Bluetooth for Windows

Configuration Guide

July 6, 2001

Document Number: BTW-DOCS-010620-1220
Version: 1.1

Confidential and Proprietary Information

Wireless Internet and Data Communication
9645 Scranton Road, Suite 205
San Diego, CA 92121
Phone: 858.453.8400
Fax: 858.453.5735
Email
Technical Support: support@widcomm.com
Information: info@widcomm.com

LICENSED SOFTWARE

Trademarks ™ and Registered Trademarks®

Table of Contents

Comments or questions about the BTW Configuration Guide are welcome. Submit questions and comments to WIDCOMM's Technical Support department at the mailing address and/or e-mail addresses listed on the cover of the guide.

List of Tables

List of Figures

1 Introduction

WIDCOMM's Bluetooth™ for Windows (BTW) software installs with a default configuration that allows the application to be used "out-of-the-box" without making decisions about security and other user-configurable options.

The default configuration settings include:

- Medium Bluetooth security.
- Service startup at system start.
- Default *My Shared Directory* and *My Inbox*.

These settings allow your computer to find the discoverable and connectable Bluetooth-enabled devices within radio range (referred to as the Bluetooth Neighborhood). Your computer will then be able to use the services on these devices, for example, surf the web. In turn, these other Bluetooth devices (referred to as remote devices) will be able to discover your computer and use its services.

Your computer will also be ready to wirelessly accept items including contacts (electronic business cards), appointments and meetings, messages received as e-mail, and notes.

1.1 BTTRAY

When BTW is installed on your computer, a shortcut for one of its components—the Bluetooth System Tray (BTTray)—is added to the Microsoft® Windows® Startup folder. On system start, it is automatically started and a BTTray icon appears in the Windows system tray to notify you that it is running. BTTray functionality provides:

- Unobtrusive notification when intervention is required to authorize a security request or enter a Bluetooth passkey.
- Dialog boxes that prompt for security authorization and allow passkey entry.
- Bluetooth "pairing" support.
- Access to the Bluetooth *Configuration* window.

The BTW Bluetooth stack is also started on system start. This program runs without user intervention. The stack is the engine behind the scenes that drives the BTW software and allows your computer and its Bluetooth device (for example, a USB dongle, a PC card, or a multi-port) to communicate with other Bluetooth devices. The stack server controls the Bluetooth device attached to your computer, protects it from unauthorized intrusion, and ensures that your computer's Bluetooth connections operate correctly.

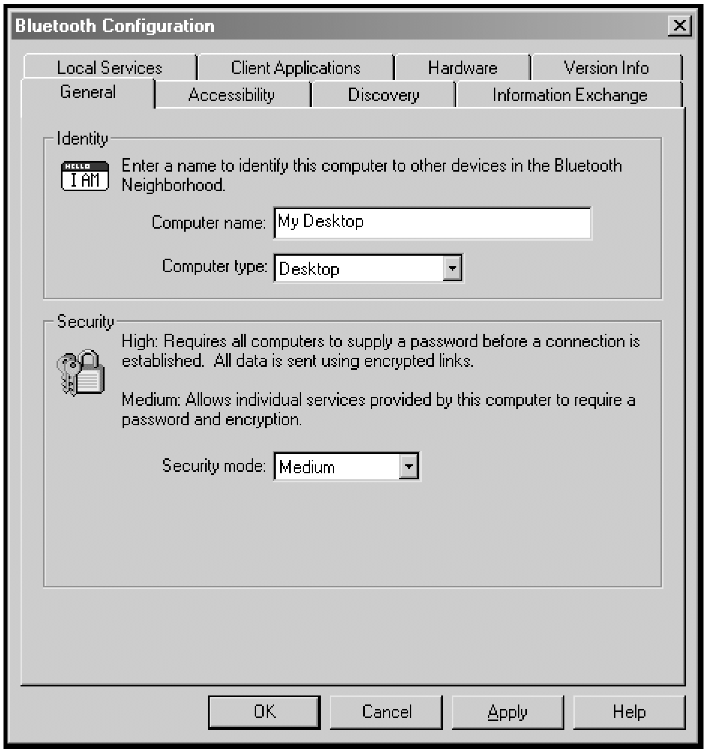
BTTray also runs in the background. It waits for notifications from the stack server that a remote device has requested access to services on your computer. However, notification is dependent upon how BTW security is configured:

- If *High* security is set in the *General* tab of the Bluetooth *Configuration* window, BTTray will display a passkey notification each time a non-paired device wants to discover local services on your computer. The *High* security setting requires all remote devices to supply a passkey, like a Personal Identification Number (PIN), before services can be discovered. All data will be sent using encrypted links.
- If *Medium* security is set in the *General* tab of the Bluetooth *Configuration* window, BTTray will display a security dialog only when the specific local service that the remote device is requesting requires authentication or authentication and authorization.

1.2 CONFIGURATION WINDOW COMPONENTS

The Bluetooth *Configuration* window uses the familiar Microsoft Windows Control Panel interface.

Figure 1: BTTray >Bluetooth Configuration window.



Enter a name to identify this computer to other devices in the Bluetooth Neighborhood.

Computer name: My Desktop

Computer type: Desktop

High: Requires all computers to supply a password before a connection is established. All data is sent using encrypted links.

Medium: Allows individual services provided by this computer to require a password and encryption.

Security mode: Medium

The *Configuration* window has eight tabs:

- *General*—computer name and type and Bluetooth device security.
- *Accessibility*—control which Bluetooth devices may discover your computer.
- *Discovery*—options that determine:
  - Whether your computer will perform a periodic search for Bluetooth devices.
  - The types of devices, if any, to be displayed in the BTW Bluetooth Neighborhood window may.
  - The filters which specify which devices or classes and types within class of devices are discovered. For example, create a filter that only looks for a specific Bluetooth device like a cellular telephone, or a filter that looks for a specific class and type of device such as “Computers – Laptops”
- *Information Exchange*—establishes:
  - Whether your computer will accept appointments, meetings, business cards, and messages received from remote devices and where to store these items.
  - The highest-level directory on your computer a remote device may share.
  - The location of your electronic business card and a setting that allows or denies remote devices the option of having your business card sent to them.
- *Local Services*—configure properties of the Bluetooth local services that BTW supports on your computer. Properties include service-level security, automatic service startup, Bluetooth Serial Port COM port, and modems for Fax and

Dial-Up Networking. Also, create additional serial services for use by applications that require serial ports such as HyperTerminal[1].

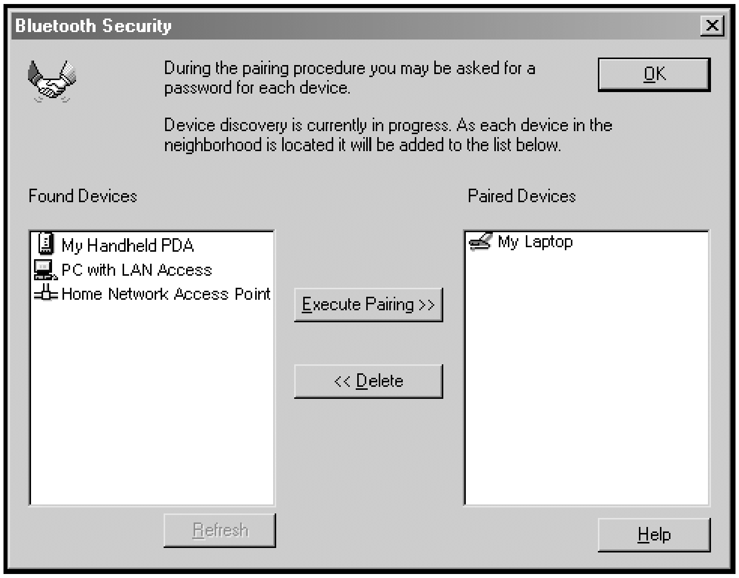
- *Client Applications*—configure properties of the Bluetooth client applications your computer will use to access Bluetooth services on a remote device. Includes authentication and encryption and COM port for the Bluetooth Serial Port application. Also, create additional COM ports.
- *Hardware*—displays Bluetooth device properties including status. Provides a means to alter a device's hardware configuration such as Country Code and Maximum Transmission Power.[LTS1]
- *Version Info*—provides version number information for BTW's components.

To view or change the configuration settings open the Bluetooth *Configuration* window as described in Section 1.4 on page 4.

1.3 SECURITY WINDOW COMPONENTS

The settings in the BTTray *Security* window (Figure 2) establish and/or break device pairing (see also Section 3.2 on page 27).

Figure 2: BTTray > Security window.



During the pairing procedure you may be asked for a password for each device.

Device discovery is currently in progress. As each device in the neighborhood is located it will be added to the list below.

The security dialog boxes (*Passkey* and *Authorization*) described in Sections 3.2 and 3.3.2 are displayed only when certain conditions are met and depend on the properties set in the *General*, *Local Services*, and *Client Applications* tabs of the *Configuration* window.

Section 1.4 on page 4 explains how to open the BTTray *Security* window.

---

[1] The HyperTerminal program is used to connect to other computers, Internet telnet sites, bulletin board systems (BBSs), online services, and host computers, using either your modem or a null modem cable.

1.4 OPEN THE CONFIGURATION OR SECURITY WINDOWS

To open the *Configuration* or *Security* windows:

> Right-click the BTTray icon in the system tray of the Windows taskbar and choose **Security** or **Configuration** from the menu.

The *Configuration* window can also be opened by clicking **Start** > **Settings** > **Control Panel** and then double-click the **Bluetooth Configuration** icon or right-click the icon and choose **Open**.

Additional ways to open the *Configuration* and *Security* windows are provided in the Bluetooth Neighborhood window and through right-click context menus.

2 Configuration

This section describes the BTW Bluetooth *Configuration* window and the settings that can be changed on the eight tabs that comprise the window.

To activate changes made on the *Configuration* window:

- Click the **OK** button located on the bottom of the *Configuration* window to apply the changes and close the window.

  OR
- Click the **Apply** button located on the bottom of the *Configuration* window to apply the changes and leave the window open.

To throw out any changes and close the window:

- Click the **Cancel** button located on the bottom of the *Configuration* window.

  OR
- Click the close button ☒ located in the upper-right corner of the *Configuration* window.

2.1 GENERAL TAB

Device properties and system security are configured in the *General* tab which is shown in Figure 1 on page 2.

2.1.1 Computer Name and Type

In the *Identity* section of the *General* tab, the *Computer name* field identifies your computer to other Bluetooth devices. This is user-configurable and is different from the *Bluetooth Device Address* (BDA) set at the factory. The BDA is shown on the *Hardware* tab. The *Computer name* is the name entered during the BTW installation process.[LTS2]

The *Computer name* field cannot be left blank. However, it should be understood that some Bluetooth devices might only list your computer by its BDA.

To change the *Computer name*:[LTS3]

1. Open the *Configuration* window. The *General* tab is displayed.
2. The current *Computer name* is highlighted. Type a new name. The old name is deleted once you begin to type.
   - A valid *Computer name* is between 1 and 247 characters, for example, *My Laptop*.
3. Click the *Configuration* window **Apply** or **OK** button.

The *Computer type* assigns your computer's device type as either *Desktop* or *Laptop*. The device type information is made available to remote devices when these are discovering other Bluetooth devices. *Desktop is the default setting.*

To change the *Computer type*:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the down arrow ▾ located at the right end of the *Computer type* field and choose **Desktop** or **Laptop** from the drop-down list.
3. Click the *Configuration* window **Apply** or **OK** button.

2.1.2 Bluetooth Security

In the *Security* section of the *General* tab, the *Security mode* sets how the Bluetooth device attached to your computer handles security.

- *High*—requires Bluetooth devices to authenticate (enter a Personal Identification Number (PIN)) with your computer before services can be discovered. Your computer and the connected Bluetooth device will send data using encrypted[2] links.
- *Medium*—the default setting—security is configured at the service-level. The local services (for example, Network Access) supported by your computer may be configured individually to require:
  - No security.
  - Authentication only.
  - Authentication and Authorization.
  - Authentication and Encryption.
  - Authentication, Authorization, and Encryption.

To change the *Security mode*:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the down arrow ▼ at the right end of the *Security mode* field and choose **Medium** or **High** from the drop-down list.
3. Click the *Configuration* window **Apply** or **OK** button.

NOTE: If the security mode is "Medium" and service-level security is not configured, any Bluetooth device will be able to discover your computer and use it's services without requiring your permission or acknowledgement.

Refer to Section 3 starting on page 25 for additional information on Bluetooth security.

---

[2] When connecting to a Bluetooth device that does not support the encryption feature, change the security mode to *Medium* and ensure that the local services and client applications supported by BTW are not configured to require encryption.

2.2 ACCESSIBILITY TAB

Specify which remote devices may access your computer.

NOTE: Security settings configured in the *General*, *Local Services*, and *Client Applications* tab also determine which devices may discover and access your computer.

The *Accessibility* tab options include:

- *Let other Bluetooth devices discover this computer*—the default configuration (the box to the right of the field is checked) allows remote devices to discover your computer. It is unavailable if the *Allow* option, *No devices to connect*, has been chosen.
- *Allow*—to change this option, click the down-arrow ▼ located at the right end of the *Allow* field and choose one of the following:
  - *All devices to connect*—this is the default setting.
  - *No devices to connect*—your computer can still initiate a connection request to a remote device, but a remote device will not be able to connect to your computer and discover or use it's local services.
  - *Only paired devices to connect*—see Section 3.2 for a description of how devices are paired.
  - *Only devices listed below to connect*—only specific device(s) selected by the *Add Device* feature are allowed to access your computer. Section 2.2.1 describes how to add and delete the specific remote device(s).

2.2.1 Control Which Devices Can Discover Your Computer

When only specific remote devices should have access to your computer, choose the Allow option *Only devices listed below to connect* and use the *Add Device* feature. Access can be taken away from the remote device(s) through the *Delete* feature.

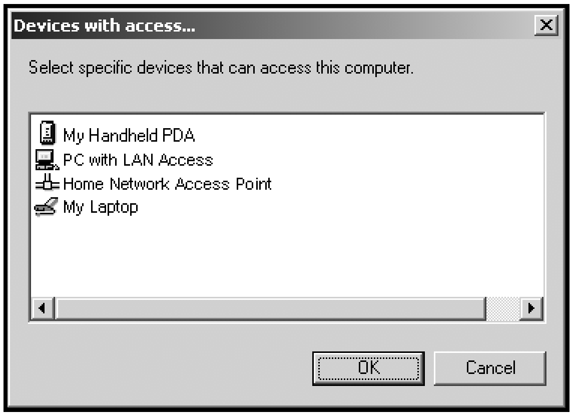
2.2.1.1 Add Device

To allow specific remote devices to access your computer:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Accessibility** tab.
3. Click the down-arrow ▼ located at the right end of the *Allow* field and choose **Only devices listed below to connect**.
4. Click the *Accessibility* tab **Add Device** button.
5. The *Devices with access...* dialog box (Figure 3, page 8) lists the remote devices found in the last Bluetooth Neighborhood device search. Scroll through the list and choose a device.
6. Click the **OK** button on the dialog box.
7. Click the *Configuration* window **Apply** or **OK** button to confirm the remote device addition.

Repeat the process to add additional devices to the list.

Figure 3: Configuration > Accessibility tab > Give access to specific devices.



Devices with access...

Select specific devices that can access this computer.

My Handheld PDA
PC with LAN Access
Home Network Access Point
My Laptop

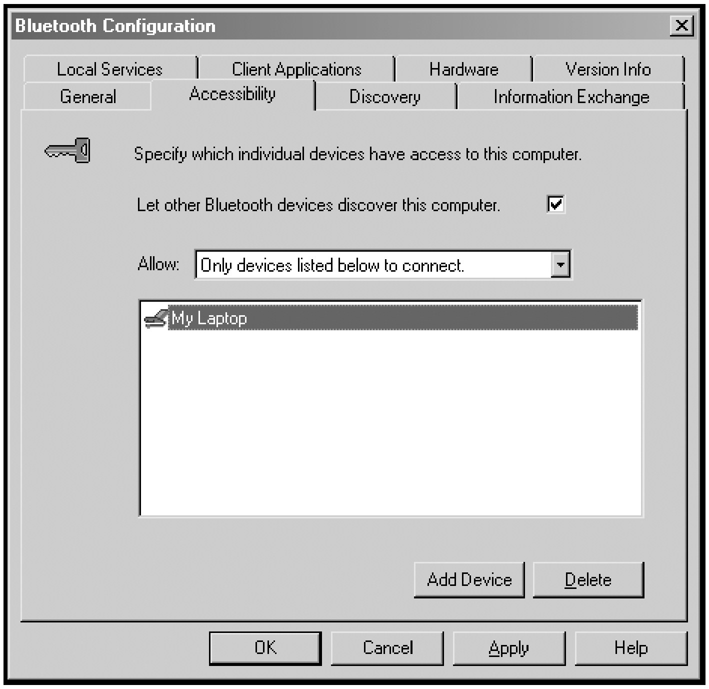
2.2.1.2 Delete Device

Take access away from a specific remote device by deleting it from the list of allowed devices. To do this:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Accessibility** tab.
3. In the *Allow list area*, click a remote device name to select it (Figure 4) and then click the **Delete** button on the *Accessibility* tab.
4. Click the *Configuration* window **Apply** or **OK** button to confirm the deletion.

Repeat these steps for each device to be deleted from the list of allowed devices.

Figure 4: Configuration > Accessibility tab > Take away a remote device's access.



Bluetooth Configuration

Specify which individual devices have access to this computer.

Let other Bluetooth devices discover this computer. ☑

Allow: Only devices listed below to connect.

My Laptop

2.3 DISCOVERY TAB

One of the options configured in the *Discovery* tab determines whether your computer will perform a periodic search for remote devices (see also Section 2.3.1).

The other option specifies through a filter the Bluetooth devices, for example, a *LAN Access Point*, which are reported, that is, listed in the Bluetooth Neighborhood window. Devices may be reported by specific device, device class, or by type within a class of devices (see also Section 2.3.2). The default setting is *Report all Bluetooth devices*.

2.3.1 Periodic Search for Devices

When the Bluetooth Neighborhood window is opened, a search for devices is automatically begun. To configure your computer to make continuous periodic device searches:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Discovery** tab.
3. Check the box labeled **Look for other Bluetooth devices**.
4. In the **Every “X” minutes** field, enter a number between 1 and 60 to set the period of time between searches.
5. Click the *Configuration* window **Apply** or **OK** button.

2.3.2 Control Remote Device Display in the Bluetooth Neighborhood

Based on the default BTW configuration settings, the Bluetooth Neighborhood window displays all the remote devices found, that is, discovered by your computer. The configuration can be changed to control which devices are displayed by adding one or more *filters* to the *Discovery* tab:

- To add filters for one or more specific devices by device name, for example, *My Laptop*, follow the steps illustrated in Figure 5 on page 10 and described in Section 2.3.2.1.
- To add filters for one or more device classes and types within class, for example, “Phone – Cellular,” follow the steps illustrated in Figure 6 on page 12 and described in Section 2.3.2.2.

The steps to delete a filter is described in Section 2.3.2.3 on page 12.

2.3.2.1 Add One or More Specific Remote Devices

The following steps add a filter that results in only specific remote devices being displayed in the Bluetooth Neighborhood window:

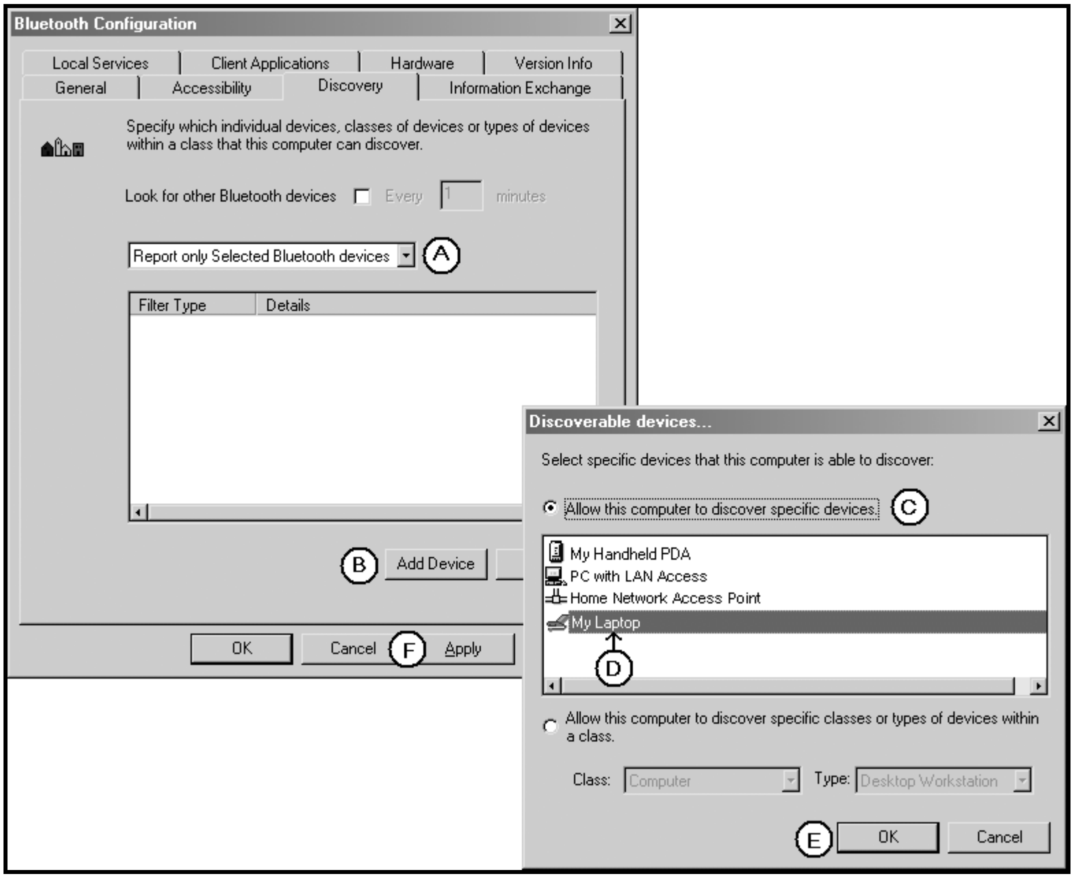
1. Open the Bluetooth Neighborhood window and complete a Search for Devices. When this is complete, open the *Configuration* window. The *General* tab is displayed.
2. Click the **Discovery** tab.
3. Click the down-arrow ▼ located at the right end of the *filter* field (Figure 5-A) and select the **Report only Selected Bluetooth devices** option from the drop-down list.
4. Click the *Discovery* tab **Add Device** button (Figure 5-B). The *Discoverable devices...* dialog box is displayed.
5. Verify that the radio button labeled **Allow this computer to discover specific devices** is selected (Figure 5-C).

6. Scroll through the dialog box list of remote devices and click the name of a device to select it (Figure 5-D).
7. Click the dialog box **OK** button (Figure 5-E). The selected remote device will appear in the *filter list* on the Discovery tab.

> ***NOTE: To select more than one device, hold down the Control (CTRL) or Shift keys while making the selections.***

8. Click the *Configuration* window **Apply** or **OK** button (Figure 5-F).

Figure 5: Configuration >Discovery tab > Adding a specific device filter (composite).



Specify which individual devices, classes of devices or types of devices within a class that this computer can discover.

Look for other Bluetooth devices ☐ Every 1 minutes

Report only Selected Bluetooth devices

Select specific devices that this computer is able to discover:

● Allow this computer to discover specific devices.

○ Allow this computer to discover specific classes or types of devices within a class.

Class: Computer Type: Desktop Workstation

2.3.2.2 Add a Specific Class & Type of Remote Device

The following steps add a filter that results in only remote devices that are a specific class and type being displayed in the Bluetooth Neighborhood window:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Discovery** tab.
3. Click the down-arrow ▼ located at the right end of the *filter* field (Figure 6-A) and select the **Report only Selected Bluetooth devices** option from the drop-down list.
4. Click the *Discovery* tab **Add Device** button (Figure 6-B). The *Discoverable devices...* dialog box is displayed.
5. Check the radio button labeled **Allow this computer to discover specific classes or types of devices within a class** to select it (Figure 6-C).
6. Click the down-arrow ▼ located at the right end of the *Class* field (Figure 6-D) and select a class from the drop-down list. The available classes and the default type, which is automatically selected, are listed in Table 1.

> ***NOTE: If the device type within a class has more than the one option, the default is the first selection in the drop-down list.***

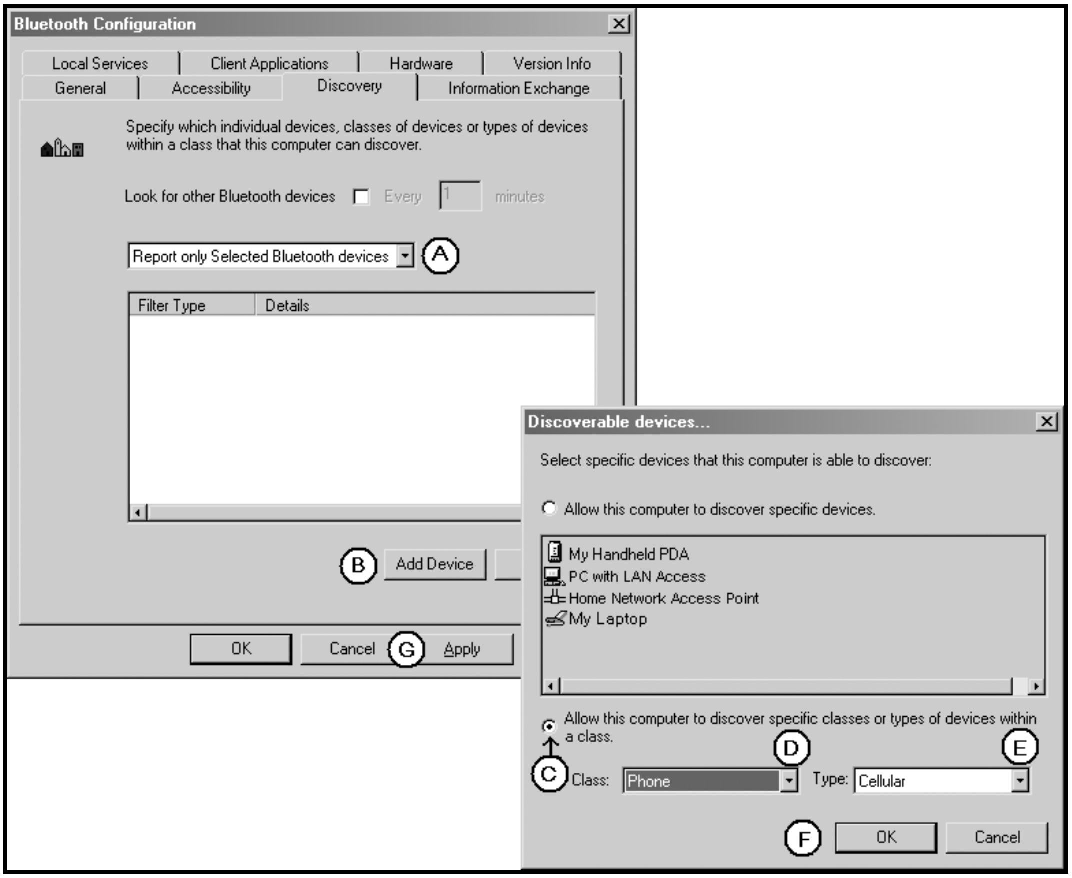
Table 1: Discovery tab > Class and Type of Device Options.

Class of Device and Type of Device Options	
Class of Device	**Type of Device**
Computer	Desktop Workstation **(default)**
	Server Class Computer
	Laptop
	Handheld PC/PDA
	Palm PC/PDA
	All
Phone	Cellular **(default)**
	Cordless
	Smart Phone
	Wired Modem or Voice Gateway
	All
LAN Access Point	All **(default)**
Audio	Headset **(default)**
	All
Peripheral	All **(default)**

7. To change the *Type* field, click the down-arrow ▼ located at the right end of the field (Figure 6-E) and select a type from the drop-down list.
8. Click the dialog box **OK** button (Figure 6-F). The selected device class and type will appear in the *filter list* on the Discovery tab.
9. Click the *Configuration* window **Apply** or **OK** button (Figure 5-F).

Repeat the *Add Device* process to select and add additional, remote device classes and types to the filter list.

Figure 6: Configuration > Discovery tab > Adding device class/type filter (composite).



Specify which individual devices, classes of devices or types of devices within a class that this computer can discover.

Look for other Bluetooth devices ☐ Every 1 minutes

Report only Selected Bluetooth devices

Select specific devices that this computer is able to discover:

○ Allow this computer to discover specific devices.

- My Handheld PDA
- PC with LAN Access
- Home Network Access Point
- My Laptop

● Allow this computer to discover specific classes or types of devices within a class.

Class: Phone

Type: Cellular

2.3.2.3 Delete

Until it is removed a filter for a specific device or class and type of device added to the *Discovery* tab will control which remote devices are displayed in the Bluetooth Neighborhood window.

To delete a filter:

1. Open the *Configuration* window. The *General tab* is displayed.
2. Click the **Discovery** tab.
3. Click a *filter* in the *filter list* area to select it. The filter is highlighted.
4. Click the *Discovery tab* **Delete** button.
5. Click the *Configuration* window **Apply** or **OK** button to confirm the deletion.

> ***NOTE: After all the filters are deleted, select the "Report all Bluetooth devices" option. Otherwise, an error message will be displayed when you click the Apply or OK button.***

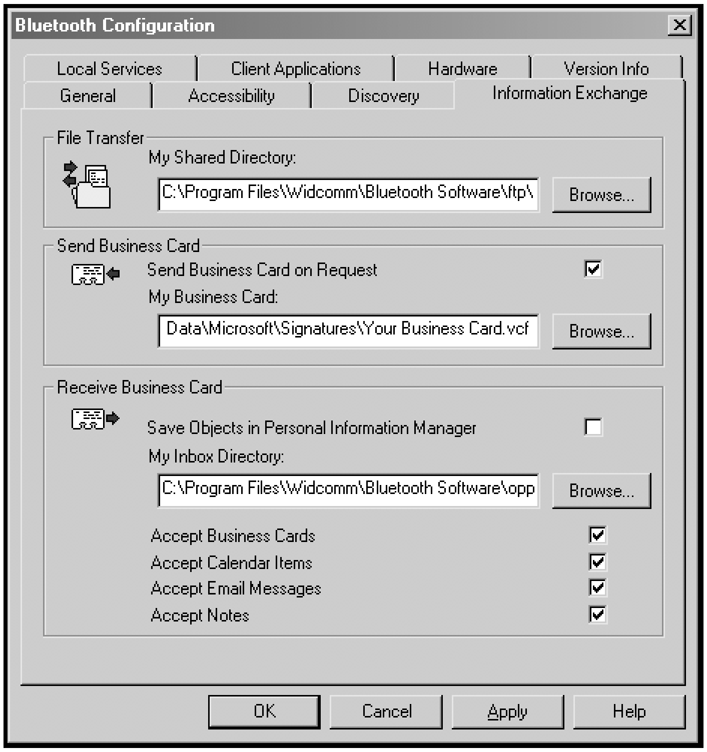
A way to override a filter (or filters) without deleting them is to select the *Discovery* tab option *Report all Bluetooth devices*. The filter window and *Add Devic*e and *Delete* buttons are disabled. To enable the filters again, select the *Report only Selected Bluetooth devices* option.

2.4 INFORMATION EXCHANGE TAB

The *Information Exchange* tab (Figure 7) options determine:

- *My Shared Directory*:
  - The highest-level directory on your computer that a remote device is able to access.
- *My Business Card*:
  - The path and filename on your computer that your electronic business card is sent from and a selection that determines if a remote device can pull your business card.
- *My Inbox Directory*:
  - The directory path where items, for example, email messages, are received from remote devices.
  - A selection that determines if the items received by your computer should be automatically stored in your personal information manager, for example, Microsoft® Outlook®.
  - The types of items (“objects”) your computer will accept.

Figure 7: Configuration > Information Exchange tab.



File Transfer

My Shared Directory: C:\Program Files\Widcomm\Bluetooth Software\ftp\

Send Business Card

Send Business Card on Request ☑

My Business Card: Data\Microsoft\Signatures\Your Business Card.vcf

Receive Business Card

Save Objects in Personal Information Manager ☐

My Inbox Directory: C:\Program Files\Widcomm\Bluetooth Software\opp

Accept Business Cards ☑
Accept Calendar Items ☑
Accept Email Messages ☑
Accept Notes ☑

2.4.1 My Shared Directory

The *My Shared Directory* setting configures the highest-level directory your computer's file structure that a remote device may access.

To change the default *My Shared Directory*:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Information Exchange** tab.
3. In the *File Transfer* section of the *Information Exchange* tab, click the **Browse** button and navigate to the new directory.
4. Click the dialog box **OK** button.
5. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

2.4.2 My Business Card

The *Send Business Card* section of the *Information Exchange* tab sets the path and filename to your electronic business card ("vcard") and an option that determines if the vcard will be sent to any remote device that requests it.

To change the default *My Business Card* directory:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Information Exchange** tab.
3. In the *Send Business Card* section of the *Information Exchange* tab, click the **Browse** button and navigate to the new directory and vcard file name (*.vcd, *.vcf, and others).
4. Click the dialog box **OK** button.
5. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

To have your *vcard* automatically sent to any remote device that requests it:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Information Exchange** tab.
3. In the *Send Business Card* section of the *Information Exchange* tab, check the box labeled *Send Business Card on Request*.
4. Click the dialog box **OK** button.
5. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

2.4.2.1 Create an Electronic Business Card

BTW does not install a default vcard. The user should create their own vcard (.vcd or .vcf) in Microsoft Outlook or Outlook Express and then redirect the *My Business Card* entry to the path and filename of the user's business card.

The general steps to create a vcard in Microsoft Outlook are:

1. Start Outlook.
2. On the *Outlook* menu bar, click **File** followed by **New** followed by **Contact**.
3. In the *Contact* dialog box, enter the business card information—name, email address, telephone number, etc.
4. After the information is entered, from the *Contact* dialog box menu bar, click **File** followed by **Save**. The contact is saved, but the dialog box remains open.
5. Export the contact to the vCard file. From the *Contact* dialog box menu bar, click **File** followed by **Export to vCard file....** The default directory is typically `...Application Data\Microsoft\Signatures\*.vcf.`

The general steps to create a *vcard* in Microsoft Outlook Express are:

1. Start Outlook.
2. On the *Outlook Express* menu bar, click **File** followed by **New** followed by **New Contact**.
3. In the *Contact* dialog box, enter the card information—name, email address, telephone number, etc.
4. Click **OK** to save the new contact to the address book.
5. Export the contact to a *vcard*. From the *Outlook Express* menu bar, click **Tools** followed by **Address Book**; click the contact to select it. From the *Address Book* menu bar, click **File** followed by **Export** followed by **Business Card** (*.vcf). In the *Save In* list, select the folder where the vcard file should be saved, then click **Save**.

For additional information on how to create contacts in Outlook and export these as *vcards* refer to Microsoft Outlook's help assistance.

2.4.3 My Inbox Directory

The *Receive Business Card* section of the *Information Exchange* tab sets the path to the directory where items, for example, email messages, are received from remote devices.

A selection determines if the received items should be automatically stored in a personal information manager, for example, Microsoft® Outlook®. You can also configure what items ("objects") your computer will accept.

To change the *My Inbox Directory*:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Information Exchange** tab.
3. In the *Receive Business Card* section of the *Information Exchange* tab, clear the check box labeled **Save Objects in Personal Information Manager** (box unchecked is the default).
4. Click the *Receive Business Card* section's **Browse** button and navigate to the new inbox directory.
5. Click the dialog box **OK** button.
6. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

To change the items your computer will accept, that is, receive, check one or more of the boxes:

- Accept Business Cards.
- Accept Calendar Items.
- Accept Email Messages.
- Accept Notes.

When the options have been set, click the *Configuration* window **Apply** or **OK** button to confirm the changes.

2.5 LOCAL SERVICES TAB

The local services provided by your computer to remote devices are specified in the *Local Services* tab. Each service can be configured individually for security, name, and other settings. The *Local Services* tab window and Service Properties dialog box are shown in Figure 8 on page 18.

The *Local Services* tab also includes options to add and delete user-defined serial services.

The local services are shown in Table 2:

Table 2: BTW Local Service Names.

Bluetooth for Windows Local Service Names		
BTW Local Service Name	**Bluetooth Specification Equivalent**	**Bluetooth Acronym**
Bluetooth Serial Port	Serial Port Profile	SPP
Dial-Up Networking	Dial-up Networking	DUN
Fax	Fax	FAX
File Transfer	File Transfer Protocol	FTP
Information Exchange	OBEX Push/Pull	OPP
Information Synchronization	OBEX IrMC Sync	SYNC
Network Access	Local Area Network Access using Point-to Point Protocol	LAP

2.5.1 Modify Local Service Properties

The properties' settings that are common to all the local services are:

- Security:
  - None (leave all *security* boxes unchecked).
  - Authentication only.
  - Authentication and Authorization.
  - Authentication and Encryption.
  - Authentication, Authorization, and Encryption.
- Startup—box checked (the default) causes the service to start when your computer is started.
- Service Name.

Additionally, some local services have additional properties:

- Network Access—has one additional setting for *Maximum Connections*.
- Dial-Up Networking—has one additional setting for *Modem*.
- Fax—has one additional setting for *Modem*.
- Bluetooth Serial Port—has one additional setting for *COM Port*.

To change a local service's properties:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Local Services** tab.
3. Double-click a *Service Name* to open the *Service Properties* dialog box.
4. Make the change(s).
5. Click the dialog box **OK** button.
6. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

The service properties, which may be changed, include:

- *Startup*—check the box to start the service when the system is initialized. Enabled is the default (box checked). If the box is not checked, the service can be manually started.

  > ***NOTE: To manually start or stop a service, refer to the instructions described in the BTW Bluetooth Neighborhood User's Guide, WIDCOMM's document number BTW-DOCS-011100-1700.***

- Security:
  - *Authorization*—check the box to require confirmation when a remote device wants to use this local service. Disabled is the default (box not checked). *Authentication is also automatically selected.*
  - *Encryption*—check the box to require the use of encrypted links to send data when this service is used. Disabled is the default (box not checked). *Authentication is also automatically selected.*
  - *Authentication*—check the box to require remote devices to authenticate when a connection is established with this service. The remote device and your computer will be required to exchange passkeys. Once the devices authenticate, they become paired and no further authentication is required unless the pairing is broken. Disabled is the default (box not checked).
- *Maximum Connections*—from the drop-down list choose the maximum number of connections this service may use.

  > ***NOTE: The Maximum Connections option is only available to the Network Access service.***

- *Modem*—from the drop-down list choose a modem this service should use.

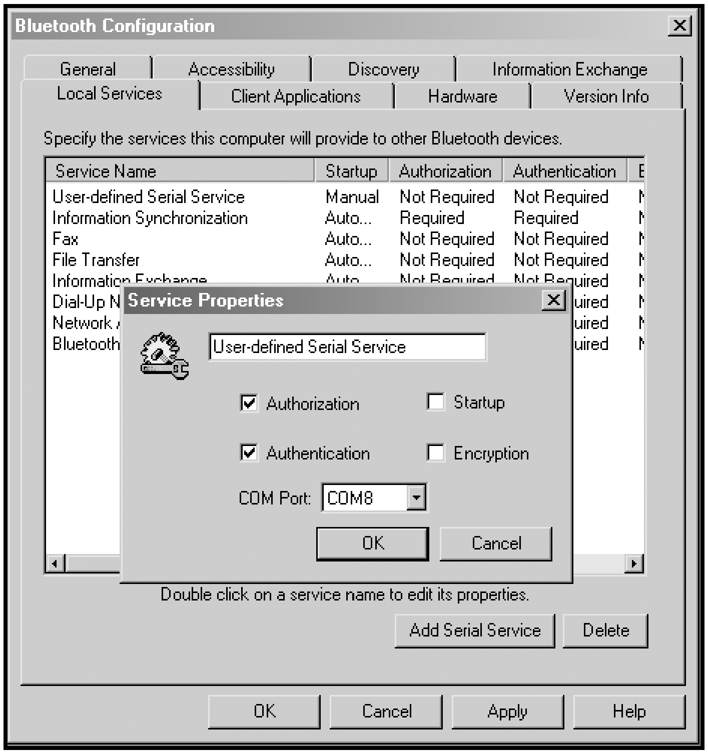
  > ***NOTE: The Modem option is only available for the Dial-Up Networking and Fax services.***

- *COM Port*—click the down arrow ▾ at the right end of the *COM Port* field and select any port not in use by the system.

  > ***NOTE: The COM Port option is only available for the Bluetooth Serial Port service and user-defined serial services.***

- *Service Name*—select the service name to highlight it and key a valid and unique name between 1 and 99 characters, for example *Other Service*. Typically, this option is used only when creating a user-defined serial service.

Figure 8: Configuration > Local Services tab > Service Properties dialog box.



Specify the services this computer will provide to other Bluetooth devices.

Service Name	Startup	Authorization	Authentication	E
User-defined Serial Service	Manual	Not Required	Not Required	N
Information Synchronization	Auto...	Required	Required	N
Fax	Auto...	Not Required	Not Required	N
File Transfer	Auto...	Not Required	Not Required	N
Information Exchange	Auto...	Not Required	Not Required	N
Dial-Up N			uired	N
Network			uired	N
Bluetooth			uired	N

User-defined Serial Service

☑ Authorization ☐ Startup

☑ Authentication ☐ Encryption

COM Port: COM8

Double click on a service name to edit its properties.

2.5.2 Add a User-defined Serial Service

Applications that use serial connections, for example, HyperTerminal, will use the Bluetooth Serial Port service to transfer data as though a physical serial cable connects your computer and the remote device.

In some instances, it may be advantageous to have more than one Bluetooth Serial Port, for example:

- When more than one serial connection is up and running at the same time (if Point-to-Multipoint connections are supported by your Bluetooth devices).
- In place of the BTW Bluetooth Serial Port service—the user-defined serial service would be configured to specific settings that your computer should use each time it makes a serial connection to a specific remote device. The name could be set to clearly identify the connection, for example, *Serial_PDA to Laptop_COM8*. This would identify a serial connection between two specific Bluetooth devices using COM port 8.

To add a user-defined serial service:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Local Services** tab.
3. Click the *Local Services* tab **Add Serial Service** button.
4. In the *Service Properties* dialog box, modify the properties:
    a) In the *Service Name* field, select *Bluetooth Serial Port* to highlight it and key a valid, user-defined serial service name between 1 to 99 characters, for example, *User-defined Serial Service.*

> ***NOTE: No two local services may have the same service name. However, a local service name and client application name can be the same.***

   b) Make changes to the security settings as desired:
      - *Authorization*—check the box to require confirmation when a remote device wants to use this service. *Authentication is automatically selected.*
      - *Encryption*—check the box to require the use of encrypted links to send data when this service is used. *Authentication is automatically selected.*
      - *Authentication*—check the box to require remote devices to authenticate when a connection is established with this service. The remote device and your computer will be required to exchange passkeys. Once the devices authenticate, they become paired and no further authentication is required unless the pairing is broken.

   c) To have this user-defined service startup automatically when the system is initialized, check the *Startup* box.

   d) Click the down arrow ▼ at the right end of the *COM Port* field and select any port not in use by the system.

5. Click the dialog box **OK** button. The user-defined serial service will be displayed in the Local Services tab service list.
6. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

2.5.3 Delete a User-defined Serial Service

To delete a user-defined serial service:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Local Services** tab.
3. In the service list area, click the *Service Name* of a user-defined serial service to select it.
4. Click the *Local Services* tab **Delete** button. The service is removed from the service list.
5. Click the *Configuration* window **Apply** or **OK** button to confirm the deletion.

> ***NOTE: The Delete button can only be used to delete the Bluetooth Serial Port service or user-defined serial services.***

2.6 CLIENT APPLICATIONS TAB

In the context of this guide, client applications are the local software that allows your computer to interact with other Bluetooth devices that provide a similar local service. For example, the Bluetooth Serial Port client application on your computer allows it to establish a virtual COM port with a remote device that provides the Bluetooth specification Serial Port Profile service.

The *Client Applications* tab options provide a means to configure each client application individually for security, name, and other settings.

The *Client Applications* tab also has options to delete applications and/or add a user-defined COM port. This is similar to the Add Serial Service feature on the *Local Services* tab.

The BTW client applications share the same names as the BTW Local Services (see Table 2, page 16). The following is a brief description of what each client application is used for:

- Bluetooth Serial Port—configures a local virtual COM Port. Legacy applications can then use the port.
- Dial-Up Networking—configures the over-the-air connection to a modem on a remote device. The remote modem can then be used to connect to an Internet Service Provider (ISP).
- Fax—makes a connection available for use when this device interacts with other Bluetooth devices. The connection is used to fax documents as though the fax device, for example, a fax modem, was physically attached to your computer. In actuality, the fax is connected to the remote device.
- File Transfer—makes a connection available for use when your computer carries out file system actions on a remote device:
  - Obtain a directory list.
  - Get and put files.
  - Change folders.
  - Delete files.
- Information Exchange—makes a connection available for use when your computer wants to:
  - Send to and receive business cards from a remote device.
  - Receive calendar items, email messages, and notes from a remote device.
- Information Synchronization—makes a connection available to synchronize personalize information management databases.
- Network Access—provides LAN access via a remote server.

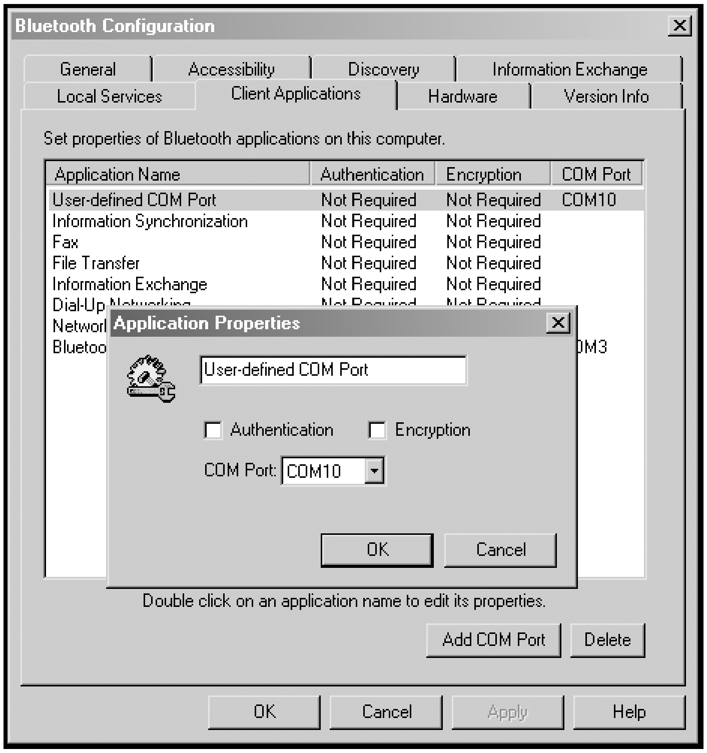
2.6.1 Modify Client Application Properties

The options in the *Application Properties* dialog boxes (Figure 9) are the same for all applications except for the Bluetooth Serial Port application, which has an additional COM Port setting.

To change a client application's properties:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Client Applications** tab.
3. Double-click an *Application Name* to open the *Application Properties* dialog box.
4. Make the change(s).
5. Click the dialog box **OK** button.
6. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

Figure 9: Configuration > Client Applications tab > Application Properties dialog box.



Set properties of Bluetooth applications on this computer.

Application Name	Authentication	Encryption	COM Port
User-defined COM Port	Not Required	Not Required	COM10
Information Synchronization	Not Required	Not Required	
Fax	Not Required	Not Required	
File Transfer	Not Required	Not Required	
Information Exchange	Not Required	Not Required	
Dial-Up Networking	Not Required	Not Required	
Networl			
Bluetoo			M3

User-defined COM Port

☐ Authentication ☐ Encryption

COM Port: COM10

Double click on an application name to edit its properties.

The client application properties, which may be changed, include:

- Security:
  - *Encryption*—check the box to require the use of encrypted links when sending data. Disabled is the default (box not checked). *Authentication is automatically selected.*
  - *Authentication*—check the box to require remote devices to authenticate when a connection is established with this application. The remote device and your computer will be required to exchange passkeys. Once the devices authenticate, they become paired and no further authentication is required unless the pairing is broken. Disabled is the default (box not checked).

- *COM Port*—from the drop-down list choose a Virtual COM Port for the connection made with this application. Choose any port not in use by the system.

> ***NOTE: The COM Port option is only available for the Bluetooth Serial Port client application and user-defined COM ports.***

- *Application Name*—select the application name to highlight it and key a valid and unique name between 1 and 99 characters, for example, *Other Application*. Typically, this option is only used when creating a user-defined COM port.

2.6.2 Add a User-defined COM Port

Applications that use serial connections, for example, HyperTerminal, will use the Bluetooth Serial Port client application to transfer data as though a physical serial cable connects your computer and the remote device.

In some instances, it may be advantageous to have more than one Bluetooth Serial Port, for example:

- When more than one serial connection is up and running at the same time (if Point-to-Multipoint connections are supported by your Bluetooth devices).
- In place of the BTW Bluetooth Serial Port client application—the user-defined COM port would be configured to specific settings that your computer should use each time it makes a serial connection to a specific remote device. The name could be set to clearly identify the connection, for example, *Serial_PDA to Laptop_COM8*. This would identify a serial connection between two specific Bluetooth devices using COM port 8.

To add a user-defined COM port:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Client Applications** tab.
3. Click the *Client Applications* tab **Add COM Port** button.
4. In the *Application Properties* dialog box, modify the properties:
   a) In the *application name* field, select *Bluetooth Serial Port* to highlight it and key a valid, user-defined COM port name between 1 to 99 characters, for example, *User-defined COM Port.*

   > ***NOTE: No two client applications may have the same name. However, a local service name and client application name can be the same.***

   b) Make changes to the security settings as desired:
      - *Encryption*—check the box to require the use of encrypted links when sending data. *Authentication is automatically selected.*
      - *Authentication*—check the box to require your computer and the remote devices to authenticate when a connection is established. Both devices will be required to exchange passkeys. Once the devices authenticate, they become paired and no further authentication is required unless the pairing is broken.

   c) Click the down arrow ▼ at the right end of the *COM Port* field and select any port not in use by the system.
5. Click the dialog box **OK** button. The user-defined COM port will be displayed in the *Client Applications* tab list.
6. Click the *Configuration* window **Apply** or **OK** button to confirm the change.

2.6.3 Delete a User-defined COM Port

To delete a user-defined COM port:

1. Open the *Configuration* window. The *General* tab is displayed.
2. Click the **Client Applications** tab.
3. In the service list area, click the *Application Name* of a user-defined COM port to select it.
4. Click the *Client Applications* tab **Delete** button. The COM port is removed from the application list.
5. Click the *Configuration* window **Apply** or **OK** button to confirm the deletion.

NOTE: The Delete button can only be used to delete the Bluetooth Serial Port client application or user-defined COM ports.

2.7 HARDWARE TAB

The *Hardware* tab displays the properties of the Bluetooth device (for example, PC card, multi-port, or USB dongle) installed on your computer. This tab also provides a means to alter the Bluetooth device's hardware configuration such as Country Code and Maximum Transmission Power.

2.7.1 Bluetooth Device Properties

Various device properties information is displayed. These include, but are not limited to Manufacturer, Firmware Revision, Device Status, and Device Address—this is the *Bluetooth Device Address* or *BDA* / *BD Addr* set at the factory.

2.7.2 Bluetooth Device Hardware Settings

The hardware configuration of the Bluetooth device installed on your computer has up to two settings that can be changed. The default settings will be appropriate for most users. However if changes need to be made, click the **Advanced** button located toward the bottom right of the *Hardware tab* to display the *Advanced Settings* dialog box:

- *Country Code*—click the down arrow ▼ and choose an option from the drop-down list:
  - *North America, Europe (except France), Japan*—this is the default setting.
  - *France*—if operating a device in France, change to this setting. The Bluetooth connection will be limited to the 23 channels (out of the 79 total channels in the unlicensed 2.4 GHz spectrum) that are available in France.
- *Maximum Transmission Power "X" dBm*—where "X" is a number between eight (8) and twenty (20), in increments of two (2), e.g., 8, 10...18, 20. Click the down arrow ▼ and select a power setting from the drop-down list.
  A higher setting extends the range for the Bluetooth wireless connection. For example, if a remote device is in an office separate from your computer, the maximum transmission power may need to be boosted in order to communicate with the remote device. However, a higher maximum transmission power setting (widened range) may increase the number of unwanted connection requests that your computer will receive from other remote devices.

NOTE: The Maximum Transmission Power setting is not available for all Bluetooth devices. Hardware settings may vary depending upon the device.

Save the *Advanced Settings* changes to update the BTW configuration:

1. Click the **Apply** button to close the *Advanced Settings* dialog box.
2. When the *activate new settings* message is displayed, press the **Yes** button. Your Bluetooth device (not your computer) will reset and any active Bluetooth wireless connections will be disconnected. If you click the *No* button, the new settings will not be applied until the Bluetooth device and/or the computer are restarted.

Click the *Cancel* button on the *Advanced Settings* dialog box to discard any changes.

2.8 VERSION INFO TAB

Provides version number information for BTW and its component. There are no options to configure.

3 Security

3.1 INTRODUCTION

3.1.1 Device Identity

Each Bluetooth device has a unique forty-eight-bit binary *Bluetooth Device Address* (BDA) burned into its Read-Only Memory (ROM) during the manufacturing process. This address cannot be changed by the end-user.

A device's BDA is usually displayed in hexadecimal format. For example, a valid BDA is 00:D0:B7:03:2E:9F.

Each Bluetooth device also has an operator-configurable, user-friendly name to help distinguish it from other Bluetooth devices in the Bluetooth Neighborhood.
Valid user-friendly names include:

- Bob's PC.
- Randy's Laptop.
- John Q. Public's PDA.

User-friendly names make it easer to recognize the devices in the Bluetooth Neighborhood. However, because individuals other than the user can change the name, it is not reliable for security purposes.

3.1.2 Security Levels

Bluetooth offers three primary levels of security:

- None—all Bluetooth devices are allowed to connect. This is the BTW default security configuration. The *Local Services* and *Client Applications* do not require Authorization, Authentication, or Encryption. Services are started automatically at system start. The *Medium* security setting on the *Configuration* window *General* tab allows the individual local services and client applications to determine the actual level of security.
- Service Level—individual local services on your computer may be disabled. The disabled services will not start automatically when your computer is started. These services will not be available to any remote device. At the service level, the following options may be set:
  - Encryption—data will be sent using encrypted links. This provides additional security.
  - Authorization—authorization must be given to a remote device before it can connect to a service on your computer. This is usually done by physically clicking an on-screen button.
  - Authentication—a remote device must provide a link key (like a password). The link key is generated through the passkey process the first time the remote device connects to your computer.
- Link Level—in BTW when security is configured as *High*, all devices discovering your computer, regardless of which local service the remote device is attempting to use, will be required to provide a link key.
  - Authentication—a remote device must provide a link key. The link key is generated through the passkey process the first time the remote device connects to your computer.

Each Bluetooth-enabled device may handle security in a slightly different manner. Refer to the user guide provided with a Bluetooth device for additional information.

3.1.2.1 Service Level

Each Bluetooth service (for example, Network Access) can be selectively disabled.

If all Bluetooth services are disabled, your computer is unable to accept connections from a remote device.

Your computer can still initiate outgoing connections to other Bluetooth devices, but incoming connections will not be allowed.

Advantages: Extremely strong security.

Disadvantages: It is non-selective; it shuts out all incoming Bluetooth connections for a particular service.

3.1.2.2 Encryption

The Bluetooth specification allows for encrypted transactions using a key size of up to 128 bits.

Some Bluetooth devices do not support encryption. If a device or service is configured to use encryption and attempts a connection with a device that does not support encryption, the connection may fail unexpectedly.

Advantages: Protects against radio frequency snooping.

Disadvantages: The receiving unit must also support encryption.

3.1.2.3 Authorization

Authorization provides name-level security.

A visual warning notifies the local operator that a remote device is attempting to access the system.

The local operator can open a dialog box that provides:

- Name-level security information—the user-friendly name of the device attempting access.
- The type of access the requesting device is trying to achieve.

Based on the information provided in the dialog box, the operator may authorize or deny access by physically clicking an on-screen button.

If the initial notification is ignored, access is denied after a preset timeout period expires.

Authorization does not provide foolproof security since Bluetooth device names are configurable by the end-user.

Advantages: Ease of use—requires a dialog box response.

Disadvantages: Weak security.

3.1.2.4 Authentication

Authentication requires a passkey from the remote device attempting to access your computer.

A visual security notification is given when a remote device attempts to access your computer.

When the notification is acknowledged, a dialog box opens; it provides:

- Name-level security information—the user-friendly name of the device attempting access.
- A place to enter a passkey.

The operator of the remote system must enter the identical passkey or access is denied.

If the security notification is ignored, access is denied after a preset timeout period expires.

Advantages: Stronger security.

Disadvantages: Passkeys must be protected.

3.1.2.5 Link Keys

To avoid entering a passkey time-after-time for a known and trusted remote device, a link key can be created.

A link key is a mathematical construct created from:

- The passkey.
- The *Bluetooth Device Address* (BDA) of the remote device.
- An internally generated, random number.

There is no limit to the number of link keys that may be created.

Devices that share a link key are "paired."

Paired devices are authenticated automatically, without operator intervention.

3.2 PAIRING

BTW users usually will want to *pair*[3] the devices frequently used for Bluetooth wireless connections. This will save time by minimizing interaction with BTW security processes—such as passkey entry and authorization.

For example, if you pair your laptop computer and cellular telephone, persistent security is established between the devices. This will enable the laptop to quickly access the Internet with a Dial-Up Networking connection on the cellular telephone without entering passkeys after the initial connection is made.

Devices are paired through BTW's BTTray *Security* window. This process can take place at the time of the first connection between two devices, or for ease of use, can be done before the first connection is made.

Only pair devices that are in your control—your cellular telephone, your laptop computer, your desktop computer. Additionally, give the paired devices access to only those services that will be used. For example, a laptop is most likely only going to use the cellular telephone's Dial-Up Networking service.

Once a device is paired it remains paired even if the user:

- Stops the Bluetooth connection(s) between the devices.
- Reboots one or both devices.
- Stops and starts the services on the devices.

NOTE: A paired device will be displayed in the Bluetooth Neighborhood window even if the device is not within radio range and/or powered on at the time Bluetooth Neighborhood is opened and explored.

For additional information on how to pair a specific device, refer to the quick-start guide or other setup manual received with your Bluetooth device.

---

[3] Pairing is also referred to as bonding.

3.2.1 Pair Devices before First Connection

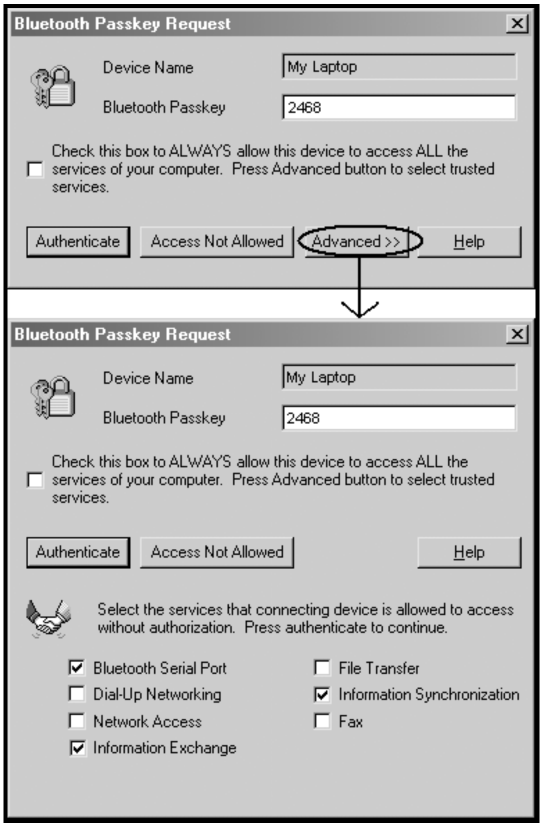
To pair your computer with a remote device before the first connection:

1. Right-click the *BTTray* icon in the Windows system tray and choose the **Security** option. The Bluetooth *Security* window is displayed (Figure 2, page 3).
2. In the *Found Devices* list, click the name of the remote device to be paired, for example, *My Laptop*. Scroll down if necessary. The list displays all remote devices currently within radio range. As needed, click the *Refresh* button to update the list.
3. Click the **Execute Pairing>>** button. A *Passkey Request* dialog box appears.
4. Set the *Passkey Request* dialog box options as follows:
   a) In the *Bluetooth Passkey* field, key a valid passkey—a valid passkey is 1 to 16 characters, for example, *2468*.

   > ***NOTE: A passkey is like a Personal Identification Number (PIN). The same number must be entered as a passkey on the remote device being paired.***

   b) To pair the device with authorization to use *all the local services* on your computer, click the check box labeled **Check this box to ALWAYS allow this device to access ALL the services of your computer. Press Advanced button to select trusted services.**
   OR
   To pair the device with authorization to use *selected local services*, click the **Advanced >>** button (Figure 10) and select the services by clicking the check box next to each service name.

Figure 10: Security > Pair Devices > Passkey Request dialog box (composite).



Device Name: My Laptop
Bluetooth Passkey: 2468

☐ Check this box to ALWAYS allow this device to access ALL the services of your computer. Press Advanced button to select trusted services.

Select the services that connecting device is allowed to access without authorization. Press authenticate to continue.

☑ Bluetooth Serial Port
☐ Dial-Up Networking
☐ Network Access
☑ Information Exchange
☐ File Transfer
☑ Information Synchronization
☐ Fax

5. Click the **Authenticate** button.
6. On the remote device, respond to the pairing request.

> ***NOTE: If BTW is installed on the remote device, click the BTTray icon when the security notification appears (see Section 3.3.1, page 31). Enter the same passkey entered on your computer (Step 4-a) and press the Authenticate button.***

The paired device will be displayed in the *Paired Devices* list (Figure 2, page 3) of the Bluetooth *Security* window.

Figure 10 shows pairing with a device and authorizing it to use selected services on your computer. In this example, the remote device, *My Laptop*, is authorized to use the three selected services—Bluetooth Serial Port, Information Exchange, and Information Synchronization. When *My Laptop* connects and uses an authorized service it will not be required to enter a passkey or receive any additional authorization. However, if *My Laptop* tries to connect to an unauthorized service, for example, *Dial-Up Networking*, user intervention will be required to authorize the paired device to use the service. See Section 3.3.2, beginning on page 32, for additional information.

3.2.2 Pairing Devices during First Connection

Devices may also be paired during the first actual Bluetooth wireless connection. To do this simply wait until your computer attempts to connect to a remote device that requires authentication or a remote device attempts to connect to a service on your computer that requires authentication.

On your computer a security notification will be given (see also Section 3.3.1 on page 31), when that is responded to the *Passkey Request* dialog box described in Section 3.2.1 and shown in Figure 10, page 28, will be displayed. Set the *Passkey Request* dialog box options as follows:

1. In the *Bluetooth Passkey* field, enter a valid passkey—a valid passkey is 1 to 16 characters, for example, *2468*.

> ***NOTE: A passkey is like a Personal Identification Number (PIN). The same number must be entered as a passkey on the remote device being paired. Just like a PIN if you forget the passkey number, you will have to break the paired relationship and start over.***

2. If the remote device initiated the connection, your computer is the *server* and it must authorize the remote device to use either *all the local services* on your computer or *selected local services*. If your computer is the client, skip to step 3:
   - To authorize use of *all the local services*, click the check box labeled **Check this box to ALWAYS allow this device to access ALL the services of your computer. Press Advanced button to select trusted services.**

   OR

   - To authorize the use of only *selected local services*, click the **Advanced >>** button and select the services by clicking the check box next to each service name.
3. Click the **Authenticate** button.

Once the passkey is entered, it is stored and the devices become paired. Security notifications will only appear during future connections if either device attempts to use a service on the other device for which authorization has not yet been given.

3.2.3 Break Paired Device Relationship

When devices are paired, the configuration information is saved on both your computer and the remote device. BTW displays the paired device name(s) in the *Paired Devices* list of the Bluetooth *Security* window (Figure 2, page 3). Devices remain paired until the relationship is broken, that is, deleted, on both devices.

To break a paired device relationship on your computer:

1. Right-click the *BTTray* icon in the Windows system tray and choose the **Security** option. The Bluetooth *Security* window is displayed (Figure 2, page 3).
2. In the *Paired Devices* list, click the name of the paired device, for example, *My Laptop*. Scroll down if necessary.
3. Click the **<< Delete** button.
4. Click the **Done** button to confirm the deletion and close the window.

To cancel the deletion before the window closes, click the close button ☒ in the upper-right corner of the window.

To break a paired device relationship on the remote device (if BTW is installed):

NOTE: If the remote device does not have BTW installed refer to the pairing instructions that came with the Bluetooth device.

1. Right-click the *BTTray* icon in the Windows system tray and choose the **Security** option. The Bluetooth *Security* window is displayed (Figure 2, page 3).
2. In the *Paired Devices* list, click the name of the paired device, for example, *My Computer*. Scroll down if necessary.
3. Click the **<< Delete** button.
4. Click the **Done** button to confirm the deletion and close the window.

To cancel the deletion before the window closes, click the close button ☒ in the upper-right corner of the window.

NOTE: Failure to break the pairing on both sides (your computer and the remote device) may result in unpredictable behaviors and pose a security risk.

3.3 HANDLING SECURITY FOR NON-PAIRED DEVICES

With Bluetooth wireless connections, the device acting as the server, that is, the device providing a Bluetooth service, controls security. For example, if a remote device connects to your computer and uses one of its local services, your computer is the *server* and the remote device is the *client*.

When BTW security is configured on your computer[4] to require authentication, a security notification will be displayed it each time a non-paired remote device ("client") attempts to connect. You can give the client permission (*authorize* and *authenticate*) to use your computer's services or you can deny the request.

Section 3.2—Pairing describes a method to grant ongoing permission to a remote device to use all or selected services on your computer. Once paired and authorized, a client will be able to use your computer's services without any notification.

---

[4] Security can be configured in the *General* tab – *Security* mode or in the *Local Services* tab or *Client Applications* tab for individual services.

However, if pairing is not desirable, permission can be given on a connection-by-connection basis. Permission can be at two levels, authentication and authorization or authentication only:

- Authentication requires the client and server to enter the same passkey on both devices during the first connection.
- Authentication and Authorization requires the passkey and the additional step of authorizing access to services not previously authorized.

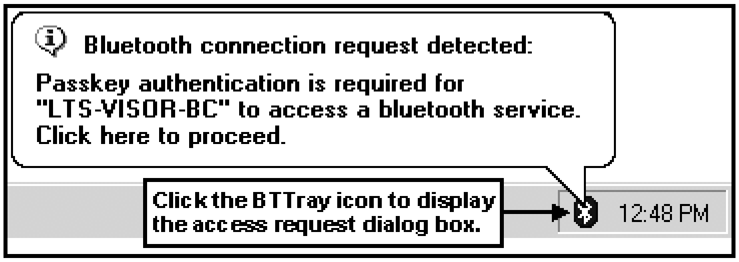
3.3.1 Security Notifications

If BTW is configured for *High* security or when a local service is configured for authentication and authorization or authentication only, a visual warning provides a security notification that a remote device is attempting to connect to your computer.

The method of notification depends on the Windows operating system and is described below:

- Windows 2000 and Windows Me—the security notification is given in a bubble help message that is displayed on your computer. An example is shown in Figure 11.
- Windows 98SE—a flashing BTTray icon in the Windows system tray provides the security notification.

Figure 11: Security notification > Windows 2000 and Windows Me > Bubble message.



Bluetooth connection request detected:

Passkey authentication is required for "LTS-VISOR-BC" to access a bluetooth service. Click here to proceed.

Click the BTTray icon to display the access request dialog box.
12:48 PM

To respond to a security notification:

- As shown in Figure 11, click the BTTray icon (not the bubble message) to display a dialog box.
- Set the options in the dialog box. These options will determine how security will be handled between your computer and the connecting remote device.

If you ignore the security notification, after a preset timeout period has expired, the connection request will fail.

Two possible security dialog boxes will be displayed on your computer:

- Bluetooth Passkey Request (Authentication).
- Bluetooth Authorization Request.

The option(s) set in these dialog boxes and the actions taken will determine how access for a connection and future connections between your computer and a remote device are handled.

3.3.2 When Authorization is Required

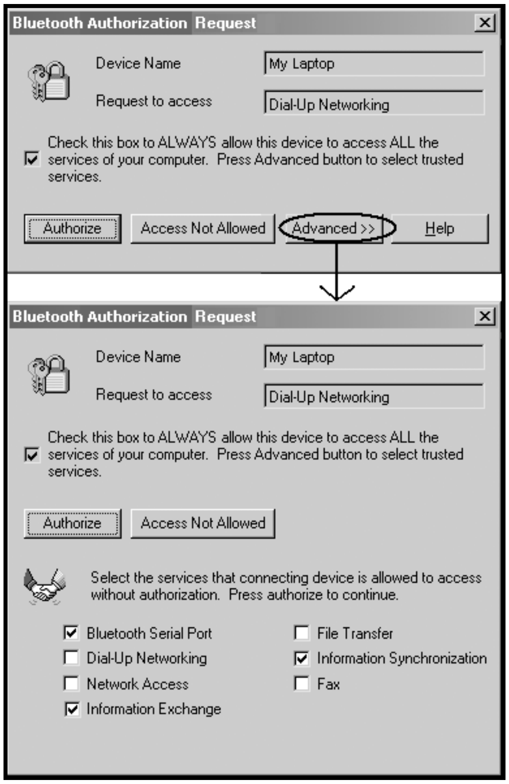
In BTW, when authorization is configured at the service level, an *Authorization Request* dialog box is displayed when a remote device that has been previously authenticated (entered a passkey) tries to connect to a local service for which it has not been previously authorized to use.

The *Authorization Request* dialog box may be responded to in a variety of ways:

> ***NOTE: A response is determined by how the options are set and which action is chosen. In general the responses are:***

- Give a remote device ongoing authorization to use all services on your computer (similar to pairing devices, but done when a connection is being made instead of ahead of time).
- Give a remote device ongoing authorization to use only selected services on your computer.
- During future connections, remove services a remote device was previously authorized to use. This can only be done when a remote device requests to use a service it was not previously authorized to use.
- Deny the remote device's request to connect.

Figure 12: Security > Authorization Request dialog box (composite).



Bluetooth Authorization Request

Device Name: My Laptop

Request to access: Dial-Up Networking

☑ Check this box to ALWAYS allow this device to access ALL the services of your computer. Press Advanced button to select trusted services.

Bluetooth Authorization Request

Device Name: My Laptop

Request to access: Dial-Up Networking

☑ Check this box to ALWAYS allow this device to access ALL the services of your computer. Press Advanced button to select trusted services.

Select the services that connecting device is allowed to access without authorization. Press authorize to continue.

☑ Bluetooth Serial Port
☐ Dial-Up Networking
☐ Network Access
☑ Information Exchange
☐ File Transfer
☑ Information Synchronization
☐ Fax

3.3.2.1 Authorize Requested Service Only

To authorize a remote device to use the local service it has requested, that is, the service name that appears in the *Request to access* field (Figure 12):

1. On the *Bluetooth Authorization Request* dialog box, ensure the box labeled **Check this box to ALWAYS allow this device to access ALL the services of your computer. Press Advanced button to select trusted services** is unchecked.
2. Press the **Authorize** button. The dialog box will close.

3.3.2.2 Authorize Selected Services

To authorize a remote device to use the local service it has requested, that is, the service name that appears in the *Request to access* field (Figure 12) and other selected services:

1. On the *Bluetooth Authorization Request* dialog box, ensure the box labeled **Check this box to ALWAYS allow this device to access ALL the services of your computer. Press Advanced button to select trusted services** is checked.
2. Press the **Advanced>>** button to expand the *Passkey Request* dialog box.
3. All the boxes to the left of each service name will be checked. Leave the boxes checked for the services the remote device is authorized to use. Clear the boxes of the services the remote device is not authorized to use.
4. Press the **Authorize** button. The dialog box will close.

3.3.2.3 Authorize All Services

To authorize a remote device to use the local service it has requested, that is, the service name that appears in the *Request to access* field (Figure 12) and all other services on your computer:

1. On the *Bluetooth Authorization Request* dialog box, ensure the box labeled **Check this box ALWAYS to allow this device to access ALL the services of your computer. Press Advanced button to select trusted services** is checked.
2. If the check box is checked but also "grayed out," press the **Advanced>>** button to expand the *Passkey Request* dialog box and check any unchecked box next to the service names.
3. Press the **Authorize** button. The dialog box will close.

3.3.2.4 Deny Authorization Request

To deny a remote device's access to a local service on your computer:

1. When the security notification is received, click the BTTray icon to display the *Bluetooth Authorization Request* dialog box in its collapsed form.
2. Click the dialog box's **Access Not Allowed** button. The remote device will not be allowed to access the specified service on your computer. The dialog box will close.

If a security notification is ignored it will expire after a preset timeout period. This also will cause the access request to fail.