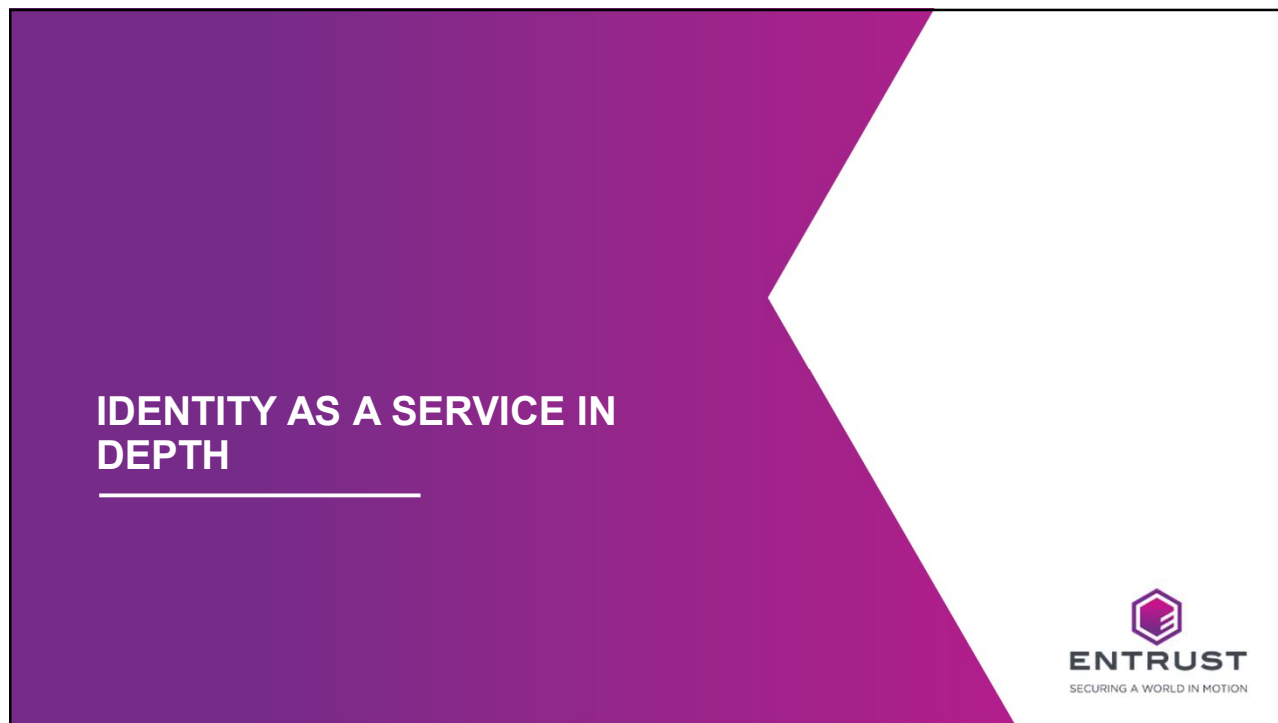
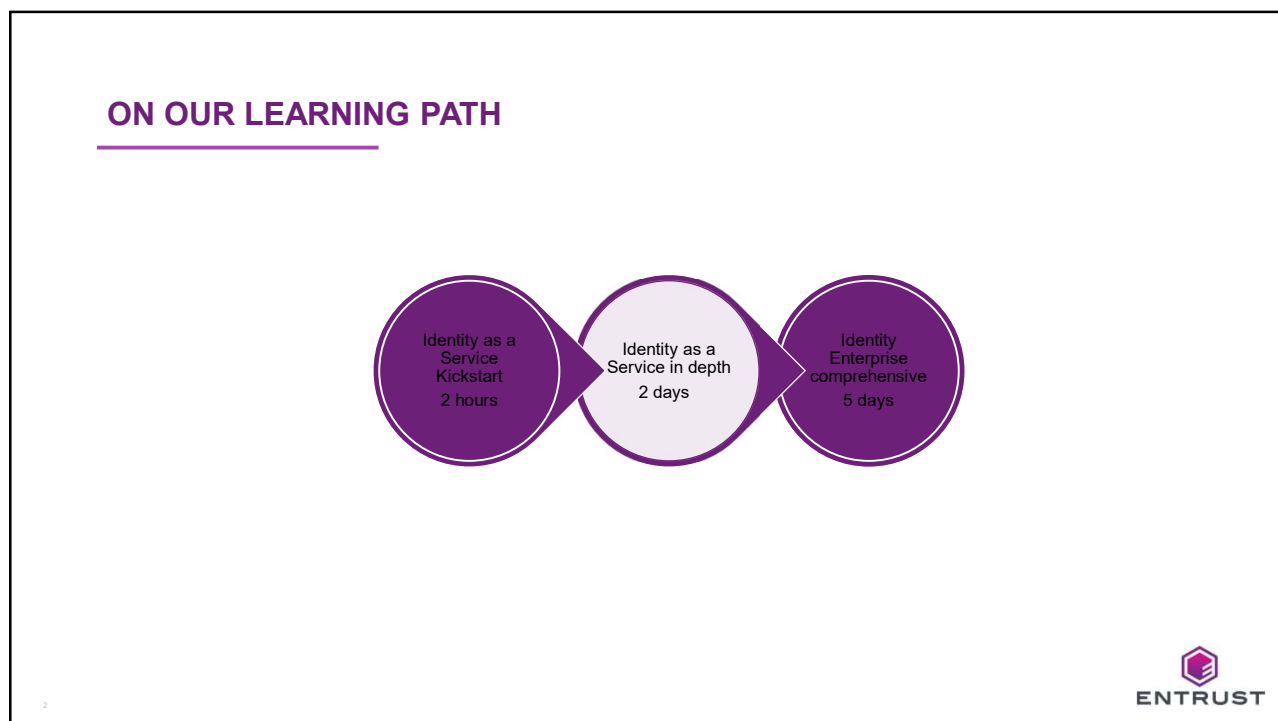




1



2

OUR TOPICS

REFRESHER AND USE CASES



Review architecture
Review steps for
setup/configuration
Our three use cases

ADDING USERS



Importing Users with Bulk
Manually Creating users
User Sync

DEFINING AUTHENTICATORS



Licensing and policy
Assigning to users
Distribution and self service

DEFINING RESOURCES



Resource templates
Resource rules
Using groups



3

OUR LABS

DAY 1 LABS



Create user base with manual,
bulk and synchronization
Create groups, roles.
Setup and issue authentication

DAY 2 LABS



Smart Credentials
Resource Rules
Implementing our Use Cases



4

IDENTITY AS A SERVICE TRIAL

Start Free IDaaS Trial

Start your 60-day free trial today.

First Name*

Last Name*

Company Email*

This email address will be used to send one-time passwords for access to the trial environment

Mobile Phone*

Company Name*

Country*

Compose a URL to host your IDaaS instance:

URL Prefix*

Hosted Region*

URL to host your IDaaS Instance

Terms of use*

☐ By checking this box and clicking 'Request Free Trial' I confirm that I have read and agree to the Identity as a Service Terms of Service (or for Managed Service Providers (MSPs), the Terms of Service (MSP Model)) including those agreements, policies, or additional documents made available therein via hyperlink or by reference.

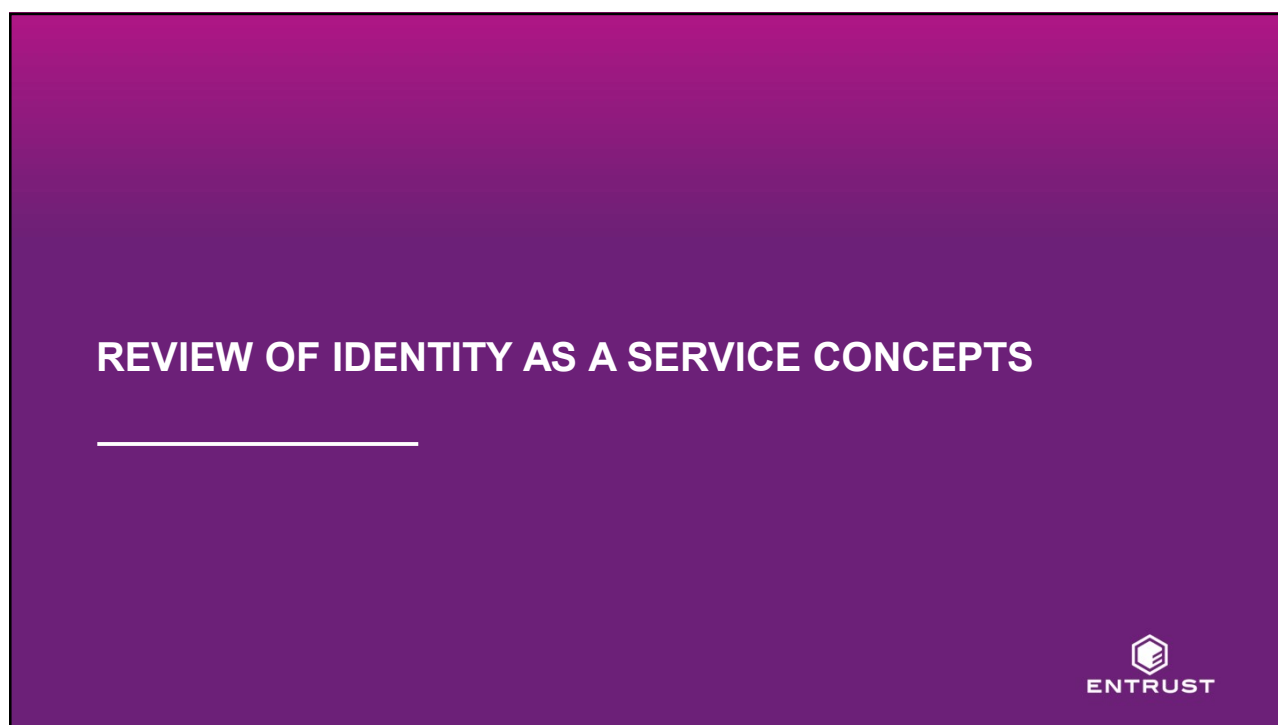
Use your work information here

Use a unique URL i.e. your name and select closest region

Trial Link
(<https://in.entrust.com/IDaaS/>)


ENTRUST

5



6

AUTHENTICATION – PEOPLE PROVING WHO THEY ARE

The diagram illustrates the concept of authentication, where individuals prove their identity. It features a large hexagon on the left with a person icon and a purple ribbon seal. To the right, a cluster of smaller hexagons contains icons representing various authentication methods: two people, a question mark, a grid of dots, a document with a seal, a wireless signal, and a smartphone. The ENTRUST logo is visible in the bottom right corner.

7

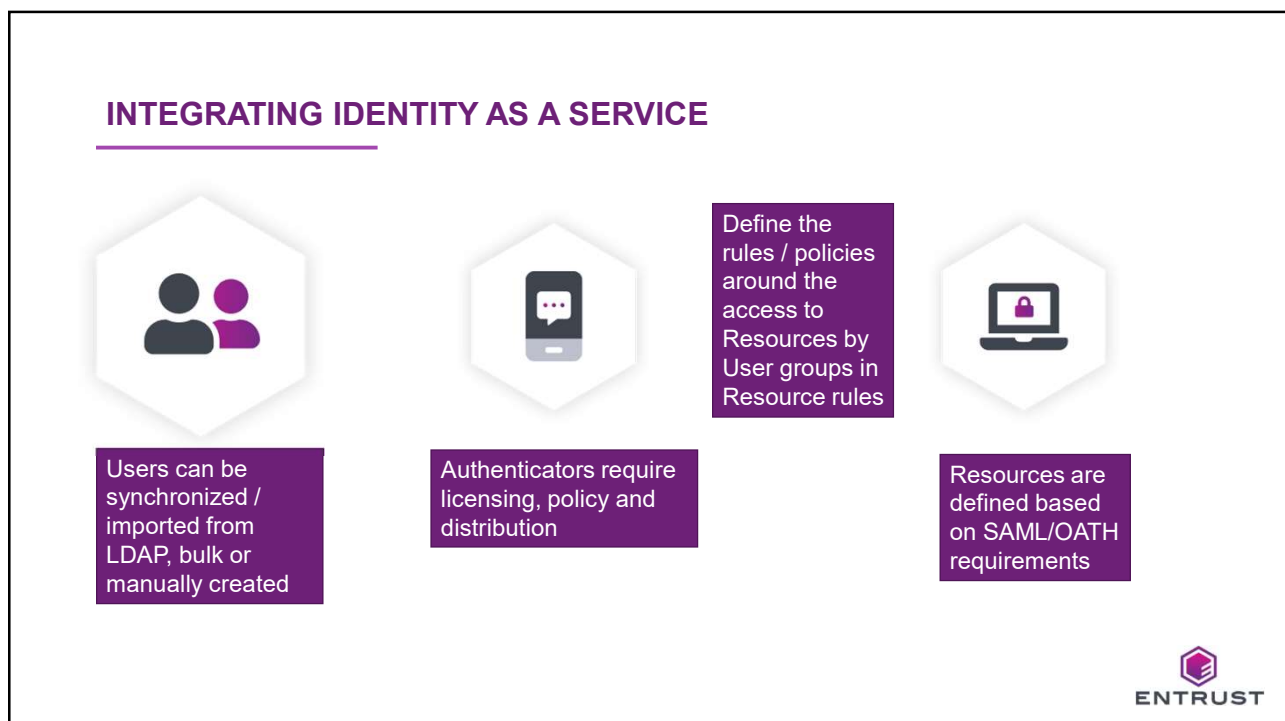
AUTHORIZATION – WHAT ARE THEY ALLOWED TO ACCESS

The diagram illustrates the concept of authorization, where individuals are granted access to specific resources. It features a large hexagon on the left with a person icon and a purple ribbon seal. To the right, a cluster of smaller hexagons contains icons representing various resources: two people, a server rack, a VM monitor, a building, and a laptop with a lock icon. The ENTRUST logo is visible in the bottom right corner.

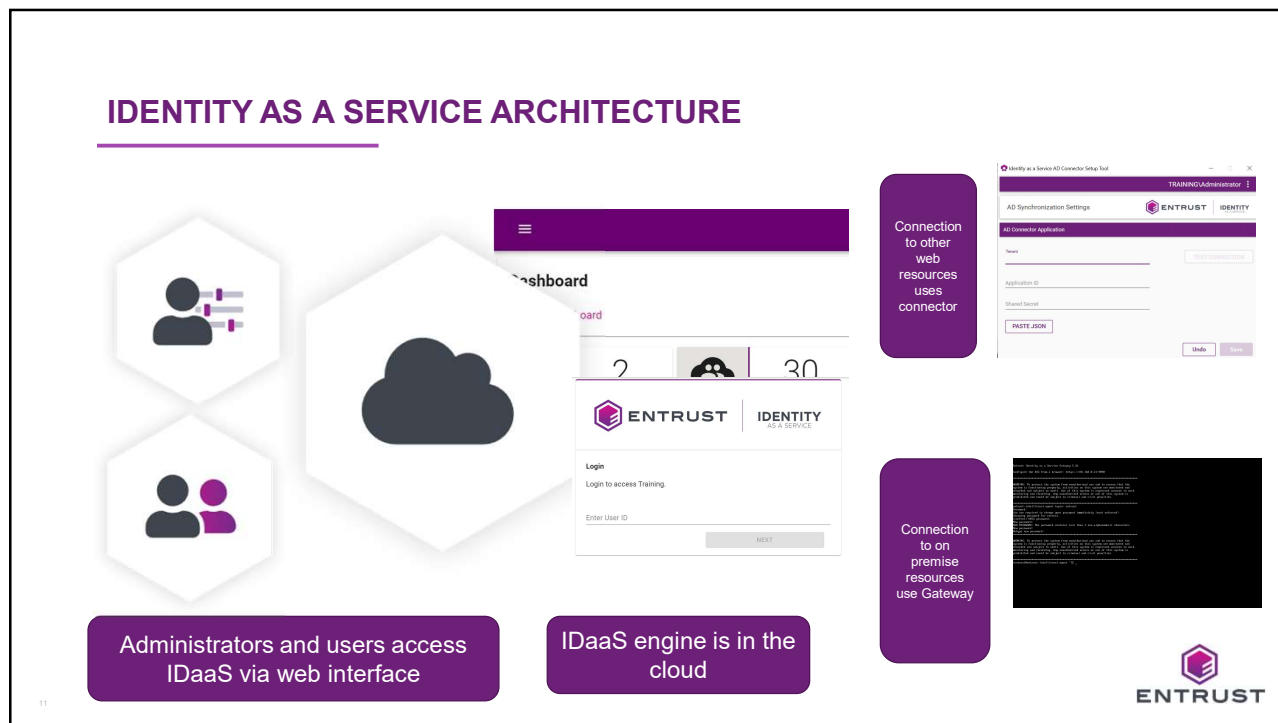
8



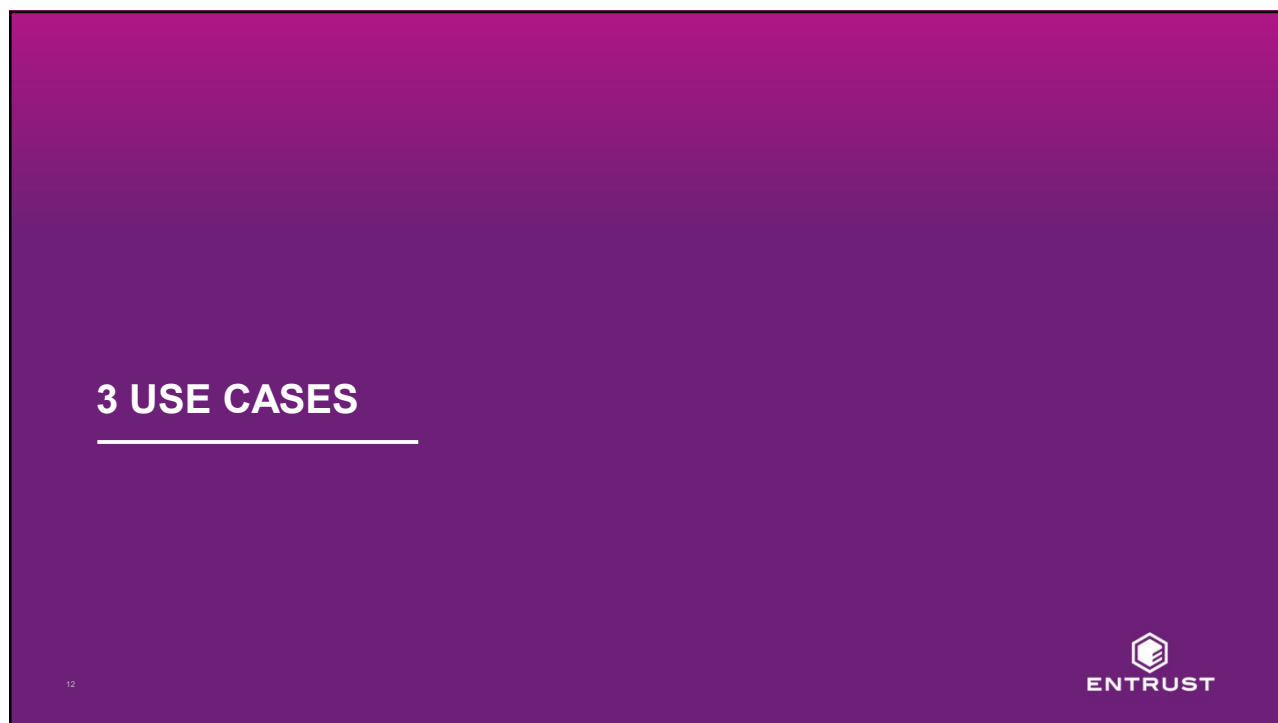
9



10



11



12

USE CASE 1 – THE ADMINISTRATORS

Administrators who are net new



Accessing administration application



Using smart credentials push on their phone



13

USE CASE 2 – OUR INTERNAL EMPLOYEES

Employees from internal LDAP Directory



Accessing Salesforce and VPN and support group can access AWS



Using question and answer or OTP



14

USE CASE 3 – OUR PARTNER BASE

Partners in Cloud Active Directory



Accessing desktop application for account management and future application access



Using a grid card, password and Token depending policy



15

REQUIREMENTS

Users	Groups	Authenticators	Applications	Rules
Alice admin	All	SC push OTP	IDaaS admin role is superuser	
Fred admin	All	SC push OTP	IDaaS admin role is User Administrator	
Bob partner	Partner	Soft token OTP	self management tool	
Joe partner	Partner	Soft token OTP	IDaaS admin role is User Administrator	
Carol Ops	Employees Support	Grid card	AWS	
Harold employee	Employees	Q/A	Salesforce, windows login	



16

LETS GET STARTED

17



17

LETS GET LOGGED IN

- › Login to your trial (lab) environment

A login form for Entrust Identity AS A Service. The form has a white background with a purple border. At the top, it features the Entrust logo and the text 'IDENTITY AS A SERVICE'. Below this, the word 'Login' is displayed, followed by the instruction 'Login to access Training.'. There is a text input field labeled 'Enter User ID' and a 'NEXT' button at the bottom right.

18

DEFINING YOUR USER POPULATION

19



19

MANAGING USERS IN IDENTITY AS A SERVICE

Local - Manually create as required

Local - Import via bulk operations

External or Synchronize with external source

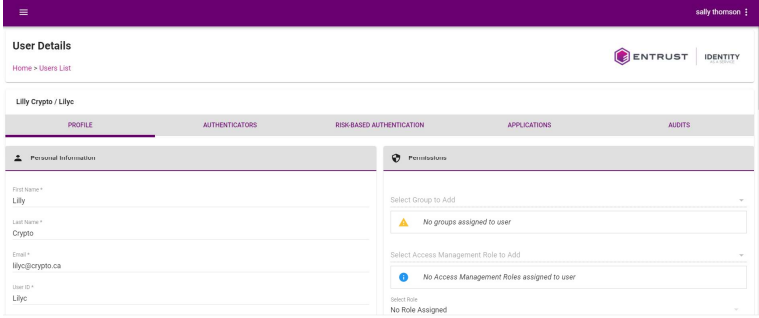


20



THE USER PROFILE

- › Users should be members of groups
- › They should have contact information required by authenticators



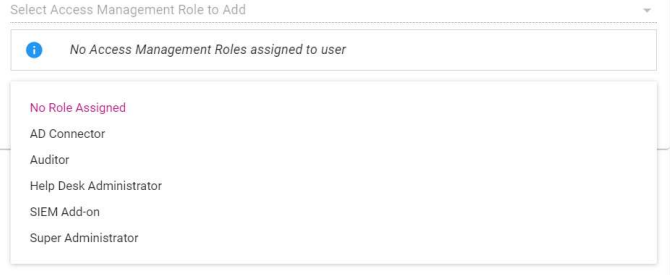


21



ROLES... ARE THEY AN ADMINISTRATOR?

- › Users DO NOT have a role
- › Roles manage administrative rights





22



SOURCE – ARE WE SYNCHRONIZING THIS ACCOUNT

- › Source can be
 - Local (no sync)
 - External
 - Directory

Last Name	Email	Source	Last Authentication Time
Crypto	ssthomsonis@gmail.com	Local	Never
thomson	sally.thomson@entrust.com	Local	31 Oct 2022 16:28:05


ENTRUST

23



ALIAS, ATTRIBUTES AND OTP PREFERENCES

- › Attributes and alias may be required for some resources
- › Users are assigned attributes based on a set of default attributes plus any custom attributes you define
- › Attributes can be synchronized with your Active Directory, including the password, which can be used as the first factor authenticator
- › OTP delivery preferences can be personalized

★ Required Attributes

No required user attributes are defined

👤 Aliases

ADD

No Aliases added

☆ Optional Attributes

ADD

No optional user attributes are defined

⚙️ OTP Delivery Preferences

Preferred OTP Delivery
System Default (SMS)

Preferred OTP Email Contact
System Default (Email)

Preferred OTP SMS Contact


ENTRUST

24



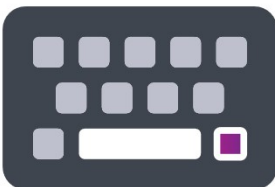
GROUPS

- › Groups are necessary for assigning applications and authenticators
- › Users can be members of different groups
- › Groups are assigned at creation time or assigned after using bulk operations
- › Creating and managing groups requires the Superuser role
- › Groups can be used to identify AD synchronized users and manually added users





25



LAB 1 CREATE ADMINISTRATORS

- › Create new groups for our use cases
- › Create any new Administrative roles required
- › Create one of the Administrative users required for our use cases
 - (we will add the rest using bulk operations in the next exercise)



26

BULK ADDING USERS



27

ACCESSING BULK OPERATIONS



- My Profile
- My Activity
- Dashboard
- Members
 - Users
 - Groups
 - Roles
- Attributes
- Resources
- Configuration
- Policies
- Customization
- Bulk Operations**
- Reports

Bulk Operations

Home > Bulk Operations List

Bulk Operations

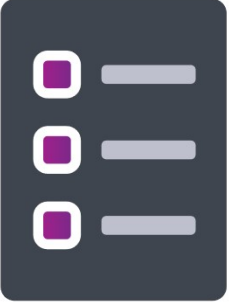


☐	State	Name	File Name
--------------------------	-------	------	-----------

Rows per page: 10 Total: 0



28



USING BULK OPERATIONS PANEL

» Different operations will require different input file contents

1 Operation Setup
2 File to upload
3 Start/Stop

Actions

Action for bulk operation ▾

Maximum Number of Retries
Five (5)

Name
Name of operation (Required)

Description
Describe operation

Operations

The operation type for selected Action ▾

1 Operation Setup

Import
Assign
Reset
Delete
Set

Import operation ▾

Maximum Number of Retries
Five (5)

Name
Name of operation (Required)

Description
Describe operation



ENTRUST

29

Table: User system attributes

Attribute	Header Value	Required
+ User ID	userId	Yes
+ First Name	firstName	Yes*
+ Last Name	lastName	Yes*
+ Email	email	Yes*
+ Mobile	mobile	Yes*
+ Phone	phone	No*
+ User Principal Name	userPrincipalName	No*
+ State	state	No
+ Locked	locked	No
+ Group	group	No

INPUT FILE FORMAT

» Sample files can be viewed in Bulk operations panel

» Download or copy contents to create file for use in bulk operation

1 Operation Setup
2 File to upload
3 Start/Stop

Actions

Set ▾

File Delimiter
☐ Pipe (|)
☒ Comma (,)

Maximum Number of Retries
Five (5)

Name
Name of operation (Required)

Description
Describe operation

Operations

Users ▾

Operation Type
Update or Create Users ▾

Sample Bulk File

A bulk CSV file for bulk creating or updating users.
 # Headers are supported in different formats. For more details, see <https://>
 # The following is a sample CSV file format for import or set bulk users op
 userId,firstName,lastName,email,mobile,state,userPrincipalName
 jdoe,jane,doe,jdoe@acmecorp.com,+13234234234,ACTIVE,jdoe@acmecorp.com

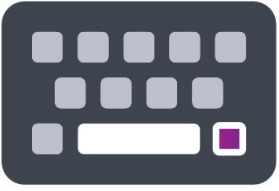
COPY TO CLIPBOARD

DOWNLOAD



ENTRUST

30



LAB 2 CREATE ADMINISTRATORS

- › Import the remainder of your administrators using a bulk file,
- › Ensure they are assigned appropriate roles, groups and authenticators



31

31

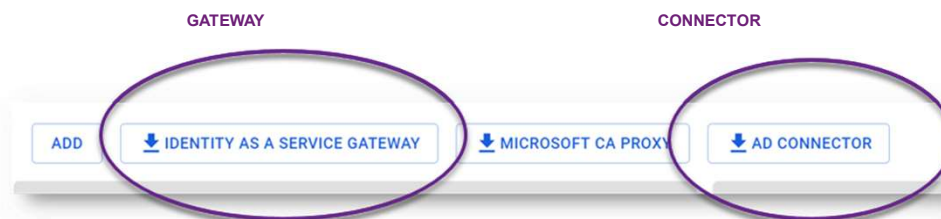
SYNCHRONIZING USERS WITH OTHER DATA SOURCES



32

32

GATEWAY OR CONNECTOR?



Configure an **internal** Gateway to sync users from an on-premise Directory.
Synchronization can be managed and on demand.

Configure an AD Connector directory to sync users from a **cloud** Directory using a lightweight AD connector native Windows application.

Changes made to your Active Directory are automatically synced with Identity as a Service. You do not need to trigger synchronization.



33

DEFINING THE DIRECTORY

Identify a unique name (points to Directory Name)

name used to administer your directory in LDAP format and Password must have read-only access to AD (points to Username)

Hostname and Port (points to Hostname and Port fields)

enter the full DN used by your company directory. For example, DC=AnyCorp, DC=biz (points to Root Domain Naming Context)

If you enable SSL, prompted for certificate (points to Use SSL checkbox)

Identify the search base (starting point) in the Directory to pull users from (points to SearchBases field)

If you define a group it will limit the users that are imported (points to Group Filters field)

Form Fields:

- Directory Name*: Training Directory
- Username*: cn=manager
- Password: [password field]
- Hostname*: Instructor.acme.com
- Port*: 389
- Root Domain Naming Context*: ou=network,dc=acme,dc=com
- Use SSL: ☐
- SearchBases: ou=ca0,ou=network
- Group Filters: No Group



34

ATTRIBUTE MAPPING

Identify the attribute mapping

System User Attributes

First Name*
givenName

Phone*
telephoneNumber

Email*
mail

Mobile*
mobile

Last Name*
sn

State*
userAccountControl

User ID*
sAMAccountName

Custom User Attributes

Location

Map any custom attributes

Synchronization

Synchronization Agent
DirectoryGateway

Page Size*
100

Crawl Frequency*
1 hr

User Object Class*
USER

Group Synchronization*
All Groups

Group Name Attribute*
sAMAccountName

Identify the synchronization User object class? sAMAccountName?

CANCEL SAVE

Some Common required attributes

Salesforce	



SYNCHRONIZING ON PREMISE ACTIVE DIRECTORY USING A GATEWAY





WHAT IS A GATEWAY

- › A gateway is an application you install within a Virtual Machine in your organization that can talk to your cloud IDaaS instance.
- › It provides a proxy between your organizational applications and the Identity as a Service authentication engine in the cloud.
- › Each Gateway can have multiple instances and to ensure high availability, it is recommended that you add at least two instances to your gateway.



37



HOW WILL WE USE THE GATEWAY

- › In our use cases our internal Active Directory will use the Directory Synchronization element of the gateway to establish and synchronize users within their AD with IDaaS.
- › This will be a synchronization based on a specific group in AD
- › These users will then login to IDaaS for the first time and activate any authenticators we have assigned them
- › They will be using their familiar AD password to access IDaaS



38

THE COMPONENTS OF A GATEWAY

Syncs Active Directory users and groups with Identity as a Service.

Gateway Instance Details

Name: on-prem-ad-internalgateway-2022-12-08:15:14:48:218
Version: 5.26
State: Active
SSL Hostname: internalgateway

Agents

Directory Sync	Last Heartbeat: 08 Dec 2022 10:42:29
IdentityGuard	Last Heartbeat: 08 Dec 2022 10:42:31
Management	Last Heartbeat: 08 Dec 2022 10:42:29
Password / Microsoft CA Gateway	Last Heartbeat: 08 Dec 2022 10:42:31 Last Heartbeat from CA Gateway: 08 Dec 2022 10:42:32
RADIUS	Last Heartbeat: 08 Dec 2022 10:42:31
SIEM	Last Heartbeat: 08 Dec 2022 10:42:24

Allows existing Entrust Identity Enterprise integrations and other clients to use Identity as a Service in place of Entrust Identity Enterprise

Performs Active Directory password authentication, password reset, and password change requests

Performs RADIUS authentication for services such as VPN. Supporting the following protocols PAP, CHAP, MSCHAPv1, MSCHAPv2 for OTP and Token 2FA



39

ESTABLISHING A GATEWAY

SETUP GATEWAY IN IDAAS



Define the Gateway as a resource in Identity as a Service

Its best to do 2 instances for redundancy

DOWNLOAD/ INSTALL GATEWAY IN YOUR ENVIRONMENT



Download the Gateway VM and install in your environment

You will use the code generated in step 1 to connect IDaaS to Gateway

SETUP RESOURCES USING GATEWAY (DIRECTORY)



Now define the resource (Directory) and point it to the Gateway



40

DEFINING THE GATEWAY IN IDAAS

RESOURCES GATEWAYS

ADD A NEW GATEWAY

NAME THE GATEWAY

COPY THE GATEWAY CODE

Define a Gateway in Resources Gateways.

Click the plus and add a Gateway

Provide a Meaningful name for the Gateway.

This will be required when the Gateway is installed in your environment. As part of the Gateway setup, you will be asked for this code



41

YOUR GATEWAY IS READY TO BE ACTIVATED

Gateways

[Home](#) > Gateways List

+
IDENTITY AS A SERVICE GATEWAY
MICROSOFT CA PROXY
AD CONNECTOR

My Company Gateway 1
 My Company Gateway 1-unregistered-2022-11-01:13:00:42:05

ⓘ For high availability it is strongly recommended that you add at least one more Gateway Instance.

+ ADD INSTANCE



42

NEXT DOWNLOAD AND INSTALL THE GATEWAY

DOWNLOAD THE VM

Identity as a Service Gateway Download URL

Your Download URL is valid until 02 Nov 2022 09:25:48

[VMWARE VSPHERE](#) [MICROSOFT HYPER-V](#)

VMware vSphere: Download the vSphere image to deploy the Gateway to a VMware platform.

Microsoft Hyper-V: Download the Hyper-V image to deploy the Gateway to Microsoft Hyper-V.

For more help on deploying the Identity as a Service Gateway refer to the [documentation](#).

idaas-esg-5.26.ova
0.2/2.6 GB, 2 mins left

Choose the environment you will be using and download the gateway

OPEN THE OVA WITH YOUR VM



Open

POWER ON THE VM



The CentOS Linux will start



44

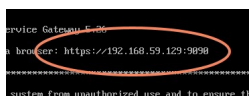
NEXT DOWNLOAD AND INSTALL THE GATEWAY

LOGIN WILL APPEAR



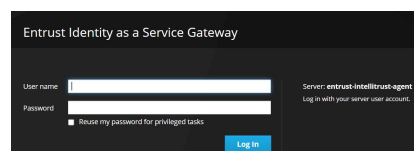
You can login here .

YOU CAN NOW ALSO USE THE WEB INTERFACE



Browse to the address presented to use the web interface to install the Gateway

LOGIN TO THE GATEWAY



Login with entrust as both username and password, then change it



45

NEXT DOWNLOAD AND INSTALL THE GATEWAY

CHANGE THE PASSWORD



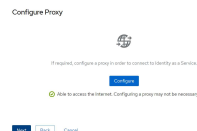
Must have special character,
WRITE IT DOWN

GET STARTED AND SETUP THE GATEWAY



Click the Get started button and
click Next through most of the
screens

THE CONNECTION SHOULD BE OK



On the Configure Proxy screen
you should not have to configure
it as the Connection to the Internet
should be connected.



46

CONNECT GATEWAY TO IDAAS

Paste in the Registration Code and click
Register

Registration Parameters

Registration Code

Paste the registration code from the Identity as a Service portal.

SSL Certificate
Hostname

entrust-intellitrust-agent

A self-signed certificate will be created for SSL communication to the IdentityGuard agent. Please enter the fully qualified domain name of this host that should be used in the SSL certificate.

Register

Next Back Cancel

This came from the
Gateway setup you can
generate the code
again



47

RETURNING TO IDAAS WE CAN NOW VIEW THE GATEWAY

Gateways
Home > Gateways List

+ IDENTITY AS A SERVICE GATEWAY MICROSOFT CA PROXY AD CONNECTOR

on prem ad	on prem ad-internalgateway-2022-12-08:15:14:48:218 5.2.0	
	on prem ad-unregistered-2022-12-15:15:21:22:83 5.2.0	

+ ADD INSTANCE

Legend

Gateway Status

Add instance for HA

- Export SSL Certificate
- Generate CSR
- Re-Activate
- Rename
- Disable
- Advanced Settings
- Delete

ENTRUST

48

DEFINING THE DIRECTORY TO SYNCHRONIZE

Directories
Home > Directories List

Directories

- Active Directory (on-premise)
- LDAP Directory (on-premise)
- Azure Directory (Preview)
- AD Connector Directory

Host Name

No Rows To Show

Rows per page: 20 Total: 0

Legend

First select the type of Directory to define

ENTRUST

49

DEFINING THE DIRECTORY

Connection Settings

Directory Name *

Username *

Password *

Directory Servers ? ADD

No Directory Servers defined.
At least 1 Directory Server must be added.

Directory Server

Hostname *
This field is required.

Port *
389

☐ Use SSL

CANCEL ADD

ENTRUST

50

SEARCHBASES AND GROUPS

SearchBases & Group Filters

Root Domain Naming Context *

SearchBases ? ADD

No SearchBases defined. The Root DN will be searched.

Group Filters ADD

No Group Filters defined.

Can synchronize with specific groups or SB

ENTRUST

51

ATTRIBUTE MAPPING IS PRE DEFINED

★ Attribute Mappings

System User Attributes

Email *
mail

First Name *
givenName

Last Name *
sn

User ID *
sAMAccountName

Mobile
mobile

State
userAccountControl

Phone
telephoneNumber

User Principal Name
userPrincipalName

Custom User Attributes

salesforceid



52

CHOOSE THE GATEWAY

↻ Synchronization

Synchronization Agent

on prem ad
v5.26



53

VIEWING DIRECTORY

The screenshot displays the Entrust Identity Cloud user interface. On the left is a navigation sidebar with options: My Profile, My Activity, Dashboard, Members, Resources, Applications, Authorization, Resource Rules, Directories (highlighted), Gateways, and Tokens. The main content area is titled 'Directories' and includes a breadcrumb 'Home > Directories List'. Below the title is a table of configured directories.

Conn...	Name ↑	Host Name	Type	Sync Status	Last Update	Actions
	AWS Directory	DC01.training.entrust.com	AD Connector			[Icon]
	AWS MSA Proxy Dir	dc01.training.entrust.com	On-premise	Waiting for sync to start	13 Dec 2022 14:24:45	[Icon] [Icon] [Icon]
✓	Azure AD TrainingEDC	trainingedc	Azure	Sync Complete	21 Dec 2022 08:00:01	[Icon] [Icon] [Icon]
	TaffactiveDir	192.168.121.128	On-premise	Sync Complete	13 Dec 2022 14:15:12	[Icon] [Icon] [Icon]

The Entrust logo is visible in the bottom right corner of the interface.

54

USING AD CONNECTOR WITH A CLOUD DIRECTORY

This slide features a solid purple background with the title 'USING AD CONNECTOR WITH A CLOUD DIRECTORY' in white text. The Entrust logo is positioned in the bottom right corner.

55

CONNECTOR SETUP

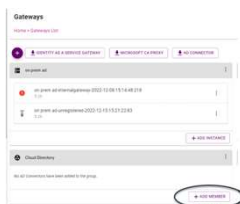
Defining the Connector and installing is similar to Gateway but using Json file instead of registration code

DEFINE THE AD CONNECTOR IN IDAAS



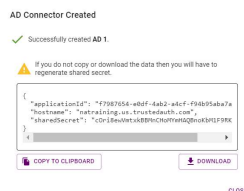
In Gateways, click the + then add a new AD Connector Group

ADD MEMBER



Once the group is created, add a member

COLLECT JSON FILE



The Json file will be available best to download it

DOWNLOAD CONNECTOR



Now download the Connector software and copy to the AWS/Cloud system



56

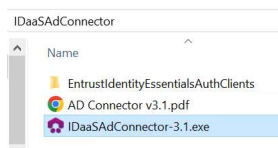
INSTALL CONNECTOR IN CLOUD

COPY THE SOFTWARE TO THE CLOUD SYSTEM



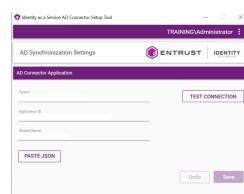
Copy both the json and the connector software

INSTALL BY RUNNING .EXE



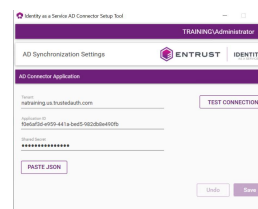
The IDaaSAdConnector will have an executable to run to install

WHEN ASKED PASTE OR UPLOAD THE JSON FILE



The Json file information will complete the page

TEST THE CONNECTION



Click test connection and this should now verify your cloud connector can reach IDaaS



57

DEFINE THE DIRECTORY

» Now define the directory and point to the new connector as the way to connect to the Directory

Directories

- Active Directory (on-premise)
- LDAP Directory (on-premise)
- Azure Directory (Preview)
- AD Connector Directory**

Add Directory

Home > Directories List

General Settings

Directory Name *

AD Connector Group *

in the cloud ad

Choose the connector group we just defined

ENTRUST IDENTITY

58

DEFINE THE CONNECTION SETTINGS AND FILTERS

Connection Settings

Account and Directory Servers ?

Username

Password

☐ Use SSL ?

Directory Servers ?

ADD

Directory authentication

SearchBases & Group Filters

Domain Naming Context ?

Root Domain Naming Context

Group Filters

ADD

No Group Filters defined.

Root DN of Dir and any group filters

ENTRUST

59

DEFINE ATTRIBUTE MAPPING AND SYNCHRONIZATION

Attributes are pre mapped but can add new or edit

The screenshot displays the Entrust user management interface. The top navigation bar is purple with a menu icon and the user name 'sally thomson'. The main content area is divided into two panels. The left panel, titled 'Attribute Mappings', shows 'System User Attributes' with a list of attributes: Email (mail), First Name (givenName), Last Name (sn), User ID (sAMAccountName), Mobile (mobile), State (userAccountControl), and Phone (telephoneNumber). The right panel, titled 'Synchronization', shows settings for 'User Object Class' (user), 'Group Synchronization' (All Groups), 'Group Name Attribute' (sAMAccountName), and 'User De-synchronization Policy' (User becomes a local Identity as a Service user and is disabl...). A purple callout bubble points to the 'All Groups' dropdown in the Synchronization panel.

Define synchronization settings



60

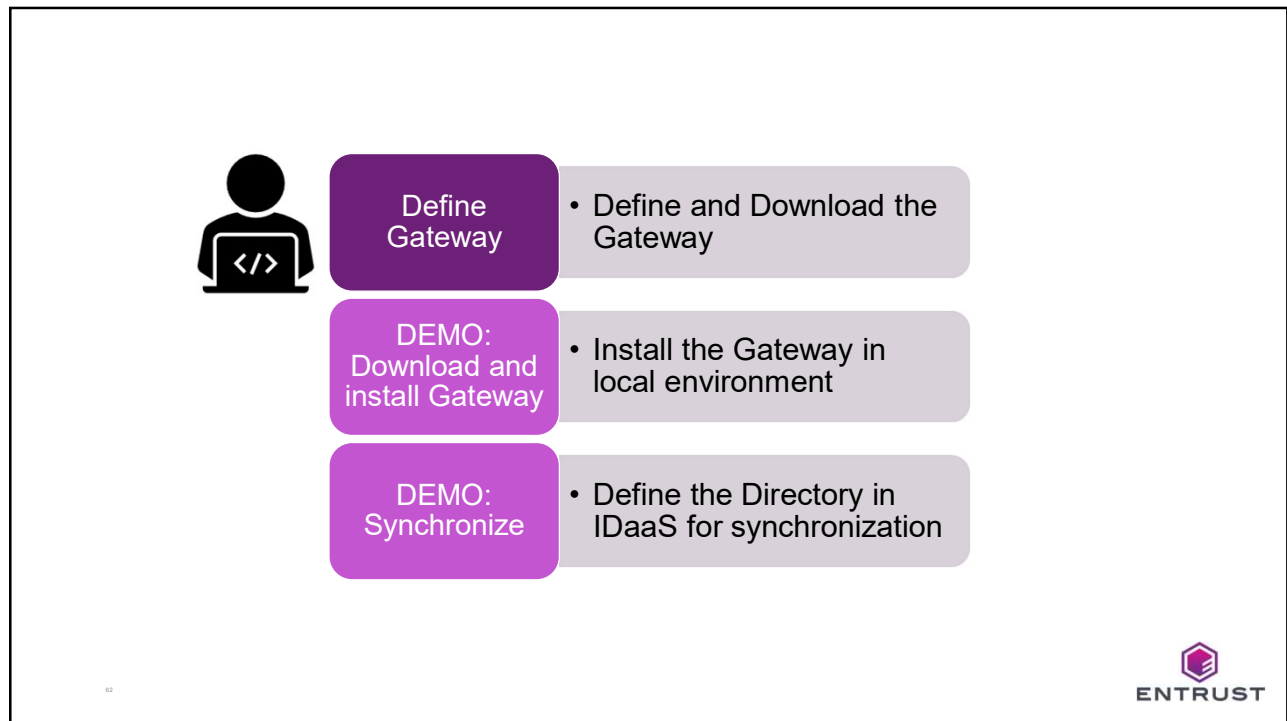
ENSURE ADDITIONAL ATTRIBUTES FOR APPLICATIONS ARE SET

The screenshot displays the Entrust user management interface. The top navigation bar is purple with a menu icon and the user name 'sally thomson'. The main content area is divided into two panels. The left panel, titled 'User Principal Name', shows a text input field with the value 'userPrincipalName'. The right panel, titled 'Custom User Attributes', shows a text input field with the value 'salesforceid'. A purple callout bubble points to the 'salesforceid' input field.

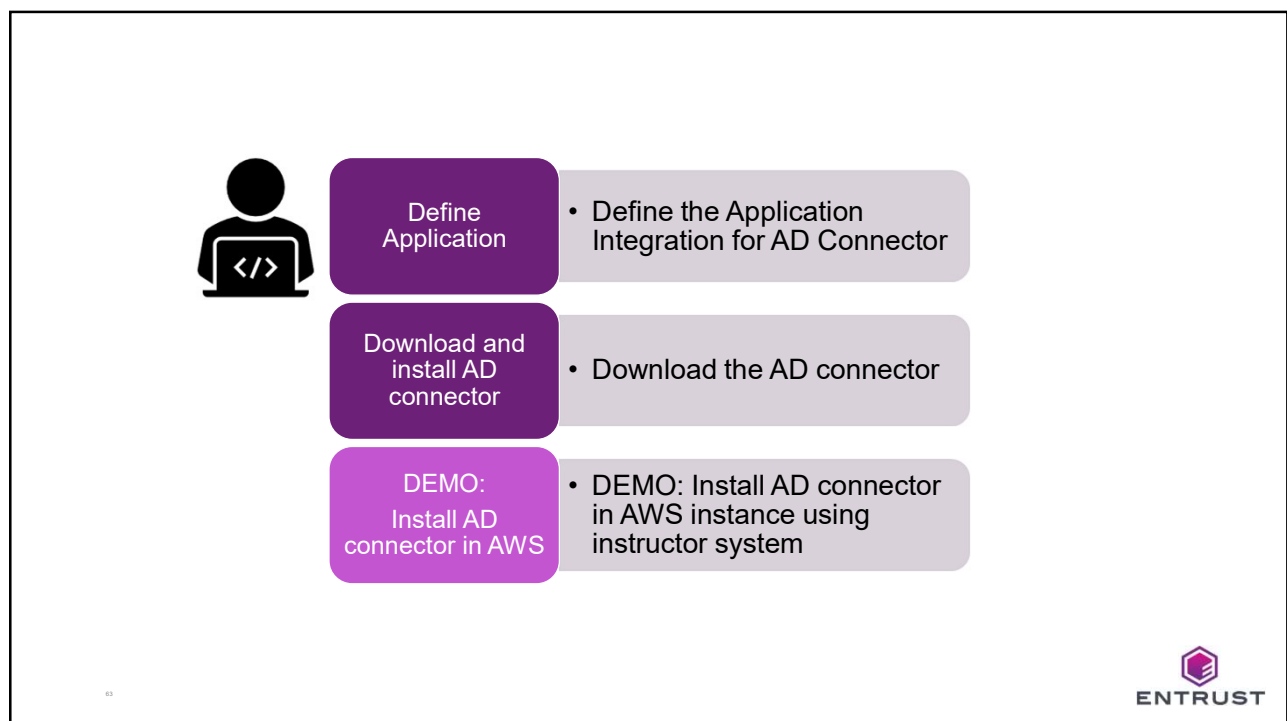
In anticipation of Salesforce SSO



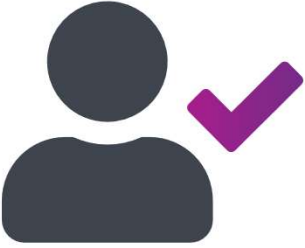
61



62



63



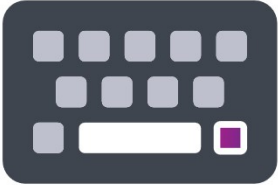
BREAK AND POLL

Please complete the poll on screen we will return in 20 minutes

64



64



LAB SETUP SYNCHRONIZATION

- › Using your lab, setup a gateway.
Instructor will then demonstrate the connection to a VM
- › Setting up a cloud data synchronization using connector
Instructor will demonstrate and provide you with details to connect to cloud AD

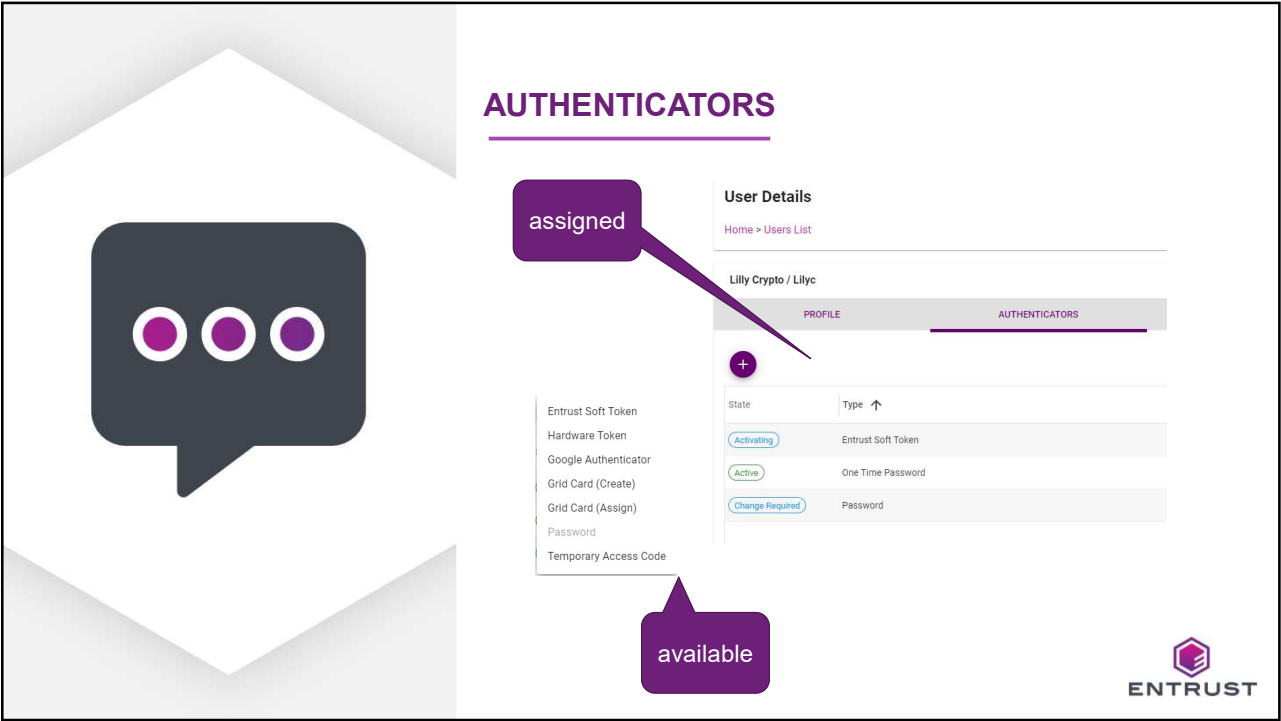
65



65



66



67



AUTHENTICATOR CONSIDERATIONS

Consider the following when assigning authenticators to users:

- A user must have at least one authenticator assigned but may have more than one.
- A user can choose to receive their OTP by voice, email, or SMS if they have a phone number, email address, or mobile device registered to their account.
- Assigned tokens have a token state (either Active or Inactive). Only tokens in an Active state can be used for authentication.
- The resource rules associated with an application determine which authenticators can be used to log in to an application.
- Users created in Identity as a Service through Active Directory (AD) sync are automatically assigned an authenticator.



68



AUTHENTICATORS WE WILL SETUP

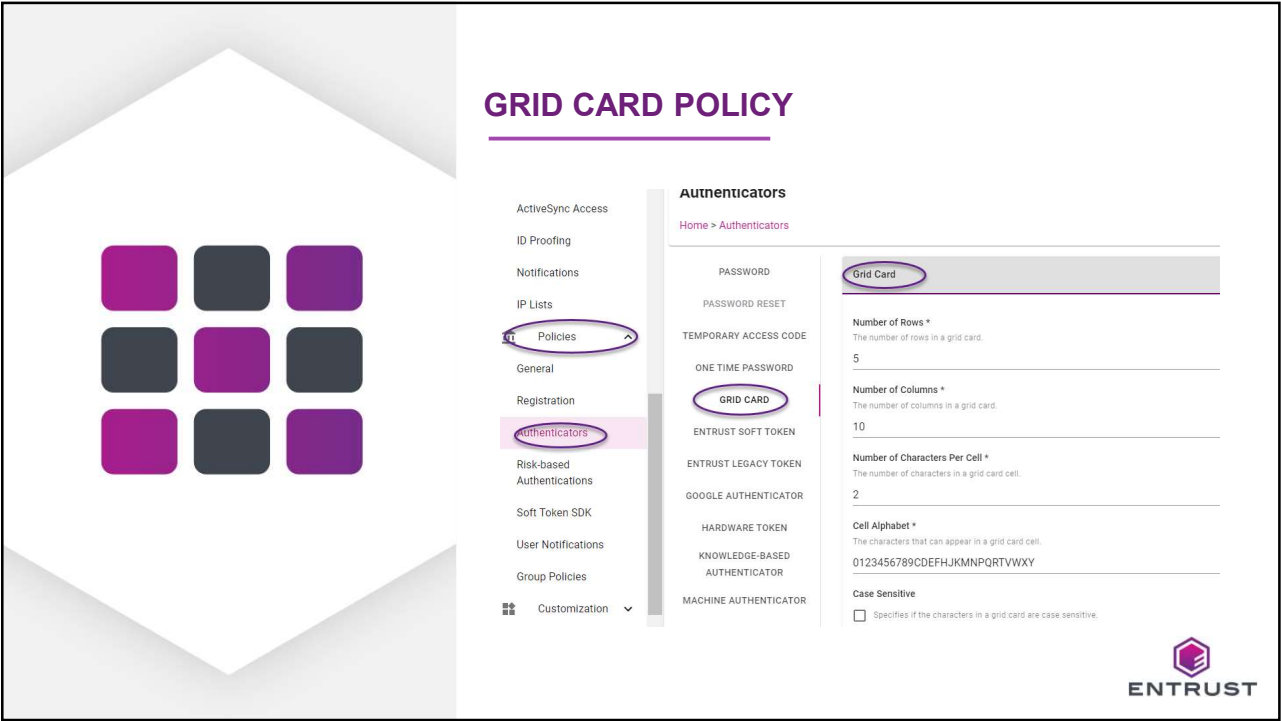
- Grid cards
- Tokens
- Password
- OTP
- Question and answer
- Smart credentials



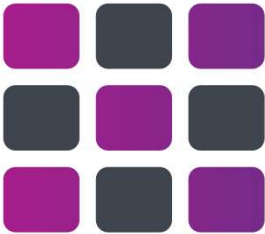
69



70



71



GENERATING GRID CARDS

Resources

- Applications
- Authorization
- Resource Rules
- Directories
- Gateways
- Tokens
- Grid Cards

Grid Cards

[Home > Grid Cards](#)

Grids

Generate

Import

Unassigned Grid Card Generation

Total Number of Grid Cards to Create *

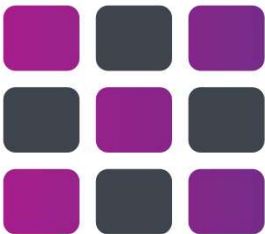
This field is required.

CANCEL SUBMIT

Grids

Serial #	Date Added	Date Last Used	Actions
1	01 Nov 2022 10:05:45	Never	
2	01 Nov 2022 10:05:45	Never	
3	01 Nov 2022 10:05:45	Never	
4	01 Nov 2022 10:05:45	Never	

72



ASSIGNING GRID CARDS

From grid listing

Actions

-
-
-
-

Assign Grid Card

Select user to assign Grid Card 1

User ID *

This field is required.

CANCEL ASSIGN

Via Bulk

Operation Setup

Actions: Assign

Operations: Entrust Soft Tokens

Maximum Number of Retries: Five (5)

Name: Name of operation (Required)

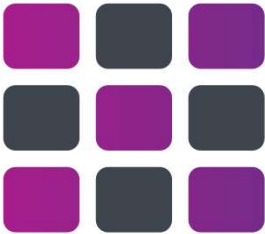
Description: Describe operation



ENTRUST

73

36



ASSIGNING GRID CARDS

» In the user account

Assign Grid Card



To assign a Grid Card to this profile, enter the card serial number.

Serial Number *

This field is required.

CANCEL
ASSIGN



ENTRUST

74



SELF SERVICE GRID CARDS

» Users can be given the option to add a grid in their account

Registration

Home > Registration

Authenticator Provisioning

Automatic Authenticator Provisioning

Configure the authenticators to be automatically provisioned to user.

Password

☒ Automatically create a password for new users.

Tokens

☒ The type of token automatically created when the user is created.

Entrust Soft Token

User Portal

Available Authenticators

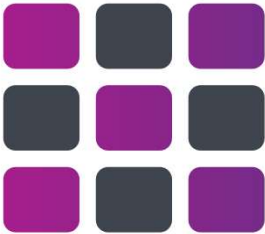
Select the authenticators that users can add to their account.

- ☒ Entrust Soft Token
- ☒ FIDO2
- ☒ Google Authenticator
- ☒ **Grid Card**
- ☒ Hardware Token
- ☒ Knowledge-based Authenticator
- ☒ Machine Authenticator
- ☒ Password



ENTRUST

75



CREATE OR ASSIGN?

» In their profile they can assign (register) or create one

Lilly Crypto / Lilyc

PROFILE

AUTHENTICATORS

Entrust Soft Token

Hardware Token

Google Authenticator

Grid Card (Create)

Grid Card (Assign)

Password

Temporary Access Code

↑

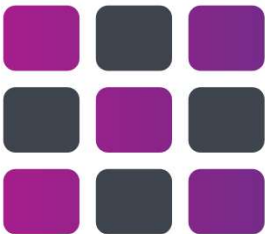
t Soft Token

me Password

ord



76



CREATE OR ASSIGN?

» In their profile they can assign (register) or create one

Lilly Crypto / Lilyc

PROFILE

AUTHENTICATORS

Entrust Soft Token

Hardware Token

Google Authenticator

Grid Card (Create)

Grid Card (Assign)

Password

Temporary Access Code

↑

t Soft Token

me Password

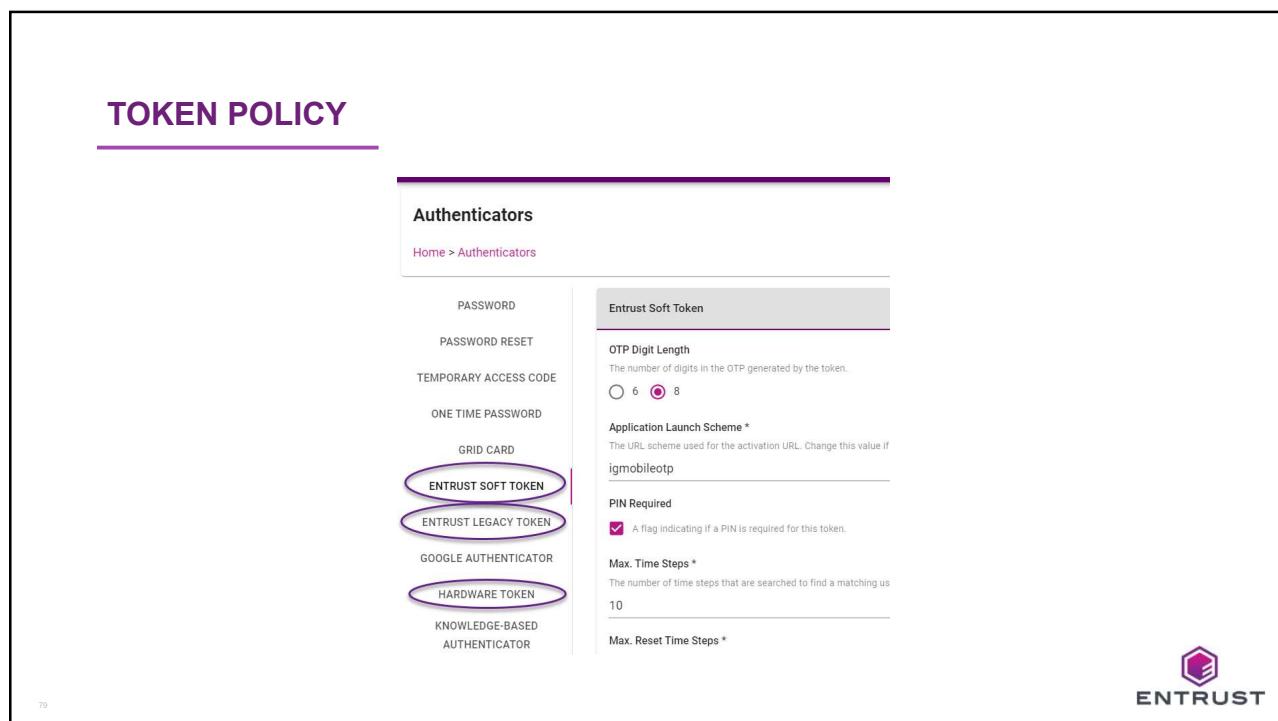
ord



77



78



79

LICENSING TOKENS

Add Bulk Operation

[Home](#) > [Bulk Operations List](#)

1 Operation Setup 2 File to upload 3 Start/Stop

Operation: **Import** System: **Hardware Tokens**

Password: **used the password**

Specify groups to be assigned to imported tokens

Select Group to add: **No groups assigned**

Maximum Number of Retries: **Five (5)**

Name: **Name of operation (Required)**

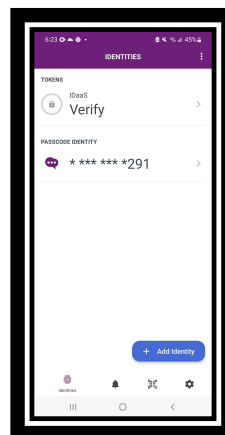
Description: **Describe operation**



80

SOFT TOKENS AUTHENTICATING WITH YOUR PHONE

- › Various apps available for synchronizing numbers for authentication
- › Licensed by users



81



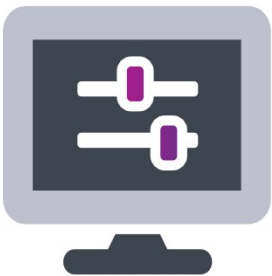
HARD TOKENS FOR AUTHENTICATION

- › Typically, a small hardware element that has changing number patterns
- › Licensed by device





82



MACHINE AUTHENTICATION AND FINGERPRINTING

- › Use your phone or laptop as a factor of authentication

Device Fingerprint Attributes

Home > Device Fingerprint Attributes

IDENTITY

Web Browsers

Device Fingerprint Attributes

The device fingerprint attributes are used to validate a machine authentication when Device Fingerprint Required is selected. For more help please refer to the [Administration Guide](#).

Attribute Name	Enabled	Type
application	Yes	CONSTANT
urlURL	Yes	LIST
plugins	Yes	LIST
localStorage	Yes	CONSTANT
indexedDB	Yes	CONSTANT

Machine Authentication

Enable Machine Registration

☒ Enabling this feature allows users to register a Machine Authentication.

Authentication Required for Machine Registration

Machine Registration requires authentication:

Entrust / Google / Fingerprint Token

Maximum Number of Machine Devices *

Set the maximum number of devices a user can have registered.

10

Machine Authentication Security Level

☒ Machine Fingerprint Required

☐ Securement Fingerprint Required

☐ Device Fingerprint Required

(If enabled, one must be selected.)

Machine Risk Level *

Set the risk level at which machine authentication fails.

0

Machine Secret Lifetime in Hours *

Set the lifetime in hours of a machine secret.

0

Count Failed Machine Authentication as Login Failure

☐ If flag is set, whether a failed machine authentication increments the user's failed authentication (total) count.



83

POLICIES FOR AUTHENTICATORS



84

AUTHENTICATOR POLICES

-  Policies ^
- General
- Registration
- Authenticators
- Risk-based Authentications
- Soft Token SDK
- User Notifications
- Group Policies



85

GENERAL POLICY

General

Lockout Count *
The number of failed authentication attempts before the user is locked.

Lockout Mode *
The mode of lockout. It can be set to 'Hard' or 'Soft'.

Lockout Duration *
The duration of the lockout in minutes.

Lockout Lifetime *
The lifetime of the lockout in minutes.

Authentication Lifetime *
The lifetime of the authentication session in minutes.

Password Authentication Lifetime *
The lifetime of the password authentication session in minutes.

Password Transpiration Lifetime *
The lifetime of the password transpiration session in minutes.

Maximum Number of Password Transpirations *
The maximum number of password transpirations per user.

Dynamic Linking Transpiration Lifetime *
The lifetime of the dynamic linking transpiration session in minutes.

Maximum Grade Per User *
The maximum grade per user.

Maximum Tokens Per User *
The maximum number of tokens per user.

Maximum Passwords Per User *
The maximum number of passwords per user.

Authentication Session Lifetime *
The lifetime of the authentication session in minutes.

Password Transpiration Lifetime *
The lifetime of the password transpiration session in minutes.

Maximum Number of Password Transpirations *
The maximum number of password transpirations per user.

Available Authenticators *
Select the authenticators that users can add to their account.

Show Other Applications *
Show XaaS applications, SaaS integrations, and custom applications that use the Duo API in My Profile.

Edit User Profile *
Allow users to edit their contact attributes.



86

REGISTRATION POLICY

Registration

Home > Registration

Authenticator Provisioning

Automatic Authenticator Provisioning
Configure the authenticators to be automatically provisioned to user.

Password *
Automatically create a password for new users.

Token *
The type of token automatically created when the user is created.

Authenticator *
Entrust Soft Token

User Portal

Available Authenticators
Select the authenticators that users can add to their account.

☒ Entrust Soft Token

☒ FIDO2

☒ Google Authenticator

☒ Grid Card

☒ Hardware Token

☒ Knowledge-based Authenticator

☒ Machine Authenticator

☒ Password

Show Other Applications
☐ Show XaaS applications, SaaS integrations, and custom applications that use the Duo API in My Profile.

Edit User Profile
☐ Allow users to edit their contact attributes.

Registration

Registration Enabled *
Enabling this feature allows users to register second factor authenticators when they log in to Identity as a Service for the first time.



87

AUTHENTICATOR POLICY

[Home > Authenticators](#)

PASSWORD	Password
PASSWORD RESET	
TEMPORARY ACCESS CODE	
ONE TIME PASSWORD	
GRID CARD	
ENTRUST SOFT TOKEN	
ENTRUST LEGACY TOKEN	
GOOGLE AUTHENTICATOR	
HARDWARE TOKEN	
KNOWLEDGE-BASED AUTHENTICATOR	
MACHINE AUTHENTICATOR	
FIDO2	
	Minimum Length * The minimum number of characters in the password 8
	Lifetime Days * Sets the number of days a password is valid. A valid 90
	Minimum Lifetime * Specifies the number of days after a password is changed 0
	Passwords Kept in History * Specifies the number of recently used passwords to keep 8
	Minimum Password Strength * Specifies the minimum acceptable strength for passwords Good
	Active Directory Complexity Requirements

88



USER NOTIFICATION

User Notifications

[Home > User Notifications](#)

User Notifications

Enable User Contact Notifications

☒ Enabling this feature allows users to receive system notifications when their contact information changes.

Notifications Email

The end user email addresses that receive notification when user contact information changes. Notifications are not delivered to users without an email address.

☒ Primary Email ☐ All Emails

This feature notifies the user of account changes to allow for a quick response in the event of unauthorized changes.

89



GROUP POLICIES

Group Policies

Home > Group Policies

Add Group Policy

☒ Enabled

Name *

Select group

At least one must be selected.

Setting Categories

 No settings categories defined.

Settings

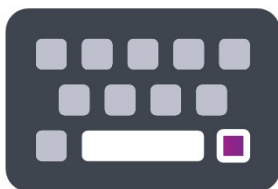
- Authenticator Provisioning
- General
- Risk-based Authentications
- Registration
- User Portal
- User Notifications
- Authenticators
 - Entrust Legacy Token
 - Entrust Soft Token
 - FIDO2
 - Google Authenticator
 - Grid Card
 - Hardware Token
 - Knowledge-based Authenticator
 - Machine Authenticator
 - One Time Password



90

LAB

- › Setup all the authenticators we require for our use cases
- › The license file will be made available through the instructor



91

REGISTRATION OPTIONS



92

REGISTRATION OPTIONS TO SIMPLIFY DEPLOYMENT

Policies Registration sets overall global registration options

Registration

Home > Registration

ENTRUST IDENTITY

Authenticator Provisioning

Automatic Authenticator Provisioning
Configure the authenticators to be automatically provisioned to user.

Password
☒ Automatically create a password for new users.

Token
☒ The type of token automatically created when the user is created. Entrust Soft Token

Smart Credential
☐ Automatically enroll a smart credential for new users.

General

Smart Credential Definition *
Select the smart credential definition that should be used for users.
PIV

These authenticators will be forced for activation during registration login



93

USER PORTAL SETTINGS

User Portal

Available Authenticators
Select the authenticators that users can add to their account.

☒	Entrust Soft Token
☐	Passkey/FIDO2
☐	Google Authenticator
☒	Grid Card
☐	Hardware Token
☒	Knowledge-based Authenticator
☒	Machine Authenticator
☒	Password
☒	Smart Credential

Show Other Applications
☐ Show RADIUS applications, IDaaS integrations, and custom applications that use the IDaaS API in My Profile.

Edit User Profile
☐ Allow users to edit their contact attributes.

Identify what authenticators will be available in their user profile page

My Profile

Home > My Profile

APPLICATIONS

- Entrust Soft Token
- Hardware Token
- Google Authenticator
- Grid Card
- FIDO2
- Password
- Machine Authenticator
- Knowledge-based Authenticator

94



94

GLOBAL REGISTRATION SETTINGS

Registration

Registration Enabled
☒ Enabling this feature allows users to register second factor authenticators when they log in to identify as a Service for the first time.

User Registration Period (days) *
The number of days a user has to self-register after their account is enabled for registration.
30

Registration Authenticators
Configure the second factor authenticators that can be registered. At least one authenticator must be set to Required or Optional.

Entrust Soft Token *	Optional
Passkey/FIDO2 *	Disabled
Google Authenticator *	Disabled
Grid Card *	Optional
Hardware Token *	Disabled
Knowledge-based Authenticator *	Optional
Smart Credential *	Disabled

Identify what authenticators to have available and if they are disabled, mandatory or optional

95



95



AUTHENTICATOR LOCKOUT BEHAVIOR

General

[Home](#) > [General](#)

 General

Lockout Count *
The number of failed authentication attempts before the user is locked.

5

Lockout Mode *
The lockout mode specifies whether a locked out authenticator locks out the user or just the authenticator.

Authenticator

Lockout Lifetime *
The amount of time before the user is automatically unlocked. A value of 0 means the user remains locked until unlocked by an administrator.

0 day

Mode is whether we lock just the authenticator or the user

**ENTRUST**