FortiToken Two Factor Authentication
Solutions Guide

Solutions Guide

November 16, 2012

33-100-188900-20121116

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Introduction

This guide covers various usage and deployment scenarios for Fortinet's range of two-factor authentication solutions.

Motivation for strong authentication

Virtually all enterprise organizations do business online and keep sensitive date on networks accessible from end-user devices. However, as witnessed by the many publicized breaches that have occurred in the recent past, not all enterprises have been successful in protecting against such attacks.

Remote access to network resources, including VPNs and web sites, are often protected only with simple user name and password credentials. This allows a determined hacker to gain access to these resources relatively easily. Further, weak internal security renders both wired and wireless LANs vulnerable as we are seeing more attacks from within the perimeter.

These trends have given rise to increasing mandates all around the world to comply with security standards for assurance of networks, applications and data. The common denominator for securing user authentication is the addition of a second factor for validation of the user's identity; hence the term "two factor authentication" (2FA). Generally, in 2FA, the first factor is something you know, for example, your password. Typically, the second factor is something you have. That something is the security token.

Overview of two-factor authentication

A security token is used as part of a system to prove one's identity electronically as a prerequisite for accessing network resources. There are many types of hardware and software based tokens, sometimes referred to as dongles, key fobs, authentication tokens, USB tokens and cryptographic tokens. The use of a security token as the second factor by the end-user solves the problems of using only static passwords.

Token authentication solutions all require a client and server component. The client component is the Security Token itself; the server component is the Authentication Server (also called Validation Server). The two components share secret keys that are related to each other and used to independently perform cryptographic operations such that the outputs can be compared for validation purposes.

Most enterprises contain diverse user communities with respect to their behaviors, risks and technical knowledge. Therefore, enterprises need strong authentication solutions that are flexible enough to secure online resources across a wide spectrum of environments. Your choice of solution can mean the difference between economically providing adequately high security tools that can be easily adopted by your users, and paying too much for a solution that leaves security holes and is too hard to use.

Fortinet authentication server and token types

Fortinet's 2FA solutions are cost-effective, highly secure and easy to administer and use. Our solutions help organizations comply with SOX, PCI, HIPPA and other regulatory requirements that implicitly or explicitly require two-factor authentication. Organizations can chose the specific type of security solution depending on the risk associated with various types of transactions, and budgetary constraints, while providing reliable evidence of all network related user and administrative activities required for passing compliance audits.

Fortinet security tokens, known as FortiToken, come in a variety of form factors and platforms. Specifically, the FortiToken product line includes:

- **FortiToken-200** - Hardware device capable of generating time-based One Time Password values required on the client side. The token has neither a physical nor logical connection to the client computer. It has a display to visually show the generated OTP authentication codes, which the user then enters manually along with login id and password via a keyboard or keypad.
- **FortiToken-200CD** - This is the same type of token as the FortiToken-200 but differs in the method of server-side activation.
- **FortiToken Mobile** - Software implementation of the FortiToken-200 that can be installed on a Smartphone.
- **FortiToken-300** - USB hardware device that must be physically connected to the client computer to use for client certificate based authentication. It requires software to be installed on the host computer.

All of the above listed tokens can be used for two-factor authentication. The FortiToken-300 can also be used for other security purposes by virtue of its PKI certificate functionality (e.g., encryption and signing).

FortiToken is the client side equipment for strong authentication solution. There is also a requirement to deploy an authentication server on the back end. Here, Fortinet offers two product options for authentication server: FortiGate and FortiAuthenticator.

FortiGate

The FortiGate unit is generally specified as the authentication server in the case where a single FortiGate unit is deployed for VPN. This would be for relatively small installations. The big advantage of using a FortiGate unit is that the Authentication Sever functionality is built-in; there is no additional hardware or software to purchase resulting in significant cost saving. Tokens are specific to each instance of the FortiGate unit. The FortiGate unit authentication also allows the integration with existing AD/LDAP directory servers.

FortiAuthenticator

FortiAuthenticator is generally specified as the authentication server in the case where multiple FortiGate units and other Radius client/NAS devices are deployed. FortiAuthenticator is a full function stand-alone RADIUS Authentication server. Tokens can be used for any VPN/Firewall/NAS RADIUS Client. FortiAuthenticator also includes native LDAP server functionality as well as the ability to integrate with external LDAP directories. Further, the REST API of FortiAuthenticator makes it possible to add two factor authentication to your non-RADIUS based web applications. Finally, FortiAuthenticator has a user self service portal that can minimize touch points in the provisioning process as well as Help Desk calls.

FortiToken solutions

Fortinet's strong authentication servers and clients provide strong, two-factor authentication for remote users on laptops, browsers, tablets and Smartphones solutions that are secure, easy and affordable.

Fortinet offers a variety of security tokens in the FortiToken product line in addition to a choice of Authentication Server platforms. They can be used to securely authenticate to a PC, Server, network, application or website. FortiToken solutions can be deployed for a single purpose, such as remote VPN access. A single token can also be used for multiple purposes, for example, LAN login and VPN login.

Fortinet solutions are standards based and will minimize IT labor and cost-of-ownership through simple installation, tokens that don't expire, end-user self-service, and out-of-the-box integration into your existing network infrastructure. They supports a flexible range of two-factor OATH compliant, time-based, OTP hardware tokens, soft tokens for mobile devices, SMS and email options and client certificates.

The benefits of Fortinet strong authentication for the enterprise include:

- Mitigating risk of weak, static password authentication, which is shown to lead to breaches, malware attacks, and policy violations.
- Low (zero) cost two-factor authentication options
- Increasing productivity with secure connections to data and applications from any location through a variety of devices and authentication methods to suit the enterprise and their users.
- Ensuring compliance with regulatory standards
- Lowering costs associated with equipment, compliance, help desk calls, implementation, administration, and forced token replacement.

Trusted by large and small businesses, governments, law enforcement and banks around the world, Fortinet, with its strong authentication solutions for remote access, will provide the security you need for your organization.

The table below shows the possible combinations of Fortinet Authentication Servers and Tokens that can be used to solve your two-factor authentication problem. Your specific criteria will dictate the optimal choice for your environment.

Table 1: Combinations of Fortinet authentication servers and tokens for two-factor authentication

Authentication Server	Token (Client)	Certificate Authority
FortiGate	FortiToken-200/FortiToken Mobile	N/A
FortiGate	FortiToken-200CD/FortiToken Mobile	N/A
FortiAuthenticator	FortiToken-200/FortiToken Mobile	N/A
FortiAuthenticator	FortiToken-200CD/FortiToken Mobile	N/A
FortiGate or Third Party	FortiToken-300	FortiAuthenticator

The determination of the solution footprints above is based on the fact that FortiGate has a built-in authentication server function that comes standard with every FortiOS device and virtual

machine and FortiAuthenticator is an external authentication server. The authentication server for PKI certificate based solutions using FortiToken-300 depends on the application. For example, FortiGate VPN access would require FortiGate unit as the authentication server, whereas Windows smartcard login would require Windows server to perform the authentication.

Candidate applications for two-factor authentication

The table below shows a list of typical applications that should be secured using two-factor authentication and indicates if an external Authentication Server is required to do so.

Table 2: Deployment context for various applications using two-factor authentication

Applications Using Built-In FortiGate Authentication Server (note: these can also be configured to use an external authentication server)	**Network Access Servers (NAS), Applications Requiring External RADIUS Authentication Server (FortiAuthenticator)**		**Applications Requiring External Authentication Server (FortiAuthenticator) with Authentication API**	**Certificate Based Applications Not Requiring External Authentication Server**
	Fortinet device and apps	Third party VPN (RADIUS clients)		
FortiGate SSL VPN	FortiManager Admin login	Cisco IOS based switches and routers	Web sites	VPN
FortiGate IPsec VPN	FortiMail Admin login	Cisco ASA	Homegrown networked applications	Windows Smartcard login
FortiGate Captive Portal	FortiWeb Admin login	Citrix Access Gateway		Microsoft Outlook web application
FortiGate Admin login		Linux server with PAM module		
FortiDNS Admin login		Apache with mod-auth-radius module		

FortiToken Solutions Criteria

Attack vectors are rising exponentially, with trends like BYOD and more endpoints of all types connected to the network. Strong authentication inside and outside the perimeter is absolutely essential as part of a layered security best practice. But you need to work within your financial and technical resource constraints to deploy an effective solution that takes into account operational fit, administration, ease-of-use and budget.

Some of the differentiating variables in the customer's environment affecting the choice of FortiToken strong authentication solution are:

- **Size of end-user population**: In general, if you have many end users that will be assigned tokens, you will want to centralize the token management in FortiAuthenticator. Both the FortiGate unit and FortiAuthenticator allow integration with existing AD/LDAP directories
- **Number of FortiGate units that need to authenticate users**: If your network consists of only FortiGate units and all you want is secure remote VPN access, you may want to use the FortiGate as your authentication server.

- **Fortinet non-RADIUS devices, third Party RADIUS devices and other Non-RADIUS clients/applications that need to authenticate users**: FortiAuthenticator is required enabling two-factor authentication for non-FortiGate clients.
- **Regulatory Compliance**: Industry regulations will require you to comply with best practices for protecting access to resources and often specify two-factor authentication.
- **BYOD Policy**: If your policy allows end-users Smartphones for business applications, whether company issued or BYOD, you may consider using the FortiToken Mobile as an alternative to hard tokens.
- **Multiple tokens per end users**: If you want to assign separate tokens for access to various systems, you don't want to require your end-users to carry additional hardware. Mobile apps, such as FortiToken Mobile, allow users to install multiple tokens on the same device.

FortiToken deployment scenarios

This section describes FortiToken solution alternatives relative to the variables in the customer's environment. Table 2 below shows the FortiToken solution for various characteristics of the customer environment in which it will be deployed.

Table 3: Solution footprint deployment criteria

Deployment Environment Attribute	**Fortinet Solution Footprint**				
	FortiGate		**FortiAuthenticator**		
	FortiGate plus FortiToken-200 and/or FortiToken Mobile	FortiGate plus FortiToken-200CD and/or FortiToken Mobile	FortiAuthenticator plus FortiToken-200 and/or FortiToken Mobile	FortiAuthenticator plus FortiToken-200 and/or FortiToken Mobile	FortiToken-300 plus FortiAuthenticator (CA)
Size of end user population	Small	Small, Medium	Large	medium, Large	Any
Number of FortiGate devices (or HA clusters) that need to authenticate users	One	Few	Any	Any	Any
Need to authenticate users to third party devices, applications and/or web sites	No	No	Yes	Yes	Yes
Regulatory compliance required	Yes	Yes	Yes	Yes	Yes
BYOD polices	Allowed (for FortiToken Mobile	Allowed (for FortiToken Mobile	Allowed (for FortiToken Mobile	Allowed (for FortiToken Mobile	N/A
All or some users require multiple credentials/tokens	Yes (with FortiToken Mobile)	Yes (with FortiToken Mobile)	Yes (with FortiToken Mobile)	Yes (with FortiToken Mobile)	Yes

The remainder of this section provides more detailed context for each of the types of FortiToken solutions.

FortiGate authentication server with FortiToken-200 and/or FortiToken Mobile

The simplest, most cost-effective solution for securing FortiGate VPN (SSL or IPSec) access is to use the FortiGate unit as the authentication Server. Because the FortiGate unit is used as the VPN Server as well as the authentication server, there is no need to deploy FortiAuthenticator or any other external authentication server in the solution. The end users can all be provisioned with hard tokens. If BYOD policy allows end users to use their own Smartphones, or if the organization issues Smartphones, they can be provisioned with FortiToken Mobile tokens. FortiToken Mobile tokens also enable users to carry multiple tokens all on the same device.

This solution has tremendous advantage from an administrative and cost perspective if you have only a single FortiGate cluster that you are using to authenticate VPN users. There is no need to deploy another hardware or virtual appliance to perform and manage authentication. The whole operation is already centralized in your FortiGate unit, with no additional licensing or support costs.

Not only can FortiToken be used to secure administrative access to the FortiGate unit, it also can be used to enable two-factor authentication for FortiGate IPSec VPN, SSL VPN and captive portal users, thereby increasing the ROI even further.

For security reasons, it is generally not recommended to install the same FortiToken-200 tokens on multiple FortiGate units. Therefore, by default FortiToken-200 can only be activated once online via the FortiGuard hosted token activation server.

Figure 1: FortiToken Authentication with FortiGate

FortiGate authentication server with FortiToken-200CD and/or FortiToken Mobile

Although Fortinet recommends the use of FortiAuthenticator to centralize the management of the tokens and eliminate the administrative overhead of tending to tokens across multiple FortiGate units, there are cases where FortiAuthenticator is not practical or necessary. This could be because of capital expense budget limitations. Or it could be the case that you are an MSSP and you want your staff members to have one hard token to use to get administrative access to all the FortiGate units used to provide security services to your clients. In this case, it might make sense to use this solution so you can install the same token but with a different user id across multiple FortiGate units.

If you want to install the same instance of FortiToken on multiple FortiGate units or FortiGate HA clusters using the built-in FortiGate authentication server to authenticate users, then you should use the FortiToken-200CD tokens. However, care must be taken to make sure that the user and token configurations are consistent across the FortiGate units. If you are setting up so that a given user can use his/her token to authenticate on multiple FortiGate units, then you must make sure that changes made on one FortiGate with respect to token configuration are in sync and compatible with the other FortiGate devices.

The FortiToken-200 by default has a one-time activation limit via the secure Fortinet cloud-based seed server so that it can be activated and installed on only one FortiGate unit. However, because the FortiToken-200CD activation file is encrypted and in your control, you can securely activate the tokens repeatedly across multiple FortiGate devices without worry. Therefore, the FortiToken-200CD solution applies to environments where separate FortiGate units are deployed with no centralized authentication server, and users must have two-factor authentication access to each FortiGate unit. Another reason to use FortiToken-200CD is if you have any concern or network limitation that would prevent you from using Fortinet's FortiGuard to activate your tokens.

If your BYOD policy allows end users to use their own Smartphones, or if the organization issues Smartphones, they can be provisioned with FortiToken Mobile tokens. FortiToken Mobile tokens also enable users to carry multiple tokens all on the same device.

FortiAuthenticator with FortiToken-200 and/or FortiToken Mobile

FortiAuthenticator should be used as the centralized authentication server where there are multiple FortiGate units and/or other authentication clients. This includes heterogeneous environments consisting of multiple third party Network Access Servers (NAS), RADIUS-based VPN devices and applications, homegrown applications and web sites.

Any RADIUS-based client can be easily integrated with FortiAuthenticator, virtually out of the box. Nearly every VPN server available on the market supports RADIUS, including Cisco, Checkpoint, Juniper, SonicWall and Microsoft RRAS. Many other commercial products such as Citrix Access Gateway, Oracle and Microsoft IAS include RADIUS client functionality for simple integration with a RADIUS server such as FortiAuthenticator.

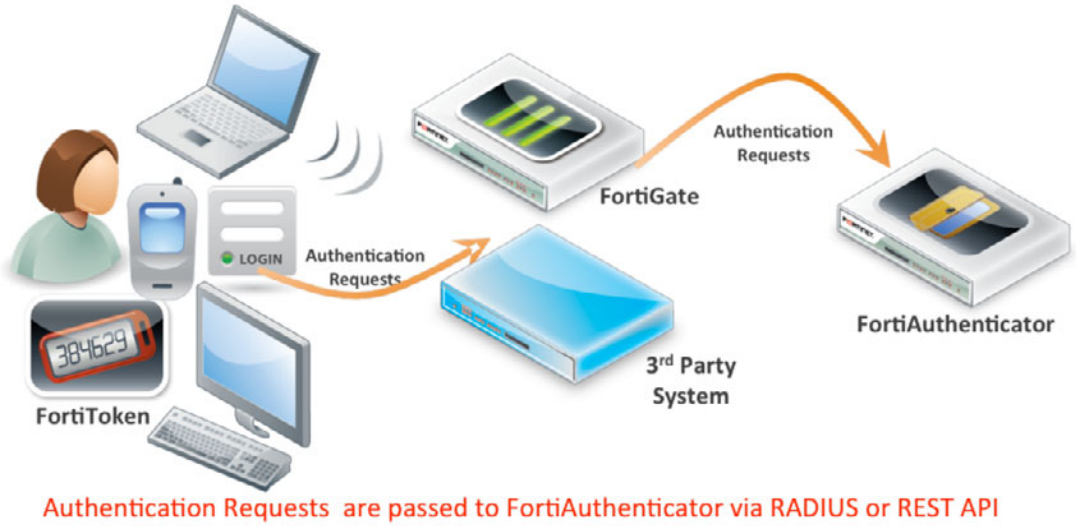
Non-RADIUS clients can also be easily integrated using the available Representational State Transfer (REST) API. Use this API to allow your applications to make authentication calls to FortiAuthenticator over the HTTPS protocol. This allows you to securely integrate any web-based or networked application into an authentication client of FortiAuthenticator.

For deployment environments involving a large number of end users who are going to be assigned tokens, FortiAuthenticator simplifies the management of the tokens as well as centralizes the validation function thereby eliminating the need to manually synchronize user data across multiple authentication servers.

FortiAuthenticator also offers an end-user portal for self-service registration and authentication management functions, such as password reset. You can further increase your return on investment (ROI) on FortiAuthenticator by using its native Certificate management, 802.1X Port Network Access Control, and FSSO support. These functions are included in the FortiAuthenticator at no additional licensing or support cost.

If your BYOD policy allows end users to use their own Smartphones, or if the organization issues Smartphones, they can be provisioned with FortiToken Mobile tokens. FortiToken Mobile tokens also enable users to carry multiple tokens all on the same device.

Figure 2: FortiToken Authentication with FortiAuthenticator



FortiAuthenticator with FortiToken 200CD and/or FortiToken Mobile

The criteria for using this solution footprint are the same as for the case above, except where there is a concern or policy against using a vendor that stores the token seeds in an online database. The FortiToken-200CD does not use an online seed store for activation; everything you need to install and activate the tokens is included in an encrypted file on a CD shipped in a tamper-evident package. The FortiToken Mobile activation is done dynamically through the Fortinet cloud and the seeds are deleted from the cloud as soon as they are installed on the end user's device.

If your BYOD policy allows end users to use their own Smartphones, or if the organization issues Smartphones, they can be provisioned with FortiToken Mobile tokens. FortiToken Mobile tokens also enable users to carry multiple tokens all on the same device.

FortiGate authentication server with FortiToken-300 and FortiAuthenticator Certificate Authority

The choice of PKI technology depends on the perceived threat on the resources you want to protect. Networks containing data that are bound to strict regulatory compliance, such as government entities, are the primary candidates for PKI-based two-factor authentication solutions.

For organizations that need to be absolutely sure of a user's identity, where the threat risk is quite high, when the damage from a security breach is great, or when the access credentials are shared between multiple applications (federated identity), PKI solutions make sense.

Fortinet's enterprise access solution is designed to help an organization's security and compliance objectives at a higher ROI by providing end users with a single, secure credential for remote access to networks and websites, as well as LAN access and login to a PC. This solution can also be used to digitally sign and encrypt email and documents, thereby further increasing ROI. For example, with a single token credential, an end user can be enabled for two-factor authentication access to corporate VPN, Windows domain login and Microsoft Outlook Web Access. Further the same token can be used to store user certificates for digital signing and encryption of documents and emails.

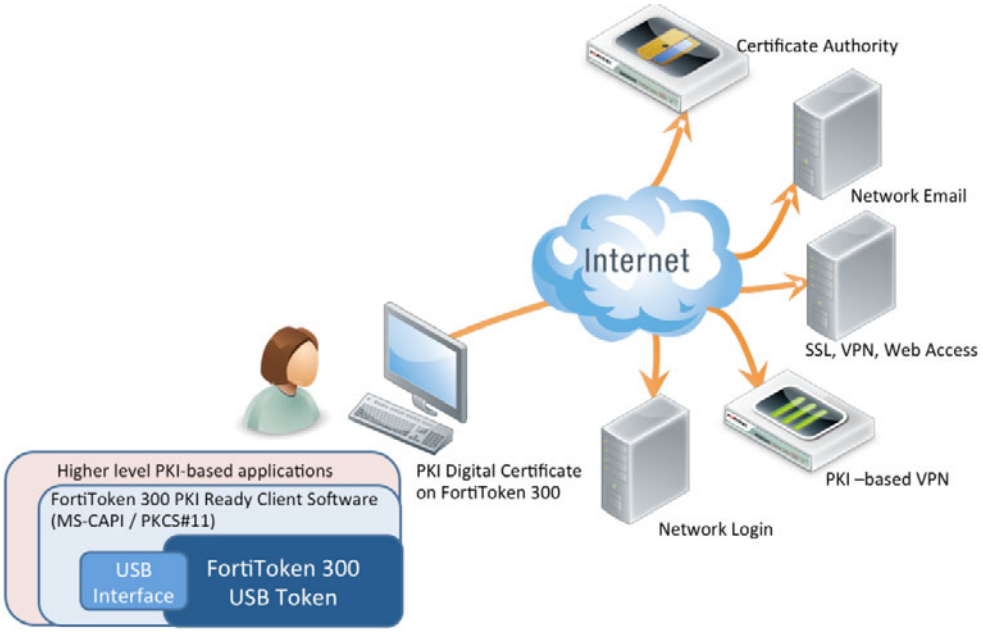
Many web-based applications are already PKI enabled, while other's support federated login that can be enabled for PKI certificates. USB Smartcards for PKI certificates can be used for stronger authentication into VPN, Windows desktops, laptops and servers. Besides the

advantage of effectively defending against insiders, USB Smartcards themselves are highly secure in that the private keys stored in the hardware cannot be exported or otherwise extracted.

PKI certificate deployment has traditionally been difficult and expensive. Fortinet makes it much easier and more cost-effective through the introduction of FortiAuthenticator, which can be used in conjunction with the FortiToken-300 USB Smartcard to deploy a simple, turnkey, single vendor solution that enables enterprises turn up a scalable PKI infrastructure and issue certificates to end users in short order. The benefits of the Fortinet PKI Smartcard solution are:

- Reduced risk of network attacks, compliance issues and financial liabilities with standards-based, “government” strong authentication
- Increased productivity and adoption with convenient and simple user experience
- Enhanced ROI with one universal client certificate for more efficient certificate management, and faster deployment of authenticating networks and apps.

Figure 3: Authentication with FortiToken-300



Summary

Two factor authentication is necessary today to protect your network. There are many choices in vendors and technologies to solve your two-factor authentication problem. Fortinet, the leader in network security, brings you a wide spectrum of choices in client and server components to tailor a solution for your unique needs. With solutions from zero cost server function to hardware and mobile tokens supporting third party systems, Fortinet has a solution to suit any requirement and budget.