FireTower Security Solution Installation Planning and Software Components

July 2017

Table of Contents:

1. Getting up and running on FireTower Security Solution for the first time

You should first assess your security requirements and familiarize yourself with the settings available within FireTower. This will help you decide if the default settings provide the balance between performance and security that you require.

Plan your installation structure

Step	Action	Description
1	Plan your installation structure	Before you install FireTower, consider the size and geographical distribution of your network to determine the installation architecture. To ensure good network and database performance, you need to evaluate several factors. These factors include how many computers need protection, whether any of those computers connect over a wide-area network. 1. If your network is small, is located in one building, and has fewer than 100 clients, you could install FireTower Server on a non-dedicated computer 2. If your network has more than 100 clients, you should install FireTower Server on a dedicated computer 3. If your network is geographically dispersed, you need to provide a routable IP address so those computers connect over a wide-area-network can communicate with the FireTower Server.

Prepare for and then install FireTower Server

Step	Action	Description
2	Prepare for and then install FireTower Server	1. Make sure the computer on which you install the FireTower server meets the minimum system requirements. Windows desktop Operating System 7/8/10 and Windows Server Operating System 2008/2012/2016 (x64 only) 2. To install FireTower Server, you must be logged on with an account with local administrator access. 3. You also need to provide data base server administration credentials to create the database and the database user. These are specifically for use with the FireTower server.

Step	Action	Description
		4. You install all the prerequisites first. After you install the prerequisites, you then install FireTower Server. You could choose the root administrator login ID to FireTower Cyber Console. Password is defaulted to "admin" and can be changed from FireTower Cyber management console

Add Groups, and Profiles

Step	Action	Description
3	Add groups, profiles	1. You use groups to organize the client computers, and apply a different level of security to each group. You can use the default domain or workgroup, or add new groups. If you add new groups, you can use the following group structure as a basis: (1) Computer types (desktops, laptops, servers), (2) locations (Boston, New York, D.C.), or (3) Organizations (Marketing, Sales, Customer Relations), etc. 2. You use grouping to apply different policies and settings to computers based on specific criteria. For example, you can apply different endpoint security protection profiles to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall. By default, groups inherit their policies and settings

Activate the Product License

Step	Action	Description
4	Activate the Product License	You need to enter the product key obtained from Sampan Security, Inc. or its Value-Added Resellers when you install FireTower Server. After the installation you will be able to see the license information from Cyber Console\Account Management Tab. Please contact Sampan Security, Inc. for FireTower Security Solution subscription renewal or for additional client licenses

Decide on a client deployment method

Step	Action	Description
5	Decide on a client deployment method	Determine which client deployment method would work best to install the client software on your computers in your environment. You could use a combination of deployment methods that best in your network environment. To manually install FireTower client software at client computers, you must be logged on with an account that grants local administrator access. If the client computers are part of an Active Directory domain, you must be logged on to the computer that hosts FireTower Server with an account that grants domain controller administrator access and credentials.

Prepare the Client for Installation

Step	Action	Description
6	Prepare the client for installation	1. Make sure that the computers on which you install the client software meet the minimum system requirements. Windows XP/Vista/7/8/10 (x86 or x64) and Windows 2003/2008/2012/2016 (x86 or x64) 2. All the client computers to be deployed remotely with FireTower client software must have the file sharing option turned on (Control Panel\Network and Sharing Center\Change Advanced Sharing Settings) 3. You should also install the FireTower client software on the computer that hosts FireTower Server 4. Depending on the Anti-Virus software already installed on the client computers, you may have to temporarily deactivate the AV software during installation.

Deploy to install client software

Step	Action	Description
7	Deploy to install client software	For each grouping, you could assign different administrator (by creating a user account and associate it with the designated group) and different endpoint protection profile. Each client computer could associate with more than one group. Create a custom enrollment package with a specific endpoint protection profile and deploy to those clients assigned to this group, or you could create a generic enrollment package and install to all client computers and manually assign the grouping, group administrator and endpoint protection profile using Cyber Management Console.

Client Installation Verification

Step	Action	Description
8	Check that the computers are listed in the groups that you expected and that the clients communicate with the FireTower Server	In the Cyber Management Console, on the Dashboard, click any group on the upper left pane should display at the bottom left pane all the client computers enrolled and associated with that group with the icon in Green (live through client computer heartbeat)

2. Software Components of FireTower Security Solution

Component	Description
FireTower Server	FireTower Server is a management server that manages the client computers that connect to enterprise network FireTower Server includes the following subcomponents: 1. Secure communication to and from the client computers and the server 2. The Cyber Management Console is the interface to the FireTower Server. The Cyber Console coordinates and manages client computers persistence mechanism change

	event authentication and stack up in the enterprise threat database maintained at the FireTower Server. 3. The embedded enterprise threat database stores security profiles and events from all the client computers together with real-time authentication. 4. Inter-Host Intrusion Prevention System with built-in analytics enables continuous monitoring and incident response investigation of Zero-day and advanced attacks. 5. Cyber Console for Windows and for Browser can remote log on to the FireTower Server with an intranet or internet connection.
FireTower Endpoint Client	The FireTower Client software runs on the following Windows computers (Windows Desktop Operating Systems: XP/Vista/7/8/10 and Windows Server Operating Systems: 2003/2008/2012/2016) (x86 and x64)
Autorun Setting Repository (ASR)	A cloud-based Autorun Setting Repository (ASR) is used for persistence mechanism authentication. ASR provides FireTower client detection scheme with ratings for Autorun entries and identifies them as known good, known bad, or unknown (possibly zero-day)

3. System Requirements for FireTower Security Solution

Component	Requirements
Client Computer Operating System (Desktop)	Windows Desktop Operating Systems: XP/Vista/7/8/10 (x86 or x64)
Client Computer Operating System (Server)	Windows Server Operating Systems: 2003/2008/2012/2016 (x86 or x64)
FireTower Server Operating System (Desktop)	Windows Desktop Operating Systems: 7/8/10 (x64 only) Dedicated computer or shared with other applications

FireTower Server Operating System (Server)	Windows Server Operating Systems: 2008/2012/2016 (x64 only) Dedicated computer or shared with other applications

4.   Internationalization requirements

Current availability: English and Japanese

Unicode based software can be easily translated to other languages.

5.   Network Architecture Considerations

1. Local and remote computers: Remote computers may have slower network connections. You may want to use a different installation method than the one you use to install to local computers
2. Portable computers such as notebook computers: Portable computers can connect to FireTower Server remotely if FireTower Server has a routable IP address or DNS server.
3. Computers that are located in secure areas: Computer that are located in secure areas may need different endpoint protection profile settings from the computers that are not located in secure areas.
4. Remote Console: Administrators can use a remote computer that runs the Cyber Console for Windows software to access FireTower server (with routable IP address or DNS service). Administrators may use a remote computer when they are away from the office. You should ensure that remote computers meet the remote console requirements.