Table of Content

Table of Content	1
Contact form 1	5
1. Introduction	5
Start a Trial	5
Introduction	5
Getting Started	8
Implementation Guide	8
Why Use LastPass Enterprise?	9
Importing Existing Data into LastPass	10
Link Personal Account	12
How is LastPass safe?	14
Locally encrypted sensitive data	14
Government-level encryption	14
Only your users know the key to decrypt their data	14
Control your policies	14
No more using your browser's insecure password manager	14
System Requirements	14
Notes on Google Chrome	15
Implementation Guide	16
Implementation Guide	16
Phase I: Proof of Concept	16
Phase II: Enterprise-wide Roll Out	17
Migrate Data Between Accounts	17
Building a Business Case for LastPass Enterprise	18
Administrator Toolkit	19
2. Login to LastPass	21
Education Toolkit	21
Logos	21
Posters and Fliers	21
Email Resources	21
Social Graphics	21
Internal Communication Plan	22
Training Kit for End Users	23

'Table of Content'	'2/92'
The LastPass Training Kit for End Users	23
End User Survey (1 week prior to roll out)	24
Warm 'em up (2 days prior to roll out)	24
The Welcome Email	24
LastPass Experts	24
Add LastPass screencasts to your Training Modules	24
Review your progress Training Email and Self-beln Tool (48 hours after invite)	24
Review your progress (1 month after invite)	25
Training Tools	25
Online screencasts	25
Sample Survey	25
Password Questionnaire	25
Email Templates for End User Roll Out and Training	27
Email Templates for End User Roll Out & Training	27
The Admin Console	28
Reporting - Login Reports	29
Users Sub-tab	30
Set-Up Tab	31
Policies	32
Other Enterprise Options	33
Reporting - Shared Folders	36
Full List of Policies	37
Employee Welcome Emails	37
Reporting - Admin Events	38
Create New User	39
Windows Login Integration	40
LastPass Active Directory/LDAP	41
When a user profile is Created:	43
When a user profile is $ heta$ Deleted:	44
When a user profile is Disabled:	44
When a user profile is removed from the group in filter:	44
User Groups - for Policies and Shared Folders	48
Install Software	49
OPTION A: Manual Installation Using the GUI Install Wizard	49
OPTION B: Silent Installation From an Administrative Command Prompt	49
OPTION C: Install MSI File Using GPO (Group Policy Object)	50

'Table of Content'	'3/92'
LastPass Provisioning API	51
Users Tab	53
Reporting - Notifications	53
Push Sites to Users	54
Pending Users (Only for Active Directory Sync Client Users)	56
Reporting	57
LastPass Single Sign-on for Applications that Support SAML	60
Setup	64
Policies Tab	64
Other Enterprise Policy Options	64
Create New User	64
Install Software	65
SAML	65
Login Reports	65
Shared Folders	65
Admin Events	65
Notifications	65
Shared Folders	65
Multiple Permissions	68
Terminating User Accounts from Your Enterprise	72
Shared Folders with Users Outside your Enterprise	73
LastPass for Applications	73
LastPass App for Mac	73
Mobile Apps	74
Multifactor Authentication	74
LastPass Sesame	75
YubiKey	77
Duo Security	81
Google Authenticator	84
Toopher	86
RSA SecurID	87
Configure LastPass Enterprise for RSA SecurID Authentication	89
Certification Test Checklist for KSA Authentication Manager	91 01
TOA GEGUND Manualory Eurolionanty	JI

'Table of Content'	'4/92'
Full List of Policies	92
Multifactor Authentication	92
Site Map	92

Contact form 1

Your Name (required)

[text* your-name]

Your Email (required)

[email* your-email]

Subject

[text your-subject]

Your Message

[textarea your-message]

[submit "Send"]

[your-subject] [your-name] From: [your-name] <[your-email]> Subject: [your-subject]

Message Body: [your-message]

This e-mail was sent from a contact form on Enterprise Manual (https://enterprise.lastpass.com) support@lastpass.com Reply-To: [your-email]

0 0

[your-subject] Enterprise Manual Message Body: [your-message]

This e-mail was sent from a contact form on Enterprise Manual (https://enterprise.lastpass.com) [your-email] Reply-To: support@lastpass.com

0

0 Your message was sent successfully. Thanks. Failed to send your message. Please try later or contact the administrator by another method. Validation errors occurred. Please confirm the fields and submit it again. Failed to send your message. Please try later or contact the administrator by another method. Please accept the terms to proceed. Please fill in the required field. This input is too long. This input is too short.

1. Introduction

Start a Trial

Introduction

[accordion openfirst=false scroll=true clicktoclose=true]



The LastPass Enterprise Admin Manual is a comprehensive guide to the administration of LastPass Enterprise.

[tabbed_section]

[tab title="What is LastPass Enterprise?" id="t1"]

LastPass Enterprise offers your employees and admins a single, unified experience that combines the power of SAML SSO coupled with enterprise-class password vaulting. LastPass is your first line of defense in the battle to protect your digital assets from the significant risks associated with employee password re-use and phishing.

[/tab]

[tab title="Deployment" id="t2"]

LastPass Enterprise is deployed in days. It automatically 'Learns' and 'Remembers' usernames and passwords for virtually all online websites and Windows applications. It provides universal access to resources, seamlessly synchronizing passwords across all platforms and browsers. Deployed on the desktop and in the cloud, your employees will love using the powerful, intuitive features and readily adopt. Your employees can familiarize themselves with LastPass' features by using our LastPass Manual.

[/tab]

[tab title="Admin Console" id="t3"]

The Enterprise Console allows your System Administrators to install and upgrade your installation, manage policies, user configurations, applications, authentication methods and user groups. It provides centralized reporting for auditing and compliance and automated user alerts for optimizing use of the tool.

[/tab]

[/tabbed_section]

[accordion-item title="Not Just Websites: SAML SSO" id="h1"]

LastPass Enterprise supports SAML SSO for all of your essential cloud-based applications. Seamlessly onboard new users with automated provisioning and termination through our SAML dashboard.

[/accordion-item]

[accordion-item title="Education and Outreach" id="h3"]

LastPass gives you the tools and guidance that you need to ensure a seamless launch, grateful employees, and a happy boss. Our turnkey program includes a step-by-step Training Kit for the initial product intro, individual and aggregate Security Scores to measure the impact of the program, and a status summary report (coupled with email templates) to identify (and easily act on) education opportunities among your users.

[/accordion-item]

[accordion-item title="Sharing" id="h4"]

The sharing of login data is impossible to avoid in many cases. The problem with sharing is that you lose accountability. With LastPass Shared Folders, administrators can easily share credentials for a single website or for a group of sites while retaining the ability to tie activity back to the individual user. Password updates automatically and seamlessly propagate to all assigned users eliminating lock-out caused by version control issues.

[/accordion-item]

[accordion-item title="Admin Access to User Accounts" id="h5"]

In its default state, LastPass Administrators cannot access any data �stored in an employee's LastPass account. However, there are some exceptions: (1) the end user can explicitly share data with an Administrator via an individual share or a Shared Folder, or (2) the company can choose to enable either or both of the Super Admin Policies defined here https://lastpass.com/policy_doc.php. When the Super Admin Policies are enabled, a notification is sent automatically to every LastPass Admin in the Enterprise.

[/accordion-item]

[accordion-item title="Integration" id="h6"]

Already deployed SSO or Active Directory? You can use LastPass for web logins to improve productivity logging in to apps locally, or to handle apps that haven't been integrated into your SSO/Active Directory. Many implementations require minor changes for each application to specify domain or other settings that confuse users -- LastPass resolves those issues.

[/accordion-item]

[accordion-item title="Deployment" id="h7"]

LastPass supports command line install and updates. For the automated provisioning and termination of LastPass user accounts, clients can choose between: Active Directly Sync client, Windows Login Integration, or an open API. Clients looking for less automation can simply add users manually in the Enterprise Console and LastPass will take it from there with our automated welcome emails. If you need something custom to make deployment easier, let us know, we're here to help.

[/accordion-item]

[accordion-item title="Synchronization" id="h8"]

A Web 2.0 cloud based approach allows a mobile workforce seamless access to their accounts on any computer or mobile device from any location.

[/accordion-item]

[accordion-item title="Policies" id="h9"]

Enforce site-wide policies on password strength, security features and password expiration.

[/accordion-item]

[accordion-item title="Administration" id="h10"]

Employee accounts can be instantly disabled when employees leave the organization.

[/accordion-item]

[accordion-item title="Reporting" id="h11"]

Administrators can view historical data and can audit employee logins and accesses.

[/accordion-item]

[accordion-item title="Authentication" id="h12"]

Multifactor authentication offering increased security.

[/accordion-item]

[accordion-item title="Security & Privacy Is Our Priority" id="h13"]

We've taken every step we can think of to ensure your security and privacy. Using an evolved host-proof hosted solution, LastPass employs localized, government-level encryption (256-bit AES implemented in C++ and JavaScript) and local one-way salted hashes to give you complete security with the go-anywhere convenience of syncing through the cloud. All encrypting and decrypting happens on your computer - no one at LastPass can ever access your sensitive corporate data. The LastPass *****Security Challenge also allows your users to identify weak account data and provides suggestions for significantly improving online security.

[/accordion-item]

LastPass Sentry alerts your users the instant their username is found in a global database of breached accounts.

[/accordion-item] [/accordion]

Getting Started

[accordion openfirst=false scroll=true clicktoclose=true]

Getting started with LastPass Enterprise is easy, starting off with a free 14-day trial. Simply sign up for a **LastPass account** and complete the **Enterprise Trial Request Form**. Once this form is filled out, the Enterprise features will automatically be activated on the account in question and can include up to 10 individuals from your organization.

[accordion-item title="Getting Started Implementation Guide" id="0"]

Implementation Guide

Click here for a step by step guide to implementing LastPass Enterprise: Implementation Guide.

[/accordion-item] [accordion-item title="Choosing which LastPass Account to Use" id="1"]

'Enterprise' is a set of features that can be activated on any new or existing account. New Enterprise users often wonder whether to use their existing personal account, or to **create a new account** for professional purposes. Here are the options:

- Using separate accounts for personal and professional use. This is the only way to ensure that you will never lose your personal data if/when you leave the enterprise. For a more seamless experience, you can link the two accounts behind your single enterprise login. If you do choose to link your personal account, it is important to note that the logins from your personal account will never be reported in the Enterprise logs. Once you have linked a personal account, you can migrate entries from your personal account to your enterprise account. We highly recommend you use this approach.
- 2. The other option is to use a single account for both personal and professional data. This approach will ultimately give your employer control over the termination of the account, and we do not recommend this approach in most cases. The administrator of the account has the ability to 'remove user from company', which allows you to preserve your data and to continue using LastPass as a standard user. But they can also 'delete' the account, which will delete the account in its entirety including all personal logins that you may have saved.

[/accordion-item] [accordion-item title="Adding Users to Your Trial" id="2"]

Once you are in trial, you can invite other employees to the trial by email. After logging into the Admin Console, please click on Setup >> Create New User and enter in the email addresses of the employees you wish to invite.

An account will be created for them with a temporary password. They will receive a welcome email with instructions on how to reset their password and get started. If the user's email address is already associated with a LastPass account, they will be sent an

email with an activation URL.

[/accordion-item] [accordion-item title="Purchasing LastPass Enterprise" id="3"]

You must be in a trial or an active Enterprise customer in order to purchase LastPass Enterprise licenses. You can make your purchase using the purchase link found on the **Admin Console Dashboard home page**. Any additional purchases made throughout the year will be pro-rated for just a single annual renewal.

[/accordion-item] [/accordion]

Why Use LastPass Enterprise?

[accordion openfirst=false scroll=true clicktoclose=true]

Designed and built from the ground up by an experienced team of highly-talented developers, LastPass Enterprise finally delivers on the long-desired -- but rarely delivered -- promise of Enterprise SSO. LastPass Enterprise brings a new technical approach to Single Sign-On, designed and delivered the way YOU have always envisioned it.

[accordion-item title="For End Users" id="h1"]

- Dramatically improves end user experience and daily work-flow: they'll love using it
- Avoids need and frustration of having to contact help desk for password and access problems
- Eliminates negative fallout of 'password fatigue'
- Allows access from all the computers and devices they use: Windows, Mac, Linux. Every smart phone is supported too

[/accordion-item] [accordion-item title="For Help Desk" id="h2"]

- · Saves wasted time and money by not having to focus on costly repetitive resets
- · Allows staff to focus on higher-level, more intricate IT support needs

[/accordion-item] [accordion-item title="For System Administrators" id="h3"]

- Quick and easy setup, deployment, and ongoing management
- $\circ~$ Management console for both enterprise password management and reporting
- Software as a Service (SaaS) Host-proof hosted implementation provides great security without the inconvenience of another system to maintain.

[/accordion-item]

[accordion-item title="For CISO, CIO, CTO, and IT Managers" id="h4"]

- No time-consuming and costly consulting expenses just to set up, configure, and deploy
- Avoids the hidden costs of a delay in solving 'password fatigue'
- Strong, more secure password policies can now be easily enforced without the unintended consequences of 'password fatigue'
- · Overall enterprise security improved
- Allows the greater security of multi-factor authentication while improving productivity

[/accordion-item] [accordion-item title="For SVP Sales and SVP Operations" id="h5"]

- Many knowledge workers have between 20-100 passwords they use every day: now these high-value, power users can be that much more productive and happy
- A much more productive division
- Your sales force works on the run, make it easier for them to be more productive on the device they use most: their mobile phone.

[/accordion-item] [accordion-item title="For CEO" id="h6"]

- Reduces the worry, probability, and costly public fallout of a major security breach
- Actually delivers on the usually-elusive promise of E-SSO
- Improves the Bottom Line

[/accordion-item] [/accordion]

Importing Existing Data into LastPass

[accordion openfirst=false scroll=true clicktoclose=true]

Once you have installed LastPass, you may need to import your existing password entries and secure data from another LastPass account or from another password manager or file format. To do so, follow the instructions below.

[accordion-item title="Importing using pre-established formats" id="1"]

To begin, click on the LastPass Icon, click the Tools submenu, and click Import:



You will then be presented with a submenu for the Google Chrome Password Manager and �Other�. Selecting Other will open a new page with a drop-down list of options for all support import options:



Security Check	
Identities (AII)	•
Open Favorites	
About	
Advanced Tools	•
Import From	h
Import From	-
Print	•
Print Add Site	•
Print Add Site Save All Entered Data	•
Print Add Site Save All Entered Data Add Secure Note	•

We continue to add formats and password managers to the list of supported import option, so check the version of LastPass you are running if you do not see the format you need.

Since importing from each password manager is different, we have provided instructions for each under the name. Simply follow the instructions that we provide for the specific password manager that you use.

After importing, you can then begin to organize your sites into **Folders** as well as delete unnecessary or duplicate sites.

[/accordion-item]

[accordion-item title="Importing from a Generic CSV File" id="2"]

If LastPass does not support importing from your current password manager, you may be able to import using a Generic CSV (comma separated value) file. Try seeing if your current password manager has an option to export to a CSV file.

To import data from a CSV file, we suggest you use our Import Template found here: **Sample Import Spreadsheet**.

If you use your own spreadsheet instead, it is important that the title of the columns match those in the template! The column titles can include any of the following: url, username, password, extra, name, grouping, type, hostname.

Fill the columns with the values you'd like for each entry (leave blank if the value is not relevant). Please note that 'extra' means either (1) the notes section of a site entry or (2) the body of a secure note, and 'grouping' is the group (or folder) where you would like the item to be stored in your vault.

[tabbed_section]

[tab title="Importing Sites"]

To import Site data you must define at least the following values: Ψ url Ψ (typically this will be the login url), Ψ username Ψ , Ψ password Ψ and Ψ name Ψ . Ψ Extra Ψ and Ψ Group Ψ are other fields that you might consider.

[/tab]

[tab title="Importing Secure Notes"]

To import data as a generic Secure Note, enter the values as follows: ψ url ψ = http://sn, ψ extra ψ = the contents of the note. Give the note a ψ name ψ , and then consider adding ψ group ψ . It is important to leave the username and password columns blank.

[/tab]

[tab title="Importing Server Login Credentials"]

To import data as a Server Secure Note, enter the values as follows: vll = http://sn, vtype = server. You must also populate vhostname, vusername, vpasswordand vhame. In this case, you must enter the username and password in the actual username and password columns of the template, rather than the 'extra' section. Consider adding vgroup.

Please click here to download our **Sample Import Spreadsheet**, which includes examples of all 3 of the aforementioned data types.



F	a Cut i Gopy Paste ✓ Format Paint Clipboard	er G	Calibri	× 11 × A A V		Wrap Text	General \$ * % ; Number	▼ 00.00 00.€	Conditiona Formatting	Format Cell as Table × Styles × Styles
	L25	- (• f _x	···)(,	,		
	A		В	С	D	E	F		G	Н
1	url	typ	e	username	password	hostname	extra	name		folder
2	http://sn	ser	ver	server1username	server1password	server1hostname		Server	1	Server Group A
3	http://sn						Adt349fme	Guest	wireless ke	Sys Admins
4	http://community	.spi	ceworks.com/	sysadmins@acme	spiceworkspasswo	ord	confidential	Spicew	orks Admir	Sys Admins
5										

[/tab]

[/tabbed_section] [/accordion-item] [accordion-item title="Passive Imports" id="3"]

Certain password managers simply do not support export functions. In these cases you can still use LastPass to pick up this data through a 'passive' import. This entails running both password managers simultaneously, having your former password manager enter your login credentials into a site, and then using LastPass to pick up the filled website entry.

[/accordion-item]

[accordion-item title="Importing into Shared Folder" id="4"]

Please note that importing into shared folders is currently not supported. If the name of a shared folder is listed in your CSV file, you will encounter an error upon attempting to import into your LastPass Vault. Once you import your credentials, rather than moving them from the general folder to the shared folder in batches of 10 (the limit for drag and drop), simply right click and @rename@ the regular folder with the name of the Shared Folder where you would like them to go. Please note you will have to pre-create the Shared Folder before using this method to move sites.

[/accordion-item] [/accordion]

Link Personal Account

[accordion openfirst=false scroll=true clicktoclose=true]

The Link Personal Account option now allows LastPass Enterprise users to link their Personal LastPass Accounts with their Enterprise Accounts. This enables users to access their personal LastPass entries while using their Enterprise Account, all while keeping the two accounts separate.

[accordion-item title="Setting Up Your Linked Account" id="h1"]

To set up a Linked Personal Account, log in to the LastPass browser extension with your Enterprise credentials. O to the LastPass Plug-In Icon -> My LastPass Vault, and click on the "Link Personal Account" link on the left-hand actions menu. Follow the prompts.



Shared-SAML

- Once linked, the user's personal account will appear in their Enterprise Account as a separate folder in the account under the personal username/email address.
- The data that is stored in a linked personal account is entirely the property of the end user, not the Enterprise. There is no circumstance under which an Enterprise Admin can access any data in a user's linked personal account. No login events from the personal linked account will belogged in the Enterprise reporting. Upon termination of the Enterprise account, the user's Personal account will remain intert and untouched, and available for continued use by the employee.
- This personal folder is treated as a Shared Folder between the Enterprise Account and Personal Account, and is subject to the same restrictions and properties that a Shared Folder is limited to. These restrictions can be read about at the Shared Folders page.
- Data can be moved from the Personal Linked Account Folder to the Enterprise Folder, and vice versa. Click here to learn more about migrating data between accounts.

[/accordion-item] [accordion-item title="Unlinking the Accounts" id="h2"]

If at anytime you wish to unlink a personal account from an Enterprise account, you can do it two ways:

1. From within the Enterprise Account: �Vault > Left menu > Remove Linked�Personal Account



2. From the personal account: Vault > Account Settings > Show Advanced Settings > Unlink Account From Enterprise

Tools	
Remove Duplicates	Remove Duplicates
Unlink Account	Unlink Account From Enterprise
	Hide Advanced Settings Update

3. If an Admin uses the policy **Super Admin Master Password reset** on the account, the Personal account will automatically unlink.

How is LastPass safe?

[accordion openfirst=true scroll=true clicktoclose=false]

Your security and privacy are our top priority - that's why we've taken every step possible to ensure that your data is safely stored and synced in your LastPass account.

Locally encrypted sensitive data

All encryption/decryption occurs locally on the user's device, not on our servers. This means that your sensitive data does not travel over the Internet and never touches our servers, only the encrypted data does.

Government-level encryption

We use the same encryption algorithm that the U.S. Government uses for top-secret data. Your encrypted data is meaningless to us and to everyone else without the decryption key (your emails and Master Password combinations).

Only your users know the key to decrypt their data

Your encryption keys are created from your users' email addresses and Master Passwords. The Master Passwords are never sent to LastPass - only a one-way hash of your password when authenticating - which means that the components that make up your keys remain local to your users. LastPass also offers configurable corporate policies that let you add more layers of protection.

Control your policies

We know that one size does not fit all when balancing corporate security and ease of use. That's why we allow you to define your preferences by providing a full range of configurable corporate policies. We strongly encourage you to review the policy options prior to rolling out LastPass across your organization.

Generate unique, strong passwords

No more using the same password for all sites. No more writing down passwords on little pieces of paper. No more emailing yourself when you forget your password. With the LastPass **\$password generator** users can create strong passwords for each site and automatically save them to their individual vault. With LastPass, your data will be safer online than ever before without the hassle of remembering unique passwords.

No more using your browser's insecure password manager

Any malicious application can easily retrieve saved passwords from your users' browsers. With LastPass, you're protecting vyour users from these attacks!

Learn more about protecting yourself from phishing scams

[/accordion]

System Requirements

[accordion openfirst=true scroll=true clicktoclose=false]

LastPass supports the below web browsers, operating systems and mobile devices.

[tabbed_section] [tab title="Operating Systems" id="t0"]

- Windows XP
- Windows Vista
- Windows 7

- Windows 8.1
- Windows 10
- Mac OS X 10.7+
- Linux

[/tab]

[tab title="Web Browsers" id="t1"]

- Internet Explorer 8+
- Firefox 3+
- ∘ Safari�5.1+
- Google Chrome 18+
- Opera 11+
- IE Tab in Firefox (using IE Anywhere Premium Feature)

[/tab] [tab title="Mobile Devices" id="t2"]

- iPhone and iPad with iOS 7+
- Blackberry OS 4.2.1+
- Android 2.2+
- Windows Phone
- Dolphin browser

[/tab]

[tab title="Previous Platforms" id="t3"]

We have previously built versions of LastPass for platforms that we no longer develop for. Ψ Users are welcome to install and use them, but we cannot offer technical support for these versions.

- Windows Mobile 5+
- Symbian S60 3rd+
- Palm webOS

Users are strongly recommended to download and run the installer from our **website** on all browsers you regularly use.

[/tab] [/tabbed_section] [/accordion]

Notes on Google Chrome

[accordion openfirst=true scroll=true clicktoclose=true] [accordion-item title="Disabling Chrome's Password Manager" id="h0"]

It is recommended that you disable Chrome's built-in password manager by clicking on the Chrome menu >> Settings:

Ŷ

🔶 🔿 🖸 🗋	chrome://settings		
Chrome	Settings		Search settings
History	Sign in		
Extensions	Signed in as	Manage your synced data on <u>Google Dashboard</u> .	

Pass Eni	erprise Manual	16/5
Settings	Disconnect your Google Account Advanced sync settings	
About	On startup	
About	Open the New Tab page	
	Continue where you left off	
	Open a specific page or set of pages. Set pages	
Then scro	II down to select 'Show advanced settings' > Passwords and forms	
<u>^</u>		
¢.		
Se	ttings _ Do Not Track' request with your browsing traffic	
Pa	sswords and forms	
	Enable Autofill to fill out web forms in a single click. Manage Autofill settings	
	Offer to save your web passwords. Manage passwords	
And make	sure these options have been wunchecked.	
lf you wer	a proviously using Chromo's password manager, the installer will also help	
you impor	t your stored Google Chrome passwords into LastPass. The installer can be	
found at 🕫	https://lastpass.com/download.php	
lf vou con	tinue to actively participate in Chrome's Beta and dey builds, you may find	
that LastP	ass runs into occasional oproblems. Contact LastPass Support with any	
suspected	runctionality issues.	
/accordion-ite	m]	
accordion-iter	n title="Known Limitations" id="h1"]	
 Chrome had dialogs. 	as limited support for saving logins for sites with basic authentication You are able to save these logins in Firefox, and then Chrome will be able to	
AutoFill th	ese logins. If you'd like to help us work towards resolving this issue of saving	
access to	D HTTP AUTH window, Basic Auth window from Extension	
[/accordion-ite	m]	
/accordion]		
imple	mentation Guide	

Implementation Guide

***Every implementation of LastPass is different based on your unique environment and program goals. This article&serves&as a high level guide for&some of the features and options you might consider when implementing LastPass Enterprise.&

Phase I: Proof of Concept

- Follow the prompts and submit LastPass Trial Request Form to initiate a free, 14day trial including up to 10 staff members.
- Weigh provisioning options and software installation options, and determine best path for your enterprise.
- 3. Review the policy options and determine relevance for your enterprise.

- Create at least 5 beta test accounts from the 'create new users' tab of the Admin Console.
- Populate the beta accounts with top sites and applications utilized by your employees. Test all logins to make sure that they are functioning seamlessly.
- Determine who will need Admin rights within your enterprise and assign them from the Users tab of the Admin Console. Conduct Admin training as necessary.
- Determine if cloud-based Single Sign-on (using SAML) is needed/wanted. Advise your LastPass representative if support is needed for any new applications not already available. Integrate and test the desired applications.
- 8. For larger implementations, consider training one or more internal helpdesk contact(s) for end user support.
- 9. For larger implementations, determine how much education/tutorials you intend to push out to your staff. Most enterprises send only the welcome email.
- For larger implementations, consider customizing the welcome email to include internal helpdesk contact.
- Review the automated user notification options found here. These notifications are very important for driving adoption and for optimizing employee use of the service to improve the safety or your corporate data.

Phase II: Enterprise-wide Roll Out

- 1. For larger implementations, download the software to all work stations.
- 2. Purchase your LastPass licenses.
- 3. Provision all users, or provision in batches, per your preference. If using the Sync Client with Opending users configuration, then go to the Opending users page to Opending users for whom you would like accounts to be provisioned.
- Determine if any new users should be granted LastPass Admin rights. If so, assign them from the Users tab of the Admin Console. Conduct Admin training as necessary.
- 5. **Create User Groups** to help facilitate the assignment of policies and/or Shared Folders.
- 6. If using cloud-based Single Sign-on (using SAML), activate the desired groups/apps.
- 8. Owners assign Shared Folders to the appropriate users/groups.
- 9. Report any bugs or enhancement requests to LastPass using the ticket system.
- See the LastPass Training Kit for End Users for suggested training program and resources.

Migrate Data Between Accounts

[accordion openfirst=false scroll=true clicktoclose=true]

Often new LastPass Enterprise users already have an existing account under their work email address which contains both personal and work-related data. In this case, it is easy to create a new Personal account and migrate the data between the two. Once the two accounts are linked, data can be migrated from the Enterprise account to the new Personal account through the drag and drop method between folders. The steps are as follows:

[accordion-item title="Setting Up to Migrate" id="0"]

- 1. Create a new Personal account using your personal email address: https://lastpass.com/create_account.php
- 2. Link your personal account to your work account (log into your Enterprise account ->

- Look for the new personal folder in your Enterprise vault (the folder name will be your personal username)
- 4. Drag and drop any relevant sites from the Enterprise folder to any Personal folders (or right-click > move to folder)

[/accordion-item] [accordion-item title="FAQs" id="1"]

> **Can I block the migration of data from Enterprise to Personal?** Yes, this can be prevented by enacting the **Ppolicy** to prohibit updating personal account, located under the 'Limit Features' heading.

Can my employees move data from Shared Folders to their Personal account? $\pmb{\hat{v}}$

Data cannot be moved directly from a Shared Folder to the personal account, but it can be moved from the Shared folder to the Enterprise account, and then to the personal account. This too can be prevented via policies and user permissions.

[/accordion-item] [/accordion]

Building a Business Case for LastPass Enterprise

[accordion openfirst=false scroll=true clicktoclose=true]

LastPass Enterprise typically pays for itself within two to three months in the form of increased employee productivity and reduced help desk calls/cost. The following detailed ROI Calculators can be used to help quantify the impact of password automation and to help build a compelling business case for an investment in LastPass Enterprise: Pricing and ROI Calculators.

[accordion-item title="Benefits" color="Accent-Color" id="h1"]

The benefits of LastPass Enterprise go well beyond productivity and cost reduction. Our**�LastPass Enterprise Overview**�can help you articulate the importance of strong password hygiene for your company.

Our **Password Management Sample Survey** can help you establish a baseline and assess the current 'state of the nation' at your company.

If Compliance and Security are your primary concerns, the LastPass Security and Compliance document helps illuminate the impact of LastPass Enterprise on your compliance efforts.

[/accordion-item] [/accordion]

Administrator Toolkit

[accordion openfirst=false scroll=true clicktoclose=true]

We've compiled resources to help you and your business understand the benefits that LastPass Enterprise offers and how to get started with our service. Use these resources at your convenience and share with employees to facilitate the adoption of LastPass Enterprise.

[accordion-item title="Let s Celebrate NCSAM 2015 Together" color="Accent-Color" id="h4"]

Celebrated each October, National Cyber Security Awareness Month (NCSAM) is a time to learn ways to stay safe and be secure online. Join LastPass and the National Cyber Security Alliance as we celebrate the 12th annual NCSAM this October.

Here are a few ways you can show your support and materials you can use to help us make NCSAM 2015 successful!

Ways to promote security during NCSAM 2015:

- Invite more employees to LastPass. Every employee can benefit from the convenience and security of LastPass. Login to the Admin Console to add more employees to LastPass Enterprise.
- Sponsor LastPass on your campus. With turnkey, affordable Internet2 NET+ LastPass packages, all students, faculty, and staff can benefit from a campus-wide deployment of LastPass. Learn more here.
- Put passwords to the test with the LastPass Security Challenge. Or create a competition among teams to see who can get the highest scores, and who makes the most improvements in their scores.
- Host a Lunch & Learn. Using one of our presentations or resources provided on StaySafeOnline.org, schedule a time to chat with employees about good cybersecurity and password practices.
- Follow our tips on the LastPass blog. Subscribe at blog.lastpass.com!

Find more ways to get involved at the NCSAM website.

Logos

- LastPass logos
- NCSAM logos

Presentations

 LastPass NCSAM Presentation: Organize a brown bag lunch hour to introduce employees to NCSAM and explain the benefits of secure password management.

Tip Sheets

- Two-Factor Authentication: What It Is and Why It Matters(PDF)
- Instructional Flyer(PDF)
- 7 Bad Password Habits to Break Now (PDF)
- State of Security handout
- Password Security Tips handout
- More posters, handouts, infographics and tip sheets can be found on the NCSA website here.

Quizzes

- Promote the Workplace Security Risk Calculator
- Test their security knowledge with the **Online Safety Quiz**. Have an informal presentation of the quiz over a lunch hour, or have a security huddle (even virtually) to walk through the quiz and the answers.

Let us know how you plan to participate or contact us if you need assistance. We look forward to celebrating with you this October!

[/accordion-item] [accordion-item title="Evaluating Enterprise" color="Accent-Color" id="h2"]

LastPass Overview Deck A review of LastPass Enterprise and how it benefits your company.

Security White Paper In-depth technical details of LastPass' architecture.

How LastPass Works Infographic A high-level overview of LastPass' encryption and sync.

Overview of Features & Benefits How LastPass Enterprise helps managers & employees.

State of Security A snapshot of the cyber security challenges and risks businesses are faced with in 2014.

Case Study: MailChimp Learn how LastPass Enterprise solved the password security problem for the popular email marketing solution provider.

[/accordion-item] [accordion-item title="Implementation Resources" color="Accent-Color" id="h3"]

Enterprise Admin Manual How-to articles explaining deployment, onboarding, Shared Folders, and more.

Implementation Guide High level how-to guide on the deployment of LastPass Enterprise.

LastPass Enterprise Deployment Project Plan Detailed spreadsheet to assist the project team through the deployment.

Admin Overview Screencast Video tutorial detailing how to use the Enterprise Admin Console.

Internal Communication Plan A recommended plan for end user communications, training and education.

Weekly Webinar Recording A more in-depth dive into LastPass Enterprise.

[/accordion-item] [accordion-item title="Educational Resources" color="Accent-Color" id="h4"]

End User@Getting Started Guide In-depth presentation for educating employees on features and benefits of LastPass. See Internal Communication Plan for other roll-out tools and ideas.

End User Quick Reference Guide High level desk reference of end user features and benefits of LastPass Enterprise. See Internal Communication Plan for more information.

Screencasts

Video tutorials showing how to use LastPass features.

End User Manual

How-to articles for all basic and Premium LastPass features, included in Enterprise.

[/accordion-item] [/accordion]

2. Login to LastPass

Education Toolkit

[accordion openfirst=false scroll=true clicktoclose=true]

Thanks for choosing LastPass to help your students save time and better secure their digital life. Our toolkit has everything you need to spread the word around campus, educate your community, and help them benefit from secure password management with LastPass.

[accordion-item title="Branding and Identity" color="Accent-Color" id="h2"]

Logos

LastPass Logo (EPS) All LastPass logo usage variations.

LastPass Logo (PNG) PNGs of all LastPass logo variations.

Posters and Fliers

Half Page Ad A short, simple ad that can be handed out to students.

Full Page Ad A longer, more robust ad that can be handed out to students.

11x17 Inch Poster A large-scale poster that can be hung around campus.

Instructional Flyer An introduction flyer detailing how to get LastPass up and running.

Email Resources

HTML Email Template A coded template of the LastPass standard email.

Social Graphics

Facebook Post Graphics Graphics for your Facebook posts about LastPass!

Twitter Post Graphics Graphics for your tweets about LastPass!

Traditional Ads Ads sized for a variety of displays. [/accordion-item] [/accordion]

Internal Communication Plan

[accordion openfirst=false scroll=true clicktoclose=true]

LastPass Enterprise saves your employees time and increases productivity, all while improving security. Though every deployment is different, we recommend the following plan to drive adoption.

[accordion-item title="Pre-Launch Week" id="h0"]

Create "touchpoints" to build awareness of LastPass.

1. Inform

Hang posters and/or distribute flyers around the office. Post on intranet, digital signage, or employee blog. Build awareness of how LastPass will be easy, convenient, and save employees time. **Materials:** Posters, Flyers, Blog Post, Intranet/Digital Signage

2. Notify

Send a minimum of one email (or as many as one a day) to let users know you le providing a password manager that will save them time. **Materials**: Email Template, Logos

3. Challenge

Pick a competition, activity, and/or reward that you will use to drive adoption. See our list of fun ideas for driving adoption below or create your own campaign.

[button color="accent-color" hover_text_color_override="#fff" size="large" url="https://enterprise.lastpass.com/wp-content/uploads/Pre-Launch-Week-LP.zip" text="Download Assets" color_override="" image="fa-check-square"]

[/accordion-item] [accordion-item title="Launch Week" id="h1"]

Invite users and train them on how to use LastPass.

1. Activate

Send invitations to employees via the LastPass admin console.

2. Compete

Launch the competition or activity, and announce the prize.

3. Train

Host live training sessions to show employees why LastPass will save them time and how to get started. Materials: PowerPoint slides, Recorded webinar

4. Support

Post internal wiki page using our Sample FAQs. Point employees to your support resources, including the Getting Started Guide and tutorial videos. **Materials:** Sample FAQs, **Getting Started Guide**, Desktop Reference Guide, **Helpdesk**.

[button color="accent-color" hover_text_color_override="#fff" size="large" url="https://enterprise.lastpass.com/wp-content/uploads/Launch-Week.zip" text="Download Assets" color_override="" image="fa-check-square"] Evaluate the success of the launch and identify next steps.

1. Reward

Select the activity winners and celebrate their accomplishment.

2. Evaluate

Review the Notifications panel in the LastPass admin console to review adoption rate.

3. Re-Invite

Re-invite inactive users and address any adoption questions.

4. Follow-Up

Communicate with LastPass about your adoption campaign and how the team can support your organization going forward.

[/accordion-item]

[accordion-item title="Fun Ideas for Driving Adoption" id="h3"]

1. Reward Early Adopters

Incentivize the first X% of your employees to activate their account. For example, give a T-shirt to the first 5% of employees who activate their account, store a password, and create a secure note.

2. Friendly Competition

Create healthy competition by rewarding the first team to get to 100% adoption. Designate teams in the LastPass Admin Console before inviting users.

3. Hardwire It!

Consider pre-loading user vaults with passwords they need to do their work. When they see that it set up for them and LastPass starts filling their passwords automatically, they in instantly see the value of the service.

4. Scavenger Hunt

Pre-load user vaults with sites and notes that have trivia answers hidden in them. Hand out the trivia questions and let users know the answers are in LastPass. The first X number of users to find the answers get a reward.

[/accordion-item]

[/accordion]

[button color="accent-color" hover_text_color_override="#fff" size="large" url="https://enterprise.lastpass.com/wp-content/uploads/Communication_Plan.pdf" text="Download Communication Plan PDF" color_override="" image="fa-check-square"]

Training Kit for End Users

The LastPass Training Kit for End Users

Implementing LastPass in your organization will be an exciting development for administrators and employees alike. While the driver behind a LastPass Enterprise purchase is often improved security, LastPass also brings huge convenience to end users. When properly implemented, LastPass will help alleviate administrative tasks for IT and Operations, and will help save considerable time and frustration for end users. However, like all new things, there can be a learning curve. The following recommendations are intended to help create comfort among your staff as well as drive down this learning curve. We hope that you will take full advantage of these materials and advice, and contact our staff if there is anything more that you feel would help.

End User Survey (1 week prior to roll out)

Prior to implementing LastPass, we recommend that you survey your employees to establish a baseline around current password practices. This will help you to better steer your educational efforts, and will provide you a quantifiable proof point against which you can measure the impact of the program. **Click here for a sample survey**.

Warm 'em up (2 days prior to roll out)

It is a good idea to send a 'heads up' email 2 days in advance of your implementation to put context around the goals of the LastPass program and to prepare your staff for what to expect. This email is also intended to let them know that LastPass is a corporate-sponsored program so that when they receive the welcome email they are less likely to see it as a potential phishing scam. See suggested copy for the 'heads up' email here.

The Welcome Email

With most provisioning options, your end users will receive an automated welcome email from LastPass. This email can be customized to bring your own culture and message to your staff. **See the boilerplate emails here**.

LastPass Experts

We suggest you train a select group of employees to serve as "LastPass Experts". On the day of your launch, have your Experts wander the floor offering assistance and advice on how to use and optimize LastPass. For larger deployments, feel free to contact your sales representative for LastPass t-shirts for your experts.

Add LastPass screencasts to your Training Modules

Mandatory training is always best. Help your employees make the most of LastPass with a brief mandatory training. They can simply **watch the screencast** and then take a brief quiz to demonstrate completion.

Review your progress

At any point after the automated Welcome email is sent, you can check the progress of your users by visiting the **Notifications Tab**. We suggest direct outreach to staff members that have not yet enabled their account. You can program these emails to be sent automatically on a regular basis until the user has taken action.

Training Email and Self-help Tool (48 hours after invite)

It is best to offer your staff some form of training whether it is direct 'desk by desk' training, small group training, or a larger Webinar. We suggest that these invitations be sent out to end users approximately 2 days after the initial invite. **See suggested copy here**. For larger implementations, LastPass is happy to provide

training for your trainers. Please contact your rep to schedule your training session at least 5 days prior to the target roll out.

Review your progress (1 month after invite)

One month after the initiation of your LastPass program, we suggest that you visit the **Notifications Page**. Look for what you consider to be critical areas for outreach. Using the email templates, draft targeted messages to your end users that will be sent automatically based on the time frames that you designate.

Training Tools

We encourage you to distribute these tools to your End Users to help get them up to speed and to expose them to some of the broader benefits of LastPass.

LastPass Enterprise End User Training Deck LastPass Enterprise User Desk Reference Guide

Online screencasts

Getting Started with LastPass:http://youtu.be/HYNIxpRGi08 Other Screencasts: %https://lastpass.com/support_screencasts.php

Sample Survey

[accordion openfirst=false scroll=true clicktoclose=true]

When surveying your employees, we suggest that the survey be offered anonymously to promote honest answers.

Password Questionnaire

1. What system are you using to keep track of your passwords?

- Spreadsheet or other written medium (contacts, sticky notes, Word doc)
- Same or similar password everywhere
- Rotate between 3 (or so) passwords
- The password manager in my browser
- 3rd party password manager

2. How many work-related passwords do you use on a weekly basis?

- 11 � 15
- 15 � 20
- More than 20

3. Do you frequently re-set passwords because you have forgotten them?

• Yes, weekly

- Yes, monthly
- No

4. Do you check the **P**Remember Met button on login screens?

- Yes, always
- Yes, occasionally
- No

5. Do you share passwords with colleagues such as group logins to virtual meeting software, social media sites, servers, etc.?

• Yes

• No

6. Have you ever contacted the helpdesk at work regarding a password-related issue?

- Yes
- No

7. What functional team do you work for in the company (ie: sales, customer service, finance, HR, IT, etc.)

[/accordion]

Email Templates for End User Roll Out and Training

[accordion openfirst=false scroll=true clicktoclose=true]

Use our sample email templates for end user roll out and training.

[accordion-item title="The 'Heads Up' Email (2 days prior to invite)" id="h1"]

Hello Team:

We are pleased to announce that we have recently contracted with a great new service provider called LastPass. LastPass offers a service that will help you better manage your passwords. The goals of this program are to:

• Save you time by automating all of your logins.

- Eliminate the frustration of lost and forgotten passwords (and to reduce calls to our helpdesk).
- Educate you on easy ways to improve your 'password hygiene' to better protect your digital identity and our company data.

In the next couple of days, you will receive a welcome email from LastPass. Please follow the instructions to get started. While this is required, it is also something that we are certain will bring you great utility and convenience. We hope that you will embrace and enjoy this new tool.

Regards,

Your friends in IT [/accordion-item] [accordion-item title="The Automated Welcome Emails" id="h2"]

Click here for our automated email contents.

[/accordion-item] [accordion-item title="The Training Invite (2 days following invite)" id="h2"]

Hello Team:

Two days ago you should have received your invitation to create a LastPass account. Hopefully you have done so, and are enjoying the benefits of the service.

We will be conducting required training sessions at the following dates and times. Please respond to this email to reserve your spot:

XXXXXXXXXX

Attached is a desk reference that might also be helpful as you start using LastPass.

Regards, Your friends in IT

LastPass Enterprise Desk Reference

[/accordion-item] [/accordion]

Email Templates for End User Roll Out & Training

The Admin Console

[accordion openfirst=true scroll=true clicktoclose=false]

The LastPass Enterprise �Admin Console� offers every tool your administrators will need to implement and manage LastPass for your organization.

[tabbed_section]

[tab title="Opening the Admin Console"]

To open the Administration Console, click the LastPass icon on your browser bar and select 'Admin Console'. This option is visible to LastPass Administrators. The creator of a LastPass trial is made Admin by default. He or she can then assign admin rights to any other users from the **Users tab of the Admin Console**.

Search LastPass Vault	Q
🔒 My LastPass Vault	
* Sites	•
E Form Fills	►
Generate Secure Password	•
Secure Notes	•
Show Matching Sites 1	Þ
Recently Used	Þ
Tools	•
Preferences	
Help	
Admin Console	
Logoff:	٢

[/tab]

[tab title="Admin Console Home Tab"]

Clicking on the 'Enterprise Console' option will open the home page of the Admin Console shown below. The home page of the console gives you a summary of your account including: the number of users, licenses available, expiration, purchase options, security grade tiles, a snapshot of all enterprise logins over the last 7 days, and important alerts regarding features and newly added services.

LastPass **** Enterprise			HOME	SETUP	USERS	REPORTING	saml
HOME> DASHBOARD	ENTERPRISE USER MANUAL	SUPPORT	LASTPA	SS.COM	LOGOFF		
Account Detail	S			Your compa	ny has saved	7.98 hours this we	eek.
92%	6 Feature Usage				87.	1%	
Number of Users	43			Averag	e Security	Challenge S	core
Number of Licenses Remain	ning 223						
Expiration Show Recent Invoices	2015-06-19 16:08:11 Purchase More Lic	ienses	Averag	83.2 e password s	trength	Average site	3.7 s having duplicate sswords
			Avera	9.1 ge number of passwords	fweak	Average n pa	1.6 umber of blank sswords
			Numb	20 er of users rej results	porting		Show Score History



[/tab]

[tab title="Video Tutorial"]

Please see the video below for an overview of the Enterprise Administration Console:

[/tab] [/tabbed_section]

[/accordion]

Reporting - Login Reports

[accordion openfirst=true scroll=true clicktoclose=false] [accordion-item title="Login Reporting" id="h0"]

LastPa:	S **** P R I S E			HOME	SETUP	USERS	REPORTING	ENGLISH 📀
REPORTING	LOGINS	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATIO	DNS LO	GOFF		
					F	REPORTING	NODE: Show All Lo	ogins (What is this?)
LastPass expose	es a public API t	hat can be used by ente	rprise accounts to pul	l reporting dat	a. For full AP	l details, plea	se click here.	
From 1	1/13/2013							
то 1	1/13/2013			Even	ts For	All Us	ers	
Search							Event Key 🗐	Export to Excel

Submit					
Time	Username	IP Address	Action	Data	
2013-11-13 22:06:58	enterprise3@lastpass.com	70.167.240.233	Login	google.com	
2013-11-13 22:05:37	enterprise3@lastpass.com	70.167.240.233	Login	google.com	
2013-11-13 22:00:20	enterprise3@lastpass.com	70.167.240.233	Login	google.com	
2013-11-13 09:59:52	shlomit@netrot.net	67.171.11.194	Failed Login Attempt		
					Event Key

The Login Report is a comprehensive log of every login, password/username update, form filled, and site deletion that is attempted or completed by your LastPass Enterprise users. The reports can be filtered by date range, or by user and can be exported to Excel for back up. There is a link on the page to a key explaining what each action designation means.

[/accordion-item] [/accordion]

Users Sub-tab

[accordion openfirst=false scroll=true clicktoclose=false]

This tab provides you with a complete list of all LastPass accounts that have been provisioned under your enterprise, and several actions that can be taken on each:



Security Score - the security score is based on the score generated when the user runs the 'Security Challenge' from his/her vault. The score is only update and/or displayed when the Security Challenge is run.

User Details - this report offers a summary of the user a account including their general account information, security check score, policies they are subject to, shared folder access and groups they are apart of. You can click on several of these headings in order to see a detailed list pertaining to his/her account including all of the policies that are active on the account and any folders that have been shared or created by the user. Scroll to the bottom of the page and click 'Click to see sites' to see a full, read-only list of all entries stored in the user's account.

User Details for enterprise3@lastpass.com				
Last Login:	2013-11-12 18:25:02			
Sites:	20 (38 deleted)			
Form Fills:	3			
Policies:	3			
Shared Folders:	25			
Groups:	7			

Linked personal account:	No
Created:	2011-06-28 12:35:51

Usage Reporting - redirects you to the full reporting tab within the console.

Edit Name@- assign a nickname to the account that may be more recognizable to you than the user's email address.

Make or Remove Admin you can promote any number of users to admin status and remove this status at any time. Granting Admin rights means that the individual will have full access to the Admin Console.

Reset Password[©]- This option will be available only if the 'Super Admin - Password Reset' policy is enabled and if the user is 'eligible' for reset. For more information, see the 'Super Admin - Password Reset' policy at the bottom of the **Policies page**.

 ${\bf Disable \ User} \ensuremath{\hat{\bullet}}\xspace$ - temporarily disable the user's account making it inaccessible to them but not deleting the account entirely.

Edit roles[®]- This is for legacy 'roles' users. For new users, we would recommend sharing using the 'Shared Folders' feature instead. To learn more, click here:[®]Shared Folders.

Require Password Reset • This will force the user to manually reset their master password. • They will receive the notification to do this the next time the user logs in.

Delete User and **Remove User from Company:** At the bottom of the list you see **delete user** or **deference user** from company **delete**. This is a decision that you should weigh carefully. **Delete user** will delete that user a account entirely. If the user has saved any personal logins or other data to their vault then they will no longer have access to that data. Some enterprises prefer the **Remove user** from company **delete** option which will remove the user from your enterprise account, and will delete all Shared Folders from the user's account. With this option, the user will continue to have access to his/her account as a standard LastPass user.

Whether a user account is deleted, disabled or removed from the Enterprise, this will in no way impact any remaining users. For example, if the departing employee was an administrator of several Shared Folders, these folders will remain 100% available and intact for all remaining users. That said, there is a possibility that the folder will be left with no Admin. To avoid this scenario, you might consider enabling the **Super Admin** - **Shared Folders** policy.

As a best practice and an added precaution, we suggest that any shared credentials be changed upon the exit of an employee regardless of how you choose to manage their exit from LastPass. These changes to any Shared Folder will automatically sync to all assigned users, and this will give you an added layer of security.

SuperAdmin Password Reset: If an Admin has been set as a SuperAdmin Password Reset via policy, there will be option on this user actions dialog to change the password for that particular user. This change will be immediate and the Admin will be asked to create a new password for the account on the spot.

[/accordion]

Set-Up Tab

[accordion openfirst=true scroll=true clicktoclose=false]

The Set-Up Tab of the Admin Console contains many of the tools that you will need to implement LastPass and control your user's actions.

Last <mark>Pa</mark>	SS **** R P R I S E			HOME	SETUP	SAML	USERS	REPORTING
	POLICIES	CREATE NEW USER	INSTALL SOFTWARE	PUSH SITES TO USERS	API [DOCS	LOGO	FF
	Other E Manag	Enterprise Options e Trusted Mobile Devices		Manage User Groups URL Rules				

- Policies Dozens of configurable security policies including: user access rights, password strength criteria, and multifactor authentication. You can create any kind of security environment with the combination of these policies. It is very important that they be considered carefully.
- Create New User This tab offers four different provisioning options including one manual and three automated.
- Install Software This tab offers all of the tools that you may need to install the LastPass software for your users. It is always best if you can remove the burden from them and avoid download restrictions by doing the installation for them.
- Push Sites To Users Push Sites to Users is also helpful when used to push SAML specific URLs to services you have linked to your Enterprise to using LastPass SAML.
- API Docs The LastPass Provisioning API allows you to create new users, delete/disable existing users, manage user groups, push sites to users, pull reporting data, and view license utilization, via a simple REST web service interface.
- Logoff Log you out of LastPass.

[/accordion]

Policies

[accordion openfirst=false scroll=true clicktoclose=true]

LastPass offers a number of configurable policies around security levels and password strength. Each policy can be applied to all users, or an inclusive or exclusive list of users. For example, you might elect to implement a policy that will prohibit the general workforce from exporting data, while your senior executives are exempt. There are a number of important policy options on this tab. You should consider them carefully. Click here off a off a full list of LastPass Enterprise policies (note you must be logged in with an active LastPass Enterprise account to view the list).

[accordion-item title="Adding Policies" id="h0"]

Click on the 'Add Policy' button in your Setup > Policies menu to create a new policy on your Enterprise Account (see screen shot below). Select your inclusive or exclusive group of users, or leave blank. And fill in the 'Value' and 'Notes' fields where applicable. By hitting save, the policy will be activated immediately:

Policy ×
Policy IP Address Restriction
IP Address Restriction allows you to limit your users' access to their accounts to a certain set of IPs, such as only your office IP addresses. In the 'value' field, enter each IP address or partial IP address that you'd like to allow, separated by white space. For example: 71.126.154. 128.8. 120.0.0.1 would allow any address in 71.126.154.*, 128.8.*.* and 120.0.0.1 to login. Any matching IP address will allow entry. A matching DNS Value
Applies To: All Inclusive List of Users Exclusive List of Users
Notes
Cancel Save

//

Other Enterprise Options

On the Policies tab of the Admin Console, there are links to Manage Policies and to **Other Enterprise Options**. Other Enterprise Options takes you to a page containing NEVER URLS and Equivalent Domain options.

LastPass **** Enterprise				HOME	SETUP	SAML	USERS	REPORTING
POLICIE	S CREATE N	NEW USER INSTALL SC	OFTWARE PUSH SI	TES TO USERS	API D	ocs	LOGOF	Ŧ
Global Never / Only Symantec VIP Sec	URLs Global Equ ureAuth	uivalent Domains Master Pas	swords SAML Initializatio	on Duo Security	Salesforce	# RSA :	SecurID / F	ADIUS

[accordion-item title="Global Never URLs, Global Only URLs" id="h0"]

Global Never URLs and Global Only URLs enable you to create whitelists and blacklists of URLs upon which you do or do not want LastPass to be enabled.

If there is a certain, select group of URLs upon which you do not want LastPass prompts enabled, you should enter these domains under the 'Global Never URL' box.

If you want to disable LastPass prompts altogether with the exception of just a select group of domains, then you should enter these domains under the 'Global Only URL' box. We do not recommend using Only URLs unless you have a very limited use case in mind.

Global Never / Only URLs						
Enter URLs or domains, separated by commas or newlines. If you want your users to never be prompted to save sites on a certain domain, or only be prompted to save sites on a set of domains you can set that up here. We do not recommend using Only URLs unless you have a very limited use case in mind:						
Global Never URLs and Apps:	example.com, testing.com, C:\Program Files (x86)\SEQUEL ViewPoint\ViewPoint.exe, http://C:\Program Files					
Global Only URLs:		The state of the second second second				
	Update	1202010120000				

[/accordion-item]

[accordion-item title="Creating Equivalent Domains" id="h1"]

You can also create *equivalent* domains*b*. Equivalent domains allow you to manage a single login for different domains that are related. An example is Google and YouTube. Since they are both owned by the same company, your login works on both sites. So rather than having the same login twice, you can have it for one and we will treat both domains equivalently.

Enter equivalent domains separated by commas. Equivalent domains are used to share the same credentials across 2 different domains (e.g., live.com, hotmail.com) without the need to create 2 separate saved sites.

Global Equivalent Domains

- cms-woger-cdn.com, cms.woger.local
- 🛞 odesk.com,upwork.com

	Gibba Equivalent Domains.
2000	
107.070	
0.5725	Add

[/accordion-item]

[accordion-item title="Master Passwords" id="h2"]

Here you can view your user list and their master password change information, including the last time they changed their master password, logging all users our of their current sessions (destroy all sessions option), or require a password change on the users next login.

Master Password Change Information		
Username	Last Password Change	Action 🔳

Destroy All Sessions Require Password Change

[/accordion-item] [accordion-item title="SAML Initialization" id="h3"]

Here you can view your current SAML initialization status.

SAML Initialization

SAML has already been successfully initialized.

[/accordion-item] [accordion-item title="DUO Security" id="h4"]

This is where you enter the necessary information from your DUO Security console home page into LastPass to enabled DUO Security for your users.

Duo Security	
Click here if you need a Duo Secu	urity account (be sure to choose an integration type of LastPass)
Duo Security integration key: Duo Security secret key: Duo Security API hostname:	
	Update

[/accordion-item]

[accordion-item title="Salesforce#" id="h5"]

Here you can enter the API URL to be used with Salesforce# multifactor authentication.

Salesforce#

Enter the API URL to be used with Salesforce# multifactor authentication: For example: https://lkermes-developer-edition.na15.force.com/services/apexrest/otp/lastpass/validate

Salesforce# API URL:

[/accordion-item] [accordion-item title="RSA SecureID" id="h6"]

The steps here assist you in setting up RSA SecurID authentication via RADIUS.

RSA SecurID / RADIUS					
LastPass supports RSA SecurID authentication via RADIUS. You must set up a RADIUS client for LastPass in your RSA Authentication Manager. Since RSA Authentication Manager does not let you specify multiple IP addresses for a RADIUS client, we recommend using the 'ANY Client' option, and using a separate firewall to restrict connections to the necessary IP addresses. If you use the 'ANY Client' option, you also need to edit securid.ini and change CheckUserAllowedByClient from 1 to 0. This RADIUS client must be accessible from all LastPass server IP addresses. If you need a list of all LastPass server IP addresses, please send a note to support@lastpass.com or contact your sales representative. LastPass uses an outbound firewall so your server's IP must be explicitly allowed by our Operations team. Please send a note to support@lastpass.com or contact your sales representative to request a change					
RADIUS Server IP Addresses: separate multiple with commas append ':port' if not 1812 e.g. 216.162.248.81,216.162.248.82:1645					
RADIUS Shared Secret:					
RADIUS can also be used to support other multifactor au name and logos that your users will see, you can do so b	thentication options besides RSA SecurID (such as SafeNet). If you would like to customize the elow				
Service Name:	RSA SecurID				
124x124 PNG Logo:	Choose File No file chosen				
190x41 PNG Logo:	Choose File No file chosen				
	Update				

[/accordion-item] [accordion-item title="Symantec VIP" id="h7"]

This is where you provide LastPass with your certificate for Symantec VIP authentication.

Symantec VIP			0.0251.0				
LastPass supports Symantec VIP authentication. You must provide LastPass with a certificate. Within Symantec VIP Manager, go to Account - Manage VIP Certificates. Request a certificate for LastPass, then download it in PEM format.							
Certificate:	Choose File No file chosen	4692-byte file stored Delete File					
Certificate Password:							
		Update					

[/accordion-item] [accordion-item title="SecureAuth" id="h8"]

This is where you provide LastPass with your SecureAuth application ID, application key, and realm.

250	SecureAuth
100	SecureAuth
100	I setDace connecte Convertish sutheration law must require I setDace with your Convert with sension ID sension buy and value

Update

CONTRACTOR DATE	LastPass uses an outbound firewall so your server's IP must be explicitly allowed by our Operations team. Please send a note to support@lastpass.com or contact your sales representative to request a change.						
1100 CAN 8 100 W	Application ID:						
CARL AND	Application Key:	*************************					
120200000000000	Realm:						
101 01 0 X 10 X 10 X 10		Update					

ou must provide cast-ass with your secureAuth application iD, application key, and real

[/accordion-item] [/accordion]

Reporting - Shared Folders

[accordion openfirst=true scroll=true clicktoclose=true] [accordion-item title="The Shared Folders Report" id="h0"]

This report offers a master view of every Shared Folder created under the Enterprise. You can click on the column headings to sort alphabetically or by user. You can drill down on each folder to see the particular sites and notes that are contained within, as well as all assigned users and the specific access rights granted to each (ie: hidden or visible access to the credentials, admin rights, read-only/write.)

This report is read only. To guarantee Admin access to every Shared Folder created within the enterprise - including the login credentials of the stored entries, you must enable the 'Super Admin - Shared Folders' policy.

[tabbed_section][tab title="Top Level View" id="t1"]

Shared Folder Report sorted alphabetically:

LastPass 🔛	***					📟 ENGLISH 🕑		☯
ENTERPRI	ISE		HOME	SETUP	USERS	REPORTING	SAML	

Add Shared Folder

Shared Folders

▼Folder Name	Security Score	Number of Accounts	Number of Users	Users	Action
2test 60000			2	enterprise3@lastpass.com, enterprise1@lastpass.com	View
			2	enterprise7@lastpass.com, enterprise3@lastpass.com	View
Ax			3	enterprise7@lastpass.com, dana@netrot.net, enterprise3@lastpass.com (invisible)	View
blahblahblah			1	enterprise3@lastpass.com	View
Citysearch test			1	enterprise3@lastpass.com	View

[/tab]

[tab title="Individual Shared Folder View" id="t2"]

Detailed view of an individual shared folder:

REPORTING> LOGINS SHARED FOLDERS

ADMIN EVENTS NOTIFICATIONS LOGOFF
√Username	Can Administer	Read-Only	Can View Passwords
enterprise3@lastpass.com	No	Yes	No

Security Score

Security information is not available for this shared folder. As clients check in and submit security data, it will appear here.

Sites

Dor	Domain				
P	group				
B	live.com				
ió(microsoftonline.com				

[/tab] [/tabbed_section] [/accordion-item] [/accordion]

Full List of Policies

[accordion openfirst=false scroll=true clicktoclose=true]

Explanations of each policy are available here as well. Please read this carefully and take note of those that LastPass recommends.

Click here for the full list of LastPass Enterprise Policies.

Please note that you must be logged into LastPass via the browser extension and be an Admin in order to view this page.

[/accordion]

Employee Welcome Emails

[accordion openfirst=false scroll=true clicktoclose=false]

When using the Batch Provisioning option, LastPass will look-up the email to determine if the username is new or existing. Based on this looking, either of the two emails below will be sent by LastPass automatically to the end user.

[accordion-item title= "New User (no existing account under that username) Template" id="h1"]

Hi, your employer has created a LastPass Enterprise account for you. LastPass is a password management tool that allows you to safely store your everyday passwords behind a single Master Password. LastPass will then automatically log you in to your sites and applications, keeping your data secure while helping you be more productive.

Your username is _____ Your temporary password is _____

To get started, **click here** to reset your password.

Click here for a 5-minute introductory tutorial. Other helpful screencasts can be found at: https://lastpass.com/support_screencasts.php.

Thanks, The LastPass Team [accordion-item title= "Existing User Template" id="h2"]

Hi,

You have been invited to join your company's LastPass corporate account. As an existing LastPass user, you have two options:

1) Use your existing LastPass account thereby tying your current account into your company's corporate account. Depending on your company's policies, this could eventually lead to the deletion of your account by your company's admin. To use your existing LastPass account, log into your LastPass account and click on the following link to activate your account. Activate Your LastPass Account

2) Create a new account strictly for professional purposes. After creating this account, you have the option to link your personal account to it should you so choose (click here to learn more). Click here to create a new account: Create a new Account and then follow step 1 to associate this new account with the corporate account.

Thanks, The **LastPass** Team

[/accordion-item] [/accordion]

Reporting - Admin Events

[accordion openfirst=true scroll=true clicktoclose=false] [accordion-item title="The Admin Events Report" id="h0"]

The Admin Events Report provides a detailed breakdown of all administrative actions taken via the Admin Console.

Last <mark>Pass ****</mark> Enterprise			HOME	SETUP	USERS	REPORTING	ENGLISH 🕑
REPORTING> LOGINS	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATIO	DNS L	OGOFF		
					REPORTING	IODE: Show All Lo	ogins (What is this?)

LastPass exposes a public API that can be used by enterprise accounts to pull reporting data. For full API details, please click here.

From To	11/06/2013		Adr	nin Eve	nts By All Users
Search	All lisers				Event Key 폐금 Export to Excel
USEI	Submit	·			
Time		Username	IP Address	Action	Data
2013-1	1-12 19:18:43	enterprise3@lastpass.com	70.167.240.233	Add Policy	Require Password Reprompt on Copy/View
2013-1	1-06 22:00:45	enterprise3@lastpass.com	70.167.240.233	Edit Policy	Prohibit Unrestricted Mobile Logins Except Approved by Admin

- Create, delete, disable, or reactive an employee account.
- Reset a user's password
- Toggle a user as an Admin.
- Remove a user from the company.
- Add, delete or edit policies
- Add, edit or delete User Groups.
- Update Policy Users.

The full list of messages and their meanings can be found here.

[/accordion-item] [/accordion]

Create New User

[accordion openfirst=false scroll=true clicktoclose=true]

You can provision new users by going to :

Admin Console -> Setup -> Create new User tab

And then using one of the 4 methods described below. You will want to weigh these options carefully before implementing LastPass across your organization.

[accordion-item title="Batch Provisioning of Users (Mac/Windows/Linux)" id="h1"]

You can provision users under your enterprise account by entering their email in the box provided on this tab. Once submitted, the user will will receive an automated welcome email with instructions on how to reset their temporary password and get started. If the user's email address is already associated with a LastPass account, they will be sent an email with an activation URL to link their existing account to the Enterprise.

[/accordion-item] [accordion-item title="Automatic Provisioning Using Windows Login Integration" id="h2"]

LastPass can invisibly integrate with the standard Windows Login process to automatically create new users and sign existing users in.

In order to setup, simply install our *full build* with the following parameters:

lastpassfull.exe -dl=<your domain name> -cid=<company ID> -chsh=<your ID> winlogin --userinstallie --userinstallff --userinstallchrome --installforallusers -j "C:\Program Files\LastPass"

The dl parameter should be an externally resolvable domain name (not your internal Windows Domain name) and will be combined with the Windows Username to form the LastPass login. For example, if you pass -dl=xmarks.com and your windows login is bob, the resulting LastPass username will be bob@xmarks.com.

[/accordion-item]

[accordion-item title="Active Directory Sync Client" id="h3"]

LastPass offers the 'Active Directory Sync Client' which can be installed locally for ongoing synchronization between your Active Directory and LastPass. Any newly eligible profiles added to your AD will be either (1) automatically provisioned with LastPass or (2) added to our system as pending approval (depending on your preferred settings). Once provisioned, the user will will receive an automated welcome email@with instructions on how to reset their temporary password and get started. If the user's email address is already associated with a LastPass account, they will be sent an email with an activation URL to link their existing account to the Enterprise. With this Client you can opt to sync user group information as well, which can be used in turn to assign policies and Shared Folders. **Click here** to learn more about the Active Directory Sync Client. **Click here** to download the client (scroll to the bottom of the page).

[/accordion-item] [accordion-item title="LastPass Provisioning API" id="h4"]

LastPass exposes a public API that can be used by enterprise accounts to create users, deprovision users, and manage groups. The full API details and instructions can be found within the Enterprise Console > Setup > Create New Users > LastPass Provisioning API option.

Please see the link below for how to create and provision new users:

Creating New Users

[/accordion-item] [accordion-item title="Provisioning without an email address" id="h5"]

By default, when a user is provisioned, an email is sent to the user with their temporary password or an activation link (if their account exists already). However, If you must provision users who do not have an email yet (for example, you are provisioning users via Sercice Provisioning through SAML), follow the procedure below:

1. Go to Create Users in the Admin Console

- 2. Set "Send Email if Existing User?" and "Send Email if New User?" to "No"
- 3. Create the user using Batch Provisioning
- 4. Once the user is created, go to the Users page
- In the Actions column, choose "Set Initial Password". Make sure that the require Master Password reset on next login option is enabled. Store this password somewhere safe as it will be needed later for distribution
- 6. If needed, setup the account: add the user to any User Groups, Shared Folders and Policies.
- 7. When ready, give the user the initial password so they can use it to sign into their newly created account.

[/accordion-item] [/accordion]

Windows Login Integration

[accordion openfirst=false scroll=true clicktoclose=true]

LastPass can invisibly integrate with the standard Windows Login process to automatically create new users and sign existing users in. To do this, we install a DLL that hooks the Windows login flow using sanctioned/standard Windows protocols. When we receive the password, we hash it and then use the hash to create the user's LastPass credentials. We never store anything on disk and are careful to not leave anything in memory.

With Windows Login Integration, users within the LastPass Enterprise system will be provisioned using their Windows username followed by the @companydomain.com address that your Enterprise use. New users to LastPass will be created upon their first login to the Windows domain after the Login integration with LastPass is added. From that point on, users will login to the Windows domain as they normally would, and will automatically be logged into LastPass as well.

Instructions for set up can be found in the Enterprise console -> Set Up tab -> Create New User -> Automatic Provisioning Using Windows Login Integration.

[accordion-item title="Frequently Asked Questions" id="h1"]

Q: What happens if a user's windows user name and company domain address that is used to login outside of the work environment does not correlate to an@existing@e-mail address?

A: If the windows username@companydomain.com address does not correlate to an existing email address, upon first logging into the account the user will be prompted to set a **security email address** which will be used for all communications regarding LastPass. This e-mail address can be changed within the Account Settings at a later date by the individual user.

Q: How do I make sure LastPass master password changes when AD/Windows password changes?

If you change your Windows password in Windows Settings on the computer where Windows Login Integration has already been set up, we would be able to capture the event and change the master password accordingly. To ensure the event is captured, you would need to have an active LastPass session AND change the Windows password on the local machine that has Windows Login Integration enabled. If the Windows password change takes place on another machine (i.e., the admin changes the password for the user), master password and Windows password will be out of synced. In this case, the user will need to manually change the master password.

Tips for enterprise admins:

If you wish no user interaction involved in the password change process, enable Super Admin Master Password Reset Policy. It would allow you to reset users' master passwords as a super admin. When you change a user Windows password, you could also reset his or her master password in LastPass Admin Console to make sure they match. For more information about how to set up the policy, see this **FAQ**.

Q: Can a user set up a form of multi-factor authentication with LastPass while using Windows Login Integration?

A: Because we intend Windows Login integration to be a seamless login experience, we do not allow multi-factor authentication to be used when logging into the work environment where Windows Login Integration is utilized. However, when logging into the LastPass account outside of the work environment, multi-factor authentication can be used on the account, as it would on any other LastPass account. Multifactor authentication can only be set up either by logging directly into the browser extension or the online Vault at https://lastpass.com.

Q: �What happens if the user already has a LastPass Account under their work e-mail?

A: If the username and password for the LastPass account are the same as the windows login and password, LastPass will attempt to login using these credentials.

Q: **What happens if the password the user has to login to Windows is NOTOthe same as the password for the pre-existing LastPass account?** A: **The user** will see a bubble from LastPass icon in the tray that says "Login failed, does your Windows password match your LastPass password?"

Q: �What�should�the user do if his or her existing password does not match the Windows password?

A: The user will need to login to LastPass using their existing LastPass password, go to Account Settings, and change the master password to match the Windows login password.

Q: �Could a user continue to use two different passwords for Windows login and LastPass login?

A: **Y**Yes, a user could continue using two different passwords, one to login to **W**indows, and another to login to LastPass. **The AutoLogin to LastPass when** logging into Windows would continually fail, though, and this would **P**largely defeat the purpose of Windows login integration.

Q: $\ensuremath{\mathfrak{O}}$ If you delete Windows domain login can manually login to your LastPass account?

A: Yes, you can also manually login to your LastPass account using your LastPass username and password.

Q: Can you login anywhere using your LastPass credentials? A: Yes, you can always use your LastPass Credentials to login to your account and gain access to your data.

[/accordion-item] [/accordion]

LastPass Active Directory/LDAP

[accordion openfirst=false scroll=true clicktoclose=false]

The Client connects to your Active Directory using LDAP to support a variety of provisioning and management processes in LastPass. With this service, you can:

- 1. Feed relevant information from your user directory into LastPass.
- Sync new user profiles to LastPass for automated provisioning of LastPass user accounts.
- Sync disabled or deleted user profiles to LastPass for automated termination of LastPass user accounts.
- Sync user groups to LastPass for policy designations, Shared Folders, and SAML application assignments.
- Apply filters based on your groups so that only the relevant groups sync to LastPass.
- Provisioning for a number of cloud-based applications including Google Apps and Salesforce.com. Add the user in AD, and let LastPass take it from there. No local provisioning necessary.

[accordion-item title= "Installing and Configuring the Client" id="h1"]

Setting up AD/LDAP sync is easy. You simply download the client from the "Set-Up - Create New User' tab in the Admin Console, and log in to LastPass. The first step to take is to log in with your LastPass Enterprise administrator login credentials:

(LastPass LDAP Active Direc	tory Integration Client	83
	LastPass ****	
Please enter yo	our LastPass email address and master password.	
Email: Password:		
ОК		
	LastPass LDAP Active Directory Integration Client v2.0).10

After logging in, you will then be given an overview of each LDAP Active Directory sync option available and the settings that are currently in place:

9	l	astPass LDAP Active D	irectory Integratio	on Client	>
		LastPa	SS ****	l .	
AD Provi	sioning Syncl	nronization Tool			
The AD Prov Directory serv	sioning tool synchro er to LastPass, mak	onizes the users in your Active ing administration easier.			
Status					
Enabled: 🔇 Connected t) 0 AD: 🚯	Configure			
	•	2			
L					

Start by configuring the connection between LastPass and your Active Directory:

🛞 LastPass LDAP	Active Directory Integration Client	×
Configu	re Synchronization	Retum to Main Screen
New users crea address stored	ted in your Active Directory/LDAP server will be automatically created in LastPa in the directory. An email will be sent with a temporary password and instruction	ass using the email s to get started.
Enable Syn	Disable Sync	<u>Debug</u>
Connection	Connection Configuration	<u> </u>
Actions	Specify Server:	E
Sync	Credentials Cogin As current user Specify Credentials: Username: Password:	-
	LastPass LDAP Active Directory I	ntegration Client v2.0.10

After configuring your connection, click on 'Actions' to configure the Account Provisioning and Deletion options.

When a user profile is Created:

🛞 LastPass LDAP	Active Directory Integration Client	23
Configu	re Synchronization	Return to Main Screen
New users crea address stored	ted in your Active Directory/LDAP server will be automatically created in LastPa in the directory. An email will be sent with a temporary password and instructions	iss using the email s to get started.
Enable Sync	Disable Sync	Debug
Connection Actions	 When a user in active directory is created: Add the user in the Enterprise Console, but require approval Automatically create user in LastPass 	E
Sync	 When a user in active directory is deleted: Administratively disable the LastPass account Automatically delete their LastPass account 	-
	LastPass LDAP Active Directory In	ntegration Client v2.0.10

To break down the options above:

"Add the user in the Enterprise Console, but require approval": - This option will sync users between your AD and LastPass but will place them in LastPass under a 'pending' status, rather than immediately creating an account for each user. **Click here** to learn more about creating an account for 'Pending Users'.

"Automatically create user in LastPass" - When this option is enabled, LastPass will automatically create accounts for every new user, and send them an automated welcome email with a temporary password and instructions to

create their individual Master Password.

When a user profile is �Deleted:

Actions Sync	 When a user in active directory is deleted: Administratively disable the LastPass account Automatically delete their LastPass account Remove from enterprise account, but do not delete user 	Ŧ
To b	preak down the options above:	
"Ad Ente still	ministratively disable the LastPass Account:" �This will 'lock' the erprise account, and free a license for other use; however, the account will exist and be a part of the Enterprise	
"Au Lasi it w	tomatically delete their LastPass account:" T his will completely delete the the tPass account and all data included in the account. The license applied to ill be available for use on another account.	
"Re rem turn will	move from the Enterprise account, but do not delete user:" This will nove the account from the Enterprise system, free up the license, and leave the account into a regular LastPass account. All data within the account still be available for use to the user.	
Whe	n a user profile is�Disabled:	

When a user in active directory is disabled:	
 Administratively disable the LastPass account 	
 Automatically delete their LastPass account 	
© Remove from enterprise account, but do not delete user	:
	When a user in active directory is disabled: • Administratively disable the LastPass account • Automatically delete their LastPass account • Remove from enterprise account, but do not delete user

To break down the options above:

"Administratively disable the LastPass Account:" **•** This will 'lock' the Enterprise account, and free a license for other use; however the account will still exist and be a part of the Enterprise

"Automatically delete their LastPass account:" This will completely delete the LastPass account and all data included in the account. The license applied to it will be available for use on another account.

"Remove from the Enterprise account, but do not delete user:" This will remove the account from the Enterprise system, free up the license, and leave turn the account into a regular LastPass account. All data within the account will still be available for use to the user.

When a user profile is removed from the group in filter:



To break down the options above:

still exist and be a part of the Enterprise

"Automatically delete their LastPass account:" This will completely delete the LastPass account and all data included in the account. The license applied to it will be available for use on another account.

"Remove from the Enterprise account, but do not delete user:" This will remove the account from the Enterprise system, free up the license, and leave turn the account into a regular LastPass account. All data within the account will still be available for use to the user.

[/accordion-item] [accordion-item title= "Configure Groups and Filters" id="h2"]

When you are done configuring the 'Actions', click 'Sync' to configure the fields, groups and users that you would like to sync between LastPass and your Active Directory:

(*)	LastPass LDAP Active Directory Integration Client	×
Configu	e Synchronization	Return to Main Screen
New users creat address stored	ed in your Active Directory/LDAP server will be automatically created in LastF n the directory. An email will be sent with a temporary password and instructio	ass using the email ns to get started.
Sync To La	stPass Disable Sync	<u>Debug</u>
Connection	Sync Configuration	
Actions	 ✓ Sync user's full name from AD ✓ Sync user groups from AD ✓ Create groups in LastPass □ Disable Async LDAP Query 	
Sync	0 Sync Search Interval (in hours)	
Debug Options	Filter Users	~

- Sync user's full name from AD By default, LastPass only lists users by their username/email address. However, when this option is enabled, the client will sync users full name so that it appears in LastPass, as well.
- Sync user groups from AD When this option is enabled, the client will synchronize all groups from your AD into LastPass for the purpose of assigning policies.
- Create groups in LastPass If a group exists in the AD but not in LastPass, enabling this will create these groups in LastPass.
- Disable Async LDAP Query Disable tracking of ongoing changes. Sync only happens on initial run.
- Sync Search Interval in hours If the above is enabled, it will force the client to search for and update changes in a cycle according to the designated number of hours.

(*)	LastPass LDAP Active Directory Integration Client	×
Configur	e Synchronization	Return to Main Screen
New users create address stored i	ad in your Active Directory/LDAP server will be automatically created in n the directory. An email will be sent with a temporary password and instr	LastPass using the email ructions to get started.
Sync To Las	tPass Disable Sync	<u>Debug</u>
Connection	0 Sync Search Interval (in hours)	^
Actions	Cit	

	Filter Users			
0	Group:	?		
Sync	Custom LDAP Settings			
	Email Field:		3	
Debug Options				•

• Filter Users - You can limit what users are added to your Enterprise by specifying a sync filter within the AD sync client. This field should be populated with the DN string of the group you'd like to filter on. A good source for an accurate DN string is through the use of the ADSI Edit tool. When adding multiple groups to sync filters, use the full DN strings separated by the pipe symbol. An example is as follows: CN=LastPass, OU=Groups, OU=USA, DC=yourdomain, DC=com CN=LastPass2, OU=Groups, OU=USA, DC=yourdomain, DC=com
When you have completed the configuration, click 'Sync to LastPass'. The LastPass Client will continually 'listen' for changes in your active directory and continue to add and remove users. The application window can be closed and the app will continue to run in the system tray.
[/accordion-item] [accordion-item title="Active Directory FAQs" id="h3]
Do I need to designate a specific computer to run the AD sync client?
No, you can run the service on multiple computers for redundancy. The computers do not need to be dedicated to this purpose. The computer must be running Windows XP or later and can be a so workstation or server. If a part of the AD sync client requires very little computer resources (memory, disk, CPU). The sync client also should be deployed within your firewall such that it can connect directly to your AD or LDAP server.
Do I need a designated admin account used for AD Sync?
There is no need for such account. You only need to enter your credentials on LastPass AD Sync Configuration window to authenticate your right as an admin to modify the configuration. The actual syncing authentication takes place using a token that is handled separately. It is not bound to the account you used to setup the configuration in any way.
If I add a new person to my AD directory, how will that update in LP and how often does it check for changes? $\hat{\pmb{\varphi}}$
Once started, the AD sync client will register itself with your AD server. ��When a change occurs, such as when a user is added, updated, or deleted, then the sync client will immediately re-check for changes.
If I had previous users not added via AD, what happens to those users?
And any previous users that were added (manually or via another provisioning tool), \$ will be cross-checked with what is listed in AD. If the user is not listed in AD, the sync client will ignore the existing users. If the user is listed and there are any changes (ex: disabled), the client will update the account in LastPass with the changes it finds in AD.
Can I manually sync, automatically sync AD, both?
Both.��To automatically sync, simply leave the AD sync client running and it will detect changes and sync when needed.��To manually sync changes, simply start the AD sync client on an as-needed basis.
Does it work with other LDAP directories?
Yes.

I have thousands of names in my AD, will it time out while sending to LastPass?

The AD sync client has been successfully tested with AD servers having more than 10,000 users.

If I have admin accounts built into our AD directory how do I make sure that they don't import into LastPass?

You can control what users are imported in two ways:

a) By specifying a sync filter within the AD sync client to include only certain groups.

and/or

b) By specifying within the AD sync client that users be added as 'pending' and then later having an admin manually approve users from within the Enterprise Administration console.

How do I keep the name of the group from my AD directory in line with the LastPass groups?

On the AD sync client configuration screen, there is an option labeled 'Sync user groups from AD' that can be enabled.

Do you support nested group?

No, nested group is not currently supported. You may have to add multiple groups to group filters as a workaround.

AD@provisioning@didn't work, what do I do?

Click on the 'Show Debug' link within the AD sync client. Copy the debug log to a text file and open up a support ticket at **%https://lastpass.com/support. php%** and attach the file to the ticket for us to investigate.

Do groups sync and work with Shared Folders, or just policies?

Yes, groups can be mapped to both Shared Folders and policies. When a new user is added to a group, all policies and folders already assigned to the group will be automatically assigned to the new user. The folder will become available to the new user as soon as there is login activity by another sharee.

Is any functionality of grouping lost when syncing them via AD?

No, the functionality is still available.

Does Active Directory Sync run as a service?

Yes. Once you setup and run the AD LDAP sync client it will run as a persistent service. If you restart your computer, the AD Sync client will automatically restart on reboot.

What exactly is accessed and how is it transferred?

Username, name, group membership, email and account status, it's transferred via SSL to LastPass.

Will accounts created without AD sync be affected by the sync client?

No, accounts created via other means will not be synced with the client except for groups created by the AD.

The domain we log into is different than our email address. Will users be able to log into LastPass using their AD credentials?

 No - we create accounts based on the value stored as their email address in AD.

How I can make sure AD passwords and LastPass master passwords are in sync?

See this FAQ here: https://lastpass.com/support.php? cmd=showfaq&id=4456.

I'm having issues with the client, is there a debug I can send you?

Yes you can. The client will generally produce a debug automatically, and can be@found here: C:\ProgramData\LastPass\lpldap.dbg. Send this file, along with a description of your issue to the Support team by opening a support ticket here -@https://lastpass.com/supportticket.php?lpnorefresh=1.

[/accordion-item]

[/accordion]

User Groups - for Policies and Shared Folders

[accordion openfirst=true scroll=true clicktoclose=false]

User groups can be utilized to assign **policies** and/or **Shared Folders**. From the 'User Groups' sub-tab you are able to create user groups manually within LastPass Enterprise. Alternatively, for those that have elected to use the **Alternatively**. A client, the client can be configured to sync user groups automatically from your active directory.

To manually create a new group simply hit Add Group and type in the name of the Group, for example, 'Executive Team' or 'Marketing'. Then simply type in the username of the appropriate employees, and hit 'Save'. Once the group has been saved, you can jump to either policies or Shared Folders, and assign either to the group accordingly.

LastPass	***						
ENTERPR	ISE		HOME	SETUP	SAML	USERS	
USERS> USERS	CREATE NEW USER	USER GROUPS	PENDING USERS	LOGOFF			
	Groups			×			
A	Name:						
	G			_		Users	
	Ar Enter recipien	t email address				1	
	Ar					0	
	Ay					5	
	bo					0	
	B¢					1	
	Ci					1	
	de					0	
	dr					1	_
	dr					1	
	er Docc:					1	
	er					1	
	E>					3	
	Fc		Cancel	Save		1	
	Folder Full View					2	
	Folder Restricted View		-			1	
	Group1		-			1	
	Group2		-			0	

[/accordion]

Install Software

[accordion openfirst=false scroll=true clicktoclose=true]

Please take a moment to watch a video about our different@installation@options@offered@in LastPass Enterprise:

[accordion-item title="Downloading the LastPass Enterprise Client Software" id="h0"]

Download the appropriate LastPass Enterprise Client software depending on your operating system:

 For
 https://lastpass.com/lastpass_x64full.exe@(@Windows Vista, Windows Vista, Windows

[/accordion-item] [accordion-item title="Choose An Install Option That Best Suits Your Organization's Needs" id="h1"]

OPTION A: Manual Installation Using the GUI Install Wizard

Double click the downloaded file to open the GUI install wizard and follow the steps.

LastPass requires administrative rights to be installed. If required, the installer will prompt you for your Administrator's credentials, which you will have to manually enter.

OPTION B: Silent Installation From an@Administrative@Command Prompt

Open an **Administrative command prompt** and run the LastPass client software as follows:

For 32bit	lastpassfull.exe -siuserinstallieuserinstallffuserinstallchrome
Windows	installforallusers -j "C:\Program Files\LastPass"
For 64bit Windows	lastpass_x64full.exe -siuserinstallieuserinstallffuserinstallchrome installforallusers -j "C:\Program Files\LastPass"
For Mac OS X:	sudo installer -pkg lpmacosx.pkg -tgt /

You can use this option in combination with a login batch file to automate installation.

OPTION C: Install MSI File Using GPO (Group Policy Object)

- Download the MSI Installer.
- If you do not want to use our Windows Login Integration to automatically provision and log users in, skip to the final step.
- If you want to use automatic provisioning, you will need to use Microsoft's Orca to edit the MSI to assign the necessary parameters.
- Add the following variables under the properties table (CID and CHSH is unique to each Enterprise, the correct values are found in the Admin Console):

 CID
 (generated automatically in LastPass Enterprise Admin console)

 CHSH
 (generated automatically in LastPass Enterprise Admin console)

 DL
 your domain name

- WINLOGIN -winlogin
 - Save the MSI and close Orca. �(If you leave Orca open and try to run the MSI, it will fail)
 - Setup a Software Installation via a GPO and specify lastpass.msi as the install package.

[/accordion-item] [accordion-item title="Customized Installation Options" id="h2"]

All of the above options, will install the LastPass extension into Internet Explorer (Windows only), Firefox and Chrome as well as LastPass for Applications on Windows and the Safari extension on Mac OS X. View below for additional installation command line arguments for Windows.

dl demoinleain

Udulada . Namida and 42 ke sacadad 42 Ududada darana 42 ani42 and 1 ke

	5 II
LastPass	
-cid,companyid	WinLogin : LastPass provided cid value
-chsh,companyidhash	WinLogin : LastPass provided chsh value
-hidewlemail,hidewlemail	WinLogin : Hide 'Work Email' fields on setup
-hidewlalready,hidewlalready	WinLogin : Hide 'I Already Have a LastPass Account' button on setup
-uninstallwinlogin,uninstallwinlogin	WinLogin : Uninstall Windows Login integration. To be used in conjunction with
uninstall switch.	
-winlogin,winlogin	WinLogin : deprecated
-d,debug	Writes c:\lpdebug.txt to examine an issue
-si,silinstall	Silent Install
-sb,siluninstall	Silent Uninstall
-b,uninstall	Uninstall
-j,installdir	Directory to install into
-i,userinstallie	Install IE plugin
-f,userinstallff	Install FF plugin
-c,userinstallchrome	Install CR plugin
-lang,language	Default language for plugins
-delay,delay	Sleep for X seconds before doing anything
-sys,sys	Restarts EXE as high integrity process
-noshut,noshut	Do not shutdown browsers (improper install)
-nousewininet,nousewininet	Do not use Wininet for network communication
-nouninstallsurvey,nouninstallsurvey	Do not open the Uninstall Survey if the user uninstalls
-nolastappstartup,nolastappstartup	Do not Add Startup Shortcut for LastPass for Applications
-nar,noaddremove	Don't add an entry to Add or Remove Programs
-nsm,nostartmenu	Don't create a Start Menu Programs group
-ndp,nodisablepwmgrs	Don't disable browser password managers
-dnot,disablenotes	Disable Secure Notes Feature (Does not apply to Chrome)
-dide,disableidentities	Disable Identities Feature
-dvau,disablevault	Disable Vault Feature
-dcon,disablecontext	Disable Context Menus
-dexp,disableexport	Disable Export Feature
-dimp,disableimport	Disable Import Feature
-dsha,disablesharing	Disable Sharing Feature
-dpri,disableprint	Disable Print Feature

[/accordion-item] [/accordion]

LastPass Provisioning API

[accordion openfirst=false scroll=true clicktoclose=false]

LastPass exposes a public API that can be used by enterprise accounts to create users, deprovision users, and manage groups.

We are often asked about the difference between the AD Sync Client and the API. The main difference is that unlike the API, the AD Sync Client requires 0 coding/integration. The API is more powerful, but requires some integration by you to avoid having to duplicate actions.

Out of the box, the AD Sync Client will automatically track changes to your AD/LDAP server (new user is added, existing user removed/disabled, user changes groups, etc.) and invoke appropriate actions for LastPass

accounts. Similarly if you delete or disable a user in their AD, the associated LastPass account will also be disabled. These functions are also supported using the API, however they require integration on your part.

For a full list of the API details and instructions, please go to the: **@**Enterprise Console > Setup > Create New Users > LastPass Provisioning API option.

If you would like to use the API to automatically add users to shared folders, you will need to perform encryption operations yourself. Thus, you will need to know some things about the underlying encryption operations LastPass uses. They will be documented below.

[accordion-item title= "Adding a User" id="h1"]

The first step is adding the user. You must first choose the number of PBKDF2 iterations you plan to use. LastPass currently recommends 5000 as a balance between security and performance.

const unsigned char *usemame = "user@lastpass.com"; const char *password = "T5089kkUMGYT"; int iterations = 5000; unsigned char key[32]; PKC55_PBKDF2_HMAC(password, strlen(password), username, strlen(username), iterations, EVP_sha256(), 32, key);

If this function call succeeds, the user's encryption key will be present in the variable "key".

Now that you have the user's encryption key, you can use it to generate the user's password hash. This is the hash that's passed to the adduser API as parameter passwordhash. Here is an example, continuing from the above:

unsigned char hash[32]; PKCS5_PBKDF2_HMAC(key, 32, password, strlen(password), 1, EVP_sha256(), 32, hash);

If this function call succeeds, the user's password hash will be present in the variable "hash". Please note that you should hex-encode the hash before passing it to LastPass. Thus, passwordhash should always be 64 hexadecimal characters.

[/accordion-item] [accordion-item title= "Generating RSA Keys" id="h2"]

In order to immediately add the user to shared folders, you will also have to pass rsapublickey and rsaprivatekeyenc to the adduser command.

First, generate an RSA public/private key pair. This key must be 2048 bits.

Next, encode the public key in ASN.1 DER format. Then, hex-encode it. This is the value for rsapublickey that will be passed to LastPass. Click here to see an example of a valid rsapublickey.

Next, encode the private key in ASN.1 DER format. Then, hex-encode it. This is the value for rsaprivatekey that you will have to encrypt with the user's encryption key before passing it to LastPass. Click here to see an example of a valid rsaprivatekey.

Next, encrypt the rsaprivatekey using the user's encryption key. First, prepend "LastPassPrivateKey<" and append ">LastPassPrivateKey" to the rsaprivatekey. Then, encrypt via AES-CBC, using the first 16 characters of the user's encryption key as the IV. Pad via PKCS#7. Hex-encode the result to create rsaprivatekeyenc, which can then be passed to LastPass.

Once you have the passwordhash, rsapublickey, and rsaprivatekeyenc, you should be able to perform an adduser API call.

[/accordion-item] [accordion-item title= "Adding a User to a Shared Folder" id="h3"]

Now that you have created a user with valid RSA keys, you will be able to use the addusertosharedfolder API to add them to a shared folder.

First, retrieve the ID and encryption key for the shared folder you would like to add the user to. Click here to see these values for the shared folders you are in.

Next, you must encrypt the shared folder's encryption key with the user's RSA public key, first padding with OAEP. Hex-encode the result, which should end up being 512 hexadecimal bytes since you're using a 2048-bit RSA key. The result is what you should pass to LastPass as sharekey.

Next, you must encrypt the shared folder's name using the shared folder's encryption key. Be sure to encrypt the full name, including the "Shared-" prefix. For

'53/92

Once you have shareid, sharekey, and sharename, you should be able to perform an addusertosharedfolder API call.

[/accordion-item] [/accordion]

Users Tab

[accordion openfirst=false scroll=true clicktoclose=false]

The User's tab of the Admin Console includes all of the tools that you need to manage your users.

- The 'Users' sub-tab: Delete users, make Admin, view 'User Details' report, Password Reset (only with 'SuperAdmin-Password Reset' policy enabled)
- The 'Create New User' sub-tab: Provision new users
- The 'User Groups' sub-tab: Create user groups for purposes of assigning policies and Shared Folders
- The 'Pending Users' sub-tab: for Active Directory Sync users only

Please see the video below to learn more about the Users Tab:

[/accordion]

Reporting - Notifications

[accordion openfirst=true scroll=true clicktoclose=false]

[accordion-item title="The Notifications Report" id="h0"]

		Ŷ						
LastPass	****							📟 ENGLISH 🕑
ENTERP	PRISE			HOME	SETUP	USERS	REPORTING	SAML
REPORTING>	LOGINS	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATIC	INS LO	GOFF		

Add Notification | View History | Never Notify List | Upcoming Emails

The Notifications Report is a summary of various critical user statuses around which additional education or training may be warranted. These statuses include such criteria as 'inactive user', 'over 3 duplicate passwords' and 'over 5 weak passwords'. You can set up which notifications you would like to see on this page under the Add Notifications link. The goal of this report is to help optimize the use of LastPass among your end users to help improve the security of your company's digital assets. This report is your first line of defense in the campaign to educate users on the importance of good password hygiene, and how to get there.

The Notifications Report also includes quick and easy email templates that can be programmed by the administrator to dispatch automatically on a configurable timeframe.

[/accordion-item] [/accordion]

Push Sites to Users

[accordion openfirst=false scroll=true clicktoclose=true]

LastPass Enterprise Admins have the option to directly place a site in a user's vault through our new Push Sites to User feature. This feature is helpful when you would like to pre-populate a site in a user's vault so the user will have this site to use upon his or her first login to LastPass. Push Sites to Users is also helpful when used to push SAML specific URLs to services you have linked to your Enterprise to using LastPass SAML.

Admins should note that Push Sites to Users is a much different feature than **Shared Folders.** Push Sites to users places the site entry directly into a user's vault, rather than in a central folder accessible to all as with Shared Folders. Once pushed, a site cannot be removed from a user's vault by the Admin, as it is in the individual's vault like any other site entry the user may have saved. When considering which sites to push to users, please remember that you cannot remove this site at a later time.

Another unique aspect of Pushed Sites is that due to how the technology behind pushing sites works, any data you elect to push to your users is accessible on LastPass servers in unencrypted form until the data is pushed to a user. \blacklozenge Once pushed to a user, the data will leave the LastPass server and be encrypted in the user's individual vault. \blacklozenge This is NOT the case with Persistent Pushes, which will stay on the LastPass server until deactivated or deleted. \blacklozenge For more information on Persistent Pushes please see below.

[accordion-item title="How to push sites to your users" color="Accent-Color" id="h1"]

To push sites to your users, first login to your Enterprise Admin Console, and navigate to the Setup Tab. From there, you will see a sub-heading for Push Sites to Users. Once clicking the sub-heading, you will see a straightforward menu on what information to fill out when pushing sites to users:

	ass ****	3					💻 ENGLISH (€	
CNI	CRFRIS	3		HOME	SETUP	USERS	REPORTING	SAML	
SETUP>	POLICIES	CREATE NEW USER	INSTALL SOFTWARE	PUSH SITE	S TO USERS	LOGOE	F		

Push Sites to Users

Click here to view a log of previously pushed sites

This tool allows you to push sites or URLs into the LastPass accounts of one or more users within your company.

LastPass also exposes a public API that can be used to push sites programmatically. For full API details, please click here.

NOTE: Any data you enter here will be accessible to LastPass until the user(s) log into LastPass next, and the data is pushed into their account(s). For persistent pushes, the data will be accessible until the persistent push is deleted.

Upload a CSV Choose File No file chosen file:

User(s):	Please Select
URL:	
Name:	
Group:	
Username:	User's full email address
Password:	Click here to enter a password
Notes:	
Favorite	
Data is	Non-
encrypted	None NOTE: You must perform this encryption yourself. Please click here
with shared	for help with this feature.
folder:	
Push Site	
The first	option you have when pushing sites to users is to upload a CSV file
download	d a sample CSV and learn the format and information needed to do this,
use the S	Sample CSV file provided.
To manua	ally add custom fields to a site that is being pushed via CSV, you can
follow thi	is format:
fieldnam	e0, field type0, field value0, field name1, field type1, field value1
usemani	enera, text, newuser, passwordnera, password, abc125
This will	vield a text field with name username, field and value newuser, and a
password	field with name passwordfield and value abc123
The seco	nd option to use is to manually fill out the site data that you'd like to push sets ΦT_0 do this, you need to fill out this key information:
to your u	

- User(s): Select the User or User Groups you'd like to push the site to. You can also select to push to All current and future users in the Enterprise, or all current and future members of a User Group.
- 2. URL: The URL of the site entry that you'd like to push
- 3. Name: �� The name you would like the site entry to have in the users' vaults
- Group: The name of the group you'd like this site to be added under in the users' vaults
- 5. Username: The username the users will utilize to login to the site. You can select to have this be the individual's full email address that is used as their LastPass account name, ONLY the username portion of their email, OR a custom username you manually enter
- 6. Password: The password that will be used to login to the individual site
- Notes: Any notes that you would like to be entered into the notes portion of the site entry
- 8. Favorite: O Designate whether or not you'd like this site to be marked as a Favorite in users' vaults

Once you are have filled out this relevant information, you can now push the site to your user(s)! To receive the item, users must have logged out and back in via the plugin at least once.

[/accordion-item]

[accordion-item title="Persistent Site Pushes" color="Accent-Color" id="h2"]

[/accordion-item]

[accordion-item title="Previously Pushed Sites" color="Accent-Color" id="h3"]

At the top of the Push Sites to Users page is a link to view a log of previously pushed sites. This link takes you to a view of ALL previously pushed sites. This is where you can deactivate or remove persistent pushes.

SETUP>	POLICIES	CREATE NEW USER	INSTALL SOFTWARE	PUSH SITES TO USERS	LOGOFF	

Push Sites to Users

Bac	lack						
	Name	User(s)	Persistent?	Active?	Action		
	google.com	Group: Domain Users	Yes	Yes	Details Deactivate Delete		
	Yahoo	Group: test1250	Yes	Yes	Details Deactivate Delete		

This page shows the name of the pushed site, which users or user groups it was pushed to, whether or not it was persistent, and whether or not the push is still active. You can take three actions on this page regarding the previously pushed sites:

- 1. **Details:** Viewing Details shows the individual users that had the site pushed to them.
- Deactivate: Hitting deactivate prevents persistent pushes from being pushed to new users. This effectively turns the persistent push "off." Sites can be reactivated at a later time to be "re-pushed" to any new users that have been added since the push was deactivated.
- Delete: It is permanently deletes the pushed site from the system. It is will not remove the site entry from the individuals' vaults, but only the push from the LastPass servers.

If you have any more questions on pushing sites to users, please contact our support team for more information.

[/accordion-item] [/accordion]

Pending Users (Only for Active Directory Sync Client Users)

[accordion openfirst=true scroll=true clicktoclose=false] [accordion-item title="The Pending Users Sub-tab" id="0"]

This tab is strictly for those companies that have chosen to utilize the **AlastPass** AD Client to sync with Active Directory and who have configured the client such that new users from AD are added to LastPass as pending, rather than being automatically provisioned. To provision a LastPass account for a pending user, select the user and then click on 'Accept Checked'. Upon this action, LastPass will automatically provision an account and dispatch an automated welcome email to the user. To remove a user from the list, select the user(s), and click 'Reject Checked."

U		USERS	CREATE NEW USER	USER GROUPS	PENDING USERS	LOGOFF		
Sea	rch:						Accept Checked	Reject Checked
	∨ Userna	me			Name	Statu	s Select (Select	ed t All)
	ad101@	lastpass.co	m		ad101	Pendi	ng	

ad103@lastpass.com	ad103	Pending
ad104@lastpass.com	ad104	Pending 🔲
ad105@lastpass.com	ad105	Pending
ad109@lastpass.com	ad109	Pending

[/accordion-item] [/accordion]

Reporting

[accordion openfirst=false scroll=true clicktoclose=true]

LastPass offers extensive reporting geared at helping you safeguard your data and build compliance:

- Logins: Every login, password/username update, or form fill attempted or completed by your LastPass Enterprise users.
- Shared Folders: A summary of all Shared Folders under your Enterprise account, including assigned staff and their access rights relative to each folder.
- Admin Events: A log of most activities taking place with the Admin Console.
- Notifications: A user status summary report combined with easy-to-use email templates designed to automate end user alerts relative to Lastpass inactivity or sub-optimal use.

[accordion-item title="Login Reporting" id="h1"]

LastPass **** ENTERPRIST	3		HOME	SETUP	USERS	REPORTING	ENGLISH SAML
	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATIO	NS LO	GOFF		
				F	REPORTING N	IODE: Show All Lo	ogins (What is this?)
LastPass exposes a public A	PI that can be used by enterp	rise accounts to pul	l reporting data	. For full AP	I details, plea:	se click here.	
From 11/13/2013							
то 11/13/2013			Even	ts For	All Use	ers	
Search						Event Key 🎒	Export to Excel
User All Users	•						
Submit							
Time 2013-11-13 22:06:58	Username enterprise3@lastpass.com	IP Address 70.167.240.233	Login		Data		
2012 11 12 22:05:27	ontorpriso2@lastnass.com	70 167 240 222	Login		google.com		
2013-11-13 22:03:37	enterprises@iastpass.com	70.107.240.235	Login		google.com		
2013-11-13 22:00:20	enterprise3@lastpass.com	70.167.240.233	Login		google.com		
2013-11-13 09:59:52	shlomit@netrot.net	67.171.11.194	Failed Login /	Attempt			Event Key

The Login Report is a comprehensive log of every login, password/username update, form filled, and site deletion that is attempted or completed by your LastPass Enterprise users. The reports can be filtered by date range, or by user and can be exported to Excel for back up. There is a link on the page to a key explaining what each action designation means.

[/accordion-item] [accordion-item title="Shared Folders Reporting" id="h2"]

This report offers a master view of every Shared Folder created under the Enterprise. You can click on the column headings to sort alphabetically or by user. You can drill down on each folder to see the particular sites and notes that are contained within, as well as all assigned users and the specific access rights granted to each (ie: hidden or visible access to the credentials, admin rights, read-only(write.)

This report is read only. To guarantee Admin access to every Shared Folder created within the enterprise - including the login credentials of the stored entries, you must enable the 'Super Admin - Shared Folders' policy.

[tabbed_section][tab title="Top Level View" id="t1"]

Shared Folder Report sorted alphabetically:

LastPass	****						ENGLISH	♥
ENTERP	RISE		HOME	SETUP	USERS	REPORTING	SAML	
			NOTIFICATIO		COFE			

Add Shared Folder

Shared Folders

▼Folder Name	Security Score	Number of Accounts	Number of Users	Users	Action
2test 60000			2	enterprise3@lastpass.com, enterprise1@lastpass.com	View
			2	enterprise7@lastpass.com, enterprise3@lastpass.com	View
Ax			3	enterprise7@lastpass.com, dana@netrot.net, enterprise3@lastpass.com (invisible)	View
blahblahblah			1	enterprise3@lastpass.com	View
Citysearch test			1	enterprise3@lastpass.com	View

[/tab]

[tab title="Individual Shared Folder View" id="t2"]

Detailed view of an individual shared folder:

RE	EPORTING>	LOGINS	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATIONS	LOGOFF		
Sh U	nared F sers	older: (Client A Te	st				Go back
	vUsername			Can Administer	Read-Onl	у	Can View Passwords	
	enterprise3@	lastpass.com		No	Yes		No	
S	ecurity	y Score	e					

Security information is not available for this shared folder. As clients check in and submit security data, it will appear here.

	Domain								
I ive.com Improved the interprise in	🗋 gro	oup							
Image: microsoftonline.com d_section] dion-item] ion-item title="Admin Events Reporting" id="h3"] e Admin Events Report provides a detailed breakdown of all administrative tons taken via the Admin Console. asstPass ***** e Admin Events Report provides a detailed breakdown of all administrative tons taken via the Admin Console. asstPass ***** e Admin Events Report provides a detailed breakdown of all administrative tons taken via the Admin Console. asstPass ***** e NOME SETUP USERS REPORTING Admin Events Report provides a detailed breakdown of all administrative tons taken via the Admin Console. e NOME SETUP USER REPORTING tons LOGONS tons StakeD FOLDERS Admin Events By All Users RePORTING MODE: Show All Logins (What is the Admine ton the used by enterprise accounts to pull reporting data. For full API details, please click here. from 11/05/2013 Event Key Seport to Excel User Additions Loginy submit IP Address Action Data 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Add Policy Prohibit Unrestricted Mobile Logins <t< td=""><td>B live</td><td>e.com</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	B live	e.com							
d_section] iion-item] ion-item title="Admin Events Reporting" id="h3"] # Admin Events Report provides a detailed breakdown of all administrative ions taken via the Admin Console. # ENGLISH ENT E R P R IS & HOME SETUP USERS REPORTING SAML # OME SETUP USERS REPORTING SAML # OME SETUP USERS REPORTING SAML # OME SETUP USERS REPORTING SAML # CONTING" LOGINS SHARED FOLDERS ADMIN EVENTS NOTFICATIONS LOGOFF REPORTING MODE: Show All Logins (What is the Pass exposes a public API that can be used by enterprise accounts to pull reporting data. For full API details, please click here. # THOME SETUP USERS By All USERS # REPORTING MODE: Show All Logins (What is the # Admin Events By All USERS # Event Key ■ Export to Excel User At Users 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy 2013-11-06 22:00.45 enterprise3@lastpass.com 70.167.240.233 Edit Policy # Complexity Prohibit Unrestricted Mobile Logins # Exert Key Pontist Unrestricted Mobile Logins # Event Key Pontist Unrestricted Mobile Logins # Pontist Key # Event Key # Event Key # Pontist Unrestricted Mobile Logins # Pontist	🅅 mi	crosoftonline.co	m						
Admin Events Report provides a detailed breakdown of all administrative STERPRISE MORE SETUP USERS REPORTING SAML MORE SETUP USERS REPORTING SAML PORTING LOGINS MARED FOLDERS ADMIN EVENTS NOTIFICATIONS LOGOFF REPORTING MODE: Show All Logins (What is 1 rass exposes a public API that can be used by enterprise accounts to pull reporting data. For full API details, please click here. From 11/06/2013 To 11/13/2013 Search Search Submit Trice Username Prise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/Yiew 2013-11-06 22:0045 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except April 1004	d_sectio lion-iter ion-iter	on] m] n title="Admin	Events Reporting" id="	"h3"]					
ENCIRCING LOGINS SHARED FOLDERS ADMIN EVENTS NOTFICATIONS LOGOFF CPORTING ADDE: Show All Logins (What is to the service of	ne Admir tions tal	n Events Report ken via the Adr	provides a detailed brennin Console.	eakdown of all admini	strative				
ENTERPRISE HOME SETUP USERS REPORTING SAML EVENTING> LOGINS SHARED FOLDERS ADMIN EVENTS NOTIFICATIONS LOGOFF REPORTING MODE: Show All Logins (What is the set of	LastP	ass *** *							📟 ENGLISH 🤇
PORTING> LOGINS SHARED FOLDERS ADMIN EVENTS NOTIFICATIONS LOGOFF REPORTING MODE: Show All Logins (What is the Parase exposes a public API that can be used by enterprise accounts to pull reporting data. For full API details, please click here. From 11/06/2013 To 11/13/2013 Search 11/13/2013 Search 11/13/2013 Submit Submit Time Username IP Address Action Data Submit 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin	ΕΝΤΘ	ERPRISE			HOME	SETUP	USERS	REPORTING	SAML
PORTING> LOGINS SHARED FOLDERS ADMIN EVENTS NOTFICATIONS LOGOFF REPORTING MODE: Show All Logins (what is the state of the stat									
Interference Description Description Description Description From 11/06/2013 Interference Admin Events By All Users Search Interference Event Key Septent to Excel User All Users Event Key Septent to Excel Time Username IP Address Action Data 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin									
Prom 11/06/2013 To 11/13/2013 Search III Users Submit Submit Time Username 111/12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin	PORTIN	IG> LOGINS	SHARED FOLDERS		NOTIFICAT	ONS L	OGOFF		
trom 11/06/2013 To 11/13/2013 Search	EPORTIN	ig> logins	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATI	ONS L	OGOFF		
From 11/06/2013 To 11/13/2013 Search	EPORTIN	IG> LOGINS	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATI	ONS L	ogoff Reporting I	MODE: Show All L	ogins (What is t
From 11/06/2013 To 11/13/2013 Search	EPORTIN	ig> logins	SHARED FOLDERS	ADMIN EVENTS	NOTIFICAT	ONS L	ogoff REPORTING	MODE: Show All L	ogins (What is t
From 11/06/2013 To 11/13/2013 Search	EPORTIN Pass exp	IG> LOGINS oses a public AP	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATI	ONS L ta. For full Af	OGOFF REPORTING Pl details, plea	MODE: Show All L ase click here.	ogins (What is t
To 11/13/2013 Search Event Key Export to Excel User All Users Submit Submit Submit P Address Action Data 2013-11-21 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin	EPORTIN Pass exp	IG> LOGINS oses a public AP	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATI	ONS L ta. For full Al	OGOFF REPORTING I PI details, plea	MODE: Show All L ase click here.	ogins (What is t
To 11/13/2013 ACITITIE EVENUES BY AN OSETS Search Event Key Export to Excel User All Users Submit Submit 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin	PORTIN Pass exp From	IG> LOGINS oses a public AP	SHARED FOLDERS	ADMIN EVENTS	NOTIFICAT	ONS L ta. For full Al	OGOFF REPORTING I PI details, plea	MODE: Show All L ase click here.	ogins (What is ti
Search Image: Submit Event Key Seport to Excel Submit Submit Submit Image: Submit 2013-11-12 19:18:43 enterprise3@lastpass.com Atlon Data 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin	PORTIN Pass exp From	IG> LOGINS oses a public AP 11/06/2013	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATI	ONS L	OGOFF REPORTING I PI details, ple:	MODE: Show All L ase click here.	ogins (What is ti
Search Event Key Export to Excel User All Users Submit P Address Action Data 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin Event Key	PORTIN Pass exp From To	IG> LOGINS oses a public AP 11/06/2013 11/13/2013	SHARED FOLDERS	ADMIN EVENTS	NOTIFICAT reporting da	ONS L ta. For full Al Events	OGOFF REPORTING I PI details, plea B By All	MODE: Show All L ase click here.	ogins (What is t
User All Users Submit Submit 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin	PORTIN Pass exp From To	IG> LOGINS oses a public AP 11/06/2013 11/13/2013	SHARED FOLDERS	ADMIN EVENTS	NOTIFICAT reporting da	ONS L ta. For full Al Events	OGOFF REPORTING I PI details, plea B By All	MODE: Show All L ase click here.	ogins (What is ti
Submit Submit Submit Time Username IP Address Action Data 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin Event Key	PORTIN Pass exp From To Search	IG> LOGINS oses a public AP 11/06/2013 11/13/2013	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATI	ONS L ta. For full Af	OGOFF REPORTING I PI details, plea By All	MODE: Show All L ase click here.	ogins (What is ti Export to Excel
Submit Submit Submit Submit Time Username IP Address Action Data 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin Event Key	PORTIN Pass exp From To Search User	IG> LOGINS oses a public AP 11/06/2013 11/13/2013 All Users	SHARED FOLDERS	ADMIN EVENTS	NOTIFICATI	ONS L ta. For full Al	OGOFF REPORTING I PI details, plea	MODE: Show All L ase click here.	ogins (What is ti Export to Excel
Time Username IP Address Action Data 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin Event Key Event Key Event Key Event Key	PORTIN Pass exp From To Search User	IG> LOGINS oses a public AP 11/06/2013 11/13/2013 All Users	SHARED FOLDERS	ADMIN EVENTS	NOTIFICAT reporting da	ONS L ta. For full Al	OGOFF REPORTING I PI details, plea	MODE: Show All L ase click here.	ogins (What is t Export to Excel
Time Username IP Address Action Data 2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin Event Key	PORTIN Pass exp From To Search User	IG> LOGINS oses a public AP 11/06/2013 11/13/2013 All Users Submit	SHARED FOLDERS	ADMIN EVENTS terprise accounts to pull	NOTIFICAT	ONS L	ogoff REPORTING I PI details, plea	MODE: Show All L ase click here.	ogins (What is t
2013-11-12 19:18:43 enterprise3@lastpass.com 70.167.240.233 Add Policy Require Password Reprompt on Copy/View 2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin Event Key	PORTIN Pass exp From To Search User	IG> LOGINS Oses a public AP 11/06/2013 11/13/2013 All Users Submit	SHARED FOLDERS	ADMIN EVENTS terprise accounts to pull	NOTIFICATI	ONS L ta. For full Al	OGOFF REPORTING PI details, plea	MODE: Show All L ase click here.	ogins (What is ti Export to Excel
2013-11-06 22:00:45 enterprise3@lastpass.com 70.167.240.233 Edit Policy Prohibit Unrestricted Mobile Logins Except Approved by Admin	PORTIN Pass exp From To Search User Time	IG> LOGINS oses a public AP 11/06/2013 11/13/2013 All Users Submit	SHARED FOLDERS	ADMIN EVENTS terprise accounts to pull	NOTIFICAT reporting da	ons L ta. For full Al Events	ogoff REPORTING I PI details, plea By All	MODE: Show All L ase click here.	ogins (What is ti Export to Excel
Event Key	PORTIN Pass exp From To Search User Time 2013-1	IG> LOGINS oses a public AP 11/06/2013 11/13/2013 All Users Submit	SHARED FOLDERS	ADMIN EVENTS terprise accounts to pull terprise accounts to pull IP Address accom 70.167.240.23	NOTIFICAT reporting da dmin dmin Action 33 Add P	ONS L ta. For full Al Events N Dat olicy R	ogoff REPORTING I PI details, plea By All By All equire Passw opy/View	MODE: Show All L ase click here.	ogins (What is ti
	PORTIN Pass exp From To Search User Time 2013-1	IG> LOGINS oses a public AP 11/06/2013 11/13/2013 All Users Submit 1-12 19:18:43 1-06 22:00:45	SHARED FOLDERS	ADMIN EVENTS terprise accounts to pull terpr	NOTIFICAT reporting da dmin dmin 33 Add P	ONS L ta. For full Al Events olicy R c olicy P E	oGOFF REPORTING I PI details, plea By All By All equire Passw opy/View	MODE: Show All L ase click here.	ogins (What is ti Export to Excel

Report Functions

- Create, delete, disable, or reactive an employee account.
- Reset a user's password
- Toggle a user as an Admin.
- Remove a user from the company.
- Add, delete or edit policies.
- Add, edit or delete User Groups.
- Update Policy Users.

The full list of messages and their meanings can be found here.



NG> LOGINS SHARED FOLDERS

NOTIFICATIONS LOGOFF

Add Notification | View History | Never Notify List | Upcoming Emails

ADMIN EVENTS

The Notifications Report is a summary of various critical user statuses around which additional education or training may be warranted. These statuses include such criteria as 'inactive user', 'over 3 duplicate passwords' and 'over 5 weak passwords'. �You can set up which notifications you would like to see on this page under the Add Notifications link. � The goal of this report is to help optimize the use of LastPass among your end users to help improve the security of your company's digital assets. This report is your first line of defense in the campaign to educate users on the importance of good password hygiene, and how to get there.

The Notifications Report also includes quick and easy email templates that can be programmed by the administrator to dispatch automatically on a configurable time-frame.

[/accordion-item] [/accordion]

LastPass Single Sign-on for Applications that Support SAML

[accordion openfirst=false scroll=true clicktoclose=true]

LastPass Single Sign-on allows you to utilize your LastPass account as the single sign on point for a growing number of domains and associated services.

LastPass Single Sign-on uses SAML 2.0 to allow your employees to access their favorite services simply by being logged into LastPass. \diamond Once logged into LastPass, and navigating to the service's URL, \diamond the user will bypass the \diamond login screen altogether. The authentication will take place on the back end between LastPass (the Identity provider) and the desired application (the Service Provider). All access rights will be managed centrally by your LastPass Adminstrators through the Admin Console.

Please note: Using SAML does not prevent you from logging in with previous domain password, or prevent your mobile device from accessing via the account password.

[accordion-item title="Setting up SAML in LastPass Enterprise" color="Accent-Color" id="h2"]

To set up SAML in LastPass Enterprise, first go to your Enterprise Console, and select the SAML tab at the top of the console. You will then be taken to the main SAML page:



💴 ENGLISH 🕑

SAML

Submit

'LastPass Enterprise Manual' SAML. Upon clicking on the icon, you will then be shown a page with specific instructions on how to setup SAML for that app:

	All Users	•		
All Users 😵				
ntity ID:	google.com/a/lastpass.com			
aunch URL:	http://mail.lastpass.com			
Update				
utomatic creation of users is enabled for this ush this site into users' vaults	domain. Regenerate OAuth key.			
All Users 😣	All Users	T		
ntity ID:	google.com/a/xmarks.com			
aunch URL:	http://mail.xmarks.com/			
Update				
nable automatic creation of users for this do ush this site into users' vaults	main.			
l another domain				Manage Groups
bushing a site to your asers and	pre-populating then vaules, pr	Luse see our s	peenie	
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the	structions, you can then go to 're setting up. �From this tab LastPass usernames of your e	the SAML use you are able nployees:	r Map to map	
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the LastPass	structions, you can then go to 're setting up. �From this tab LastPass usernames of your e HOME	the SAML use you are able mployees: SETUP	r Map to map USERS REPORTIN	≡ english ⊙ G <u>SAML</u>
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the set application use	Istructions, you can then go to tre setting up. ∳From this tab LastPass usernames of your e HOME	the SAML use you are able t mployees: SETUP	r Map to map USERS REPORTIN	■ english ⓒ G <u>SAML</u>
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the lastPass **** LastPass **** ENTERPRIS SAML SAML Users whose SAML service provider account	Istructions, you can then go to 're setting up. From this tab LastPass usernames of your e HOME LOGOFF is not the same as their LastPass account	the SAML use you are able in ployees: SETUP	r Map to map USERS REPORTIN ded here.	■ english ⊙ G <u>SAML</u>
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the set application username to the	Istructions, you can then go to 're setting up. From this tab LastPass usernames of your e HOME .0GOFF Is not the same as their LastPass account	the SAML use you are able in ployees: SETUP	r Map to map USERS REPORTIN ded here.	■ english ⊙ G <u>SAML</u>
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the initial set up in the set username to the initial set up in the set user and the set user whose SAML service provider account la new entry	Instructions, you can then go to the setting up. From this tab LastPass usernames of your e HOME	the SAML use you are able t mployees: SETUP , entries may be ad	r Map to map USERS REPORTIN ded here.	ENGLISH O
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the subtab for the particular app you the application username to the set application username to t	Istructions, you can then go to the setting up. ∳From this tab LastPass usernames of your e HOME LOGOFF is not the same as their LastPass account LastPass Username	the SAML use you are able t nployees: SETUP	r Map to map USERS REPORTIN ded here. ded here.	ENGLISH 🕑 G <u>SAML</u> Add New ble Delete
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the initial set up in the application username to the initial set up in the application username is a set of the initial set up in the application username is a new entry initial set users users users users user username box.net username google.com/a/lastpass.com username	Istructions, you can then go to 're setting up. From this tab LastPass usernames of your e HOME .0GOFF Is not the same as their LastPass account LastPass Username LastPass Username	the SAML use you are able in ployees: SETUP , entries may be ad	r Map to map USERS REPORTIN ded here. Actions Edit Disa	Add New Add New Let Pelete Add New
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the initial set up in subtab for the particular app you the application username to the initial set up in set. LastPass Same application username to the initial set up in set. ML> SAME ML> SAME ML> SAME Same application Same application ML> SAME ML> SAME Same application Same application box.net username Societation google.com/a/lastpass.com username Same application By clicking Edit on a specific use usernames from LastPass accourtion Same application	Istructions, you can then go to the setting up. From this tab LastPass usernames of your e HOME LastPass Username LastPass Username LastPass Username rname, you can edit the indivin th name to the service account	the SAML use you are able t mployees: SETUP , entries may be ad dual mapping : name:	r Map to map	G SAML Add New ble Delete Add New ble Delete
Push Sites to Users page. After using the \$initial \$set up in subtab for the particular app you the application username to the subtab for the particular app you the application username to the subtab for the particular app you the application username to the subtab for the particular app you the application username to the subtab for the particular app you the application username to the subtab for the particular app you the application username AML> SAML SAML USERMAP If AML> SAML SAML USERMAP If users whose SAML service provider account If a new entry If box.net username	Instructions, you can then go to Pre setting up. Instructions, your end this tab LastPass usernames of your end HOME LastPass Username LastPass Username Instructions username I	the SAML use you are able t mployees: SETUP , entries may be ad	r Map to map	C SAML Add New Add New Add New Add New Lee Add New Delete Add New Be ENCLISH C ENCLISH C C C C C C C C C C C C C
Push Sites to Users page. After using the initial set up in subtab for the particular app you the application username to the initial subtab for the particular app you the application username to the initial set up in the application username to the initial set up in the application username is subtable. AML> SAML SAML USERMAP AML> SAML SAML USERMAP AML> SAML SAML USERMAP users whose SAML service provider account is a new entry box.net usemame google.com/a/lastpass.com username By clicking Edit on a specific use usernames from LastPass account is an experise in terp rise	Instructions, you can then go to Pre setting up. From this tab LastPass usernames of your e HOME Intersection of your e LastPass Username Intersection of the service account HOME HOME	the SAML use you are able in ployees: SETUP , entries may be ad dual mapping c name: SETUP	r Map to map	G SAML Add New ble Delete Add New ble Delete G SAML
Push Sites to Users page. After using the \$initial \$set up in subtab for the particular app you the application username to the instruction username After using the \$initial \$set up in subtab for the particular app you the application username to the instruction username After using the \$initial \$set up in subtab for the particular app you the application username to the instruction username After using the \$initial \$set up in the particular app you the application username After using the \$initial \$set up in the particular app you the application username google.com/a/lastpass.com username By clicking Edit on a specific use usernames from LastPass account LastPass **** E N T E R P R I S E AML> SAML SAME	In the same as their LastPass account LastPass Usernames	the SAML use you are able in ployees: SETUP , entries may be ad dual mapping r name: SETUP	r Map to map	G SAML Add New ble Delete Add New ble Delete G SAML

[/accordion-item] [accordion-item title="Supported Apps" color="Accent-Color" id="h3"]

We are working to support new apps with LastPass SAML all the time. If you currently use a service that supports SAML 2.0, you can add that manually vusing our custom services. Adding a Custom Service? Let us know by sending feedback through our support channels and we can add it to our officially supported list!

[wc_row][wc_column size="one-third" position="first"]

ADP
Akamai
Amazon Web
Services
Asana
Atlassian
Box
Cisco Webex
Citrix
ShareFile
Concur
DocuSign
Dropbox
Egnyte
Freshservice
Google Apps

[/wc_column][wc_column size="one-third"]

GoTo Meeting
Jira
Joomla
Kayako
Mantis Bug
Tracker
MoinMoin
MS Office 365
NetSuite
New Relic
Onit
OpenVoice
Pagerduty
РНРВВ
Qubole

[/wc_column][wc_column size="one-third" position="last"]

Replicon
SalesForce
Samanage
Shibboleth
Smartsheet
Splunk
Success
Factors
Uservoice
Wordpress
Wordpress Workday
Wordpress Workday Yammer
Wordpress Workday Yammer Zendesk
Wordpress Workday Yammer Zendesk Zoho

[/wc_column][/wc_row] [/accordion-item]

[accordion-item title="Service Auto-Provisoning" color="Accent-Color" id="h1"]

LastPass can automatically manage user accounts for some services. When a user first tries to login to a supported service through SAML, LastPass will create (provision) the account at the service provider. Likewise, when a user is deleted from the LastPass user database, LastPass can remove (deprovision) that account from the service if the service supports it.

Watch this screencast to see provisioning in action: click here.

These services support auto-provisioning:

- Amazon Web Services
- Box
- Google Apps
- Jira
- Joomla
- Salesforce
- WordPress
- Zendesk

[/accordion-item] [/accordion]

Setup

Policies Tab

Other Enterprise Policy Options

Create New User

Install Software

SAML

Login Reports

Shared Folders

Admin Events

Notifications

Shared Folders

[accordion openfirst=false scroll=true clicktoclose=true]

A Shared Folder is a special folder in your vault that you can use to securely and easily share sites and notes with other people in your Enterprise. Changes to the Shared Folder are synchronized automatically to everyone with whom the folder has been shared. Different access controls such as 'Hide Passwords' - can be set on a person-by-person basis or in the form of policies. Shared Folders use the same technology to encrypt and decrypt data that a regular LastPass account uses, but are designed to accommodate multiple users for the same folder.

With Shared Folders:

- Anyone can create a shared folder.
- Simple to configure and maintain.
- You can share hundreds of passwords with hundreds of users individually or via user groups.
- Changes automatically propagate to all assigned users.

[accordion-item title="Options for managing Shared Folders" color="Accent-Color" id="h2"]

Once a folder is created and populated by the folder Admin, there are three different ways in which the folder can be assigned out to additional users:

- The folder Admin@assigns and manages the folder manually. In this scenario, from his/her vault the folder admin (for example, the division manager) can@add and remove users, and edit user permissions on an individual by individual basis.
- Automate all folder assignments through the user group assignments in AD. The creator of the folder simply assigns the folder to the appropriate user group from the existing AD groups. Once this mapping is completed, the AD Sync Client will manage all user additions and removals for you based on any relevant

- changes in AD.
- 3. Centralize the management function and have a dedicated person managing the groups manually through the Admin Console. In this case, the designated individual would need to be a LastPass Admin. Using the 'Groups' function in the Admin Console, the Admin could add and delete users to groups, which would then map back to the relevant Shared Folders. The creator of the folder simply assigns the folder to the appropriate user group. In this scenario, you would typically publish the point of contact on your LastPass wiki page or internal FAQs so that users would know to whom they should direct a change request.

[/accordion-item]

[accordion-item title="Limitations of Shared Folders" color="Accent-Color" id="h3"]

The current limitations of Shared Folders are:

- Sites can be copied to multiple folders but must be updated manually in every folder. The better option is to use restrict to limit access for a specific sub-set of users, rather than copying the site into multiple folders.
- Site entries cannot be directly imported into Shared Folders.
- Form Fill Profiles cannot be shared.
- Individually shared sites cannot be added to a Shared Folder; a copy will have to be made.
- If a user is added more than once to a Shared Folder via multiple groups or individually multiple times with different permissions, the most restrictive settings take priority. If a user is added to the folder individually and via user groups, the individual permission would apply. This is important to remember when an admin is also part of a group, as they can limit their privileges.
- A Sub-folder cannot have separate permissions from its parent Shared Folder.
- Empty Shared Folders cannot be seen by users in the Online Vault; they must have data added to them first or be�viewed�in the Local Vault.
- Users MUST \$\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{\overlin}\overlin{\overline{\overlin{\verline{\overlin}\overlin{\overli

** The Pre-Create Sharing Key policy functions by creating a random password, a random sharing key, encrypting the sharing key with the password, and emailing the password to the user. This information is then flushed from our servers. Users are then required to change this password immediately on their first log in. This information is then flushed from our servers. It is less than perfectly secure as it requires you to trust us, so you are welcome to wait on creating sharing keys by having the user log into their account.

[/accordion-item]

[accordion-item title="Manually Creating and Using Shared Folders" color="Accent-Color" id="h4"]

To create a new Shared Folder, log in to your LastPass Vault and click on the Manage Shared folders

LastPass ****	Search Vault Q
🕌 Add Site	Vault Form Fill Profiles Identities Shares Credit Monitoring
Add Secure Note	Name
Create Folder	▶ 🙀 favorites
🏟 Account Settings	► ► recently used
▶ Tools	Apps assigned to me
Security Challenge 56%	(Accepted Share Offers)
User Manual	▶
Tutorials	



×

This will take you to the main Shared Folders dialog:

LastPass Shared Folder
What is a shared folder?
A shared folder is a special folder in your vault that you can use to securely and easily share sites and notes with other people in your enterprise account.
Changes to the shared folder are synchronized automatically and different access controls can be set on a person by person basis (read-only, hide passwords, etc).
View Deleted Shared Folders

Shared Folder Name	Read-only	Action
LPSUPPORT	No	No Admin Actions Available
Sales Resources	Yes	Read-only
SAML site signups	No	Edit Delete
Support	No	Edit Delete
Testing editing	No	Edit Delete
Xmarks	Yes	Read-only

This gives you the options of creating new shared folders, or editing and deleting old shared folders. To create a new Shared folder, click Create A New Shared Folder. To create a the new folder dialog, where you can enter a folder name. Once you have given the folder a name, hit Create.

🚼 LastPass Shared Folder	X
Adding shared folder Back to List	
Please give your new shared folder a name. All employees that you share this with will see a new folder in their account with this name (prefixed by 'Shared-').	
using drag and drop in your local vault, edit the group name of an existing site or add a new entry and set the group to the shared folder name.	
Folder Name:	
**Please note that as an Enterprise user all data stored in your LastPass Enterprise shared folders may be accesse or deleted by your employer.	d

[/accordion-item] [accordion-item title="Converting Standard Folders to Shared Folders" color="Accent-Color" id="h5"]

Nearly any folder in your vault can be converted to a Shared Folder (exceptions include 'Favorites' and 'Recently Used'). To convert a folder simply locate the folder in your vault and click on the double-head icon to the right of the folder name.



After creating or converting a folder, you'll be taken back to the main shared folder dialog. If norder to assign users, click I click Read to any given folder and then select the appropriate group or user from the dropdown menu. You can also add User Groups to Shared Folders. If Groups can be added and edited by LastPass Administrators only. All users who are a part of the group will be given access to the Shared Folder once you add the group.

Enter recipient email a	address or Groups			Share	
Read-only	Hide Passwords	Notify Us	er Via Email	Can Administer	

[/accordion-item]

[accordion-item title="Edit Permissions" color="Accent-Color" id="h6"]

With each user or group, you have several additional choices regarding access via the radio buttons next to each users name and when you initially add the user or group to the folder:

- Read-only prohibits the user from adding/removing items to/from a Shared Folder. It also prevents the user from saving any updated username, password or note information to the folder. However, we cannot block the update from transpiring at the site level. This option could, therefore, result in a lockout by the rest of the team. It is our recommendation, therefore, that you articulate a 'no update' policy outside of LastPass (if this is, in fact, your goal) and that you *do not* select 'read only'. If the user still updates the credentials, then the change will save back to LastPass, and the event will be captured in the reports so that you are able to track it back to the owner.
- Hide Passwords prohibits the user from seeing the credentials. They will be able to utilize the tools via autofill or autologin, but they will be unable to see the actual credentials. *
- Can Administer[®] will grant the user equal admin rights over the shared folder including: adding and removing users and restricting access to individual sites in the folder.
- Notify User Via Email will send the user a notification regarding their assignment to the shared folder. Please note, this is only available upon the initial addition of users to the group.

Once you have made these selections, hit **�**Share**�** and the user will be added to the list of assigned users with the permissions that you designated.

If a user is added to a Shared Folder multiple times via groups, the most restrictive permissions will apply to their access. If they are added multiple times but are added to the Shared Folder individually, the permissions established from the individual share will be reflected. Below are tables to to highlight different scenarios:

In each scenario, the user user@lastpass.com is a part of two groups: A and B.

Scenario 1:

User/User Group	Can Administer	Read-Only	Hide Password
А	Yes	No	No
В	No	Yes	

 $\label{eq:permissions} \mbox{Permissions} = \mbox{user} \ \mbox{cannot} \ \mbox{add/edit} \ \mbox{users} \ \mbox{in the Shared Folder} \\ \mbox{Shared Folder} \ \mbox{Shared} \ \mbox{Shared$

Scenario 2:

User/User Group	Can Administer	Read-Only	Hide Password
А	No	Yes	Yes
В	Yes	No	No

Permissions = user cannot edit sites, view passwords nor edit users in the Shared Folder.

Scenario 3:

User/User Group	Can Administer	Read-Only	Hide Password
A	No	Yes	Yes
В	No	No	No
user@lastpass.com	Yes	No	

Permissions = user can edit/add users, edit sites, and view passwords. Note that in this scenario, the user's permissions ignore permissions made in groups A and B and only take into account permissions set for the user when they are added individually.

[/accordion-item] [accordion-item title="Restrict and Remove" color="Accent-Color" id="h7"]

Next to each user s name you will see the Restrict and Remove options: The Remove button will remove the user from the folder which will automatically delete the Shared Folder from the user Vault thereby preventing any future access to the sites or notes within the folder. The Remove button will remove the user from the folder which will automatically delete the Shared Folder from the user Vault thereby preventing any future access to the sites or notes within the folder.

- 8. The **Remove** button will remove the user or groups from the shared folder. This will revoke access to the folder and any sites stored within.
- 9. The Restrict feature allows you to limit access on a site-by-site, user-by-user basis. Click @Restrict@ next to the appropriate user in order to prohibit access to any number of sites within the folder. By default, all items placed in a Shared Folder will be made available to every user unless they are restricted by moving the item from column A to column B. However, on the 'Restrict' screen, the toggle below the columns will *reverse* this logic. When selected, all items in column A will be *unavailable* to the user until they are moved to column B. Many enterprises prefer this 'opt in' rather than 'opt out' approach.

Available Items		Hidden Items	
Search:		Search:	
Name	Group 🔺	Name 🔺	Group
🗶 LastPass	(none)		
Rather than choo	osing hidden sites, ass	gn only allowed sites. All new sites	s will be hidden in this mode.

populate the folder with sites and Secure Notes via several methods:

- 10. Drag and drop
- 11. Right-click in your vault and select 'Change Group'
- 12. Edit site (in plugin) and select 'Change Group'
- 13. Add a new site and set the 'Group' to the Shared Folder name

[/accordion-item]

[accordion-item title="Adding Users to Shared Folders" color="Accent-Color" id="h8"]

You can add users to Shared Folders using **User Groups**. This is a quick and easy way to add pre-made groups of users to Shared Folders. User groups are added to Shared Folders just like individuals; the groups are created in the Admin Console and available in the dropdown list of users when you create or edit a Shared Folder. You can set 'Read-only', 'Hidden Passwords', and 'Can Administer' access once for the entire group. You can also restrict what sites the group can view just like you can for an individual user. When adding groups to Shared Folders, there are a few things to keep in mind to avoid conflicts:

- If you add a user to a User Group that is@assigned@to a Shared Folder, they will gain access to that Shared Folder.
- If you add a user to your Enterprise via the Active Directory or LDAP sync, and the user is synced straight into a group that has already been assigned access to a Shared Folder, that user will not have access to the folder until another member of the folder logs in to LastPass. Upon this event the sharing keys are exchanged between those two user accounts, making access possible by the new user. (You must ensure that the 'Precreate Sharing Keys' policy is enabled in order for this to happen automatically.)
- If a user is added to a Shared Folder more than once, the most restrictive settings will take precedence. This applies to 'Read-only', 'Hidden Password', and 'Can Administer' rights, as well as what restrictions are in place regarding what sites can be seen in the folder. This can also apply to other admin accounts.
- When a non-Enterprise admin creates a Shared Folder, they are able to add both individuals and groups. These non-admins do not have the ability to see who is in what group, so they should be aware who is in what user group before adding them to a Shared Folder.

Important note: Savvy end users could potentially access a hidden password if they capture it using advanced techniques during the login process such as using another password manager. LastPass recommends that you ensure that you've used a generated password specific to the individual site that you are sharing, and that you refrain from sharing any passwords that you are uncomfortable with the recipient obtaining. Regardless, LastPass helps facilitate the seamless update of passwords so that you can change them frequently and at a moment[®]s notice, without your end users even knowing that an update has taken place.

[/accordion-item]

[accordion-item title="Active Directory Synced Groups and Shared Folders" color="Accent-Color" id="h9"]

You can use the LastPass Active Directory Synchronization Service to automatically provision and sync users and user groups from your Active Directory into your LastPass Enterprise. AlastPass also recommends provisioning users with our simple LastPass Provisioning API.

Please see the video below to learn more about Enterprise Shared Folders: click here.

To view a brief screencast regarding the benefits and use cases for Shared Folders, **¢click here**. **•**For complete video instructions, **¢click here**.

Terminating User Accounts from Your Enterprise

[accordion openfirst=false scroll=true clicktoclose=true]

There are several termination/removal options available to your LastPass Administrator. Please consider your options carefully prior to deleting or removing users. These actions can be performed from the **Users tab** in the Admin Console using the Actions column, or can be automated using the AD Sync Client or the API. There are three main termination options:

[tabbed_section]

[tab title="Disable User"]

Disabling a user in your Enterprise puts a lock on the account. No one - not even your LastPass@administrator@- can log in to the account regardless of passwords or previous access.@ Once disabled, the license will be available for reassignment.

[/tab]

[tab title="Remove User From Company"]

Removing a user from your Enterprise will disassociate (spin out) that user's account from your company account. With this action, all Shared Folder data will be revoked immediately. LastPass will also prompt if you would like to "Delete Shares" or "Do Not Delete Shares". Selecting to "Delete shares" will delete all sites within the account that have been shared to the user from other users in the Enterprise outside of Shared Folders. The account will otherwise still be fully available for use by the account owner, including all data that has been stored in the user's vault. Once removed, the license will be available for reassignment.

[/tab]

[tab title="Delete User"]

Deleting an account **FULLY DELETES ALL CONTENTS** in the account. Any data stored within the account will be gone forever. Once deleted, the license will be available for reassignment.

[/tab]

[/tabbed section]

Please note that all LastPass Enterprise licenses are transferable once an account is disabled, removed, or deleted.

[accordion-item title= "Resetting a User's Master Password" id="h4"]

This option is only available if the **Super Admin - Password Reset policy** is in place. From the Admin Console, the Admin of the Enterprise can reset the master password on the account. This option can be leveraged under the following scenarios:

(1) You would like to lock-out the owner of the account, but still allow Admin access. This can be helpful for audit purposes; in order to update and/or terminate any credentials to which the end user had access.

(2) If you would like to assign the entire account - with all of its contents - to another employee.

[/accordion-item]

[accordion-item title= "Important Considerations" id="h5"]

- Ensuring that sites/tools are no longer accessible by the employee: If the account owner created any passwords in his vault, or if any credentials were shared visibly with him, then it is quite possible that he has stored this information elsewhere and could access these tools again in the future (outside of LastPass). In order to avoid any doubt, we therefore recommend updating all passwords when an employee account is terminated.
- Once terminated (disabled, deleted or removed), any data that the account owner has placed in a Shared Folder will remain fully intact for remaining users.
- In the case of Shared Folders, while you are never at risk of deleting the shared credentials, you are at risk of finding yourself with no remaining Admin on the folder (if the former account owner was the sole folder Admin). If this is a concern, you should consider enabling the **\$Super Admin** Shared Folders policy.
- NONE of these actions will affect a Linked Personal Account, which is why we HIGHLY RECOMMEND users utilize the Linked Personal Account Tool rather than storing personal data in an Enterprise account.
[/accordion-item] [/accordion]

Shared Folders with Users Outside your Enterprise

[accordion openfirst=true scroll=true clicktoclose=true]

LastPass supports sharing **Shared Folders** with users outside of your Enterprise system. **You can share any Shared Folder with up to five users that are not in your Enterprise.** These users can be free, premium, or in another Enterprise. The only limit is that the maximum of outside users that can be added per folder is five.

To add an outside user to a Shared Folder, do the following:

- 1. Go to your Manage Shared Folders link in your Vault as you normally would.
- 2. Type in the email address of the user you would like to add and click 'Share.'
- 3. The outside user will appear in your list of users and the user will receive an email invitation to accept the shared folder.
- 4. Once accepted, the user will be added to the Shared Folder!
- 5. Restrict what sites they see and change permissions as appropriate

If you run into the error: *****"An Error occurred - Cannot retrieve any public keys. The user may need a sharing key to be created." This means that the user you are trying to share with does not have a sharing key. To obtain the sharing key, the user must log into the LastPass Extension at least once.

[/accordion]

LastPass for Applications

[accordion openfirst=false scroll=true clicktoclose=false]

LastPass for Applications is included by default with LastPass Enterprise. This program allows you to store your application logins just like the browser plugin allows you to save your website login credentials. Benefits:

- Fills in your application login data for you; allows you to stop using the 'Remember Password' function, which can often times be saved insecurely
- When run as a tray application, LastPass for Applications has some preferences that are now possible, like logout on lock or screensaver
- Can launch your applications
- Application logins can be shared using 'Shared Folders'

Some applications will require a one-time training. Φ Applications, once trained, are trained for everyone in the enterprise.

Click here for more information on LastPass for Applications.

[/accordion]

LastPass App for Mac

[accordion openfirst=true scroll=true clicktoclose=false]

The LastPass App for Mac@is included by default with LastPass Enterprise. With convenient features like Quick Search, you have instant access to logins, passwords, and the other important details you@ve stored in LastPass without@having to open your browser.

Click here to learn more about the LastPass App for Mac.

[/accordion]

Mobile Apps

[accordion openfirst=false scroll=true clicktoclose=true]

All mobile apps included in LastPass Premium are included in LastPass Enterprise!

LastPass Mobile Apps Manuals

[/accordion]

Multifactor Authentication

[accordion openfirst=false scroll=true clicktoclose=false]

Multifactor authentication refers to a device that can be enabled for use with your LastPass account and requires a second step before you can gain access to your account. You can set up **Policies** to require multifactor authentication for your Enterprise users. Multifactor authentication devices help protect your account from keyloggers and other threats - even if your Master Password were captured, someone would be unable to gain access to your account without this second form of authentication. LastPass offers several multifactor options for your Enterprise account, including:[wc_row][wc_column size="one-half" position="first"]



Google Authenticator



Toopher Authentication



Duo Security Authentication





RSA SecurID



Yubikey Multifactor Authentication �



Symantec VIP



Transakt Authentication



Salesforce#

[/accordion]

LastPass Sesame



LastPass Premium members can use an ordinary USB thumb drive as a second form of authentication when logging into their LastPass account. Having a physical second

form of authentication will help further ensure that your account will remain safe because both your Master Password and your USB thumb drive are required to log in.

[accordion openfirst=true scroll=true clicktoclose=true] [accordion-item title="Enabling Sesame" id="h0"]

If you are already a Premium member, you can simply **download** Sesame onto your USB device and run the application. You will see the empty Sesame dialog:

	las	stpass 🕷	***
00	English	(U.S.) Welcome to La: Multifactor Authen	▼ stPass Sesame <i>tication Made Easy</i>
Select the	user to genera	ite a one time password f	or
Select the	user to genera	Ite a one time password f	Edit Remove
Select the	user to genera	inte a one time password f	Edit Remove

On your first run, you will be prompted to activate the software by Adding your LastPass login to the user list. Then, you will be sent an e-mail asking you to confirm the registry of Sesame.

By default, the email link will expire after 10 minutes to protect your security. If you click on the link and it says 'Link Expired', please re-send yourself the activation link and try again.

Once activated, Sesame will create secure One Time Passwords (OTP) that are subsequently required to login. You have the choice to copy the OTP to the clipboard or launch the browser and pass the value automatically.

Like all our multi-factor authentication options, you can elect to enable or disable Mobile and Offline Access within the settings for your particular username in Sesame:

😸 Configur	e LastPass Sesame Multifactor Authentication	
	lastpass <mark>* * * *</mark>	
	LastPass one time password authentication is currently enabled. Would you like to leave it enabled?	
	 Yes, protect me against keyloggers and spyware! Permit access to my LastPass Vault from mobile devices? Permit access to my LastPass Vault when not connected to the Internet? 	
	No, disable Sesame	
	ОК	

If you lose your USB device, you can disable Sesame authentication by logging in to LastPass and using the link on the bottom of the Sesame screen.

Sesame is a cross platform application that is available for Windows, Mac and Linux.

Note for Linux users

The USB device is mounted noexec, which prevents running executables from the drive. To fix, remount the device with the exec flag, for example by "sudo mount -o remount,exec <device> <mountpoint>".

[/accordion-item]

[accordion-item title="Administering Sesame in Enterprise" id="h1"]

You can require Sesame for your users via the 'Require LastPass Sesame' **Ppolicy**. This policy can be enabled for your Enterprise account by accessing your Enterprise console and clicking the 'Setup' tab > 'Add Policy' button > Select 'Require LastPass Sesame' from the dropdown menu:

Policy	1
Policy Require LastPass Sesame	Full list of Policie
Require use of LastPass Sesame as a second f logging into LastPass. Click the 'enabled' box t	actor of authentication when to enable this policy.
Sesame must be configured by the user as det https://helpdesk.lastpass.com/security-option authentication-with-a-usb-thumb-drive/.	scribed here: s/sesame-multifactor-
Enabled 💌	
Applies To: ❀ All ◎ Inclusive List of Users ◎ Exclusive Lis	t of Users
Notes	
	Cancel Save

[/accordion-item] [/accordion]

YubiKey



[accordion openfirst=true scroll=true clicktoclose=false]

A YubiKey is a key-sized device that you can plug into your computer's USB slot to provide another layer of security when accessing your LastPass Account. YubiKeys are a secure, easy to use, two-factor authentication device that are immune from replayattacks, man-in-the-middle attacks, and a host of other threat vectors.



YubiKey support is a **Premium** and **Enterprise** feature, and the device must be purchased through **Yubico.com** for \$25.

Up to **\$5 YubiKeys** can be associated with one LastPass account.

Once you have purchased and received your YubiKey, you can enable the device and manage your preferences by launching your **Account Settings** and clicking on the 'Multifactor Options' tab > 'YubiKey' radio button:

Edit Settings							×
General Security Equivalent Domains Never URLs	ltifactor Options	Mobile Devices	Trusted Comp	uters	URL Rules	Third Party Access	
Choose a multifactor option:	O Toopher O Du	uo Security O Trans	sakt				
I. INSERT YUBIKEY INTO USE PORT. C. OLOK INSIDE TEXT FIELD. LastPass can be configured to work in corexess button with immune from replay-attacks, man-in-i YUBIKEY. Intolioiologia YubiKeys make LastPass more se	vith YubiKeys made he-middle attacks, a	e by Yubico. YubiKeys and a host of other th	s are a secure, e nreat vectors.	easy to u	ise, two-factor	authentication device th	at are
To get your YubiKey, visit GET A	YUBIKEY!						
YubiKey Authentic	ation Ena	abled	¥	Help			
Permit Mobile Devi	ce Access Allo	w	~	Help			
Permit Offline Acc	ess Disa	allow	¥	Help			
To associate a YubiKey with your To disassociate a Yu	account, give focus ibiKey with your acc	to one of the below in count, clear the entire	nput boxes and value of the inp	press yo	our YubiKey.		
YubiKey #1				_			
YubiKey #2				-			
YubiKey #4				-			
YubiKey #5							
					Cancel	Update	

To add a new YubiKey to your LastPass account, enter the device in your USB port, click in the first empty YubiKey field, and lightly press your YubiKey on the grooved circle. You will need to enter your LastPass Master Password to save any updates you have made to your YubiKey settings.

After the field is filled, you can specify your YubiKey preferences:

YubiKey Authentication: Enable or disable your YubiKey multifactor authentication. When enabled, you will be prompted to enter the YubiKey data the next time you login to LastPass.

Permit Mobile Device Access: Controls whether mobile devices that do not possess USB ports, such as a smartphone, will be allowed to bypass YubiKey multifactor authentication when enabled.

Permit Offline Access: Controls whether access to your vault will be allowed when you are not connected to the Internet. Allowing offline access to your vault is slightly less secure since YubiKey OTPs can not be validated, and only the static portion of the key is validated.

To begin using your YubiKey, be sure that the 'YubiKey Authentication' field is marked as 'Enabled'.

To save changes to your YubiKey preferences, click 'Update' before exiting the Account Settings dialog.

To disassociate a YubiKey device with your LastPass account, simply clear the entire input field of all characters and click 'Update'.

[/accordion-item] [accordion-item title= "Logging In with YubiKey" id="h2"]

Now that you have enabled your YubiKey device, the next time you login to your LastPass account, you will be prompted to enter your YubiKey code. Simply click your LastPass Icon to login as normal, enter your email and Master Password, then submit. However, you will now be asked by LastPass to press your YubiKey device to enter the code:



YubiKey Multifactor Authentication

1. Insert your YubiKey in the USB-port with the USB-contact facing $\ensuremath{\mathsf{upward}}$

2. Wait until your YubiKey touch-button shines with a steady light





If you would like to leave YubiKey authentication enabled but do not want to enter it every time you login to a particular device, simply check the trusted computer option before swiping your YubiKey.

[/accordion-item]

[accordion-item title= "Administrating YubiKey in Enterprise" id="h3"]

You can require Yubikey for your users via the 'Require use of YubiKey' **policy**. This policy can be enabled for your Enterprise account by accessing your Enterprise console and clicking the 'Setup' tab > 'Add Policy' button > Select 'Require use of YubiKey' from the dropdown menu:

Regure use of a Yubikey as a second factor of authentication when logging into LastRass. Click the 'anabled' hox to enable this policy. YubiKeys can be purchased here: https://tere.yubic.com/. YubiKeys mus be conversion of the second second policy of the second second policy into the second second second policy of the second seco	of YubiKey 🔄 Fullist of Poic
Enabled Applies To: # All © Inclusive List of Users © Exclusive List of Users Notes	In Unknown of actor of authentication when logging the 'enabled' box to enable this policy. rchased here: https://store.yubico.com/. YubiKeys must e user as described here: stpass.com/security-options/yubiKey-authentication/.
	st of Users [©] Exclusive List of Users
Count 1	Count Cou

You can also restrict your users to only permit the use of a single YubiKey for their account via the "Only allow a single YubiKey per account" policy:

Policy	
Policy Only allow a single YubiKey per account	Full list of Police
Prevent the user's ability to setup more than 1 YubiKe default, LastPass allows a user to use up to 5 differen	y for their account. By t YubiKeys.
Enabled Multiplies To: Multiplies T	r5
Enabled Multiplies To: Multiplies T	rs
Insbled #splies To: # All	ers
Inabled 8 Applies To: # All © Inclusive List of Users © Exclusive List of Use Notes	rs
Inabled * Isplies To: # All © Inclusive List of Users © Exclusive List of Use Kotes	ars
Inabled # Isplies To: # II © Inclusive List of Users © Exclusive List of Use Kotes	85

[/accordion-item]

[accordion-item title= "Using a VIP YubiKey with LastPass" id="h4"]

The VIP enabled YubiKey (http://yubico.com/vip) has two configuration slots. When the VIP enabled YubiKey is shipped, it's first configuration slot is factory programmed for Symantec VIP credentials and the second configuration slot programmed with a standard Yubico OTP is dormant in the second identity slot and can be activated using the YubiKey Personalization Tool. The two configuration slots of the YubiKey work independently and each can be independently reconfigured into OTP or static password mode has two configuration slots.

If you touch and hold the YubiKey button between 1-3 seconds before releasing, the first configuration slot will emit the password (based on slot 1 configuration). And if you touch and hold the YubiKey button about 4-5 seconds before releasing, the second configuration slot will emit the password (based on slot 2 configuration). In case if you happen to touch and hold it longer for more than 5 seconds, the touch button indicator will flash rapidly without emitting any password.

As the second configuration slot of the YubiKey is left blank, you can program it to the YubiKey OTP mode, upload the AES Key to the online validation server and configure it to work with LastPass.

To program the second slot to work with the online Yubico OTP validation server, please follow the steps below:

- First, download and install the latest Cross Platform Personalization Tool for Windows from the Yubico Website at: http://www.yubico.com/products/servicessoftware/personalizationtools/use/@under the section "Cross platform personalization tools". There are a number of @different installers for various operating systems @ pick the installer for your operating system.
- 2. Once the Cross-Platform Personalization tool has been installed, insert your VIP YubiKey in a�USB port on your computer and launch the YubiKey Personalization Tool.
- In the Cross-Platform Personalization Menu, open the "Settings" menu by clicking on the link Update Settings on the main page or the Settings option from the menu at the top.
- 4. In the Settings menu, locate the Update Settings button in the lower right corner and click on it.
- 5. The Update YubiKey Settings menu should be displayed. If this is not the case, confirm youhave a VIP YubiKey with a firmware version of 2.3.0 or above.
- 6. Locate the section labelled Configuration Slot and select Configuration Slot 2
- 7. Locate the checkbox labelled Dormant and ensure the box is not checked
- Locate the Configuration Protection section, and open the menu labelled
 YubiKey(s)unprotected
 Keep it that way
 From this menu, select the option
 YubiKey(s) protected
 Keep it that way
- 9. This will activate the �Current Access Code I field in the Configuration Protection section. Enteryour VIP YubiKey I scurrent access code, which will be five 0s followed by the YubiKey I serial number in Decimal format, as reported by the Personalization tool.For example: If your Serial Number is \$1234567€, then your Current Access Code will be \$00 00 01 23 45 67€
- 10. Press the Button labelled �Update� to activate your VIP YubiKey�s second slot with the Yubico�OTP configuration.

Yubico also has a video that describes the steps required for uploading the AES Key. For more information, please visit the link below:

http://www.yubico.com/aes-key-upload

[/accordion-item] [accordion-item title= "Video Tutorial for Using LastPass with YubiKey" id="h5"] After you've registered the YubiKey with your LastPass account, ensure that mobile access is "disallowed" in your LastPass Icon > My LastPass Vault > Account Settings link > YubiKey tab.

Now you can use the YubiKey NEO when logging in via the LastPass Android app or used as a normal YubiKey on your desktop.

[/accordion-item] [accordion-item title= "YubiKey NEO with Windows Phone 8 App" id="h6"]

The updated Windows Phone 8 app with Yubikey NEO support (for phones that have NFC) is now available in the Windows Phone store: **http://www.windowsphone.com/en-us/store/app/lastpass/9b86eadc-16e8-df11-9264-00237de2db9e**

Configuring the Yubikey NEO should be done the same way as for Android, shown above. You also have to set the "permit mobile device access" in your LastPass vault to "disallow" in order to enable prompting.

A known issue is that when you touch the Yubikey NEO to the phone, the LastPass app will accept and verify the key, but the OS will open a dialog asking what to do with the URL, which you will have to ignore/cancel. Hopefully Microsoft will fix this in a future release of the OS.

[/accordion-item]

[/accordion]

Duo Security



[accordion openfirst=false scroll=true clicktoclose=true]

LastPass supports multifactor authentication with Duo Security. It is a secure, two-factor authentication application offered for all leading smartphone platforms, including Android, iPhone, Blackberry, and Windows Phone. You can get Duo Security here: https://www.duosecurity.com/editions

[accordion-item title="Set Up A New Application" id="h0"]

- In order to use Duo Security, a Duo account is required. Register for an@account here:@https://www.duosecurity.com/lastpass.
- 2. Login to your Duo account.

LastPass Enterprise Manual' 3. In the left menu, choose Applications > Protect Application

DUC		۹ Search for users, groups, applications, or devices	. •
Dashboard		LastPass > Applications	
ි Applications	0	Applications	+ Protect an Application
Protect an Application		Applications	
岛 Users	1		Q
2FA Devices	3		
竖 Groups	0	Name A Type C New User Policy C	Additional Information 🛇
🖻 Administrators	1	No data available i	in table
Reports		Show 25 • applications No applications yet. Click Prote	ect an Application to add one.
ᢒ Settings			« <

4. Search for LastPass in the list and click Protect this Application

		۹ Search for	users, groups, applications, or devices	1	~
💭 Dashboard		LastPass > Ap	plications > Protect an Application		
ි Applications	0	Protect an Application			
Protect an Application					
용 Users	1	Las			
2FA Devices	3	CAS	CAS (Central Authentication Service) Protect this Application Read the documentation		
A Groups	0		LabTech Software		
🖻 Administrators	1	LabTech	Protect this Application		
🖻 Reports		LastPass	LastPass		
③ Settings			Read the documentation		

 On the next page, you lifting the following information: Integration key, Secret key, and API hostname. Note these values for later.

 Optionally set up additional settings such as Group policies and Username Normalization in the Duo Admin Console. Find all options here.

[/accordion-item]

[accordion-item title="Set Up DUO In LastPass Admin Console" id="h1"]

Once you have finished setting up your new integration, then you will need to enter Duo Integration information in LastPass Admin Console.

In Admin Console, click Setup > Add Policy > Select either Require Use of Duo Security or Require Use of Any Multifactor Options. Enter the required information here and click Save.

Policy Require use of Duo Security	✓ Full list of Policies
Require use of Duo Security as a second factor of authentication when logging into LastPass. Click box to enable this policy. You must also enter y key, secret key, and API hostname in the boxes	of the 'enabled' our integration below.
Duo Security must be configured by the user.	

Enabled 🗵	
Click here if you need a Duo an integration type of LastPag	<u>Security account</u> (be sure to choose ss)
Duo Security integration key:	
Duo Security secret key:	
Duo Security API hostname:	

[/accordion-item]

[accordion-item title="Enable Duo Security As End Users" id="h2"]

Users will be prompted to enable Duo Security or select Duo Security as a multifactor authentication option when they log in to their LastPass accounts. Below is an example of the prompt to confirm Duo Security Username that users should see:

😫 LastPass	×
Please confirm your Duo Security username:	
spring@gmail.com	
Cancel OK	

Click Ok to proceed. �On the next page users will be prompted to enroll their devices:



You will then see another screen which will prompt you to choose which type of device you would like to enroll to use for two-factor authentication. Please note that LastPass currently only supports the enrolling of a single device:



Select the type of device that you would like to enroll and then click the "Continue" button. You will then be given on-screen instructions on how to enroll each specific device. Once you have enrolled the device(s) that you would like to use for Duo authentication, you can then use it to authenticate you in the login process.

[/accordion-item]

[accordion-item title="Select Duo Push or SMS As End Users" id="h3"]

When you finish enabling Duo Security as end users, you will be presented with the Duo Authentication Window after entering your login credentials to log in to LastPass next time. This is when you can switch from Duo Push to authentication codes via SMS. On the window, click "Next SMS password starts with 3 (send more)" link to have the codes sent to your registered device.

Multifactor Authentication	
	Please complete multifactor authentication on your phone or mobile device. Alternatively, enter a passcode in the box below: Next SMS passcode starts with 3 (send more) Authenticate is computer is trusted, do not require a second form of authentication.

If you wish to switch back to Duo Push, please contact your Enterprise Admins to have them disable Duo Security for your account in Admin Console > Users tab first. Then delete your registered device in Duo Admin Panel > Devices so you can start over.

[/accordion-item] [/accordion]

Google Authenticator



[accordion openfirst=true scroll=true clicktoclose=true]

Google Authenticator is a multifactor app for mobile devices. It generates timed codes used during the 2-step verification process. To use Google Authenticator, install the Google Authenticator application on your mobile device.

[accordion-item title="Installing Google Authenticator" id="h1"]

If you would like to use **Google Authenticator**, please first ensure you're using the latest LastPass browser extensions and mobile clients everywhere. You will also need a supported mobile device, to run the Google Authenticator application.

Next, install the Google Authenticator application on your mobile device. Google officially supports Android, iOS (iPhone, iPod Touch, or iPad), and BlackBerry devices. You can follow the instructions here to install Google Authenticator onto these devices.

For other devices:

If you would like to run Google Authenticator on an Android device that doesn't have access to Google Play Store, you can install from **%here**.

If you would like to run Google Authenticator on your Windows Phone, Jamie Garside has developed **Authenticator**.

If you would like to run Google Authenticator on your webOS device, Greg Stoll has developed $\mathbf{\widehat{G}Auth}.$

If you would like to run Google Authenticator on your Symbian device, or any device that supports Java ME, Rafael Beck has developed **@lwuitgauthj2me**. Alternatively, Rodrigo A. Diaz Leven has developed **@gauthj2me**.

[/accordion-item]

[accordion-item title="Setting up Google Authenticator" id="h1"]

Once you have the Google Authenticator application running on your mobile device, go to**%https://lastpass.com/?ac=1&opengoogleauth=1.%** Follow the instructions there to finish setting up Google Authenticator.

You will be prompted to use a Bar Code scanning app (Androids, iPhones and supported devices with cameras) to scan your unique bar code or you can manually enter the Google Authentication Key found on that setup page.

Ô

Edit Set	tings														
leneral	Security	Equivalent E	omains	Never UR	Ls Mult	tifactor Optic	ons Mobile	e Devices	Trusted	Computers	URL Rule:	s Th	ird Party	Access	
hoose a	multifactor op	otion: Oyub	Key 🖲	Google Auti	enticator (O Toopher	Duo Securi	ty O Tran	isakt						
	X	۵۵ 🕞	tPass ca	in be configi your n To in	ired to work Iobile device I stall the G	with Google , e that is immun Google Authe oogle Authe	Authenticator le from replay enticator ma nticator appl	: Google Au -attacks, m akes Lasti lication on	uthenticator an-in-the-m Pass more a your mot	is a secure, iddle attacks secure an olle device,	easy to use , and a host id easier to visit GOOG	two-fa of othe use. LE AUT	actor auth r threat ve "HENTICA	entication ectors.	application
1		To a	ssociate	Google Auth	enticator w	ith your accou Click her	int, scan the b re to display	oarcode bel y your bar	ow with yo code	ur Google A	uthenticator	applicat	ion.		
		Click her	if you're	e unable to s	can the barr	code (for exam	mple if you're i	using the B	ackBerry a	pplication, or	a device wi	thout a	camera).		
					Google Permit C	Authenticator	Authenticatio	en Enabl	ed 🗸	Help Help					
			Click her	e to regener	ate your Go	ogle Authentic	ator key (for	example if y	you lost you	ir Google Au	thenticator d	levice).			
														_	

After your LastPass account is registered within the Google Authenticator app, the next time you login to LastPass on an untrusted device, you will receive the Google Authentication dialog:





Go to your Google Authenticator App and input the current authentication code you see in the app into this dialog. If the code expires before you have a chance to authenticate, simply use the next code that appears in the app.

[/accordion-item]

[accordion-item title="Logging in Offline when Google Authenticator is Enabled" id="h1"]

As with our other multifactor authentication options, you can choose whether to allow LastPass to store an encrypted vault locally so you can log in without an internet connection. If you enable offline access, you will be able to login without using your Google Authenticator code in case of a connectivity issue.

With some internet configurations (typically wireless connections and waking from sleep), LastPass may log in offline first before establishing connectivity to your online vault and prompting for your authenticator code. This may cause LastPass to AutoFill any login credentials you have saved in LastPass for the current page you are on. If you wish to disable offline access, you may do so in your Account Settings.

[/accordion-item]

[accordion-item title="Administrating Google Authenticator in Enterprise" id="h2"]

You can require Google Authenticator for your users via the 'Require use of Google Authenticator' **\$policy**. This policy can be enabled for your Enterprise account by accessing your Enterprise console and clicking the 'Setup' tab > 'Add Policy' button > Select 'Require use of Google Authenticator' from the dropdown menu:

Volicy Require use of Google Authenticator Require use of Google Authenticator as second factor or han logging into LastBass. Click the anabled bas to an Google Authenticator must be configured by the user as https://helpdesk.lastpass.com/security-options/google-	Fullist of Poicies fauthentication able this policy. described here: authenticator/.
Require use of Google Authenticator as a second factor of when logging inclustrass. Click the 'enabled' box to en Google Authenticator must be configured by the user as https://helpdesk.lastpass.com/security-options/google-	of authentication able this policy. described here: authenticator/.
https://helpdesk.lastpass.com/secunity-options/google-l	authenticator/.
nabled 🖻	
Applies To: # All	
lotes	
	Cancel Save

[/accordion-item] [/accordion]

Toopher



[accordion openfirst=true scroll=true clicktoclose=false]

** Please note that due to the acquisition of Toopher by Salesforce, new users are no longer being accepted to use this feature. Current users can continue to use this feature as long as Salesforce continues to support it.

Android, iPhone, and Windows Phone. You can get Toopher@here:@https://www.toopher.com/

[accordion-item title= "Setting Up LastPass with Toopher" id="h0"]

To install Toopher with LastPass please do the following:

- Download the Toopher App to your smartphone (iOS Apple App Store or for Android from the Google Play Store).
- 2. Login to your LastPass Vault.
- 3. Select "Settings" (left sidebar).
- 4. Then select "Multifactor Options" (fourth tab from the left on top).
- Here is where you will be able to switch over to Toopher by selecting the "Toopher" radio button at the top of the page.
- 6. Once you have selected Toopher, you will be taken to a different screen. On the new screen you will switch "Toopher Authentication" from "Disabled" to "Enabled", at this time you will be prompted to enter a 2-word pairing phrase . This paring phrase will be generated by the Toopher app on your mobile device (see next step).
- 7. Open the Toopher App on your mobile device and select the "+" button in the top-right of the app screen. This will generate a 2-word pairing phrase. Back on the computer browser; Enter this 2 word pairing phrase into the browser field and then select enter.

You will receive a push notification on your phone that will prompt you to select allow or deny. Select allow, pairing is complete and you have now enabled Toopher with Last Pass.

Now if you choose, the Toopher - LastPass, two factor authentication can be automated. That is if you are on the same computer, in the same location logging into LastPass (the same site) you can tell your mobile device to automatically log you in next time. Simply slide the the automate when near here slider to the right. Now Toopher will automatically enable two factor authentication for you. This feature can be turned on or off when ever you wish.

[/accordion-item] [accordion-item title= "Administrating Toopher in Enterprise" id="h1"]

You can require access to Toopher for your users via the "Require use of Toopher" ***policy**. This policy can be enabled for your Enterprise account by accessing your Enterprise console and clicking the 'Setup' tab > 'Add Policy' button > Select 'Require use of Toopher' from the dropdown menu:

Policy	
Policy Require use of Toopher	Eut.list.of.Policie
Require use of Toopher as a second factor of a into LastPass. Click the 'enabled' box to enable enter your integration key, secret key, and API	uthentication when logging a this policy. You must also hostname in the boxes below.
Enabled 🗷	
Applies To:	t of Users
Notes	
	Cancel Save

[/accordion-item] [/accordion]

RSA SecurID





LastPass Enterprise supports RSA SecurID as a 2nd factor of authentication for user access to their LastPass Enterprise account. A second factor of authentication can protect your LastPass vault against replay-attacks, man-in-the-middle attacks, and a host of other threat vectors.

[accordion openfirst=true scroll=true clicktoclose=true] [accordion-item title="Setting up RSA SecurID with LastPass Enterprise" id="h0"]

Once enabled, the user will be prompted first for his/her LastPass Master Username and Password, and then for his/her RSA SecurID passcode. As with all of our multi-factor options, users will have the option to &trust& certain devices to eliminate the 2nd factor prompt & striking the perfect balance between security and convenience. If you prefer to disable the Trust option, this can be done using the configurable LastPass Security Policies.

RSA Authentication Manager supported features				
LastPass Enterprise				
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No			
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No			
RSA SecurID Authentication via RADIUS Protocol	Yes			
RSA SecurID Authentication via IPv6	No			
On-Demand Authentication via Native SecurID UDP Protocol	No			
On-Demand Authentication via Native SecurID TCP Protocol	No			
On-Demand Authentication via RADIUS Protocol	Yes			
Risk-Based Authentication	No			
RSA Authentication Manager Replica Support	Yes			
Secondary RADIUS Server Support	Yes			
RSA SecurID Software Token Automation	No			
RSA SecurID SD800 Token Automation	No			
RSA SecurID Protection of Administrative Interface	No			

[/accordion-item]

[accordion-item title="Agent Host Configuration" id="h1"]

To facilitate communication between LastPass Enterprise and the RSA Authentication Manager / RSA SecurID Appliance, an agent host record must be added to the RSA Authentication Manager database. The agent host record identifies LastPass Enterprise and contains information about communication and encryption. Set the Agent Type to Standard Agent when adding the authentication agent.

Since LastPass will be communicating with RSA Authentication Manager via RADIUS, a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

Note: The RADIUS client shows how must resolve to the IP address specified.

LastPass Enterprise employs a distributed architecture which encompasses many similarly configured servers. As a result of this architecture, RSA Authentication Manager administrators will need to configure agent host records and/or RADIUS clients for each LastPass Enterprise server. There are a few different methods for achieving this with varying amounts of administrative effort. These options are:

- $\circ\;$ Configure an agent host record and corresponding RADIUS client for each LastPass Enterprise server.
- Configure an agent host record for each LastPass Enterprise server with a shared RADIUS client.

Configure a shared RADIUS client that does not use an agent host record. (Global change)

Note: Refer to RSA Authentication Manager Administrators Guide for information on configuring shared RADIUS clients.

[/accordion-item]

[accordion-item title="Configuring RSA SecurID within the LastPass Admin Console" id="h2"]

This section provides instructions for configuring LastPass Enterprise with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All LastPass Enterprise components must be installed and working prior to the integration. Φ Perform the necessary tests to confirm that this is true before proceeding.

Configure LastPass Enterprise for RSA SecurID Authentication

- While logged into your LastPass Enterprise Admin Console, click on the �Setup� tab, then click on �Other Enterprise Options�. You can also go directly to�https://lastpass.com/enterprise_options.php#securid
- 2. Click on
- Enter the IP addresses of the RADIUS servers used by your RSA SecurID implementation, and enter the RADIUS shared secret as well.

Marvasol, Inc) (US) https://lastpa	ass.com/enterprise_options	s.php#securid	7 C	: 🔝 = Goo	ple		P 1	0 4	Ĥ
actDaccETT	-						ENG	сиян 👻	k
ENTERPRIS	5 E		HOME	SETUP	SAML	USERS	REPO	ORTING	
SETUP> POLICIES	CREATE NEW USER	INSTALL SOFTWARE	PUSH SITES TO US	IRS LC	GOIT				
									1
DCA CarrielD									
RSA SecurID									
RSA SecurID LastPass supports RSA Sec	curiD authentication via	RADIUS. You must set u	ip a RADIUS client for La	stPass in yo	ir RSA Authe	ntication Ma	inager. Si	ince RSA	
RSA SecuriD LastPass supports RSA Sec Authentication Manager di separate firewall to restrict	curiD authentication via oes not let you specify n t connections to the nec	RADIUS. You must set u multiple IP addresses fo cessary IP addresses. Th	ip a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be	stPass in yo commend us accessible 1	ir RSA Authe ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	nager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports RSA Sec Authentication Manager di separate firewall to restrict can view a list of all LastPar	curiD authentication via ioes not let you specify n t connections to the nec iss server IP addresses a	RADIUS. You must set u multiple IP addresses fo cessary IP addresses. Th at:	p a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be	stPass in yor commend us e accessible :	ur RSA Authe ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	inager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports RSA Sec Authentication Manager di separate firewall to restrict can view a list of all LastPa https://lastpass.com/docs/lp	curID authentication via oes not let you specify n t connections to the nec iss server IP addresses a stopp	RADIUS. You must set (multiple IP addresses fo cessary IP addresses. Th at:	ip a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be	stPass in yo commend us e accessible :	ar RSA Authe ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	inager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports RSA Sec Authentication Manager di separate firewall to restrict can view a list of all LastPar https://lastpass.com/docs/ap RAD/US Server IP Addresse	curiD authentication via oes not let you specify n t connections to the nec ss server IP addresses a sphp es:	RADIUS. You must set u multiple IP addresses fo cessary IP addresses. Th at: 216.162	up a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be 248.81.216.162.248.82.5	stPass in yor commend us e accessible 216.162.248.	ur RSA Authe ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	inager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports RSA Sec Authentication Manager di separate firewall to restrict can view a list of all LastPa https://astpass.com/docs/ip RADIUS Server IP Addresse separate multiple with con	curiD authentication via oes not let you specify n t connections to the nec iss server iP addresses a sphp es: mmas	RADIUS. You must set u multiple IP addresses fo cessary IP addresses. Th at: 216.162	p a RADIUS client for La a RADIUS client, we rec is RADIUS client must be 248 81,216 162 248 82,2	stPass in you commend us e accessible 1 216.162.248	or RSA Authe ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	nager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports RSA Sec Authentication Manager di separate firewall to restrict can view a list of all LastPa https://astpass.com/docs/ip RADIUS Server IP Addresse separate multiple with con e.g. 216.162.248.81,216.16	curID authentication via oes not let you specify n t connections to the nec ss server IP addresses a s.php es: mmas s2.248.82,216.162.248.8	RADIUS. You must set i multiple IP addresses fo cessary IP addresses. Th ad: 216.162	ip a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be 2 248 81,216 162 248 82,2	stPass in you ommend us a accessible 216.162.248.	r RSA Authe ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	inager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports RSA See Authentication Manager d separate firewail to restrict can view a list of all LastPa https://astpass.com/docs/ip Ntps://server IP Addresss separate multiple with con e.g. 216.162.248.81,216.16 RADIUS Shared Secret:	curID authentication via oes not let you specify n t connections to the nec as server IP addresses a scabe es: mmas 52.248.82,216.162.248.8	RADIUS. You must set t multiple IP addresses fo cessary IP addresses. Th at: 216.162 R3	ip a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be 248 81,216,162,248 82,2 78	stPass in yor commend us e accessible 216.162.248.	er RSA Authe ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	inager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports IRSA Sec Authentication Manager di separate frewall to restrict an vew a list of all LastPa https://astpass.com/docs/p https://astpass.com/docs/p https://astpass.com/docs/p RADIUS Server IP Addresss separate multiple with con e.g. 216.162,248.81,216.16 RADIUS Shared Secret:	curID authentication via oes not let you specify n t connections to the nec es server IP addresses a scabe es: mmas 52,248.82,216.162.248.8	RADIUS. You must set ti multiple IP addresses fo cessary IP addresses. Th at: 216.163 R3 123456	up a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be 2 248 81,216,162,248,82,2 78	stPass in yor ommend us e accessible 216.162.248	ur RSA Authe ing the 'ANY' from all Last	ntication Ma Client' optio Pass server I	nager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPass supports IRSA See Authentication Manager di separate frewall to restrict ran view a list of all LastPa RADIUS Server IP Addresss separate multiple with con e.g. 216.162.248.81,216.16 RADIUS Shared Secret:	curID authentication via oes not let you specify n t connections to the nec so server IP addresses a solo solo es: mmas S2.248.82,216.162.248.8	RADIUS. You must set 0 multiple IP addresses fo cessary IP addresses. Th at: (216.162 E3 (123456	up a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be 248 81,216 162 248 82,2 78 Update	stPass in yor commend us e accessible 216.162.248	ar RSA Authe ing the 'ANY room all Last	ntication Ma Client' optio Pass server I	inager. Si n, and us P addres:	ince RSA sing a ses. You	
RSA SecuriD LastPlass supports RSA Sec Authentication Manager di separate frewall to restrict an view a list of all LastPa https:/lastpass.com/docsip RADUUS Server IP Address separate multiple with con e.g. 216.102.248.81.216.16 RADIUS Shared Secret:	turiD authentication via oes not let you specify n connections to the nee sis server IP addresses a spe es: nmas s2,248,82,216,162,248,8	RADIUS. You must set u multiple IP addresses fo cessary IP addresses. Th at: 216.162 13 13	ip a RADIUS client for La r a RADIUS client, we rec is RADIUS client must be 248 81 216 162 248 82 2 78 Update	stPass in yor commend us e accessible : 216.162.248.	rt RSA Authe Ing the 'ANY from all Last	ntication Ma Client' optio Pass server I	inager. Si n, and us P addres:	ince RSA sing a ses. You	

4. Click @Update@ to save the values to your LastPass Enterprise account.

5. Your users will now be able to enable RSA SecurID as a multifactor authentication option within Account Settings.

[/accordion-item]

[accordion-item title="End User Settings" id="h3"]

Once the connection has been configured, your users can now enable RSA SecurID on their accounts by clicking on the LastPass Plug-in -> Preferences -> Account Settings -> Multifactor Options, and then selecting



C Link Person	SecuriD* To use RSA SecuriD with LastPass, you must already be set up to use RSA SecuriD by your RSA SecuriD administrator.	\otimes		
Add Site		牡	*	1
Add Secure	RSA SecurD Authentication Disabled · Heb	业	*	
Create Fold	Permit Offine Access Allow • Help	九	*	
User Manual Security Check ()	PLEASE NOTE: If you choose to permit offline access, your data may temporarily be available in offline mode before you complete multifactor authentication. Click here to learn more about this.	北	*	
		九	*	
		牡	*	
		牡	*	
	Cancel Update	九	*	
	> 🔛 Shared-LP	九	*	
			34	

[/accordion-item]

[accordion-item title="RSA SecurID Login Screens" id="h3"]

Login screen:



User-defined New PIN:

Iultifactor Authentication		×
RSA SecuriD'	Enter a new PIN having from 4 to 8 alphanumeric characters:	
This comput	Authenticate ter is trusted, do not require a second form of authentication. our device, click here to disable multifactor authentication	

System-generated New PIN:



Next Tokencode:





[/accordion-item]

[accordion-item title="Enforcing the Use of RSA by Your Employees through LastPass Policies" id="h4"]

With LastPass Enterprise you can leave the 2nd factor decision up to your end users, or you can mandate its use with our configurable Security Policies. To access these policies, click on the LastPass Plug-in, select �Admin Console � -> Set-Up -> Policies. Here are some policies that you might consider implementing relative to RSA SecurID:

Require use of RSA SecurID

Require use of RSA SecurID as a second factor of authentication when logging into LastPass. Click the 'enabled' box to enable this policy. RSA SecurID must be configured by the user.

Require use of any multifactor option

Require use of any multifactor option as a second factor of authentication when logging into LastPass. Click the 'enabled' box to enable this policy. YubiKey, LastPass Sesame, Google Authenticator, Toopher, Duo Security, Transakt, Salesforce#, and RSA SecurlD are the currently available options.

Restrict Multifactor Trust

Restrict computers that can be trusted by IP address (learn more about 'trusted computers' here: https://helpdesk.lastpass.com/account-settings/trusted-computers/. You can enable this policy to allow users to skip second factor authentication from trusted locations (such as the office) but still require it from remote locations.

Any of the aforementioned policies can be enabled across all users in the account, or based on some sub-set thereof.

[/accordion-item]

[accordion-item title="Certification Test Checklist for RSA Authentication Manager" id="h5"]

Certification Test Checklist for RSA Authentication Manager

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
LastPass Enterprise	3.1.50	Windows / Mac OS X / Linux / Android / iOS / Windows Phone

RSA SecurID Mandatory Functionality

RSA SecurID Authentication

Date Tested: June 30th, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
New PIN Mode		· · · ·	
Force Authentication After New PIN	N/A	N/A	
System Generated PIN	N/A	N/A	✓
User Defined (4-8 Alphanumeric)	N/A	N/A	
User Defined (5-7 Numeric)	N/A	N/A	✓
Deny 4 and 8 Digit PIN	N/A	N/A	V
Deny Alphanumeric PIN	N/A	N/A	\checkmark
Deny PIN Reuse	N/A	N/A	\checkmark
Passcode			
16 Digit Passcode	N/A	N/A	V
4 Digit Fixed Passcode	N/A	N/A	\checkmark
Next Tokencode Mode			
Next Tokencode Mode	N/A	N/A	V
On-Demand Authentication			
On Domand Authentication	NI/A	Μ/Λ	

On-Demand New PIN Load Balancing / Reliability Testing Failover (3-10 Replicas) No RSA Authentication Manager

N/A	N/A	× ×
N/A	N/A	✓
N/A	N/A	✓

'92/92'

PEW/PAR

✓=Pass × = Fail N/A = Not Applicable to Integration

[/accordion-item] [/accordion]

Full List of Policies

Multifactor Authentication

Site Map

[sitemap]

[sitemap_pages exclude="20015"]