## About this Document

### 1 Before you begin
- About the UTM Firewall Control Center
- About policies
- About device groups
- About device attributes
- Control Center Web interface
- Shortcuts
- Navigation menu
- Planning your Control Center network
- Defining necessary attributes
- Defining groups

### 2 Getting Started
- Setup overview
- Requirements
- VMware
- Supported devices
- System requirements
- McAfee Firewall Reporter
- Setting up the Control Center
- Installing the Control Center
- Starting the Control Center
- Logging into the Control Center
- Configuring the Control Center for device management
- Configuring McAfee UTM Firewall devices for Control Center management
- Setting attributes
- Enabling Control Center management
- Registering devices
- Common administrative tasks

### 3 Monitoring
- Monitoring devices
- Device Group Status
- Devices with Status
- Device Status
- Working with the device groups pane
- Checking task progress
- Viewing recent events

### 4 Definitions
- Defining device attributes from the Control Center
- Working with group views
  - Creating group views
  - Modifying group views
  - Creating device groups

### 5 Policies
- Policy overview
- Working with policies
  - Creating policies
  - Editing and deleting policies
- Networking policies
  - Enabling DNS Proxy
## Contents

- Creating a wireless policy ........................................ 39
- Firewall policies .................................................. 40
- Configuring Packet Filtering rules ................................. 40
- Creating Content Filtering rules .................................. 42
- Limiting Incoming Access .......................................... 44
- VPN policies .......................................................... 45
- Creating PPTP Client connections ................................. 45
- Creating PPTP Server connections ................................. 47
- Creating L2TP Client connections ................................. 48
- Creating L2TP Server connections ................................. 50
- Creating IPsec VPN Tunnel policies .............................. 51
- System policies ...................................................... 57
- Creating time policies ............................................. 57
- Creating user policies ............................................. 58

### 6 Operations

- Updating device firmware ......................................... 61
- Rebooting devices ................................................ 62
- Refreshing device configuration .................................. 62
- RSA Keys ............................................................. 63
- Images ............................................................... 64

### 7 Managing the Control Center

- About the System page ............................................ 65
- Control Center ...................................................... 65
- System Setup ....................................................... 66
  - General Control Center settings ............................... 66
  - Date and Time settings ....................................... 67
- Network Setup ..................................................... 70
  - Configuring the Control Center LAN connection ............ 70
  - Routes ............................................................ 73
  - DNS Hostnames ................................................ 74
- Users ................................................................. 75
  - Changing the current user password ......................... 75
  - Managing users ............................................... 75
  - Managing user groups ....................................... 77
  - NT domains ..................................................... 79
  - RADIUS .......................................................... 80
  - TACACS+ .......................................................... 81
  - Password classes ............................................. 81
  - Service Authentication ....................................... 84
- Management ......................................................... 85
  - Web configuration ............................................. 85
  - Certificates for HTTPS ....................................... 86
  - Command line access .......................................... 93
- Diagnostics .......................................................... 93
  - Viewing diagnostic information ............................... 93
  - Viewing the local system log .................................. 95
  - Performing network tests ..................................... 98
- Advanced ............................................................ 100
  - Halting the Control Center before powering down ....... 100
  - Rebooting the Control Center ................................ 101
  - Upgrading the Control Center ................................ 101
  - Configuration Files ........................................... 104
  - Directly viewing or editing the configuration files ....... 107
- Support ............................................................... 107
  - Technical support reports ..................................... 108
  - Backing up the Control Center ............................... 109

## Index

- 111
About this Document

This guide describes the features and capabilities of your McAfee® UTM Firewall Control Center (formerly SnapGear® CMS).

This guide is intended for network and security administrators. This guide assumes familiarity UTM Firewall devices and firmware, VMware Server and virtual machines, UNIX and Windows operating systems, system administration, the Internet, networks, and related terminology.

You can find additional information at the following locations:

- **Help** – Help is built into the UTM Firewall Management Console. Click the Help icon in the upper right corner of the Management Console screen.
- **Support** – Visit mysupport.mcafee.com to find product documentation, announcements, and support.
- **Product updates** – Visit my.securecomputing.com to download the latest McAfee UTM Firewall updates.

Refer to Table 1 for a list of the text conventions used.

### Table 1 Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Courier bold</td>
<td>Identifies commands and key words you type at a system prompt.</td>
</tr>
<tr>
<td>Note: A backslash () signals a command that does not fit on the same line. Type the command as shown, ignoring the backslash.</td>
<td></td>
</tr>
<tr>
<td>Courier italic</td>
<td>Indicates a placeholder for text you type</td>
</tr>
<tr>
<td>&lt;Courier italic&gt;</td>
<td>Indicates optional text</td>
</tr>
<tr>
<td>nnn.nnn.nnn.nnn</td>
<td>Indicates a placeholder for an IP address you type</td>
</tr>
<tr>
<td>Courier plain</td>
<td>Used to show text that appears on a computer screen</td>
</tr>
<tr>
<td>Plain text italics</td>
<td>Identifies the names of files and directories</td>
</tr>
<tr>
<td>Used for emphasis (for example, when introducing a new term)</td>
<td></td>
</tr>
<tr>
<td>Plain text bold</td>
<td>Identifies buttons, field names, and tabs that require user interaction</td>
</tr>
<tr>
<td>[ ]</td>
<td>Signals conditional or optional text and instructions (for example, instructions that pertain only to a specific configuration)</td>
</tr>
<tr>
<td>Caution</td>
<td>Signals be careful—in this situation, you might do something that could result in the loss of data or an unpredictable outcome.</td>
</tr>
<tr>
<td>Note</td>
<td>Used for a helpful suggestion or a reference to material not covered elsewhere in the guide</td>
</tr>
<tr>
<td>Security Alert</td>
<td>Identifies information that is critical for maintaining product integrity or security</td>
</tr>
<tr>
<td>Tip</td>
<td>Indicates time-saving actions; may help you solve a problem</td>
</tr>
</tbody>
</table>

*Note*: The IP addresses, screen captures, and graphics used within this document are for illustration purposes only. They are not intended to represent a complete or appropriate configuration for your specific needs. Features may be enabled in screen captures to make them clear; however, not all features are appropriate or desirable for your setup.
### Before you begin

#### Contents
- About the UTM Firewall Control Center
- Control Center Web interface
- Planning your Control Center network

## About the UTM Firewall Control Center

The McAfee UTM Firewall Control Center is a management tool for creating and applying policies to multiple Snapgoer devices. The UTM Firewall Control Center is packaged as a virtual appliance, making it platform-independent so the Control Center can run on any system that has VMware Server installed.

The Control Center virtual appliance organizes UTM Firewall devices into device groups. Device groups provide administrators with the ability to selectively apply policies, and to apply policies to several devices at one time.

A Control Center-managed network consists of three distinct parts: an administrative workstation, the system housing the Control Center virtual appliance, and the managed UTM Firewall devices (Figure 1).

#### Figure 1  Control Center network

![Control Center network diagram]

### About policies

Policies are groups of configuration settings. Policies are created in the Control Center and pushed down to managed devices. Each policy is assigned to a different device group. For example, a policy named Remote_Sales_Tunnel might contain IPSec tunnel rules for the Remote_Sales device group. When applied, this policy would configure IPSec Tunnel settings on every UTM Firewall device assigned to the Remote_Sales group.
About device groups

Device groups consist of one or more Snapgear devices. When creating device groups, administrators can select individual devices, or all devices that share common attributes. By assigning a policy to a device group, administrators can apply policies to multiple devices at one time. Commonly used device groups organize UTM Firewall devices by geographical region (for example, city or country), by business division (for example, sales or engineering), or by hardware model (for example, SG565 or SG720).

About device attributes

Attributes are defined by administrators in order to organize devices that share common traits into device groups.

Each UTM Firewall device comes with two built-in attributes:

- **type** – The hardware model of the device, for example, SG565 or SG720.
- **version** – the firmware version currently installed on the device, for example, 3.2 or 4.0.

Additional attributes can be defined for each device. A UTM Firewall device located in St. Paul, Minnesota (USA) used to control traffic for a sales team might have the following additional attributes and attribute values (Table 2).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>region</td>
<td>North America</td>
</tr>
<tr>
<td>country</td>
<td>USA</td>
</tr>
<tr>
<td>state</td>
<td>Minnesota</td>
</tr>
<tr>
<td>city</td>
<td>St. Paul</td>
</tr>
<tr>
<td>department</td>
<td>sales</td>
</tr>
</tbody>
</table>
Control Center Web interface

The UTM Firewall Control Center Web interface provides the primary means of configuring the Control Center virtual appliance (Figure 2).

Figure 2  Control Center Web interface

Shortcuts

Three shortcut buttons are provided in the upper right corner of the window to guide you directly to common tasks. The shortcuts are:

- **Home** – Clicking on either the McAfee logo or the **Home** button returns you to the **Monitoring** page.
- **Logout** – Click the **Logout** button to log out of the Control Center.
- **Help** – Provides Help for setting up the Control Center virtual appliance.

Navigation menu

This menu lists the four functional areas of the Control Center. Clicking a menu item takes you to the associated page. Each management area is discussed in its own chapter.

A brief overview of each functional area and their associated tabs is provided in **Table 3**.

Table 3  Navigation menu functional areas and associated tabs

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Tab</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONITORING</td>
<td>DEVICES</td>
<td>Lists the devices the Control Center is managing; provides both group summaries and individual device statuses</td>
</tr>
<tr>
<td></td>
<td>TASK QUEUE</td>
<td>Provides a list of the tasks the Control Center has performed, and allows for specific failed tasks to be retried</td>
</tr>
<tr>
<td></td>
<td>EVENT LOG</td>
<td>Provides a log of the Control Center activity</td>
</tr>
</tbody>
</table>
### Before you begin

**Control Center Web interface**

#### DEFINITIONS
The Definitions page enables the setting of device attributes and the creation of device groups and group views.

**Attributes**
- Lets you create attributes for sorting devices, and assign values to devices

**Group Views**
- Allows you to create different group views for monitoring your devices

**Device Groups**
- Provides a means to create groups of UTM Firewall devices for the easy application and distribution of policies

#### POLICIES
The Policies page allows you to create and edit policies and apply them to groups of managed devices.

**NETWORKING**
- **DNS Proxy** – Lets you enable DNS proxy for any number of devices
- **Traffic Shaping** – Allows you to enable traffic shaping and specify services for your devices
- **Wireless** – Provides a means to set the Extended Service Set ID and Wi-Fi Protected Access for managed devices

**FIREWALL**
- **Packet Filtering** – Lets you set Packet Filtering rules for multiple devices
- **Content Filtering** – Provides a means to enable content filtering and allows for the creation of block and allow lists
- **Incoming Access** – Lists the interfaces that the managed devices allow traffic on

**VPN**
- **PPTP Client** – Lets you push VPN settings down to managed devices
- **PPTP Server** – Allows you to enable PPTP servers and manages server authentication
- **L2TP Client** – Provides a means to push L2TP settings down to managed devices
- **L2TP Server** – Allows L2TP server authentication management
- **IPsec Managed Endpoint** – Allows you to designate managed devices as endpoints and to specify tunneled networks
- **IPsec Unmanaged Endpoint** – Allows you to designate endpoints that are not managed by the Control Center and to specify tunneled networks
- **IPsec Tunnel Settings** – Enables you to set IPsec VPN security settings for tunneled networks
- **IPsec Tunnel Mappings** – Provides a means of mapping tunnels to endpoints

**SYSTEM**
- **Time** – Lets you enable an NTP time server and allows configuration of NTP hosts
- **Users** – Allows you to configure user permissions for devices

#### OPERATIONS
The Operations page includes options for upgrading device firmware.

**DEVICE OPERATIONS**
- Lets you push firmware upgrades down to devices; also allows devices to restart

**IMAGES**
- Enables uploading of device firmware images to the Control Center

---

**Table 3 Navigation menu functional areas and associated tabs (continued)**

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Tab</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFINITIONS</td>
<td>Attributes</td>
<td>Lets you create attributes for sorting devices, and assign values to devices</td>
</tr>
<tr>
<td>DEFINITIONS</td>
<td>Group Views</td>
<td>Allows you to create different group views for monitoring your devices</td>
</tr>
<tr>
<td>DEFINITIONS</td>
<td>Device Groups</td>
<td>Provides a means to create groups of UTM Firewall devices for the easy application and distribution of policies</td>
</tr>
<tr>
<td>POLICIES</td>
<td>NETWORKING</td>
<td>DNS Proxy – Lets you enable DNS proxy for any number of devices</td>
</tr>
<tr>
<td>POLICIES</td>
<td>NETWORKING</td>
<td>Traffic Shaping – Allows you to enable traffic shaping and specify services for your devices</td>
</tr>
<tr>
<td>POLICIES</td>
<td>NETWORKING</td>
<td>Wireless – Provides a means to set the Extended Service Set ID and Wi-Fi Protected Access for managed devices</td>
</tr>
<tr>
<td>POLICIES</td>
<td>FIREWALL</td>
<td>Packet Filtering – Lets you set Packet Filtering rules for multiple devices</td>
</tr>
<tr>
<td>POLICIES</td>
<td>FIREWALL</td>
<td>Content Filtering – Provides a means to enable content filtering and allows for the creation of block and allow lists</td>
</tr>
<tr>
<td>POLICIES</td>
<td>FIREWALL</td>
<td>Incoming Access – Lists the interfaces that the managed devices allow traffic on</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>PPTP Client – Lets you push VPN settings down to managed devices</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>PPTP Server – Allows you to enable PPTP servers and manages server authentication</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>L2TP Client – Provides a means to push L2TP settings down to managed devices</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>L2TP Server – Allows L2TP server authentication management</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>IPsec Managed Endpoint – Allows you to designate managed devices as endpoints and to specify tunneled networks</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>IPsec Unmanaged Endpoint – Allows you to designate endpoints that are not managed by the Control Center and to specify tunneled networks</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>IPsec Tunnel Settings – Enables you to set IPsec VPN security settings for tunneled networks</td>
</tr>
<tr>
<td>POLICIES</td>
<td>VPN</td>
<td>IPsec Tunnel Mappings – Provides a means of mapping tunnels to endpoints</td>
</tr>
<tr>
<td>POLICIES</td>
<td>SYSTEM</td>
<td>Time – Lets you enable an NTP time server and allows configuration of NTP hosts</td>
</tr>
<tr>
<td>POLICIES</td>
<td>SYSTEM</td>
<td>Users – Allows you to configure user permissions for devices</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>DEVICE OPERATIONS</td>
<td>Lets you push firmware upgrades down to devices; also allows devices to restart</td>
</tr>
<tr>
<td>OPERATIONS</td>
<td>IMAGES</td>
<td>Enables uploading of device firmware images to the Control Center</td>
</tr>
</tbody>
</table>
Before you begin
Control Center Web interface

Table 3  Navigation menu functional areas and associated tabs (continued)

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Tab</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>UCC</td>
<td>Enables the Control Center; establishes registration passwords and Control Center ports; allows public key downloading</td>
</tr>
<tr>
<td></td>
<td>System Setup</td>
<td>Device – Records basic information about the Control Center, Date and Time – Sets the time and date for the Control Center.</td>
</tr>
<tr>
<td></td>
<td>Network Setup</td>
<td>Connections – Configures connections to the Control Center, DNS – Specifies static hosts for DNS</td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td>Current User – Edits preferences and password of the user currently logged into the Control Center, Users – Sets passwords for user groups, Groups – Configures permissions for user groups, Domain – Configures Windows workgroup settings, RADIUS – Configures RADIUS servers, TACACS+ – Configures TACACS+ servers, Passwords – Manages password classes, PAM – Manages authentication policies</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td>Web – Enables management over HTTP and HTTPS and specifies ports and protocols used, Command Line – Enables Telnet and SSH for the Control Center</td>
</tr>
<tr>
<td>Diagnostics</td>
<td></td>
<td>System – Provides general information about the Control Center instance, System Log – Provides a detailed report of all Control Center activity, and sets syslog parameters, Network Tests – Performs a ping or traceroute to the IP address of the Control Center virtual appliance</td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
<td>Reboot – Restarts the Control Center, Software Upgrade – Upgrades the Control Center, Configuration Files – Allows editing and uploading of individual configuration files, Device Config – Allows the direct modification of configuration settings</td>
</tr>
<tr>
<td>Support</td>
<td></td>
<td>Technical Support – Provides links to technical support, Technical Support Report – Enables downloading of report for inclusion in technical support queries</td>
</tr>
</tbody>
</table>
Planning your Control Center network

It is important to take time to plan your Control Center network. This section covers planning considerations for assigning device attributes and creating device groups.

Defining necessary attributes

List all the UTM Firewall devices you will be managing with the Control Center. Identify the following for each device:

- hardware model
- firmware version
- physical location
- network location (for example, is the device part of a LAN, does it face the Internet or the DMZ?)
- IP address
- business unit the device is serving
- primary function (routing e-mail or Web traffic, for example)
- secondary function (for example, does the device serve as a back-up for another UTM Firewall?)

This list will help you identify the attributes that need to be defined on each device before they are managed by the Control Center.

For more information about attributes, see Setting attributes on page 20.

Defining groups

Once you know the various attributes you will be defining for your managed devices, you can decide what device groups should be created.

Device groups should be organized in such a way that the devices in a group require similar configuration settings. For example, in your organization, perhaps all SnapGears used by remote users must be accessed over an IPsec tunnel. You could create a device group called Remote_Accesss that contains all such UTM Firewall devices.

For more information about device groups, see Creating device groups on page 33.
Getting Started

Contents
Setup overview
Requirements
Setting up the Control Center
Configuring McAfee UTM Firewall devices for Control Center management
Common administrative tasks

Setup overview

The steps involved in setting up your McAfee UTM Firewall Control Center network are:

1. **Meet requirements.** See Requirements on page 13
2. **Install the Control Center.** See Installing the Control Center on page 15.
3. **Define device attributes.** See Setting attributes on page 20.
4. **Enable the Control Center.** See Enabling Control Center management on page 20.
5. **Register devices.** See Registering devices on page 22.
6. **Create group views.** See Creating group views on page 32.
7. **Create device groups.** See Creating device groups on page 33.

**UTM Firewall appliance:** Some of these procedures are performed on your managed UTM Firewall devices. These procedures are proceeded by a "UTM Firewall appliance" note.

Requirements

This section covers the requirements for setting up your McAfee UTM Firewall Control Center (UCC).

**VMware**

The Control Center comes packaged as a virtual appliance. The UTM Firewall Control Center 2.0 virtual appliance can be installed on any system running VMware Server. You can download the latest version of VMware Server from www.vmware.com/download/server.

Instructions for the use of VMware Server are beyond the scope of this document. VMware documentation is available from www.vmware.com.

**Supported devices**

Control Center 2.0.2 supports UTM Firewall devices with firmware version 3.2.1 or higher. The latest firmware version are available from my.securecomputing.com. For instructions on upgrading device firmware, refer to the McAfee UTM Firewall Administration Guide.
System requirements

This section lists the requirements necessary for running and installing McAfee UTM Firewall Control Center version 2.0.

Minimum system requirements

- **CPU** – Pentium 4 2.8 GHz
- **Disk space** – 10 GB
- **RAM** – 1 GB

Recommendation for managing 25 to 250 devices

- **CPU** – Pentium 4 2.8 GHz
- **Disk space** – 20 GB
- **RAM** – 2 GB

McAfee Firewall Reporter

McAfee Firewall Reporter is a reporting solution that offers real-time data collection, monitoring, and correlated alerts to help you manage your network activity.

McAfee Firewall Reporter is free with any new UTM Firewall device purchase, and can be downloaded from http://my.securecomputing.com. McAfee Firewall Reporter can be purchased for UTM Firewall devices ordered prior to July 2007.

For McAfee Firewall Reporter system requirements, see the McAfee Firewall Reporter Product Guide available from the Knowledgebase at mysupport.mcafee.com.
Setting up the Control Center

The following sections lead you through installing and logging into the Control Center, and configuring the Control Center for device management.

Installing the Control Center

Follow these steps to install the Control Center.

1. Open a browser and log into my.securecomputing.com. If you have not already done so, create an account and register your appliances.

   Figure 3  My Secure Computing – Welcome page

2. Within my.securecomputing.com, click Activate Control Center/CMS Virtual Machine. The Product Management – Activate McAfee UTM Firewall Control Center page appears (Figure 4).
3 Enter the **McAfee UTM Firewall Control Center Serial Number** included in your McAfee UTM Firewall Control Center Activation Certificate e-mail, and click **Next**. The license agreement displays describing terms and conditions.

4 Once you have read the agreement, click **I Agree**. The CMS Download page appears.

5 Click **Download** to download the .zip file containing the Control Center virtual machine.

**Starting the Control Center**

These instructions assume you are using VMWare Workstation. If you are using a different VMWare program, such as VMWare Server or VMWare ESX, the details may be slightly different, but the procedures should be similar.

To start the Control Center virtual appliance:

1 Unzip the **UCC.zip** file to the folder on the Host Server where you store VMWare images.

   The **UCC.zip** file contains a **UCC_Workstation.zip** file and a **UCC_ESX.zip** file (for VMWare ESX users).

2 Unzip the **UCC_Workstation.zip** file.

3 Open the VMWare Workstation
4 On the Home tab, select the **Open Existing VM or Team** icon (Figure 5).

**Figure 5 Home tab**

5 Browse to the UCC.vmx file and click **Open**. The UCC tab appears (Figure 6).

**Figure 6 UCC tab**
6 In the Commands list, select **Power on the virtual machine**. The Control Center console screen appears (Figure 7).

![Figure 7 UCC console screen](image)

7 Once the console has stopped scrolling and you are presented with a “#” sign, click on the console window, and press **Enter**. The Control Center IP address is displayed (Figure 8).

![Figure 8 Control Center IP address displayed in CMS console screen](image)

The Control Center will either use the DHCP-assigned IP address, or default to 192.168.0.1.

8 Press **Control + Alt** to return to your computer.

### Logging into the Control Center

To log into the Control Center:

1 Open a browser and navigate to the IP address of your virtual machine. The Login screen appears (Figure 9).

![Figure 9 Login window](image)

2 Enter your user name and password to log into the Control Center. The default user name/password is **root/default**. You are prompted to change this user name the first time you log in.

### Logging out of the Control Center

You can log out at any time by clicking the red **Logout** icon in the upper right corner of the screen.
Configuring the Control Center for device management

In order for the Control Center to manage devices, enable the Control Center and set a registration password.

To enable the Control Center and set the registration password:

1. Log into the Control Center.
2. From the navigation menu, click SYSTEM. The UCC page appears (Figure 10).

**Figure 10  UCC page**

3. Select the Enabled check box. This allows devices to connect to the Control Center virtual appliance.
4. Enter a password in the Registration password and Confirm fields. The registration password will be used to authenticate devices when they attempt to connect to the Control Center (see Configuring McAfee UTM Firewall devices for Control Center management on page 20).
5. [Optional] The first time a device connects to the Control Center, it is vulnerable to “man-in-the-middle” attacks. To prevent such an attack, you can specify the Control Center RSA public key on the device before connecting. To download the public key file, click Download public key.
   
   **Note:** The public key is automatically configured on managed devices once they are registered with the Control Center. This ensures the security of all subsequent connections with managed devices.
6. Click Submit.
Configuring McAfee UTM Firewall devices for Control Center management

Configuring a UTM Firewall device for use with the Control Center is a three-part process: setting attributes, enabling Control Center management, and registering the device.

Setting attributes

Each UTM Firewall device possesses attributes which are determined by the device type and version. Others attributes are user-defined. The Control Center groups devices according to these attributes. Device groups are used to monitor devices, and to assign policies (see Working with group views on page 32 and Creating device groups on page 33).

UTM Firewall appliance: This procedure is performed on each UTM Firewall device that the Control Center manages.

To define an attribute:

1. Log into the UTM Firewall Management Console.
2. In the System menu, click Management and select the UCC tab.
3. Select the UCC Attributes tab. The UCC Device Attributes page appears.
4. Click New. The Edit UCC Device Attribute page appears (Figure 11).

Figure 11  UTM Firewall Edit UCC Device Attributes page

5. The following information is used to characterize the device for grouping:
   - **Attribute Name** – Enter a name for the attribute (for example: Company, Department, Region, Location, or BranchType).
   - **Attribute Value** – Enter a value for the attribute that corresponds with the Attribute Name (for example, if the Attribute Name is Region, the Attribute Value might be Northwest).
6. Click Finish.

Enabling Control Center management

McAfee UTM Firewall Control Center uses a dynamic registration model for adding UTM Firewall devices. This means that to add a device to the Control Center, you configure the device with the details of the Control Center virtual appliance, and then the device appears in the Control Center.

UTM Firewall appliance: This procedure is performed on each UTM Firewall device that the Control Center manages.

To enable Control Center management:

1. On the UTM Firewall Management Console, from the System menu, click Management.
2. Select the UCC tab. The UTM Firewall Control Center Configuration page appears (Figure 12).
3 Select the **Enable Central Management** check box.

4 Enter the **IP address of UCC**.

5 [Conditional] If you have the RSA public key for the Control Center, click the **Browse** button next to the Upload public key field, and navigate to the public key file.

6 Enter the Registration password in the **Registration password** and **Confirm password** fields.

7 Click **Submit**. The device appears in the Control Center device group pane (**Figure 13**).
Registering devices

Before applying policies to UTM Firewall devices, those devices must be registered with the Control Center. When you first log into the Control Center, the Monitoring page is open to the Devices tab. On the left side of the page is the device group pane. The device group pane lists all the UTM Firewall devices enabled for Control Center management (Figure 13).

**Figure 13 Initial group view**

To see all the devices that have been enabled for Control Center management, but have not yet been registered, select **Show Unregistered** from the Device Groups drop-down list. The device group pane is now populated only with unregistered devices (Figure 14).

**Figure 14 Unregistered devices in the device group pane**
To register a device with the Control Center:

1. From the device group pane, select the unregistered device (if the devices are not visible, select **Show Devices** from the Device Groups drop-down menu). The Device Status page appears (**Figure 15**).

   **Figure 15  Device Status page for an unregistered device**

   ![Device Status page for an unregistered device](image)

2. Click **Register**. A Status bar appears at the bottom of the screen indicating that the register operation has been initiated.

3. Click the **Refresh** button above the device group pane. The newly registered device no longer appears in the device group pane (select **Show Registered** from the Device Groups drop-down menu to see the device).
Common administrative tasks

Your devices are enabled for Control Center management, have their Control Center attributes set and are registered with the Control Center. You can start monitoring devices, creating policies, performing upgrades, and modifying device settings, all from the Control Center Web interface.

Common administrative tasks include:

- **Managing Control Center device registration.** See *Registering devices on page 22.*
- **Planning for and creating group views.** See *Working with group views on page 32.*
- **Planning for and creating groups.** See *Creating device groups on page 33.*
- **Creating and applying security and networking policies.** See *Working with policies on page 35.*
- **Checking policy compliance.** See *Working with policies on page 35.*
- **Setting up accounts for other administrators.** See *Creating a user on page 76.*
- **Cloning your Control Center VMware Image for DR scenarios.** For VMware documentation, go to www.vmware.com.
- **Updating the Control Center.** See *Upgrading the Control Center on page 101.*
- **Updating device firmware.** See *Updating device firmware on page 61.*
- **Monitoring device status views.** See *Monitoring devices on page 25.*
- **Inspecting managed device logs with the Control Center and McAfee Firewall Reporter.** See *Viewing recent events on page 30,* and the *McAfee Firewall Reporter Product Guide* available from the KnowledgeBase at mysupport.mcafee.com.
- **Inspecting Control Center logs.** See *Viewing the local system log on page 95.*
- **Rebooting the Control Center.** See *Advanced on page 100.*
- **Rebooting devices.** See *Rebooting devices on page 62.*
Monitoring

Contents

Monitoring devices
Checking task progress
Viewing recent events

Monitoring devices

When you first log into the McAfee UTM Firewall Control Center, the Devices tab of the Monitoring page is shown. This tab provides a quick snapshot of the devices being managed by the Control Center, and provides status indicators for each device (Figure 16).

Figure 16 Monitoring page – Devices tab

The Devices tab is split into three areas: Device Groups, Monitor Devices and Device Status Summary.

- **Device Groups** – Device groups are listed on the left side of the page in the Device Groups Pane. Beside each group is a number that shows the number of devices the group contains, including devices in subgroups. For example, **ALL (150)** indicates that a total of 150 devices are under management.

The color of the group changes from **green** (meaning every device in the group is functioning as expected) to **black**, **orange** or **red** if any device in the group is in **unknown/reboot**, **failover** or **error** state respectively.

Status precedence is maintained in the above order. For example, if any one device is in the error state, the group it belongs to is red, even if another device in that same group is in the failover state. Group status indicates the most severe device status among the devices the group contains.

Clicking on a group loads the Device Group Status for that group. Clicking on a device loads the Device Status for that device. See **Device Group Status on page 26** and **Device Status on page 27**.
To show a different group view in the Device Groups Pane, select a different group view from the **Current Group View** drop-down list and click **Set**. See *Working with the device groups pane on page 28*.

- **Monitor Devices** – The Monitor Devices section contains a brief overview of the Devices tab.
- **Devices Status Summary** – At the bottom of the Devices tab is the Device Status Summary. Here the number of devices with a given status is listed. Clicking on the number of devices listed takes you to the Devices with Status page. See *Devices with Status on page 27*.

**Device Group Status**

On a Device Group Status page, all the devices belonging to that group are listed (including devices in subgroups), along with their current status, their location, and their hardware and firmware versions (Figure 17).

**Figure 17  Device Group Status page**

![Device Group Status page](image)

Clicking on a device name opens the Web management console for that device in a new browser window. Clicking on the status link takes you to the Device Status page for that device. See *Device Status on page 27* for details.

System log messages for all devices may be accessed by selecting a filter level and clicking **Show Logs**.
**Devices with Status**

Here, each device is listed with their location and hardware and firmware versions (Figure 18).

**Figure 18 Devices with Status: up page**

Clicking on the status link (up in this case) takes you to the Device Status page for that device. See *Device Status on page 27* for details. Clicking a device name provides access to that device in a new browser window.

**Device Status**

A Device Status page provides a brief summary of the managed device, presenting certain details such as the device’s IP address, or the date and time of the last update. The Device Status page also provides a number of per-device operations.

The device status page is accessed by selecting a status from the group monitoring view, or by clicking on a device while *Show Devices* is in effect in the device group pane (Figure 19).

**Figure 19 Device Status page**
Monitoring

Monitoring devices

System log messages for this device may be shown by selecting a filter level and clicking Show Logs.

From the Device Status page you can:

- Click the **Device Name** to open the UTM Firewall Management Console for that device in a new browser window.
  
  **Note:** The Device Name link uses the Control Center as a proxy, so it not necessary to have the device enabled for web administration over the Internet.

- Click the **Summary** button to show an abbreviated event log for the device. This includes Control Center eventlog messages, Warning and Error syslog messages, and tasks applied to this device.

- Click the **Delete** button to remove the device from the group view (this option is not available for devices that are up).

- Select a level of detail from the **System Log** drop down menu and click **Show Logs** to view the system logs of the device.

If the Device status is up, the Device Status page provides four more options (Figure 20).

**Figure 20** Device Status page - Up options

![Device Status page - Up options](image)

- Click the **Refresh Config** button to update the configuration information from the device. Normally the Control Center only refreshes device configuration when a device connects, or when a policy is applied, but the button allows you to update it upon command. The Last Update field tells you when the device configuration was last refreshed.

- Click the **Unmanage** button to remove the device from Control Center management.
  
  **Note:** If an unmanaged device is still configured for management by the Control Center, then the device reappears in the device group list when the device next sends an updated notification.

- Click the **Reboot** button to restart the device.

- Click the **Upgrade** button to open the Device Operations tab. From here you can select a firmware version to upgrade the device to. See **Updating device firmware on page 61** for more information on firmware upgrades.

**Working with the device groups pane**

The device groups pane provides a quick survey of device statuses.

- **Show All/Show Registered/Show Unregistered** – If there are unregistered UTM Firewall devices communicating with the Control Center, those devices are marked with an asterisk (*). To see only registered devices in the device groups pane, select **Show Registered** from the Device Groups drop-down menu. To see only unregistered devices, select **Show Unregistered** from the DEvice Groups drop-down menu. To see all devices again, select **Show All**.
Checking task progress

Any time an operation is performed upon a managed device, that task is listed in the Control Center Task Queue. To access the Control Center Task Queue, select MONITORING from the navigation menu, and then select the TASK QUEUE tab (Figure 21).

The task queue shows all executed and in-progress tasks requested of the Control Center. The most recent tasks are shown at the top of the list.

The task queue lists the name, type (Reboot, for example), and date and time created for each task. As the task is applied to each device, devices progress from Pending to Succeeded or Failed. Once all devices have either succeeded or failed at the task, the task is complete. Completed tasks are listed in black. Pending tasks and tasks that have failed on one or more devices are listed in red.

Note: Old tasks are periodically archived and are no longer available in the task list.

Clicking the Detail button next to each task opens the Control Center Task Detail page (Figure 22).

This page shows detailed task information, including which devices have succeeded and failed. Clicking the Retry Failed Devices button re-issues the command to failed devices if the task is complete and one or more devices has failed. This can be useful if some devices failed due to an intermittent network outage.

Click the Done button to return to the Task Queue.
Viewing recent events

You can view recent events by selecting **MONITORING** from the navigation menu and clicking the **EVENT LOG** tab.

The Control Center event log is displayed here, most recent events first. Each message includes the username of the user who initiated the event (or **Control Center** for a system-initiated event), the date and time of the event, and an event description (Figure 23).

![Event Log tab](image)

Clicking on a device link opens the Device Status page for that device.

To change which messages are displayed, select a level (**All messages**, **Errors and warnings**, or **Errors only**) and click **Refresh**.

**Note:** Message display settings are persistent for each user.

Click the **show all** link to advance the log if it doesn’t fit in the browser window.

Old events are periodically archived and are no longer available in the list.
Defining device attributes from the Control Center

You can set a managed device’s McAfee UTM Firewall Control Center attributes from the Control Center Web interface.

To set Control Center attributes:

1. Select **DEFINITIONS** from the navigation menu. The Attributes tab appears (Figure 24).

   **Figure 24 Attributes tab**

   ![Attributes tab](image)

2. Enter an attribute name in the Definition Name field, and click **New Definition**. The Create Attribute Definition dialog for the new attribute appears (Figure 25).

   **Figure 25 Create Attribute Definition dialog**

   ![Create Attribute Definition dialog](image)
Definitions
Working with group views

3 Each device enabled for Control Center management is listed in the Device column. Enter a value for each device in the Value column, and click Create Definition.

4 The attribute is now listed on the Attributes tab. Values for subsequently added devices can be entered by clicking the Edit button next to each attribute.

---

Working with group views

Four different group views come supplied with the initial Control Center installation.

- The default group view sorts UTM Firewall devices by company, then by division, and then by sub-division. These values must be set for each managed device. If a value has not been set for a device, that value is listed as unknown.

- The location group view sorts UTM Firewall devices by country, then by city, and then by state. If any of these values have not been set for a device, the value is listed as unknown in the group view.

- The organization group view sorts UTM Firewall devices by company, then by department, and then by division. If a value has not been set for a device, that value is listed as unknown.

- The type_version group view sorts UTM Firewall devices by appliance model, and then by firmware version. These two values are provided by default on all UTM Firewall devices.

These group views can be customized, and more group views can be created. See Creating group views on page 32, Modifying group views on page 33 and Setting attributes on page 20 for details.

To change which group view is currently being shown in the device groups pane, select a group view from the Current Group View drop-down list and click Set.

Creating group views

You can create group views other than the defaults. For example, you could create a Region group view to monitor devices by location, or a Version_Only group view to quickly assess which devices need firmware updates.

To create a new group view:

1 On the Monitoring page, select Add/Edit from the group view drop-down menu, or

Navigate to: DEFINITIONS > Group Views (Figure 26).

Figure 26  Group Views tab

2 Enter a name for the new group view in the text box and click New Definition. The Create Group View Definition dialog appears (Figure 27).
Definitions
Creating device groups

3 For each level in the new group view, starting with Level 1, select an attribute from the Attribute drop-down list. If the attribute is optional, select the Optional check box.

Note: If you do not mark an attribute as optional, the word unknown is displayed in the group view in place of any missing attribute values.

If you have fewer than five levels in your hierarchy, remaining blank levels are ignored.

4 Click Create Definition. The new group view is added to the group view list, and can be selected from the group view drop-down menu on the Monitoring page.

Modifying group views
You can edit the default, type_version, organization and location group views provided at installation. As you develop your own group views, you can edit those using this same procedure.

To edit a group view:
1 Navigate to: DEFINITIONS > Group Views (Figure 26).
2 Select the Edit button next to the group view you wish to edit. The Edit Group View Definition dialog appears.
3 Make changes to the fields as necessary.
4 Click Update Definition.

Creating device groups
Before you can create policies, you must create Device Groups to assign those policies to. Device groups allow policies to be applied to multiple devices at one time. You can create device groups based on device versions, locations, or any other device attributes you have set for your managed devices.

To create a device group:
1 Navigate to: DEFINITIONS > Device Groups. (Figure 28)
2 Enter a name for the device group in the Definition Name field and click New Definition. This opens the Create Group Definition dialog (Figure 29).

**Figure 29 Create Device Group Definition dialog**

3 Select a Group View from the drop-down menu, or accept the current group view shown.

4 Select the groups and devices you wish to include in the new device group. If you select a group, all the devices in that group are included in the new device group.

5 Click Create Definition. The new device group is added to the group list on the Groups tab, and can be selected when creating or editing policies.
Policy overview

McAfee UTM Firewall Control Center allows groups of configuration settings to be created as named policies and applied across multiple devices.

The Policies page contains four tabs: Networking, Firewall, VPN and System. These configuration areas mirror those used when managing a UTM Firewall device directly, and should be familiar to UTM Firewall administrators.

Each configuration area is further divided into a number of sub-areas. For example, the Firewall configuration area encompasses the following sub-categories, each with their own tab: Packet Filtering, Content Filtering and Incoming Access (Figure 30).

Figure 30  Policies page

Working with policies

On the tab for each configuration area, there is a list of configured policies. In the default installation, some configuration groups have default policies (such as disabled and enabled for DNS Proxy), however some configuration groups have no sensible defaults, so the list starts unpopulated for these configuration groups.

You can sort the configured policies list by selecting a device group from the drop-down list and clicking Filter. Only policies currently applied to the device group are shown.
To apply a policy to devices, click the **Apply** button next to the policy. The policy is applied to all the devices in the device group listed in the Devices column. You can see the progress of the task by navigating to **MONITORING > Task Queue**.

If you wish to check whether certain devices conform to a specific policy, then select the policy and click **Check**. The message indicates whether the associated devices conform to the selected policy. This is useful if you suspect that a device has been modified outside of the Control Center, or perhaps by another user within the Control Center.

### Creating policies

To create a policy:

1. Enter a unique name for the policy in the text entry field and click **New Policy**. This opens a Create Policy dialog.
   
   **Note:** Case is ignored when creating unique policy names. For example, you can not have a policy named "Strict" and a policy named "strict" at the same time.

2. Select a device group from the **Devices** drop-down menu. When the policy is applied, the configurations set by the policy is administered to all devices in this device group.

3. Fill out the policy fields.

4. Click **Create Policy**. The new policy is added to the policy list.

   Clicking **Cancel** cancels the creation of the policy.

You can create a new policy based on an existing policy by entering a unique policy name in the text field and clicking **Duplicate** beside the appropriate existing policy.

### Editing and deleting policies

To modify a policy:

1. Click the **Edit** button next to the policy. This opens the Edit Policy page.

2. Fill out the policy fields and click **Update Policy**.

   Clicking **Cancel** cancels any changes you have made.

   Click **Delete Policy** to remove the existing policy.
Networking policies

Use the Control Center to create and manage policies for DNS proxies, traffic shaping and wireless networking.

Enabling DNS Proxy

UTM Firewall devices can be configured to run as Domain Name Servers. Each device acts as DNS proxy and then passes incoming DNS requests to the appropriate external DNS server. All the computers on the LAN should then use the device’s IP address as their DNS server.

To enable devices as DNS proxies:

1. Select POLICIES from the navigation menu and click the NETWORKING tab. The DNS Proxy tab appears (Figure 31).

![Figure 31 DNS Proxy tab](image)

2. Select the Edit button next to the enabled policy. This opens the Edit DNS Proxy Policy: enabled dialog (Figure 32).

![Figure 32 Edit DNS Proxy Policy: enabled dialog](image)

3. Select the device group from the Devices drop-down menu that contains the devices you wish to enable as DNS proxies, and click Update Policy. This returns you to the DNS proxy tab.

4. Click the Apply button next to the enabled policy.
Configuring Traffic Shaping
Traffic shaping allows you to give preference to certain types of network traffic to maintain quality of service when a network connection is under heavy load.

To configure traffic shaping for managed devices:

1. Navigate to POLICIES > NETWORKING > Traffic Shaping. The Traffic Shaping tab appears (Figure 33).

   **Figure 33  Traffic Shaping tab**

2. Enter a unique name for the new policy in the Policy Name field and click **New Policy**. This opens the Create Traffic Shaping Policy dialog (Figure 34).

   **Figure 34  Create Traffic Shaping Policy dialog**

3. Select a device group from the **Devices** drop-down menu.

4. Select the **Enable Traffic Shaping** check box.

5. Select a default priority from the **Default Priority** drop-down list. If you select a priority of **Unchanged**, managed devices do not assign a priority to traffic except for the services specified by the policy.

   **Note:** For configurations with limited bandwidth, it is recommended that the default priority be set to **low**.

6. Add any services that are a part of the traffic shaping policy. For each service, enter a port range and source and destination address ranges. Select a protocol and a priority. Click **Update Services** to add the service to the Services list for the protocol.

   **Note:** Selecting the **Delete** check box next to an existing service will delete that service from the Services list when the **Update Services** button is clicked.

7. Click **Create Policy**. This returns you to the Traffic Shaping tab.

8. Click the **Apply** button next to the newly created policy.
Creating a wireless policy

Security Alert: Wireless LAN is not recommended for gateway appliances in high-security environments. If used, wireless users should receive their ESSID and WPA Key from an authorized agent.

To create a wireless policy for managed devices:

1. Navigate to: POLICIES > NETWORKING > Wireless. The Wireless tab appears (Figure 35).

   **Figure 35  Wireless tab**

   ![Wireless tab](image)

2. Enter a unique name for the new policy and click Create Policy. This opens the Create Wireless Settings Policy tab (Figure 36).

   **Figure 36  Create Wireless Settings Policy tab**

   ![Create Wireless Settings Policy tab](image)

3. Select a device group from the Devices drop-down menu.

4. Enter an ESSID for your wireless users.

5. Select the Bridge Between Clients check box to have the UTM Firewall device forward packets between wireless clients at the wireless level.

   Security Alert: Packets sent between wireless clients at the wireless level are not restricted by the firewall.

6. Leave the Broadcast ESSID check box unselected.

7. Select a WPA Algorithm from the drop-down menu. Options are: TKIP and AES.

8. Enter a WPA Key.

   Note: Selecting AES and using a WPA key of at least 23 characters is recommended for wireless LANs.

9. Click Create Policy. This returns you to the Wireless tab.

10. Click the Apply button next to the newly created policy.
Firewall policies

The Control Center can create and manage policies for Packet Filtering, Content Filtering and Incoming Access.

Configuring Packet Filtering rules

Packet filter rules match network packets based on a combination of incoming and outgoing interface, source and destination address, and destination port and protocol. Once a packet is matched, it can be logged and allowed, disallowed (dropped), or rejected.

To configure packet filtering rules for managed devices:

1. Select POLICIES from the navigation menu and click the FIREWALL tab. The Packet Filtering tab appears (Figure 37).

**Figure 37  Packet Filtering tab**

2. Enter a unique name for the new policy and click New Policy. This opens the Create Packet Filter Policy dialog (Figure 38).
3 Select a device group from the Devices drop-down menu.

4 Enter a meaningful description in the Description field.

5 Select the Enable check box.

6 Select an action from the drop-down list. The available actions are: Accept, Reject, and Drop.

7 Select Incoming and Outgoing interfaces from the drop-down lists.

8 Enter a Source Address. Leaving this field blank is the equivalent of allowing IP addresses from any source.

9 Enter a Destination Address. Leaving this field blank is the equivalent to entering “any.”

10 Select a protocol from the drop-down list. The options are Any, TCP, UDP, ICMP, and IP.

11 Enter a destination port in the Port field.

12 [Conditional] If you are configuring Port Forwarding:
   a Enter an address in the To Destination Address field. Traffic is directed to this address.
   b Enter a port in the To Port field. Traffic is routed to this port.

13 Select the Log check box.

14 Enter a prefix for the log entries generated by the packet filtering rules in the Log Prefix field.

   Note: Logging is crucial to high-security implementations. Syslogs for all managed devices can be viewed by the Control Center, and can also be streamed to McAfee Firewall Reporter for analysis and archiving.

15 Click Create Policy. This returns you to the Packet Filtering tab.
16 Repeat steps 2-16 for each Packet Filter rule in your configuration. As Packet Filter policies are added, use the **Move Up** and **Move Down** buttons to set the policies in the order in which the Packet Filtering rules are executed on the managed machines.

**Tip:** Configure the last policy in the list to reject or drop all traffic to any Destination Port. Any other Packet Filtering rules should be restricted to required services or encrypted transport.

17 When all the Packet Filter rules have been created, select a device group from the drop-down list and click **Apply**.

**Creating Content Filtering rules**

The Content Filtering system enables you to monitor and limit the types of web-based content that can be accessed by users.

The Control Center Policy controls for Content Filtering assume that the Access Control Proxy has already been configured and the McAfee Web Filtering Subscription Certificate and Private Key have already been installed on each UTM Firewall device the policy is applied to.

To apply a content filtering policy:

1. **Navigate to:** **POLICIES > FIREWALL > Content Filtering.** The Content Filtering tab appears (**Figure 39**).

   **Figure 39  Content Filtering tab**

   ![Content Filtering tab](image)

2. Enter a unique name for the new policy and click **New Policy.** This opens the Create Content Filtering Policy dialog (**Figure 40**).

   ![Create Content Filtering Policy dialog](image)
3 Select a device group from the **Devices** drop-down menu.

4 Select one or more of the **Enable Content Filtering on...** check boxes.

5 [Optional] Select the **Enable Cache** check box to store the results of Category queries.

6 [Optional] Select the **Require Authentication** check box to force users to authenticate themselves before they can access restricted content.

7 Select a default filtering action (**Allow** or **Deny**).

8 [Optional] Enter specific URLs into the **Block** and **Allow** lists.
9  {Optional] Select the Webwasher Settings and Block Categories you wish to include in the policy.

Note: Webwasher Settings and Block Categories are only applied to devices that are configured with a valid McAfee Web Filtering license.

a Select the Enable Webwasher content filtering check box to enable Webwasher content filtering.

b Select the Cache Webwasher requests to store content rating results. This improves device performance at the cost of 2 MB of device memory.

c Select the Allow pages that are unrated by Webwasher check box to allow users to access pages that have no ratings. If the box is left un-selected, access to any unrated page is denied.

d Select the Allow access to newly-defined categories check box to allow users access to new categories that have not yet been explicitly allowed or blocked.

e Select the Send user details to Webwasher, with the request check box to send user names to the Webwasher reporting service.

10 Click Create Policy. This returns you to the Content Filtering tab.

11 Click the Apply button next to the newly created policy.

Limiting Incoming Access

It is important to limit access to your UTM Firewall devices. Some management methods are inappropriate in a high-security environment.

To limit Incoming Access on managed devices:

1 Navigate to: POLICIES > FIREWALL > Incoming Access. The Incoming Access tab appears (Figure 41).

Figure 41  Incoming Access tab

2 Enter a unique name for the new policy and click New Policy. This opens the Create Incoming Access Policy dialog (Figure 42).
3 Select a device group from the **Devices** drop-down menu.

4 Select the check boxes of the remote management methods you wish to allow for each type of interface.  
   **Caution:** Make sure you leave yourself some way to communicate with your managed devices. If you disallow all management methods, you have no way of making any changes to your devices until the devices are manually reset to their factory default settings.

5 If you do not want the devices to respond to echo requests, make sure the **ICMP Echo Request** check box is un-selected.

6 Click **Create Policy**. This returns you to the Incoming Access tab.

7 Click the **Apply** button next to the newly created policy.

---

**VPN policies**

VPN policies allow you to set PPTP, L2TP or IPsec connection settings for managed devices.

**Creating PPTP Client connections**

This section leads you through setting up PPTP Client connections.

To set PPTP Client connections for managed devices

1 Select **POLICIES** from the navigation menu and click the **VPN** tab. The PPTP Client tab appears (Figure 43).
2 Enter a unique name for the new policy and click **New Policy**. This opens the Create PPTP Client VPN Policy dialog (Figure 44).

**Figure 44 Create PPTP Client VPN Policy dialog**

3 Select a device group from the **Devices** drop-down menu.

4 Enter a descriptive name for the connection in the **Connection Name** field.

5 Select the **Endpoint Type** of the remote endpoint (either **Managed Device** or **Unmanaged Device**).

6 [Conditional, Unmanaged endpoints only] Enter the IP address of the PPTP server in the **Server IP Address** field.

7 [Optional] If you know the netmask of the remote network, you can enter it in the **Remote Netmask**.

8 If the Remote Device is managed by the Control Center, select the device from the **Remote Device** drop-down list.

9 Enter the **Username** and **Password** required for authentication with the server.

10 [Optional] If multiple machines are using the managed devices to access a remote network and you wish to avoid setting up a route for each device from the remote PPTP server, select the **Use NAT** check box.

11 [Optional] If you want all device traffic to go over the PPTP VPN tunnel, select the **Tunnel is default route** check box.

12 [Optional] If you have remote networks other than the PPTP server you want to access through the PPTP VPN tunnel, enter them into the **Remote Networks** table. After you have entered the network’s IP address or hostname and Netmask, click **Apply** to add them to the Remote Networks table.

13 Once all the fields are completed, click **Create Policy**. This returns you to the PPTP Client tab.

14 Click the **Apply** button next to the new policy.
Creating PPTP Server connections

The PPTP Server is a virtual private network server that supports multiple VPN tunnels. It allows remote Windows clients to securely connect to the local network.

Currently three authentication sources are supported with the PPTP Server policy, RADIUS, TACACS+ and Local User Database. However if Local User Database is selected, the username/passwords must be configured through User policies (see Creating user policies on page 58).

To set PPTP server connections for managed devices:

1. Navigate to: POLICIES > VPN > PPTP Server. The PPTP Server tab appears (Figure 45).

2. Enter a unique name for the new policy and click New Policy. This opens the Create PPTP Server VPN Policy dialog (Figure 46).

3. Select a device group from the Devices drop-down menu.

4. Select the Enable PPTP Server check box.

5. Select an Authentication Method from the drop-down list. The options are:
   - None
   - PAP (basic)
   - CHAP (strong)
   - MSCHAP (stronger)
   - MSCHAPv2 (recommended)
6 Select an **Encryption Level** from the drop-down list. The options are:
- No encryption
- Accept any encryption settings
- Require some encryption
- Require basic (40 bit) encryption
- Require strong (128 bit) encryption (recommended)

7 Select the **Authentication Source** (RADIUS, TACACS+ or Local User Database) from the drop-down list.

8 [Conditional, RADIUS or TACACS+ only] Enter the IP address of the **Authentication Server**.

9 [Conditional, RADIUS or TACACS+ only] Enter the password that is used to authenticate clients in the **Authentication Secret** field.

10 Enter the range of viable client IP addresses in the **Client Address Range** field.

11 Click **Create Policy**. This returns you to the PPTP Server tab.

12 Click the **Apply** button next to the newly created policy.

**Creating L2TP Client connections**

The L2TP client enables the device to establish a VPN to a remote network running a L2TP server. To set L2TP client connections for managed devices:

1 Navigate to: **POLICIES > VPN > L2TP Client**. The L2TP Client tab appears (Figure 47).

   **Figure 47  L2TP Client tab**

2 Enter a unique name for the new policy and click **New Policy**. This opens the Create PPTP Server VPN Policy dialog (Figure 48).
Figure 48  Create L2TP Client VPN Policy dialog

3 Select a device group from the Devices drop-down menu.
4 Enter a name for the connection in the Connection Name field.
5 Select the Endpoint Type (managed or unmanaged) from the drop-down list.
6 Enter the IP address of the L2TP server in the Server IP Address field.
7 [Optional] If you know the netmask of the server enter it into the Remote Netmask field.
8 [Conditional] If connecting to a managed device, select the device from the Remote Device drop-down list.
9 Enter the Username and Password used to authenticate clients to the server.
10 Select the Required encryption level for the connection from the drop-down list.
11 If you wish to use NAT, select the Use NAT check box.
12 [If you wish to pass all traffic through the L2TP tunnel, select the Tunnel is default route check box.
13 For each Remote Network you want to access through the L2TP VPN tunnel, enter a Network address and Netmask in the Remote Networks table and click Apply.
14 Click Create Policy. This returns you to the L2TP Client tab.
15 Click the Apply button next to the newly created policy.
Creating L2TP Server connections

The L2TP Server is a virtual private network server that supports multiple VPN tunnels. It allows remote Windows clients to securely connect to the local network.

If Local User Database is selected, the username/passwords must be configured through User policies (see Creating user policies on page 58).

Additionally, if LT2P tunnels are accepted from Windows Clients, a matching IPSec tunnel must be created to encrypt the data. This tunnel is not currently automatically created by the Control Center.

To set PPTP server connections for managed devices:

1. Navigate to: POLICIES > VPN > L2TP Server. The L2TP Server tab appears (Figure 49).

   **Figure 49**  L2TP Server tab

2. Enter a unique name for the new policy and click New Policy. This opens the Create L2TP Server VPN Policy dialog (Figure 50).

   **Figure 50**  Create L2TP Server VPN Policy dialog

3. Select a device group from the Devices drop-down menu.

4. Select the Enable L2TP Server check box
5 Select an **Authentication Method** from the drop-down list. The options are:

- None
- PAP (basic)
- CHAP (strong)
- MSCHAP (stronger)
- MSCHAPv2 (recommended)

6 Select an **Encryption Level** from the drop-down list. The options are:

- No encryption
- Accept any encryption settings
- Require some encryption
- Require basic (40 bit) encryption
- Require strong (128 bit) encryption (recommended)

7 Select the **Authentication Source** (RADIUS, TACACS+ or Local User Database) from the drop-down list in the field provided.

8 Enter the IP address of the **Authentication Server**.

9 Enter the password that is used to authenticate clients in the **Authentication Secret** field.

10 Enter the range of viable client IP addresses in the **Client Address Range** field.

11 Click **Create Policy**. This returns you to the PPTP Server tab.

12 Click the **Apply** button next to the newly created policy.

**Creating IPsec VPN Tunnel policies**

Creating an IPsec VPN tunnel policy is done in three steps.

1 **Configure endpoints** *(page 51)*.

2 **Configure Tunnel Settings** *(page 54)*

3 **Configure Tunnel Mappings** *(page 56)*

This process allows multiple IPsec VPN tunnel policies to be grouped together under a single policy that can be pushed down to managed devices. Each step is described below.

**Endpoint policies**

You can create two kinds of endpoint policies. IPsec Managed Endpoint policies are used to store configuration information for McAfee UTM Firewall devices managed by the Control Center. IPsec Unmanaged Endpoint policies are used to store information for remote devices that are NOT managed by the Control Center. Once endpoint policies are created they are added to the endpoint selection lists for Tunnel Mapping policies. When the Tunnel Mapping policies are applied, endpoint policy settings are automatically applied to managed devices. Unmanaged devices still need to be configured for the IPsec VPN tunnel.
To create an IPsec Managed Endpoint policy:

1. Navigate to: **POLICIES > VPN > IPsec Managed Endpoint**. The IPsec Managed Endpoint tab appears (Figure 51).

   **Figure 51  IPsec Managed Endpoint tab**

   ![IPsec Managed Endpoint tab](image)

2. Enter a unique name for the new policy and click **New Definition**. This opens the Create IPSEC VPN Managed Endpoint Definition dialog (Figure 52).

   **Figure 52  Create IPSEC VPN Endpoint Definition dialog**

   ![Create IPSEC VPN Endpoint Definition dialog](image)

3. Select a device group from the **Devices** drop-down menu.

4. Enter an **Interface**. If you leave this field blank, the policy uses the default route.

5. Select an **Address type** from the drop-down menu. Options are:
   - **Automatically determined**
   - **Static IP address**
   - **Dynamic IP address**
   - **DNS hostname**

6. Leave the **Initiate tunnel** and **Initiate rekey** check boxes selected.

   **Note:** Initiating negotiations from both ends of a VPN tunnel can be inefficient for large VPN configurations.
7 Add tunneled networks to the **Tunneled Networks** list as needed:
   a Select an **Address Type** from the drop-down list.
   b Enter a **Network** for the tunnel.
   c Enter a **Netmask** for the tunnel.
   d Click **Apply**. Repeat steps a-d for each Tunneled Network you wish to add to the policy.

8 Click **Create Policy**. This returns you to the IPsec Managed Endpoint tab. The new policy appears in the policy list.

To create an IPsec Unmanaged Endpoint policy:
1 Navigate to: **POLICIES > VPN > IPsec Unmanaged Endpoint**. The IPsec Unmanaged Endpoint tab appears (Figure 53).

**Figure 53** IPsec Unmanaged Endpoint tab

<table>
<thead>
<tr>
<th>NETWORKING</th>
<th>FIREWALL</th>
<th>VPN</th>
<th>SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPTP Client</td>
<td>PPTP Server</td>
<td>L2TP Client</td>
<td>L2TP Server</td>
</tr>
<tr>
<td>IPsec Tunnel Settings</td>
<td>IPsec Tunnel Interfaces</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPsec VPN Unmanaged Endpoint Definitions**

- **Definition Name**
- **New Definition**

2 Enter a unique name for the new policy and click **New Definition**. This opens the Create IPSEC VPN Unmanaged Endpoint Definition dialog (Figure 54).

**Figure 54** Create IPSEC VPN Unmanaged Endpoint Definition dialog

- **Address type** (Static IP, Dynamic IP or DNS hostname) from the drop-down list.
- **Optional**] Enter the remote **Endpoint ID**.
- Select an **Authentication method** (Preshared key or RSA digital key signature) from the drop-down list.
- [Conditional, RSA public keys only] Enter the **RSA public key** into the provided field.
7 Leave the **Initiate tunnel** and **Initiate rekey** check boxes selected.

*Note:* Initiating negotiations from both ends of a VPN tunnel can be inefficient for large VPN configurations.

8 Add tunneled networks to the **Tunneled Networks** list as needed:
   a Select an **Address Type** from the drop-down list.
   b Enter a **Network** for the tunnel.
   c Enter a **Netmask** for the tunnel.
   d Click **Apply**. Repeat steps a-d for each Tunneled Network you wish to add to the policy.

9 Click **Create** Policy. This returns you to the IPsec Unmanaged Endpoint tab. The new policy appears in the policy list.

**IPsec Tunnel Settings**

IPSec VPN tunnels are supported with Main Mode and Aggressive Mode Keying, preshared secrets and RSA keys. Once an IPsec Tunnel Settings policy has been created it can be selected when creating IPsec Tunnel Mapping policies.

*Note:* The Control Center uses a single RSA key across all configured IPSec tunnels. The Control Center expects this key to be pre-generated before any IPSec tunnels are configured.

*Note:* If the remote end of an IPsec VPN tunnel is not a UTM Firewall device under the management of this Control Center, then the remote device is NOT automatically configured. See **Endpoint policies on page 51** in for more details.

To create an IPsec Tunnel Settings policy:

1 Navigate to: **POLICIES > VPN > IPsec Tunnel Settings**. The IPsec Tunnel Settings tab appears (Figure 55).

**Figure 55  IPsec Tunnel Settings tab**

2 Enter a unique name for the new policy and click **New Definition**. This opens the Create IPSEC VPN Tunnel Settings Policy dialog (Figure 56).
3 Select a **Phase 1 proposal** from the drop-down list.

4 Enter the time in seconds before the Phase 1 key is renegotiated in the **Phase 1 key lifetime** field.

5 Enter the maximum amount of time in seconds between the current key expiring and a new key being negotiated in the **Rekey margin** field.

6 Enter the maximum percentage that the Rekey margin should be randomly increased by in the **Rekey fuzz** field.

7 Select a **Phase 2 proposal** from the drop-down list.

8 Enter a **Phase 2 key lifetime**.

9 Select an option for **Perfect forward secrecy** form the drop-down list. The options are:
   - No perfect forward secrecy
   - Diffie-Hellman Group 1 (768 bit)
   - Diffie-Hellman Group 1 (1024 bit)
   - Diffie-Hellman Group 1 (1536 bit)
   - 2048 bit
   - 3072 bit
   - 4096 bit

10 [Optional] If you wish to apply IPComp compression before encryption, select the **IP payload compression** check box.

11 [Optional] If you want to enable Dead Peer Detection (DPD), select the **Dead peer detection** check box.

12 [Conditional] If you enabled Dead Peer Detection, enter the time in seconds before sending DPD notifications in the **Delay** field.
13 [Conditional] If you enabled Dead Peer Detection, set the time in seconds to wait for a DPD acknowledgement before restarting the tunnel in the Timeout field.

14 Click Create Definition. This returns you to the IPsec Tunnel Settings tab. The new Tunnel Settings policy appears in the policy list.

**IPsec Tunnel Mappings**

This feature allows a number of IPSEC VPN tunnel policies to be grouped together under a single policy which can then be applied to various devices. It allows multiple VPN tunnels to be configured. This is the preferred method of configuring multiple tunnels on a device since the Control Center virtual appliance replaces the existing IPsec configuration when it applies a policy.

To create an IPsec Tunnel Mappings policy:

1. Navigate to: **POLICIES > VPN > IPsec Tunnel Mappings**. The Ipsec Tunnel Mappings tab appears (Figure 57).

   **Figure 57  IPsec Tunnel Mappings tab**

   ![Figure 57  IPsec Tunnel Mappings tab](image)

2. Enter a name for the new policy in the text field and click **New Policy**. The Create IPsec VPN Tunnel/Endpoint Mapping Policy dialog appears (Figure 58).

   **Figure 58  Create IPsec Tunnel/Endpoint Mapping Policy dialog**

   ![Figure 58  Create IPsec Tunnel/Endpoint Mapping Policy dialog](image)

3. Enter a name for the tunnel in the **Tunnel Name** field.

4. Select the **Enable** check box.

5. Select an **Authentication mode** (main mode automatic keying or aggressive mode automatic keying) from the drop down list.
6 Select an **Authentication method** (preshared secret or RSA digital key signature) from the drop-down list.

7 Create a Preshared secret:

8 Select the **Generate random secret** check box.

   or

   Enter a preshared secret in the **Preshared secret** field.

   **Note:** Because tunnel mapping settings are pushed down to managed devices, the preshared secrets match even though they are not visible until the policy is created.

9 Select a policy from the **Left endpoint** drop-down list. The left and right endpoint drop-down lists are populated with policies from the IPsec Managed Endpoint and Ipsec Unmanaged Endpoint tabs.

10 Select a policy from the **Right endpoint** drop-down list.

11 Select a policy from the **Tunnel settings** drop-down list. This list is populated with policies from the IPsec Tunnel Settings tab.

12 Click **Create Policy**. This returns you to the IPsec Tunnel Mappings tab. The new Tunnel Mapping policy is added to the policy list. When the policy is applied, all managed endpoint settings and tunnel settings are pushed down to the associated devices.

---

### System policies

System policies allow you to set basic system settings on multiple devices.

### Creating time policies

Time policies allow you to set NTP settings for multiple managed devices.

**Note:** Time zones must be set on UTM Firewall devices before time policies can be applied.

To create a Time policy:

1 Navigate to: **POLICIES > SYSTEM > Time**. The Time tab appears (Figure 59).

**Figure 59 Time tab**

2 Enter a name for the new policy in the **Policy Name** field and click **New Policy**. This opens the Create Time Server Policy dialog (Figure 60).
3. Select a device group from the **Devices** drop-down list.

4. Select the **NTP Server Enabled** check box to enable an NTP server to retrieve and serve time updates.

5. [Optional] If you want the NTP server to set the time as quickly as possible after device start-up, select the **Set time quickly** check box.

6. Specify one or more NTP servers:
   - a. Enter the hostname or IP address of the NTP server in the **NTP Host** field.
   - b. Select **Server** or **Peer** as the **NTP Host Type**.
   - c. Click **Apply**.
   - d. Repeat steps a-c for each NTP server in your network.

7. Click **Create Policy**. This returns you to the Time tab. The new policy is listed in the policies table.

### Creating user policies

User policies allow you to set Administrative User permissions for managed devices.

To create a user policy:

1. Navigate to: **POLICIES > SYSTEM > Users**. The Users tab appears (Figure 61).

2. Enter a name for the new policy in the **Policy Name** field and click **New Policy**. This opens the Create Users Policy dialog (Figure 62).
3 Select a device group from the **Devices** drop-down list.

4 Enter a **User Name** and **Password**.

5 Select the **Enabled** check box. If the Enabled check box is not selected, the user name and password will not be accepted by the devices the policy is applied to.

6 Select the check boxes of the services hosted on the device the user should have access to.

   - **Dialin** – the user can access a Dial-in service hosted on the device.
   - **PPTP** – the user can access a PPTP VPN hosted on the device.
   - **L2TP** – the user can access a L2TP VPN hosted on the device.
   - **Shares** – the user can access Samba shares hosted on the device.
   - **Internet** – the user can access the Internet through the device.
   - **Bypass Content Filtering** – the user can bypass content filtering while accessing the Internet through the device.
   - **Change Password** – the user can access the Web Management Console of the device to change their password.
   - **Administration** – the user can make changes to the UTM Firewall device’s configuration from the Web management console.
   - **Diagnostics** – the user can view restricted diagnostic information from the Web management console.
   - **Encrypted save/restore all** – the user can save and restore the configuration of the UTM Firewall device on the Save/Restore page.
   - **Login** – the user can access the command-line administration interface of the UTM Firewall device with telnet and ssh.

7 Repeat steps 4 and 5 for each user you wish to add to the policy.

8 Click **Create Policy**. This returns you to the Users tab. The new policy appears in the policy list.
Policies
System policies
Operations

Contents
Updating device firmware
Rebooting devices
Refreshing device configuration
RSA Keys
Images

Updating device firmware

Use the following procedure to update the firmware images of managed devices.

To update firmware on managed devices:

1. Select OPERATIONS from the navigation menu. The DEVICE OPERATIONS tab appears (Figure 63).

![Figure 63 Device Operations tab](image)

2. Select a Firmware image from the Firmware image drop-down list.

   The Firmware image select list shows all firmware images which have been installed or downloaded (see Images on page 64). The Control Center validates that the selected image is compatible with all of the target devices.

3. [Optional] Check the Ignore Version check box if you are downgrading.

   Caution: Downgrading firmware is not generally supported and could result in the loss of existing configuration settings.

4. Enter any extra netflash options in the Netflash options field if instructed to do so by McAfee technical support.
5. Click **Update Firmware** to begin upgrading devices. You can see the progress of the task using the Task Queue.

**Note:** For simplicity of upgrading devices in a network with different device types and/or versions, use a device group hierarchy specification with **type** and **version** as the last two fields (such as the preconfigured **type_version** setting). This allows similar devices to be easily grouped for updating one image at a time.

**Caution:** All of the warnings in the *McAfee UTM Firewall Administration Guide* regarding possible loss of device configuration and power loss during update apply to the Control Center virtual appliance. You should review that section before upgrading firmware using the Control Center.

---

### Rebooting devices

The DEVICE OPERATIONS tab provides a **Reboot Devices** button to allow selected devices to be rebooted. This operation is added to the task queue, and the progress may be monitored from the Task Queue.

To reboot managed devices:

1. Select **OPERATIONS** from the navigation menu. The DEVICE OPERATIONS tab appears (*Figure 63*).
2. Select the devices you wish to reboot from the group view on the left.
3. Click **Reboot Devices**.

### Refreshing device configuration

The DEVICE OPERATIONS tab provides a **Refresh Configuration** button. Generally a device automatically notifies the Control Center when its configuration is modified, triggering the Control Center to read the updated configuration from the device. However if network connectivity is intermittent, it is possible for the Control Center to be out-of-date for a period of time. The **Refresh Configuration** button causes the Control Center to immediately retrieve updated configuration from the selected devices.

To retrieve device configuration information from managed devices:

1. Select **OPERATIONS** from the navigation menu. The DEVICE OPERATIONS page appears (*Figure 63*).
2. Select the devices you wish to refresh from the group view on the left.
3. Click **Refresh Configuration**.
RSA Keys

The Control Center supports configuring IPSec tunnels with RSA key authentication. To support this, an RSA key must be generated on each device that participates in an IPSec tunnel with RSA key authentication (one key for any number of tunnels).

To generate RSA keys for a group:

1. Select **OPERATIONS** from the navigation menu and select the **RSA KEYS** tab (Figure 64).

![Figure 64 RSA Keys tab](image)

2. Select a device group or specific device from the group view.

3. Specify the size of the keys to generate.

   **Note:** Keys of 2048 bits can take a long time to generate.

4. [Optional] Select the **Replace Existing Key** check box if you wish to replace a previously generated key with a new one.

   **Note:** If you have existing IPSec tunnels, remote hosts need to be reconfigured with the new key.

5. [Optional] Select the **Generate on Device** check box if you wish to generate keys on the devices. If you have a small number of keys to generate, then it is faster to generate them with the Control Center since the Control Center host is (usually) much more powerful than the UTM Firewall devices. However if you have many keys to generate, distributing the processing across many devices may be faster.

6. Click **Generate Keys** to begin generating the keys on the selected devices. The progress may be monitored from the Task Queue.

   **Note:** Selecting a large key size and generating keys on devices may cause the task to show as **Failed**, even though the keys are eventually generated.
Images

The Control Center maintains a repository of firmware images on which are available for upgrading devices.

To add images to the firmware repository:

1. Select **OPERATIONS** from the navigation menu and click the **IMAGES** tab (Figure 65).

   **Figure 65  Images tab**

   ![Images tab](image)

2. [Conditional] If you have a firmware image stored locally,
   a. Click **Browse** to locate the file.

      **Note:** Only binary images should be uploaded, not the netflash executables.

   b. [Optional] Select the **Overwrite Existing Image** check box if you want to replace the existing firmware image with the new one.

   c. Click **Upload Image**. This uploads the image and store it in the firmware directory, making it available for firmware upgrades.

3. [Conditional] If you have access to a firmware image on-line,
   a. Specify a URL in the **Image URL** field, for example,

      ![URL example](https://www.securecomputing.com/snapgear/downloads/snapgear/firmware/SnapGearLITE300_v3.2.0_20080916.sgu)

      The **binary image** should be selected, not the netflash executable.

   b. Click **Download Image**. This fetches the image and store it in the firmware directory, making it available for firmware upgrades.

      **Note:** The GUI remains unresponsive until the image has either been downloaded successfully or failed to download.
Managing the Control Center

About the System page

The System page provides configuration options for the McAfee UTM Firewall Control Center. Each tab on the System page offers access to different configuration options. Each set of configuration options is described in its own section.

Control Center

Control Center options include allowing devices to connect to the Control Center, setting the device registration password, setting time-out parameters, selecting ports for Control Center traffic, and downloading the Control Center public key.

Enabling the Control Center, creating a registration password, and downloading the Control Center public key are discussed in Configuring the Control Center for device management on page 19.

Control Center port and time-out settings are initially set to default values. To change Control Center port and time-out settings:

1. From the navigation menu, click SYSTEM. The Control Center page appears (Figure 66).

Figure 66  Control Center page

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>☑</td>
</tr>
<tr>
<td>Registration Password</td>
<td></td>
</tr>
<tr>
<td>Confirm</td>
<td></td>
</tr>
<tr>
<td>Idle timeout (s)</td>
<td>120</td>
</tr>
<tr>
<td>Reconnect timeout (s)</td>
<td>120</td>
</tr>
<tr>
<td>SSH port</td>
<td>22</td>
</tr>
<tr>
<td>Syslog port</td>
<td>514</td>
</tr>
<tr>
<td>Firmware port</td>
<td>31</td>
</tr>
</tbody>
</table>

Submit  Download public key
The Control Center periodically pings devices to ensure they are up and running if not other operations are taking place. The following fields determine how long the Control Center waits to determine if a device is down.

- **Idle timeout** – Enter a number of seconds for the Control Center to wait between pings. The default is 120.
- **Reconnect timeout** – Enter a number of seconds for the Control Center to wait after a device disconnects before considering the device to be down. The default is 120.

The following fields determine the ports the Control Center listens on for traffic from managed devices.

- **SSH port** – Specify the SSH port that the Control Center will listen on for connections from managed devices. The default is port 22.
  
  *Note:* The SSH port for device communication must be different than the SSH port for command line access to the Control Center. See *Command line access on page 93* for more information.

- **Syslog port** – Specify the port to listen on for syslog communication from managed devices. The default is port 514.

- **Firmware port** – Specify the port to listen on for firmware upgrades from managed devices. The default is port 81.

Click *Submit*.

---

**System Setup**

System setup options include general Control Center settings, NTP server settings, and language options.

**General Control Center settings**

The Device settings page allows you to set some basic Control Center settings. Administrative Contact and Device Location are used to populate fields on some Management pages.

To update the general settings:

1. Navigate to SYSTEM > SYSTEM SETUP > Device. The Device tab appears (Figure 67).

   **Figure 67 Device tab**

2. Enter a hostname for the Control Center virtual appliance in the **Hostname** field. A hostname must begin with an alphabetic character, and can consist of letters, numbers or hyphens.

3. [Optional] In the **Administrative Contact** field, enter the contact information for the local administrator.

4. [Optional] In the **Device Location** field, specify the physical location of the Control Center virtual appliance.

5. [Optional] Enter the 16-digit serial number of the Control Center device in the **Serial Number** field.
Date and Time settings

Use the Date and Time tab to set the date and time on the Control Center virtual appliance. Setting the Control Center clock to the correct date and time is important; otherwise, the timestamps of system log messages do not match the time of the event. If you use certificates for SSL or IPsec, it is especially important that you set the date and time correctly, as certificates include a start date and time before which they do not function and an expiry date and time after which they do not function. All changes to the time are logged in the System Log to assist with tracking a chain of events.

Setting locality

You must select a locale (time zone) before you can set the date and time.

To set the locale for the Control Center:

1. Navigate to SYSTEM > System Setup > Date and Time. If you have not yet set the locality, the Locality tab appears. Otherwise, click the Locality tab (Figure 68).

Figure 68  Locality tab

2. Select your local region from the Region list.

3. Click Submit.
Syncing appliance date and time with a PC
Use this procedure to set the date and time of your Control Center virtual appliance to that of a personal computer. You must have JavaScript enabled in your Web browser to sync your Control Center time with a PC.

To sync Control Center time with a PC:

1. Navigate to SYSTEM > System Setup > Date and Time. The Set Date and Time tab appears (Figure 69).

**Figure 69  Set Date and Time tab**

2. Click Sync Date and Time. You can compare the current times between the UTM Firewall device and your PC.

Manually setting the appliance date and time
Use this procedure to manually set the date and time of your Control Center virtual appliance. In rare circumstances, it may be desirable for the time on the machine to not be synchronized to a PC or NTP server. You can use the manual configuration method to artificially set the Control Center virtual appliance to any time between 2002 and 2030.

To manually set the date and time:

1. Navigate to SYSTEM > System Setup > Date and Time. The Set Date and Time tab appears (Figure 69).
2. Select the Year, Month, Date, Hour, and Minute from the lists.
3. Click the lower Set Date and Time. An action successful message is displayed and the time is set to your selections.
Enabling the NTP time server

Use this procedure to configure the Network Time Protocol (NTP) services for the Control Center. The Control Center can use an NTP server or peer running the NTP to provide for time synchronization across a network. The Control Center uses NTP version 4.0.

Be sure to set the Locality correctly before enabling the NTP feature. See Setting locality on page 67 for instructions.

1. Navigate to SYSTEM > System Setup > Date and Time > NTP Time Server. The NTP Time Server tab appears (Figure 70).

**Figure 70  NTP Time Server tab**

![NTP Time Server tab](image)

2. In the NTP Time Server pane, select the Enabled check box.

3. [Optional] Select the Set time quickly check box if you want the NTP server to set the time as quickly as possible after startup. This setting exchanges accuracy for speed.

4. Add the NTP hosts the Control Center will use to the NTP Hosts list:
   a. Enter the address of an NTP host in the IP Address field
   b. Select either Server or Peer from the Type drop-down list.
   c. Click Add.

5. Click Submit.

Synchronizing clocks to the Control Center

Local hosts can synchronize their clocks to the Control Center by specifying the IP address of the Control Center virtual appliance as their network time server in the Windows Date and Time Properties dialog box.

**Prerequisite:** The host running Windows must not be connected to a domain controller.

To synchronize a clock to the Control Center:

1. In Windows XP, click Start > Settings > Control Panel > Date and Time > Internet Time tab.
2. Enter the IP address of the Control Center machine as the Network Time Server.
3. Click OK.
**Network Setup**

The Network Setup configuration area contains controls for configuring Control Center connections and adding DNS hostname information.

**Configuring the Control Center LAN connection**

You configure the direct Control Center connection settings, ethernet settings and aliases.

**Control Center direct connection**

By default, the Control Center uses a DHCP-assigned IP address. If you prefer, you can dictate a static IP address that the Control Center uses.

To change direct connection settings for the Control Center:

1. Navigate to **SYSTEM > Network Setup > Connections**. The Connections tab appears (Figure 71).

**Figure 71  Connections tab**

2. Select the **Edit** icon next to the Control Center LAN connection. This opens the Direct Connection tab (Figure 72).

**Figure 72  Direct Connection tab**

3. Enter a name for the connection in the **Connection Name** field.

4. De-select the **DHCP assigned** check box if you do NOT want DHCP to configure the interface.

5. [Conditional] If DHCP is NOT selected, enter the IP address you want to assign to the Control Center in the **IP Address** field.

6. [Conditional] If DHCP is NOT selected, enter the **Subnet Mask** you want to use for the Control Center port.
7 [Optional] Enter the IP address you want to use as the default gateway for Control Center traffic in the **Gateway** field.

8 [Optional] Enter the addresses of any DNS servers you want the Control Center to use in the **DNS Server** field.

9 Click **Update**.

**Control Center Ethernet settings**

You can change the Maximum Transfer Unit (MTU) size and the Ethernet speed for your Control Center interface.

To change Ethernet settings for the Control Center:

1 Navigate to **SYSTEM > Network Setup > Connections**. The Connections tab appears (Figure 71).

2 Select the **Edit** icon next to the Control Center LAN connection, and then click the **Ethernet Configuration** tab (Figure 73).

![Figure 73 Ethernet Configuration tab](image)

3 Specify an MTU size for the interface in the **MTU** field. The default is 1500.

4 Select a speed and duplex mode for the Ethernet interface from the **Ethernet Speed** drop-down list. The options are:
   - Default Auto Negotiation
   - 100 Base Tx - Full Duplex
   - 100 Base Tx - Half Duplex
   - 10 BaseT - Full Duplex
   - 10 BaseT - Half Duplex

5 Click **Update**.
**Aliases**

You can set Aliases for the Control Center connection.

To create an alias:

1. Navigate to **SYSTEM > Network Setup > Connections**. The Connections tab appears. (Figure 71).
2. Select the **Edit** icon next to the Control Center LAN connection, and then click the **Aliases** tab (Figure 74).

**Figure 74 Aliases tab**

![Figure 74 Aliases tab]

3. Click the **New** button. This opens the Edit Interface Aliases dialog (Figure 75).

**Figure 75 Edit Interface Aliases dialog**

![Figure 75 Edit Interface Aliases dialog]

4. Enter an **Alias IP Address** and **Alias Subnet Mask**.
5. Click **Finish**. This returns you to the Aliases tab. The new alias appears on the Aliases list.
Routes

Use the routes tab to add static routes to the network. Once a route has been added to the network, it appears in the Static Routes table.

To add a new static route:

1. Navigate to SYSTEM > Network Setup > Routes. The Routes tab appears (Figure 76).

2. Click New. The Edit Static Routes dialog appears. The Enable check box is automatically selected (Figure 77).

3. Enter the Target Address for the route. Packets are compared to the Target Address (and to the Subnet Mask) to determine whether or not they should be sent on the route.

4. Enter the Subnet Mask for the route. If you enter 32, then only packets that match the Target Address exactly will be sent along the route.

5. Select an interface from the Interface drop-down menu. For most Control Center configurations, this will be LAN A. This is the interface that packets destined for the Target Address will be sent on.

6. Enter the Gateway to send packets destined for the Target Address to.

7. Enter a Metric for the connection. When two or more routes match, the route with the lower metric will be given priority over routes with a higher metric.

8. Click Finish. The route is added to the Static Routes table (Figure 78). If the route was successfully created, the entry in the State Column will be “Installed.” If the route could not be created, the entry will be “Not Installed.” This occurs when the Target Address is unreachable from a direct connection, or when the Interface for the route has not yet started.
Managing the Control Center

Network Setup

Figure 78  Static Routes table

<table>
<thead>
<tr>
<th>Target Address</th>
<th>Subnet Mask</th>
<th>Interface</th>
<th>Gateway</th>
<th>Metric</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>32</td>
<td>LAN (Port A)</td>
<td>0</td>
<td></td>
<td>Installed</td>
</tr>
<tr>
<td>10.90.255.255</td>
<td>32</td>
<td>LAN (Port A)</td>
<td>0</td>
<td></td>
<td>Not Installed</td>
</tr>
</tbody>
</table>

DNS Hostnames

The DNS tab contains a list of static hosts for the Control Center. The static host list maps hostnames to IP addresses so that the hostnames resolve correctly even if DNS is unavailable.

To add a hostname to the Static Hosts list:

1. Navigate to SYSTEM > Network Setup > DNS. The DNS tab appears (Figure 79).

   Figure 79  DNS tab

2. Click New. This opens the Edit Static Host dialog (Figure 80).

   Figure 80  Edit Static Host dialog

3. Enter the IP Address and Hostname for the static host in the fields provided.

4. Click Finish. The new static host is added to the Static Hosts list.
Users

This section details adding administrative as well as local users for PPTP, L2TP, or dial-in access, or access through the Web proxy.

Changing the current user password

The current user can change their password and other settings on the Current User page. Depending on the privileges granted to the current user, some of the fields may be unavailable.

To change your password:

1. Select SYSTEM from the navigation menu, and then select Users. The Current User tab appears (Figure 81).

   **Figure 81  Current User tab**

2. [Optional] Enter a new description in the Description field is you so desire.

3. Enter the new user password in the Password field.

4. Repeat the new password in the Confirm Password field.

5. [Optional] If you would like to be asked to verify any changes made from the Web management console before those changes are applied to the UTM Firewall device, select the Confirm Configuration Changes check box.

6. Click Submit. Use the new password the next time you log into the management console.

Managing users

The Users page allows you to create and edit users.

User accounts allow administrative duties to be spread among a number of different people according to their level of competence and trust. Each administrative user has a password they use to authenticate when connecting to the Control Center. They also have a number of access controls that modify what they can and cannot do using the Control Center Web interface.

There is one special user, root, who has the role of the final administrative user, or super user. The access privileges for the root user cannot be lowered, and the root user cannot not be deleted or disabled. You can disallow telnet or ssh connections using the root account, however.
Creating a user
To create a user:
1. Navigate to SYSTEM > Users > Users. The Users tab appears (Figure 82).

Figure 82 Users tab

2. Click New. The Edit User Information dialog appears (Figure 83).

Figure 83 Edit User Information dialog

3. Enter a Username (login name). The username must start with an alphabetic character, but can consist of alphanumeric characters.

4. [Optional] Enter a description of the user in the Description field.

5. Enter a password in the Password field. The password can be one or more characters of any type.

6. Confirm the password in the Confirm Password field.

7. Select a Password Class for the user. Password class defines such parameters as the number of log-in attempts allowed, or how often a user must change their password. See Creating a new Password class on page 81 for details.

8. [Optional] Select one or more groups that the user is a part of. Users gain all the permissions of the groups they belong to.

9. Click Finish. The administrative user is displayed in the edit box and is enabled by default.

To disable a user, clear the check box next to their name.
**Managing the Control Center**

**Users**

**Editing a user**
To edit a user:

1. Navigate to **SYSTEM > Users > Users**. The Users tab appears (Figure 82).
2. Click the edit icon next to their username. The Edit User Information page is displayed.
3. Make your changes and click **Finish**.

**Deleting a user**
To remove a user:

1. Navigate to **SYSTEM > Users > Users**. The Users tab appears (Figure 82).
2. Click the delete icon next to their username.
3. Confirm the delete. The user is removed from the list of users.

*Note*: The root user cannot be deleted.

**Managing user groups**
Groups enable you to assign access control lists (ACLs) to multiple users, by assigning user with similar privileges to the same group. You can create new groups and edit existing ones on the Groups page.

**Creating a group**
To create a group:

1. Navigate to **SYSTEM > Users > Groups**. The Groups tab appears (Figure 84).
   
   **Figure 84  Groups tab**

<table>
<thead>
<tr>
<th>UCC</th>
<th>System Setup</th>
<th>Network Setup</th>
<th>Users</th>
<th>Management</th>
<th>Diagnostics</th>
<th>Advanced</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Click the **New** button. This opens the Edit Group Settings dialog (Figure 85).
3 Enter a name for the group in the **Group** field.

4 Select the check boxes of one or more User ACLs.

5 [Optional] If the group includes users with administrative responsibilities, select one of the built-in **Predefined Administration Roles** from the drop-down menu. The pre-defined roles are:
   - Administration
   - Diagnostic

6 [Optional] Select an access level for each Administrative ACL. Options are:
   - **No Access**
   - **Read Access**
   - **Write Access**

   **Note:** Write Access includes read access.

7 [Optional] You can include the group in another group or groups by selecting the check boxes of the pertinent groups from the group list.

8 Click **Finish**. The newly created group is added to the group list on the Groups tab, and can be selected when creating or editing users.
**Editing a group**
To edit a group:

1. Navigate to **SYSTEM > Users > Groups**. The Groups tab appears (Figure 84).
2. Select the edit icon next to the group you wish to edit. This opens the Edit Group Settings page.
3. Make the necessary changes to the ACLs and group memberships.
4. Click **Finish**.

**Deleting a group**
To remove a group:

1. Navigate to **SYSTEM > Users > Groups**. The Groups tab appears (Figure 84).
2. Select the delete icon next to the group you wish to edit. A pop-up window appears asking you to confirm the deletion.
3. Click **OK**.

**NT domains**
The Domain page allows you to specify a Windows NT domain and primary and secondary servers so that authentication can take place against the domain controller.

To configure your Windows NT workgroup settings:

1. Navigate to **SYSTEM > Users > Domain**. The Domain tab appears (Figure 86).

![Figure 86 Domain tab](image)

2. In the NT Domain field, enter domain name.
3. Enter the Primary Server.
4. Enter the Secondary Server.
5. Click **Submit**.
### RADIUS

The Control Center can be configured to access a central repository of users and passwords on a RADIUS server to authenticate connections.

Multiple RADIUS servers can be added by clicking **New** or the **Add Above** or **Add Below** buttons. If multiple RADIUS servers are configured, the order in which they are queried can be set by using the **Move Up** and **Move Down** arrows next to each server.

To configure the Control Center for one or more RADIUS servers:

1. Navigate to **SYSTEM > Users > RADIUS**. The RADIUS tab appears (Figure 87).

![Figure 87 RADIUS tab](image)

2. Click **New**. The RADIUS Server Details dialog opens (Figure 88).

![Figure 88 RADIUS Server Details dialog](image)

3. Enter the **RADIUS Server** address from which to obtain client authentication information.

4. Enter a port number in the **RADIUS Server Port** field. This can be any integer in the range: 1-65535. The default is port 1812. Some older RADIUS servers use port 1645.

5. Enter and confirm a secret string in the **RADIUS Secret** field. The secret is used to access the RADIUS server, and can be 1 or more characters of any type.

6. Click **Finish**. The new RADIUS server appears on the RADIUS server list.
Managing the Control Center

Users

**TACACS+**

The Control Center can be configured to access a central repository of users and passwords on a TACACS+ server to authenticate connections.

To configure the Control Center for a TACACS+ server:

1. Navigate to **SYSTEM > Users > TACACS+**. The TACACS+ tab appears (Figure 89).

   ![Figure 89 TACACS+ Configuration page](image)

2. Enter the address from which to obtain client authentication information in the **TACACS+ Server** field. This address can be a fully qualified domain name of the form `host.domain.com`. Each label (such as host or domain) can consist of alphanumeric characters including hyphens. Each label cannot begin or end with the hyphen (-) character. The address can also be an IP address of the form `a.b.c.d`.

3. Enter the secret used to access the TACACS+ server in the **TACACS+ Secret** field. The secret can be 1 or more characters of any type.

4. Enter the secret again in the **Confirm TACACS+ Secret** field.

5. Click **Submit**.

**Password classes**

Password classes allow you to set administrative lock-out parameters for the passwords of different users (see Editing a user on page 77 for instructions on how to assign password classes to users). Two Password classes are defined for you from the outset: default and PCI-DSS. The default Password class defines no administrative lock-out parameters on passwords. The PCI-DSS class sets administrative lock-out settings in accordance with the user authentication and password management requirements of the PCI DSS. Other PCI DSS 1.1 and 1.2 requirements are met by the Control Center by default, and require no further administrative management. You can also create your own custom class.

**Creating a new Password class**

To create a new password class:

1. Navigate to **SYSTEM > Users > Passwords**. The Passwords tab appears (Figure 90).

   ![Figure 90 Passwords tab](image)

2. Click **New**. This opens the Edit Password Class Setting dialog (Figure 91).
3 Enter a descriptive name for the new password class in the **Class Name** field.

4 Accept the default field entries, or replace them with your own preferred values.

   **Note:** The default values meet PCI DSS user authentication and password management requirements.

Each field is described below.

   **Note:** A setting with a value of zero (0) is ignored.

- **Failed attempts before locking unit** – the maximum number of times a user can enter an incorrect login name or password before they can no longer access the unit.

- **Lock out time period** – the duration of the lock out in seconds.

- **Reauthentication idle time** – the amount of time a user may do nothing before having to log in to the unit again.

- **Disuse deletion time** – the number of days an account may be idle before it is automatically removed from the system.

- **Deletion warning time** – the number of days before an account is deleted that an email warning of the impending deletion is sent to the address entered into the Warning email address field.

- **Disuse disable time** – the number of days an account can sit idle before being disabled.

- **Disable warning time** – the number of days before an account is disabled that an e-mail warning of the impending disabling is sent to the address in the Warning email address field.

- **Warning email address** – the email address that warnings are sent to.

- **Email server** – the SMTP server of the Warning email address.
• **Minimum password length** – the minimum length for passwords in this class.

• Selecting the following check boxes places restrictions on how passwords in this class are formed. The more options selected, the more secure passwords are.

  • **Passwords must include letter(s)** – all passwords must include at least one (1) letter.
  
  • **Passwords must include mixed cases** – all passwords must contain both lower- and upper-case characters.
  
  • **Passwords must include digit(s)** – all passwords must include at least one (1) number.
  
  • **Passwords must include other character(s)** – all passwords must include at least one (1) character that is neither a letter nor a number.
  
  • **Password lifetime** – the number of days before a new password must be chosen.
  
  • **Number of illegal historic passwords** – number of password changes that must occur before a password can be re-used.
  
  • **Change of passwords on first access** – select this check box to force users to change their passwords the first time they log into the unit.

5 Once all the fields have been filled to your satisfaction, click **Finish**.

**Editing a password class**

To edit an existing password class:

1. Navigate to **SYSTEM > Users > Passwords**. The Passwords tab appears (Figure 90).
2. Click the edit icon next to the Password class you wish to edit.
3. Enter the new values in the fields as necessary.
4. When you are satisfied with the changes, click the **Finish** button.

**Deleting a password class**

To remove a password class:

1. Navigate to **SYSTEM > Users > Passwords**. The Passwords tab appears (Figure 90).
2. Select the delete icon next to the password class to remove.
3. A pop-up window appears asking if you are sure you want to delete the class. Click **OK**.
4. The password class is removed from the list of classes.
Service Authentication

The Control Center provides a Pluggable Authentication Manager (PAM) to configure authentication policies for the services running on your Control Center virtual appliance.

To set authentication policies for a service

1. Navigate to **SYSTEM > Users > PAM**. The PAM tab appears (Figure 92).

   **Figure 92  Pluggable Authentication Manager tab**

   ![Pluggable Authentication Manager tab](image)

2. For each service,
   a. Select an **Authentication Method**. Options are:
      - **Local** – the service is authenticated against the UTM Firewall device’s internal database.
      - **Disabled** – no authentication for the service is possible.
      - **NT Domain** – the service is authenticated against a Windows workgroup server.
        
        **Note**: Selecting NT Domain requires the fields on the Domain tab be completed. See **NT domains** on page 79.
      - **TACACS+** – the service is authenticated against a remote TACACS+ server.
        **Note**: Selecting TACACS+ requires the fields on the TACACS+ tab be completed. See **TACACS+** on page 81.
      - **RADIUS** – the service is authenticated against a remote RADIUS server.
        **Note**: Selecting RADIUS requires the fields on the RADIUS tab be completed. See **RADIUS** on page 80.

3. Enter the amount of time in seconds for a successful authentication to be cached in the **Authentication Lifetime (seconds)** field.

   **Note**: In order to maintain PCI DSS compliance, this time out value should be less than the time out value specified for any associated Password class. See **Password classes** on page 81.

4. Enter the maximum number of authentications that may be cached at one time in the **Maximum Cached Authentications** field.

   **Note**: When the **Maximum Cached Authentications** value is reached, authentications are removed from the cache before they have expired, resulting in increased load on the authentication servers.
5 Select a **Default Group** for the service. When an authentication source is unable to provide enough detail about a user for the Control Center to assign that user permissions, the permissions of the group specified here are used instead.

   **Note:** A default group must be specified for TACACS+.

6 [Optional] De-select the **Override Default Group** check box if you want the Control Center to always use the default group permissions even when user information is available to the authentication source.

7 Click **Submit** to save your changes.

You can clear any changes made to the PAM table by clicking the **Clear Authentication Cache** button.

---

**Management**

The Control Center can be managed from the Control Center Web interface, or from an ssh or telnet connection. The Management menu provides configuration options that control how the Control Center is managed.

**Web configuration**

You can enable or disable HTTP protocols, change HTTP port numbers, and create or upload certificates for securing access to the Web interface using HTTPS on the Web page.

**Configuring the Web interface**

Use this procedure to configure access to the Control Center Web interface.

**Caution:** Do NOT disable both HTTP and HTTPS access to the Control Center Web interface. Doing so prevents all access to the Web interface. If this occurs, you must edit the configuration file using SSH to reestablish access.

To set Web interface access

1 Select **SYSTEM** from the navigation menu, and then select the **Management** tab. The Web tab appears (Figure 93).

**Figure 93  Web tab**

<table>
<thead>
<tr>
<th>Web</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Management Configuration</td>
<td></td>
</tr>
</tbody>
</table>
| UCC can be configured to run its web admin server on a port other than the HTTP default (80). Changing the default administration port is recommended if you intend to allow UCC to be configured externally, not just from the trusted (LAN) side on your network. Note: To continue configuration of UCC you will need to point your browser to the new administration port (e.g. a device at IP address 10.0.0.1 using administration port 888 is http://10.0.0.1:888/).
| HTTP Configuration | |
| Enable HTTP Management | ✔ |
| Port for HTTP | 80 |
| HTTPS Configuration | |
| Enable HTTPS Management | ✔ |
| Port for HTTPS | 443 |
| HTTPS Protocols | |
| Use SSL 2.0 | ✔ |
| Use SSL 3.0 | ✔ |
| Use TLS 1.0 | ✔ |
| **Submit** | **Upload Certificate** | Create Certificate |
2 Ensure the **Enable HTTP Management** check box is selected.

3 The Control Center Web interface runs on the default HTTP port 80. To use the default port for another purpose, change the port number in **Port for HTTP** field.

   If you change the Web server port number, you must include the new port number in the URL to access the pages. For example, if you change the Web administration to port number 888, the URL to access the Web administration is similar to: `http://192.168.0.1:888`.

4 [Optional, recommended] To enable secure HTTP (HTTPS), select the **Enable HTTPS Management** check box.

5 [Optional] The Web management console runs on the default HTTPS port 443. You can change the port number in the **Port for HTTPS** field.

   To access the Web management console securely using SSL encryption, add an “s” to http so that the URL becomes `https://` instead of `http://`. An example URL: `https://10.0.0.1:443`

   If you plan to use secure HTTPS to access the console, either uploading an SSL certificate or manually creating a more customized certificate than the default out-of-box certificate is recommended. For instructions, see To upload an SSL certificate on page 86 and Creating an SSL certificate on page 87.

6 [Optional] Select one or more of the check boxes listed beneath HTTPS Protocols to specify the protocols a client can use to access the Control Center Web interface over HTTPS.

7 Click **Submit**.

**Certificates for HTTPS**

A certificate for HTTPS (Secure HTTP) access is generated automatically when the appliance is first booted. The certificate contains default information for country, city, and related fields. It is enough to allow HTTPS access out-of-the-box, and it is relatively secure as no two UTM Firewall devices have the same certificate. However, it is strongly recommended that an appropriate site-specific certificate either be uploaded or manually created at the earliest possible convenience. A proper certificate enables remote clients to establish the Control Center's authenticity upon connection using chain of trust, signed root-certificate, or site-specific fingerprint. If you have purchased or created SSL certificates for a Web server, you can upload them to the Control Center.

To upload an SSL certificate

1 Select **SYSTEM** from the navigation menu, and then select the **Management** tab. The Web tab appears (Figure 93).

2 Click **Upload certificate**. The Add Local and Private Certificates dialog appears (Figure 94).

   ![Figure 94 Add Local and Private Certificates dialog](image)
3 Click **Browse** to locate the **Local Certificate** (RSA x509 certificate) and its corresponding **Private Key Certificate**.

4 Click **Submit**.

**Creating an SSL certificate**

Use this procedure to manually create or update a self-signed certificate on the Control Center. The optional fields are used to create the distinguished name of the certificate. For best results, complete all optional fields.

When you access the Control Center Web interface using HTTPS, your Web browser may give warnings about the authenticity of the certificate since it has not been signed by a known Certificate Authority. For more information, see *To upload an SSL certificate on page 86*. Otherwise, if you want to import your certificate into the IE browser, see *Installing your certificate in your browser on page 88*.

To create an SSL certificate:

1 Select **SYSTEM** from the navigation menu, and then select the **Management** tab. The Web tab appears (Figure 93).

2 Click **Create SSL certificates**. The SSL Certificate Setup dialog appears (Figure 95).

**Figure 95  SSL Certificate Setup dialog**

![SSL Certificate Setup dialog](image)

3 [Optional] Select the appropriate country from the **Country** list.

4 [Optional] Enter the state or province in the **State or Province** field.

5 [Optional] Enter the name of your organization in the **Organization or Company** field.

6 [Optional] Enter your department in the **Section or Organization appliance** field.

7 Enter the IP address in the **Host name** field.

8 [Optional] Enter an e-mail address in the **e-mail Address** field.
9. Select a certificate key length from the **Generate an RSA key of** list. Available options are:

- 512 bits (default)
- 1024 bits
- 1536 bits
- 2048 bits
- 3072 bits
- 4096 bits

**Note:** The more bits in the key, the longer it takes to generate the certificate. Larger keys take much longer to generate than smaller keys. A 1024-bit key takes more than double the amount of time to generate than a 512-bit key. Similarly a 4096-bit key takes more than four times as long as it would take for a 1024-bit key. Patience is advised when generating 4096-bit keys. Key generation is a very CPU-intensive operation that is not directly related to the effort required to use the key.

10. Click **Submit**. A message informs you that an SSL certificate is currently being created. Generating a certificate usually takes a few minutes; exact time depends on the key length. When the certificate has been created, the message “A valid SSL certificate has been installed” is displayed under the Web tab.

### Installing your certificate in your browser

Use this procedure to install your manually created certificate into the Internet Explorer browser. The certificate is already installed on the Control Center.

**Prerequisites:**

- Create a self-signed certificate manually with more detail than the shipped default. See *Creating an SSL certificate* on page 87.
- Enable HTTPS. See *Web configuration* on page 85.

When you access the Control Center Web interface using HTTPS, your Web browser may give warnings about the authenticity of the certificate since it has not been signed by a known Certificate Authority. This procedure installs the certificate in the browser.

Uploading a certificate signed by an authority is the most secure and recommend method. For more information, see *To upload an SSL certificate* on page 86.

To install a certificate in your Internet browser:

1. Access the Control Center Web interface using your HTTPS URL.

2. When the IE browser’s Security Alert dialog box is displayed, click **View Certificate**. The general certificate information is displayed (Figure 96).
3 You can view the Details or Certification by click the relevant tab. Click **Install Certificate**. The wizard begins (Figure 97).

**Figure 97 Certificate Import Wizard**

4 Click **Next**. The Certificate Store page appears (Figure 98).
5 Select the **Automatically select store based on type** option and click **Next** (Figure 99).

6 Click **Finish** (Figure 100).
A security warning dialog box displays the thumbprint and requests you to confirm the import (Figure 101).

Click Yes. The Certification Path is displayed (Figure 102).
9 Click **OK**. You no longer receive alerts when you access the console via https.

10 To view the certificates installed in the browser, click **Tools > Internet options > Content tab > Certificates** button. The Certificates dialog box appears (Figure 103).
Command line access

The Control Center is configured to allow telnet and ssh service access by default.

To alter the command line access to the Control Center:

1. Navigate to SYSTEM > Management > Command Line. The Command Line tab appears (Figure 104).

   **Figure 104  Command Line tab**

   ![Command Line Management Configuration](image)

2. Select or clear the appropriate check boxes.

   - Selecting the **Enable Telnet Service** check box allows telnet access to the Control Center.
   - Selecting the **Enable SSH Service** check box allows ssh access to the Control Center.

3. Click **Submit** to save the configuration changes.

Diagnostics

Low-level diagnostic information and network tests are provided to assist you in diagnosing network problems.

Viewing diagnostic information

The System tab displays information including the current version, serial number, network settings, and the status of Internet connections (Figure 105).
To view basic diagnostic information about the Control Center

1. **Select SYSTEM** from the navigation menu, and then select the **Diagnostics** tab. The System tab appears.
2. **Scroll** the file to view the available information.
Managing the Control Center
Diagnostics

Viewing the local system log

The system log contains debugging information that may be useful in determining whether all services for the Control Center are operating correctly. Every message recorded by a service on the Control Center has an associated logging level such as “Debug” or “Warning”. By default, all log level messages are posted to the System Log. You can filter the displayed messages or reset the default filtering level.

Log output is color-coded by output type. General information and debug output is black, warnings and notices are blue, and errors are red.

To open and navigate the system log

1. Navigate to SYSTEM > Diagnostics > System Log. The View Log tab appears (Figure 106).

   Figure 106 View Log tab

2. Within this log, you can do the following:
   - Click Go to end of Log link to go to the end of the log.
   - Click Go to start of Log link to go return to the top.
   - To search for a string, enter characters in the Match this string field at the bottom of the page and click Update. The log isolates your search terms.
   - To clear the system log messages, click Clear Messages.
   - To filter the log output to display based on output type, select an option from the Display list. To reset the default filtering level, see Configuring local system log settings on page 96.
Configuring local system log settings
By default, all messages are recorded in the System Log. The Filter Level setting allows you to control which classes of messages are recorded in the system log.

Tip: If your logging requirements generate extremely large log sizes, McAfee recommends using a remote syslog server. See Enabling remote system logging on page 97.

To change log settings:

1. Navigate to SYSTEM > Diagnostics > System Log > Local Syslog. The Local Syslog tab appears (Figure 107).

   Figure 107  Local Syslog tab

2. Select a default filtering level from the Filter Level list. Available options include:
   - Absolutely Everything (most verbose)
   - Everything but Debug
   - Notices, Warnings, and Errors
   - Errors and Warnings
   - All Error Conditions
   - Emergency, Alerts, and Critical Errors
   - Emergency and Alerts Errors
   - Emergency Errors only (least verbose)

3. [Optional] Every message recorded in the System Log includes a basic time stamp. To force a more precise and standardized time stamp with every message, select the Include extended ISO date check box.

4. To increase the size of this buffer to retain more messages when tracking down issues, enter an increased integer value in the Syslog buffer size field. This field specifies the maximum size of the local buffer that contains syslog messages.

   Caution: For best results, keep the log size approximately half the size of the available space to accommodate rotating system logs.

5. Click Submit.
Enabling remote system logging
Use this procedure to redirect the system log messages to a remote system. System log messages can be sent to a remote syslog server, which allows you to keep system log messages persistently.

Tip: There are freely available syslog servers for the Windows platform. For more information, refer to the article, How do I enable remote logging? in the KnowledgeBase at mysupport.mcafee.com.

To enable remote system logging:

1. Navigate to SYSTEM > Diagnostics > System Log > Remote Syslog. The Remote Syslog tab appears (Figure 108).

Figure 108  Remote Syslog tab

2. Select the Enable Remote Logging check box.

3. Enter the IP address or DNS hostname for the remote syslog server in the Remote Host field.

4. Enter the Remote Port on which the remote syslog server is listening for syslog messages. Typically, the default is correct.

5. Set the Filter Level to only send syslog messages at this level or above.

6. [Optional] To force a more precise and standardized time stamp with every message, select the Include extended ISO date check box. The date is prepended to syslog messages before being sent.

7. Click Submit.
**Managing the Control Center**

**Diagnostics**

**Directing the Control Center system log to an e-mail account**
You can send all Control Center system log messages to an e-mail account.

To send system log messages to an e-mail account:

1. Navigate to **SYSTEM > Diagnostics > System Log > Email Delivery**. The Email Delivery tab appears (Figure 109).

   ![Email Delivery tab](Figure 109 Email Delivery tab)

2. Select the **Enable Email Logging** check box.

3. Enter the address of an **Email Server** (SMPT server) that accepts e-mail for forwarding.

4. Enter one (1) or more **Email Addresses** to send the system log messages to.

5. Specify the **Sender Email** address that System Log messages are sent from.

6. Set the **Filter Level** to only send syslog messages at the selected level or above.

7. Specify the number of seconds to wait after receiving a system log message before sending an e-mail in the **Delay to Send** field. This allows multiple system log messages to accumulate before sending an e-mail containing all messages.

8. Enter the maximum number of system log messages that are allowed to accumulate before the Control Center sends a syslog e-mail in the **Messages per Email** field. The default setting of 0 means no maximum, and is typically appropriate for all systems except those that experience heavy traffic.

9. Click **Submit**.

**Performing network tests**

The basic network tests of ping and traceroute help test the current functionality of the Control Center virtual appliance.
Ping test
Use this procedure to perform a ping test within the Web management console. Use the ping test to verify packets are able to reach and return from a specific host either on the Internet or on your local network.

To perform a ping test:
1. Navigate to SYSTEM > Diagnostics > Network Tests. The Network Tests tab appears (Figure 110).

   **Figure 110  Network Tests tab**

2. Enter the IP Address of the box you want to ping in the **IP Address of Remote Machine** field.
3. [Optional] Select an interface from the **Source Interface** list.
4. [Optional] To perform a reverse DNS names lookup on IP addresses, select the **Lookup DNS Names** check box.
5. Click **Ping**.

   The results of the test are displayed (Figure 111).

   **Figure 111  Ping test results**
**Traceroute test**

Use this procedure to perform a traceroute test within the Web management console. The traceroute test traces the network path that packets travel as they attempt to reach and return from a specific host either on the Internet or on your local network.

To perform a traceroute:

1. Navigate to SYSTEM > Diagnostics > Network Tests. The Network Tests tab appears (Figure 110).
2. Enter the IP Address you want to trace packet routing for in the IP Address of Remote Machine field.
3. [Optional] Select an interface from the Source Interface list.
4. [Optional] To perform a reverse DNS names lookup on IP addresses, select the Lookup DNS Names check box.
5. Click either ICMP Traceroute or UDP Traceroute. The results of the test are displayed (Figure 112).

**Figure 112** Traceroute results (UDP traceroute)

---

**Advanced**

The Advanced configuration area includes rebooting and upgrading the Control Center and modifying configuration files.

**Halting the Control Center before powering down**

Use this procedure to halt the Control Center before you power down. This ensures all configuration is saved. Allow the Control Center 20-30 seconds before powering down after a halt.

To halt the Control Center:

1. Navigate to SYSTEM > Advanced > Reboot. The Reboot tab appears (Figure 113).
2. Click Halt.
Rebooting the Control Center

Use this procedure to perform a reboot of the Control Center virtual appliance. Normally, this should not be required, but if so, should be done from the user interface rather than from the command line to prevent configuration from being lost. Rebooting does not erase your Control Center configuration; however, network connections such as your Internet connection are terminated and reestablished when the device is up and running again.

To reboot the Control Center:

1. Navigate to SYSTEM > Advanced > Reboot. The Reboot tab appears (Figure 113).
2. Click Reboot. It usually takes around 10 seconds before the Control Center is up and running again.

Upgrading the Control Center

Periodically, McAfee releases new versions of the UTM Firewall Control Center. If a new version fixes an issue you have been experiencing, or contains a new feature you want to use, go to the download page on the product registration Web site to obtain the latest version. You can then load the new version with a flash upgrade.

Upgrades are generally performed using HTTP. Remote upgrades can also be performed using TFTP if you have a TFTP server at the remote site.

Upgrading the Control Center using HTTP

Use this procedure to perform a flash upgrade of the Control Center using HTTP.

Prerequisite: Download the binary image file (.sgu).

To upgrade the Control Center using HTTP:

1. Navigate to SYSTEM > Advanced > Flash Upgrade > Upgrade via HTTP. The Upgrade via HTTP tab appears (Figure 114).

   ![Figure 114 Upgrade via HTTP tab]

2. In the Flash Region section, select the Firmware radio button.
3. Click Browse to locate the .sgu file on your local system.
4 Enter any **Extra Parameters** only at the request of McAfee technical support staff.

**Tip:** Should you require to downgrade your firmware or restore a configuration from an earlier firmware version, enter `-i` in the Extra Parameters field to circumvent the firmware version checking.

5 Click **Upgrade**. Wait for the upgrade to complete.

**Upgrading the Control Center using TFTP**

Trivial File Transfer Protocol (TFTP) is a simplified version of FTP that allows transfer of files between computers over a network. An alternative method to flash upgrades via HTTP is to install and configure a TFTP server and use that for flash upgrades. The majority of Linux distributions include a TFTP server; Windows users can download one from [http://www.snapgear.com/ftp/tools/tftpd32j.zip](http://www.snapgear.com/ftp/tools/tftpd32j.zip).

**Note:** Although TFTP is an option for upgrading, this program is not supported by McAfee technical support.

**Prerequisites:**
- Download the binary image file (**.sgu**). Go to the product Web site for instructions on obtaining this file.
- Place the **.sgu** file in the directory your TFTP is serving files from, usually: `/tftpboot/`

To flash upgrade with TFTP, you can either use the Flash Upgrade (TFTP) page or run a command on the command line interface.

**Upgrading using TFTP from the Web management console**

**Prerequisite:** Download the binary image file (**.sgu**) and place it on the machine running the TFTP server.

To upgrade firmware using the TFTP page

1 Navigate to **SYSTEM > Advanced > Flash Upgrade > Upgrade via TFTP**. The Upgrade via TFTP tab appears (Figure 115).

**Figure 115  Upgrade via TFTP page**

2 Enter the IP address of the machine running the TFTP server in the **IP address** field.
3 Enter the name of the image file in the **Filename** field. Place this file in the directory your TFTP is serving files from, usually: `/tftpboot/`.

4 Enter any **Extra Parameters** only at the request of McAfee technical support staff.

5 Click **Upgrade**. The firmware upload only accepts valid firmware images and only accepts newer images appropriate for your device. Wait for the upgrade to complete.

**Upgrading using TFTP from the command line interface**

Use this procedure to perform a flash upgrade using TFTP on the command line interface.

*Note:* The Control Center Web interface provides the same functionality as the command line interface for flash upgrades via TFTP. Using the command line for flash upgrades is only recommended if the upgrade from the Web interface TFTP page is failing, and you want additional diagnostic information.

To upgrade using TFTP from the command line:

1 Establish a telnet or SSH connection to the Control Center virtual appliance.

2 Login and run the command:

   ```
   netflash <TFTP server address> <image.sgu>
   ```

   where `<TFTP server address>` is the address of your TFTP server, and `<image.sgu>` is the binary image filename. Your telnet or SSH connection is terminated once the upgrade commences.
Configuration Files

The Configuration Files tab provides direct and quick access to configuration files within the Edit Files tab.

Editing a configuration file

Use this procedure to manually edit configuration files within the Control Center Web interface. Binary files cannot be selected and do not have an edit icon.

Caution: Make sure you edit in the “Custom entries below here” section if present in the configuration file.

To manually view or edit a configuration file:

1. Select SYSTEM from the navigation menu, and select the Advanced tab and the Configuration Files tab. The Edit Files tab appears (Figure 116).

Figure 116  Edit Files tab

The Filename column indicates the configuration file name. The Size column indicates the amount of space on the configuration that a file is using. There is a limited amount of configuration space available on an appliance. The Mode column indicates whether a file has read (r), write (w), and delete (x) access.

Caution: Exercise caution when manually editing configuration files. Manually modifying or deleting the configuration files of your UTM Firewall device may render the appliance inoperable until a factory erase has been performed.

2. To edit a file, select the check box next to the filename and click its edit icon.

Tip: You can also click the Modify button at the bottom of the configuration files list. To edit multiple files, select the check boxes for the files and click Modify. An edit window opens for each file you want to modify.

The Modify File dialog appears (Figure 117). The name of the file you are editing displays in the Filename field.
3 Carefully make your edits in the text box.

4 Click Finish.

Creating a configuration file
To manually create a configuration file:
1 Navigate to SYSTEM > Advanced > Configuration Files. The Edit Files tab appears (Figure 116).
2 Scroll to the bottom of the page and click New. An empty Modify File page appears.
3 Enter the filename, enter the configuration details, and click Finish. The file is added to the list of configuration files. Note that any files you create manually have the “x” attribute (able to delete) displayed in the Mode column.

Deleting a configuration file
Use this procedure to delete a configuration file. Exercise care when performing this operation as it cannot be reversed.

Caution: Manually deleting the configuration files of your Control Center virtual appliance may render the appliance inoperable.

To delete a configuration file:
1 Navigate to SYSTEM > Advanced > Configuration Files. The Edit Files tab appears (Figure 116).
2 Select the delete icon next to the file you want to delete. You are prompted to confirm the delete.
3 Click OK.

Tip: You can also click the Delete button at the bottom of the configuration files list. To delete multiple files, select the check boxes for the files and click Delete.
Uploading a configuration file

Configuration files may be uploaded from your local PC directly to the Control Center virtual appliance.

To upload a configuration file:

1. Navigate to SYSTEM > Advanced > Configuration Files > Upload File. The Upload File tab appears (Figure 118).

   **Figure 118** Upload File tab

   ![Upload File tab](image)

2. To locate the file on your local PC that you want to upload, click **Browse**. Locate the file and click **Open**, or type the full path to the file in the **File to Upload** field.

3. [Optional] You can upload it to an alternative file name on your system by specifying another name in the **Destination File Name** field.
   
   **Caution:** Any existing file with the same name is overwritten.

4. Click **Submit**.
Directly viewing or editing the configuration files

It is possible to view or modify the Control Center configuration directly. This should only be done when requested by technical support.

Caution: Do not edit this file without the assistance of technical support.

To view and edit Control Center configuration files:

1. Navigate to **SYSTEM > Advanced > Device Config**. The Device Config tab appears (Figure 119).

   ![Figure 119  Device Config tab](image)

   - **Display/Modify Device Configuration**
     - Warning: This page allows configuration settings to be modified directly. Do this at your own risk, and preferably only as instructed by the appropriate Technical Support personnel.
     - `acl debug: 0 auth.radius
       port: 1012
       secret:
       server:
       auth.radius_server (nonexistent)
     auth.amb
       domain:
       server:
       server1addr:
       server2addr:
     auth.tecacs
       secret:
       server:
     attr
       satlocale: 1
       setpassword: 1
     omnasever
     ssh_timeout: 30
   
2. Make changes as instructed by technical support personnel.

Support

The Support page provides links to technical support resources. This page provides information about the firmware release notes, links to the Knowledge Base and the Technical Support site, and a link that allows you to download the technical support report. The technical support report is used to assist technical support staff with troubleshooting the configuration of your appliance. When contacting Technical Support, you should always download and attach a technical support report. See Technical support reports on page 108 for details.

To access the Technical Support page, select **SYSTEM** from the navigation menu, click the **Support** tab, and then click **Technical Support**. The Technical Support tab appears (Figure 120).
Managing the Control Center
Support

Figure 120  Technical Support tab

Technical support reports

The Technical Support Report page is an important and invaluable resource for the technical support team to use to analyze issues with the Control Center. If you experience an issue with the Control Center, and you need to contact the technical support team, always include the technical support report with your support request. With this report the technical support staff have the information they need to assist you.

Security Alert: To maintain your security and privacy, the technical support report removes any confidential information such as passwords and keys.

Tip: Generate the technical support report when the issue is occurring. In addition, generate a report on each of the appliances involved, and attach them to the support request in plain text format.

To generate a technical support report:

1. Navigate to SYSTEM > Support > Technical Support Report. The Technical Support Report tab appears (Figure 121).

Figure 121  Technical Support Report tab

2. [Optional] Select the Include full logs check box if you want to include all log entries in the technical support report. Otherwise, only the most recent log entries are included.

3. Click Download.

4. Save the report as a text file.

5. Submit a support request and attach the technical support report in plain text format.
Backing up the Control Center

The Control Center must be backed up at the virtual appliance level. The files that are crucial to restoring the Control Center are:

- **UCC.cfg** – contains Control Center configuration settings and policies
- **UCC.var** – contains Control Center log files
- **UCC.vmx** – contains the generated MAC address for the Control Center

To back up the Control Center:

1. On the host server, navigate to the folder containing the Control Center virtual appliance.
2. Copy the **UCC.cfg**, **UCC.var**, and **UCC.vmx** files to another location, or copy the entire Control Center folder to another location.
Index

A
attributes
  device attributes
    defining from the Control Center 31
    setting 20
attributes, device
  defined 8

B
backing up the Control Center 109

C
certificates 86
  creating 87
  installing in browser 88
  uploading 86
command line access 93
configuration files 104
  creating 105
  deleting 105
  editing 104, 107
  uploading 106
Content Filtering policies 42
Control Center
  backing up 109

D
date
  setting the Control Center 67, 68
  syncing 68
device attributes
  defined 8
  listing necessary 12
device group pane 32
device groups
  defined 8
  listing necessary 12
device groups pane 28
Device Status 27
devices
  see UTM Firewall devices 25
diagnostics 93
DNS Proxy policies 37

E
event log 30

F
firewall policies 40
firmware
  storing images on the Control Center 64
  updating device 61

G
Group Status 26
group view
  changing 32
  creating a 32
  modifying a 33
groups
  creating 33
  editing 79
  user groups 77
groups, device
  defined 8
halting the Control Center 100

I
Incoming Access policies 44
installation 15
IPsec
  endpoint policies 51
  managed endpoint policies 52
  tunnel mapping policies 56
  tunnel policies 54
  unmanaged endpoint policies 53

L
L2TP
  Client policies 48
  Server policies 50
logging
  remote 97
logging in 18
logging out 18

M
McAfee Firewall Reporter 14
monitoring devices 25

N
Navigation menu 9
Networking policies 37
NT domains 79
NT workgroups 79

P
Packet Filtering policies 40
PAM 84
password classes 81
  creating 81
deleting 83
  editing 83
PCI DSS 81
ping tests 99
Pluggable Authentication Manager
  see PAM 84
policies
  creating 36
  defined 7
  deleting 36
  editing 36
  managing 35
  see also specific policies 36
ports
  Control Center traffic 65
PPTP
  Client policies 45
  Server policies 47
public key
  downloading 19
R
RADIUS 80
rebooting the Control Center 100
reports
  technical support report 108
root user 75
RSA Keys 63
S
server
  RADIUS 80
  TACACS+ 81
shortcuts 9
SSL
  see certificates 86
Supported Devices 13
system log
  configuring settings 96
  logging 95
  remote logging 97
System policies 57
system requirements 14
T
TACACS+ 81
Task Queue 29
technical support report 108
time
  setting Control Center 67, 68
time policies 57
time-out 65
traceroute tests 100
Traffic Shaping policies 38
U
UCC page 65
upgrading the Control Center 101
  using HTTP 101
  using TFTP 102
user groups 77
  creating 77
  deleting 79
user policies 58
users 75
  current 75
  deleting 77
  editing 77
  root 75
  see also user groups 77
UTM Firewall devices 20
  device status 27
  enabling Control Center management on 20
  monitoring 25
  rebooting 62
  registering with the Control Center 22
  setting attributes 20
  updating 61
V
VMware 13
VPN policies 45
W
Web access 85
Web interface 9
  configuring 85
wireless policies 39