Bridgit® 4.6

Installation and system administrator's guide

Contents

Chapter 1: Welcome 1

Bridgit server software 1
Bridgit client software 2
SMART Scheduler 3
SMART Scheduler Outlook add-in 3

Chapter 2: Installing Bridgit software 5

Preparing for installation 6
Installing Bridgit server software 14

Chapter 3: Configuring the server software 23

Setting passwords 23
Changing Bridgit server setup options 26
Setting meeting options 26

Chapter 4: Managing a GSN 31

Bridgit servers in a GSN 31
Bridgit clients in a GSN 35

Chapter 5: Administering the server software 37

Viewing status information 37
Managing servers and meetings 40
Controlling Bridgit software services 41
Customizing the Bridgit server's web page 42
Downloading the Bridgit client 42

Chapter 6: Using SMART Scheduler 43

Installing SMART Scheduler server software 43
Configuring SMART Scheduler server 45
Upgrading SMART Scheduler server 46
Installing the SMART Scheduler Outlook add-in 46
Installing the SMART Scheduler Outlook add-in from a command line 48
Removing the SMART Scheduler Outlook add-in 50

Chapter 7: Bandwidth and scalability 53

Bandwidth requirements 53
Examples of bandwidth requirements 54
Scaling Bridgit 54

Appendix A: Troubleshooting 55

Using the Bridgit troubleshooting tool 56

Monitoring a meeting's performance – presenter 60

Monitoring a meeting's performance – participant 61

Minimizing network latency 62

Troubleshooting Bridgit server connections 64

Troubleshooting administration tool connections 68

Troubleshooting SMART Scheduler 71

Index 73

Chapter 1
Welcome

Bridgit server software 1

SMART Bridgit Administration Tools 1

Global Server Network (GSN) option 2

Bridgit client software 2

Bridgit software and SMART Meeting Pro software 3

Bridgit software and SMART Notebook software 3

SMART Scheduler 3

SMART Scheduler Outlook add-in 3

Bridgit® conferencing 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. 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 Bridgit client software, refer to its online Help.

Bridgit server software

Bridgit server software passes data between clients and authenticates client connections using optionally implemented passwords.

SMART Bridgit Administration Tools

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

When you install Bridgit server software, a shortcut to SMART Bridgit Administration Tools appears on the server’s desktop.

Global Server Network (GSN) option

The Bridgit Global Server Network (GSN) is a network of 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.

Bridgit client software

Bridgit client software transmits meeting data to and from the Bridgit server and displays it to the meeting participants. It is integrated with SMART Meeting Pro™ software or SMART Notebook™ collaborative learning software.

Features and highlights of Bridgit client software include the following:

- 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 Voice over Internet Protocol (VoIP) technology

Bridgit software and SMART Meeting Pro software

Bridgit software is integrated with SMART Meeting Pro software and SMART Product Drivers to provide screen sharing and simultaneous viewing of multiple shared displays, VoIP and webcam functionality. Bridgit works best with the following versions of SMART Meeting Pro software:

- SMART Meeting Pro 4.x and 3.1 software
- SMART Meeting Pro Premium 2.3 software
- SMART Meeting Pro PE (Personal Edition) software

For detailed information on this functionality, refer to SMART Meeting Pro software documentation.

Bridgit software and SMART Notebook software

Bridgit software is integrated with SMART Notebook software to provide instant conferencing capabilities. Bridgit works best with SMART Notebook 11.x and 10.8 software. For detailed information on this functionality, refer to SMART Notebook software documentation.

SMART Scheduler

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

Chapter 2
Installing Bridgit software

Preparing for installation 6

Computer requirements 6

Bridgit server software requirements 6

Bridgit client software requirements 7

SMART Scheduler requirements 8

SMART Scheduler Outlook add-in requirements 8

Software licensing 8

Supported virtualization environment 8

Access requirements 8

Network administration experience 9

Access to servers and infrastructure components on your network 9

Administrator rights 10

Security 10

Passwords 10

Domain names 11

Registered domain name 11

IPv4/IPv6 addresses 12

Bridgit and firewalls 12

Configuring firewalls 13

Configuring proxy servers 13

Installing Bridgit server software 14

Installing the server software 15

Upgrading Bridgit server software 19

Licensing Bridgit server software 19

Activating using the SMART activation server 19

Activating your license manually 20

Removing server or user licenses 21

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

Preparing for installation

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 53.
- Your system performs best if you use a high performance server or a dedicated server with no other applications installed.

Computer requirements

Bridgit server software requirements

Each server must meet the following minimum requirements:

- 3.1 GHz quad-core processor
- 4 GB of RAM
- Windows Server® 2003, 2008 R2 or 2012 (32-bit or 64-bit) operating system
- 250 Mbps network interface card (NIC) that supports TCP/IP

NOTES

- 1 Gbps NIC is recommended.
- Increased hardware capabilities improve overall meeting performance.
- The recommended maximum number of open microphones with this configuration is 100.
- The recommended maximum number of shared webcams with this configuration is 100.

Bridgit client software requirements

Bridgit client software allows meeting participants to interact and collaborate directly with each other and supports up to nine shared webcams and nine open microphones per meeting. In order for you to share audio and video with other meeting participants, your computer must meet the following minimum requirements.

Requirements	Windows operating systems	Mac OS X operating system software
Operating systems	• Windows XP SP3 • Windows 7 • Windows 8	• Mac OS X 10.6 (Snow Leopard) • Mac OS X 10.7 (Lion) • Mac OS X 10.8 (Mountain Lion)
Client (without VoIP audio or webcam video)	• 2 GHz processor • 1 GB of RAM • Broadband Internet connection	• 2.0 GHz Intel® processor • 1 GB of RAM • Broadband Internet connection
Client (with VoIP audio or webcam video)	• 2.33 GHz dual-core processor • 2 GB of RAM • Broadband Internet connection	• 2.4 GHz Intel dual-core processor • 2 GB of RAM • Broadband Internet connection
Proxy server	• If you're using Firefox®, Internet Explorer® 6 or Opera Internet browsers, configure the browser's proxy settings and the operating system's proxy settings with the server's proxy settings. • For all other browsers, configure the operating system's proxy settings with the server's proxy settings.	Configure the operating system's proxy settings with the server's proxy settings.
Webcam	• Compatibility with DirectShow® 9 driver • Supports 24-bit RGB color	• Internal webcam or iSight camera • QuickTime application program
Audio	• Sound card • Speakers or headphones • Microphone	• Sound card • Speakers or headphones • Microphone

NOTE

You can download or update SMART software from smarttech.com/downloads.

SMART Scheduler requirements

- 2 GHz processor
- 1 GB of RAM
- Windows Server 2003, 2008 R2 or 2012 (32-bit or 64-bit) operating system
- Microsoft Exchange Server 2007 SP1, 2010, 2010 SP1, 2010 SP2 or 2013
- Microsoft .NET Framework 4 Client Profile
- 10 Mbps NIC that supports TCP/IP
- Network connection to your Microsoft Exchange Server and Bridgit server
- You must have Bridgit server installed and running on either a separate computer (recommended) or, if required, on the same computer where you'll install the SMART Scheduler server.

SMART Scheduler Outlook add-in requirements

- 2 GHz processor
- 1 GB of RAM
- Microsoft Outlook 2007, 2010 or 2013
- Network connection to your Microsoft Exchange Server and Bridgit server

Software licensing

After the 60-day free evaluation period, users can no longer conduct meetings on the server and must purchase and activate a software license.

To continue using the software after the evaluation period, you need to purchase a license before the evaluation period expires.

When you purchase a license a Bridgit software license, you're purchasing a server license for up to 500 concurrent users and you receive one product key.

Supported virtualization environment

Bridgit software supports VMware® vSphere™ Hypervisor 4.1.

Access requirements

Before you can successfully install and use a Bridgit server software, you must correctly configure your network environment. 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

Bridgit server software functions in a complex network environment. Do not attempt to install or configure the 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.

Network configuration	Type of access
Private local area network (LAN) use	If your 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 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 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 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.

Network configuration	Type of access
Use of SMART Scheduler	If you want to use the 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 install and configure Bridgit server software, 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 Bridgit server computer.

Security

Bridgit software complies with Secure Sockets 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 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.

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. Bridgit software for Mac OS X operating system software also implements 256-bit SSL encryption.

Passwords

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

IMPORTANT

If you assign a server access password, SMART recommends that you also assign a meeting creation password.

Password type	Description
Server access password	An optional password that a meeting participant uses when connecting to a Bridgit server. The server access password allows the participant 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 meeting creation password.
Meeting creation password	An optional password that a meeting owner uses to create a meeting on the Bridgit server. Users who type the meeting creation password can also see the list of active meetings on the server. NOTE After you install Bridgit server software, you can use SMART Bridgit Administration Tools to create additional server access and meeting creation passwords.
Meeting password	A password that a meeting participant uses to join a meeting. The meeting creator sets this password.
Administrator access password	A password that server administrators creates 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 Bridgit server is accessible to clients connecting via the Internet. If you use a private domain name, your 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 Bridgit server GSN.

IPv4/IPv6 addresses

During the installation process, Bridgit software detects the IP addresses bound to the servers' network interface cards. You can choose to bind 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. Select **Start > Run** on the computer where you'll install the Bridgit server software.
2. Type **cmd**, and then press ENTER.

   A *Command Prompt* dialog box 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 Bridgit server to determine the IP address that the network's DNS returns.
5. Compare this IP address to the 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 Bridgit server.
- The ping can fail for reasons unrelated to the public domain name and still resolve to a computer name or IP address.

Bridgit and firewalls

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 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 Bridgit servers with only HTTP connectivity.

Configuring firewalls

You can install your Bridgit server software 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 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 Bridgit server to display the web page from which the users download the Bridgit client. • Initial connection to the Bridgit server from the Bridgit client when looking for meetings to join or when creating new meetings. • Fallback communication method for all other Bridgit functions when other ports are unavailable (lower performance than other ports).
80	TCP/Bridgit	• Primary port for data, screen viewing and webcam traffic for Bridgit meetings. • If this port is limited to only HTTP, Bridgit software attempts to use the secondary port (9933) for this traffic. • If this port is blocked or unavailable, Bridgit software uses HTTP on the primary port, which can affect performance.
9933	TCP/Bridgit	Secondary port for data, screen viewing and webcam traffic for Bridgit meetings.
9901 to 9920	UDP/Bridgit	• Primary port range for VoIP audio traffic for Bridgit meetings. • If these ports are blocked or unavailable, Bridgit software falls to TCP or HTTP on the primary or secondary port, which can negatively affect performance.

Configuring proxy servers

You can configure your Bridgit server software to work with any proxy server that adheres to the RFC 2068 HTTP standard. If you install your 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

Although 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 Bridgit server.

Installing Bridgit server software

When you install Bridgit server software, consider the following points:

- If you install Bridgit server software on a dedicated server with one network interface card (NIC), select **All** (default) to bind 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 Bridgit to the internal NIC. Use port forwarding to redirect external requests to the external NIC.
- If you install 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 Bridgit in either of the following ways:
  - 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 to Bridgit client (for example, **server.company.com**).

IMPORTANT

Before you start SMART Bridgit Administration Tools, you might need to temporarily disable the other services listening on the same port as Bridgit services. When you finish configuring Bridgit server software, restart the services you disabled.

Installing the server software

To install Bridgit server software

1. Go to smarttech.com/downloads.
2. Download Bridgit software and run the **ConferenceServicesSetup.exe** file.

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

   The *License Agreement* page appears.
4. Read the agreement. If you accept, 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* dialog box appears.
5. Click **Next** to use the default destination folder.

   OR

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

   The *Server Address Configuration* page appears.

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

Option	Description
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* box. **NOTES** ○ If you select all addresses, Bridgit software clients can use any IP address assigned to the server computer to contact the 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, Bridgit software has automatically detected that you don't have more than one IP address to choose from.
Public domain name	Each Bridgit server requires a fully qualified domain name (for example, conference.company.com:88 or server.company.com:88) or a host name (for LAN access only). **IMPORTANT** If you use the computer's network host name as the domain name, the server is accessible only from within the LAN. Internet users do not have access to the server. Do not mix fully qualified domain names and computer host names within the same Bridgit GSN.

8. Click **Next**.

   The *Server Port Configuration* page appears.

9. Configure the ports using the following options:

Option	Description
Primary TCP port	By default, Bridgit software uses port 80 as its primary port. If your server is running another application that uses port 80, you must assign 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, 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 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, 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 Bridgit meetings. You must open a range of UDP ports (9901 to 9920) on your firewall to use this feature. **NOTES** ○ If you configure 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 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, Bridgit software opens 20 UDP ports to allow 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.

10. Click **Next**.

    The *Server Password Security* page appears.

11. Optionally, create the following passwords for server password security:

Password	Description
Server access	An optional password that a meeting participant uses when connecting to a Bridgit server. The server access password allows the participant 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 meeting creation password.
Meeting creation	An optional password that a meeting owner uses to create a meeting on the Bridgit server. Users who type the meeting creation password can also see the list of active meetings on the server. **NOTE** After you install Bridgit server software, you can use SMART Bridgit Administration Tools to create additional server access and meeting creation passwords.

12. Click **Next**.

    The *Ready to Install* page appears.

13. Click **Back** to change the settings.

    OR

    Click **Install** to begin the installation.

    The *Installing SMART Bridgit* dialog box appears and the installation validates. The setup status appears on the green status bar.

14. Click **Finish** in the *SMART Bridgit – InstallShield Wizard* 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, to install user licenses, to change the server settings and to view status information. For more information on SMART Bridgit Administration Tools, click **Help** to open the *Bridgit Administrator's Help*.

IMPORTANT

The Bridgit software installation includes a 60-day evaluation license for the server and up to 500 concurrent users. See *Licensing Bridgit server software* on the next page for information on installing and activating server and user licenses.

Upgrading Bridgit server software

To upgrade your Bridgit server software

1. Go to smarttech.com/downloads.
2. Download Bridgit software and run the **ConferenceServicesSetup.exe** file.

   A message appears asking if you want to upgrade or repair the program components from the previous version, and warning you that all open meetings will be closed during the upgrade.
3. Click **Yes** to close an open meeting and continue with the upgrade.

   The *SMART Bridgit – InstallShield* wizard appears. Follow the procedure in *Installing the server software* on page 15.

   OR

   Click **No**, and then end the meeting using the on-screen instructions.

Licensing Bridgit server software

Once your 60-day trial expires, you must activate your server and user licenses to continue using Bridgit software.

NOTES

- If you upgrade from version 3 to version 4, your version 3 licenses continue to work with version 4.
- If you upgrade from a version earlier than 3.1, the software's VoIP audio features aren't available.

Activating using the SMART activation server

To activate your license using the SMART activation server

1. Double-click the **SMART Bridgit Administration Tools** icon on the server's desktop, and then click the **Licensing** tab.
2. Select the server you want to activate from the *Server* list.
3. Click **Install Server License**.

   The *Install Server License* dialog box opens.
4. Type your product key in the *Product Key* box, and then click **OK**.

After you activate the product key, your server software information appears in the *Licenses for selected server* table, the related status changes to *Activated*, and you have 500 installed licenses.

IMPORTANT

When you purchase the Bridgit 4.6 software service license, you're purchasing a server license and one product key that activates the server for up to 500 concurrent users.

Activating your license manually

To activate your license by e-mail

1. Double-click the **SMART Bridgit Administration Tools** icon on the server's desktop, and then click the **Licensing** tab.
2. Right-click the license you want to activate in the *Licenses for selected server* table, and then select **Activate**.

   The *Activate License* dialog box appears.
3. Click **Activate manually**, and then click **Continue**.

   The *Manual Activation* dialog box appears.

   IMPORTANT

   This dialog box contains your product key and installation ID which a SMART support specialist uses to create your activation key.
4. E-mail your product key and installation ID to SMART support (smarttech.com/contactsupport).

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

   NOTE

   You have 60 days from the date of installation to enter the activation key.
5. Right-click the license you want to activate in the *Licenses for selected server* table, and then select **Activate**.
6. Click **Activate Manually**, and then type the activation key.
7. 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*.

To activate your license by phone

1. Call SMART Support (smarttech.com/contactsupport) and request your product key and installation ID.

   The SMART Support representative uses your product key and installation ID to create and provide your activation key.

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

   A confirmation dialog box appears.

3. Click **OK**.

Chapter 3
Configuring the server software

Setting passwords 23
Changing the server access password 23
Changing the meeting creation password 24
Changing the administrator access password 25
Assigning an API authorization password 26
Changing Bridgit server setup options 26
Setting meeting options 26
Disabling remote control 27
Disabling webcams 27
Disabling text chat 27
Disabling the Raise Hand feature 28
Disabling the Knock feature 28
Adding a message of the day 29
Configuring meeting audio settings 29
Using Voice over Internet Protocol (VoIP) 29
Using third-party audio 30

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

Setting passwords

You can assign, change or remove many of the passwords users and administrators use with 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 should also assign a meeting creation password.

To change server access passwords

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

   NOTES

   - To revoke a password, remove it from the list.
   - If the server access password and meeting creation password are identical, you're prompted for only the server access password.

4. 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're invited to. The participant can't view the list of other active meetings on the server.

Changing the meeting creation password

Meeting creation passwords are optional. Assign a meeting creation 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 meeting creation password.

To change meeting creation passwords

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

   NOTES

   - To revoke a password, remove it from the list.
   - If the server access password and meeting creation password are identical, you're prompted for only the server access password.

4. 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 Bridgit server using an administrator access password.

To assign an administrator access password

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

   NOTES

   - You can assign only one administrator access password.
   - The administrator appears as *Administrator* in a 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 authorization password

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

To assign an API authorization password

1. Double-click the **SMART Bridgit Administration Tools** icon on the server's desktop, and then click the **Security** tab.
2. Select **API authorization password** in the *Server access passwords* area.
3. Type the password you want to assign.
4. Click **Apply**.

NOTES

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

Changing Bridgit server setup options

Administrators can change server setup information including the registered domain name and primary and secondary port numbers.

To change the server setup options

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

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

Setting meeting options

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

Disabling remote control

To prevent presenters from sharing control of their computers with other participants, disable the remote control setting in SMART Bridgit Administration Tools.

To disable remote control

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Options** tab.
2. Clear the **Enable Remote Control** check box.

NOTES

- Remote control is available in active meetings until they end.
- Remote control is disabled in new meetings and the option doesn't appear to meeting participants.

Disabling webcams

To prevent participants from sharing video, disable the webcam setting in SMART Bridgit Administration Tools.

To disable webcams in Bridgit meetings

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

NOTES

- Webcams are available in active meetings until they end.
- Webcams are disabled in new meetings and the option doesn't appear to meeting participants.

Disabling text chat

To prevent participants from sharing chat messages, disable the text chat setting in SMART Bridgit Administration Tools.

To disable text chat in Bridgit meetings

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Options** tab.

2. Clear the **Enable Chat** check box.

> **NOTES**
>
> - Text chat is available in active meetings until they end.
> - Text chat is disabled in new meetings and the option doesn't appear to meeting participants.

Disabling the Raise Hand feature

To prevent participants from interrupting the meeting with the Raise Hand feature, disable the feature in SMART Bridgit Administration Tools.

To disable the raise hand feature in Bridgit meetings

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Options** tab.
2. Clear the **Enable Raise Hand** check box.

> **NOTES**
>
> - The Raise Hand feature is available in active meetings until they end.
> - The Raise Hand feature is disabled in new meetings and the option doesn't appear to meeting participants.

Disabling the Knock feature

To prevent participants from knocking and entering a meeting without a password, disable the Knock feature in SMART Bridgit Administration Tools.

To disable the knock feature in Bridgit meetings

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Options** tab.
2. Clear the **Enable Knock** check box.

> **NOTES**
>
> - The Knock feature is available in active meetings until they end.
> - The Knock feature is disabled in new meetings and the **Knock to Join** button doesn't appear to participants trying to join the meeting.

Adding a message of the day

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

To add a message of the day

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Options** tab.
2. Select the display frequency in the *Message of the day* area.
3. Type the message in the *Message of the Day* text box (maximum 256 characters).
4. Click **Apply**.

Configuring meeting audio settings

Using Voice over Internet Protocol (VoIP)

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

Up to nine participants in a meeting can speak concurrently using Bridgit's VoIP feature. 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 nine people are in a meeting, participants can open and close their microphones to give others the opportunity to speak.

To disable meeting audio

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Audio/Video** tab.
2. Clear the **Enable Audio** check box.

NOTES

- Meeting audio is available in active meetings until they end.
- Meeting audio is disabled in new meetings.

To select a default audio optimization when using VoIP

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Audio/Video** tab.

2. 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.

Using third-party audio

If you're using a third-party voice 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 voice bridge

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Audio/Video** tab.
2. Select **Use a third-party Voice Bridge or audio-conferencing provider**.

Chapter 4

Managing a GSN

Bridgit servers in a GSN 31
Setting up a local GSN server 32
Adding a remote Bridgit server to the GSN 32
Removing a local server from a GSN 33
Removing a Bridgit server from a GSN 33
Changing GSN server information 34
Manually reconnecting to a remote GSN server 34
Ending a GSN meeting 34
Bridgit clients in a GSN 35
Connecting to a GSN server 35
Selecting or viewing GSN server information 35
Disabling the Pick fastest server option 36

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

You don’t have to install the GSN separately. Install the Bridgit server software and use SMART Bridgit Administration Tools to configure the GSN options. See *Installing the server software* on page 15 for installation information.

Bridgit servers in a GSN

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

NOTE

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

Setting up a local GSN server

When you install 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, and then click the **Servers** tab.
2. Type a name for your server in the *Description* box in the *Server setup information* area.
3. Type a password for the server in the *Server password* box.
4. Click **Apply**.

   NOTE

   The **Apply** button is enabled when you enter a server password.

Adding a remote Bridgit server to the GSN

To add a remote Bridgit server to the GSN

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

   The *Add Server* dialog box appears.

3. Type the server address, server port and GSN password for the server you want to add, and then click **OK**.

   NOTES

   - All three boxes 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’s 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 add the server, the *Server list* displayed on every member server of the GSN updates with the new server information. If meetings are running that include these servers, the *Conference Server* list on the *Meetings* tab also updates.

Removing a local server from a GSN

To remove a local server from a GSN

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server’s desktop, and then click the **Servers** tab.
2. Select the local server you want to remove in the *Server list*.
3. Click **Remove Local**, 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 *Meetings* list of the server computer hosting them.

Removing a Bridgit server from a GSN

To remove a Bridgit server from a GSN

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server’s desktop, and then click the **Servers** tab.
2. Select the server you want to remove in the *Server list*.

3. 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 when the server is removed, they remain on the *Meetings* 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, and then click the **Servers** tab.
2. Type new information in the *Description* box or the *Server password* box.
3. Click **Apply**.

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

Manually reconnecting to a remote GSN server

To manually reconnect to a remote GSN server

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

> **NOTE**
>
> The **Reconnect** button is unavailable when there's already a valid connection or when no server is selected.

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, and then click the **Meetings** tab.
2. Select a meeting in the list.

3. Click **End meeting**.

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

Bridgit clients in a GSN

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 GSN servers is similar to connecting to a single 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. In your Internet browser, go to your Bridgit server.
2. Click the **Download Software** link, and then run the client software.

Selecting or viewing GSN 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 of the *SMART Bridgit Software* dialog box, if you want to connect to a different server.

   The *Server Information* dialog box appears.

> **NOTES**
>
> - *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 the server's 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* dialog box 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.

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

Chapter 5

Administering the server software

Viewing status information 37

- Viewing active meetings 38
- Broadcasting messages to meeting participants 38
- Viewing status information 38
- Viewing and saving usage reports 39
  - Viewing and saving server usage reports 39
  - Setting log purge frequency 40

Managing servers and meetings 40

- Placing a server on hold 40
- Ending a meeting 41

Controlling Bridgit software services 41

Customizing the Bridgit server’s web page 42

Downloading the Bridgit client 42

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

When you install Bridgit server software, a shortcut to SMART Bridgit Administration Tools appears on the server’s desktop.

Viewing status information

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

Viewing active meetings

To view active meetings

Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Meetings** 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 meeting participants

To broadcast a message to all meeting participants

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

   Your message appears on each meeting participant's screen.

Viewing status information

To view status information

Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Servers** tab.

A table of active servers appears. The table 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 the local server is unable to contact it
  - On hold – an administrator placed the server on hold

Viewing and saving usage reports

Viewing and saving server usage reports

To view server usage reports

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server’s desktop, and then click the **Report** tab.

   A server usage report for the current week appears.

2. Use the **Report start date** and **Report end date** calendars to select report dates, 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, and then click the **Report** tab.

   A server usage report for the current week appears.

2. 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.

3. Click **Save Report**.

   If no entries are selected, a *Save As* dialog box appears. Skip to step 5.

   OR

   If entries are selected, a *Save All Items* dialog box appears. Proceed to step 4.

4. Click **Save All Entries** or **Save Selection**.

   A *Save As* dialog box appears.

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

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 1 and 120 days.

To set log purge frequency

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Report** tab.
2. Enter the number of days you want the log to store information for in the *Logs purged after* box.
3. 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 it doesn't end active meetings.

Place a server on hold when you want to perform maintenance 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, and then click the **Servers** tab.
2. Select the server in the *Server list* that you want to place on hold or to reactivate.
3. Click **On Hold**, and then click **OK** when asked to confirm.

   The server status changes to *On Hold*.

   OR

   Click **Re-activate**.

   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, and then click the **Meetings** tab.
2. Select the meeting you want to end, and then click **End Meeting**.
3. If you want to broadcast a message to meeting participants as the meeting ends, type it in the *Message* box.
4. Click **OK**.

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

Controlling Bridgit software services

You can use the Windows Services administration console to control 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 Bridgit software services

1. Open the Windows Services administration console (**Control Panel > System and Security > 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 Meeting Service**.

   The *SMART Bridgit Meeting 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 Bridgit server's web page

After you configure the Bridgit server, users can download the Bridgit client by visiting the server's address in an Internet browser.

To customize the Bridgit server's web page

1. Go to **C:\Program Files (x86)\SMART Technologies\SMART Bridgit\res**.
2. Back up the following files by copying them to a temporary location:
   - **ClientDownloadPageWin.htm**
   - **ClientDownloadPageMac.htm**
   - **ClientDownloadPageiOS.htm**
3. Customize the above files.

   The files should contain links to download the Bridgit client for Windows operating systems, Mac OS X operating system software or iOS operating system software.

File	Link
ClientDownloadPageWin.htm	`<a href="Bridgit.exe">`
ClientDownloadPageMac.htm	`<a href="Bridgit.zip">`
ClientDownloadPageiOS.htm	`<a href="`*`[Bridgit app store URL]`*`">`

Downloading the Bridgit client

To download the Bridgit client

1. In your Internet browser, go to your Bridgit server.
2. Click the **Download Software** link, and then run the client software.

Chapter 6

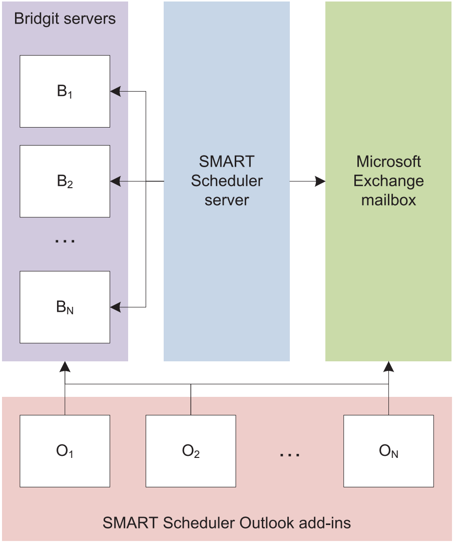
Using SMART Scheduler

Installing SMART Scheduler server software 43
Locating the SMART Scheduler server software installation file 44
Installing the software 44
Configuring SMART Scheduler server 45
Upgrading SMART Scheduler server 46
Installing the SMART Scheduler Outlook add-in 46
Installing the SMART Scheduler Outlook add-in from a command line 48
Removing the SMART Scheduler Outlook add-in 50

If you're using a Windows operating system, the SMART Scheduler option integrates the Bridgit server with Microsoft Exchange Server and Microsoft Outlook Clients. This enables you to schedule single or recurring meetings that use Bridgit software.

Installing SMART Scheduler server software

As shown in the following diagram, a SMART Scheduler server can manage only one Microsoft Exchange mailbox but multiple Bridgit servers (if those Bridgit servers are the same version).



IMPORTANT

- Because a SMART Scheduler server can manage only one Microsoft Exchange mailbox, all SMART Scheduler Outlook add-ins linked to the mailbox must be the same version.
- As indicated in *Upgrading SMART Scheduler server* on page 46, upgrade all components of the Bridgit ecosystem (Bridgit servers, SMART Scheduler server and SMART Scheduler Outlook add-ins) at the same time.

Locating the SMART Scheduler server software installation file

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

To locate the SMART Scheduler server software installation file

On the computer where you're installing the software, browse to your Bridgit server by typing

http://*[yourserver.com]*/SMARTSchedulerServerSetup.exe

in the address bar, where *[yourserver.com]* is the URL of your Bridgit server.

OR

On your Bridgit server, go to

C:\Program Files (x86)\SMART Technologies\SMART Bridgit\SMARTSchedulerInstallers

and then copy the **SMARTSchedulerServerSetup.exe** file to the computer you're installing 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.

IMPORTANT

Before installing SMART Scheduler server software, you must install Microsoft .NET Framework 4 Client Profile. If the installer is unable to find Microsoft .NET Framework 4 Client Profile, it prompts you to install this prerequisite software.

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 doesn’t run on computers that have Microsoft Outlook installed.

2. Click **Next** to continue.

   The *Software License Agreement* appears.

3. Read the agreement. If you accept it, 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* dialog box 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* dialog box appears.

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

   The *SMART Scheduler server Configuration* dialog box appears.

7. Type your SMART Scheduler e-mail credentials and Windows authentication information in the appropriate boxes, and then click **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.

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 where you installed SMART Scheduler server and double-click the **SMARTSchedulerServerConfig.exe** file.

   The *SMART Scheduler Server Configuration* dialog box opens.

2. Change your SMART Scheduler e-mail credentials or Windows authentication information as required.
3. Click **OK** to save the changes.

☞ IMPORTANT

- If you change the SMART Scheduler e-mail address, none of the meetings scheduled using the old e-mail address will run.
- After changing the e-mail address on the server, you must also change the e-mail address in the SMART Scheduler Outlook add-in. For instructions, see *To change the SMART Scheduler settings for all new meetings* in your *Bridgit 4.6 user's guide* (smarttech.com/kb/170396) or Bridgit Help.

Upgrading SMART Scheduler server

To upgrade your SMART Scheduler server software

1. Upgrade your Bridgit server.

   See *Upgrading Bridgit server software* on page 19 for instructions.

2. Upgrade your SMART Scheduler server software.

   See *Installing SMART Scheduler server software* on page 43 for instructions.

3. Upgrade SMART Scheduler Outlook add-in.

   See *To upgrade the add-in from a command line* on page 50.

Installing the SMART Scheduler Outlook add-in

The SMART Scheduler Outlook add-in enables you to automatically create a Bridgit meeting that accompanies a Microsoft Outlook meeting.

You can install the add-in on any computer that can communicate with your Bridgit server, but the add-in must be installed and configured by an administrator. Once the add-in is installed, any user can change individual profile settings. These changes affect only the profile of the user that set them. The administrator settings remain the same.

☞ IMPORTANT

Close Outlook before you download the .msi file and install the add-in.

To download the .msi file

1. Go to:

Outlook version	Path
32 bit	**http://*[yourserver.com]*/SMARTSchedulerOutlookAddinSetupx86.msi**
64 bit	**http://*[yourserver.com]*/SMARTSchedulerOutlookAddinSetupx64.msi**

   where *[yourserver.com]* is the address for your Bridgit server.

2. Press ENTER.
3. Click **Run** to install the file.

   The *SMART Scheduler Outlook Add-in – InstallShield Wizard* welcome page appears.

To install the SMART Scheduler Outlook add-in

1. Press **Next** in the welcome screen.

   The *Software License Agreement* page appears.

2. If you accept, 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* page appears.

3. Click **Next** to install to the default folder, or click **Change** to specify another folder.

   The *SMART Scheduler Outlook Add-in Preferences* page appears.

4. Type the name of the *Default Bridgit Server* to use when setting up Bridgit meetings.
5. Type the SMART Scheduler e-mail address.

   > **NOTE**
   >
   > The Microsoft Exchange Server administrator creates this address when he or she creates the mailbox on the Microsoft Exchange Server.

6. If you want the meetings to be password protected by default, leave **Password protect meetings by default** selected.

7. If you want to use formatting in your messages, select **Preserve Rich Text formatting**. Otherwise, clear the check box to use plain text.

   NOTE

   Rich text formatting can cause unexpected behavior when you use the SMART Scheduler Outlook add-in with other third-party Outlook add-ins and extensions.

8. Click **Next**.

   The *Ready to Install the Program* page appears.

9. Click **Install**.

   When the add-in successfully installs, the *InstallShield Wizard Completed* page appears.

10. If you want Outlook to start after the wizard closes, leave **Start Outlook** selected.

11. Click **Finish** to close the wizard.

Installing the SMART Scheduler Outlook add-in from a command line

To install the add-in from a command line

1. Open a Command Prompt window, then type **cmd** in the *Open* box, and then click **OK**.

   The *cmd.exe* dialog box appears.

2. Type **cd** followed by a space, and then type the path to the directory that contains the installer.

3. Execute the installer with any appropriate msi-related parameters.

   NOTE

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

4. Specify configuration options for the installer.

Option	Description
SERVERNAME	The address of the Bridgit server on which your SMART Scheduler meetings will run.
USEPASSWORD	Whether your SMART Scheduler meetings are password protected (0 or 1).
MAILBOX	The SMART Scheduler e-mail 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 (1) or plain text formatting (0).

EXAMPLE

```
msiexec.exe /i "C:\[Source file location]\
  SMARTSchedulerOutlookAddinSetupx86.msi" /qn
  SERVERNAME=[yourserver.com] USEPASSWORD=1 USERTF=1
  MAILBOX="[Scheduler mailbox]"
```

where *[Source file location]* is the path to the .msi file, *[yourserver.com]* is the URL of your Bridgit server, and *[Scheduler mailbox]* is the SMART Scheduler e-mail address.

NOTE

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

5. Press ENTER.

   The SMART Scheduler Outlook add-in installs.

To upgrade the add-in from a command line

1. Upgrade Bridgit server software (see *Upgrading Bridgit server software* on page 19) and SMART Scheduler server software (see *Installing SMART Scheduler server software* on page 43).
2. Follow the steps in *To install the add-in from a command line* on page 48, and then close and restart Outlook.

> **NOTE**
>
> You can leave Outlook running during the upgrade, but you must restart it for the changes to take effect.

Removing the 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 support 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:

Software version	Product code
4.0	{916243FB-5A56-4CF1-B75B-6F4236977C12}
4.1	{EF2064B4-D050-4A45-B28A-F8BA573AB0B5}
4.2	{2F255E33-D2B6-4EC5-BE45-124E7A6BE420}
4.5	{2F255E33-D2B6-4EC5-BE45-124E7A6BE420}
4.6	{B600355A-F5A2-44BA-8C3E-A56792F5654E}
4.6 SP1	{B7C3471A-CE8F-44C2-A79C-5E3606D7E46A}

> **NOTE**
>
> Include the braces when entering a product code value.

To remove the add-in from the uninstaller

1. Open Windows Control Panel’s Install or Remove Programs tool.
2. Remove the installed SMART Scheduler Outlook add-in software.

To remove the add-in from a command line

1. Open a Command Prompt window.
2. Type the following command (including quotation marks), and then press ENTER:

```
msiexec.exe /x"[Path to .msi]\
  SMARTSchedulerOutlookAddinSetupx86.msi" /q
```

OR

Type the following command, and then press ENTER:

```
msiexec.exe /x[Product code] /q
```

Chapter 7

Bandwidth and scalability

Bandwidth requirements 53
Examples of bandwidth requirements 54
Scaling Bridgit 54

Bandwidth requirements

Bridgit software performs best when you allocate at least 1 Mbps of network bandwidth on your server for each meeting participant, both inbound to, and outbound from, the server.

EXAMPLE

If you have a 5 Mbps bandwidth connection to your server, you can support up to five concurrent participants with four open microphones and four webcams at optimal performance (1 Mbps per user × 5 users = 5 Mbps).

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

Bridgit software resource	Bandwidth required
One shared desktop with a 1024 × 768 resolution	9 Kbps
One open microphone using the standard quality setting	25 Kbps
One open microphone using the low quality setting	15 Kbps
One open webcam using the standard quality setting	250 Kbps
One open webcam using the moderate quality setting	200 Kbps
One open webcam using the low quality setting	60 Kbps

TIP

Most shared desktops maintain a bandwidth load of about 9 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 1800 Kbps, while maintaining an average of 300 Kbps.

Examples of bandwidth requirements

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

Bridgit resource	Bandwidth required
One shared desktop with a resolution of 1024 × 768	9 Kbps
Four open microphones using the standard quality setting	25 Kbps × 4 = 100 Kbps
Four open webcams with moderate activity	200 Kbps × 4 = 800 Kbps
Total bandwidth required for each participant	9 Kbps + 100 Kbps + 800 Kbps = 909 Kbps
Total bandwidth required for all 4 participants	909 Kbps × 4 participants = 3,636 Kbps or 3.636 Mbps

Scaling Bridgit

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

Appendix A
Troubleshooting

Using the Bridgit troubleshooting tool 56
- Screen capture technology 56
- Sharing color quality 58
- Audio 59
- Connection 59
- Ink 60

Monitoring a meeting’s performance – presenter 60
- View the meeting performance for each participant 60
- Improving performance 60

Monitoring a meeting’s performance – participant 61
- Viewing the meeting performance for your computer 61
- Improving performance 62

Minimizing network latency 62
- Verifying communication protocol 63
- Checking for firewalls 64
- Measuring latency and packet loss 64

Troubleshooting Bridgit server connections 64
- Verifying the network’s DNS configuration 65
- Verifying Bridgit server configuration 66
- Manually updating the Windows registry 67
- Configuring the client’s HOSTS file 68
- Verifying port forwarding and firewall configuration 68

Troubleshooting administration tool connections 68
- Directing IP traffic to the Bridgit server 69
- Moving the server’s IP address to the top of the IP settings list 70
- Stopping applications using the server’s IP port 70

Troubleshooting SMART Scheduler 71

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

Using the Bridgit troubleshooting tool

Bridgit software has a troubleshooting tool that you can use to determine the cause of issues you could have.

To open the troubleshooting tool

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

   The Bridgit lobby screen appears.

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

   The *About SMART Bridgit Software* dialog box appears.

3. Select **Technical Support > Troubleshooting**.

   The *Troubleshooting* dialog box appears.

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

- *Screen capture technology* below
- *Sharing color quality* on page 58
- *Audio* on page 59
- *Connection* on page 59
- *Ink* on page 60

For more assistance, contact SMART Support (smarttech.com/contactsupport).

Screen capture technology

This section provides an overview of the various technologies that Bridgit software uses when you share your desktop during a meeting.

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

Type of technology	Description
Mirror drivers	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. **NOTE** Mirror drivers behave unexpectedly on computers with Windows 7 operating systems.

Type of technology	Description
Redraw hooks	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 perform a screen capture every time something changes on the screen. **NOTE** Redraw hooks behave unexpectedly on computers with Windows 7 operating systems.
Four times per second capture	If Bridgit software can't use either of the above technologies, it captures the shared screen four times per second, compresses the image, and then sends it to the recipient. This method offers the lowest performance, but it uses the lowest bandwidth.

Use the options outlined in this section to resolve issues with sharing speed and image quality.

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 whether hardware acceleration is on or off.	If you use a low-end video card in your system and you disable hardware acceleration, you increase the performance of your computer.
Mirror driver availability	• *available* – The mirror driver is installed. • *unavailable* – The mirror driver isn't installed. • *disable by OS* – Your computer has Windows 7, which causes the mirror driver to behave unexpectedly.	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.

Field/option	Description	When to use / why it's important
Enable redraw hooks	Select to share using redraw hooks. NOTE Redraw hooks behave unexpectedly with Windows 7 operating system.	If your pointer is flickering, you might want to try clearing this option.
Enable mirror driver	Select to share using mirror driver.	• If your shared applications aren't being captured correctly, you might want to try clearing 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 is cleared by default. You can select it to improve sharing when bandwidth is limited.

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.	• Clear 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 Bridgit’s software-based echo cancellation can interfere with. • Clear 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. • Clear 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 connected Bridgit software to the server.	• Status only • To change which server is in use, double-click the **SMART Bridgit Client** icon on your desktop or in the Dock, and then click the server icon .
Fastest server	• Displays the server in the Global Server Network (GSN) that you’re connected to. • Bridgit software selected this server due to its speed of connection.	• Status only • Bridgit software detects this server automatically.

Field	Description	When to use / why it’s important
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	Fallback communication protocol when TCP/UDP is restricted.	Status only
Pick fastest server	Select to enable the automatic selection of the fastest server.	If you clear this option, Bridgit software connects to the server you specified, regardless of whether there is a faster server available in the same GSN.

Ink

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

Monitoring a meeting’s performance – presenter

When you present in a meeting, an hourglass could appear on the **Show/Hide Participant List** button while 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.

View the meeting performance for each participant

To view the meeting performance for each participant

Click the **Show/Hide 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, ToolTips and so on.
- Stop sharing your webcam.
- Optimize your desktop for sharing. Select **Menu > About SMART Bridgit > Technical Support > Troubleshooting**, and then select **Optimize desktop for sharing** and 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 **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 **Show/Hide 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 **Show/Hide Participant List** button turns red .

Viewing the meeting performance for your computer

To view the meeting performance for your computer

Click the **Show/Hide 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 dialog box* 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. Select **Control Panel > Display > Settings > Advanced**. Click the **Troubleshoot** tab and drag the level of *Hardware acceleration* toward **None**. Test 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 Bridgit software.

Symptoms

- Connecting to the Bridgit server takes a long time.
- The screen updates slowly when you view a shared desktop.
- Bridgit software 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 *Verifying communication protocol* below.
- Check if you’re connecting through a proxy server. See *Bridgit and firewalls* on page 12.
- Check your network bandwidth. See *Examples of bandwidth requirements* on page 54.
- Measure latency and packet loss rate. See *Measuring latency and packet loss* on the next page.

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 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.

Verifying communication protocol

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 Bridgit software’s troubleshooting tool to determine the network protocol you’re using. See *Using the Bridgit troubleshooting tool* on page 56.

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, contact your administrator to open the TCP and UDP ports to connect to the Bridgit server. See *Administering the server software* on page 37. See *Bridgit and firewalls* on page 12 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 Bridgit troubleshooting tool. See *Using the Bridgit troubleshooting tool* on page 56.

   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. Contact your administrator to open the TCP and UDP ports to connect to the Bridgit server.

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.

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 Bridgit server connections

This section helps you resolve connection issues that are caused by your Bridgit server software or your network environment.

Bridgit server connection issues can result from an incorrect domain name server (DNS) configuration for routing to the 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 Bridgit client connects to a 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.

  When you're unable to connect to Bridgit server software and Bridgit client software is causing the issue, see *You're unable to connect to the Bridgit server because of issues with the Bridgit client computer* (smarttech.com/kb/099567).
- An error message appears when you connect to a Bridgit server from an Internet browser.

Solution

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

- *Verifying the network's DNS configuration* below
- *Verifying Bridgit server configuration* on the next page
- *Manually updating the Windows registry* on page 67
- *Configuring the client's HOSTS file* on page 68
- *Verifying 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 Bridgit server's IP address.

To verify that the DNS is configured correctly

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

   The server's network configuration information appears, including its IP address.
2. Type **nslookup *[Server domain name]*** and then press ENTER.

   OR

   Type **ping *[Server domain name]*** using the domain name for the Bridgit Server, and then press ENTER.

   The IP address that the network's DNS resolves to appears.
3. Compare the IP addresses.

NOTES

- If the IP addresses are the same, the network's DNS is configured correctly. See *Troubleshooting Bridgit server connections* on page 64.
- If the IP addresses are different, the network's DNS isn't configured correctly.

  OR

  The 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 68 to add the domain name to the Windows HOSTS file.

Verifying Bridgit server configuration

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

To verify the domain name or IP address

1. Double-click the **SMART Bridgit Administration Tools** shortcut on the server's desktop, and then click the **Setup** tab.

   For more information, see *Configuring the server software* on page 23.

   NOTE

   If the *SMART Bridgit Administration Tools* window doesn't appear, see *Manually updating the Windows registry* on the 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 you compared in *Verifying the network's DNS configuration* on the previous page.
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 the previous page to verify the port forwarding and firewall configurations.

   If the domain names or IP addresses are different, type your 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 Administration Tools* dialog box closes.

5. Select **Start > Control Panel > System and Security > Administrative Tools > Services**.

   The *Services* dialog box appears.

6. Right-click **SMART Bridgit Master Service**, and then select **Restart**.

   The *SMART Bridgit Master Service* restarts.

   NOTE

   Other Bridgit clients disconnect from the Bridgit server when you complete this procedure.

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

   The *SMART Bridgit Conference Service* starts.

   NOTES

   If clients are still unable to connect to the server, see *Verifying the network's DNS configuration* on page 65 to verify the port forwarding and firewall configurations.

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 Bridgit server's domain name or IP address in the *MasterServerDomainName* boxes.

3. Exit the Windows registry editor.

4. Select **Start > Control Panel > System and Security > Administrative Tools > Services**.

   The *Services* dialog box appears.

5. Right-click **SMART Bridgit Master Service**, and then select **Restart**.

   The *SMART Bridgit Master Service* restarts.

   NOTE

   Other clients disconnect from the Bridgit server when you complete this procedure.

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

   The *SMART Bridgit Conference Service* restarts.

If clients are still unable to connect to the server, see *Verifying port forwarding and firewall configuration* below 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. Go to **C:\Windows\system32\drivers\etc** on the Bridgit client computer, and then open the **HOSTS** file.
2. Add an entry so that the domain name you're using to connect to the Bridgit server resolves to the server's IP address.

   This procedure is effective for 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 Bridgit server connections* on page 64 to configure the Bridgit server software.

Verifying port forwarding and firewall configuration

If clients are still unable to connect to the server, verify that port forwarding on the network routers is configured to give clients access to the server, and that firewalls protecting the Bridgit server allow clients to access the server. See *Verifying communication protocol* on page 63 and *Checking for firewalls* on page 64.

If the problems persist, the Bridgit client (not the server) could be the cause. See *You're unable to connect to the Bridgit server because of issues with the Bridgit client computer* (smarttech.com/kb/099567).

Troubleshooting administration tool connections

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

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

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

Directing IP traffic to the Bridgit server

To direct IP traffic to the IP address bound to the Bridgit server

1. Open a Command Prompt 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. For more information, see *Verifying Bridgit server configuration* on page 66.

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

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

4. Type your IP address and host name 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 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 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. Select **Start > Control Panel> Network Connections**.
3. Right-click the network device that Bridgit software is bound to, and then select **Properties**.
4. Click **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. Click the **IP Settings** tab.
8. Remove all the IP addresses above the 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 Bridgit software's primary port available

1. Stop applications that use Bridgit software's primary port.
2. Open SMART Bridgit Administration Tools and configure Bridgit software. For more information, see *Verifying Bridgit server configuration* on page 66.
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 a **Command Prompt** window, and then browse to the *SMART Scheduler Server* folder.

   The default folder is **C:\Program Files (x86)\SMART Technologies\SMART Scheduler Server**.

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

   The SMART Scheduler server 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. Open a **Command Prompt** window, and then browse to the *SMART Scheduler Server* folder.

   The default folder is **C:\Program Files (x86)\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>>log.txt**, and then press ENTER.

   The SMART Scheduler server service starts. The log information re-directs to the **log.txt** file.

4. Wait a few minutes, and then press CTRL+C.

   The server stops and the command prompt returns.

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

   The SMART Scheduler server service starts.

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

Index

A

access requirements 8
activation
    manual 20
    using the SMART activation server 19
administrator rights 10
AGC 59
API 26
audio 7, 29, 59

B

bandwidth
    examples 54
    requirements for 53
Bridgit client software
    about 2
    computer requirements for 7
    downloading 42
Bridgit server software
    about 1
    administering 37
    changing the password for 25
    computer requirements for 6
    configuring 23
    customizing the web page of 42
    installing 14
    scaling 54
    upgrading 19
    verifying configuration of 66
broadcast messages 38

C

chat 27
client software See Bridgit client software
color quality 58
command lines 48
communication protocols 63
computer requirements
    Bridgit client software 7
    Bridgit server software 6
    SMART Scheduler 8
    SMART Scheduler Outlook add-in 8

D

domain names
    entering in the Windows registry 67
    public versus private domain names 11
    verifying DNS configuration 65
downloads 42

F

firewalls
    checking for 64
    configuring 13
    verifying configuration of 68
FQDNs 11

G

GSN
    about 2
    adding a remote server 32
    changing server information 34
    connecting to a server 35
    ending a meeting 34
    manually reconnecting to a remote server 34
    removing a server 33

setting up a server 32

H

hand, raising and lowering 28
HOSTS files 68
HTTP 63

I

ink 60
installation
Bridgit server software 14
SMART Scheduler 43
SMART Scheduler Outlook add-in 46
Internet connections 9
IP addresses 12, 67-68, 70
IP traffic 69
IPv4/IPv6 addresses 12

K

keys See licenses
knock 28

L

LANs 9
latency 62
licenses
about 8, 19
activating 19
removing 21
logs See usage reports

M

Mac OS X operating system software 7
Meeting Pro software See SMART Meeting Pro software
meetings
changing passwords for 23-24
ending 41
monitoring performance of 60-61
setting options for 26
viewing active 38
message of the day 29

N

network protocols See communication protocols
Notebook software See SMART Notebook software

O

Outlook add-in See SMART Scheduler Outlook add-in

P

packet loss 64
passwords
about 10
administrator access 25
API authorization 26
meeting creation 24
server access 23
performance
participant 61
presenter 60
Pick fastest server option, disabling 36
ports
troubleshooting 59
verifying port forwarding 68
prerequisites
access See access requirements
computer See computer requirements
product keys See licenses
protocols See communication protocols
proxy servers
computer requirements for 7
configuring 13
troubleshooting 59

R

remote control 27
reports See usage reports
requirements
- access See access requirements
- computer See computer requirements

RSA encrypted key exchange 10

S

scaling 54
screen capture technology 56
security 10
server software See Bridgit server software
SMART Bridgit Administration Tools
- about 1
- administering Bridgit software with 37
- configuring Bridgit software with 23

SMART Meeting Pro software 3
SMART Notebook software 3
SMART Scheduler
- about 3, 43
- access rights for 10
- computer requirements for 8
- configuring 45
- installing 43
- troubleshooting 71
- upgrading 46

SMART Scheduler Outlook add-in
- about 3
- computer requirements for 8
- installing 46
- removing 50
- upgrading 50

software licenses See licenses
SRTP 10, 29
SSL 10

T

TCP 63
text chat See chat
third-party voice bridges 30
troubleshooting 55

U

UDP 63
upgrades
- Bridgit server software 19
- SMART Scheduler 46
- SMART Scheduler Outlook add-in 50

usage reports 39

V

virtualization environments 8
voice bridges 30
VoIP 7, 19, 29, 59

W

WANs 9
web pages 42
webcams
- computer requirements for 7
- disabling 27

Windows operating systems 7
Windows registry 67

SMART Technologies

smarttech.com/support

smarttech.com/contactsupport

smarttech.com/kb/170397