

4. On the License Agreement screen, check the 'I accept' option and click **Next**.

Figure 0-2 Endpoint Access Manager Agent License Agreement

5. On the Server Settings screen, type in the Endpoint Access Manager Server's name**.** If you ran cgAgent.msi with the server name parameter previously, the server name you entered appears in the Server Settings screen. Click **Next.**

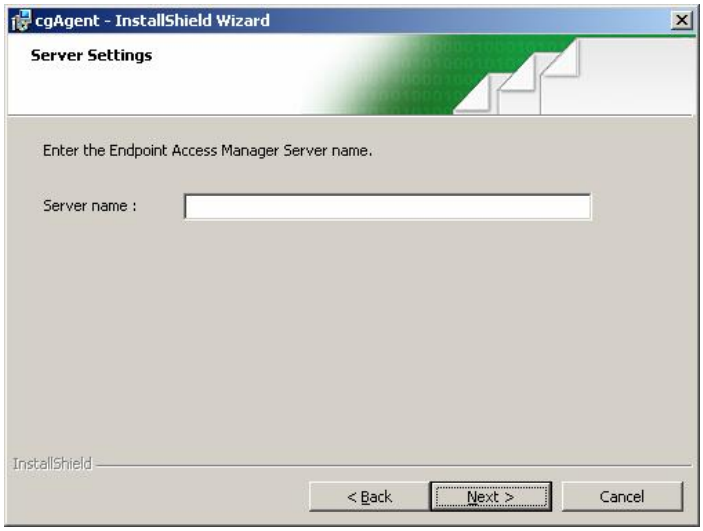


Figure 0-3 Endpoint Access Manager Server Settings

6. Now you can install Endpoint Access Manager Agent.

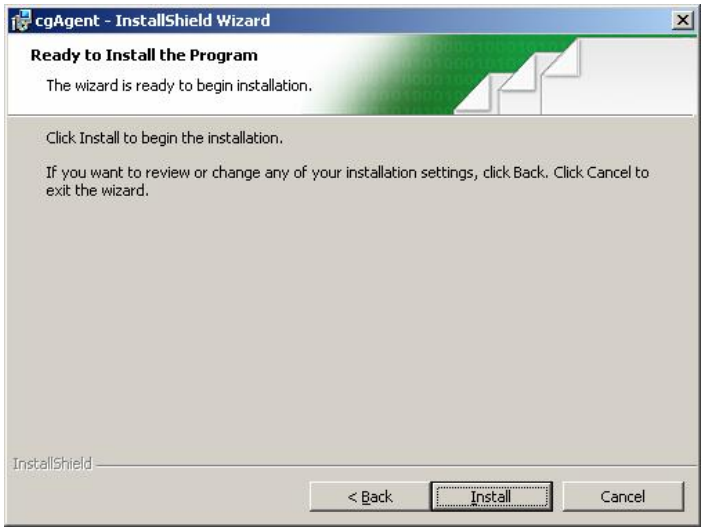


Figure 0-4 Endpoint Access Manager Agent Install

Installation Using Login Script

To install the agent using a login script, add the following to the login script:

Msiexec.exe/i(=Directory name)*\cgagent.msi/qn SERVERNAME=cgservername*

The SERVERNAME parameter defines the Endpoint Access Manager server. It is mandatory and must appear in the script. You can define optional parameters to configure the agent as described below:

- BLUE (TRUE/FALSE) – allows offline use of BlueTooth. The default value is FALSE.
- WIFI (TRUE/FALSE) – allows offline use of WIFI. The default value is FALSE.
- MODEM (TRUE/FALSE) – allows offline use of the modem. The default value is FALSE.
- AGENTPORT – defines the agent listening port. The default value is 7710.
- SERVERPORT – defines the server listening port. The default value is 8810.

Example: *Msiexec.exe/i*(=Directory name)*\cgagent.msi/qn SERVERNAME=cgservername WIFI=TRUE AGENTPORT=1234*

Note: You can also install Endpoint Access Manager Agent using other methods such as SMS or GPO.

Automatic Installation

Endpoint Access Manager enables automatic installation of agents on computers in the network, using the Active Directory synchronization feature. Once every preset interval the Active Directory and the Endpoint Access Manager database synchronize and agents are installed on new computers drawn from the Active Directory. This feature allows you to define a time interval during which the synchronization takes place and the necessary action (agent installation). Active Directory synchronization is inactive by default and needs to be configured and started. The configuration is not done via the console.

Note: The above description refers to a manual startup of the Active Directory synchronization service. To avoid having to reactivate the service after restart, go to **Start → Run** and type **services.msc**. Right-click the startup type of the Active Directory Synchronization Service, and select **Automatic**.

To configure Active Directory synchronization:

1. Go to **Start → Programs → ControlGuard → Endpoint Access Manager → Synchronization Settings**.

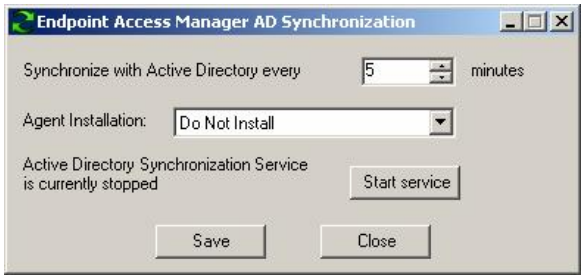


Figure 0-5 Active Directory Synchronization

2. Set the time interval for synchronization.
3. Set the required action (install agent or do not install).
4. Click **Start Service** to start Active Directory synchronization.

Installation via Console

To install an Endpoint Access Manager agent using the console, see Endpoint Access Manager User Manual, page 48).

Unloading Endpoint Access Manager's Agent

In some cases you may want to unload the Endpoint Access Manager's agent directly from the computer on which it is installed (e.g communication problems).

To unload the Endpoint Access Manager's agent driver:

1. Start the computer in Safe Mode.
2. Wait until the message "Press Esc to cancel loading <*version number*> engine" appears.
3. Click **Esc**. The message "Enter Password:" appears.

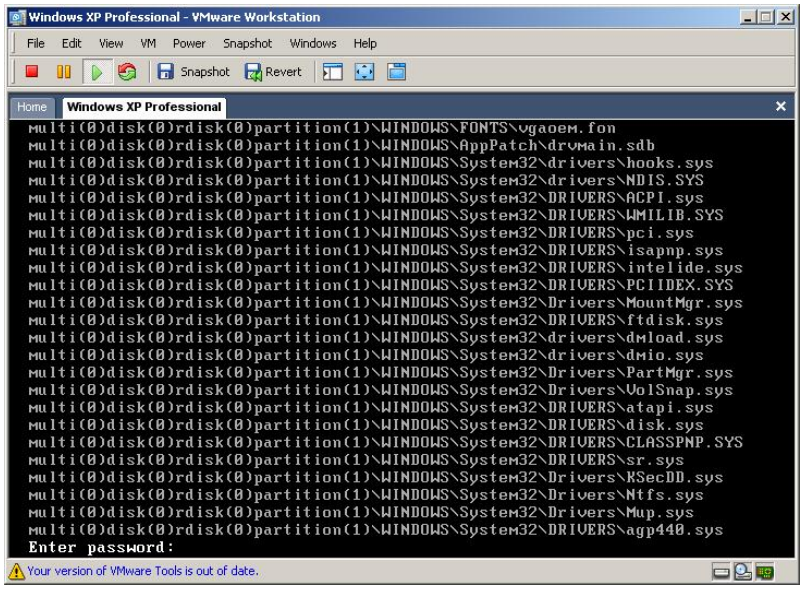


Figure 0-6 Unloading Screen

4. Type in the password. (To obtain the password, run passgen.exe from the ControlGuard server's installation folder in advance.). The message "Engine is not loaded" appears.

> **Note**: The Password is based on a combination of the computer's name and the current date. Make sure the dates in both the workstation and the Server are updated. The password is valid only for the date it was generated on.

Uninstalling Endpoint Access Manager's Agent

To uninstall Endpoint Access Manager's agent, see Endpoint Access Manager User Manual, page 49).

Index

A

agent, *4*
- automatic installation, 25
- installation, *20*
- linked, 20
- login script installation, 24
- manual installation, 21
- uninstalling, *26*
- unlinked, 20
- unloading, 26

C

certification, 18
- EAM MSI, 19

console, *4*

E

EAM MSI, 19

Endpoint Access Manager
- activation. See Setup
- installation. *See* Setup

R

reports, *4*

S

setup
- installation, *6*
- pre requirements, *5*