PLEASE THINK BEFORE YOU PRINT

SMART Bridgit™ 4.2

Installation and System Administrator's Guide

Windows® Operating Systems

Extraordinary made simple™ | SMART™

Product registration

If you register your SMART product, we'll notify you of new features and software upgrades.

Register online at smarttech.com/registration.

Keep the following information available in case you need to contact SMART Technical Support.

Product key: _____

Date of purchase: _____

11/2010

Contents

Chapter 1

Introducing SMART Bridgit™ software

SMART Bridgit™ software is a cost effective client/server application that lets you easily schedule meetings to connect, share and collaborate between SMART Board interactive whiteboards, interactive displays and local and remote participants anytime, anywhere. SMART Bridgit software supports private local and wide area network (LAN and WAN) installations as well as public deployment scenarios that use a fully qualified domain name via the Internet.

For detailed information about using the SMART Bridgit client software, refer to its online Help.

Software components

Once you install and configure SMART Bridgit Server software, computers that meet the minimum requirements can connect to your server, download the SMART Bridgit client software and create or join meetings.

SMART Bridgit Server software (Windows® only)

SMART Bridgit Server passes data between clients and authenticates client connections using optionally implemented passwords.

SMART Bridgit Administration Tools

SMART Bridgit Server software also includes an Administration Tools application. You can use SMART Bridgit Administration Tools to configure servers and view their statuses, manage your

SMART Bridgit software licenses and change password, sharing and remote control settings. You can also use the tools to set up a message of the day and configure chat and video settings.

When you install SMART Bridgit Server software, a shortcut to SMART Bridgit Administration Tools appears on your desktop.

SMART Bridgit client software

SMART Bridgit client software transmits meeting data to and from the SMART Bridgit Server and displays it to the meeting participants.

Features and highlights

- Share multiple displays with local and remote participants
- Share applications running on your SMART Board interactive whiteboard or computer desktop with meeting participants
- Host live demos, presentations, training events, webinars and ad hoc collaborative sessions
- Share and work on meeting notes simultaneously with remote participants
- Help colleagues and customers navigate Internet and intranet sites
- Request permission to remotely control a meeting participant's computer
- View off-site meeting participants using webcams
- Speak with, and listen to, meeting participants using VoIP technology

SMART Bridgit software and SMART Meeting Pro™ Premium software

SMART Bridgit software is integrated with SMART Meeting Pro Premium software and SMART Product Drivers to provide screen sharing and simultaneous viewing of multiple shared displays, VoIP and webcam functionality. SMART Bridgit works best with SMART Meeting Pro Premium version 2.1 and 2.2. For detailed information on this functionality, refer to SMART Meeting Pro Premium documentation.

SMART Bridgit software and SMART Notebook™ collaborative learning software

SMART Bridgit software is integrated with SMART Notebook software and SMART Product Drivers to provide instant conferencing capabilities. SMART Bridgit works best with SMART Notebook versions 10.0 and 10.6 and SMART Product Drivers versions 10.6 SP2 and 10.7. For detailed information on this functionality, refer to SMART Notebook software documentation.

Global Server Network (GSN) option

The SMART Bridgit Global Server Network is a network of SMART Bridgit Servers at different geographical locations. The GSN optimizes bandwidth and reduces latency by detecting the fastest server in each GSN and then automatically connecting the client to that server, regardless of the server they initially connected to.

For example, if there are five clients in North America and five clients in Europe all connecting to the same meeting, and the GSN consists of one server on each continent, each client automatically connects to the nearest, fastest server. This results in only one high latency overseas connection, instead of five overseas connections. A GSN works just as well for different buildings in the same city, or even different networks in the same building.

SMART Scheduler

SMART Scheduler allows you to create meetings in Microsoft® Outlook® that will automatically start on a specified SMART Bridgit Server. SMART Scheduler monitors the Microsoft Exchange server for upcoming SMART Bridgit meetings and starts the meeting on the SMART Bridgit Server at the appropriate time.

SMART Scheduler Outlook add-in

To use SMART Scheduler, install the SMART Scheduler Outlook add-in on your client computers. This add-in consists of a toolbar that appears in the standard meeting request window in Microsoft Outlook.

You can create a meeting in Outlook that uses SMART Bridgit software by selecting the **This is a SMART Bridgit Meeting** check box in the meeting creation dialog box. Both the meeting creator and the attendees will see a booking in their Outlook calendar that contains a link to the SMART Bridgit meeting.

Chapter 2

Installing SMART Bridgit software

This chapter contains information you will need to prepare for installation as well as procedures that will lead you through the installation process of SMART Bridgit software and its options.

Preparing for installation

SMART Bridgit software is scalable, so system requirements vary. The maximum number of users that a server can support is constrained by both the server hardware and the network bandwidth available to that server. The exact number of users supported varies depending on the available bandwidth and the use of Voice over Internet Protocol (VoIP) audio and webcam functionality. Allowing more than the recommended number of simultaneous users may negatively impact performance. To support more users, configure multiple servers to operate as a global server network (GSN).

NOTES

- To determine the amount of bandwidth you need, see *Bandwidth requirements* on page 51.
- Your system performs best if you use a high performance server or a dedicated server with no other applications installed.

Server system requirements

Each server must meet the following minimum requirements:

- 1.2 GHz Intel® Pentium® 4 processor (or equivalent)
- Windows XP SP3, Windows Server 2003 R2, or Windows Server 2008 R2 operating system
- 1 GB of RAM
- 100 Mbps (1 Gbps NIC recommended) network interface card (NIC) that supports the TCP/IP protocol

NOTE

Increased hardware and network specifications improve overall meeting performance.

Software licensing

During the 60-day free evaluation period, the server allows five concurrent user connections. After the evaluation version expires, users can no longer conduct meetings on the server. At or before this point, you must purchase and activate a software license.

Managing software licenses

To continue using SMART Bridgit software, purchase the software before the evaluation period expires. Visit smarttech.com/where+to+buy to find out where you can buy SMART Bridgit Server software licenses and user licenses.

After you purchase the software, you receive an e-mail that includes product keys for activating the server software and user licenses.

Five concurrent users can connect to a SMART Bridgit meeting using a single server license. The server license starts with the letters BDS and must be installed and activated before you can install a user license, which starts with the letters BDC. To allow more than five concurrent users, you must purchase additional user licenses.

Access requirements

Before you can successfully install and use a SMART Bridgit Server, you must correctly configure your network environment. SMART Bridgit Server software doesn't automatically do this. Therefore you need access to various components of your network infrastructure before you can configure your network environment appropriately.

Network administration experience

IMPORTANT

SMART Bridgit Server functions in a complex network environment. Do not attempt to install or configure the SMART Bridgit Server software unless you're an experienced network administrator with a full understanding of how your network functions.

Access to servers and infrastructure components on your network

Different network configurations use different types of access.

Private local area network (LAN) use

If your SMART Bridgit Server will be used only in a private LAN, you need access to the following components of your LAN infrastructure:

- An administrator login account with installation rights for the server computer you'll install SMART Bridgit Server software on.
- Physical or remote login access, and an administrator login account with configuration rights, for your network's DHCP and DNS servers.

- You could also need physical or remote login access to, and an administrator login account with configuration rights for, your network's domain server which controls the software firewall configurations for all of your network's client computers. This is dependent on your local network's domain policies.

Use by different networks connected to a wide area network (WAN)

If your SMART Bridgit Server will be used by different networks connected to a WAN, you'll need access to the following components of your LAN or WAN infrastructure:

- Physical or remote login access to, and an administrator login account with configuration rights for, the routers, WAN firewalls, and proxy servers between different segments of your WAN.
- Physical or remote login access to, and an administrator login account with configuration rights for, all DNS servers in each segment of your WAN.

Use by clients with an Internet connection

If your SMART Bridgit Server will be accessible to clients via the Internet, you need access to the following components:

- Physical or remote login access to, and an administrator login account with configuration rights for, the routers, firewalls and proxy servers between your network and the Internet.
- Login access with configuration rights to the Internet registrar which controls your company's public Internet DNS records.

Use of SMART Scheduler

If you want to use the SMART Bridgit Outlook add-in and SMART Scheduler integration with Microsoft Exchange, you need physical or remote login access to, and an administrator login account with configuration rights for, your company's domain server. This server is used to create user accounts for use on your Microsoft Exchange Server.

Administrator rights

After you've installed and configured the SMART Bridgit Server, you may want to administer the server to check information such as performance logs and use records. To do this, your administrator needs physical or remote login access and a user login account on the SMART Bridgit Server computer.

About SMART Bridgit security

Server security

SMART Bridgit software complies with the Secure Socket Layer (SSL) 3.0, to encrypt data transmitted using a TCP connection. It uses OpenSSL to generate a self-signed SSL certificate used for data encryption. Each time the server starts, it generates a new 1024-bit SSL certificate and it negotiates a new 256-bit encryption key with each client. However, if a client is unable to negotiate a set of encryption keys with the server, no connection is established.

SMART Bridgit software also uses Secure Real-time Transport Protocol (SRTP) to encrypt audio traffic transmitted using a UDP connection. These encryptions prevent third parties from intercepting data transmitted between client and server.

The cipher suite negotiated between a Windows operating system server and client is an AES256-SHA cipher suite, including RSA encrypted key exchange, digest authentication, and 256-bit SSL data encryption. SMART Bridgit software for Mac OS operating system software also implements 256-bit SSL encryption.

Client security

System administrators and meeting creators can set four types of passwords to enhance SMART Bridgit software security. These passwords aren't mandatory.

IMPORTANT

If you assign a server access password, you must also assign a conference creation password.

Password type	Description
Server access password	The password a meeting participant uses when connecting to the SMART Bridgit Server. The server administrator sets this password, which allows the participant to view the list of meetings on the server.
Conference creation password	A password required to create a new meeting. The server administrator sets this password, which prevents unauthorized users from creating meetings.
Meeting password	A password that meeting participants use to join a meeting. The meeting creator sets this password.
Administrator access password	A password that server administrators create to allow them to join any meeting on the server. Administrators can then monitor meetings and ensure the server is being used appropriately.

Domain names

If you're using a public domain name, your SMART Bridgit Server is accessible to clients connecting via the Internet. If you use a private domain name, your SMART Bridgit Server is accessible only to clients connecting from within your LAN.

Registered domain name

To access a server over the Internet, you must use a fully qualified domain name (FQDN) that exists in the records of a public DNS server. If an FQDN isn't available for your server, users can access your server over the Internet using its IP address directly.

IMPORTANT

Do not mix FQDNs and unqualified domain names (those not registered on a DNS server) in the same SMART Bridgit Server Global Server Network (GSN).

IPv4/IPv6 addresses

During the installation process, SMART Bridgit software detects the IP addresses bound to the servers' network interface cards. You can choose to bind SMART Bridgit software to one or all of the computers' IP addresses, if there is more than one IP address assigned to the computer.

To check if your public domain name resolves to an IP address

1. On the computer where you'll install the SMART Bridgit Server software, select **Start > Run**.
2. Type **cmd**, and then press ENTER.

   A *Command Prompt* window appears.
3. Use the **ipconfig** command to determine the server's IP address.
4. Use either the **nslookup** command or the **ping** command against the domain name for the SMART Bridgit Server to determine the IP address that the network's DNS returns.
5. Compare this IP address to the SMART Bridgit Server's IP address from step 3.

   If the IP addresses are the same, the network's DNS is configured correctly.

NOTES

- Your domain name must resolve to a valid IP address for you to be able to use it to configure your SMART Bridgit Server.
- The ping can fail for reasons unrelated to the public domain name and still resolve to a computer name or IP address.

SMART Bridgit and firewalls

SMART Bridgit software automatically detects and employs the most secure and efficient methods available to connect clients and to maintain optimal meeting performance. However, SMART recommends installing your SMART Bridgit Server behind a firewall to prevent unauthorized access.

The firewall must open port 80 for HTTP traffic coming into the server and going out to the client.

NOTE

SMART doesn't recommend deploying SMART Bridgit Servers with only HTTP connectivity.

Configuring firewalls

You can install your SMART Bridgit Server behind a software firewall, proxy server, hardware firewall or router. For optimal performance, enable both primary and secondary TCP ports and a range of UDP ports for Voice over Internet Protocol (VoIP) audio on the server.

- Firewalls for the server should allow inbound communication to the server on all specified ports.
- Firewalls for the client should allow outbound communication from the client on all specified ports.

For best performance, allow inbound TCP and UDP traffic to the server on the default ports specified in the following table.

Default ports	Type/protocol	Use
80	TCP/HTTP	• Initial connection to the SMART Bridgit Server to display the web page from which the users download the SMART Bridgit client. • Initial connection to the SMART Bridgit Server from the SMART Bridgit client when looking for meetings to join or when creating new meetings. • Fallback communications method for all other SMART Bridgit functions when other ports are unavailable (lower performance than other ports).
80	TCP/SMART Bridgit	• Primary port for data, screen viewing and webcam traffic for SMART Bridgit meetings. • If this port is limited to only HTTP protocol, SMART Bridgit attempts to use the secondary port (9933) for this traffic. If this port is blocked or unavailable, SMART Bridgit uses the HTTP protocol on the primary port, which can affect performance.

Default ports	Type/protocol	Use
9933	TCP/SMART Bridgit	Secondary port for data, screen viewing and webcam traffic for SMART Bridgit meetings.
9901 to 9920	UDP/SMART Bridgit	• Primary port range for VoIP audio traffic for SMART Bridgit meetings. • If these ports are blocked or unavailable, SMART Bridgit will fall back to TCP or HTTP protocol on the primary or secondary port, which can negatively effect performance.

Configuring proxy servers

You can configure your SMART Bridgit Server to work with any proxy server that adheres to the RFC 2068 HTTP standard. If you install your SMART Bridgit Server software behind a proxy server, you must create access policy rules for inbound and outbound traffic on that proxy server. You can further enhance your network security by enabling authentication, such as basic, digest or NT LAN Manager (NTLM) authentication.

NOTE

While proxy servers protect internal networks from intruders, they unavoidably introduce network latency.

If you incorporate a proxy server, configure each meeting participant's Internet browser to allow access to the SMART Bridgit Server.

Client system requirements

Without VoIP audio or webcams

Windows®

- 1.2 GHz Pentium® III processor, 512 MB of RAM
- Windows 7, Windows XP SP3 or Windows Vista® operating system
- Broadband Internet connection

Mac

- 1.2 GHz PowerPC® G4 or G5 processor or Intel® processor
- Mac OS 10.4.X, 10.5.X or 10.6.X operating system software
- 512 MB of RAM
- Broadband Internet connection

With VoIP audio and webcams

Windows

- 1.2 GHz Pentium III processor, 1 GB RAM
- Windows 7, Windows XP SP3 or Windows Vista® operating system
- Broadband Internet connection

Mac

- 1.2 GHz PowerPC G4 or G5 processor or Intel processor
- Mac OS 10.4.X, 10.5.X or 10.6.X operating system software
- 1 GB of RAM
- Broadband Internet connection

Webcam requirements

Windows

- DirectShow 9 driver compatibility
- 24-bit RGB color support

Mac

- Internal webcam or iSight camera
- QuickTime video capture
- 24-bit RGB color support

Audio requirements

- Sound card
- Speakers or headphones
- Microphone

Internet browser requirements

Windows

- Internet Explorer® 6.0, 7.0 or 8.0
- Opera 9 or 10
- Firefox® 2.0, 3.0 or 3.5

Mac

- Firefox 2.0, 3.0 or 3.5
- Safari 3.0

Software requirements

- Microsoft Outlook® or another e-mail program

  NOTE

  Although SMART Bridgit works with many e-mail programs, it works best with Microsoft Outlook. If you use a different e-mail program, e-mail invitations might not work correctly.

- SMART Board software or SMART Notebook software 10.0 or later

  NOTE

  You can download a free upgrade of SMART Notebook software from http://smarttech.com/software.

Prerequisites for SMART Scheduler

Minimum computer requirements
Microsoft Exchange Server

Use either Microsoft Exchange Server 2003 or 2007.

SMART Scheduler Server

- 1.2 GHz Intel Pentium 4 processor or equivalent
- 1 GB of RAM
- Windows XP SP3, Windows Server 2003 R2 or Windows Server 2008 R2 operating system
- 10 Mbps network interface card that supports the TCP/IP protocol
- Network connection to your Microsoft Exchange Server 2003 or 2007
- CDO 1.2.1 (Microsoft Collaboration Data Objects), version 6.5.8165.0 or later. You can also download this software during the server installation.

SMART Scheduler Outlook client add-in

- 1.2 GHz Pentium III Processor
- 512 MB of RAM

- Microsoft Outlook 2003 SP3 or Outlook 2007 SP2
- Network connection to your Microsoft Exchange Server

System requirements

Before you install SMART Scheduler Server, ensure your system meets these requirements:

- You must set up a dedicated mailbox on the Microsoft Exchange Server that the SMART Scheduler Server computer has access to. SMART Scheduler Server uses this mailbox to manage SMART Bridgit meetings.
- You must have a local administrator account set up in the Windows domain associated with the mailbox described above. SMART Scheduler Server uses Windows user authentication to run the service as well as to access the Exchange mailbox.
- The SMART Scheduler Server must not have Microsoft Outlook installed on it.
- You must have SMART Bridgit Server installed and running on either a separate computer (recommended) or, if required, on the same computer where you'll install SMART Scheduler Server.

IMPORTANT

- Do not use a personal mailbox for SMART Scheduler Server software. The SMART Scheduler Server software will automatically and permanently delete anything in this mailbox, including e-mail messages and calendar appointments.
- The SMART Scheduler Server must have a network communication path to both the SMART Bridgit Server and your Microsoft Exchange Server. It should be installed on the same network segment as your Microsoft Exchange Server.
- If you install the SMART Bridgit Server in a different segment of your network, such as an isolated DMZ segment between your LAN and the Internet, do not install the SMART Scheduling Server on the same computer as the SMART Bridgit Server.

Installing SMART Bridgit Server software

Introduction

When installing the SMART Bridgit Server software, consider the following points:

- If you install SMART Bridgit Server software on a dedicated server with one network interface card (NIC), select All (default) to bind SMART Bridgit to all IP addresses. If your network uses network address translation (NAT), use port forwarding to redirect external requests to the NIC.
- If the server is multi-homed (has multiple NICs), select the internal IP address to bind SMART Bridgit to the internal NIC. Use port forwarding to redirect external requests to the external NIC.
- If you install SMART Bridgit Server software on a server running other web server applications (for instance Microsoft IIS, or any other web server application using Port 80), you can configure SMART Bridgit by:
  - Using IP specific binding. Each server binds to a specific IP address. You can add multiple IP addresses to a single NIC on Windows servers by selecting **Control Panel > Network Connections > Internet Protocol (TCP/IP)**.
  - Customizing the default primary server port. In this case, multiple applications can bind to the same IP address but on different ports. This setup requires users to specify the port when connecting SMART Bridgit client (for example **server.company.com**).

Installing the server software

To install SMART Bridgit Server software

1. Download SMART Bridgit software, and then double-click the **ConferenceServicesSetup.exe** file you downloaded.
2. Run the software.

   The SMART Bridgit - Installshield Wizard opens and displays the start-up screen.
3. Click **Next**.

   The *Licence Agreement* page appears.
4. Read the license agreement, and if you agree, click **I accept**, and then click **Next**.

   NOTE

   If you want to keep a hard copy of the agreement for your records, click **Print**.

   The *Destination Folder* window appears.

5. Click **Next** to use the default destination folder.

   OR

   Click **Change** if you want to select a new location for SMART Bridgit software, browse to the desired folder, click **OK**, and then click **Next**.

   The *Customization* page appears.

6. Configure your server by selecting one of the following options:

IPv4 address and IPv6 address	The installation software detects all IP addresses assigned to the server. To use all the addresses, select **All** in the *IPv4 address* or *IPv6 address* boxes. **NOTES** ○ If you select all addresses, SMART Bridgit software clients can use any IP address assigned to the server computer to contact the SMART Bridgit Server. To restrict the IP addresses through which your server is reachable, select a specific IP address. ○ If the IP address fields are unavailable, SMART Bridgit software has automatically detected that you don't have more than one IP address to choose from.
Public domain name	Each SMART Bridgit Server requires a fully qualified domain name (for example, server.company.com or conference.company.com) or a host name (for LAN access only). **IMPORTANT** If you use the computer's network host name as the domain name, the server will be accessible only from within the local area network. Internet users won't have access to the server. Do not mix fully qualified domain names and computer host names within the same SMART Bridgit GSN.

7. Click **Next**.

   The *Server Port Configuration* page appears.

8. Configure the ports using the following options:

Primary TCP port	By default, SMART Bridgit software uses port 80 as its primary port. If your server is running another application that uses port 80, you must assign SMART Bridgit software to an unoccupied port. Configure your firewall to allow incoming and outgoing TCP traffic on your chosen port.
Enable secondary TCP port	By default, SMART Bridgit software uses port 9933. If you want to use a different port, make sure it doesn't conflict with any other applications running on the server computer. **NOTE** If your server is running another application that uses either of these ports, you must assign SMART Bridgit software's primary and secondary ports to unoccupied ports. Configure your firewall to allow incoming and outgoing TCP traffic on the chosen ports.
Enable UDP ports (audio optimization)	Whenever possible, SMART Bridgit software uses UDP for audio transmission to avoid the additional overhead of TCP in a timing-sensitive situation. SMART strongly recommends that you enable UDP to minimize audio lag in SMART Bridgit meetings. You must open a range of UDP ports (9901 to 9920) on your firewall to use this feature. **NOTES** ○ If you configure SMART Bridgit Server software to use a TCP port that isn't the default, users must specify the port when connecting to the server. For example, to connect to a SMART Bridgit Server on port 8080, users must type server.company.com: 8080. ○ A UDP port supports up to 10 participants with optimal performance. By default, SMART Bridgit software opens 20 UDP ports to allow to approximately 200 concurrent participants. Open more ports to accommodate more participants. ○ If your network uses a firewall, you must configure it to allow incoming TCP and UDP traffic on these ports.

9. Click **Next**.

   The *Server Password Security* page appears.

10. Create the following passwords for Server password security, if desired:

Server Access password	This optional password is used by the client to connect to a SMART Bridgit Server. The Server Access password allows the user to access the server and view the list of meetings on it. **IMPORTANT** If you assign a Server Access password, you should also assign a Conference Creation password.
Conference Creation password	This optional password is used by the client to create a meeting on the SMART Bridgit Server. Users who type the conference creation password can also see the list of active meetings on the server. **NOTE** After you've installed SMART Bridgit Server software, you can use SMART Bridgit Administration Tools to create additional server access and conference creation passwords.

11. Click **Next**.

    The *Ready to Install* page appears.

12. Click either **Install** to start the installation, or **Back** to change the settings.

    After you click *Install*, the *In Progress* window appears and the installation validates. The setup status appears on the green status bar.

13. Click **Finish** to complete the installation.

After you finish installing the software, use SMART Bridgit Administration Tools to activate the server software using a valid server product key, install user licenses, change the server settings and view status information.

IMPORTANT

The SMART Bridgit software installation includes a 60-day evaluation license for the server and concurrent users. See *Licensing SMART Bridgit Server software* on next page for information on installing and activating server and user licenses.

Upgrading SMART Bridgit Server software

To upgrade your SMART Bridgit Server software

1. Download SMART Bridgit software. Go to http://www.smarttech.com/downloads.
2. Double-click the **ConferenceServicesSetup.exe** file you saved.

3. Run the software.

   A message appears asking if you want to update or repair the program components from the previous version and warning you that all open meetings will be closed during the update.

4. To close the meetings and continue with the service update, click **Yes**.

   Otherwise, click **No**, and then end the meetings using the on-screen instructions.

If you choose to continue with the services update, the InstallShield wizard appears. Follow the procedure in *Installing the server software* on page 16.

Licensing SMART Bridgit Server software

Once your 60-day trial expires, you must activate your server and optional user software licenses to continue using SMART Bridgit software. If you have more than one user license, activate the others next.

NOTE

If you upgrade from SMART Bridgit software version 3 to version 4, your version 3 licenses continue to work with version 4. However, if you upgrade from a version earlier than 3.1, the software's Voice Over Internet Protocol (VoIP) audio features aren't available. To enable the VoIP audio features after you upgrade from version 3.0 or earlier, purchase an audio upgrade license from your authorized SMART reseller.

Activating using the SMART activation server

To activate your license using SMART activation server

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Licensing** tab.
3. In the *Server* list, select the server you want to activate.
4. Click **Install Server License** to install and activate the server license.
5. Type your product key in the **Product Key** box, and then click **OK**.

   After you activate the product key, your license information appears in the *Licenses for selected server* table and the related license status changes to *Activated*.

6. If you have a user license, click **Install User License** to install and activate the client licenses.
7. Type your product key in the **Product Key** box, and then click **OK**.

   The license status changes to *Activated*.

8. SMART Bridgit software uses a web service to automatically activate your SMART Bridgit Server and user license.

   NOTE

   If the service isn't available or if another error occurs, you must manually activate the license.

Activating your license manually

To manually activate your license by e-mail

1. Right-click the license you want to activate in the *Licenses for selected server* table, and then click **Activate**.
2. Click **Activate manually**, and then click **Continue**.

   The *Activate License* dialog box appears.
3. Click the **To automatically generate an e-mail** link.

   Your default e-mail software opens a new message addressed to support@smarttech.com. The message contains your product key and an installation ID that a Technical Support specialist uses to create your activation key.
4. Send the e-mail.

   You'll receive a reply e-mail with your activation key.

   NOTE

   You have 60 days from the date of installation to enter the activation key.

To manually activate your license by phone

1. If you aren't connected to the Internet, or if e-mail isn't available, click the **If an e-mail does not appear** link.

   The *Manual Activation Assistance* dialog box appears with SMART Technical Support telephone contact information, your product key and your installation ID. When you call Technical Support, provide the support specialist with these numbers.
2. When you receive an activation key, double-click the **SMART Bridgit Administration Tools** icon on your desktop, and then select the **Licensing** tab.
3. Right-click the license you want to activate, and then select **Activate**.
4. Click **Activate Manually**, and then type the activation key.

5. Click **OK**.

   After you activate the product key, your license information appears in the *Licenses for selected server* table and the related license status changes to *Activated*.

Removing server or user licenses

If you remove a server license or a bundle of user licenses, the product keys remain valid and you can add them again at any time.

To remove server or user licenses

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Licensing** tab.
3. Right-click the licenses you want to remove in the *Licenses for selected server* table, and then click **Delete**.

   A confirmation dialog box appears.
4. Click **OK**.

Chapter 3
Configuring the server software

You can use SMART Bridgit Administration Tools on any SMART Bridgit Server to assign client access and server access passwords, create a message of the day, and enable remote control. If you're using a GSN, these settings automatically update on all your SMART Bridgit Servers.

Setting passwords

You can assign, change or remove many of the passwords users and administrators use with SMART Bridgit.

Changing the server access password

Server access passwords are optional. Assign a server access password if you want users to have to type a password before they can view the list of active meetings on a server. You can assign as many server access passwords as necessary.

IMPORTANT

If you assign a server access password, you must also assign a conference creation password.

To change server access passwords

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Security** tab.
3. Select the **Server access password** check box in the *Client access passwords* area.
4. Type the passwords you want to use. Use a semicolon to separate multiple passwords (for example, apple;banana;pear).

   NOTE

   To revoke a password, remove it from the list.

5. Click **Apply**.

   NOTES

   - Remember to give the passwords to everyone who's authorized to view the list of active meetings.
   - Participants who receive an e-mail invitation to join a meeting can click the link in the invitation to bypass the server access password. However, the participant can join only the meeting they were invited to. The participant can't view the list of other active meetings on the server.

Changing the conference creation password

Conference creation passwords are optional. Assign a server access password if you want users to have to type a password before they can create a meeting. You can assign as many passwords as necessary.

IMPORTANT

If you assign a server access password, you must also assign a conference creation password.

To change conference creation passwords

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Security** tab.
3. Select the **Conference creation password** check box in the *Client access passwords* area.

4. Type the passwords you want to use. Use a semicolon to separate multiple passwords (for example, apple;banana;pear).

   NOTE

   To revoke a password, remove it from the list.

5. Click **Apply**.

   NOTE

   Remember to give the passwords to everyone who's authorized to create meetings.

Changing the administrator access password

Administrators can access and monitor any meeting on the SMART Bridgit Server using an administrator access password.

To assign an administrator access password

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Security** tab.
3. Select the **Admin access password** check box in the *Client access passwords* area.
4. Type the passwords you want to assign.
5. Click **Apply**.

   NOTES

   - You can assign only one administrator access password.
   - The administrator appears as *Administrator* in a SMART Bridgit meeting's participant list, but doesn't have any special capabilities in the meeting.
   - If you create a meeting that uses the same password as the administrator's, no meeting members appear as *Administrator* in the participant list.

Assigning an API password

Only original equipment manufacturers (OEMs) using the SMART Bridgit application programming interface (API) use this authorization password.

To assign an API authorization password

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Security** tab.

3. Select the **API authorization password** check box in the *Server access passwords* area.
4. Type the password you want to assign.
5. Click **Apply**.

NOTES

- You can assign only one API authorization password.
- To revoke the password, clear the API authorization password box.
- Remember to give the password to third-party users whose systems are integrated with SMART Bridgit software.

Changing SMART BridgitServer setup options

Administrators can access and monitor any meeting on the SMART Bridgit Server using an administrator access password.

To change the server setup options

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Setup** tab.
3. Modify the options as required.

   For information on the options, see *Domain names* on page 10 and *SMART Bridgit and firewalls* on page 11 .

   Configuration changes on this page don't take effect until you restart both the SMART Bridgit master and the software services in Windows Services Manager (see *Modifying SMART Bridgit software services* on page 41).

Setting meeting options

You can configure, enable and disable several features of SMART Bridgit that are available to meeting participants.

Configuring meeting audio settings

By default, SMART Bridgit software's audio is enabled, allowing meeting participants to talk to each other during meetings.

Up to four participants in a meeting can talk concurrently using SMART Bridgit's Voice over Internet Protocol (VoIP) feature . SMART Bridgit's VoIP implementation incorporates Secure Real-Time

Transport Protocol (SRTP) communication on UDP ports, processing audio data as a steady stream with minimal lag time.

When more than four people are in a meeting, participants can open and close their microphones to give others the opportunity to talk.

To disable meeting audio

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Audio** tab.
3. Clear the **Enable Audio** check box.

   Meeting audio is disabled in new meetings. However, audio remains available in active meetings until they end.

To select a default audio optimization when using VoIP

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Audio** tab.
3. Select **Use VoIP Audio**, and then select one of the following:
   - **Optimize for high audio quality** provides the best quality meeting audio. It also consumes the most bandwidth.
   - **Optimize for low bandwidth** uses less bandwidth but doesn't provide optimal audio quality.

Third-party audio
If you're using a third-party audio bridge instead of VoIP, you can provide the telephone number and meeting code to participants so they can join the meeting.

To notify participants of a third-party audio bridge

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Audio** tab.
3. Select the **Use a third party audio conferencing provider** option.

Disabling webcams

To disable webcams in SMART Bridgit meetings

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Options** tab.
3. Clear the **Enable Webcams** check box.

   Webcams are disabled in new meetings. However, webcams remain available in active meetings until they end.

   NOTE

   When you disable webcams, the option no longer appears to meeting participants.

Disabling text chat

To disable text chat in SMART Bridgit meetings

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Options** tab.
3. Clear the **Enable Chat** check box.

   Text chat is disabled in new meetings. However, chat remain available in active meetings until they end.

   NOTE

   When you disable text chat, the option no longer appears to meeting participants.

Adding a message of the day

Select this option to create a message users see when they open SMART Bridgit client.

To add a message of the day

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Options** tab.
3. Select the display frequency to use in the *Message of the day* area (select either **Don't show**, **Show once per day** or **Show every time client runs**).

4. Type the message in the *Message of the Day* text box (maximum 256 characters).
5. Click **Apply**.

Chapter 4

Managing a Global Server Network (GSN)

About the Global Server Network

A SMART Bridgit GSN is a network of SMART Bridgit servers in different geographical locations. A GSN optimizes bandwidth and reduces latency for enterprise SMART Bridgit deployment.

You don't have to install the GSN separately. Install the SMART Bridgit Server software and use SMART Bridgit Administration Tools to configure the GSN options. See *Installing the server software* on page 16 for installation information.

SMART Bridgit Servers in a GSN

You install each server in a GSN as an independent SMART Bridgit Server. Once included in a GSN, each independent server becomes a node in the network with independent server capabilities.

Requirements and prerequisites

The requirements for a GSN Server are the same as a standard SMART Bridgit Server. See *Preparing for installation* on page 6 for details.

Setting up a local GSN server

When you install SMART Bridgit Server software, a shortcut to SMART Bridgit Administration Tools appears on your desktop.

NOTES

- Changes made on the *Options*, *Audio* and *Security* tabs in SMART Bridgit Administration Tools on one server in a GSN automatically apply to all servers in that GSN.
- Your server name should describe your local server in plain language.
- The server password is used by other servers in the GSN to add your server. This password is mandatory.

To set up your local GSN server

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Servers** tab.
3. Type a name for your server in the *Description* field in the *Server Setup Information* section of the window.
4. Type a password for the server in the *Server Password* field.
5. Click **Apply**.

> **NOTE**
>
> The *Apply* button is enabled only once you enter a server password.

Adding a remote server to the GSN

To add a remote SMART Bridgit server to the GSN

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Servers** tab.
3. Click **Add**.

   The *Add Server* dialog box appears.
4. Type the **Server Address**, **Server Port** number and **GSN Password** for the server you want to add, and then click **OK**.

> **NOTES**
>
> - All three fields must be filled in before the OK button is available.
> - If you try to subscribe to your own server, an error message appears.
> - If there is no GSN, but you have two servers and want to form a GSN with them, you can use either server to add the other.
> - If there are two or more servers in a GSN, you can't add your server to that GSN. An existing member must add your server.

Once you've added the server, the *Server list* displayed on every member server of the GSN updates with the new server information. If meetings are running which include these servers, the *Conference Server* list on the *Conference* tab also updates.

Removing a server from a GSN

To remove a SMART Bridgit server from a GSN

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Servers** tab.
3. Select the server you want to remove in the *Server list*.
4. Click **Remove**, and then click **OK** to confirm.

NOTES

- The server is removed from every user's *Server list*.
- If clients are connected to meetings at the time of the server removal, they remain on the *Conferences* list of the server computer hosting them.

Changing GSN server information

To change GSN server information

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Servers** tab.
3. Type new information in the *Description* field or the *Server Passwords* field.
4. Click **Apply**.

   The new information is pushed to all other servers in the GSN.

Ending a GSN meeting

To end a meeting on the local GSN server

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Conferences** tab.
3. Select a meeting in the list.

4. Click **End conference**.

> **NOTE**
>
> You can end meetings that exist on your local server only. If the meeting was created on a remote server, the *End Conference* button is unavailable.

SMART Bridgit clients in a GSN

SMART Bridgit clients in a GSN detect and connect to the GSN server with the fastest connection speed. Once this selection and connection is complete, the GSN optimizes the bandwidth for the network.

Connecting to a GSN server

Connecting to a server in a GSN

Connecting to GSN servers is similar to connecting to a single SMART Bridgit server. The main difference is that the SMART GSN client automatically detects the fastest server in the GSN and connects you to it, regardless of the server address you enter.

To connect to the GSN

1. Open your web browser.
2. Type the name of the server you want to connect to in the *Address* bar.

   The *Download SMART Bridgit Software* page appears, including basic instructions and a link for downloading the SMART Bridgit software client.
3. Click the **Download Software** link,and then run the software.

   The *SMART Bridgit Software* client dialog box appears.

Selecting or viewing server information

To select or view a GSN server

1. Double-click the **SMART Bridgit** icon  on your desktop.

   The *SMART Bridgit Software* dialog box appears.

2. Click the server icon  in the bottom left corner.

   The *Server Information* window appears.

   - *Starting server* is the name or address you typed into your browser.
   - *Fastest server* is the name or address of the fastest server in the GSN.

3. Type the name of the new server or select a server from the drop-down list.
4. Click **Connect**.

Disabling the *Pick fastest server* option

NOTE

For best results, SMART recommends always using the *Pick fastest server* option.

To disable the *Pick fastest server* option

1. Double-click the **SMART Bridgit** icon  on your desktop.

   The *SMART Bridgit Software* dialog box appears.

2. Click the small SMART Bridgit icon  in the upper-left corner.
3. Select **About SMART Bridgit**.

   The *About SMART Bridgit Software* window appears.

4. Click the **Technical Support** tab, and then click the **Troubleshooting** tab.
5. Clear the **Pick fastest server** check box in the *Connection* area of the window.

   The next time you connect to a GSN, you'll connect to the server you designate, regardless of connection speed and network traffic.

Chapter 5

Administering the server software

About SMART Bridgit Administration Tools

SMART Bridgit Server software includes an Administration Tools application. You can use SMART Bridgit Administration Tools to configure servers and view their statuses, manage your SMART Bridgit software licenses and change password, sharing and remote control settings. You can also use the administration tools to set up a message of the day and configure chat and video settings.

When you install SMART Bridgit Server software, a shortcut to SMART Bridgit Administration Tools appears on your desktop.

IMPORTANT

Before you start SMART Bridgit Administration Tools, you may need to temporarily disable the other services listening on the same port as SMART Bridgit services. When you finish configuring SMART Bridgit Server software, re-start the services you disabled.

Viewing status information

You can use SMART Bridgit Administration Tools to view status information for SMART Bridgit Server software, including active meetings, licenses and server usage.

Viewing active meetings

To view active meetings

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Conferences** tab.

   A table of active meetings appears. The table includes the following information:

   - when the meeting was created
   - the meeting's name
   - who created the meeting
   - the number of participants
   - the GSN server hosting the meeting

Broadcasting messages to participants

To broadcast a message to all meeting participants

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Conferences** tab.
3. Select the meeting to which you want to broadcast a message, and then click **Send Message**.
4. Type the message you want to broadcast in the **Message** box.
5. Click **OK**.

   Your message appears on each meeting participant's screen.

Viewing status information

To view status information

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Servers** tab.

   A table appears. It includes the following information:

   - server IP address or domain name
   - a description of the server
   - the port being used for the server
   - the number of active meetings
   - the server's status, which can include the following:
     - Alive: The server is active and users can connect.
     - Offline: The server is offline or can't be contacted by the local server.
     - On hold: An administrator has placed the server on hold.

Viewing and saving usage reports

To view server usage reports

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Report** tab.

   A server usage report for the current week appears.
3. To view a report for a different time period, select the **Report start date** and **Report end date** that you want, and then click **Refresh**.

   A report appears for the period you select.

To save a server usage report as a text file

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Report** tab.

   A server usage report for the current week appears.

3. In the server usage report, select the entries you want to save.

   OR

   Ensure no entries are selected if you want to save the entire report.

4. Click **Save Report**.

   A *Save As* dialog box appears.

5. Enter a file name and destination, and then click **OK**.

Setting log purge frequency

You can control how long the log stores information about server usage. The default value is 30 days, which means log entries older than 30 days are automatically deleted from the log. You can use any setting between one and 120 days.

To set log purge frequency

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Report** tab.
3. Enter the number of days you want the log to store information for in the *Logs purged after* box.
4. Click **Apply**.

Managing servers and meetings

You can change the connection status of servers and end meetings using SMART Bridgit Administration Tools.

Placing a server on hold

When you place a server on hold, it doesn't allow users to connect, but doesn't end active meetings.

Place a server on hold when you want to perform maintenance procedures on the server. This allows active participants to finish their meetings, and allows you to maintain the server when they're finished.

To place a server on hold or reactivate it

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Servers** tab.
3. In the *Server list*, select the server you want to place on hold or reactivate.

4. Click **On Hold**, and then click **OK** when asked to confirm.

   OR

   Click **Re-activate Server**.

   The server status changes to *Alive*.

Ending a meeting

To end a meeting

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop.
2. Click the **Conferences** tab.
3. Select the meeting you want to end.
4. Click **End Conference**.

   If you want to broadcast a message to meeting participants as the meeting ends, type it in the *Message* box.
5. Click **OK**.

   A notification dialog box and your message appear on each meeting participant's screen, and the meeting ends.

Modifying SMART Bridgit software services

You can use the Microsoft Windows Services administration console to control SMART Bridgit software services without restarting the computer.

IMPORTANT

If you stop the services from the Windows Services administration console, all meetings currently running end without warning the users.

To control SMART Bridgit software services

1. Open the Windows Services administration console (**Control Panel > Administrative Tools > Services**).
2. Double-click **SMART Bridgit Master Service**.

   The *SMART Bridgit Master Service Properties* dialog box appears.
3. Click **Start**, **Stop**, **Pause**, **Restart** or **Resume** in the *General* tab to control the service.

4. Click **OK**.
5. Double-click **SMART Bridgit Conference Service**.

   The *SMART Bridgit Conference Service Properties* dialog box appears.
6. Click the **General** tab.
7. Click **Start**, **Stop**, **Pause**, **Restart** or **Resume** to control the service.
8. Click **OK**.

Customizing the SMART Bridgit Server's web page

After you configure the SMART Bridgit Servers, users can download the SMART Bridgit client by visiting the server's address in a web browser.

To customize the SMART Bridgit Server's web page

1. Create a web page file called **CustomPage.htm**.
2. Customize the web page as desired.

   It should contain links to download the SMART Bridgit client for both Windows operating systems and Mac OS X operating system software. You may also want to include the SMART Scheduler Outlook Add-in installer.

   The paths for these files are:

Windows	http://*yourbridgitserverurl*/Bridgit.exe
Mac OS X	http://*yourbridgitserverurl*/Bridgit.zip
SMART Scheduler Outlook Add-in	http://*yourbridgitserverurl*/BridgitSchedulerOutlookAddinSetup.msi

   where *yourbridgitserverurl* is the URL of your SMART Bridgit Server.

3. Save it in the server's application directory.

NOTES

- The default directory location is **C:\Program Files\SMART Technologies\SMART Bridgit**.
- For enhanced security, SMART Bridgit Server makes **CustomPage.htm** available only to a web browser. If your custom page includes images or other files, those images and files must be hosted on a different server and referenced with absolute links in the custom page.

Downloading the SMART Bridgit client

To download the SMART Bridgit client

1. Open your web browser.
2. Type the name or the URL of the server you want to connect to in the address bar.

   The *Download SMART Bridgit Software* page appears, including basic instructions and a link for downloading the SMART Bridgit client software.
3. Click **Download Software**, and then run the software.

   The *SMART Bridgit Software* client dialog box appears.

Chapter 6
Using SMART Scheduler

Introduction

The SMART Scheduler option integrates your SMART Bridgit Server with your Microsoft Exchange Server and Microsoft Outlook clients to provide the ability to schedule single or recurring meetings that use SMART Bridgit software.

Installing SMART Scheduler Server software

The SMART Scheduler Server software installation file is included with your SMART Bridgit Server software.

To locate the SMART Scheduler Server software installation file

On the computer where you'll install the software, browse to your SMART Bridgit Server by typing

http://<*yourserver.com*>/SMARTSchedulerServerSetup.exe

in the address bar, where <*yourserver.com*> is the URL of your SMART Bridgit Server.

OR

On your SMART Bridgit Server, browse to

C:\Program Files\SMART Technologies\SMART Bridgit\SMARTSchedulerInstallers

and then copy the **SMARTSchedulerServerSetup.exe** file to the computer you'll install it on.

Installing the software

The ports that the Microsoft Exchange Server or Exchange client use depend upon the versions installed. The network administrator can restrict the Exchange Server's range of allowed TCP ports or can map static TCP ports. Refer to the Microsoft Exchange Server and Outlook clients section in this article http://support.microsoft.com/kb/832017.

To install SMART Scheduler Server software

1. Double-click the **SMARTSchedulerServerSetup.exe** installation file.

   The *SMART Scheduler Server – InstallShield Wizard* welcome screen appears.

   NOTE

   The installer won't run on a computer with Microsoft Outlook.

2. Click **Next** to continue.

   If you don't have Microsoft Collaboration Data Object (CDO) installed on your computer, the *CDO Installation Required* window appears. Go to the *To install Microsoft CDO* procedure below.

   If CDO is installed the *Software License Agreement* appears.

3. Read the agreement. If you accept it, click **Next**.

   NOTE

   If you want to keep a hard copy of the agreement for your records, click **Print**.

   The Destination Folder window appears.

4. Click **Next** to install to the default folder, or click **Change** to specify another folder location.
5. Click **Install**.

   If the installation is successful, the *InstallShield Wizard Completed* window appears.

6. Click **Configure** to set up the mailbox.

   The *SMART Scheduler Server Configuration* window appears.

7. Type your Microsoft exchange logon credentials and Windows authentication information in the fields provided, and then press **OK**.

   The setup application installs the SMART Scheduler Server which runs as a service. The application then verifies that the specified Windows user account has access to the Microsoft Exchange mailbox and that the mailbox is functioning correctly. Any errors are reported to you.

To install Microsoft CDO

1. Select the **Download CDO Installer** check box, and then click **Finish**.
2. Run the downloaded software.

   The *Choose Directory for Extracted Files* dialog box appears.
3. Click **OK** to accept the default location, or type a new directory location.

   The CDO Installation file downloads to the specified directory.
4. Browse to the specified directory, and then double-click the **ExchangeMapiCdo.msi** file.
5. Return to step 3 in the preceding procedure.

Configuring SMART Scheduler Server

After you install SMART Scheduler Server software, you can change the server name and password settings.

To change the SMART Scheduler Server settings

1. Browse to the directory where you installed SMART Scheduler Server, and then double-click the **SMARTSchedulerServerConfig.exe** file.

   The *SMART Scheduler Server Configuration* window opens.
2. Change your Microsoft Exchange logon credentials or Windows authentication information as required.
3. Click **OK** to save the changes.

IMPORTANT

- If you change the name of your SMART Scheduler mailbox, none of the meetings scheduled using the old mailbox name will run.
- After changing the name of the mailbox on the server, you must also change the name of the mailbox in the SMART Scheduler Outlook add-in. For instructions, see *To change the SMART Scheduler settings for all new meetings* in your *SMART Bridgit User Guide* or SMART Bridgit online help.

Upgrading SMART Scheduler Server

To upgrade your SMART Scheduler Server software

1. Upgrade your SMART Bridgit Server.

   See *Upgrading SMART Bridgit Server software* on page 19.

2. Using Windows Control Panel's Add or Remove Programs tool, remove the installed SMART Scheduler Server software.
3. Remove Microsoft Messaging, API and Collaboration Data Objects (CDO).

   NOTE

   The current versions of these components are installed during the procedure.

4. Install the SMART Scheduler Server software.

   See *Installing SMART Scheduler Server software* on page 45 for instructions.

Installing the Outlook client add-in from a command line

To install the add-in from a command line

1. Select **Start > Run**, and then type **cmd** in the *Open* box.
2. Click **OK**.

   The *cmd.exe* window appears.

3. Type **cd** followed by a space, and then type the path to the directory that contains the installer.
4. Execute the installer with any appropriate msi-related parameters.

   NOTE

   For a list of msi-related parameters, **type msiexec /?** and press ENTER.

5. Specify configuration options for the installer.

SERVERNAME	is the address of the SMART Bridgit Server on which your SMART Scheduler meetings will run.
USEPASSWORD	specifies whether or not your SMART Scheduler meetings are password protected. This parameter is either 0 or 1.
MAILBOX	is the SMART Scheduler email address **NOTE** The Microsoft Exchange Server administrator creates this address and the mailbox on the Microsoft Exchange Server at the same time.
USERTF	specifies whether your e-mail messages use rich text formatting (parameter = 1) or plain text formatting (parameter = 0).

EXAMPLE

```
msiexec.exe /i
"C:\<SourceFileLocation>\SMARTSchedulerOutlookAddinSetup.msi" /qn
SERVERNAME=<yourserver.com> USEPASSWORD=1 USERTF=1
MAILBOX="Scheduler Mailbox
```

where <SourceFileLocation> is the path to the .msi file, and <yourserver.com> is the URL of your SMART Bridgit Server.

NOTE

If you have a space in your mailbox name, you must use triple quotations marks before and after the name. If there is no space, quotation marks are not required.

6. Press ENTER.

   The SMART Scheduler Outlook add-in installs.

To upgrade the add-in from a command line

Follow the steps in the *To install the add-in from a command line* procedure above, and then close and restart Outlook.

NOTE

You can leave Outlook running during the upgrade, but you must restart it before the changes will take effect.

Removing SMART Scheduler Outlook add-in

IMPORTANT

Do not remove files for other SMART software products you want to continue to use. If you are unsure, contact SMART Technologies for more information.

Before you can perform the default removal procedure, you must obtain the product code for your version of SMART Scheduler Outlook add-in. You can find your product code in the following table.

SMART Scheduler Outlook add-in product codes

Software version	Product code
4.0.500.0	{916243FB-5A56-4CF1-B75B-6F4236977C12}
4.1.169.0 (Current)	{EF2064B4-D050-4A45-B28A-F8BA573AB0B5}

NOTE

Include the braces when entering a product code value.

To remove the add-in silently

1. Select **Start > Run**, and then type **cmd** in the *Open* box.
2. Click **OK**.

   The *cmd.exe* window appears.
3. Type the following command (including quotation marks), and then press ENTER:

   msiexec.exe /x"*path to .msi***\SMARTSchedulerOutlookAddinSetup.msi" /q**

   OR

   Type the following command, and then press ENTER:

   msiexec.exe /x*{ProductCode}* **/q**

Chapter 6
Bandwidth and scalability

Bandwidth requirements

SMART Bridgit software performs best when you allocate at least 250 Kbps of network bandwidth on your server for each meeting participant, both inbound to, and outbound from, the server.

EXAMPLE

If you have a 1.5 Mbps bandwidth connection to your server, you can support a maximum of six concurrent participants at optimal performance (250 Kbps × 6 = 1,500 Kbps or 1.5 Mbps).

Use the following table to estimate bandwidth requirements for SMART Bridgit software.

SMART Bridgit software resource	Bandwidth required
One shared desktop with a 1024 × 768 resolution	60 Kbps (without video)
One open microphone using the standard quality setting	30 Kbps
One open microphone using the low quality setting	23 Kbps
One open webcam with moderate activity	40 Kbps

TIP

Most shared desktops maintain a bandwidth load of about 60 Kbps. However, the bandwidth required for a shared desktop depends on the display's resolution, the complexity of the content being shared and the frequency at which the content changes. For example, a shared desktop with a photographic desktop background requires more bandwidth than a shared desktop with a plain, solid colored background.

As an extreme example, a shared desktop with a complex photographic background and frequent content changes can peak at 1,800 Kbps, while maintaining an average of 300 Kbps.

Examples of bandwidth requirements

The following table can help you determine typical bandwidth usage for SMART Bridgit meetings.

SMART Bridgit resource	Bandwidth required
One shared desktop with a resolution of 1024 × 768	60 Kbps
Four open microphones using the standard quality setting	30 Kbps × 4 = 120 Kbps
Four open webcams with moderate activity	40 Kbps × 4 = 160 Kbps
Totals:	
Bandwidth required for each participant	60 + 120 Kbps + 160 Kbps = 340 Kbps
Bandwidth required for all 4 participants	340 Kbps × 4 participants = 1,360 Kbps or 1.36 Mbps

Scaling SMART Bridgit

SMART Bridgit software is scalable. A SMART Bridgit Server software maintains its availability, reliability and performance when the number of meeting participants increases on the server.

#	SMART Bridgit software resources		Total computers	NIC speed	Max. client connections
	Outbound from Server		Server		
1	• One shared desktop with a resolution of 1024 × 768 • Four open microphones using the standard quality setting • Four open webcams with moderate activity	340 Mbps	4	1 Gbps	1,000
2	• One shared desktop with a resolution of 1024 × 768 • Four open microphones using the standard quality setting	180 Mbps	4	1 Gbps	1,000
3	• One shared desktop with a resolution of 1024 × 768 • Four open webcams with moderate activity	220 Mbps	4	1 Gbps	1,000
4	• One shared desktop with a resolution of 1024 × 768	60 Mbps	2	100 Mbps	800

Appendix A
Troubleshooting and support

This section includes troubleshooting topics and information on how to get technical support. It also shows how you can use the SMART Bridgit software troubleshooting tool to help optimize your system configuration and resolve problems.

Using the SMART Bridgit troubleshooting tool

SMART Bridgit software has a troubleshooting tool that you can use to determine the cause of issues you may have. If your troubleshooting attempts aren't successful, contact SMART Technical Support for further assistance. See *Customer support* on page 72.

To open the troubleshooting tool

1. Open SMART Bridgit client software and create a test meeting.

   The SMART Bridgit lobby screen appears.

2. Select **Menu > About SMART Bridgit**.

   The *About SMART Bridgit Software* dialog box appears.

3. Click the **Technical Support** tab, and then click **Troubleshooting**.

   The *Troubleshooting* tool opens.

The features of the *Troubleshooting* tool are described in the following sections:

- *Screen capture technology* on next page
- *Sharing color quality* on page 57
- *Audio* on page 57
- *Connection* on page 58
- *Ink* on page 58

Screen capture technology

This section provides an overview of the various technologies that SMART Bridgit software uses when you share your desktop during a meeting. Use the options outlined in this section to resolve issues with sharing speed and image quality.

SMART Bridgit software uses the following three types of technology to share screens during a meeting.

Mirror drivers

SMART Bridgit software attempts to use this sharing method first because it offers the best performance. It requires an installation which is automatically done if you have administrator rights and on Windows XP. One disadvantage of this technology is that it doesn't capture some parts of the shared screen, such as command prompt windows and some 3D content.

NOTE

Mirror drivers won't run as intended if you are running Windows Vista or Windows 7 operating systems.

Redraw hooks

SMART Bridgit software reverts to using redraw hooks if it can't use mirror drivers. Redraw hooks are automatically downloaded from the server when needed and performs a screen capture every time something changes on the screen.

NOTE

This technology is unavailable in 64-bit Windows 7 operating systems.

Four times per second capture

If SMART Bridgit software can't use either of the above technologies, it captures the shared screen four times per second, compresses and then sends the image to the recipient. This method offers the lowest performance, but it uses the lowest bandwidth.

Information fields and options

Field/option	Description	When to use/why it's important
Presenting status	Displays either *Not currently presenting* or the method of screen capture in use: • *Capturing screen 4 times per second (display 0)* • *Using RedrawHooks.dll (display 0)* • *Using mirror driver (display 0)*	
Hardware acceleration status	Indicates if hardware acceleration is on or off	To increase performance, turn hardware acceleration off.
Mirror driver availability	• *available* – the mirror driver is installed • *unavailable* – the mirror driver couldn't be installed • *disable by OS* – you are running either Windows Vista or Windows 7, which don't allow the mirror driver to run as intended	When video mirroring is active, each time the system draws to the primary video device at a location inside the mirrored area, a copy of the draw operation is executed on the mirrored video device in real time.
Enable redraw hooks	Select to share using redraw hooks	If your pointer is flickering, you might want to disable this option. **NOTES** • This option is unavailable in 64-bit Windows 7 operating system. • You should enabled this option only for testing purposes. If both redraw hooks and the mirror driver are disabled, screen updates are limited to four times per second.
Enable mirror driver	Select to share using mirror driver	If your shared applications aren't being captured correctly, you might want to disable this option. Otherwise, leave this option enabled.

Sharing color quality

Use the following options to adjust the quality of shared color images and video.

Field	Description	When to use/why it's important
Share in full color	Select to share in the highest color depth available (usually 24 or 32 bits per pixel) Clear to share in 256 color mode	Clearing this option causes bandwidth usage to drop, but it increases the load on the presenter's computer. The image quality of the shared screen is reduced.
Optimize desktop for sharing	Slows down the frequency of screen captures and removes your desktop background to decrease the amount of bandwidth used	This option isn't selected by default. You can use it to improve sharing when bandwidth is limited. This option is valid only if mirror drivers and redraw hooks are enabled

Audio

Use the following options to adjust your audio settings.

Option	Description	When to use/why it's important
Enable echo cancellation	Enables echo cancellation for VoIP audio	Disable this option only if the computer's power is very limited, because it takes slightly more processing power to have this enabled. Some hardware devices contain echo cancellation that SMART Bridgit's software-based echo cancellation can interfere with. Disable this option if you are having problems with echo cancellation.
Enable AGC	Enables automatic gain control (AGC)	AGC adjusts the volume of your microphone to a reasonable level in case you have your volume set too high. Disable this option if you prefer full control over the volume.

Connection

This section provides server connection status details, as well as information on ports and proxy connections.

Field	Description	When to use/why it's important
Starting server	Displays the server name that you typed when you installed and configured SMART Bridgit Server for the first time	Status only To change which server is in use, double-click the **SMART Bridgit client** icon on your desktop, and then click .
Fastest server	Displays the server in the Global Server Network (GSN) that you're connected to. SMART Bridgit software selected this server due to its speed of connection	Status only SMART Bridgit software detects this server automatically
TCP port	Displays the port your system is using for screen sharing, video conferencing and chat.	Status only
UDP port	The port used for VoIP audio	Status only
Proxy connection	Shows if audio is going through a proxy server	Status only
Pick fastest server	Select to enable the automatic selection of the fastest server	If you clear this option, your computer connects to the server you specified when you started the meeting, regardless of whether there is a faster server available in the same GSN.

Ink

Clear this check box to disable SMART Bridgit's remote and local ink ability. This is useful if you want to write on a SMART Board interactive whiteboard instead of using SMART Bridgit software's ink capability.

Monitoring a meeting's performance – presenter

When you present in a meeting, an hourglass  could appear on the participant list button while SMART Bridgit software sends updates to the other participants. The hourglass disappears once all the participants can see your desktop.

If the hourglass remains, one or more participants are lagging behind the meeting.

To view the meeting performance for each participant

Click the participant list button  .

The participant list appears. The delay interval (in seconds) appears to the right of the name of the participant who's lagging. The chat icon is also covered by an hourglass.

If participants continue to lag behind the meeting, you can take steps to improve the meeting's performance.

Improving performance

If you're presenting a meeting and you find that some participants are seeing events on your desktop several seconds after they happen, you can try a number of things:

- Use a solid-color desktop background rather than a complex wallpaper.
- Disable animations or fades in list boxes, windows, menus, tool tips and so on.
- Stop sharing your webcam.
- Optimize your desktop for sharing. Select **Menu > About SMART Bridgit > Technical Support > Troubleshooting**, select the **Optimize desktop for sharing** check box, and then click **OK**.
- Reduce the screen resolution in your operating system's display settings or share only a portion of the desktop.

NOTES

- The procedure for reducing the desktop resolution varies between versions of Windows operating system. However, the option is always available in **Control Panel > Display > Settings**.

- The procedure for reducing the desktop resolution varies between versions of the Mac operating system software. However, the option is always available in the **Apple ( ) menu > System Preferences > Displays**.
- If you're the meeting owner, you can choose an audio optimization setting that could improve performance.

If none of these options helps significantly, contact your network administrator and report that you're experiencing slow network performance.

Monitoring a meeting's performance – participant

When you view the shared desktop, the participant list button turns yellow  if your computer is 5 to 10 seconds behind the presenter's. If your computer is more than 10 seconds behind the presenter's, the participant list button turns red  .

To view the meeting performance for your computer

Click the participant list button.

The delay interval (in seconds) appears to the right of your name.

If your computer continues to lag behind the meeting, you and the presenter can take steps to improve performance.

Improving performance

If you're participating in a meeting and you see events on the presenter's desktop several seconds after they happen, you can try a number of things:

- Hide the webcam window.
- Stop sharing your webcam.
- Stop using audio and use text messaging (chat) instead.
- Avoid using the *Fit presenter's desktop to window* option if you're using a less powerful computer. If your desktop is the same size or larger than the presenter's, you can view the shared desktop in Full Screen mode without using scroll bars.

  NOTE

  This can improve performance for slow computers, but not for slow networks.

- Reduce the level of Windows hardware acceleration by browsing to **Control Panel > Display > Settings > Advanced**. Click the **Troubleshoot** tab and drag the level of *Hardware acceleration* toward **None**. Test SMART Bridgit software's performance and reduce the hardware acceleration more if necessary.

  NOTE

  This can improve performance for slow computers, but not for slow networks.

If none of these options helps significantly, contact your network administrator and report that you're experiencing slow network performance.

Minimizing network latency

This topic details steps you can take if your client's program is slow or unresponsive during a meeting. Latency, the time lag between sending a message to a remote computer and receiving a response, can cause noticeable performance issues in SMART Bridgit software.

Symptoms

- Connecting to the SMART Bridgit Server takes a long time.
- The screen updates slowly when you view a shared desktop.
- The program doesn't respond to your mouse or keyboard when you use remote control.

Solution

Try the following to troubleshoot network latency issues:

- Verify that you're using TCP and UDP network protocols. See *Verify communication protocol* on next page.
- Check if you're connecting through a proxy server. See *SMART Bridgit and firewalls* on page 11.
- Check your network bandwidth. See *Examples of bandwidth requirements* on page 52.
- Measure latency and packet loss rate. See *Measuring latency and packet loss* on next page.
- Other suggestions below.

Other Suggestions

Because you have limited control over the network outside of your LAN, you have limited control over network latency issues. However, you might be able to improve the connection between your LAN and your Internet Service Provider (ISP).

You can also try these options:

- Read the specifications of your server and client computer Ethernet card throughput rates. Also, check your network device rates. If they're low, upgrade the hardware.
- Verify that your Internet transmit and receive speeds match the speed guaranteed by your ISP.

Verify communication protocol

SMART Bridgit software uses three types of network protocols:

- TCP for data and video
- UDP for VoIP audio
- HTTP if a client is unable to connect to the server using TCP

Communications using TCP and UDP have lower network delays than those using HTTP protocol, and using them helps to prevent latency issues.

Use SMART Bridgit software's troubleshooting tool to determine the network protocol you're using. See *Using the SMART Bridgit troubleshooting tool* on page 54.

Ensure that values appear in the *TCP Port* and *UDP Port* fields. If these fields have *N/A* in them, or if the *Proxy Connection* option is selected, open the TCP and UDP ports using SMART Bridgit Administration Tools on the SMART Bridgit server. See *Administering the server software* on page 37. See *SMART Bridgit and firewalls* on page 11 for information about configuring firewalls and proxy servers.

Checking for firewalls

To determine if the client is behind a firewall

1. On the client computer, open the SMART Bridgit troubleshooting tool. See *Using the SMART Bridgit troubleshooting tool* on page 54.

   The *Connection* area displays the ports and protocols the client computer is using to communicate with the server. If a client is communicating through a proxy server or if the client's UDP and secondary TCP ports are blocked by a firewall, the *Proxy Connection* check box is selected.

2. Enable the TCP and UDP ports using SMART Bridgit Administration Tools. See *Administering the server software* on page 37.

Measuring latency and packet loss

Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. Packet loss rates depend on factors including bandwidth, communication path reliability and router buffer size. When packets are lost, latency increases as the network devices try to recover the information.

Microsoft Windows operating systems include the PathPing tool to measure packet loss rate and latency. PathPing sends packets to each router on the path to a destination for an interval, and then it computes results based on the packets returned from each hop. Since PathPing shows how much packet loss is seen for any router or link, you can determine which routers or links are causing network problems. For more information on using PathPing to determine network latency and packet loss, see the Microsoft website.

Troubleshooting SMART Bridgit Server connections

This section help you resolve connection problems that are caused by your SMART Bridgit Server software or your network environment.

SMART Bridgit Server connection problems can result from an incorrect domain name server (DNS) configuration for routing to the SMART Bridgit Server or from the server computer's domain and IP address and port forwarding settings on the network servers, routers or firewalls.

Symptoms

- When a SMART Bridgit client connects to a SMART Bridgit Server that's running on the same computer, a *The <servername.com> server is not available. Try again later or select another server* error message appears.

  This error message can also appear when a client's software causes the issue.

  See Unable to Connect to the Bridgit Software Server (Client Side) for more information when your SMART Bridgit client software causes the issue.

- An error message appears when you connect to a SMART Bridgit Server from an Internet browser.

Solution

Verify that you're using the latest version of SMART Bridgit Server software. See *Upgrading SMART Bridgit Server software* on page 19. If the software upgrade doesn't resolve the issue, try these procedures:

- *Verifying the network's DNS configuration* on next page
- *Verifying SMART Bridgit Server configuration* on next page
- *Manually updating the Windows registry* on page 67

- *Configuring the client's Hosts file* on page 67
- *Verify port forwarding and firewall configuration* on page 68

Verifying the network's DNS configuration

Verify that the network's DNS is configured correctly so the IP address resolved by the network's DNS is the same as the SMART Bridgit Server's IP address.

To verify that the DNS is configured correctly

1. Open a Command Prompt window on the SMART Bridgit Server, type **ipconfig** and then press ENTER.

   The server's network configuration information appears, including its IP address.

2. Type **nslookup** and then press ENTER.

   OR

   Type **ping <ServerDomainName>** using the domain name for the SMART Bridgit Server, and then press ENTER.

   The IP address that the network's DNS resolves appears.

3. Compare the IP addresses.

NOTES

- If the IP addresses are the same, the network's DNS is configured correctly. See *Troubleshooting SMART Bridgit Server connections* on previous page.
- If the IP addresses are different, the network's DNS isn't configured correctly.

  OR

  The SMART Bridgit Server is located on a LAN or virtual LAN but the domain name resolves to a router on a different LAN, and your network's router doesn't allow loop-back communication. See *Configuring the client's Hosts file* on page 67 to add the domain name to the Windows HOSTS file.

Verifying SMART Bridgit Server configuration

Verify the domain name or IP address, and then configure the SMART Bridgit Server software.

To verify the domain name or IP address

1. Open the SMART Bridgit Administration Tools **Setup** tab. See *Configuring the server software* on page 23.

NOTE

If the *SMART Bridgit Software Administration Tools* window doesn't appear, see *Manually updating the Windows registry* on next page to enter the domain name or IP address manually in the Windows registry.

2. Compare the domain name or IP address in the *Registered Domain Name* box to the domain name or IP address from the previous procedure.
3. If the domain names or IP addresses are the same, but clients are still unable to connect to the server, see *Verifying the network's DNS configuration* on previous page to verify the port forwarding and firewall configurations.

   If the domain names or IP addresses are different, type your SMART Bridgit Server's domain name or IP address in the *Registered Domain Name* box, and then click **Apply**.

   The *Restart Services* dialog box appears.
4. Click **Close Administrative Tools**.

   The *SMART Bridgit Software Administration Tools* window closes.
5. Select **Start > Control Panel > Administrative Tools > Services**.

   The *Services* window appears.
6. Right-click **Bridgit Master Service**, and then select **Restart**.

   The *Bridgit Master Service* restarts.

NOTE

Other SMART Bridgit clients will disconnect from the SMART Bridgit Server when you complete this procedure.

7. Right-click **Bridgit Conference Service**, and then select **Restart**.

   The *Bridgit Conference Service* starts.

NOTES

If clients are still unable to connect to the server, see *Verifying the network's DNS configuration* on previous page to verify the port forwarding and firewall configurations.

If you're unable to use SMART Bridgit Software Administration Tools, see *Manually updating the Windows registry* on next page to enter the domain name or IP address manually in the Windows registry.

Manually updating the Windows registry

CAUTION

Use caution when you open the Windows registry editor. If you incorrectly modify the Windows registry, you can damage your computer's operating system. Back up your registry before performing the following procedure.

To enter the domain name or IP address in the Windows registry

1. Start the Windows registry editor and browse to **HKEY_LOCAL_MACHINE\SOFTWARE\SMART Technologies Inc.\Bridgit Data-conferencingSoftware\3.0**.
2. Type your SMART Bridgit Server's domain name or IP address in the Value data fields for both *MasterServerDomainName* and *ConferenceServerDomainName*.
3. Exit the Windows registry editor.
4. Select **Start > Control Panel > Administrative Tools > Services**.

   The *Services* window appears.
5. Right-click **Bridgit Master Service**, and then click **Restart**.

   The *Bridgit Master Service* restarts.

   NOTE

   Other clients will disconnect from the SMART Bridgit Server when you complete this procedure.
6. Right-click **Bridgit Conference Service**, and then click **Restart**.

   The *Bridgit Conference Service* restarts.

If clients are still unable to connect to the server, see *Verify port forwarding and firewall configuration* on next page to verify the port forwarding and firewall configurations.

If the domain name resolves to your router's public IP address, and your router doesn't allow loop-back communication, see *Configuring the client's Hosts file* below to add the domain name to the Windows HOSTS file.

Configuring the client's Hosts file

If the domain name resolves to your router's public IP address, and your router doesn't allow loop-back communication, follow this procedure to add the domain name to the Windows HOSTS file.

To add the domain name to the Windows HOSTS file

1. On the SMART Bridgit client computer, browse to **Windows\system32\drivers\etc**, and then open the **HOSTS** file.
2. Add an entry so that the domain name you're using to connect to the SMART Bridgit Server resolves to the server's IP address.

   This procedure is effective for SMART Bridgit clients on this computer only. Other clients can use a direct IP address or the IP address resolved from the domain name by your network's DNS server.

3. See *Troubleshooting SMART Bridgit Server connections* on page 64 to configure the SMART Bridgit Server software.

Verify port forwarding and firewall configuration

If clients are still unable to connect to the server, verify that port forwarding on the network routers are configured to give clients access to the server, and that firewalls protecting the SMART Bridgit Server allow clients to access the server. See *Verify communication protocol* on page 63 and *Checking for firewalls* on page 63.

If the problems persist, the SMART Bridgit client (not the server) could be the cause. See Unable to connect to Bridgit Software Server (Client Side).

Troubleshooting Administration Tool connections

Symptom

When you install SMART Bridgit software with IP binding, SMART Bridgit Administration Tools doesn't connect to the SMART Bridgit Server.

Solution

Use one of the following procedures to connect SMART Bridgit Administration Tools to the SMART Bridgit Server:

- *Directing IP traffic to the SMART Bridgit Server* below (recommended solution)
- *Moving the server's IP address to the top of the IP Settings list* on next page
- *Stopping applications using the server's IP port* on next page

Directing IP traffic to the SMART Bridgit Server

To direct IP traffic to the IP address bound to the SMART Bridgit Server

1. Open the **cmd.exe** window, type **hostname**, and then press ENTER.

   Note the computer name that appears.

2. If you don't know the IP address that was entered when the server was installed, open SMART Bridgit Administration Tools, and then select the **Setup** tab.

   Note the server's IP address in the *IPv4 Address* drop-down list.

3. Browse to **C:\WINDOWS\system32\drivers\etc** and then open the **HOSTS** file.

4. Type your IP address and hostname on a new line at the bottom of the file

   EXAMPLE

   192.168.0.8 bridgitserver.

5. Save the **HOSTS** file.

   You can now open SMART Bridgit Administration Tools and configure the SMART Bridgit Server software. See *Configuring the server software* on page 23.

IMPORTANT

Because other applications can use the hostname, you should remove the line you added in step 4 after you configure the SMART Bridgit Server. You can remove the line or comment it out (by inserting a "#" character at the beginning of the line).

Moving the server's IP address to the top of the IP Settings list

To move the server's IP address to the top of the IP settings list

1. If you don't know the IP address that was entered when the server was installed, open SMART Bridgit Administration Tools, and then select the **Setup** tab.

   Note the server's IP address in the *IPv4 Address* drop-down list.
2. Open the **Control Panel** and double-click **Network Connections**.
3. Right-click the network device that SMART Bridgit software is bound to, and then select **Properties**.
4. Select **Internet Protocol (TCP/IP)** in the *This connection uses the following items* list.
5. Click **Properties**.
6. Select the **General** tab, and then click **Advanced**.

   The Advanced TCP/IP Settings dialog box appears.
7. Select the **IP Settings** tab.
8. Remove all the IP addresses above the SMART Bridgit Server's address.
9. Replace the addresses below the server's address.
10. Restart the server.

Stopping applications using the server's IP port

TIP

Perform this procedure when it won't affect other users.

To make SMART Bridgit's primary port available

1. Stop applications that use to SMART Bridgit software's primary port.
2. Open SMART Bridgit Administration Tools and configure SMART Bridgit software.

3. Close SMART Bridgit Administration Tools.
4. Start the applications that you stopped in step 1.

Troubleshooting SMART Scheduler

After the you install and configure SMART Scheduler, it runs silently as a Windows service. It doesn't have a user interface when running, and it doesn't create a log file by default. Follow these steps to gather more information when troubleshooting.

To display a SMART Scheduler Server log

1. Open the **Command Prompt** window, and then navigate to the *SMART Scheduler Server* folder.

   The default folder is **C:\Program Files\SMART Technologies\SMART Scheduler Server**.

2. Type **net stop SMART Scheduler Server**, and then press ENTER.

   The SMART Scheduler Server Windows service stops.

3. Type **SMARTSchedulerServer.exe**, and then press ENTER.

   The SMART Scheduler Server service starts. A series of text lines appear.

4. Look for and record any error information in the log that can help you identify a problem.
5. Press CTRL-C.

   The server stops and the command prompt returns.

6. Type **net start SMART Scheduler Server**, and then press ENTER.

   The SMART Scheduler Server service starts.

To create a server log file

1. Repeat the first 3 steps of the above procedure, substituting **SMARTSchedulerServer.exe>>log.txt** for the command in step 3.

   Instead of appearing on screen, the log information re-directs to the **log.txt** file.

2. After a few minutes, press CTRL-C.

   The server stops and the command prompt returns.

3. Type **net start SMART Scheduler Server**, and then press ENTER.

   The SMART Scheduler Server service starts.

4. Locate the **log.txt** file, and then open it in a text editor.

Customer support

Online information and support

Visit www.smarttech.com/support to view and download user's guides, how-to and troubleshooting articles, software and more.

Training

Visit www.smarttech.com/trainingcenter for training materials and information about our training services.

Technical support

If you experience difficulty with your SMART product, please contact your local reseller before contacting SMART Support. Your local reseller can resolve most issues without delay.

NOTE

To locate your local reseller, visit www.smarttech.com/wheretobuy.

All SMART products include online, telephone, fax and e-mail support:

Online	www.smarttech.com/contactsupport
Telephone	+1.403.228.5940 or Toll Free 1.866.518.6791 (U.S./Canada) (Monday to Friday, 5 a.m. – 6 p.m. Mountain Time)
Fax	+1.403.806.1256
E-mail	support@smarttech.com

General inquiries

Address	SMART Technologies 3636 Research Road NW Calgary, AB T2L 1Y1 CANADA
Switchboard	+1.403.228.5940 or Toll Free 1.866.518.6791 (U.S./Canada)
Fax	+1.403.228.2500
E-mail	info@smarttech.com

Registration

To help us serve you, register online at www.smarttech.com/registration.

Index

SMART™

Toll Free 1.866.518.6791 (U.S./Canada)
or +1.403.228.5940
www.smarttech.com