



CrossTec Corporation

White Paper

Deploying and Using the CrossTec Gateway

Deploying and Using the CrossTec Gateway

With the increased use of the Internet a common question asked by customers using CrossTec Remote is “Can I connect to and remote control a machine behind a firewall?” or “Does CrossTec work with NAT?” This has been possible with previous versions of CrossTec Remote; however, to do so involved complex configurations of firewalls to allow incoming connections.

This became even more complex when both the CrossTec Control and Client were behind firewalls. In CrossTec Remote Version 8.0 we introduced a Gateway component that will simplify this method of connection and remove the need for Complex Firewall Configurations.

What Is the CrossTec Gateway?

The CrossTec Gateway is a component in CrossTec Remote Control Version 8.0, which provides a stable and secure method for connecting Clients and Controls via the Internet using HTTP, and delivers web-based remote control without the need for modifications to existing Firewall configurations.

The Gateway acts as a go between for a CrossTec Control and CrossTec Client, and when using a Gateway there is no direct communication between the Client and Control. When the CrossTec Client is configured to use the HTTP Protocol, the Client connects to the Gateway at start up using the HTTP Protocol.

A User at a CrossTec Control can then connect to the gateway using the HTTP Protocol and Browse for connected Clients, then connect to any number of Clients that are attached to that gateway.

As there is no direct connection between CrossTec Client and Control, and the protocol used is HTTP, this means that each of these can be situated behind a Firewall configured to use NAT (Network Address Translation) without the need to make configuration changes. In order for the Gateway to effectively connect a Client and Control, both the CrossTec Control and Client must be able to connect to the Gateway using the HTTP Protocol on the gateway's configured port (the Default Port is 443).

The Gateway can be located in various different Network locations as shown in the following Example Scenarios.

CrossTec Gateway Configuration Utility

Configuration

Gateway Port: WARNING: Changing the port number will result in the termination of all current connections and sessions

CMPI (secs): Comms. Management Packet Interval.

Gateway Event Log Files

These settings will only be applied when the Gateway service is restarted

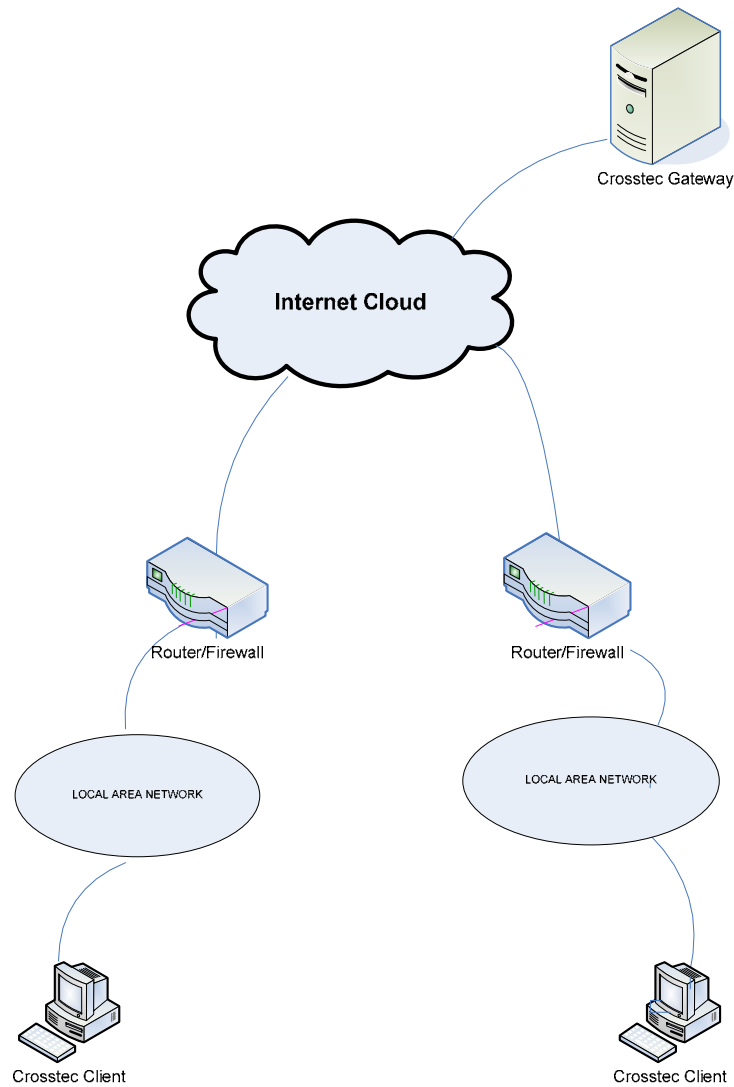
Location:

Maximum file size: Kb

Gateway Keys

Description	Creation Date
crosstec	Fri Jun 30 15:05:53 2006

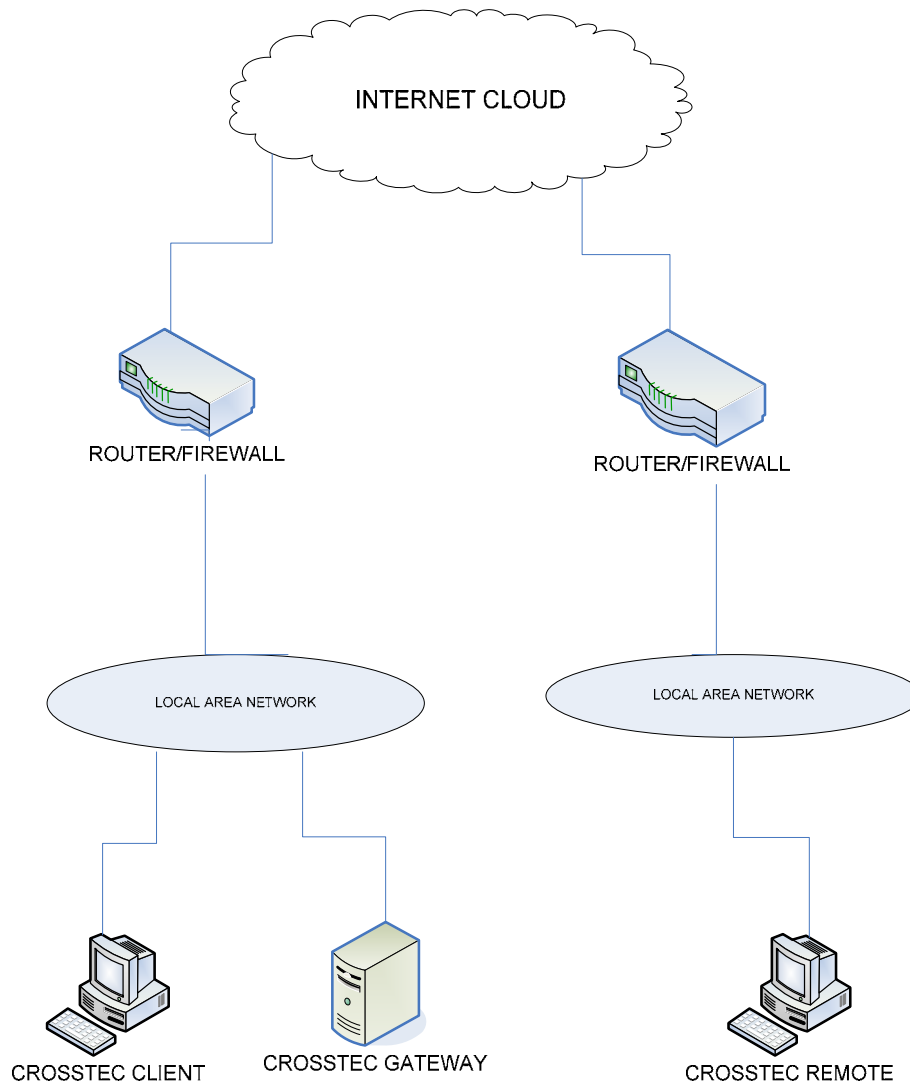
Scenario 1
CrossTec Gateway on the Public Internet



In this scenario the CrossTec Gateway is installed on the Public Internet. In this example No Configuration changes would normally need to be made to either of the firewalls. However the machine that is running the CrossTec Gateway is freely available on the Internet and could be open to an attack.

Scenario 2

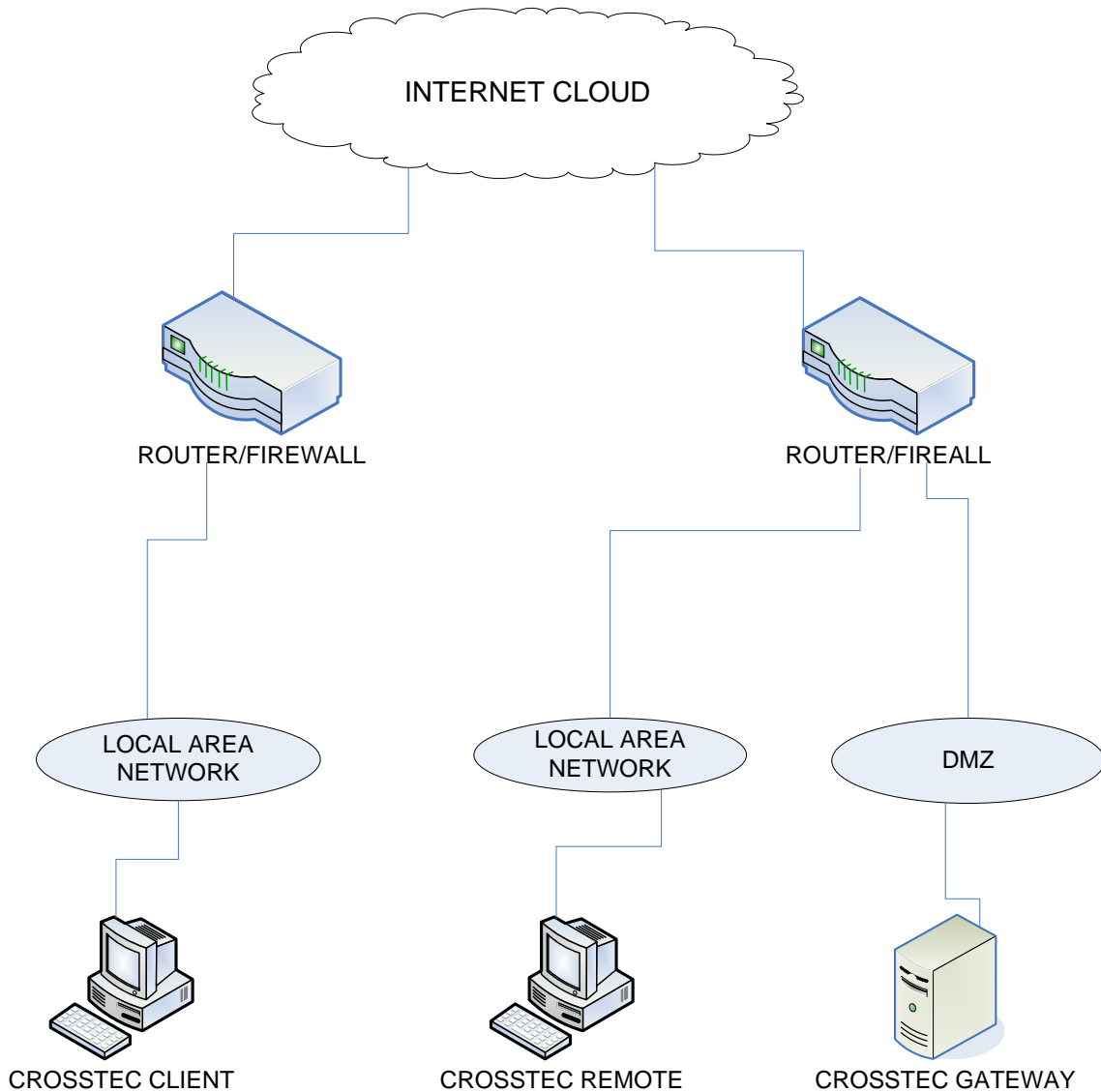
CrossTec Gateway on the Client Network



In this scenario the firewall at the CrossTec Client site would need to be configured to allow incoming HTTP Connections to the Gateway (on the CrossTec Gateways Configured Port Number). This would be similar to having a Web server installed at the CrossTec Client's Network and making this web server publicly available to users on the Internet.

The Advantage of this location for the gateway is that the machine running the CrossTec gateway is now protected from attack by a firewall. However this configuration does require some configuration changes to the firewall at the CrossTec Client's Site.

Scenario 3 CrossTec Gateway on a DMZ

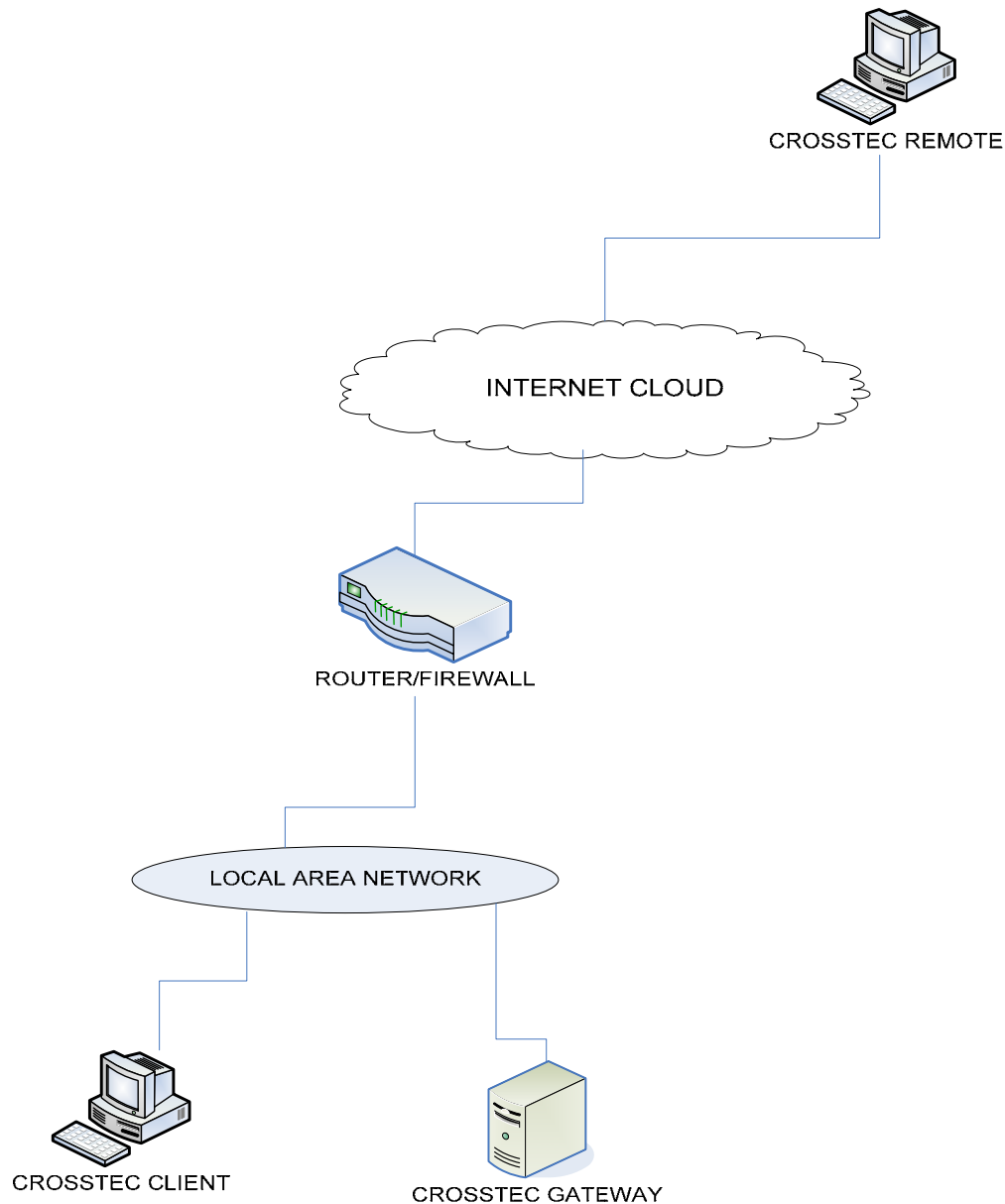


In this scenario the firewall at the CrossTec Control site would need to be configured to allow incoming HTTP Connections to the Gateway (on the CrossTec Gateways Configured Port Number). This would be similar to having a Web server installed on the DMZ and making this web server publicly available to uses on the Internet.

The Advantage of this location for the gateway is that the machine running the CrossTec gateway is now protected from attack by a firewall. However this configuration does require some configuration changes to the firewall at the CrossTec Controls Site

Scenario 4

CrossTec Gateway on the CrossTec Clients Network with a CrossTec Control on the public Internet



In this scenario the firewall at the CrossTec Client site would need to be configured to allow incoming HTTP Connections to the Gateway (on the CrossTec Gateways Configured Port Number). This would be similar to having a Web server installed at the CrossTec Clients Network and making this web server publicly available to users on the Internet. This Example could be used to Provide remote access to users working from home.

Installing the CrossTec Gateway

The CrossTec Gateway can only be used on an NT based Operating System (Win2k, NT, XP) as the CrossTec Gateway installs as a service. The Gateway is not installed by default. To install the CrossTec Gateway run the standard CrossTec Installation package.

When prompted for an installation type, select Custom. The Next screen should then display a list of CrossTec Components from this list of components select Gateway and continue through the installation. At the end of the Installation the "CrossTec Gateway Configuration Utility" will run as shown below

CrossTec Gateway Configuration Utility

Configuration

Gateway Port: WARNING: Changing the port number will result in the termination of all current connections and sessions

CMPI (secs): Comms. Management Packet Interval.

Gateway Event Log Files

These settings will only be applied when the Gateway service is restarted

Location:

Maximum file size: Kb

Gateway Keys

Description	Creation Date
Crosstec GW	Thu Jul 13 15:52:23 2006

Here you can set the Port Number that the Gateway will accept connections on. The Default Port is 443. The Default port for the HTTP Protocol on the Internet is Port 80 you can configure the Gateway to accept connections on port 80; however, some Internet service providers (ISPs) utilize Cache or Proxy servers that Cache HTTP Traffic on port 80, if your ISP uses a cache or Proxy server then the gateway connections will fail.

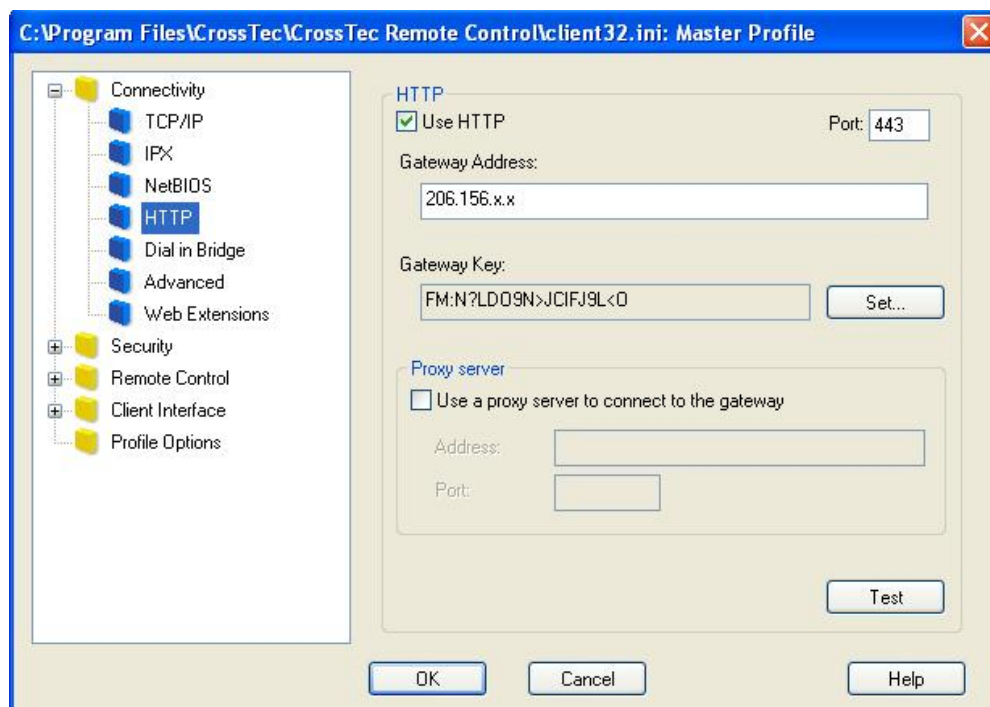
You can also specify the location and maximum size of the Gateways log file. The Logging functions of the gateway are explained in detail later in this document. You can also add a Gateway Key. Gateway keys are used to

authenticate CrossTec Clients and Controls, therefore ensuring that unauthorized users cannot use the Gateway. You must set at least one Gateway Key before you can apply the configuration as the Gateway will not accept any connections unless at least one Gateway Key is configured.

Setting up Clients to Use the Gateway

To configure a Client to use the HTTP protocol you will need to run the CrossTec Configurator.

- Run the Configurator and Press the “Basic” Button
- Open the “Connectivity” Group and select “HTTP” you should then see the HTTP Configuration shown below.



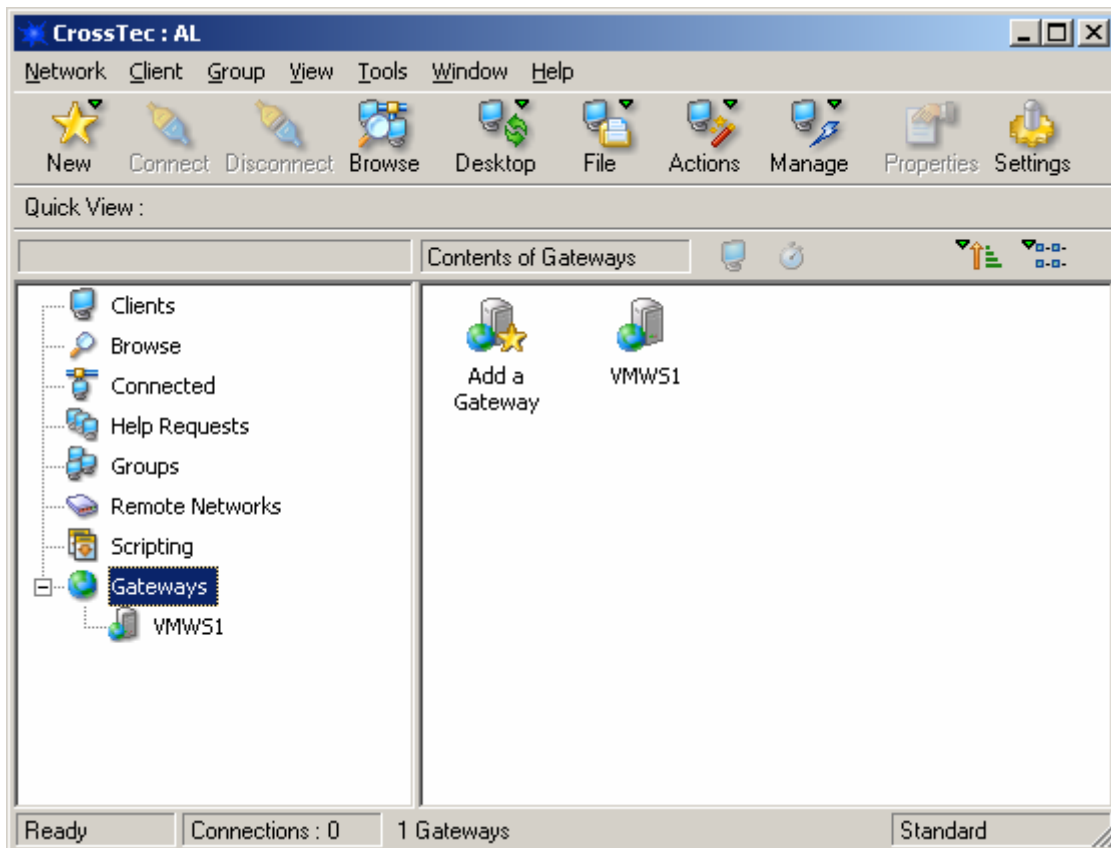
- To enable HTTP you will need to check the “Use HTTP” Option
- Enter the port number, which the Gateway you are going to use is configured for, the default being 443.
- Enter the TCP/IP address of the CrossTec Gateway.
- Press the “Set” Button to set a Gateway Key the key you set must be identical to one of the Gateway Keys added to the Gateway.

Once you have completed the configuration save the configuration and restart the CrossTec Client. The Client should then connect to the Gateway. The entire configuration for a CrossTec Client is stored in the Configuration file and this can be easily copied or Deployed (Using CrossTec Deploy) to other CrossTec Clients, for details see the Online Help or Manual.

Setting Up a Control to use the CrossTec Gateway

Before you can connect to a CrossTec Client using a CrossTec Gateway you must add that Gateway to your CrossTec Control. To do this, follow the steps below.

- Run the CrossTec Control
- In the left hand pane select the Gateways Group
- Double click on the “Add a Gateway” Icon
- At the first step give this Gateway and Name and Description here you can enter any details you wish that describe the Gateway.
- At the next step enter the IP Address of the Gateway and the Port that the gateway is configured for (Default is 443)
- At the next step press the “Set” Button and set the Gateway Key that you will use.



Note If the gateway is configured with multiple Gateway Keys then when you browse for Clients on this gateway you will only see Clients that are using the same Gateway Key that you enter here. You can have multiple gateways configured in your CrossTec Control with the same IP address but different Gateway Keys. Once you have a Gateway Configured in your control you can browse the Gateway for a list of connected Clients.

Securing the CrossTec Gateway

The Gateway can support multiple Gateway keys, each Key must be a minimum of 8 characters, and Gateway Keys can be added to the Gateway dynamically without disrupting any Current Connections. The Gateway will not accept connections from a CrossTec Control or Client unless a Gateway key Configured at the CrossTec Client or CrossTec Control has also been entered at the Gateway.

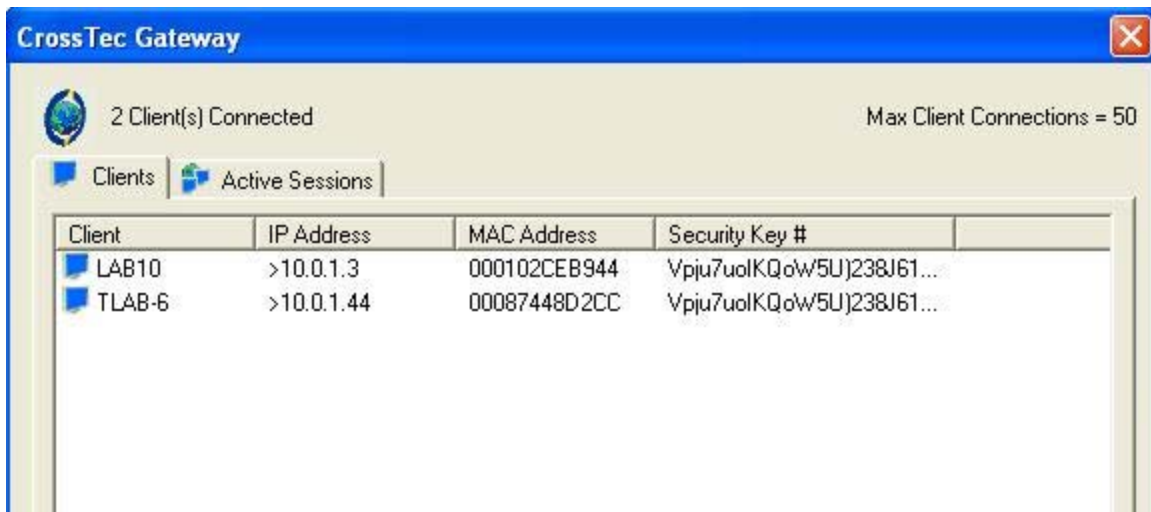
Clients support one key only and the Control is able to support multiple Gateways with different keys, all Gateway Key data is sent encrypted between the Client, Control and Gateway. Once connected to the Gateway all Client and Control security such as user names, Security Keys, etc... will function normally. A Control can only connect and Browse for clients that are using the same Gateway Key as the Control.

Gateway Key connection Matrix

CONTROL GATEWAY KEY	GATEWAY "GATEWAY KEYS"	CLIENT GATEWAY KEY	RESULTS
"TESTING 1"	"TESTING 2"	"TESTING 1"	No Connection from client or control
"TESTING2"	"TESTING1" "TESTING2"	"TESTING1"	Client connects to gateway but Control can not connect to this client or see the client in a browse
"TESTING1"	"TESTING1"	"TESTING1"	Client connects, Control can connect to the Client and see the Client in a browse
"TESTING2"	"TESTING1"	"TESTING2"	No Connection from client or control
"TESTING2"	"TESTING1" "TESTING2" "TEST3"	"TEST2"	Client connects, Control can connect to the Client and see the Client in a browse

Logging and Monitoring the CrossTec Gateway

The Gateway runs as a service and is displayed as an icon in the system tray. If you right click on this Icon a shortcut menu is displayed giving options to “Open”, “Configure” or “About”. If you select Open the CrossTec Gateway Status window is displayed The “Clients” Tab will show a list of all the CrossTec Clients currently connected to this Gateway.



The “Active Sessions” tab displays a list of current connections between a CrossTec Control and a CrossTec Client with the date and time that the connection started as shown below.



The CrossTec Gateway creates a log file that records activity through the Gateway. The log file name is gw001.log and is stored in the locations specified in the Gateway configuration dialog.

Gw001.log Example

08-Dec-02, 16:11:20, CrossTec V9.50, running on Windows NT 5.0, platform 2

08-Dec-02, 16:11:20, Gateway started, Max. Licensed connections: 5, listening port: 80

08-Dec-02, 16:15:32, Gateway stopped

The following is a list of events that are logged to the CrossTec Gateway Log file or Windows Event Viewer:

- **Gateway started. Mac licensed connections: <max_connections>**
This event is logged when the Gateway is first started.
- **Failed to start gateway**
This event is logged when the Gateway fails to start.
- **Gateway stopped**
This event is logged when the Gateway is stopped.
- **Listening on port <port_number>**
This event is logged when the Gateway starts listening on the specified port. This occurs during start-up and when a change in the Gateway port is applied in the Gateway Configurator.
- **Listening on port <port_number>**
This event is logged when the Gateway starts listening on the specified port. This occurs during start-up and when a change in the Gateway port is applied in the Gateway Configurator.
- **Failed to bind to listening port <port_number>**
This event is logged when the Gateway fails to assign the specified port to listen for incoming connections. The port is probably being used by another application.
- **Reloading configuration**
This event is logged by the Gateway when the administrator has used the Gateway Configurator to apply configuration changes.
- **Listen port has changed. All current connections and sessions will be terminated.**
This event is logged by the Gateway when the administrator modifies the listening port in the Gateway Configurator and then applies the change whilst the gateway is running.

Events Format

<product_name> <product_version>, running on <operating_system>
<operating_system_version> <operating_system_service_pack> (build
<build_number>), platform <platform_number>

This event is logged when the Gateway is first started. A typical example would be as follows:

CrossTec V9.50D, running on Windows NT 5.0 Service Pack 3 (build 2195),
platform 2

Reloading Gateway Keys

This event is logged by the Gateway when the administrator has used the Gateway Configurator to apply configuration changes – which may have included additions or removals to the list of Gateway keys.

- **Client <clientname> connected**
This event is logged when a Client connects to the Gateway
- **Client <clientname> disconnected**
This event is logged when a Client disconnects from the Gateway.
- **Control <controlname> connected to Client <clientname>**
This event is logged when a Control connects to a Client.
- **Control <controlname> disconnected from Client <clientname>**
This event is logged when a Control disconnects from a Client.
- **License exceeded. Rejecting connection from Client <clientname> (<real_ip_address>, <public_ip_address>)**
This event is logged when a client connecting to the Gateway would exceed the licensed number of Clients.
- **Security check failed for Client <clientname> (<real_ip_address>).**
- **Terminating connection from <public_ip_address>**
This event is logged when a new Client connection fails to provide a valid Gateway Key.
- **Security check failed for control browse. Terminating connection from <public_ip_address>**
This event is logged when a Control fails to provide a valid Gateway Key during a browse Clients request.
- **Security check failed for Control <controlname>. Rejecting connection request to Client <clientname> from <public_ip_address>**
This event is logged when a control fails to provide a valid Gateway Key during a connection request to a Client.
- **Client/Control security check failed for Control <controlname>.**
- **Rejecting connection request to Client <clientname> from <public_ip_address>**
This event is logged when the Gateway Key provided by the Control during a connection request to a client does not match the Gateway Key supplied by the Client.

Further Information

If you require any further information regarding CrossTec Remote, you can contact the CrossTec Technical Support Team using the following details:

Technical Support Department
Phone: 1-800-675-0729
Email: tech@CrossTeccorp.com

Visit us on the Web

Our web site: <http://www.CrossTeccorp.com/>
Support Knowledge Base: [Product Support](#)