Giuseppe "Gippa" Paternò

Protecting virtual datacenters

A secure access to VMware vCloud with SecurePass

www.gpaterno.com

June 2012

Page intentionally
Left blank

Table of contents

Preface

Technology is great; it allows to do simply the same things that could have taken ages just a few years ago. Before virtualization, even creating a simple highly available web site would have been a nightmare, requiring at least a week's worth of work. And what about updates? Keeping your fingers crossed every time, hoping that everything worked well or with little effort. Now, with a simple wizard, just about anyone can exploit high availability or roll-back to a previous snapshot if something goes wrong.

I've played with a lot of virtualization technologies: VMware, KVM, Xen, Solaris Containers, OpenVZ, LXC and more. VMware vCloud is the first infrastructure software I've ever seen in production that allows you to configure your virtual environments and datacenters through your web browser.

As a "security guy", my first thought was: what if I can exploit a man-in-the middle attack, steal the password to administer a virtual datacenter of a bank and delete machines for fun or steal confidential data?

This publication describes how I addressed the issue of breaking into virtual datacenters on two different organizations that adopted VMWare vCloud. The target audience of this publication is a VMWare vCloud administrator or an end customer, both wishing to understand the security risks behind cloud technologies and wishing to enhance such security. Basic knowledge of Internet protocols is required.

The author

Giuseppe Paternò is currently contracted as EMEA Technical Manager by Canonical Ltd, the company behind Ubuntu, and he's the CTO of GARL, the leading Swiss Bank for Digital Identities. He worked in the past for Sun Microsystems and IBM and participates in the Italian security communities. As an expert in computer security architectures, he works with the most famous companies in telecommunications, government and finance.

More information on his background on his personal web site
http://www.gpaterno.com/ or LinkedIn http://www.linkedin.com/in/gpaterno.

Acknowledgements

A big thank you goes to: Pancrazio "Ezio" De Mauro, for reading and correcting my English; my wife Maria, for being so patient while conducting tests and being with me for better and for worse; Marco Righini of Intel, Nicola Moresi and Renato Rossi of Moresi.Com, for giving me the chance of playing with vCloud extensively; Donatella Dalla Benetta for taking care of the design and graphics of this whitepaper.

Copyright

Disclaimer

I do not speak on behalf of my employer and/or contracting parties, nor am I authorized to represent them publicly. All and any opinion and results expressed in this document are solely mine and do not represent my employer and/or contractor point-of-view. All the tests and any project contribution are done as an independent researcher out of my working hours.

1 Considerations on Cloud Security

Cloud and digital identities

Let's face it, cloud sounds like yet another marketing buzzword, it can mean just anything or nothing. What's the difference in between cloud and the good old hosting or housing or colocation? Probably, at the end of the day, nothing much. But cloud is meant to be something really revolutionary and an opportunity for everybody in the IT world.

Probably the catalysts for this revolution are ubiquitous Internet and having enough bandwidth to accommodate for almost any application. Web 2.0 enriched the user experience so much that a full javascript application can replace a traditional client/server or mainframe application, being more intuitive and therefore requiring less training for users.

> “What happens if someone is able to steal your virtual datacenter's credentials or gain “administrative access?”

I'm currently writing this paper in a plane from Europe to the USA, flying at 35.000 feets over the Atlantic and yet having full Internet connectivity. Would you believe that 10 years ago? Probably not. And that's why this enabled a new revolution: the Cloud.

While Cloud itself is not technically any different from traditional hosting, housing or outsourcing with geographical business continuity, the revolution is in the concept of optimizing costs while allowing greater flexibility. These advantages are accomplished both on the client and the provider by leveraging virtualization to the extreme, hardware or application virtualization alike.

Especially in these days of international financial crisis, outsourcing all or part of a company's own infrastructure can lower IT costs so that more resources can be focused on the core business of the company. Yet, current technologies enable even more flexibility in IT, by designing custom infrastructure through easy-to-use web interfaces and forgetting about server or network failures: a provider's underlying virtualization software will take care of it on behalf of customers. This enables IT to focus on their own objectives, i.e. supporting their company's business, for example creating new projects that help improving processes and procedures.

It all sounds good and easy, but what about your company security? You are outsourcing part of your datacenter in a virtual datacenter hosted in a provider, or you are storing part of your core data in an application hosted somewhere. In the not so distant past, you would store your physical files in a secure drawer of a secure room; in old-fashioned IT, you would have your servers in a secure room or datacenter with multiple firewalls. But how about accessing and administering your datacenter from a web browser anywhere in the world? This changes the way security has been conceived so far. What happens if someone is able to steal your virtual datacenter's credentials or gain administrative access? This person will be able to control any machine, any network equipment and any data, potentially disrupting your business or -even worse- selling precious information to competitors.

Cloud is a great opportunity, but in this scenario, digital identities are more and more a crucial part of the IT security infrastructure. This is not something that can be dealt with a simple username and password. You would not lock the door of your house with a key that can be opened with a toothpick, would you?

Cloud and ISO 17799

As cloud computing achieves increasing popularity, concerns are being voiced about security issues introduced when adopting this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures.

The British had an extraordinary vision of IT security needs: they created the BS7799 standard, which eventually became ISO 17799. ISO 17799 is an information security standard published by the International Organization for Standardization (ISO) and provides best practice recommendations on information security management.

In the original ISO 17799, section 7 describes access controls and environmental facilities for data centers and other critical IT equipment areas. Here's a summary of the main points:

1. Secure areas - describes the need for concentric layers of physical controls to protect sensitive IT facilities from unauthorized access.
2. Equipment security - critical IT equipment, cabling etc. should be protected against physical damage, fire, flood, theft etc., both on- and off-site. Mains power supplies should be secured. IT equipment should be maintained and disposed of securely.
3. General controls - describes the need for clear-desk and clear-screen policies, and authorization processes for removal of IT assets from site.

In the cloud world, are the above points still valid? Probably not any more if you decided to trust a cloud provider. However these best practices are still valid for cloud providers themselves, and can be useful to select the best cloud provider.

> "Best practices are still valid for cloud providers themselves, and can be useful to select the best cloud provider"

What still makes sense is section 9 of ISO 17799 that covers access control, in detail:

1. Business requirements for access control - business requirements for access control should be clearly documented in an access policy statement (role based access control).
2. User access management - access rights allocation to users should be strictly controlled through user registration and administration procedures, including special restrictions over the allocation of privileges and passwords, and regular access rights reviews.
3. User responsibilities - users should be made aware of their responsibilities of choosing strong passwords and keeping them confidential.
4. Network access control - access to network services should be controlled, both within the organization and between organizations.
5. Operating system access control - operating system security facilities and utilities should be used appropriately to identify the administrators who are able to login and perform commands on the systems.

6. Application access management - application systems should incorporate security controls to restrict unauthorized access. Sensitive systems may require dedicated/isolated platforms and special handling.
7. Monitoring system access and use - systems should be monitored for access policy violations and other security events such as use of privileges and alarms/exception conditions.
8. Mobile computing and teleworking - there should be formal policies covering the secure use of portable PCs, PDAs, cellphones etc., and secure teleworking ("working from home" and other forms of mobile working).

Do these points matter in the cloud? Yes, surely they are still very important.

No matter if you deal with a traditional environment or a virtual infrastructure, tracking down who's doing what and who is accessing your data and your infrastructure IS still the most important aspect of your application and infrastructure security. And this leads to another key aspect: identifying your users plays a delicate and strategic role in your organization.

Identity theft

Properly identifying your users is very important: you must ensure that the user is really who he/she claims to be. In an old-fashioned Intranet, where all data is securely "stored" behind your premises, you can rely on a weaker mechanism of identifying users. You let your colleague Alice look at your data because she's maybe sitting behind you, and therefore she's trusted as she's inside your premises.

But how about cloud? Cloud means that Alice is not any longer sitting behind of you, but she's located somewhere in the world, sitting probably by an hot desk or even sitting on a plane. Would you trust someone that claims to be Alice calling you on the phone and asking to reveal vital company information?

Probably not. But you could if she was using some social engineering tricks such as "you don't you recognize my voice? We were in the same company meeting last year. How's your daughter?". If you think that this trick won't work with you, I bet it will work with most of your colleagues: are you aware of the problems related to identity theft?

Recent studies revealed that in 2010, data breaches of private information doubled that of 2009 (Javelin Strategy & Research, 2010). The rate of data breaches due to identity theft is doubling each year. Just to make an example, only in the USA there were 10 million victims of identity theft in 2008 (Javelin Strategy and Research, 2009) and 35 billion corporate and government records were compromised in 2010 (ITRC). Businesses across the world lose $221 billion a year due to identity theft (Aberdeen Group).

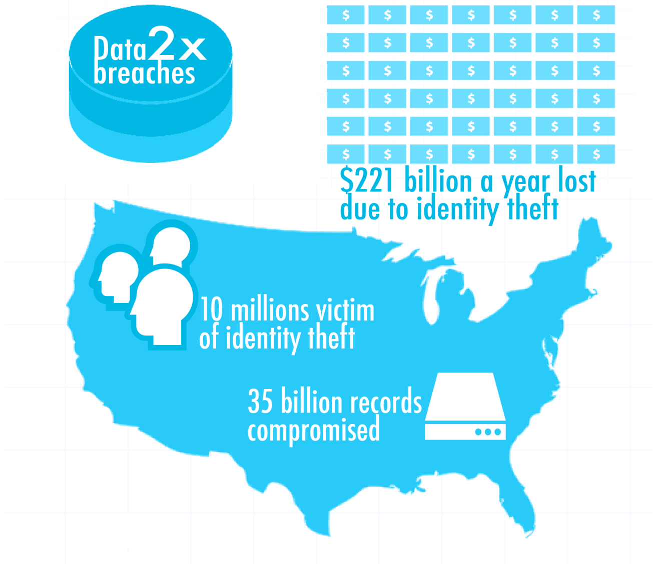
To give you an idea of what identity theft means in practical terms, it can take up to 5840 hours to correct damage from identity theft (ITRC Aftermath Study, 2004).

In the Cloud, identity theft can only make this number grow. Would you trust a simple username and password then, like trusting someone claiming to be Alice's over the phone?

A matter of trust

Trusting someone over the phone is not that bad if you can recognize the number that she's calling from. In the security world, this is called a multifactor authentication, it means that you recognize both Alice voice and the caller ID. But trusting the caller ID means trusting your mobile network provider.

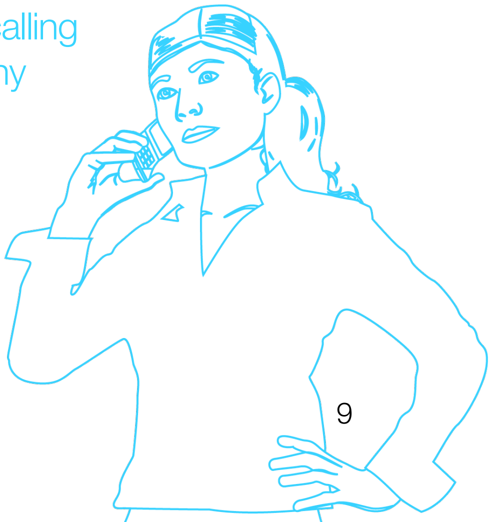
In a traditional IT structure, you would adopt a strong authentication mechanism located in your premises, but that can be really costly.



In the cloud that means that you would install all these pieces of software in a virtual provider. You paid a lot of money and yet you can't tell if this software has been compromised by a malicious user.

How do you know that the user is "knocking" at your virtual infrastructure and your application is really who he/she claims to be?

> “Would you trust someone that claims to be Alice calling you on the phone and asking to reveal vital company information?”



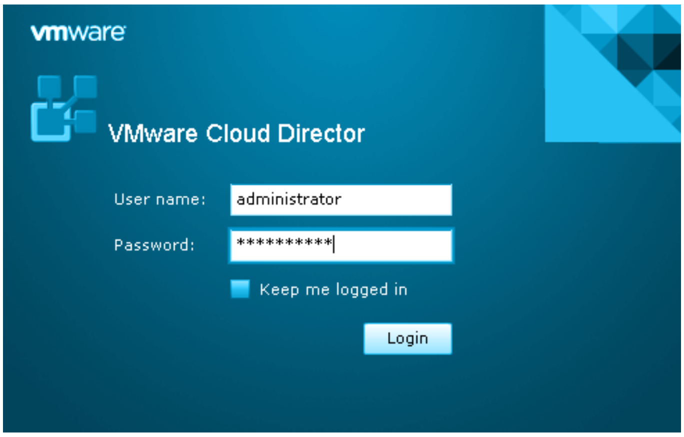
2 Virtual Datacenter Infrastructures

Infrastructure as a Service (IaaS)

Infrastructure as a Service is the foundation of cloud services: in this most basic cloud service model, an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components, often in the form of virtual servers, virtual storage and virtual networks. The service provider owns the equipment and is responsible for housing, running and maintaining it, leaving to the client the task to focus on their applications instead of maintaining the hardware.

There are a number of players supplying IaaS infrastructure software, one of which is VMware with its vCloud Director software, it's probably the most popular cloud infrastructure software alongside OpenStack. The value of VMware cloud offering, if compared to OpenStack, is that a customer who already embraced VMware technology is able to move their infrastructure from its premises to a virtual datacenter hosted in a Cloud Provider easily from a convenient web portal. OpenStack, on the other end, is more suited for Unix-based stateless services.

VMWare vCloud Director



User name: administrator

Password: **********

VMware vCloud Director is a cloud computing management platform that allows organizations to be able to deploy services and consume resources on demand through an easy to use web portal.

More specifically, VMware vCloud Director is a software solution which provides interface, automation, and management capabilities. Such capabilities allow enterprises and service providers to supply traditional vSphere resources as a Web-based service, thus hiding the complexity of a full infrastructure to final customers.

Cloud Providers and large IT outsourcers/providers are among the organizations which can benefit the most from VMware vCloud Director, because they can resell their underlying hardware infrastructure (servers, networks and physical space) as virtual datacenters (vDatacenter).

An easy to use Web interface provides an excellent way for anybody to architect, deploy and manage a vDatacenter focusing on business needs, rather than worrying about the underlying physical structure and hardware failures.

From a Customer perspective, either internal or external, this new way of accessing a virtual datacenter from the Internet can lower the total cost of ownership compared to an IT infrastructure entirely deployed in-house.

Through the flexible model of VMware vCloud Director, each Cloud Provider or large IT outsourcer can charge back by creating its own model, ranging from pay-as-you-go to an all-inclusive offer.

Security threats of vDatacenters

So you are comfortably sitting in an hotel bar 10.000 km away from home, like I am at the moment, administering and creating new systems and networks from the web. That's absolutely great!

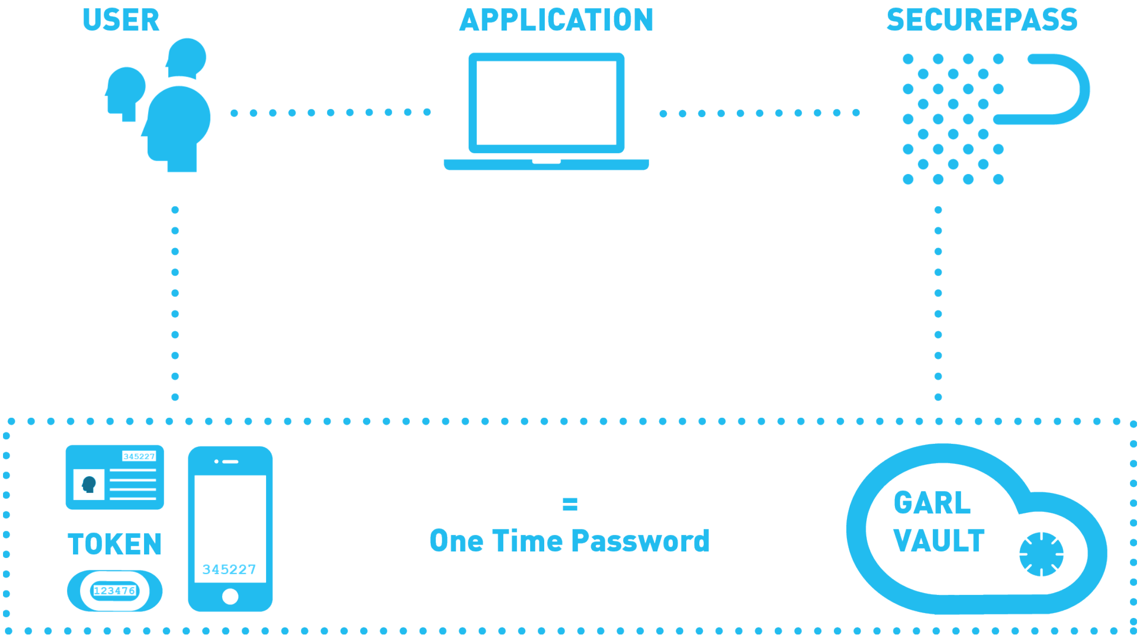
But what if someone is sitting behind me stealing my password? He/she would be able to log-in to my vDatacenter portal and basically do whatever he/she wants, including destroying machines or -even worse- leaking precious company data.

Because vDatacenters allow great flexibility by orchestrating customers' datacenters, identity theft increases the risks of data being compromised or services being disrupted: by compromising a single identity, a malicious user can log in to the vCloud portal and fully control the virtual datacenter from anywhere.

3 Secure identity for the cloud

SecurePass

Although extremely flexible and useful, the vCloud portal can be the weakest link of your datacenter security if not properly hardened. Would you jeopardize your entire datacenter security having a password such as "abc123" or someone sitting behind and taking note of your password?



The obvious choice is then introducing a stronger authentication mechanism, but some concerns might arise. What kind of strong security solution? Will the infrastructure be compatible with VMware vCloud? Which kind of security infrastructure should be deployed? Of course the infrastructure must be able to cope with multiple datacenters and have redundant Internet access. But how much will it cost to license, deploy and manage? Do more people in the organization need training? How about monitoring security threats?

SecurePass is an on-line identity and strong authentication provider that can address these issues by providing secure, reliable, easy and affordable identity services.

SecurePass comes with a strong authentication system based on one-time passwords (OTP) and standard protocols to access it: by using both, it is possible to mitigate the risks of identity theft in VMware vCloud in a matter of minutes without having to pay money upfront to set up the whole infrastructure and, more importantly, without wasting time.

GARL, the bank behind SecurePass

But how can SecurePass be trusted? Unlike traditional service providers that come from an IT background, GARL is an independent and neutral Swiss Bank for Digital Identities born in 2008 and has a strong banking background. GARL aims to honor the Swiss centennial tradition of quality banking to create innovative and secure products for the digital era.

> "A strong authentication system based on one-time passwords (OTP) and standard protocols"

Highly inspired by Swiss laws of 1934 on bank secrecy, customers' privacy and protection are GARL's top priorities. GARL's multi-datacenter multi-national facilities have countermeasures against digital breaches, guaranteed by the same teams who protected most of the European financial banks: their internal Security Intelligence Bureau is at the heart of the design and protection of the bank's infrastructure.

GARL's main offices are located in Switzerland and United Kingdom.

4 Virtual Datacenters Scenarios

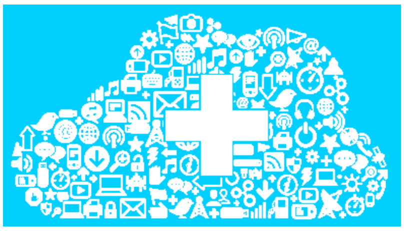
Cloud providers: external vs internal customers

Cloud Providers offer their customers an efficient infrastructure for applications and systems, making their IT department more focused on their core business while not not having to worry about the underlying platform. But who are their typical customers?

We usually think of Cloud Providers as evolved hosting/housing providers giving their services to organizations connected the Internet. But sometimes we forget that large and multinational organization have IT departments that provide their services to their own internal customers. The financial crisis also opened up another interesting scenario, i.e. companies in the same territory or heterogeneous companies grouping together in a consortium to share their IT expenses and bring costs down.

All of these entities can benefit from adopting a cloud infrastructure but they are certainly in need of a better security and strong authentication to manage their vDataCenters.

I had a chance to secure VMware vCloud access for two companies that reflect both external and internal customers. In the following paragraphs I will describe the two scenarios.



BeCloud by Moresi.com

Moresi.Com comes from a traditional hosting/housing background. The founder and CEO, Nicola Moresi, always bet on virtual to be the "nextbigthing" in hosting/housing and decided to embrace it even before it was marketed as "Cloud". The company adopted VMware as a platform for delivering virtual servers to their customers and vCloud was the natural choice to provide a full virtual datacenter experience to their customers. BeCloud is Moresi.Com's offering for virtual datacenters and is currently the largest vCloud installation in Switzerland.

Typical customers of BeCloud are companies for which data protection is top priority: Moresi.Com made security, business continuity and data confidentiality the key values for their BeCloud offering. As an important part of this strategy, the CEO wanted to provide a secure access to their virtual datacenter as a complementary option to their offering, so that their customers enjoy a further level of protection when accessing their own virtual datacenters.

Hardware Manufacturer Core Lab

The hardware manufacturer I worked with holds several datacenters across the globe. But there's only one datacenter that is used for testing new software both from internal personnel and external companies around the world.

The lab is focused on running benchmarks, showing and evaluating Cloud Solutions and Storage and, more importantly, running proof of concepts.

> "The lab is focused on running benchmarks, showing and evaluating Cloud Solutions and Storage and, more importantly, running proof of concepts."

Most of the proof of concepts and software testing are delivered through extensive use of virtual machines. The peculiarity of these scenarios is that the infrastructure is unknown at the beginning and creating best practices is part of the test itself. Due to the dynamic nature of the environment, the preparation of virtual machines involved the work of a high-experienced dedicated IT staff to setup the infrastructure and to fulfill the requests.

VMware vCloud director was the perfect choice to let end-users architect the infrastructure on their own without waiting for any staff to process the change requests. Machines and networks can be easily provisioned on-demand from a comfortable web interface in a matter of seconds.

Patents protect most of the tested software and hardware and often they are not yet on the market or is even under active development. The lab holds therefore precious information that must be kept confidential.

The challenge was to protect the confidential data of the manufacturer's key partners by providing a secure access to the virtual datacenters that are accessed world-wide.

5 Securing vDatacenters with SecurePass

Technical pre-requisites

This document will not go through the initial setup of VMware vCloud Director. I will assume that the VMware infrastructure is running and vCloud Director has been set up.

Before proceeding any further, please download the GoDaddy Certificate Authority bundle by going to the GoDaddy website
https://certs.godaddy.com/anonymous/repository.seam and downloading the gd_bundle.crt file.

Please also ensure that outbound LDAPS traffic is allowed from the vCloud portal.

Opening an account with SecurePass

SecurePass is very similar to a banking product and you will need a Premier "checking account" to operate with vCloud. The difference in between Standard and Premier is that the Standard account offers RADIUS and CAS as access protocols, while Premier adds LDAP. We will see later why LDAP is important for our deployment.

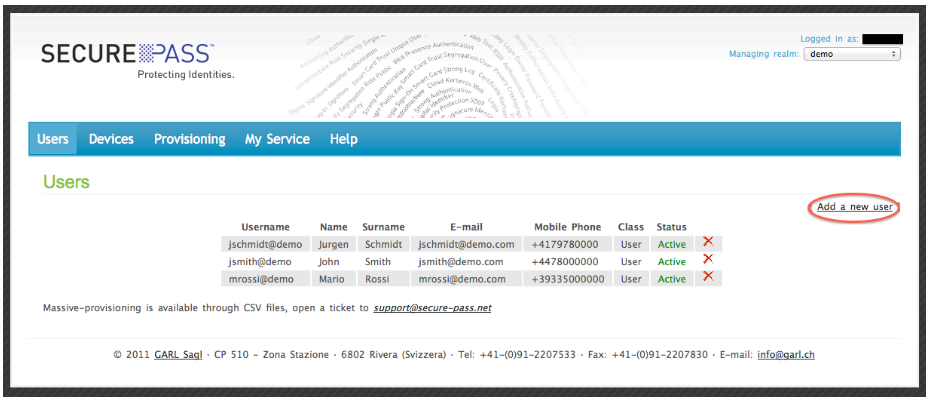
To open an account with SecurePass, go to the website www.secure-pass.net/open and select Apply online. Choose this option only if you have a mobile number within European Union or Switzerland AND you own an Apple iOS (iPhone/iPod touch/iPad), Blackberry or Android.

The country restriction is due to SecurePass' upstream SMS provider, as the service will send you an SMS to verify your credentials. It is known to work with major USA mobile carriers and other countries as well, but heavily depends on mobile operators. If you have one of the above devices, try opening it online. If you don't receive an SMS within 24 hours, send an e-mail to support@secure-pass.net and request an alternative identity verification method.

Opening an account with SecurePass is straightforward and it normally takes 10-15 minutes. After provisioning your software token, you will be able to access the web control panel of your SecurePass account at https://admin.secure-pass.net/

This on-line procedure will create a Standard account. You will need to contact support@secure-pass.net to upgrade to a Premier account.

If you don't own Apple iOS (iPhone/iPod touch/iPad), Blackberry or Android, please do not apply online: either contact a SecurePass advisor via www.secure-pass.net/advisors or apply via fax as you will need an hardware token. Please remember to mention you need a Premier account.



Logged in as: [redacted]

Managing realm: demo

Users

Username	Name	Surname	E-mail	Mobile Phone	Class	Status	
jschmidt@demo	Jurgen	Schmidt	jschmidt@demo.com	+4179780000	User	Active	✕
jsmith@demo	John	Smith	jsmith@demo.com	+4478000000	User	Active	✕
mrossi@demo	Mario	Rossi	mrossi@demo.com	+39335000000	User	Active	✕

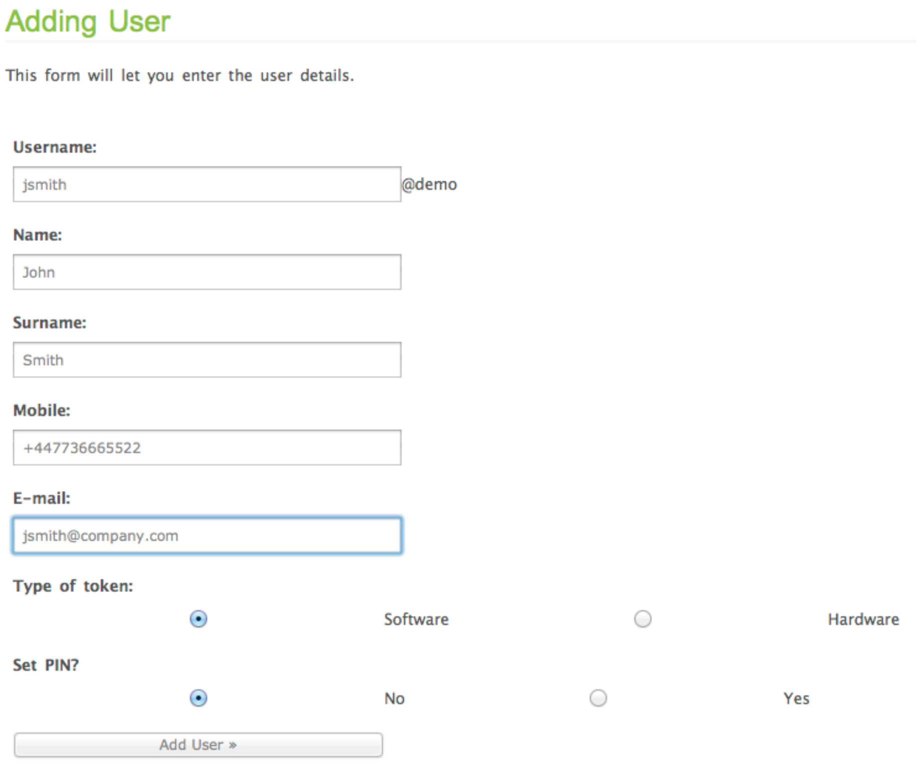
Massive-provisioning is available through CSV files, open a ticket to *support@secure-pass.net*

© 2011 GARL Sagl · CP 510 – Zona Stazione · 6802 Rivera (Svizzera) · Tel: +41-(0)91-2207533 · Fax: +41-(0)91-2207830 · E-mail: info@garl.ch

Create cloud admin users in SecurePass

After your account is created, you will need to add the users who will be able to log in to the vCloud portal. Access your SecurePass control panel via https://admin.secure-pass.net and select Add a new user.

By selecting Add a new user you will be prompted for additional information as follows:



Adding User

This form will let you enter the user details.

Username: jsmith @demo

Name: John

Surname: Smith

Mobile: +447736665522

E-mail: jsmith@company.com

Type of token: ● Software ○ Hardware

Set PIN? ● No ○ Yes

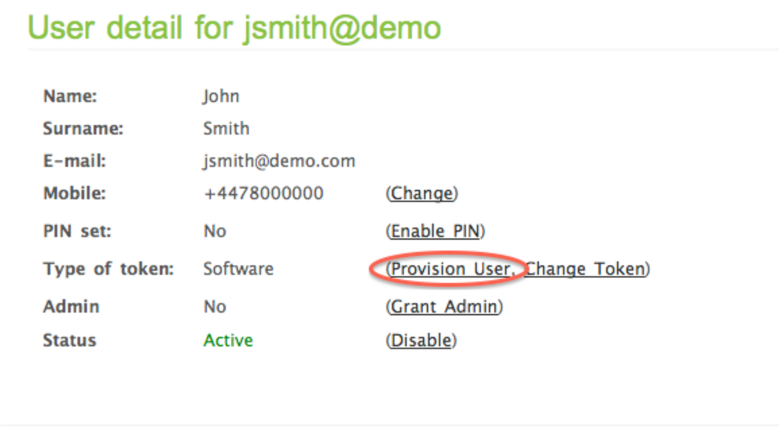
Complete the form with the following:

Username	The username that will be associated with the user. The panel will automatically associate the realm/domain of your account.
Name	User's first name
Surname	User's surname/last name
Mobile	Enter a valid mobile number starting with the country code, i.e. with the leading "+". For example, +41 for Switzerland.
E-mail	Enter the user's email address. It's absolutely crucial that the email address is valid as the user will receive provisioning email(s) from SecurePass
Type of token	Software means a software token on mobile (Android, Apple iOS and BlackBerry) Hardware means an hardware token. You will need to enter a valid model and serial number if you purchase the token from SecurePass. Don't forget to press TAB after entering a valid serial number to complete the seed parameter automatically.
Set PIN	No, leave the account without extra PIN (not recommended) Yes, sets an extra PIN to the One Time Password. PIN can be any character and any length.

Provision a user

After you've added an user to the system, and if you chose a software token for him/her, you will need to "provision" his/her account. Provisioning in this context means sending an email to the user to automatically configure the software token on his/her smartphone. For this step to be completed, it is fundamental that the user can receive emails on his/her smartphone with the address specified earlier.

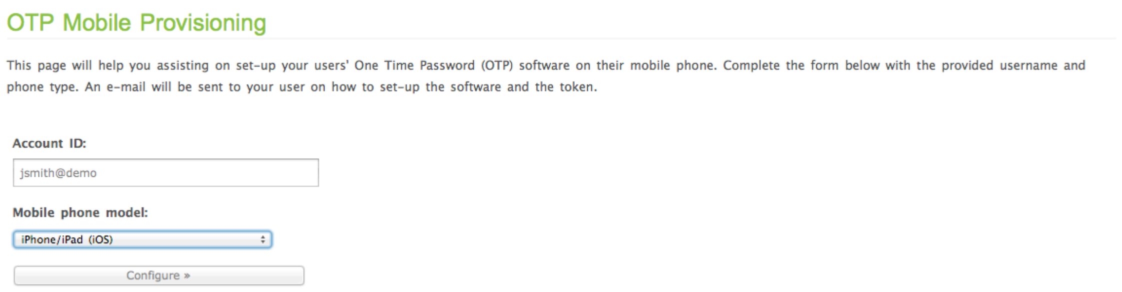
From the control panel, select the user by clicking on the appropriate row. You will be placed in the user's details as follows:



User detail for jsmith@demo

Name:	John	
Surname:	Smith	
E-mail:	jsmith@demo.com	
Mobile:	+4478000000	(Change)
PIN set:	No	(Enable PIN)
Type of token:	Software	(Provision User, Change Token)
Admin	No	(Grant Admin)
Status	Active	(Disable)

Select the Provision User link, that will bring you in the OTP mobile provisioning page:



OTP Mobile Provisioning

This page will help you assisting on set-up your users' One Time Password (OTP) software on their mobile phone. Complete the form below with the provided username and phone type. An e-mail will be sent to your user on how to set-up the software and the token.

Account ID: jsmith@demo

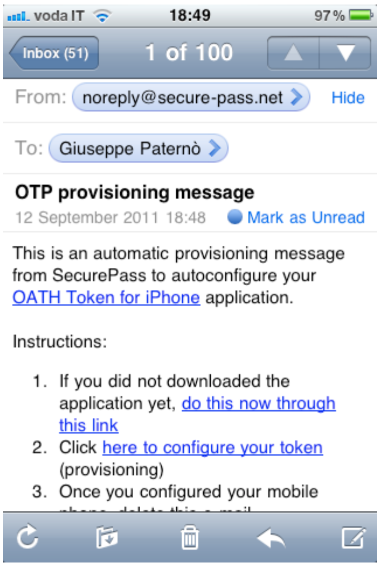
Mobile phone model: iPhone/iPad (iOS)

Select the appropriate model, i.e. Apple iPhone/iPad/iPod Touch (iOS), Android, Blackberry or Software token for Mac/Windows/Linux.

Note that your smartphone clock must be synchronized with a time server or have the correct time set in any other way. A misconfiguration of the clock means that you will not be able to use your software token.

The following example applies to Apple iOS, which is the easiest case.

1. SecurePass will send you a provisioning e-mail, as shown below, that you should read on your iPhone



From: noreply@secure-pass.net

To: Giuseppe Paternò

OTP provisioning message

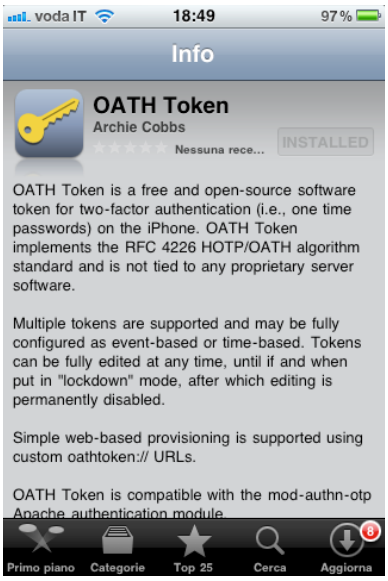
12 September 2011 18:48 Mark as Unread

This is an automatic provisioning message from SecurePass to autoconfigure your OATH Token for iPhone application.

Instructions:

1. If you did not downloaded the application yet, do this now through this link
2. Click here to configure your token (provisioning)
3. Once you configured your mobile

2. Follow the instruction on the e-mail and click on the first link: it connects to the iTunes application download page. Download and install it:



OATH Token

Archie Cobbs

Nessuna rece...

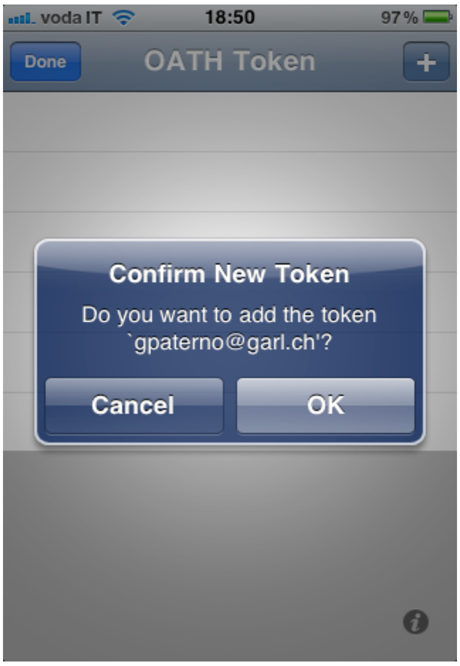
OATH Token is a free and open-source software token for two-factor authentication (i.e., one time passwords) on the iPhone. OATH Token implements the RFC 4226 HOTP/OATH algorithm standard and is not tied to any proprietary server software.

Multiple tokens are supported and may be fully configured as event-based or time-based. Tokens can be fully edited at any time, until if and when put in "lockdown" mode, after which editing is permanently disabled.

Simple web-based provisioning is supported using custom oathtoken:// URLs.

OATH Token is compatible with the mod-authn-otp Apache authentication module

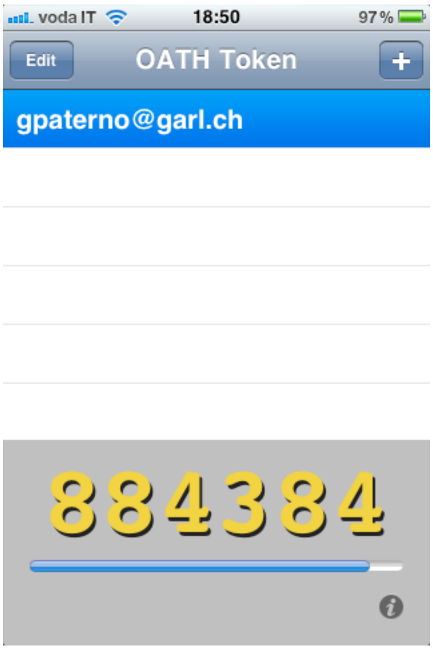
3. Return to the provisioning email and tap on the second link to configure your token. The link will open the OATH Token application and ask your permission to add the new token as shown; tap OK.



Confirm New Token

Do you want to add the token `gpaterno@garl.ch'?

4. The token has now been provisioned. Click on the token named with your username to show your OTP value:



gpaterno@garl.ch

884384

You will now be able to generate a valid SecurePass OTP on your chosen iOS device. Instructions are available for the following smartphones:

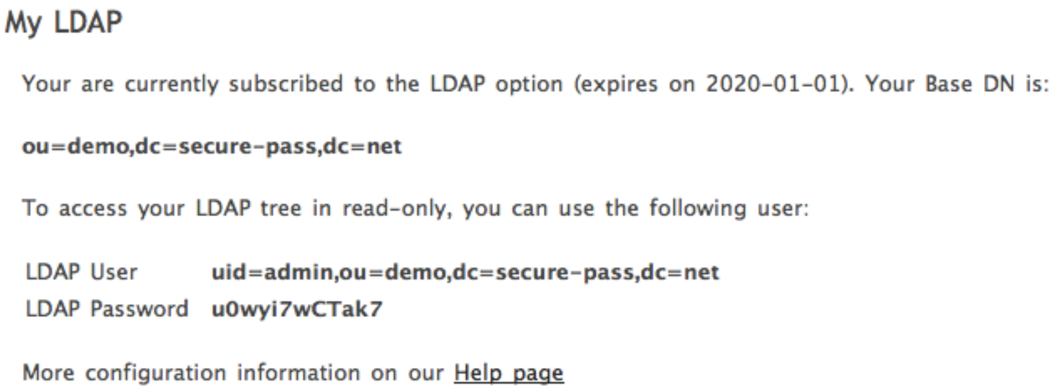
- Android on http://www.secure-pass.net/wiki/index.php/Help:Android
- BlackBerry on http://www.secure-pass.net/wiki/index.php/Help:BlackBerry
- Token for desktop (Windows/Mac/Linux) on http://www.secure-pass.net/wiki/index.php/Help:ConfigureSoftToken

LDAP Support in SecurePass

The Lightweight Directory Access Protocol (or LDAP) is an application protocol for accessing directory services. SecurePass supports company identity access through the LDAP protocol, both for authentication purposes and for accessing user information.

We will use the SecurePass LDAP protocol, which comes with a Premier account, to be able to provide secure authentication to VMware vCloud Director.

In the My Service page of the SecurePass administrative interface, you will find the parameters to bind to the SecurePass LDAP service in read-only mode.



My LDAP

Your are currently subscribed to the LDAP option (expires on 2020-01-01). Your Base DN is:

ou=demo,dc=secure-pass,dc=net

To access your LDAP tree in read-only, you can use the following user:

LDAP User	**uid=admin,ou=demo,dc=secure-pass,dc=net**
LDAP Password	**u0wyi7wCTak7**

More configuration information on our Help page

Please take note of these parameters as we will need those while configuring vCloud organisations. Before going any further, please take note of the hostnames for the availability zones for the LDAP service:

Datacenter Zone	Hostname
Ticino, Switzerland	ldap1.secure-pass.net
Milan, Italy	ldap2.secure-pass.net

vCloud Organizations

An Organization is the fundamental vCloud Director grouping which contains users, the vApps that they create, and the resources that vApps use. It is a top-level container in a cloud that contains one or more Organization Virtual Data Centers (Org vDCs) and Catalog entities. It owns all the virtual resources for a cloud instance. A vCloud Organization can have many Org vDCs.

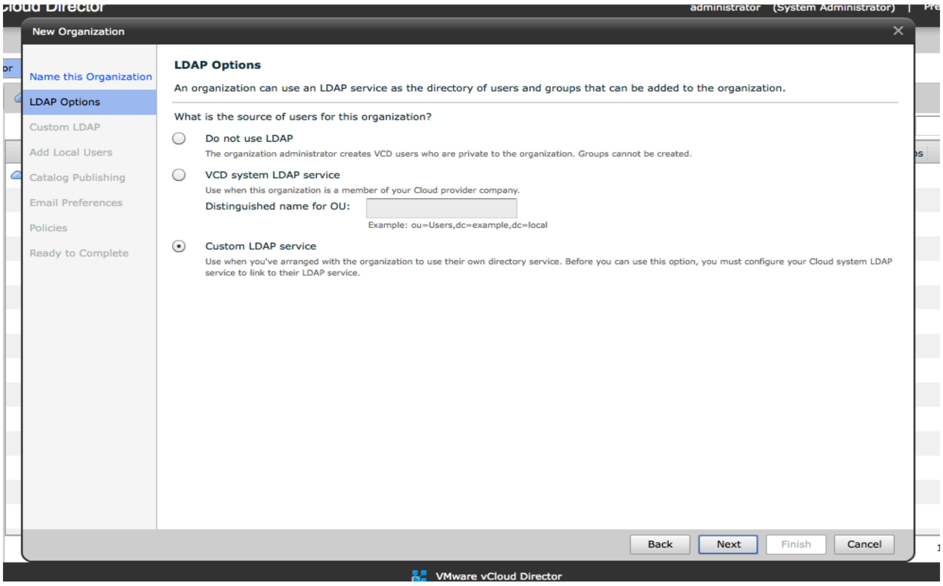
An organization can be internal to your company or accessible by a customer organization that is using your Cloud Director.

Organizations in vCloud have the ability to use an external LDAP server as an external directory and authentication methodology. We will use this feature to link VMWare vCloud to SecurePass and offer secure access to organizations and virtual datacenters (vDatacenter).

Configuring new Organizations

It is possible to specify an LDAP source during the creation of the Organization. Launch the Create a New Organization wizard from the VMware vCloud Director user interface home page and specify the name and description as you would with a standard vCloud Organization.

When the wizard asks for the LDAP Options, specify Custom LDAP service and click next as shown below.



LDAP Options

An organization can use an LDAP service as the directory of users and groups that can be added to the organization.

What is the source of users for this organization?

○ Do not use LDAP
The organization administrator creates VCD users who are private to the organization. Groups cannot be created.

○ VCD system LDAP service
Use when this organization is a member of your Cloud provider company.
Distinguished name for OU:
Example: ou=Users,dc=example,dc=local

● Custom LDAP service
Use when you've arranged with the organization to use their own directory service. Before you can use this option, you must configure your Cloud system LDAP service to link to their LDAP service.

On the Custom LDAP tab, proceed by filling the information on the Connection section.

Server

Enter the hostname of the nearest LDAP server to your datacenter, ex:" ldap2.secure-pass.net". For information on the nearest available server, please refer to the previous paragraph "LDAP in SecurePass"

Port

Specify 636, i.e. SSL based

Base distinguished name

Specify the Base DN as it appears in your LDAP option in the My Service section of SecurePass.

SSL

Click on Use SSL

SSL Certificate

Please provide the file "'gd_bundle.crt"' as downloaded from GoDaddy. To download the file, go to the GoDaddy repository as specified in "technical prerequisites" and select gd_bundle.crt

Authentication method

Specify simple

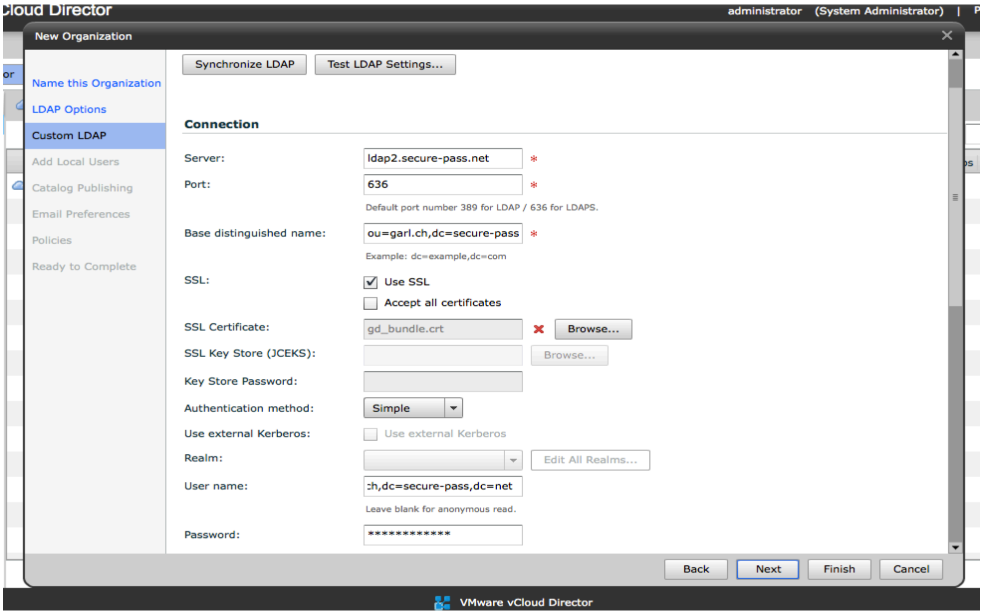
User name

Specify the LDAP user as it appears in your LDAP option in the My Service section of SecurePass.

Password

Specify the LDAP password as it appears in your LDAP option in the My Service section of SecurePass

Look at the screenshot below for an example.



Connection

Server: ldap2.secure-pass.net *

Port: 636 *

Default port number 389 for LDAP / 636 for LDAPS.

Base distinguished name: ou=garl.ch,dc=secure-pass *

Example: dc=example,dc=com

SSL: ☑ Use SSL

□ Accept all certificates

SSL Certificate: gd_bundle.crt

SSL Key Store (JCEKS):

Key Store Password:

Authentication method: Simple

Use external Kerberos: □ Use external Kerberos

Realm:

User name: :h,dc=secure-pass,dc=net

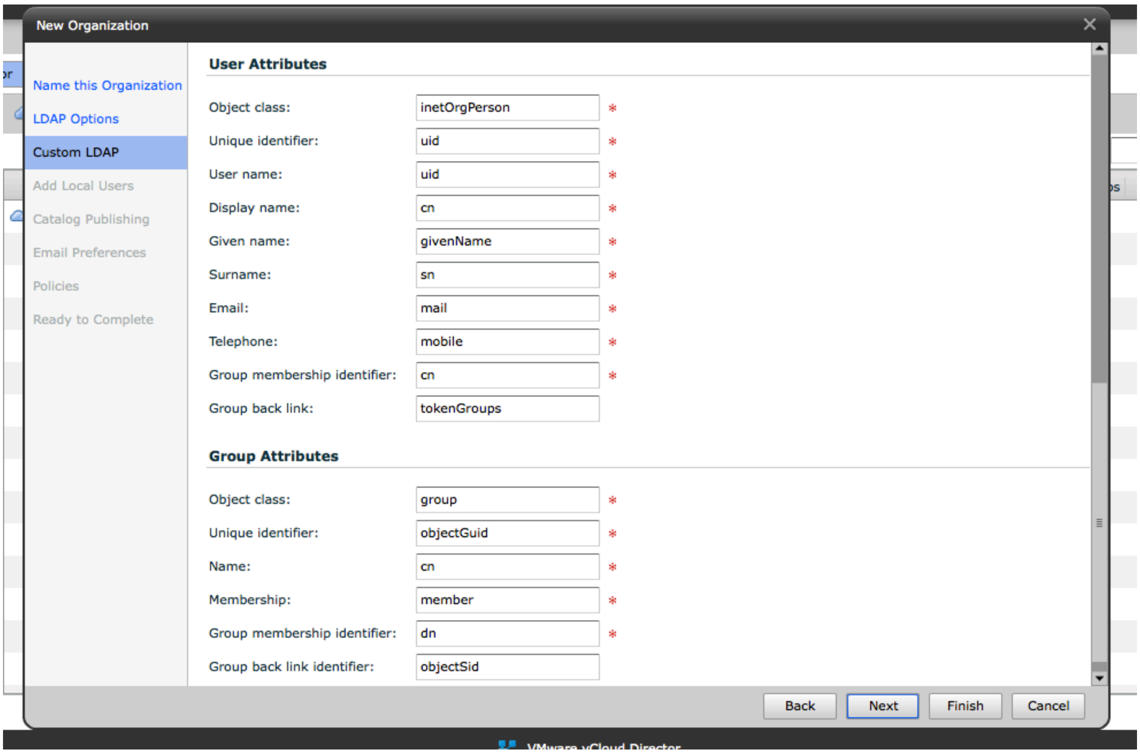
Leave blank for anonymous read.

Password: ************

Scroll down the page and fill in the User Attributes configuration as follows:

Object Class	inetOrgPerson
Unique identifier	uid
User name	uid
Display name	cn
Given name	givenName
Surname	sn
Email	mail
Telephone	mobile
Group membership identifier	cn

Please leave Group Attributes as it is, as groups are currently not implemented in SecurePass. Check again this page from time to time as it may change in the near future.



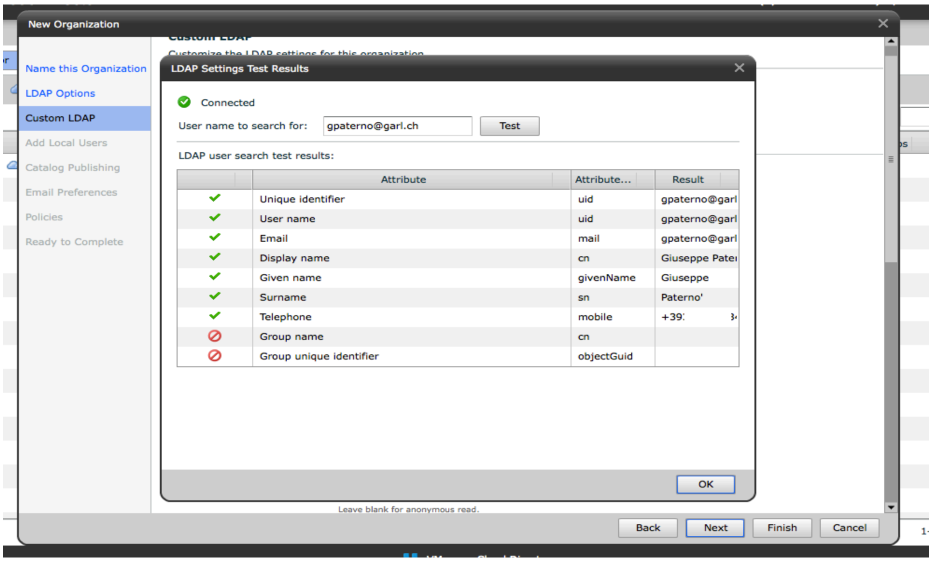
User Attributes

Object class:	inetOrgPerson *
Unique identifier:	uid *
User name:	uid *
Display name:	cn *
Given name:	givenName *
Surname:	sn *
Email:	mail *
Telephone:	mobile *
Group membership identifier:	cn *
Group back link:	tokenGroups

Group Attributes

Object class:	group *
Unique identifier:	objectGuid *
Name:	cn *
Membership:	member *
Group membership identifier:	dn *
Group back link identifier:	objectSid

Press the Test LDAP Settings button and try to search for an existing user. Please note that the user has the full user@domain notation, as for the example below. If it does not work, please check that the vCloud Director has the permission to access external LDAPS through a firewall and that the LDAP settings are the ones reported in the My Service section of SecurePass admin interface.



LDAP Settings Test Results

✓ Connected

User name to search for: gpaterno@garl.ch [Test]

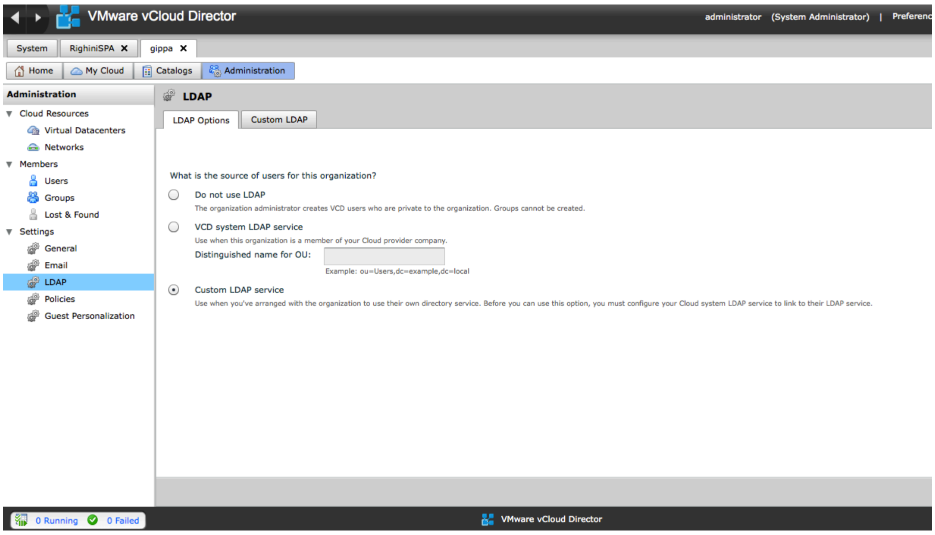
LDAP user search test results:

	Attribute	Attribute...	Result
✓	Unique identifier	uid	gpaterno@garl
✓	User name	uid	gpaterno@garl
✓	Email	mail	gpaterno@garl
✓	Display name	cn	Giuseppe Pater
✓	Given name	givenName	Giuseppe
✓	Surname	sn	Paterno'
✓	Telephone	mobile	+39: 3
⊘	Group name	cn	
⊘	Group unique identifier	objectGuid	

Configuring existing Organizations

It is possible to link an Organization to SecurePass after its creation. Go to the organization properties or select Administration->Settings->LDAP as per the screenshot below.

In the LDAP Options tab, please specify Custom LDAP service



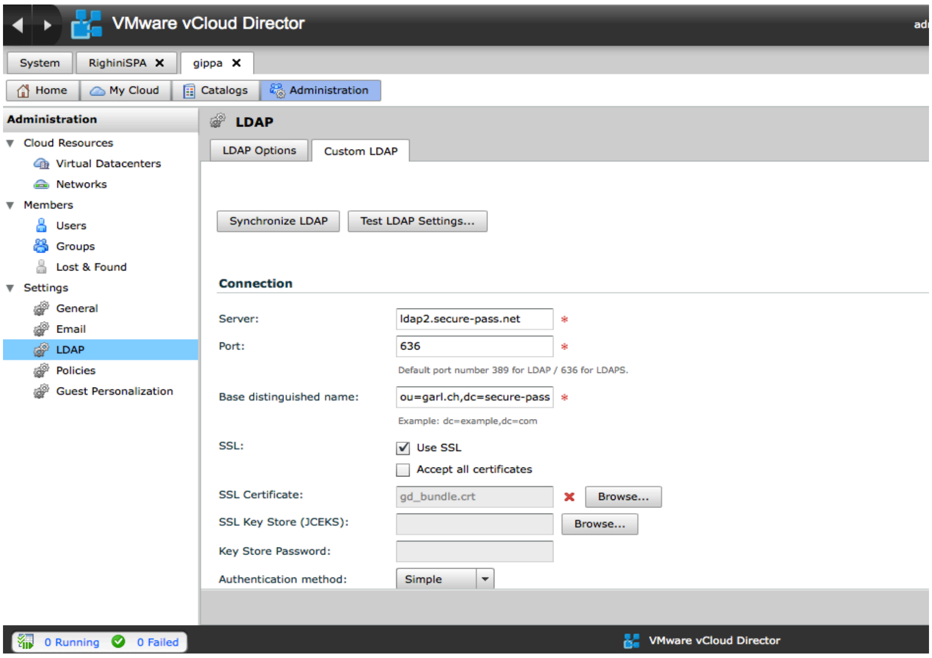
What is the source of users for this organization?

○ Do not use LDAP
The organization administrator creates VCD users who are private to the organization. Groups cannot be created.

○ VCD system LDAP service
Use when this organization is a member of your Cloud provider company.
Distinguished name for OU:
Example: ou=Users,dc=example,dc=local

● Custom LDAP service
Use when you've arranged with the organization to use their own directory service. Before you can use this option, you must configure your Cloud system LDAP service to link to their LDAP service.

In the Custom LDAP tab, please specify all the settings as described in the previous section Configuring new Organizations.



Server: ldap2.secure-pass.net *

Port: 636 *

Default port number 389 for LDAP / 636 for LDAPS.

Base distinguished name: ou=garl.ch,dc=secure-pass *

Example: dc=example,dc=com

SSL: ☑ Use SSL

☐ Accept all certificates

SSL Certificate: gd_bundle.crt

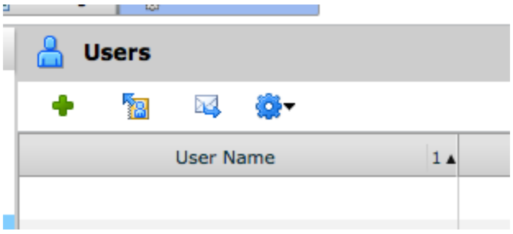
SSL Key Store (JCEKS):

Key Store Password:

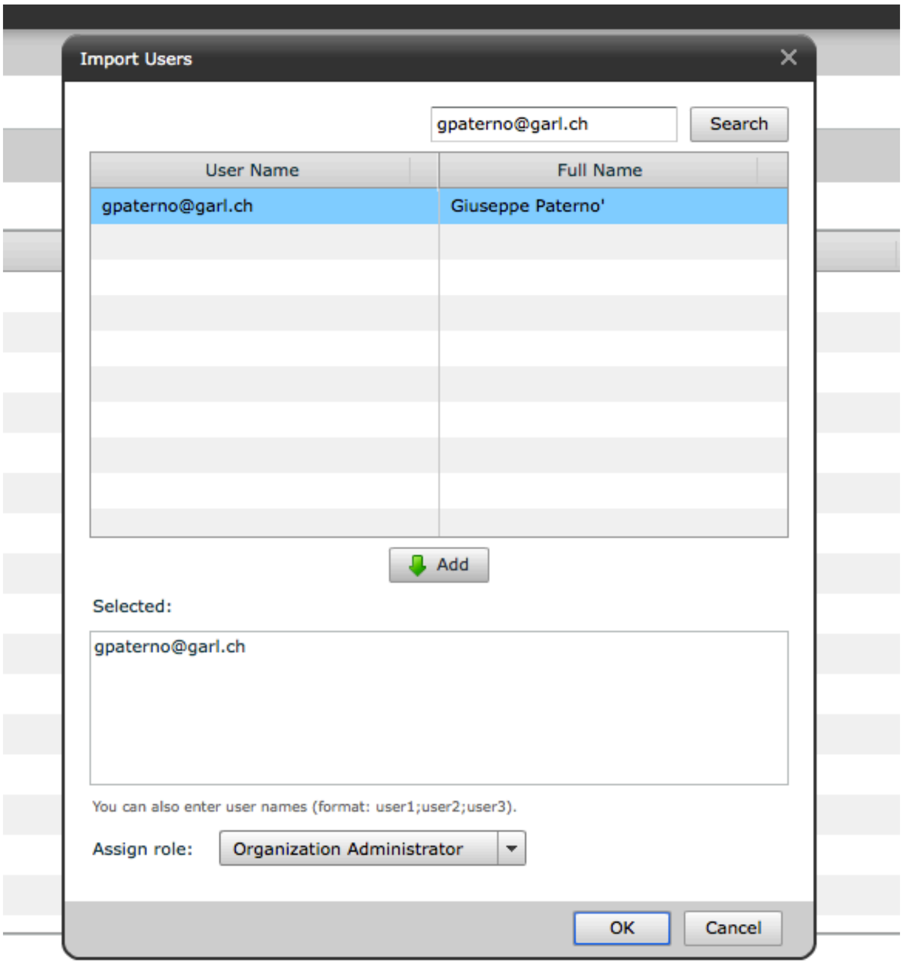
Authentication method: Simple

Importing Users

You now need to import users from SecurePass and assign them a role. Go to Administration->Members->Users and click Import Users from LDAP, the second icon from the left.



Search for a user. If you do not know the username, just click the Search button, or fill in the username and click on Search. Once you find the name, click on its record and press the Add button. Finally, assign the appropriate role as per the example below.



Import Users

gpaterno@garl.ch

User Name	Full Name
gpaterno@garl.ch	Giuseppe Paterno'

Selected:

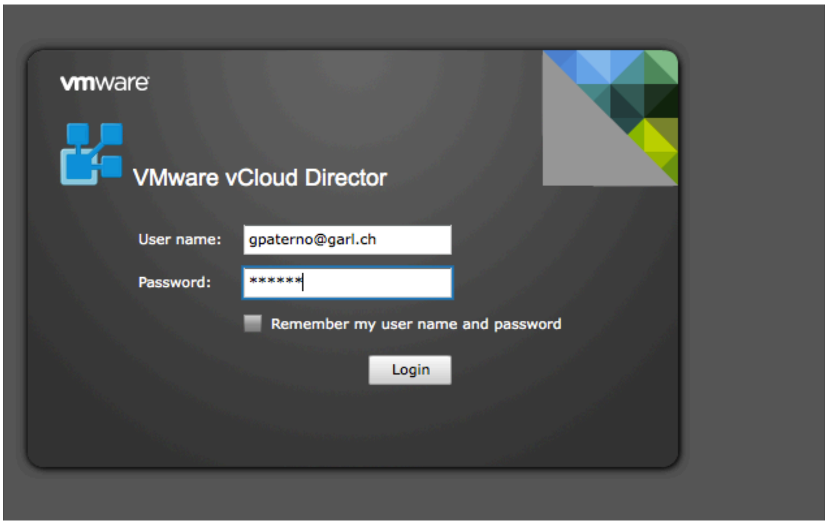
gpaterno@garl.ch

You can also enter user names (format: user1;user2;user3).

Assign role: Organization Administrator

Logging in

Once you have completed all the steps above, you are ready to login to your organization with the current SecurePass One Time Password and the optional PIN.



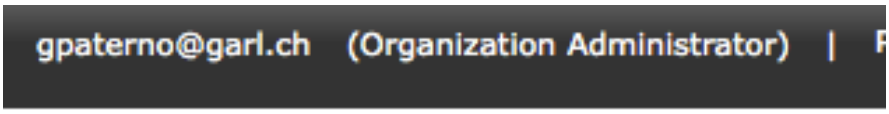
User name: gpaterno@garl.ch

Password: ******

□ Remember my user name and password

Open your organization URL, for example https://vcloud.domain/cloud/org/example, and use your full username in the form of user@domain as the example below.

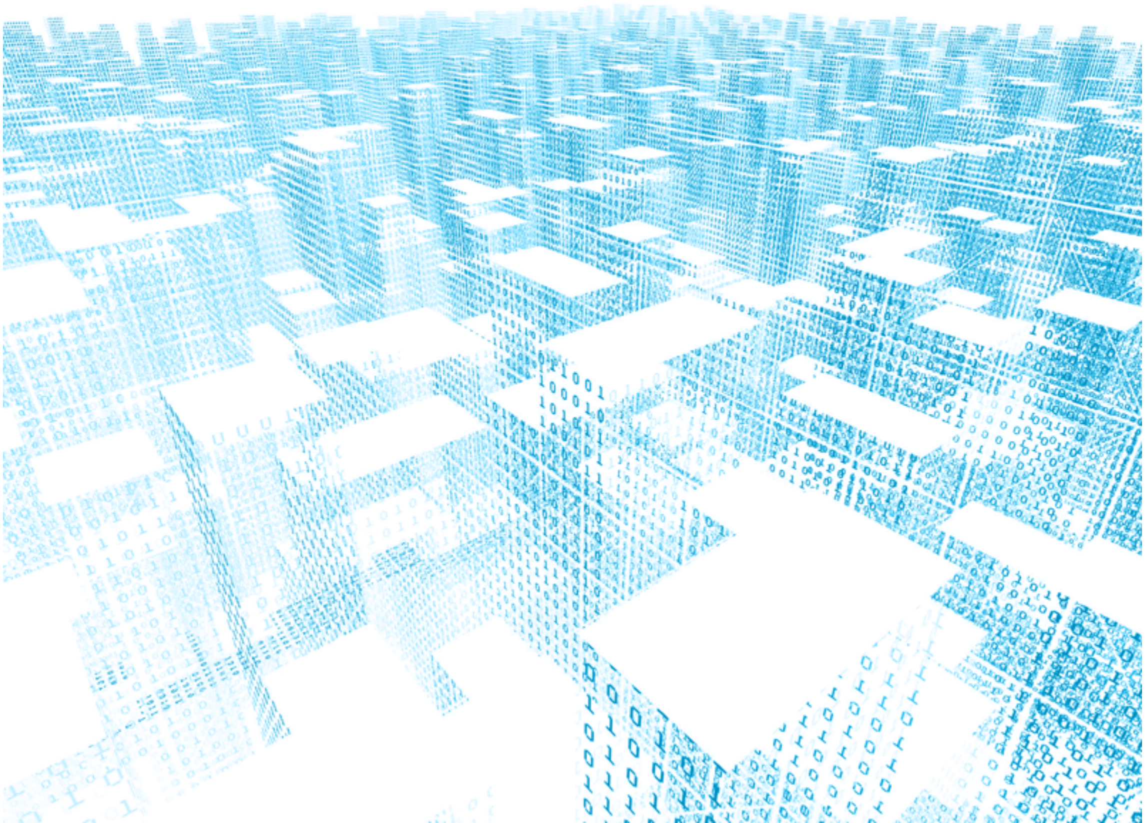
If everything is set up correctly, you will be able to login using SecurePass. Your SecurePass username will be displayed in the upper-right corner with your role as for the example below.



gpaterno@garl.ch (Organization Administrator) |

6 Conclusions

Companies that embraced vCloud, such as Cloud Providers and large IT organizations, can offer secure access to vDatacenters without any additional effort and, more importantly, without paying additional money upfront, as SecurePass is a pay as you use service.



Appendix: Creative common license

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

1. "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.
2. "Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined above) for the purposes of this License.
3. "Distribute" means to make available to the public the original and copies of the Work through sale or other transfer of ownership.
4. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.
5. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.
6. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.
7. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.
8. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by

any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

9. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

2. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

1. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections; and,
2. to Distribute and Publicly Perform the Work including as incorporated in Collections.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Adaptations. Subject to 8(f), all rights not expressly granted by Licensor are hereby reserved, including but not limited to the rights set forth in Section 4(d).

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

1. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the Uniform Resource Identifier (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested.
2. You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.
3. If You Distribute, or Publicly Perform the Work or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Collection, at a minimum such credit will appear, if a credit for all contributing authors of Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.
4. For the avoidance of doubt:
   a. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;

   b. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License if Your exercise of such rights is for a purpose or use which is otherwise than noncommercial as permitted under Section 4(b) and otherwise waives the right to collect royalties through any statutory or compulsory licensing scheme; and,
   c. Voluntary License Schemes. The Licensor reserves the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License that is for a purpose or use which is otherwise than noncommercial as permitted under Section 4(b).

5. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

1. This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.
2. Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

1. Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.
2. If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
3. No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
4. This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.
5. The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law

includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.