Quick Start Guide Appliance

Contents

- 4.2.1. Introduction
- 4.2.2. Part 1: Setup the LinOTP Smart Virtual Appliance
- 4.2.3. Basic Configuration Quick Start
- 4.2.4. Part 2: Connecting to the User Directory, Rollout of Tokens
- 4.2.5. Appendix: Practical Tips and Legal Notes

4.2.1. Introduction

Thank you for purchasing a LinOTP Smart Virtual Appliance for strong user authentication

This Quick start guide is divided into two parts and an appendix:

- This chapter describes the access and setup of the appliance with final activation via the WEB UI of the appliance.
- Afterwards, the LinOTP management is configured to manage the tokens. <u>Quick Start</u> <u>Guide Token Management</u>

Licensing

LinOTP Smart Virtual Appliance can be acquired with a existing LinOTP Enterprise Subscription and Support License. Subscription and Support are licensed for the number of active token managed in LinOTP. You can find instructions on installing the license file during the configuration wizard in part 2 of this Quick Start Guide. Please have a look at <u>Install a</u> <u>new license</u>.

Documentation, Support & Notes

A complete introduction can be found in the LinOTP Manual, which you can download from the Appliance menu using the help function.

You will find more information for technical support as well as practical tips at: https://www.linotp.de/support.html

4.2.2. Part 1: Setup the LinOTP Smart Virtual Appliance

For accessing the web configuration interface of the Appliance you have to know the IP address. If you automatically receive your IP address, you can allow it to be displayed directly in the console of LinOTP Smart Virtual Appliance. To do so, log in with the user name: "root" and the password "eBai6Lait9" directly in the console. The IP address will be displayed (version 2.0) or enter the command "ifconfig" - the address will appear in the second line below eth0 (inet addr:)

```
Debian GNU/Linux 10 linotpappliance tty1
linotpappliance login: root
Password:
Last login: Mon Oct 17 11:51:27 CEST 2022 from 192.168.100.1 on pts/0
Linux linotpappliance 4.19.0–21–amd64 #1 SMP Debian 4.19.249–2 (2022–06–30) x86_64
Linux linotpappliance 4.19.0–20–amd64 #1 SMP Debian 4.19.235–1 (2022–03–17) x86_64 GNU/Linux
**********************
         Welcome to the LinOTP Smart Virtual Appliance (SVA)
≠ You are now entering a limited shell to the SVA.
¥ For basic IP configuration, the command 'setup_appliance.py'
¥ can be used, but we recommend configuring your SVA using the
 web interface.
 You could enter a normal shell by typing: 'unsupported'
! but we recommend not doing that!
! This would give you a complete root shell. Be aware. You can
break many things here.
YOU ARE THEN PROCEEDING ON YOUR OWN RISK!
# If you have any questions please contact our technical support.
                          support@keyidentity.com
*********************
Please proceed configuring your SVA using the web interface at
'https://192.168.100.230:8443'
/ou are in a limited shell.
Γype '?' or 'help' to get the list of allowed commands
Type '?'
<u>r</u>oot:~$
```

Note

We recommend conducting all additional configuration of the web interface after installation!

When opening the configuration interface of the appliance *https://[IP address of your LinOTP]:8443*, a window will appear with a certificate warning that varies based on the browser used. In general, you should take this kind of certificate warning seriously when visiting websites, as these provide information regarding possible security risks and thus associated risks for the visitors of a website. In the case of LinOTP Appliance, however, there is no risk. The warning notification appears because LinOTP Smart Virtual Appliance presents the browser with a self-signed certificate when opened. Therefore, please ignore the certificate warning and confirm the access to the IP address requested (your configuration interface of the appliance). If your browser allows, you can add the IP address of your LinOTP Smart Virtual Appliance to the list of trusted sites.

As an alternative to the certificate delivered, you can also add your own certificate at a later time using the Appliance Management. To do so, please refer to the LinOTP Manual (Chapter IV "LinOTP Appliance Manual", Section 8 "Change the Server SSL Certificate")

LinOTP Smart Virtual Appliance

Username:		٢
Password:		P
	Login	

You will be asked for a user name and password on the login screen that then opens. Enter "root" here as the user name and the initial root password "eBai6Lait9". For security reasons, you should change this password in the fourth-step of configuration wizard (Configuration – Quick Start, 4. User Roles and Passwords) described in the following.

If LinOTP is intended to be operated behind a firewall, for example in a DMZ, please be sure to take the correct configuration of the firewall rules into account. You will find the corresponding section in the LinOTP Manual, (Chapter IV "LinOTP Appliance Manual", Section 14 "Network Integration")

4.2.3. Basic Configuration - Quick Start

If you have not already done so, open your browser and access the Configuration interface of the LinOTP Appliance as described on page 9 under number 11. You can correspondingly ignore the certificate warning and log on with the root password.

Right after the login [Appliance version 2.0 upward] you will be asked whether you want to restore a backup or to setup the new machine manually.

Please check the box "*Restore a LinOTP Smart Virtual Appliance from a backup file*" if you would like to restore the machine from a backup file. You will see the head of the website changing to contain fewer configuration items. Continue otherwise with the normal setup procedure as described below.



License Agreement

Please read the license agreement carefully. To advance to the next step, check the box following "I accept the license agreement" and click on "Next". By doing so, you declare your acceptance of the license agreement.

0 License License agreement	1 Support Install support license	2 Network Hostname and network	3 Time Time and time	
4 Accounts Administrator and root	5 RADIUS Configure RADIUS client	6 Key Generation Create encryption keys		
License Agreement LinOTP Smart Virtual Applianc Software-License and Limitati The software product "LinOTP LinOTP Smart Virtual Applianc WebGUI), "usb configure", "ap "lse show version", "appliance servi the Rollout-, Update-mechanis documentation, "LinOTP Virtua "LinOTP Installation Guide", Appliance Manual", "LinOTP Mo Start Guide" - referred to as the product and the component	e ons Smart Virtual Appliance" and r e Web Application (Appliance A ppliance configure", "setup app e-diskfree", "setmackey", "set ce restart", "appliance-update ms and the components LinOTP NLIOTP User Guide", "LinOTP "LinOTP User Guide", "LinOTP "LinOTP User Guide", "LinOTP sidule Development Guide" and "L 'Software' hereafter - as wel is are licensed, not sold. Iacceptth	elated components PI, Appliance Liance", version", "test-ssh- ", "auto-backup" and anual and/or LinOTP Management Guide", mart Virtual Quick las all copies of elicense agreement		
			Next	

Registration of your Enterprise Support and Subscription license

By default the LinOTP Smart Virtual Appliance offers the ability to run on a demo license which is restricted for 14 days and to maximum 5 tokens.

0 License License agreement	1 Support Install support license	2 Network Hostname and network	3 Time Time and timezone or NTP
4 Accounts Administrator and root	5 RADIUS Configure RADIUS client	6 Key Generation Create encryption keys	
LinOTP Support and Subscr	iption License		
Use a 14 day evaluation license includir	g up to 5 tokens.		
		Bravious	Nove

To run the LinOTP Smart Virtual Appliance in a production mode uncheck the evaluation checkbox and enter your LinOTP Enterprise Token license and your LinOTP Enterprise

Subscription and Support update key.

Your LinOTP Enterprise Token license is the license file (*.*pem* file format), which you received with the purchase of your LinOTP Enterprise Subscription and Support. Activate the license by using "Set License".

0 License License agreement	1 Support Install support license	2 Network Hostname and network	3 Time Time and timezone or NTP
4 Accounts Administrator and root	5 RADIUS Configure RADIUS client	6 Key Generation Create encryption keys	
LinOTP Support and Subsc	ription License ng up to 5 tokens.		
Select a support and subscription license file	for your LinOTP instaliation.		
Datei auswählen Keine ausgewählt Appliance update key			
Please enter the appliance update key (form	erly known as 'serial number') update key		
		Previous	Next Activate

The LinOTP Enterprise Subscription update key is a 8 digit number received as well with your purchase. It is use to keep your system up to date.

0 License License agreeme	ent 1	Support Install support license	2	Network Hostname and network	3 Time Time and timez	
4 Accounts Administrator and	d root	RADIUS Configure RADIUS client	6	Key Generation Create encryption keys		
LinOTP Support	t and Subscriptio	n License 5 tokens. in, Deutschland				
Datei auswählen _P Appliance updat Please enter the applianc 03511217	011-20271418.pem te key re update key (formerly know Check update	vn as 'serial number') key				
				Previous	Next	Activate

Basic Network Configuration

Network Interface

Enter the IP address and netmask via which the LinOTP Appliance should be accessed here. Enter the default gateway under gateway.

Hostname and DNS

Enter the hostname of the LinOTP server here. You can freely select this hostname, however, it should not already be used by another device in the network. Please enter the name of the domain in which the LinOTP Appliance is located separately in the next field. A list of domains can be entered in the "Search" field that will also be searched. Normally, you will enter the domain names there again.

0 Lic	ense nse agreement	1	Support Install support license	2	Network Hostname and network	3	Time Time and time	
4 Ac Admi	counts inistrator and root	5	RADIUS Configure RADIUS client	6	Key Generation			
Network	interface							
IP Address:	192.168.100.193							
Netmask:	255.255.255.0	۲,						
Gateway:	192.168.100.1							
Hostnam	ne and DNS							
Hostname:	linotp01							
Domain:	corp.example.edu							
Search:	corp.example.edu							
Nameserver:	192.168.100.1							
					Previous		Next	Activate

The field 'Nameserver:' understands the following syntax:

192.168.0.1, 172.168.0.1

a comma (no comma at the end) separates the lines 'nameserver...' in /etc/resolv.conf.

Setting the Time and Date

In a third step, you can change the date, time or time zone, if necessary. An NTP server can be entered from which the time is automatically received, if applicable.

0 Lice	cense nse agreement	1 Support Install support license	2 Network Hostname and network	3 Time Time and timezone or NTP
	counts	5 RADIUS Configure RADIUS client	6 Key Generation Create encryption keys	
Time an	d Timezone			
Date:	10/19/22			
Time:	10:53			
Timezone:	Europe/Berlin	~		
NTP server:	2.de.pool.ntp.org, 0.de.pool.	I.ntp.org iburst		
			Previou	is Next Activate

The field 'NTP server:' understands the following syntax:

en.pool.ntp.org iburst, 0.debian.pool.ntp.org, 192.168.0.1

a comma (no comma at the end) separates the lines 'server...' in /etc/ntp.conf.

User Roles and Passwords

The LinOTP Appliance generally recognizes three different roles:

- 1. LinOTP Administrator the LinOTP Administrator manages LinOTP. She does not have any rights on the level of the Appliance, operating system or on the network level. The name can be chosen and additional administrators can be configured later in the running system.
- 2. Appliance Administrator the Appliance Admin may only change the Appliance functions and provide access rights. They may change passwords, but not the root password.
- 3. Root Administrator the Root Admin has the most rights on the Smart Virtual Appliance. He has no access to LinOTP, but can manage everything on the Appliance.

	LinOTP Admin	Root Admin	Appliance Admin
1. Tokenmanagement	ja	nein	nein
2. Appliancemanagement	nein	ja	ja
3. SSH Anmeldung	nein	ja	nein
4. Passwortänderung	nein	alle	nicht von root

Now provide and/or change the passwords for these three roles. The "Old root password" requested for the Root Admin role is the initial root password "eBai6Lait9".

Note

Note regarding password complexity

For security reasons, be certain to select sufficiently complex passwords when changing the passwords. Passwords are deemed to be sufficiently complex by today's standards when they meet the following criteria:

- Password length of at least 10 characters
- Combination of upper case and lower case letters, number and special characters Once you have entered and/or changed all of the passwords, go ahead to the next step by clicking the "Next" button.

Please note that the input mask depicted can only be exited when all fields have been completed and the newly entered passwords are highlighted. Scrolling backwards using the "Previous" button is also not possible until the fields have been fully completed.

0 License License agreement	1 Support Install support license	2 Network Hostname and network	3 Time Time and timezone or NTP
4 Accounts Administrator and root	5 RADIUS Configure RADIUS client	6 Key Generation Create encryption keys	
LinOTP Administrator User name: admin	Ũ		
New password: •••••••• Confirm new password: ••••••			
Appliance Administrator (ap	padmin)		
New password:	12 12		
System Administrator (root)			
Current password: •••••••	P 7		
Confirm new password:			
		Previous	Next Activate

Definition of the RADIUS Clients

In this step, you will define the first RADIUS client to be allowed to issue authentication queries to the RADIUS server of the LinOTP Appliance. Additional clients can be added and managed via the LinOTP Management after the completion of the initial configuration.

RADIUS (Remote Authentication Dial In User Service) is the most frequently used client server protocol for the authentication, authorization and administration of users of dial in connections in a computer network. One generally distinguishes between the RADIUS server, which conducts the validation of the login query, and the RADIUS client, which sends the authentication query. Typical examples of a RADIUS client are a VPN gateway, a firewall as well as a portal server or terminal server.

LinOTP naturally also functions with the LinOTP RADIUS client "LinOTP Authentication Provider for Windows (LAP)" which allows you to make a RADIUS-based login to the Windows operating system or Windows Terminal Server. In order to be able to use RADIUS, enter the subnetwork of the RADIUS client ("Netmask") and its IP address. You can freely select the name of the "New RADIUS Client". In addition, the password ("Secret") is required for the RADIUS communication. If you do not plan to us RADIUS authentication or want to configure it later, you can check "No RADIUS Client access configuration" and skip the configuration.

0 License License agreement	1 Support Install support license	2 Network Hostname and network	3 Time Time and timezone or NTP		
4 Accounts Administrator and root	5 RADIUS Configure RADIUS client	6 Key Generation Create encryption keys			
RADIUS client access config	guration				
New RADIUS client: VPNF5					
IP Address: 192.168.100.123					
Netmask: 255.255.255	Û				
Secret:	P				
Secret:	A.				
Short name (optional): f5					
No RADIUS client ac	cess configuration				
The LinOTP Smart Virtual Appliance will act a your Firewall or VPN Gateway will be your R	as RADIUS server. Here you need to specify a ADIUS clients. The RADIUS client will ask the	RADIUS client allowed to connect to the LinO LinOTP Smart Virtual Appliance, if the users c	TP Smart Virtual Appliance. For example redential can be authenticated or not.		
For the LinOTP Smart Virtual Appliance RAD network mask, your RADIUS client is located client (Firewall or VPN Gateway) you will req Appliance RADIUS server.	For the LinOTP Smart Virtual Appliance RADIUS server you need to define, which IP addresses are allowed to run authentication requests. Therefor you need to specify the IP and network mask, your RADIUS client is located in. You also need to specify the shared RADIUS secret, which is used to secure the RADIUS communication. To configure your RADIUS client (Firewall or VPN Gateway) you will require to set the LinOTP Smart Virtual Appliance address and the same RADIUS secret as specified here for the LinOTP Smart Virtual Appliance RADIUS server.				
If you don't want to configure the RADIUS se the Appliance management web interface.	rver right now, you can check the checkbox be	elow the form. You can change and thereby act	tivate RADIUS for more clients at any time in		
		Previous	Next Activate		

Key Generation and Database Passwords

In the last step, you decide whether the factory installed keys for SSH, SSL and to encrypt the files in the database and the internal database passwords should be generated again. This is absolutely recommended when running the wizard for the first time in order to prevent unauthorized third parties with knowledge of the factory installed keys and passwords from accessing the system or the files.

In addition, you can specify in this mask whether the Appliance should be shut down after the completion of the configuration. You should definitely use this option if you have changed the IP address of the Appliance or want to move it into another VLAN. In this case, the Appliance will only be accessible via the new IP address after the activation of the configuration and can no longer be administrated and/or turned off via the existing browser session.

Click the "Activate" button to save all entries, activate and – if selected – shutdown the Appliance. All further configurations can be made from any computer within the network.

0 License License agreement	1 Support Install support license	2 Network Hostname and network	3 Time Time and timezone or NTP
4 Accounts Administrator and root	5 RADIUS Configure RADIUS client	6 Key Generation Create encryption keys	
Encryption keys and passwe	ords	anted. If you do not want to use these lows w	ou con generate these lows anow
 create new SSH keys. create new SSL server certificate. create new signing keys for audit trail. create new database encryption key. create new internal MySQL passwords for a server server	or the MySQL root user and for the LinOTP da	itabase user.	
		Previous	Next Activate

Finish Appliance Configuration	×
Verifying configuration data: Saving configuration data: Creating new encryption key: Creating new SSH keys: Setting new SQL server password: Creating audit key pair: Creating new server certificate: Installing appliance support license: Setting update key: Upgrading system: Activate new configuration:	done done done done done done done done
Forward	to appliance administration

Now, by logging back into the SVA *https://<linotp_fqdn>:8443*, the configuration just created can be checked and changed. The details are described here <u>The Appliance Dashboard</u>. It should be checked that the license and the update key are installed correctly so that the system can receive update. Just have a look at the dashboard.

4.2.4. Part 2: Connecting to the User Directory, Rollout of Tokens

Open the LinOTP Management Interface

Open the browser on your administration computer and enter the IP address of your LinOTP server in the address line as you did previously when performing the network basic configuration *https://[IP address of your LinOTP]/manage* You may receive the certificate warning already mentioned at this point, deal with this as described on p. 10. Then log in with the access data of the previously defined LinOTP Administrator (the name can be freely issued before).

🗖 📘 Management Login -	n: × +	-	o x					
← C ▲ Nicht siche	← C ▲ Nicht sicher https://linotp01.corp.example.edu/manage/login 🔞							
Userna Passwo LinOTP 3.2 – Copyright (C) netgo Grr	Login to LinOTP Manage-UI							

Creating User ID Resolvers

User ID Resolvers are required in order to make a connection from LinOTP to user directories. These can be LDAP based directory services (Microsoft Active Directory, Novell eDirectory, Open LDAP, amongst others), SQL-based databases or flat files such as /etc/passwd.

A User ID Resolver represents the connection to the respective directory service or respective database. LinOTP only requires read permissions for its access to the target systems.

← C ▲ Nicht	sicher <mark>https</mark> :/	//linotp01.corp	o.example.e	du/mana	ge/				ŵ	•
LinOTP Config 🔹	Tools Im	nport Token File	e Help) ~					L	inOTP
UserIdResolvers								admin@linotp_admins (LinOTF	local	_admins) 🔻
Realms	Token View	User View	Policies	Audit	Trail					
System Config	Lost Toker	n 🛛 🛛 Token	Info ¢	Resync To	oken					
Provider Config	Serial Number	Active Usern	name F	Realm	Туре	Login Attempts Failed	Description	Max Login Attempt OTP Length	Cour	nt Window
Token Config										
Policies										
+ Enroll										
↔ Assign										
← Unassign										
 Enable 										
 Disable 										
≖ Set PIN										
⊯ Reset Failcounter										
© Set Expiration	Find			Login Name	~	Search				
To Delete	۹ 15 ۲	I ■ Page 1	of 1	N S	No ite	ems				

In the start screen, select the item "useridresolvers" in the "LinOTP Config" menu. In the window that opens, click on the option "New" and select the correct directory type (we will choose LDAP for the following example).

Resolver	ж
Create a new or select one available UserIdReso	lver:
LinOTP_local_admins [sqlresolver]	admin managed
+ New A Edit 9 Duplicate	Delete Kose

Re	solver	×	
Cre	Creating a new UserIdResolver		×
	Which type of resolver do you want to create?		
	⊘ Cancel LDAP SQL Fla	atfile	2

Server Configuration		
Resolver name:	winad	
Server-URI:	Idaps://w2k19dc1.corp.example.edu, Id	daps://w2k19dc2.corp.example.edu
TI C.		ions
115.	Only allow system-trusted certificate	es
BaseDN:	dc=corp,dc=example,dc=edu	
BindDN:	query@corp	
Bind Password:	•••••	
	If security relevant information is changed, for e provided to avoid unprivileged exposure of the	example the URL, the password has to be password
Timeout:	5	
Sizelimit:	500	Connection test successful
	No anonymous referral chasing	Number of users found: 35
Mapping Attributes		
Coordefilter	SAMAccountiname	Ok
Searchniter:	(sAMAccountName=*)(objectClass=us	er)
Userfilter:	(&(sAMAccountName=%s)(objectClass	s=user))
Attribute mapping:	{ "username": "sAMAccountName", "ph	none" : "telephoneNumber", "mobile" : "m
UID Type:	objectGUID	
P	reset Active Directory	Preset LDAP

Enter the following information in the input mask:

• **Resolver name** (freely selectable)

- Server URL (the URL address through which the directory service or database is accessible), this can be either ldap://adl.example.net, ldap://adl.example.net for LDAP (LinOTP will try to establish a secure connection via StartTLS) or ldaps://adl.example.net, ldaps://adl.example.net for LDAP (LinOTP will try to establish a secure connection via StartTLS) or ldaps://adl.example.net, ldaps://adl.example.net for LDAPS a certificate is required for the latter method.
- BaseDN (Base Distinguished Name), consisting of the domain components. The BaseDN determines the point at which the directory tree of the User ID Resolver begins to search for users. Please separate the domain components into multiple entries, for example, "linotp.local" becomes "dc=linotp,dc=local".
- **BindDN** (Bind Distinguished Name, also account, account name), what is meant here is the user account with which the access to the directory service is made (only read permissions are required). The form of the ntries that you have to use depends on the underlying LDAP and/or Microsoft Active Directory[®] (AD) structure.

For example, the LDAP directory "administrator@dir.linotp.de" would become "cn=administrator,cn=user,dc=dir,dc=linotp,dc=de". The information "cn=user" is required because the "User" is located in the AD directory in our example. This is not always the case. Another, frequently encountered version that refers to organizational units can appear as follows: "cn=test.user,ou=users,ou=linotp, dc=linotp,dc=de". Alternatively, the entry "user@domain" can also always be used with AD directories.

- **Bind Password** (the password assigned to the BindDN).
- With AD structures, please also check the box "No anonymous referral chasing" (you can find more information in the LinOTP Manual, chapter I, article 3.2).
- By clicking the button "Test LDAP connection", it can be verified whether the user directory can be accessed with the information provided.
- Click the "Preset AD" or "Preset LDAP" button in accordance with the selected user directory type. LinOTP will then automatically fill the fields in the lower third of the screen.
- Close the process with "Save".

A window will appear that shows the resolver you have created (name and type). You can now connect to additional user directories ("New"), editing existing resolvers ("Edit") or delete them ("Delete"). To do so, the listed resolvers must be marked (highlighted). Then close this window with "Close".

Note

Detailed information about UserIdResolver configuration can be found at Configuring UserIdResolvers.

Creating Realms

A realm must be created after connecting to the user directory. Realms consist of a number of users that can come from different user directories. They offer extensive options for the grouping of users, which could allow them to be distinguished on the basis of their function or departmental affiliation. Multi-client infrastructures can also be easily depicted with realms.



To do so, select the corresponding menu item, "Realms", in the "LinOTP Config" menu and click on "New" in the window that opens.

Realms	×
Create a new realm or select one available realm:	
linotp_admins [LinOTP_local_admins]	admin
+ New ∠ Edit © Delete × Close Close Close Close <td>ear Default</td>	ear Default

First of all, enter a name and then select the User ID Resolver of a connected user directory (the selection will be highlighted). You can select multiple User ID Resolver to join them together in one realm.

Save the configuation:

Edit Realm	×
You are creating a new realm. You may add resolvers by holding down Ctrl- Key and left-clicking.	
Realm name:	_
corp-usen	
winad [Idapresolver]	
LinOTP_local_admins [sqlresolver] admin	
⊘ Cancel	

Close the "Realms" dialog:

Realms	×
Create a new realm or select one available realm:	
linotp_admins [LinOTP_local_admins]	admin
corp-user [winad]	default
+ New / Edit	Clear Default

Now the users from the selected realm are displayed in the "User View" tab.

inOTP Config	Tools	Import Token File	e He	lp –					LinC
								adm	in@linotp_admins (LinOTP_local_admi
elected User	Token View	User View	Policies	Audit Trail					
Selected Token									
	Username	UserIdResolver		Surname	Given Name	Email	Mobile	Phone	User ID
	ötzi	winad (LDAPIdRes	olver)		ötzi				76e9dd0c1dc6a9449561d298c5f
	ulli	winad (LDAPIdRes	olver)		ulli				06c1c9d97d8b104b8005e7e4644
alms:	ulla	winad (LDAPIdRes	olver)		ulla				7fbd98c8d5a2e84d9ac37441ab4
rp-user 🗸	tommy	winad (LDAPIdRes	olver)	tommy	tommy				2d9df7f8a25bc34c99cc78a13a69
	sebastian	winad (LDAPIdRes	olver)	Bach	J Sebastian				8fbc1b4ad78eee40beb7dc4850e
L Enroll	rainere	winad (LDAPIdRes	olver)	Endres	Rainer				071d4c3984c8d340bd6ebc1bd61
	query	winad (LDAPIdRes	olver)	User	Query				4a2c36cea8f2ff4e875dd1ae118b
⇔ Assign	petra	winad (LDAPIdRes	olver)		petra				180672591e8589429a60693f4ae
	peterc	winad (LDAPIdRes	olver)	Czaska	Peter				8f89a17c109a3140b2f227bd10d6
	peteradm	winad (LDAPIdRes	olver)		retep				a5ca29cfeadf354f9409debdf86d7
 Enable 	peter	winad (LDAPIdRes	olver)	Czaska	Peter		+491511		1ea7eaf90dbed04dad6648c44a4
	otto	winad (LDAPIdRes	olver)		otto				302c2704b048f7449bd35df777cc
	olli	winad (LDAPIdRes	olver)		olli				817276d4796f8b43985c9d0c47a
set PIN	maxmayer	winad (LDAPIdRes	olver)	Mayer	Max				d9aed628cea7c749aaf46adc782
. Denet	mark	winad (LDAPIdRes	olver)		mark				05fdc4d46d5f554095b2b0f30a61
Failcounter	Find			Username v	Search				

Token

You will also find extensive information about this topic in the LinOTP Manual (Chapter I "LinOTP Management Guide", Section 6 "Managing Tokens").

Hardware Token

In order to use the tokens, first import the file with the token seed files (import record). A seed file represents the secret key a token needs to generate the OTP value. To do so, select the item "Import Token File" from the menu and then the file type ("SafeNet/Aladdin XML" in our example).

OTP Config	Tools	Import Token File He	p –					Lin
		SafeNet/ Aladdin XML					adm	in@linotp_admins (LinOTP_local_adm
ected User	Token Vie	OATH CSV	Audit Trail					
ected Token	Username	YubiKey CSV	Surname	Given Name	Email	Mobile	Phone	User ID
	ötzi	Feitian XML		ötzi				76e9dd0c1dc6a9449561d298c5f
	ulli			ulli				06c1c9d97d8b104b8005e7e4644
	ulla	OATH compliant PSKC		ulla				7fbd98c8d5a2e84d9ac37441ab4
S.	tommy	T	tommy	tommy				2d9df7f8a25bc34c99cc78a13a69
usei 👻	sebastian	Tagespasswort Token File	Bach	J Sebastian				8fbc1b4ad78eee40beb7dc4850e
	rainere	eToken DAT File	Endres	Rainer				071d4c3984c8d340bd6ebc1bd61
+ Enroll	query	······,	User	Query				4a2c36cea8f2ff4e875dd1ae118b
↔ Assign	petra	winad (LDAPIdResolver)		petra				180672591e8589429a60693f4ae
	peterc	winad (LDAPIdResolver)	Czaska	Peter				8f89a17c109a3140b2f227bd10d6
	peteradm	winad (LDAPIdResolver)		retep				a5ca29cfeadf354f9409debdf86d7
 Enable 	peter	winad (LDAPIdResolver)	Czaska	Peter		+491511		1ea7eaf90dbed04dad6648c44a4
	otto	winad (LDAPIdResolver)		otto				302c2704b048f7449bd35df777cc
	olli	winad (LDAPIdResolver)		olli				817276d4796f8b43985c9d0c47a
■ Set PIN	maxmayer	winad (LDAPIdResolver)	Mayer	Max				d9aed628cea7c749aaf46adc782
It Reset	mark	winad (LDAPIdResolver)		mark				05fdc4d46d5f554095b2b0f30a61
	Tind		[Linearen	Carach				

First find the file with the token serial numbers and accompanying seed files that you received from your dealer. Now click the "Load Token File" button to load the token seed file/import record. The tokens loaded are now displayed in the "Token View".

OATH CSV Token File		×
Here you can upload a CSV file for your OATH token. The file is supp	oosed to contain one token per line:	
For HOTP and TOTP tokens:		
Serial number, Seed, Type, [OTP length], [Time step], [hashlib]		
Possible Values:		
Type -> HOTP, TOTP OTP length -> 6, 8 Time step -> Recommendation 30		
Hashlib -> SHA1, SHA256, SHA512		
For OCRA2 tokens:		
Serial Number, Seed, Type, Ocra Suite		
Type -> OCRA2 Ocra Suite -> OCRA-1:HOTP-SHA256-8:C-QN08, OCRA-1:HOTP-SHA256-8:C-QA64		
Default values:		
Type -> HOTP OTP length -> 6 Time step -> 30 Hashlib -> Choosen based on hash length. Fallback: SHA1		
Please choose the token file: Datei auswählen feitianc200.csv Target realm: corp-user v		
	☞ Load Token File	el

Soft Token

In order to enroll an initial software token, switch to "Token View".

← C ▲ Nicht sicher https://linotp01.corp.example.edu/manage/#										ය 🙁 …
LinOTP Config	Tools	Import To	ken File	Help						LinOTP
								admin@linotp_a	dmins (LinOTP	_local_admins) ▼
Selected User	Token Vie	w User	View Po	licies Audit	Trail					
Selected Token	Lost T	oken	Token Info	© Resync T	oken	♣ Set Token Realm				
	Serial Num	per Active	Username	Realm	Туре	Login Attempts Failed	Description	Max Login Attempt	OTP Length	Count Window
	2608624901	916 true		corp-user	TOTP	0	imported	10	6	10
Realms:										
+ Enroll ↔ Assign										

Click on "Enroll" and select "HMAC event based" and "Generate HMAC key" to generate a new seed. The QR code generated can be read by various software tokens (Google Authenticator or FreeOTP, for example).

Token type HM	AC time based	winad (LDAPide	Resolver)).
Create a new O Token seed:	ATH token - HMAC time	based	
O Enter seed			
Google Auth OTP digits Hash algorithm Time step Description	enticator compliant 6 ~ sha1 ~ 30 seconds ~ my first token		
Token PIN: Enter PIN: Confirm PIN:			
		+ Enroll	⊘ Cancel
en enrollment			
OATH Soft Token	OTP seed	S.	
L	the token in OATH compatib	le Soft Tokens (FreeOTP, (syntax).	Google

Assigning Tokens

Now assign the newly loaded tokens to your users. To do so, search for the corresponding user in "User View" and mark them (the entry will be highlighted).

Switch to "Token View" and select the token that should be assigned to the user (the entry will be highlighted).



Then click "assign" in the menu to the left to assign the token. If you switch back to "Token View" after this process, the name of the user will be displayed in the corresponding column behind the assigned token.

Setting the Token PIN



Certain scenarios require a higher level of security in handling tokens. The underlying principle is strong or two-factor authentication. It is more secure than simple typing in a password or showing a card, as a user must prove both factors of possession (token) and knowledge (password or PIN) to receive access.

To do so, set a PIN for your token.

- First select the desired token (the entry will be highlighted).
- Click on the "SET PIN" button in the left-hand side menu. A dialog window will appear where you can set the PIN yourself.

Your LinOTP Appliance is now fully configured and the tokens have been rolled out and assigned. You can being using your Appliance!

Please make sure to correspondingly configure your RADIUS clients before the first use. We have compiled a practical test as well as some useful information and tips for you on the following two pages. Please read these carefully in order to avoid any later complications.

We wish you a great deal of success for the use of your LinOTP product!

Practical Test

Before you place the LinOTP Appliance in live operation, you have the opportunity to test whether all of the configuration steps have been successfully completed using one of the rolled out tokens.

- Select the token of a user whose user name you know.
- Type *https://[IP address of your LinOTP]/auth/index* into the address line of your browser.
- Enter the user name for the selected token in the login screen.
- Generate an OTP value with the selected token and enter it along with the OTP PIN.

LinOTP will report a successful authentication process to you.

If the authentication fails, please check the configuration of your LinOTP Appliance, especially User ID Resolvers and tokens. The audit trail log in LinOTP Management can provide you with useful details for this. Also make sure that you have selected the proper token and that you have not made any typing errors. If you continue to be unable to make a valid authentication, please contact your LinOTP dealer.

Use Information and Notes

Backup and Software Update

a. Backup: We strongly recommend backing up the LinOTP configuration as well as the database at regular intervals. In the event of a defect with the appliance, this is the only way that the rolled out tokens can continue to be used seamlessly and without a new rollout. In Appliance Management, LinOTP offers a func- tion for automating the backup process. Please consult the LinOTP Manual (chapter IV, article 13).

b. Software Update: Our developers work continuously to improve our products. Take advantage of patches and new features by updating the LinOTP Software and the Appliance at regular intervals. Appliance Management also provides an automated function for this; all you require is a valid software subscription & support license in order to use it. You can find more information about this in the LinOTP Manual (chapter IV, article 12).

Important URLs and Administrator Roles

The following table provides an overview of the most important URLs as well as the admin roles.

	LinOTP Admin	Root Admin	Appliance Admin
1. Tokenmanagement	ja	nein	nein
2. Appliancemanagement	nein	ja	ja
3. SSH Anmeldung	nein	ja	nein
4. Passwortänderung	nein	alle	nicht von root

HA Mode

Additional, in part varying, configuration steps are necessary for use in HA mode. You will find an introduction for this in the LinOTP Manual (chapter IV, article 10).

4.2.5. Appendix: Practical Tips and Legal Notes

License Conditions

The software of the Virtual Appliance, Hardware Appliance and LinOTP are protected by copyright. You can find the complete license conditions at <u>Install a new license</u>. In addition, they are displayed upon the first use of the Appliance as the first step of the configuration wizard.

We would like to expressly thank the members of the Debian project here.

Support Addresses

In the event of support questions or hardware defects, please contact us. If you would like information regarding our standard support offers, hardware replacement service as well as the additional support options which incur charges, please contact or inform yourself of our support offer at: <u>https://linotp.de/support.html</u>

Alternatively, you can reach us at +49 6151 86086-277 or via email to support@linotp.de

About netgo LinOTP

netgo GmbH - LinOTP is the leading vendor of secure connection technologies centered around vendor independent logon security and identity management.

netgo LinOTP belongs to the netgo group GmbH.

Hausanschrift:

Pallaswiesenstrasse 174a 64293 Darmstadt

Unternehmensdaten:

Vertretungsberechtigte: Sebastian Meyer, Michael Schmiedel Pallaswiesenstrasse 174a 64293 Darmstadt Germany

Office address:

Pallaswiesenstrasse 174a 64293 Darmstadt Germany

Corporate data:

Authorized representatives: Sebastian Meyer, Michael Schmiedel Place of business: Berlin Commercial register : HRB 84278 B District court: Amtsgericht Berlin-Charlottenburg Purchase tax-ID: DE 813 533 741

Contact:

Phone: +49 6151 86086-0 Fax: +49 6151 86086-299 e-mail: <u>sales@linotp.de</u>