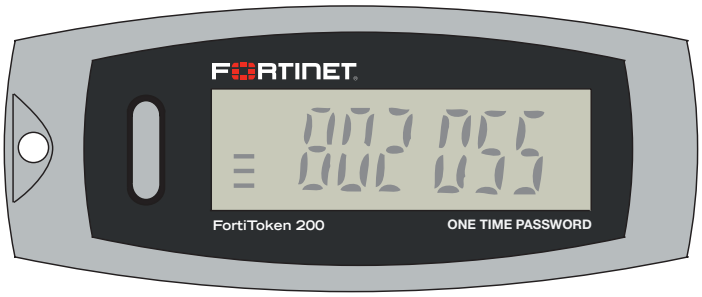
FortiToken-200

FortiToken-200 is a small hardware token generator that fits on a key-chain. Simply press the button and the FortiToken-200 generates and displays a secure one-time password (OTP) that you enter along with your regular password for secure authentication and access to critical applications and sensitive data.

The time remaining is shown on a bar graph in 10-second increments. After the 60 seconds is up, the password expires and the FortiToken display turns off.



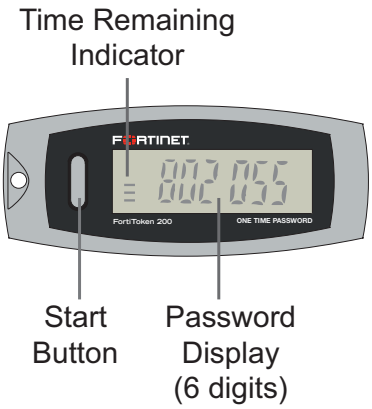
Step 1. Unpacking

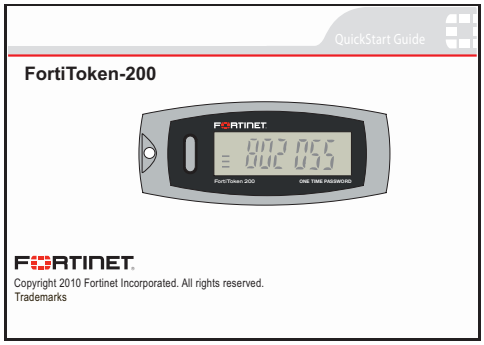
Open the shipping carton and carefully unpack its contents. The carton should contain the following items:

- FortiToken-200 units
- FortiToken-200 QuickStart Guide (QSG)

If any item is found missing or damaged, please contact your local reseller for replacement.

Package Contents:





Step 2. Activating the FortiToken unit

Before you can successfully use the FortiToken-200 token generator, it must be activated on the FortiGate system. The following requirements must be met before you can do this:

- The FortiGate unit system time must be configured to synchronize with a Network Time Protocol (NTP) server.
- The FortiGate unit must be able to access the FortiGuard Distribution Network (FDN).

To activate one or more FortiToken units

1. Log in to the web-based manager of your FortiGate unit.
2. Go to *User* > *FortiToken* > *FortiToken.* Select *Create New.* Then add the serial numbers for each FortiToken unit you have and select *OK*.
3. Each FortiToken unit will automatically activate. The *Status* field will indicate *Activating*. Select *Refresh*, and you should see the *Status* field changed to *Active*.
4. Select the check box for the activated FortiToken unit, then on the toolbar select *Synchronization*. The Synchronize FortiToken dialog box appears.
5. Press the *Start* button of your FortiToken unit and enter the 6-digit token password in the *First Code* field. Wait until the FortiToken time expires, then press the *Start* button again to generate a second password and enter it into the *Next Code* field. Select *OK*.

Step 3. Assigning FortiTokens to Users

To use token authentication, a user account must be enabled to use two-factor authentication and must be assigned the serial number of an activated FortiToken device. The device serial number cannot be shared by multiple users.

To assign a FortiToken unit to a user

1. Do one of the following:

- To assign a FortiToken to an administrator (super-users only), go to *System* > *Admin* > *Administrator* and select the check box for the administrator account you want to configure, then select *Edit* from the toolbar.
- To assign a FortiToken to a regular user, go to *User* > *User* > *User* and select the check box for the user account you want to configure, then select *Edit* from the toolbar.

2. In the dialog box, select the *Enable Two-factor Authentication* check box. Under *Deliver Token Code by,* select the *FortiToken* option and then select the FortiToken serial number you want to assign to the selected user account. Select *OK*.

Step 4. Logging In with FortiToken

After they have been activated and assigned to users, the FortiToken units can be used to log in securely to your network through the SSL-VPN client, the standalone FortiClient SSL-VPN tunnel client, the FortiClient console, or the FortiGate Web-based Manager. This section explains the login procedure for each method.

To log in using the SSL-VPN Client

1. In the SSL-VPN web login page, enter your user name and password and select *Sign In.* The login page refreshes and the *FortiToken Code* field appears.
2. Press the *Start* button of your FortiToken unit, type the generated token password into the *FortiToken Code* field on the login page and then select *Login*. You must do this within the 60 seconds while the token password is still valid.

To log in using the standalone FortiClient SSL-VPN tunnel client

1. Go to *Start* > *All Programs* > *FortiClient* > *FortiClient SSL-VPN.*
2. In the FortiClient SSL-VPN client, select the *Connection Name* from the list.
3. Enter your user name, then press the *Start* button of your FortiToken unit.
4. In the *Password* field, type your password concatenated with the generated token password. For example, if your password is `password` and your token code is 123456, you would enter `password123456`.
5. Select *Connect* to initiate the connection. You must do this within 60 seconds while the token password is still valid.

To log in using the FortiClient console (IPsec VPN)

1. In the FortiClient console, go to *VPN* > *Connections, s*elect the connection you want to start and select *Connect*.
2. In the VPN Login dialog box, enter your user name and password and select *OK.* The login page refreshes and the *FortiToken Code* field appears.
3. Press the *Start* button of your FortiToken unit, type the generated token password into the *FortiToken Code* field and select *OK*. You must do this within 60 seconds while the token password is still valid.

To log in using the FortiGate Captive Web Portal (Firewall Identity Check)

1. Connect to the captive web portal.
2. In the Authentication Required dialog box, enter your user name and password. Then select *Continue.* The FortiToken Required dialog box appears.
3. Press the *Start* button of your FortiToken unit, type the generated token password into the *Token Code* field and select *Continue*. You must do this within 60 seconds while the token password is still valid.

To log in using the FortiGate Web-based Manager (super-user administrators only)

1. In your web-browser, enter the URL (using https) of the FortiGate unit you want to access.
2. In the Login dialog box, enter your user name and password and then select *Login*. The login page refreshes and the *Token Code* field appears.
3. Press the *Start* button of your FortiToken unit, type the generated token password into the *Token Code* field and select *Login*. You must do this within 60 seconds while the token password is still valid.

Regulatory Compliance: FCC Class A Part 15, / CE Mark

July 24 2012
01-430-135980-20120724

Visit these links for more information and documentation for your Fortinet product:

- **Technical Documentation:** http://docs.fortinet.com
- **Knowledge Base**: http://kb.fortinet.com
- **Technical Support:** https://support.fortinet.com
- **Training Services:** http://training.fortinet.com