BlackBerry Enterprise Server

IT Policy Getting Started Guide

BlackBerry Enterprise Server IT Policy Getting Started Guide
Last revised: 18 July 2003

Part number: PDF-04755-008

At the time of publication, this documentation complies with the BlackBerry Enterprise Server stand alone utility accompanying this release of BlackBerry Enterprise Server.

© 1997-2003 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, 'Always On, Always Connected', the "envelope in motion" symbol and the BlackBerry logo are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The handheld and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current listing of applicable patents.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Research In Motion Limited, or any of its subsidiaries, affiliates, agents, licensors, or resellers. There are no warranties, express or implied, with respect to the content of this document.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion Europe
Centrum House, 36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada

Contents

About this guide **5**
Audience 5
Organization 5
Installation and administration documentation 6

CHAPTER 1 **Getting started** **7**
IT Policy Manager 8
Components 9
How the BlackBerry Desktop Manager uses the IT Policy file 9
The policy.inf file 10
Conventions 10
Values 10
Types of policy keys 11
Default keys 11
Policy keys 11
Planning IT policy deployment 11
Local 11
Distributed 12
Installing the ITPolicy tool 12
To install the IT Policy tool 12

CHAPTER 2 **Deploying IT policy settings** **13**
Defining IT Policy settings 14
Editing the policy file 14
To edit the policy file 15
Changing a key's attribute 16
Generating a compiled policy file 17
To generate a compiled policy file 17
Deploying a compiled policy file on a local computer 19
To deploy a policy file before desktop software installation 19
To deploy the policy file after desktop software installation 19
Deploying a compiled policy file on a network server 20
To deploy a policy file before desktop software installation 20
To deploy a policy file after desktop software installation 21
Deploying group-level policies 21
Decrypting a compiled policy file 22
To decrypt a compiled policy file 22

APPENDIX A **IT policy values** **23**
Desktop manager configuration settings 24

Synchronization settings 25
Redirector settings 26
Backup and restore settings 26
Handheld security settings 27
Messaging settings 29
Owner information 31
Weblink settings 31
Browser settings 32
Third party application settings 33
TLS Application settings 34
STK settings 35

APPENDIX B **Example IT policy settings 37**
Handheld security 37
Desktop manager 38
Synchronization 39
Redirector settings 40
Backup and restore 41
Messaging 42
Owner information 43

About this guide

The *IT Policy Getting Started Guide* explains how to define policy settings using the stand alone IT Policy tool. You can set IT policies using BlackBerry Enterprise Server Management if you have installed it with BlackBerry Enterprise Server 3.5 for Microsoft Exchange or later.

The stand alone tool and this guide are available for use if setting policies through the stand alone IT Policy tool is necessary (for example, if users on BlackBerry Enterprise Server version 3.5 or later for Microsoft Exchange are running handheld or desktop versions that do not support wireless IT Policy synchronization). Refer to "IT Policy Manager" on page 8 for more information about support issues.

Audience

This guide is intended for system administrators who are responsible for deploying IT policy settings for BlackBerry users.

Organization

This guide contains sections on the following topics:

- IT policy overview
- getting started
- deploying IT policy settings
- IT policy values
- example IT policy settings

Installation and administration documentation

In addition to the IT Policy Getting Started Guide, the following documentation is included with the BlackBerry™ Enterprise Server for Lotus® Domino™:

- *BlackBerry Enterprise Server for Lotus Domino Installation and Getting Started Guide*
- *BlackBerry Enterprise Server for Lotus Domino User Administration Guide*
- *BlackBerry Enterprise Server for Lotus Domino Monitoring and Troubleshooting Guide*

The following documentation is included with the BlackBerry™ Enterprise Server for Microsoft® Exchange:

- *BlackBerry Enterprise Server for Microsoft Exchange 5.5 Installation and Getting Started Guide*
- *BlackBerry Enterprise Server for Microsoft Exchange 2000 Installation and Getting Started Guide*
- *BlackBerry Enterprise Server for Microsoft Exchange Administration Guide*

The documentation can be found in the `Docs` directory, which is located with the installed software and on the root of the installation CD.

You can also refer to the online Help (installed with your software) for procedures, tips, and troubleshooting. To open the online Help, click **Help** in the main window of any BlackBerry Enterprise Server administrative tool.

Chapter 1
Getting started

This section provides information on the following topics:

- about the IT Policy Manager
- components
- how the BlackBerry Desktop Manager uses the IT Policy file
- the policy.inf file
- types of policy keys
- planning IT policy deployment
- installing the ITPolicy tool

IT Policy Manager

The IT Policy Manager allows you to define preferred handheld and desktop software settings. It allows you to verify that BlackBerry users have consistent settings by globally applying the desired parameters. The IT Policy Manager does this by interacting with the BlackBerry Desktop Manager to define and enforce the customized configuration. You can use the IT Policy Manager to define BlackBerry Wireless Handheld and BlackBerry Desktop Software behavior.



Note: You can set IT policies using BlackBerry Enterprise Server Management if you have installed it with BlackBerry Enterprise Server 3.5 for Microsoft Exchange or later.

The IT Policy Manager is a stand alone tool; it and this documentation are available for use if setting policies through the stand alone IT Policy tool is necessary.

You must use the stand alone IT Policy tool if you are running either of the following:

- a version earlier than 4.0 of BlackBerry Enterprise Server for Lotus Domino
- a version earlier than 3.5 of BlackBerry Enterprise Server for Microsoft Exchange

You must use the stand alone IT Policy tool if users on BlackBerry Enterprise Server version 3.5 or later for Microsoft Exchange are running any of the following:

- BlackBerry Desktop Software versions earlier than 3.5
- handheld versions earlier than version 2.5 of the handheld software for the RIM 850 Wireless Handheld™, RIM 857 Wireless Handheld™, RIM 950 Wireless Handheld™, and RIM 957 Wireless Handheld™
- handheld versions earlier than version 3.6 of the handheld software for the BlackBerry 5800 Series, BlackBerry 6510 Series, BlackBerry 6750 Series, and BlackBerry 6700 Series of wireless handhelds).



Note: With BlackBerry Enterprise Server 3.5 or later, and supported desktop, and handheld versions, policy settings are synchronized and updated over the wireless network. Wireless synchronization of IT policy is not supported with BlackBerry Desktop Software versions earlier than 3.5 or with handheld versions earlier than those mentioned above.



Warning: If a user has a handheld that supports wireless synchronization of IT policy and a desktop that does not support wireless synchronization of IT policy you must use the BlackBerry Enterprise Server Management console to apply IT policy items on the handheld and the stand alone IT Policy Manager utility to enforce IT policy items on the desktop.

If a user has a desktop that supports wireless synchronization of IT policy and a handheld that does not support wireless synchronization of IT policy you must use the BlackBerry Enterprise Server Management console to apply IT policy items on the desktop and the stand alone IT Policy Manager utility to enforce IT policy items on the handheld.

For example, if you have a user running BlackBerry Desktop Software version 3.5 with version 3.3 of the handheld software for a BlackBerry 5800 Series handheld, then you must send handheld policy items using the stand alone IT Policy Manager's policy.bin file and send desktop policy items using the BlackBerry Enterprise Server Management console.

Warning: The following applies to BlackBerry Enterprise Server for Microsoft Exchange only: Server and user level IT policy menu items in BlackBerry Enterprise Server Management are hidden for servers that do not yet support IT policy. To determine the version of the server that is installed, when the BlackBerry Enterprise Server service is first started, the version is recorded in the administration service account mailbox. If the BlackBerry Enterprise Server has never been started (or if it is an earlier BlackBerry Enterprise Server version than 3.5 for Microsoft Exchange), then no version is recorded, and IT policy items appear to be unsupported and are not available. The solution is to start the BlackBerry Enterprise Server service after installation.

You can use IT PolicyManager to define the following settings:

- handheld security options
- synchronization options
- redirector options
- backup and restore options
- messaging options
- hide advanced desktop software functionality

Components

The IT Policy Manager consists of the following components:

- `ITPolicy.exe`: an editor that allows you to modify the parameters contained in the `policy.inf` file and generate a compiled file that can be read by the desktop software.
- `policy.inf`: contains the policy parameters that you modify. The values in this file are used to generate a compiled binary file.
- `policy.bin`: the compiled version of the `policy.inf` file. This file is read by BlackBerry Desktop Manager, which then enforces the defined policy parameters.
- `keyword.txt`: lists the policy.inf parameters and describes the permitted values.

How the BlackBerry Desktop Manager uses the IT Policy file

On startup, the BlackBerry Desktop Manager looks in the registry for a key that defines the path and the filename of the `policy.bin` file, and, depending on the result, one of the following scenarios applies:

- If the key is present and has a value, the BlackBerry Desktop Manager attempts to locate the specified file in the specified path.
- If the key is not present, the BlackBerry Desktop Manager attempts to locate the file in the root of the install directory (for example, `C:\Program Files\Research In Motion\BlackBerry`).

If the BlackBerry Desktop Manager fails to locate the file, it does not apply the policy settings. If the BlackBerry Desktop Manager successfully locates the file, it reads it to determine the required IT Policy changes. Depending on each value's attribute (`default` or `policy`) and the actual value, the BlackBerry Desktop Manager may make changes to the desktop or BlackBerry Wireless Handheld configuration.

Note: The default and policy distinction is an important one. The values in default keys are only read the first time the compiled policy file is read by the desktop software. This means that subsequent changes to `default` keys will not be read by the BlackBerry Desktop Manager; if you modify these values after initial deployment, the configurations will not be reset. Refer to "Types of policy keys" on page 11 for more information.

The policy.inf file

The `policy.inf` file is a text file that contains configuration options for many of the BlackBerry Desktop Software and BlackBerry Wireless Handheld features. By modifying the values in this file, generating binary output, and distributing the binary file, you can globally modify the behavior of the BlackBerry Desktop Software and/or the BlackBerry Wireless Handheld.

Conventions

The file uses the following conventions:

- A semi-colon (;) at the beginning of a line comments it out.
- A backslash (\) at the end of a line allows line continuation for string values.
- Values are one of the following types:
  - boolean: true or false
  - integer: a numeric value within the specified range
  - string: alphanumeric
- Values have either the default or policy attribute. These attributes control how the BlackBerry Desktop Manager interprets the value. Refer to "Types of policy keys" below for more information.
- A `policy.inf` file can contain either all keys or as few as one to generate a `policy.bin` file.

Values

The values in the file are grouped according to the desktop or handheld functionality that the settings modify. The values are grouped under the following headings:

- Desktop Manager Configuration
- Synchronization. Synchronize for PIM, Email and Folder Management defaults
- Redirector Configuration
- Backup/Restore Configuration
- Device Security Settings
- Messaging Settings
- Owner Information

Each value in the `policy.inf` file is described in comment fields within the file. You can also find a topic for each value in the online help.

Types of policy keys

The keys in the IT Policy Manager file have attributes that determine whether the values can be updated subsequent to the initial launch of the policy file. These attributes are `default` and `policy`. If no key attribute is defined, the attribute is interpreted as `default`.

The attributes are enclosed in curly braces {} after the key name in the .inf file.

Default keys

Keys with the default attribute are set only once to configure settings. The BlackBerry Desktop Manager reads these settings the first time it reads the compiled policy file (`policy.bin`). When the BlackBerry Desktop Manager reads the `policy.bin` file subsequent to the initial launch, it ignores the values associated with the `default` keys.

Both of the examples below show a key with the `default` attribute as it would appear in the .inf file:

```
PasswordRequired {default} = true
PasswordRequired = true
```



Note: A key with no defined attribute is interpreted as having the `default` attribute.

Policy keys

Keys with the `policy` attribute are set every time the `policy.bin` file is changed or updated. The BlackBerry Desktop Manager reads these settings every time it reads the `policy.bin` file. If the setting's timestamp differs from that of the `policy.bin` file, the value defined in the `policy.bin` file is applied.

The example below shows a key with the policy attribute, as it would appear in the .inf file:

```
PasswordRequired {policy} = true
```

Planning IT policy deployment

There are two IT Policy deployment scenarios you can use: local and distributed. This topic discusses the advantages and disadvantages to help you determine which approach is most suitable for your environment.

Local

Local deployment consists of locally storing the IT Policy file on each user's workstation.

Advantages

- The BlackBerry Desktop Manager automatically looks for a local policy file, so no workstation configuration is required.
- Network problems will not interfere with file availability.

Issues

- You must define a mechanism for distributing the policy file to users' workstations.
- Users can delete the file from their workstation. If the BlackBerry Desktop Manager fails to locate the file on startup, it does not apply the policy settings.

Distributed

Distributed deployment consists of storing the policy file on a network server and ensuring that users' workstations point to the file.

Advantages

- The policy file can be maintained in a single location.
- Users cannot delete the file.

Issues

- Workstations must be configured to ensure that the BlackBerry Desktop Manager locates the distributed file. However, once a workstation is set up for initial deployment, further configuration changes are not required.

  In the event that the desktop software cannot locate the `policy.bin` file, the BlackBerry Desktop Manager informs the user and says that it will process a local copy (if available).



Note: The ITPolicy setting `ShowPolicyErrMsg` allows you to supress this warning message.

Installing the ITPolicy tool

The IT Policy tool is not installed when you install the BlackBerry Enterprise Server Software or the administrative tools.

The IT Policy tool can be installed on any administrative computer.

To install the IT Policy tool

1. Insert the BlackBerry Enterprise Server installation CD into the CD-ROM drive of the computer on which you are installing the IT Policy tool.
2. Copy the `itpolicy` directory, located on the CD root, to the desired location on the local computer. For example, if the computer is used to administer the BlackBerry Enterprise Server, copy the directory into `Program Files\Research In Motion\BlackBerry Enterprise Server`.

Chapter 2
Deploying IT policy settings

This section provides information on the following topics:

- defining IT Policy settings
- editing the policy file
- generating a compiled policy file
- deploying a compiled policy file on a local computer
- deploying a compiled policy file on a network server
- deploying group-level policies
- decrypting a compiled policy file

Defining IT Policy settings

Configuring user IT Policy settings consists of the following tasks:

1. Using the IT Policy program to edit the desired values in the `policy.inf` file. Refer to "Editing the policy file" below for more information.
2. Generating the `policy.bin` file. Refer to "Generating a compiled policy file" on page 17 for more information.
3. Deploying the compiled file locally (refer to page 19) or on a server (refer to page 20).



Note: If you have not deployed initial IT Policy changes, you should consider which deployment scenario best suits your environment. Refer to "Planning IT policy deployment" on page 11 for more information.

Editing the policy file

If this is your initial edit to the policy file (`policy.inf`), changes to both default and policy keys are reflected when the desktop software reads the policy file.

If you are editing the file subsequent to initial IT Policy deployment, changes you make to parameters with `default` (or unspecified) attributes will not result in different handheld or desktop behavior. Refer to "Types of policy keys" on page 11 for more information.

The example below shows the following policy password settings defined in the `policy.inf` file:

- force password
- user cannot disable password
- password must be a minimum of 7 characters

Example: policy password settings

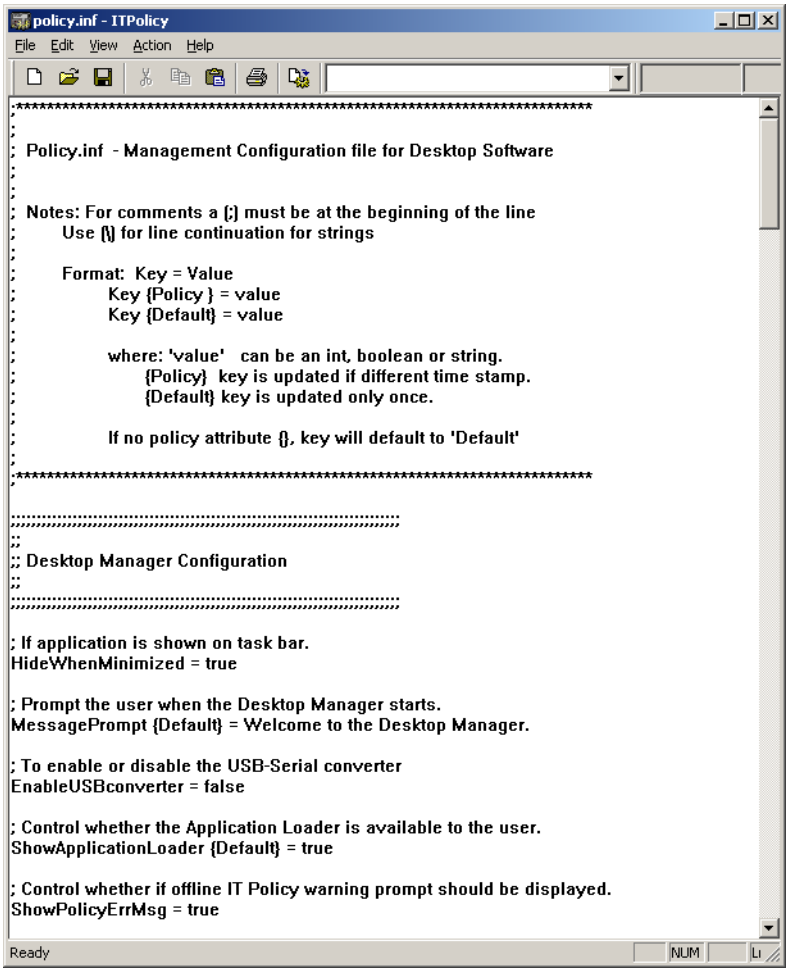
```
; Determine if the password is required on device
PasswordRequired {policy}= true

; Determine if the user can disable the password
UserCanDisablePassword = false

; Minimum length of the password.
; Valid range is 1 to 12 characters, inclusive.
;
; This value indicates the minimum length of an acceptable device
; security password.
MinPasswordLength {policy} = 7
```

To edit the policy file

1. In Windows Explorer, navigate to the directory in which you installed `ITPolicy.exe`.
2. Double-click `ITPolicy.exe` to launch the IT Policy Manager.
3. On the **File** menu, click **Open**. A directory dialog box appears.
4. Browse to the `policy.inf` file and double-click it to open it in the ITPolicy Manager. Refer to "The policy.inf file" on page 10 for more information.



ITPolicy Manager — policy.inf file

5. Modify the desired values.
6. Save your changes.
7. Generate the `policy.bin` file. Refer to "Generating a compiled policy file" on page 17 for more information.
8. Deploy the compiled file locally (refer to page 19) or on a server (refer to page 20).

Note: The new settings are applied the next time the user starts the Desktop Software and, if necessary, when the handheld is connected to the desktop.

Changing a key's attribute

You can change a value's attribute; for example, you might want to make subsequent modifications to a key you initially defined as default. You may also want to change a policy key to a default key to prevent future modifications.

To change a key's attribute, add the new attribute (if applicable, replacing the existing attribute), contained in curly braces, to the desired key. The attributes are not case-sensitive. The syntax is as follows:

key {*attribute*} = value

Where *key* is the name of the key whose value you're modifying, and *attribute* is either `default` or `policy`.

Generating a compiled policy file

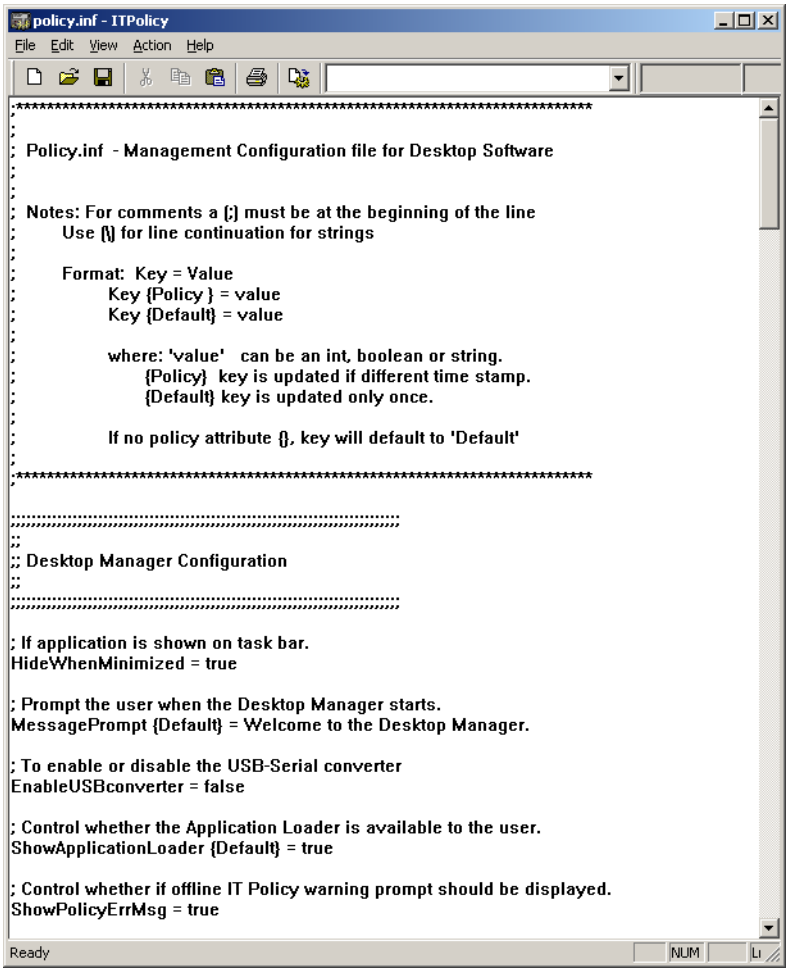
Once you've made the desired changes to the policy file, you must generate the binary file that is read by the desktop software.



Note: Compiling and distributing this file applies all values within it. You should closely review the contents of the file to ensure that it contains only values that will result in desired changes to users' BlackBerry handhelds and BlackBerry Desktop Software. If you only want to define a few values, you should back up the original file, remove the keys that do not apply, and generate only the changes you want to define.

To generate a compiled policy file

1. In Windows Explorer, navigate to the directory in which you installed `ITPolicy.exe`.
2. Double-click `ITPolicy.exe` to launch the IT Policy Manager.
3. On the **File** menu, click **Open**. A directory dialog box appears.
4. Browse to the .inf file that you want to compile and double-click it to open it in the ITPolicy Manager.



ITPolicy Manager — policy.inf file

5. On the **Action** menu, click **Generate**. A confirmation dialog box appears.
6. Click **OK**.
7. Deploy the compiled file locally (refer to page 19) or on a server (refer to page 20).

Deploying a compiled policy file on a local computer

To deploy the `policy.bin` file, complete the steps below the heading that reflects your preferred deployment scenario.

There are two scenarios for local deployment: initial and subsequent. Initial deployment takes place before users have installed the BlackBerry Desktop Software. Subsequent deployment takes place if policy files are being deployed for users with BlackBerry Desktop Software installed.



Note: After deployment, the new settings are applied the next time the user starts the desktop software and, if necessary, when the handheld is connected to the desktop.

To deploy a policy file before desktop software installation

1. To deploy the `policy.bin` file to users' local machine, copy the contents of the Desktop Software installation CD to a file server.
2. Ensure that the `policy.bin` file is installed with the BlackBerry Desktop Software by completing one of the following actions:
   - Copy the `policy.bin` file to the same directory as the Desktop Software installer.
   - To the `setup.ini` file, located in the same directory as the Desktop Software installer, add the following lines:

     ```
     [Policy]
     PolicyPath=c:\Program Files\Research In Motion\BlackBerry\
     policy.bin
     ```



Note: Verify that the path is set for the user who will be running the desktop software.

The new settings are implemented the next time the user starts the Desktop Software and, if necessary, when the handheld is connected to the desktop.

To deploy the policy file after desktop software installation

1. To deploy the `policy.bin` file to users' local machines, distribute the file and verify that it is placed in the default BlackBerry install path (`C:\Program Files\Research In Motion\BlackBerry`).

2. If the default BlackBerry install path was not used, you must also create a path registry setting that allows the BlackBerry Desktop Manager to locate the `policy.bin` file. The following registry entry is required:

   ```
   HKEY_CURRENT_USER\Software\Research In Motion\BlackBerry\
   Policy Manager\Path
   ```

   Where *Path* is a key, named Path, whose value is the full path to `policy.bin`. For example, `C:\BlackBerry\policy.bin`.



Note: Verify that the path is set for the user who will be running the desktop software.

The new settings are applied the next time the user starts the Desktop Software and, if necessary, when the handheld is connected to the desktop.

Deploying a compiled policy file on a network server

There are two scenarios for distributed deployment: initial and subsequent. Initial deployment takes place before users have installed the BlackBerry Desktop Software. Subsequent deployment takes place if policy files are being deployed for users with BlackBerry Desktop Software installed.



Note: After deployment, the new settings are applied the next time the user starts the desktop software and, if necessary, when the handheld is connected to the desktop.

To deploy a policy file before desktop software installation

1. Place the `policy.bin` file in the desired server location.
2. To the `setup.ini` file, located in the same directory as the Desktop Software installer, add the following lines:

   ```
   [Policy]
   PolicyPath=path\policy.bin
   ```

   Where *path* is the server location of the policy.bin file. For example, `\\server1\BlackBerry\Policy_File\policy.bin`.



Note: Verify that the path is set for the user who will be running the desktop software.

The new settings are implemented the next time the user starts the Desktop Software and, if necessary, when the handheld is connected to the desktop.

To deploy a policy file after desktop software installation

1. Place the `policy.bin` file in the desired server location.
2. Verify that the required registry setting is defined on each user's workstation. The following registry entry is required:

   ```
   HKEY_CURRENT_USER\Software\Research In Motion\BlackBerry\
   Policy Manager\Path
   ```

   Where *Path* is a key, named Path, whose value is the `.bin` file's full network path. For example, `\\server1\BlackBerry\Policy_File\policy.bin`

Note: Verify that the path is set for the user who will be running the desktop software.

The new settings are implemented the next time the user starts the Desktop Software and, if necessary, when the handheld is connected to the desktop.

Deploying group-level policies

When you define a single IT Policy file for all users, they are restricted to the same IT Policy settings. However, you may have multiple user groups, all with different needs.

In this case, it makes sense to deploy group-wide, rather than global, policies. By deploying multiple versions of the compiled policy file, you can apply settings to specific groups within your user base. For example, you can create an executive policy to apply to executive users and a sales policy to apply to the sales team. All other users could point to a more generic IT Policy file.

1. In Windows Explorer, navigate to the directory in which you installed `ITPolicy.exe`.
2. Double-click `ITPolicy.exe` to launch the IT Policy Manager.
3. On the **File** menu, click **Open**. A directory dialog box appears.
4. Browse to the `policy.inf` file and double-click it to open it in the ITPolicy Manager.
5. On the **File** menu, click **Save As**. A directory dialog box appears.
6. Browse to the location in which you want to save the new file, type a descriptive name, and then click **Save**.

Note: While this action modifies the .inf filename, the compiled file is still named `policy.bin`. To ensure that you don't overwrite any existing policy files, save each group-level file to a separate directory. (The compiled policy file must be named policy.bin; this is the only file the BlackBerry Desktop Software reads to determine policy settings.)

7. Modify the desired group-specific values.

Note: If you have already deployed an IT Policy file, the desktop software will read only changes to parameters with policy attributes. Refer to "Types of policy keys" on page 11 for more information.

8. Save your changes.

9. On the **Action** menu, click **Generate** to create the compiled file. The generated file is named `policy.bin`.
10. Deploy the compiled file either locally or on a server.
11. Verify that the users' workstations point to the relevant file.



Note: After deployment, the new settings are applied the next time the user starts the desktop software and, if necessary, when the handheld is connected to the desktop.

Decrypting a compiled policy file

You can decrypt a `policy.bin` file to view the settings that it contains; this is useful if you deploy multiple group-level policy files. Because each compiled file is named `policy.bin`, you might want to verify a file's contents.

To decrypt a compiled policy file

1. In Windows Explorer, navigate to the directory in which you installed `ITPolicy.exe`.
2. Double-click `ITPolicy.exe` to launch the IT Policy Manager.
3. In Windows Explorer, navigate to the `policy.bin` file that you want to decrypt.
4. Drag the file onto the IT Policy Manager. The file opens as an `.inf` file that you can view, modify, or compile.

Appendix A
IT policy values

This appendix lists and describes the settings provided with the IT Policy tool. The settings are grouped in the following categories:

- Desktop manager configuration settings
- Synchronization settings
- Redirector settings
- Backup and restore settings
- Handheld security settings
- Messaging settings
- Owner information
- Weblink settings
- Browser settings
- Third party application settings
- TLS Application settings
- STK settings

Refer to "Planning IT policy deployment" on page 11 for more information on planning and deploying IT policy settings.

Desktop manager configuration settings

The desktop manager settings define BlackBerry Desktop Manager configuration.

Keyword	Value	Description
HideWhenMinimized	boolean	Defines whether the Desktop Manager button is shown on the task bar when the application is minimized. (The Desktop Manager icon still appears in the Windows Systray.)
MessagePrompt	string	Defines a message to appear the first time BlackBerry Desktop Manager is started. **Note:** The message appears only the first time BlackBerry Desktop Manager is started after the updated IT Policy has been applied.
EnableUSBconverter	boolean	Defines whether the **USB to Serial Converter** option is enabled.
ShowApplicationLoader	boolean	Defines whether the Application Loader icon appears in the BlackBerry Desktop Manager window. A value of false means that users cannot use Application Loader to load applications on their handheld.
ShowPolicyErrMsg	boolean	Defines whether an error dialog will appear if Desktop Manager cannot locate the policy file (`policy.bin`) during startup.
AllowDesktopAddIns	boolean	Defines whether the desktop enables the user to configure and execute Desktop Addins (third-party COM-based extensions that access the handheld databases during synchronization). When this policy is set to FALSE, the Configure Add-ins and Execute Add-in actions options are disabled on the desktop.
DesktopPasswordTimeout	integer 0-720	Defines whether to specify the time, in minutes, until the desktop caches the handheld password in memory. The allowable range of values is 0 to 720 minutes. If the value is set to 0, the cache timeout is disabled; the password cache is cleared only when the handheld is removed from the cradle, disconnecting to the computer, regardless of the length of time the handheld is connected in the cradle. The value defaults to 10 minutes.
AllowDeviceSwitch	boolean	This setting defines whether the Desktop software can enable and disable the user switching handhelds. When set to TRUE, the user can switch handhelds; when set to FALSE, the user cannot switch handhelds.

Synchronization settings

The synchronization settings define the desktop software's synchronization behaviour.

Keyword	Value	Description
SynchronizeNowPIM	boolean	Defines whether PIM information is synchronized when users click **Synchronize now** in the Intellisync window.
SynchronizeNowEmail	boolean	Defines whether email is synchronized when users click **Synchronize now** in the Intellisync window.
SynchronizeNowDateTime	boolean	Defines whether the date and time are synchronized when users click **Synchronize now** in the Intellisync window.
AllowWirelessEmailSynchronization	boolean	On supported server and handheld versions, wireless email reconciliation support for the server and all its users is enabled by default. If this policy item is not added to the IT policy to which a user is assigned, wireless email reconciliation support is still enabled by default. This enables the Wireless Reconcile option on the handheld by default. Set this policy item to false to disable wireless email reconciliation on the handheld.
AutoSynchronizePIM	boolean	Defines whether PIM information is automatically synchronized when users connect their handheld to their computer and start the desktop software or connect their handheld to their computer with the desktop software running.
AutoSynchronizeEmail	boolean	Defines whether email is automatically synchronized when users connect their handheld to their computer and start the desktop software or connect their handheld to their computer with the desktop software running.
AutoSynchronizeDateTime	boolean	Defines whether the date and time are automatically synchronized when users connect their handheld to their computer and start the desktop software or connect their handheld to their computer with the desktop software running.
SyncFoldersInsteadOfImport	boolean	Defines whether the desktop software synchronizes folders instead of performing an import.
FolderConflictDesktopWins	boolean	If SyncFoldersInsteadOfImport is true, defines which data is used in the event of conflict between the user's handheld and Microsoft Exchange or Lotus Notes.
DisableWirelessCalendar	boolean	Defines whether wireless calendar synchronization is disabled. If this value is true, users cannot select the wireless calendar connector.

Redirector settings

Keyword	Value	Description
AutoSignature	string	Defines the signature appended to all messages sent from handhelds. If you want to specify that no autosignature appear, you must remove the string that appears for this value and leave the field empty. Removing the string prevents users from appending their own signature.
ForwardMessagesToHandheld	boolean	Defines whether messages are forwarded to handhelds.
ForwardMessagesInCradle	boolean	Defines whether messages are forwarded to the handheld when it is connected to the computer.
ForwardWhenRulesDontApply	boolean	Defines whether messages are forwarded to the handheld if filter rules do not apply. A value of false means the message is held at the desktop.
FilterRuleFile	string	Enables you to point to files that contain filter rules that are used to determine which messages are forwarded to the handheld.
DontSaveSentMessages	boolean	Defines whether messages sent from handhelds are copied to the user's **Sent** folder.

Backup and restore settings

Keyword	Value	Description
AutoBackupEnabled	boolean	Controls enabling of the Automatically backup my handheld option.
AutoBackupFrequency	integer 1-99	Defines how often, in days, data is automatically backed up (if Automatic Backup is enabled) when the handheld is connected to the computer, and the desktop software is running.
AutoBackupIncludeAll	boolean	If AutoBackupEnabled is true , defines whether automatic backup includes all handheld data.
AutoBackupExcludeEmail	boolean	If AutoBackupIncludeAll is false , defines whether automatic backup excludes email.
AutoBackupExcludeSync	boolean	If AutoBackupIncludeAll is false, defines whether automatic backup includes data selected by the user for synchronization.

Handheld security settings

Note: After handheld settings are deployed, they take effect when users next connect their handheld to the computer.

Keyword	Value	Description
Allow Attachment Viewing	boolean	Defines whether users are enable d or disabled to view attachments on the handheld. By default, if no setting is specified for this item, attachment viewing is enabled for all users who are on a BlackBerry Enterprise Server with attachment service installed, running, and connected to the BlackBerry Enterprise Server through an attachment connector.
AllowExternalConnections	boolean	Defines whether all external connections from the handheld can be enabled and disabled. By default, if no setting is specified for this item, all external connections are enabled on the handheld.
AllowInternalConnections	boolean	Defines whether all internal connections from the handheld can be enabled and disabled. By default, if no setting is specified for this item, all internal connections are enabled on the handheld.
AllowSplitPipeConnections	boolean	Defines whether applications can be enabled and disabled to open both internal and external connections simultaneously. Enabling split pipe connections presents a security issue because, when enabled, applications can surreptitiously collect data from inside the firewall and send it outside the firewall without any auditing. By default, if no setting is specified for this item, split pipe connections are disabled on the handheld.
ForceLockWhenHolstered	boolean	Defines whether you can enable or disable automatic locking of the handheld when placed in the holster. When set to TRUE, locking is enabled, requiring the user to enter a password each time the user removes the handheld from the holster.
MaximumPasswordHistory	integer 0 - 15	Defines the maximum number of prior passwords against which new passwords can be checked to prevent reuse of the old passwords. Entering 0 disables password reuse. Entering 5, for example, prevents reuse of the last 5 passwords used on the handheld. This policy item is available only on the Java-enabled handhelds.

Keyword	Value	Description
SetMaximumPasswordAttempts	integer 3 - 10	Defines the number of security password attempts (incorrect passwords entered) allowed on the handheld before the handheld data is erased and the handheld disabled. If you set a maximum number of password attempts, notify handheld users of the maximum number so that they do not exceed that number when trying to recall a forgotten password. This policy item is available only on the Java-enabled handhelds.
SetPasswordTimeout	integer 0 - 60	Defines the amount of time, in minutes, before the security timeout occurs on the handheld. Set the value to 0 to disable automatic locking of the handheld. The value specified must be less than or equal to the value set for the MaxSecurityTimeout policy item if it is set. This policy item is available only on the Java-enabled handhelds.
SuppressPasswordEcho	boolean	Prevent password characters from printing onscreen ('echoing') after the maximum number of allowable failed password attempts. This policy item is available only on the Java-enabled handhelds.
PasswordRequired	boolean	Defines whether password protection is required on the handheld.
UserCanDisablePassword	boolean	Defines whether users can disable password protection on the handheld.
MinPasswordLength	integer 1-12	Defines the minimum number of characters allowed for a handheld password.
PasswordPatternChecks	integer 0,1	Defines whether at least one alphabetic and one numeric character is required in handheld passwords. A value of 0 indicates that no password pattern checking is performed.
MaxSecurityTimeout	integer 1-60	Defines the maximum time in minutes allowed before a handheld security time out occur.s. Users can select any duration shorter than the maximum time. Typically, set this option if your organization has a security policy. If you do not have a security policy, the recommended minimum value is **30**.
UserCanChangeTimeout	boolean	Defines whether users can modify the maximum security timeout settings. If this value is false, the MaxSecurityTimeout value is used as the security timeout duration.
MaxPasswordAgeInDays	integer 0-365	Defines how frequently, in days, users are prompted to change their password. A value of 0 indicates that there is no maximum password age.

Keyword	Value	Description
LongTermTimeoutEnable	boolean	Defines whether the long term security time out is enabled or disabled on the handheld. This policy item is available only on the Java-enabled handhelds. This policy item is available only on the Java-enabled handhelds.
ForceLoadCount	integer 0-999	Defines how many times a handheld user is allowed to decline when prompted to update the handheld. If the value is 0 or higher, and the user declines to update their handheld software the specified number of times, the BlackBerry Desktop loader forces the handheld software to update. Set the value to -1 to disable the forced update and reminder messages.
ForcedHandheldUpdateMessage	string	Defines a string that appears (in place of the default string) when users are required to update to a later version of the BlackBerry handheld.

Messaging settings

The messaging options define which message services users are permitted to use on their handheld.

Keyword	Value	Description
AllowPINtoPIN	boolean	Defines whether users are permitted to send PIN-based messages from their handheld. If the value is false, the functionality is hidden from users.
AllowBCCRecipients	boolean	Defines whether users can specify blind carbon copy recipients for messages they send from their handheld.
AllowSMS	boolean	Defines whether users can send short message server (SMS) messages from their handheld. This policy item is available only on the Java-enabled handhelds.
AllowPhone	boolean	Defines whether users can use the phone functionality provided by Research In Motion on the handheld. This policy item is available only on the Java-enabled handhelds. **Warning:** When AllowPhone is set to false, all phone functionality is disabled on the handheld, including emergency calling. You may wish to advise users for whom the phone application has been disabled that emergency calls cannot be made on the handheld.

Keyword	Value	Description
AllowBrowser	boolean	Defines whether users are permitted to use the handheld's Web browser.
AllowOtherEmailServices	boolean	Defines whether users can use email services other than the handheld's default service book. If the value is false, users are restricted to the default service book. **Note:** if this value is not present, the default is to allow other email services.
AllowOtherBrowserServices	boolean	Defines whether users can use browser services other than the handheld's default internet service book. If the value is false, users are restricted to the default desktop service book. **Note:** if this value is not present, the default is to allow other internet services.

Owner information

The owner information settings define the owner information associated with users handhelds.

Keyword	Value	Description
OwnerName	string	Defines the handheld's owner name. The owner name is displayed when handheld security is active and when users select **Options** > **Owner** on their handheld. A value of * indicates that the value is read from the desktop software's registry settings.
OwnerInfo	string	Defines the handheld's owner information. Owner information is displayed when handheld security is active and when users select **Options** > **Owner** on their handheld. A value of * indicates that the value is read from the desktop software's registry settings.

Weblink settings

These values control the appearance and behaviour of the WebLink extension.

Keyword	Value	Description
ShowWebLink	boolean	Defines whether the handheld user has access to the Web Link icon on the Desktop. A value of False hides the icon from the user. This setting requires that you also specify a value for the WebLinkURL setting.
WebLinkURL	string	Defines the URL to be used when a user double-clicks the WebLink icon in desktop manager.
WebLinkLabel	string	Defines the WebLink icon's label.

Browser settings

The Browser settings control the behaviour of the handheld Browser application.

Keyword	Value	Description
HomePageAddress	string	Defines the URL address of the Home Page used by the WML Browser. If you do not specify a URL, the handheld will use the default Home Page URL address. Typically, organization's set the URL to their intranet address. Set this option according to your organization's requirements.
HomePageAddressReadOnly	boolean	Defines whether the URL address of the Home Page can be modified by the handheld user. Most organizations set this option to make the URL Read-Only (not writable).
EnableWAPConfig	boolean	Defines whether to disable (hide) the WAP browser icon even if the carrier has provisioned the WAP browser and the appropriate service books are present. This policy item is available only on the Java-enabled handhelds.
DefaultBrowserConfigUID	string	Defines a unique ID for the Browser Config Service Record, which sets the default browser to use (for example, when opening links in email messages). Typically, set this option to the unique ID of the default Browser Config Service Record. This policy item is available only on the Java-enabled handhelds.
MDSBrowserTitle	string	Defines a name in the ribbon of the Mobile Data Service Browser window. This policy item is available only on the Java-enabled handhelds.

Third party application settings

Third party applications settings enable control of third party application downloads and use on the handheld.

Keyword	Value	Description
DisallowThirdPartyAppDownloads	boolean	Defines whether to disallow downloading to the handheld of third party applications (in other words, applications not authored by Research In Motion).
AllowThirdPartyUseSerialPort	boolean	Defines whether to enable or disable third party applications to use the serial port, IrDA or USB ports on the handheld. By default, if no setting is specified for this item, third party applications are automatically enabled to run using the serial port, IrDA or USB ports on the handheld.

TLS Application settings

The TLS settings define properties that apply to the TLS protocol.

keyword	value	description
TLSDisableInvalidConnection	integer 0-2	Use this policy item to enable or disable the use of connections to servers with invalid certificates during TLS connections. Set to 0 to disallow invalid connections, 1 to allow invalid connections, or 2 to prompt the handheld when invalid connections are used.
TLSDisableUntrustedConnection	integer 0-2	Use this policy item to enable or disable the use of untrusted connections during a TLS connection. Set to 0 to disallow untrusted connections, 1 to allow untrusted connections, or 2 to prompt the handheld when untrusted connections are used.
TLSDisableWeakCiphers	integer 0-2	Use this policy item to enable or disable the use of weak ciphers during a TLS connection. Set to 0 to disable weak ciphers, 1 to enable weak ciphers, or 2 to prompt the handheld when weak ciphers are used.
TLSMinimumStrongDHKeyLength	integer 512-4096 bits	Use this policy item to specify the minimum DH key size, in bits, allowed for use in the TLS connection. A default value of 1024 is used if this value is not set.
TLSMinimumStrongECCKeyLength	integer 160-571 bits	Use this policy item to specify the minimum ECC key size, in bits, allowed for use in the TLS connection. A default value of 163 is used if this value is not set.
TLSMinimumStrongDSAKeyLength	integer 512-1024 bits	Use this policy item to specify the minimum DSA key size, in bits, allowed for use in TLS connections. A default value of 1024 is used if this value is not set.
TLSMinimumStrongRSAKeyLength	integer 512-4096 bits	Use this policy item to specify the minimum RSA key size, in bits, allowed for use in TLS connections. A default value of 1024 is used if this value is not set.
TLSRestrictFIPSCiphers	boolean	Allows you to enable or disable the use of any cipher that is not FIPS compliant. Set to TRUE to restrict use of non-FIPS compliant ciphers; set to **FALSE** to enable use of any non-FIPS compliant ciphers. If no setting is specified for this item, by default, use of any non-FIPS compliant cipher is disabled.

STK settings

The SIM Took Kit (STK) settings define properties that apply to the STK.

keyword	value	description
DisableSTKSetupCall	boolean	This setting specifies whether or not the ability of the SIM to originate an outgoing call, supplementary service request, or short message is enabled or disabled. By default, if no setting is specified for this item, the default is to enable the SIM to originate outgoing calls, service requests or messages.
DisableSTKProvideLocalInfo	boolean	This setting specifies whether or not to prevent the network or SIM from querying the handheld for network location related information. The information is limited to current network and cell identities, the handheld IMEI, the current date and time, and some measurement results. By default, if no setting is specified for this item, the default is to enable the network or SIM to query the handheld for network location related information.
DisableSTKCallControl	boolean	This setting specifies whether or not the ability of the SIM to modify an outgoing call, supplementary service request, or short message is enabled or disabled. By default, if no setting is specified for this item, the default is to enable the SIM to modify outgoing calls, service requests or messages.

Appendix B
Example IT policy settings

This appendix contains examples of the following IT policy settings:

- handheld security
- desktop manager
- synchronization
- redirector settings
- backup and restore
- messaging
- owner information

Refer to "IT policy values" on page 23 for more information on the settings, their permitted values, and descriptions. Refer to "Planning IT policy deployment" on page 11 for more information on planning and deploying IT policy settings.

Handheld security

The following example shows a `policy.inf` file with the following handheld security settings:

- A password is required.
- The user cannot disable the password.
- The password must be at least 7 characters long.
- The password must contain at least one alphabetic and one numeric character.
- The user cannot set a handheld security timeout longer than 15 minutes.
- The user is prompted to change the password every 30 days.
- The user is not prompted for the password every hour.



Note: The values marked {default}, or with no attribute defined, will not be changed subsequent to their initial deployment unless they are changed to {policy}. Refer to "Types of policy keys" on page 11 for more information.

Example: policy.inf handheld security settings

```
PasswordRequired {policy}= true

UserCanDisablePassword = false

MinPasswordLength {policy} = 7

PasswordPatternChecks {policy} = 1

MaxSecurityTimeout {policy} = 15

UserCanChangeTimeout {policy} = TRUE

MaxPasswordAgeInDays {policy} =30

LongTermTimeoutEnable {policy} = false
```

Desktop manager

The desktop manager settings define desktop manager configuration.

The following example shows a `policy.inf` file with the following desktop manager settings:

- When desktop manager is minimized, it is not shown on the Windows task bar.
- Users do not see the **Application Loader** icon.
- If desktop manager cannot locate the IT Policy file when it starts, users will not see the warning dialog box.



Note: The values marked {default}, or with no attribute defined, will not be changed subsequent to their initial deployment unless they are changed to {policy}. Refer to "Types of policy keys" on page 11 for more information.

Example: policy.inf desktop manager settings

```
HideWhenMinimized = true

ShowApplicationLoader {Default} = false

ShowPolicyErrMsg = false
```

Synchronization

The policy synchronization settings override the settings defined in the Intellisync window in users' desktop software.

The following example shows a `policy.inf` file with the following synchronization settings:

- When the user clicks **Synchronize now** in the Intellisync window, PIM information is synchronized.
- When the user clicks **Synchronize now** in the Intellisync window, email is synchronized.
- When the user clicks **Synchronize now** in the Intellisync window, the date and time synchronize.
- When users connect their handheld to their computer with the desktop software running, the date and time automatically synchronize.
- In the event of conflict between the user's handheld and Microsoft Exchange or Lotus Notes, Microsoft Exchange or Lotus Notes wins.
- Wireless calendar synchronization is enabled.



Note: The values marked {default}, or with no attribute defined, will not be changed subsequent to their initial deployment unless they are changed to {policy}. Refer to "Types of policy keys" on page 11 for more information.

Example: policy.inf synchronization settings

```
SynchronizeNowPIM = true

SynchronizeNowEmail = true

SynchronizeNowDateTime = true

AutoSynchronizeDateTime = true

FolderConflictDesktopWins = true

DisableWirelessCalendar = false
```

Redirector settings

The policy redirector settings override the settings defined in the Redirector Settings window in users' desktop software.

The following example shows a `policy.inf` file with the following redirector settings:

- Messages are forwarded to users' handhelds.
- Messages are not forwarded to the handheld if the handheld is inserted in the cradle.
- Messages sent from a handheld are copied to the user's **Sent** folder.



Note: The values marked {default}, or with no attribute defined, will not be changed subsequent to their initial deployment unless they are changed to {policy}. Refer to "Types of policy keys" on page 11 for more information.

Example: policy.inf redirector settings

```
ForwardMessagesToHandheld = true

ForwardMessagesInCradle = false

DontSaveSentMessages = false
```

Backup and restore

The policy backup and restore settings override the settings defined in the Backup and Restore window in users' desktop software.

The following example shows a `policy.inf` file with the following backup and restore settings:

- Handheld data is automatically backed up.
- The automatic backup occurs every seven days.



Note: The values marked {default}, or with no attribute defined, will not be changed subsequent to their initial deployment unless they are changed to {policy}. Refer to "Types of policy keys" on page 11 for more information.

Example: policy.inf backup and restore settings

```
AutoBackupEnabled = true

AutoBackupFrequency = 7
```

Messaging

The messaging settings define the permitted messaging types.

The following example shows a `policy.inf` file with the following messaging settings:

- PIN messaging is not permitted.
- SMS messaging is not permitted.
- Only the Enteprise edition service book is permitted on the handheld.



Note: The values marked {default}, or with no attribute defined, will not be changed subsequent to their initial deployment unless they are changed to {policy}. Refer to "Types of policy keys" on page 11 for more information.

Example: policy.inf messaging settings

```
AllowPINtoPIN {policy} = false

AllowSMS {policy} = false

AllowOtherEmailServices {policy} = false
```

Owner information

The owner information settings define the handheld's owner name and information. This information is shown when the handheld is locked or when the user selects **Options** > **Owner**.

The following example shows a `policy.inf` file with the following messaging settings:

- The owner name is read from the desktop software's registry settings.
- The owner information will display as defined below.



Note: The values marked {default}, or with no attribute defined, will not be changed subsequent to their initial deployment unless they are changed to {policy}. Refer to "Types of policy keys" on page 11 for more information.

Example: policy.inf owner information settings

```
OwnerName {default} = *

OwnerInfo {default} = Please return to ACME Corporation\
Phone # (888) 888-8888\
888 Eighth St\
Waterloo ON\
N2L 3W8
```



© 2003 Research In Motion Limited
Published in Canada