ADMINISTRATOR GUIDE

wwGate^{TM}

Version 1.0

September 2013

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

This is the wwGate Administrator's Guide intended for system administrators, service provider application programmers, quality assurance professionals, and support personnel. This guide describes how to install/uninstall wwGate to provide end users with WWPass security services within a Single Sign-On (SSO) SAML framework. The concepts and principles and instructions described in this document provide the necessary information to successfully implement WWPass authentication features into your enterprise infrastructure. wwGate will require an administrator with admin privileges to install/monitor the application and ensure that a proper Microsoft® Active Directory® connection is maintained.

This document assumes that the reader has experience working in a Linux® shell environment.

The concepts, principles, and APIs described in this document provide the necessary information to successfully implement and interact with WWPass authentication features.

Licensing

License Agreement

Third-Party Licenses

This product may include software developed by parties other than WWPass. The text of the license agreements applicable to third-party software in this product may be viewed online at *wwpass.com*.

Supported Operating Systems

Currently, wwGate only uses the Ubuntu® Linux Operating System. Other Posix®-compliant Operating Systems are not supported but may also allow this product to work with little or no modification.

Customer Assistance

If you encounter a problem or have a question, you can contact the WWPass Service Desk as follows:

Phone	1-888-WWPASS0 (+1-888-997-2770)
Email	support@wwpass.com
Online	Support form

CHAPTER 1 — INTRODUCTION

Introducing wwGate

Modern sophisticated attacks of all sorts can compromise security and lead to loss of intellectual property, sensitive communication, or important customer data. wwGate 1.0 virtual appliance enables enterprises to collaborate and share resources with enhanced security, user experience, and IT control using the standards-based protocol Security Assertion Markup Language 2.0 (SAML 2.0). wwGate can handle all authentication requests made by internal and external clients/customers/workers for enterprise resources, and simplifies the burden of deployment and management costs by taking advantage of VMware® vSphere™ virtualization technology.

About the Security Assertion Markup Language

The Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging authentication and authorization information between parties, in particular, between an Identity Provider (IdP) and a Service Provider (SP). The SAML 1.0 specification standard was initially introduced by the Organization for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee in 2002. Since then, the SAML standard was updated with SAML v1.1 and SAML 2.0 in 2003 and 2005 respectively. The most common benefit of SAML 2.0 implementations to enterprise users is Web Single Sign-On. wwGate combines the benefits of Identity Provider initiated Web Single Sign-On with the WWPass strong cloud-based two-factor authentication.

wwGate Advantages

wwGate has the following advantages:

- Simplified installation and configuration of Identity Provider (IdP) services.
- Out of the box integration with existing Microsoft Active Directory infrastructure.
- Single Sign-On Services to cloud Services Providers like:
  - SalesForce.com®
  - Google Apps for Business™
  - Dropbox™ for Business
  - Juniper® Secure Access SSL VPN Series Appliance
- Develop and manage SAML metadata and attribute exchange policies.
- Two-factor authentication eliminating the need for username and password credentials.

The most common benefit of SAML 2.0 implementations to enterprise users is Web Single Sign-On. The wwGate combines the benefits of Identity Provider initiated Web Single Sign-On with the WWPass strong cloud-based two-factor authentication.

Functional Description

wwGate is a self-contained virtual appliance that can be incorporated into an enterprise environment to implement or extend the current enterprise security infrastructure. The virtual appliance described herein is enabled when a Service Provider receives a request to access a site or service that the provider wishes to protect from unauthorized access. Upon receiving the HTTP request, the virtual appliance, which contains a SAML-compliant server, accesses the WWPass module which then initiates a WWPass authentication transaction. As a result of the transaction, WWPass will return an authentication message to the Service Provider. After a successful authentication, the user is then validated against the enterprise's Microsoft Active Directory infrastructure using the userPrincipalName object. Upon successful validation from Active Directory, the user will then be granted access to the web site or service.

If the user is no longer valid in Active Directory or if permissions have been revoked, the user will be blocked from access to the web site or service. Once this initial authentication has been completed, the user can now access any other supported Service Provider without the need to provide account credentials but still retain a high level of security.

wwGate is a server module that can handle all authentication requests made by internal and external clients/customers/workers for enterprise resources.

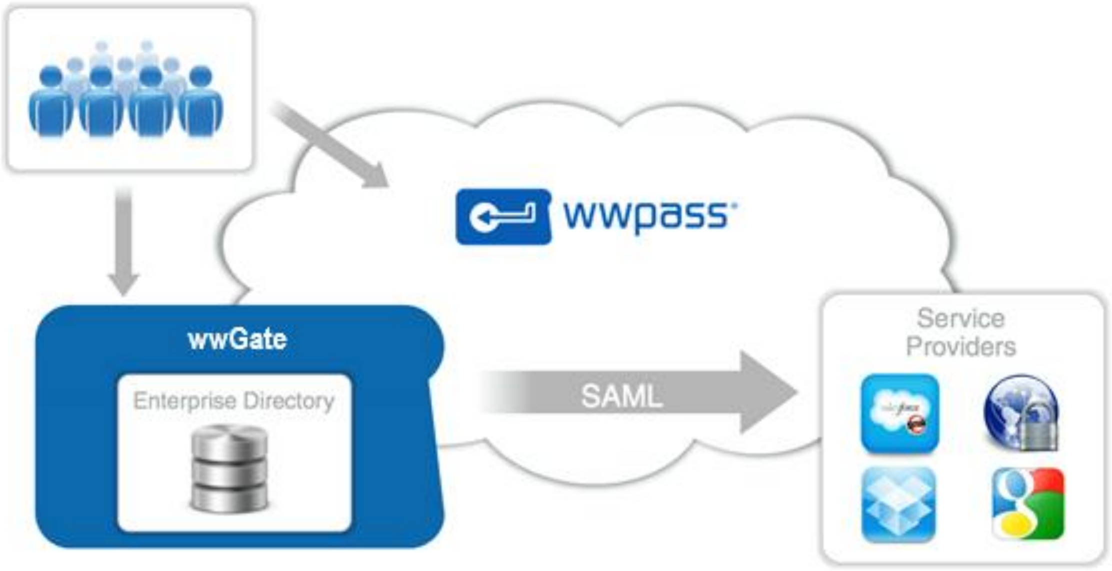


Figure 1. wwGate Application Flow

wwGate uses an open-source Apache™ httpd installation that is configured to use several other open-source products in concert with the WWPass SimpleSAML.php security module, which is incorporated into SimpleSAML as part of the authentication system.

When a request for access to a WWPass-enabled web site/service is received by the httpd server, it will first pass on the request to the SimpleSAMLphp WWPass Authentication Module. This module parses the access request and then sends on an authentication request to the WWPass Authentication Cloud. Next, the user is validated against the Microsoft Active Directory instance. Once the user has been authenticated/denied, a return message is passed. Upon successful authentication by this second identity check, the user is forwarded on to the site/service initially requested.

wwGate is configured to use:

- **Secure Sockets (SSL)** for secure communications
- **PHP** to handle the data input from the web page(s)
- **LibCuRL** to parse the data input for passing on to the WWPass service
- **SimpleSAML** to pass authentication data in XML format

wwGate consists of a preconfigured OVF-compatible open-source virtual environment that contains open-source packages for the Apache httpd / PHP / LDAP / SSL / LibCuRL / SimpleSAML / SimpleSAML.php modules.

All communications between the WWPass authentication module (residing within the enterprise infrastructure) and the WWPass authentication system uses the SSL transport.

Communication with Microsoft Active Directory is enabled through an LDAP bind that accesses the publicly-readable ADO element of the user.

wwGate is unique in that the underlying infrastructure is almost entirely reliant on open-source applications. By basing the entire software package on the Apache httpd web server, the product is firmly rooted in a robust, mature, tested infrastructure that is proven to handle a high number of connections. However, no open-source or third party libraries are used in the WWPass authentication module.

CHAPTER 2 — REQUIREMENTS

Supported Functionality and Requirements

The functionality and requirements supported by wwGate are shown in the following table:

Functionality	Requirements
Virtualization	VMware vSphere v5.0 and above
Directory Stores	Microsoft Active Directory 2003/2008/2012
Supported Browsers*	Internet Explorer® 8, 9 and 10 (32bit & 64bit) Chrome® 20+ Mozilla® Firefox® 14+ Opera™ 16+ Safari® 5
Supported Federation Protocols**	SAML v2.0
Minimum Requirements	Storage Space: 10GB Memory: 1GB RAM (minimum) CPU: 1 64-Bit Intel® or AMD® processor

*Web browser and Internet connectivity is required to activate a WWPass KeySet and authenticate into WWPass enabled applications with a PassKey

**An Information technology (IT) term, Federated Identity Management is part of Identity management, and amounts to having a common set of policies, practices and protocols in place to manage the identity and trust of IT users and devices across organizations. Federation protocols allow users to reuse electronic identities, saving administrators redundant work in maintaining user accounts and provide a consistent, trustworthy infrastructure.

System Requirements for Installation

The following table lists the software packages that must be installed and configured prior to running wwGate, and to allow for proper integration and post-install testing.

Requirement	Details
.OVA/.OVF-compliant virtual environment application	WWPass will provide an OVA/OVF virtual appliance for incorporation in a virtualized environment. Currently only VMware's vSphere is supported. Other virtual environment applications will be supported in future releases.
Microsoft Active Directory (AD)	A Windows Active Directory domain used to administer to users and set permissions.
Internet Access	Inbound/Outbound TCP connections must be allowed from your network to/from reserved network port 443 (HTTPS).
Domain Name	In order to successfully integrate with the WWPass Authentication System, a valid domain name is required

CHAPTER 3 — SETUP FOR ADMINISTRATORS

Smart Start for Administrator Setup

The 'Smart Start' below provides an overview of the main setup steps for wwGate administrators. It highlights essential tasks that must be performed to ensure wwGate works satisfactorily with their system(s).

Smart Start

- Install wwGate
- Configure wwGate for use with Microsoft Active Directory as required
- Verify Configuration is Nominal
- Configure interface: WWPass Settings – Access Code (On/Off)
- Configure interface: WWPass Settings – SPID Certificate
- Configure interface: WWPass Settings – Private Key
- Configure interface: WWPass Settings – Root CA Certificate
- Configure interface: Metadata Settings – Google Apps for Business
- Configure interface: Metadata Settings – Dropbox for Business
- Configure interface: Metadata Settings – Juniper
- Configure interface: Metadata Settings – Salesforce
- Configure interface: Metadata Settings – Metadata Options
- Configure interface: Admin Console
- Configure interface: Single Sign On (SSO)
- Configure interface: Authentication Audit Log Settings.
- Chose Service Provider as desired.
  - Google Apps for Business
  - Dropbox
  - Juniper
  - Salesforce

Installing wwGate

Use the following steps to install wwGate within the virtual environment application for the first time.

Note: For these instructions, it is assumed that you are ready to incorporate the virtual appliance into a supported and existing virtualized VMware vSphere environment.

Initial wwGate OVF Deployment

1. Contact your WWPass Corporation sales representative to receive wwGate OVF file.

2. Start the VMware vSphere virtual application environment.

3. From the vSphere Client menu bar, select **File->Deploy OVF Template** (Figure 2).

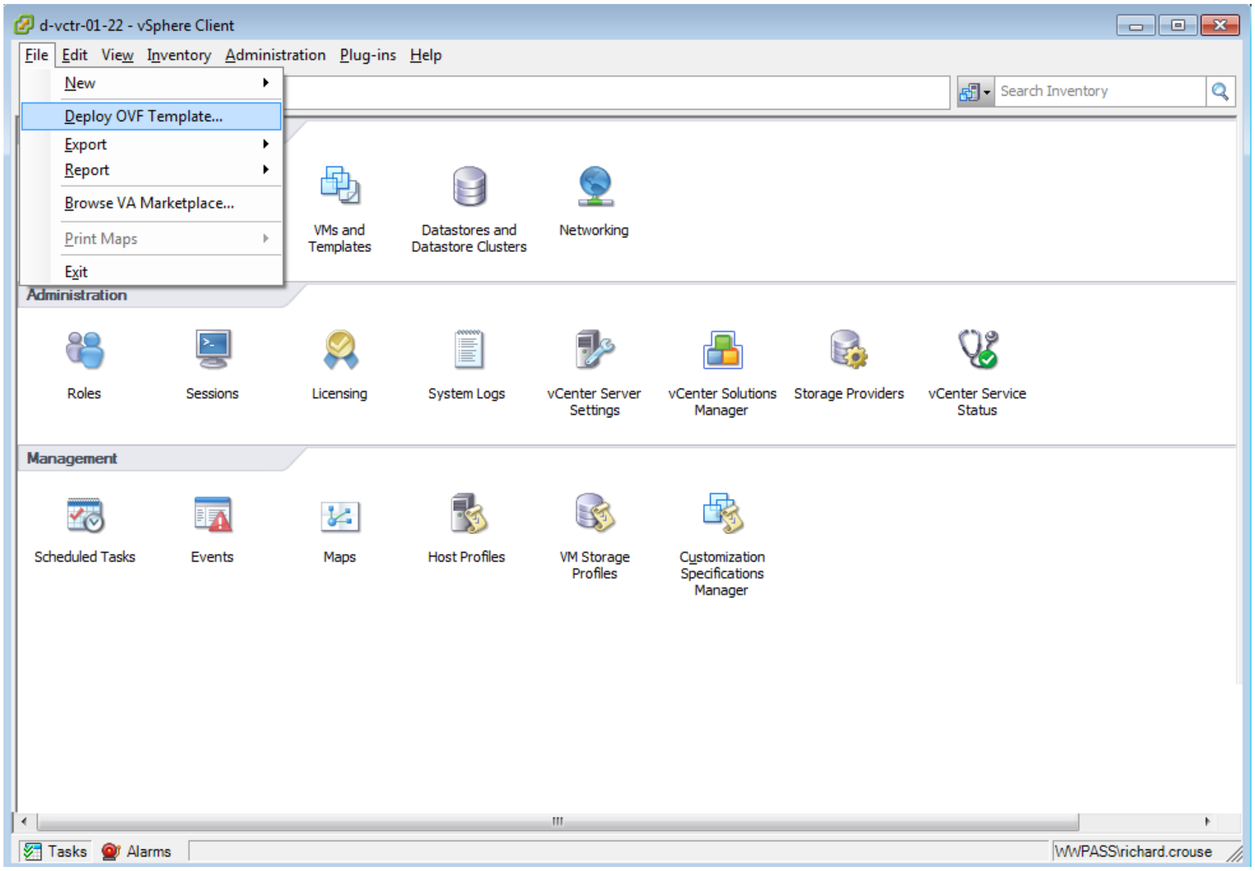
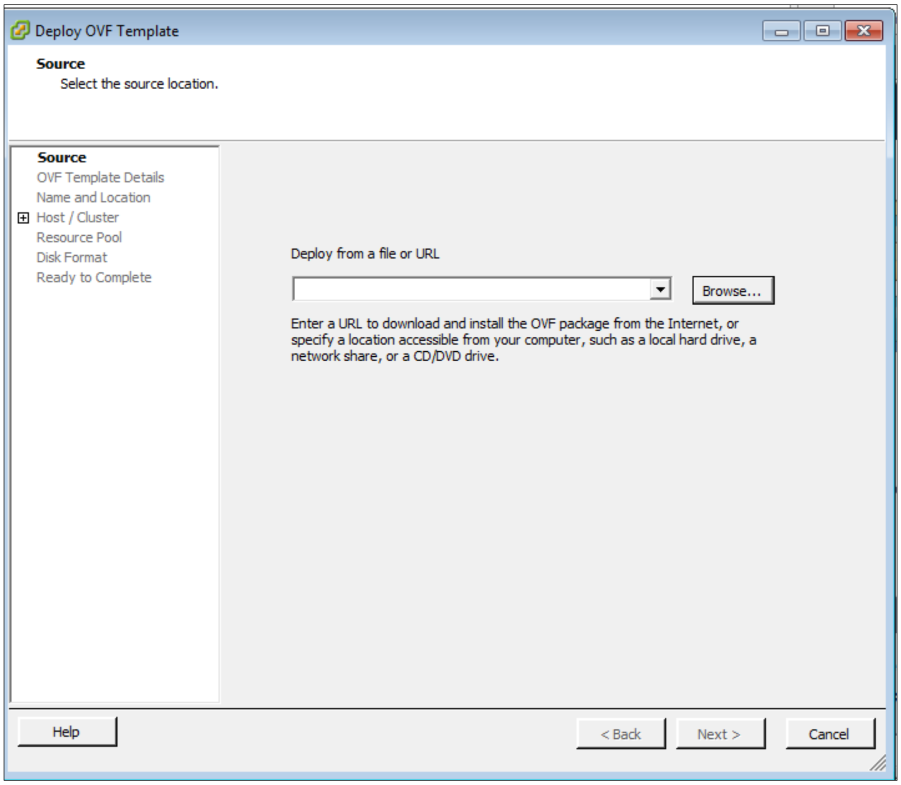


Figure 2. Deploying the vSphere Client OVF Template

4. Answer all vSphere application deployment questions on the “Deploy OVF Template” screen (Figure 3).



Source

Select the source location.

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Figure 3. Deploy OVF Template Screen

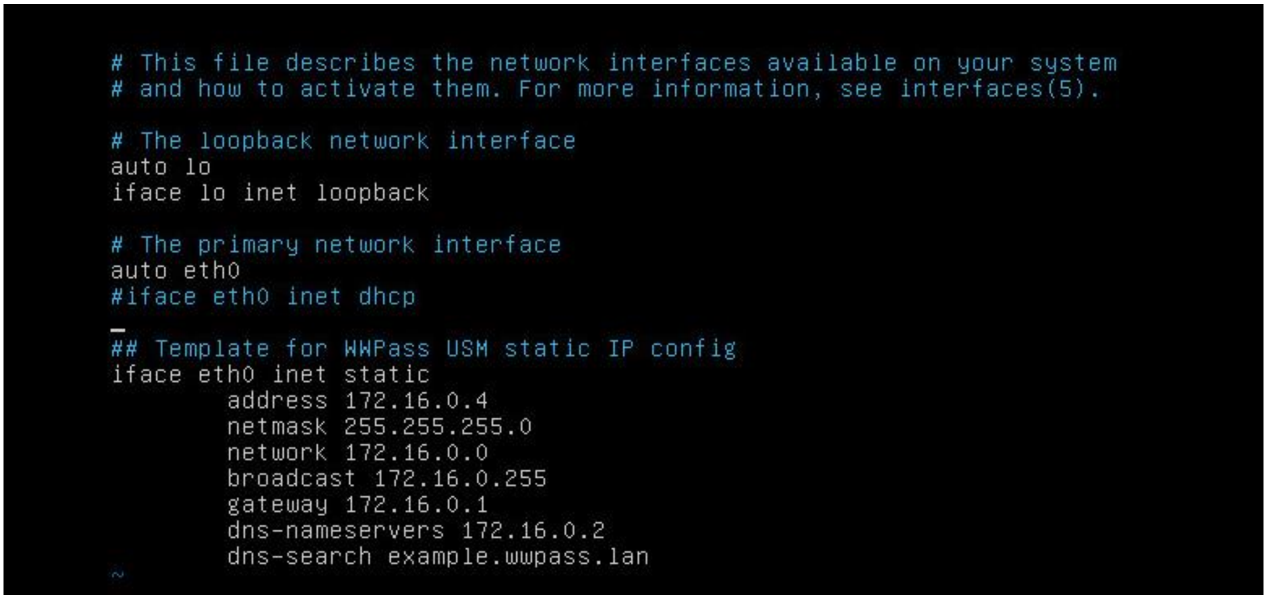
5. Select 'thick' deployment (optimal) but use the recommended hard disk size of 10GB.

6. If the virtual instance has not automatically started, select the virtual instance from the list on the left side and then right-click to expose the sub-menu and select **Power;** then **Power On.**

Adding a Static IP

1. At the Linux Shell (Figure 4), execute the command *sudo vi /etc/network/interfaces* to edit the network configuration.

2. Restart the networking service to apply your changes by executing the command *sudo /etc/init.d/networking restart* to access wwGate web UI and SSH.



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp
_
## Template for WWPass USM static IP config
iface eth0 inet static
        address 172.16.0.4
        netmask 255.255.255.0
        network 172.16.0.0
        broadcast 172.16.0.255
        gateway 172.16.0.1
        dns-nameservers 172.16.0.2
        dns-search example.wwpass.lan
~
```

Figure 4. Adding the Static Network

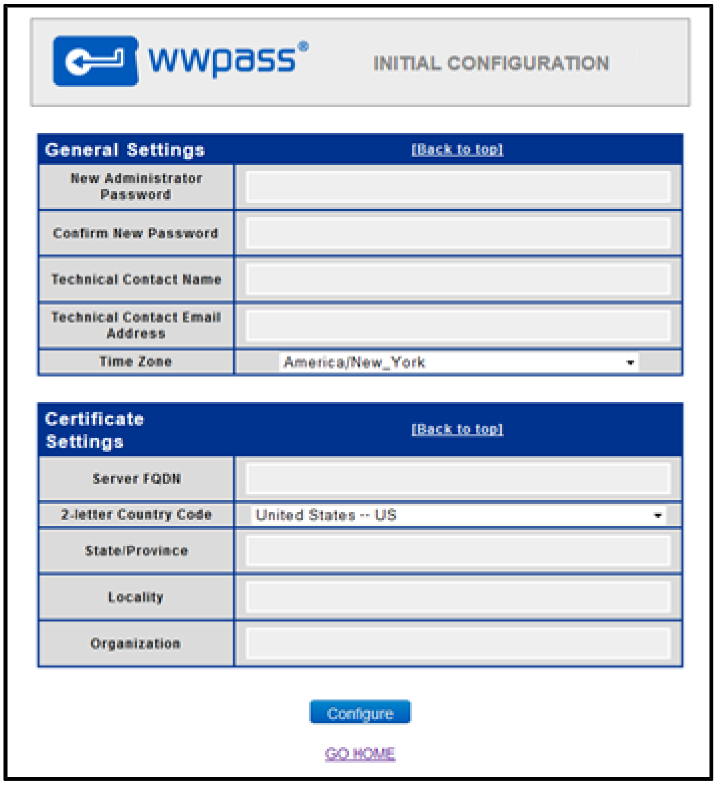
wwGate Initial Configuration

> **Note:** During the Initial Configuration, you work with an initial configuration screen (Figure 5). After the initial configuration settings are entered and submitted to the system, this screen is no longer available when accessing the web page. If you need to update the configuration again, access this screen by entering the following address: `https://saml-idp.yourdomain.com/admin/setup.php`

1. After all of the settings have been entered, within another virtual instance, or from a physical PC on the same network, open a web browser and enter in the address that wwGate was configured for. (i.e. https://www.saml-idp.yourdomain.com/admin).

    a. wwGate Initial Configuration screen is displayed.

2. Use the default credentials to login. Login/Pass: **admin/wwpass**. As soon as you log on, you will be asked to create a new password.



INITIAL CONFIGURATION

General Settings	[Back to top]
New Administrator Password	
Confirm New Password	
Technical Contact Name	
Technical Contact Email Address	
Time Zone	America/New_York

Certificate Settings	[Back to top]
Server FQDN	
2-letter Country Code	United States -- US
State/Province	
Locality	
Organization	

Figure 5. wwGate Initial Configuration Screen

3. When you have finished entering the configuration settings, verify that all fields are filled before clicking **Configure** to submit the settings to the system.

Additional Steps

- Verify that the local firewall (if applicable) has been set to allow traffic to the server FQDN address set in the previous setup screen
- Contact your WWPass Sales Representative to obtain the OVF download that contains a valid SPID

Configuring the Active Directory

This procedure configures Microsoft Active Directory 2003/2008/2012 for integration with wwGate.

Start wwGate Application

If wwGate is not currently running, start the application now.

1. Open a web browser and enter the address: `https://saml.yourdomainname.com/admin`

2. Press **Enter**.

3. Log into the WWPass Administrator Console using your login/password WWPass Passkey credentials.

4. On the administrator console, under the table titled "User Authentication Settings" click **Add.**

There should be no Active Directory installation configured at this time

Steps for Active Directory Integration

1. In the "User Authentication Settings" page, click on **Change**.

2. From the list of Identity sources, click **Select** (next to the Microsoft Active Directory listing).

3. Within the Microsoft Active Directory Settings window, input your desired values.

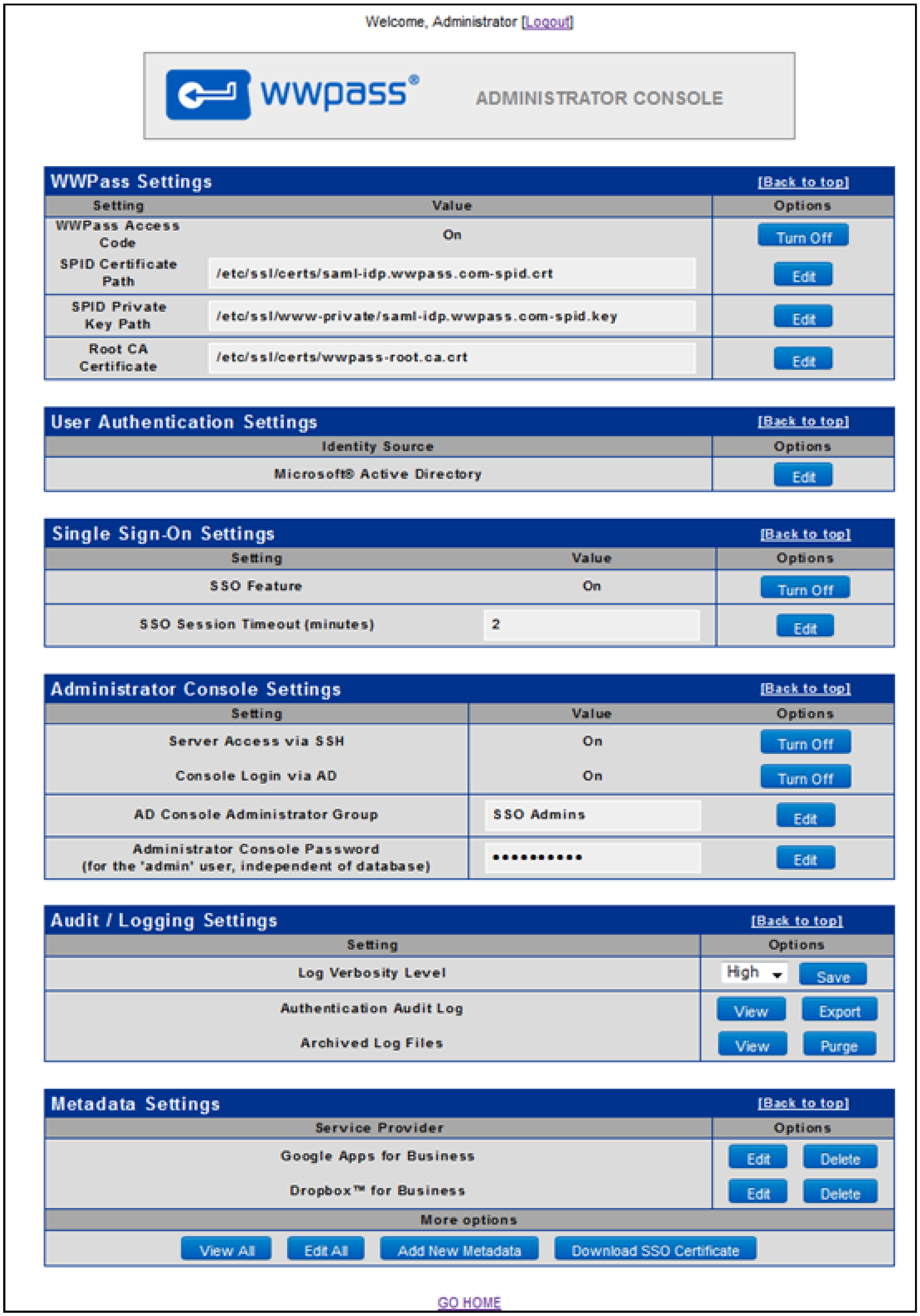
   Example:

   - ***Host IP/FQDN:*** *10.25.22.11*
   - ***Domain:*** *wwpass.lan*
   - ***Base DN:*** *ou=office, dc=wwpass, dc=lan*
   - ***Bind Username:*** *xxxxx*
   - ***Bind Password:*** *xxxxx*
   - ***Authorized Group:*** *Users*

4. Click **Update**.

Configuring wwGate

Clicking **Configure** on the wwGate Initial Configuration Screen (Figure 5) launches the wwGate Administrative Console (Figure 6).



Welcome, Administrator [Logout]

wwpass® ADMINISTRATOR CONSOLE

WWPass Settings [Back to top]

Setting	Value	Options
WWPass Access Code	On	Turn Off
SPID Certificate Path	/etc/ssl/certs/saml-idp.wwpass.com-spid.crt	Edit
SPID Private Key Path	/etc/ssl/www-private/saml-idp.wwpass.com-spid.key	Edit
Root CA Certificate	/etc/ssl/certs/wwpass-root.ca.crt	Edit

User Authentication Settings [Back to top]

Identity Source	Options
Microsoft® Active Directory	Edit

Single Sign-On Settings [Back to top]

Setting	Value	Options
SSO Feature	On	Turn Off
SSO Session Timeout (minutes)	2	Edit

Administrator Console Settings [Back to top]

Setting	Value	Options
Server Access via SSH	On	Turn Off
Console Login via AD	On	Turn Off
AD Console Administrator Group	SSO Admins	Edit
Administrator Console Password (for the 'admin' user, independent of database)	●●●●●●●●●●●	Edit

Audit / Logging Settings [Back to top]

Setting	Options
Log Verbosity Level	High ▾ Save
Authentication Audit Log	View Export
Archived Log Files	View Purge

Metadata Settings [Back to top]

Service Provider	Options
Google Apps for Business	Edit Delete
Dropbox™ for Business	Edit Delete

More options

View All | Edit All | Add New Metadata | Download SSO Certificate

GO HOME

Figure 6. wwGate Administrative Console

The following procedures configure wwGate within the virtual environment application.

Configuring the WWPass Settings

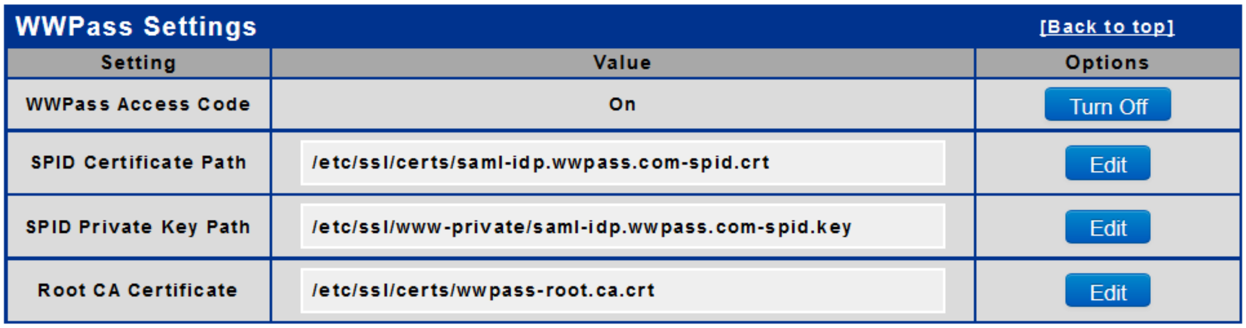
1. Set the WWPass Access Code to **On** (Figure 7).

2. Enter the SPID Certificate Path.
   For example, `/etc/ssl/certs/saml-idp.wwpass.com.spid.crt`.

> **Tip:** Another way to get the SPID onto wwGate is to use WinSCP (for Windows) to transfer files to wwGate. (Remember to enable SSH.)

3. Enter the SPID Private Key Path.
   For example, `/etc/ssl/www,private/saml-idp.wwpass.com.spid.key`.

4. Enter the Root CA Certificate as required.



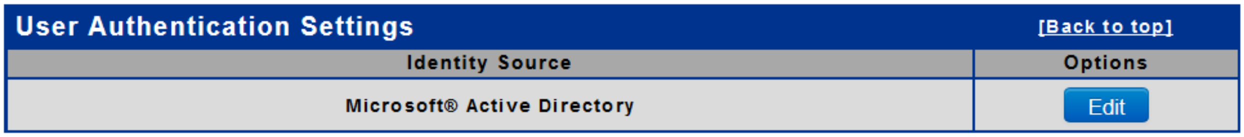
WWPass Settings [Back to top]

Setting	Value	Options
WWPass Access Code	On	Turn Off
SPID Certificate Path	/etc/ssl/certs/saml-idp.wwpass.com-spid.crt	Edit
SPID Private Key Path	/etc/ssl/www-private/saml-idp.wwpass.com-spid.key	Edit
Root CA Certificate	/etc/ssl/certs/wwpass-root.ca.crt	Edit

Figure 7. WWPass Settings Pane

Setting User Authentication

5. Verify that the *Identity Source* is set to the **Microsoft Active Directory** (Figure 8).



User Authentication Settings [Back to top]

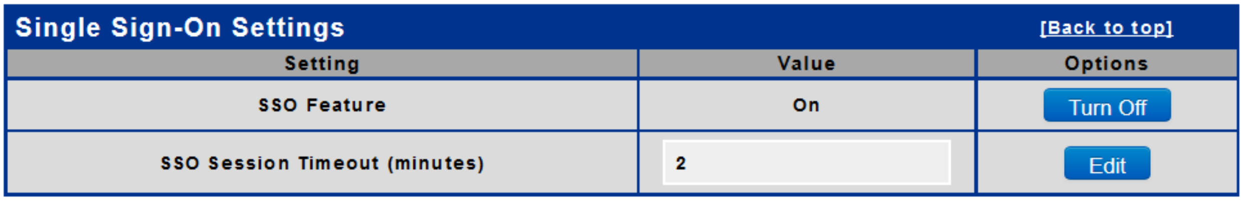
Identity Source	Options
Microsoft® Active Directory	Edit

Figure 8. User Authentication Settings Pane

Single Sign-On Settings

6. Verify that the *SSO Feature* is set to **On** (Figure 9).

7. Enter the SSO Session Timeout (minutes) value. For example, **2**.



Single Sign-On Settings [Back to top]

Setting	Value	Options
SSO Feature	On	Turn Off
SSO Session Timeout (minutes)	2	Edit

Figure 9. Single Sign-On Settings Pane

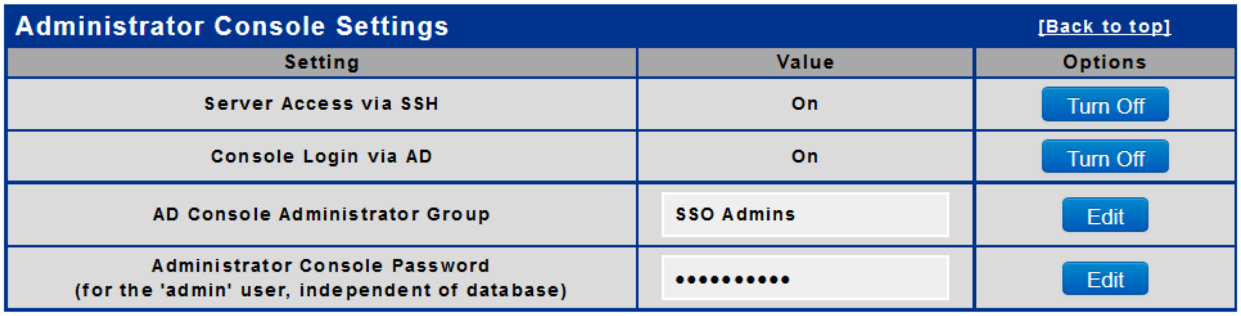
Administrator Console Settings

8. Verify that the *Server Access via SSH* Setting is **On** (Figure 10).

9. Verify that the *Console Login via AD* Setting is **On**.

10. Enter a value for the *AD Console Administrator Group*. For example, **SSO Admins**.

11. Enter a value for the Administrator Console Password.



Administrator Console Settings [Back to top]

Setting	Value	Options
Server Access via SSH	On	Turn Off
Console Login via AD	On	Turn Off
AD Console Administrator Group	SSO Admins	Edit
Administrator Console Password (for the 'admin' user, independent of database)	●●●●●●●●●●	Edit

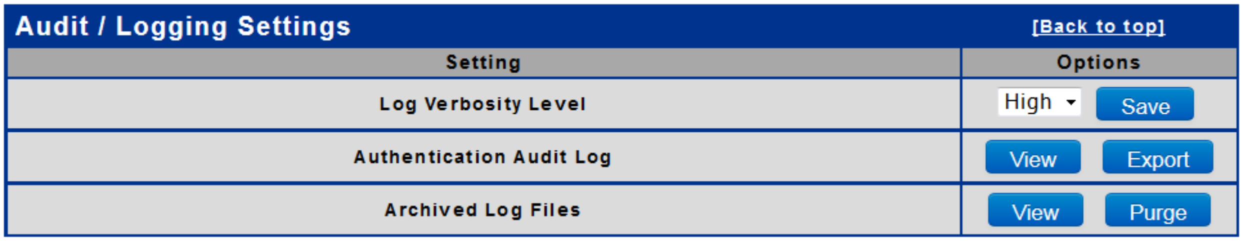
Figure 10. Administrator Console Settings Pane

Audit/Logging Settings

12. Set the wwGate *Log Verbosity Level*. For example, **High** (Figure 11).

13. Verify that you can view the *Authentication Audit Log* by clicking the **View Option**.

14. Verify that you can view the *Archived Log Files* by clicking the **View Option**.



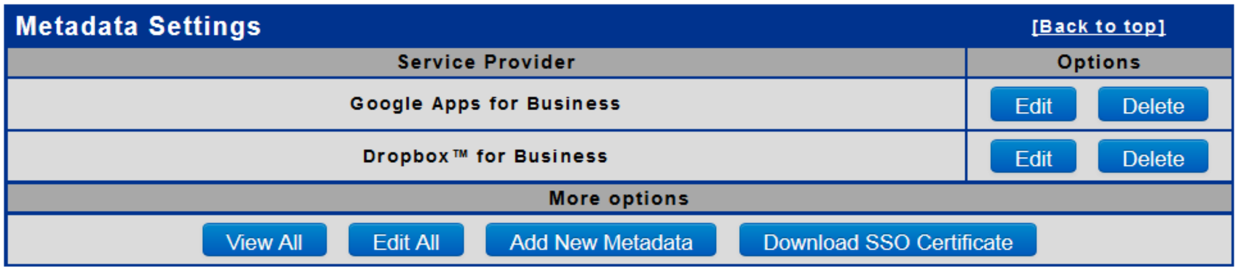
Audit / Logging Settings [Back to top]

Setting	Options
Log Verbosity Level	High ▾ Save
Authentication Audit Log	View Export
Archived Log Files	View Purge

Figure 11. Audit/Logging Settings Pane

Metadata Settings

15. Choose your *Service Provider*. For example, **Dropbox for Business** (Figure 12).



Metadata Settings [Back to top]

Service Provider	Options
Google Apps for Business	Edit Delete
Dropbox™ for Business	Edit Delete

More options

Figure 12. Metadata Settings Pane

Note: You will not be able to replace an existing SSO certificate using any browser other than Google Chrome 20+.