SafeNet Security Management Center II

Installation Guide

SafeNet
The Foundation of Information Security

safenet-inc.com

SafeNet Proprietary

P/N 007-007850-402 (Rev A, October 2010)

Software Version 4.0C

SafeNet, Inc.

4690 Millennium Drive

Belcamp, Maryland 21017

USA

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:

Phone: 800-545-6608

Email: support@safenet-inc.com

www.safenet-inc.com

Contents

Chapter 1

Introduction

Welcome to the *SMCII Installation Guide*. This guide provides you with the necessary information for installing the Security Management Center II on your network, and for maintaining that installation. This guide is intended primarily for network administrators who will be responsible for the installation and maintenance of the SMCII system.

In this guide, you will find procedures for installing SMCII on the Solaris™ and Windows® operating systems.

About SMCII

SafeNet Security Management Center (SMCII) redefines network security management. A robust, Web-based, management platform, the SMCII centrally manages encryptors deployed on the enterprise network. SMCII remotely configures, monitors, and performs firmware updates, thereby reducing the cost of network security management.

SMCII allows you to remotely configure, monitor, and perform firmware updates for SafeNet's high speed network encryptor families:

- SafeNet ATM Encryptor II (SAEII)
- SafeNet Conversion Encryptor (SCE)
- SafeNet Ethernet Encryptor (SEE)
- SafeNet Link Encryptor (SLE)
- SafeNet SONET Encryptor (SSE)

SMCII acts as an SNMP proxy for Network Management Systems (NMS), providing bi-directional connectivity between SafeNet devices and the NMS.

Additionally, SMCII provides a secure SSL management channel using HTTPS between the client workstation and the management server, and a secure communication channel between the management server and the managed devices.

For security, SMCII encrypts fields in the database that contain sensitive data.

For information on configuring, maintaining, and monitoring devices from the SMCII and database-related tasks, refer to the *SMCII Online Users Guide*.

SMCII Software Package

The SMCII software package includes the following components:

- SMCII Installation CD
- License Agreement

About This Guide

How This Guide Is Organized

This guide contains the following chapters:

Chapter 1: Introduction—This chapter provides an introduction to SMCII, along with a description of the information you will find in this guide.

Chapter 2: System Requirements—This chapter provides specific information on the system requirements for installing and running SMCII on the Solaris and Windows operating systems.

Chapter 3: Installation Procedures—This chapter provides instructions for installing SMCII.

Chapter 4: Migration Procedures—This chapter provides information on migrating your legacy SMC database to SMCII.

Chapter 5: Uninstall Procedures—This chapter provides instructions for uninstalling SMCII.

Chapter 6: Troubleshooting—This chapter provides information on issues that may be encountered during installation, upgrade, and uninstallation of SMCII.

Reader Response

Tell Us What You Think

As you read this, the documentation team at SafeNet is hard at work preparing the next edition. Your feedback could be instrumental in helping us improve this guide.

We are very interested in hearing from you about:

- **Good ideas**—Tell us about some part of this manual that you think works well; we'll be sure to maintain it.
- **Ideas that need work**—Tell us about an area that you feel needs to be improved; we'll punch it up.
- **Information not included**—Did we miss something? Let us know so we can make sure it gets included in the next edition.
- **Information that's not clear**—Did you find something hard to follow? We'll rethink it and rewrite it.
- **Information that's not correct**—Did something get past our arduous technical editing process? Help us fix it.

How To Contact Us

If you can offer any comments, suggestions or compliments about this manual, please let us know. We'd love to hear from you.

E-mail us at:

TechPubs@safenet-inc.com

Chapter 2

System Requirements

This chapter describes the minimum hardware and software requirements to operate SMCII, along with information about third-party software and system password requirements. To maintain security integrity, SafeNet recommends that SMCII operate on a dedicated system.

Hardware Requirements

Unix Operating System

For the UNIX operating system, the following list defines the hardware requirements:

- Solaris™ 10 operating system
- Sun SPARC™ Enterprise Server (single CPU or more)
- 2 GB RAM
- 60 GB hard drive (minimum) / 160 GB (recommended)
- Network interface card

Windows Operating System

For the Windows operating system, the following list defines the hardware requirements:

- Windows Server® 2008 Standard x86 Edition with Service Pack 2
- Windows Server® 2008 Standard x64 Edition with Service Pack 2
- Windows Server® 2003 R2 Standard x86 Edition with Service Pack 2
- Windows Server® 2008 R2
- Windows 7® Professional (32-bit and 64-bit)
- Windows Vista® Business with Service Pack 3 (32-bit and 64-bit)
- Windows XP® Professional with Service Pack 2 (32-bit)
- Intel® Pentium® 4 processor (minimum)
- 2 GB RAM
- 60 GB hard drive (minimum) / 160 GB (recommended)
- Network interface card

Software Requirements

UNIX Operating System

- SMCII requires Solaris™ 10.
- The SMCII workstation must have a default route configured. To determine this, enter this command:

  ```
  netstat -rn
  ```

  In the response, look for **0.0.0.0** or **default**.
- Before installing SMCII, download and install the recommended patches for your system from the Sun Web site:

  www.sun.com/software/download/index.html
- 40 GB of free hard disk space dedicated to SMCII.
- Swap space of at least 2 GB is required to run the Web client.
- Firefox (version 3.x) Web browser is supported.
- Internet Explorer 8 Web browser is supported.
- Javascript must be enabled in Firefox to run the Web client.
- The SMCII installer will use the */tmp* directory to extract the install package. If the */tmp* directory does not have enough disk space, the following message displays to indicate that the root directory will be used for this purpose:

  Preparing to install...
  WARNING: /tmp does not have enough disk space!
  Attempting to use / for install base and tmp dir.
- The server system must be configured with as much swap space as available RAM, up to a maximum of 8 GB.

  For example, if the system has 4 GB of RAM, it should be configured with 4 GB of swap space.

  The size of available swap can be set in many ways, including when the system is initially partitioned. Here is one way to increase swap space on a system that does not require new partitions:

  ```
  mkfile 4096m /export/data/swapfile

  swap -a /export/data/swapfile
  ```

  These two commands will add a 4 GB swap file. The size and the name of the file are up to you. The "swap -a" command is only effective for the current session. To permanently add this additional swap to the system, add the following line to the */etc/vfstab* file, which is read on each reboot:

  ```
  /export/data/swapfile - - swap - no -
  ```

Windows Operating System

- SMCII requires Windows Server® 2008 Standard (SP2), or Windows Server® 2003 R2 Standard (SP2).
- The SMCII workstation must have a default route configured. To determine this, enter this command:

  ```
  netstat -rn
  ```

  In the response, look for **0.0.0.0** or **default**.
- Before installing SMCII, download and install the recommended updates for your system from the Microsoft Web site:

  www.update.microsoft.com
- 40 GB of free hard disk space dedicated to SMCII.
- Physical memory of at least 2 GB is required to run the Web client.
- Firefox (version 3.x) Web browser is supported. To ensure the proper display of timestamp values in Windows Server® 2003 R2 (Japanese Edition), it is recommended that the Japanese version of Firefox be installed.
- Internet Explorer 8 Web browser is supported. (**Note**: The SMCII browser address must be added to the Trusted Sites list to view appropriate results with Internet Explorer 8 Web browser on Win2008 Server.)
- Javascript must be enabled to run the Web client.

Third-party Software

The following third-party software is used in SMCII:

- Java:1.6.0_14
- JBoss: 5.1.0
- MySQL (Windows): 5.1.34
- MySQL (Solaris): 5.1.32 NDB 7.0.5

Feature Constraints

SMCII offers some features that are not supported on certain platforms, or cannot be combined with each other. A typical SMCII configuration can support virtually any combination of the following:

- operating system (32- or 64-bit)
- IPv6 or IPv4 addresses
- Pairing/Replication

Listed below is a brief overview of the features that have specific constraints.

Clustering

The Clustering feature is only supported on Solaris 10. Clustering is a form of high availability which allows multiple, active servers to remain synchronized. Users can access SMCII on any server in the cluster at any time. All changes made to one server are immediately and automatically mirrored on all other servers in the cluster.

IPv6 is supported, but the servers must be dual-stack because the cluster traffic must use IPv4 addresses.

HARemote Viewer

The HARemote Viewer feature is only recommended for legacy SMC users with SSEs, SEEs, SCEs, or SAEIIs that are running firmware versions prior to 3.4, and have not already had IPSec disabled. Note that there is no firmware released for SAEII that is 3.4 or greater, so this applies to all SAEIIs.

HARemote is only supported on Solaris 10 or Windows Server 2003, and does not support 64-bit or IPv6 addresses.

Luna Integration

The **Key Storage** selection in the SMCII is used to store private keys in one of two places—in the SMCII database, or in a Luna HSM (Hardware Security Module) with firmware version 4.4 or higher. Luna integration is supported on all operating systems, and supports both IPv6 and IPv4 addresses. However, the servers must be dual-stack because the Luna only supports IPv4 addresses.

The Luna software installation CD includes two installs for Solaris and for Windows—a 32-bit version and a 64-bit version. To integrate the Luna with the SMCII, you must install the 32-bit version of the Luna software.

Port Assignments

The tables in this section describe all of the ports that are necessary for the operation of SMCII. The intended use of these tables is to assist in the configuration of firewalls. Table 2-1 is relevant for both IPsec and non-IPSec; table 2-2 is relevant to IPsec only. There are certain ports that only need to be open when using either replication or clustering, as noted in the **Description** column.

Note: The following ports must be opened specifically for Windows 2008 Server: UDP 161, UDP 162, TCP 8080, TCP 8443, and FTP 21.

Table 2-1 Port and Protocol Assignments (IPsec and non-IPSec)

Port	Protocol	Function	Description
21	TCP	FTP	This is used to download firmware to SEE, SAEII, SSE, and SCE devices. If it is blocked, you will not be able to download firmware to these device types.
69	UDP	TFTP	This port is used to download firmware to SLE devices. If it is blocked, you will not be able to download firmware to these devices.
161	UDP	SNMP	This is used by SMCII for: - SLE Management - Trap Forwarding - SNMP Proxy If you are not using any of these features, and not managing SLE devices, this port can be blocked.
162	UDP	SNMP	This is used by SMCII for: - SLE Management - Trap Forwarding - SNMP Proxy If you are not using any of these features, and not managing SLE devices, this port can be blocked.
3306		MySQL	REPLICATION ONLY: This port is used for MySQL replication. It can be blocked if you are not using replication.
8080	TCP	HTTP/SSL	This is used by SMCII Server to communicate with web browser clients. It must be open. When installing SMCII on a Windows operating system, ensure this port is not being used by any Web service (for example, IIS Web Service).
8443	TCP	HTTP/SSL	This is used by SMCII Server to communicate with web browser clients. It must be open.
8444	TCP	HTTP/SSL	This is used for communication between Paired servers. This port may be blocked if you are not using Pairing.
1098,1099, 3873,4444, 4445	TCP	JBOSS RPC	CLUSTER ONLY: These ports are used by JBoss to send messages between SMCII cluster nodes. They can be blocked if you are not using clustering.

Table 2-2 Port and Protocol Assignments (IPsec only)

Port	Protocol	Function	Description
IP(50)	ESP	IPsec	IPsec traffic between SMCII and the SSE, SEE, SAEII, and SCE devices. If you are not managing any of these device types, this port can be blocked.
500	UDP	ISAKMP	Used for IPsec key exchange between SMCII and the SSE, SEE, SAEII, and SCE devices. If you are not managing any of these device types, this port can be blocked.
4500	TCP	IPsec-NAT-T	Used for NAT-T traversal compatibility with IPsec.

Performance Factors

Several factors can negatively affect server performance. Keep the following in mind when configuring your system:

- The number of managed devices directly affects your system requirements and performance.
- These factors can also affect performance:
  - Network's physical layout
  - Slow connections
  - Overloaded gateways
  - Network stability

SMCII Password Requirements

Password Format Rules

SMCII user passwords must adhere to these format rules:

- Each password must be 8 to 16 characters in length.
- Password characters must be part of the ASCII alphanumeric and special character sets. Typical characters include: # _ % & $ *
- Each password must contain at least one uppercase letter, one lowercase letter, one numeric character (digit), and one special character. Spaces are not supported. For example, **Onetwo_3** would be an acceptable password.
- A password cannot contain three identical consecutive characters. For example, a password can contain **ss**, but not **sss**.
- A password cannot be the same as the username in any form. Nor can it contain a partial or duplicated username, or a backwards user name.
- A new password must be different from the old password.
- The SMCII password history count is 3, which means that, when setting the password, you cannot use any of the last 3 saved passwords. Once the fourth password is saved, you may use the first password again. It should be noted, however, that the SMCII Super User can change a password to any password regardless of the history.
- The SMC password retry count can be configured within SMCII. Refer to the *SMCII Online Users Guide* for information on this function.

  Note: The **DB Root User Password** (the MySQL password) that is required during SMCII installation must be 6 to 16 characters, and should not begin with a special character or include the $ symbol.

Customizing Password Requirements

SMCII allows you to customize user password strength criteria for your particular requirements. These customized rules apply only to user passwords and not to the SMCII database password created during installation. The following fields on the **Password Properties** screen in the SMCII can be customized:

- **Minimum Lower Case Characters**
- **Minimum Upper Case Characters**
- **Maximum Password Length**
- **Minimum Uppercase Characters**
- **Minimum Numeric Characters**
- **Minimum Special Characters**
- **Password History**

For more information on this feature, refer to the *SMCII Online Users Guide*.

- This page intentionally left blank -

Chapter 3

Installation Procedures

This chapter provides information on the installation of SMCII on a Solaris or Windows operating system. Instructions are provided for first-time installation, upgrade installation from a prior version, and database migration preparation. Steps for starting SMCII after installation are also included.

Before You Begin

Perform the following tasks prior to starting a new SMCII installation or upgrade.

Solaris

- Exit all programs before starting the installation.
- Stop and disable the Solaris SNMP Services.
  - Stop SNMP with the command **/etc/init.d/init.dmi stop**
  - Disable SNMP with the command **svcadm disable snmpdx sma**
- Disable the FTP service with the command **svcadm disable /network/ftp**.
- MySQL database server installed by other than SMCII must be stopped and disabled.
- In order to run SMCII after installation, Javascript must be enabled in Firefox.
- (Upgrades only) When upgrading a clustered network, you must add the following property to the **/etc/my.cnf** file in order to avoid the creation of duplicate tables, which can cause severe issues:

  lower_case_table_names=1

Windows

- Exit all programs before starting the installation.
- Stop and disable the following Windows Services. Port conflicts (shown in parentheses) will prevent the services from running concurrently with SMCII. (For additional information about the ports required by Windows Services, go to http://support.microsoft.com/kb/832017.)
  - SNMP service (port 161)
  - SNMP Trap service (port 162)
  - FTP Publishing service (port 21)
  - Application Layer Gateway service (port 21)
  - Trivial FTP Daemon (port 69)
  - IPSec services (ports 500 and 4500)

Note: *If the SNMP and SNMP Trap services are not disabled, SMCII will not receive traps from devices.*

- During a local/remote installation or uninstallation of the HARemote component, you may experience a brief loss of network connectivity, but it will automatically be restored by Windows. If you are planning to install the **HARemote** component (via the **Custom** installation), it is recommended that you close all network shares and stop any network file transfers before you begin.

- MySQL database server installed by other than SMCII must be stopped and disabled.
- In order to run SMCII after installation, Javascript must be enabled in Firefox.
- Remove McAfee® antivirus software prior to installing SMCII.
- Configure the server to use a static IP address. Obtaining an IP address automatically through DHCP is not recommended.

Database Migration

Database migration allows you to import settings from a legacy SMC database. Only data related to encryptor devices can be imported. You must have the legacy SMC database encryption and access passwords in order to perform this operation.

Caution

*If you are installing the new SMCII on the same computer on which the old SMC is currently installed, make sure you back up the legacy SMC database **before** proceeding with the data migration. Refer to Chapter 4, "Migrating From Legacy SMC" for legacy backup details.*

Note: *Migration is only supported from SMC versions 2.0.2b3199 and 2.1.*

Refer to Chapter 4, "Migrating From Legacy SMC" for details on the database migration procedure.

First-Time Installation

There are two methods for installing SMCII:

- **Console Mode Installation**—This installation method is performed entirely from the command line and is supported by all versions of Solaris and Windows.
- **GUI Mode Installation**—This installation method is launched from the command line and presents separate graphical screens for each phase of the installation. This installation can be performed locally at the server or remotely on machines with graphics capability.

Note: *In Solaris, when the installation is initiated, you may see the following message: Preparing to install...* ***smcSetup.bin: !: not found****.*

Please ignore this message. The installer will proceed with the installation.

Console Mode Installation

To perform a console mode installation, perform the following steps. Note that all commands are case-sensitive. Additionally, all options that are selected by default are marked with "**->.**"

1. At the command prompt:
   - In Solaris:
     Log in as a super user (root).
   - In Windows:
     Log on as the Administrator user.
2. Insert the SMCII installation CD and change to that drive.
3. Type the following command, and then press **Enter**:
   - In Solaris:
     . /smcSetup.bin
   - In Windows:
     smcSetup.exe -i console
4. The **Introduction** screen displays. Press **Enter** to continue.
5. The **License Agreement** screen displays. Type **Y** to accept, and then press **Enter** to continue.

6. The **Choose Install Set** screen displays. The following options are available:
   - **1 - Typical:** This option installs the SMCII application only (without HARemote). This is the default option.
   - **2 - Custom:** This option installs SMCII and any additional selected features, such as the **HARemote** application which is used for secure communication between the server and IPsec enabled devices. **Note**: This option is not available on Windows Server® 2008.

   Type **1** or **2**, and then press **Enter**.
7. Skip this step if you selected 1 (**Typical**) in the previous step. If you chose 2 (**Custom**) in the previous step, select the feature(s) to install with SMCII and then click **Next**.
8. The **Choose Install Folder** screen displays. The default installation path is:
   - In Solaris:
     /opt/SafeNet/SMCII
   - In Windows:
     C:\Program Files\SafeNet\SMCII

     To accept the default, press **Enter**. To specify an alternate install folder, type an absolute path, and then press **Enter**.
9. You are prompted to confirm the installation folder. If correct, type **Y**, and then press **Enter**. If incorrect, type **N** and repeat step 7.
10. The **Database Configuration** screen displays. Type a database root user password. To start over, type **back**, and then press **Enter**.

Note: *The password should be 6-16 characters in length, must contain at least one lowercase and one uppercase character, one special character, and a number. Do not start with a special character. You cannot use punctuation, spaces, or the following characters: + & = @ $*

---

11. The **Database Confirmation** screen displays. Re-enter the database password to confirm your original entry. To change the password, go to the next step and type **back**. Press **Enter** to return to the previous screen.
12. The **Pre-Installation Summary** screen displays. Review the information and press **Enter** to continue.
13. When installation has finished, the **Install Complete** screen will display. Press **Enter** to exit the install program.
14. (Windows only) Reboot the server and then verify that IPSec Service has not restarted. If the service started, stop and disable it.

You are now ready to start the SMCII application. Refer to page 33.

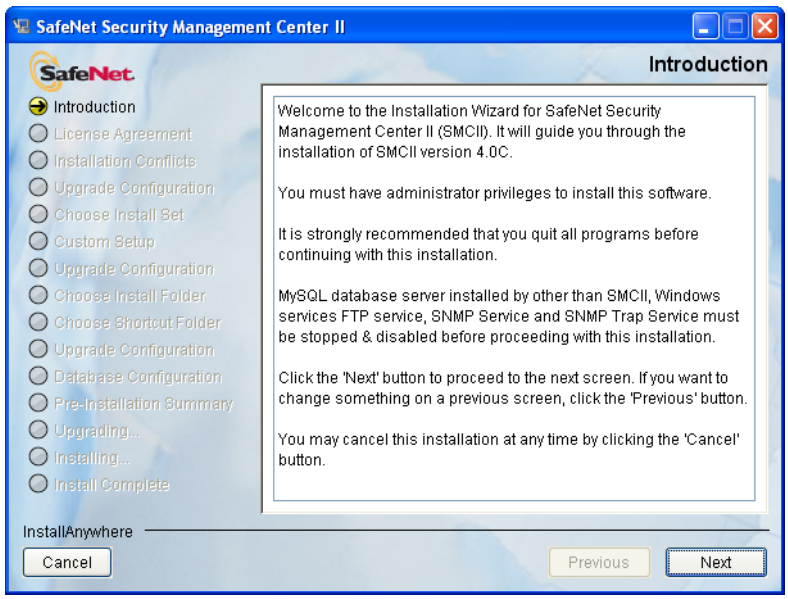
GUI Mode Installation

To perform a GUI mode installation, perform the following steps.

1. At the command prompt:
   - In Solaris:
     Log in as a super user (root).
   - In Windows:
     Log on as the Administrator user.
2. Insert the SMCII installation CD and change to that drive.
3. From the CD, run the appropriate file:
   - In Solaris:
     smcSetup.bin -i gui
   - In Windows:
     smcSetup.exe

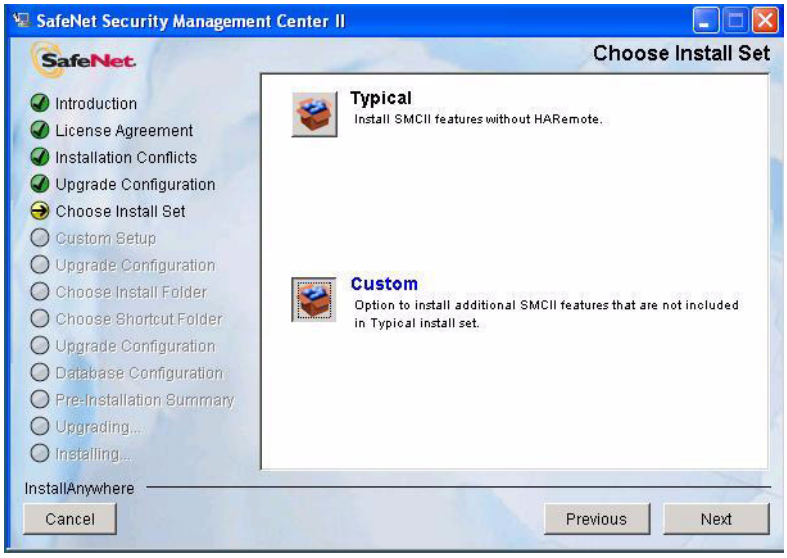
     The screen below displays with a progress indicator bar.

4. The **Introduction** screen displays. Click **Next**.

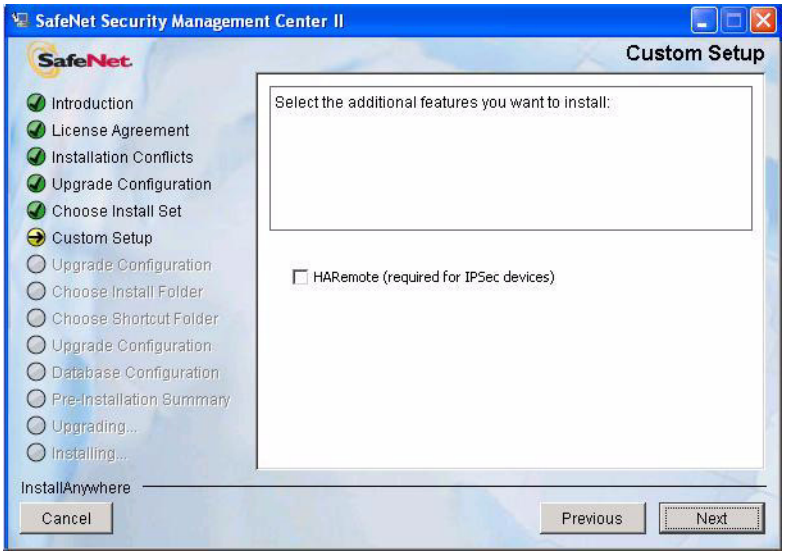


5. On the **License Agreement** screen, scroll down to read through the terms. Click **I Accept**, and then click **Next**. *(Note: You must scroll down in order to make the **I Accept** button active.)*

6. On the **Choose Install Set** screen, choose the type of installation to perform, and then click **Next**:
   - **Typical:** This option installs the SMCII application only (without HARemote). This is the default option.
   - **Custom:** This option installs SMCII and any additional selected features (such as the **HARemote** application which is used for secure communication between the server and IPsec enabled devices). **Note**: This option is not available on Windows Server® 2008.

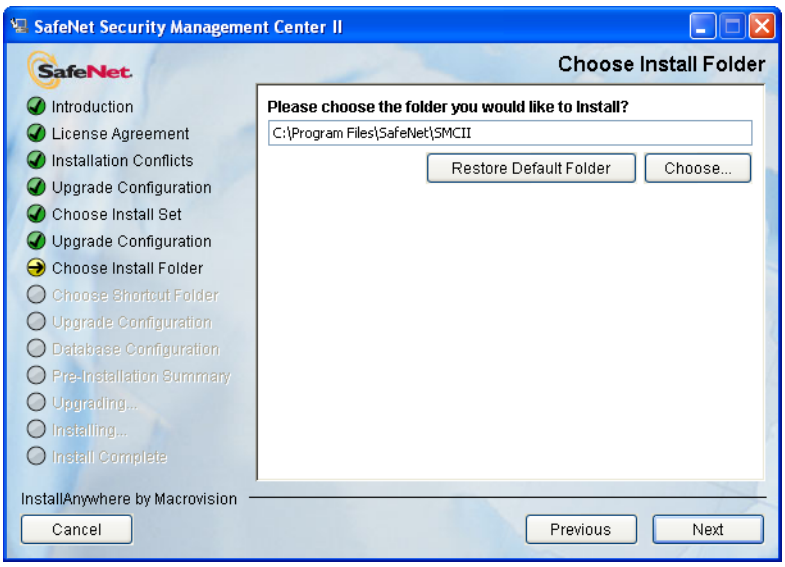


7. Skip this step if you selected **Typical** in the previous step. If you chose **Custom** in the previous step, select the feature(s) to install with SMCII and then click **Next**.



8. On the **Choose Install Folder** screen, the default installation path is:
   - **In Solaris:**
     /opt/SafeNet/SMCII
   - **In Windows:**
     C:\Program Files\SafeNet\SMCII

     To accept the default, click **Next**. To specify an alternate install folder, type an absolute path or click **Choose** and browse to the desired location, and then click **Next**.



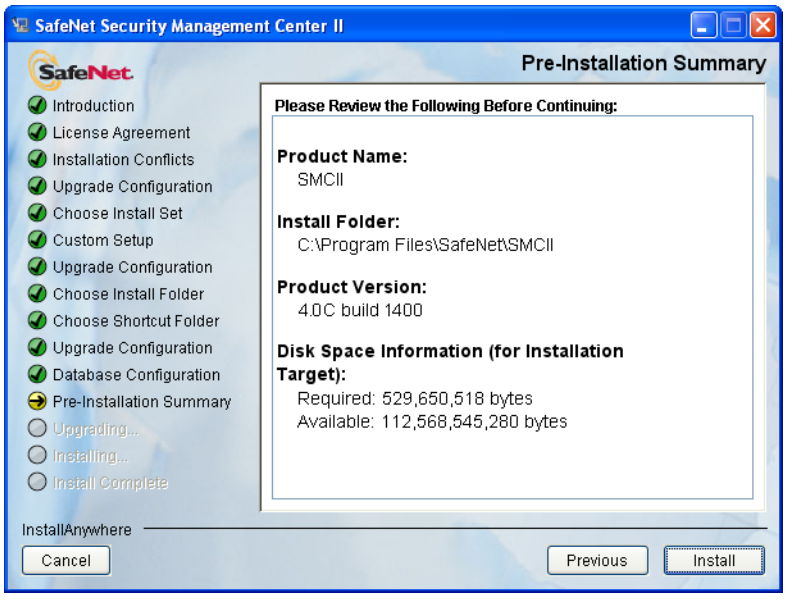
9. (Windows only) On the **Choose Shortcut Folder** screen, click Next to accept the default, or select the desired option and then click **Next**.

10. On the **Database Configuration** screen, specify the following (refer to the *SMCII User Password Requirements* on page 13):
    - **DB Root User Password**: Enter a database root user password for the SMCII database.
    - **Confirm DB Root User Password**: Re-enter the database root user password to confirm your original entry.

Note: *The database password should not start with a special character or include the $ symbol.*

Click **Next** to continue.

11. The **Pre-Installation Summary** screen displays. If you need to correct any information, do so now by clicking **Previous**. When ready to begin installation, click **Install**.



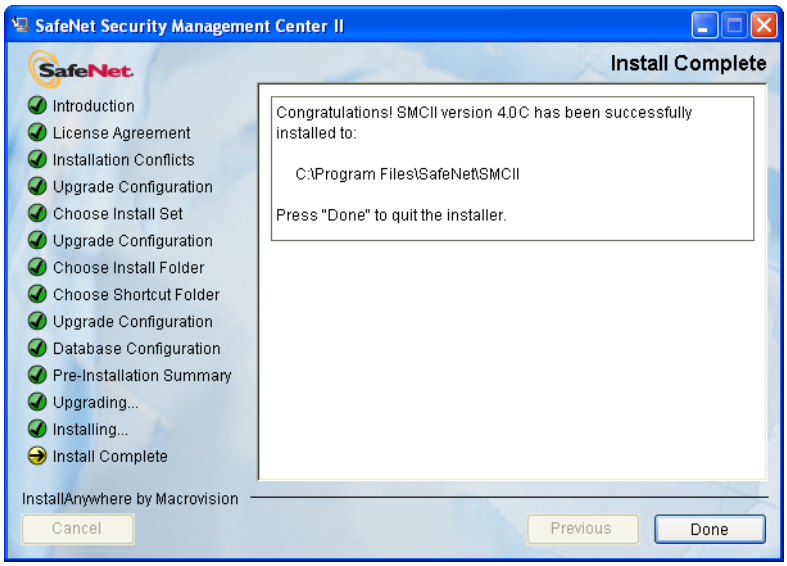
Caution

If you abort the installation at any time while files are being installed, you will be required to manually remove any files installed up to that point. To do so, delete the install folder, and delete the ***com.zerog.registry.xml*** *file.*

In Solaris, this file is located here:
/var/.com.zerog.registry.xml

In Windows, this file is located here:
C:\Program Files\Zero G Registry\com.zerog.registry.xml
By default, this directory is hidden. Change the Windows Explorer folder option to show the hidden folder in the Windows Control Panel.

12. A progress box displays, tracking the installation and configuration of SMCII. When the **Install Complete** screen displays, click **Done**.



13. (Windows only) Reboot the server and then verify that IPSec Service has not restarted. If the service started, stop and disable it.

You are now ready to start the SMCII application. Refer to page 33.

Upgrade Installation

There are two methods for performing an upgrade installation of SMCII:

- **Console Mode Installation**—This upgrade method is performed entirely from the command line and is supported by all versions of Solaris and Windows.
- **GUI Mode Installation**—This upgrade method is launched from the command line and presents separate graphical screens for each phase of the installation. This type of installation can be performed locally at the server or remotely on machines with graphics capability.

Note: *Upgrades are supported from legacy SMC version 2.0.2b3199 and 2.1.*

Note: *If you are upgrading from SMCII version 1.2, 2.0, 2.1, 2.6, or 3.x to the current version, all saved reports in the database will be deleted.*

Note: *In Solaris, when the installation is initiated, you may see the following message: Preparing to install...* ***smcSetup.bin: !: not found****.*

Please ignore this message. The installer will proceed with the installation.

Console Mode Upgrade Installation

To perform a console mode upgrade installation, perform the following steps. Note that all commands are case-sensitive. Additionally, all options that are selected by default are marked with "**->**."

As a precaution, back up the database before you begin. Refer to "Backup and Restore" on page 34.

1. At the command prompt:
   - In Solaris:
     Log in as a super user (root).
   - In Windows:
     Log on as the Administrator user.
2. Insert the SMCII installation CD and change to that drive.
3. Type the following command, and then press **Enter**:
   - In Solaris:
     . /smcSetup.bin
   - In Windows:
     smcSetup -i console
4. The **Introduction** screen displays. Press **Enter** to continue.
5. The **License Agreement** screen displays. Type **Y** to accept, and then press **Enter** to continue.

6. The **Upgrade Configuration** screen displays. Enter the number of your choice, and then press **Enter** to continue.
   - **1 - Update prior version** - With this type of upgrade, all data will be preserved. This option is highlighted by default.
   - **2 - Remove prior version and install this version (lose old data)** - With this type of upgrade, all files, including the database files, will be removed. Select this upgrade type only if you are certain that you want to start fresh and not retain any of your data.
7. If HARemote was previously installed, the **Custom Setup** screen displays with the HARemote option already selected. Either leave the option selected to re-install HARemote, or de-select the option to remove HARemote, and then click **Next**.

   If HARemote was not previously installed, the **Choose Install Set** screen displays. Choose the type of installation to perform, and then click **Next**:
   - **1 - Typical:** This option installs the SMCII application only (without HARemote). This is the default option.
   - **2 - Custom:** This option installs SMCII and any additional selected features, such as the **HARemote** application which is used for secure communication between the server and IPsec enabled devices. **Note**: This option is not available on Windows Server® 2008.

   Type **1** or **2**, and then press **Enter**.
8. Skip this step if you selected 1 (**Typical**) in the previous step. If you chose 2 (**Custom**) in the previous step, select the feature(s) to install with SMCII and then click **Next**.
9. (This step only applies to upgrades from version 2.1 or earlier.) Type the SMCII super user name, and then press **Enter**.
10. (This step only applies to upgrades from version 2.1 or earlier.) Type the SMCII super user password. (Note that the **Backspace** and **Delete** keys cannot be used to correct input. To start over, type **back**, and then press **Enter**.) Press **Enter** to continue after entering the password.
11. Type the SMCII database password. (Note that the **Backspace** and **Delete** keys cannot be used to correct input. To start over, type **back**, and then press **Enter**.) Press **Enter** to continue after entering the password.
12. The **Pre-Installation Summary** screen displays. Review the information and press **Enter** to continue.
13. The **Ready To Install** screen displays. Press **Enter** to begin installation. After a moment, the installation progress indicator appears.
14. When installation has finished, the **Install Complete** screen will display. Press **Enter** to exit the install program.
15. To start SMCII, refer to "Starting SMCII" on page 33.

GUI Mode Upgrade Installation

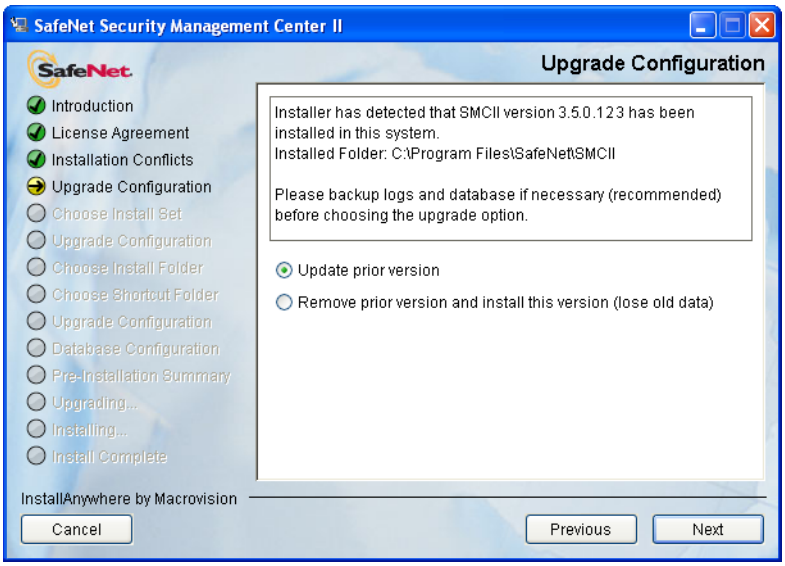
As a precaution, back up the database before you begin. Refer to "Backup and Restore" on page 34.

1. At the command prompt:
   - In Solaris:
     Log in as a super user (root).
   - In Windows:
     Log on as the Administrator user.
2. Insert the SMCII installation CD and change to that drive.
3. From the CD, run the file **smcSetup.bin -i gui** (Solaris) or **smcSetup** (Windows). The screen below displays with a progress indicator bar.

4. The **Introduction** page displays. Click **Next**.

5. On the **License Agreement** page, scroll down to read through the terms. Click **I Accept**, and then click **Next**. *(Note: You must scroll down in order to make the **I Accept** button active.)*

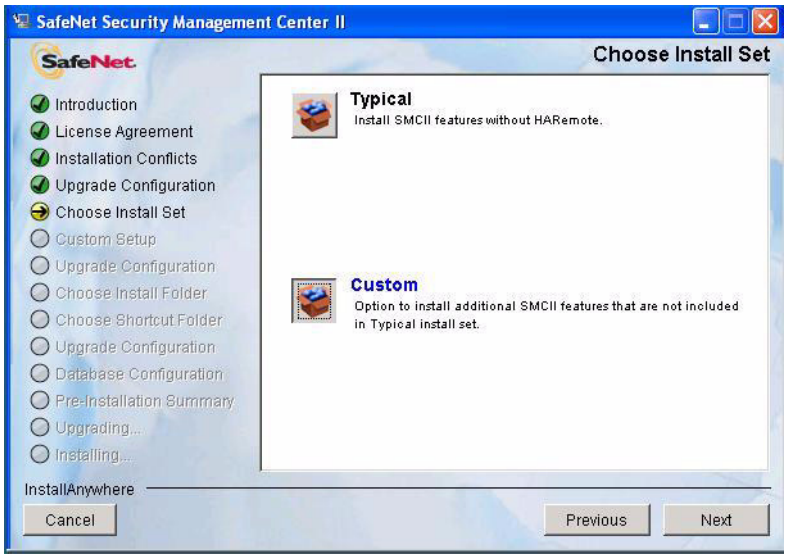
6. The first **Upgrade Configuration** screen displays. Select the type of upgrade you wish to perform, and then click **Next** to continue.
   - **Update prior version** - With this type of upgrade, all data will be preserved. This option is highlighted by default.
   - **Remove prior version and install this version (lose old data)** - With this type of upgrade, all files, including the database files, will be removed. Select this upgrade type only if you are certain that you want to start fresh and not retain any of your data.



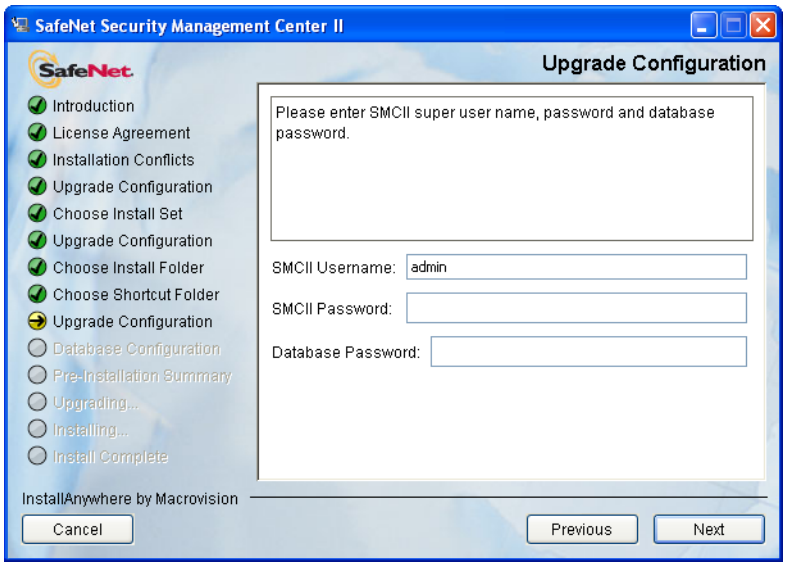
7. If HARemote was previously installed, the **Custom Setup** screen displays with the **HARemote** option already selected. Either leave the option selected to re-install HARemote, or de-select the option to remove HARemote, and then click **Next**.

   If HARemote was not previously installed, the **Choose Install Set** screen displays. Choose the type of installation to perform, and then click **Next**:

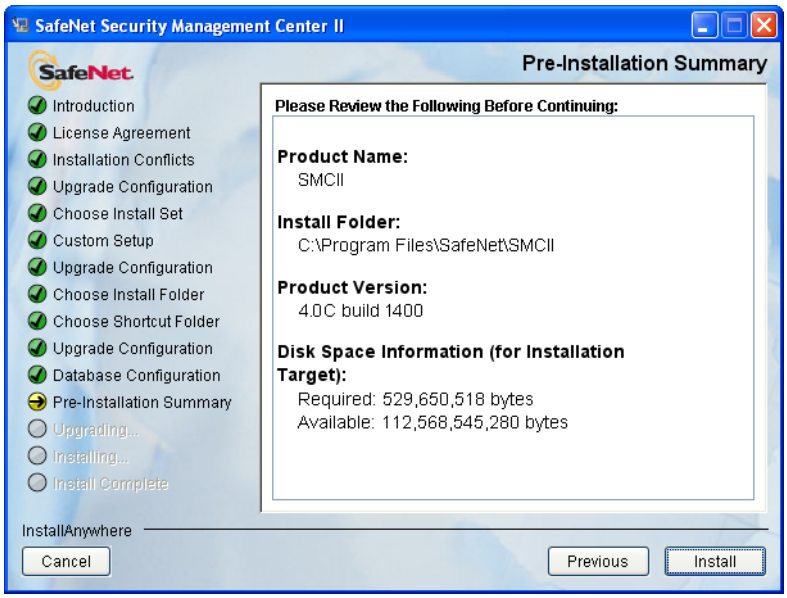
   - **Typical:** This option installs the SMCII application only (without HARemote). This is the default option.
   - **Custom:** This option installs SMCII and any additional selected features, such as the **HARemote** application which is used for secure communication between the server and IPsec enabled devices. **Note**: This option is not available on Windows Server® 2008.



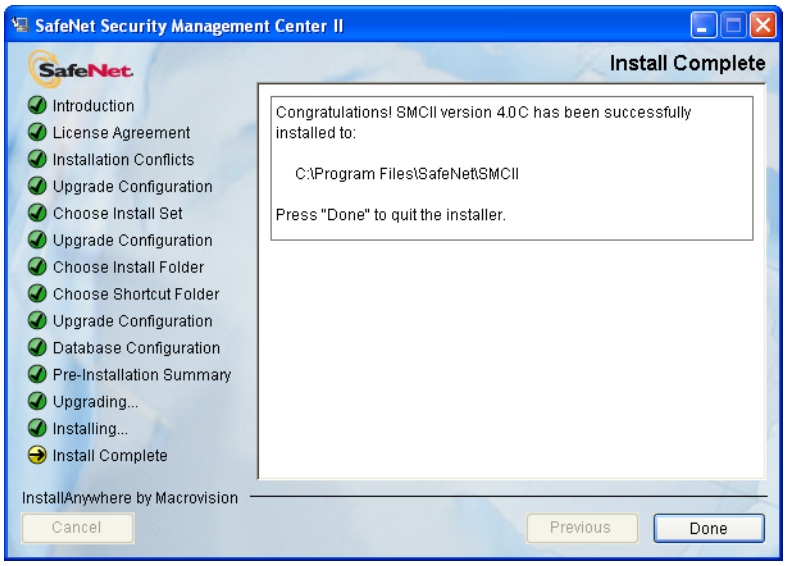
8. When the second **Upgrade Configuration** page displays, enter the **SMCII Username**, **SMCII Password**, and the **Database Password** (this is the MySQL DB User Password that was entered when SMCII was first installed). Click **Next**. (**Note:** SMCII Username and SMCII Password only applies to upgrades from version 2.1 or earlier.)



9. The **Pre-Installation Summary** page displays. If you need to correct any information, do so now by clicking **Previous**. When ready to begin installation, click **Install**.



10. You are prompted to wait while the system is configured. A progress box displays, tracking the installation and configuration of SMCII. When the **Install Complete** page displays, click **Done**.



You are now ready to start the SMCII application. Refer to page 33.

Starting SMCII

In order to run SMCII, Javascript must be enabled in your Internet browser application.

To start the SMCII application:

1. Launch your Internet browser application.
2. In the **Address** field, enter the IP address of the SMCII server, followed by the appropriate HTTP port number. An example of the correct command format is as follows:

   `http://192.168.0.1:8080`

   If the network has a DNS configured, and the server host name resolves correctly, `http://<servername>:8080` can also be used to start the application.

Caution

When logging in, SMCII will lock a user's account if they attempt to log in with an incorrect password five times; however, SMCII will never lock all super user accounts. At least one super user account will always remain unlocked.

3. When the login box displays, enter user ID **admin** and password **admin**.

Note: *If you have upgraded from a previous version, make sure you use the admin password that was used in the **previous** version.*

4. You will be immediately prompted to change the password. Enter the current password of **admin** and then specify and confirm a new password.

Note: *A password must be 8-16 characters in length, must contain at least one uppercase letter, one lowercase letter, one special character (# _ % & $ *), and one number. Spaces and punctuation are not allowed. The password cannot be the same, reverse, or substring of the user name.*

Backup and Restore

Database Backup and Restore

Database backups are essential and should be performed on a regular basis. SMCII database backup and restore procedures can be performed by using either of the following methods:

- utilities included with the MySQL® program (the database upon which SMCII is built), which requires the user to know the specific command line parameters to input to complete the procedures
- predefined scripts, which prompt the user for the appropriate input to complete the procedures

The MYSQL utility for backing up the database is called **mysqldump**, and is located in the **[SMCII_INSTALL_DIR]/mysql/bin** directory. The backup and restore procedures are run from the command line.

For complete documentation on using this utility, see *http://dev.mysql.com/doc/refman/5.0/en/mysqldump.html*.

For information regarding a backup and restore strategy, see *http://dev.mysql.com/doc/refman/5.0/en/backup-strategy-example.html*.

Refer to page 35 for details on these backup and restore procedures.

The predefined scripts for backing up and restoring the database are called **backupdb.bat** and **restoredb.bat** (for Windows), and **backupdb.sh** and **restoredb.sh** (for Solaris), and are located in the **[SMCII_INSTALL_DIR]/util/bin** directory. Refer to page 37 for details on these backup and restore procedures.

Note: *Firmware images that are uploaded to SMCII are stored on the server's file system—NOT in the SMCII database. During an SMCII database backup, these firmware images are not backed up. Make sure to store copies of the firmware images in a separate backup. If an SMCII system is restored from a backup to a new server, you will need to re-upload the firmware images to the new server.*

Scripts Backup

SMCII also provides a backup procedure for user-defined scripts stored in the **[SMCII_INSTALL_DIR]/** directory. To ensure full functionality in a restored database, it is imperative that you back up scripts after performing a **mysqldump** to backup or restore a database.

User-defined Scripts Backup Procedure

User-defined scripts are stored in the **[SMCII_INSTALL_DIR]/** directory, in a subfolder called **/scripts**. At runtime, when any script is executed, its contents are written to the **/gitdata** subfolder, which is also stored in the **[SMCII_INSTALL_DIR]/** directory. To ensure full functionality in the restored database, it is imperative that you back up the **/scripts** and **/gitdata** folders after performing a **mysqldump** to backup or restore a database.

Failure to perform this backup procedure will affect **Configuration > Scripts > Script History** page functionality, and previously run script instances and their details cannot be viewed.

To ensure proper functionality, while backing up the database from one instance of SMCII (smc1) to another instance of SMCII (smc2), separately copy the **/scripts** and **/gitdata** folders from the **[SMCII_INSTALL_DIR]**/ directory of smc1, to the **[SMCII_INSTALL_DIR]**/ directory of smc2.

Database Backup Procedure

During the backup procedure, you will be required to enter the database password specified during the installation of SMCII, so be sure to have this handy before you begin.

To run the backup program, perform the following steps:

1. Open a command prompt.
2. At the command prompt, change to:
   - In Solaris:
     [SMCII_INSTALL_DIR]/mysql/bin
   - In Windows:
     [SMCII_INSTALL_DIR]\mysql\bin
3. To back up the entire database, enter the following command:
   - In Solaris:
     ./mysqldump --hex-blob -u root -p apollodb > backup.sql
   - In Windows:
     mysqldump --hex-blob -u root -p apollodb > backup.sql
4. When prompted, enter the database password (the same database password specified during the installation of SMCII).

Database Restore Procedure

To run the restore procedure, perform the following steps:

1. Stop the appropriate service:
   - For Solaris:
     If the JBoss service is running, stop it using the following command:
     /etc/init.d/smcjboss stop
   - For Windows:
     If the SMC Application Server is running, stop it using the following command:
     - In the Windows Control Panel, open **Administrative Tools > Services**.
     - Right-click on **SMCII Application Server** and select **Stop**.
2. At the command prompt, change to:
   - In Solaris:
     [SMCII_INSTALL_DIR]/mysql/bin
   - In Windows:
     [SMCII_INSTALL_DIR]\mysql\bin
3. Enter the following command:
   - In Solaris:
     ./mysql -u root -p
   - In Windows:
     mysql -u root -p
4. To drop the existing database and create and empty one, enter the following commands:
   mysql>drop database apollodb;
   mysql>create database apollodb;
   mysql>quit
5. To restore the entire database, enter the following command:
   - In Solaris:
     ./mysql -u root -p apollodb < backup.sql
   - In Windows:
     mysql -u root -p apollodb < backup.sql

     (where "backup.sql" is the file name specified for your backup file)

6. Start the appropriate service:
   - For Solaris:
     /etc/init.d/smcjboss start
   - For Windows:
     - In the Windows Control Panel, open **Administrative Tools > Services**.
     - Right-click on **SMCII Application Server** and select **Start**.
7. When prompted, enter the database password (the same database password specified during installation of SMCII).

Database Backup Procedure (using scripts)

The predefined backup scripts can only be used to backup an existing database of an installed version of SMCII 4.0 or above. For SMCII version 3.5 and below, this procedure cannot be used. Instead, please refer the Database Backup Procedure section on page 35.

The predefined backup scripts are stored in the **[SMCII_INSTALL_DIR]/util/bin** directory. Use these scripts if you do not know the appropriate arguments to use with the command line database backup utilities.

In Windows

Run **backupdb.bat** with the following arguments:

Argument	Description
[-u] [--username]	<MYSQL username>
[-p] [--password]	<MYSQL password>
[-d] [--directory]	<Directory where backup file is to be created> (Defaults to [SMCII_INSTALL_DIR]/mysql/bin/)
[**-f] [--file]**	<Name of backup SQL file> (Defaults to smc_db_backup.sql)
[-c] [--cron]	<create timestamp distinguished files> This option ensures a unique file name every time the backup is executed. If this option is selected, the backup utility appends the timestamp of the backup file creation to the filename specified by the user on command-line or console. **Note:** This option helps to create recurring backup files on a periodic basis, rather than overwriting the existing backup files when executed.

Examples

The following command (with arguments specified) …

backupdb.bat -uroot -pSafenet_1 -d "C:\Files\" -f "backupfile.sql"

… will create the *C:\Files\backupfile.sql* file.

The following command (without arguments specified) …

backupdb.bat

… will prompt the user for the following:

Please enter username: root

Please enter password:

Note:

If a directory is not specified, it will take the default as SMCII_Install_Directory/mysql/bin.

If a filename is not specified, it will take the default filename as smc_db_backup.sql.

Therefore, the backup file path would be: SMCII_Install_Directory/mysql/bin/smc_db_backup.sql.

In Solaris

Run **backupdb.sh** with the following arguments:

Argument	Description
[-u] [--username]	<MYSQL username>
[-p] [--password]	<MYSQL password>
[-d] [--directory]	<Directory where backup file is to be created> (Defaults to [SMCII_INSTALL_DIR]/mysql/bin/)
[**-f] [--file]**	<Name of backup SQL file> (Defaults to smc_db_backup.sql)
[-c] [--cron]	<create timestamp distinguished files> This option ensures a unique file name every time the backup is executed. If this option is selected, the backup utility appends the timestamp of the backup file creation to the filename specified by the user on command-line or console. **Note:** This option helps to create recurring backup files on a periodic basis, rather than overwriting the existing backup files when executed.

Examples

The following command (with arguments specified) …

backupdb.sh -uroot -pSafenet_1 -d "/space/smc/" -f "backupfile.sql"

… will create the /space/smc/backupfile.sql file.

The following command (without arguments specified) …

backupdb.sh

… will prompt the user for the following:

Please enter username: root

Please enter password:

Note:

If a directory is not specified, it will take the default as SMCII_Install_Directory/mysql/bin.

If a filename is not specified, it will take the default filename as smc_db_backup.sql.

Therefore, the backup file path would be: SMCII_Install_Directory/mysql/bin/smc_db_backup.sql.

Database Restore Procedure (using scripts)

The predefined restore scripts can only be used to restore an existing database of an installed version of SMCII 4.0 or above. For SMCII version 3.5 and below, this procedure cannot be used. Instead, please refer the Database Restore Procedure section on page 36.

The predefined restore scripts are stored in the **[SMCII_INSTALL_DIR]/util/bin** directory. Use these restore scripts if you do not know the appropriate arguments to use with the command line database restore utilities.

In Windows

Run **restoredb.bat** with the following arguments:

Argument	Description
[-u] [--username]	<MYSQL username>
[-p] [--password]	<MYSQL password>
[-d] [--directory]	<Directory where backup file is located> (Defaults to [SMCII_INSTALL_DIR]/mysql/bin/)
[**-f] [--file]**	<Name of backup SQL file> (Defaults to smc_db_backup.sql)

Examples

The following command (with arguments specified)…

restoredb.bat -uroot -pSafenet_1 -d "C:\Files\" -f "backupfile.sql"

… will attempt to restore the *C:\Files\backupfile.sql* backup file.

The following command (without arguments specified) …

restoredb.bat

… will prompt for the following:

Please enter username: root

Please enter password:

The following command (without a directory or file specified) …

restoredb.bat -uroot -pSafenet_1

… will attempt to restore the default file from the default location (i.e., *C:\Program Files\SafeNet\SMCII\mysql\bin\smc_db_backup.sql*).

If the file does not exist, the script will return an error and then exit.

In Solaris

Run **restoredb.sh** with the following arguments:

Argument	Description
[-u] [--username]	<MYSQL username>
[-p] [--password]	<MYSQL password>
[-d] [--directory]	<Directory where backup file is located> (Defaults to [SMCII_INSTALL_DIR]/mysql/bin/)
[**-f] [--file]**	<Name of backup SQL file> (Defaults to smc_db_backup.sql)

Examples

The following command (with arguments specified)…

./restoredb.sh -uroot -pSafenet_1 -d "/space/smc/" -f "backupfile.sql"

… will attempt to restore the /space/smc/backupfile.sql (assuming SMCII_INSTALL_DIR is */space/smc/)*.

The following command (without arguments specified) …

./restoredb.sh

… will prompt the user for the following …

Please enter username: root

Please enter password:

The following command (without a directory or file specified) …

./restoredb.sh -uroot -pSafenet_1

… will attempt to restore the default file from default location (assuming SMCII_INSTALL_DIR is */space/smc/*, and the file looked for will be */space/smc/mysql/bin/smc_db_backup.sql*).

If file doesn't exist, the script will return an error and exit.

- This page intentionally left blank -

Chapter 4

Migrating From Legacy SMC

Database migration allows you to import settings from a legacy SMC database. Only data related to encryptor devices can be imported. You must have the legacy SMC database encryption and access passwords in order to perform this operation.

This chapter provides information on migrating your legacy SMC database to SMCII.

Caution

Migration is only supported from SMC versions 2.0.2b3199 and 2.1.

Before You Migrate

The migration procedure requires the execution of certain steps before legacy SMC is uninstalled. Make sure you complete the steps in this section before performing the data migration procedure described on page 46.

Back Up the Legacy SMC Database

Perform a manual backup of the legacy SMC database on the server as described below. These steps can be performed any time prior to upgrading to SMCII. Note that this backup procedure is not the same procedure normally used to backup and restore the SMC database.

While the procedure below must be performed prior to migration, you should also perform a standard legacy backup, as well as follow the new backup procedure in the migration instructions.

1. At the command prompt, change to:
   - In Solaris:
     [Legacy_SMC_INSTALL_DIR]/mysql/bin
   - In Windows:
     [Legacy_SMC_INSTALL_DIR]\mysql\bin
2. Type the command:
   - In Solaris:
     ./mysqldump pmdb --hex-blob -uroot –p > legacy_backup.sql
   - In Windows:
     mysqldump pmdb --hex-blob -uroot –p > legacy_backup.sql

     The file **legacy_backup.sql** will be created.

Note: ***IMPORTANT!*** *This file is created in the legacy install directory (**[Legacy_SMC_INSTALL_DIR]/mysql/bin** in Solaris, or **[Legacy_SMC_INSTALL_DIR]\mysql\bin** in Windows).*

Please copy this file to a location other than the legacy SMC install directory as this directory will be deleted when legacy SMC is uninstalled.

If you are installing the new SMCII on the same computer on which the old SMC is currently installed, you should now uninstall the old SMC.

3. After installing SMCII, import the backup file into a separate database called **legacydb**. (Use the current DB Root User Password (the MySQL password) when importing from legacy.sql.)
   - At the command line, type the following command:
     - In Solaris:
       ./mysql -uroot -p
     - In Windows:
       mysql -uroot -p
   - Next, type the command: **create database legacydb;**
4. Quit the **mysql** prompt and run the following command to import the backup file into the database:
   - In Solaris:
     ./mysql -uroot -p legacydb < legacydb_backup.sql
   - In Windows:
     mysql -uroot -p legacydb < legacydb_backup.sql
5. (Solaris only) In a cluster environment, shut down HighAssurance Remote by deactivating the security policy on all but one cluster node. Type the following command: **/etc/init.d/vpnclient stop**

Note: *After the migration is complete, make sure to* ***re-activate*** *HighAssurance Remote to ensure all clustered servers have an updated security policy.*

---

6. Proceed to "Performing a Data Migration" on page 46.

Performing a Data Migration

Data migration can only be performed after you have installed or upgraded SMCII. Make sure you have completed the steps in the "Before You Migrate" section before you proceed.

To perform a data migration, follow the steps below:

1. Click **Administration > Data Migration**.
2. Enter the **DB Encryption Password**. This is the database encryption password currently used for the legacy SMC database.
3. Click **Migrate**.

After You Migrate

After performing the database migration, perform the following step to drop the legacy database file.

1. Go to the command line.
2. Type the following command:
   - In Solaris:
     ./mysql -uroot -p
   - In Windows:
     mysql -uroot -p
3. Type the following command: **drop database legacydb;**

You will also need to re-certify SLE devices after migration.

Imported devices may have the same IP addresses as devices already in SMCII prior to import. Please check for these duplicate IP addresses and edit settings as necessary.

- This page intentionally left blank -

Chapter 5

Uninstall Procedures

This chapter provides information on uninstalling the SMCII application on the Solaris or Windows operating system.

Caution

Before SMCII is uninstalled, make sure that you back up the database in order to save it. Refer to "Backup and Restore" on page 34. You should also place the backup file onto an external media, such as a CD-RW or tape. For backup procedures, refer to the SMCII Online User Guide. You may also wish to run the debug mode in order to capture information about the SMCII installation, should any issues occur during uninstallation. This information could prove useful to Customer Support.

Uninstalling SMCII

Uninstall Procedure

There are two methods for installing SMCII:

- **Console Mode Installation** - This method is performed entirely from the command line and is supported by all versions of Solaris.
- **GUI Mode Installation** - This method is launched from the command line and presents separate graphical screens for each phase of the installation. This method can be performed locally at the server or remotely on machines with graphics capability.

Console Mode Uninstall

To uninstall SMCII, perform the following steps. You must have the administrator user name and password. Note that all commands are case-sensitive.

1. At the command prompt:
   - In Solaris:
     Log in as a super user (root).
   - In Windows:
     Log on as the Administrator user.
2. Type the following command, and then press **Enter**:
   - In Solaris:
     [SMCII_INSTALL_DIR]/Uninstall/Uninstall_SMCII
   - In Windows:
     [SMCII_INSTALL_DIR]\Uninstall\Uninstall_SMCII.exe -i console
3. The **Introduction** screen displays. Press **Enter** to continue.
4. The **SMCII Administration** screen displays. Enter the SMCII Administrator user name, and then press **Enter**.
5. Enter the SMCII Administrator user password, and then press **Enter**. Note that the password will be visible.
6. The **Uninstalling** screen displays indicating the progress of the uninstallation process.
7. When uninstallation has finished, the **Uninstall Complete** screen will display. Press **Enter** to exit.

If there are files that could not be removed during the uninstallation process, you will be notified and you will have to remove them manually. Check the SMCII install directory and the **/opt/SafeNet/HARemote** directory (in Solaris) or the **C:\Program Files\SafeNet\SMCII\haremote** directory (in Windows) for any extraneous files and remove them accordingly.

GUI Mode Uninstall

1. Run the uninstall utility:

   In Solaris:
   [SMCII_INSTALL_DIR]/Uninstall/Uninstall_SMCII -i gui

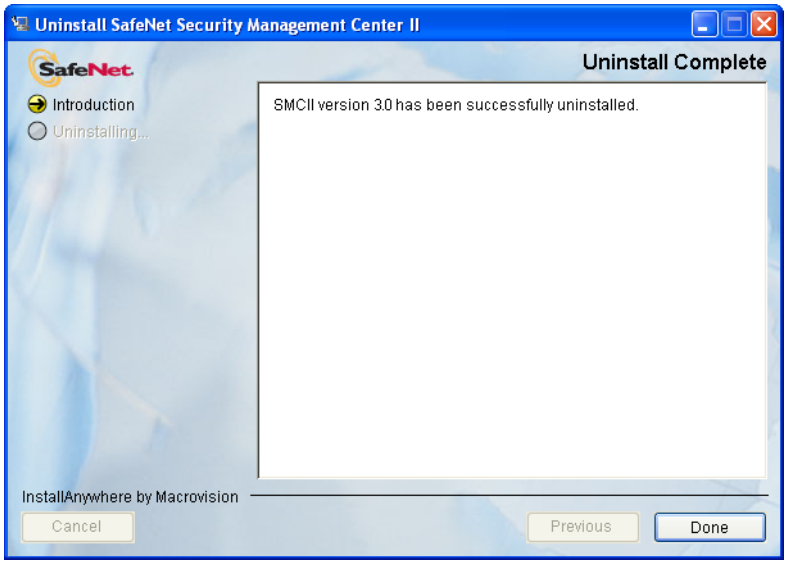
   In Windows:
   Click on **Start > Programs > SafeNet SMCII > Uninstall SMCII**.

   -or-

   In the Windows Control Panel, open **Add or Remove Programs**.
   Select the **SMCII** program, and then click **Change/Remove**.

2. The **Uninstall SafeNet Security Management Center II** screen displays. Click **Uninstall** to proceed.

3. You are prompted to wait while the system is configured. When the process is finished, the **Uninstall Complete** screen displays. Click **Done**.



If there are files that could not be removed during the uninstallation process, you will be notified and you will have to remove them manually. Check the SMCII install directory and the **/opt/SafeNet/HARemote** directory (in Solaris) or the **C:\Program Files\SafeNet\SMCII\haremote** directory (in Windows) for any extraneous files and remove them accordingly.

Manual Uninstallation

If the uninstall process should fail to start or fail during the uninstallation process, use the following steps to uninstall SMCII manually.

Solaris

1. If the JBoss service is running, stop it using the following command:

   /etc/init.d/smcjboss stop

2. If the MySQL database service is running, stop it using the following command:

   /etc/rc3.d/S98mysql stop

3. If the HighAssurance Remote service is running, stop it using the following command:

   /etc/init.d/vpnclient stop

4. Uninstall HighAssurance Remote using the script **/opt/SafeNet/HARemote/_uninst/uninstall.sh**.

5. Remove the SMCII installation directory.

6. Remove the following links:

   /etc/rc3.d/S99smcjboss

   /etc/rc3.d/S98mysql

   /etc/init.d/smcjboss

   /etc/init.d/mysql

   /etc/init.d/vpnclient

7. Remove the product registry file **/var/.com.zerog.registry.xml**.

Windows

1. Stop the SMCII and MySQL services.
   - In the Windows Control Panel, open **Administrative Tools > Services**.
   - Right-click on **SMCII Application Server** and select **Stop**.
   - Right-click on **SMCII MySQL** and select **Stop**.
2. Stop the HighAssurance Remote service (also in **Administrative Tools > Services**) if is running.
   - Right-click on **SafeNet IKE Service** and select **Stop**.
3. Uninstall HighAssurance Remote.
   - In the Windows Control Panel, open **Add or Remove Programs**.
   - Select the **SafeNet HighAssurance Remote** program, and then click **Change/Remove**.
4. Remove the SMCII services using the following commands:
   - **<SMCII_INSTALL_DIR>\jboss\bin\wrapper.exe -r <SMCII_INSTALL_DIR>\jboss\bin\wrapper.conf**
   - **<SMCII_INSTALL_DIR>\mysql\bin\mysqld.exe --remove "SMCII MySQL"**
   - **<SMCII_INSTALL_DIR>\util\bin\wrapper.exe -r <SMCII_INSTALL_DIR>\util\conf\wrapper.conf**
5. Remove the installation registry file **com.zerog.registry.xml**, located in **C:\Program Files\Zero G Registry.**

Note: *By default, the **Zero G Registry** directory is hidden. Change the Windows Explorer folder option to show the hidden folder in the Windows Control Panel.*

Chapter 6

Troubleshooting

This chapter provides information on issues that may be encountered during installation, upgrade, and uninstallation of SMCII.

Running the Installer in Debug Mode

Debug mode is a maintenance function that allows you to detect issues that may occur during the SMCII installation and uninstallation processes. The information captured during this process could prove useful to Customer Support should any issues arise.

Solaris

To capture debug output during the SMCII installation or uninstallation for a Solaris operating system, enter the following at the command line prior to beginning the installation or uninstallation procedure.

```
export LAX_DEBUG=true
```

Windows

To view or capture debug output from a Win32 installer, press and hold the **<CTRL>** key immediately after launching the installer and until a console window displays. Before exiting the installer, copy the console output to a text file to review later. On some Windows NT systems, run the installer once with the **<CTRL>** key pressed down (this resets the scroll back buffer for the console window), then quit and run the installation again.

Installer Logs

When SMCII is installed, an *SMCII_InstallLog.log* file is placed in the **[SMCII_INSTALL_DIR]** directory after the installer exits. If problems occur during the installation, view this log first to troubleshoot and resolve the problem.

If **Debug** mode is enabled for SMCII installation or uninstallation, debug output is sent to the console window. Before exiting the installer, copy the console output to a text file to review later.

If **Debug** mode is enabled, the following additional log files are placed in the installation root directory after the installer exits:

- *SMCII_PreInstallDebug.log*
- *SMCII_PostInstallDebug.log*
- *SMCII_PreUninstallDebug.log*
- *SMCII_PreUninstallDebug.log*

These log files contain system and installer variables, installer actions, and output results, and are typically used to troubleshoot issues by support personnel.

Prompt to Select Another Location During Installation

If the following message displays during an SMCII installation, please contact SafeNet Customer Support to request another SMCII Installation CD:

"Please select another location to extract the installer to"

Upgrading From a Prior Version (Solaris only)

When upgrading to the latest version of SMCII on Solaris, the installer may stall when attempting to shutdown the *jboss* process of the previously installed version of SMCII. It will usually stall after the following prompt (if you are using the command line installer):

"Installer is now ready to install SMCII version 3.5C onto your system at the following location:

/space/smc

PRESS <ENTER> TO INSTALL:"

If this issue occurs:

1. Stop the stalled installation process with Ctrl-C.
2. Kill the *jboss* process.

- OR -

1. Reboot the server machine.
2. Restart the installation.

java.lang.StackOverflowError During Uninstall

In rare circumstances, the installer may fail to create the installer properties file, *[SMCII_INSTALL_DIR]/Uninstall/installvariables.properties.* This file is required for uninstallation. Failure to create it will result in a java.lang.StackOverflowError message during uninstall.

If the uninstaller reports this error, rename the installer properties backup file *[SMCII_INSTALL_DIR]/Uninstall/installvariables.properties.bak* to *installvariables.properties*.

If this backup file is also missing, then uninstall SMCII using the Manual Uninstallation procedure (refer to page 53).

- This page intentionally left blank -