UTM Basic Configuration

This guide describes how to use the Unified Threat Management appliance (UTM) Basic Setup Wizard to configure the UTM for connection to your network. It also describes how to register the UTM with NETGEAR. For information about other features and for complete configuration steps, see the *ProSecure Unified Threat Management (UTM) Appliance Reference Manual* at: *http://downloadcenter.netgear.com*.

This guide contains the following sections:

- Steps for Basic Configuration
- Log In to the UTM
- Use the Setup Wizard to Perform the Basic Configuration
- Verify Correct Installation
- Register the UTM with NETGEAR
- What to Do Next

Steps for Basic Configuration

Typically, the UTM is installed as a network gateway to function as a combined LAN switch, firewall, and content scan engine to protect the network from all incoming and outgoing malware threats.

The following steps are required to complete the basic and security configuration of your UTM:

- Connect the UTM physically to your network. Connect the cables and restart your network according to the instructions in the installation guide. The installation guide is on the NETGEAR website at: http://downloadcenter.netgear.com.
- 2. Log in to the UTM. After logging in, you are ready to set up and configure your UTM. See Log In to the UTM on page 2.
- 3. Use the Setup Wizard to configure basic connections and security. In this step you connect the UTM to an internet service provider (ISP). See Use the Setup Wizard to Perform the Initial Configuration on page 6.
- 4. Verify the installation. See Verify Correct Installation on page 25.
- 5. Register the UTM. See Register the UTM with NETGEAR on page 25.

Qualified Web Browsers

To configure the UTM, you need Microsoft Internet Explorer 6 or later, Mozilla Firefox 3 or later, or Apple Safari 3 or later. Browsers must have JavaScript, cookies, and SSL enabled.

Log In to the UTM

To connect to the UTM, your computer needs to be configured to obtain an IP address automatically from the UTM through DHCP.

- > To connect and log in to the UTM:
 - 1. Start any of the qualified web browsers, as explained in the previous section, *Qualified Web Browsers*.
 - 2. In the address field, enter https://192.168.1.1. The NETGEAR Configuration Manager Login screen displays in the browser.

NETGEAR PROSECURE	ProSecure Unified Threat Management UTM9S
Login	# NETGEAR Configuration Manager Login
	Username: admin Password / Passcode: •••••• Domain: geardomain • User Portal Login Link
	Login Reset

Figure 1. Login screen

- 3. In the Username field, type **admin** in all lowercase letters.
- 4. In the Password / Passcode field, type **password** in all lowercase letters.

Note: The UTM user name and password are not the same as the user name or password you might use to log in to your Internet connection.

5. Click Login. The web management interface displays, showing the System Status screen.

Note: After 5 minutes of inactivity (the default login time-out), you are automatically logged out.

System Status Ad	tive llears & VDNe	Dachhoard Dia	anostics Logs &	Reports Oua	ranting Email Not	tification
votom Status Notwor	k Status Datail	lad Status VI	AN Status	Ctatictics		
ystem status Networ	k Status Detail		AN Status XDS	Statistics		
Status						(
System CPU	43%	Memory	46.	37% Disk		39.83%
Application Control Status OFF Application Control Mode GLOBAL						
ReadyNas Status OFF Quarantine Status OFF						
Active TCP connection	15 22	Active UDP of	connections 22			
Services	SMTP(ON)	POP3(ON)	IMAP(ON)	HTTP(ON)	HTTPS(OFF)	FTP(ON)
Active Connections	0	0	0	2	0	0
Anti-Virus	ON	ON	ON	ON	OFF	ON
	System Name: Firmware Info	UTM9	9S			
	System Name: Firmware Info	uTM9	əs			
	System Name: Firmware Info Type	rmation: Ver	9S rsion	Last Dov	wnloaded	
	System Name: Firmware Info Type active	UTM UTM UTM UTM UTM UTM UTM UTM	95 rsion .0-112	Last Do 2012-08-	vnloaded 02 22:53:13	
	System Name: Firmware Info Type active secondary	UTM9 Prmation: Ver 3.1 7 3.1	95 rsion .0-112 .0-99	Last Do 2012-08- 2012-07-	wnloaded 02 22:53:13 18 22:48:19	
	System Name: Firmware Info Type active secondary Compone	rmation: Ver 3.1 , 3.1 ent Cur	95 rsion .0-112 .0-99 rrent Version	Last Do 2012-08- 2012-07- Last Up	wnloaded 02 22:53:13 18 22:48:19 fate	
	System Name: Firmware Info Type active secondary Compone Scan engin	ermation: Press	95 rsion .0-112 .0-99 rrent Version 110913.806.0.0	Last Do 2012-08- 2012-07- Last Up 2012-07-	wnloaded 02 22:53:13 18 22:48:19 date 30 10:38:05	
	System Name: Firmware Info Type active secondary Compone Scan engin Pattern file	e UTMS rmation: Ver 3.1 r 3.1 ent Cur ne 201 e 201	PS rsion .0-112 .0-99 rrent Version 110913.806.0.0 1110211111	Last Do 2012-08- 2012-07- Last Up 2012-07- 2012-07-	wnloaded 02 22:53:13 18 22:48:19 date 30 10:38:05 30 10:38:05	
	System Name: Firmware Info Type active secondary Compone Scan engin Pattern file Firewall	ermation: Press	es rsion .0-112 .0-99 rrent Version .10913.806.0.0 .110211111 .3.0.8-28	Last Do 2012-08- 2012-07- Last Up 2012-07- 2012-07- 2012-08-	wnloaded 02 22:53:13 18 22:48:19 date 30 10:38:05 30 10:38:05 02 22:53:13	
	System Name: Firmware Info Type active secondary Compone Scan engin Pattern file Firewall + More	rmation: rmation: Ver 3.1 	95 rsion .0-112 .0-99 rrent Version 110913.806.0.0 .110211111 .3.0.8-28	Last Do 2012-08- 2012-07- Last Up 2012-07- 2012-07- 2012-08-	<pre>wnloaded 02 22:53:13 18 22:48:19 date 30 10:38:05 30 10:38:05 02 22:53:13</pre>	
	System Name: Firmware Info Type active secondary Compone Scan engin Pattern file Firewall + More License Expira Email Prot	rmation: Ver 3.1 3.1	PS rsion .0-112 .0-99 rrent Version 110913.806.0.0 .110211111 .3.0.8-28	Last Do 2012-08- 2012-07- Last Up 2012-07- 2012-07- 2012-08- 2015-05-	<pre>wnloaded 02 22:53:13 18 22:48:19 date 30 10:38:05 30 10:38:05 02 22:53:13</pre>	
	System Name: Firmware Info Type active secondary Compone Scan engin Pattern file Firewall + More License Expira Email Prot		95 rsion .0-112 .0-99 rrent Version 110913.806.0.0 1110211111 .3.0.8-28	Last Do 2012-08- 2012-07- Last Up 2012-07- 2012-07- 2012-08- 2015-06- 2015-06-	<pre>wnloaded 02 22:53:13 18 22:48:19 date 30 10:38:05 30 10:38:05 02 22:53:13 04 04</pre>	
	System Name: Firmware Info Type active secondary Compone Scan engin Pattern file Firewall + More License Expira Email Prot Web Prote Support &	UTMS rmation: Ver 3.1 me 201 a 201 a 201 b 02_ ation Date: ation action Ation	PS rsion .0-112 .0-99 rrent Version 110913.806.0.0 .110211111 .3.0.8-28	Last Dov 2012-08- 2012-07- 2012-07- 2012-07- 2012-08- 2015-06- 2015-06- 2015-06-	wnloaded 02 22:53:13 18 22:48:19 Jate 30 10:38:05 30 10:38:05 02 22:53:13 04 04	
	System Name: Firmware Info Type active secondary Compone Scan engin Pattern file Firewall + More License Expira Email Prot Web Prote Support & Application	rmation: Ver 3.1 3.1 a.1 a.1 a.1 a.1 a.1 a.1 a.1 a	PS rsion .0-112 .0-99 rrent Version .10913.806.0.0 .110211111 .3.0.8-28	Last Do 2012-08- 2012-07- 2012-07- 2012-07- 2012-08- 2015-06- 2015-06- 2015-06-	wnloaded 02 22:53:13 18 22:48:19 date 30 10:38:05 30 10:38:05 02 22:53:13 04 04 04	

Figure 2. System Status Screen

Use the Setup Wizard to Perform the Basic Configuration

The Setup Wizard facilitates the basic configuration of the UTM by taking you through 10 screens, the last of which allows you to save the configuration. To perform the initial WAN setup manually, see the reference manual.

> To start the Setup Wizard:

1. Select **Wizards** from the main navigation menu. The Welcome to the Netgear Configuration Wizard screen displays:

Network Config Network Security Application Security VPN Users Administration Monitoring Support Wir	ards
Welcome to the NETGEAR Configuration Wizard (0
O IPSec VPN Wizard	
○ SSL ¥PN Wizard	
Next	

- 2. Select the Setup Wizard radio button.
- 3. Click Next. The first Setup Wizard screen displays.

The following sections explain the 9 configuration screens of the Setup Wizard. On the 10th screen, you can save your configuration.

The tables in the following sections explain the buttons and fields of the Setup Wizard screens.

4

Setup Wizard Step 1 of 10: LAN Settings

Setup Wizard step 1 of 10 :LAN S	ettings			
₩ LAN TCP/IP Setup				0
IP Address:19	2.168.1.1	s	Subnet Mask: 255	.255 .255 .0
# DHCP				()
🔿 Disab	le DHCP Server			
⊙ Enab	e DHCP Server	~	Enable LDAP in	formation
Domain Name: netg	ear.com	LDAP Server:		
Starting IP Address: 192	.168.1.2	Search Base:		
Ending IP Address: 192	.168.1.100	port:	0 (enter	0 for default port)
Primary DNS Server:]			
Secondary DNS Server:]			
WINS Server:				
Lease Time: 24	Hours			
Орнср	Relay			
Relay Gateway:				J
III DNS Proxy				0
Enat	le DNS Proxy:			
Inter ¥LAN Routing				0
Enat	le Inter VLAN Routing:			
Ba	ck Ne	xt	Cancel	

Figure 3. LAN Settings screen

Enter the settings as explained in the following table and click **Next**.

Note: In this first step, you are configuring the LAN settings for the UTM's default VLAN. For more information about VLANs, see the reference manual.

Setting	Description					
LAN TCP/IP Setup						
IP Address	Enter the IP address of the UTM's default VLAN (the factory default address is 192.168.1.1).					
	 Note: Always make sure that the LAN port IP address and DMZ port IP address are different subnets. Note: If you change the LAN IP address of the UTM's default VLAN while connected through the browser, you are disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address from 192.168.1.1 to 10.0.0.1, you now need to enter https://10.0.0.1 in you browser to reconnect to the web management interface. 					
Subnet Mask	Enter the IP subn IP address. The l address that you as the subnet ma	et mask. The subnet mask specifies the network number portion of an JTM automatically calculates the subnet mask based on the IP assign. Unless you are implementing subnetting, use 255.255.255.0 sk (computed by the UTM).				
DHCP	•					
Disable DHCP Server	If another device on your network is the DHCP server for the default VLAN, or if you will configure the network settings of all of your computers manually, select the Disable DHCP Server radio button to disable the DHCP server. By default, this radio button is not selected, and the DHCP server is enabled.					
Enable DHCP Server	Select the Enable Dynamic Host Co for all computers	Select the Enable DHCP Server radio button to enable the UTM to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration or all computers connected to the default VLAN. Enter the following settings.				
	Domain Name	This setting is optional. Enter the domain name of the UTM.				
	Starting IP Address	Enter the starting IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the ending IP address. The IP address 192.168.1.2 is the default starting address.				
	Ending IP Address	Enter the ending IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address.				
		Note: The starting and ending DHCP IP addresses should be in the same network as the LAN TCP/IP address of the UTM (that is, the IP address in the LAN TCP/IP Setup section as described earlier in this table).				
	Primary DNS Server	This setting is optional. If an IP address is specified, the UTM provides this address as the primary DNS server IP address. If no address is specified, the UTM provides its own LAN IP address as the primary DNS server IP address.				

 Table 1. Setup Wizard Step 1: LAN Settings screen settings

Setting	Description				
	Secondary DNS Server	This setting is optional. If an IP address is specified, the UTM provides this address as the secondary DNS server IP address.			
	WINS Server	This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.			
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.			
DHCP Relay	Select the DHCP DHCP server som	Relay radio button to use the UTM as a DHCP relay agent for a newhere else on your network. Enter the following setting:			
	Relay Gateway	The IP address of the DHCP server for which the UTM serves as a relay.			
Enable LDAP information	Select the Enable Lightweight Direct settings.	E LDAP information check box to enable the DHCP server to provide tory Access Protocol (LDAP) server information. Enter the following			
	Note: The LDAP settings that you specify as part of the VLAN profile are used only for SSL VPN and UTM authentication, but not for web and email security.				
	LDAP Server	The IP address or name of the LDAP server.			
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begins. You can specify multiple search objects, separated by commas. The search objects include: • CN (for common name) • OU (for organizational unit) • O (for organizational unit) • C (for country) • DC (for domain) For example, to search the Netgear net domain for all last names of			
		Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net			
	Port	The port number for the LDAP server. The default setting is 0 (zero).			
DNS Proxy					
Enable DNS Proxy	This setting is opt to provide a LAN selected by defau	tional. Select the Enable DNS Proxy radio button to enable the UTM IP address for DNS address name resolution. This radio button is IIt.			
	Note: When the addresses of the	DNS Proxy option is disabled, all DHCP clients receive the DNS IP SP but without the DNS proxy IP address.			

 Table 1. Setup Wizard Step 1: LAN Settings screen settings (continued)

Setting	Description
Inter VLAN Routing	
Enable Inter VLAN Routing	This setting is optional. To ensure that traffic is routed only to VLANs for which inter-VLAN routing is enabled, select the Enable Inter VLAN Routing check box. This setting is disabled by default. When the Enable Inter VLAN Routing check box is not selected, traffic from this VLAN is not routed to other VLANs and traffic from other VLANs is not routed to this VLAN.

Table 1. Setup Wizard Step 1: LAN Settings screen settings (continued)

Setup Wizard Step 2 of 10: WAN Settings



Figure 4. WAN Settings screen

Enter the settings as explained in the following table and click **Next**.

Note: Instead of manually entering the settings, you can also click the **Auto Detect** action button at the bottom of the screen. The autodetect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

Table 2.	Setup Wizard	Step 2:	WAN Settings	screen settings
----------	--------------	---------	--------------	-----------------

Setting	Description				
ISP Login					
Does your Internet connection require a login?	If you need to enter login information every time you connect to the Internet your ISP, select the Yes radio button. Otherwise, select the No radio button the default setting, and skip the ISP Type section. If you select the Yes radio enter the following settings.				
	Login	The login name that your ISP has assigned to you.			
	Password	The password that your ISP has assigned to you.			
ISP Type					
What type of ISP connection do you use?	If your connection is PPI button. Based on the con are highlighted. If your Is radio button and skip this settings.	PoE or PPTP, then you need to log in. Select the Yes radio nnection that you select, the text fields that require data entry SP has not assigned any login information, then select the No s section. If you select the Yes radio button, enter the following			
Austria (PPTP)	If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this radio button and enter the following settings:				
	Account Name	The account name is also known as the host name or system name. Enter the valid account name for the PPTP connection (usually your email ID assigned by your ISP). Some ISPs require you to enter your full email address here.			
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You can leave this field blank.			
	Idle Timeout	Select the Keep Connected radio button to keep the connection always on. To log out after the connection is idle for a period:			
		1. Select the Idle Timeout radio button.			
		 In the time-out field, enter the number of minutes to wait before disconnecting. 			
		This is useful if your ISP charges you based on the time that you are logged in.			
	My IP Address	The IP address assigned by the ISP to make the connection with the ISP server.			
	Server IP Address	The IP address of the PPTP server.			

Setting	Description				
Other (PPPoE)	If you have installed login software such as WinPoET or Enternet, then your connection type is PPPoE. Select this radio button and enter the following settings:				
	Account Name	The valid account name for the PPPoE connection.			
	Domain Name	The name of your ISP's domain or your domain name if your ISP has assigned one. You can leave this field blank.			
	Idle Timeout	Select the Keep Connected radio button to keep the connection always on. To log out after the connection is idle for a period:			
		1. Select the Idle Timeout radio button.			
		2. In the time-out field, enter the number of minutes to wait before disconnecting.			
		This is useful if your ISP charges you based on the period that you are logged in.			
		Note: When you use a PPPoE connection and select the Idle Timeout radio button, you cannot configure load balancing. To use load balancing on a PPPoE connection, select the Keep Connected radio button.			
	Connection Reset	Select the Connection Reset check box to specify a time when the PPPoE WAN connection is reset. The connection is disconnected momentarily and then reestablished. Then, specify the disconnect time and delay.			
	Disconnect Time	Specify the hour and minutes when the connection should be disconnected.			
	Delay	Specify the period in seconds after which the connection should be reestablished.			
Internet (IP) Address Click the Current IP Ac	Idress link to see the curr	ently assigned IP address.			
Get Dynamically from ISP	If your ISP has not assigned you a static IP address, select the Get dynamically from ISP radio button. The ISP automatically assigns an IP address to the UTM using DHCP network protocol.				
	Client Identifier	Select the Client Identifier check box if your ISP requires the client identifier information to assign an IP address using DHCP			

Table 2.	Setup	Wizard	Step 2:	WAN	Settings	screen	settings	(continued	I)
----------	-------	--------	---------	-----	----------	--------	----------	------------	----

UTM Basic Configuration

Vendor Class Identifier

Select the **Vendor Class Identifier** check box if your ISP requires the vendor class identifier information to assign an IP address using DHCP.

Setting	Description			
Use Static IP Address	If your ISP has assigned you a fixed (static or permanent) IP address, select the Use Static IP Address radio button and enter the following settings.			
	IP Address The static IP address assigned to you. This address the UTM to your ISP.			
	Subnet Mask	The subnet mask, which is usually provided by your ISP.		
	Gateway IP Address	The IP address of the ISP's gateway, which is usually provided by your ISP.		
Domain Name Server	(DNS) Servers			
Get Automatically from ISP	If your ISP has not assigned any Domain Name Servers (DNS) addresses, select the Get Automatically from ISP radio button.			
Use These DNS Servers	If your ISP has assigned DNS addresses to you, select the Use These DNS Servers radio button. Make sure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries might cause connectivity issues.			
	Primary DNS Server The IP address of the primary DNS server.			
	Secondary DNS Serve The IP address of the secondary DNS server.			

 Table 2. Setup Wizard Step 2: WAN Settings screen settings (continued)

Setup Wizard Step 3 of 10: System Date and Time

Setup Wizard Step 3 of 10 :System Date and Time	
Set Time, Date and NTP Servers	()
Date / Time: (GMT) Greenwich Mean Time : Edinburgh, London 🛛 💌	
Automatically Adjust for Daylight Savings Time	
 Use Default NTP Servers 	
O Use Custom NTP Servers	
Server 1 Name / IP Address: time-g.netgear.com	
Server 2 Name / IP Address: time-h.netgear.com	
Current Time: Mon Apr 13 16:53:12 GMT+0000 2012	
Back Next Cancel	

Figure 5. System Date and Time screen

Enter the settings as explained in the following table and click **Next** to go to the following screen.

Setting	Description					
Set Time, Date, and NT	P Servers					
Date/Time	From the drop-down list, select the local time zone in which the UTM operates. The correct time zone is required for scheduling to work correctly. The UTM includes a real-time clock (RTC), which it uses for scheduling.					
Automatically Adjust for Daylight Savings Time	If daylight savings tin for Daylight Saving	If daylight savings time is supported in your region, select the Automatically Adjust for Daylight Savings Time check box.				
NTP Server (default or custom)	 r Select either the Use Default NTP servers or Use Custom NTP Servers radio buttone use Default NTP Servers. The UTM's RTC is updated regularly by contacting default NETGEAR NTP server on the Internet. Use Custom NTP Servers. The UTM's RTC is updated regularly by contacting of the two NTP servers (primary and backup), both of which you need to specify the fields that become available with this selection. Note: If you select this option but leave either the Server 1 or Server 2 field blank, the fields are set to the default NETGEAR NTP servers is available at the function of the two functions. 					
	Server 1 Name / IP Enter the IP address or host name of the primary NTP server. Address					
	Server 2 Name / IP Address	Enter the IP address or host name of the backup NTP server.				

 Table 3. Setup Wizard Step 3: System Date and Time screen settings

Setup Wizard Step 4 of 10: Services

s	etup Wizard S	Step 4 of 10 :Ser	vices					
				~				2
3	Email E				4	₩ Web	_	()
	Enable	Service	Ports to Scan			Enable	Service	Ports to Scan
		SMTP	25			Image: A start of the start	HTTP	80
	Image: A start of the start	POP3	110				HTTPS	443
		IMAP	143			v	FTP	21
			Back	N e	R	t 👘	Cancel	

Figure 6. Services screen

Table 4.	Setup	Wizard	Step 4:	Services	screen	settings
----------	-------	--------	---------	----------	--------	----------

Setting	Description			
Email				
SMTP	SMTP scanning is enabled by default on standard service port 25.	To disable any of these services, clear		
POP3	POP3 scanning is enabled by default on standard service port 110.	the corresponding check box. You can change the standard service port or add another port in the corresponding		
IMAP	IMAP scanning is enabled by default on standard service port 143.	Ports to Scan field.		
Web				
HTTP	HTTP scanning is enabled by default on standard service port 80.	To disable HTTP scanning, clear the corresponding check box. You can change the standard service port or add another port in the corresponding Ports to Scan field.		
HTTPS	HTTPS scanning is disabled by default.	To enable HTTPS scanning, select the corresponding check box. You can change the standard service port (443) or add another port in the corresponding Ports to Scan field.		
FTP	FTP scanning is enabled by default on standard service port 21.	To disable FTP scanning, clear the corresponding check box. You cannot change the standard service port in the corresponding Ports to Scan field.		

Setup Wizard Step 5 of 10: Email Security

Setup Wi	izard Step 5 of 10 :Em	ail Security			
# Action	n				()
	Anti-Virus	Service	Action		
		SMTP	Block infected email	•	
		POP3	Delete attachment	-	
		IMAP	Delete attachment	•	
🕮 Scan	Scan Exceptions				
Sk	cip ▼ if the file or mess	age is larger than 2048	KB(Maximum: 10240 KB)		
		Back Ne	xt Cancel		

Figure 7. Email Security screen

Enter the settings as explained in the following table and click **Next** to go to the following screen.

Table 5.	Setup	Wizard	Step	5:	Email	Security	/ screen	settings
							,	

Setting	Description
Action	
SMTP	From the SMTP drop-down list, select one of the following actions to be taken when an infected email is detected:
	• Block infected email. This is the default setting. The email is blocked, and a log entry is created.
	• Delete attachment . The email is not blocked, but the attachment is deleted, and a log entry is created.
	 Log only. Only a log entry is created. The email is not blocked, and the attachment is not deleted.
	 Quarantine attachment. The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created.
	 Quarantine infected email. The email is quarantined on a ReadyNAS, and a log entry is created.
POP3	From the POP3 drop-down list, select one of the following actions to be taken when an infected email is detected:
	• Delete attachment . This is the default setting. The email is not blocked, but the attachment is deleted, and a log entry is created.
	• Log only. Only a log entry is created. The email is not blocked, and the attachment is not deleted.
	• Quarantine attachment. The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created.

Setting	Description
IMAP	From the IMAP drop-down list, select one of the following actions to be taken when an infected email is detected:
	• Delete attachment . This is the default setting. The email is not blocked, but the attachment is deleted, and a log entry is created.
	• Log only. Only a log entry is created. The email is not blocked, and the attachment is not deleted.
	• Quarantine attachment. The email is not blocked, but the attachment is quarantined on a ReadyNAS, and a log entry is created.
Scan Exceptions	

Table 5. Setup Wizard Step 5: Email Security screen settings (continued)

The default maximum size of the file or message that is scanned is 2048 KB, but you can define a maximum size of up to 10240 KB. However, setting the maximum size to a high value might affect the UTM's performance. From the drop-down list, select one of the following actions to be taken when the file or message exceeds the maximum size:

• Skip. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. · Block. The file is blocked and does not reach the end user.

Setup Wizard Step 6 of 10: Web Security



Figure 8. Web Security screen

Enter the settings as explained in the following table and click **Next** to go to the following screen.

Setting	Description
Action	
НТТР	From the HTTP drop-down list, select one of the following actions to be taken when an infected web file or object is detected:
	• Delete file . This is the default setting. The web file or object is deleted, and a log entry is created.
	• Log only. Only a log entry is created. The web file or object is not deleted.
	• Quarantine file. The web file or object is quarantined, and a log entry is created
	Select the Streaming check box to enable streaming of partially downloaded and scanned HTTP file parts to the user. This method allows the user to experience more transparent web downloading. Streaming is enabled by default.
HTTPS	From the HTTPS drop-down list, select one of the following actions to be taken when an infected web file or object is detected:
	• Delete file . This is the default setting. The web file or object is deleted, and a log entry is created.
	• Log only. Only a log entry is created. The web file or object is not deleted.
	• Quarantine file. The web file or object is quarantined, and a log entry is created.
	Select the Streaming check box to enable streaming of partially downloaded and scanned HTTPS file parts to the user. This method allows the user to experience more transparent web downloading. Streaming is enabled by default.
FTP	From the FTP drop-down list, select one of the following actions to be taken when an infected web file or object is detected:
	• Delete file . This is the default setting. The FTP file or object is deleted, and a log entry is created.
	• Log only. Only a log entry is created. The FTP file or object is not deleted.
	• Quarantine file. The FTP file or object is quarantined, and a log entry is created.
Scan Exceptions	

Table 6. Setup Wizard Step 6: Web Security screen settings

The default maximum size of the file or object that is scanned is 2048 KB, but you can define a maximum size of up to 10240 KB. However, setting the maximum size to a high value might affect the UTM's performance. From the drop-down list, select one of the following actions to be taken when the file or message exceeds the maximum size:

• Skip. The file is not scanned but skipped, leaving the end user vulnerable. This is the default setting. • Block. The file is blocked and does reach the end user.

Setup Wizard Step 7 of 10: Web Categories to Be Blocked

Setup Wizard Step 7 of 10 :Web Categorie	s to be blocked	
≅ Blocked Web Categories		0
Enable Blocking	Allow All	Block All Set to Defaults
Commerce		
Advertisements & Pop-Ups	Business	Banking/Finance
Real Estate		
Drugs and Violence		
Alcohol & Tabacco	📕 🗹 Hate & Intolerance	Illegal Drugs
Tasteless	📕 🗹 Violence	📕 🗹 Weapons
Education		
Education	📕 🗌 Health & Medicine	School Cheating
Gaming		
📕 🗹 Gambling	Games	
Inactive Sites		
Network Errors	📕 🗖 Parked Domain	
Internet Communication and Sea	arch	
📕 🗹 Anonymizers	Chat	Forums
General	Image/Photo Sharing	Instant Messaging
Job Search	Peer-to-Peer	Private IP Addresses
Streaming Media & Downloads	Search Engines & Portals	Translators
Webmail		
Leisure and News		- 0-
Arts	Dating & Personals	
Fashion & Beauty	Greeting Cards	Leisure & Recreation
News	Non-Profits	Personal Sites
Restaurants & Dining	Social Networking	Sports
Botnetr	Criminal Activity	Hacking
Illegal Software		Phishing & Fraud
Spam Sites	Virus Infected/Compromise	d
Politics and Religion		70
Cults	Government	Politics
E Religion		
Sexual Content		
Child Abuse Images	Nudity	Pornography/Sexually Explicit
Sex Education		
Technology		
📕 🗌 Computers & Technology	Download Sites	Information Security
UnCategorized		
📕 🗹 UnCategorized		
Note:		
Blocked by Default		
Blocked Categories Scheduled Days:		(7)
Do you want this schedule to be	active on	Monday
all days or specific days	7 Tuesday	Wednesday
All Days O Spec	cific Days	Friday
	J Saturday	
Blocked Categories Time of Day:		0
Do you want this schedule to b	e active	12 Hour 00 Micute AM
all day or at specific times durin	g the day?	12 Hour 00 Minute DM
All Day O Spe	cific Times	
Back	Next	ancel

Figure 9. Blocked Web Categories screen

Table 7. Setup Wizard Step 7: Web Categories to be blocked screen settings

Setting	Description						
Blocked Web Categories	Blocked Web Categories						
Select the Enable Blocking selected.)	check box to enable blocking of web categories. (By default, this check box is						
Select the check boxes of an section in the following way:	ny web categories that you want to block. Use the action buttons at the top of the						
· Allow All. All web catego	pries are allowed.						
· Block All. All web catego	pries are blocked.						
• Set to Defaults. Blocking reference manual for infor- preceded by a green squa blocked by default.	and allowing of web categories are returned to their default settings. See the mation about the web categories that are blocked by default. Categories that are are are allowed by default; categories that are preceded by a pink square are						
Blocked Categories Sched	luled Days						
Make one of the following se	elections:						
Select the All Days radio	button to enable content filtering to be active all days of the week.						
• Select the Specific Days radio button to enable content filtering to be active on the days that are specified by the check boxes.							
Blocked Categories Time of Day							
Make one of the following se	Make one of the following selections:						
· Select the All Day radio button to enable content filtering to be active all 24 hours of each selected day							

Select the All Day radio button to enable content filtering to be active all 24 hours of each selected day.
Select the Specific Times radio button to enable content filtering to be active during the time that is specified

by the Start Time and End Time fields for each day that content filtering is active.

Setup Wizard Step 8 of 10: Email Notification

dministrator Email Notifi	cation Settings	
Show as mail sender: SMTP server:	UTM_Notifications@netgear.com mail.yourdomain.com :25	
User name: Password:		
Send notifications to:	admin@yourdomain.com	

Figure 10. Email Notification screen

Setting	Description	
Administrator Email Notif	fication Settings	
Show as mail sender	A descriptive name enter UTM_Notifica	of the sender for email identification purposes. For example, tions@netgear.com.
SMTP server	The IP address and outgoing email SM ⁻ Note: If you leave	I port number or Internet name and port number of your ISP's IP server. The default port number is 25. this field blank, the UTM cannot send email notifications.
This server requires authentication	If the SMTP server authentication che	requires authentication, select the This server requires eck box, and enter the user name and password.
	User name	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.
Send notifications to	The email address email address of the	to which the notifications should be sent. Typically, this is the e administrator.

 Table 8. Setup Wizard Step 8: Email Notification screen settings

Setup Wizard Step 9 of 10: Signatures & Engine

opuate settings	(
Update : Update From:	Scan engine and Signatures • Default update server • Server address:
Update Frequency	(
⊖ Weekly [○ Daily [⊙ Every [Sunday 23 ¥ : 00 ¥ (hh:mm) 01 ¥ : 00 ¥ (hh:mm) 1 hour ¥
HTTPS Proxy Settings	(
Enable Proxy serv This serve	er: : r requires authentication:

Figure 11. Signatures & Engine screen

Table 9.	Setup Wizard	d Step 9: Signature	es & Engine screen settings	\$
----------	--------------	---------------------	-----------------------------	----

Setting	Description
Update Settings	
Update	 From the drop-down list, select one of the following options: Never. The pattern and firmware files are never automatically updated. Scan engine and Signatures. The pattern and firmware files are automatically updated according to the settings in the Update Frequency section of the screen (see explanations later in this table).
Update From	 Set the update source server by selecting one of the following radio buttons: Default update server. Files are updated from the default NETGEAR update server. Server address. Files are updated from the server that you specify. Enter the IP address or host name of the update server in the Server address field.

Update Frequency

Specify the frequency with which the UTM checks for file updates:

- Weekly. From the drop-down lists, select the weekday, hour, and minutes that the updates occur.
- Daily. From the drop-down lists, select the hour and minutes that the updates occur.

• Every. From the drop-down list, select the frequency with which the updates occur. The range is from 15 minutes to 12 hours.

HTTPS Proxy Settings

Enable	If computers on the Enable check settings.	the network connect to the Internet through a proxy server, select of box to specify and enable a proxy server. Enter the following
	Proxy server	The IP address and port number of the proxy server.
	User name	The user name for proxy server authentication.
	Password	The password for proxy server authentication.

Setup Wizard Step 10 of 10: Saving the Configuration

Setup Wizard Step 10 o	of 10			
	The s	ystem will be rest	arted	
	Note: The	system IP address is :	192.168.1.1	
	Back	Apply	Cancel	

Figure 12. Save the configuration screen

Click **Apply** to save your settings and automatically restart the system.

Verify Correct Installation

Test the UTM before deploying it in a production environment. These quick tests are designed to ensure that your UTM is functioning correctly.

Test Connectivity

> Verify that network traffic can pass through the UTM:

- 1. Ping an Internet URL.
- 2. Ping the IP address of a device on either side of the UTM.

Test HTTP Scanning

> Verify that the UTM scans HTTP traffic correctly:

- 1. Log in to the UTM web management interface, and then verify that HTTP scanning is enabled. For information about how to enable HTTP scanning, see the reference manual.
- 2. If client computers have direct access to the Internet through your LAN, try to download the eicar.com test file from *http://www.eicar.org/download/eicar.com*.

The eicar.com test file is a *legitimate* denial of service (DoS) attack and is safe to use because it is not a malware threat and does not include any fragments of malware code. The test file is provided by EICAR, an organization that unites efforts against computer crime, fraud, and misuse of computers or networks.

3. Check the downloaded eicar.com test file, and note the attached malware information file.

Register the UTM with NETGEAR

To receive threat management component updates and technical support, you need to register your UTM with NETGEAR. The UTM is bundled with four 30-day trial licenses:

- Web protection
- Email protection
- Support and maintenance
- Application control and IPS

The service license keys are provided with the product package (see the reference manual). For electronic licensing, you do not need the service license keys (see *Electronic Licensing* on page 27).



IMPORTANT:

Activating the service licenses initiates their terms of use. Activate the licenses *only* when you are ready to start using this unit. If your unit has never been registered before, you can use the 30-day trial period for all four types of licenses to perform the initial testing and configuration. To use the trial period, do *not* click Register in *Step 4* of the following procedure click Trial instead.

- > If your UTM is connected to the Internet, you can activate the service licenses:
 - 1. Select **Support > Registration**. The Registration screen displays:

n Online Sup	oort :: Malware Analysis :: Registratio	n 💠 Knowledge Base 🙃 Documenta	ation ::
stration			
nline Registration			
Registration Key:			
			Free too Marco Date
NG281C-AE02-D425-D2B	E-421B-D132-5E12-E12E-C34B	License Lype	2013-04-06
NG281C-AE02-D425-D2B	E-A21B-D132-5F12-F12E-C3AB	Email Protection	2013-04-06
NG281C-AE02-D425-D2B	E-A21B-D132-5F12-F12E-C3AB	Support & Maintenance	2013-04-06
NG281C-AE02-D425-D2B	E-A21B-D132-5F12-F12E-C3AB	Application Control & IPS	2013-04-06
Customer Information			
customer information			
Company Name:			
First Name:			
Last Name:			
Email Address:			
Email Address.			
Fax Number:			
Phone Number:			
Address:			
Country:		~	
VAR Information			
Company Name:			
First Name:			
Last Name:			
Email Address:			
Fax Number:			
Phone Number:			
Address:			
Country:		*	

- 2. Enter the license key in the Registration Key field.
- 3. Fill out the customer and value-added reseller (VAR) fields.

4. Click **Register**. The UTM activates the license and registers the unit with the registration and update server.



WARNING:

To activate the 30-day trial period for a license, do *not* click Register but click Trial instead. For more information, see the Important information at the beginning of this section.

5. Repeat *Step 2* and *Step 4* for additional license keys.

Note: The 30-day trial licenses are revoked once you activate the purchased service license keys. The purchased service license keys offer 1 year or 3 years of service.

> To change customer or VAR information after you have registered the UTM:

- 1. Make the changes on the Registration screen.
- 2. Click **Update Info**. The new data is saved by the registration and update server.

> To retrieve and display the registered information:

Click **Retrieve Info**. The registered data is retrieved from the registration and update server.

Electronic Licensing

If you have purchased the UTM with a 1- or 3-year license, you can use the electronic licensing option. When the UTM is connected to the Internet, you need to enter only your customer information and optional value-added reseller (VAR) information on the Register screen but do not need to enter the license numbers. When you click Register, the UTM automatically downloads and activates the license keys because the serial number of the UTM is linked to the license.

If you have purchased licenses from a VAR (either directly or over the web) *after* purchase of the UTM, the VAR should provide you the license keys. To register and activate the license keys, follow the registration procedure explained in the previous section.

Automatic Retrieval of Licenses after a Factory Default Reset

When you reset the UTM to the original factory default settings after you have entered the license keys to activate the UTM, the license keys are erased. The license keys and the different types of licenses that are available for the UTM are no longer displayed on the Registration screen. However, after you have reconfigured the UTM to connect to the Internet and to the NETGEAR registration server, the UTM retrieves and restores all registration information based on its MAC address and hardware serial number. You do not need to reenter the license keys and reactivate the UTM.

If you have been directed to use a nondefault update server, you first need to enter the update server address in the Server address field on the Signatures & Engine screen and click **Apply**.

What to Do Next

You have connected your UTM to your network. The UTM is now ready to scan the protocols and services that you specified and perform automatic updates based on the update source and frequency that you specified.

If you need to change the settings or view reports or logs, log in to the UTM web management interface. Use the default IP address or the IP address that you assigned to the UTM in *Setup Wizard Step 1 of 10: LAN Settings* on page 7.

To configure these additional features see the reference manual:

- Configure WAN mode (required to use multiple WAN ports)
- Configure authentication domains, groups, and users
- Manage digital certificates for VPN connections
- Configure IPSec VPN clients and gateways
- Configure SSL VPN clients