## Contents

### Introduction 13
- Before you begin ................................................. 13
- How this guide is organized .................................. 13

### Introduction to authentication 15
- What is authentication? ........................................ 15
- Methods of authentication ..................................... 15
  - Local password authentication ............................. 16
  - Server-based password authentication .................... 16
    - Dynamic profiles .......................................... 16
    - Single Sign On authentication using FSSO ............ 16
  - Certificate-based authentication .......................... 17
    - Certificate authorities ................................. 17
    - Certificates for users .................................. 17
  - Two-factor authentication ................................ 18
- Types of authentication ......................................... 18
  - Firewall authentication (identity-based policies) .... 18
    - FSSO ..................................................... 19
    - NTLM .................................................... 19
    - Certificates ............................................ 19
    - Dynamic profile ........................................ 19
    - FortiGuard Web Filter override authentication ....... 19
  - VPN authentication .......................................... 20
    - Authenticating IPsec VPN peers (devices) .......... 20
    - Authenticating IPsec VPN users ....................... 20
    - Authenticating SSL VPN users ......................... 21
    - Authenticating PPTP and L2TP VPN users ............ 21
- User’s view of authentication .................................. 21
  - Web-based user authentication ............................ 21
  - VPN client-based authentication ........................... 22
- FortiGate administrator’s view of authentication ......... 22

### Authentication and User in the web-based manager 23
- User ............................................................. 23
  - Local user accounts ....................................... 23
    - Local user accounts configuration settings .......... 24
  - IM users .................................................... 26
    - IM users configuration settings ....................... 26
  - Authentication settings .................................. 27
## Contents

User groups .................................................. 28
  User Group .................................................. 29
    User Group configuration settings ......................... 29
Firewall user groups ........................................ 31
Fortinet Single Sign-On (FSSO) user groups .................. 32
SSL VPN user groups ......................................... 32
  **Dynamically assigning VPN client IP addresses from a user group** .................................... 33

Remote ...................................................... 33
  Administrators ............................................... 33
  RADIUS ...................................................... 34
    RADIUS configuration settings .......................... 34
  LDAP .......................................................... 36
    LDAP configuration settings ............................. 36
    Using Query ............................................... 38
  TACACS+ ..................................................... 39
    TACAS+ configuration settings ............................ 39

FortiToken .................................................. 40
  FortiToken configuration settings ......................... 40

Fortinet Single Sign On Agent (FSSO) ........................ 42
  Fortinet Single Sign-on Agent configuration settings .... 43

PKI ........................................................... 45
  PKI configuration settings ................................ 45
  Peer users and peer groups ................................ 46

Monitor ...................................................... 47
  Firewall monitor list ....................................... 47
  IM user monitor list ....................................... 48
  The Banned User list ..................................... 49

**Authentication servers** ................................ 51

FortiAuthenticator servers .................................. 51

RADIUS servers .............................................. 51
  Microsoft RADIUS servers ................................ 52
  RADIUS user database .................................... 52
  RADIUS authentication with a FortiGate unit ............... 52
  RADIUS attribute value pairs .............................. 52
  Vendor-specific attributes ................................ 53
  Role Based Access Control ................................ 54
  Configuring the FortiGate unit to use a RADIUS server .. 54
    Troubleshooting RADIUS ................................ 56

LDAP servers ................................................ 56
  Components and topology .................................. 57
    Binding ..................................................... 57
    Supported versions ....................................... 57
  LDAP directory organization ................................. 57
Contents

IPsec VPN access ........................................... 87
Configuring a firewall user group ......................... 87
Multiple group enforcement support ....................... 88
User group timeouts ....................................... 88
FSSO user groups ........................................... 90
Configuring Peer user groups ............................ 90
Viewing, editing and deleting user groups.................. 90
   Editing a user group ................................... 91
   Deleting a user group ................................... 91

Configuring authenticated access .......................... 93
   Authentication timeout .................................. 93
   Security authentication timeout ......................... 93
   SSL VPN authentication timeout ......................... 93
   Password policy ......................................... 94
      Configuring password minimum requirement policy . 94
      Maximum logon attempts and blackout period .......... 95
   Authentication protocols ................................. 96
   Authentication in security policies ..................... 96
      Enabling authentication protocols .................... 97
      Authentication replacement messages ................ 98
   Access to the Internet .................................. 100
   Configuring authentication security policies ........... 100
      Disclaimer ............................................. 101
      Enabling security logging ............................ 102
   Identity-based policy ................................... 103
      Identity-based sub-policies ........................... 104
   FSSO authentication ................................... 104
   NTLM authentication .................................... 105
   Certificate authentication ............................... 106
      Certificate redirect authentication .................... 106
   Dynamic profile ........................................ 107
   Restricting number of concurrent user logons .......... 107
   VPN authentication ..................................... 107
      Configuring authentication of SSL VPN users .......... 108
      Configuring authentication timeout .................... 108
      Configuring authentication of remote IPsec VPN users .... 108
         Configuring XAuth authentication ..................... 109
      Configuring authentication of PPTP VPN users and user groups 110
      Configuring authentication of L2TP VPN users/user groups 111

Certificate-based authentication .......................... 113
   What is a security certificate? .......................... 113
   Certificates overview ................................... 114
   Certificates and protocols .............................. 114
SSL and HTTPS ............................................... 114
Certificate-related protocols ................................. 115
IPsec VPNs and certificates ................................ 115
Certificate types on the FortiGate unit .................... 115
Certificate signing ............................................ 116
Managing X.509 certificates ................................. 116
Generating a certificate signing request .................. 117
Generating certificates with CA software ................. 118
Server certificate ............................................ 118
CA certificate ................................................. 119
PKI certificate ................................................ 119
Obtaining a signed server certificate from an external CA. 119
Installing a CA root certificate and CRL to authenticate remote clients 120
Troubleshooting certificates ................................ 121
Certificate is reported as expired when it is not .......... 121
A secure connection cannot be completed (Certificate cannot be found) 121
Online updates to certificates and CRLs .................. 122
Local certificates .............................................. 122
CA certificates .................................................. 123
Certificate Revocation Lists ................................. 123
Backing up and restoring local certificates ............... 124
Configuring certificate-based authentication .............. 125
Authenticating administrators with security certificates 125
Authenticating SSL VPN users with security certificates 125
Authenticating IPsec VPN users with security certificates 126
Example — Generate a CSR on the FortiGate unit ......... 127
Example — Generate and Import CA certificate with private key pair on OpenSSL 128
Assumptions .................................................... 128
Generating and importing the CA certificate and private key 128
Example — Generate an SSL certificate in OpenSSL ....... 129
Assumptions .................................................... 129
Generating a CA signed SSL certificate .................. 129
Generating a self-signed SSL certificate ................... 130
Import the SSL certificate into FortiOS .................... 130

**FSSO integration with Windows AD or Novell** 133
Introduction to FSSO ........................................ 133
Using FSSO in a Windows AD environment ............... 134
FSSO security ................................................. 134
FSSO Controller agent (CA) ................................ 134
FSSO user logon event monitoring ......................... 135
DC Agent mode ................................................ 135
Polling mode .................................................... 136
NTLM authentication with FSSO ............................. 137
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTLM in a multiple domain environment</td>
<td>138</td>
</tr>
<tr>
<td>Using FSSO in a Novell eDirectory environment</td>
<td>140</td>
</tr>
<tr>
<td>FSSO for Windows AD</td>
<td>140</td>
</tr>
<tr>
<td>FSSO components for Windows AD</td>
<td>140</td>
</tr>
<tr>
<td>FSSO Installation</td>
<td>141</td>
</tr>
<tr>
<td>Standard versus Advanced mode</td>
<td>141</td>
</tr>
<tr>
<td>Installing FSSO for Windows AD</td>
<td>141</td>
</tr>
<tr>
<td>Installing FSSO without using an administrator account</td>
<td>143</td>
</tr>
<tr>
<td>Updating FSSO with Windows AD</td>
<td>144</td>
</tr>
<tr>
<td>Configuring Fortinet Single Sign On with Windows AD</td>
<td>145</td>
</tr>
<tr>
<td>Configuring Windows AD server user groups</td>
<td>145</td>
</tr>
<tr>
<td>Configuring Collector agent settings</td>
<td>146</td>
</tr>
<tr>
<td>Configuring Directory Access settings</td>
<td>149</td>
</tr>
<tr>
<td>BaseDN example</td>
<td>150</td>
</tr>
<tr>
<td>Configuring the Ignore User List</td>
<td>150</td>
</tr>
<tr>
<td>Configuring FortiGate group filters</td>
<td>151</td>
</tr>
<tr>
<td>Configuring FSSO ports</td>
<td>152</td>
</tr>
<tr>
<td>TCP ports for FSSO agent with client computers</td>
<td>152</td>
</tr>
<tr>
<td>Configuring ports on the Collector agent computer</td>
<td>153</td>
</tr>
<tr>
<td>Configuring alternate user IP address tracking</td>
<td>153</td>
</tr>
<tr>
<td>Viewing FSSO component status</td>
<td>153</td>
</tr>
<tr>
<td>Viewing Collector agent status</td>
<td>153</td>
</tr>
<tr>
<td>Viewing DC agent status</td>
<td>154</td>
</tr>
<tr>
<td>Selecting Domain Controllers and working mode for monitoring</td>
<td>154</td>
</tr>
<tr>
<td>FSSO for Novell eDirectory</td>
<td>154</td>
</tr>
<tr>
<td>FSSO components for Novell eDirectory</td>
<td>155</td>
</tr>
<tr>
<td>Installing FSSO for Novell</td>
<td>155</td>
</tr>
<tr>
<td>Configuring Fortinet Single Sign On with Novell networks</td>
<td>155</td>
</tr>
<tr>
<td>Configuring the eDirectory agent</td>
<td>156</td>
</tr>
<tr>
<td>Adding an eDirectory server</td>
<td>157</td>
</tr>
<tr>
<td>Configuring a group filter</td>
<td>157</td>
</tr>
<tr>
<td>Configuring FSSO on FortiGate units</td>
<td>158</td>
</tr>
<tr>
<td>Configuring LDAP server access</td>
<td>158</td>
</tr>
<tr>
<td>Specifying your Collector agents or Novell eDirectory agents</td>
<td>160</td>
</tr>
<tr>
<td>Selecting Windows user groups (LDAP only)</td>
<td>161</td>
</tr>
<tr>
<td>Viewing information imported from the Windows AD server</td>
<td>161</td>
</tr>
<tr>
<td>Creating Fortinet Single Sign-On (FSSO) user groups</td>
<td>162</td>
</tr>
<tr>
<td>Creating security policies</td>
<td>162</td>
</tr>
<tr>
<td>Users belonging to multiple groups</td>
<td>164</td>
</tr>
<tr>
<td>Resolve usernames Using FSSO Agent</td>
<td>165</td>
</tr>
<tr>
<td>Enabling guest access through FSSO security policies</td>
<td>165</td>
</tr>
<tr>
<td>FortiOS FSSO log messages</td>
<td>165</td>
</tr>
<tr>
<td>Enabling authentication event logging</td>
<td>165</td>
</tr>
<tr>
<td>Viewing FSSO log messages</td>
<td>166</td>
</tr>
</tbody>
</table>
Testing FSSO ................................................................. 167
Troubleshooting FSSO .................................................... 168
  General troubleshooting tips for FSSO ......................... 168
  User status “Not Verified” on the Collector agent .......... 169
  After initial configuration, there is no connection to the Collector agent .......... 169
  Collector Agent service freezing and shutting down. ........ 170
  FortiGate performance is slow on a large network with many users ....... 170
  Users from the Windows AD network are not able to access the network .... 171
  Users on a particular computer (IP address) can not access the network .... 171
  Guest users do not have access to network. .................. 171
  Can’t find the DCAgent service ................................. 172
  User logon events not received by FSSO Collector agent. .... 172
  User list from Windows AD is empty. ......................... 172
  Mac OS X users can’t access external resources after waking from sleep mode. 173

Dynamic profiles and end points ........................................ 175
Overview ................................................................... 175
  When to use FSSO or dynamic profiles ......................... 176
  End points .................................................................. 177
  Dynamic profiles and security policies ......................... 177
    Dynamic profile UTM profile groups ......................... 178
    Dynamic security policies ....................................... 178
  Accounting system RADIUS configuration .................... 180
  User context list ..................................................... 180
  Accepting sessions only from dynamic profile users ....... 181
    Dynamic Profile Users Only option ............................ 182
Configuring dynamic profile ........................................... 182
  Make dynamic profiles visible .................................... 183
  RADIUS server configuration for dynamic profiles .......... 183
    Restrictions and requirements ................................ 183
    Profile group name ............................................... 183
    Advanced dynamic profile RADIUS server configuration - CLI 186
    Carrier endpoints .................................................. 187
Configuring dynamic profile-based security policies ............ 189
  Configuration concepts ............................................. 190
    Only allow dynamic profile users .............................. 190
    Only allow dynamic profile users, but traffic shape protocols .......... 190
    Allow multiple dynamic profile groups ..................... 190
    Promote dynamic profile users .................................. 190
    Schedule-based policies ......................................... 191
Configuring end points ................................................ 191
  Configuring end points - CLI ...................................... 191
  Controlling MMS service access based on a user’s end point - FortiCarrier Only 192
    Configuring end point filtering - FortiOS Carrier only .......... 192
    Configuring end point filter lists ............................. 193
User Authentication for FortiOS 4.0 MR3

Contents

Regular expression vs. wildcard match pattern .................................................. 194
Blocking access to the network based on end points - FortiOS Carrier only .... 194
Carrier Endpoint Filter Lists .............................................................................. 195
Extracting carrier end points for notifications - FortiOS Carrier only .......... 197
Configuring MMS address translation - FortiOS Carrier only ......................... 197
Timeout options ................................................................................................ 199
Log settings ....................................................................................................... 200
Carrier end point filters and blocking ............................................................... 201
  Controlling access to MMS services based on a user’s carrier end point.. 202
  Filtering MMS flows from selected carrier end points............................... 202
  Configuring carrier end point filtering ......................................................... 202
Blocking network access for IP addresses based on carrier end points ......... 203
Viewing and defining a carrier end point IP filter list ..................................... 204
Adding additional blocked IP addresses ............................................................ 206
Troubleshooting dynamic profiles ................................................................. 206
  General dynamic profile troubleshooting ...................................................... 206
  Dynamic profile related diag commands ....................................................... 207

Monitoring authenticated users ........................................................................ 209
Monitoring firewall users .................................................................................. 209
Monitoring SSL VPN users .............................................................................. 209
Monitoring IPsec VPN users ............................................................................. 210

Examples and Troubleshooting ........................................................................ 211
Firewall authentication example ......................................................................... 211
  Overview ......................................................................................................... 211
  Creating a locally-authenticated user account ............................................. 212
  Creating a RADIUS-authenticated user account ......................................... 212
  Creating user groups ...................................................................................... 213
    Creating the FSSO user group .................................................................... 213
    Creating the Firewall user group ............................................................... 215
  Defining policy addresses ............................................................................. 215
  Creating security policies .............................................................................. 215
LDAP Dial-in using member-attribute ............................................................... 217
Dynamic Profile example .................................................................................. 219
  Assumptions .................................................................................................. 219
  Topology ........................................................................................................ 219
  General configuration .................................................................................... 220
  Configuring RADIUS .................................................................................... 220
  Configuring FortiGate interfaces .................................................................... 220
  Configuring dynamic profile RADIUS server on FortiGate ......................... 222
  Configuring FortiGate regular and dynamic profile security policies ........... 223
    Schedules, address groups, and services groups ....................................... 223
    Configuring regular security policies ......................................................... 224
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring dynamic profile security policy</td>
<td>225</td>
</tr>
<tr>
<td>Testing</td>
<td>226</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>227</td>
</tr>
<tr>
<td>Index</td>
<td>229</td>
</tr>
</tbody>
</table>
Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This chapter contains the following topics:

- Before you begin
- How this guide is organized

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- Any third-party software or servers have been configured using their documentation.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

Introduction to authentication describes some basic elements and concepts of authentication.

Authentication and User in the web-based manager describes the web-based manager interface of FortiOS, specifically the Authentication and User top level menu items.

Authentication servers describes external authentication servers, where a FortiGate unit fits into the topology, and how to configure a FortiGate unit to work with that type of authentication server.

Dynamic profiles and end points describes how to set up dynamic profiles and carrier end points to identify users that are using RADIUS settings. Some parts are specific to FortiOS Carrier.

Users and user groups describes the different types of user accounts and user groups. Authenticated access to resources is based on user identities and user group membership. Two-factor authentication methods, including FortiToken, provide additional security.

Configuring authenticated access provides detailed procedures for setting up authenticated access in security policies and authenticated access to VPNs.
FSSO integration with Windows AD or Novell describes how to install and configure the Fortinet Single Sign On (FSSO) on Windows AD or Novell network domain controllers and the FortiGate unit. With FSSO, network users have single sign-on access to resources through the FortiGate unit. Earlier versions of FSSO were called FSAE.

Certificate-based authentication describes authentication by means of X.509 certificates.

Monitoring authenticated users describes FortiOS authenticated user monitor screens.

Examples and Troubleshooting provides a configuration example and troubleshooting in which Windows AD and other network users are provided authenticated access to the Internet.
Introduction to authentication

Identifying users and other computers—authentication—is a key part of network security. This section describes some basic elements and concepts of authentication.

The following topics are included in this section:

- What is authentication?
- Methods of authentication
- Types of authentication
- User’s view of authentication
- FortiGate administrator’s view of authentication

What is authentication?

Businesses need to authenticate people who have access to company resources. In the physical world this may be a swipe card to enter the building, or a code to enter a locked door. If a person has this swipe card or code, they have been authenticated as someone allowed in that building or room.

Authentication is the act of confirming the identity of a person or other entity. In the context of a private computer network, the identities of users or host computers must be established to ensure that only authorized parties can access the network. The FortiGate unit enables controlled network access and applies authentication to users of security policies and VPN clients.

Methods of authentication

FortiGate unit authentication is divided into three basic types: password authentication for people, certificate authentication for hosts or endpoints, and two-factor authentication for additional security beyond just passwords. An exception to this is that FortiGate units in an HA cluster and FortiManager units use password authentication.

Password authentication verifies individual user identities, but access to network resources is based on membership in user groups. For example, a security policy can be configured to permit access only to the members of one or more user groups. Any user who attempts to access the network through that policy is then authenticated through a request for their username and password.

Methods of authentication include:

- Local password authentication
- Server-based password authentication
- Certificate-based authentication
- Two-factor authentication
Local password authentication

The simplest authentication is based on user accounts stored locally on the FortiGate unit. For each account, a username and password is stored. The account also has a disable option so that you can suspend the account without deleting it.

Local user accounts work well for a single-FortiGate installation. If your network has multiple FortiGate units that will use the same accounts, the use of an external authentication server can simplify account configuration and maintenance.

You create local user accounts in the web-based manager under User > User. This page is also used to create accounts where an external authentication server stores and verifies the password.

Server-based password authentication

Using external LDAP, RADIUS, or TACACS+ authentication servers is desirable when multiple FortiGate units need to authenticate the same users, or where the FortiGate unit is added to a network that already contains an authentication server.

When you use an external authentication server to authenticate users, the FortiGate unit sends the user’s entered credentials to the external server. The password is encrypted. The server’s response indicates whether the supplied credentials are valid or not.

You must configure the FortiGate unit to access the external authentication servers that you want to use. The configuration includes the parameters that authenticate the FortiGate unit to the authentication server.

You can use external authentication servers in two ways:

- Create user accounts on the FortiGate unit, but instead of storing each user’s password, specify the server used to authenticate that user. As with accounts that store the password locally, you add these users to appropriate user groups.
- Add the authentication server to user groups. Any user who has an account on the server can be authenticated and have the access privileges of the FortiGate user group. Optionally, when an LDAP server is a FortiGate user group member, you can limit access to users who belong to specific groups defined on the LDAP server.

Dynamic profiles

Managed Security Service Providers (MSSPs) and carrier service providers can use the FortiOS dynamic profile configuration to dynamically assign profile groups to customer traffic. Using the dynamic profile, FortiOS can receive RADIUS Start records from service provider accounting systems when customers connect to service provider networks. In real time, FortiOS can extract identifying information and profile group names from these RADIUS Start records and match the identifying information with the customer communication session. FortiOS can then dynamically select and apply the profile group named in the RADIUS Start record to the communication session. Some parts of dynamic profiles and end points are FortiOS Carrier-only features. See “Dynamic profiles and end points” on page 175.

Single Sign On authentication using FSSO

“Single sign on” or “Single user Sign On” means that users logged on to a computer network are authenticated for access to network resources through the FortiGate unit without having to enter their username and password again. Fortinet Single Sign On (FSSO) provides Single Sign On capability for:

- Microsoft Windows networks using either Active Directory or NTLM authentication
- Novell networks, using eDirectory
FSSO monitors user logons and sends the FortiGate unit the username, IP address, and the list of Windows AD user groups to which the user belongs. When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

For detailed information about FSSO, see “FSSO integration with Windows AD or Novell” on page 133.

Certificate-based authentication

An RSA X.509 server certificate is a small file issued by a Certificate Authority (CA) that is installed on a computer or FortiGate unit to authenticate itself to other devices on the network. When one party on a network presents the certificate as authentication, the other party can validate that the certificate was issued by the CA. The identification is therefore as trustworthy as the Certificate Authority (CA) that issued the certificate.

To protect against compromised or misused certificates, CAs can revoke any certificate by adding it to a Certificate Revocation List (CRL). Certificate status can also be checked online using Online Certificate Status Protocol (OCSP).

RSA X.509 certificates are based on public-key cryptography, in which there are two keys: the private key and the public key. Data encrypted with the private key can be decrypted only with the public key and vice versa. As the names suggest, the private key is never revealed to anyone and the public key can be freely distributed. Encryption with the recipient’s public key creates a message that only the intended recipient can read. Encryption with the sender’s private key creates a message whose authenticity is proven because it can be decrypted only with the sender’s public key.

Server certificates contain a signature string encrypted with the CA’s private key. The CA’s public key is contained in a CA root certificate. If the signature string can be decrypted with the CA’s public key, the certificate is genuine.

Certificate authorities

A certificate authority can be:

- an organization, such as VeriSign Inc., that provides certificate services
- a software application, such as Microsoft Certificate Services or OpenSSH

For a company web portal or customer-facing SSL VPN, a third-party certificate service has some advantages. The CA certificates are already included in popular web browsers and customers trust the third-party. On the other hand, third-party services have a cost.

For administrators and for employee VPN users, the local CA based on a software application provides the required security at low cost. You can generate and distribute certificates as needed. If an employee leaves the organization, you can simply revoke their certificate.

Certificates for users

FortiGate unit administrators and SSL VPN users can install certificates in their web browsers to authenticate themselves. If the FortiGate unit uses a CA-issued certificate to authenticate itself to the clients, the browser will also need the appropriate CA certificate.

FortiGate IPsec VPN users can install server and CA certificates according to the instructions for their IPsec VPN client software. The FortiClient Endpoint Security application, for example, can import and store the certificates required by VPN connections.
FortiGate units are also compatible with some Public Key Infrastructure systems. For an example of this type of system, see “RSA ACE (SecurID) servers” on page 66.

**Two-factor authentication**

A user can be required to provide both something they know (their username and password combination) and something they have (certificate or a random token code). Certificates are installed on the user’s computer.

Two-factor authentication is available for PKI users. For more information, see “Certificate” on page 78.

Another type of two-factor authentication is to use a randomly generated token (multi-digit number) along with the username and password combination. One method is a FortiToken — a one-time passcode (OTP) generator that generates a unique code every 60 seconds. Others use email or SMS text messaging to deliver the random token code to the user or administrator.

When one of these methods is configured, the user enters this code at login after the username and password have been verified. The FortiGate unit verifies the token code after as well as the password and username. For more information, see “Two-factor authentication” on page 78.

**Types of authentication**

FortiOS supports two different types of authentication based on your situation and needs.

Security policy authentication, or identity-based policies, is easily applied to all users logging on to a network, or network service. For example, if a group of users on your network such as the accounting department who have access to sensitive data need to access the Internet, it is a good idea to make sure the user is a valid user and not someone trying to send company secrets to the Internet. Security policy authentication can be applied to as many or as few users as needed, and it supports a number of authentication protocols to easily fit with your existing network.

VPN authentication can be for both the remote VPN device as well as the VPN users. VPNs are used to communicate with locations outside the company network as if they were part of the company network. This level of trust, once a VPN is established, is easily established with authentication to verify the remote user is in fact a valid user. In this situation without authentication, anyone malicious or otherwise could connect to the company network with potentially full access.

**Firewall authentication (identity-based policies)**

Security policies enable traffic to flow between networks. If you want to limit which users have access to particular resources, you create identity-based policies (IBP) that allow access only to members of specific user groups. Authentication, a request for username and password, is triggered when a user attempts to access a resource for which data must pass through an identity-based policy.

The user’s authentication expires if the connection is idle for too long, 30 minutes by default but that can be customized.

Identity-based policies are the mechanism for FSSO, NTLM, certificate based, and dynamic profile authentication.
**FSSO**

Fortinet Single Sign on (FSSO) provides seamless authentication support for Microsoft Windows Active Directory (AD) and Novell eDirectory users in a FortiGate environment.

On a Microsoft Windows or Novell network, users authenticate with the Active Directory or Novell eDirectory at logon. FSSO provides authentication information to the FortiGate unit so that users automatically get access to permitted resources. See “Introduction to FSSO” on page 133.

**NTLM**

The NT LAN Manager (NTLM) protocol is used when the MS Windows Active Directory (AD) domain controller can not be contacted. NTLM is a browser-based method of authentication.

The FSSO software is installed on each AD server and the FortiGate unit is configured to communicate with each FSSO client. When a user successfully logs into their Windows PC (and is authenticated by the AD Server), the FSSO client communicates the user's name, IP address, and group login information to the FortiGate unit. The FortiGate unit sets up a temporary access policy for the user, so when they attempt access through the firewall they do not need to re-authenticate. This model works well in environments where the FSSO client can be installed on all AD servers.

In system configurations where it is not possible to install FSSO clients on all AD servers, the FortiGate unit must be able to query the AD servers to find out if a user has been properly authenticated. This is achieved using the NTLM messaging features of Active Directory and Internet Explorer.

Even when NTLM authentication is used, the user is not asked again for their username and password. Internet Explorer stores the user's credentials and the FortiGate unit uses NTLM messaging to validate them in the Windows AD environment.

Note that if the authentication reaches the timeout period, the NTLM message exchange restarts. For more information on NTLM, see “NTLM authentication” on page 105 and “NTLM authentication with FSSO” on page 137, and

**Certificates**

Certificates can be used as part of an identity-based policy. All users being authenticated against the policy are required to have the proper certificate. See “Certificate-based authentication” on page 17.

**Dynamic profile**

Dynamic profile is a remote authentication method that does not require any local users to be configured, and relies on RADIUS Start records to provide the FortiGate unit with authentication information. That information identifies the user and user group, which is then matched using a security policy. See “Dynamic profiles and end points” on page 175.

**FortiGuard Web Filter override authentication**

Optionally, users can be allowed the privilege of overriding FortiGuard Web Filtering to view blocked web sites. Depending on the override settings, the override can apply to the user who requested it, the entire user group to which the user belongs, or all users who share the same web filter profile. As with other FortiGate features, access to FortiGuard overrides is controlled through user groups. Firewall and Directory Services user groups are eligible for the override privilege. For more information about web filtering and overrides, see the UTM chapter of this FortiOS Handbook.
VPN authentication

Authentication involves authenticating the user. In IPsec VPNs authenticating the user is optional, but authentication of the peer device is required.

This section includes:
- Authenticating IPsec VPN peers (devices)
- Authenticating IPsec VPN users
- Authenticating SSL VPN users
- Authenticating PPTP and L2TP VPN users

Authenticating IPsec VPN peers (devices)

A VPN tunnel has one end on a local trusted network, and the other end is at a remote location. The remote peer (device) must be authenticated to be able to trust the VPN tunnel. Without that authentication, it is possible for a malicious hacker to masquerade as a valid VPN tunnel device and gain access to the trusted local network.

The three ways to authenticate VPN peers are with a preshared key, RSA X.509 certificate, an a specific peer ID value.

The simplest way for IPsec VPN peers to authenticate each other is through the use of a preshared key, also called a shared secret. The preshared key is a text string used to encrypt the data exchanges that establish the VPN tunnel. The preshared key must be six or more characters. The VPN tunnel cannot be established if the two peers do not use the same key. The disadvantage of preshared key authentication is that it can be difficult to securely distribute and update the preshared keys. See “Authenticating the FortiGate unit with a pre-shared key” on page 211.

RSA X.509 certificates are a better way for VPN peers to authenticate each other. Each peer offers a certificate signed by a Certificate Authority (CA) which the other peer can validate with the appropriate CA root certificate. For more information about certificates, see “Certificate-based authentication” on page 113.

You can supplement either preshared key or certificate authentication by requiring the other peer to provide a specific peer ID value. The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

Authenticating IPsec VPN users

An IPsec VPN can be configured to accept connections from multiple dynamically addressed peers. You would do this to enable employees to connect to the corporate network while traveling or from home. On a FortiGate unit, you create this configuration by setting the Remote Gateway to Dialup User.

It is possible to have an IPsec VPN in which remote peer devices authenticate using a common preshared key or a certificate, but there is no attempt to identify the user at the remote peer. To add user authentication, you can do one of the following:
- require a unique preshared key for each peer
- require a unique peer ID for each peer
- require a unique peer certificate for each peer
- require additional user authentication (XAuth)

The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.
Authenticating SSL VPN users

SSL VPN users can be
- user accounts with passwords stored on the FortiGate unit
- user accounts authenticated by an external RADIUS, LDAP or TACACS+ server
- PKI users authenticated by certificate

You need to create a user group for your SSL VPN. Simply create a firewall user group, enable SSL VPN access for the group, and select the web portal the users will access. SSL VPN access requires an SSL VPN security policy that permits access to members of your user group.

Authenticating PPTP and L2TP VPN users

PPTP and L2TP are older VPN tunneling protocols that do not provide authentication themselves. FortiGate units restrict PPTP and L2TP access to users who belong to one specified user group. Users authenticate themselves to the FortiGate unit by username/password. You can configure PPTP and L2TP VPNs only in the CLI. Before you configure the VPN, create a firewall user group and add to it the users who are permitted to use the VPN. Users are authenticated when they attempt to connect to the VPN. For more information about configuring PPTP or L2TP VPNs, see the FortiGate CLI Reference.

User’s view of authentication

From the user’s point of view, they see a request for authentication when they try to access a protected resource, such as an FTP repository of intellectual property or simply access a website on the Internet. The way the request is presented to the user depends on the method of access to that resource.

VPN authentication usually controls remote access to a private network.

Web-based user authentication

Security policies usually control browsing access to an external network that provides connection to the Internet. In this case, the FortiGate unit requests authentication through the web browser.

The user types a username and password and then selects Continue or Login. If the credentials are incorrect, the authentication screen is redisplayed with blank fields so that the user can try again. When the user enters valid credentials, access is granted to the required resource. In some cases, if a user tries to authenticate several times without success, a message appears, such as: “Too many bad login attempts. Please try again in a few minutes.” This indicates the user is locked out for a period of time. This prevents automated brute force password hacking attempts. The administrator can customize these settings if required.

After a defined period of user inactivity (the authentication timeout, defined by the FortiGate administrator), the user’s access expires. The default is 5 minutes. To access the resource, the user will have to authenticate again.
VPN client-based authentication

A VPN provides remote clients with access to a private network for a variety of services that include web browsing, email, and file sharing. A client program such as FortiClient negotiates the connection to the VPN and manages the user authentication challenge from the FortiGate unit.

FortiClient can store the username and password for a VPN as part of the configuration for the VPN connection and pass them to the FortiGate unit as needed. Or, FortiClient can request the username and password from the user when the FortiGate unit requests them.

SSL VPN is a form of VPN that can be used with a standard Web browser. There are two modes of SSL VPN operation (supported in NAT/Route mode only):

- web-only mode, for remote clients equipped with a web-browser only
- tunnel mode, for remote computers that run a variety of client and server applications.

FortiGate administrator’s view of authentication

Authentication is based on user groups. The FortiGate administrator configures authentication for security policies and VPN tunnels by specifying the user groups whose members can use the resource. Some planning is required to determine how many different user groups need to be created. Individual user accounts can belong to multiple groups, making allocation of user privileges very flexible.

A member of a user group can be:

- a user whose username and password are stored on the FortiGate unit
- a user whose name is stored on the FortiGate unit and whose password is stored on a remote or external authentication server
- a remote or external authentication server with a database that contains the username and password of each person who is permitted access

The general process of setting up authentication is as follows:

1. If remote or external authentication is needed, configure the required servers.
2. Configure local and peer (PKI) user identities. For each local user, you can choose whether the FortiGate unit or a remote authentication server verifies the password. Peer members can be included in user groups for use in security policies.
3. Create user groups.
   - Add local/peer user members to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server’s database can authenticate. You can only configure peer user groups through the CLI.
4. Configure security policies and VPN tunnels that require authenticated access.

For authentication troubleshooting, see the specific chapter for the topic or for general issues see “Troubleshooting” on page 227.
Authentication and User in the web-based manager

This section provides an introduction to the web-based manager User menu. The following topics are included in this section:

- User
- User groups
- Remote
- FortiToken
- Fortinet Single Sign On Agent (FSSO)
- PKI
- Monitor

The word “unit” refers to the FortiGate unit. The words “FortiGate unit” are used when talking about different Fortinet products in one sentence. For example, “The Central Management menu provides the option of remotely managing your FortiGate unit by a FortiManager unit.”

User

The User menu allows you to configure authentication settings and user accounts. The User menu also allows you to configure user groups, remote servers, as well as monitor users.

A user is a user account that consists of a user name, password and in some cases, other information that can be configured on the unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group. For more information about user groups, see “User groups” on page 28.

This topic contains the following:

- Local user accounts
- IM users
- Authentication settings

Local user accounts

A local user is a user configured on a unit. The user can be authenticated with a password stored on the unit (the user name and password must match a user account stored on the unit) or with a password stored on an authentication server. The user name must match a user account stored on the unit and the user name and password must match a user account stored on the authentication server associated with the user.
When configuring a user account, you can enable two-factor authentication. This feature allows you to add what is referred to as a FortiToken, which is a serial number used in login credentials, and this FortiToken can be emailed to the user or sent to their mobile phone. Two-factor authentication is a security measure that provides an additional log in credential, in this case a FortiToken, that the user must enter so that they can log in. You must have the FortiToken device to use the FortiToken feature on your unit.

**Local user accounts configuration settings**

Local users are configured in User > User > User. Use the following table when configuring local user accounts.

<table>
<thead>
<tr>
<th>User page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual local user's list that you created. On this page, you can edit, delete or create a new local users list.</td>
</tr>
</tbody>
</table>

**Note:** If you want to have users always authenticate whenever their time expires, use the hard-timeout value in the auth-type command. This is available only in the CLI.

<table>
<thead>
<tr>
<th>Create New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a new local user account. When you select Create New, you are automatically redirected to New User page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a user from the list. Removing the user name removes the authentication configured for the user.</td>
</tr>
<tr>
<td>The Delete icon is not available if the user belongs to a user group.</td>
</tr>
<tr>
<td>To remove multiple local user accounts from within the list, on the User page, in each of the rows of user accounts you want removed, select the check box and then select Delete.</td>
</tr>
<tr>
<td>To remove all local user accounts from the list, on the User page, select the check box in the check box column and then select Delete.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifies a user's account settings. When you select Edit, you are automatically redirected to the Edit User page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>The local user name.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>The authentication type to use for this user. The authentication types are Local (user and password stored on Fortinet unit), LDAP, RADIUS, and TACACS+ (user and password matches a user account stored on the authentication server).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Two-factor Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates the status of whether two-factor authentication is configured for the user.</td>
</tr>
<tr>
<td>A gray x displays if there is no two-factor authentication enabled for the user. A green check mark displays if two-factor authentication is enabled for the user.</td>
</tr>
</tbody>
</table>
Ref.

Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (UTM > Antivirus > Profile), 1 appears in Ref.

To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object.

To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:

- **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at.
- **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page.
- **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy’s settings appear within the table.

**New User page**

Provides settings for configuring whether to allow or block a local user from authenticating.

<table>
<thead>
<tr>
<th><strong>User Name</strong></th>
<th>A name that identifies the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disable</strong></td>
<td>Select to prevent this user from authenticating.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Select to authenticate this user using a password stored on the unit and then enter the password. Best practices dictate that the password be at least six characters long.</td>
</tr>
<tr>
<td><strong>Match users on LDAP servers</strong></td>
<td>Select to authenticate this user using a password stored on an LDAP server. Select the LDAP server from the list. You can select only an LDAP server that has been added to the Fortinet LDAP configuration. For more information, see “LDAP” on page 36.</td>
</tr>
<tr>
<td><strong>Match users on RADIUS server</strong></td>
<td>Select to authenticate this user using a password stored on a RADIUS server. Select the RADIUS server from the list. You can select only a RADIUS server that has been added to the Fortinet RADIUS configuration. For more information, see “RADIUS” on page 34.</td>
</tr>
<tr>
<td><strong>Match users on TACACS+ server</strong></td>
<td>Select to authenticate this user using a password stored on a TACACS server. Select the TACACS+ server from the list. You can select only a TACACS server that has been added to the Fortinet TACACS configuration. For more information, see “TACACS+” on page 39.</td>
</tr>
<tr>
<td><strong>Enable Two-factor Authentication</strong></td>
<td>Select to enable the two-factor authentication feature. When you enable this feature, FortiToken, Email to and SMS appear below. You can enable two-factor authentication for FortiGate administrators as well as users. For more information about enabling two-factor authentication for FortiGate administrators, see “Associating FortiTokens with accounts” on page 83.</td>
</tr>
</tbody>
</table>
IM users

Instant Messenger (IM) protocols are gaining in popularity as an essential way to communicate between two or more individuals in real time. Some companies even rely on IM protocols for critical business applications such as Customer/Technical Support.

The most common IM protocols in use today include AOL Instant Messenger, Yahoo Instant Messenger, MSN messenger, and ICQ. Fortinet units allow you to set up IM users that either allow or block the use of applications, to determine which applications are allowed.

IM users configuration settings

IM users are configured in the CLI first, and then appear in User > User > IM. IM users must be configured using the `config imp2p` command in the CLI.

The following are IM user configuration settings in User > User > IM.

<table>
<thead>
<tr>
<th>IM page</th>
<th>Lists each individual IM user. On this page, you can edit, delete or create a new IM user. You can also filter the information by protocol or policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates an IM user. When you select Create New, you are automatically redirected to the Edit User page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies an IM user's settings. When you select Edit, you are automatically redirected to the Edit User page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes an IM user from the list on the page. To remove multiple IM users from within the list, on the IM page, in each of the rows of users you want removed, select the check box and then select Delete. To remove all IM users from the list, on the IM page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Protocol:</td>
<td>Filter the information on the page using a specific protocol. For example, only ICQ users appear when the protocol selected is ICQ. You can use both Protocol and Policy to filter the information on the page. For example, only ICQ users that are blocked appear when protocol is set to ICQ and policy is set to Block.</td>
</tr>
</tbody>
</table>
Authentication and User in the web-based manager

The Authentication submenu provides settings for configuring authentication timeout, protocol support, and authentication certificates.

When user authentication is enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (depending on the connection protocol):

<table>
<thead>
<tr>
<th>Policy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the information on the page using a specific policy. For example, only policies that are blocked appear when the policy selected is Block. You can use both Protocol and Policy to filter the information on the page. For example, only ICQ users that are blocked appear when protocol is set to ICQ and policy is set to Block.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>The type of instant messaging protocol. For example, ICQ is for all ICQ instant messaging software.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>The type of action that will be taken when the protocol is detected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (UTM &gt; Antivirus &gt; Profile), 1 appears in Ref. . To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:</td>
</tr>
</tbody>
</table>

- **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at.
- **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page.
- **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy’s settings appear within the table.

---

**Edit User page**

Provides settings for configuring an IM user.

<table>
<thead>
<tr>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select an instant messaging protocol from the drop-down list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the user name for accessing the IM user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the type of action that will be taken when the protocol is detected, for example, the protocol AIM will be blocked.</td>
</tr>
</tbody>
</table>

### Authentication settings

The Authentication submenu provides settings for configuring authentication timeout, protocol support, and authentication certificates.

When user authentication is enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (depending on the connection protocol):
User groups

A user group is a list of user identities. An identity can be:
- a local user account (user name and password) stored on the Fortinet unit
- a local user account with a password stored on a RADIUS, LDAP, or TACACS+ server
- a RADIUS, LDAP, or TACACS+ server (all identities on the server can authenticate)
- a user or user group defined on a Directory Service server.

Each user group belongs to one of three types: Firewall, Directory Service or SSL VPN.
In most cases, the unit authenticates users by requesting each user name and password. The unit checks local user accounts first. If the unit does not find a match, it checks the RADIUS, LDAP, or TACACS+ servers that belong to the user group. Authentication succeeds when the unit finds a matching user name and password.

This topic contains the following:
- User Group
- Firewall user groups
- Fortinet Single Sign-On (FSSO) user groups
- SSL VPN user groups

**User Group**

For each resource that requires authentication, you specify which user groups are permitted access. You need to determine the number and membership of user groups appropriate to your authentication needs.

Users that are associated with multiple groups have access to all services within all the user groups that they are associated with. This is only available in the CLI. The command used is `auth-multi-group`, which is enabled by default. This feature checks all groups a user belongs to for firewall authentication.

**User Group configuration settings**

The following are user group configuration settings in `User > User Group > User Group`.

<table>
<thead>
<tr>
<th><strong>User Group page</strong></th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new user group. When you select Create New, you are automatically redirected to New User Group page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a user group from the list on the User Group page. You cannot delete a user group that is included in a security policy, a dialup user phase 1 configuration, or a PPTP or L2TP configuration. To remove multiple user groups, expand the section (either Firewall or Directory Service, and in each of the rows of user groups you want removed, select the check box and then select Delete. To remove all user groups, on the User Group page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies membership and options of a group. When you select Edit, you are automatically redirected to the Edit User Group page.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The name of the user group. User group names are listed by type of user group: Firewall, Directory Service and SSL VPN. For more information, see &quot;Fortinet Single Sign-On (FSSO) user groups&quot; on page 32, and &quot;SSL VPN user groups&quot; on page 32.</td>
</tr>
</tbody>
</table>
### Members

The Local users, RADIUS servers, LDAP servers, TACACS+ servers, Directory Service users/user groups or PKI users found in the user group.

<table>
<thead>
<tr>
<th>Ref.</th>
</tr>
</thead>
</table>
| Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (UTM > Antivirus > Profile), 1 appears in Ref.

To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object.

To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:

- **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at.

- **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page.

- **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy’s settings appear within the table.

### New User Group page

Provides settings for configuring a list of users and/or groups.

**Note:** The Remote authentication servers section does not appear unless there is a RADIUS, LDAP, or TACAS+ server configured.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name of the user group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the user group type. See “Firewall user groups” on page 31, “SSL VPN user groups” on page 32 and “Fortinet Single Sign-On (FSSO) user groups” on page 32.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Select this group in any security policy that requires Firewall authentication.</td>
</tr>
<tr>
<td>Fortinet Single Sign-On (FSSO)</td>
<td>Select this group in any security policy that requires FSSO authentication.</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>Select this group in any security policy with Action set to SSL VPN. See “SSL VPN access” on page 86. This option is not available in Transparent mode.</td>
</tr>
<tr>
<td>Allow SSL-VPN Access</td>
<td>Select the type of SSL VPN access from the drop-down list.</td>
</tr>
</tbody>
</table>
A firewall user group provides access to a security policy that requires authentication and lists the user group as one of the allowed groups. The unit requests the group member's user name and password when the user attempts to access the resource that the policy protects. The reason for the name firewall user group is when creating a new user group you have the option to select Firewall or FSSO as the group type.

You can also authenticate a user by certificate if you have selected this method.

A firewall user group can also provide access to an IPSec VPN for dialup users. In this case, the IPSec VPN phase 1 configuration uses the Accept peer ID in dialup group peer option. The user’s VPN client is configured with the user name as peer ID and the password as pre-shared key. The user can connect successfully to the IPSec VPN only if the user name is a member of the allowed user group and the password matches the one stored on the unit.

A user group cannot be a dialup group if any member is authenticated using a RADIUS or LDAP server.
You can also use a firewall user group to provide override privileges for FortiGuard web filtering.

**Fortinet Single Sign-On (FSSO) user groups**

On a network, you can configure the unit to allow access to members of FSSO user groups who have been authenticated on the network. The Fortinet Single Sign On Agent must be installed on the network domain controllers.

An FSSO user group provides access to a security policy that requires FSSO type authentication and lists the user group as one of the allowed groups. The members of the user group are FSSO users or groups that you select from a list that the unit receives from the FSSO servers that you have configured. For more information, see “Fortinet Single Sign On Agent (FSSO)” on page 42.

An FSSO user group cannot have SSL VPN access.

You cannot use FSSO user groups directly in Fortinet security policies. You must add FSSO groups to Fortinet user groups. An FSSO group belong to only one Fortinet user group according to best practices. If you assign it to multiple Fortinet user groups, the unit recognizes only the last user group assignment.

You can also use an FSSO user group to provide override privileges for FortiGuard web filtering.

**SSL VPN user groups**

An SSL VPN user group provides access to a security policy that requires SSL VPN type authentication and lists the user group as one of the allowed groups. Local user accounts, LDAP, and RADIUS servers can be members of an SSL VPN user group. The unit requests the user’s user name and password when the user accesses the SSL VPN web portal. The user group settings include options for SSL VPN features.

An SSL VPN user group can also provide access to an IPSec VPN for dialup users. In this case, the IPSec VPN phase 1 configuration uses the Accept peer ID in dialup group peer option. You configure the user’s VPN client with the user name as peer ID and the password as pre-shared key. The user can connect successfully to the IPSec VPN only if the user name is a member of the allowed user group and the password matches the one stored on the unit.

A user group cannot be an IPSec dialup group if any member is authenticated using a RADIUS or LDAP server.

For information on configuring user groups, see “User groups” on page 28. For SSL VPN information, see “SSL VPN access” on page 86.

By default, the web-based manager displays Firewall options. You cannot add local users to a group that is used to authenticate administrators.
Dynamically assigning VPN client IP addresses from a user group

SSL VPN tunnel mode, dialup IPSec VPN, and PPTP VPN sessions can assign IP addresses to remote users by getting the IP address to assign to the user from the Framed-IP-Address field in the RADIUS record received when the RADIUS server confirms that the user has authenticated successfully. For more information about RADIUS fields, see RFC 2865 and RFC 2866.

For the unit to dynamically assign an IP address, the VPN users must be configured for RADIUS authentication and you must include the IP address to assign to the user in the Framed-IP-Address RADIUS field on your RADIUS server. You configure each type of VPN differently. In each case you are associating the configuration that assigns IP addresses to users with a user group.

Assigning IP addresses from a RADIUS record replaces dynamically assigning IP addresses from an address range. You cannot include an IP address range and assigning IP addresses from a RADIUS record in the same configuration.

Remote

Remote authentication is generally used to ensure that employees working offsite can remotely access their corporate network with appropriate security measures in place. In general terms, authentication is the process of attempting to verify the (digital) identity of the sender of a communication such as a login request. The sender may be someone using a computer, the computer itself, or a computer program. Since best practices dictate a computer system be used only by those who are authorized to do so, there must be a measure in place to detect and exclude any unauthorized access.

On a unit, you can control access to network resources by defining lists of authorized users, called user groups. To use a particular resource, such as a network or VPN tunnel, the user must:

- belong to one of the user groups that is allowed access
- correctly enter a user name and password to prove his or her identity, if asked to do so.

This topic contains the following:

- Administrators
- RADIUS
- LDAP
- TACACS+

Administrators

A local administrator account, admin, is configured by default on all FortiOS units. If you have remote servers configured, you can create remote administrator accounts as well. These are accounts with local administrator privileges that use remote authentication. One version of this are wildcard administrator accounts. See “Example — wildcard admin accounts - CLI” on page 61.

Configuring a remote administrator account is the same as a local administrator account with the following differences:

- You must have a remote authentication server and user group with an associated authentication server configured before creating the administrator account.
• Even though the administrator account will be authenticated remotely, when creating
the account using the web-based manager you must enter a password or the account
will not be created. You are not prompted for the password if the account is created in
the CLI. This password acts as a backup password in case the remote server does
not respond during authentication. The exception to this is when wildcard admin is
selected — for wildcard administrators, the password field is skipped over.

RADIUS

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication,
authorization, and accounting functions. Fortinet units use the authentication function of
the RADIUS server. You must configure the server before you configure the Fortinet users
or user groups that will need it to use the RADIUS server for authentication.

If you have configured RADIUS support and a user is required to authenticate using a
RADIUS server, the unit sends the user’s credentials to the RADIUS server for
authentication. If the RADIUS server can authenticate the user, the user is successfully
authenticated with the unit. If the RADIUS server cannot authenticate the user, the unit
refuses the connection. You can override the default authentication scheme by selecting
a specific authentication protocol or changing the default port for RADIUS traffic.

The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645, use
the CLI command, `config system global`, to change the default RADIUS port.

If you want to configure settings for UTF-8 encoding, you must enable this in the CLI
using the `config vpn ssl setting` command.

RADIUS configuration settings

The following are RADIUS server configuration settings in User > Remote > RADIUS.

<table>
<thead>
<tr>
<th>RADIUS page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual RADIUS server that you created. On this page, you can edit, delete or create a new RADIUS server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a new RADIUS server. The maximum number is 10. When you select Create New, you are automatically redirected to the New RADIUS Server page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a RADIUS server from the list on the RADIUS page. Note: You cannot delete a RADIUS server that has been added to a user group. To remove multiple RADIUS servers from within the list, on the RADIUS page, in each of the rows of servers you want removed, select the check box and then select Delete. To remove all RADIUS servers from the list, on the RADIUS page, select the check box in the check box column and then select Delete.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifies settings within a RADIUS server configuration. When you select Edit, you are automatically redirected to the Edit RADIUS Server page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name that identifies the RADIUS server on the unit.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>The type of server, either query or dynamic start.</td>
</tr>
</tbody>
</table>
### Server Name/IP
- **Server Name/IP**: Domain name or IP address of the RADIUS server.

### Ref.
- **Ref.**: Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (UTM > Antivirus > Profile), 1 appears in Ref.
- **Ref.**: To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object.
- **Ref.**: To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:
  - **View the list page for these objects**: automatically redirects you to the list page where the object is referenced at.
  - **Edit this object**: modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page.
  - **View the details for this object**: table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy’s settings appear within the table.

### New RADIUS Server page
- **New RADIUS Server page**: Provides settings for configuring a RADIUS server.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter the name that is used to identify the RADIUS server on the unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select either <strong>Query</strong> or <strong>Dynamic Start</strong>.</td>
</tr>
<tr>
<td><strong>Primary Server Name/IP</strong></td>
<td>Enter the domain name or IP address of the primary RADIUS server.</td>
</tr>
<tr>
<td><strong>Primary Server Secret</strong></td>
<td>Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key length can be up to a maximum of 16 characters. <strong>Note</strong>: Best practices dictate that the server secret key should be the maximum length for security reasons.</td>
</tr>
<tr>
<td><strong>Secondary Server Name/IP</strong></td>
<td>Enter the domain name or IP address of the secondary RADIUS server, if you have one.</td>
</tr>
<tr>
<td><strong>Secondary Server Secret</strong></td>
<td>Enter the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key can be up to a maximum length of 16 characters.</td>
</tr>
<tr>
<td><strong>Authentication Scheme</strong></td>
<td>Select <strong>Use Default Authentication Scheme</strong> to authenticate with the default method. The default authentication scheme uses PAP, MS-CHAP-V2, and CHAP, in that order. <strong>Select Specify Authentication Protocol</strong> to override the default authentication method, and choose the protocol from the list: MS-CHAP-V2, MS-CHAP, CHAP, or PAP, depending on what your RADIUS server needs.</td>
</tr>
</tbody>
</table>
LDAP

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. An LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and require a user to authenticate using an LDAP server, the unit contacts the LDAP server for authentication. To authenticate with the unit, the user enters a user name and password. The unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the unit successfully authenticates the user. If the LDAP server cannot authenticate the user, the unit refuses the connection.

Fortinet LDAP supports password renewal, and these settings are configured in the CLI. There are settings for a warning that the password is going to expire, and threshold of the expiry as well.

LDAP configuration settings

The following are LDAP server configuration settings in User > Remote > LDAP. You can use both IPv6 and IPv 4 addresses when configuring LDAP servers.

<table>
<thead>
<tr>
<th><strong>LDAP page</strong></th>
<th>Creates a new LDAP server. The maximum number is 10. When you select Create New, you are automatically redirected to the New LDAP Server page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Removes the LDAP server configuration from the list on the LDAP page. To remove multiple LDAP servers from within the list, on the LDAP page, in each of the rows of servers you want removed, select the check box and then select Delete. To remove all LDAP servers from the list, on the LDAP page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Delete</td>
<td>Modifies settings from within an LDAP server configuration. When you select Edit, you are automatically redirected to the Edit LDAP Server page.</td>
</tr>
<tr>
<td>Edit</td>
<td>The name that identifies the LDAP server on the unit.</td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
</tbody>
</table>
Server Name/IP | The domain name or IP address of the LDAP server.
---|---
Port | The TCP port used to communicate with the LDAP server.
Common Name Identifier | The common name identifier for the LDAP server. Most LDAP servers use cn. However, some servers use other common name identifiers such as uid.
Distinguished Name | The distinguished name used to look up entries on the LDAP servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
Ref. | Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (UTM > Antivirus > Profile), 1 appears in Ref. . To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object. To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:
- **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at.
- **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page.
- **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy’s settings appear within the table.

**New LDAP Server page**

Provides settings for configuring an LDAP server.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name that identifies the LDAP server on the Fortinet unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name/IP</td>
<td>Enter the domain name or IP address of the LDAP server.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Enter the TCP port used to communicate with the LDAP server. By default, LDAP uses port 389. If you use a secure LDAP server, the default port changes when you select Secure Connection.</td>
</tr>
<tr>
<td>Common Name Identifier</td>
<td>Enter the common name identifier for the LDAP server. The maximum number of characters is 20.</td>
</tr>
</tbody>
</table>
Using Query

The LDAP Distinguished Name Query list displays the LDAP Server IP address, and all the distinguished names associated with the Common Name Identifier for the LDAP server. The tree helps you to determine the appropriate entry for the DN field. You can see the distinguished name associated with the Common Name identifier, by expanding CN identifier and then selecting the DN from the list. The DN you select is displayed in the Distinguished Name field. You must select OK to save your selection in the Distinguished Name field of the LDAP Server configuration.
If you want to see the users with the LDAP Server user group for the selected Distinguished Name, expand *Distinguished Name* in the LDAP Distinguished Name Query tree.

**TACACS+**

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS+ server is 49.

**TACAS+ configuration settings**

The following are TACACS+ server configuration settings in *User > Remote > TACACS+*.

<table>
<thead>
<tr>
<th><strong>TACACS+ page</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists each individual TACACS+ server that you created. On this page, you can edit, delete or create a new TACACS+ server.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Create New</strong></th>
<th>Creates a new TACACS+ server. The maximum number of TACACS+ servers that you can create is 10. When you select <em>Create New</em>, you are automatically redirected to the New TACACS+ Server page.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Delete</strong></th>
<th>Removes a TACACS+ server from the list on the TACACS+ page. To remove multiple TACACS+ servers from within the list, on the TACACS+ page, in each of the rows of servers you want removed, select the check box and then select <em>Delete</em>. To remove all TACACS+ servers from the list, on the TACACS+ page, select the check box in the check box column and then select <em>Delete</em>.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Edit</strong></th>
<th>Modifies settings within a TACACS+ server configuration. When you select <em>Edit</em>, you are automatically redirected to the Edit TACASCS+ Server page.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>The name of the TACACS+ server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>The server domain name or IP address of the TACACS+ server.</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>The supported authentication method. TACACS+ authentication methods include: Auto, ASCII, PAP, CHAP, and MSCHAP.</td>
</tr>
</tbody>
</table>
FortiToken Authentication and User in the web-based manager

In User > FortiToken > FortiToken, you can add token password codes that are then used by users to authenticate when logging in, for example the FortiGate unit. These token password codes are generated by the FortiToken device, which is a small device that generates a unique token password code. This can then be activated by the unit so that it can then be used for authentication purposes. This code provides additional security for you and users. This is part of the two-factor authentication feature, providing an extra login credential to prove that the user is who they claim to be.

For more information about FortiToken and two-factor authentication, see “FortiToken” on page 80.

FortiToken configuration settings

You can apply two-factor authentication to administrators that are logging into the FortiGate unit.

The following are FortiToken configuration settings in User > FortiToken > FortiToken.
**FortiToken page**

Lists each individual FortiToken list that is currently being used and which user the token is being used by. A FortiToken list provides up to ten FortiToken serial numbers that one user can use to authenticate when entering log in credentials.

**Note:** You can import FortiToken serial numbers from a file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Creates a new FortiToken list. When you select Create New, you are automatically redirected to the Add new FortiToken page.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies the settings within the FortiToken list. When you select Edit, you are automatically redirected to the Edit new FortiToken page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a FortiToken list from within the list on the FortiToken page. To remove multiple token serial numbers from within the list, on the FortiToken page, in each of the rows of codes you want removed, select the check box and then select Delete. To remove all token codes from the list, on the FortiToken page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Import</td>
<td>Select to import FortiToken serial numbers from a file. When you select Import, the Upload window appears. From the Upload window you can select Browse to locate the file and then select OK to import the file to the unit.</td>
</tr>
<tr>
<td>Activate</td>
<td>Activates the FortiToken device so that you can use the device to code so that the code can then be used by a user or FortiGate administrator.</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Select to synchronize the FortiToken with an NTP server. This allows the unit’s system time to be the same as the FortiToken’s system time.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the FortiToken device. This serial number is found on the back of the device.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the FortiToken, whether it is activated or not.</td>
</tr>
<tr>
<td>Drift</td>
<td>The synchronization of the unit’s system time and the FortiToken’s time, which can “drift” away or become unsynchronized. When you synchronize the FortiToken, it calculates the unit’s and its own drift. The drift is the number of minutes that the FortiToken has drifted away from the unit’s system time. The minutes is shown in integers only. If drift is zero, then the FortiToken’s internal time is the same as the unit’s system time. If the drift is -1, the FortiToken is lagging behind the unit by one minute. If the drift is 1, then the FortiToken is ahead of the unit by one minute.</td>
</tr>
<tr>
<td>User</td>
<td>The user that the FortiToken is currently being used by.</td>
</tr>
</tbody>
</table>
Fortinet Single Sign On Agent (FSSO)

Windows Active Directory (AD) and Novell eDirectory provide central authentication services by storing information about network resources across a domain (a logical group of computers running versions of an operating system) in a central directory database. Each person who uses computers within a domain receives his or her own unique account/user name. This account can be assigned access to resources within the domain based on the role of the user. In a domain, the directory resides on computers that are configured as domain controllers. A domain controller is a server that manages all security-related features that affect the user/domain interactions, security centralization, and administrative functions.

Fortinet units use security policies to control access to resources based on user groups configured in the policies. Each Fortinet user group is associated with one or more Directory Service user groups. When a user logs in to the Windows or Novell domain, a Fortinet Single Sign On Agent (FSSO) sends the user’s IP address and the names of the Directory Service user groups to which the user belongs to the FortiGate unit.
The Fortinet Single Sign On Agent has two components that you must install on your network:

- The domain controller (DC) agent must be installed on every domain controller to monitor user logins and send information about them to the collector agent.
- The Collector agent must be installed on at least one domain controller to send the information received from the DC agents to the Fortinet unit. Alternately a FortiAuthenticator server can take the place of the Collector agent in an FSSO polling mode configuration.

The unit uses this information to maintain a copy of the domain controller user group database. Because the domain controller authenticates users, the unit does not perform authentication. It recognizes group members by their IP address.

You must install the Fortinet Single Sign On Agent on the network and configure the unit to retrieve information from the Directory Service server. For more information about Fortinet Single Sign On Agent, see the “Introduction to FSSO” on page 133.

**Fortinet Single Sign-on Agent configuration settings**

The following are configuration settings for collector agents in User > FSSO > FSSO Agent.

<table>
<thead>
<tr>
<th><strong>FSSO Agent page</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists all the collector agents’ lists that you have configured. On this page, you can create, edit or delete FSSO agents.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> You can create a redundant configuration on your unit if you install a collector agent on two or more domain controllers. If the current (or first) collector agent fails, the Fortinet unit switches to the next one in its list of up to five collector agents.</td>
<td></td>
</tr>
</tbody>
</table>

| **Create New** | Creates a new agent. When you select Create New, you are automatically redirected to the New page. |
| **Edit** | Modifies settings within the Collector agent list. When you select Edit, you are automatically redirected to the Edit page. To remove multiple agents from within the list, on the FSSO Agent page, in each of the rows of servers you want removed, select the check box and then select Delete. To remove all agents from the list, on the FSSO Agent page, select the check box in the check box column and then select Delete. |
| **Delete** | Removes an agent from the list on the page. |
| **Add User/Group** | Adds a user or group to the list on the FSSO Agent page. You must know the distinguished name for the user or group. When you select Add User/Group, you are automatically redirected to the Add User/Group page. |
| **Edit User/Group** | Modifies users or groups from the remote server. When you select Edit Users/Groups, you are automatically redirected to the Edit Users/Groups page. |
| **Refresh** | Refreshes the current information on the page. |
| **Name** | The name of the FSSO agent list. |
| **FSSO Agent IP/Name** | The IP address or name of the agent or agents. |
Ref.  | Displays the number of times the object is referenced to other objects. For example, av_1 profile is applied to a security policy; on the Profile page (UTM > Antivirus > Profile), 1 appears in Ref. .

To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object.

To view more information about how the object is being used, use one of the following icons that is available within the Object Usage window:

- **View the list page for these objects** – automatically redirects you to the list page where the object is referenced at.

- **Edit this object** – modifies settings within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy and so, when this icon is selected, the user is redirected to the Edit Policy page.

- **View the details for this object** – table, similar to the log viewer table, contains information about what settings are configured within that particular setting that the object is referenced with. For example, av_1 profile is referenced with a security policy, and that security policy’s settings appear within the table.

---

### New page

Provides settings for configuring FSSO agents. You can configured up to five agents, either Collector or Novell eDirectory.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the FSSO agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FSSO Agent IP/Name</strong></td>
<td>Enter the IP address or name of the Directory Service server where this collector agent is installed. The maximum number of characters is 63.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the TCP port used for Directory Service. This must be the same as the Fortinet listening port specified in the Fortinet Single Sign On Agent collector agent configuration.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password for the collector agent. This is required only if you configured your Fortinet Single Sign On Agent collector agent to require authenticated access.</td>
</tr>
<tr>
<td><strong>LDAP Server</strong></td>
<td>Select the check box and select an LDAP server to access the Directory Service.</td>
</tr>
</tbody>
</table>
PKI

Public Key Infrastructure (PKI) authentication utilizes a certificate authentication library that takes a list of peers, peer groups, and/or user groups and returns authentication successful or denied notifications. Users only need a valid certificate for successful authentication—no user name or password are necessary. Firewall and SSL VPN are the only user groups that can use PKI authentication.

If you use the CLI to create a peer user, best practices dictate that you enter a value for either subject or ca. If you do not do so, and then open the user record in the web-based manager, you will be prompted to enter a subject or ca value before you can continue.

PKI configuration settings

If your unit is currently running FortiOS 4.0 MR2 or higher, you must configure a PKI user first in the CLI to enable the PKI menu in the web-based manager, then you can then configure other PKI users in User > PKI > PKI.

The following are PKI configuration settings in User > PKI > PKI.

PKI page

Lists each individual PKI user that you have created. On this page, you can edit, delete or create a new PKI user.

<table>
<thead>
<tr>
<th>Create New</th>
<th>Creates a new PKI user. When you select Create New, you are automatically redirected to the New PKI User page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Removes a PKI user from the list on the PKI page. The delete icon is not available if the peer user belongs to a user group. Remove it from the user group first. To remove multiple PKI users from within the list, on the PKI page, in each of the rows of users you want removed, select the check box and then select Delete. To remove all PKI users from the list, on the PKI page, select the check box in the check box column and then select Delete.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies settings within the PKI user configuration. When you select Edit, you are automatically redirected to the Edit PKI User page.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the PKI user.</td>
</tr>
<tr>
<td>Subject</td>
<td>The text string that appears in the subject field of the certificate of the authenticating user.</td>
</tr>
<tr>
<td>CA</td>
<td>The CA certificate that is used to authenticate this user. <strong>Note:</strong> PKI certificate authentication supports the extraction of the user name from within the UPN field, which allows users to log in without having to enter their user name. This is available only in the CLI.</td>
</tr>
</tbody>
</table>
You can define peer users and peer groups used for authentication in some VPN configurations and for PKI certificate authentication in security policies. Defining peer users and peer groups is configured in the CLI.

A peer user is a digital certificate holder that can use PKI authentication. Before using PKI authentication, you must define peer users to include in the user group that is incorporated into the firewall authentication policy.

When defining a peer user, you need:

- a peer user name
- the text from the subject field of the certificate of the authenticating peer user, or the CA certificate used to authenticate the peer user.

You can add or modify other configuration settings for PKI authentication.
Peer users are created in User > PKI > PKI for authentication; however, you must enter a value for at least one of the fields, Subject or CA. You can configure peer user groups only through the CLI.

PKI certificate authentication supports the extraction of the user name from within the UPN field, which allows users to log in without having to enter their user name. This is available only in the CLI.

Monitor

You can go to the Monitor menu to view lists of currently authenticated users, authenticated IM users, and banned users. For each authenticated user, the list includes the user name, user group, how long the user has been authenticated (Duration), how long until the user’s session times out (Time left), and the method of authentication used. The list of IM users includes the source IP address, protocol, and last time the protocol was used. The Banned User list includes users configured by administrators in addition to those quarantined based on AV, IPS, or DLP rules.

This topic contains the following:
- Firewall monitor list
- IM user monitor list
- The Banned User list

Firewall monitor list

In some environments, it is useful to determine which users are authenticated by the Fortinet unit and allow the system administrator to de-authenticate (stop current session) users. With the Firewall monitor, you can de-authenticate all currently authenticated users, or select single users to de-authenticate. To permanently stop a user from re-authenticating, change the Fortinet configuration (disable a user account) and then use the User monitor to immediately end the user’s current session.

Monitored firewall users are viewed from User > Monitor > Firewall.

Firewall page

Lists all authenticated firewall users that are currently authenticated by the Fortinet unit and are active. This page allows you to refresh the information on the page, as well as filter the information.

<table>
<thead>
<tr>
<th>Refresh</th>
<th>Refresh the Firewall user monitor list.</th>
</tr>
</thead>
</table>
| Filter Settings | Select to filter the information on the page. Filters appears automatically after selecting Filter Settings, below the column headings. Use to configure filter settings.  
**Note:** Filter Settings configures all filter settings. Filter icons are used to configure filter settings within that column.  
To apply a filter setting, select the plus sign beside Add new filter and then select and enter the information required. Repeat to add other filter settings.  
To modify settings, select Change beside the setting and edit the settings.  
To clear all filter settings, select the icon beside Clear all filters. |
To use a filter icon to filter settings within a column, select the filter icon in the column; Filters appears. Within Filters, configure the settings for that column.

Select to filter the information on the page. Filters appears automatically after selecting Filter Settings, below the column headings. Use to configure filter settings.

**Note:** Filter Settings configures all filter settings. Filter icons are used to configure filter settings within that column.

**De-authenticate All Users**
Stop authenticated sessions for all users in the Firewall user monitor list. Users must re-authenticate with the firewall to resume their communication session.

**Page Controls**
Use to navigate through the list.

**Column Settings**
Customize the table view. You can select the columns to hide or display and specify the column displaying order in the table.

**User Name**
The user names of all connected remote users.
In the **User Name** column heading, there is a green arrow beside the name. This green arrow allows you to sort the list alphabetically. By default, the green arrow is up and when you select it, the green arrow is down. The green up arrow indicates that the list is in alphabetical order, starting with the letter A; when the green arrow is down, the list is the opposite.

**User Group**
The user group that the remote user is part of.

**Policy ID**
The policy identification number.

**Duration**
Length of time since the user was authenticated.

**IP Address**
The user’s source IP address.

**Traffic Volume**
The amount of traffic that is going through the unit, that is generated by the user.

**Method**
Authentication method used for the user by the unit (authentication methods can be Fortinet Single Sign On Agent, firewall authentication, or NTLM).

**IM user monitor list**
User lists can be managed to allow or block certain users. Each user can be assigned a policy to allow or block activity for each IM protocol. Each IM function can be individually allowed or blocked providing the administrator the granularity to block the more bandwidth consuming features such as voice chat while still allowing text messaging.
The IM user monitor list displays information about instant messaging users who are currently connected. The list can be filtered by protocol. After IM users connect through the firewall, the unit displays which users are connected. You can analyze the list and decide which users to allow or block. A policy can be configured to handle unknown users.

**Active IM users are viewed from User > Monitor > IM.**

**IM users who are already logged on before changes are made to the IM user profile will not be affected until their next login. You cannot disconnect users who have already logged on by enabling logon blocking.**
The Banned User list

The Banned User list shows all IP addresses and interfaces blocked by NAC quarantine. The list also shows all IP addresses, authenticated users, senders, and interfaces blocked by Data Leak Prevention (DLP). The system administrator can selectively release users or interfaces from quarantine or configure quarantine to expire after a selected time period.

All sessions started by users or IP addresses on the Banned User list are blocked until the user or IP address is removed from the list. All sessions to an interface on the list are blocked until the interface is removed from the list.

You can configure NAC quarantine to add users or IP addresses to the Banned User list under the following conditions:

- **Users or IP addresses that originate attacks detected by IPS** - To quarantine users or IP addresses that originate attacks, enable and configure Quarantine Attackers in an IPS Sensor Filter.

- **IP addresses or interfaces that send viruses detected by virus scanning** - To quarantine IP addresses that send viruses or interfaces that accept traffic containing a virus, enable Quarantine Virus Sender in an antivirus profile.

- **Users or IP addresses that are banned or quarantined by Data Leak Prevention** - Set various options in a DLP sensor to add users or IP addresses to the Banned User list.

For more information, see FortiOS Handbook UTM guide.

Banned users are viewed from User > Monitor > Banned User.
<table>
<thead>
<tr>
<th><strong>Ban key</strong></th>
<th>The Ban key.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Protocol</strong></td>
<td>The protocol that was used by the user or IP address added to the Banned User list.</td>
</tr>
<tr>
<td><strong>Cause or rule</strong></td>
<td>The Fortinet function that caused the user or IP address to be added to the Banned User list. <em>Cause or rule</em> can be IPS, Antivirus, or Data Leak Prevention.</td>
</tr>
<tr>
<td><strong>Created</strong></td>
<td>The date and time the user or IP address was added to the Banned User list.</td>
</tr>
<tr>
<td><strong>Expires</strong></td>
<td>The date and time the user or IP address will be automatically removed from the Banned User list. If <em>Expires</em> is <em>Indefinite</em>, you must manually remove the user or host from the list.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Removes the selected user or IP address from the Banned User list.</td>
</tr>
</tbody>
</table>
Authentication servers

FortiGate units support the use of external authentication servers. An authentication server can provide password checking for selected FortiGate users or it can be added as a member of a FortiGate user group.

If you are going to use authentication servers, you must configure the servers before you configure FortiGate users or user groups that require them.

MAC OS and iOS devices, including iPhones and iPads, can perform user authentication with FortiOS units using RADIUS servers, but not with LDAP or TACACS+ servers.

This section includes the following topics:
- FortiAuthenticator servers
- RADIUS servers
- LDAP servers
- TACACS+ servers
- FSSO servers
- RSA ACE (SecurID) servers

FortiAuthenticator servers

FortiAuthenticator is an Authentication, Authorization, and Accounting (AAA) server, that includes a RADIUS server, an LDAP server, and can replace the FSSO Collector Agent on a Windows AD network. Multiple FortiGate units can use a single FortiAuthenticator for FSSO, remote authentication, and FortiToken management.

For more information, see the FortiAuthenticator Administration Guide.

RADIUS servers

Remote Authentication and Dial-in User Service (RADIUS) is a broadly supported client-server protocol that provides centralized authentication, authorization, and accounting functions. RADIUS clients are built into gateways that allow access to networks such as Virtual Private Network servers, Network Access Servers (NAS), as well as network switches and firewalls that use authentication. FortiGate units fall into the last category.

RADIUS servers use UDP packets to communicate with the RADIUS clients on the network to authenticate users before allowing them access to the network, to authorize access to resources by appropriate users, and to account or bill for those resources that are used. RADIUS servers are currently defined by RFC 2865 (RADIUS) and RFC 2866 (Accounting), and listen on either UDP ports 1812 (authentication) and 1813 (accounting) or ports 1645 (authentication) and 1646 (accounting) requests. RADIUS servers exist for all major operating systems.

You must configure the RADIUS server to accept the FortiGate unit as a client. FortiGate units use the authentication and accounting functions of the RADIUS server.
Microsoft RADIUS servers

Microsoft Windows Server 2000, 2003, and 2008 have RADIUS support built-in. Microsoft specific RADIUS features are defined in RFC 2548. The Microsoft RADIUS implementation can use Active Directory for user credentials.

For details on Microsoft RADIUS server configurations, refer to Microsoft documentation.

RADIUS user database

The RADIUS user database is commonly an SQL or LDAP database, but can also be any combination of:

• usernames and passwords defined in a configuration file
• user account names and passwords configured on the computer where the RADIUS server is installed.

If users are members of multiple RADIUS groups, then the user group authentication timeout value does not apply. See “Membership in multiple groups” on page 89.

RADIUS authentication with a FortiGate unit

To use RADIUS authentication with a FortiGate unit

• configure one or more RADIUS servers on the FortiGate unit
• assign users to a RADIUS server

When a configured user attempts to access the network, the FortiGate unit will forward the authentication request to the RADIUS server which will match the username and password remotely. Once authenticated the RADIUS server passes the authorization granted message to the FortiGate unit which grants the user permission to access the network.

The RADIUS server uses a “shared secret” key along with MD5 hashing to encrypt information passed between RADIUS servers and clients, including the FortiGate unit. Typically only user credentials are encrypted. Additional security can be configured through IPSec tunnels.

RADIUS attribute value pairs

RADIUS packets include a set of attribute value pairs (AVP) to identify information about the user, their location and other information. The FortiGate unit sends the following RADIUS attributes.

Table 1: FortiOS supported RADIUS attributes

<table>
<thead>
<tr>
<th>RADIUS Attribute</th>
<th>Name</th>
<th>Description</th>
<th>AVP type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Acct-Session-ID</td>
<td>Unique number assigned to each start and stop record to make it easy to match them, and to eliminate duplicate records.</td>
<td>44</td>
</tr>
<tr>
<td>2</td>
<td>username</td>
<td>Name of the user being authenticated</td>
<td>1</td>
</tr>
</tbody>
</table>
Table 1: FortiOS supported RADIUS attributes

<table>
<thead>
<tr>
<th>RADIUS ATTRIBUTE</th>
<th>AUTHENTICATION METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS-Identifier</td>
<td>Web</td>
</tr>
<tr>
<td>Identifier or IP address of the Network Access Server (NAS) that is requesting authentication. In this case, the NAS is the FortiGate unit.</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>XAuth of IPsec (without DHCP)</td>
</tr>
<tr>
<td>Address to be configured for the user.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Fortinet-VSA</td>
<td>XAuth of IPsec (with DHCP)</td>
</tr>
<tr>
<td>See “Vendor-specific attributes” on page 53</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Acct-Input-Octets</td>
<td>PPTP/L2TP (in PPP)</td>
</tr>
<tr>
<td>Number of octets received from the port over the course of this service being provided. Used to charge the user for the amount of traffic they used.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Acct-Output-Octets</td>
<td>SSL-VPN</td>
</tr>
<tr>
<td>Number of octets sent to the port while delivering this service. Used to charge the user for the amount of traffic they used.</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

Table 2 describes the supported authentication events and the RADIUS attributes that are sent in the RADIUS accounting message.

Table 2: RADIUS attributes sent in RADIUS accounting message

<table>
<thead>
<tr>
<th>RADIUS ATTRIBUTE</th>
<th>AUTHENTICATION METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS-Identifier</td>
<td>Web</td>
</tr>
<tr>
<td>Identifier or IP address of the Network Access Server (NAS) that is requesting authentication. In this case, the NAS is the FortiGate unit.</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>XAuth of IPsec (without DHCP)</td>
</tr>
<tr>
<td>Address to be configured for the user.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Fortinet-VSA</td>
<td>XAuth of IPsec (with DHCP)</td>
</tr>
<tr>
<td>See “Vendor-specific attributes” on page 53</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Acct-Input-Octets</td>
<td>PPTP/L2TP (in PPP)</td>
</tr>
<tr>
<td>Number of octets received from the port over the course of this service being provided. Used to charge the user for the amount of traffic they used.</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Acct-Output-Octets</td>
<td>SSL-VPN</td>
</tr>
<tr>
<td>Number of octets sent to the port while delivering this service. Used to charge the user for the amount of traffic they used.</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

Vendor-specific attributes

Vendor specific attributes (VSA) are the method RADIUS servers and client companies use to extend the basic functionality of RADIUS. Some major vendors, such as Microsoft, have published their VSAs, however many do not.

In order to support vendor-specific attributes (VSA), the RADIUS server requires a dictionary to define which VSAs to support. This dictionary is typically supplied by the client or server vendor.

The Fortinet RADIUS vendor ID is 12365.

The FortiGate unit RADIUS VSA dictionary is supplied by Fortinet and is available through the Fortinet Knowledge Base (http://kb.forticare.com) or through Technical Support. Fortinet’s dictionary for FortiOS 4.0 and up is configured this way:

```shell
##
Fortinet’s VSA’s
#
```
Note that using the Fortinet-Vdom-Name, users can be tied to a specific VDOM on the FortiGate unit. See the documentation provided with your RADIUS server for configuration details.

**Role Based Access Control**

In Role Based Access Control (RBAC), network administrators and users have varying levels of access to network resources based on their role, and that role’s requirement for access specific resources. For example, a junior accountant does not require access to the sales presentations, or network user account information.

There are three main parts to RBAC: role assignment, role authorization, and transaction authorization. Role assignment is accomplished when someone in an organization is assigned a specific role by a manager or HR. Role authorization is accomplished when a network administrator creates that user’s RADIUS account and assigns them to the required groups for that role. Transaction authorization occurs when that user logs on and authenticates before performing a task.

RBAC is enforced when FortiOS network users are remotely authenticated via a RADIUS server. For users to authenticate, an identity-based security policy must be matched. That policy only matches a specific group of users. If VDOMs are enabled, the matched group will be limited to a specific VDOM. Using this method network administrators can separate users into groups that match resources, protocols, or VDOMs. It is even possible to limit users to specific FortiGate units if the RADIUS servers serve multiple FortiOS units.

For more information on identity-based policies, see “Authentication in security policies” on page 96.

**Configuring the FortiGate unit to use a RADIUS server**

The information you need to configure the FortiGate unit to use a RADIUS server includes

- the RADIUS server’s domain name or IP address
- the RADIUS server’s shared secret key.

You can optionally specify the NAS IP or Called Station ID. When configuring the FortiGate to use a RADIUS server, the FortiGate is a Network Access Server (NAS). If the FortiGate interface has multiple IP addresses, or you want the RADIUS requests to come from a different address you can specify it here. Called Station ID applies to carrier networks. However, if the NAS IP is not included in the RADIUS configuration, the IP of the FortiGate unit interface that communicates with the RADIUS server is used instead.

A maximum of 10 remote RADIUS servers can be configured on the FortiGate unit. One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see “Creating users” on page 74.
On the FortiGate unit, the default port for RADIUS traffic is 1812. Some RADIUS servers use port 1645. If this is the case with your server, you can either:

- Re-configure the RADIUS server to use port 1812. See your RADIUS server documentation for more information on this procedure.

or

- Change the FortiGate unit default RADIUS port to 1645 using the CLI:

```bash
config system global
  set radius_port 1645
end
```

One wildcard admin account can be added to the FortiGate unit when using RADIUS authentication. This uses the wildcard character to allow multiple admin accounts on RADIUS to use a single account on the FortiGate unit. See “Example — wildcard admin accounts - CLI” on page 61.

**To configure the FortiGate unit for RADIUS authentication - web-based manager**

1. Go to `User > Remote > RADIUS` and select `Create New.`
2. Enter the following information and select OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>A name to identify the RADIUS server on the FortiGate unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Query. Selecting a Type of Dynamic Start configures the Dynamic Profile feature. See “Dynamic profiles and end points” on page 175.</td>
</tr>
<tr>
<td>Primary Server Name/IP</td>
<td>Enter the domain name (such as fgt.exmaple.com) or the IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Primary Server Secret</td>
<td>Enter the server secret key, such as radiusSecret. This can be a maximum of 16 characters long. This must match the secret on the RADIUS primary server.</td>
</tr>
<tr>
<td>Secondary Server Name/IP</td>
<td>Optionally enter the domain name (such as fgt.exmaple.com) or the IP address of the secondary RADIUS server.</td>
</tr>
<tr>
<td>Secondary Server Secret</td>
<td>Optionally, enter the secondary server secret key, such as radiusSecret2. This can be a maximum of 16 characters long. This must match the secret on the RADIUS secondary server.</td>
</tr>
<tr>
<td>Authentication Scheme</td>
<td>If you know the RADIUS server uses a specific authentication protocol, select it from the list. Otherwise select Use Default Authentication Scheme. The Use Default option will usually work.</td>
</tr>
<tr>
<td>NAS IP/ Called Station ID</td>
<td>Enter the IP address to be used as an attribute in RADIUS access requests. <strong>NAS-IP-Address</strong> is RADIUS setting or IP address of FortiGate interface used to talk to RADIUS server, if not configured. <strong>Called Station ID</strong> is same value as NAS-IP Address but in text format.</td>
</tr>
<tr>
<td>Include in every User Group</td>
<td>When enabled this RADIUS server will automatically be included in all user groups. This is useful if all users will be authenticating with the remote RADIUS server.</td>
</tr>
</tbody>
</table>
3  Select OK.

To configure the FortiGate unit for RADIUS authentication - CLI example

```
config user radius
edit ourRADIUS
  set auth-type auto
  set server 10.11.102.100
  set secret radiusSecret
end
```

For more information about RADIUS server options, refer to the FortiGate CLI Reference.

Troubleshooting RADIUS

To test the connection to the RADIUS server use the following command:

```
diagnose test authserver radius-direct <server_name or IP> <port number> <secret>
```

For the port number, enter -1 to use the default port. Otherwise enter the port number to check.

Additional RADIUS related troubleshooting is located at “Troubleshooting FSSO” on page 168

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

The scale of LDAP servers range from big public servers such as BigFoot and Infospace, to large organizational servers at universities and corporations, to small LDAP servers for workgroups that may be using OpenLDAP. This document focuses on the institutional and workgroup applications of LDAP.

This section includes:

- Components and topology
- LDAP directory organization
- Configuring the FortiGate unit to use an LDAP server
- Example — wildcard admin accounts - CLI
- Example of LDAP to allow Dial-in through member-attribute - CLI
- Troubleshooting LDAP

For MAC OS and iOS devices to authenticate, you must use MS-CHAP-v2 authentication. In the CLI, the command is set auth-type ms_chap_v2.
Components and topology

LDAP organization starts with directories. A directory is a set of objects with similar attributes organized in a logical and hierarchical way. Generally, an LDAP directory tree reflects geographic and organizational boundaries, with the Domain name system (DNS) names to structure the top level of the hierarchy. The common name identifier for most LDAP servers is `cn`, however some servers use other common name identifiers such as `uid`.

When LDAP is configured and a user is required to authenticate the general steps are:
1. The FortiGate unit contacts the LDAP server for authentication.
2. To authenticate with the FortiGate unit, the user enters a username and password.
3. The FortiGate unit sends this username and password to the LDAP server.
4. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit.
5. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit.

Binding

Binding is the step where the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server based on that user’s permissions.

The FortiGate unit can be configured to use one of three types of binding:
- anonymous - bind using anonymous user search
- regular - bind using username/password and then search
- simple - bind using a simple password authentication without a search

You can use simple authentication if the user records all fall under one domain name (`dn`). If the users are under more than one `dn`, use the anonymous or regular type, which can search the entire LDAP database for the required username.

If your LDAP server requires authentication to perform searches, use the regular type and provide values for username and password.

Supported versions

The FortiGate unit supports LDAP protocol functionality defined in RFC 2251: Lightweight Directory Access Protocol v3, for looking up and validating usernames and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3, including FortiAuthenticator. In addition, FortiGate LDAP supports LDAP over SSL/TLS, which can be configured only in the CLI.

FortiGate LDAP does not support proprietary functionality, such as notification of password expiration, which is available from some LDAP servers. FortiGate LDAP does not supply information to the user about why authentication failed.

LDAP directory organization

To configure your FortiGate unit to work with an LDAP server, you need to understand the organization of the information on the server.

The top of the hierarchy is the organization itself. Usually this is defined as Domain Component (DC), a DNS domain. If the name contains a dot, such as `example.com`, it is written as two parts separated by a comma: `dc=example,dc=com.`
In this example, Common Name (CN) identifiers reside at the Organization Unit (OU) level, just below DC. The Distinguished Name (DN) is ou=People,dc=example,dc=com.

**Figure 1: LDAP object hierarchy**

In addition to the DN, the FortiGate unit needs an identifier for the individual person. Although the FortiGate unit GUI calls this the Common Name (CN), the identifier you use is not necessarily CN. On some servers, CN is the full name of a person. It might be more convenient to use the same identifier used on the local computer network. In this example, User ID (UID) is used.

**Locating your identifier in the hierarchy**

You need to determine the levels of the hierarchy from the top to the level that contain the identifier you want to use. This defines the DN that the FortiGate unit uses to search the LDAP database. Frequently used distinguished name elements include:

- **uid** (user identification)
- **pw** (password)
- **cn** (common name)
- **ou** (organizational unit)
- **o** (organization)
- **c** (country)

One way to test this is with a text-based LDAP client program. For example, OpenLDAP includes a client, `ldapsearch`, that you can use for this purpose.

Enter the following at the command line:

```
ldapsearch -x '(objectclass=*)'
```

The output is lengthy, but the information you need is in the first few lines:

```
version: 2
#
# filter: (objectclass=*)
# requesting: ALL

dn: dc=example,dc=com
dc: example
objectClass: top
objectClass: domain

 dn: ou=People,dc=example,dc=com
```

ou: People
objectClass: top
objectClass: organizationalUnit
...

dn: uid=tbrown,ou=People,dc=example,dc=com
uid: tbrown
cn: Tom Brown

In the output above, you can see tbrown (uid) and Tom Brown (cn). Also note the dn is ou=People, dc=example, dc=com.

### Configuring the FortiGate unit to use an LDAP server

After you determine the common name and distinguished name identifiers and the domain name or IP address of the LDAP server, you can configure the server on the FortiGate unit. The maximum number of remote LDAP servers that can be configured is 10.

One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see “Creating users” on page 74.

#### To configure the FortiGate unit for LDAP authentication - web-based manager

1. Go to User > Remote > LDAP and select Create New.
2. Enter a name for the LDAP server.
3. In Server Name/IP enter the server’s FQDN or IP address.
4. If the server does not use port 389, enter the port number in the Server Port field.
5. Enter the Common Name Identifier (20 characters maximum).
   - cn is the default, and is used by most LDAP servers.
6. In the Distinguished Name field, enter the base distinguished name for the server using the correct X.500 or LDAP format.
   - The FortiGate unit passes this distinguished name unchanged to the server. The maximum number of characters is 512.
   - If you don’t know the distinguished name, leave the field blank and select the Query icon to the right of the field. See the “Using the Query icon” on page 60.
7. In Bind Type, select Regular.
8. In User DN, enter the LDAP administrator’s distinguished name.
9. In Password, enter the LDAP administrator’s password.
10. Select OK.

To verify your Distinguished Name field is correct, you can select the Query icon. If your DN field entry is valid, you will see the part of the LDAP database it defines. If your DN field entry is not valid, it will display an error message and return no information.

For detailed information about configuration options for LDAP servers, see the Online Help on your FortiGate unit or the FortiGate CLI Reference.

#### To configure the FortiGate unit for LDAP authentication - CLI example

```
config user ldap
edit ourLDAPsrv
    set server 10.11.101.160
    set cnid cn
```
set dn cn=users,dc=office,dc=example,dc=com
set type regular
set username cn=administrator,cn=users,dc=office,dc=example,dc=com
set password w5AIgVMlkgyPQ
set password-expiry-warning enable
set password-renewal enable
end

**password-expiry-warning and password-renewal**

In SSLVPN, when an LDAP user is connecting to the LDAP server it is possible for them to receive any pending password expiry or renewal warnings. When the password renewal or expiry warning exists, SSLVPN users will see a prompt allowing them to change their password.

`password-expiry-warning` allows FortiOS to detect from the LDAP server when a password is expiring or has expired using server controls or error codes.

`password-renewal` allows FortiOS to perform the online LDAP password renewal operations the LDAP server expects.

On an OpenLDAP server, when a user attempts to logon with an expired password they are allowed to logon on but only to change their password.

When changing passwords on a Windows AD system, the connection must be SSL-protected.

**Using the Query icon**

The LDAP Distinguished Name Query list displays the LDAP directory tree for the LDAP server connected to the FortiGate unit. This helps you to determine the appropriate entry for the DN field. To see the distinguished name associated with the Common Name identifier, select the Expand icon next to the CN identifier. Select the DN from the list. The DN you select is displayed in the Distinguished Name field. Select OK and the Distinguished Name you selected will be saved in the Distinguished Name field of the LDAP Server configuration.

To see the users within the LDAP Server user group for the selected Distinguished Name, expand the Distinguished Name in the LDAP Distinguished Name Query tree.
Example — wildcard admin accounts - CLI

A wildcard admin account is an administrator account with the wildcard option enabled. This option allows multiple different remote administration accounts to match one local administration account, avoiding the need to set up individual admin accounts on the FortiGate unit. Instead multiple LDAP admin accounts will all be able to use one FortiGate admin account.

The initial benefit of wildcard admin accounts is fast configuration of the FortiGate unit's administration account to work with your LDAP network. The many to one ratio saves on effort, and potential errors.

The ongoing benefit is that as long as the users on the LDAP system belong to that group, and the test admin user settings don’t change on the FortiGate unit, no other work is required. This point is important as it can help avoid many system updates or changes that would otherwise require changes to the LDAP administrator account configuration. Even if a user is added to or removed from the LDAP group, no changes are required on the FortiGate unit.

Two potential issues with wildcard admin accounts are that multiple users may be logged on to the same account at the same time. This becomes an issue if they are changing the same information at the same time. The other potential issue is that security is reduced because multiple people have login access for the same account. If each user was assigned their own account, a hijacking of one account would not affect the other users.
Note that wildcard admin configuration also applies to RADIUS. When configuring for RADIUS, configure the RADIUS server, and RADUS user group instead of LDAP. When using web-based management, wildcard admin is the only type of remote administrator account that does not require you to enter a password on account creation. That password is normally used when the remote authentication server is unavailable during authentication.

In this example, default values are used where possible. If a specific value is not mentioned, it is set to its default value.

**Configuring the LDAP server**

The important parts of this configuration are the username and group lines. The username is the domain administrator account. The group binding allows only the group with the name GRP to access.

```plaintext
To configure LDAP server - CLI
config user ldap
  edit "ldap_server"
    set server "192.168.201.3"
    set cnid "sAMAccountName"
    set dn "DC=example,DC=com,DC=au"
    set type regular
    set username "CN=Administrator,CN=Users,DC=example,DC=COM"
    set password *
    set group "CN=GRP,OU=training,DC=example,DC=COM"
    set filter ""
next
end
```

```plaintext
To configure the user group and add the LDAP server - CLI
config user group
  edit "ldap_grp"
    set member "ldap"
  config match
    edit 1
      set server-name "ldap"
      set group-name "TRUE"
next
end
```

**Configuring the admin account**

The wildcard part of this example is only available in the CLI for admin configuration. When enabled, this allows all LDAP group members to login to the FortiGate unit without the need to create a separate admin account for each user. In effect the members of that group will each be able to login as “test”.

The `dn` used here is as an example only. On your network use your own domain name.
To configure the admin account - CLI

```
config system admin
  edit "test"
  set remote-auth enable
  set accprofile "super_admin"
  set wildcard enable
  set remote-group "ldap_grp"
next
end
```

For troubleshooting, test that the admin account is operational, and see “Troubleshooting LDAP” on page 64.

Example of LDAP to allow Dial-in through member-attribute - CLI

In this example, users defined in MicroSoft Windows Active Directory (AD) are allowed to setup a VPN connection simply based on an attribute that is set to TRUE, instead of based on being part of a specific group.

In AD, the "Allow Dial-In" property is activated in the user properties, and this sets the msNPAllowDialin attribute to "TRUE".

This same procedure can be used for other member attributes, as your system requires. This example works with FortiOS 4.0 MR2. The filter command was removed in FortiOS 4.0 MR3.

Configuring LDAP member-attribute settings

To accomplish this with a FortiGate unit, the member attribute must be set. Setting member attributes can only be accomplished through the CLI using the member-attr keyword - the option is not available through the web-based manager.

Before configuring the FortiGate unit, the AD server must be configured and have the msNPAllowDialin attribute set to "TRUE" for the users in question. If not, those users will not be able to properly authenticate.

The dn used here is as an example only. On your network use your own domain name.

To configure user LDAP member-attribute settings - CLI

```
config user ldap
  edit "ldap_server"
    set server "192.168.201.3"
    set cnid "sAMAccountName"
    set dn "DC=fortinet,DC=com,DC=au"
    set type regular
    set username "fortigate@example.com"
    set password ******
    set filter "(&(uid=%u)(msNPAllowDialin=TRUE))"
    set member-attr "msNPAllowDialin"
next
end
```

Configuring LDAP group settings

A user group that will use LDAP must be configured. This example adds the member ldap to the group which is the LDAP server name that was configured earlier.
To configure LDAP group settings - CLI

```plaintext
cfg user group
    edit "ldap_grp"
        set member "ldap"
    config match
        edit 1
            set server-name "ldap"
            set group-name "TRUE"
        next
        end
    next
    end
```

Once these settings are in place, users can authenticate.

Troubleshooting LDAP

The examples in this section use the values from the previous example.

**LDAP user test**

A quick way to see if the LDAP configuration is correct is to run a diagnose CLI command with LDAP user information. The following command tests with a user called `netAdmin` and a password of `fortinet`. If the configuration is correct the test will be successful.

```
FGT# diag test authserver ldap ldap_server netAdmin fortinet
```

If the configuration is not correct, the output will look similar to:

```
'ldap_server' is not a valid ldap server name — an LDAP server by that name has not been configured on the FortiGate unit, check your spelling.
authenticate 'netAdmin' against 'ldap_server' failed! — the user netAdmin does not exist on ldap_server, check your spelling of both the user and server and ensure the user has been configured on the FortiGate unit.
```

**LDAP authentication debugging**

For a more in-depth test, you can use a `diag debug` command. The sample output from a shows more information about the authentication process that may prove useful if there are any problems.

Ensure the "Allow Dial-in" attribute is still set to "TRUE" and run the following CLI command. `fnbamd` is the Fortinet non-blocking authentication daemon.

```
FGT# diag debug enable
FGT# diag debug reset
FGT# diag debug application fnbamd -1
FGT# diag debug enable
```

The output will look similar to:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups-attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='TRUE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Passed group matching
```

If the "Allow Dial-in" attribute is not set but it is expected, the last line of the above output will instead be:

```
fnbamd_auth_poll_ldap-Failed group matching
```
When users connect to their corporate network remotely, they do so through a remote access server. As remote access technology has evolved, the need for security when accessing networks has become increasingly important. This need can be filled using a Terminal Access Controller Access-Control System (TACACS+) server.

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ allows a client to accept a username and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies the user access to the network.

TACACS+ offers fully encrypted packet bodies, and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS’s UDP protocol.

There are several different authentication protocols that TACACS+ can use during the authentication process:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>Machine-independent technique that uses representations of English characters. Requires user to type a username and password that are sent in clear text (unencrypted) and matched with an entry in the user database stored in ASCII format.</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol (PAP) Used to authenticate PPP connections. Transmits passwords and other user information in clear text.</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge-Handshake Authentication Protocol (CHAP) Provides the same functionality as PAP, but is more secure as it does not send the password and other user information over the network to the security server.</td>
</tr>
<tr>
<td>MS-CHAP</td>
<td>MicroSoft Challenge-Handshake Authentication Protocol v1 (MSCHAP) Microsoft-specific version of CHAP.</td>
</tr>
<tr>
<td>default</td>
<td>The default protocol configuration, Auto, uses PAP, MS-CHAP, and CHAP, in that order.</td>
</tr>
</tbody>
</table>

**Configuring a TACACS+ server on the FortiGate unit**

A maximum of 10 remote TACACS+ servers can be configured for authentication.

One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see “Creating users” on page 74.

**To configure the FortiGate unit for TACACS+ authentication - web-based manager**

1. Go to User $>$ Remote $>$ TACACS+ and select Create New.
2. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name of the TACACS+ server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name/IP</td>
<td>Enter the server domain name or IP address of the TACACS+ server.</td>
</tr>
</tbody>
</table>
To configure the FortiGate unit for TACACS+ authentication - CLI

```
config user tacacs+
  edit <server_name>
    set auth-type {ascii | auto | chap | ms_chap | pap}
    set key <server_key>
    set tacacs+-port <tacacs+_port_num>
    set server <domain>
  end
```

**FSSO servers**

Novell and Microsoft Windows networks provide user authentication based on directory services: eDirectory for Novell, Active Directory for Windows. Users can log on at any computer in the domain and have access to resources as defined in their user account. The Fortinet Single Sign On (FSSO) agent enables FortiGate units to authenticate these network users for security policy or VPN access without asking them again for their username and password.

When a user logs in to the Windows or Novell domain, the FSSO agent sends the FortiGate unit the user's IP address and the names of the user groups to which the user belongs. The FortiGate unit uses this information to maintain a copy of the domain controller user group database. Because the domain controller authenticates users, the FortiGate unit does not perform authentication. It recognizes group members by their IP address.

In the FortiOS FSSO configuration, you specify the server where the FSSO Collector agent is installed. The Collector agent retrieves the names of the Novell or Active Directory user groups from the domain controllers on the domains, and then the FortiGate unit gets them from the Collector agent. You cannot use these groups directly. You must define FSSO type user groups on your FortiGate unit and then add the Novell or Active Directory user groups to them. The FSSO user groups that you created are used in security policies and VPN configurations to provide access to different services and resources.

FortiAuthenticator servers can replace the Collector agent when FSSO is using polling mode. The benefits of this is that FortiAuthenticator is a stand-alone server that has the necessary FSSO software pre-installed. For more information, see the [FortiAuthenticator Administration Guide](#).

For more information about Directory Services and FSSO, see “FSSO integration with Windows AD or Novell” on page 133.

**RSA ACE (SecurID) servers**

SecurID is a two-factor system that uses one-time password (OTP) authentication. It is produced by the company RSA. This system includes portable tokens carried by users, an RSA ACE/Server, and an Agent Host. In our configuration, the FortiGate unit is the Agent Host.
Components

When using SecurID, users carry a small device or “token” that generates and displays a random password. According to RSA, each SecurID authenticator token has a unique 64-bit symmetric key that is combined with a powerful algorithm to generate a new code every 60 seconds. The token is time-synchronized with the SecurID RSA ACE/Server.

The RSA ACE/Server is the management component of the SecurID system. It stores and validates the information about the SecurID tokens allowed on your network. Alternately the server could be an RSA SecurID 130 Appliance.

The Agent Host is the server on your network, in this case it is the FortiGate unit, that intercepts user logon attempts. The Agent Host gathers the user ID and password entered from their SecurID token, and sends that information to the RSA ACE/Server to be validated. If valid, a reply comes back indicating it is a valid logon and the FortiGate unit allows the user access to the network resources specified in the associated security policy.

Figure 3: RSA SecurID network diagram

Configuring the SecurID system

To use SecurID with a FortiGate unit, you need:
• to configure the RSA server and the RADIUS server to work with each other (see RSA server documentation)
• To configure the RSA SecurID 130 Appliance
  or
• To configure the FortiGate unit as an Agent Host on the RSA ACE/Server
• To configure the FortiGate unit to use the RADIUS server
• To create a SecurID user group and user
• To configure a security policy with SecurID authentication

The following instructions are based on RSA ACE/Server version 5.1, or RSA SecurID 130 Appliance, and assume that you have successfully completed all the external RSA and RADIUS server configuration steps listed above.

For this example, the RSA server is on the internal network, with an IP address of 192.128.100.100. The FortiGate unit internal interface address is 192.168.100.3; RADIUS shared secret is fortinet123, RADIUS server is at IP address 192.168.100.102.
To configure the RSA SecurID 130 Appliance
1. Go to the IMS Console for SecurID and logon.
2. Go to RADIUS > RADIUS Clients, and select Add New.
3. Enter the following information to configure your FortiGate as a SecurID Client, and select Save.

### RADIUS Client Basics

<table>
<thead>
<tr>
<th>Client Name</th>
<th>FortiGate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated RSA Agent</td>
<td>FortiGate</td>
</tr>
</tbody>
</table>

### RADIUS Client Settings

<table>
<thead>
<tr>
<th>IP Address</th>
<th>192.168.100.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make/Model</td>
<td>Select Standard Radius</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>fortinet123</td>
</tr>
<tr>
<td>Accounting</td>
<td>Leave unselected</td>
</tr>
<tr>
<td>Client Status</td>
<td>Leave unselected</td>
</tr>
</tbody>
</table>

To configure the FortiGate unit as an Agent Host on the RSA ACE/Server
1. On the RSA ACE/Server computer, go to Start > Programs > RSA ACE/Server, and then Database Administration - Host Mode.
2. On the Agent Host menu, select Add Agent Host.
3. Enter and save the following information.

<table>
<thead>
<tr>
<th>Name</th>
<th>FortiGate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>192.168.100.3</td>
</tr>
<tr>
<td>Secondary Nodes</td>
<td>Optionally enter other IP addresses that resolve to the FortiGate unit.</td>
</tr>
</tbody>
</table>

If needed, refer to the RSA ACE/Server documentation for more information.

To configure the FortiGate unit to use the RADIUS server
1. Go to User > Remote > RADIUS and select Create New.
2. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Query</td>
</tr>
<tr>
<td>Primary Server Address</td>
<td>192.168.100.102</td>
</tr>
<tr>
<td>Secondary Server Address</td>
<td>Optionally select Test to ensure the IP address is correct and the FortiGate can contact the RADIUS server.</td>
</tr>
</tbody>
</table>
To create a SecurID user group and user

1. Go to User > User Group, and select Create New.
2. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>RSA_group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Authentication servers</td>
<td>Select the RSA server.</td>
</tr>
</tbody>
</table>

3. Go to User > User, and select Create New.
4. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>User Name</th>
<th>wloman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match User on RADIUS server</td>
<td>RSA</td>
</tr>
<tr>
<td>Add this user to groups</td>
<td>Select RSA_group</td>
</tr>
</tbody>
</table>

To test this configuration, on your FortiGate unit use the CLI command:

diag test auth rad RSA auto w1oman 111111111

The series of 1s is the one time password that your RSA SecurID token generates and you enter.

**Using the SecurID user group for authentication**

You can use the SecurID user group in several FortiOS features that authenticate by user group including:

- Security policy
- IPsec VPN XAuth
- PPTP VPN
- SSL VPN

The following sections assume the SecurID user group is called securIDgrp and has already been configured. Unless otherwise states, default values are used.

**Security policy**

To use SecurID in a security policy, you must include the SecurID user group in an identity-based security policy. This procedure will create a security policy that allows HTTP, FTP, and POP3 traffic from the internal interface to wan1. If these interfaces are not available on your FortiGate unit, substitute other similar interfaces.

To configure a security policy with SecurID authentication

1. Go to Policy > Policy.
2. Select Create New.
3. Select internal for Source Interface/Zone.
Select wan1 for Destination Interface/Zone.

For both Source Address and Destination Address select all.

Select Enable identity-based Policy and select Add.

Move securIDgrp from the Available User Groups to the list on the right.

Move HTTP, FTP, and POP3 from Available Services to the list on the right.

Select OK.

You are returned to the security policy creation page, with the information you just entered in the identity-based policy (IBP) table as Rule ID 1.

Select OK.

The SecurID security policy is configured.

To generate usage reports on traffic authenticated with this policy, when you are adding the IBP rule, enable Log Traffic.

To either limit traffic or guarantee minimum bandwidth for traffic that uses the SecurID security policy, when you are adding the IBP rule, select traffic shaping and select one of the default shapers from the list such as guarantee-100kbps.

To customize any challenge pages or logon pages users will see when authenticating against this security policy, select Customize Authentication Messages and select the icon that appears. This takes you to the Edit Message page where you can customize the login challenge page, login failed page, and others.

For more details on configuring security policies, see the FortiOS Handbook FortiGate Fundamentals guide.

**IPsec VPN XAuth**

Extended Authentication (XAuth) increases security by requiring additional user authentication information in a separate exchange at the end of the VPN Phase 1 negotiation. If the SecurID user group is used, this extended information will require users to enter their SecurID code. For more on XAuth, see “Configuring XAuth authentication” on page 109.

This Phase 1 configuration will be named securIDxAuth and it will connect with IP address 10.11.101.155 on the wan1 interface.

To configure IPsec VPN XAuth with SecurID authentication - web-based manager

1. Go to VPN > IPsec > Auto Key (IKE).
2. Select Create Phase 1.
3. Enter securIDxAuth for Name.
5. Select Preshared Key for Authentication Method.
6. Enter fortinet for the Pre-shared Key.
7. Select Advanced.
8. For XAuth, select Enable as Server.
9. Select AUTO for Server Type.
10. Select securIDgrp for User Group.
11. Select OK.
**PPTP VPN**

PPTP VPN is configured in the CLI. In the PPTP configuration (`config vpn pptp`), set `usrgrp` to the SecurID user group.

**SSL VPN**

In the SecurID user group, select the appropriate web portal for these users. In the security policy for the SSL VPN, include the SecurID user group in the list of selected user groups.
Users and user groups

FortiGate authentication controls system access by user group. By assigning individual users to the appropriate user groups you can control each user’s access to network resources. The members of user groups are user accounts, of which there are several types. Local users and peer users are defined on the FortiGate unit. User accounts can also be defined on remote authentication servers.

This section describes how to configure local users and peer users and then how to configure user groups. For information about configuration of authentication servers see “Authentication servers” on page 51.

This section contains the following topics:
- Users
- User groups

Users

A user is a user account consisting of username, password, and in some cases other information, configured on the FortiGate unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group. There are several different types of user accounts with slightly different methods of authentication:

<table>
<thead>
<tr>
<th>User type</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local user, password stored on the FortiGate unit</td>
<td>The username and password must match a user account stored on the FortiGate unit. Authentication by FortiGate security policy.</td>
</tr>
<tr>
<td>Local user, password stored on a remote server</td>
<td>The username must match a user account stored on the FortiGate unit and the username and password must match a user account stored on the remote authentication server.</td>
</tr>
<tr>
<td>Authentication server user</td>
<td>A FortiGate user group can include user accounts or groups that exist on a remote authentication server.</td>
</tr>
<tr>
<td>FSSO user</td>
<td>With Fortinet Single Sign On (FSSO), users on a Microsoft Windows or Novell network can use their network authentication to access resources through the FortiGate unit. Access is controlled through FSSO user groups which contain Windows or Novell user groups as their members.</td>
</tr>
<tr>
<td>Peer user with certificate authentication</td>
<td>A peer user is a digital certificate holder that authenticates using a client certificate. No password is required, unless two-factor authentication is enabled.</td>
</tr>
</tbody>
</table>

This section includes:
- Local users
- PKI or peer users
Local users

Local users are defined on the FortiGate unit. To define a local user you need:

- a username
- a password or the name of the authentication server that contains the user account

If the user is authenticated externally, the username on the FortiGate unit must be identical to the username on the authentication server. You may also still be prompted for a password. If the connection to the remote authentication server is interrupted during authentication the local password will be used if it exists to ensure access.

Local users are authenticated through authentication security policies. See this section includes:

- Creating users
- Removing users
- Removing references to users

Creating users

Before configuring any authentication, except dynamic profiles, you must first create local users. For more about dynamic profiles, see “Configuring dynamic profile” on page 182.

When creating a new user, there are only two differences between a local and a remote user:

- local users require a password to be configured
- remote users do not require a password, but do require a remote authentication server to be configured

To create a local user - web-based manager

1. Go to User > User and select Create New.
2. Enter the username in the username field.
   - Select Password and type a password. Best practices dictate that the password be at least six characters long.

To authenticate this user using an external authentication server, select the Match user option for the appropriate type of server and select the server name. Password is not required. You must configure the remote server access first. See “Authentication servers” on page 51.
3 Optionally select *Enable Two-factor Authentication* to use that option with this user. When enabled, additional options will be displayed. Select one of the following options and configure it as stated.

- Select *FortiToken*, and choose the FortiToken serial number to associate with this user.
- Select *Email to* and enter the user’s email address to email them the token code.
- Select *SMS* and enter the Mobile Provider from the list, and enter the user’s mobile phone number that will receive the token code in a text message.

4 Select **OK**.

---

The Mobile Provider for SMS must be entered in the CLI using the `config user sms-provider` command before it will be available to select in the web-based manager.

---

**To create a local user - CLI examples**

**Locally authenticated user**

```bash
config user local
  edit user1
    set type password
    set passwd ljt_pj2gpepfdw
  end
```

**User authenticated on an LDAP server**

```bash
config user local
  edit user2
    set type ldap
    set ldap_server ourLDAPsvr
  end
```

**User authenticated on a RADIUS server**

```bash
config user local
  edit user3
    set type radius
    set radius_server ourRADIUSsvr
  end
```

**User authenticated on a TACACS+ server**

```bash
config user local
  edit user4
    set type tacacs+
    set tacacs+_server ourTACACS+svr
  end
```

**User authenticated with a FortiToken**

```bash
config user local
  edit user5
    set type password
    set passwd ljt_pj2gpepfdw
    set two_factor fortitoken
    set fortitoken 182937197
  end
```
User authenticated using email

```fortios
config user local
edit user6
    set type password
    set passwd ljt_pj4h7epfdw
    set two_factor email
    set email-to user6@sample.com
end
```

User authenticated using SMS text message

```fortios
config user sms-provider
edit “Sample Mobile Inc”
    set mail-server mail.sample.com
end
```

```fortios
config user local
edit user7
    set type password
    set passwd 3ww_pjt68dw
    set two_factor sms
    set sms-provider “Sample Mobile Inc”
    set sms-phone 2025551234
end
```

Removing users

Best practices dictate that when a user account is no longer in use, it be deleted. Removing local and remote users from FortiOS involve the same steps.

If the user account is references by any configuration objects those references must be removed before the user can be deleted. See “Removing references to users” on page 76.

To remove a user from the FortiOS configuration - web-based manager

1. Go to User > User.
2. Select the check box of the user that you want to remove.
3. Select Delete.
4. Select OK.

To remove a user from the FortiOS configuration - CLI example

```fortios
config user local
    delete user4444
end
```

Removing references to users

You cannot remove a user that belongs to a user group. Remove the user from the user group first, and then delete the user.

To remove references to a user - web-based manager

1. Go to User > User > User.
2. If the number in the far right column for the selected user contains any number other than zero, select it.
A more detailed list of object references to this user is displayed. Use its information to find and remove these references to allow you to delete this user.

**PKI or peer users**

A PKI, or peer user, is a digital certificate holder. A PKI user account on the FortiGate unit contains the information required to determine which CA certificate to use to validate the user’s certificate. Peer users can be included in firewall user groups or peer certificate groups used in IPsec VPNs. For more on certificates, see “Certificates overview” on page 114.

To define a peer user you need:
- a peer username
- the text from the subject field of the user’s certificate, or the name of the CA certificate used to validate the user’s certificate

**Creating a peer user**

The configuration page for PKI users in the web-based manager is not available unless there is at least one peer user defined. Follow the CLI-based instructions to create the first peer user. Optionally, you can then logon to the web-based manager to configure additional PKI (peer) users.

**To create a peer user for PKI authentication - CLI example**

```
config user peer
edit peer1
  set subject E=peer1@mail.example.com
  set ca CA_Cert_1
end
```

**To create a peer user for PKI authentication - web-based manager**

1. Go to *User > PKI* and select *Create New*.
2. Enter the user name.
3. Fill in at least one of the following fields:

<table>
<thead>
<tr>
<th>Subject</th>
<th>The text string that appears in the Subject field of the user’s certificate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Select the CA certificate that must be used to authenticate this peer user.</td>
</tr>
</tbody>
</table>

4. Optionally you can select Two-factor authentication. See “Two-factor authentication” on page 78.
5. Select *OK*.

There are other configuration settings that can be added or modified for PKI authentication. For example, you can configure the use of an LDAP server to check access rights for client certificates. For information about the detailed PKI configuration settings only available through the CLI, see the *FortiGate CLI Reference*.
Two-factor authentication

The standard logon requires a username and password. This is one factor authentication—your password is one piece of information you need to know to gain access to the system.

Two factor authentication adds the requirement for another piece of information for you logon. Generally the two factors are something you know (password) and something you have (certificate, token, etc.). This makes it harder for a hacker to steal your logon information. For example if you have a FortiToken device, the hacker would need to both use it and know your password to gain entry to your account.

Two-factor authentication is available on both user and admin accounts. But before you enable two-factor authentication on an administrator account, you need to ensure you have a second administrator account configured to guarantee administrator access to the FortiGate unit if you are unable to authenticate on the main admin account for some reason.

The methods of two-factor authentication include:

- Certificate
- Email
- SMS
- FortiToken

Certificate

You can increase security by requiring both certificate and password authentication for PKI users. Certificates are installed on the user’s computer. Requiring a password also protects against unauthorized use of that computer.

Optionally peer users can enter the code from their FortiToken instead of the certificate.

To create a peer user with two-factor authentication - web-based manager

While configuring a peer user (see “PKI or peer users” on page 77), select Require two-factor authentication and enter a password.

To create a peer user with two-factor authentication - CLI example

```
config user peer
  edit peer1
    set subject E=peer1@mail.example.com
    set ca CA_Cert_1
    set two-factor enable
    set passwd fdktguefheygfe
  end
```

For more information on certificates, see “Certificates overview” on page 114.

Email

Two-factor email authentication sends a randomly generated six digit numeric code to the specified email address. Enter that code when prompted at logon. This token code is valid for 60 seconds. If you enter this code after that time, it will not be accepted.
A benefit is that you do not require mobile service to authenticate. However, a potential issue is if your email server does not deliver the email before the 60 second life of the token expires.

The code will be generated and emailed at the time of logon, so you must have email access at that time to be able to receive the code.

**To enable email two-factor authentication - web-based manager**

1. Go to the email server under `Log&Report->Log Config->Alert e-mail`.
2. Enter the SMTP Server and Email from address.
3. If applicable, enable Authentication on the SMTP server and enter the SMTP username and password to use.
4. Select Apply.
5. To modify an administrator account, go to `System > Admin > Administrators`. To modify a user account go to `User > User`.
6. Select an existing account or select Create New.
7. Select `Enable Two-factor Authentication`.
8. Select Email to.
9. Enter the email address.
10. Select OK.

**SMS**

SMS two-factor authentication sends the token code in an SMS text message to the mobile device indicated when this user attempts to logon. This token code is valid for 60 seconds. If you enter this code after that time, it will not be accepted. Enter this code when prompted at logon to be authenticated.

SMS two-factor authentication has the benefit that you do not require email service before logging on. A potential issue is if the mobile service provider does not send the SMS text message before the 60 second life of the token expires.

Before configuring SMS, you must configure the email server for sending email from the FortiGate unit and one or more SMS providers in the CLI.

**To configure the SMTP email address for your FortiGate unit - web-based manager**

1. Go to the email server under `Log&Report->Log Config->Alert e-mail`.
2. Enter the `SMTP Server` and `Email from` address.
3. If applicable, enable Authentication on the SMTP server and enter the SMTP username and password to use.
4. Select Apply.

**To configure an SMS provider - CLI**

```bash
config user sms-provider
  edit <provider_name>
    set mail-server <server_email>
  next
end
```
To configure SMS two-factor authentication - web-based manager

1. To modify an:
   - administrator account, go to System > Admin > Administrators, or
   - user account go to User > User.
2. Select an existing account or select Create New.
4. Select SMS.
5. Choose the SMS provider from the drop down list.
6. Enter the phone number of the mobile device that will receive the SMS text messages.

If you have problems receiving the token codes via SMS messaging, contact your mobile provider to ensure you are using the correct phone number format to receive text messages and that your current mobile plan allows text messages.

FortiToken

FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's username and password as two-factor authentication. The code displayed changes every 60 seconds, and when not in use the LCD screen is blanked to extend the battery life.

FortiTokens have a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. Do not put the FortiToken on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and must be treated with similar care.

Any time information about the FortiToken is transmitted, it is encrypted. When the FortiGate unit receives the code that matches the serial number for a particular FortiToken, it is delivered and stored encrypted. This is in keeping with the Fortinet's commitment to keeping your network highly secured.

FortiTokens can be added to user accounts that are local, IPSec VPN, SSL VPN, and even Administrators. See "Associating FortiTokens with accounts" on page 83.

A FortiToken can only be associated with one account at a time on a FortiGate unit. However, multiple FortiGate units can have the same FortiToken registered. This is useful for employees who travel between offices.

If a user loses their FortiToken, it can be locked out using the FortiGate so it will not be used to falsely access the network. Later if found, that FortiToken can be unlocked on the FortiGate to allow access once again. See "FortiToken maintenance" on page 84.

There are three tasks to complete before FortiTokens can be used to authenticate accounts:

1. Adding FortiTokens to the FortiGate
2. Activating a FortiToken on the FortiGate
3. Associating FortiTokens with accounts

The FortiToken authentication process

The steps during FortiToken two-factor authentication are as follows.

1. User attempts to access a network resource.
2 FortiGate unit matches the traffic to an authentication security policy, and FortiGate unit prompts the user for username and password.

3 User enters their username and password.

4 FortiGate unit verifies their information, and if valid prompts the user for the FortiToken code.

5 User gets the current code from their FortiToken device.

6 User enters current code at the prompt.

7 FortiGate unit verifies the FortiToken code, and if valid allows access to the network resources such as the Internet.

The following steps are only if the time on the FortiToken has drifted from the time on the FortiGate unit and needs to be synchronized.

8 If time on FortiToken has drifted, FortiGate unit will prompt user to enter a second code to confirm.

9 User gets the next code from their FortiToken device.

10 User enters the second code at the prompt.

11 FortiGate unit uses both codes to update its clock to match the FortiToken and then proceeds as in step 7.

**Figure 4: FortiToken authentication process**

When configured the FortiGate unit accepts the username and password, authenticates them either locally or remotely, and prompts the user for the FortiToken code. The FortiGate then authenticates the FortiToken code. When FortiToken authentication is enabled, the prompt field for entering the FortiToken code is automatically added to the authentication screens.
Even when an Administrator is logging in through a serial or Telnet connection and their account is linked to a FortiToken, that Administrator will be prompted for the token’s code at each login.

If you have attempted to add invalid FortiToken serial numbers, there will be no error message. The serial numbers will simply not be added to the list.

Adding FortiTokens to the FortiGate

Before one or more FortiTokens can be used to authenticate logons, they must be added to the FortiGate. The import feature is used to enter many FortiToken serial numbers at one time.

One FortiToken can be added to multiple FortiGate units. This is useful for maintaining two-factor authentication for employees over multiple office locations, such as for employees who travel frequently between offices.

To manually add a FortiToken to the FortiGate - web-based manager

1. Go to User > FortiToken > FortiToken.
2. Select Create New.
3. Enter one or more serial numbers for the FortiToken or FortiTokens you have.
4. Select OK.

To import multiple FortiTokens to the FortiGate - web-based manager

1. Go to User > FortiToken > FortiToken.
2. Select Import.
3. Browse to the local file location on your local computer.
   - The file must be a text file with one FortiToken serial number per line.
4. Select OK.

To add two FortiTokens to the FortiGate - CLI

```
config user fortitoken
edit <serial_number>
next
edit <serial_number2>
next
end
```

Activating a FortiToken on the FortiGate

Once one or more FortiTokens have been added to the FortiGate unit, they must be activated before being available to be associated with accounts. The process of activation involves the FortiGate querying FortiGuard servers about the validity of each FortiToken. The serial number and information is encrypted before it is sent for added security.

A FortiGate unit requires a connection to FortiGuard servers to activate a FortiToken.
To activate a FortiToken on the FortiGate unit - web-based manager

1. Go to User > FortiToken.
2. Select one or more FortiTokens with a status of New.
3. Select Activate.
4. Refresh web browser. The status of selected FortiTokens will change to Activated.

The selected FortiTokens are now available for use with user and admin accounts.

To activate a FortiToken on the FortiGate unit - CLI

```
config user fortitoken
   edit <token_serial_num>
      set status activate
   next
end
```

Associating FortiTokens with accounts

The final step before using the FortiTokens to authenticate logons is associating a FortiToken with an account. The accounts can be local user or administrator accounts.

To add a FortiToken to a local user account - web-based manager

1. Ensure that your FortiToken serial number has been added to the FortiGate successfully, and its status is Activated.
2. Go to User > User, and select Create New.
3. Enter the username and password for this user account.
4. Select Enable Two-factor Authentication.
5. Select FortiToken, and select the serial number from the list that matches that user’s FortiToken.
6. Select OK.

To add a FortiToken to a local user account - CLI

```
config user local
   edit <username>
      set type password
      set passwd "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set status enable
   next
end
```

To add a FortiToken to an administrator account - web-based manager

1. Ensure that your FortiToken serial number has been added to the FortiGate successfully, and its status is Activated.
2. Go to System > Admin > Administrators, and select an admin account.
   This account is assumed to be configured except for two-factor authentication.
4. Select FortiToken, and select the serial number from the list that matches that user’s FortiToken.
5 Select OK.

**To add a FortiToken to a local user account - CLI**

```plaintext
config user local
  edit <username>
    set type password
    set passwd "myPassword"
    set two-factor fortitoken
    set fortitoken <serial_number>
    set status enable
next
end
```

The `fortitoken` keyword will not be visible until `fortitoken` is selected for the two-factor keyword.

---

**FortiToken maintenance**

Once FortiTokens are entered into the FortiGate unit, there are only two tasks to maintain them — changing the status,

**To change the status of a FortiToken between Activated and Locked - CLI**

```plaintext
config user fortitoken
  edit <token_serial_num>
    set status lock
next
end
```

Any user attempting to login using this FortiToken will not be able to authenticate.

**To list the drift on all FortiTokens configured on this FortiGate unit - CLI**

```plaintext
# diag fortitoken drift
FORTITOKEN        DRIFT
```

This command lists the serial number and drift for each FortiToken configured on this FortiGate unit. This command is useful to check if it is necessary to synchronize the FortiGate and any particular FortiTokens.

---

**Monitoring users**

To monitor user activity in the web-based manager, go to **Users > Monitor > Firewall**. The list of users who are logged on is displayed with some information about them such as their user group, security policy ID, how long they have been logged on, their IP address, traffic volume, and their authentication method as one of FSSO, NTLM, or firewall (FW-auth).

From this screen you can de-authenticate all users who are logged on. The de-authenticate button is at the top left of this screen.
To see information about banned users go to User > Monitor > Banned Users. Displayed information about users who have been banned includes what application the triggered the ban (Application Protocol), the reason for the ban (Cause or rule), Created, and when the ban expires.

**Filtering the list of users**

When there are many users logged on, it can be difficult to locate a specific user or multiple users to analyze. Applying filters to the list allows you to organize the user list to meet your needs, or only display some the users that meet your current requirements.

Select Column Settings at the bottom of the screen to adjust columns that are displayed for users, including what order they are displayed in. This can be very helpful in locating information you are looking for.

The username column includes a green arrow to the right of the title. Select this arrow to sort the list of users by ordering them in ascending (down arrow) or descending order. This is the only column that allows this.

Each column heading has a grey filter icon. Click on the filter icon to configure a filter for the data displayed in that column. Each column has similar options including a field to enter the filtering information, a checkbox to select the negative of the text in the field, and the options to add more fields, apply the filter, clear all filters, or cancel without saving. To enter multiple terms in the field, separate each of them with a comma. To filter entries that contain a specific prefix, use an * (asterisk).

When removing existing filters, you must select Apply for the removal to take place.

For example, to create a filter to display only users with an IP address of 10.11.101.x who authenticated using one of security policies five through eight, and who belong to the user group Accounting.

**To configure a user monitor filter - web-based manager**

1. Go to User > Monitor > Firewall.
2. Select filter icon for IP address.
3. Enter 10.11.101.0.
4. Select Add new filter.
5. From the list of fields select Policy ID and enter 5-8.
6. Select Add new filter.
7. From the list of fields select User Group and enter Accounting.
8. Select Apply.

**User groups**

A user group is a list of user identities. An identity can be:
- a local user account (username/password) stored on the FortiGate unit
- a local user account with the password stored on a RADIUS, LDAP, or TACACS+ server
- a PKI user account with digital client authentication certificate stored on the FortiGate unit
User groups

- a RADIUS, LDAP, or TACACS+ server, optionally specifying particular user groups on that server
- a user group defined on an FSSO server.

Identity-based policies and some types of VPN configurations allow access to specified user groups only. This restricted access enforces Role Based Access Control (RBAC) to your organization’s network and its resources. Users must be in a group and that group must be part of the security policy.

You cannot change the type of a group unless the group is empty.

In most cases, the FortiGate unit authenticates users by requesting their username and password. The FortiGate unit checks local user accounts first. If a match is not found, the FortiGate unit checks the RADIUS, LDAP, or TACACS+ servers that belong to the user group. Authentication succeeds when a matching username and password are found. If the user belongs to multiple groups on a server, those groups will be matched as well.

FortiOS does not allow username overlaps between RADIUS, LDAP, or TACACS+ servers.

There are two types of FortiGate user groups: Firewall user groups, and FSSO user groups.

Firewall user groups

Firewall user groups are used locally as part of authentication and can contain any type of user identity except an FSSO group. When a user attempts to access resources controlled by an Identity-Based Policy (IBP), the FortiGate unit requires authentication from that user. If the user authenticates successfully and is a member of one of the permitted groups, the session is allowed to proceed.

This section includes:
- SSL VPN access
- IPsec VPN access
- Configuring a firewall user group
- User group timeouts
- Viewing, editing and deleting user groups

SSL VPN access

In any firewall user group, you can enable SSL VPN access and select the web-portal that the users can access. When the user connects to the FortiGate unit via HTTPS on the SSL VPN port (default 10443), the FortiGate unit requests a username and password.

SSL VPN access also requires an SSL VPN security policy (Action is SSL VPN) with an identity-based rule enabling access for the user group. For more information, see the FortiOS Handbook SSL VPN guide.
IPsec VPN access

A firewall user group can provide access for dialup users of an IPsec VPN. In this case, the IPsec VPN phase 1 configuration uses the **Accept peer ID in dialup group peer** option. The user’s VPN client is configured with the username as peer ID and the password as pre-shared key. The user can connect successfully to the IPsec VPN only if the username is a member of the allowed user group and the password matches the one stored on the FortiGate unit.

A user group cannot be used as a dialup group if any member of the group is authenticated using an external authentication server.

For more information, see the FortiOS Handbook IPsec VPN guide.

Configuring a firewall user group

A user group can contain:

- local users, whether authenticated by the FortiGate unit or an authentication server
- PKI users
- authentication servers, optionally specifying particular user groups on the server

To create a Firewall user group - web-based manager

1. Go to User > User Group and select Create New.
2. Enter a name for the user group.
3. In Type, select Firewall.
4. From the Available Users list, select users and then select the right arrow button to move the names to the Members list.

   If you select an authentication server as a group member, by default all user accounts on the authentication server are members of this FortiGate user group. Follow steps 5 through 8 if you want to include only specific user groups from the authentication server. Otherwise, select OK.

5. Select Add.
6. To add a remote authentication server, select Add and select the authentication server from the drop down Remote Server list.

   The option to add remote servers is available only if at least one remote server has been configured.

7. In the Group Name field, either select Any to match all possible groups, or select Specify and enter the group name in the appropriate format for the type of server.

   For example, an LDAP server requires LDAP format, such as: cn=users, dn=office, dn=example, dn=com

8. Repeat steps 5 through 7 to add all the authentication server user groups that are required.

9. Select OK.

To create a firewall user group - CLI example

In this example, the members of accounting_group are User1 and all of the members of rad_accounting_group on myRADIUS external RADIUS server.
User groups

Multiple group enforcement support

Previously, when a user belonged to multiple user groups, this user could only access the group services that were within one group. With multiple group enforcement, a user can access the services within the groups that the user is part of.

For example, userA belongs to user_group1, user_group2, user_group3, and user_group4; previously userA could only access services within one of those four groups, typically the group that matches the first security policy. This can be annoying if HTTP access is in user_group1, FTP access is in user_group2, and email access is in user_group3. Now userA can access services within user_group1, user_group2, user_group3, and user_group4.

This feature is available only in the CLI and is enabled by default. It applies to RADIUS, LDAP, and TACACS+ servers. The new command for this feature is `auth-multi-group` found in `config user settings` and checks all groups a user belongs to for authentication.

User group timeouts

User groups can have timeout values per group in addition to FortiGate-wide timeouts. There are essentially three different types of timeouts that are configurable for user authentication on the FortiGate unit — idle timeout, hard timeout, and session timeout. These are in addition to any external timeouts such as those associated with RADIUS servers.
If VDOMs are enabled, the global level user setting `authtimeout` is the default all VDOMs inherit. If VDOMs are not enabled, user settings `authtimeout` is the default. The default timeout value is used when the `authtimeout` keyword for a user group is set to zero.

Each type of timeout will be demonstrated using the existing user group `example_group`. Timeout units are minutes. A value of zero indicates the global timeout is used.

### Membership in multiple groups

When a user belongs to multiple groups in RADIUS groups, the group auth-timeout values are ignored. Instead the global timeout value is used. The default value is 5 minutes, but it can be set from 1 to 480 minutes.

```
config user settings
  set auth-timeout-type idle-timeout
  set auth-timeout 300
end
```

#### Idle timeout

The default type of timeout is idle timeout. When a user initiates a session, it starts a timer. As long as data is transferred in this session, the timer continually resets. If data flow stops, the timer is allowed to advance until it reaches its limit. At that time the user has been idle for too long, and the user is forced to re-authenticate before traffic is allowed to continue in that session.

**To configure user group authentication idle timeout - CLI**

```
config user settings
  set auth-timeout-type idle-timeout
end

config user group
  edit example_group
    set auth-timeout 480
    next
end
```

#### Hard timeout

Where the idle timeout is reset with traffic, the hard timeout is absolute. From the time the first session a user establishes starts, the hard timeout counter starts. When the timeout is reached, all the sessions for that user must be re-authenticated. This timeout is not affected by any event.

**To configure user group authentication hard timeout - CLI**

```
config user settings
  set auth-timeout-type hard-timeout
end
config user group
  edit example_group
    set auth-timeout 480
    next
```
Session timeout
The session timeout works much like the hard timeout in that its an absolute timer that can not be affected by events. However, when the timeout is reached existing sessions may continue but new sessions are not allowed until re-authentication takes place. The timeout can be set from 1 to 480 minutes. Setting the timeout value to zero removes the timeout value allowing the user to remain logged on without limit.

To configure a user group authentication new session hard timeout - CLI

```plaintext
config user setting
    set auth-timeout-type new-session
end

config user group
    edit example_group
        set authtimeout 30
    next
end
```

FSSO user groups
FSSO user groups are part of FSSO authentication and contain only Windows or Novell network users. No other user types are permitted as members. Information about the Windows or Novell user groups and the logon activities of their members is provided by the Fortinet Single Sign On (FSSO) which is installed on the network domain controllers.

You can specify FSSO user groups in identity-based security policies in the same way as you specify firewall user groups. FSSO user groups cannot have SSL VPN or dialup IPsec VPN access.

For information about configuring FSSO user groups, see “Creating Fortinet Single Sign-On (FSSO) user groups” on page 162. For complete information about installing and configuring FSSO, see “FSSO integration with Windows AD or Novell” on page 133.

Configuring Peer user groups
Peer user groups can only be configured using the CLI. Peers are digital certificate holders defined using the `config user peer` command. The peer groups you define here are used in dialup IPsec VPN configurations that accept RSA certificate authentication from members of a peer certificate group. For more information, see “Authenticating IPsec VPN users with security certificates” on page 126.

To create a peer group - CLI example

```plaintext
config user peergrp
    edit vpn_peergrp1
        set member pki_user1 pki_user2 pki_user3
    end
```

Viewing, editing and deleting user groups
To view the list of FortiGate user groups, go to User > User Group.
Editing a user group

When editing a user group in the CLI you must set the type of group this will be — either a firewall group, or a Fortinet Single Sign-On Service group. Once the type of group is set, and members are added you cannot change the group type without removing the members.

In the web-based manager, if you change the type of the group any members will be removed automatically.

To edit a user group - web-based manager
2. Select the check box for the user group that you want to edit.
3. Select the Edit button.
4. Modify the user group as needed.
5. Select OK.

To edit a user group - CLI example
This example adds user3 to Group1. Note that you must re-specify the full list of users:

```
config user group
edit Group1
set group-type firewall
    set member user2 user4 user3
end
```

Deleting a user group

Before you delete a user group, you must ensure there are no objects referring to it such as security policies. If there are, you must remove those references before you are able to delete the user group.

To remove a user group - web-based manager
2. Select the check box for the user group that you want to remove.
3. Select the Delete button.
4. Select OK.

To remove a user group - CLI example

```
config user group
    delete Group2
end
```
Configuring authenticated access

When you have configured authentication servers, users, and user groups, you are ready to configure security policies and certain types of VPNs to require user authentication.

This section describes:
- Authentication timeout
- Password policy
- Authentication protocols
- Authentication in security policies
- VPN authentication

Authentication timeout

An important feature of the security provided by authentication is that it is temporary—a user must re-authenticate after logging out. Also if a user is logged on and authenticated for an extended period of time, it is a good policy to have them re-authenticate at set periods. This ensures a user's session is cannot be spoofed and used maliciously for extended periods of time — re-authentication will cut any spoof attempts short. Shorter timeout values are more secure.

Security authentication timeout

You set the security user authentication timeout to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 480 minutes (8 hours).

To set the security authentication timeout - web-based manager

1. Go to User > User > Authentication.
2. Enter the Authentication Timeout value in minutes.
   The default authentication timeout is 5 minutes.
3. Select Apply.

SSL VPN authentication timeout

You set the SSL VPN user authentication timeout (Idle Timeout) to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 28 800 seconds. The default timeout is 300 seconds.

To set the SSL VPN authentication timeout - web-based manager

1. Go to VPN > SSL > Config.
2. Enter the Idle Timeout value (seconds).
3. Select Apply.
Password policy

Password authentication is effective only if the password is sufficiently strong and is changed periodically. By default, the FortiGate unit requires only that passwords be at least eight characters in length. You can set a password policy to enforce higher standards for both length and complexity of passwords. Password policies can apply to administrator passwords or IPsec VPN preshared keys.

To set a password policy in the web-based manager, go to System > Admin > Settings. In the CLI, use the config system password-policy command.

The default minimum password length on the FortiGate unit is eight characters, but up to 32 characters is permitted. Fortinet suggests a minimum length of 14 characters.

Users usually create passwords composed of alphabetic characters and perhaps some numbers. Password policy can require the inclusion of uppercase letters, lowercase letters, numerals or punctuation characters.

Configuring password minimum requirement policy

Best practices dictate that passwords include:

• one or more uppercase characters
• one or more lower case characters
• one or more of the numerals
• one or more non alphanumeric characters, such as punctuation marks.

The minimum number of each of these types of characters can be set in both the web-based manager and the CLI.

The following procedures show how to force administrator passwords to contain at least two uppercase, four lower case, two digits, and one non-alphanumeric characters. Leave the minimum length at the default of eight characters.

To change administrator password minimum requirements - web-based manager

1 Go to System > Admin > Settings.
2 Select Enable Password Policy.
3 Select Must Contain.
4 Enter the following information:

<table>
<thead>
<tr>
<th>Type</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uppercase Letters</td>
<td>2</td>
</tr>
<tr>
<td>Lower case Letters</td>
<td>4</td>
</tr>
<tr>
<td>Numerical Digits</td>
<td>2</td>
</tr>
<tr>
<td>Non-alphanumeric Letters</td>
<td>1</td>
</tr>
</tbody>
</table>

5 Under Apply Password Policy to, select Admin Password.
6 Select Apply.

To change administrator password minimum requirements - CLI

```
config system password-policy
set status enable
set apply-to admin-password
set min-upper-case-letter 2
set min-lower-case-letter 4
```
set min-number 2
set min-non-alphanumeric 1
set change-4-characters enable
next
end

The `change-4-characters` option forces new passwords to change a minimum of four characters in the old password. Changing fewer characters results in the new password being rejected. This option is only available in the CLI.

**Password best practices**

In addition to length and complexity, there are security factors that cannot be enforced in a policy. Guidelines issued to users will encourage proper password habits.

Best practices dictate that password expiration also be enabled. This forces passwords to be changed on a regular basis. You can set the interval in days. The more sensitive the information this account has access to, the shorter the password expiration interval should be. For example 180 days for guest accounts, 90 days for users, and 60 days for administrators.

Avoid:

- real words found in any language dictionary
- numeric sequences, such as “12345”
- sequences of adjacent keyboard characters, such as “qwerty”
- adding numbers on the end of a word, such as “hello39”
- adding characters to the end of the old password, such as “hello39” to “hello3900”
- repeated characters
- personal information, such as your name, birthday, or telephone number.

**Maximum logon attempts and blackout period**

When you logon and fail to enter the correct password you could be a valid user, or a hacker attempting to gain access. For this reason, best practices dictate to limit the number of failed attempts to logon before a blackout period where you cannot logon.

To set a maximum of five failed authentication attempts before the blackout, using the following CLI command:

```plaintext
config user setting
set auth-invalid-max 5
next
end
```

To set the length of the blackout period to five minutes, or 300 seconds, once the maximum number of failed logon attempts has been reached, use the following CLI command:

```plaintext
config user setting
set auth-blackout-time 300
next
end
```
Authentication protocols

When user authentication is enabled on a security policy, the authentication challenge is normally issued for any of the four protocols, HTTP, HTTPS, FTP, and Telnet, which are dependent on the connection protocol. By making selections in the Protocol Support list, the user controls which protocols support the authentication challenge. The user must connect with a supported protocol first, so that they can subsequently connect with other protocols.

For example, if you have selected HTTP, FTP, or Telnet, a username and password-based authentication occurs. The FortiGate unit then prompts network users to input their security username and password. If you have selected HTTPS, certificate-based authentication (HTTPS, or HTTP redirected to HTTPS only) occurs.

For certificate-based authentication, you must install customized certificates on the FortiGate unit and on the browsers of network users. If you do not install certificates on the network user’s web browser, the network users may see an SSL certificate warning message and have to manually accept the default FortiGate certificate. The network user’s web browser may deem the default certificate as invalid.

When you use certificate authentication, if you do not specify any certificate when you create the security policy, the global settings are used. If you specify a certificate, the per-policy setting will overwrite the global setting. For more information about the use of certificate authentication see “Certificate-based authentication” on page 113.

To set the authentication protocols

1. Go to User > User > Authentication.
2. In Protocol Support, select the required authentication protocols.
3. If using HTTPS protocol support, in Certificate, select a Local certificate from the drop-down list.
4. Select Apply.

Authentication in security policies

Security policies control traffic between FortiGate interfaces, both physical interfaces and VLAN subinterfaces. Without authentication, a security policy enables access from one network to another for all users on the source network. Authentication enables you to allow access only for users who are members of selected user groups. To include authentication in a security policy, you must create an identity-based policy.
The style of the authentication method varies by the authentication protocol. If you have selected HTTP, FTP or Telnet, a username and password-based authentication occurs. The FortiGate unit prompts network users to input their security username and password. If you have selected HTTPS, certificate-based authentication (HTTPS or HTTP redirected to HTTPS only) occurs. You must install customized certificates on the FortiGate unit and on the browsers of network users, which the FortiGate unit matches.

You can configure user authentication for security policies only when Action is set to Accept. If the policy is set to Deny, IPsec, or SSL VPN the options will be different.

This section includes:
- Enabling authentication protocols
- Authentication replacement messages
- Access to the Internet
- Configuring authentication security policies
- Identity-based policy
- FSSO authentication
- NTLM authentication
- Certificate authentication
- Dynamic profile
- Restricting number of concurrent user logons

**Enabling authentication protocols**

Users can authenticate using FTP, HTTP, HTTPS, and Telnet. However, these protocols must be enabled first. Another authentication option is to redirect any attempts to authenticate using HTTP to a more secure channel that uses HTTPS. This forces users to a more secure connection before entering their user credentials.

**To enable support for authentication protocols - web-based manager**

1. Go to User > User > Authentication.
2. Select one or more of HTTP, HTTPS, FTP, Telnet, or Redirect HTTP Challenge to a Secure Channel (HTTPS). Only selected protocols will be available for use in authentication.
3. Select the Certificate to use, for example Fortinet_Factory.
4. Select Apply.

**To enable support for authentication protocols - CLI**

```
config user setting
    set auth-type ftp http https telnet
    set auth-cert Fortinet_Factory
end
```
Authentication replacement messages

A replacement message is the body of a webpage containing a message about a blocked website message, a file too large message, a disclaimer, or even a login page for authenticating. The user is presented with this message instead of the blocked content. Authentication replacement messages are the prompts a user sees during the security authentication process such as login page, disclaimer page, and login success or failure pages. These are different from most replacement messages because they are interactive requiring a user to enter information, instead of simply informing the user of some event as other replacement messages do.

Replacement messages have a system-wide default configuration, a per-VDOM configuration, and disclaimers can be customized for multiple security policies within a VDOM.

These replacement messages are used for authentication using HTTP and HTTPS. Authentication replacement messages are HTML messages. You cannot customize the security authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

More information about replacement messages can be found in the config system replacemsg section of the FortiOS CLI Reference.

Table 4: List of authentication replacement messages

<table>
<thead>
<tr>
<th>Replacement message name (CLI name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login challenge page</strong> (auth-challenge-page)</td>
<td>This HTML page is displayed if security users are required to answer a question to complete authentication. The page displays the question and includes a field in which to type the answer. This feature is supported by RADIUS and uses the generic RADIUS challenge-access auth response. Usually, challenge-access responses contain a Reply-Message attribute that contains a message for the user (for example, “Please enter new PIN”). This message is displayed on the login challenge page. The user enters a response that is sent back to the RADIUS server to be verified. The Login challenge page is most often used with RSA RADIUS server for RSA SecurID authentication. The login challenge appears when the server needs the user to enter a new PIN. You can customize the replacement message to ask the user for a SecurID PIN. This page uses the %%QUESTION%% tag.</td>
</tr>
</tbody>
</table>
Table 4: List of authentication replacement messages

<table>
<thead>
<tr>
<th>Replacement message name (CLI name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclaimer page</td>
<td>Prompts user to accept the displayed disclaimer when leaving protected network. The web-based manager refers to this as User Authentication Disclaimer, and it is enabled with a security policy that also includes at least one identity-based policy. When a security user attempts to browse a network through the FortiGate unit using HTTP or HTTPS this disclaimer page is displayed. The extra pages seamlessly extend the size of the page from 8 192 characters to 16 384 and 24 576 characters respectively. When configuring the disclaimer page in the web-based manager this is shown by its size being 24 576 characters. See “Disclaimer” on page 101.</td>
</tr>
<tr>
<td>Email token page</td>
<td>The page prompting a user to enter their email token. See “Email” on page 78.</td>
</tr>
<tr>
<td>FortiToken page</td>
<td>The page prompting a user to enter their FortiToken code. See “FortiToken” on page 80.</td>
</tr>
</tbody>
</table>
| Keepalive page                      | The HTML page displayed with security authentication keepalive is enabled using the following CLI command:  
```plaintext
config system global  
set auth-keepalive enable  
end
```
Authentication keepalive keeps authenticated firewall sessions from ending when the authentication timeout ends. In the web-based manager, go to User > Options to set the Authentication Timeout. This page includes %%%TIMEOUT%%%. |
| Login failed page                   | The Disclaimer page replacement message does not redirect the user to a redirect URL or the security policy does not include a redirect URL. When a user selects the button on the disclaimer page to decline access through the FortiGate unit, the Declined disclaimer page is displayed. |
| Login page                          | The authentication HTML page displayed when users who are required to authenticate connect through the FortiGate unit using HTTP or HTTPS. Prompts the user for their username and password to login. This page includes %%%USERNAMEID%% and %%%PASSWORDID%% tags. |
| Declined disclaimer page            | The page displayed if a user declines the disclaimer page. See “Disclaimer” on page 101. |
Table 4: List of authentication replacement messages

<table>
<thead>
<tr>
<th>Replacement message name (CLI name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Token page (auth-sms-token-page)</td>
<td>The page prompting a user to enter their SMS token. See “SMS” on page 79.</td>
</tr>
<tr>
<td>Success message (auth-success-msg)</td>
<td>The page displayed when a user successfully authenticates. Prompts user to attempt their connection again (as the first was interrupted for authentication).</td>
</tr>
</tbody>
</table>

Access to the Internet

A policy for accessing the Internet is similar to a policy for accessing a specific network, but the destination address is set to all. The destination interface is the one that connects to the Internet Service Provider (ISP). For general purpose Internet access, the Service is set to ANY.

Access to HTTP, HTTPS, FTP and Telnet sites may require access to a domain name service. DNS requests do not trigger authentication. You must configure a policy to permit unauthenticated access to the appropriate DNS server, and this policy must precede the policy for Internet access. Failure to do this will result in the lack of a DNS connection and a corresponding lack of access to the Internet.

Configuring authentication security policies

To include authentication in a security policy, you must create an identity-based policy. An identity-based policy can authenticate by certificate, FSSO, and NTLM. The two exceptions to this are dynamic profiles and FSSO Agents. See “Configuring dynamic profile” on page 182, and “Introduction to FSSO” on page 133.

Before creating an identity-based security policy, you need to configure one or more users and firewall user groups. For more information, see “Users and user groups” on page 73.

Creating the security policy is the same as a regular security policy except you must select the action specific to your authentication method:

Table 5: Authentication methods allowed for each policy Action

<table>
<thead>
<tr>
<th>Action</th>
<th>Authentication method</th>
<th>Where authentication is used</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCEPT</td>
<td>FSSO Agent or identity-based policy — FSSO</td>
<td>See “FSSO integration with Windows AD or Novell” on page 133.</td>
</tr>
<tr>
<td>ACCEPT</td>
<td>identity-based policy — NTLM</td>
<td>See “NTLM authentication” on page 105.</td>
</tr>
<tr>
<td>ACCEPT</td>
<td>identity-based policy — Certificates</td>
<td>See “Configuring certificate-based authentication” on page 125.</td>
</tr>
<tr>
<td>ACCEPT</td>
<td>Dynamic Profile</td>
<td>See “Configuring dynamic profile-based security policies” on page 189.</td>
</tr>
<tr>
<td>IPSEC</td>
<td>IPsec Phase 1 and 2</td>
<td>See “Configuring authentication of remote IPsec VPN users” on page 108.</td>
</tr>
<tr>
<td>SSL-VPN</td>
<td>SSL certificates</td>
<td>See “Configuring authentication of SSL VPN users” on page 108.</td>
</tr>
<tr>
<td>DENY</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>
Disclaimer

When configuring any authentication security policy, there is an option to enable a disclaimer. The disclaimer is a replacement message that when enabled, web traffic matching this policy will be presented with the disclaimer that the user must choose to agree or decline.

The default disclaimer contains a warning that any content the user is about to access is the responsibility of the user and not the company or owner of the network. It is presented in Figure 5. You can customize the text and the appearance to as required.

To change the disclaimer
1. Go to System > Config > Replacement messages.
2. Expand Authentication
3. Select Disclaimer page to edit.
4. Select the existing disclaimer text, and copy it to a separate file.
5. Make changes

Figure 5: Default disclaimer message

Customizing authentication replacement messages

Customizing disclaimers or other authentication replacement messages involves changing the text of the disclaimer message, and possibly the overall appearance of the message.

Disclaimers are useful in many situations. Often companies find it useful to brand the disclaimers with their specific company policy text, logo, and design. One example of this is at an Internet cafe where customers pay for usage and must accept terms of usage before accessing the internet. The cafe benefits from a customized disclaimer that alerts the customer to their online policies. The same is true for other authentication replacement messages such as the login page.
Changing the disclaimer at System > Config > Replacement messages is not the same as selecting to customize a disclaimer used in a policy. The System > Config location is the default message that all disclaimers inherit. The security policy location is a customized disclaimer that inherits the default format for the disclaimer message, but then can be customized for this policy.

If identity-based policy is enabled, the disclaimer option is not available. Instead, Customize Authentication messages is available in the Enable identity-based Policy section. Selecting the Edit icon allows you to customize the listed authentication replacement messages which includes the disclaimer.

To customize the disclaimer for a security policy - web-based manager
1. Go to Policy > Policy. Either select an existing policy and edit or select Create New.
2. Enable Disclaimer, and select Customize Disclaimer Message.
3. Select the edit icon to edit the Disclaimer page, and change your text or layout as needed.

Enabling security logging

There are two types of logging that relate to authentication — event logging, and security logging.

When enabled, event logging records system events such as configuration changes, and authentication. To configure event logging, go to Log & Report > Log Config > Log Setting and in the Event Log Settings section, select the check box beside Enable. Select the events you want to log, such as authentication.

When enabled security logging will log UTM and security policy traffic

You must enable logging within a security policy, as well as the options that are applied to a security policy, such as UTM features. Event logs are enabled within the Event Log page.

For more information on logging, see the FortiOS Log and Reporting guide.

For more information on specific types of log messages, see the FortiOS Log Message Reference.

You need to set the logging severity level to Notification when configuring a logging location to record traffic log messages.

To enable logging within an existing security policy - web-based manager
1. Go to Policy > Policy.
2. Expand to reveal the policy list of a policy.
3. Select the security policy you want to enable logging on and then select Edit.
4. To log all general firewall traffic, select the check box beside Log Allowed Traffic.
5. On the security policy’s page, select the check box beside UTM.
6. Select the protocol option list from the drop-down list beside Protocol Options.
   - By default, the Protocol Options check box is selected. You must choose a list from the drop-down list.
7 For each row under UTM, select the check box beside each of the profiles and/or sensors that you want applied to the policy; then select the profile or sensor from the drop-down list as well.

8 To apply other options, such as application lists, repeat step 7 and choose the option from the drop-down list.

9 Select OK.

Identity-based policy

An identity-based policy (IBP) performs user authentication in addition to the normal security policy duties. If the user does not authenticate, access to network resources is refused. This enforces Role Based Access Control (RBAC) to your organization’s network and resources.

User authentication can occur through any of the following supported protocols, including: HTTP, HTTPS, FTP, and Telnet. The authentication style depends on which of these protocols is included in the selected security services group and which of those enabled protocols the network user applies to trigger the authentication challenge.

For username and password-based authentication (HTTP, FTP, and Telnet) the FortiGate unit prompts network users to enter their username, password, and token code if two-factor authentication is selected for that user account. See “Two-factor authentication” on page 78. For certificate-based authentication, including HTTPS or HTTP redirected to HTTPS only, see “Certificate authentication” on page 106.

Enable identity-based Policy and Enable Dynamic Profile are mutually exclusive. When one of the two options is selected, the other is hidden. When both are not selected, both are visible again.

Set the ACCEPT Action, and select Enable identity-based Policy. In the web-based manager you can confirm this by changing Action from the default of ACCEPT to DENY. Note that nearly all of the fields are not available until you switch back to ACCEPT.

Set these commands in the CLI to see the other identity-based commands that were hidden before. In the following procedure, this is policy number 7.

```
config firewall policy
edit 7
set action ACCEPT
set identity-based enable
next
end
```

With identity-based policies, once the FortiGate unit matches the source and destination addresses, it processes the identity sub-policies for the user groups and services. This means unique security policies must be placed before an identity-based policy to be effective.

When the identity-based policy has been configured, the option to customize authentication messages is available. This allows you to change the text, style, layout, and graphics of the replacement messages associated with this firewall policy. When enabled, customizing these messages follows the same method as changing the disclaimer. See “Disclaimer” on page 101.

The types of authentication available in identity-based policies are

- FSSO authentication
• NTLM authentication
• Certificate authentication

Identity-based sub-policies

Once IBP is enabled in a policy, a table appears. Selecting Add allows you to configure authentication rules which are added to this table as sub-policies.

Just as with regular security policies, with these identity-based sub-policies traffic is matched from the top of the list of sub-policies down until the criteria is met. If there is no matching policy packets are dropped, even if they have been authenticated. Each sub-policy has its own UTM profile fields, traffic shaping, logging, and so on that take effect when the User Group, Service and Schedule are matched.

The order of these sub-policies is just as important as with regular security policies. For example if a user is a member of two groups, and each group has a separate sub-policy entry, the top one in the list will be matched first.

FSSO authentication

Identity-based security policies are an integral part of any FSSO configuration. These policies are how user information is acquired to sent to the FSSO Collector agent and the AD domain controllers. See “FSSO authentication” on page 104.

In the following procedure, Example.com is a company that has its employees and authentication servers on an internal network. The FortiGate unit intercepts all traffic leaving the internal network and requires FSSO authentication to access network resources on the Internet. The following procedure configures the security policy for FSSO authentication. FSSO is installed and configured including the RADIUS server, FSSO Collector agent, and user groups on the FortiGate

For the following procedure, the internal interface is port1 and the external interface connected to the Internet is port2. There is an address group for the internal network called company_network. The FSSO user group is called fsso_group, and the FSSO RADIUS server is fsso_rad_server.

To configure an FSSO authentication security policy - web-based manager

1. Go to Policy > Policy.
2. Select Create New.
3. Enter the following information.
   - Source Interface/Zone: port1
   - Source Address: company_network
   - Destination Interface/Zone: port2
   - Destination Address: all
   - Action: ACCEPT
   - Enable NAT: enabled
4. Select Enable identity-based Policy.
5. Select Add to add groups of users to this authentication policy.
6 Select the `fsso_group`, and the `FSSO_Guest_users` usergroups in the Available User Groups list and move them to the Selected User Groups list.

`FSSO_Guest_users` is a default user group enabled when FSSO is configured. It allows guest users on the network who do not have FSSO account to still authenticate and have access to network resources. See “Enabling guest access through FSSO security policies” on page 165.

7 Select HTTP, HTTPS, FTP, and Telnet for in the Available Services list, and move them to the Selected Services list.

8 Select always for the Schedule.

9 Enable Log Allowed Traffic.

10 Select UTM, and enable default AntiVirus, IPS, Web Filter, an Email filter.

11 Select OK.

A new line of information will appear in the identity-based policy table. The table lists the ID, user group or groups, the service or services, schedule, UTM, and logging selected for the rule. Use this display to verify your information was entered correctly.

12 Select Fortinet Single Sign-On (FSSO).

13 Optionally select Customize Authentication messages to change the default authentication messages to suit example.com’s company design and policies.

14 Select OK.

15 Ensure the FSSO authentication policy is at the top of the list so it will be attempted to be matched before any other policy.

An Example.com employee on the internal company network logs on to the internal network using their RADIUS username and password. When that user attempts to access the Internet, which requires FSSO authentication, the FortiGate authentication security policy intercepts the session, checks with the FSSO Collector agent to verify the user’s identity and credentials, and then if everything is verified the user is allowed access to the Internet.

**NTLM authentication**

The NT LAN Manager (NTLM) protocol is used when the MS Windows Active Directory (AD) domain controller can not be contacted. NTLM uses web browsers to send and receive authentication information. See “NTLM” on page 19 and “NTLM authentication with FSSO” on page 137.

NTLM authentication is enabled when you configure FSSO and enable NTLM in the identity-based policy (IBP). There must be at least one FSSO Collector agent configured on the FortiGate. Any users and user groups associated with the security policy will use NTLM to authenticate without further configuration. However some extra configuration in the CLI may be required for certain cases including guest access, and defining NTLM enabled browsers.

If there are multiple domains, a trust relation must exist between them. This is automatic if they are in a forest. With the trust relation, only one FSSO DC agent needs to be installed. Without the trust relation, FSSO DC agents must be installed on each domain controller.

**NTLM guest access - CLI**

Guest profile access may be granted to users failing NTLM authentication, such as visitors who have no user credentials on the network. To allow guest users in NTLM, use the following CLI command:
config firewall policy
  edit 8
    set action accept
    set identity-based enable
    set ntlm enable
    set ntlm-guest enable
  next
end

**NTLM enabled browsers - CLI**

User agent strings for NTLM enabled browsers allow the inspection of initial HTTP-User-Agent values, so that non-supported browsers are able to go straight to guest access without needlessly prompting the user for credentials that will fail. `ntlm-guest` must be enabled to use this option.

```
config firewall policy
  edit 9
    set action accept
    set identity-based enable
    set ntlm enable
    set ntlm-guest enable
    set ntlm-enabled-browsers <user_agent_string>
  next
end
```

`<user_agent_string>` is the name of the browser that is NTLM enabled. Examples of these values include “MSIE”, “Mozilla” (which includes FireFox), and “Opera”.

Value strings can be up to 63 characters in length, and may not contain cross site scripting (XSS) vulnerability characters such as brackets. The FortiGate unit prevents use of these characters to prevent exploitation of cross site scripting (XSS) vulnerabilities.

**Certificate authentication**

Certificates can be used as part of an identity-based policy. A customized certificate must be installed on the FortiGate unit and in the web browser, which the FortiGate unit will attempt to match.

All users being authenticated against the policy are required to have the proper certificate, which must be imported into the FortiGate unit. See “Certificate-based authentication” on page 113.

To require the user to accept a disclaimer to connect to the destination, select Enable Disclaimer. If the user is to be redirected after accepting the disclaimer, enter the URL in the Redirect URL to field. You can edit the User Authentication Disclaimer replacement message text in System > Config > Replacement Messages.

**Certificate redirect authentication**

Under User > User > Authentication select Redirect HTTP Challenge to a Secure Channel (HTTPS). This forces users to use secure connections to send their authentication information.

The following steps happen during a redirect:

1. User tries to access the Internet and the HTTP traffic hits the FortiGate security policy with authentication and HTTPS redirect enabled.

2. The FortiGate redirects the user with the HTTPS port and IP address of the interface connected to the user, such as internal.
3 User authenticates over the HTTPS connection as with normal authentication.
4 On successful authentication, the FortiGate provides access to the Internet as originally requested.

**Dynamic profile**

Only one security policy can be configured for dynamic profile in a VDOM. Also only one RADIUS server and one dynamic profile group can be configured per VDOM. When one dynamic profile security policy has been configured, the option is not visible when creating other policies. After deleting the dynamic profile security policy, the option is again visible when configuring other security policies.

![Enable identity-based Policy and Enable Dynamic Profile are mutually exclusive. When one of the two options is selected, the other is hidden. When both are not selected, both are visible again.](image)

By enabling the Dynamic Profile Users Only option, other non-dynamic profile users will not match this policy. This can be useful if you want to enforce all users to be part of the dynamic profile group—in which case you have a deny all profile after this one.

For more information, see “Configuring dynamic profile-based security policies” on page 189.

**Restricting number of concurrent user logons**

Some users on your network may often have multiple account sessions open at one time either to the same network resource or accessing to the admin interface on the FortiGate unit.

While there are valid reasons for having multiple concurrent sessions open, hackers also do this to speed up their malicious work. Often a hacker is making multiple attempts to gain access to the internal network or the admin interface of the FortiGate unit, usually from different IP addresses to appear to the FortiGate unit as legitimate users. For this reason, the more concurrent sessions a hacker has open at once, the faster they will achieve their goal.

To help prevent this, you can limit concurrent user sessions to the same IP address. This allows valid users to continue their legitimate work while limiting hackers activity.

**To enable administrator concurrent session restrictions - CLI**

```plaintext
config system global
  set admin-concurrent enable
end
```

**VPN authentication**

All VPN configurations require users to authenticate. Authentication based on user groups applies to:

- SSL VPNs
- PPTP and L2TP VPNs
- an IPsec VPN that authenticates users using dialup groups
- a dialup IPsec VPN that uses XAUTH authentication (Phase 1)
You must create user accounts and user groups before performing the procedures in this section. If you create a user group for dialup IPsec clients or peers that have unique peer IDs, their user accounts must be stored locally on the FortiGate unit. You cannot authenticate these types of users using a RADIUS or LDAP server.

Configuring authentication of SSL VPN users

The general procedure for authenticating SSL VPN users is:

1. Configure user accounts.
2. Create one or more user groups for SSL VPN users.
   See “Configuring user accounts and user groups for SSL VPN” in the FortiOS Handbook SSL VPN guide.
3. Enable SSL VPN.
4. Optionally, set inactivity and authentication timeouts.
5. Configure a security policy with SSL VPN action. Add an identity-based rule to allow access for the user groups you created for SSL VPN users.
   See “Configuring security policies” in the FortiOS Handbook SSL VPN guide.

Configuring authentication timeout

By default, the SSL VPN authentication expires after 8 hours (28 800 seconds). You can change it only in the CLI, and the time entered must be in seconds. For example, to change this timeout to one hour, you would enter:

```
config vpn ssl settings
  set auth-timeout 3600
end
```

If you set the authentication timeout (auth-timeout) to 0 when you configure the timeout settings, the remote client does not have to re-authenticate unless they log out of the system. To fully take advantage of this setting, the value for idle-timeout has to be set to 0 also, so that the client does not time out if the maximum idle time is reached. If the idle-timeout is not set to the infinite value, the system will log out if it reaches the limit set, regardless of the auth-timeout setting.

Configuring authentication of remote IPsec VPN users

An IPsec VPN on a FortiGate unit can authenticate remote users through a dialup group. The user account name is the peer ID and the password is the pre-shared key. Authentication through user groups is supported for groups containing only local users. To authenticate users using a RADIUS or LDAP server, you must configure XAUTH settings. See “Configuring XAuth authentication” on page 109.

To configure user group authentication for dialup IPsec - web-based manager

1. Configure the dialup users who are permitted to use this VPN. Create a user group with Type:Firewall and add them to it.
   For more information, see “Users and user groups” on page 73.
2  Go to VPN > IPsec > Auto Key (IKE), select Create Phase 1 and enter the following information.

<table>
<thead>
<tr>
<th>Name</th>
<th>Name for group of dialup users using the VPN for authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>List of the types of remote gateways for VPN. Select Dialup User.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>List of authentication methods available for users. Select Preshared Key and enter the preshared key.</td>
</tr>
<tr>
<td>Peer Options</td>
<td>Select Accept peer ID in dialup group. Select the user group that is to be allowed access to the VPN. The listed user groups contain only users with passwords on the FortiGate unit.</td>
</tr>
</tbody>
</table>

The Accept peer ID in dialup group option does not support authentication of users through an authentication server. The user accounts must exist on the FortiGate unit.

3  Select Advanced to reveal additional parameters and configure other VPN gateway parameters as needed.

4  Select OK.

To configure user group authentication for dialup IPsec - CLI example

The peertype and usgrgrp options configure user group-based authentication.

```
config vpn ipsec phase1
edit office_vpn
  set interface port1
  set type dynamic
  set psksecret yORRAzltNghztV32jend
  set proposal 3des-sha1 aes128-sha1
  set peertype dialup
  set usgrgrp Group1
end
```

Configuring XAuth authentication

Extended Authentication (XAuth) increases security by requiring additional user authentication information in a separate exchange at the end of the VPN Phase 1 negotiation. The FortiGate unit asks the user for a username and password. It then forwards the user’s credentials (the password is encrypted) to an external RADIUS or LDAP server for verification.

XAuth can be used in addition to or in place of IPsec phase 1 peer options to provide access security through an LDAP or RADIUS authentication server. You must configure a dialup user group whose members are all externally authenticated.

None of the users in this dialup user group can have their passwords stored on the FortiGate unit.
To configure authentication for a dialup IPsec VPN - web-based manager
1. Configure the users who are permitted to use this VPN. Create a user group and add the users to the group.
   For more information, see “Users and user groups” on page 73.
2. Go to VPN > IPsec > Auto Key (IKE).
3. Select Create Phase 1 and configure the basic VPN phase1 settings.
   Remote Gateway must be Dialup User.
4. Select Advanced to reveal additional parameters and enter the following information.

<table>
<thead>
<tr>
<th>XAuth</th>
<th>Select Enable as Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>Select PAP, CHAP, or AUTO. Use CHAP whenever possible. Use PAP with all implementations of LDAP and with other authentication servers that do not support CHAP, including some implementations of Microsoft RADIUS. Use AUTO with the Fortinet Remote VPN Client and where the authentication server supports CHAP but the XAuth client does not.</td>
</tr>
<tr>
<td>User Group</td>
<td>Select the user group that is to have access to the VPN. The list of user groups does not include any group that has members whose password is stored on the FortiGate unit.</td>
</tr>
</tbody>
</table>

5. Select OK.
For more information about XAUTH configuration, see the IPsec VPN chapter of this FortiOS Handbook.

To configure authentication for a dialup IPsec VPN - CLI example
The xauthtype and authusrgrp fields configure XAuth authentication.
```
config vpn ipsec phase1
edit office_vpn
  set interface port1
  set type dynamic
  set psksecret yORRAzltNGhzgtV32jend
  set proposal 3des-sha1 aes128-sha1
  set peertype dialup
  set xauthtype pap
  set authusrgrp Group1
end
```

Some parameters specific to setting up the VPN itself are not shown here. For detailed information about configuring IPsec VPNs, see the FortiOS Handbook IPsec VPN guide.

Configuring authentication of PPTP VPN users and user groups
Configuration of a PPTP VPN is possible only through the CLI. You can configure user groups and security policies using either CLI or web-based manager.

To configure authentication for a PPTP VPN
1. Configure the users who are permitted to use this VPN. Create a security user group and add them to it.
   For more information, see “Users and user groups” on page 73.
2. Configure the PPTP VPN in the CLI as in this example.
   ```
   config vpn pptp
   ```
set status enable
set sip 192.168.0.100
set eip 192.168.0.110
set usrgrp PPTP_Group
end

The sip and eip fields define a range of virtual IP addresses assigned to PPTP clients.

3 Configure a security policy. The source interface is the one through which the clients will connect. The source address is the PPTP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.

Configuring authentication of L2TP VPN users/user groups

Configuration of a L2TP VPN is possible only through the CLI. You can configure user groups and security policies using either CLI or web-based manager.

To configure authentication for a PPTP VPN

1 Configure the users who are permitted to use this VPN. Create a user group and add them to it.

For more information, see “Users and user groups” on page 73.

2 Configure the L2TP VPN in the CLI as in this example.

```
config vpn l2tp
  set status enable
  set sip 192.168.0.100
  set eip 192.168.0.110
  set usrgrp L2TP_Group
end
```

The sip and eip fields define a range of virtual IP addresses assigned to L2TP clients.

3 Configure a security policy. The source interface is the one through which the clients will connect. The source address is the L2TP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.
Certificate-based authentication

This section provides an overview of how the FortiGate unit verifies the identities of administrators, SSL VPN users, or IPsec VPN peers using X.509 security certificates.

The following topics are included in this section:

- What is a security certificate?
- Certificates overview
- Managing X.509 certificates
- Configuring certificate-based authentication
- Example — Generate a CSR on the FortiGate unit
- Example — Generate and Import CA certificate with private key pair on OpenSSL
- Example — Generate an SSL certificate in OpenSSL

What is a security certificate?

A security certificate is a small text file that is part of a third-party generated public key infrastructure (PKI) to help guarantee the identity of both the user logging on and the website they are logging in.

A certificate includes identifying information such as the company and location information for the website, as well as the third-party company name, the expiry date of the certificate, and the encrypted public key.

FortiGate units use X.509 certificates to authenticate single sign-on (SSO) for users. The X.509 standard has been in use since before 2000, but has gained popularity with the Internet’s increased popularity. X.509 v3 is defined in RFC 5280 and specifies standard formats for public key certificates, certificate revocation lists, and a certification path validation algorithm. The unused earlier X.509 version 1 was defined in RFC 1422.

The main difference between X.509 and PGP certificates is that where in PGP anyone can sign a certificate, for X.509 only a trusted authority can sign certificates. This limits the source of certificates to well known and trustworthy sources. Where PGP is well suited for one-on-one communications, the X.509 infrastructure is intended to be used in many different situations including one-to-many communications. Some common filename extensions for X.509 certificates are listed in Table 6.

Table 6:  Common certificate filename extensions

<table>
<thead>
<tr>
<th>Filetype</th>
<th>Format name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.pem</td>
<td>Privacy Enhanced Mail (PEM)</td>
<td>Base64 encoded DER certificate, that uses &quot;-----BEGIN CERTIFICATE-----&quot; and &quot;-----END CERTIFICATE-----&quot;</td>
</tr>
<tr>
<td>.cer</td>
<td>Security CERtificate</td>
<td>Usually binary DER form, but Base64-encoded certificates are common too.</td>
</tr>
<tr>
<td>.crt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.der</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Certificates overview

Certificates play a major role in authentication of clients connecting to network services via HTTPS, both for administrators and SSL VPN users. Certificate authentication is optional for IPsec VPN peers.

- Certificates and protocols
- IPsec VPNs and certificates
- Certificate types on the FortiGate unit

Certificates and protocols

There are a number of protocols that are commonly used with certificates including SSL and HTTPS, and other certificate-related protocols.

SSL and HTTPS

The secure HTTP (HTTPS) protocol uses SSL. Certificates are an integral part of SSL. When a web browser connects to the FortiGate unit via HTTPS, a certificate is used to verify the FortiGate unit’s identity to the client. Optionally, the FortiGate unit can require the client to authenticate itself in return.

By default, the FortiGate unit uses a self-signed security certificate to authenticate itself to HTTPS clients. When the certificate is offered, the client browser displays two security messages.

- The first message prompts users to accept and optionally install the FortiGate unit’s self-signed security certificate. If the user does not accept the certificate, the FortiGate unit refuses the connection. When the user accepts the certificate, the FortiGate login page is displayed, and the credentials entered by the user are encrypted before they are sent to the FortiGate unit. If the user chooses to install the certificate, the prompt is not displayed again.
- Just before the FortiGate login page is displayed, a second message informs users that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit redirects the connection (away from the distinguished name recorded in the self-signed certificate) and can be ignored.

Optionally, you can install an X.509 server certificate issued by a certificate authority (CA) on the FortiGate unit. You can then configure the FortiGate unit to identify itself using the server certificate instead of the self-signed certificate. For more information, see the FortiOS Handbook SSL VPN guide. or “Authenticating SSL VPN users with security certificates” on page 125.

After successful certificate authentication, communication between the client browser and the FortiGate unit is encrypted using SSL over the HTTPS link.

Table 6: Common certificate filename extensions

<table>
<thead>
<tr>
<th>Extension</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.p7b</td>
<td>PKCS#7 SignedData</td>
<td>Structure without data, just certificates or CRLs. PKCS#7 is a standard for signing or encrypting (officially called &quot;enveloping&quot;) data.</td>
</tr>
<tr>
<td>.p7c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.p12</td>
<td>PKCS#12</td>
<td>May contain certificate(s) (public) and private keys (password protected)</td>
</tr>
<tr>
<td>.pfx</td>
<td>personal information exchange (PFX)</td>
<td>Older format. Came before PKCS#12. Usually today data is in PKCS#12 format.</td>
</tr>
</tbody>
</table>
Certificate-related protocols

There are multiple protocols that are required for handling certificates. These include the Online Certificate Status Protocol (OCSP), Secure Certificate Enrollment Protocol (SCEP), and Server-based Certificate Validation Protocol (SCVP).

Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) allows the verification of X.509 certificate expiration dates. This is important to prevent hackers from changing the expiry date on an old certificate to a future date.

Normally certificate revocation lists (CRLs) are used, but OCSP is an alternate method available. However a CRL is a public list, and some companies may want to avoid the public exposure of their certificate structure even if it is only invalid certificates.

The OSCP check on the certificate’s revocation status is typically carried out over HTTP with a request-response format. The authority responding can reply with a status of good, revoked, or unknown for the certificate in question.

Secure Certificate Enrollment Protocol

Secure Certificate Enrollment Protocol (SCEP) is an automated method of signing up for certificates. Typically this involves generating a request you send directly to the SCEP service, instead of generating a file request that may or may not be signed locally.

Server-based Certificate Validation Protocol

Server-based Certificate Validation Protocol (SCVP) is used to trace a certificate back to a valid root level certificate. This ensures that each step along the path is valid and trustworthy.

IPsec VPNs and certificates

Certificate authentication is a more secure alternative to preshared key (shared secret) authentication for IPsec VPN peers. Unlike administrators or SSL VPN users, IPsec peers use HTTP to connect to the VPN gateway configured on the FortiGate unit. The VPN gateway configuration can require certificate authentication before it permits an IPsec tunnel to be established. See “Authenticating IPsec VPN users with security certificates” on page 126.

Certificate types on the FortiGate unit

There are different types of certificates available that vary depending on their intended use. FortiOS supports local, remote, CA, and CRL certificates.

Local certificates

Local certificates are issued for a specific server, or web site. Generally they are very specific, and often for an internal enterprise network. For example a personal web site for John Smith at www.example.com (such as http://www.example.com/home/jsmith) would have its own local certificate.

These can optionally be just the certificate file, or also include a private key file and PEM passphrase for added security.
Remote certificates
Remote certificates are public certificates without a private key. For dynamic certificate revocation, you need to use an Online Certificate Status Protocol (OCSP) server. The OCSP is configured in the CLI only. Installed Remote (OCSP) certificates are displayed in the Remote Certificates list.

CA root certificates
CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of www.example.com instead of just the smaller single web page.

Certificate revocation list
Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

Certificate signing
The trust in a certificate comes from the authority that signs it. For example if VeriSign signs your CA root certificate, it is trusted by everyone. While these certificates are universally accepted, it is cumbersome and expensive to have all certificates on a corporate network signed with this level of trust.

With self-signed certificates nobody, except the other end of your communication, knows who you are and therefore they do not trust you as an authority. However this level is useful for encryption between two points — neither point may care about who signed the certificate, just that it allows both points to communicate. This is very useful for internal networks and communications.

A general rule is that CA signed certificates are accepted and sometimes required, but it is easier to self-sign certificates when you are able.

For more on the methods of certificate signing see “Generating a certificate signing request” on page 117.

Managing X.509 certificates
Managing security certificates is required due to the number of steps involved in both having a certificate request signed, and then distributing the correct files for use.

You use the FortiGate unit or CA software such as OpenSSL to generate a certificate request. That request is a text file that you send to the CA for verification, or alternately you use CA software to self-validate. Once validated, the certificate file is generated and must be imported to the FortiGate unit before it can be used. These steps are explained in more detail later in this section.

This section provides procedures for generating certificate requests, installing signed server certificates, and importing CA root certificates and CRLs to the FortiGate unit.

For information about how to install root certificates, CRLs, and personal or group certificates on a remote client browser, refer to your browser’s documentation.

This section includes:
Generating a certificate signing request

Whether you create certificates locally with a software application or obtain them from an external certificate service, you will need to generate a certificate signing request (CSR).

When you generate a CSR, a private and public key pair is created for the FortiGate unit. The generated request includes the public key of the FortiGate unit and information such as the FortiGate unit’s public static IP address, domain name, or email address. The FortiGate unit’s private key remains confidential on the FortiGate unit.

After you submit the request to a CA, the CA will verify the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign the certificate, and you install the certificate on the FortiGate unit.

The Certificate Request Standard is a public key cryptography standard (PKCS) published by RSA, specifically PKCS10 which defines the format for CSRs. This is defined in RFC 2986.

To generate a certificate request in FortiOS - web-based manager

1. Go to **System > Certificates > Local Certificates**.
2. Select **Generate**.
3. In the **Certificate Name** field, enter a unique meaningful name for the certificate request. Typically, this would be the hostname or serial number of the FortiGate unit or the domain of the FortiGate unit such as example.com.

   Do not include spaces in the certificate name. This will ensure compatibility of a signed certificate as a PKCS12 file to be exported later on if required.

4. Enter values in the **Subject Information** area to identify the FortiGate unit:
   - If the FortiGate unit has a static IP address, select **Host IP** and enter the public IP address of the FortiGate unit. If the FortiGate unit does not have a public IP address, use an email address (or fully qualified domain name (FQDN) if available) instead.
   - If the FortiGate unit has a static IP address and subscribes to a dynamic DNS service, use a FQDN if available to identify the FortiGate unit. If you select **Domain Name**, enter the FQDN of the FortiGate unit. Do not include the protocol specification (http://) or any port number or path names.

   If a domain name is not available and the FortiGate unit subscribes to a dynamic DNS service, an “unable to verify certificate” type message may be displayed in the user’s browser whenever the public IP address of the FortiGate unit changes.

   - If you select **E-Mail**, enter the email address of the owner of the FortiGate unit.
5 Enter values in the **Optional Information** area to further identify the FortiGate unit.

<table>
<thead>
<tr>
<th>Organization Unit</th>
<th>Name of your department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icon.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Legal name of your company or organization.</td>
</tr>
<tr>
<td>Locality (City)</td>
<td>Name of the city or town where the FortiGate unit is installed.</td>
</tr>
<tr>
<td>State/Province</td>
<td>Name of the state or province where the FortiGate unit is installed.</td>
</tr>
<tr>
<td>Country</td>
<td>Select the country where the FortiGate unit is installed.</td>
</tr>
<tr>
<td>e-mail</td>
<td>Contact email address.</td>
</tr>
</tbody>
</table>

6 From the **Key Size** list, select 1024 Bit, 1536 Bit or 2048 Bit. Larger keys are slower to generate but more secure.

7 In **Enrollment Method**, you have two methods to choose from. Select **File Based** to generate the certificate request, or **Online SCEP** to obtain a signed SCEP-based certificate automatically over the network. For the SCEP method, enter the URL of the SCEP server from which to retrieve the CA certificate, and the CA server challenge password.

8 Select OK.

The request is generated and displayed in the **Local Certificates** list with a status of **PENDING**.

9 Select the **Download** button to download the request to the management computer.

10 In the **File Download** dialog box, select **Save** and save the Certificate Signing Request on the local file system of the management computer.

11 Name the file and save it on the local file system of the management computer. The certificate request is ready for the certificate to be generated.

### Generating certificates with CA software

CA software allows you to generate unmanaged certificates and CA certificates for managing other certificates locally without using an external CA service. Examples of CA software include ssl-ca from OpenSSL (available for Linux, Windows, and Mac) or genslcert from SuSE, MS Windows Server 2000 and 2003 come with a CA as part of their certificate services, and in MS Windows 2008 CA software can be installed as part of the Active Directory installation. See "Example — Generate and Import CA certificate with private key pair on OpenSSL" on page 128.

The general steps for generating certificates with CA software are:

1. Install the CA software as a stand-alone root CA.
2. Provide identifying information for your self-administered CA.

While following these steps, the methods vary slightly when generating server certificates, CA certificates, and PKI certificates.

### Server certificate

1. Generate a Certificate Signing Request (CSR) on the FortiGate unit.
2 Copy the CSR base-64 encoded text (PKCS10 or PKCS7) into the CA software and generate the certificate.
   PKCS10 is the format used to send the certificate request to the signing authority.
   PKCS7 is the format the signing authority can use for the newly signed certificate.
3 Export the certificate as a X.509 DER encoded binary file with .CER extension
4 Upload the certificate file to the FortiGate unit Local Certificates page (type is Certificate).

CA certificate
1 Retrieve the CA Certificate from the CA software as a DER encoded file.
2 Upload the CA certificate file to the FortiGate unit CA Certificates page at System > Certificates > CA Certificates.

PKI certificate
1 Generate a Certificate Signing Request (CSR) on the FortiGate unit.
2 Copy the CSR base-64 encoded text (PKCS#10 or PKCS#7) into the CA software and generate the certificate.
   PKCS10 is the format used to send the certificate request to the signing authority.
   PKCS7 is the format the signing authority can use for the newly signed certificate.
3 Export the certificate as a X.509 DER encoded binary file with .CER extension.
4 Install the certificate in the user’s web browser or IPsec VPN client as needed.

Obtaining a signed server certificate from an external CA
To obtain a signed server certificate for a FortiGate unit, you must send a request to a CA that provides digital certificates that adhere to the X.509 standard. The FortiGate unit provides a way for you to generate the request.

To submit the certificate signing request (file-based enrollment)
1 Using the web browser on the management computer, browse to the CA web site.
2 Follow the CA instructions for a base-64 encoded PKCS#10 certificate request and upload your certificate request.
3 Follow the CA instructions to download their root certificate and CRL.
   When you receive the signed server certificate from the CA, install the certificate on the FortiGate unit.

To install or import the signed server certificate - web-based manager
1 On the FortiGate unit, go to System > Certificates > Local Certificates.
2 Select Import.
3 From Type, select Local Certificate.
4 Select Browse, browse to the location on the management computer where the certificate was saved, select the certificate, and then select Open.
5 Select OK, and then select Return.
Installing a CA root certificate and CRL to authenticate remote clients

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and CRL from the issuing CA. When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiGate unit according to the procedures given below.

To install a CA root certificate

1. After you download the root certificate of the CA, save the certificate on the management computer. Or, you can use online SCEP to retrieve the certificate.
2. On the FortiGate unit, go to System > Certificates > CA Certificates.
3. Select Import.
4. Do one of the following:
   - To import using SCEP, select SCEP. Enter the URL of the SCEP server from which to retrieve the CA certificate. Optionally, enter identifying information of the CA, such as the filename.
   - To import from a file, select Local PC, then select Browse and find the location on the management computer where the certificate has been saved. Select the certificate, and then select Open.
5. Select OK, and then select Return.

The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).

To import a certificate revocation list

A Certificate Revocation List (CRL) is a list of the CA certificate subscribers paired with certificate status information. The list contains the revoked certificates and the reason(s) for revocation. It also records the certificate issue dates and the CAs that issued them.

When configured to support SSL VPNs, the FortiGate unit uses the CRL to ensure that the certificates belonging to the CA and remote peers or clients are valid. You must download the CRL from the CA web site on a regular basis.

1. After you download the CRL from the CA web site, save the CRL on the management computer.
2. Go to System > Certificates > CRL.
3. Select Import.
4  Do one of the following:
   • To import using an HTTP server, select HTTP and enter the URL of the HTTP server.
   • To import using an LDAP server, select LDAP and select the LDAP server from the list.
   • To import using an SCEP server, select SCEP and select the Local Certificate from the list. Enter the URL of the SCEP server from which the CRL can be retrieved.
   • To import from a file, select Local PC, then select Browse and find the location on the management computer where the CRL has been saved. Select the CRL and then select Open.

5  Select OK, and then select Return.

Troubleshooting certificates

There are times when there are problems with certificates — a certificate is seen as expired when its not, or it can’t be found. Often the problem is with a third party website, and not FortiOS. However, some problems can be traced back to FortiOS such as DNS or routing issues.

Certificate is reported as expired when it is not

Certificates often are issued for a set period of time such as a day or a month, depending on their intended use. This ensures everyone is using up-to-date certificates. It is also more difficult for hackers to steal and use old certificates.

Reasons a certificate may be reported as expired include:
   • It really has expired based on the “best before” date in the certificate
   • The FortiGate unit clock is not properly set. If the FortiGate clock is fast, it will see a certificate as expired before the expiry date is really here.
   • The requesting server clock is not properly set. A valid example is if your certificate is 2 hours from expiring, a server more than two time zones away would see the certificate as expired. Otherwise, if the server’s clock is set wrongly it will also have the same effect.
   • The certificate was revoked by the issuer before the expiry date. This may happen if the issuer believes a certificate was either stolen or misused. It is possible it is due to reasons on the issuer’s side, such as a system change or such. In either case it is best to contact the certificate issuer to determine what is happening and why.

A secure connection cannot be completed (Certificate cannot be found)

Everyone who uses a browser has encountered a message such as This connection is untrusted. Normally when you try to connect securely to a website, that website will present its valid certificate to prove their identity is valid. When the website’s certificate cannot be verified as valid, the message appears stating This connection is untrusted or something similar. If you usually connect to this website without problems, this error could mean that someone is trying to impersonate or hijack the website, and best practices dictates you not continue.

Reasons a website’s certificate cannot be validated include:
   • The website uses an unrecognized self-signed certificate. These are not secure because anyone can sign them. If you accept self-signed certificates you do so at your own risk. Best practices dictate that you must confirm the ID of the website using some other method before you accept the certificate.
The certificate is valid for a different domain. A certificate is valid for a specific location, domain, or sub-section of a domain such as one certificate for support.example.com that is not valid for marketing.example.com. If you encounter this problem, contact the webmaster for the website to inform them of the problem.

There is a DNS or routing problem. If the website’s certificate cannot be verified, it will not be accepted. Generally to be verified, your system checks with the third party certificate signing authority to verify the certificate is valid. If you cannot reach that third party due to some DNS or routing error, the certificate will not be verified.

Firewall is blocking required ports. Ensure that any firewalls between the requesting computer and the website allow the secure traffic through the firewall. Otherwise a hole must be opened to allow it through. This includes ports such as 443 (HTTPS) and 22 SSH).

Online updates to certificates and CRLs

If you obtained your local or CA certificate using SCEP, you can configure online renewal of the certificate before it expires. Similarly, you can receive online updates to CRLs.

Local certificates

In the `config vpn certificate local` command, you can specify automatic certificate renewal. The relevant fields are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>scep-url &lt;URL_str&gt;</code></td>
<td>The URL of the SCEP server. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td><code>scep-password &lt;password_str&gt;</code></td>
<td>The password for the SCEP server.</td>
</tr>
<tr>
<td><code>auto-regenerate-days &lt;days_int&gt;</code></td>
<td>How many days before expiry the FortiGate unit requests an updated local certificate. The default is 0, no auto-update.</td>
</tr>
<tr>
<td><code>auto-regenerate-days-warning &lt;days_int&gt;</code></td>
<td>How many days before local certificate expiry the FortiGate generates a warning message. The default is 0, no warning.</td>
</tr>
</tbody>
</table>

In this example, an updated certificate is requested three days before it expires.

```plaintext
config vpn certificate local
edit mycert
    set scep-url http://scep.example.com/scep
    set scep-server-password my_pass_123
    set auto-regenerate-days 3
    set auto-regenerate-days-warning 2
end
```
CA certificates

In the `config vpn certificate ca` command, you can specify automatic certificate renewal. The relevant fields are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scep-url &lt;URL_str&gt;</td>
<td>The URL of the SCEP server. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>auto-update-days &lt;days_int&gt;</td>
<td>How many days before expiry the FortiGate unit requests an updated CA certificate. The default is 0, no auto-update.</td>
</tr>
<tr>
<td>auto-update-days-warning &lt;days_int&gt;</td>
<td>How many days before CA certificate expiry the FortiGate generates a warning message. The default is 0, no warning.</td>
</tr>
</tbody>
</table>

In this example, an updated certificate is requested three days before it expires.
```
config vpn certificate ca
  edit mycert
    set scep-url http://scep.example.com/scep
    set auto-update-days 3
    set auto-update-days-warning 2
  end
```

Certificate Revocation Lists

If you obtained your CRL using SCEP, you can configure online updates to the CRL using the `config vpn certificate crl` command. The relevant fields are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-url &lt;http_url&gt;</td>
<td>URL of the server used for automatic CRL certificate updates. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>scep-cert &lt;scep_certificate&gt;</td>
<td>Local certificate used for SCEP communication for CRL auto-update.</td>
</tr>
<tr>
<td>scep-url &lt;scep_url&gt;</td>
<td>URL of the SCEP CA server used for automatic CRL certificate updates. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>update-interval &lt;seconds&gt;</td>
<td>How frequently, in seconds, the FortiGate unit checks for an updated CRL. Enter 0 to update the CRL only when it expires.</td>
</tr>
<tr>
<td>update-vdom &lt;update_vdom&gt;</td>
<td>VDOM used to communicate with remote SCEP server for CRL auto-update.</td>
</tr>
</tbody>
</table>

In this example, an updated CRL is requested only when it expires.
```
config vpn certificate crl
  edit cert_crl
    set http-url http://scep.example.com/scep
    set scep-cert my-scep-cert
    set scep-url http://scep.ca.example.com/scep
    set update-interval 0
    set update-vdom root
  end
```
Backing up and restoring local certificates

The FortiGate unit provides a way to export and import a server certificate and the FortiGate unit’s personal key through the CLI. If required (to restore the FortiGate unit configuration), you can import the exported file through the System > Certificates > Local Certificates page of the web-based manager.

As an alternative, you can back up and restore the entire FortiGate configuration through the System > Maintenance > Backup & Restore page of the web-based manager. The backup file is created in a FortiGate-proprietary format.

To export a server certificate and private key - CLI

This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server. Ensure that your TFTP server is running and accessible to the FortiGate unit before you enter the command.

1. Connect to the FortiGate unit through the CLI.
2. Type the following command:

   ```
   execute vpn certificate local export tftp <cert_name> <exp_filename> <tftp_ip>
   ```

   where:
   - `<cert_name>` is the name of the server certificate; typing `?` displays a list of installed server certificates.
   - `<exp_filename>` is a name for the output file.
   - `<tftp_ip>` is the IP address assigned to the TFTP server host interface.
3. Move the output file from the TFTP server location to the management computer for future reference.

To import a server certificate and private key - web-based manager

1. Go to VPN > Certificates > Local Certificates and select Import.
2. In Type, select PKCS12 Certificate.
3. Select Browse. Browse to the location on the management computer where the exported file has been saved, select the file, and then select Open.
4. In the Password field, type the password needed to upload the exported file.
5. Select OK, and then select Return.

To import separate server certificate and private key files - web-based manager

Use the following procedure to import a server certificate and the associated private key file when the server certificate request and private key were not generated by the FortiGate unit. The two files to import must be available on the management computer.

1. Go to VPN > Certificates > Local Certificates and select Import.
2. In Type, select Certificate.
3. Select the Browse button beside the Certificate file field. Browse to the location on the management computer where the certificate file has been saved, select the file, and then select Open.
4 Select the *Browse* button beside the *Key file* field. Browse to the location on the management computer where the key file has been saved, select the file, and then select *Open*.

5 If required, in the *Password* field, type the associated password, and then select *OK*.

6 Select *Return*.

**Configuring certificate-based authentication**

You can configure certificate-based authentication for FortiGate administrators, SSL VPN users, and IPsec VPN users.

In Microsoft Windows 7, you can use the certificate manager to keep track of all the different certificates on your local computer. To access certificate manager, in Windows 7 press the Windows key, enter “certmgr.msc” at the search prompt, and select the displayed match. Remember that in addition to these system certificates, many applications require you to register certificates with them directly.

To see FortiClient certificates, open the FortiClient Console, and select VPN. The VPN menu has options for My Certificates (local or client) and CA Certificates (root or intermediary certificate authorities). Use Import on those screens to import certificate files from other sources.

**Authenticating administrators with security certificates**

You can install a certificate on the management computer to support strong authentication for administrators. When a personal certificate is installed on the management computer, the FortiGate unit processes the certificate after the administrator supplies a username and password.

To enable strong administrative authentication:

- Obtain a signed personal certificate for the administrator from a CA and load the signed personal certificate into the web browser on the management computer according to the browser documentation.
- Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see “Installing a CA root certificate and CRL to authenticate remote clients” on page 120).
- Create a PKI user account for the administrator.
- Add the PKI user account to a firewall user group dedicated to PKI-authenticated administrators.
- In the administrator account configuration, select *PKI* as the account *Type* and select the *User Group* to which the administrator belongs.

**Authenticating SSL VPN users with security certificates**

While the default self-signed certificates can be used for HTTPS connections, it is preferable to use the X.509 server certificate to avoid the redirection as it can be misinterpreted as possible session hijacking. However, the server certificate method is more complex than self-signed security certificates. Also the warning message is typically displayed for the initial connection, and future connections will not generate these messages.

X.509 certificates can be used to authenticate IPsec VPN peers or clients, or SSL VPN clients. When configured to authenticate a VPN peer or client, the FortiGate unit prompts the VPN peer or client to authenticate itself using the X.509 certificate. The certificate supplied by the VPN peer or client must be verifiable using the root CA certificate installed on the FortiGate unit in order for a VPN tunnel to be established.
To enable certificate authentication for an SSL VPN user group

1. Install a signed server certificate on the FortiGate unit and install the corresponding root certificate (and CRL) from the issuing CA on the remote peer or client.

2. Obtain a signed group certificate from a CA and load the signed group certificate into the web browser used by each user. Follow the browser documentation to load the certificates.

3. Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see “Installing a CA root certificate and CRL to authenticate remote clients” on page 120).

4. Create a PKI user for each SSL VPN user. For each user, specify the text string that appears in the Subject field of the user’s certificate and then select the corresponding CA certificate.

5. Use the `config user peergrp` CLI command to create a peer user group. Add to this group all of the SSL VPN users who are authenticated by certificate.

6. Go to VPN > SSL > Config.

7. Select Enable SSL-VPN.

8. Go to Policy.

9. Select the Edit icon in the row that corresponds to the SSL-VPN security policy for traffic generated by holders of the group certificate.


11. Select OK.

Authenticating IPsec VPN users with security certificates

To require VPN peers to authenticate by means of a certificate, the FortiGate unit must offer a certificate to authenticate itself to the peer.

To enable the FortiGate unit to authenticate itself with a certificate:

1. Install a signed server certificate on the FortiGate unit.
   See “To install or import the signed server certificate - web-based manager” on page 119.

2. Install the corresponding CA root certificate on the remote peer or client. If the remote peer is a FortiGate unit, see “To install a CA root certificate” on page 120.

3. Install the certificate revocation list (CRL) from the issuing CA on the remote peer or client. If the remote peer is a FortiGate unit, see “To import a certificate revocation list” on page 120.

4. In the VPN phase 1 configuration, set Authentication Method to RSA Signature and from the Certificate Name list select the certificate that you installed in Step 1.

To authenticate a VPN peer using a certificate, you must install a signed server certificate on the peer. Then, on the FortiGate unit, the configuration depends on whether there is only one VPN peer or if this is a dialup VPN that can have multiple peers.

To configure certificate authentication of a single peer

1. Install the CA root certificate and CRL.

2. Create a PKI user to represent the peer. Specify the text string that appears in the Subject field of the user’s certificate and then select the corresponding CA certificate.

3. In the VPN phase 1 Peer Options, select Accept this peer certificate only and select the PKI user that you created.
To configure certificate authentication of multiple peers (dialup VPN)

1. Install the corresponding CA root certificate and CRL.
2. Create a PKI user for each remote VPN peer. For each user, specify the text string that appears in the Subject field of the user’s certificate and then select the corresponding CA certificate.
3. Use the `config user peergrp` CLI command to create a peer user group. Add to this group all of the PKI users who will use the IPsec VPN. In the VPN phase 1 Peer Options, select Accept this peer certificate group only and select the peer group that you created.

Example — Generate a CSR on the FortiGate unit

This example follows all the steps required to create and install a local certificate on the FortiGate unit, without using CA software.

The FortiGate unit is called myFortiGate60, and is located at 10.11.101.101 (a private IP address) and http://myfortigate.example.com. Mr. John Smith (john.smith@myfortigate.example.com) is the IT administrator for this FortiGate unit, and the unit belongs to the Sales department located in Greenwich, London, England.

To generate a certificate request on the FortiGate unit - web-based manager

1. Go to System > Certificates > Local Certificates.
2. Select Generate.
3. In the Certificate Name field, enter myFortiGate60 (since the IP address is private, we will use the FQDN instead).
5. Enter values in the Optional Information area to further identify the FortiGate unit.

<table>
<thead>
<tr>
<th>Organization Unit</th>
<th>Sales.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Example.com</td>
</tr>
<tr>
<td>Locality (City)</td>
<td>Greenwich</td>
</tr>
<tr>
<td>State/Province</td>
<td>London</td>
</tr>
<tr>
<td>Country</td>
<td>England</td>
</tr>
<tr>
<td>e-mail</td>
<td><a href="mailto:john.smith@myfortigate.example.com">john.smith@myfortigate.example.com</a></td>
</tr>
</tbody>
</table>

6. From the Key Size list, select 2048 Bit or the most secure option available to you.
7. In Enrollment Method, select File Based to generate the certificate request.
8. Select OK.

The request is generated and displayed in the Local Certificates list with a status of PENDING.

FortiGate IPSec VPNs do not support CRL lookups.
9 Select the Download button to download the request to the management computer.
10 In the File Download dialog box, select Save and save the Certificate Signing Request on the local file system of the management computer.
11 Name the file and save it on the local file system of the management computer.

Example — Generate and Import CA certificate with private key pair on OpenSSL

This example explains how to generate a certificate using OpenSSL on MS Windows. OpenSSL is available for Linux and Mac OS as well, however their terminology will vary slightly from what is presented here.

Assumptions

Before starting this procedure, ensure that you have downloaded and installed OpenSSL on Windows. One source is http://www.slproweb.com/products/Win32OpenSSL.html.

Generating and importing the CA certificate and private key

The two following procedures will generate a CA certificate file and private key file, and then import it to the FortiGate unit as a local certificate.

To generate the private key and certificate

1 At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the following command:
   `cd c:\OpenSSL-Win32\bin`
2 Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet123.
   `openssl genrsa -des3 -out fgtcapriv.key 2048`
   This command generates an RSA DES3 2038-bit encryption key.
3 The following command will generate the certificate using the key from the previous step.
   `openssl req -new -x509 -days 3650 -extensions v3_ca -key fgtcapriv.key -out fgtca.crt`
   This step generates an X509 CA certificate good for 10 years that uses the key generated in the previous step. The certificate filename is fgtca.crt.
   You will be prompted to enter information such as PEM Pass Phrase from the previous step, Country Name, State, Organization Name, Organizational Unit (such as department name), Common Name (the FQDN), and Email Address.

To import the certificate to the FortiGate unit - web-based manager

1 Go to System > Certificates > Local Certificates.
2 Select Import.
3 Select Certificate for Type.
   Fields for Certificate file, Key file, and Password are displayed.
4 For Certificate file, enter `c:\OpenSSL-Win32\bin\fgtca.crt`
5 For Key file, enter `c:\OpenSSL-Win32\bin\fgtcapriv.key`
6. For Password, enter the PEM Pass Phrase you entered earlier, such as fortinet123.
7. Select OK.

The Certificate will be added to the list of Local Certificates and be ready for use. It will appear in the list as the filename you uploaded — fgtca. You can add comments to this certificate to make it clear where it’s from and how it is intended to be used. If you download the certificate from FortiOS, it is a .CER file.

It can now be used in “Authenticating IPsec VPN users with security certificates” on page 126, and “Authenticating SSL VPN users with security certificates” on page 125.

Optionally, you can install the certificate as a CA Certificate. CA certificates are used in HTTPS proxy/inspection. To do this, under CA Certificates select Import. Select Local PC and enter the certificate file c:\OpenSSL-Win32\bin\fgtca.crt. Then select OK. This certificate will be displayed in the CA Certificate list under the name CA_Cert_1.

Example — Generate an SSL certificate in OpenSSL

This example explains how to generate a CA signed SSL certificate using OpenSSL on MS Windows. OpenSSL is available for Linux and Mac OS as well, however their terminology will vary slightly from what is presented here.

This example includes:
- Assumptions
- Generating a CA signed SSL certificate
- Generating a self-signed SSL certificate
- Import the SSL certificate into FortiOS

Assumptions

- Before starting this procedure, ensure that you have downloaded and installed OpenSSL on MS Windows. One download source is http://www.slproweb.com/products/Win32OpenSSL.html.

Generating a CA signed SSL certificate

This procedure assumes:

- you have already completed “Example — Generate and Import CA certificate with private key pair on OpenSSL” on page 128 successfully.

To generate the CA signed SSL certificate

1. At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the following command:
   ```
   cd c:\OpenSSL-Win32\bin
   ```

2. Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet.
   ```
   openssl genrsa -des3 -out fgtssl.key 2048
   ```
   This command generates an RSA DES3 2038-bit encryption key.

3. Create a certificate signing request for the SSL certificate. This step requires you to enter the information listed in step 3 of the previous example — “To generate the private key and certificate” on page 128. You can leave the Challenge Password blank.
   ```
   openssl req -new -key fgtssl.key -out fgtssl.csr
   ```
4 Using the CSR from the previous step, you can now create the SSL certificate using the CA certificate that was created in "Example — Generate and Import CA certificate with private key pair on OpenSSL" on page 128.

```bash
openssl x509 -req -days 365 -in fgtssl.csr -CA fgtca.crt -CAkey fgtcapriv.key -set_serial 01 -out fgtssl.crt
```

This will generate an X.509 certificate good for 365 days signed by the CA certificate fgtca.crt.

**Generating a self-signed SSL certificate**

This procedures does not require any existing certificates.

1 At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the following command:

```bash
cd c:\OpenSSL-Win32\bin
```

2 Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet.

```bash
openssl genrsa -des3 -out fgtssl.key 2048
openssl req -new -key fgtssl.key -out fgtssl.csr
openssl x509 -req -days 365 -in fgtssl.csr -signkey fgtssl.key -out fgtssl.crt
```

These commands:

- generate an RSA 3DES 2048-bit private key,
- generate an SSL certificate signing request, and
- sign the CSR to generate an SSL .CRT certificate file.

**Import the SSL certificate into FortiOS**

**To import the certificate to FortiOS- web-based manager**

1 Go to System > Certificates > Local Certificates.

2 Select Import.

3 Select Certificate for Type.

   Fields for Certificate file, Key file, and Password are displayed.

4 For Certificate file, enter `c:\OpenSSL-Win32\bin\fgtssl.crt`.

5 For Key file, enter `c:\OpenSSL-Win32\bin\fgtssl.key`.

6 For Password, enter the PEM Pass Phrase you entered, such as fortinet.

7 Select OK.

The SSL certificate you just uploaded can be found under System > Certificates > Local Certificates under the name of the file you uploaded — fgtssl.

**To confirm the certificate is uploaded properly - CLI**

```bash
config vpn certificate local
edit fgtssl
get
end
```

The get command will display all the certificate's information. If it is not there or the information is not correct, you will need to remove the corrupted certificate (if it is there) and upload it again from your PC.
To use the new SSL certificate - CLI

    config vpn ssl settings
    set servercert fgtssl
    end

This assigns the fgtssl certificate as the SSL server certificate. For more information see the FortiOS Handbook SSL VPN guide
FSSO integration with Windows AD or Novell

This chapter provides information, installation instructions, and troubleshooting for Fortinet Single Sign On (FSSO) agent. Earlier versions of this product were named Fortinet Server Authentication Extension (FSAE).

The following topics are included:

- Introduction to FSSO
- FSSO for Windows AD
- FSSO for Novell eDirectory
- Configuring FSSO on FortiGate units
- FortiOS FSSO log messages
- Testing FSSO
- Troubleshooting FSSO

Introduction to FSSO

The Fortinet Single Sign On (FSSO) agent connects FortiGate Fortinet security appliances to the corporate authentication servers, such as Microsoft Active Directory and Novell E-Directory, allowing security policies to be defined on the FortiGate unit based on the user information residing on the corporate authentication servers. FSSO, a component installed on the authentication server or a standalone server, provides user authentication information to the FortiGate unit so users can automatically gain access to the permitted resources with a single sign on. Older versions were called Fortinet Server Authentication Extension (FSAE).

On a Microsoft Windows or Novell network, users authenticate with the Active Directory or Novell eDirectory at logon. It would be inconvenient if users then had to enter another username and password for network access through the FortiGate unit. FSSO provides authentication information to the FortiGate unit so that users automatically get access to permitted resources.

There are several mechanisms for passing user authentication information to the FortiGate unit:

- FSSO software installed on a Windows AD network monitors user logons and sends the required information to the FortiGate unit. The FSSO software can obtain this information by polling the AD domain controllers or by using an FSSO agent on each AD domain controller that monitors user logons in real time. Optionally, a FortiGate unit running FortiOS 3.0 MR6 or later can obtain group information directly from AD using Lightweight Directory Access Protocol (LDAP). See “Using FSSO in a Windows AD environment” on page 134.
On a Windows AD network, the FSSO software can also serve NT LAN Manager (NTLM) requests coming from client browsers (forwarded by the FortiGate unit) with only one or more Controller agents installed. See “NTLM authentication with FSSO” on page 137.

FSSO software installed on a Novell network monitors user logons and sends the required information to the FortiGate unit. The FSSO software can obtain information from the Novell eDirectory using either the Novell API or LDAP. See “Using FSSO in a Novell eDirectory environment” on page 140.

A FortiAuthenticator server can act as a replacement for the Collector agent in polling mode in a Windows AD network. FortiAuthenticator can also be configured with internal or external LDAP and RADIUS servers. For more information, see the FortiAuthenticator Administration Guide.

Consult the latest FortiOS and FSSO Release Notes for operating system compatibility information.

### Using FSSO in a Windows AD environment

FSSO installed in a Windows AD environment can provide two kinds of services:

- Monitor user logon activity and send the information to FortiGate unit so that the FortiGate unit can support Single user Sign On (SSO).
- Provide NTLM authentication service for requests coming from FortiGate.

SSO is very convenient for users, but may not be supported across all platforms. NTLM is not as convenient, but it enjoys wider support.

FSSO is certified for the Microsoft Windows Server 2003 (32- and 64-bit editions) and is supported on the Microsoft Windows Server 2008 (32- and 64-bit editions) operating systems.

### FSSO security

When the different components of FSSO are communicating there are some inherent security features.

FSSO installation requires an account with network admin privileges. The security inherent in these types of accounts helps ensure access to FSSO configurations is not tampered with.

User passwords are never sent between FSSO components. The information that is sent is information to identify a user including the username, group or groups, and IP address. NTLM uses base-64 encoded packets, and uses a unique randomly generated challenge nonce to avoid sending user information and password between the client and the server. For more information on NTLM, see “NTLM authentication with FSSO” on page 137.

### FSSO Controller agent (CA)

The FSSO Controller agent (CA), or FSSO agent, is a service installed on a Windows computer that has access to both the FortiGate unit and each of the domain controller agents (DC agents).

The CA is responsible for DNS lookups, group verification, workstation checks, and as mentioned FortiGate updates of logon records. The FSSO Collector Agent sends Domain Local Security Group and Global Security Group information to FortiGate units. The CA communicates with the FortiGate over TCP port 8000 and it listens on UDP port 8002 for updates from the DC agents.
The FortiGate unit can have up to five CAs configured for redundancy. If the first on the list is unreachable, the next is attempted, and so on down the list until one is contacted. See “Configuring FSSO on FortiGate units” on page 158.

All DC agents must point to the correct Collector agent port number and IP address on domains with multiple DCs. See “Configuring Collector agent settings” on page 146.

**FSSO user logon event monitoring**

A FSSO agent installed in a Windows AD environment monitors which users logon to which workstations and pass that information to the FortiGate unit. The FortiGate uses that information to apply its security policies.

When a Windows AD user logs on at a workstation in a monitored domain, FSSO

- detects the logon event and records the workstation name, domain, and user,
- resolves the workstation name to an IP address,
- uses Active Directory to determine which groups the user belongs to,
- sends the user logon information, including IP address and groups list, to the FortiGate unit
- creates one or more log entries on the FortiGate unit for this logon event as appropriate.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. The selection consist of matching the FSSO group or groups the user belongs to with the security policy or policies that match that group. If the user belongs to one of the permitted user groups associated with that policy, the connection is allowed. Otherwise the connection is denied.

With Windows AD, FSSO can use one of two different working modes to monitor user logon activity: DC Agent mode or Polling mode.

**Table 7: FSSO DC Agent mode versus Polling mode**

<table>
<thead>
<tr>
<th></th>
<th>DC Agent mode</th>
<th>Polling Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Installation</strong></td>
<td>Complex — Multiple installations: one agent per DC plus Controller agent, requires a reboot</td>
<td>Easy — only Controller agent installation, no reboot required</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Shares resources with DC system</td>
<td>Has own resources</td>
</tr>
<tr>
<td><strong>Network load</strong></td>
<td>Each DC agent requires minimum 64kbps bandwidth, adding to network load</td>
<td>Increase polling period during busy period to reduce network load</td>
</tr>
<tr>
<td><strong>Level of Confidence</strong></td>
<td>Captures all logons</td>
<td>Potential to miss a login if polling period is too great</td>
</tr>
</tbody>
</table>

**DC Agent mode**

DC Agent mode is the standard mode for FSSO. In DC Agent mode (see Figure 6), a Fortinet authentication agent is installed on each domain controller. These DC agents monitor user logon events and pass the information to the Collector agent, which stores the information and sends it to the FortiGate unit.
The DC agent installed on the domain controllers is not a service like the Collector agent — it is a DLL file called dcagent.dll and is installed in the Windows\system32 directory. It must be installed on all domain controllers of the domains that are being monitored.

Figure 6: FSSO in DC agent mode

DC Agent mode provides reliable user logon information, however you must install a DC agent on every domain controller. A reboot is needed after the agent is installed. Each installation requires some maintenance as well. For these reasons it may not be possible to use the DC Agent mode.

Each domain controller connection needs a minimum guaranteed 64kpbs bandwidth to ensure proper FSSO functionality. You can optionally configure traffic shapers on the FortiGate unit to ensure this minimum bandwidth is guaranteed for the domain controller connections.

Polling mode

In Polling mode there are two options — NetAPI polling, and Event log polling. Both share the advantages of being transparent and agentless.

NetAPI polling is used to retrieve server logon sessions. This includes the logon event information for the Controller agent. NetAPI runs faster than Event log polling but it may miss some user logon events under heavy system load. It requires a query round trip time of less than 10 seconds.

Event log polling may run a bit slower, but will not miss events, even when the installation site has many users that require authentication. It does not have the 10 second limit or NetAPI polling. Event log polling requires fast network links. Event log polling is required if there are Mac OS users logging into Windows AD.

In Polling mode (see Figure 7), the Collector agent polls port 445 of each domain controller for user logon information every few seconds and forwards it to the FortiGate unit. There are no DC Agents installed, so the Collector agent polls the domain controllers directly.
A major benefit of Polling mode is that no FSSO DC Agents are required. If it is not possible to install FSSO DC Agents on your domain controllers, this is the alternate configuration available to you. Polling mode results in a less complex install, and reduces ongoing maintenance. The minimum permissions required in Polling mode are to read the event log or call NetAPI. To install FSSO with minimum permissions, see “Installing FSSO without using an administrator account” on page 143.

**NTLM authentication with FSSO**

In a Windows AD network, FSSO can also provide NTLM authentication service to the FortiGate unit. When the user makes a request that requires authentication, the FortiGate unit initiates NTLM negotiation with the client browser. The FortiGate unit does not process the NTLM packets itself. Instead, it forwards all the NTLM packets to the FSSO service to process.

NTLM has the benefit of not requiring an FSSO agent, but it is not transparent to users, and the user’s web browser must support NTLM.

The NTLM protocol protects the user’s password by not sending it over the network. Instead, the server sends the client a random number that the client must encrypt with the hash value of the user’s password. The server compares the result of the client’s encryption with the result of its own encryption. The two will match only if both parties used the same password.
If the NTLM authentication with the Windows AD network is successful, and the user belongs to one of the groups permitted in the applicable security policy, the FortiGate unit allows the connection.

Fortinet has tested NTLM authentication with Internet Explorer and Firefox browsers.

**NTLM in a multiple domain environment**

In a multiple domain environment for NTLM, the important factor is that there is a trust relation between the domains. In a forest, this relation is automatically created. So you can install FSSO agent on one of the domain controllers without worry.

But in case of multiple domains that are not in a forest, you need to create a trust relation between the domains. If you do not want to have a trust relation between your multiple domains, you need to use FSAE 4.0 MR1 and the DC agent needs to be installed once on each domain. Then you can use security policies to configure server access.

In Figure 9, three domains are shown connected to the FSSO Collector agent server. The Client logs on to their local Domain Controller, which then sends the user logon event information to the Collector Agent. When the Client attempts to access the Internet, the FortiGate unit contacts the Collector Agent for the logon information, sees the Client is authenticated, and allows access to the Internet. There are multiple domains each with a domain controller agent (DCagent) that sends logon information to the Collector agent. If the multiple domains have a trust relationship, only one DCagent is required instead of one per domain.
Understanding the NTLM authentication process

1. The user attempts to connect to an external (internet) HTTP resource. The client application (browser) on the user’s computer issues an unauthenticated request through the FortiGate unit.

2. The FortiGate is aware that this client has not authenticated previously, so responds with a 401 Unauthenticated status code, and tells the client which authentication method to reply with in the header: Proxy-Authenticated: NTLM. Then the initial session is dismantled.

3. The client application connects again to the FortiGate, and issues a GET-request, with a Proxy-Authorization: NTLM <negotiate string> header. <negotiate-string> is a base64-encoded NTLM Type 1 negotiation packet.

4. The FortiGate unit replies with a 401 “proxy auth required” status code, and a Proxy-Authenticate: NTLM <challenge string> (a base 64-encoded NTLM Type 2 challenge packet). In this packet is the challenge nonce, a random number chosen for this negotiation that is used once and prevents replay attacks.

5. The client sends a new GET-request with a header: Proxy-Authenticate: NTLM <authenticate string>, where <authenticate string> is a NTLM Type 3 Authentication packet that contains:
   - username and domain
   - the challenge nonce encoded with the client password (it may contain the challenge nonce twice using different algorithms).

The TCP connection must be kept alive, as all subsequent authentication-related information is tied to the TCP connection. If it is dropped, the authentication process must start again from the beginning.
6 If the negotiation is successful and the user belongs to one of the groups permitted in the security policy, the connection is allowed. Otherwise, the FortiGate unit denies the authentication by issuing a 401 return code and prompts for a username and password. Unless the TCP connection is broken, no further credentials are sent from the client to the proxy.

If the authentication policy reaches the authentication timeout period, a new NTLM handshake occurs.

Using FSSO in a Novell eDirectory environment

FSSO in a Novell eDirectory environment works similar to the FSSO Polling mode in the Windows AD environment. The eDirectory agent polls the eDirectory servers for user logon information and forwards it to the FortiGate unit.

When a user logs on at a workstation, FSSO:
- detects the logon event by polling the eDirectory server and records the IP address and user ID,
- looks up in the eDirectory which groups this user belongs to,
- sends the IP address and user groups information to the FortiGate unit.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FSSO is supported on the Novell E-Directory 8.8 operating system

FSSO for Windows AD

This section explains what the FSSO components are for Windows AD, how to install them, and how to configure them.

- FSSO components for Windows AD
- Standard versus Advanced mode
- Installing FSSO for Windows AD
- Configuring Fortinet Single Sign On with Windows AD

FSSO components for Windows AD

FSSO has two components, or agents, to install on your network:
- the Collector agent must be installed on one or more network computers
- the Domain Controller (DC) agent must be installed on every domain controller if you will use DC Agent mode, but is not required if you use Polling mode.

FSSO is supported on Microsoft Windows Server 2003 (32- and 64-bit editions) and Microsoft Windows Server 2008 (32- and 64-bit editions) operating systems.
FSSO Installation

The FSSO installer first installs the Collector agent. You can then continue with installation of the DC agent, or you can install it later by going to Start > Programs > Fortinet > Fortinet Server Authentication Extension > Install DC Agent. The installer will install a DC agent on the domain controllers of all of the trusted domains in your network.

Each domain controller connection needs a minimum guaranteed 64kpbs bandwidth to ensure proper FSSO functionality. Traffic shapers configured on the FortiGate can help guarantee these minimum bandwidths.

You can create a redundant configuration if you install the Collector agent on two or more servers. This provides improved reliability. If the current Collector agent fails, the FortiGate unit will switch to the next Collector agent in its list. The list can have up to five Collector agents.

In Windows 2008 by default, you do not have administrative user rights if you are logged on as a user other than as the built-in administrator, even if you were added to the local Administrators group on the computer.

Ensure you have administrative rights on the servers where you are installing FSSO. Best practices dictate that you install FSSO using the built-in local administrator account. If you are logged on to another account and try to install FSSO, you may see a security alert dialog box requesting your permission to use or install the program.

Best practices dictate that before installing FSSO, you create a dedicated account with administrator privileges and a password that does not expire. Optionally, you can install FSSO without an admin account. See “Installing FSSO without using an administrator account” on page 143.

Standard versus Advanced mode

Part of installing FSSO for Windows is choosing Standard or Advanced mode. The main difference between Standard and Advanced mode is the naming convention used when referring to username information.

Standard mode uses regular Windows convention: Domain\Username. Advanced mode uses LDAP convention: CN=User, OU=Name, DC=Domain.

If there is no special requirement to use LDAP—best practices dictate you setup FSSO in Standard mode. This mode is easier to setup, and is usually easier to maintain and troubleshoot.

Standard and advanced modes have the same level of functionality with the following exceptions:

1. Users have to create Group filters on the Collector agent. This differs from Advanced mode where Group filters are configured from the FortiGate unit. Fortinet strongly encourages users to create filters from CA.

2. Advanced mode supports nested or inherited groups. This means that users may be a member of multiple monitored groups. Standard mode does not support nested groups so a user must be a direct member of the group being monitored.

Installing FSSO for Windows AD

To install FSSO, you must obtain the FSSO Setup file from the Fortinet Support web site. Then you follow these two installation procedures on the server that will run the Collector agent. This can be any server or domain controller that is part of your network. These procedures also installs the DC Agent on all of the domain controllers in your network.
To install the Collector agent

1. Create an account with administrator privileges and a password that does not expire. See Microsoft Advanced Server documentation for help with this task.
   
   To use a non-admin read only account, see “Installing FSSO without using an administrator account” on page 143.

2. Logon to the account that you created in Step 1.

3. Double-click the FSSOSetup.exe file.
   
   The FSSO InstallShield Wizard starts.

4. Select Next. Optionally, you can change the installation location.

5. Select Next.

   This procedure will install using the currently running account. If you want FSSO to use another existing admin account, change the username: field in the InstallShield Wizard to the correct username using the format DomainName\UserName. For example if the account is jsmith and the domain is example_corp you would enter example_corp\jsmith in the Username: field.

6. In the Password field, enter the password for the account listed in the username field. This is the account you are logged onto currently.

7. Select Next.

8. By default, FSSO authenticates users both by monitoring logons and by accepting authentication requests using the NTLM protocol.

   If you want to support only NTLM authentication
   
   • Clear the Monitor user logon events and send the information to Fortinet check box.
   
   • Select the Serve NTLM authentication requests coming from FortiGate check box.

   If you do not want to support NTLM authentication
   
   • Clear the Serve NTLM authentication requests coming from FortiGate check box.
   
   • Select the Monitor user logon events and send the information to Fortinet check box.

   You can change these options after installation.

9. Select the access method to use for Windows Directory:

   • Select Standard to use Windows domain and username credentials.
   
   • Select Advanced if you will set up LDAP access to Windows Directory.

   See “Standard versus Advanced mode” on page 141.

10. Select Next and then select Install.

11. For DC Agent mode, when the FSSO InstallShield Wizard completes Collector agent installation, ensure that Launch DC Agent Install Wizard is selected and then select Finish.

   If you see an error such as Service Fortinet Single Sign On agent (service_FSAE) failed to start, there are two possible reasons for this. Verify the user account you selected has sufficient privileges to run the FSSO service. Also verify the computer system you are attempting to install on is a supported operating system and version.
To install the DC Agent

1. If you have just installed the Collector agent, the FSSO - Install DC Agent wizard starts automatically. Otherwise, go to Start > Programs > Fortinet > Fortinet Single Sign On > Install DC Agent.

2. Verify the Collector agent IP address.
   - If the Collector agent computer has multiple network interfaces, ensure that the one that is listed is on your network. The listed Collector agent listening port is the default. Only change this if the port is already used by another service.

3. Select Next.

4. Select the domains to monitor and select Next.
   - If any of your required domains are not listed, cancel the wizard again by going to Start > Programs > Fortinet > Fortinet Single Sign On > Install DC Agent.

5. Optionally, select users that you do not want monitored. These users will not be able to authenticate to FortiGate units using FSSO. You can also do this later. See “Configuring Fortinet Single Sign On with Windows AD” on page 145.

6. Select Next.

7. Optionally, clear the check boxes of domain controllers on which you do not want to install the DC Agent.

8. Select the Working Mode as DC Agent Mode. While you can select Polling Mode here, in that situation you would not be installing a DC Agent. For more information, see “DC Agent mode” on page 135 and “Polling mode” on page 136.

9. Select Next.

10. Select Yes when the wizard requests that you reboot the computer.

If you reinstall the FSSO software on this computer, your FSSO configuration is replaced with default settings.

If you want to create a redundant configuration, repeat the procedure “To install the Collector agent” on page 142 on at least one other Windows AD server.

When you start to install a second Collector agent, cancel the Install Wizard dialog appears the second time. From the configuration GUI, the monitored domain controller list will show your domain controllers un-selected. Select the ones you wish to monitor with this Collector agent, and select Apply.

Before you can use FSSO, you need to configure it on both Windows AD and on the FortiGate units. The next section and “Configuring FSSO on FortiGate units” on page 158 will help you accomplish these two tasks.

**Installing FSSO without using an administrator account**

Normally when installing services in Windows, it is best to use the Domain Admin account, as stated earlier. This ensures installation goes smoothly and uninterrupted, and when using the FSSO agent there will be no permissions issues. However, it is possible to install FSSO with a non-admin account in Windows 2003 or 2008 AD.

The following instructions for Windows 2003 are specific to the event log polling mode only. Do not use this procedure with other FSSO configurations.
Windows 2003

There are two methods in Windows 2003 AD for installing FSSO without an admin account — add the non-admin user to the security log list, and use a non-admin account with read-only permissions. A problem with the first method is that full rights (read, write, and clear) are provided to the event log. This can be a problem when audits require limited or no write access to logs. In those situations, the non-admin account with read-only permissions is the solution.

To add the non-admin user account to the Windows 2003 security log list

1. Go to Default Domain Controller Security Settings > Security Settings > User Rights Assignment > Manage auditing and security log.
2. Add the user account to this list.
3. Repeat these steps on every domain controller in Windows 2003 AD.
4. A reboot is required.

To use a non-admin account with read-only permissions to install FSSO on Windows 2003

The following procedure provides the user account specified with read only access to the Windows 2003 AD Domain Controller Security Event Log which allows FSSO to function.

1. Find out the SID of the account you intend to use.
2. Then create the permission string. For example:
   (A;;0x1;;;S-1-5-21-4136056096-764329382-1249792191-1107)
   A means Allow,
   0x1 means Read, and
   S-1-5-21-4136056096-764329382-1249792191-1107 is the SID.
3. Then, append it to the registry key
4. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Security\CustomSD.
5. Repeat these steps on every domain controller in Windows 2003 AD.
6. A reboot is required.

Windows 2008

In Windows 2008 AD, if you do not want to use the Domain Admin account then the user account that starts the FSSO agent needs to be added to the Event Log Readers group.

When the user is added to the Event Log Readers group, that user is now allowed to have read only access to the event log and this is the minimal rights required for FSSO to work.

Updating FSSO with Windows AD

After FSSO is installed on your network, you may want to upgrade to a newer version. The following procedure helps ensure you have a trouble free upgrade. How you update FSSO depends on if you are using polling mode or DCAgent mode.

For polling mode, since there are no DC agents you only need to upgrade the Collector. However in DCAgent mode, each DC Agent must be updated as well.
To update FSSO in DCAgent mode

1. Go to the system32 directory on all DC’s and rename the dcagent.dll file to dcagent.dll.old.
   This ensures the when the upgrade is pushed to the DC it does not overwrite the old file. If there are any problems this makes it easy to revert to the old version.

2. Run the FSSO setup .exe file to update the collector. When this is completed, ignore any reboot message.

3. Go to Programs > Fortinet > Fortinet Single Sign On > Install DC Agent and push the DC agent out to all servers. All DC’s will now need to be rebooted so that the new dll file is loaded.

4. After the reboot, go to all DC’s and delete the dcagent.dll.old files.

Configuring Fortinet Single Sign On with Windows AD

On the FortiGate unit, security policies control access to network resources based on user groups. With Fortinet Single Sign On, this is also true but each FortiGate user group is associated with one or more Windows AD user groups. This is how Windows AD user groups get authenticated in the FortiGate security policy.

Fortinet Single Sign On sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate units.

To avoid this problem, you can configure the Fortinet Single Sign On Collector agent to send logon information only for groups named in the FortiGate unit’s security policies. See “Configuring FortiGate group filters” on page 151.

On each server with a Collector agent, you will be

- Configuring Windows AD server user groups
- Configuring Collector agent settings, including the domain controllers to be monitored
- Configuring Directory Access settings
- Configuring the Ignore User List
- Configuring FortiGate group filters for each FortiGate unit
- Configuring FSSO ports
- Configuring alternate user IP address tracking

In some environments where user IP addresses change frequently, it might be necessary to configure the alternate IP address tracking method. For more information, see “Configuring alternate user IP address tracking” on page 153.

Configuring Windows AD server user groups

FortiGate units control network resource access at the group level. All members of a user group have the same network access as defined in FortiGate security policies.

You can use existing Windows AD user groups for authentication to FortiGate units if you intend that all members within each group have the same network access privileges.
Otherwise, you need to create new user groups for this purpose.

If you change a user’s group membership, the change does not take effect until the user logs off and then logs on again.

The FSSO Agent sends only Domain Local Security Group and Global Security Group information to FortiGate units. You cannot use Distribution group types for FortiGate access. No information is sent for empty groups.

Refer to Microsoft documentation for information about creating and managing Windows AD user groups.

Configuring Collector agent settings

You need to configure which domain controllers the Collector agent will use and which domains to monitor for user logons. You can also alter default settings and settings you made during installation. These tasks are accomplished by configuring the FSSO Collector Agent, and selecting either Apply to enable the changes.

At any time to refresh the FSSO Agent settings, select Apply.

To configure the Collector agent

1. From the Start menu, select Programs > FortiNet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.
Enter the following information and then select **Save&Close**.

<table>
<thead>
<tr>
<th><strong>Monitoring user logon events</strong></th>
<th>Select to automatically authenticate users as they logon to the Windows domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support NTLM authentication</strong></td>
<td>Select to facilitate logon of users who are connected to a domain that does not have the FSSO DC Agent installed.</td>
</tr>
<tr>
<td><strong>Collector Agent Status</strong></td>
<td>Shows RUNNING when Collector agent is active.</td>
</tr>
<tr>
<td><strong>Listening ports</strong></td>
<td>You can change FSSO Collector Agent related port numbers if necessary.</td>
</tr>
<tr>
<td><strong>FortiGate</strong></td>
<td>TCP port for FortiGate units. Default 8000.</td>
</tr>
<tr>
<td><strong>DC Agent</strong></td>
<td>UDP port for DC Agents. Default 8002.</td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Log level</strong></td>
<td>Select the minimum severity level of logged messages.</td>
</tr>
<tr>
<td><strong>Log file size limit (MB)</strong></td>
<td>Enter the maximum size for the log file in MB.</td>
</tr>
<tr>
<td><strong>View Log</strong></td>
<td>View all Fortinet Single Sign On agent logs.</td>
</tr>
<tr>
<td><strong>Log logon events in separate logs</strong></td>
<td>Record user login-related information separately from other logs. The information in this log includes data received from DC agents user logon/logoff information workstation IP change information data sent to FortiGate units</td>
</tr>
<tr>
<td><strong>View Logon Events</strong></td>
<td>If <strong>Log logon events in separate logs</strong> is enabled, you can view user login-related information.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Require authenticated connection from FortiGate</strong></td>
<td>Select to require the FortiGate unit to authenticate before connecting to the Collector agent.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “fortinetcanada”.</td>
</tr>
</tbody>
</table>
### Timers

| **Workstation verify interval (minutes)** | Enter the interval in minutes at which the Fortinet Single Sign On Collector agent connects to client computers to determine whether the user is still logged on. The default is every 5 minutes. The interval may be increased if your network has too much traffic.  

**Note:** This verification process creates security log entries on the client computer.  
If ports 139 or 445 cannot be opened on your network, set the interval to 0 to prevent checking. See “Configuring FSSO ports” on page 152. |
| **Dead entry timeout interval** | Enter the interval in minutes after which Fortinet Single Sign On Agent purges information for user logons that it cannot verify. The default is 480 minutes (8 hours).  
Dead entries usually occur because the computer is unreachable (such as in standby mode or disconnected) but the user has not logged off. A common reason for this is when users forget to logoff before leaving the office for the day.  
You can also prevent dead entry checking by setting the interval to 0. |
| **IP address change verify interval** | Fortinet Single Sign On Agent periodically checks the IP addresses of logged-in users and updates the FortiGate unit when user IP addresses change. IP address verification prevents users from being locked out if they change IP addresses, as may happen with DHCP assigned addresses.  
Enter the verification interval in seconds. The default is 60 seconds. You can enter 0 to prevent IP address checking if you use static IP addresses.  
This does not apply to users authenticated through NTLM. |
| **Cache user group lookup result** | Enable caching.  
Caching can reduce group lookups and increase performance. |
| **Cache expire in (minutes)** | Fortinet Single Sign On Agent caches group information for logged-in users.  
Enter the duration in minutes after which the cache entry expires. If you enter 0, the cache never expires.  
A long cache expire interval may result in more stale user group information. This can be an issue when a user’s group information is changed. |
| **Clear Group Cache** | Clear group information of logged-in users.  
This affects all logged-in users, and may force them to re-logon. |
## Configuring Directory Access settings

The FSSO Collector Agent can access Windows Active Directory in one of two modes:

- **Standard** — the FSSO Collector Agent receives group information from the Collector agent in the `domain\user` format. This option is available on FortiOS 3.0 and later.

<table>
<thead>
<tr>
<th>Common Tasks</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show Service Status</strong></td>
<td>View information about the status of the Collector agent and connected FortiGate units. See “Viewing FSSO component status” on page 153.</td>
</tr>
<tr>
<td><strong>Show Monitored DCs</strong></td>
<td>Shows detailed information about connected Domain Controller agents. Use the Select DC to Monitor button to select domain controllers to monitor and choose Working Mode. See “Selecting Domain Controllers and working mode for monitoring” on page 154.</td>
</tr>
<tr>
<td><strong>Show Logon Users</strong></td>
<td>View a list of currently logged-in users. Select the column headers to sort the list.</td>
</tr>
<tr>
<td><strong>Select Domains to Monitor</strong></td>
<td>Select this button to remove domains that you do not want to monitor. From the Domain Filter dialog box that displays, clear check boxes for unwanted domains and select OK.</td>
</tr>
<tr>
<td><strong>Set Directory Access Information</strong></td>
<td>See “Configuring Directory Access settings” on page 149.</td>
</tr>
<tr>
<td><strong>Set Group Filters</strong></td>
<td>Configure group filtering for each FortiGate unit. See “Configuring FortiGate group filters” on page 151.</td>
</tr>
<tr>
<td><strong>Set Ignore User List</strong></td>
<td>Exclude users such as system accounts that do not authenticate to any FortiGate unit. See “Configuring the Ignore User List” on page 150.</td>
</tr>
<tr>
<td><strong>Sync Configuration With Other Agents</strong></td>
<td>Copy this Collector agent’s Ignore User List and Group Filters to the other Collector agents to synchronize the configuration. You are asked to confirm synchronization for each Collector agent.</td>
</tr>
<tr>
<td><strong>Export Configuration</strong></td>
<td>Export Fortinet Single Sign On Agent configuration to a text file. The file is named <code>saved_config.txt</code> and is saved in the Fortinet Single Sign On Agent program directory.</td>
</tr>
<tr>
<td><strong>Save &amp; Close</strong></td>
<td>Save the modified settings and exit.</td>
</tr>
<tr>
<td><strong>Apply</strong></td>
<td>Apply changes now.</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Change all settings to the default values.</td>
</tr>
<tr>
<td><strong>Help</strong></td>
<td>View the online Help.</td>
</tr>
</tbody>
</table>

To view the version and build number information for your FSSO Collector Agent configuration, selecting the Fortinet icon in the upper left corner of the Collector agent Configuration screen and select About Fortinet Single Sign On Agent configuration.
• Advanced — the FSSO Collector Agent obtains user group information using LDAP. The benefit of this method is that it is possible to nest groups within groups. This option is available on FortiOS 3.0 MR6 and later. The group information is in standard LDAP format.

If you change AD access mode, you must reconfigure your group filters to ensure that the group information is in the correct format.

To configure Directory Access settings
1. From the Start menu select Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.
3. From the AD access mode list, select either Standard or Advanced.
4. If you selected Advanced AD access mode, select Advanced Setting and configure the following settings and then select OK:

<table>
<thead>
<tr>
<th>AD server address</th>
<th>Enter the address of your network’s global catalog server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD server port</td>
<td>The default AD server port is 3268. This must match your server port.</td>
</tr>
<tr>
<td>BaseDN</td>
<td>Enter the Base distinguished name for the global catalog. This is the point in the tree that will be considered the starting point by default.</td>
</tr>
<tr>
<td>username</td>
<td>If the global catalog accepts your Fortinet Single Sign On Agent agent’s credentials, you can leave these fields blank. Otherwise, enter credentials for an account that can access the global catalog.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

BaseDN example
An example DN for Training Fortinet, Canada is DN = ou=training, ou=canada, dc=fortinet, dc=com. If you set the BaseDN to ou=canada, dc=fortinet, dc=com then when Fortinet Single Sign On Agent is looking up user credentials, it will only search the Canada organizational unit, instead of all the possible countries in the company. Its a short cut to entering less information and faster searches.
However, you may have problems if you narrow the BaseDN too much when you have international employees from the company visiting different offices. If someone from Fortinet Japan is visiting the Canada office in the example above, their account credentials will not be matched because they are in DN = ou=japan, dc=fortinet, dc=com instead of the BaseDN ou=canada, dc=fortinet, dc=com. The easy solution is to change the BaseDN to simply be dc=fortinet, dc=com. Then any search will check all the users in the company.

Configuring the Ignore User List
The Ignore User List excludes users that do not authenticate to any FortiGate unit, such as system accounts. The logons of these users are not reported to FortiGate units. This reduces the amount of required resources on the FortiGate unit especially when logging logon events to memory.
To configure the Ignore User List

1. From the Start menu select Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.

2. In the Common Tasks section, select Set Ignore User List.

   The current list of ignored users is displayed. To view ignored usernames, expand each domain.

3. Do any of the following:
   - To remove a user from the list, select the check box beside the username and then select Remove. The user’s login is no longer ignored.
   - To add users to be ignored, select Add, select the check box beside each required username, and then select Add.

4. Select OK.

Configuring FortiGate group filters

FortiGate group filters actively control which user logon information is sent to each FortiGate unit. You need to configure the group filter list so that each FortiGate unit receives the correct user logon information for the user groups that are named in its security policies. These group filters help limit the traffic sent to the FortiGate unit, and help limit the logon events logged.

The maximum number of Windows AD user groups allowed on a FortiGate depends on the model. Low end models up to 300A support 256 Windows AD user groups, where mid and high end models support 1024 groups. This is per VDOM if VDOMs are enabled on the FortiGate unit.

You do not need to configure a group filter on the Collector agent if the FortiGate unit retrieves group information from Windows AD using LDAP. In that case, the Collector agent uses the list of groups you selected on the FortiGate unit as its group filter.

The filter list is initially empty. You need to configure filters for your FortiGate units using the Add function. At a minimum, create a default filter that applies to all FortiGate units without a defined filter.

<table>
<thead>
<tr>
<th>FortiGate SN</th>
<th>The serial number of the FortiGate unit to which this filter applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>An optional description of the role of this FortiGate unit.</td>
</tr>
<tr>
<td>Monitored Groups</td>
<td>The Windows AD user groups that are relevant to the security policies on this FortiGate unit.</td>
</tr>
<tr>
<td>Add</td>
<td>Create a new filter.</td>
</tr>
</tbody>
</table>

If no filter is defined for a FortiGate unit and there is no default filter, the Collector agent sends all Windows AD group and user logon events to the FortiGate unit. While this normally is not a problem, limiting the amount of data sent to the FortiGate unit improves performance by reducing the amount of memory the unit uses to store the group list and resulting logs.

To configure a FortiGate group filter

1. From the Start menu select Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.

2. In the Common Tasks section, select Set Group Filters.

   The FortiGate Filter List opens. It has the following columns:
Select Add to create a new filter. If you want to modify an existing filter, select it in the list and then select Edit.

Enter the following information and then select OK.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default filter</td>
<td>Select to create the default filter. The default filter applies to any FortiGate unit that does not have a specific filter defined in the list.</td>
</tr>
<tr>
<td>FortiGate Serial Number</td>
<td>Enter the serial number of the FortiGate unit to which this filter applies. This field is not available if Default is selected.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this FortiGate unit’s role in your network. For example, you could list the resources accessed through this unit. This field is not available if Default is selected.</td>
</tr>
<tr>
<td>Monitor the following groups</td>
<td>The Collector agent sends to the FortiGate unit the user logon information for the Windows AD user groups in this list. Edit this list using the Add, Advanced and Remove buttons.</td>
</tr>
</tbody>
</table>

**TCP ports for FSSO agent with client computers**

Windows AD records when users log on but not when they log off. For best performance, Fortinet Single Sign On Agent monitors when users log off. To do this, Fortinet Single Sign On Agent needs read-only access to each client computer’s registry over TCP port 139 or 445. Open at least one of these ports — ensure it is not blocked by firewalls.

If it is not feasible or acceptable to open TCP port 139 or 445, you can turn off Fortinet Single Sign On Agent logoff detection. To do this, set the Collector agent workstation verify interval to 0. The FSSO Collector Agent assumes that the logged on computer remains logged on for the duration of the Collector agent dead entry timeout interval — by default this is eight hours.
Configuring ports on the Collector agent computer

On the computer where you install the Collector agent, you must make sure that the firewall does not block the listening ports for the FortiGate unit and the DC Agent. By default, these are TCP port 8000 and UDP port 8002. For more information about setting these ports, see “Configuring Collector agent settings” on page 146.

Configuring alternate user IP address tracking

In environments where user IP addresses change frequently, you can configure Fortinet Single Sign On Agent to use an alternate method to track user IP address changes. Using this method, Fortinet Single Sign On Agent responds more quickly to user IP address changes because it directly queries workstation IP addresses to match users and IP addresses.

This feature requires FSAE version 3.5.27 or later, Fortinet Single Sign On Agent any version, and FortiOS 3.0 MR7 or later.

To configure alternate user IP address tracking
1. On the computer where the Collector agent is installed, go to Start > Run.
2. Enter regedit or regedt32 and select OK.
   The Registry Editor opens.
3. Find the registry key
   HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\collectoragent.
4. Set the supportFSAEauth value (dword) to 00000001.
5. Close the Registry Editor.
6. From the Start menu select Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.
7. Select Apply.
   The Fortinet Single Sign On Agent service restarts with the updated registry settings.

Viewing FSSO component status

It is important to know the status of both your Collector agents and DC agents.

Viewing Collector agent status

Use the Show Service Status to view your Collector agent information in the Status window. The Status window displays:

- the version of the software
- the status of the service
- the number of connected FortiGate units
- connected FortiGate information such as serial number, IP address, and time connected

To view Collector agent status
1. From the Start menu select Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.
2. In the Common Tasks section, select Show Service Status.
   The Fortinet Single Sign On Collector agent Status window opens.
Optionally select Get NTLM statistics in the Status window to display NTLM information such as number of messages received, processed, failed, in the queue.

**Viewing DC agent status**

Use the Show Monitored DCs to view the status of DC agents.

**To view domain controller agent status**

1. From the Start menu select Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.
2. In the Common Tasks section, select Show Monitored DCs.

For each DC Agent, the following information is displayed:

- IP address
- number of logon events received
- the last logon event
- when last logon was received.

To change which DC agents are monitored or change the working mode for logon event monitoring, select Select DC to Monitor.

**Selecting Domain Controllers and working mode for monitoring**

You can change which DC agents are monitored or change the working mode for logon event monitoring between DC agent mode and polling mode.

When polling mode is selected, it will poll port 445 of the domain controller every few seconds to see who is logged on.

1. From the Start menu select Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent.
2. In the Common Tasks section, select Show Service Status.
3. Select Select DC to Monitor.

<table>
<thead>
<tr>
<th>Working Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DC Agent mode</strong></td>
<td>a Domain Controller agent monitors user logon events and passes the information to the Collector agent. This provides reliable user logon information, however you must install a DC agent on every domain controller in the domain.</td>
</tr>
<tr>
<td><strong>Polling mode</strong></td>
<td>the Collector agent polls each domain controller for user logon information. Under heavy system load this might provide information less reliably. However installing a DC agent on each domain controller is not required in this mode.</td>
</tr>
</tbody>
</table>

**FSSO for Novell eDirectory**

The components you need to install depend on whether you are installing FSSO on Windows AD or Novell eDirectory. FSSO supports the Novell E-Directory 8.8 operating system.

This section includes:

- FSSO components for Novell eDirectory
- Installing FSSO for Novell
FSSO components for Novell eDirectory

For a Novell network, there is only one FSSO component to install — the eDirectory agent. In some cases, you also need to install the Novell Client.

Installing FSSO for Novell

To install FSSO, you must obtain the FSAE_Setup_eDirectory file from the Fortinet Support web site. Perform the following installation procedure on the computer that will run the eDirectory agent. This can be any server or domain controller that is part of your network.

This section includes:

- Configuring the eDirectory agent
- Adding an eDirectory server
- Configuring a group filter

To install the FSSO eDirectory agent

1. Create an account with administrator privileges and a password that does not expire. See Novell documentation for more information.
2. Logon to the account that you created in Step 1.
   - The Fortinet eDirectory Agent InstallShield Wizard starts.
4. Optionally, fill in the username and Organization fields.
5. Select the Anyone who uses this computer (all users) option.
6. Select Next.
7. Optionally, enter any of the following information:

<table>
<thead>
<tr>
<th>eDirectory Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
</tr>
<tr>
<td>Use secure connection (SSL)</td>
</tr>
<tr>
<td>Search Base DN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>eDirectory Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
</tr>
<tr>
<td>User password</td>
</tr>
</tbody>
</table>

8. Select Next.
9. Select Install.

Configuring Fortinet Single Sign On with Novell networks

You need to configure the eDirectory agent for it to communicate with eDirectory servers. You may have provided some of this information during installation.

This section includes:

- Configuring the eDirectory agent
• Adding an eDirectory server
• Configuring a group filter

**Configuring the eDirectory agent**

You need to configure the eDirectory agent for it to communicate with eDirectory servers.

**To configure the eDirectory agent**

1. From the Start menu select Programs > Fortinet > eDirectory Agent > eDirectory Config Utility.
2. The eDirectory Agent Configuration Utility dialog opens. Enter the following information and select OK.

### eDirectory Authentication

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Enter a username that has access to the eDirectory, using LDAP format.</td>
</tr>
<tr>
<td>User password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Listening port</td>
<td>Enter the TCP port on which Fortinet Single Sign On Agent listens for connections from FortiGate units. The default is 8000. You can change the port if necessary.</td>
</tr>
<tr>
<td>Refresh interval</td>
<td>Enter the interval in seconds between polls of the eDirectory server to check for new logons. The default is 30 seconds.</td>
</tr>
</tbody>
</table>

### FortiGate Connection Authentication

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require authenticated connection from FortiGate</td>
<td>Select to require the FortiGate unit to authenticate before connecting to the eDirectory Agent.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “FortinetCanada”.</td>
</tr>
<tr>
<td>User logon info search method</td>
<td>Select how the eDirectory agent accesses user logon information: LDAP or Native (Novell API). LDAP is the default. If you select Native, you must also have the Novell Client installed on the PC.</td>
</tr>
</tbody>
</table>

### Logging

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log level</td>
<td>Select Debug, Info, Warning or Error as the minimum severity level of message to log or select None to disable logging.</td>
</tr>
<tr>
<td>Log file size limit (MB)</td>
<td>Enter the maximum size for the log file in MB.</td>
</tr>
<tr>
<td>View Log</td>
<td>View the current log file.</td>
</tr>
<tr>
<td>Dump Session</td>
<td>List the currently logged-on users in the log file. This can be useful for troubleshooting.</td>
</tr>
</tbody>
</table>
Adding an eDirectory server

Once the eDirectory agent is configured, you add one or more eDirectory servers.

To add an eDirectory server

1. In the eDirectory Agent Configuration Utility dialog box (see the preceding procedure, “Configuring the eDirectory agent”), select Add.

2. The eDirectory Setup dialog box opens. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>eDirectory Server Address</th>
<th>Enter the IP address of the eDirectory server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>If the eDirectory server does not use the default port 389, clear the Default check box and enter port number.</td>
</tr>
<tr>
<td>Use default credential</td>
<td>Select to use the credentials specified in the eDirectory Configuration Utility. See “Configuring the eDirectory agent” on page 156. Otherwise, leave the check box clear and enter a username and Password below.</td>
</tr>
<tr>
<td>username</td>
<td>Enter a username that has access to the eDirectory, using LDAP format.</td>
</tr>
<tr>
<td>User password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Use secure connection (SSL)</td>
<td>Select to connect to the eDirectory server using SSL security.</td>
</tr>
<tr>
<td>Search Base DN</td>
<td>Enter the base Distinguished Name for the user search.</td>
</tr>
</tbody>
</table>

Configuring a group filter

The eDirectory agent sends user logon information to the FortiGate unit for all user groups unless you either configure an LDAP server entry for the eDirectory on the FortiGate unit and select the groups that you want to monitor configure the group filter on the eDirectory agent.

If both the FortiGate LDAP configuration and the eDirectory agent group filter are present, the FortiGate user group selections are used.

To configure the group filter

1. From the Start menu select Programs > Fortinet > eDirectory Agent > eDirectory Config Utility.

2. Select Group Filter.
3 Do one of the following:
   • Enter group names, then select Add.
   • Select Advanced, select groups, and then select Add.
4 Select OK.

Configuring FSSO on FortiGate units

To configure your FortiGate unit to operate with either a Windows AD or a Novell eDirectory FSSO install, you
   • Configure LDAP access to the Novell eDirectory or Windows AD global catalog. Skip this step if you are using FSSO Standard mode. See “Configuring LDAP server access” on page 158.
   • Specify the Collector agent or Novell eDirectory agent that will provide user logon information. See “Specifying your Collector agents or Novell eDirectory agents” on page 160.
   • Add Active Directory user groups to FortiGate user groups. See “Selecting Windows user groups (LDAP only)” on page 161.
   • Create security policies for FSSO-authenticated groups. See “Creating Fortinet Single Sign-On (FSSO) user groups” on page 162 and “Creating security policies” on page 162.
   • Optionally, specify a guest protection profile to allow guest access. See “Enabling guest access through FSSO security policies” on page 165.

Configuring LDAP server access

LDAP access is required if your network has a Novell eDirectory agent or a Collector agent using Windows Advanced AD access mode. If you are using FSSO Standard mode, go to “Specifying your Collector agents or Novell eDirectory agents” on page 160.

The LDAP configuration on the FortiGate unit not only provides access to the LDAP server, it sets up the retrieval of Windows AD user groups for you to select in FSSO. The LDAP Server configuration (in User > Remote > LDAP) includes a function to preview the LDAP server’s response to your distinguished name query. If you already know the appropriate Distinguished Name (DN) and User DN settings, you may be able to skip some of the following steps.

1 Go to User > Remote > LDAP and select Create New.
2 Select the Query distinguished name button to the right of the Distinguished Name field.
   A new window opens.
3 If more than one name is listed, you might need to explore each name following the steps below to determine which one is relevant to your needs.
4 Copy the name string to the Distinguished Name field and select OK.
   This closes the window and copies the name string to the Distinguished Name field of the LDAP Server configuration.
5 Set Bind Type to Regular.
6 In the User DN field, enter the administrative account name that you created for FSSO.
   For example, if the account is FSSO_Admin, enter “cn=FSSO_Admin,cn=users”.

7 Make sure that the User DN entry ends with a comma and append the string from the Distinguished Name field to the end of it.

Example: cn=FSSO_Admin,cn=users,dc=office,dc=example,dc=com

8 Enter the administrative account password in the Password field.

9 Select the Query distinguished name button again.

The LDAP Distinguished Name Query window opens:

**Figure 10: Authenticated DN query**

You can expand any of the DNs that contain entries. When you select an expandable DN, the Distinguished Name field is updated. Look for the DN that contains the users or groups whose logon you want to monitor.

10 Select the DN that you want to monitor and then select OK.

This closes the window and updates the Distinguished Name field of the LDAP Server configuration with the selected Domain Name Identifier (DNI).

11 Check the following fields and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the LDAP server.</td>
</tr>
<tr>
<td>Common Name Identifier</td>
<td>The default common name identifier is cn. This is correct for most LDAP servers. However some servers use other identifiers such as uid.</td>
</tr>
<tr>
<td>Secure Connection</td>
<td>Do not select. The Collector agent does not support secure connection.</td>
</tr>
</tbody>
</table>

**To configure LDAP for FSSO - CLI example**

```
config user ldap
edit "ADserver"
    set server "10.11.101.160"
    set cnid "cn"
    set dn "cn=users,dc=office,dc=example,dc=com"
```
Specifying your Collector agents or Novell eDirectory agents

You need to configure the FortiGate unit to access at least one Collector agent or Novell eDirectory agent. You can specify up to five servers on which you have installed a Collector or eDirectory agent. The FortiGate unit accesses these servers in the order that they appear in the list. If a server becomes unavailable, the next one in the list is tried.

To specify Collector agents - web-based manager

1. Go to User > FSSO > FSSO Agent and select Create New.
2. Enter a Name for the Windows AD server. This name appears in the list of Windows AD servers when you create user groups.
3. Enter the following information for each of up to five collector agents and select OK:

<table>
<thead>
<tr>
<th>FSSO Agent IP/Name</th>
<th>Enter the IP address or the name of the server where this agent is installed. Maximum name length is 63 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter the TCP port used for FSSO. You must enter the port number for the server. This must be the same as the FortiGate listening port specified in the Novell eDirectory or Collector agent configuration. TCP port 8000 is used by default. See “Configuring Collector agent settings” on page 146 or “User list from Windows AD is empty” on page 172.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the Collector agent or eDirectory agent. For the Collector agent, this is required only if you configured the agent to require authenticated access.</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>For Novell eDirectory, enable. For Windows AD, enable if the Collector agent is configured to use Advanced AD access mode. Select the LDAP server you configured previously. See “Configuring LDAP server access” on page 158.</td>
</tr>
</tbody>
</table>

To specify the FSSO Collector agent - CLI

```
config user fsso
edit WinGroups
set ldap-server ADserver
set password ENC
G7GQV7NEq1iCM9jKmVmJJPVvQ2+wtNEe9T0iYA5Sa+EqT2J8zh0rbkJFD
r0RmY3c4LaoXds0BczAldONmcGfthTxxwGsugzGpbJdC71spF1QYtj
set server 10.11.101.160
set port 8000
end
```
Selecting Windows user groups (LDAP only)

If the Collector agent uses Advanced AD access mode, the FortiGate unit obtains user group information using LDAP. You need to select the Windows user groups that you want to monitor. These user group names are then available to add to FSSO user groups.

To select Windows user groups - web-based manager

1. Go to User > FSSO > FSSO Agent.
   The list of FSSO agent servers is displayed.
2. Select the Edit Users/Groups icon.
   The FortiGate unit performs an LDAP query and displays the result.
3. Select the check boxes of the user groups that you want to monitor and then select OK.
   You can also use the Add User/Group icon to select a group by entering its distinguished name.

Viewing information imported from the Windows AD server

You can view the domain and group information that the FortiGate unit receives from the AD Server. Go to User > FSSO > FSSO Agent. The display differs for Standard and Advanced AD access mode.

| Create New | Add a new FSSO agent server. |
| Name       |                             |
| Server     | The name defined for the FSSO agent server. |
Creating Fortinet Single Sign-On (FSSO) user groups

You cannot use Windows or Novell groups directly in FortiGate security policies. You must create FortiGate user groups of the FSSO type and add Windows or Novell groups to them.

**To create a user group for FSSO authentication - web-based manager**

2. Select Create New.
   The New User Group dialog box opens.
3. In the Name box, enter a name for the group, FSSO_Internet_users for example.
4. In Type, select Fortinet Single Sign-On (FSSO).
5. From the Available Members list, select the required FSSO groups.
   Using the CTRL or SHIFT keys, you can select multiple groups.
6. Select the green right arrow button to move the selected groups to the Members list.
7. Select OK.

**To create the FSSO_Internet-users user group - CLI**

```
config user group
edit FSSO_Internet_users
   set group-type fsso-service
   set member
      CN=Engineering,cn=users,dc=office,dc=example,dc=com
      CN=Sales,cn=users,dc=office,dc=example,dc=com
end
```

Creating security policies

Policies that require FSSO authentication are very similar to other security policies. Using identity-based policies, you can configure access that depends on the FSSO user group. This allows each FSSO user group to have its own level of access to its own group of services.
In this situation, Example.com is a company that has its employees and authentication servers on an internal network. The FortiGate unit intercepts all traffic leaving the internal network and requires FSSO authentication to access network resources on the Internet. The following procedure configures the security policy for FSSO authentication. FSSO is installed and configured including the RADIUS server, FSSO Collector agent, and user groups on the FortiGate.

For the following procedure, the internal interface is `port1` and the external interface connected to the Internet is `port2`. There is an address group for the internal network called `company_network`. The FSSO user group is called `fsso_group`, and the FSSO RADIUS server is `fsso_rad_server`.

To configure an FSSO authentication security policy - web-based manager

1. Go to `Policy > Policy`.
2. Select `Create New`.
3. Enter the following information.
4. Select `Enable identity-based Policy`.
5. Select `Add` to add groups of users to this authentication policy.
6. Select the `fsso_group`, and the `FSSO_Guest_users` usergroups in the `Available User Groups` list and move them to the `Selected User Groups` list.
   - `FSSO_Guest_users` is a default user group enabled when FSSO is configured. It allows guest users on the network who do not have FSSO account to still authenticate and have access to network resources. See “Enabling guest access through FSSO security policies” on page 165.
7. Select HTTP, HTTPS, FTP, and Telnet for in the `Available Services` list, and move them to the `Selected Services` list.
8. Select always for the `Schedule`.
   - Logging FSSO logon events helps troubleshoot any FSSO related issues.
10. Select UTM, and enable default AntiVirus, IPS, Web Filter, an Email filter.
11. Select OK.
   - A new line of information will appear in the identity-based policy table. The table lists the ID, user group or groups, the service or services, schedule, UTM, and logging selected for the rule. Use this display to verify your information was entered correctly.
13. Optionally select `Customize Authentication messages` to change the default authentication messages to suit example.com’s company design and policies.
14. Select OK.
15 Ensure the FSSO authentication policy is at the top of the list so it will be attempted to be matched before any other policy.

To create a security policy for FSSO authentication - CLI

config firewall policy
dit 0
   set srcintf internal
   set dstintf wan1
   set srcaddr company_network
   set dstaddr all
   set action accept
   set identity-based enable
   set nat enable
   config identity-based-policy
dit 1
   set schedule any
   set groups company_network FSSO_guest_users
   set service HTTP HTTPS FTP TELNET
end
end

Here is an example of how this FSSO authentication policy is used. Example.com employee on the internal company network logs on to the internal network using their RADIUS username and password. When that user attempts to access the Internet, which requires FSSO authentication, the FortiGate authentication security policy intercepts the session, checks with the FSSO Collector agent to verify the user’s identity and credentials, and then if everything is verified the user is allowed access to the Internet.

Users belonging to multiple groups

Before FSSO 4.0 MR3, if a user belonged to multiple user groups, the first security policy to match any group that user belonged too was the only security policy applied. If that specific group did not have access to this protocol or resource where another group did, the user was still denied access. For example, test_user belongs to group1 and group2. There are two FSSO authentication policies — one matches group1 to authenticate FTP traffic and one matches group2 to authenticate email traffic. The group1 policy is at the top of the list of policies. If test_user wants to access an email server, the first policy encountered for a group test_user belongs to is the group1 policy which does not allow email access and test_user is denied access. This is despite the next policy allowing access to email. If the order was reversed in this case, the traffic would be matched and the user’s traffic would be allowed through the firewall. However if the policy order was reversed, FTP traffic would not be matched.

As of FSSO 4.0 MR3, if a user belongs to multiple groups multiple then attempts to match the group are attempted if applicable. Using the above example, when the attempt to match the group1 policy is made and fails, the next policy with a group that test_user is a member of is attempted. In this case, the next policy is matched and access is granted to the email server.

When configuring this example the only difference between the policies is the services that are listed and the FSSO user group name.

Authenticating through multiple groups allows administrators to assign groups for specific services, and users who are members of each group have access to those services. For example there could be an FTP group, an email group, and a Telnet group.
Resolve usernames Using FSSO Agent

When configuring a security policy, there is an option to enable the feature Resolve usernames Using FSSO Agent without configuring an identity-based policy.

If an FSSO server and user group are configured, but no identity-based policy is enabled then logon events do not generate a log entry — essentially the logon event goes unnoticed by the FortiGate unit.

If this option is enabled then when there is no identity-based policy configured, the logon event will still be logged on the traffic log along with the username. The username will be resolved from the FSSO information.

Enabling guest access through FSSO security policies

You can enable guest users to access FSSO security policies. Guests are users who are unknown to the Windows AD or Novell network and servers that do not logon to a Windows AD domain.

To enable guest access in your FSSO security policy, add an identity-based policy assigned to the built-in user group FSSO_Guest_Users. Specify the services, schedule and protection profile that apply to guest users — typically guests receive reduced access to a reduced set of services. See “Creating security policies” on page 162.

FortiOS FSSO log messages

There are two types of FortiOS log messages — firewall and event. FSSO related log messages are generated from authentication events. These include user logon and log off events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues. For more information on firewall logging, see “Enabling security logging” on page 102. For more information on logging, see the FortiOS Handbook Log and Reporting guide.

This section includes:
- Enabling authentication event logging
- Viewing FSSO log messages

Enabling authentication event logging

For the FortiGate unit to log events, that specific type of event must be enabled under logging.

When VDOMs are enabled certain options may not be available, such as CPU and memory usage events. You can enable event logs only when you are logged on to a VDOM; you cannot enable event logs globally.

To ensure you log all the events need, set the minimum log level to Notification or Information. Firewall logging requires Notification as a minimum. The closer to Debug level, the more information will be logged. While this extra information is useful, you must

To enable event logging

2. In the Event Log Settings section, select the check box beside Enable.
You must select the following events:

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System activity event</td>
<td>All system-related events, such as ping server failure and gateway status.</td>
</tr>
<tr>
<td>Admin event</td>
<td>All administration events, such as user logins, resets, and configuration updates.</td>
</tr>
<tr>
<td>Firewall authentication event</td>
<td>All firewall-related events, such as user authentication.</td>
</tr>
<tr>
<td>CPU &amp; memory usage (every 5 min)</td>
<td>Real-time CPU and memory events only, at 5-minute intervals.</td>
</tr>
</tbody>
</table>

Optionally you can enable any or all of the other logging event options.

Select Apply.

Select OK.

**Viewing FSSO log messages**

If you have configured logging to a FortiAnalyzer unit, FortiGate unit's local disk or system memory, you can view log messages from either the web-based manager or CLI. The following procedures explain how to view log messages from the Log Access menu in the web-based manager, and how to view log messages from within the CLI.

Figure 13 on page 167 shows the event log filtered for authentication log entries, and the display columns customized.

Table 8 on page 167 lists the log message IDs and descriptions for FSSO related log messages. Use this table to help identify FSSO log messages on the FortiGate unit. Note that for the log messages to be displayed, the Minimum Log Level must be set to the Severity or lower for the log entry to be logged.

When viewing log messages in the Raw format in Memory, the ten-digit log ID number is used; however, when viewing the same log messages, in Raw format, in Disk, the five-digit log ID number is used (except for traffic logs which have only one-digit log IDs). This five-digit log identification number is used because of log size reduction that occurred in FortiOS 4.0 MR1.

**To view log messages - web-based manager**

2. Select the log menu that you want to view log messages in.
   - For example, the attack log messages in Log&Report > Log & Archive Access > Traffic Log.
3. Within the page, use any one of the following to view each log message:
   - Download Raw Log – downloads the log file to your PC. Column Settings – customize what columns display on the page.
   - Filter Settings – filter the information within the page.
   - Detailed Information – display the log table on the right side of the page, at the bottom (default), or hide the log table.

   For more on viewing logs, see the FortiOS Handbook Log and Reporting guide.
4. To display current log messages on the page, select Refresh.
To view log messages - CLI

1. Enter the following to configure how the log messages will be displayed, as well as what log messages you want to display:
   - `execute log filter category <category_number>`
   - `execute log filter start-line <line_number>`
   - `execute log filter view-lines <lines_per_view>`

2. Enter the following to display the logs messages within the CLI:
   - `execute log display`

3. Log messages appear and stop when the maximum number of view-lines is reached.

Figure 13: Authentication log messages

Table 8: List of FSSO related log messages

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>43008</td>
<td>Notification</td>
<td>Authentication was successful</td>
</tr>
<tr>
<td>43009</td>
<td>Notification</td>
<td>Authentication session failed</td>
</tr>
<tr>
<td>43010</td>
<td>Warning</td>
<td>Authentication locked out</td>
</tr>
<tr>
<td>43011</td>
<td>Notification</td>
<td>Authentication timed out</td>
</tr>
<tr>
<td>43012</td>
<td>Notification</td>
<td>FSSO authentication was successful</td>
</tr>
<tr>
<td>43013</td>
<td>Notification</td>
<td>FSSO authentication failed</td>
</tr>
<tr>
<td>43014</td>
<td>Notification</td>
<td>FSSO user logged on</td>
</tr>
<tr>
<td>43015</td>
<td>Notification</td>
<td>FSSO user logged off</td>
</tr>
<tr>
<td>43016</td>
<td>Notification</td>
<td>NTLM authentication was successful</td>
</tr>
<tr>
<td>43017</td>
<td>Notification</td>
<td>NTLM authentication failed</td>
</tr>
</tbody>
</table>

For more information on logging, see the FortiOS Handbook Log and Reporting guide.

Testing FSSO

Once FSSO is configured, you can easily test to ensure your configuration is working as expected. For additional FSSO testing, see “Troubleshooting FSSO” on page 168.

1. Logon to one of the stations on the FSSO domain, and access an Internet resource.
2. Connect to the CLI of the FortiGate unit, and if possible log the output.
Enter the following command:
```
diagnose debug authd fsso list
```

Check the output. If FSSO is functioning properly you will see something similar to the following:
```
----FSSO logons----
IP: 192.168.1.230  User: ADMINISTRATOR  Groups: VLAD-AD/DOMAIN USERS
IP: 192.168.1.240  User: ADMINISTRATOR  Groups: VLAD-AD/DOMAIN USERS
Total number of users logged on: 2
----end of FSSO logons----
```

The exact information will vary based on your installation.

Check the FortiGate event log, for FSSO-auth action or other FSSO related events with FSSO information in the message field. For a list of FSSO log message IDs, see Table 8 on page 167.

To check server connectivity, run the following commands from the CLI:
```
FGT# diagnose debug enable
FGT# diagnose debug authd fsso server-status

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBS-2003</td>
<td>connected</td>
</tr>
</tbody>
</table>
```

Troubleshooting FSSO

When installing, configuring, and working with FSSO some problems are quite common. A selection of these problems follows including explanations and solutions.

Some common Windows AD problems include:
- General troubleshooting tips for FSSO
- User status “Not Verified” on the Collector agent
- After initial configuration, there is no connection to the Collector agent
- FortiGate performance is slow on a large network with many users
- Users from the Windows AD network are not able to access the network
- Users on a particular computer (IP address) can not access the network
- Guest users do not have access to network
- Can’t find the DCagent service
- User logon events not received by FSSO Collector agent
- User list from Windows AD is empty
- Mac OS X users can’t access external resources after waking from sleep mode

General troubleshooting tips for FSSO

The following tips are useful in many FSSO troubleshooting situations.
- To help locate the problem, configure a sniffer policy to capture FSSO logon messages along with other information.

If FSSO is in use the log messages captured by a sniffer policy will include a user name if the IP address in the log message corresponds to the IP address if a user who has been authenticated with FSSO.
• Ensure all firewalls are allowing the FSSO required ports through.

FSSO has a number of required ports that must be allowed through all firewalls or connections will fail. These include: ports 139, 389 (LDAP), 445, 636 (LDAP) 8000, and 8002.

• Ensure the Collector agent has at least 64kbps bandwidth to the FortiGate unit.

If not the Collector agent does not have this amount of bandwidth, information FSSO information may not reach the FortiGate unit resulting in outages. The best solution is to configure traffic shaping between the FortiGate unit and the Collector agent to ensure that minimum bandwidth is always available.

User status “Not Verified” on the Collector agent

When selecting “Show logon Users” in the Collector agent, some users may have their status set as “Not Verified”.

The Collector agent receives logon events for users from the DC agents, but Windows does not generate log out events. As such, the Collector agent needs to verify that the user is still logged on by checking the registry on that host.

If the Collector agent cannot connect to the host on ports 139 and 445 to perform this check, the host status is set to “Not Verified” and a log entry will be added to the Collector agent logs:

"01/01/2010 01:23:45 [ 1884] name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)"

Solution

There are a few things that can cause the Collector agent not to be able to connect to the user’s work station. Below is a list of the most common causes:

• Most commonly, a host firewall on the user’s workstation or a router on the network prevents remote access on ports 139 and/or 445. Try opening the ports on the host firewall.

• If the remote registry service is not running on the user’s workstation, the Collector agent will not be able to connect to the registry remotely. Make sure the remote registry service is running.

• This problem may also be caused by a known MS upgrade issue.

Using Regedit.exe, edit "\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers", set permissions for winreg and allow Local Service with R and W permissions.

After initial configuration, there is no connection to the Collector agent

The Collector Agent has been configured but now cannot be contacted. This may be a regular connectivity problem. The section Troubleshooting Connectivity in the FortiOS Handbook Troubleshooting guide will help locate and identify any network problems. Other solutions specific to FSSO are listed here.

Solution

If there are no network problems that can be identified, try the following solutions.

• The Windows AD network must be configured before configuring the FortiGate unit. This includes the domain controller agents, and Collector agents.

• Ensure the DC agents point to the correct collector agent port and IP address.
Ensure that TCP port 8000, and UDP port 8002 are not blocked.

FSSO is very dependent on DNS, ensure the forward DNS zone has no stale records and after adding it to the domain if the DNS entry is not in the zone add it.

An error in the DNI field on the FortiGate unit will prevent connections. Select the browse button next to the field to confirm it can connect correctly to the Windows AD server and return information. See

If the secure check box is selected, ensure that LDAP v3 is being used since earlier LDAP does not support secure TLS connections.

Ensure that the default LDAP ports are not being blocked on the network. These ports include port 389, and port 636. If you change the default ports, ensure both the FortiGate unit and the Windows AD server are using the same port numbers and that those ports are allowed through all firewalls on your network.

If you are using FSSO in polling mode, ensure that port 445 is not blocked by firewalls.

Collector Agent service freezing and shutting down

FSSO problem.

Solution

FortiGate performance is slow on a large network with many users

FSSO sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate units. Logon tracking is logged to memory, and may reduce performance in extreme situations.

To avoid this problem, you can configure the Collector agent to send logon information only for groups named in the FortiGate unit’s security policies. Also you can configure the Ignore User list on the FortiGate unit to avoid tracking unnecessary logons.

Also logging to memory can consume large amounts of FortiGate system memory. To lessen the memory used, change the logging from the default level of Information to a less frequent level such as Error or Warning. This results in less information being logged and frees system memory to improve overall FortiGate system performance. However, if you are trying to troubleshoot a problem one of the first things to do is to change the logging severity to Information or possibly even Debug to provide you with additional information while solving your problem.

Solution

Add users to the Ignore User list. This a best practice for admin accounts whose logon information will not be sent to the FortiGate unit. This is useful for automated accounts that may logon many times. Examples of accounts in this category include:

- IIS services
- AV
- other system accounts

For more information on configuring the Ignore users list, see “Configuring the Ignore User List” on page 150.
Users from the Windows AD network are not able to access the network

If nobody can access the network and your network has only one Collector agent, when it goes offline no users will have access. However if only some users can not access the network, it is likely that user group changes were made recently that are causing the problems.

Solutions

- If there is only one Collector agent, configure additional Collector agents in the domain to act as backups. They will provide the redundancy required if the original collector goes offline. Remember to add them to the FortiGate FSSO entry under User > FSSO > FSSO Agent on the web-based manager or config user fss in the CLI. If the server and port for the new agent are not in the list, it will not be contacted.
- Ensure the Collector agent has at least 64kbps bandwidth to the FortiGate unit. If not, information FSSO information may not reach the FortiGate unit resulting in outages. The best solution is to configure traffic shaping between the FortiGate unit and the Collector agent to ensure that minimum bandwidth is always available.
- If some users can not connect, verify their Windows AD records to find groups in common, and investigate the state of those groups focusing on any recent changes. It may be a group or permission change is the reason.
- There may be a a problem with the user list. See “User list from Windows AD is empty” on page 172.

Users on a particular computer (IP address) can not access the network

Windows AD Domain Controller agent gets the username and workstation where the logon attempt is coming from. If there are two computers with the same IP address and the same user trying to logon, it is possible for the authentication system to become confused and believe that the user on computer_1 is actually trying to access computer_2.

Windows AD does not track when a user logs out. It is possible that a user logs out on one computer, and immediate logs onto a second computer while the system still believes the user is logged on the original computer. While this is allowed, information that is intended for the session on one computer may mistakenly end up going to the other computer instead. The result would look similar to a hijacked session.

Solutions

- Ensure each computer has separate IP addresses.
- Encourage users to logout on one machine before logging onto another machine.
- If multiple users have the same username, change the usernames to be unique.
- Shorten timeout timer to flush inactive sessions after a shorter time.

Guest users do not have access to network

A group of guest users was created, but they don’t have access.

Solution

The group of the guest users was not included in a policy, so they do not fall under the guest account. To give them access, associate their group with a security policy.

Additionally, there is a default group called FSSO_Guest_Users. Ensure that group is part of an identity-based security policy to allow traffic.
Can’t find the DCagent service

The DCagent service can’t be found in the list of regular windows services. This is because it has no associated Windows service.

Instead DCagent is really `dcagent.dll` and is located in the `Windows\system32` folder. This DLL file is loaded when windows boots up and it intercepts all logon events processed by the domain controller to send these events to the Collector agent (CA).

Solution

To verify that the DCagent is installed properly

1. Check that DCagent.dll exists in `%windir%\system32` folder.
2. Check that the registry key exists:
   `\HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\dcagent`  
   If both exist, the DCagent is properly installed.

User logon events not received by FSSO Collector agent

When a a warning dialog is present on the screen on the Collector agent computer, the Collector agent will not receive any logon events. Once the dialog has been closed normal operation will resume.

If polling mode is enabled, it is possible the polling interval is too large. Use a shorter polling interval to ensure the collector agent is capturing all logon events.

If NetAPI polling mode is enabled, consider switching to Event log polling as it provides letter accuracy.

User list from Windows AD is empty

FSSO server is configured. I have received a list of windows AD groups. However, a user list is empty.

Solution

There could be 2 problems:

In most cases, the FortiGate receives login information, but can’t translate the Windows AD group into the protection profile. Make sure that all the required Windows AD groups are included in the FortiGate user groups and that all FortiGate user groups are included into the authentication security policy.

There may be a problem with AD FSSO service running on the Windows AD server.

To ensure the problem is on windows side

2. Enable firewall authentication event logging and debug level logging on the FortiGate.
3. Ask one or more users to log in into windows.
4. Check the FortiGate logs for the logon event from the Windows AD server.

If there is no new logon event entry in the logs, the problem is with Windows side. Use MS Windows AD documentation to troubleshoot the problem.
Mac OS X users can't access external resources after waking from sleep mode

When client computers running Mac OS X (10.6.X and higher) wake up from sleep mode, the user must authenticate again to be able to access external resources. If the user does not re-authenticate, the user will maintain access to internal web sites, but will be unable to access any external resources. This issue is caused by Mac OS X not providing sufficient information to the FSAE. This results in the FortiGate blocking access to the user because they cannot be authenticated.

Solution

The security settings on client computer(s) must be configured to require that a username and password be entered when exiting sleep mode or screen saver. With this feature enabled in Mac OS X, the FortiGate will receive the authentication information it requires to authenticate the user and allow them access.

Note that if the user reverts their settings to disable the password requirement, this will cause the issue to reappear.
Dynamic profiles and end points

This section explains how to set up the FortiOS dynamic profile and end point features to identify users and communication sessions. This section also describes configuring FortiOS Carrier HTTP header options, and end points.

This section describes:
- Overview
- Configuring dynamic profile
- Configuring dynamic profile-based security policies
- Configuring end points
- Timeout options
- Log settings
- Troubleshooting dynamic profiles

Overview

Network administrators can add customer identifying information and profile group names to their RADIUS server accounts. In response to a user connecting to the company network, if the RADIUS server successfully authenticates that user it sends a RADIUS Start record to FortiOS. In real time, FortiOS can extract identifying information and profile group names from these RADIUS Start records and match the identifying information with the customer communication session. FortiOS can then dynamically select and apply the profile group named in the RADIUS Start record to the communication session.

The application of parental-type controls to user sessions at a school is a useful example of the dynamic profile and multiple profile groups with different levels of access. Administrators can create profile groups that provide different levels of parental controls. Then these different levels of controls can be applied to communication sessions; the level of parental control depending on the profile group name added to the user account in the accounting system. This would allow teachers and student accounts to have different parental control settings. It would also allow teachers and students to logon to the school network from different locations, with different IP addresses, and still have the same restrictions for their level of account. It would also allow for difference between younger and older student controls, as appropriate.
Another example is on a mobile phone network with a mobile service provider. The mobile phone may access the network from many physical or network locations. With FortiOS Carrier dynamic profiles enabled on the provider network, that user will be identified as the same user and given the same privileges no matter where they logon. This makes it easier for mobile providers to track customers and provide extended services where warranted, or block access to some resources as may also be warranted. It also allows carriers to treat customers from other carriers who are using their network differently according to any agreements that might exist between carriers or even countries.

While FortiOS Carrier dynamic profiles and end points are very similar to those objects defined in FortiOS, in FortiOS Carrier there are some differences. These differences will be noted in the documentation. For definitions of carrier related terms, see the FortiOS Handbook Carier guide.

Figure 14: Information flow between customers, the accounting system, and FortiOS

When to use FSSO or dynamic profiles

FSSO and dynamic profiles have much in common. Both use RADIUS servers for authentication and accounting. Both are single sign on (SSO) solutions. For these and other reasons its valid to wonder why use one method over the other. There are three main points FSSO and dynamic profiles differ on.

When to use FFSO

1 *Your large network has a complex Windows AD authentication server already configured.* FSSO is designed to work with an established Windows AD or Novell eDirectory network. Its agent software installations sit on the various servers to help send the required information to the FortiGate unit for authentication. Dynamic profiles does not require this extra software to be installed, but its performance may suffer as a result on large networks.

2 You have multiple authentication groups that require different levels of access. FSSO can be configured to work with 512 groups or more (depending on your FortiGate model). Dynamic profiles allows one group per VDOM.
Dynamic profiles require no user or user group configuration. For Dynamic profile, configure the RADIUS server, and security policy. FSSO requires more configuration, but as a result allows more flexibility as well.

### End points

The term for customer identifying information is an **end point**. An end point can be any information the service provider uses to identify a customer and the device that the customer is using to connect to the network. For example, if the customer is using a mobile phone, the end point could be the phone's MSISDN number. The end point information must be included in the RADIUS Start record and must be available in the customer communication session (for example, in the HTTP header).

This is not the Endpoint Control feature referred to in other parts of FortiOS — that is a different feature for application control. End points in this chapter are used with the dynamic profile feature and RADIUS records to identify users.

In most cases, FortiOS Carrier can find the end point and IP address in customer communication sessions. An important exception is WAP traffic. Because WAP traffic may have the source IP address changed from the customer’s IP address to the IP address of the WAP server, extra configuration may be required to extract the end point and source IP address from WAP traffic. See FortiOS Handbook Carrier guide for information on configuring FortiOS Carrier for WAP traffic.

Without the end point, customers can only be identified by the IP address of the device that they are using. Because IP addresses may not be permanent or multiple users may be behind a NAT device and sharing a single IP address, the additional end point information is a more reliable and accurate way to identify individual customers. See “Configuring end points” on page 191.

### Dynamic profiles and security policies

For FortiOS to use the dynamic profile, you must add a security policy that includes the feature. Then all traffic that matches that profile will be authenticated by the configured RADIUS server.

Dynamic profile and identity-based policy are mutually exclusive options. When one is enabled, the other is hidden.

You can configure a maximum of one dynamic profile security policy per VDOM.

The general steps to configure a dynamic profile security policy are:

1. Create a new UTM profile group with a name that matches the dynamic profile group name that will be in the RADIUS attribute.
2. Create a new security policy and set the required fields (source, destination, schedule, service and action) as normal.
3. Enable **Dynamic Profile**, and select the dynamic profile from the list.
4. Enable **Dynamic Profile Users Only**.
5. Select other optional fields as required, and select OK when done.
Dynamic profile UTM profile groups

UTM profile groups allow you to create a group of UTM services and associate them together for a specific purpose. This group is then applied to one or more security policies. The benefit of this method is that you can have multiple configurations for AntiVirus, IPS, Application control and such, but only select the versions or services you require. To make changes in the future you change that IPS configuration for example and all UTM profile groups that use that IPS configuration will be updated as well.

When creating a dynamic profile UTM profile group, the group name must match the RADIUS server profile group name that was specified in the RADIUS server configuration. This group name is used to match traffic.

To create a dynamic profile UTM profile group - web-based manager

1. Go to UTM > Profile Group.
   - If this options is not visible, go to System > Admin > Settings and enable firewall related displays.
2. Select Create New.
3. Enter the Name. For example, my_dyn_prof_group. The name has to be the same as the dynamic profile group name used when configuring the RADIUS server for dynamic profiles. See “RADIUS server configuration for dynamic profiles” on page 183.
4. Select default for the various UTM services. All entries have at least a default entry, and may have additional entries if they have been configured. For additional UTM configuration details, see the FortiOS Handbook UTM guide.
5. Select the web and email protocols to apply dynamic profile to. This can include any or all of HTTP, HTTPS, FTP, IMAP, POP3, SMTP, IM, and NNTP. Best practices dictate that if you do not use some of these protocols, do not configure those ones. For all protocols selected, enable monitor to ensure statistics are collected for the Dashboard.
6. Select OK.

To create a dynamic profile UTM profile group - CLI

```
config firewall profile-group
  edit my_dyn_prof_group
    set av_profile default
    set profile_protocol_options default
    set webfilter-profile default
    set spamfilter-profile default
    set ips-sensor default
  next
end
```

Dynamic security policies

The following procedures use a dynamic profile group called my_dyn_prof_group to create a security policy to allow traffic between wan1 and internal for all traffic at any time of day. It allows a group of services called allowed_protocols that includes protocols for web traffic, email, and other useful business applications.
Even though you have configured a UTM profile with AV, webfilter, spam, and IPS you must also configure UTM in the security policy. The UTM profile is used to match the dynamic profile group name on the RADIUS server. Configuring UTM within the security policy ensures that level UTM will be applied to any users who fail the dynamic profile authentication check. Otherwise those users would be left without any UTM, which can leave a gap in your security depending how those users are handled.

When this policy has been created, place it at the top of the security policy list to ensure it will be matched first. Otherwise it is possible another policy will match the users but without Authentication resulting in an unsecure user gaining access. Ensure there are policies lower in the list to catch any traffic that needs access through the FortiGate unit without requiring Authentication, as well as the final implicit deny policy at the bottom. You may have to enable Display Implicit security Policies under System > Admin > Settings to see it.

**To create a dynamic profile security policy - web-based manager**

1. Go to Policy.
2. Select Create New.
3. Enter the following information.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>wan1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>internal</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

4. Select Enable Dynamic Profile.
5. Select my_dyn_prof_group for Profile.
   This is the UTM profile group created earlier.
7. Add the comment “Dynamic Profile policy” to help identify this security policy in a list of policies.
8. Select OK.

**To create a dynamic profile security policy - CLI**

```bash
config firewall policy
edit 0
   set srcintf wan1
   set srcaddr any
   set dstintf internal
   set dstaddr any
   set action accept
   set dynamic-profile enable
   set dynamic-profile-access http imap pop3 smtp
   set dynamic-profile-group my_dyn_prof_group
   set utm-status enable
   set av-profile default
   set webfilter-profile default
   set spamfilter-profile default
```

FortiOS™ Handbook v3: User Authentication
01-433-122870-20111216
http://docs.fortinet.com/
set ips-sensor default
set profile-protocol-options default
set comments "Dynamic Profile policy"
next
end

Accounting system RADIUS configuration

You can configure FortiOS dynamic profiles to work with most RADIUS-based accounting systems. In most cases, you only need to do the following to your RADIUS accounting system before you can use dynamic profiles.

- Add a profile group name field to customer accounts on the RADIUS server so that the name is added to the RADIUS Start record sent by the accounting system to the FortiOS unit. Profile group names do not need to be added for all users, only to the accounts of customers who will use the dynamic profile feature on the FortiOS unit. If a profile group is not found in a RADIUS Start record regular RADIUS authentication will be used instead of dynamic profile if the user is configured for that type of authentication. See “RADIUS authentication with a FortiGate unit” on page 52.

- Configure your accounting system to send RADIUS Start records to the FortiOS unit. You can send the RADIUS Start records to any FortiOS network interface. If your FortiOS unit is operating with virtual domains (VDOMs) enabled, the RADIUS Start records must be sent to a network interface in the management VDOM.

User context list

FortiOS maintains a dynamic user context list—a list of current end points, IP addresses, and the profile group name received in RADIUS Start records. FortiOS uses timeouts to make sure that the list contains only current information, removing entries that are no longer needed (see “Timeout options” on page 199).

FortiOS can also remove entries from the user context list if the accounting system sends a RADIUS Stop record when a customer finishes a communication session. When FortiOS receives a RADIUS Stop record, the end point in the record is removed from the user context list. The RADIUS Stop records are optional, but they make sure FortiOS maintains an accurate user context list.

Figure 15: FortiOS dynamic profile information flow

You can use the IP Filter list to block access through FortiOS for end points. To use this feature, add end points to the list and select block traffic. FortiOS uses the user context list to look up an end point in the IP filter list to find the find source IP address that the end point is using. Then at the IP level, FortiOS blocks all sessions from the source IP address. guide
Accepting sessions only from dynamic profile users

Extracting an end point from the content of a communication session creates extra processing overhead for the FortiOS unit. This extra overhead is acceptable for communication sessions where you want to apply dynamic profiles because of the ability to examine the content of the communication session.

However, communication sessions that do not have an end point in the user context list also create the same extra processing overhead only to be dropped when no match is found. In some cases you can reduce the amount of processing overhead by adding specific source and destination addresses to a dynamic profile security policy so that the policy matches fewer sessions. However, this may or may not work depending on factors such as your network design and security policy.

A better solution is to select Dynamic Profile Users Only in the security policy. If this option is selected, the dynamic profile policy only accepts sessions with source addresses that are in the user context list. Sessions with source addresses that are not in the user context list do not match the policy. For sessions that don’t match the policy, the FortiOS unit continues searching down the policy list for a match.

You can add policies below the dynamic profile policy to apply various FortiOS features to non-dynamic profile sessions. For example:
• To block all non-dynamic profile sessions, make the next policy in the list a deny policy that matches all traffic. You could select Log Violation Traffic in this policy to log all non-dynamic profile sessions.

• To use traffic shaping to reduce the bandwidth available for non-dynamic profile sessions, apply a restrictive traffic shaper to the policy below the dynamic profile policy.

**Dynamic Profile Users Only option**

The *Dynamic Profile Users Only* option also allows you to differentiate between dynamic profile and regular sessions without including a profile group in the dynamic profile policy. You can use this property to apply a profile group only to non-dynamic profile traffic by adding a profile group to the next policy in the list. All dynamic profile sessions would use the dynamic profile policy and all non-dynamic profile sessions would use the next policy.

One example use of this configuration would be if you can assume that your dynamic profile users are not a security risk and you want to give them the benefit of enhanced performance of firewall sessions that do not apply a profile group.

> *With Dynamic Profile User Only selected, the FortiOS unit does not wait for the User Context Creation Timeout to see if a matching entry is added to the user context list. If there is a delay in receiving the RADIUS record and adding entries to the user context list, it is possible that sessions may not be matched with the dynamic profile security policy when as expected. If users experience this problem you may need to improve the performance of your RADIUS server, network, or FortiOS Carrier unit. For more information about the User Context Creation Timeout, see “Timeout options” on page 199.*

**Configuring dynamic profile**

For dynamic profile to work, your RADIUS accounting system needs to send all the user information to the FortiOS unit which will then match the user session to a dynamic profile security policy. The users do not need to be configured on the FortiOS unit as they are being authenticated by the RADIUS server. Once the RADIUS server authenticates the user, its just a matter of the security policy allowing the type of traffic in the session—just like an identity-based security policy after the user has authenticated.

You can configure one dynamic profile RADIUS server and one dynamic profile security policy per VDOM on your FortiOS unit. If you provide services to multiple networks by using VDOMs, this allows you to provide each network with their own dynamic profile configuration. Alternately you can configure a separate profile group in each VDOM’s RADIUS server configuration to provide different levels of service to different user groups.

To enable dynamic profiles, the following configuration is required:

• ensure dynamic profile is visible in web-based manager

• configure the single RADIUS server for dynamic profiles under *User > Remote > RADIUS*

• optionally configure UTM Profile Group

• configure dynamic profile security policy

This section includes:

• Make dynamic profiles visible

• RADIUS server configuration for dynamic profiles
Make dynamic profiles visible

Dynamic profiles are not required by everyone, and the extra information displayed in the web-based manager may be confusing. For this reason, dynamic profiles can optionally be hidden.

If you want to configure dynamic profiles, you must first ensure dynamic profiles are not hidden in FortiOS.

To make dynamic profiles visible - web-based manager
1. Go to System > Admin > Settings.
2. Enable Dynamic Profile Support on GUI.
3. Select Apply.

To make dynamic profiles visible in GUI - CLI

```
cfg-global
  cfg-system-global
    set gui-dynamic-profile-display enable
end
```

RADIUS server configuration for dynamic profiles

A RADIUS server must be configured on FortiOS for dynamic profile to work. If it is not, then the FortiOS unit does not listen for the RADIUS start record it needs for notification that the user was authenticated.

Restrictions and requirements

There are no restrictions on which brand of RADIUS servers can be used with FortiOS. The only requirements are that your RADIUS server supports the configuration FortiOS requires. Read this configuration section to ensure your RADIUS server can be properly configured using the documentation for your RADIUS server. This documentation does not explain how to configure your RADIUS server.

Only one RADIUS server can be configured for dynamic profiles per VDOM. Once one server is configured, the option to create more in the web-based manager is grayed-out and in the CLI attempting to enable the feature returns an error.

Profile group name

The profile group name is a means to identify which users on the RADIUS server are valid for the FortiOS unit and which are not. For example some users may have internal only access or be for automated processes that are internal network only. These users do not need to access resources outside their subnet, and will not use the FortiOS unit firewall. Using this method, FortiOS enforces Role Based Access Control (RBAC).

Also the profile group name allows multiple FortiOS units to share the Same RADIUS server by assigning each FortiOS unit a different group name and possibly even use a different RADIUS attribute as well. This can be useful if you only have one RADIUS server on your networks but have multiple FortiOS units protecting different network segments—for security reasons different users may have different levels of access to different parts of the network.
This example uses a RADIUS server called myRADIUS.example.com. This server uses “Login-IP Host” for both endpoint attribute and endpoint blocking. It uses “Vendor-Specific” for profile along with a value of “forti_dyn_prof”. This means when dynamic profile is trying to match the profile group, the group name it is looking to match will be in the Vendor-Specific RADIUS attribute and the value will be forti_dyn_prof. You may use different attributes for your configuration as is required.

The RADIUS server configuration will use the default settings where possible. This procedure assumes there is no existing dynamic profile server already configured.

**To configure a dynamic profile RADIUS server - web-based manager**

1. Go to User > Remote > Radius.
2. Select Create New.
3. For Name, enter myRADIUS.example.com. This is the name of the RADIUS server on the network.
4. For Type, select Dynamic Start. This enables dynamic profiles.
5. Enter the following information, and select OK:
### Dynamic profiles and end points

#### Configuring dynamic profile

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint Attribute</strong></td>
<td>Select the RADIUS attribute “Login-IP Host” from drop-down list. This attribute will be used to uniquely identify the user and enable extraction of endpoint information. Some RADIUS attributes are only for use with FortiOS Carrier and carrier networks. These attributes relate to mobile devices such as *-Station-Id.</td>
</tr>
<tr>
<td><strong>Profile Attribute</strong></td>
<td>Select the RADIUS attribute “Vendor-Specific” from drop-down list. This attribute will be used to uniquely identify the user and enable extraction of security profile information. RBAC is enabled with Vendor-Specific attributes. See “Role Based Access Control” on page 54. Some RADIUS attributes are only for use with FortiOS Carrier and carrier networks. These attributes relate to mobile devices such as *-Station-Id.</td>
</tr>
<tr>
<td><strong>Endpoint Blocking Attribute</strong></td>
<td>Select the RADIUS attribute “Login-IP Host” from drop-down list. This attribute will be used to uniquely identify the user and enable extraction of endpoint blocking information. Some RADIUS attributes are only for use with FortiOS Carrier and carrier networks. These attributes relate to mobile devices such as *-Station-Id.</td>
</tr>
<tr>
<td><strong>Send RADIUS Response</strong></td>
<td>Select this option. FortiOS will send RADIUS responses after receiving RADIUS Start and Stop records. This setting may be required by your accounting system.</td>
</tr>
<tr>
<td><strong>Validate RADIUS Secret</strong></td>
<td>Select to use RADIUS shared secret for responses and validating requests for dynamic profile.</td>
</tr>
<tr>
<td><strong>Flush IP sessions on STOP</strong></td>
<td>Select to terminate all firewall TCP and UDP sessions associated with an IP after receiving a RADIUS STOP message for a dynamic profile. If left open it can result in unwanted traffic from an earlier user being assigned to a new user if the same IP address was assigned.</td>
</tr>
<tr>
<td><strong>Profile Key</strong></td>
<td>For this example, enter “forti_dyn_prof”, short for (fortios dynamic profile). Contains the profile group name to be matched in Profile Attribute. This is the profile group from the RADIUS server that the user belongs to. The profile group is how RADIUS users can be divided into different groups and access levels.</td>
</tr>
<tr>
<td><strong>Log All Events</strong></td>
<td>Select to log all possible dynamic profile related events. To select individual events, go to the CLI command <code>dp-log-dyn_flags</code> and select individual events to log. See “Advanced dynamic profile RADIUS server configuration - CLI” on page 186.</td>
</tr>
</tbody>
</table>

💡 Dynamic profiles always use the RADIUS `framed-ip-addr` field to get the IP address associated with the end point.
Advanced dynamic profile RADIUS server configuration - CLI

In the CLI, the following keywords are specific to configuring a RADIUS server for dynamic profile. The CLI keywords provide more in-depth options than found in the web-based manager. In the following example the RADIUS server uses secret123 for the server secret, and the server is located at the IP address of 10.21.101.10.

The dynamic profile RADIUS server keywords are found under config user radius.

To repeat the example above:

```
config vdom
edit root
config user radius
edit myRADIUS.example.com
   set dynamic_profile enable
   set auth-type auto
   set server myRADIUS.example.com
   set secret secret123
   set source-ip 10.21.101.10
   set use-management-vdom enable
   set dp-context-timeout 7200
   set dp-log-dyn-flags accounting-event accounting-stop-missed
      context-missing endpoint-block profile-missing protocol-error radiusd-other
   set dp-profile-attribute Vendor-Specific
   set dp-profile-attribute-key “forti_dyn_prof”
   set dp-radius-response enable
   next
end
```

nas-ip defines the station ID, commonly used with FortiOS Carrier, and is not used in this example.

use-management-vdom ensures that all requests are sent over the management VDOM instead of the current VDOM. When multiple VDOMs are enabled, the management VDOM always has access to servers such as FortiGuard which may help ensure connections to RADIUS servers as well. If each VDOM sends its own requests, changes to that VDOM may unknowingly cause problems with the sending of RADIUS requests.

dp-context-timeout defines how long before the user context is cleared from the table. The default is eight hours (28 800 seconds) which is generally OK. However, in this example we are using two hours (7 200 seconds). This is more secure, but may require clients to reconnect if they maintain an open connection for periods longer than two hours.

dp-log-dyn-flags allows you to set which dynamic profile related events you want to log. In the example, all flags were selected. This customizing allows you to ensure all the necessary information is logged while also allowing you to remove any unused events from the log to save space and time. Available log events include accounting-event, accounting-stop-missed, context-missing, endpoint-block, none, profile-missing, protocol-error, and radiusd-other. See “Log settings” on page 200.

dp-profile-attribute and dp-profile-attribute-key work together. Essentially the first field tells FortiOS which RADIUS attribute will contain the name of the profile group (such as Fortinet-Group-Name in the Vendor Specific Attribute), and the second field has the group name, or profile group name, to look for.
It is likely that different users will have different strings in the selected RADIUS attribute, but FortiOS is only concerned with the one string that identifies its users. This is the same name as the UTM profile that is applied to the dynamic profile in the security policy. Role based access control is accomplished this way. See “Dynamic profiles and security policies” on page 177.

dp-radius-response tells FortiOS to send a response when the system receives a RADIUS start message. Some RADIUS servers require this to be enabled. It allows the RADIUS server to ensure the Start Record was received, which will prevent retries and such which will in turn improve system performance overall.

For additional dynamic profile configuration, see the FortiOS CLI reference.

**Carrier endpoints**

When you are configuring the dynamic profile RADIUS server in the CLI, you have the option of configuring carrier endpoints as well. If you set endpoint-translation enable, this enables the endpoint series of CLI commands. See “Configuring end points” on page 191.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic_profile</td>
<td>Enable dynamic profile feature. Default is disable. Note that identity-based policy and dynamic profile are mutual exclusive — when one is enabled, the other is hidden. When disabled, all related keywords (dp-*) are hidden.</td>
</tr>
<tr>
<td>dp-carrier-endpoint-attribute</td>
<td>Enter the RADIUS Attribute used to hold End Point name. By default this value is Calling-Station-Id.</td>
</tr>
<tr>
<td>dp-carrier-endpoint-block-attribute</td>
<td>Select “Login-IP Host”. This is the RADIUS Attribute used to hold the endpoint to block. The list of available attributes to use is extensive. By default this value is Calling-Station-Id. Some RADIUS attributes are only for use with FortiOS Carrier and carrier networks. These attributes relate to mobile devices such as *-Station-Id.</td>
</tr>
<tr>
<td>dp-context-timeout</td>
<td>Timeout value in seconds for user context table entries (0 = infinite). Default is 28 800 seconds. See “Timeout options” on page 199.</td>
</tr>
<tr>
<td>dp-flush-ip-session</td>
<td>Enable to flush user IP asessions on RADIUS accounting stop. By default this is set to disabled.</td>
</tr>
<tr>
<td>dp-hold-time</td>
<td>Enter the time in seconds to hold in proxy connection state to receive RADIUS START. Default time is 5 seconds.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dp-log-dyn_flags</td>
<td>Select one or more dynamic profile events to log. Events available include:</td>
</tr>
<tr>
<td></td>
<td>- accounting-event</td>
</tr>
<tr>
<td></td>
<td>- accounting-stop-missed</td>
</tr>
<tr>
<td></td>
<td>- context-missing</td>
</tr>
<tr>
<td></td>
<td>- endpoint-block</td>
</tr>
<tr>
<td></td>
<td>- none</td>
</tr>
<tr>
<td></td>
<td>- profile-missing</td>
</tr>
<tr>
<td></td>
<td>- protocol-error</td>
</tr>
<tr>
<td></td>
<td>- radiusd-other</td>
</tr>
<tr>
<td></td>
<td>By default, all event types are enabled except none.</td>
</tr>
<tr>
<td>dp-log-period</td>
<td>Enter the minimum time period in seconds to use for event logs. Default is 0.</td>
</tr>
<tr>
<td>dp-mem-percent</td>
<td>Enter the maximum percentage of system memory to use for context tables. The default for this is set to 4%.</td>
</tr>
<tr>
<td>dp-profile-attribute</td>
<td>Select “Vendor-Specific”. This is the RADIUS Attribute used to hold the security profile group name. By default this is set to Class.</td>
</tr>
<tr>
<td></td>
<td>To extract a profile group name from the RADIUS Start record, set this field to the name of the RADIUS attribute that contains the profile group name.</td>
</tr>
<tr>
<td></td>
<td>Some RADIUS attributes are only for use with FortiOS Carrier and carrier networks. These attributes relate to mobile devices such as *-Station-Id.</td>
</tr>
<tr>
<td>dp-profile-attribute-key</td>
<td>Enter a string in this field if the Profile Attribute always contains the same text string directly before the profile group name. For example, if the Profile Attribute always includes the string profile_name= before the profile group name (for example, profile_name=&lt;profile_name_str&gt;), set the Profile Key to profile_name. FortiOS uses the string in the Profile Key to extract the profile name from the complete Profile Attribute string.</td>
</tr>
<tr>
<td>dp-radius-response</td>
<td>Enable to send RADIUS response packets. By default this is set to disable.</td>
</tr>
<tr>
<td>dp-radius-server-port</td>
<td>If required, change the UDP port number used by the RADIUS accounting server for sending RADIUS records. The default is 1813. FortiOS Carrier listens for RADIUS Start and Stop records on this port.</td>
</tr>
</tbody>
</table>
Configuring dynamic profile-based security policies

Only one security policy can be configured for dynamic profile in a VDOM. Also only one RADIUS server and one dynamic profile group can be configured per VDOM. When one dynamic profile security policy has been configured, the option is not visible when creating other policies. After deleting the dynamic profile security policy, the option is again visible when configuring other security policies.

By enabling the *Dynamic Profile Users Only* option, other non-dynamic profile users will not match this policy. This can be useful if you want to enforce all users to be part of the dynamic profile group—in which case you have a deny all profile after this one.

If you want to allow all users access to the resources this security policy allows, do not enable the *Dynamic Profile Users Only* option.

**To create dynamic profile-based security policies - web-based manager**

1. Go to *Policy > Policy*.
2. Select *Create New*.
3. Enter the Source, Destination, Schedule, Service and Action information as you would for any security policy.
4. Select *Enable Dynamic Profile*.
   
   If this option does not appear, another security policy has dynamic profile enabled already.
5. Select *Profile Group*, and choose a configured group from the list.
   
   The dynamic profile Profile Group uses the UTM Profile Group list, located under *UTM > Profile Group > Profile Group*.
6. Optionally select *Dynamic Profile Users Only*. See “Accepting sessions only from dynamic profile users” on page 181 and “Dynamic Profile Users Only option” on page 182.
7. Select UTM, Traffic Shaping, Endpoint Security, and other settings as you would for any other security policy.
8. Select OK.

If the RADIUS server and users have been configured, you can now start authenticating users with dynamic profile.

<table>
<thead>
<tr>
<th>dp-secret</th>
<th>Enter the RADIUS shared secret for responses and validating requests for dynamic profile by the RADIUS accounting server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dp-validate-request-secret</td>
<td>Enable to validate RADIUS request shared secret. Select if you want FortiOS Carrier to verify that the RADIUS secret matches the RADIUS secret in the RADIUS Start or End record. You can use the RADIUS secret to verify that the RADIUS record is valid.</td>
</tr>
</tbody>
</table>

In FortiOS Carrier, while creating or editing the identity based policy the service list includes MMS as an option.
Configuration concepts

Between identity-based policies, dynamic profiles, and traffic shaping there are many possible ways to configure your security policies to work with dynamic profiles. A few common ideas are presented here.

While many security options such as AV, webfiltering, and endpoint control are not mentioned here they are perfectly valid for use with dynamic profile security policies and are critical to maintaining network security.

These concepts include:

- Only allow dynamic profile users
- Only allow dynamic profile users, but traffic shape protocols
- Allow multiple dynamic profile groups
- Promote dynamic profile users
- Schedule-based policies

Only allow dynamic profile users

In this security policy configuration, there are only two policies needed. The first one will allow all dynamic profile authenticated users, and the second will deny everyone else.

This can be a problem for guest users visiting the office. It may also prove to be too restrictive in other ways as well.

Only allow dynamic profile users, but traffic shape protocols

This configuration is the same as the last one with one change. Different protocols (HTTPS, HTTP, telnet, ftp, etc.) will have different bandwidths allotted to each of them, and each will need its own security policy and traffic shaper to implement this. Each policy will be an IBP allow policy.

This is useful to ensure that important protocols or applications have the needed bandwidth to function properly. An example is VoIP applications that require a minimum level of bandwidth to guarantee a level of service.

Allow multiple dynamic profile groups

This configuration is the same as the last one, but uses multiple VDOMs to allow one profile group per VDOM. This configuration can be useful if you provide services to multiple networks with multiple VDOMs, or if you have one network with multiple levels of user access and want to differentiate between different dynamic profile users.

Promote dynamic profile users

It is possible that non-dynamic profile users are allowed on your network, but they will not have the same amount of resources available to them. This configuration is the same as the last one, but for the traffic shaping protocols there is no identity-based policy involved.

It is possible to have the users still authenticate if you want, by using IBPs and certificates. This would maintain a higher level of security on your network by requiring all users to authenticate in some form or another.
Schedule-based policies

Up to now, no mention has been made of scheduling. It is possible to have a policy only active at certain times of the day, or certain days of the week. This would allow a school to configure “during class” and “after school” schedules that may vary. Or at a company, different policies might be used over the lunch hour, for example relaxing company Internet browsing policies.

Schedules can be used by any security policy, but remember when that policy is offline you likely want a different policy in place allowing some traffic through. If you deny all traffic at times, you may run into problems with blocking even administrator access and be forced to use the console interface to access the FortiOS unit.

Configuring end points

An end point contains enough information about a user to be unique. This includes the IP address, profile, and group the user belongs to at a minimum. The end point information must be included in the RADIUS Start record and must be available in the customer communication session (for example, in the HTTP header).

Note that while the feature name is carrier end point, the feature is common to both FortiOS and FortiOS Carrier except where noted in the text.

This section includes:

- Configuring end points - CLI
- Controlling MMS service access based on a user’s end point - FortiCarrier Only
- Blocking access to the network based on end points - FortiOS Carrier only
- Extracting carrier end points for notifications - FortiOS Carrier only

Configuring end points - CLI

Dynamic profile end points are configured per RADIUS user that will be authentication using the dynamic profile. End points are only configurable in the CLI.

The following CLI keywords are specific to configuring end points. The end point keywords are found under `config user radius, when` set dynamic-profile is enabled.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpoint-translation</td>
<td>Enable/disable endpoint-translation configure. Default is disabled. When disabled, all carrier endpoint translation related keywords (ep-*) are hidden. The example dynamic profile in Figure expects the end point to be in the Calling-Station-ID attribute. For details about RADIUS attributes see RFC 2138 and RFC 2866.</td>
</tr>
<tr>
<td>ep-carrier-endpoint-convert-hex</td>
<td>Enable to enable converting end point to and from HEX string.</td>
</tr>
<tr>
<td>ep-carrier-endpoint-header</td>
<td>Enable to allow custom information to be added to HTTP headers. This option is commonly used on carrier networks. Default is x-up-calling-line-id.</td>
</tr>
</tbody>
</table>
You can control access to MMS services for users according to their end point by configuring end point filtering (also called end point blocking). End point filtering can filter MM1, MM3, MM4, and MM7 messages according to the end points in the From or To addresses of the messages. For a definition of end points, see “End points” on page 177.

You configure end point filtering by creating an end point filter list containing end point patterns. A end point pattern can match one end point or can use wildcards or regular expressions to match multiple end points.

For each pattern, you select the action that FortiOS Carrier takes on a message when the pattern matches a end point in the message. Actions include blocking the message, exempting the message from mass MMS scanning and exempting the message from all scanning. You can also intercept the message and archive the message to a FortiAnalyzer unit.

To apply an end point filter list, you need to add the list to the MMS Scanning > Carrier End Point Block section of an MMS protection profile.

### Configuring end point filtering - FortiOS Carrier only

**To apply end point filtering - web-based manager**

1. Go to UTM > Carrier > Carrier End point Filter Lists.
2. Add or edit an end point filter list.
3. Add or edit end point patterns in the list. See “Configuring end point filter lists” on page 193.
4. Go to UTM > Carrier > MMS Profile and add or edit an MMS protection profile.
5. Expand MMS Scanning and select Carrier End Point Block.
6. Select the MMS protocols to apply the end point filter list to—one or more of MM1, MM3, MM4 and MM7.
7. Select the end point filter list to apply.
8. Add the MMS protection profile to a protection profile.

| ep-carrier-endpoint-header-suppress | Select Enable to prevent use of HTTP headers |
| ep-carrier-endpoint-prefix | Enable to prefix end point values with additional information |
| ep-ip-header-suppress | Enable/disable HTTP header suppression. |
| ep-missing-header-fallback | Specify either the policy-profile or the session-ip address to act as a backup when the extracted header is not present. Default is policy-profile. |
| ep-profile-query-type | Specify the type of dynamic profile query as one of extract-carrier-endpoint, extract-ip, session-ip. Use the IP address when the full carrier endpoint information is not available. The default is session-ip. |
9. Add the protection profile to the dynamic profile security policy that accepts the MMS messages that you want to filter.

**Configuring end point filter lists**

To configure an end point filter list - web-based manager

1. Go to UTM > Carrier > Carrier End Point Filter Lists.
2. Select Create New.
3. Enter the following information and select OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the end point filter list. You select this name in an MMS protection profile.</td>
</tr>
<tr>
<td>Comments</td>
<td>Optional description of the end point filter list.</td>
</tr>
<tr>
<td>Check/Uncheck All</td>
<td>Select the check box to enable all end point patterns in the MMS filter list. Clear the check box to disable all entries on the MMS filter list. You can also select or clear individual check boxes to enable or disable individual end point patterns.</td>
</tr>
<tr>
<td>Pattern</td>
<td>The pattern that FortiOS Carrier uses to match with end points. The pattern can be a single end point or consist of wildcards or Perl regular expressions that will match more than one end point. See “Regular expression vs. wildcard match pattern” on page 194.</td>
</tr>
</tbody>
</table>
| Action | Select the action taken by FortiOS Carrier for messages from a carrier end point that matches the end point pattern:  
  * None - No action is taken.  
  * Block - MMS messages from the end point are not delivered and FortiOS Carrier records a log message.  
  * Exempt from mass MMS - MMS messages from the end point are delivered and are exempt from mass MMS filtering. Mass MMS filtering is configured in MMS protection profiles and is also called MMS Bulk Email Filtering and includes MMS message flood protection and MMS duplicate message detection.  
  * Exempt from all scanning - MMS messages from the end point are delivered and are exempt from all MMS protection profile scanning. MMS messages are not subject to protection profile filtering, just MMS protection profile filtering. |
| Content Archive | MMS messages from the end point are delivered, the message content is DLP archived according to MMS DLP archive settings. Content archiving is also called DLP archiving. |
| Intercept | MMS messages from the end point are delivered. Based on the quarantine configuration, attached files may be removed and quarantined. |
Regular expression vs. wildcard match pattern

A wildcard character is a special character that represents one or more other characters. The most commonly used wildcard characters are the asterisk (*), which typically represents zero or more characters in a string of characters, and the question mark (?), which typically represents any one character.

In Perl regular expressions, the ‘.’ character refers to any single character. It is similar to the ‘?’ character in wildcard match pattern. As a result:

- fortinet.com not only matches fortinet.com but also fortinetacom, fortinetbcom, fortinetccom, and so on.

To match a special character such as ‘.’ and ‘*’ use the escape character ‘\’. For example:

- To match fortinet.com, the regular expression will be: fortinet\.com

In Perl regular expressions, ‘*’ means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- forti*.com matches fortiiiii.com but does not match fortinet.com

To match any character 0 or more times, use ‘.*’ where ‘.’ means any character and the ‘*’ means 0 or more times. For example, the wildcard match pattern forti*.com will therefore be fort.\.com.

Blocking access to the network based on end points - FortiOS Carrier only

You can use end point IP filtering to block traffic from source IP addresses associated with end points. You can also configure FortiOS Carrier to record log messages whenever end point IP filtering blocks traffic. End point IP filtering blocks traffic at the IP level, before the traffic is accepted by a security policy.

To configure end point IP filtering, go to UTM > Carrier > IP Filter and add end points to the IP filter list. For each end point you can enable or disable both blocking traffic and logging blocked traffic.

You cannot add end point patterns to the end point IP filter list. You must enter complete and specific end points that are valid for your network.

The only action available is block. You cannot use end point IP filtering to exempt end points from IP filtering or to content archive or quarantine communication sessions.
FortiOS Carrier looks in the current user context list for the end points in the IP filter list and extracts the source IP addresses for these end points. Then any communication session with a source IP address that matches one of these IP addresses is blocked at the IP level, before the communication session is accepted by a security policy.

FortiOS Carrier dynamically updates the list of IP addresses to block as the user context list changes. Only these updated IP addresses are blocked by end point IP filtering.

**Carrier Endpoint Filter Lists**

A carrier end point filter list contains carrier end point patterns. A pattern can match one carrier end point or can use wildcards or regular expressions to match multiple carrier end points. For each pattern, you select the action that the unit takes on a message when the pattern matches a carrier end point in the message. Actions include blocking the message, exempting the message from MMS scanning, and exempting the message from all scanning. You can also configure the pattern to intercept the message and content archive the message to a FortiAnalyzer unit.

**Viewing and defining an end point IP filter list**

To view the end point IP filter list, go to *UTM > Carrier > IP Filter*.

You define a end point IP filter list by adding IP addresses to it. From this list, you can select *Create New* to add a new IP address or select the *Edit* icon beside an entry that you want to change.

There is only one IP filter list, and each entry can be blocked or allowed. The single list prevents configuration issues by applying all IP filters to all MMS protection profiles that use IP filtering.

Once the IP filters are configured, it is applied to all Carrier Endpoints as their traffic hits the security policies.

<table>
<thead>
<tr>
<th><strong>Carrier end point IP filter list</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create New</strong></td>
</tr>
</tbody>
</table>
| **Edit** | Edit the IP filter list entry. You can change the end point, enable or disable blocking, and enable or disable logging blocked traffic.  
If multiple entries are selected, Edit is not available. |
| **Delete** | Delete one or more selected end points from the list. |
| **Enable** | Select an end point entry, and select enable to enable blocking for that entry.  
The Enable icon will be green with a checkmark. |
| **Disable** | Select an end point entry, and select disable to disable blocking for that entry. This effectively turns off this entry.  
The Enable Icon will be grey with an X. |
| **Remove All Entries** | Remove all entries from the end point IP filter list. |
Example

You can use IP filtering on Carrier Endpoints when a handheld on your carrier network is known to be sending spam or malware. You can easily use IP filtering to block the traffic from that unit, log it, or both. This allows you to escalate your response, and even monitor afterwards as well.

In this example the handheld IP address is 10.11.101.99 and since they are sending malware this IP address will be both logged and blocked.

To create an IP filter list entry to block an address - web-based manager

1. Go to UTM > Carrier > IP Filter.
2. Select Create New.
3. Enter 10.11.101.199 for the Carrier End Point.
4. Select Log Blocked Traffic and Block Traffic.
5. Select OK.

Adding additional blocked IP addresses

In the future, additional IP filters can be added both to the Carrier End Point filtering list, and to the firewall address list. To add additional filters to the filtering list, repeat the procedure To create an IP filter list entry to block an address for each new additional IP address to be filtered.

To add additional firewall addresses to be matched in the security policy, enter each additional new IP address as a separate firewall address, and in the security policy for the address select multiple and then select all the IP_Filter_xx addresses. Using a logical naming convention for additional IP filters such as IP_Filter_02, IP_Filter_xx, etc. will help with configuration.
Extracting carrier end points for notifications - FortiOS Carrier only

The sender’s carrier end point is used to provide logging and reporting details to the mobile operator and to identify the sender of infected content.

When MMS messages are transmitted, the From field may or may not contain the sender’s address. When the address is not included, the sender information will not be present in the logs and the FortiOS Carrier unit will not be able to notify the user if the message is blocked unless the sender’s address is made available elsewhere in the request. One reason for this is if multiple users are behind the same NAT device.

Beyond logging, the sender address is also important for billing, end point control, and applying security policies. It is also important for differing levels of URL access.

FortiOS Carrier can extract the sender’s address from an extended HTTP header field in the HTTP request. This field must be added to the HTTP request before it is received by FortiOS Carrier. If this field is present, it will be used instead of the sender’s address in the MMS message for logging and notification. If this header field is present when a message is retrieved, it will be used instead of the To address in the message. If this header field is not present the content of the To header field is used instead.

Alternatively, FortiOS Carrier can extract the sender’s address from a cookie. The cookie is sent as part of the HTTP header.

You can configure MMS address translation to extract the sender’s carrier end point so that it can be added to log and notification messages. You can configure MMS address translation settings to extract carrier end points from HTTP header fields or from cookies. You can also configure MMS address translation to add an end point prefix to the extracted carrier end points.

To configure MMS address translation, go to Firewall > MMS Profile. Select Create New or select the Edit icon beside an existing profile. Expand MMS Address Translation. Complete the fields as described in the following table and select OK.

Configuring MMS address translation - FortiOS Carrier only

MMS address translation changes the address from using the one embedded in the MMS message to using the additional HTTP Header Field (if present) or a cookie to get the address.

This applies to MM1 and MM7 messages — messages sent to or from handsets, and messages sent to or from content providers. These are the only message types that use the HTTP headers that enable this feature.

To configure MMS address translation - web-based manager

1. Go to UTM > Carrier > MMS Profile.
2. Select Create New.
3. Expand MMS Address Translation.
4. Select settings for MM1 and MM7 as required.
5. Select OK.
Configuring end points

Dynamic profiles and end points

HTTP header field example

For this example, in FortiOS Carrier we are concerned about MMS traffic between content providers — MM7 traffic only. The default x-up-calling-line-id will be used in the HTTP header along with a country code of 9811. The Sender Address does need converting from hex. The prefix will be added to Logging/Notification using the MSISDN for the prefix.

To configure MMS address translation using HTTP header field

1. Go to UTM > Carrier > MMS Profile.
2. Select Create New.
3. Enter MMS_addr_http_header for the Profilename.
4. Expand MMS Address Translation.
5. Under MM7, select HTTP Header Field for Sender Address Source.
6. Under MM7, enter x-up-calling-line-id for Sender Address Identifier.
7. Under MM7, select Convert Sender Address From / To HEX.
8. Select Enable for Add End Point Prefix for Logging / Notification.
9 Enter 9811 for Prefix.
10 Select OK.

If the Sender Address Source is HTTP Header Field, the address and its identifier in the HTTP request header takes the format:

\[
\text{<Sender Address Identifier>: <MSISDN_value>}
\]

Where the \(<\text{MSISDN_value}>\) is the carrier end point. For example, the HTTP header might contain:

\[\text{x-up-calling-line-id: 9811301234}\]

where \(\text{x-up-calling-line-id}\) would be the Sender Address Identifier, and \(9811301234\) would be the MSISDN.

**Cookie example**

If you want the address to persist, then use a cookie. Keep in mind that cookies are a less secure method than the HTTP header field option because of their persistence.

For this example we are concerned about traffic to and from handsets and will only be using MM1. A non-standard field for Sender Address Identifier will be used: \(\text{x-up-calling-cookie}\), and a country code of 467. The Sender Address does not need converting from hex. The prefix will be added to Logging/Notification using the MSISDN for the prefix.

To configure MMS address translation using cookies - web-based manager

1 Go to UTM > Carrier > MMS Profile.
2 Select Create New.
3 Enter MMS_addr_cookie for the Profilename.
4 Expand MMS Address Translation.
5 Under MM1, select Cookie for Sender Address Source.
6 Under MM1, enter x-up-calling-cookie for Sender Address Identifier.
7 Select Enable for Add End Point Prefix for Logging / Notification.
8 Enter 467 for Prefix.
9 Select OK.

For MM1 messages, a cookie can now be referenced for the Sender's address. Any messages that trigger logging or notification that use this address translation will include the 467 prefix for added identification.

A sample HTTP request header resulting from this configuration would be:

\[
\text{Cookie: id=0123jf!a; x-up-calling-cookie=467301297}\]

where 0123jf!a is the cookie id, x-up-calling-cookie is the Sender Address Identifier, and 467301297 is the MSISDN.

**Timeout options**

Dynamic profile timeouts control how long FortiOS keeps entries in the user context list. Entries are removed when a RADIUS stop record is received by FortiOS, but otherwise entries remain in the context list until they timeout.
Usually you would not want entries staying in the user context list if they are not being used. A smaller list is easier and more efficient for FortiOS to manage. As well, because user context information can change, a smaller list means incorrect or out-of-date information is more likely to be removed.

However, some situations may benefit from keeping the entries in the user context list for a longer period of time. This may reduce network load and provide other benefits, but the security risk must be kept in mind as well.

<table>
<thead>
<tr>
<th>User Context Entry Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the number of seconds that a user context entry can remain in the list without FortiOS Carrier receiving a communication session from the end point. If a user context entry is not being looked up, then the user must no longer be connected to the network.</td>
</tr>
<tr>
<td>This timeout is only required if FortiOS Carrier does not receive the RADIUS Stop record. However, even if the accounting system does send RADIUS Stop records, this timeout must be set in case FortiOS Carrier misses one.</td>
</tr>
<tr>
<td>The default user context entry timeout is 28800 seconds (8 hours). You can keep this timeout relatively high because it is not usually a problem to have a long list. But a timeout is usually required because FortiOS Carrier normally removes entries that are no longer used.</td>
</tr>
<tr>
<td>You might want to reduce this timeout if the accounting server does not send RADIUS Stop records. Also, if customer IP addresses change often, you might want to set this timeout lower so that out-of-date entries are removed from the list.</td>
</tr>
<tr>
<td>Avoid entering a setting that is too low. FortiOS Carrier may remove user context entries for users who are still connected.</td>
</tr>
<tr>
<td>Set the timeout to 0 if you do not want FortiOS Carrier to remove entries from the list except in response to RADIUS Stop messages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Context Creation Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>If FortiOS Carrier receives a communication session and can’t find a corresponding end point and IP address in the user context list, the system waits for the User Context Creation Timeout. If a match is not found after this timeout, FortiOS Carrier applies the profile group in the security policy to the communication session.</td>
</tr>
<tr>
<td>The default user context creation timeout is 5 seconds. You might want to increase this timeout if the default profile group, instead of the dynamic profile, is being applied to users. This could be happening if there is a delay before FortiOS Carrier receives the RADIUS Start record from the accounting server.</td>
</tr>
<tr>
<td>If you set this timeout to 0, FortiOS Carrier blocks communication sessions that do not have a matching entry in the user context list.</td>
</tr>
</tbody>
</table>

Log settings

You can use Log settings to configure FortiOS Carrier to record event log messages for dynamic profile events. You can also set a log message period to group log messages.

When using a dynamic profile, RADIUS attributes are included in the log information including framed IP address, radius username, and profile group.
### Log Message Period

Enter the time in seconds to group event log messages for dynamic profile events. For example, if the log message period is 30 seconds, FortiOS Carrier generates groups of single-event log messages every 30 seconds instead of generating event log messages continuously. The grouped log messages generated each period contain a count of how many events of that type occurred.

If you set this period to 0, FortiOS Carrier generates all event log messages in real time.

### Protocol Errors

Select to have FortiOS generate event log messages if RADIUS protocol errors occur. One example could be a RADIUS record containing a RADIUS secret that does not match the one added to the dynamic profile.

### Missing Profile Errors

Select to have FortiOS generate an event log message whenever FortiOS Carrier cannot find a profile group name in a RADIUS start message that matches the name of a profile group added to FortiOS Carrier.

### Missing Context Errors

Select to have FortiOS generate an event log message whenever a user context creation timeout expires indicating that FortiOS Carrier was not able to match a communication session because a matching entry was not found in the user context list.

### Missed Accounting ‘Stop’ Events

Select to have FortiOS generate an event log message whenever a user context entry timeout expires indicating that FortiOS Carrier removed an entry from the user context list without receiving a RADIUS Stop message.

### Accounting Events

Select to have FortiOS generate an event log message when FortiOS Carrier does not find the expected information in a RADIUS record. This may happen, for example, if a RADIUS record contains more than the expected number of addresses.

### Other Log Messages

Select to have FortiOS generate event log messages for other events. The event is described in the log message. For example, a log message may be generated if the memory limit for the user context list is reached and the oldest entries in the table have been dropped.

---

# Carrier end point filters and blocking

Carrier end points are available on FortiOS units as well as FortiOS Carrier units. However, only FortiOS Carrier units can handle MMS traffic. In the following section, any reference to MMS messages is FortiOS Carrier only material.

This section includes:

- Controlling MMS service access based on a user’s end point - FortiCarrier Only
- Blocking access to the network based on end points - FortiOS Carrier only
- Extracting carrier end points for notifications - FortiOS Carrier only
Controlling access to MMS services based on a user's carrier end point

You can control access to MMS services for users according to their carrier end point by configuring carrier end point filtering (also called carrier end point blocking). Carrier end point filtering can filter MM1, MM3, MM4, and MM7 messages according to the carrier end points in the From or To addresses of the messages.

For a definition of carrier end points, see “End points” on page 177.

You configure carrier end point filtering by creating a carrier end point filter list containing carrier end point patterns. A carrier end point pattern can match one carrier end point or can use wildcards or regular expressions to match multiple carrier end points.

For each pattern, you select the action that FortiOS Carrier takes on a message when the pattern matches a carrier end point in the message. Actions include blocking the message, exempting the message from mass MMS scanning and exempting the message from all scanning. You can also intercept the message and archive the message to a FortiAnalyzer unit.

To apply a carrier end point filter list, you need to add the list to the MMS Scanning > Carrier End Point Block section of an MMS protection profile.

Filtering MMS flows from selected carrier end points

You may want to block specific MMS protocols or block all of them depending on the situation. For example if you wanted to block traffic from selected handsets, you only need to select MM1 traffic. The benefit of this is a more specific match allows you to create individual security policies for each situation on your network. Extending the example you would have one policy for MM1 handset traffic, another policy for Internet MM3 traffic, another policy for Content Provider MM7 traffic, and another policy for inter-provider MM4 traffic.

Dividing traffic into smaller groups enables focused logging and reporting, while providing a more secure and customized firewall solution for your specific needs. When something changes, its easier to update a specific smaller security policy than to update a single large complex rambling policy.

Configuring carrier end point filtering

To apply carrier end point filtering - web-based manager

1. Go to UTM > Carrier End Point > Carrier End point Filter Lists.
2. Add or edit a carrier end point filter list.
3. Add or edit carrier end point patterns in the list.
4. Go to UTM > Carrier > MMS Profile and add or edit an MMS protection profile.
5. Expand MMS Scanning and select Carrier End Point Block.
6. Select the MMS protocols to apply the carrier end point filter list to (MM1, MM3, MM4 and MM7).
7. Select the carrier end point filter list to apply.
8. Add the MMS protection profile to a protection profile.
9. Add the protection profile to a security policy that accepts the MMS messages that you want to filter.

To configure a carrier end point filter list - web-based manager

To configure a carrier end point filter list go to UTM > Carrier > Carrier End Point Filter Lists.
### Blocking network access for IP addresses based on carrier end points

You can use carrier end point IP filtering to block traffic from source IP addresses associated with carrier end points. You can also configure FortiOS Carrier to record log messages whenever carrier end point IP filtering blocks traffic. Carrier end point IP filtering blocks traffic at the IP level, before the traffic is accepted by a security policy.

For a definition of carrier end points, see “End points” on page 177.
To configure carrier end point IP filtering, go to UTM > Carrier > IP Filter and add carrier end points to the IP filter list. For each carrier end point you can enable or disable both blocking traffic and logging blocked traffic.

You cannot add carrier end point patterns to the carrier end point IP filter list. You must enter complete and specific carrier end points that are valid for your network.

The only action available is block. You cannot use carrier end point IP filtering to exempt carrier end points from IP filtering or to content archive or quarantine communication sessions.

FortiOS Carrier looks in the current user context list for the carrier end points in the IP filter list and extracts the source IP addresses for these carrier end points. Then any communication session with a source IP address that matches one of these IP addresses is blocked at the IP level, before the communication session is accepted by a security policy.

FortiOS Carrier dynamically updates the list of IP addresses to block as the user context list changes. Only these updated IP addresses are blocked by carrier end point IP filtering.

Configuring end point IP filtering includes:
- Viewing and defining a carrier end point IP filter list
- Adding additional blocked IP addresses

### Viewing and defining a carrier end point IP filter list

To view the carrier end point IP filter list, go to UTM > Carrier > IP Filter.

You define a carrier end point IP filter list by adding IP addresses to it. From this list, you can select Create New to add a new IP address or select the Edit icon beside an entry that you want to change.

There is only one IP filter list, and each entry can be blocked or allowed. The single list prevents configuration issues by applying all IP filters to all MMS protection profiles that use IP filtering.

Once the IP filters are configured, it is applied to all Carrier Endpoints as their traffic hits the security policies.

<table>
<thead>
<tr>
<th>Carrier end point IP filter list</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create New</strong></td>
</tr>
<tr>
<td><strong>Edit</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td><strong>Enable</strong></td>
</tr>
</tbody>
</table>
You can use IP filtering on Carrier Endpoints when a handheld on your carrier network is known to be sending spam or malware. You can easily use IP filtering to block the traffic from that unit, log it, or both. This allows you to escalate your response, and even monitor afterwards as well.

In this example the hand held device IP address is 10.11.101.99 and since they are sending malware this IP address will be both logged and blocked. The following general steps are required.

1. Create an IP filter list entry to block an address
2. Create an MMS protection profile to use this IP filter list
3. Create a firewall address for the blocked IP address, and create incoming and outgoing security policies that use the firewall address and MMS profile.

Firewall configuration is not explained here. See the Fundamentals guide.

To create an IP filter list entry to block an address - web-based manager

1. Go to UTM > Carrier > IP Filter.
2. Select Create New.
3. Enter 10.11.101.199 for the Carrier End Point.
4. Select Log Blocked Traffic and Block Traffic.
5. Select OK.

To create an MMS protection profile to use the IP filter
1. Go to UTM > Carrier > MMS profile.
2. Select Create New.
3. Enter ipFilteringProfile as the Profilename.
4. Expand MMS Scanning.
5. Select all MMS protocols for Carrier End Point Block.
6. Select my IP filter list from the Option menu for Carrier End Point Block.
7. Select any other settings as required for this MMS protection profile.
8. Select OK.

Adding additional blocked IP addresses
In the future, additional IP filters can be added both to the Carrier End Point filtering list, and to the firewall address list. To add additional filters to the filtering list repeat general step 1 for each new additional IP address to be filtered. To add additional firewall addresses to be matched in the security policy, enter each additional new IP address as a separate firewall address, and in the security policy for the address select multiple and then select all the IP_Filter_xx addresses. Using a logical naming convention for additional IP filters such as IP_Filter_02, IP_Filter_xx, etc. will help with configuration.

Troubleshooting dynamic profiles

This section provides you with some commands and methods for troubleshooting dynamic profile issues.

This section includes:
- General dynamic profile troubleshooting
- Dynamic profile related diag commands

General dynamic profile troubleshooting

When you are troubleshooting, work your way down the list. The first solution is more general, and each solution becomes more specific as you move down the list.

- If dynamic profiles are not displayed anywhere in the web-based manager they must un-hidden. Go to System > Admin > Settings and select Dynamic Profile Support on GUI. If VDOMs are enabled, this is at the global level.
- Dynamic server option does not appear in RADIUS server configuration. This means there is already one dynamic RADIUS server configured. To configure another you must first locate and remove the original configuration.
- Dynamic profile option is not displayed in security policies. There are two possible reasons for this. The first is that there is already another security policy with dynamic profile enabled—this must be removed before you can configure another dynamic security policy. Second, when identity-based policy is selected in a security policy dynamic profile is not displayed. For dynamic profile option to reappear, un-select identity-based profile.
• Valid users not being authenticated. It is possible that it is taking too long for the FortiOS unit to receive the RADIUS start record, and the security policy is failing from lacking that information.

**Dynamic profile related diag commands**

You can use the following FortiOS diagnose commands to debug communication between the RADIUS server and FortiOS:

```
diag test application radiusd 2
```
Clears the user context list. This is similar to having all users log off.

```
diag test application radiusd 3
```
Shows the user context list (user, profile, ip)

```
diag test application radiusd 5
```
Displays RADIUS statistics such as the number of RADIUS Start and Stop packets received, the number of packet errors and so on.

```
diag dynamic-profile query ip 10.0.0.1
```
A filter that displays the same kind of information as `diagnose test application radiusd 3`.

```
diag dynamic-profile query profile-usage <vdom_name>
```
Displays a summary of profile usage for the named VDOM.

```
diag debug application radiusd 3
```
Displays carrier end points and their associated profile group names. An example entry for carrier end point 5551231234 and profile group name profile_name could be:

```
<000.000000> [49]: received from radiusd -- msgId=41, profile=profile_name, endpoint=5551231234 [49]: delayed setup for profile profile_name)
```

In the following example, the command `diagnose test application radiusd 3` displays three entries in the user context list. In this example, the carrier end points are listed under endpoint and they are all email addresses. This example output uses example IP addresses and domain names.

```
index,"time left (hh:mm:ss)",ip,endpoint,profile,rc,"Default Profile?",Blacklist?
1,07:08:07,"192.168.23.7","33example@example.com","PackageVAS2",1, No, No
2,07:23:32,"192.168.33.112","45example@example.com","PackageVAS2",1, No, No
3,07:28:32,"172.20.123.71","332example@example.com","PackageVAS1",1, No, No
```
Monitoring authenticated users

This section describes how to view lists of currently logged-in firewall and VPN users. It also describes how to disconnect users.

The following topics are included in this section:
- Monitoring firewall users
- Monitoring SSL VPN users
- Monitoring IPsec VPN users

Monitoring firewall users

To monitor firewall users, go to User > Monitor > Firewall>

Figure 16: Firewall users listed in monitor

You can de-authenticate a user by selecting the Delete icon for that entry.

You can filter the list of displayed users either by selecting the funnel icon for one of the column titles or selecting Filter Settings.

Select Column Settings to add or remove columns to the display, or rearrange the order of the columns displayed.

Optionally, you can select De-authenticate all users. Best practices dictate that this only be used in extreme cases since all users will momentarily lose their network resource connections.

Monitoring SSL VPN users

You can monitor web-mode and tunnel-mode SSL VPN users by username and IP address.

To monitor SSL VPN users, go to VPN > Monitor > SSL-VPN Monitor. To disconnect a user, select the user and then select the Delete icon.

Figure 17: Monitoring SSL VPN users

The first line, listing the username and IP address, is present for a user with either a web-mode or tunnel-mode connection. The Subsession line is present only if the user has a tunnel mode connection. The Description column displays the virtual IP address assigned to the user’s tunnel-mode connection.
For more information about SSL VPN, see the *FortiOS Handbook SSL VPN guide*.

**To monitor SSL VPN users - CLI**

To list all of the SSL VPN sessions and their index numbers:

```
execute vpn sslvpn list
```

The output looks like this:

<table>
<thead>
<tr>
<th>Index</th>
<th>User</th>
<th>Auth Type</th>
<th>Timeout</th>
<th>From</th>
<th>HTTPS in/out</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>user1</td>
<td>1</td>
<td>256</td>
<td>172.20.120.51</td>
<td>0/0</td>
</tr>
</tbody>
</table>

SSL-VPN sessions:

<table>
<thead>
<tr>
<th>Index</th>
<th>User</th>
<th>Source IP</th>
<th>Tunnel/Dest IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>user2</td>
<td>172.20.120.51</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>

You can use the Index value in the following commands to disconnect user sessions:

**To disconnect a tunnel-mode user**

```
execute vpn sslvpn del-tunnel <index>
```

**To disconnect a web-mode user**

```
execute vpn sslvpn del-web <index>
```

You can also disconnect multiple users:

**To disconnect all tunnel-mode SSL VPN users in this VDOM**

```
execute vpn ssl del-all tunnel
```

**To disconnect all SSL VPN users in this VDOM**

```
execute vpn ssl del-all
```

---

### Monitoring IPsec VPN users

To monitor IPsec VPN tunnels in the web-based manager, go to *VPN > Monitor > IPsec Monitor*. Usernames are available only for users who authenticate with XAuth.

You can close a tunnel by selecting its *Bring Down* link in the *Status* column.

**Figure 18: Monitoring dialup VPN users**

<table>
<thead>
<tr>
<th>Type</th>
<th>Dialup</th>
<th>Name</th>
<th>Remote Gateway</th>
<th>Timeout</th>
<th>Status</th>
<th>Incoming Data</th>
<th>Outgoing Data</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dialup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>172.20.120.51</td>
<td>1116</td>
<td>Brin Down</td>
<td>79233170 B</td>
<td>171655314 B</td>
<td>user2</td>
<td></td>
</tr>
</tbody>
</table>

For more information, see the *FortiOS Handbook IPsec VPN guide*. 
Examples and Troubleshooting

This chapter provides an example of a FortiGate unit providing authenticated access to the Internet for both Windows network users and local users.

The following topics are included in this section:

- Firewall authentication example
- LDAP Dial-in using member-attribute
- Dynamic Profile example
- Troubleshooting

Firewall authentication example

Figure 19: Example configuration

Overview

In this example, there is a Windows network connected to Port 2 on the FortiGate unit and another LAN, Network_1, connected to Port 3.

All Windows network users authenticate when they logon to their network. Members of the Engineering and Sales groups can access the Internet without entering their authentication credentials again. The example assumes that the Fortinet Single Sign On (FSSO) has already been installed and configured on the domain controller.
LAN users who belong to the Internet_users group can access the Internet after entering their username and password to authenticate. This example shows only two users, User1 is authenticated by a password stored on the FortiGate unit, User2 is authenticated on an external authentication server. Both of these users are referred to as local users because the user account is created on the FortiGate unit.

**Creating a locally-authenticated user account**

User1 is authenticated by a password stored on the FortiGate unit. It is very simple to create this type of account.

**To create a local user - web-based manager**

1. Go to User > User and select Create New.
2. Enter the following information: username, Password.
3. Select OK.

<table>
<thead>
<tr>
<th>username</th>
<th>User1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>hardtoguess</td>
</tr>
</tbody>
</table>

**To create a local user - CLI**

```
config user local
edit user1
  set type password
  set passwd hardtoguess
end
```

**Creating a RADIUS-authenticated user account**

To authenticate users using an external authentication server, you must first configure the FortiGate unit to access the server.

**To configure the remote authentication server - web-based manager**

1. Go to User > Remote > RADIUS and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>OurRADIUSsrv</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Server Name/IP</td>
<td>10.11.101.15</td>
</tr>
<tr>
<td>Primary Server Secret</td>
<td>OurSecret</td>
</tr>
<tr>
<td>Authentication Scheme</td>
<td>Select Use Default Authentication Scheme</td>
</tr>
</tbody>
</table>

**To configure the remote authentication server - CLI**

```
config user radius
edit OurRADIUSsrv
  set server 10.11.102.15
  set secret OurSecret
  set auth-type auto
end
```

Creation of the user account is similar to the locally-authenticated account, except that you specify the RADIUS authentication server instead of the user’s password.
To configure a remote user - web-based manager

1. Go to User > User and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>User2</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Select Match user on RADIUS server and then select OurRADIUSsrv from the list.</td>
</tr>
</tbody>
</table>

To configure a remote user - CLI

```
config user local
   edit User2
      set name User2
      set type radius
      set radius-server OurRADIUSsrv
   end
```

Creating user groups

There are two user groups: an FSSO user group for FSSO users and a firewall user group for other users. It is not possible to combine these two types of users in the same user group.

Creating the FSSO user group

For this example, assume that FSSO has already been set up on the Windows network and that it uses Advanced mode, meaning that it uses LDAP to access user group information. You need to

- configure LDAP access to the Windows AD global catalog
- specify the collector agent that sends user logon information to the FortiGate unit
- select Windows user groups to monitor
- select and add the Engineering and Sales groups to an FSSO user group

To configure LDAP for FSSO - web-based manager

1. Go to User > Remote > LDAP and select Create New.
2. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>ADserver</td>
</tr>
<tr>
<td>Server Name / IP</td>
<td>10.11.101.160</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>dc=office,dc=example,dc=com</td>
</tr>
<tr>
<td>Bind Type</td>
<td>Regular</td>
</tr>
<tr>
<td>User DN</td>
<td>cn=FSSO_Admin,cn=users,dc=office,dc=example,dc=com</td>
</tr>
<tr>
<td>Password</td>
<td>set_a_secure_password</td>
</tr>
</tbody>
</table>

Leave other fields at their default values.
3. Select OK.
To configure LDAP for FSSO - CLI

```
config user ldap
  edit "ADserver"
    set server "10.11.101.160"
    set dn "cn=users,dc=office,dc=example,dc=com"
    set type regular
    set username "cn=administrator,cn=users,dc=office,dc=example,dc=com"
    set password set_a_secure_password
  next
end
```

To specify the collector agent for FSSO - web-based manager

1. Go to User > FSSO and select Create New.
2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>WinGroups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter on one line</td>
<td></td>
</tr>
<tr>
<td>Collector IP/Name</td>
<td>10.11.101.160</td>
</tr>
<tr>
<td>Port</td>
<td>8000</td>
</tr>
<tr>
<td>Password</td>
<td>fortinet_canada</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>ADserver</td>
</tr>
</tbody>
</table>

To specify the collector agent for FSSO - CLI

```
config user fsso
  edit "WinGroups"
    set ldap-server "ADserver"
    set password ENC
      G7GQV7NEqiiCM9jKmVmJJPVvhhQ2+wtNEe9T0iYA5Sa+EqT2J8zh0rbkJFDr0RnY3c4LaoXds0BczAl0DNmcGfthTxxwGsigzGpbJdC71spFLQYty
    set server "10.11.101.160"
end
```

To select Windows user groups to monitor - web-based manager

1. Go to User > FSSO > FSSO Agent.
2. Expand WinGroups, then select the Edit Users/Groups icon.
3. Select the Engineering and Sales groups and then select OK.

To create the FSSO_Internet-users user group - web-based manager

1. Go to User > User Group and select Create New.
2. Enter the group name, FSSO_Internet_users.
4. In the Available Members list, select the Engineering and Sales groups and then select the right arrow button to move them to the Members list.
5. Select OK.
To create the FSSO_internet-users user group - CLI

```
config user group
edit FSSO_internet_users
set group-type directory-service
set member
  CN=Engineering,cn=users,dc=office,dc=example,dc=com
  CN=Sales,cn=users,dc=office,dc=example,dc=com
end
```

Creating the Firewall user group

The non-FSSO users need a user group too. In this example, only two users are shown, but additional members can be added easily.

To create the firewall user group - web-based manager

1. Go to User > User Group and select Create New.
2. Enter the following information and then select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>Internet_users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Firewall</td>
</tr>
<tr>
<td>Members</td>
<td>User1, User2</td>
</tr>
</tbody>
</table>

To create the firewall user group - CLI

```
config user group
edit Internet_users
set group-type firewall
set member User1 User2
end
```

Defining policy addresses

Go to Firewall Objects > Address and create the following addresses:

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Internal_net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.11.102.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>Port 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address Name</th>
<th>Windows_net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Subnet / IP Range</td>
</tr>
<tr>
<td>Subnet / IP Range</td>
<td>10.11.101.0/24</td>
</tr>
<tr>
<td>Interface</td>
<td>Port 2</td>
</tr>
</tbody>
</table>

Creating security policies

Two security policies are needed: one for firewall group who connect through port3 and one for FSSO group who connect through port2.

To create a security policy for FSSO authentication - web-based manager

1. Go to Policy > Policy and select Create New.
2 Enter the following information:

<table>
<thead>
<tr>
<th>Source interface</th>
<th>Port2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address</td>
<td>Windows_net</td>
</tr>
<tr>
<td>Destination interface</td>
<td>Port1</td>
</tr>
<tr>
<td>Destination address</td>
<td>all</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Enable</td>
</tr>
</tbody>
</table>

3 Select *Enable identity-based Policy* and then select *Add*.

In the *New Authentication Rule* window, enter the following information, and then select OK:

<table>
<thead>
<tr>
<th>User Group</th>
<th>FSSO_Internet_users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>UTM</td>
<td>Optionally, enable UTM options.</td>
</tr>
</tbody>
</table>

4 Select OK.

**To create a security policy for FSSO authentication - CLI**

```
config firewall policy
edit 0
set srcintf port2
set dstintf port1
set srcaddr Windows_net
set dstaddr all
set action accept
set identity-based enable
set nat enable
config identity-based-policy
edit 1
set schedule always
set groups FSSO_Internet_users
set service ANY
end
end
```

**To create a security policy for local user authentication - web-based manager**

1 Go to *Policy > Policy* and select *Create New*.

2 Enter the following information:

<table>
<thead>
<tr>
<th>Source interface</th>
<th>Port3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address</td>
<td>Internal_net</td>
</tr>
<tr>
<td>Destination interface</td>
<td>Port1</td>
</tr>
<tr>
<td>Destination address</td>
<td>all</td>
</tr>
</tbody>
</table>
3 Select **Enable identity-based Policy** and then select **Add**.

In the **New Authentication Rule** window, enter the following information, and then select **OK**:

<table>
<thead>
<tr>
<th>User Group</th>
<th>Internet_users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>UTM</td>
<td>Optionally, enable UTM options.</td>
</tr>
</tbody>
</table>

4 Select **OK**.

**To create a security policy for local user authentication - CLI**

```plaintext
config firewall policy
edit 0
set srcintf port3
set dsrcintf port1
set srcaddr internal_net
set dstaddr all
set action accept
set identity-based enable
set nat enable
config identity-based-policy
edit 1
set schedule always
set groups Internet_users
set service ANY
end
end
```

**LDAP Dial-in using member-attribute**

In this example, users defined in MicroSoft Windows Active Directory (AD) are allowed to setup a VPN connection simply based on an attribute that is set to TRUE, instead of based on the group they are in like normal. In AD the "Allow Dialin" property is activated in the user properties, and this sets the `msNPAllowDialin` attribute to "TRUE".

This same procedure can be used for other member attributes, as your system requires.

To accomplish this with a FortiGate unit, member-attribute must be set. This can only be accomplished through the CLI - the option is not available through the web-based manager.

Before configuring the FortiGate unit, ensure the AD server has the `msNPAllowDialin` attribute set to "TRUE" for the users in question. If not, those users will not be able to authenticate.

**To configure user LDAP member-attribute settings - CLI**

```plaintext
config user ldap
edit "ldap_server"
set server "192.168.201.3"
```
LDAP Dial-in using member-attribute

set cnid "sAMAccountName"
set dn "DC=fortilabanz,DC=com,DC=au"
set type regular
set username "fortigate@sample.com"
set password ******
set filter "(&(uid=%u)(msNPAllowDialin=TRUE))"
set member-attr "msNPAllowDialin"
next
end

To configure LDAP group settings - CLI

config user group
edit "ldap_grp"
set member "ldap"
config match
edit 1
set server-name "ldap"
set group-name "TRUE"
next
next
end

Once these settings are in place, users that are a member of the ldap user group will be able to authenticate.

To ensure your settings are correct, here is the sample output from a diag debug command that shows the authentication process.

When the "Allow Dial-in" attribute is set to "TRUE" the following will likely be in the output:
get member_of_groups-Get the memberOf groups.
get member_of_groups- attr='msNPAllowDialin', found 1 values
get member_of_groups-val[0]='TRUE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Passed group matching

If the attribute is not set but it is expected, the following will likely be in the output:
get member_of_groups-Get the memberOf groups.
get member_of_groups- attr='msNPAllowDialin', found 1 values
get member_of_groups-val[0]='FALSE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Failed group matching

The only difference between these two outputs is the last line which is either passed or failed based on if the member-attribute is set to the expected value or not.
Dynamic Profile example

A common dynamic profile topology involves a medium sized company network of users connecting to the Internet through the FortiGate unit, and authenticating with a RADIUS server. Dynamic profile authentication was selected because it is fast and relatively easy to configure.

This section includes:
- Assumptions
- Topology
- General configuration
- Configuring RADIUS
- Configuring FortiGate regular and dynamic profile security policies
- Testing

Assumptions

- VDOMs are not enabled
- The admin super_admin administrator account will be used for all FortiGate unit configuration.
- Any other devices on the network do not affect the topology of this example, and therefore are not included.
- Anywhere settings are not described, they are assumed to be default values.
- third-party RADIUS server is installed on a server box.
- BGP is used for any dynamic routing.
- Authentication event logging under Log&Report has been configured.

Topology

Example.com has an office with 20 users on the internal network. These users need access to the Internet to do their jobs. The office network is protected by a FortiGate-60C unit with access to the Internet through the wan1 interface, the user network on the internal interface, and all the servers are on the DMZ interface. This includes an Ubuntu Linux server running FreeRADIUS. For this example only two users will be configured — Pat Lee with an account name plee, or plee@example.com, and Kelly Green with an account name kgreen, or kgreen@example.com.
General configuration

1. Configuring RADIUS with users, user group, and FortiGate information.
2. Configuring FortiGate interfaces
3. Configuring dynamic profile RADIUS server on FortiGate
4. Configuring FortiGate regular and dynamic profile security policies

Configuring RADIUS

Configuring RADIUS includes configuring the RADIUS server such as FreeRADIUS, a radius client on user’s computers, and configuring users in the system. For this example the two users will be Pat Lee, and Kelly Green. They belong to a group called exampledotcom_employees. When it is all configured, the RADIUS daemon needs to started.

The users have a RADIUS client installed on their PCs that allows them to authenticate through the RADIUS server.

FreeRADIUS can be found on the freeradius.org website. For any problems installing FreeRADIUS, see the FreeRADIUS documentation.

Configuring FortiGate interfaces

Before configuring the dynamic profile security policy, configure FortiGate interfaces. This includes defining DHCP servers for the dmz and internal networks as these networks typically use DHCP. However, wan1 is assigned a static IP address by the ISP and does not need a DHCP server.

Table 9: FortiGate interfaces used in this example

<table>
<thead>
<tr>
<th>Interface</th>
<th>Subnet</th>
<th>Act as DHCP Server</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>wan1</td>
<td>172.20.120.141</td>
<td>No</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>dmz</td>
<td>10.11.101.100</td>
<td>Yes: x.x.x.110-.250</td>
<td>Servers, including RADIUS server</td>
</tr>
<tr>
<td>internal</td>
<td>10.11.102.100</td>
<td>Yes: x.x.x.110-.250</td>
<td>Internal user network</td>
</tr>
</tbody>
</table>
To configure FortiGate interfaces - web-based manager

1. Go to System > Network > Interface.
2. Select wan1 to edit.
3. Enter the following information and select OK.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing Mode</td>
<td>Manual</td>
</tr>
<tr>
<td>IP/Netmask</td>
<td>172.20.120.141/255.255.255.0</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>HTTPS, SSH</td>
</tr>
<tr>
<td>Comments</td>
<td>Internet</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Up</td>
</tr>
</tbody>
</table>

4. Select dmz to edit.
5. Enter the following information and select OK.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing Mode</td>
<td>Manual</td>
</tr>
<tr>
<td>IP/Netmask</td>
<td>10.11.101.100/255.255.255.0</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>HTTPS, SSH, PING, SNMP</td>
</tr>
<tr>
<td>Comments</td>
<td>Servers</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Up</td>
</tr>
</tbody>
</table>

6. Select internal to edit.
7. Enter the following information and select OK.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Internal network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing Mode</td>
<td>Manual</td>
</tr>
<tr>
<td>IP/Netmask</td>
<td>10.11.102.100/255.255.255.0</td>
</tr>
<tr>
<td>Administrative Access</td>
<td>HTTPS, SSH, PING</td>
</tr>
<tr>
<td>Comments</td>
<td>Internal network</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Up</td>
</tr>
</tbody>
</table>

To configure DHCP servers - web-based manager

1. Go to System > Network > DHCP Server.
2. Select Create New.
3. Enter the following information and select OK.

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>dmz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Server</td>
</tr>
</tbody>
</table>
Configuring dynamic profile RADIUS server on FortiGate

The FortiGate unit needs the RADIUS server information to be able to properly connect to it. Only one entry can be configured. If you cannot create one, ensure there is not already one configured.

The Profile Key entry must match the group name for users on the RADIUS server to be validated. Enable all logging if possible as it will assist with troubleshooting.

To configure the dynamic profile RADIUS server

2. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>dynamic_profile_server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Dynamic Start</td>
</tr>
<tr>
<td>Endpoint Attribute</td>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Profile Attribute</td>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Endpoint Blocking Attribute</td>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Send RADIUS Response</td>
<td>enable</td>
</tr>
<tr>
<td>Validate Radius Secret</td>
<td>enable</td>
</tr>
<tr>
<td>Profile Key</td>
<td>my_dyn_prof_group</td>
</tr>
<tr>
<td>Log All Events</td>
<td>enable</td>
</tr>
</tbody>
</table>
Configuring FortiGate regular and dynamic profile security policies

With the RADIUS server and FortiGate interfaces configured, security policies can be configured. This includes both dynamic profile and regular policies, as well as addresses and address groups. All policies require NAT to be enabled.

Table 10: security policies needed for dynamic profile

<table>
<thead>
<tr>
<th>Seq. No.</th>
<th>From -&gt; To</th>
<th>Type</th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>internal -&gt; wan1</td>
<td>dynamic profile</td>
<td>business hours</td>
<td>Authenticate outgoing user traffic.</td>
</tr>
<tr>
<td>2</td>
<td>internal -&gt; wan1</td>
<td>regular</td>
<td>always</td>
<td>Allow essential network services and VoIP.</td>
</tr>
<tr>
<td>3</td>
<td>dmz -&gt; wan1</td>
<td>regular</td>
<td>always</td>
<td>Allow servers to access Internet.</td>
</tr>
<tr>
<td>4</td>
<td>internal -&gt; dmz</td>
<td>regular</td>
<td>always</td>
<td>Allow users to access servers.</td>
</tr>
<tr>
<td>5</td>
<td>any -&gt; any</td>
<td>deny</td>
<td>always</td>
<td>Implicit deny all traffic that hasn’t been matched</td>
</tr>
</tbody>
</table>

The dynamic profile policy must be placed at the top of the policy list so it is matched first. The only exception to this is if you have a policy to deny access to a list of banned users. In this case, that policy must go at the top so the dynamic profile does not mistakenly match a banned user or IP address.

This section includes:
- Schedules, address groups, and services groups
- Configuring regular security policies
- Configuring dynamic profile security policy

Schedules, address groups, and services groups

This section lists the lists that need to be configured before security policies are created. Creating these lists is straightforward, so the essential information has been provided here but not step by step instructions. For more information on firewall related details, see

Schedules

Only one schedule needs to be configured — business_hours. This is a fairly standard Monday to Friday 8am to 5pm schedule, or whatever days and hours covers standard work hours at the company.

Address groups

The following address groups need to be configured before the security policies.

<table>
<thead>
<tr>
<th>Address group Name</th>
<th>Interface</th>
<th>Address range included</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal_network</td>
<td>internal</td>
<td>10.11.102.110 to 10.11.102.250</td>
</tr>
<tr>
<td>company_servers</td>
<td>dmz</td>
<td>10.11.101.110 to 10.11.101.250</td>
</tr>
</tbody>
</table>
Service groups

The following service groups need to be configured before the security policies. Note that the services listed are suggestions and may include more or less as required.

<table>
<thead>
<tr>
<th>Service group Name</th>
<th>Interface</th>
<th>Description of services to be included</th>
</tr>
</thead>
<tbody>
<tr>
<td>essential_network_services</td>
<td>internal</td>
<td>Any network protocols required for normal network operation such as DNS, NTP, BGP.</td>
</tr>
<tr>
<td>essential_server_services</td>
<td>dmz</td>
<td>All the protocols required by the company servers such as BGP, HTTP, HTTPS, FTP, IMAP, POP3, SMTP, IKE, SQL, MYSQL, NTP, TRACEROUTE, SOCKs, and SNMP.</td>
</tr>
<tr>
<td>dynamic_profile_services</td>
<td>internal</td>
<td>Any protocols required by users HTTP, HTTP, FTP,</td>
</tr>
</tbody>
</table>

The following security policy configurations are basic and only include logging, and default AV and IPS.

Configuring regular security policies

Regular security policies allow or deny all non-dynamic profile traffic. This is essential as there are network services—such as DNS, NTP, and FortiGuard—that require access to the Internet.

To configure regular security policies - web-based manager

1. Go to Policy > Policy, and select Create New.
2. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>internal_network</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>essential_network_services</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>enable</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>enable</td>
</tr>
<tr>
<td>UTM</td>
<td>enable</td>
</tr>
<tr>
<td>Enable Antivirus</td>
<td>enable Default</td>
</tr>
<tr>
<td>Enable IPS</td>
<td>enable Default</td>
</tr>
<tr>
<td>Enable VoIP</td>
<td>enable Default</td>
</tr>
<tr>
<td>Comments</td>
<td>Essential network services</td>
</tr>
</tbody>
</table>

3. Select Create New, enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>dmz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>company_servers</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
</tbody>
</table>
Examples and Troubleshooting

Dynamic Profile example

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>essential_server_services</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>enable</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>enable</td>
</tr>
<tr>
<td>UTM</td>
<td>enable</td>
</tr>
<tr>
<td>Enable Antivirus</td>
<td>enable Default</td>
</tr>
<tr>
<td>Enable IPS</td>
<td>enable Default</td>
</tr>
<tr>
<td>Comments</td>
<td>Company servers accessing the Internet</td>
</tr>
</tbody>
</table>

4 Select Create New, enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>internal_network</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>dmz</td>
</tr>
<tr>
<td>Destination Address</td>
<td>company_servers</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>all</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>enable</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>enable</td>
</tr>
<tr>
<td>UTM</td>
<td>enable</td>
</tr>
<tr>
<td>Enable Antivirus</td>
<td>enable Default</td>
</tr>
<tr>
<td>Enable IPS</td>
<td>enable Default</td>
</tr>
<tr>
<td>Comments</td>
<td>Access company servers</td>
</tr>
</tbody>
</table>

Configuring dynamic profile security policy

A dynamic profile security policy has less configuration than a regular security policy. Before configuring the policy, you must configure a UTM Profile Group. This group name must match the RADIUS user group name.

If \( UTM > \text{Profile Group} \) is not visible, to go \( \text{System} > \text{Admin} > \text{Settings} \) and display it on the GUI.

To configure UTM profile group

1. Go to \( UTM > \text{Profile Group} > \text{Profile Group} \), and select Create New.
2. Enter the name exampledotdcom_employees.
4. Select OK.
To configure dynamic profile security policy

1. Go to Policy > Policy, and select Create New.
2. Enter the following information, and select OK.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>internal_network</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>business_hours</td>
</tr>
<tr>
<td>Service</td>
<td>all</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>Log Allowed Traffic</td>
<td>enable</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>enable</td>
</tr>
<tr>
<td>Enable Dynamic Profile</td>
<td>Enable</td>
</tr>
<tr>
<td>Profile Group</td>
<td>exampledotcom_employees</td>
</tr>
<tr>
<td>Dynamic Profile Users Only</td>
<td>enable</td>
</tr>
<tr>
<td>UTM</td>
<td>enable</td>
</tr>
<tr>
<td>Enable Antivirus</td>
<td>enable Default</td>
</tr>
<tr>
<td>Enable IPS</td>
<td>enable Default</td>
</tr>
<tr>
<td>Enable Web Filter</td>
<td>enable Default</td>
</tr>
<tr>
<td>Enable Email Filter</td>
<td>enable Default</td>
</tr>
<tr>
<td>Comments</td>
<td>Access company servers</td>
</tr>
</tbody>
</table>

Testing

Once configured, a user only needs to logon to their PC using their RADIUS account. After that when they attempt to access an Internet website, the FortiGate unit will use their session information to get their RADIUS information. Once the user is verified, they are allowed access to the website.

To test the configuration perform the following steps.

1. Have user plee logon to their PC, and try to access an Internet website.
2. The FortiGate unit will contact the RADUS server for user plee’s information.
3. Once confirmed, plee will have access to the website.

Each step generates log entries that enable you to verify that each step was successful. If a step is unsuccessful, confirm your configuration is correct and see "Troubleshooting dynamic profiles" on page 206.
Troubleshooting

In the web-based manager, a good tool for troubleshooting is the packet counter column on the security policy page (Policy > Policy). This column displays the number of packets that have passed through this security policy. Its value when you are troubleshooting is that when you are testing your configuration (end to end connectivity, user authentication, policy use) watching the packet count for an increase confirms any other methods you may be using for troubleshooting. It provides the key of which policy is allowing the traffic, useful information if you expect a user to require authentication and it never happens. For more information about authentication security policies, see “Authentication in security policies” on page 96.

This section addresses how to get more information from the CLI about users and user authentication attempts to help troubleshoot failed authentication attempts.

- `diag firewall iprope authuser`  
  Shows the IP of where your computer is connected from. This is useful to confirm authorization and VPN settings.

- `diag firewall iprope resetauth`  
  Clear all authorized users from the current list. Useful to force users to re-authenticate after system or group changes. However, this command may easily result in many users having to re-authenticate, so use carefully.

- `diag firewall auth list`  
  List all the authorized users on this system.

- `diag debug disable`  
- `diag application auth 1`  
- `diag debug enable`
  See the stream of authentication system messages displayed enter the following commands. Best practices dictate the use of a terminal program that logs output so you can save the system messages to analyze later.
For more information on troubleshooting specific features, go to that section of this document. Most sections have troubleshooting information at the end of the section. In addition to that information, see the FortiOS Handbook Troubleshooting guide for general troubleshooting information.
Index

A
A, 98
accounting system
RADIUS, 180
Active Directory - see Directory Service
Active Directory (AD), 19, 66, 133
access mode, 150
adding or configuring
authenticated access, 93
carrier end point IP filter, 195, 204
carrier end point MMS filter, 192
carrier end point MMS filter list, 193, 202
dynamic profile, 182
local users, 74
log messages, FortiOS Carrier, 200
logging of events, 165
peer user groups, 90
peer users, 77
RADIUS, 180
user groups, 87
adding, configuring defining
authentication settings, 27
carrier end point MMS filter list, 202
Directory Service user groups, 32
firewall user groups, 31
FortiToken, 40
FSSO, 43
LDAP server, 36
SSL VPN user groups, 32
TACACS+ server, 39
user authentication settings, 27
user groups, 28
Address Translation, 197
advanced mode (FSSO), nested groups, 141
ASCII, 65
attributes, RADIUS, 52
authenticating users
FortiGate, local, 73
with LDAP servers, 74
with RADIUS servers, 74
with TACACS+ servers, 74
authentication
certificate-based, 96
configuring access, 93
defining settings, 27
disclaimer, 101
firewall policy, 96, 100
guest users, 165
IPsec VPN, 108
L2TP, 21, 111
overview, 114
PPTP, 21, 110
protocols, 96
replacement messages, 98
SSL VPN, 108
SSL VPN timeout, 108
timeout, 93
two-factor, 40
VPN, 107
VPN client-based, 22
web-based user, 21
XAuth, 109
authentication protocols, 97
ASCII, 65
CHAP, 65
MS-CHAP, 65
PAP, 65
setting, 96
TACACS+ servers, 65
authentication servers
Directory Service, 66
LDAP, 56
RADIUS, 51
TACACS+, 65
B
backup password, 62
banned users
cause or rule, 85
billing, 197
binding
LDAP servers, 57
customer communication session, 177, 191
customer identifying information, 177

certificates
import, 124
importing CRL, 120
OSCP, 115
root CA, installing, 120
self-signed, 114
signed server, installing, 119
Single Sign On (SSO), 113
dynamic profile, 175, 182
assigning profile groups, 16
carrier end point, 191
configuring the accounting system, 180
event log messages, 200
log message period, 201
log settings, 200
profile group, 179
RADIUS, 16
RADIUS Stop record, 180
timeout options, 199
user context list, 180
Users Only, 181
VDOMs, 182
WAP traffic, 177

eDirectory, 66, 134
servers, 157
eDirectory - see Directory Service
elements, distinguished names, 58
email token, 78
directory
LDAP servers, 57
Directory Service
servers, 66
user groups, 90
disclaimer
customized, 102
default, 102
distinguished names
elements, 58
LDAP servers, 58
list of, 60
max size, 59
domain component, LDAP servers, 57
Domain Name Identifier (DNI), 159
dynamic profile
assigning profile groups, 16
carrier end point, 191
configuring the accounting system, 180
event log messages, 200
log message period, 201
log settings, 200
profile group, 179
RADIUS, 16
RADIUS Stop record, 180
timeout options, 199
user context list, 180
Users Only, 181
VDOMs, 182
WAP traffic, 177

certificates
import, 124
importing CRL, 120
OSCP, 115
root CA, installing, 120
self-signed, 114
signed server, installing, 119
Single Sign On (SSO), 113
dynamic profile, 175, 182
assigning profile groups, 16
carrier end point, 191
configuring the accounting system, 180
event log messages, 200
log message period, 201
log settings, 200
profile group, 179
RADIUS, 16
RADIUS Stop record, 180
timeout options, 199
user context list, 180
Users Only, 181
VDOMs, 182
WAP traffic, 177

certificates
import, 124
importing CRL, 120
OSCP, 115
root CA, installing, 120
self-signed, 114
signed server, installing, 119
Single Sign On (SSO), 113
dynamic profile, 175, 182
assigning profile groups, 16
carrier end point, 191
configuring the accounting system, 180
event log messages, 200
log message period, 201
log settings, 200
profile group, 179
RADIUS, 16
RADIUS Stop record, 180
timeout options, 199
user context list, 180
Users Only, 181
VDOMs, 182
WAP traffic, 177

eDirectory, 66, 134
servers, 157
eDirectory - see Directory Service
elements, distinguished names, 58
email token, 78
directory
LDAP servers, 57
Directory Service
servers, 66
user groups, 90
disclaimer
customized, 102
default, 102
distinguished names
elements, 58
LDAP servers, 58
list of, 60
max size, 59
domain component, LDAP servers, 57
Domain Name Identifier (DNI), 159
dynamic profile, 175, 182
assigning profile groups, 16
carrier end point, 191
configuring the accounting system, 180
event log messages, 200
log message period, 201
log settings, 200
profile group, 179
RADIUS, 16
RADIUS Stop record, 180
timeout options, 199
user context list, 180
Users Only, 181
VDOMs, 182
WAP traffic, 177

eDirectory, 66, 134
servers, 157
eDirectory - see Directory Service
elements, distinguished names, 58
email token, 78
directory
LDAP servers, 57
Directory Service
servers, 66
user groups, 90
disclaimer
customized, 102
default, 102
distinguished names
elements, 58
LDAP servers, 58
list of, 60
max size, 59
domain component, LDAP servers, 57
Domain Name Identifier (DNI), 159
dynamic profile, 175, 182
assigning profile groups, 16
carrier end point, 191
configuring the accounting system, 180
event log messages, 200
log message period, 201
log settings, 200
profile group, 179
RADIUS, 16
RADIUS Stop record, 180
timeout options, 199
user context list, 180
Users Only, 181
VDOMs, 182
WAP traffic, 177

Extended Authentication (XAuth), 70

F
failed authentication attempts, 95
filter
carrier end point, 192, 202
carrier end point MMS filtering, 192, 202
filter list
carrier end point, 202
IP, 180
FireFox, 106
firewall
configuring user groups, 87
creating user groups, 87
identity based policy, 189
IPsec VPN dialup user access, 86
policy authentication, 96, 100
user authentication timeout, 93
user groups, 86
firewall policy
user groups, 31
firewall policy and strong authentication, 126
FortiClient Endpoint Security peer, 20
FortiGate
authenticating users, 73
authenticating with XAuth, 109
configuring to use LDAP, 59
configuring to use RADIUS, 54
IPsec VPN, 108
FortiGate LDAP configuration, 157
FortiGuard
Antispam, 13
Antivirus, 13
Fortinet Server Authentication Extension (FSAE), 19, 100, 133
Fortinet Single Sign On (FSSO), 133
Fortinet Single Sign On Agent (FSSO), 43
FortiOS 3.0 MR7, 153
FortiOS Carrier, 191
FortiToken, 40, 80
framed-ip-addr
RADIUS field, 185
FSAE 4.0 MR1, 138
FSAE version 3.5.27, 153
FSSO
components, 140
DC Agent mode, 135
DNI, 159
DNI field, 170
guest, 158, 165
identity-based policy, 162
LDAP, 161
logoff detection, 152
Mac OS, 136
nested groups, 141
Polling Mode, 137
Polling mode, 135
supported operating systems, 134, 140
TCP port 8000, 160
trust relation, 138
FSSO agent
FortiGate configuration, 160
FSSO_Guest_Users, 171
FSSO_Guest_Users group, 165
G
group filters
FortiGate, on collector agent, 151
groups
user, 28
Windows AD, viewing on FortiGate, 161
guest account, 158, 165
H
hierarchy
LDAP servers, 57
, 172
HTTP header, 177, 191, 198
HTTP Header Field, 197
HTTP-User-Agent, 106
I
Identity based policies (IBP), 18, 189
Identity based policy (IBP), 105
identity-based policy, 162
Local ID, 20
NTLM guest, 105
NTLM user agent strings, 106
Idle timeout
VPN connection, 22
Ignore User List, 150
Internet Service Provider (ISP), 100
interval
log message, 201
IP address range
setting for L2TP VPN, 111
setting for PPTP VPN, 110
setting for SSL VPN, 108
IP filter
carrier end point, 194, 195, 203, 204
IP filter list, 180
IPsec
server type, 110
IPsec VPN
configuring authentication for, 108
dialup users, access to, 86
dialup users, configuring authentication for, 108
peer, 115
L
L2TP, 21
VPN, configuring authentication for, 111
LDAP, 156
access, collector agent, 149
configuring server, 36
fnbamd, 64
wildcard admin, 62
LDAP servers, 56, 157
  authenticating users with, 74
  binding, 57
  common name, 58
  configuring FortiGate unit to use, 59
  directory, 57
  Distinguished Name Query list, 60
  distinguished names, 58
  domain component, 57
  hierarchy, 57
  protocols, 57
  RFC compliance, 57
Lightweight Directory Access Protocol (LDAP), 133
  FortiGate configuring, 158
  XAuth authentication with, 109
Linux, 128
Local certificates
  generating request, 117, 127
  installing signed, 119
local user, 23
local users
  configuring, 74
  creating, 74
  deleting from FortiGate configuration, 76
  removing from FortiGate configuration, 76
log file, 156
log message
  grouping, 201
  interval, 201
logging
  dynamic profile, 200
  logging in, security messages, 114
  logon blackout period, 95
  logon events
    logging to memory, 150
M
Mac OS, 128, 136
management VDOM, 180
MicroSoft Challenge-Handshake Authentication Protocol v1 (MSCHAP), 65
MM1 message blocking MMS filter list, 192, 202
MM4, 192, 202
MM7, 192, 202
MMS Address Translation, 197
MMS filter list
  adding to an MMS protection profile, 192, 202
MMS message
  blocking using carrier end point MMS filtering, 192, 202
  mobile service provider, 176
  mode, operation, 13
Mozilla, 106
MS Windows Active Directory (AD), 19, 105
MS-CHAP, 65
MSIE, 106
MSISDN. See also carrier end point, 177
  multiple account sessions, limits, 107
  multiple group enforcement, 88
N
Network Access Server (NAS), 53, 54
non-dynamic profile sessions, 181
Novell eDirectory, 134
Novell eDirectory - see Directory Service
NT LAN Manager (NTLM), 19, 105, 134
NTLM, 100
  authentication, 142
  Guest profile access, 105
  HTTP-User-Agent, 106
  NTLM mode, 137
  user agent strings, 106
  XSS vulnerability, 106
NTLM enabled browsers, 106
NTLM statistics, 154
NT-style domain mode implementation, 136
O
one time passcode (OTP), 18, 66, 80
Online Certificate Status Protocol (OCSP), 115, 116
OpenLDAP, 56
OpenSSL, 116
Opera, 106
  operation mode, 13
P
PAP, 65, 110
password
  administrator, 13
Password Authentication Protocol (PAP), 65
  pattern
    carrier end point, 192, 193, 195, 202, 203
peer user groups
  configuring, 90
  creating, 90
peer users, 73, 77
  configuring, 77
  creating, 77
Perl regular expression
  carrier end point pattern, 192, 202
Perl regular expressions
  carrier end point pattern, 195
PKI, 45
PKI authentication - see peer users
PKI certificate
  PKCS, 119
PKI user, 77
Polling mode, 137, 154
polling mode
  event log polling, 136
  NetAPI polling, 137
port 10443, 86
port 445, 136
port 8000, 156
port, RADIUS servers, 55
PPTP, 21
PPTP PPTP VPN
  configuring authentication for, 110
Index

PPTP VPN
- IP address range, 110
- preshared key, 20
- profile group
  - assigning dynamically, 16
  - dynamic profile, 16
- profile group, dynamic profile, 182
- profile, dynamic, 175
- protocols
  - authentication, 96
  - LDAP servers, 57
- public key cryptography standard (PKCS), 117
- public key infrastructure (PKI), 113

Q
- Query list
  - LDAP Distinguished Name, 60

R
- RADIUS
  - accounting system, 180
  - attributes, 52
  - authentication servers, 51
  - dynamic profile, 16
  - End record, 175
  - framed-ip-addr field, 185
  - long key, 52
  - server port, 188
  - servers, 34
  - Start record, 16, 175, 177, 191
  - Stop record, 180
  - vendor ID, 53
  - viewing server list, 34
  - XAuth authentication with, 109
- RADIUS servers
  - attribute dictionary, 53
  - authenticating users with, 74
  - changing default port, 55
  - configuring FortiGate unit to use, 54
  - default port, 55
  - port, 55
  - VSA, 53
- registry
  - key, 153
  - remote service, 169
- Release Notes, 134
- remote administrator, 62
- remote user authentication, 33
- removing
  - local users from FortiGate configuration, 76
  - user group from FortiGate configuration, 91
- replacement messages
  - authentication, 98
  - RSA
  - SecurID, 98
- revocation list, importing, 120
- RFC 2865, 33
- RFC 2866, 33
- RFC 2986, 117
- RFC 5280, 113
- RFC compliance
  - LDAP servers, 57
  - Role Based Access Control (RBAC), 54, 86, 103, 183
  - root certificate, installing, 120
  - RSA, 66
  - X.509, 20
  - RSA SecurID, 98

S
- Secure Certificate Enrollment Protocol (SCEP), 115
- secure HTTP (HTTPS), 114
  - firewall policy, 69
  - self-signed certificate, 114
  - self-validate, 116
  - Sender Address Identifier, 199
  - server certificate
    - installing signed, 119
    - obtaining, 119
  - servers
    - configuring XAuth authentication using, 109
  - session hijacking, 125
  - session timeout, 90
- setting
  - authentication protocols, 96
  - firewall policy authentication, 96
  - firewall user authentication timeout, 93
  - SSL VPN authentication timeout, 93, 108
  - shared secret, 20
  - Single Sign On (SSO), 113
  - Single user Sign On (SSO), 134
  - SMS token, 79
  - SQL, 52
  - SSL, 114
  - SSL Client Certificate Restrictive option, 126
  - SSL VPN
    - authentication timeout, 93, 108
    - Subsession, 209
    - user authentication, 108
    - user groups, configuring, 86
    - user groups, IPsec VPN dialup users, 86
    - user groups, creating, 86
  - SSL VPN user groups, 86
  - strong authentication, 125
    - for administrators, 125
    - for SSL VPN users, 125

T
- TACACS+
  - configuring server, 39
TACACS+ servers, 65
  ASCII, 65
  authenticating users with, 74
  authentication protocols, 65
  changing default port, 65
  CHAP, 65
  default port, 65
  max number, 65
  MS-CHAP, 65
  PAP, 65
  port, 65
  TCP port, 156
  TCP port 49, 65
  TCP ports
    for collector agent, 152
  Terminal Access Controller Access-Control System (TACACS+), 65
  timeout
    dynamic profile, 199
    session, 90
    user context creation, 200
    user context entry, 200
    user group, 88
  Traffic shaper, FSAE
    minimum bandwidth, 136, 141
  tunnel mode
    SSL VPN IP range, 108
  two-factor authentication, 18, 40, 78
    email, 78
    FortiToken, 80
    SMS, 79
  types of user groups, 85
  types of users, 73

U
  user authentication
    IPsec VPN dialup users, 108
    L2TP VPN, 111
    logon blackout period, 95
    PKI, 45
    PPTP VPN, 110
    protocols, 96
    remote, 33
    SSL VPN, 108
    timeout, 93
    XAuth, 109
  User Context Creation Timeout, 182
  user context list, 180
    carrier end point, 180
    dynamic profile, 180
    timeout for removing entries, 200
    user context creation timeout, 200
    user context entry timeout, 200
    waiting for new entries, 200
  user groups, 85
    configuring, 28
    creating, 87
    Directory Service, 32, 90
    firewall, 31, 86
    on authentication servers, 87
    on FortiGate unit, 162
    peer, configuring, 90
    peer, creating, 90
    SSL VPN, 32
    types of, 85
    Windows AD, 145
  user IP address, 153
  user logoff
    ports 139 and 445, 152
  usergroup timeouts, 88
  username overlap, 86
  Users, 97
  users, 73
    banned, 85
    local, creating, 74
    local, deleting from FortiGate configuration, 76
    local, removing from FortiGate configuration, 76
    peer, configuring, 77
    peer, creating, 77
    types of, 73

V
  VDOM
    management, 180
  Vendor specific attributes (VSA), 53
  viewing
    carrier end point IP filter list, 195, 204
    LDAP server list, 36
    RADIUS server list, 34
    TACACS+ server, 39
  virtual domains (VDOMs), 180
  VPN
    authentication, 107
    client-based authentication, 22
    idle timeout, 22
    IPsec, 108
    L2TP, 111
    PPTP, 110
    SSL, 108
  VSA
    dictionary, 53
    RADIUS servers, 53

W
  WAP traffic, 177
    dynamic profile, 177
  web-based user authentication, 21
  wildcard
    carrier end point pattern, 192, 195, 202
  wildcard admin configuration, 62
  Windows 2008, 52
  Windows Active Directory (AD), 42
    forest, 138
    trust relation, 138
Index

Workstation verify interval
  collector agent configuration, 148

X

X.509, 113, 125
  managing security certificates, 116
  server certificate, 114

XAUTH, 107
  configuring authentication with, 109
  XSS vulnerability characters, 106
  x-up-calling-line-id, 198