Bridgit™ Conferencing Software: Security, Firewalls, Bandwidth and Scalability

SMART Technologies

Bridgit™ Conferencing Software: Security, Firewalls, Bandwidth and Scalability

Overview

Bridgit™ conferencing software is a multi-functional and highly secure tool for communicating live audiovisual information over a network to conference participants worldwide. With Bridgit software, you can:

- Share your desktop with conference participants.
- Interact with a conference participant's computer (remote control).
- Watch conference participants who are using webcams.
- Speak with, and listen to, conference participants using Voice over Internet Protocol (VoIP) technology.

A Bridgit software server can host one or thousands of conferences at the same time. Conference participants—also called *clients*—can connect to conferences through the Internet or through a local area network (LAN).

This document provides an overview of Bridgit software installation and setup requirements, and is designed as a supplement to the Bridgit Conferencing Software Installation Guide. It also includes information about Bridgit software security features.

Installing Bridgit Software

You can install Bridgit software on either a dedicated server or a server running other software. If the server is running other software, you can install Bridgit software in the following ways:

- using IP specific binding and the default server ports
- using IP specific binding and customizing the default server ports
- binding the software to all interfaces and customizing the default server ports

Installing Bridgit Software Services

Bridgit software includes a master service and a conference service. The master service authenticates client connections and balances the client load between primary and secondary servers. The conference service transmits conference data to and from conference participants.

When you install Bridgit software on a server, you install both services by default. A server with both services installed is called a primary Bridgit software server.

Creating a Server Cluster

The speed and number of processors in your primary server determine the number of clients that can connect without compromising performance. However, if you host hundreds or thousands of conferences at the same time, you can create a server cluster to increase the capacity and performance of Bridgit software. To set up a server cluster, install only the conference service on one or more additional servers, called secondary servers, and then connect them to the primary server.

In a server cluster, clients initially connect to the primary server. If the client load on the primary server becomes too high, Bridgit software automatically balances the load by routing clients to secondary servers, as required.

NOTE: See *Scaling Bridgit Software* on page 13 for more information about the processor resources required to host a high volume of client connections.

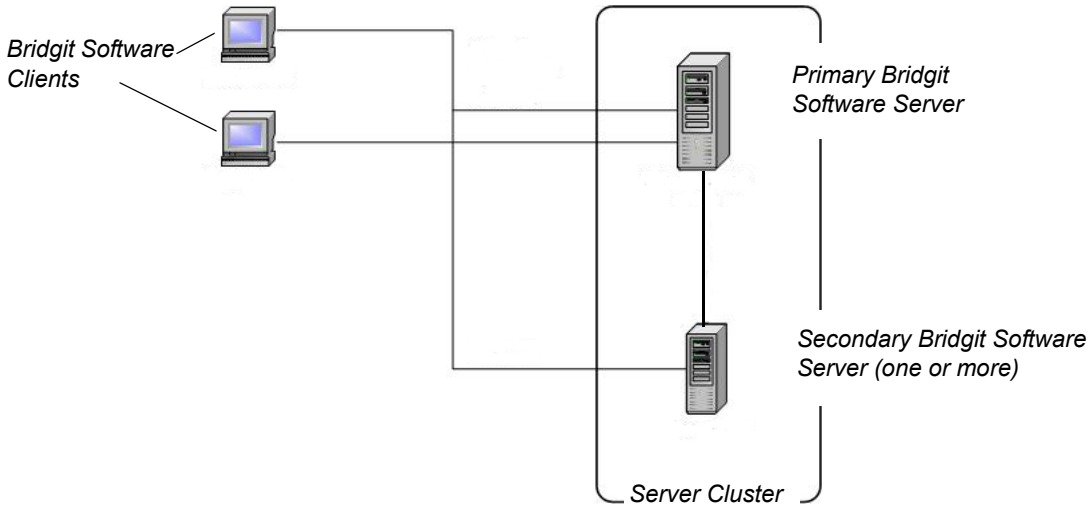

Figure 1: Example of a Server Cluster

Using Firewalls with Bridgit Software

Bridgit software automatically detects and employs the most secure and efficient methods available to connect clients and maintain optimal conference performance. However, we recommend installing your Bridgit software server behind a firewall, to prevent unauthorized access.

Configuring Firewalls

You can install your Bridgit software server behind a software firewall, such as a proxy server, or a hardware firewall, such as a router. For best performance, allow inbound TCP and UDP traffic to the server on the default ports specified in Table 1.

Default Port(s)	External, Server Side Firewall	Internal, Client Side Firewall
80	• HTTP/TCP inbound and outbound data and video traffic on the primary port	• HTTP/TCP outbound data and video traffic on the primary port • No inbound traffic required
9933	• TCP inbound and outbound data and video traffic on a secondary port (recommended)	• TCP outbound data and video traffic on a secondary port (recommended) • No inbound traffic required
9901–9920	• UDP inbound and outbound audio traffic (recommended)	• UDP outbound audio traffic (recommended) • No inbound traffic required

Table 1: Default Port Allocation

IMPORTANT

If port 80 in your firewall is already restricted to HTTP traffic, you must enable and configure a secondary port. The default secondary port for Bridgit software is port 9933.

You can configure your Bridgit software server to work with any proxy server that adheres to the RFC 2068 HTTP standard. If you install your Bridgit software server 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 enablling authentication, such as basic, digest or NT LAN Manager (NTLM) authentication.

If you incorporate a proxy server, configure each conference participant’s Internet browser to access the Bridgit software server.

Figure 2 illustrates how to set up a Bridgit software server so that external clients can connect to conferences through the Internet and internal clients can connect through a LAN.

NOTE: See *Allocating Network Ports* on page 7 for detailed port allocation information.

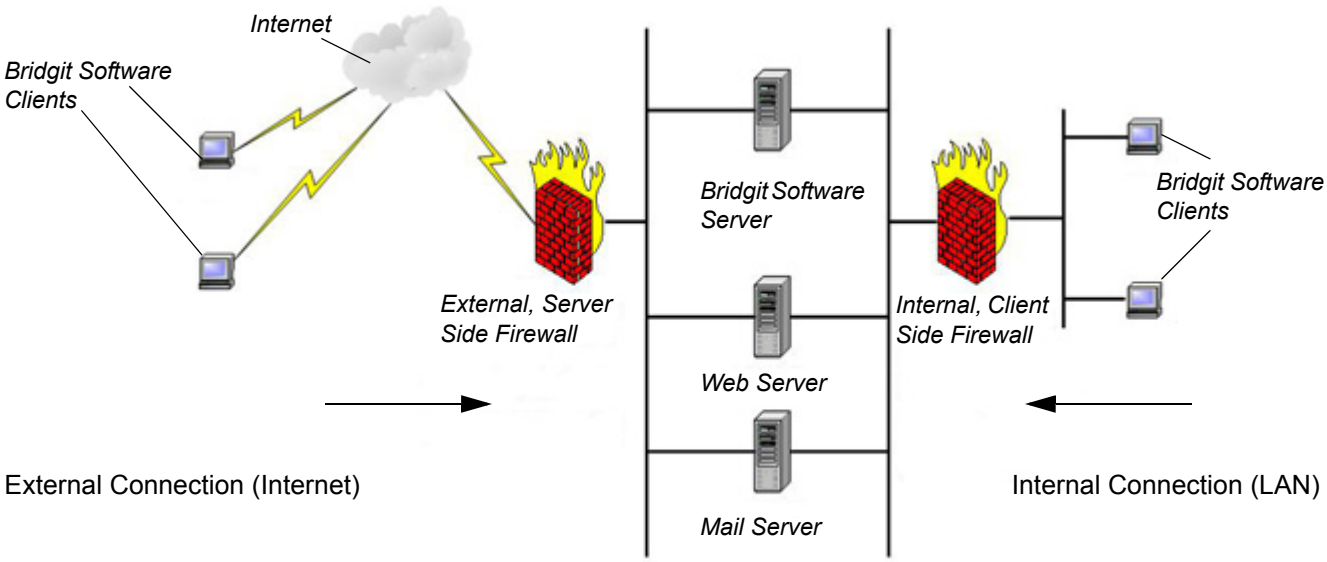

Figure 2: External and Internal Client Connections

Allocating Network Ports

The ports that the Bridgit software server opens to receive incoming traffic from conference participants depend on the ports allocated on both client side and server side firewalls. Use the following seven configuration options to allocate ports. Table 2 describes the port allocations illustrated in Figure 3.

Option	HTTP Port 80	TCP Port 80	TCP Port 9933	UDP Ports 9901–9920	Data and Video Port	Audio Port
	Outbound on Client Side Firewall				Inbound on Server Side Firewall	
1	Allow	Allow	Allow	Allow	80	9901–9920
2	Allow	Allow	Allow	Block	80	80
3	Allow	Allow	Block	Allow	80	9901–9920
4	Allow	Allow	Block	Block	80	80
5	Allow	Block	Allow	Allow	9933	9901–9920
6	No firewall				80	9901–9920
7	No firewall				80	9901–9920

Table 2: Network Port Allocation

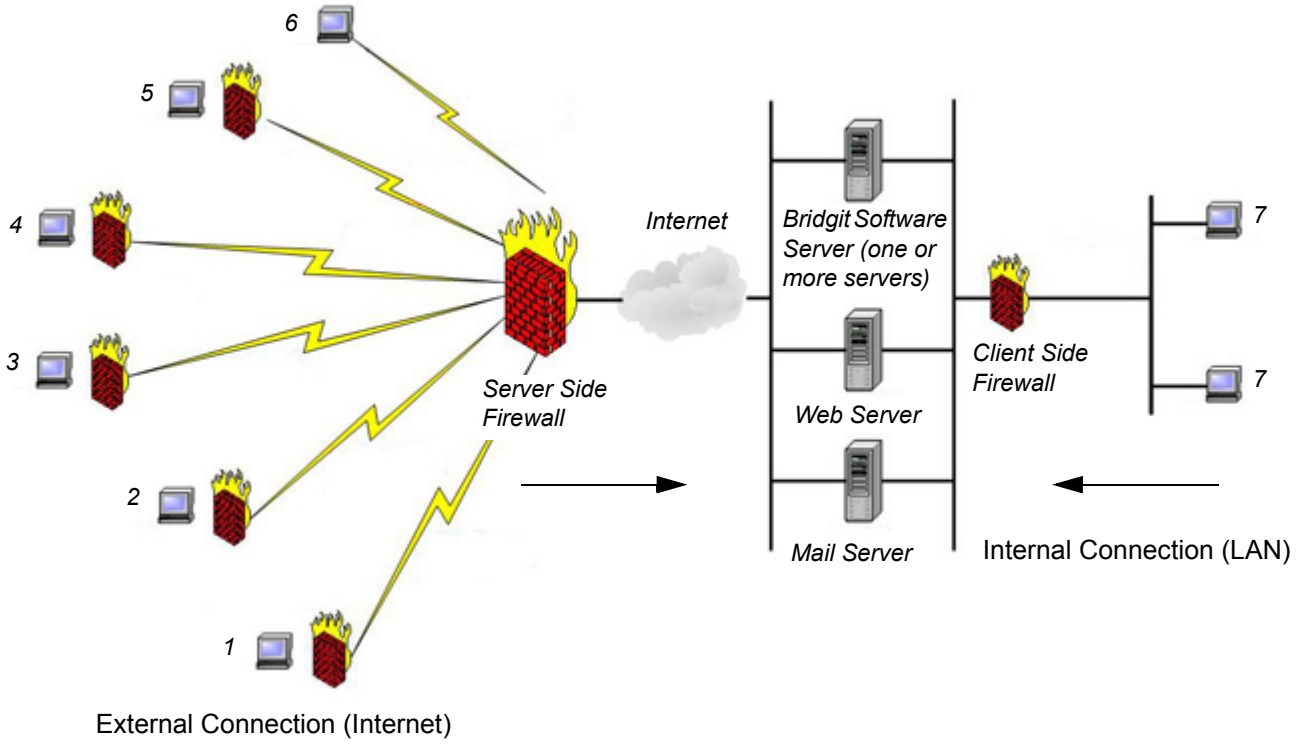

Figure 3: Network Port Allocation

Allocating a Data and Video Channel

When a Bridgit software client joins a conference, Bridgit software creates a dedicated data and video channel on the server. When possible, Bridgit software creates this channel using a TCP connection, which provides the highest quality data and video transmission. If Bridgit software is unable to create the channel using a TCP connection, it uses secure, encapsulated HTTP tunneling. If Bridgit software is unable to create a channel using either TCP or HTTP connections, the Bridgit software client window automatically closes and an error message appears.

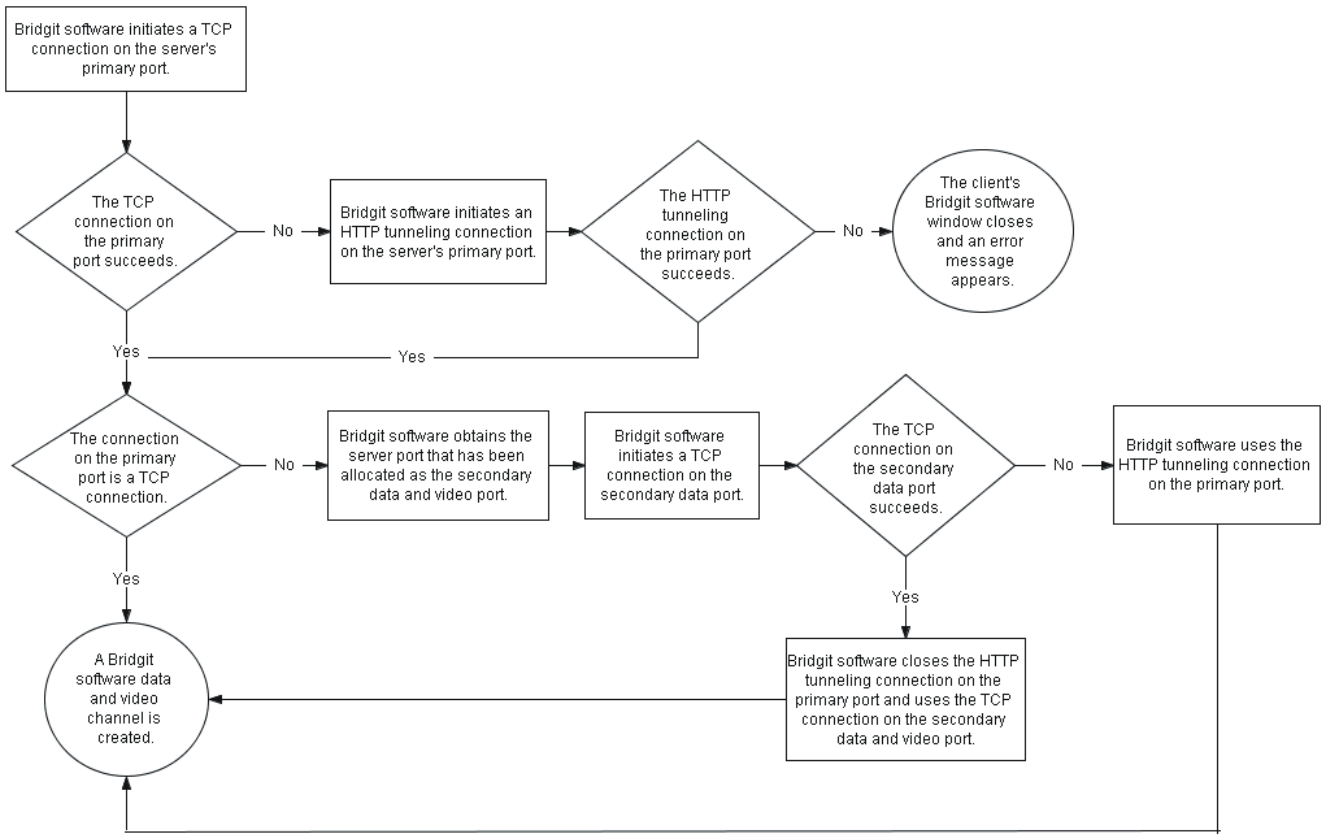

Figure 4: Client Side Channel Allocation for Data and Video Transmission

Allocating an Audio Channel

After allocating a data and video channel, Bridgit software creates an audio channel. When possible, Bridgit software creates this channel using a UDP connection, which provides the highest quality audio transmission. If Bridgit software is unable to create the channel using a UDP connection, it creates an audio channel using the same protocols as the data and video channel.

Although there is no limit to the number of clients that a UDP port can support, audio transmission is optimal with a maximum of 10 participants allocated to a single UDP port.

By default, Bridgit software opens 20 UDP ports on the server (ports 9901–9920), enabling up to approximately 200 conference participants to communicate concurrently using high quality audio transmission. Bridgit software automatically balances the audio transmission load by allocating audio ports as required.

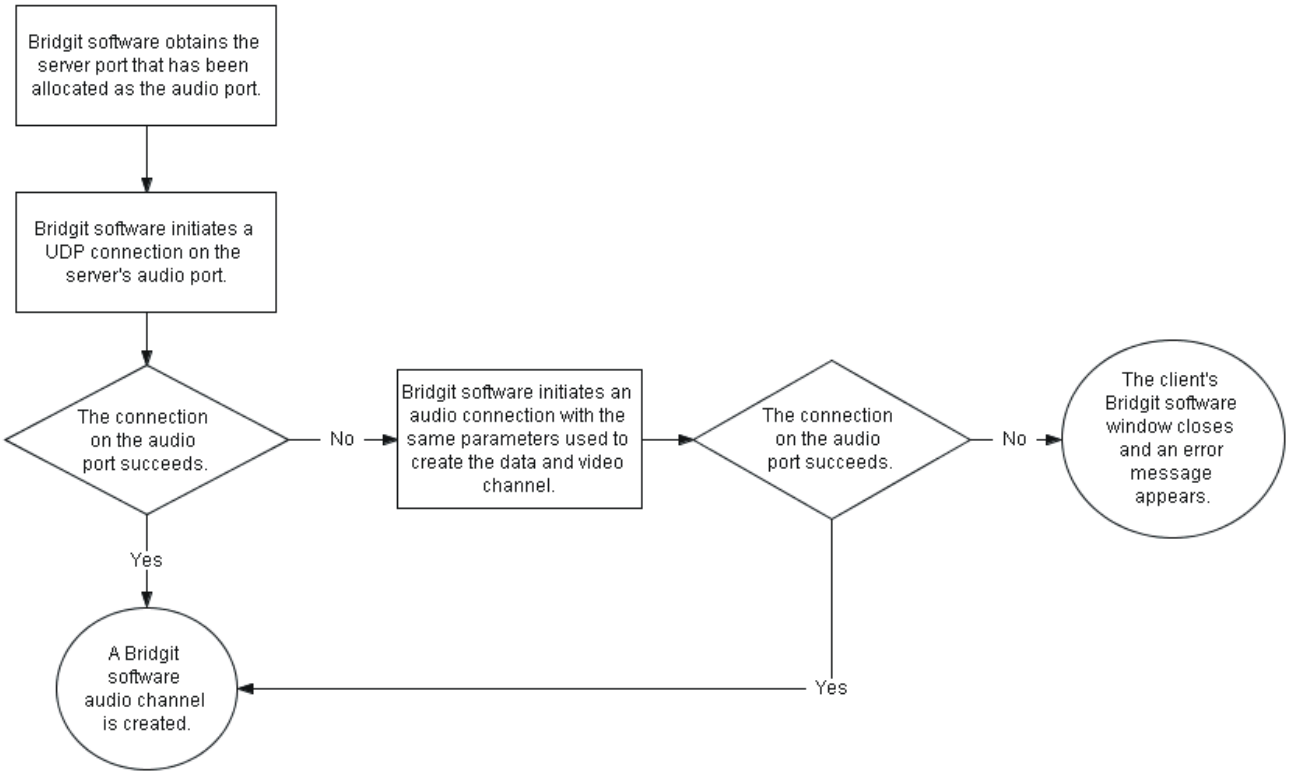

Figure 5: Client Side Channel Allocation for Audio Transmission

Using the VoIP Feature in Bridgit Software

Up to four participants in a conference can talk concurrently using the VoIP feature in Bridgit software. VoIP in Bridgit software incorporates Secure Real-Time Transport Protocol (SRTP) communication on UDP ports, so audio data is processed as a steady and continuous stream, with minimal lag time.

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

Security Features

Server Side Security

Bridgit software incorporates the OpenSSL library, implementing Secure Socket Layer (SSL) version 3.0, to encrypt data transmitted using a TCP connection. Bridgit software also incorporates the libSRTP library, to encrypt audio traffic transmitted using a UDP connection, implementing SRTP. These encryptions prevent third parties from intercepting data transmitted between client and server.

When a Bridgit software server starts, it generates a server certificate. The server uses this certificate to negotiate a cipher suite and a set of encryption keys with each connecting client. However, if a client is unable to negotiate a set of encryption keys with the server, no connection is established.

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 operating system software also implements 256-bit SSL encryption.

Bridgit software hashes all passwords before sending them over a network or storing them in a registry.

Client Side Security

System administrators and conference creators can set three types of password to enhance Bridgit software client side security. These passwords aren't mandatory.

Password Type	Allowed Action
conference viewing password	view a listing of open conferences
conference creation password	create a conference
conference participation password	join a conference

Bandwidth Usage

Bridgit software performs optimally when you allocate at least 250 Kbps of network bandwidth on your server for each conference participant, both inbound to, and outbound from, the server. For example, if you have a 1.5 Mbps bandwidth connection to your server, you can support a maximum of six concurrent participants at optimal performance (250 Kbps × 6 = 1,500 Kbps or 1.5 Mbps).

Use Table 3 to estimate bandwidth requirements for Bridgit software resources.

Bridgit Software Resource	Bandwidth Required
one shared desktop with a resolution of 1024 × 768	60 Kbps
one open microphone using the standard quality setting	30 Kbps
one open microphone using the low quality setting	23 Kbps
one open webcam with moderate activity	40 Kbps

Table 3: Required Bandwidth for Bridgit Software Resources

TIP

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

Although it's unlikely to occur, a shared desktop with a complex photographic desktop background and frequent content changes can peak at a load of 1,800 Kbps, while maintaining an average load of 300 Kbps.

Examples of Bandwidth Requirements

The following two tables can help you determine typical bandwidth usage for Bridgit software conferences.

Bridgit Software Resource	Bandwidth Required
one shared desktop with a resolution of 1024 × 768	60 Kbps
four open microphones using the standard quality setting	30 Kbps × 4 = 120 Kbps
four open webcams with moderate activity	40 Kbps × 4 = 160 Kbps
total bandwidth required for each participant	**60 + 120 Kbps + 160 Kbps = 340 Kbps**
total bandwidth required for all participants	**340 Kbps × 4 participants = 1,360 Kbps or 1.36 Mbps**

Table 4: Example of a Bridgit Software Conference with Four Participants

Bridgit Software Resource	Bandwidth Required
one shared desktop with a resolution of 1024 × 768	60 Kbps
two open microphones using the standard quality setting	30 Kbps × 2 = 60 Kbps
total bandwidth required for each participant	**60 Kbps + 60 Kbps = 120 Kbps**
total bandwidth required for all participants	**120 Kbps × 10 participants = 1,200 Kbps or 1.2 Mbps**

Table 5: Example of a Bridgit Software Conference with 10 Participants

Scaling Bridgit Software

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

Table 6 outlines Bridgit software requirements for a high volume server.

Example	Bridgit Software Resources		Total Processors	Data Transfer Rate (Network Interface Card)	Maximum Client Connections
	Outbound from Server		Server		
1	• one shared desktop with a resolution of 1024 × 768 • four open microphones using the standard quality setting • four open webcams with moderate activity	340,000 Kbps	4	1,000 Mbps	1,000
2	• one shared desktop with a resolution of 1024 × 768 • four open microphones using the standard quality setting	180,000 Kbps	4	1,000 Mbps	1,000
3	• one shared desktop with a resolution of 1024 × 768 • four open webcams with moderate activity	220,000 Kbps	4	1,000 Mbps	1,000
4	• one shared desktop with a resolution of 1024 × 768	48,000 Kbps	2	100 Mbps	800

Table 6: Bridgit Software Server Requirements

SMART Technologies
1207 – 11 Avenue SW, Suite 300
Calgary, AB T3C 0M5
CANADA

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