BlueSoleil User Guides

This chapter describes how to use the menu, toolbar, shortcuts of BlueSoleil. It includes:

- BlueSoleil Environment
- *Bluetooth* Connection Management
- Configurations
- *Bluetooth* Security

For details on how to use *Bluetooth* profiles in BlueSoleil , please refer to Getting Started with BlueSoleil .

See Also

Getting Started with BlueSoleil

BlueSoleil Environment

The BlueSoleil Graphical User Interface includes:

- Main Window
- Service Window
- Menus

See Also

Bluetooth Connection Management Device Configurations

Main Window

Main Window displays the local device (red ball) and the remote devices detected in range. Connecting and disconnecting operations are conducted here. Connections are indicated in lines between the local device and connected remote devices.

By default BlueSoleil starts with the Main Window open. To return to the Main Windows after switching views, click **View | Main Window**.

The following elements are included:

- Local *Bluetooth* Device
- Remote *Bluetooth* Devices
- *Bluetooth* Service Buttons of Remote Device

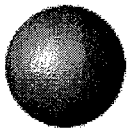
See Also

Local *Bluetooth* Device Remote *Bluetooth* Devices *Bluetooth* Service Buttons of Remote Device

Local *Bluetooth* Device

The Local *Bluetooth* enabled device, known as "**My Device**", represents the user's computer that is running BlueSoleil.

Icon:



Operations:

- Hover mouse to display the local *Bluetooth* device's name or address (if without name).
- Click on the red ball to start or stop searching for *Bluetooth* devices in range.
- Right-click on the red ball to display a pop-up menu of related operations (e.g., General Inquiry, My Services, Security, etc.).

See Also

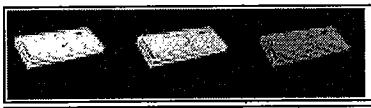
Main Window Remote *Bluetooth* Devices *Bluetooth* Service Buttons of Remote Device

Remote *Bluetooth* Devices

Remote devices are other *Bluetooth* enabled devices that are in the *Bluetooth* radio range of your local device. BlueSoleil uses different icons to indicated different types of remtoe devices..

Icons

Devices	Icon	Devices	Icon
Personal Computer		Laptop	
Modem		Mobile	
PDA		LAN Access Point	

Keyboard		Mouse	
Microphone		HiFi Audio	
Loud Speaker		Headset	
Printer		Scanner	
FAX		Camera	
Game bar		Server	
Unknown device			

Icon Meanings

Remote devices can be in any of three states, which BlueSoleil indicates with different colors.

- White- Idle. The normal state of the device.
- Yellow- Selected. you have selected the device.
- Green- Connected. The device is connected to your computer.

Operations

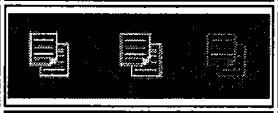
- Single-click on the icon to select.
- Double-click on the icon to search for the services supports by the remote Bluetooth device .
- Right-click on the icon to display a pop-up menu of related operations (e.g. Refresh Devices, Pair Devices, Connect, etc.).

See Also

Main Window Local *Bluetooth* Device *Bluetooth* Service Buttons of Remote Device

Bluetooth Service Buttons of Remote Device

Service buttons at the top of the Main Window represent a range of *Bluetooth* services potentially supported by Remote Devices .

Services	Button Image	**Services**	Button Image
PAN		DUN	
SPP		LAP	
FTP		SYNC	
OPP		HCRP	
HID		FAX	
BIP		AV	
Headset			

Icon Meanings

There are 3 states for the service icons, indicated by different colors.

- White- Idle. The normal state.
- Yellow- Available. The *Bluetooth* service is available on the selected remote device.
- Green- Connected. The *Bluetooth* service is active in a connection with the remote device.

Operations

- Hover your mouse over the service icon to display the name of the service.
- Single-click on the service icon to connect.
- Right-click on the service icon to display a pop-up menu of related operations.

See Also

Main Window Local *Bluetooth* Device Remote *Bluetooth* Devices

Service Window

The service Window displays the local *Bluetooth* services, (i.e., the *Bluetooth* services supported by BlueSoleil). Use the Service Window to start and stop services, as well as to configure service properties. To access the Service Window, click **View | Service Window**.

Following element is included:

- Local Service List
- Service Status

See Also

Main Window Menus

Local Device Status

The local device status can be viewed from the **Local Device Status** dialog box.

Right click whichever local service icon in service window and select the **Status**... on the pop-up menu.

The **Local Device Status** dialog will be displayed.

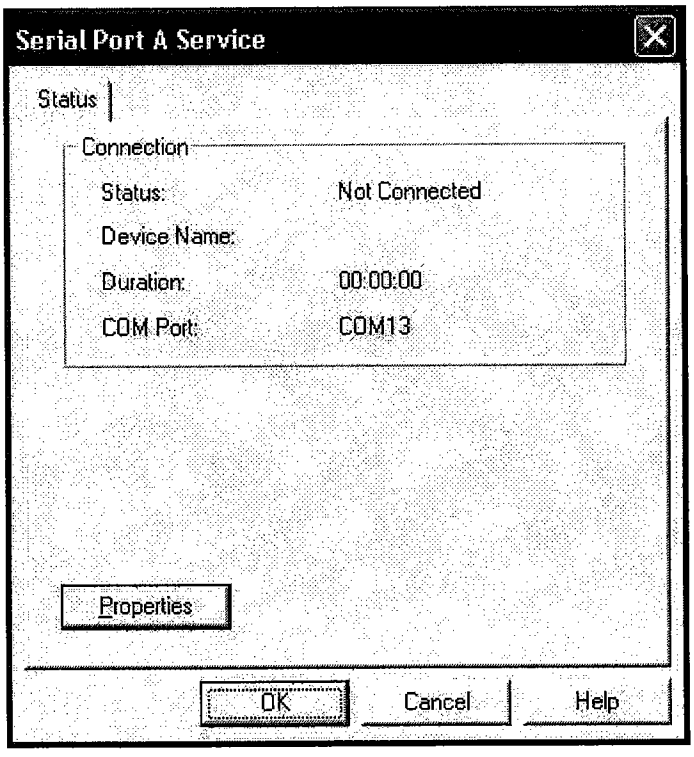


Figure1: Local Service Status (e.g. Serial Port A service)

Connection:

Status: Whether the local service is connected.

Device Address: Display the *Bluetooth* address of remote device which connect to the service.

Duration: The time elapsed since the connection was set up.

COM Port: The virtual *Bluetooth* COM ports connected by remote device.

PAN Service Status dialog has some difference among others.

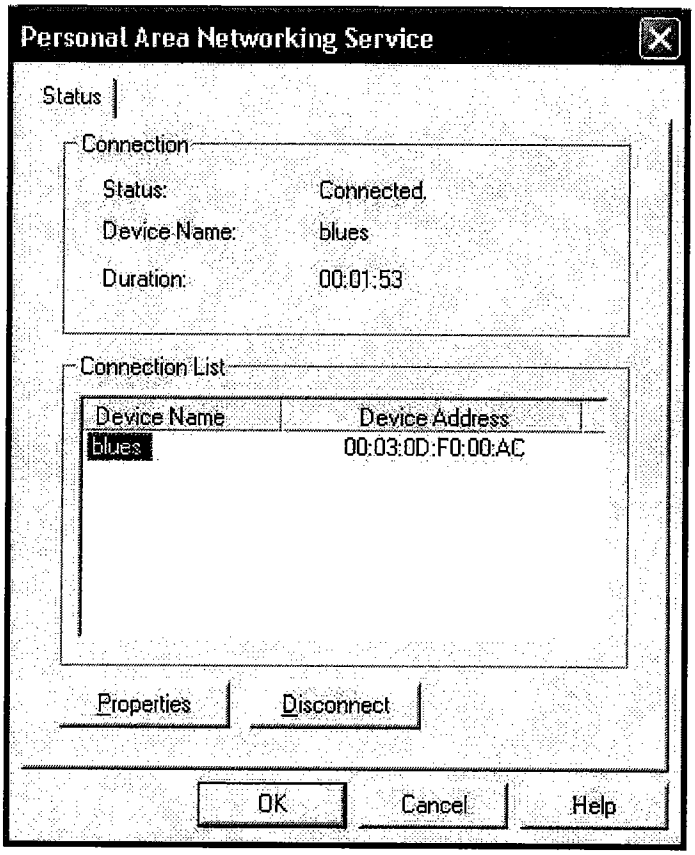


Figure2: Local Service Status (PAN)

Connection:

Status: Whether the local service is connected.

Device Address: Display the *Bluetooth* address of remote device which connect to the service.

Duration: The time elapsed since the connection was set up.

Connection List:

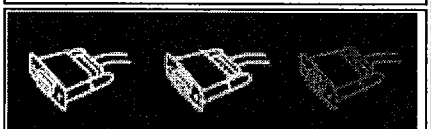
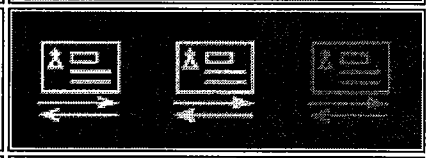
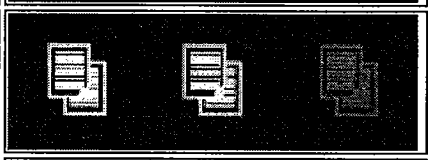
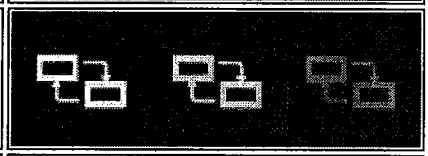
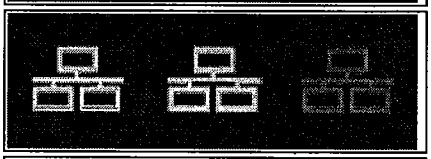
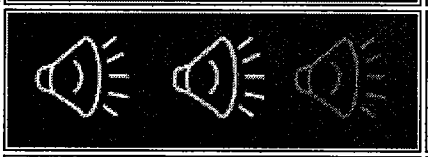
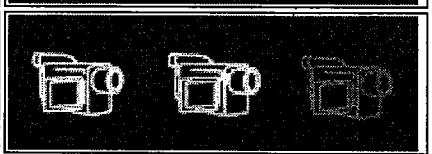
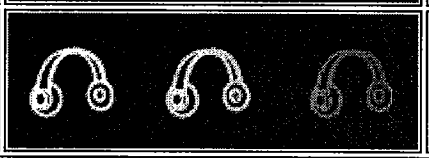
Display the names and addresses of remote devices which connect to the local service.

See Also

Service Window

Local Service List

The Local Service List displays all the *Bluetooth* services supported by the local computer. Use this screen to start/stop services.

Services	Icons	Services	Icons
PAN		SPP	
OPP		FTP	
SYNC		LAP	
A2DP		BIP	
Headset AG			

Icon Meanings

There are 3 states for the local *Bluetooth* services, indicated by different icon colors.

- White- Idle. The service has not been started.
- Pink- Started. The local *Bluetooth* service has been started.
- Green- Connected. Some remote device has connected to the service.

Operations

- Single-click on the icon to select the service.
- Double-click on the icon to Start/Stop a service.
- Right-click to display a pop-up menu of related operation .

See Also

Service Window

Menus

BlueSoleil contains the following six menus:

- File Menu
- View Menu
- My *Bluetooth* Menu
- My Services Menu
- Tools Menu
- Help Menu

File Menu

- **Hide** --- Hide the BlueSoleil window. Connections can still run when the window is hidden.
- **Always on Top** --- Keep BlueSoleil window always on top.
- **Exit** --- Exit BlueSoleil.

You can also exit BlueSoleil by right-clicking on the task tray icon at the bottom of your screen. In the pop-up menu, click Exit.

View Menu

- **Main Window** --- Show the BlueSoleil Main Window .
- **Service Window** --- Show the BlueSoleil Service Window.
- **Arrange Devices** --- Arrange all remote devices by Device Name, Device Address or Device Type.
- **Refresh Devices** --- Refresh the list of remote devices detected by BlueSoleil.

Figure 6 Unplug HID Device

- ***Bluetooth* Device** --- Advanced hardware configuration, recommended for advanced users only. Please refer to 4.2 Hardware Configuration for more details.

Help Menu

- **Contents and Index** --- Access BlueSoleil Online Help.
- **About BlueSoleil** --- Information about your version of BlueSoleil.

See Also

Main Window Service Window

Bluetooth Connection Management

Bluetooth Connection Management includes:

- Find Remote Devices
- Connect and Disconnect
- Connect via Shortcut
- Status
- Properties

See Also

BlueSoleil Environment Device Configurations

Find Remote Devices

To set up a *Bluetooth* connection, the remote device must be found first. There are 3 ways to find remote devices in BlueSoleil.

Inquire Device

1. Single-click the red ball in the main window to start inquiry.
2. *Bluetooth* devices within the radio range will be shown around the center ball.
3. Wait for a few seconds until the names of all the devices are obtained.

Add Device from History List

The devices which had been found or connected can be added from the history device list directly.

1. Select menu **Tools | Add Device from History**.... The **History** dialog box pops up.
2. Select the device from the list and click button **Add**, the device will be added to the main window.

Add a New Device by Entering Device Address

If the device cannot be found by **Inquiring**, you can enter the device address to add the device.

1. Select menu **Tools | Add New Device**.... The **Add *Bluetooth* Neighbor Device Manually** dialog box pops up.
2. Enter the *Bluetooth* device address and click button **OK**, the device will be added to the main window.

Note: *The device type will be unknown if add it by inputting its Bluetooth address.*

See Also

Connection Management Connect and Disconnect Connect Via Shortcut
Status Properties

Connect and Disconnect

Connect

1. Select a remote device and double click it to browse its services.
   Bluetooth passkey may be asked if security level of either side is set to high and they are not paired devices.
   After service browsing, the services the remote device supports are highlighted by changing the color of the service buttons on the top of the main window.
2. Single click one of the service button to connect.
   After connection is setup, the remote device and the service button will turn green.

Note: *Users can right click the remote device icon or the service button to pop up operation menu for connection.*

Disconnect

Method 1: Select the remote device, right click the service button. On the popup menu, select **Disconnect**.
Method 2: Right click the device icon. On the pop-up menu, select **Disconnect | (the connection you want to disconnect)**.
Method 3: For FTP and Synchronization connection, close the operation window, the connection will be disconnected.
Method 4: Disconnect from the remote device directly.
Method 5: If the local *Bluetooth* device is removed or the remote device is closed, all the connections will be disconnected. If the remote device moves out of the radio range, all the

connections with the remote device will be disconnected in 1 minute.

See Also

Connection Management Properties | Find Remote Device | Connect Via Shortcut | Status

Connect via Shortcut

After a connection is set up, users can generate a shortcut on Windows desktop. Users can connect later using the shortcut without device inquiry and service browsing steps.

Shortcuts applies to Personal Area Networking, Dial-Up network, FTP and AV.

Steps

1. Save shortcut
   After connected, right click the device icon, select the **Save Connection as Shortcut** on the popup menu.
2. Execute the shortcut on desktop.

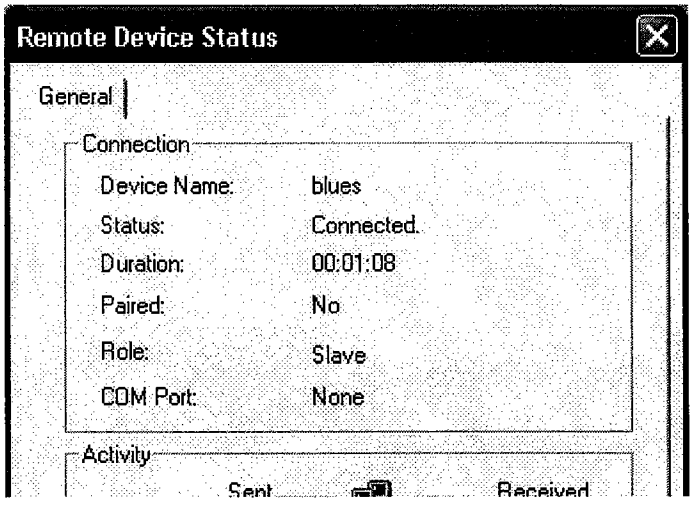
See Also

Connection Management | Find Remote Device | Connect and Disconnect | Status Properties

Remote Device Status

The remote device status can be viewed from the **Remote Device Status** dialog box.

Right click the remote device icon and select the **Status...** on the popup menu. The **Remote Device Status** dialog box will be displayed.



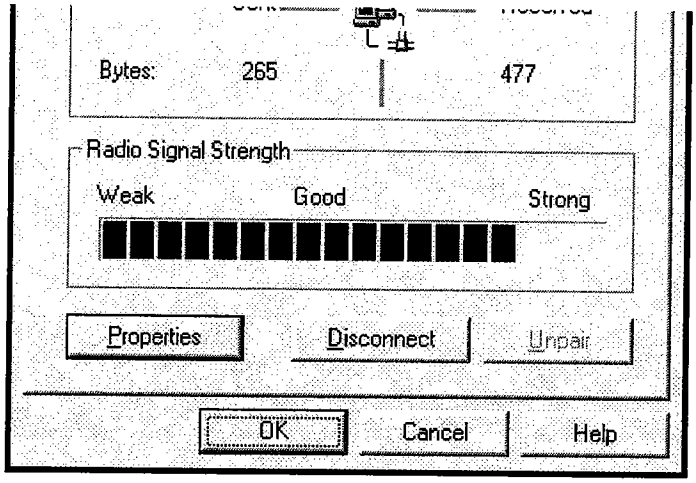


Figure 1 Remote Device Status

- Connection:
  Device Name: The remote *Bluetooth* device's name.
  Status: Whether the remote device is connected to the local device.
  Duration: The time elapsed since the connection was set up.
  Paired: Whether this device is paired with the local device.
  Role: The *Bluetooth* Master/Slave role of the remote device for this connection.
  COM Port: The virtual *Bluetooth* COM ports used for the connection(s), especially for DUN, FAX, SPP, and LAP.
- Activity:
  The amount of the data sent and received.
- Radio Signal Strength:
  This is the RSSI of the remote device. This index indicates the radio quality between the remote device and the local device. If the radio signal is too weak, the data transferring speed will be slow.
- Properties Button:
  Display the remote device's properties.
- Disconnect Button:
  Disconnect one of the connection(s) between the remote device and the local device.
- Unpair Button:
  Remove the paired relationship between the remote device and the local device.

See Also

Connection Management Find Remote Device Connect and Disconnect Connect Via Shortcut Properties

Remote Device Properties

The remote device's properties can be viewed from the **Remote Device Property** dialog box.

Right click the remote device icon and select the **Properties...** on the popup menu. The **Remote Device Property** dialog will be displayed.

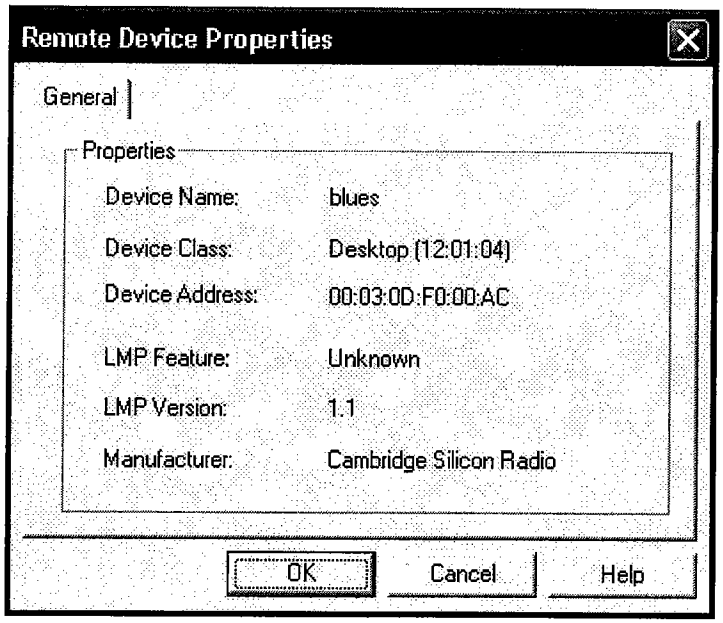


Figure 1 Remote Device Property Dialog

Device Name: The remote *Bluetooth* device's name.
Device Class: The remote device's device class. *Bluetooth* devices are classified by device type, such as Desktop, Laptop, Headset, LAN Access Point, and other enabled devices.
Device Address: The remote device's *Bluetooth* device address.
LMP Feature: The features that the remote device supports.
LMP Version: The version of the LMP firmware of the remote device.
Manufacturer: The manufacturer of the remote device.

See Also

Connection Management Find Remote Device Connect and Disconnect Connect Via Shortcut Status

Device Configurations

The local device configurations include:

- Local Device Hardware Configuration
- Local Device Properties Configuration

See Also

BlueSoleil Environment *Bluetooth* Connection Management

Hardware Configuration

BlueSoleil supports the following kinds of *Bluetooth* radio adapters: USB, CompactFlash card (UART or BCSP).

To access the hardware configuration screens, click **Tools | *Bluetooth* Device...**,

- ***Bluetooth* Device**
  Select the type of *Bluetooth* enabled device that you plan to use, either a USB adapter or a CompactFlash (CF) card. (Figure 1).

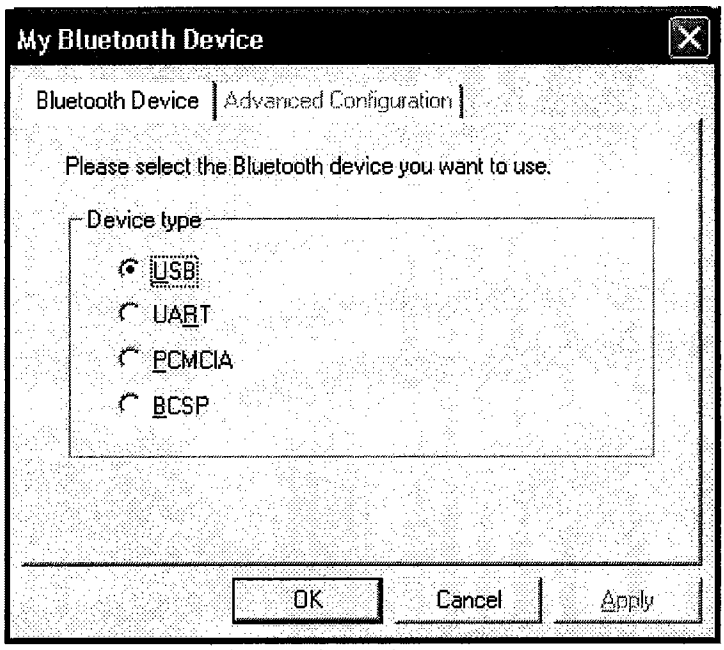
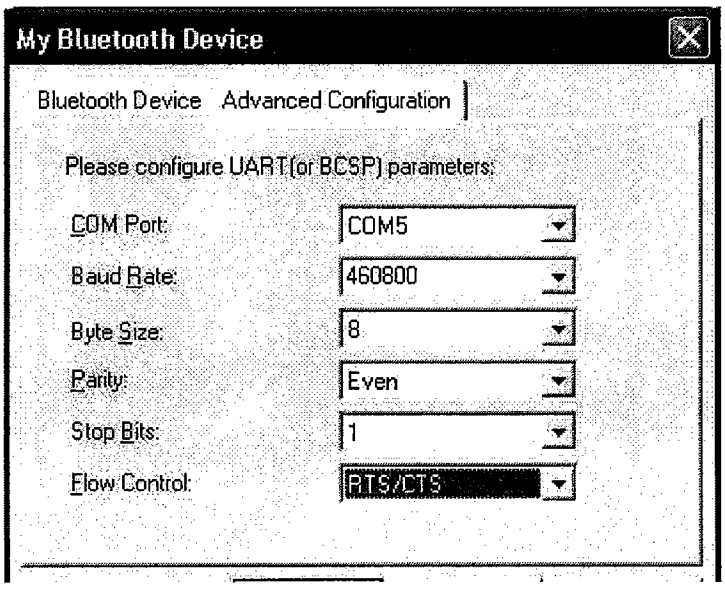


Figure 1 Select *Bluetooth* Device

- **Advanced Configuration**
  The **Advanced Configuration** page will be enabled only if you selected CF in the *Bluetooth* Device screen. Use the *Advanced Configuration* screen to configure detailed parameters including COM Port, Baud Rate, Byte Size, Parity, Stop Bits, and Flow Control.



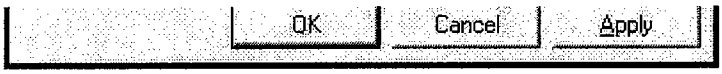


Figure 2 Advanced Configurations For UART Hardware Device

See Also

Properties Configuration

Properties Configuration

To configure the properties of your local device, click **My *Bluetooth* | Properties...**,

General

- Device Name
  The local device's name, which will be shown to other *Bluetooth* enabled devices.
- Device Type
  The device's type of your local computer (i.e., Desktop, Laptop or Server).
- Device Address
  The address of the local device. Every *Bluetooth* enabled device has a unique device.

Figure 1 General Properties Page

Accessibility

Connect Property

- Connectable: Permits other *Bluetooth* enabled devices to connect with your computer.

- Non-Connectable: Prohibits other *Bluetooth* enabled devices from connecting with your computer.

Discovery Mode

- General Discoverable: Permits other *Bluetooth* enabled devices to detect your computer.
- Limited Discoverable: Permits other *Bluetooth* enabled devices to detect your computer with Limited Inquiry.
- Non-Discoverable: Permits other *Bluetooth* enabled devices to detect your computer with Limited Inquiry. Prohibits other *Bluetooth* enabled devices from detecting your computer.

Bonding Mode (Pairing Mode)

- Accepts Bonding: Allow other *Bluetooth* enabled devices to pair with your computer. If the other device initiates a pairing procedure with your computer, each device must enter the same passkey before the they will be paired.
- Does Not Accept Bonding: Rejects pairing attempts initiated by other *Bluetooth* enabled devices.

Figure 2 Accessibility Properties Page

Hardware

View information about your *Bluetooth* hardware.

- Manufacturer: The manufacturer of the local *Bluetooth* device.
- HCI Version: The HCI version of the local *Bluetooth* device.
- HCI Edition: The HCI edition of the local *Bluetooth* device.
- LMP Version: The LMP version of the local *Bluetooth* device.
- LMP Subversion: The LMP subversion of the local *Bluetooth* device.

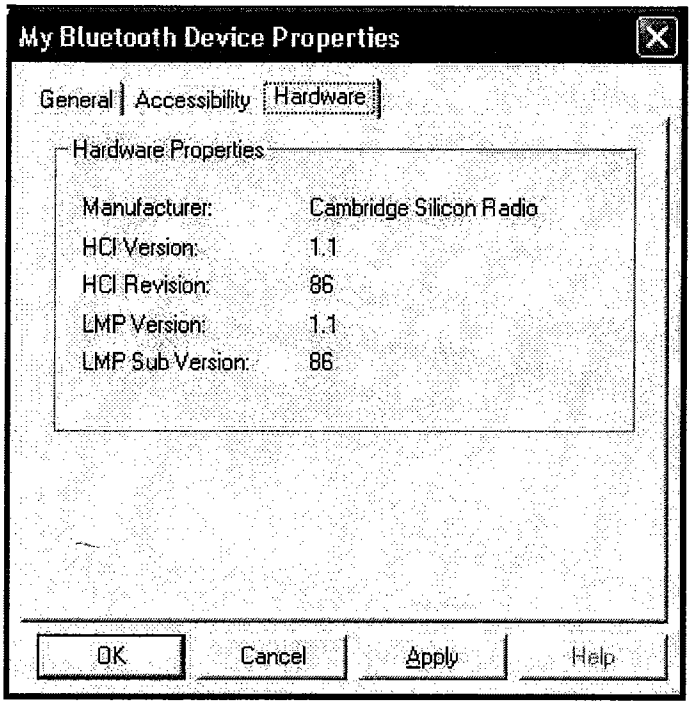


Figure 3 Hardware Properties Page

See Also

Hardware Configuration

Security Configuration

Use the Security Configuration screens to specify the security settings of your local device, it includes:

- General Security
- Pairing Devices Management
- Local Services Security

See Also

Bluetooth Security Conceptions

Pair / Un-pair Devices

Once a remote device has paired with your computer by exchanging passkeys, passkeys will no

longer be required for further connections between your computer and the device.

How to pair with another device

- **Automatically**
  If a passkey is required for connection, the devices will be paired automatically the first time they successfully exchange passkeys and connect. After a device has successfully paired with your computer, the remote device icon in the Main Window will have a red checkmark next to it.
- **Manually**
  In the Main Window, right click on the device icon, and in the pop-up menu, select Pair Device. In the Enter *Bluetooth* Passkey screen, enter the same passkey that you enter on the remote device. After a device has successfully paired with your computer, the remote device icon will have a red checkmark next to it.

How to un-pair with another device

- **Manually**
  In the Main Window, right-click on the device icon, and in the pop-up menu, select Unpair. The red checkmark next to the device icon will disappear.

See Also

Pairing Devices Management

General Security

To access the security configuration screen, click **My *Bluetooth* | Security...**

Security Level

- **Low**
  If checked, other devices will be able to access your device freely without entering a passkey.
  However, if the remote device requires a passkey to connect, then both devices need to exchange passkeys.
- **Medium**
  The medium level is service level security, you can assign the appropriate level of access for each specific service. For more detail, see Local Services Security.
- **High**
  If checked, passkeys must be exchanged for every incoming and outgoing connection, unless the two devices have already paired in the past.

Bluetooth Passkey

- **Set Default Passkey**

Use this setting to create a default passkey for all connections. This saves you the effort of manually creating a passkey whenever one is required.

Data Encryption

- **Enable Data Encryption**
  If checked, the data transmitted will be encrypted.

See Also

Pairing Devices Management Local Services Security

Pairing Devices Management

To access the device security configuration screen, click **My *Bluetooth* | Security** and click on the Devices tab.

Paired Devices List Box

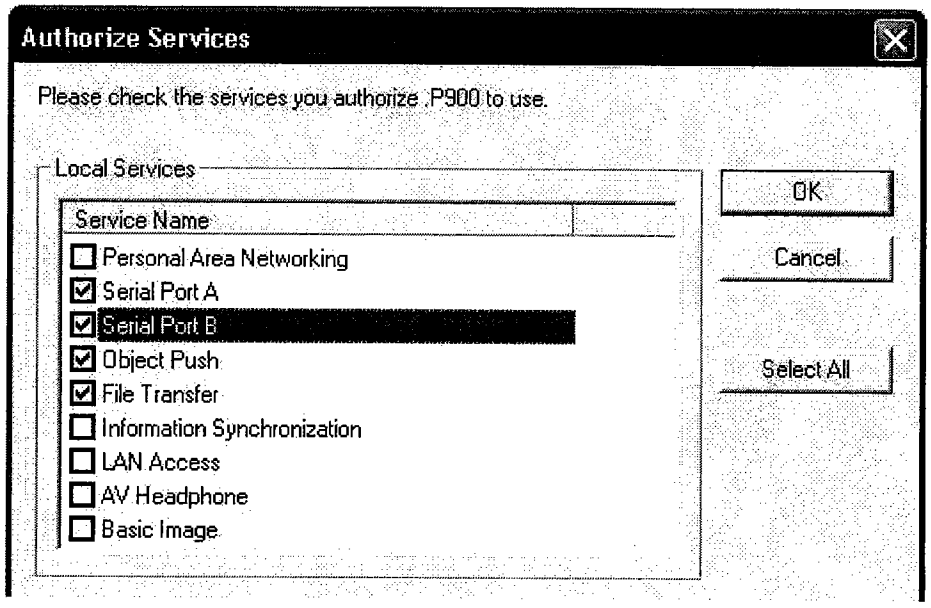
This screen lists devices which have already paired with the local device.

Remove Pairing Button

Click to remove the pairing relationship between the selected device and the local device.

Authorization Button

Click to select the local *Bluetooth* services that you wish to allow the selected paired device to use. A list of local services will appear. Select the services you wish to allow on the remote device, then click OK.



Only the local services that require authentication will be listed. The local services that do not require authentication can be accessed freely.

***Note**:*

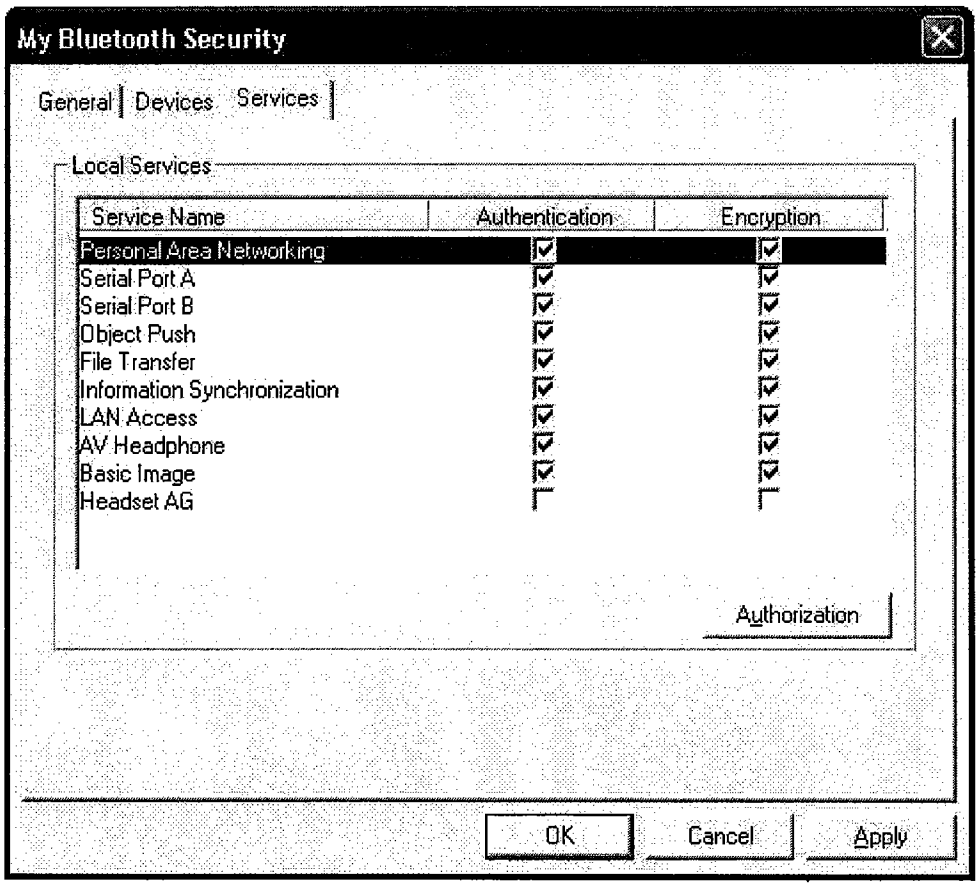
- *The screen will only list the local services that require authentication. The local services that do not require authentication can be accessed freely.*
- *The Authorization button is enabled only when the Security Level is set to Medium.*

See Also

Pair/Un-pair Devices General Security Local Services Security

Local Services Security

To access the local services security configuration screen, click **My *Bluetooth* | Security** and click on the Services tab. You can only configure security for local services when the Security Level is set to Medium. (Set the Security Level in the General Security.)



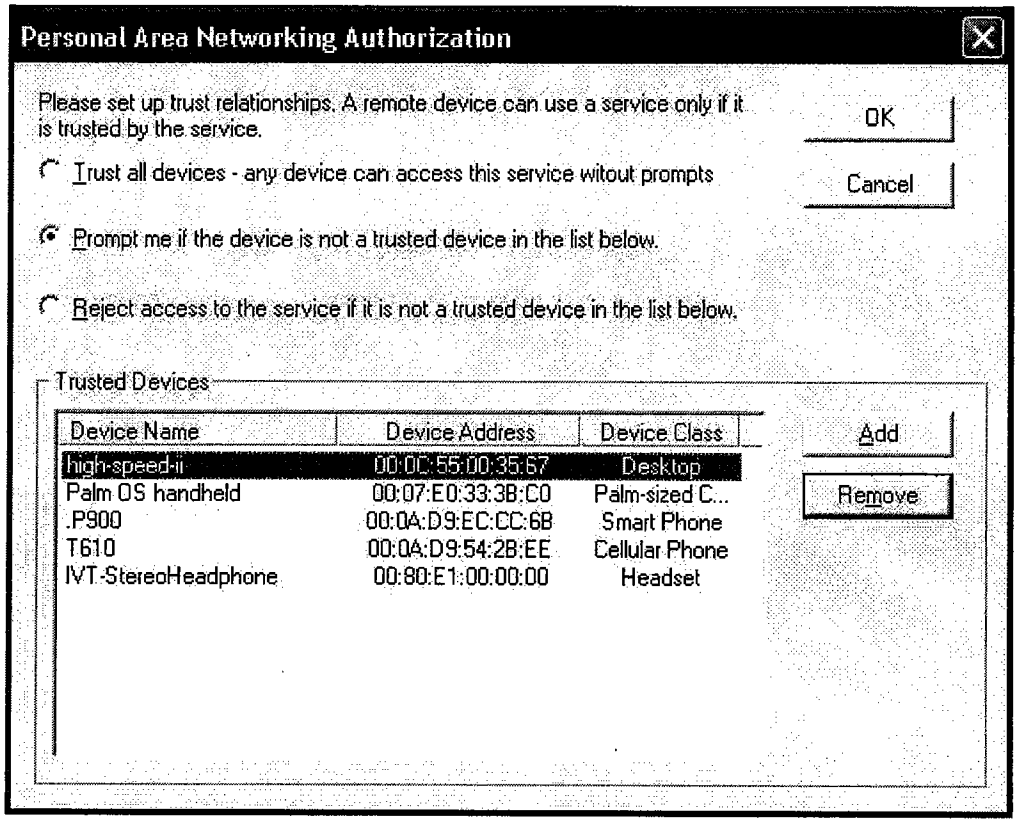
Local Services:

- **Authentication**

If checked, a passkey is required whenever a remote device attempts to connect with this service.

- **Encryption**
  If checked, data transmitted between devices for this service will be encrypted.

Authorization Button:
Click to select the devices you wish to allow to use the selected service.



In the **Service Authorization** screen, enter the following settings:

- **Trusted Devices**
  Select to trust devices listed in this screen to use the selected service on your device. A device can freely access the service from your local device when trusted. Click **Add/Remove** to edit the device list.
- **Trust all devices**
  Connection requests will be accepted from every device.
- **Prompt to user if the device is not a trusted device of this service**
  If a non-trusted device attempts to access the service, a dialog will appear to allow you to accept or reject the connection.
- **Reject the device to use the service if it is not a trusted device of this service**
  If a non-trusted device attempts to access the service, the connection will be rejected automatically without informing the user.

Notes: *If a device is trusted for a service, it may connect to this service on your local device without informing you.*

See Also

General Security Pairing Devices Management

Properties Configuration

To configure the properties of your local device, click **My *Bluetooth* | Properties...,**

General

- Device Name
  The local device's name, which will be shown to other *Bluetooth* enabled devices.
- Device Type
  The device's type of your local computer (i.e., Desktop, Laptop or Server).
- Device Address
  The address of the local device. Every *Bluetooth* enabled device has a unique device.

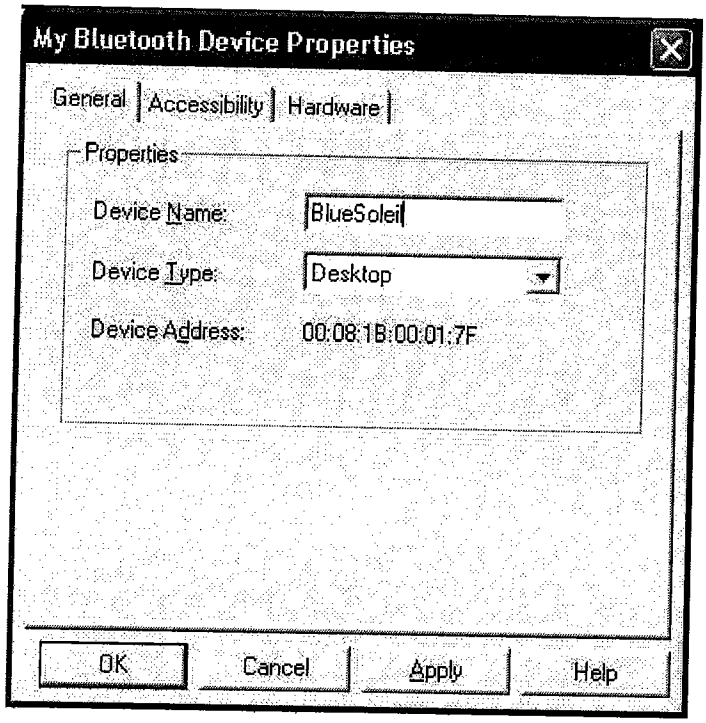


Figure 1 General Properties Page

Accessibility

Connect Property

- Connectable: Permits other *Bluetooth* enabled devices to connect with your computer.
- Non-Connectable: Prohibits other *Bluetooth* enabled devices from connecting with your computer.

Discovery Mode

- General Discoverable: Permits other *Bluetooth* enabled devices to detect your computer.
- Limited Discoverable: Permits other *Bluetooth* enabled devices to detect your computer with Limited Inquiry.
- Non-Discoverable: Permits other *Bluetooth* enabled devices to detect your computer with Limited Inquiry. Prohibits other *Bluetooth* enabled devices from detecting your computer.

Bonding Mode (Pairing Mode)

- Accepts Bonding: Allow other *Bluetooth* enabled devices to pair with your computer. If the other device initiates a pairing procedure with your computer, each device must enter the same passkey before the they will be paired.
- Does Not Accept Bonding: Rejects pairing attempts initiated by other *Bluetooth* enabled devices.

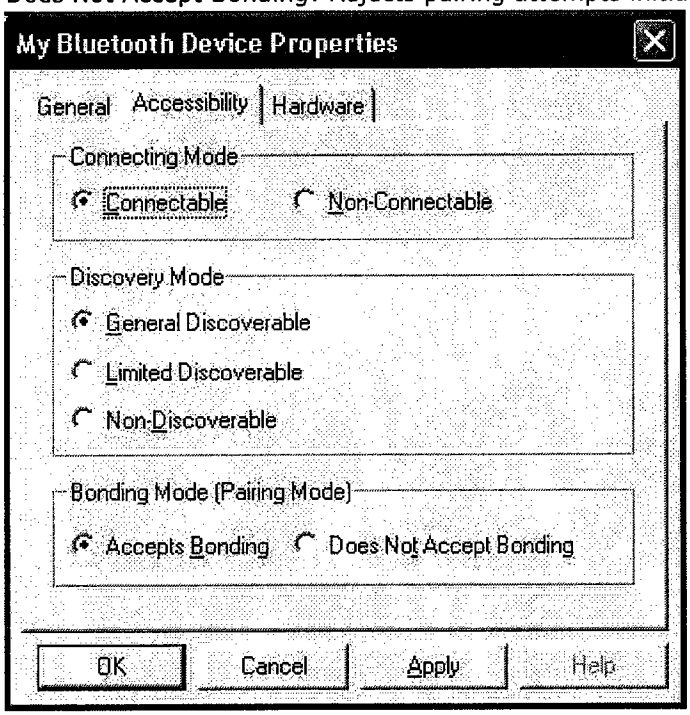
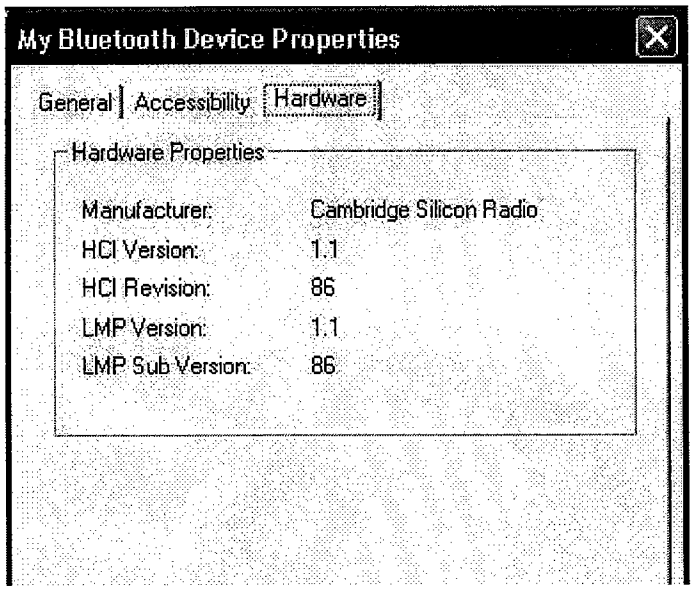


Figure 2 Accessibility Properties Page

Hardware

View information about your *Bluetooth* hardware.

- Manufacturer: The manufacturer of the local *Bluetooth* device.
- HCI Version: The HCI version of the local *Bluetooth* device.
- HCI Edition: The HCI edition of the local *Bluetooth* device.
- LMP Version: The LMP version of the local *Bluetooth* device.
- LMP Subversion: The LMP subversion of the local *Bluetooth* device.



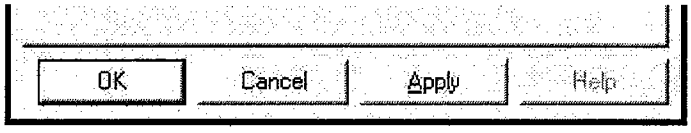


Figure 3 Hardware Properties Page

See Also

Hardware Configuration

Security Configuration

Use the Security Configuration screens to specify the security settings of your local device, it includes:

- General Security
- Pairing Devices Management
- Local Services Security

See Also

Bluetooth Security Conceptions

Pair / Un-pair Devices

Once a remote device has paired with your computer by exchanging passkeys, passkeys will no longer be required for further connections between your computer and the device.

How to pair with another device

- **Automatically**
  If a passkey is required for connection, the devices will be paired automatically the first time they successfully exchange passkeys and connect. After a device has successfully paired with your computer, the remote device icon in the Main Window will have a red checkmark next to it.
- **Manually**
  In the Main Window, right click on the device icon, and in the pop-up menu, select Pair Device. In the Enter *Bluetooth* Passkey screen, enter the same passkey that you enter on the remote device. After a device has successfully paired with your computer, the remote device icon will have a red checkmark next to it.

How to un-pair with another device

- **Manually**
  In the Main Window, right-click on the device icon, and in the pop-up menu, select Unpair. The red checkmark next to the device icon will disappear.

See Also

Pairing Devices Management

General Security

To access the security configuration screen, click **My *Bluetooth* | Security...**

Security Level

- **Low**
  If checked, other devices will be able to access your device freely without entering a passkey.
  However, if the remote device requires a passkey to connect, then both devices need to exchange passkeys.
- **Medium**
  The medium level is service level security, you can assign the appropriate level of access for each specific service. For more detail, see Local Services Security.
- **High**
  If checked, passkeys must be exchanged for every incoming and outgoing connection, unless the two devices have already paired in the past.

Bluetooth Passkey

- **Set Default Passkey**
  Use this setting to create a default passkey for all connections. This saves you the effort of manually creating a passkey whenever one is required.

Data Encryption

- **Enable Data Encryption**
  If checked, the data transmitted will be encrypted.

See Also

Pairing Devices Management Local Services Security

Pairing Devices Management

To access the device security configuration screen, click **My *Bluetooth* | Security** and click on the Devices tab.

Paired Devices List Box

This screen lists devices which have already paired with the local device.

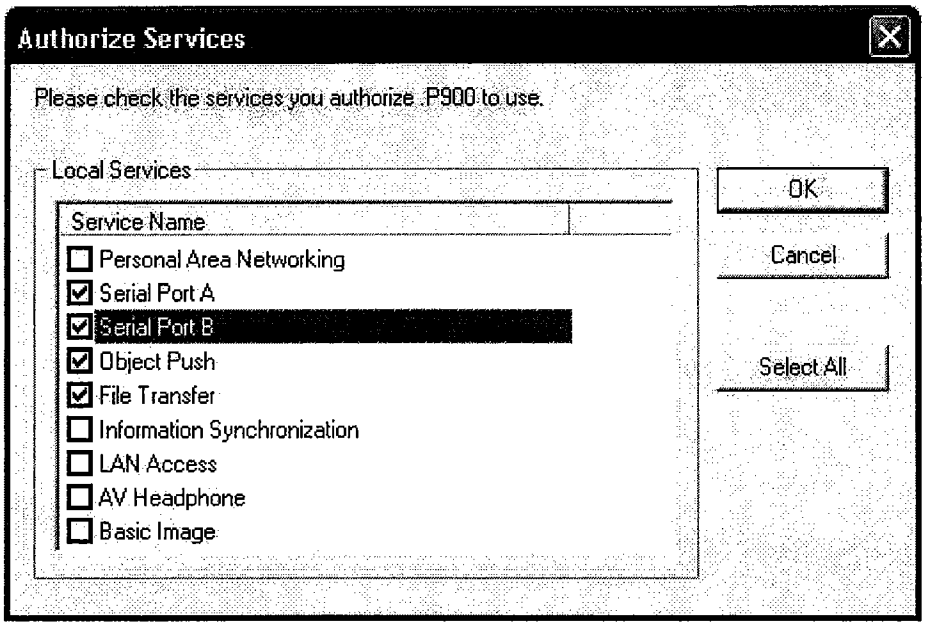
Remove Pairing Button

Click to remove the pairing relationship between the selected device and the local

device.

Authorization Button

Click to select the local *Bluetooth* services that you wish to allow the selected paired device to use. A list of local services will appear. Select the services you wish to allow on the remote device, then click OK.



Only the local services that require authentication will be listed. The local services that do not require authentication can be accessed freely.

Note:

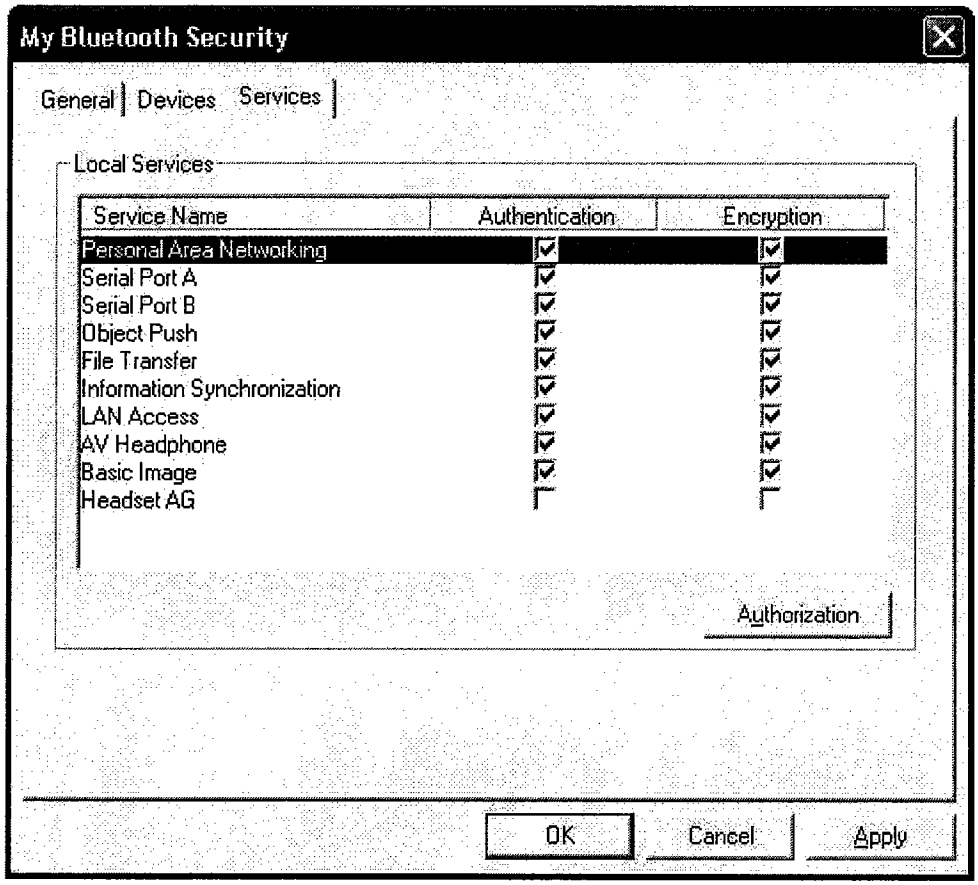
- *The screen will only list the local services that require authentication. The local services that do not require authentication can be accessed freely.*
- *The Authorization button is enabled only when the Security Level is set to Medium.*

See Also

Pair/Un-pair Devices General Security Local Services Security

Local Services Security

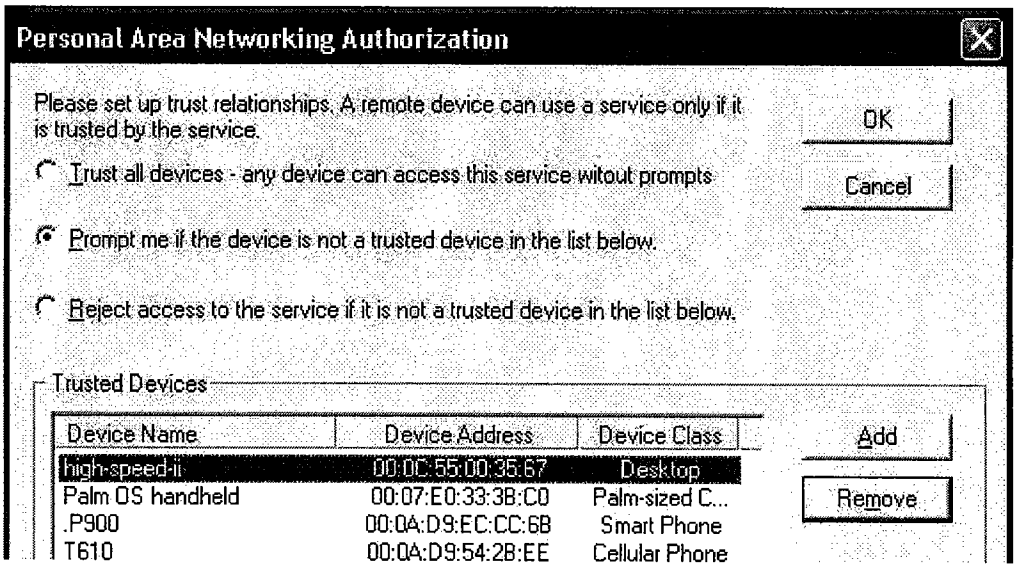
To access the local services security configuration screen, click **My *Bluetooth* | Security** and click on the Services tab. You can only configure security for local services when the Security Level is set to Medium. (Set the Security Level in the General Security.)

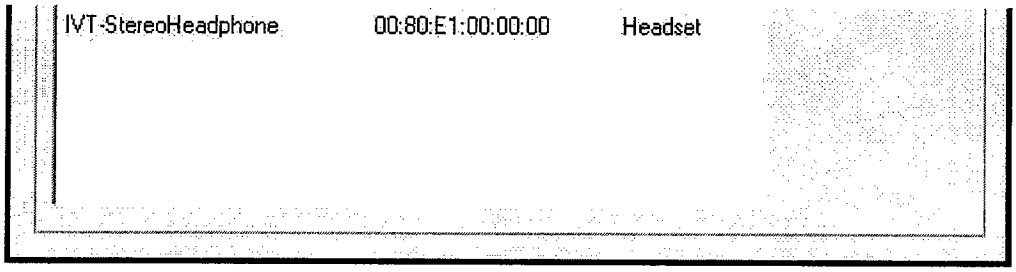


Local Services:

- **Authentication**
  If checked, a passkey is required whenever a remote device attempts to connect with this service.
- **Encryption**
  If checked, data transmitted between devices for this service will be encrypted.

Authorization Button:
Click to select the devices you wish to allow to use the selected service.





In the **Service Authorization** screen, enter the following settings:

- **Trusted Devices**
  Select to trust devices listed in this screen to use the selected service on your device. A device can freely access the service from your local device when trusted. Click **Add/Remove** to edit the device list.
- **Trust all devices**
  Connection requests will be accepted from every device.
- **Prompt to user if the device is not a trusted device of this service**
  If a non-trusted device attempts to access the service, a dialog will appear to allow you to accept or reject the connection.
- **Reject the device to use the service if it is not a trusted device of this service**
  If a non-trusted device attempts to access the service, the connection will be rejected automatically without informing the user.

Notes: *If a device is trusted for a service, it may connect to this service on your local device without informing you.*

See Also

General Security Pairing Devices Management

Troubleshooting

Cannot start My *Bluetooth*?

When the program starts, the local device address is 00:00:00:00:00:00. Please check whether you have properly plug-in your *Bluetooth* USB dongle or *Bluetooth* CF card and whether the device is powered up. *Bluetooth* USB dongles can be detected automatically if they are in the IVT known device list (If you are using a device of a new model, please contact IVT so that the model can be added to list). Some *Bluetooth* CF card device cannot be detected automatically. Users need to configure the parameters in the menu **Tools | *Bluetooth* Device...** to enable the device.

How can I find my *Bluetooth* device information?

On the center ball, my device, right click and select **Properties...** on the popup menu. In the **My *Bluetooth* Device** dialog box, there are device names, device addresses, device manufacturers, device HCI and LMP (Link Manager Protocol) versions and editions.

Can't find the remote device you want?

First, please check whether the remote device is in discoverable mode. If the remote device is set to non-discoverable, other devices cannot find it. Second, please check whether the remote device is within the radio range. *Bluetooth* devices have 3 classes. Class 1 devices are high power devices. Their transmission range are 50 to 100 meters. Class 2 and class 3 devices are low power devices. Their transmission range are 10-20 meters. If you still cannot find the remote device, you can (1) find the device from the history list, so that you can add it directly to the orbit. Find the tool from **Tools | Add Device from History...**. (2) If the device is not in the history list, you can also add a new device directly by inputting the remote device address. Find the tool from **Tools | Add New Device...**.

Can't find the remote device services?

First, please verify that whether the remote device is in connectable mode. If the remote device is set to non-connectable, other devices cannot connect to it.

Second, please verify whether the remote device is within the radio range.

Third, please check whether the remote device has connections already. Currently, some *Bluetooth* devices do not support scatter net. That is, the device has limitations in supporting connection among multi-devices at the same time. It is recommended that users try to connect point to point if the connection cannot be set up.

Fourth, please verify whether both sides have input the right *Bluetooth* passkey if any side is at security level High. The *Bluetooth* passkey must be the same at both sides. If both sides have set Fixed Passkey (the default passkey) and the passkeys are different, the connection cannot be set up with the authentication failure error.

Terms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Authentication Authentication is the process of verifying "who" is at the other end of the link. Authentication is performed for devices. In *Bluetooth* this is achieved by the authentication procedure based on the stored link key or by pairing (entering a PIN).

Authorization Authorization is the process of deciding if device X is allowed to access service Y. This is where the concept of "trusted" exists. Trusted devices (authenticated and indicated as "trusted"), are allowed to access services. Mistrusted or unknown devices may require authorization based on user interaction before access to services is granted.

B

Bluetooth *Bluetooth* is an open specification for a cutting-edge technology that enables short-range wireless connections between desktop and laptop computers, personal digital assistants, cellular phones, printers, scanners, digital cameras and even home appliances ?on a globally available band (2.4GHz) for worldwide compatibility. In a nutshell, *Bluetooth* unplugs your digital peripherals and makes cable clutter a thing of the past.

***Bluetooth* Authentication** *Bluetooth* authentication is the procedure to verify whether another *Bluetooth* enabled device has the right to access your computer. During this procedure, a *Bluetooth* passkey is asked for on both connection sides. If the passkeys are the same, the authentication procedure is a success and the connection can be setup. If the passkeys are different, then authentication fails and the connection cannot be setup.

***Bluetooth* Authorization** *Bluetooth* authorization is the procedure to verify whether you are going to allow (authorize) other *Bluetooth* enabled devices to use *Bluetooth* services on your *Bluetooth* enabled devices. This procedure takes function in *Bluetooth* security Mode 2 and applies to your *Bluetooth* services only. Every *Bluetooth* service in your BlueSoleil has the setting of authorization. And there is an authorization devices list for every service, which records the devices that you have authorized. The user can change the authorization status for each device.?nbsp;

***Bluetooth* Connection** *Bluetooth* functions are in the model of Client/Server. One *Bluetooth* device provides services, and another *Bluetooth* device uses these *Bluetooth* services. After connection, a *Bluetooth* link is set up between two devices, and the link is called a *Bluetooth* connection. Users can disconnect the connection after finishing his job on *Bluetooth*.

***Bluetooth* Connection Shortcut** Connection shortcut is used for saving time in searching devices and browsing services. After a connection is established, it can be saved as a shortcut. The shortcut can be used later to re-establish the connection, without searching the remote *Bluetooth* devices and browsing services. After a connection is setup, the connection can be saved as a shortcut, which can be used later without searching *Bluetooth* devices or browsing services. ?nbsp;

***Bluetooth* Device** *Bluetooth* devices are addressed in two ways: (1) When referring to the local device configuration, a *Bluetooth* Device is the local *Bluetooth* hardware which can be a USB dongles, a UART device, a PCMCIA card or a BCSP device. The user is expected to select the interface of his *Bluetooth* device in his configuration. (2) When referring to the *Bluetooth* application, it is the *Bluetooth* system as a whole, e.g. a *Bluetooth* modem, *Bluetooth* mobiles or a *Bluetooth* PDA etc. My PC together with the BlueSoleil and the *Bluetooth* dongle would also be addressed as a remote *Bluetooth* device by other *Bluetooth* devices.

***Bluetooth* Device Address** A unique 48-bit address that distinguishes between different *Bluetooth* transceivers. Every *Bluetooth* device has a unique address so that other devices can find it and communicate with it. The address appears in the form of 00:03:20:00:0D:0A.

***Bluetooth* Device Class** According to the *Bluetooth* standard, every *Bluetooth* device is assigned a device type, which is represented in device class. The *Bluetooth* device class is three bytes in length in

the form of 04:01:00. On the computer side, the class may be Server, Desktop or Laptop. Users will be asked to select it during the first time starting.

***Bluetooth* Device Inquiry** To use *Bluetooth*, the user has to find the remote device first. The searching procedure is called device inquiry. There are two kinds of inquiry procedure, named General Inquiry and Limited Inquiry. General Inquiry will find all the *Bluetooth* devices in general discoverable mode and limited discoverable mode. Limited Inquiry will find only the devices in limited discoverable mode.

***Bluetooth* Dongle** A *Bluetooth* device which can be added onto a PC or a notebook to make it *Bluetooth* enabled. Typically a USB device.

***Bluetooth* Pairing** *Bluetooth* Bonding is the creation of a relationship between two devices, which are known to each other prior to the bonding procedure. A user initiates the bonding procedure and enters a passkey to create a bond between two devices. This differs from the authentication procedure where the user is requested to enter a passkey during the establishment of the link.

***Bluetooth* Passkey** In the *Bluetooth* authentication procedure, a *Bluetooth* passkey is requested on both connection sides. The same *Bluetooth* passkey should be input on both sides. If the passkeys are the same, the authentication procedure is successful and connections can be setup. If the passkeys are different, the connection and authentication will fail.

***Bluetooth* Peripheral Device** This is the implementation of the *Bluetooth* Human Interface Device profile (HID). By using HID, a *Bluetooth* peripheral input device such as *Bluetooth* mouse or keyboard can interface with the host PC remotely.

***Bluetooth* Security** *Bluetooth* security is an important part for the wireless communication technology. Illegal access to your computer can be rejected. There are three levels of security: Low, Medium and High. In Low level, there is no security check. In Medium level, remote *Bluetooth* devices can browse your services. Security is set on every service. The service can be set to request or not request for authentication and authorization. If you request for authentication, the remote device will be asked to enter the same passkey as the one in your PC . Otherwise, the *Bluetooth* passkey is not asked. If authorization is set, the remote device has to be in the authorized devices list. If not, there will be a dialog to ask the user to confirm whether you are going to allow a remote device to use your some services.

***Bluetooth* Service** A *Bluetooth* device may offer certain functions for other *Bluetooth* devices to use. These functions are called *Bluetooth* services. For example, a *Bluetooth* mobile phone can offer 4 services, which include synchronization, dial-up networking, file transfer and serial port. In BlueSoleil, all services need to be started manually before using. The user can also stop the service.

***Bluetooth* Service Browse** A remote *Bluetooth* device can provide one or more *Bluetooth* services. To use the services that the remote device provides, the user has to find the services first. This is called service browse.

C

Connectable *Bluetooth* devices can be connectable or non-connectable. When the device is connectable, other devices can connect to it.

D

DHCP The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP.

E

Encryption When a *Bluetooth* link is encrypted, data are encrypted into unreadable data using a secret key or password before they are sent over the air. Data are decrypted after they reach the remote device using the same key or password that was used to encrypt it.

G

General Discoverable *Bluetooth* devices have 3 modes: General discoverable, Limited discoverable and Non-discoverable mode. A *Bluetooth* device will respond to a General Inquiry if it is

in general discoverable or limited discoverable mode.

H

HID A Human Interface device such as keyboard and mouse.

I

ICS Internet Connection Sharing. For more detailed information about ICS, please refer to the help topic Internet Connection Sharing of Microsoft Windows.

L

Limited Discoverable *Bluetooth* devices have 3 modes: General discoverable, Limited discoverable and Non-discoverable mode. In Limited discoverable mode, a *Bluetooth* device will only respond to a Limited Inquiry.

LAN Access Point One of entities defined in the LA profiles, the LAN Access Point acts like a router between a *Bluetooth* piconet and an external network.

N

NAP (Networking Access Point) A network access point is a unit that contains one or more *Bluetooth* radio devices and acts as a bridge, proxy, or router between a *Bluetooth* network and some other network technology (10baseT, GSM, etc).

NAT Network address translation, which is used to re-map IP #'s from one address range to another range of network addresses.

Non-connectable A *Bluetooth* devices can be connectable or non-connectable. When it is non-connectable, other devices cannot connect to it. This is used in BlueSoleil only when the user does not want other device to connect to their computer.

Non-discoverable *Bluetooth* devices have 3 modes: General discoverable, Limited discoverable and Non-discoverable mode. In Non-discoverable mode, a *Bluetooth* device will not respond to any inquiry so no device can find it.

Non-pairable A *Bluetooth* device can be pairable or non-pairable. When it is non-pairable, it will not accept a bonding request from other devices.?nbsp;

P

Pairable A *Bluetooth* device can be pairable or non-pairable. When it is pairable, it will accept a bonding request from other devices. After the bonding process is finished successfully, two devices are paired. They now form a trusted relationship. There is no need to exchange *Bluetooth* Passkeys the next time they connect.

Pairing Devices Pairing allows you to avoid entering access information each time a connection is set up. Paired devices share a unique Link Key, which they exchange each time they connect.

PIM Personal Information Management.

R

Radio Signal Strength *Bluetooth* works on 2.4G ISM band. The radio signal is stronger when the remote device is closer or the remote device has a higher radio output. The radio signal is weak when the remote device is distant or the remote device has a weak radio output. The strength of the remote device's radio signal affects the quality of the communication of the two *Bluetooth* devices. When the radio signal is weak, the *Bluetooth* data transferring speed is slow. However, if the two devices are too close and the radio signal is too strong, the *Bluetooth* data transferring speed is also slow because the "sound" is too loud to "hear". The radio signal strength is always referred to as RSSI in *Bluetooth*.

Remote *Bluetooth* Device All the other *Bluetooth* enabled devices are called remote *Bluetooth* devices in the term of my *Bluetooth* device. They could be a *Bluetooth* modem, *Bluetooth* mobiles or a *Bluetooth* PDA etc.

T

Trusted Device Device having unrestricted access to all services on the server.