Contents

Chapter 1  Introduction
- Welcome ........................................................................................................... 1
- Overview ........................................................................................................... 2
- Definitions of Terms ........................................................................................... 2
- Before You Begin ............................................................................................... 3
- Hardware and Software Requirements ............................................................ 3
- Other Requirements ........................................................................................... 4
  - GINA ........................................................................................................... 4
  - Boot Record ................................................................................................. 4
  - Server Share ................................................................................................. 4
- Related Documentation ...................................................................................... 5
- Feedback .......................................................................................................... 5

Chapter 2  Master Installation
- Overview ........................................................................................................... 7
- Before You Begin ............................................................................................... 7
- Performing the Master Installation ..................................................................... 8
- After Installing ................................................................................................. 15

Chapter 3  Pointsec PC Management Console
- Overview ......................................................................................................... 17
- Starting PCMC ................................................................................................. 18
- Local Pointsec PC Settings ............................................................................... 19
  - Accessing Local Settings ............................................................................. 19
  - Editing Local Settings ................................................................................. 21

Chapter 4  Creating a Pointsec PC Profile
- Overview ......................................................................................................... 23
- Creating an Update Validation Password ......................................................... 24
- Creating a Configuration Set ........................................................................... 24
- Creating a Profile ............................................................................................. 27
  - Creating a New Profile ................................................................................ 28
  - Adding a Group to the New Profile .............................................................. 30
  - Creating a User Account ............................................................................ 32
  - Adding User Accounts to the Group ........................................................... 34
  - Configure the Temporary User .................................................................. 36

Chapter 5  Deploy Pointsec PC to Your Clients
- Overview ......................................................................................................... 39
- Deploy Pointsec PC to a Client .......................................................................... 40
- Utilize Logon Scripts ....................................................................................... 41
- Results of Script Execution ............................................................................ 41

Chapter 6  FAQ

Index .................................................................................................................... 73
Welcome

Thank you for choosing Pointsec PC. We hope that you will be satisfied with this solution and our support services. Check Point products provide your business with the most up to date and secure solutions available today.

Check Point also delivers worldwide technical services including educational, professional and support services through a network of Authorized Training Centers, Certified Support Partners and Check Point technical support personnel to ensure that you get the most out of your security investment.

For additional information on Pointsec PC and other Check Point products, please visit http://www.checkpoint.com or call Check Point at 1(800) 829-8391. For additional technical information, refer to: http://support.checkpoint.com.

Welcome to the Check Point family. We look forward to meeting all of your current and future network, application and management security needs.
Overview

Pointsec PC is a centrally managed, full disk encryption product that can encrypt data, operating systems and temporary files without relying on user interaction. Pointsec PC performs the encryption transparently to the user, who never needs to bother about what to encrypt and when.

Because Pointsec PC is centrally managed, a Pointsec system administrator can deploy, update, and upgrade settings, accounts and software from a central location.

Figure 1-1 illustrates the difference between file based encryption and full disk encryption.

Figure 1-1    Full Disk vs. File Based Encryption

Definitions of Terms

In this document, the following basic terms are used:

Table 1-1    Basic terms used in this document

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>The user’s computer where you deploy Pointsec PC after creating an installation profile.</td>
</tr>
<tr>
<td>Interactive Installation</td>
<td>Information about the installation is displayed for the user during the installation process.</td>
</tr>
</tbody>
</table>
Before You Begin

Before installing Pointsec PC (that is, the master and live installations), verify that a server share has been prepared and that the required software and hardware have been installed as described in the following three sections.

Hardware and Software Requirements

For the minimum hardware and software requirements for installing Pointsec PC see the Pointsec PC 6.3.1 Release Notes. The Release notes also document various restrictions you should know about before you start.

Note that:

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master installation</td>
<td>The administrator performs the initial installation. This installation includes installing Pointsec PC Management Console, the tool used for creating and configuring an installation profile, and for deploying that profile onto users’ workstations in order to install Pointsec PC.</td>
</tr>
<tr>
<td>Live installation</td>
<td>The installation on users’ workstations.</td>
</tr>
<tr>
<td>Locked out</td>
<td>A user becomes locked out from a Pointsec PC-protected computer if he or she has entered the wrong password too many times.</td>
</tr>
<tr>
<td></td>
<td>To re-gain access to the information on the computer, the user must get help from a Remote Help administrator.</td>
</tr>
<tr>
<td>Profile</td>
<td>To allow you to centrally manage Pointsec PC on users’ computers (so-called clients), the system uses install, update and uninstall profiles. This concept allows you to install, update and uninstall Pointsec PC from a central location.</td>
</tr>
<tr>
<td>Silent Installation</td>
<td>No information about the installation is displayed for the user during the installation process.</td>
</tr>
</tbody>
</table>
Other Requirements

- Systems that will not be used for system administrative purposes do not need .NET Framework.
- Root directory may not be compressed
- RAID is not supported
- Drives that are to be protected by Pointsec PC must be assigned a permanent drive letter and must not be hidden.

GINA

A Pointsec-specific GINA is installed during the Pointsec PC installation. The Pointsec-specific GINA replaces the system's existing GINA. Once this is done, Pointsec PC will chain the GINA that was replaced.

Although interoperability issues are rare, it is considered best practice to review your system for additional software that utilizes the GINA component.

Note - To configure Pointsec to not add the Pointsec GINA, please see the Pointsec PC Installation Guide.

At the time of writing, general information on GINAs is available at http://www.webopedia.com/term/g/gina.html.

Boot Record

During the Pointsec PC installation, the client's boot record is replaced.

Verify whether or not your system contains additional software that inserts a boot record.

Server Share

Before installing, it is very important that you prepare a secure server share to be used for storing the Pointsec PC recovery file. The recovery file is needed to restore encrypted information if the user account becomes locked out.

Note - Since anything you store on the local hard disk will be encrypted, you must NOT store the recovery file on the local hard disk.
Related Documentation

In addition to this Quick Start Guide, the following documentation is supplied together with the Pointsec PC software:

**Table 1-2  Pointsec PC documentation**

<table>
<thead>
<tr>
<th>Title</th>
<th>This document contains ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Pointsec PC Installation Guide</em></td>
<td>Information relevant when installing the master installation of Pointsec PC.</td>
</tr>
<tr>
<td><em>Pointsec PC Administrator’s Guide</em></td>
<td>Information relevant when creating and configuring an installation profile, and when installing Pointsec PC on users’ workstations (=live installations).</td>
</tr>
</tbody>
</table>
| *Pointsec PC Release Notes*       | • System requirements<br>• Current information about the product, such as:<br>  
  • new features and functions in the current release<br>• problems that have been fixed since the previous release, and<br>• any known issues about the current release. |

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please contact your technical sales contact if you have comments on this guide.
Chapter 2

Master Installation

In This Chapter

Overview .................................................. page 7
Before You Begin ........................................ page 7
Performing the Master Installation ................ page 8
After Installing ........................................... page 15

Overview

The master installation is the initial Pointsec PC installation process. It includes Pointsec PC Management Console, the tool used for creating and configuring an installation profile, and deploying Pointsec PC on users' workstations.

During the master installation, you create two user accounts. These accounts are needed to authenticate to Pointsec PC after the installation, otherwise the system will be unable to boot.

Before You Begin

Before you begin to perform the master installation, make sure you have the Pointsec PC license number available.
Performing the Master Installation

To install the Pointsec PC master installation:

1. Run the Pointsec for PC.msi file.

   The Pointsec for PC.msi file is available on the installation media in the following location:

   `\Pointsec_PC_EW_Ed_6.3.1\1_Pointsec for PC`

   The License Agreement window opens:

   ![License Agreement](image1)

   Figure 2-1   License Agreement

2. Read the license agreement and click Accept to continue or Cancel to abort the installation.

   If you click Accept, the Read me text window opens:

   ![Readme Text](image2)

   Figure 2-2   Readme Text

3. Select whether or not you would like to view the README.txt and click Next to continue.
If you selected not to view the README.txt file, the following Welcome window opens with a brief explanation of what to expect during the installation:

**Figure 2-3  Welcome Window**

4. Read the text in the window and click Next to continue.

The following dialog opens:

**Figure 2-4  Identification Information**

5. Add the following info:
   - Your name
   - Your company's name
Performing the Master Installation

- License number. Either write your license number in the **Serial Number** field or click **Insert** to browse for a Check Point license file (*.lic) to use.

**Note** - The information entered in this dialog can be changed when you prepare the installation profile to be deployed on users' workstations during the live installation. If you get a "Invalid entry, please correct and resubmit" message, the license key or Check Point license is not valid.

6. Click **Next** to continue.

   Next, you will add user accounts:

   **Figure 2-5** Add a User Account

   ![Add a User Account](image)

   7. Create the first two master installation user accounts.

      The user accounts created in the following steps are required to authenticate to Pointsec PC before booting the system. Without authentication, the system will not boot.

      a. In the Add a User account dialog, enter the following information:

         - In the **User account name** field, type **ADMIN1**.
         - Under **Authentication method**, make sure **Password** is selected.
         - In the **Password** and **Confirm password** fields, type **Password1**.

      b. Click **Next** to continue. The Add a user account dialog opens again, enter the following information this time:

         - In the **User account name** field type **ADMIN2**.
         - Under **Authentication method**, make sure **Password** is selected.
         - In the **Password** and **Confirm password** fields, type **Password2**.

      c. Click **Next** to continue. The Select Drivers window opens:
Performing the Master Installation

Chapter 2  Master Installation  11

Figure 2-6  Select Drivers

8. Do not select anything here. Just click Next to continue.

   The Protect Volumes window opens:

   Note - This dialog is relevant only if you have selected smart card as the authentication method for the user accounts you just created. In this Quick Start Guide, the use of smart cards is not described. Please see the Pointsec PC Installation Guide for more information.

9. Clear the Encryption checkbox for each volume in the list that appears.

   Note - Mounted volumes will not appear in the Volume list. Pointsec PC does not support mounted volumes. To protect a mounted volume, permanently assign a drive letter and restart the installation process.

10. Click Next to continue.

   The Recovery File Search Path dialog opens:
Performing the Master Installation

11. In the fields provided, set the location of your recovery and log files.

   **Note** - Do not store the recovery file on a local hard drive that is selected for encryption.

12. Click **Next** to continue.

   The Access to Network Paths dialog opens:

   **Figure 2-9**  Access to Network Paths

   Access to network paths - If a specific Windows user account has to be used to access the previously configured paths it can be configured here.

   In this guide we assume that the local system account (which is set by default) has access to the configured paths.

13. Click **Next** to continue.
The Ready to Install window opens:

**Figure 2-10  Ready to Install**

![Ready to Install](image)

14. Click **Next** to begin the Pointsec PC installation.

The Installing Pointsec window opens:

**Figure 2-11  Installing Pointsec PC**

![Installing Pointsec](image)

When the installation is complete, the InstallShield Wizard Completed window opens:
Performing the Master Installation

15. Click **Finish**. The Pointsec PC Installer Information window opens:

**Figure 2-13**  Pointsec PC Installer Information

16. Click **Yes** to reboot the system now.

During the reboot process, Pointsec PC is activated and performs the second part of the master installation. As part of the reboot process, you will be prompted to enter the user account name and password.

The User Account Information dialog opens:

**Figure 2-14**  User Account Identification

17. In the **User account name** field, enter **ADMIN1**. In the **Password** field, enter **Password**. Click **OK** to continue.

The Confirmation window opens:
The Confirmation window displays the date and time of your last successful logon.

18. Press **Continue** or wait for the window to automatically disappear.
   At this point, the operating system will reboot.

**After Installing**

Once the operating system is up and running, the following Pointsec PC icon will be displayed in the task bar:

**Figure 2-16** Pointsec PC Icon

**Note** - During this master installation process, encryption was not selected and therefore it will not be initiated.

Now that you have performed the initial master installation of Pointsec PC, you will need to become acquainted with Pointsec PC Management Console, PCMC, the administration tool used for managing Pointsec PC installation profiles and deployment onto users’ workstations. See "Pointsec PC Management Console" on page 17 for an overview of this tool.
Chapter 3

Pointsec PC Management Console

In This Chapter

Overview .......................................................... page 17
Starting PCMC .................................................. page 18
Local Pointsec PC Settings .................................. page 19
  Accessing Local Settings ................................ page 19
  Editing Local Settings ................................... page 21

Overview

This chapter presents an overview of the Pointsec administration tool, Pointsec PC Management Console, or PCMC in short. PCMC is used for managing Pointsec PC installation profiles and deployment onto users’ workstations.

If you need a more detailed description of how to use PCMC and its settings, please see the Pointsec PC Administrator’s Guide.

The accounts used in this overview were specified in Chapter 2, “Master Installation”.

Note - Do not change any of the Pointsec PC settings while working through this chapter. Pointsec PC is highly configurable; selecting an unintended setting may lock you out of the system.
Starting PCMC

This section provides step-by-step instructions on how to open and run Pointsec PC.

To run Pointsec PC:

1. Start the Pointsec PC Management Console (PCMC) by selecting Start → All Programs.

2. In the list that appears, select Pointsec → Pointsec PC → Management Console.

   The Management Console Authentication window opens:

   ![Management Console Authentication](image)

3. Enter the following:

<table>
<thead>
<tr>
<th>In the field</th>
<th>Enter the following ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User account name</td>
<td>ADMIN1</td>
</tr>
<tr>
<td>Password</td>
<td>Password1</td>
</tr>
</tbody>
</table>

   **Note** - The account you use to authenticate is one of the accounts you created during the master installation. See chapter 2, “Master Installation” on page 7.

4. Click **OK** to start PCMC.

   The following window opens:
5. Navigate among the three different sections using the folder tree on the left side of the window or using the large icons under the Pointsec PC section of the window.

These are the three sections of PCMC:

- **Local** enables you to edit settings for the PC where PCMC is installed.
- **Remote** enables you to create and manage deployment profiles for your client PCs.
- **Remote Help** enables you to remotely reset user account passwords.

In this chapter, only **Local** settings will be described. For information on

- **Remote** settings, see chapter 4, “Creating a Pointsec PC Profile” on page 23
- **Remote Help** settings, see chapter 5, “Deploy Pointsec PC to Your Clients” on page 39.

**Local Pointsec PC Settings**

This section contains a brief overview of the features in the **Local** Pointsec PC section. A full description of the settings is beyond the scope of this Quick Start guide, but can be found in the Pointsec PC Administrator’s Guide accompanying the product.

The Local settings apply to the computer where you performed the master installation, including PCMC.

**Accessing Local Settings**

To access the Local settings:
1. Click the **Local** folder (see Figure 3-2).

The following window opens:

![Figure 3-3  Local Settings Overview](image)

The Local window contains the following sections:

- **Actions**
  - **Edit Settings** enables you to edit the Pointsec PC settings for the local PC.
  - **Print Settings** enables you to print the active Pointsec PC settings on the local PC.
  - **Export Settings to CSV File** exports the active Pointsec PC settings to a CSV file.
  - **View Local Log Database** enables you to view the Pointsec PC logs generated by the local PC.
  - **Export Local Log Database** enables you to export the Pointsec PC logs generated by the local PC.
  - **Status** displays general status information regarding Pointsec PC on your local PC.
  - **Encryption** displays the encryption status for your local PC.

**Note** - Encryption is not enabled in this example since it was not selected during installation.
Editing Local Settings

To edit local Pointsec PC settings:

1. Click **Edit Settings** to access this feature of Pointsec PC.

   The following window opens:

   ![Edit Settings](image)

   The **Local** settings contain the following levels:

   - **System Settings** - the global settings for Pointsec PC. If a setting is not enabled on this level, it will not be available on the group level.

   - **Groups** - decides what settings will be available for individual user accounts.

2. To edit a setting, double-click the setting. The available options for the setting are displayed, and you can set the appropriate option.
Chapter 4

Creating a Pointsec PC Profile

In This Chapter

Overview
Creating an Update Validation Password
Creating a Configuration Set
Creating a Profile

Overview

As described in “Pointsec PC Management Console” on page 17, PCMC consists of a section called Remote. Pointsec PC profiles are created, edited and managed in the Remote section.

To centrally manage your clients, Pointsec PC uses four types of profiles: install profiles, update profiles, upgrade profiles, and uninstall profiles. This concept allows you to install, update, upgrade from Pointsec for PC 4.x/5.x, and uninstall clients, all from a central location.

In this chapter, you will learn how to create a working profile that is ready for client deployment. You can modify the profile after creating it.

Creating a profile can be divided into the following steps:

• Creating an update validation password, see page 24
• Creating a configuration set, see page 24
• Creating a profile, see page 27.
Creating an Update Validation Password

When working through the steps outlined in this chapter, modify the search paths, user account names, password, etc., to personalize the profile to your environment.

**Note** - Please read and follow the steps in Chapter 2, “Master Installation” prior to working and reading through this chapter. Remember that once the profile is created, the Master Install profile should be removed and subsequently reinstalled using the profile created in this chapter.

**Creating an Update Validation Password**

To create a profile, you must first set an Update Validation Password.

To use profiles securely, a shared secret is required between your profiles and the clients that you are managing. This shared secret is a password that is set for your clients and your profiles.

The profile will inherit its password from the workstation on which the profile is created.

**To create the Update Validation password:**

1. Start Pointsec PC Management Console (PCMC) as described in “Starting PCMC” on page 18.
2. Select Local → Edit Settings → Install.
3. Double click Set Update Validation Password and enter the password in the field provided.

   The password entered in this step will be used in the profile you create as the shared secret which verifies whether or not a profile can be imported.

**Creating a Configuration Set**

Before creating the new profile, you must first create a Configuration set. Configuration sets make profile management, editing and deployment easier.

**To create a configuration set:**

1. In PCMC, select Remote. The following window opens:
1. In the **New Configuration Set** box (see Figure 4-1) click **New Set**.

The following window opens:

**Figure 4-2**  **New Configuration Set Wizard**

2. Click **Next** to continue.

The following window opens:

**Figure 4-3**  **New Configuration Set Wizard - Name**

...
3. Enter a descriptive name for the configuration set.  

**Note** - You can select to automatically create a directory structure if you want Pointsec PC to create folders, however this won't be described in this guide. For more information on this, see the *Pointsec PC Administrator's Guide*.

4. Click **Next** to continue.

   The following window opens:

   **Figure 4-4** New Configuration Set Wizard - Path Settings

   ![Path Settings Window]

5. Specify a **Profile Storage Path**, the path to a directory that will hold the profiles while you edit them. The profiles you are working on will be stored in this directory until you publish them. When you’ve configured a storage path, click **Next**.

   Best practice is to specify all paths in UNC format (Written in the form: `\\<server>\<share>\...`).

   **Note** - You must click **Add** for the path to be included in the set.

6. Specify an **Update Profile Path**, the path to a directory from which clients will pull update and uninstall profiles. When finished, click **Next**.

   **Warning** - Never set your Update Profile Path so it matches the Profile Storage Path. If the same settings are implemented on the clients it will cause them to start importing profiles that you're still working on and that haven't been published. The Profile Storage path is your "personal profiles in progress" storage.

7. Specify an **Install Path**, the path to a directory containing the Pointsec PC installation package. When finished, click **Next**.

8. Specify a **Central Log Path**, a path to a directory into which the clients in the set will copy their log files. When finished, click **Next**.
9. Specify a **Recovery Path**, a path to a directory into which the clients in the set will copy their recovery files. When finished, click **Next**.

10. Specify an **Upgrade Path**, a path to a directory in which upgrade package files are located and from which clients download these files. When finished, click **Next**.

11. Create the set by clicking **Finish**:

   ![Figure 4-5](image)

   Figure 4-5

   12. The set is created and you are now returned to the PCMC GUI.

   Note that the set configuration is saved when the set is created.

   You see the configuration set you created under the **Remote** branch of the PCMC folder tree, as shown in the following image:

   ![Figure 4-6](image)

   Next, you will create the profile.

---

### Creating a Profile

**In This Section**

- Creating a New Profile: page 28
- Adding a Group to the New Profile: page 30
- Creating a User Account: page 32
- Adding User Accounts to the Group: page 34
- Configure the Temporary User: page 36
Creating a New Profile

Once the Update Validation password is set and the configuration set has been created, you can create a Pointsec PC profile.

To create a Pointsec PC profile:

1. Right-click the Profile icon and select New Profile as shown in the following figure:

![New Profile](image)

The New Profile menu contains the following options:

- Install Silent
- Install Interactive
- 4.x/5.x Upgrade Silent
- 4.x/5.x Upgrade Interactive
- Update
- Uninstall

2. Select Install Silent.

The following dialog opens:

![Name and Protection](image)

3. Enter the name of the profile and its password in the fields provided.

**Note** - The Profile Protection password is used to protect the profile from unauthorized editing and should not be confused with the Update Validation password.

The following dialog opens:
Figure 4-9

4. Since we are making this profile from scratch we do not want to base the profile on our existing settings or any existing profiles, so leave that check box unchecked. Then click Next and Finish to complete the wizard.

**Editing Install Settings**

Select Install, and edit the Install settings according to the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Enter the name of your company.</td>
</tr>
<tr>
<td>Product Owner</td>
<td>Pointsec Client at</td>
</tr>
<tr>
<td>Product Serial Number</td>
<td>Enter your Pointsec PC license number or choose your Check Point license file.</td>
</tr>
<tr>
<td>Set Log Password</td>
<td>Enter a strong password that you'll remember. This password will be used to protect the log files.</td>
</tr>
<tr>
<td>Select Volume Protection</td>
<td>Open and check that the following default values are set:</td>
</tr>
<tr>
<td></td>
<td>Algorithm: AES</td>
</tr>
<tr>
<td></td>
<td>Volumes 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11 selected for preboot authentication and encryption.</td>
</tr>
</tbody>
</table>

**Note** - Ensure that the upgrade, update profile, recovery, and central log path have the same values as the paths entered when creating the set.

This completes the system settings part of your new profile. Next, you will populate the system with groups.
Adding a Group to the New Profile

The group created in this section will be the group that contains the System Administrator users. For this reason, this group will be assigned system administration level permissions.

To add a group to the new profile:

1. Right-click the Groups icon and select New Group.

The following dialog opens:

2. In the field provided, enter ‘My System Admins’ as the name for the group and click OK.

Note - Pointsec PC can only be as secure as its configuration. There are several considerations to be made related to group and user account settings. Therefore you need to review what settings best suit your organization.

For example, in this guide we will not grant permissions to anyone besides members of the system admin group to provide Remote Help. The reason for this is that we have configured the System Administrators as fixed password user accounts who are allowed to receive remote help. If user accounts outside the system administrators group would be allowed to provide remote help, they could potentially gain System Administrator access.

Please contact your Sales Engineers for assistance with suggestion for a best practice for your organization.
Adding a Group to the New Profile

**Editing Group Settings**
1. Select the group you want to edit, for example My Sys Admins, and then **Group Settings**.
2. Change the setting Set Group Authority Level to <=9 (Group Authority Level of 9, and allow changing settings of groups with equal authority level).

**Editing Permissions Settings**
1. Select **Group Settings → Permissions**.
2. Assign the following permissions/values for the group you just created:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Assign this value:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Credentials</td>
<td>Yes</td>
</tr>
<tr>
<td>Change Single Sign-On</td>
<td>Yes</td>
</tr>
<tr>
<td>View Logs</td>
<td>Yes</td>
</tr>
<tr>
<td>Uninstall</td>
<td>Yes</td>
</tr>
<tr>
<td>Management Console Login</td>
<td>Yes</td>
</tr>
<tr>
<td>Create Recovery Media</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow Logon to Hibernated System</td>
<td>Yes</td>
</tr>
<tr>
<td>Change to Fixed Password</td>
<td>Yes</td>
</tr>
<tr>
<td>Change to Dynamic Token</td>
<td>Yes</td>
</tr>
<tr>
<td>Change to Smart Card</td>
<td>Yes</td>
</tr>
<tr>
<td>Change Credentials in the Pointsec PC tray</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Editing Privileged Permissions Settings**
1. Select **Group Settings → Privileged Permissions**.
   Assign the following permissions/values for the group you just created:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Assign this value:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Permissions</td>
<td>Yes</td>
</tr>
<tr>
<td>Change Privileged Permissions</td>
<td>Yes</td>
</tr>
<tr>
<td>Create User Accounts</td>
<td>Yes</td>
</tr>
<tr>
<td>Create Groups</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced Profile Editing</td>
<td>Yes</td>
</tr>
<tr>
<td>Create Profiles</td>
<td>Yes</td>
</tr>
<tr>
<td>Remove User Accounts</td>
<td>Yes</td>
</tr>
<tr>
<td>Remove Groups</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Creating a User Account

To avoid having to set up a specific user account per workstation, Pointsec PC offers an user account type called temporary user. A temporary user account contains the following characteristics:

- A temporary user account is converted into a normal user account when a successful login is completed.
- The temporary user account’s username and password can be communicated to your organization.
- The first time your users are prompted to authenticate themselves to Pointsec PC in the preboot environment, they will use the temporary user account’s username and password. When the user logs on again, she will be prompted to change her username and password to personalize the user account.

To create a temporary user account:

1. Create a new group. See “Adding a Group to the New Profile” on page 30 for additional information.
   
   For example purposes, name the group Local Users.

   Normally the default settings can be given to end users. However, since the default values are a compromise between security and usability, some of the values will be changed in the following steps.

2. Select Edit Settings → Groups → Local Users.

<table>
<thead>
<tr>
<th>Table 4-3</th>
<th>Privileged Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting</td>
<td>Assign this value:</td>
</tr>
<tr>
<td>Remove Profiles</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit System Settings</td>
<td>Yes</td>
</tr>
<tr>
<td>Access to Local</td>
<td>Yes</td>
</tr>
<tr>
<td>Access to Remote</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4-4</th>
<th>Remote Help Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting</td>
<td>Assign this value:</td>
</tr>
<tr>
<td>Provide &quot;Remote Password Change&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>Provide &quot;One-Time Logon&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>Receive &quot;Remote Password Change&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>Receive &quot;One-Time Logon&quot;</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Editing Remote Help Settings


2. Assign the following permissions/values for the group you just created:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Assign this value:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Profiles</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit System Settings</td>
<td>Yes</td>
</tr>
<tr>
<td>Access to Local</td>
<td>Yes</td>
</tr>
<tr>
<td>Access to Remote</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4-4</th>
<th>Remote Help Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting</td>
<td>Assign this value:</td>
</tr>
<tr>
<td>Provide &quot;Remote Password Change&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>Provide &quot;One-Time Logon&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>Receive &quot;Remote Password Change&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>Receive &quot;One-Time Logon&quot;</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Creating a User Account
3. Select **Group Settings**.

   Edit the settings for the group according to the instructions below; leave all settings not listed with the default value:

<table>
<thead>
<tr>
<th>Table 4-5</th>
<th>Group Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Comments</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Set an expiration date for this group.</td>
</tr>
</tbody>
</table>

   **Note** - Remember to set the expiration date well within the time frame that you expect your users to activate the temporary user account. If the configured date has passed, logon will not be possible with the temporary account.

4. Select **Group Settings → Logon**.

   For **Logon** settings, assign the following permissions/values for the group you just created:

<table>
<thead>
<tr>
<th>Table 4-6</th>
<th>Logon Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Comments</td>
</tr>
<tr>
<td>Set Max Failed Logons</td>
<td>5</td>
</tr>
</tbody>
</table>

5. Select **Group Settings → Authentication Settings → Fixed Password**.

   For **Fixed Password** settings, assign the following permissions/values for the group you just created:

<table>
<thead>
<tr>
<th>Table 4-7</th>
<th>Fixed Password Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Comments</td>
</tr>
<tr>
<td>Set Minimum Age</td>
<td>1</td>
</tr>
<tr>
<td>Set Maximum Age</td>
<td>90</td>
</tr>
<tr>
<td>Password History</td>
<td>5</td>
</tr>
</tbody>
</table>

6. Select **Group Settings → Permissions**.

   For **Permissions** settings, assign the following permissions/values for the group you just created:

<table>
<thead>
<tr>
<th>Table 4-8</th>
<th>Permissions Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Comments</td>
</tr>
<tr>
<td>Change Credentials</td>
<td>Yes</td>
</tr>
<tr>
<td>Change Single Sign-On</td>
<td>Yes</td>
</tr>
<tr>
<td>Uninstall</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Adding User Accounts to the Group

7. Select **Group Settings → Permissions → Remote Help**.

   For **Remote Help** settings, assign the following permissions/values for the group you just created:

   **Table 4-9**  Remote Help Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive &quot;Remote Password Change&quot;</td>
<td>Yes</td>
</tr>
<tr>
<td>Receive &quot;One-Time Logon&quot;</td>
<td>Yes</td>
</tr>
</tbody>
</table>

8. Select **Group Settings → Single Sign-On**.

   For **Single Sign-On** settings, assign the following permissions/values for the group you just created:

   **Table 4-10**  Single Sign-ON Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSO</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The group and user accounts are complete. The PCMC GUI appears as follows:

**Figure 4-12**  Pointsec PC GUI

Next, you must add user accounts to your groups.

### Adding User Accounts to the Group

To populate the **My System Admins** group:
1. Select **Groups → My System Admins.**

   **Figure 4-13**  Add User Account

2. Right-click **User Accounts** and select **Add User Account.**

   The following dialog opens:

   **Figure 4-14**  User Account Details

3. Enter the following:

   - In the **User account name** field, enter **SYSADMIN1**.
   - In the **Type of user account** field, select **Normal**.
   - In the **Authentication method** section, select **Password**.

   Click **Next** to continue.

   The following window appears:
4. In the Password and Confirm Password fields, enter My1secretpw.

   Remember the password requirements that was specified for the My System Admin group. In this dialog you can also force a password change.

   Click Next to continue. The summary window appears.

5. Click Finish.

   Repeat step 1 through step 5 to add the following two additional user accounts.

<table>
<thead>
<tr>
<th>Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSADMIN2</td>
<td>My2secretpw</td>
</tr>
<tr>
<td>SYSADMIN3</td>
<td>My3secretpw</td>
</tr>
</tbody>
</table>

Next, add the temporary user account.

**Configure the Temporary User**

To configure the temporary user:

1. Collapse the My System Admins group and expand the Local Users to show the User Account icon.

2. Right-click the User Account icon connected to the Local Users group and choose Add User Account.

   The following dialog opens:
3. Enter the following:
   - In the User account name field enter TEMPUSER.
   - In the Type of user account field select Temporary.
   - In the Authentication method section select Password.
   
   Click Next to continue. Another dialog box opens.

4. In the Password and Confirm Password fields, enter T3mpPWD.

   Remember the password requirements that were specified for the "Local Users" group.

   Click Next to continue, a summary dialog opens.

5. Click Finish.

   **Note** - When adding the temporary user account, you do not have the option of forcing a password change in the Password Details dialog (see Figure 4-15).

When deploying Pointsec PC with the temporary user account feature, you must manage the user account via the group the user account belongs to since when the temporary user account is activated to a normal user account, it changes username and unique identifier.

Now your profile is ready to be deployed to your client workstations.
Deploy Pointsec PC to Your Clients

In This Chapter

Overview

Deploy Pointsec PC to a Client

Overview

Deploying Pointsec PC to your clients essentially means that the software will be installed with the configurations set during the creation of the Installation profile (see chapter 4, “Creating a Pointsec PC Profile” on page 23).

To recap: this is what we selected when creating our profile:

- Silent installation profile.
- Specified our "global" system settings.
- Created the groups that should be available on the clients.
- Populated the groups with user accounts.

Now we should prepare and copy the Pointsec PC install package to a central location that our clients can access.
Deploy Pointsec PC to a Client

In This Section

<table>
<thead>
<tr>
<th>Utilize Logon Scripts</th>
<th>page 41</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results of Script Execution</td>
<td>page 41</td>
</tr>
</tbody>
</table>

In this section, the Pointsec PC installation package is prepared and copied to a central location to which clients have access.

**Note** - For example purposes it will be assumed that the share that is used for hosting the installation, recovery log, and update paths is available and that full permissions are granted to all users in your environment. In addition, we will assume that users are local administrators on their systems. For complete information on permission requirements, see the *Pointsec PC Installation Guide* and the *Pointsec PC Administrator’s Guide*.

To deploy Pointsec PC to a client:

1. When you created the Configuration Set (see “Creating a Configuration Set” on page 24), you also created a storage path (see Figure 4-5).
   a. Open an Explorer window to the path specified in the Storage Path field.
   b. Locate the Silent_Install_Profile.isp file. This file contains your configuration.

2. Browse to the folder 1_Pointsec for PC in the Pointsec PC installation media.

3. Copy the Silent_Install_Profile.isp profile file to the root of 1_Pointsec for PC.

   **Figure 5-1**
   ```
<table>
<thead>
<tr>
<th>Dirs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language Packs</td>
</tr>
<tr>
<td>Modules</td>
</tr>
<tr>
<td>Tools</td>
</tr>
<tr>
<td>Packages</td>
</tr>
<tr>
<td>1_Pointsec for PC</td>
</tr>
<tr>
<td>predefined</td>
</tr>
<tr>
<td>Profile</td>
</tr>
<tr>
<td>Silent_Install_Profile.isp</td>
</tr>
</tbody>
</table>
   ```

4. Copy the 1_Pointsec for PC folder (along with its content) to a server share that your end users can access.
Go through the following checklist to make sure you are ready for the deployment.

<table>
<thead>
<tr>
<th>Item</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile configuration is done.</td>
<td>✓</td>
</tr>
<tr>
<td>You have stored your system administrator credentials in a secure place.</td>
<td>✓</td>
</tr>
<tr>
<td>Server shares are set up.</td>
<td>✓</td>
</tr>
<tr>
<td>User permissions to server shares have been set up.</td>
<td>✓</td>
</tr>
<tr>
<td>Your clients meet the system requirements.</td>
<td>✓</td>
</tr>
<tr>
<td>You have done the software inventory on your clients.</td>
<td>✓</td>
</tr>
<tr>
<td>You have communicated the credentials for the Temporary User account to your end users.</td>
<td>✓</td>
</tr>
<tr>
<td>You have set up a location from which the clients will be deployed.</td>
<td>✓</td>
</tr>
<tr>
<td>Your users have the appropriate permissions on their local machines.</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Utilize Logon Scripts**

Pointsec for PC.msi is the file that starts the Pointsec PC installation; there are various ways to get the Pointsec for PC.msi running on the clients. This guide will not go into details on this; the important thing is that you get the command to run on your clients. In this example we will utilize logon scripts.

**To run Pointsec for PC.msi on the clients:**

1. Add the following command to the logon script that is executed when your users log on:

   `Msiexec.exe /i "[PATH TO MSI]\Pointsec for PC.msi" REBOOT=R /q`

   **Note:** Exclude '{' and text within from the command. The /q switch instructs InstallShield to run the installation silently.

**Results of Script Execution**

Since the Silent Install was selected and the /q command was used, the user will not see anything during the first phase of the Pointsec PC installation. When the system is rebooted, the following can be seen on the user's screen:
Once the system completes the reboot process, the following preboot authentication dialog opens:

**Figure 5-3** Preboot Authentication

1. Authenticate with the Temporary User credentials (see to “Creating a User Account” on page 32) and click **OK**.

   The following window opens:

**Figure 5-4** Warning to Change Password and Username

2. Click **OK** to continue.

   The following window opens:
3. In the **User account name** field, enter a new name and click **OK**.
   The following dialog opens:

   **Figure 5-5**  Change Account Name

4. In the **New Password** and **Confirm you new password** fields, enter a new password and click **OK**.
   The first logon is complete and the system boots normally.
Chapter 6

FAQ

This chapter will briefly cover some of the most common Pointsec PC questions.

For additional information, see the documentation provided with the product:

- Pointsec PC Installation Guide
- Pointsec PC Administrator’s Guide
- Pointsec PC Release Notes

Question 1:
I want to add a user account and change settings on the PCs on which I have deployed Pointsec. How do I do this?

Answer 1:
The best way to achieve this is to add the user to an update profile and deploy this profile to the system where you want the user account to be added.

To create an update profile:
1. Start PCMC and select Remote.
2. Open the configuration set that you used to create the installation profile.
3. Right-click Profiles, and select New Profile → Update.
4. Give your update profile a meaningful name.
5. Set a Profile protection password (to avoid unauthorized editing).
6. Select Base the new profile on existing settings.
7. Select Base on existing profile.
8. Depending on what you want to achieve with the update profile, select one or more of the options below:
a. Select System Settings if you want to edit and update your clients’ system settings.

b. Select Groups if you want to edit group settings.

c. Select User Accounts if you want to edit specific user accounts within the groups.

9. Browse to the profile that you want to use as a base (normally the last profile you deployed), and click OK.

   **Tip** - If this is your first update profile, use the Installation profile you used to install the clients.

10. Authenticate to the profile that you want to base your setting on

11. Edit the profile, and click OK.

You now have an update profile that you can deploy to your clients.

   **Note** - To avoid unintended changes when creating a profile based on an existing profile, it is important to understand difference between the actions Remove user account/group and Mark for Removal.

   - **Remove**: Do not include in profile, leave account/group unaffected by profile.
   - **Mark for Removal**: Use profile to remove/delete account/group from client PC.

When you base the update profile on an existing profile and select to include groups and users, select Remove to remove the users/groups that you want to leave unaffected when the profile is deployed.

**Question 2:**

How do I deploy an update profile to my client PCs?

**Answer 2:**

Here are two methods to deploy an update profile, via PCMC or manually.

**Deploying an update profile via PCMC:**

Prerequisites: You must have an update profile created with the intended configuration set.

1. Open PCMC
2. Open the Configuration Set that contains the profile you would like to deploy
3. In the main window to the right: press Publish Profile.
4. Click Next in the first wizard window
5. Select the profile that you would like to deploy and click Next
6. Review the Predefined Publication Path
   a. If this is the same path that you set for your clients to check for update profiles, click **Next**.
   b. If the path is not the same path that you set for your clients to check for update profiles, check the **Use a user-specified path** checkbox.

7. Either enter or browse to the same path that you set your clients to and check for update profiles, and click **Next**.

8. Review the summary window and click **Next**.

9. Click **Finish** in last wizard window.

The update profile is now available for client download.

**Deploying an update profile manually:**

**Prerequisites:** You must have an update profile with the appropriate Profile Validation Password set.

1. Locate the profile in the location that serves as the storage path for your configuration set.

2. Copy the profile to the path you designated for your clients to check for update profiles.

The update profile is available for client download.

**Question 3:**

I can access my client system directly via my network. Is there a way for me to push an update to my clients?

**Answer 3:**

Yes, you can deploy a profile by placing it directly on your clients.

Copy the profile you would like to deploy to the client folder: `C:\Program Files\Pointsec\Pointsec for PC\Work`

The client PC will import the profile automatically within a few moments.

**Question 4:**

I noticed a file called **Precheck.txt** in the installation folder. What is this file?

**Answer 4:**

The **Precheck.txt** file is a configuration file that Pointsec PC reads when the installation starts that determines how Pointsec PC will be installed. The default settings in this file will work in most environments. Any edits to this file must be made prior to deployment. Note that the file may be read-only.
The *Precheck.txt* file contains the following entries:

- **ShowRecoverMessages=**
  - Default is **No**. This is normally the best option to avoid unwanted messages being displayed to the users.
  - Set to **Yes** to notify end users when the recovery file is edited unsuccessfullly.

- **ExtendedLogging=**
  - Default is **No**.
  - Set to **Yes** to enable the logging of user/group status at each boot.

- **UpdateSSO=0**
  - Default is 0 (zero).
  - Pointsec PC will add the Pointsec GINA to the system, replacing existing GINAs. If you are experiencing interoperability issues with other software that utilize GINA you can set UpdateSSO=4 to instruct Pointsec not to add the Pointsec GINA to the system.

**Note** - You will lose functionality in Pointsec PC. For example, single sign-on and password synchronization requires the Pointsec GINA to be in place in order to operate.

**Question 5:**

I want to deploy software during the weekend on my client PCs and will be using Wake on LAN to boot up the systems. I will need to configure Pointsec for Wake on LAN. How do I do this?

**Answer 5:**

1. Open PCMC and select **Remote** → `<set name>` → **Profiles**, and choose to create a new Update profile.

   ![Profiles](image)

   **Figure 6-1**

2. Click **Next** to continue from the welcome page in the wizard.

3. Select a name and password for the profile, then click **Next**.

   The following is an example of the New Profile window:
4. Choose to base it on an existing profile, and then click **Next**.
5. Select the profile to base it on from the tree view and make sure to only base it on "System Settings" by unchecking the "Base on: Groups" and "Base on: User Accounts". After making these selections, click **Next**.

6. Enter the profile password for the base profile, then click **Next**.
7. Click **Finish**.
8. Select **Edit Settings → System Settings → Wake on LAN**.
The **Wake on LAN** settings as shown in the following table:

### Table 6-1  Wake on LAN Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Enable Wake on LAN                  | Yes  
Enables the feature.                      |
| Set Start Delay                     | 0  
Do not wait for the local user logon and boot directly. |
| Allow Windows Logon                 | No  
Prohibits the local logon to Windows when the system is booted in WOL-mode. |
| Set Expiration Date                 | Set the date.  
Give yourself enough time buffer to complete maintenance. |
| Set Max Number of Logons Allowed    | Set the number or reboots your maintenance will require.  
Give yourself a buffer by adding a few extra logons. |

9. Save and deploy the profile to your clients.

10. Boot the clients via the NIC.

    Pointsec PC will now boot the system. It will allow Windows to start and remote maintenance to be performed.

    **Note** - A local user logon will disable Wake on LAN on the client. Therefore, it is best practice to instruct your users to leave their systems running when they leave. The profile enabling Wake on LAN is then deployed (either to the work folder or to the update profile path). Once the profile is imported, reboot the systems. This will reduce the number of systems that abort the Wake on LAN session.

**Question 6:**

Is there a way to reduce the number of logons my users must perform?

**Answer 6:**

You can enable single sign-on in the user accounts via group settings.

**To enable single sign-on on the group level:**

1. Open PCMC and select **Remote → <Set name> → Profiles**, and choose to create a new Update profile. Create a new update profile based on a previous profile.
2. Click **Next** to continue from the welcome page in the wizard.

The following dialog opens:

![Figure 6-5](image)

3. Select a name and password for the profile, then click **Next**.

4. Choose to base it on an existing profile, and then click **Next**.

5. Select the profile to base it on from the tree view and make sure to only base it on "Groups" by deselecting the "Base on: System Settings" and "Base on: User Accounts". After making these deselections, click **Next**.
6. Enter the profile password for the base profile, then click **Next**.

7. Click **Finish**.

8. Expand the group for which you would like to enable Single Sign-On and navigate to the Single Sign-On section.

9. Set the values under the Single Sign-On according below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSO</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enables the feature</td>
</tr>
<tr>
<td>Entrust SSO</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Enables SSO to Entrust/</td>
</tr>
<tr>
<td>Smart Card Triggers Windows SSO Logon</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

10. Save and deploy the profile to your clients.

When the profile is imported on the clients, single sign-on will be enabled for all users in the group that you edited. Users will now receive the following information prior to the Windows logon the next time they boot the system:
Once the user clicks **OK**, the user is logged on normally to Windows. Credentials are now stored and will be used during the next boot, eliminating the need for the user to authenticate to Windows during boot up.

**Note -**

- Users will still be required to authenticate with their Windows password when the workstation is locked in Windows.
- Entrust SSO will enable single sign-on with the Entrust certificate. This feature requires that the Pointsec PC password exactly matches the Entrust certificate password.

**Question 7:**

My users tend to forget their passwords. Is there anything that I can do?

**Answer 7:**

You can enable single sign-on to remove the need for Windows authentication during reboot. To make things even easier, you can enable both single sign-on and password synchronization.

**To enable single sign-on to remove the need for Windows authentication:**

1. Open the PCMC, navigate to **Remote → <Set name> → Profiles**, and choose to create a new Update profile. Create a new update profile based on a previous profile.

2. Click **Next** to continue from the welcome window in the wizard.
3. Select a name and password for the profile, then click **Next**.

   **Figure 6-10**

4. Choose to base it on an existing profile, and then click **Next**.

5. Select the profile to base it on from the tree view, and make sure to base it on only "Groups" by deselecting the "Base on: System Settings" and "Base on: User Accounts". After making these deselections, click **Next**.

   **Figure 6-11**

6. Enter the profile password for the base profile, then click **Next**.

7. Click **Finish**.

8. Expand the group for which you would like to enable Password Synchronization.

9. Move to the group’s Password Synchronization section.
10. Set "Synchronize Windows Password to Preboot" to **Yes**.
11. Set "Synchronize Preboot Password to Windows" to **Yes**.
12. Save and deploy the profile to your clients.

**Result:** The Pointsec PC user accounts in the group for which you enabled Password Synchronization will see the following window next time they logon:

**Figure 6-13**

They enter their Pointsec password and click OK to synchronize the Pointsec PC password with the password used in the Windows authentication.

**Figure 6-14**

The user has now changed the Pointsec PC password and the new password (the same one as used in Windows) should now be used in Pointsec PC preboot authentication.

**Note** -
- In order for the password synchronization feature to work, the Pointsec settings that govern the password will need to allow for the new password, length, complexity etc. If the password used in Windows does not comply with the password setting: the synchronization will not be successful.
- User account will also need to be granted the Pointsec permission to change password.
**Question 8:**
What can my users do via the Pointsec tray application?

**Answer 8:**
The Pointsec tray application enables end users to configure the following Pointsec PC features:

- **Information** - Provides information regarding the encryption status.
- **Change credentials** - If enabled for the user account, this feature allows the user to change credentials.
- **Lock workstation** - Enables the Windows lock workstation function.
- **Choose Language** - Allows users to change the language Pointsec uses. The language change affects both PCMC and Pointsec preboot authentication.

**Question 9:**
All of my clients were deployed via an installation profile except one that I installed manually (stand-alone) with the same user accounts and passwords. Now I would like to uninstall this system but I cannot get the stand-alone machine to import the uninstallation profile. It imports regular update profiles successfully. What is wrong?

**Answer 9:**
Always use the installation profile to install new clients in such environments, since each Pointsec PC user account is tied to a unique ID that is used internally.

When you create an uninstall profile, you internally authenticate with the unique IDs created via the installation profile. These IDs are not available on the stand-alone machine.

**In order to uninstall this machine remotely you must:**
1. Create an update profile that adds two user accounts with permissions to uninstall.
2. Apply the update profile both to the stand-alone machine and the system that you use to create the uninstall profile.
3. Create a new uninstall profile and use the two new user accounts to authorize the uninstall process.

**Question 10:**
I created a new profile and configured the settings on the group level. When I adjusted the settings on the user account level, some settings were shown in red and had different values. Why?
**Answer 10:**

A specified value at the group level is blocking your ability to make changes at the user level. The specified setting instructs PCMC that the specific group level value may not be replaced on the user account level with settings that are less secure.

**In order to remove the inheritance:**

1. Select the specific Group level.
2. Right-click the Specified Value setting.
3. Select **Reset Value**.

The specified value is removed and changes on the user account level will be allowed.

**Question 11:**

Why are some settings sections grayed out on the user account level in PCMC?

**Answer 11:**

The grayed-out settings indicate that they are not applicable for the current settings. For example; smart card settings are not applicable for a user account that is using a fixed password. If the authentication method is changed to smart card, the settings are made available.

**Question 12:**

How do I create Pointsec PC recovery media?

**Answer 12:**

Recovery media is created from the PCMC. Two user accounts with permission to create recovery media are required to perform this procedure.
To create recovery media:
1. On the administrator's PC, open PCMC and select Remote.
2. Click Create Recovery Media (see Figure 4-1).
3. The wizard starts. Click Next to continue.
4. Select Browse file system for recovery file, and Click Next.
5. Browse to the recovery file for the system you would like to recover, and click Next.

   The following authentication dialog opens:
   Figure 6-15  Authentication Prompt

   ![Authentication Prompt](image)

6. Authenticate as a user allowed to create recovery media.
7. Authenticate using a second user account that is authorized to create recovery media.

   You are informed that the recovery file is unlocked.
8. Click OK.
9. Select the media that you would like to use as your recovery media and click OK.

   A bootable recovery media is now created.

You can now boot your system and run the recovery file.

Question 13:
How is a recovery performed on a machine?

Answer 13:
To perform recovery on a machine:

Note - There is no reboot button in the recovery application. Therefore, if you boot a system on Pointsec recovery media by mistake, you must remove the media and press Ctrl-Alt-Del.
1. Ensure that your recovery media is set correctly in the system BIOS boot order.
2. Connect the recovery media to the system.
3. Press the Power On button.
   The following dialog opens:
   **Figure 6-16** Authentication

   ![Authentication](image)

   4. Authenticate with user credentials that have permission to uninstall.
   5. Click **OK**.
   The following window opens:
   **Figure 6-17** Recovery File

   ![Recovery File](image)

   6. Click **Recover All**.
   The following window opens:
The decryption process begins. The length of the decryption process depends on the size and condition of the hard drive.

Once the disk is decrypted, the following message is displayed:

7. Remove the recovery media and press **Ctrl-Alt-Del** to reboot the system.

The disk is now decrypted. The Pointsec PC program files and registry components must be removed by uninstalling Pointsec PC via Add/Remove programs in the Control Panel. This must be done before Pointsec PC can be reinstalled.

**Question 14:**

How does a user change the Pointsec password in the preboot authentication?
**Answer 14:**

**To change the Pointsec password:**

1. In the Pointsec logon dialog box, enter the Username and Password.
2. Click **Change Password**.
3. Enter a new password.
4. Confirm the new password, and click **OK**.

The password is changed successfully and you are logged on.

**Note** -

- Users require permission to change their password.
- Users can change their password via the Pointsec PC tray application, if they have the permission to do so.

**Question 15:**

What are Dynamic Tokens and how are they used with Pointsec PC?

**Answer 15:**

A Dynamic Token is a hardware device that generates one-time passwords. These passwords can be connected to your Pointsec user account to allow logon with a one-time generated password. Pointsec PC supports the X9.9 standard for Dynamic Tokens.

The following process shows how to add a Dynamic Token to a user account manually via a profile.

**Note** - If you have a Pointsec PC Dynamic Token, see the documentation provided for additional information.

1. Ensure that you have the Dynamic Token key information.
2. Open PCMC and select **Remote**.
3. Create a new update profile based on a previous profile.
4. In the New Profile window (see **Figure 6-2**), select **User Accounts**.
5. Ensure that **System Settings** is not selected.
6. Remove the users who you do not want to be affected by the profile.
7. Right-click the user account for which you would like to change the authentication method and select **Name and Authentication**.
8. Select **Dynamic Token**, and click **Next**.
9. Select **Add dynamic token by manually entering values**, and click **Next**.

The following dialog opens:
Figure 6-20  Add Dynamic Token Manually

10. Add the Token information for the token device that you want to connect to the user, and click **Next**.
11. Click **Next** in the Summary window that appears.
12. Save and deploy the profile to your clients. See “Deploy Pointsec PC to Your Clients” for additional information.

The user account will now use the Dynamic Authentication method during the Pointsec PC preboot authentication.

**Question 16:**
What is the end user’s interaction when using the Dynamic Token authentication method?

**Answer 16:**
The Dynamic Token authentication method presents a challenge to the user and the user must respond to authenticate to the system.

**To authenticate via a Dynamic Token:**
1. In the Pointsec PC preboot authentication dialog box, enter the user account name.
2. A challenge is displayed.
3. Enter your PIN in the token.
4. Enter the challenge you received in step 2 in the token.
5. A response is displayed in the token.
6. Enter the response in the Pointsec PC preboot authentication, and click **OK**.

If the response to the challenge is correct, the system will boot.
Question 17:
What permissions do I need to set for my organization’s users on the server share?

Answer 17:
The network share should allow the RXWD permission to all users. You can limit the permission on the network share by activating the Pointsec Service Start service. See the documentation provided with the product for additional information.

Question 18:
How do I reset a Pointsec password remotely?

Answer 18:
Use the following Remote Help step-by-step process to reset the Pointsec password remotely. Remote Help requires the participation of both an administrator and a user.

1. The administrator opens PCMC and selects Remote Help.
2. During Pointsec preboot, the user enters a username and clicks Remote Help.
3. In the following PCMC Remote Help window, the administrator performs these tasks:

   a. Select Remote Password Change.
   b. Enter an End-User Account Name.
   c. In Helper Account Name field, enter the username associated with the account on the user’s system that has permissions to provide Remote Help, and click Generate.
4. The administrator reads the challenge presented in Step 2 to the user.
   In this example the number is 6141673450.3

Note - The administrator must grant the user permission at the group and user level to enable the user to reset the Pointsec password remotely.
5. In Pointsec preboot, the **user** enters the challenge in the field **Response One**.

   In this example, the number is 6141673450.

6. In Pointsec preboot, the **user** reads the Challenge to the **administrator**.

   In this example, the number is 2508182273.

7. In PCMC Remote Help, the **administrator** enters the challenge in the field **Challenge from end user**.

8. In PCMC Remote Help, the **administrator** performs the following tasks:
   a. Enters the password for the account specified as Helper Account
      In this example, the account is SYSADMIN1.
b. Clicks the Generate button

c. Reads the output in field **Response Two** to the user

9. In Pointsec preboot, the **user** performs the following tasks:
   a. Enters **Response two** from administrator and presses **OK**
   b. Changes password when prompted and presses **OK**

If the user’s account was locked due to too many failed logon attempts, it is now unlocked and the password is changed.

**Question 19:**

What are the steps that I must perform to uninstall Pointsec PC from Add/Remove Programs in the Control Panel locally on a system?

**Answer 19:**

**To uninstall Pointsec PC locally:**

1. Perform two authentications using user accounts that are permitted to uninstall.

   **Figure 6-25** Uninstallation

2. Once the authentications are complete, you will be asked to select which volumes you want to uninstall. Normally, you would select all available volumes.
3. Once you select the volumes, click **Next**.

4. Click **Next** in the **Summary** window that appears to start uninstallation.

Pointsec PC will now initiate uninstallation. The process will begin with decryption. preboot authentication will be enforced until decryption is completed. Pointsec PC Windows components will be uninstalled during the first reboot after decryption is complete.

**Question 20:**

Can I resize partitions when Pointsec PC is installed?

**Answer 20:**

Do not resize, merge, or move partitions while Pointsec PC is installed. Doing so may lead to permanent loss of data.

**Question 21:**

It seems practical to set C: as the recovery path for my clients. Is this a bad idea?

**Answer 21:**

Yes. The recovery file is used to recover your system in case of a system failure. Storing the recovery file on the encrypted disk will prohibit any recovery attempts.
THIRD PARTY TRADEMARKS AND COPYRIGHTS

Entrust is a registered trademark of Entrust Technologies, Inc. in the United States and other countries. Entrust’s logos and Entrust product and service names are also trademarks of Entrust Technologies, Inc. Entrust Technologies Limited is a wholly owned subsidiary of Entrust Technologies, Inc. FireWall-1 and SecuRemote incorporate certificate management technology from Entrust.

Verisign is a trademark of Verisign Inc.

The following statements refer to those portions of the software copyrighted by University of Michigan. Portions of the software copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided “as is” without express or implied warranty. Copyright © Sax Software (terminal emulation only).

The following statements refer to those portions of the software copyrighted by Carnegie Mellon University.

Copyright 1997 by Carnegie Mellon University. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following statements refer to those portions of the software copyrighted by The Open Group.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The following statements refer to those portions of the software copyrighted by The OpenSSL Project. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT “AS IS” AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following statements refer to those portions of the software copyrighted by Eric Young. THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Copyright © 1998 The Open Group.

The following statements refer to those portions of the software copyrighted by Jean-loup Gailly and Mark Adler Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler. This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

The following statements refer to those portions of the software copyrighted by the Gnu Public License. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The following statements refer to those portions of the software copyrighted by Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Expal maintainers. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions. The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR...
This software consists of voluntary contributions made by many individuals on behalf of the PHP Group. The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <http://www.php.net>. This product includes the Zend Engine, freely available at <http://www.zend.com>.

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright (c) 2003, Itai Tzur <itzur@actcom.co.il>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Neither the name of Itai Tzur nor the names of other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright © 2003, 2004 NextHop Technologies, Inc. All rights reserved.

Confidential Copyright Notice

Except as stated herein, none of the material provided as a part of this document may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including but not limited to, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of NextHop Technologies, Inc. Permission is granted to display, copy, distribute and download the materials in this document for personal, non-commercial use only, provided you do not modify the materials and that you retain all copyright and other proprietary notices contained in the materials unless otherwise stated. No material contained in this document may be "mirrored" on any server without written permission of NextHop. Any unauthorized use of any material contained in this document may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes. Permission terminates automatically if any of these terms or conditions are breached. Upon termination, any downloaded and printed materials must be immediately destroyed.

Trademark Notice

The trademarks, service marks, and logos (the "Trademarks") used and displayed in this document are registered and unregistered Trademarks of NextHop in the US and/or other countries. The names of actual companies and products mentioned herein may be Trademarks of their respective owners. Nothing in this document should be construed as granting, by implication, estoppel, or otherwise, any license or right to use any Trademark displayed in the document. The owners aggressively enforce their intellectual property rights to the fullest extent of the law. The Trademarks may not be used in any way, including in advertising or publicity pertaining to distribution of, or access to, materials in this document, including use, without prior written permission. Use of Trademarks as a "hot" link to any website is prohibited unless establishment of such a link is approved in advance in writing. Any questions concerning the use of these Trademarks should be referred to NextHop at U.S. +1 734 222 1600.

U.S. Government Restricted Rights

The material in document is provided with "RESTRICTED RIGHTS." Software and accompanying documentation are provided to the U.S. government ("Government") in a transaction subject to the Federal Acquisition Regulations with Restricted Rights. The Government’s rights to use, modify, reproduce, release, perform, display or disclose are restricted by paragraph (b)(3) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause at DFAR 252.227-7014 (Jun 1995), and the other restrictions and terms in paragraph (g)(3)(i) of Rights in Data-General clause at FAR 52.227-14, Alternative III (Jun 87) and paragraph (c)(2) of the Commer-cial Computer Software-Restricted Rights clause at FAR 52.227-19 (Jun 1987).
Index

A
accessing
  local settings 19
  Remote Help 63
  remote settings 23
adding groups and user accounts 30, 34

B
boot record 4

C
checklist for deployment 41
client 2, 40
configuration set, creating 24
configuring temporary user 36
creating a user account 32

definition
  client 2
  GINA 4
  interactive installation 2
  live installation 3
  locked out 3
  master installation 3
  profile 3
  silent installation 3
deployment
  checklist 41
  overview 39
  update profile 46, 47
  using logon scripts 41
  using Wake on LAN 48
documentation
  feedback 5
  related 5
  Dynamic Tokens 61, 62

e
editing
group settings 31
install settings 29
permissions settings 31
Remote Help settings 32

F
frequently asked questions 45

G
GINA, Pointsec-specific 4
group
  adding to new profile 30
  adding user accounts to 34
  settings 31
  troubleshooting 56
information
  other Check Point products 1
  technical 1
installation
  interactive, definition of 2
  master 7
  profile 3
  silent installation 3
  interactive installation, definition of 2

L
live installation, definition of 3
local settings
  accessing 19
  editing 21
  for Pointsec PC 19
  locked out, definition of 3
  logging on after installation on client 41
  logon scripts, utilizing for deployment 41

M
master installation 3, 7

O
overview
  creating a profile 23
  deployment 39
  Pointsec PC Management Console 17

P
partitions, resizing 66
password
  changing 60
  resetting remotely 63
  synchronization 53
  PCMC, overview of 17
  permissions 31
  for users on server share 63
  Pointsec
    PC Management Console, overview 17
    tray application 56
  Precheck.txt file 47
  privileged permissions 31
  profile
    adding a group to 30
    configuration set, creating 24
    creating 23, 27
    definition of 3
    types 23
    update validation password 24

Q
questions and answers 45

R
recovery
  creating recovery media 57
  file, storage of 4
path, do not use C
  66
performing 58
Remote Help
  editing settings 32
  resetting password remotely
  with 63
resizing partitions 66

S
server share
  for recovery file 4
  permissions for users on 63
settings
  changing 45
  group 31
  local 19
  permissions, editing 31
Remote Help, editing 32
silent installation, definition of 3
single sign-on
  and password
  synchronization 53
  enabling 50

T
technical info, additional 1
temporary user, configuring 36
terms 2
troubleshooting 56, 57

U
uninstalling Pointsec PC 56, 65
update
  profile 46, 47
  validation password,
  creating 24
user
  account 45
  adding 34
  creating 32
level settings,
  troubleshooting 56
temporary 36

W
Wake on LAN
  deploying Pointsec PC
  using 48