AVAYA ENGAGE®

ConvergeOne

Password Management and SSO/SAML for Remote Workers, Avaya Sets, and Soft Clients

AVAYA ENGAGE®

Chris Clauss

Manager, Avaya UC Engineering

Collaboration - ConvergeOne

David Lover

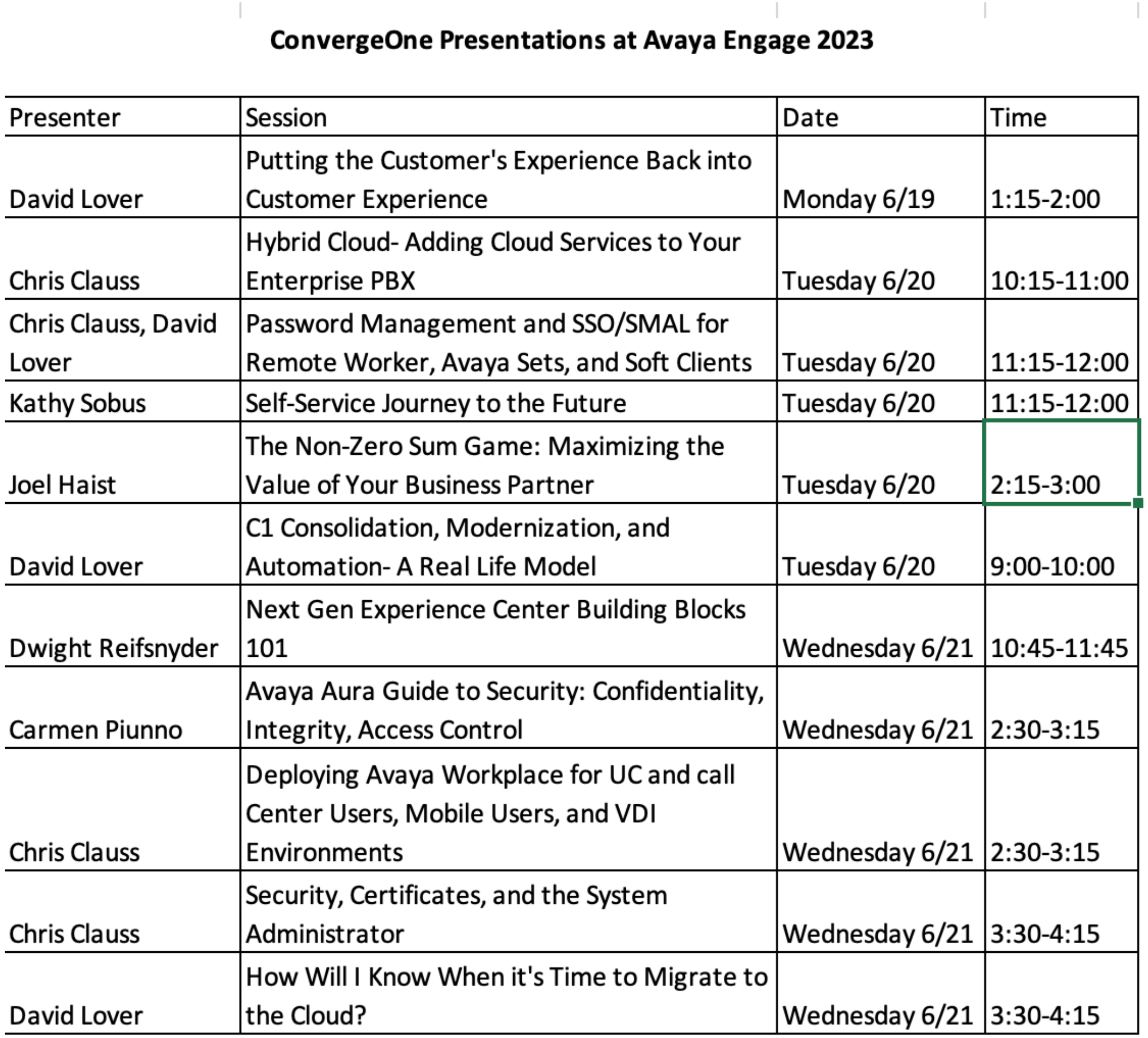
VP Strategy and Technology

ConvergeOne

Feel The Impact

ConvergeOne

Visit our Other Sessions!



ConvergeOne Presentations at Avaya Engage 2023

Presenter	Session	Date	Time
David Lover	Putting the Customer's Experience Back into Customer Experience	Monday 6/19	1:15-2:00
Chris Clauss	Hybrid Cloud- Adding Cloud Services to Your Enterprise PBX	Tuesday 6/20	10:15-11:00
Chris Clauss, David Lover	Password Management and SSO/SMAL for Remote Worker, Avaya Sets, and Soft Clients	Tuesday 6/20	11:15-12:00
Kathy Sobus	Self-Service Journey to the Future	Tuesday 6/20	11:15-12:00
Joel Haist	The Non-Zero Sum Game: Maximizing the Value of Your Business Partner	Tuesday 6/20	2:15-3:00
David Lover	C1 Consolidation, Modernization, and Automation- A Real Life Model	Tuesday 6/20	9:00-10:00
Dwight Reifsnyder	Next Gen Experience Center Building Blocks 101	Wednesday 6/21	10:45-11:45
Carmen Piunno	Avaya Aura Guide to Security: Confidentiality, Integrity, Access Control	Wednesday 6/21	2:30-3:15
Chris Clauss	Deploying Avaya Workplace for UC and call Center Users, Mobile Users, and VDI Environments	Wednesday 6/21	2:30-3:15
Chris Clauss	Security, Certificates, and the System Administrator	Wednesday 6/21	3:30-4:15
David Lover	How Will I Know When it's Time to Migrate to the Cloud?	Wednesday 6/21	3:30-4:15

Communications Trends

- **User-Centricity (As opposed to Device Centricity)**
  - No longer a digital set where the port defines the identity of the device - An IP Phone user now needs to log into their phone or soft phone to assign identity.
- **Mobility**
  - Accessible anywhere, outside of secure enterprise network
  - SBCs enable app to server security using just username and password

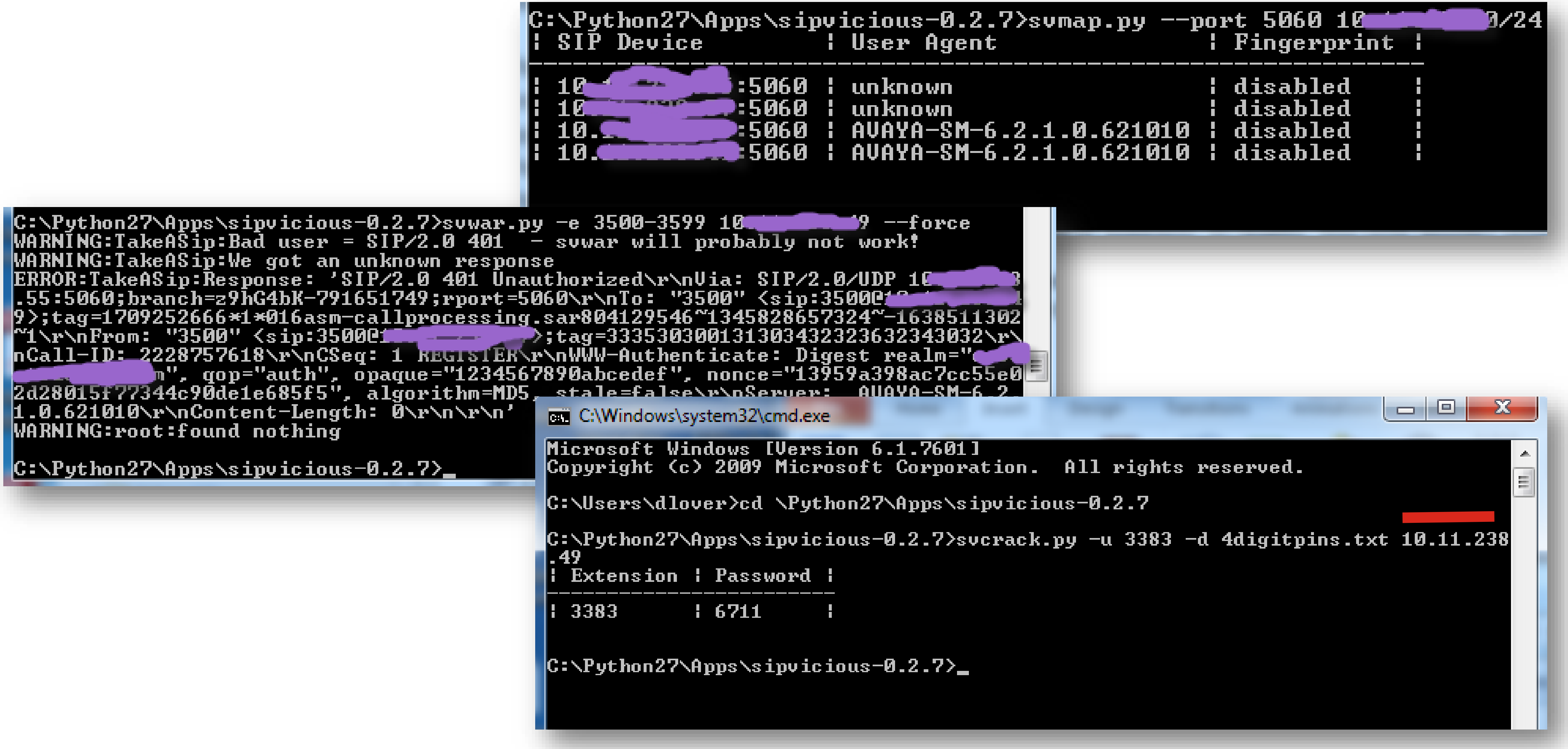
Your Communications Environment is not Secure by Default

- SIPVicious is a family of tools that are used to test the vulnerability of SIP based servers
- Your internal employees know your password scheme
- Your ex-employees know your password scheme
- You have no policy and enforcement mechanism – without a lot of manual effort and cost

SIPVicious

- SIPVicious is a family of tools that are used to test the vulnerability of SIP based servers.
  - svmap - this is a SIP scanner. Lists SIP devices found on an IP range
  - svwar - identifies active extensions on a PBX
  - svcrack - an online password cracker for SIP PBX
  - svreport - manages sessions and exports reports to various formats
  - svcrash - attempts to stop unauthorized svwar and svcrack scans

Station PINs



```
C:\Python27\Apps\sipvicious-0.2.7>svmap.py --port 5060 10[redacted]0/24
| SIP Device             | User Agent                 | Fingerprint |
------------------------------------------------------------------------
| 10[redacted]:5060      | unknown                    | disabled    |
| 10[redacted]:5060      | unknown                    | disabled    |
| 10.[redacted]:5060     | AVAYA-SM-6.2.1.0.621010    | disabled    |
| 10.[redacted]:5060     | AVAYA-SM-6.2.1.0.621010    | disabled    |
```

```
C:\Python27\Apps\sipvicious-0.2.7>svwar.py -e 3500-3599 10[redacted]9 --force
WARNING:TakeASip:Bad user = SIP/2.0 401  - svwar will probably not work!
WARNING:TakeASip:We got an unknown response
ERROR:TakeASip:Response: 'SIP/2.0 401 Unauthorized\r\nVia: SIP/2.0/UDP 1[redacted]
.55:5060;branch=z9hG4bK-791651749;rport=5060\r\nTo: "3500" <sip:3500@[redacted]
9>;tag=1709252666*1*016asm-callprocessing.sar804129546~1345828657324~-1638511302
~1\r\nFrom: "3500" <sip:3500@[redacted]>;tag=33353030013130343232363232343032\r\
nCall-ID: 2228757618\r\nCSeq: 1 REGISTER\r\nWWW-Authenticate: Digest realm="[redacted]
[redacted]m", qop="auth", opaque="1234567890abcedef", nonce="13959a398ac7cc55e0
2d28015f77344c90de1e685f5", algorithm=MD5, stale=false\r\nServer: AVAYA-SM-6.2.
1.0.621010\r\nContent-Length: 0\r\n\r\n'
WARNING:root:found nothing

C:\Python27\Apps\sipvicious-0.2.7>_
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\dlover>cd \Python27\Apps\sipvicious-0.2.7

C:\Python27\Apps\sipvicious-0.2.7>svcrack.py -u 3383 -d 4digitpins.txt 10.11.238
.49
| Extension | Password |
------------------------
| 3383      | 6711     |


C:\Python27\Apps\sipvicious-0.2.7>_
```

Station PINs

- A typical PC can do about 70 registration / second
  - 4-digit pin (0000-9999) can be hacked in 142 seconds
  - 5-digit pin (00000-99999) can be hacked in 23.8 minutes
  - 6-digit pin (000000-999999 can be hacked in 3.9 hours
  - 7-digit pin (0000000-9999999) can be hacked in 1.6 days
  - 8-digit pin (00000000-99999999) can be hacked in 2.4 weeks

Steps to secure user accounts

- Start with an appropriately long and/or complex password that is difficult to guess or brute force hack.
- Change passwords frequently
- Turn on Firewalls that contain “rate limiting” to slow down a hacker’s brute force speed.

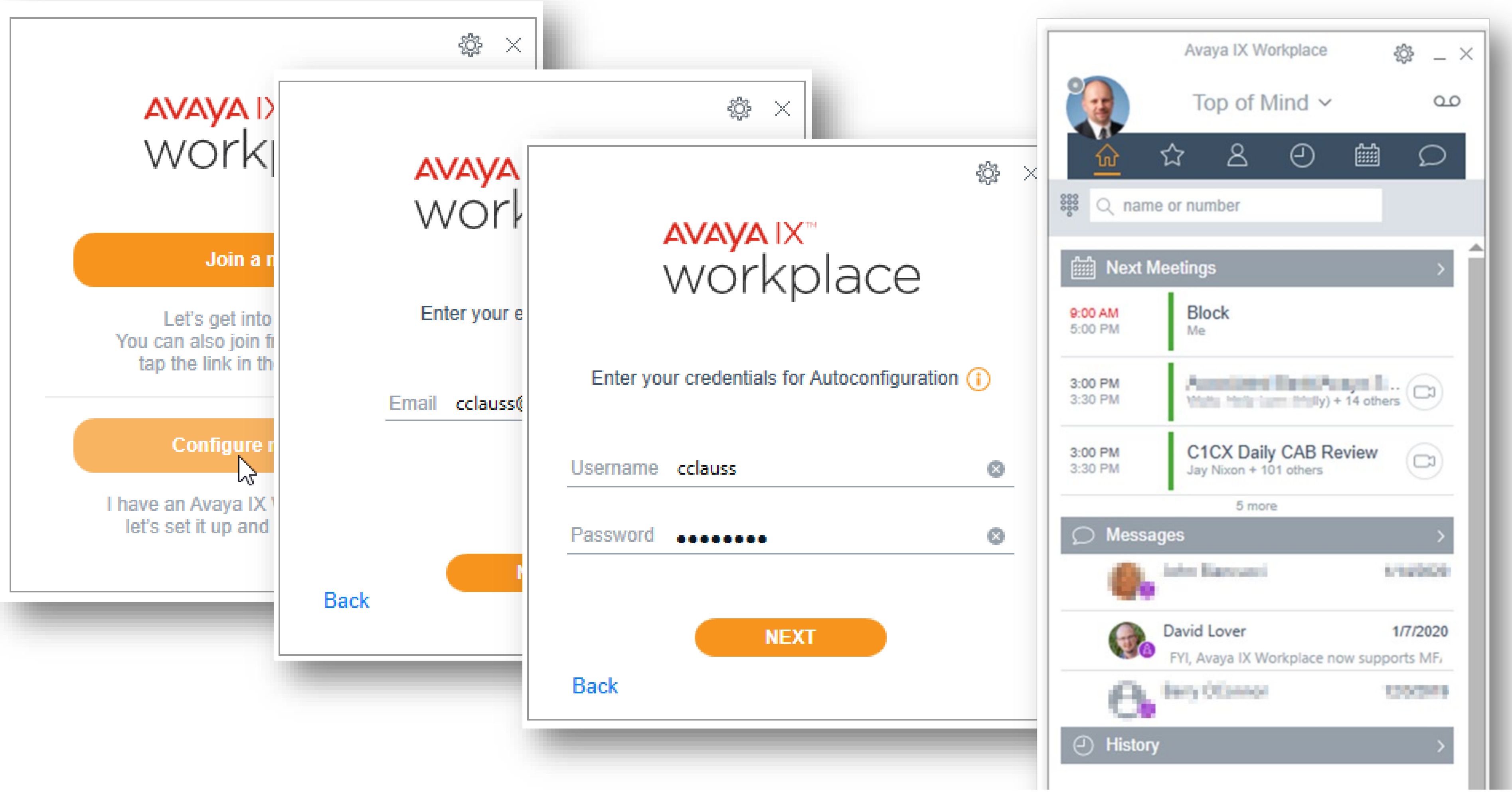
Note: PCI Data Security Standard 4.0 - Password Requirements

- 12 Characters (containing both numbers and letters)
- Ensure the last 4 passwords cannot be re-used
- Requires Passwords to be changed every 90 days

What is or will be driving security in your organization?

- Devices
  - Remote Worker
  - Internet Connected Device
  - BYOD
  - Hosted Solutions
- Security Teams
  - Are they asking for audits?
  - Are they taking notice of U/C?
  - Is management worried (news)?
- What needs to be secured?
  - Voice conversations
  - The systems themselves

End user login / ease of configuration



Enter your credentials for Autoconfiguration

Username cclauss

Password ●●●●●●●●●

9:00 AM 5:00 PM	Block Me
3:00 PM 3:30 PM	…lly) + 14 others
3:00 PM 3:30 PM	C1CX Daily CAB Review Jay Nixon + 101 others

David Lover 1/7/2020
FYI, Avaya IX Workplace now supports MF/

What you don’t didn’t about logins…

Really Important!

- A phone or soft client always uses SIP station login and SIP station password to connect to Session Manager or SBC.
- An attacker can use this information to login a station, even if you are using other authentication techniques.
- The best way to protect against this – leverage the tools Avaya and C1 provide so that SIP station passwords can be impossible to guess.
- Never give a user a station password. Use single sign on.

Avaya Aura Device Services to the rescue!

Device services provides…

Single Sign on Support using LDAP or SAML

Dynamic Configuration of workplace clients, Agent for Desktop, and physical sets, matching users to customer LDAP and A/D groups to define features.

Provides enterprise directory services to soft clients.

Administrators manage user configurations across the enterprise from a single pain of glass.

Synchronization of users between enterprise and Avaya Cloud services – Spaces.

Authentication

Who do we authenticate to?

- LDAP providers (generally MS Active Directory)
  Lightweight Directory Access Protocol
- SAML providers (MS Azure / ADFD / Okta / etc.)
  Security Assertion Markup Language

LDAP Authentication

Pros / Cons

- LDAP is great for on-prem authentication.
- Simple query against LDAP to validate login.
- Very easy to implement with compatibility across many applications.
- Applications pass logins / passwords to LDAP for authentication.
- Problem – the application knows the login / password?!?

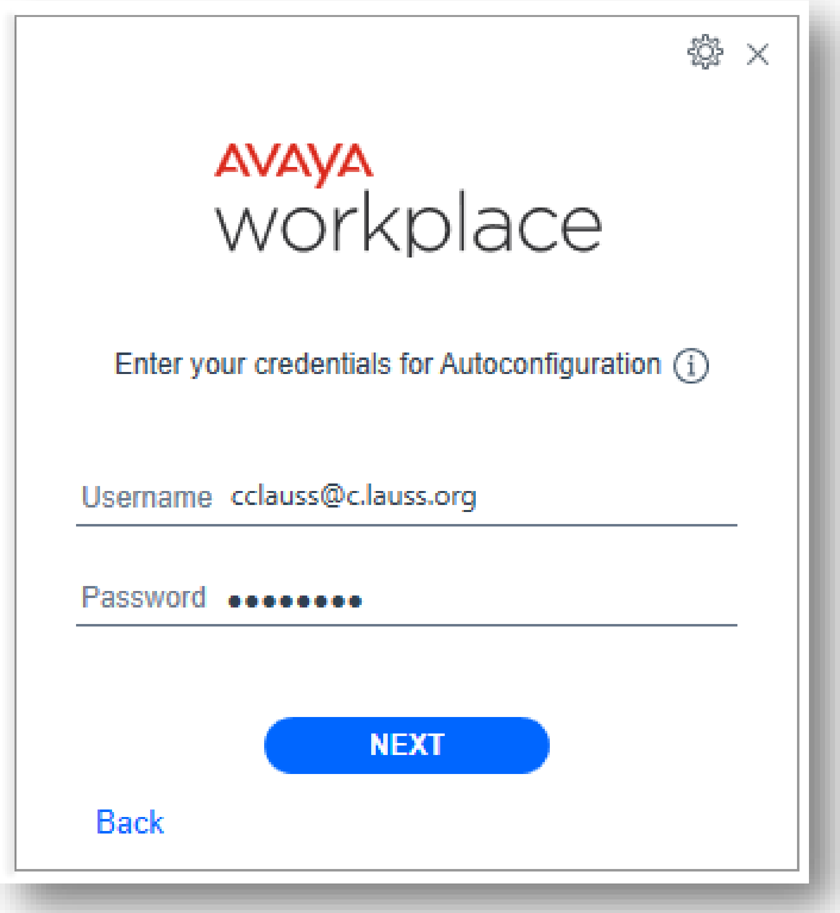
SAML Authentication

Pros / Cons

- Designed for cloud.
- Logins are redirected to a trusted SAML identity provider via an external app (usually a web browser).
- Application never knows login / password.
- Provider sends a token back to application. The token indicates if login was successful and how long it is valid.
- Implies that trust must be configured between the application and the identity provider. Difficult to implement?!?

LDAP Authentication on Workplace Client

- Login and password entered in the application itself.
- Credentials are passed to AADS securely and AADS proxies a login to LDAP server to validate the login / password.
- AADS matches that user to System Manager and pulls the station login and password.
- AADS sends that information back to workplace to login the user.

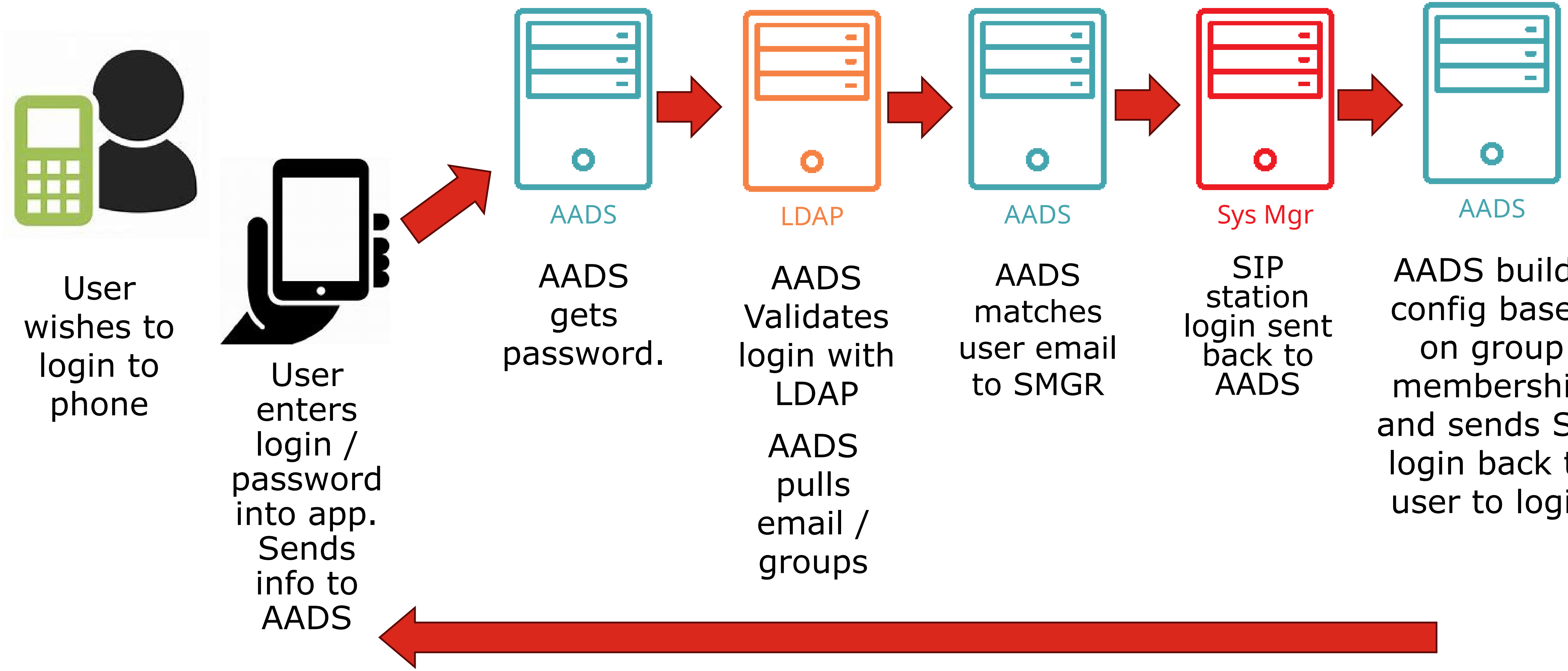


Enter your credentials for Autoconfiguration

Username cclauss@c.lauss.org

Password ●●●●●●●●●

Single Sign On - LDAP



User wishes to login to phone

User enters login / password into app. Sends info to AADS

AADS gets password.

AADS Validates login with LDAP

AADS pulls email / groups

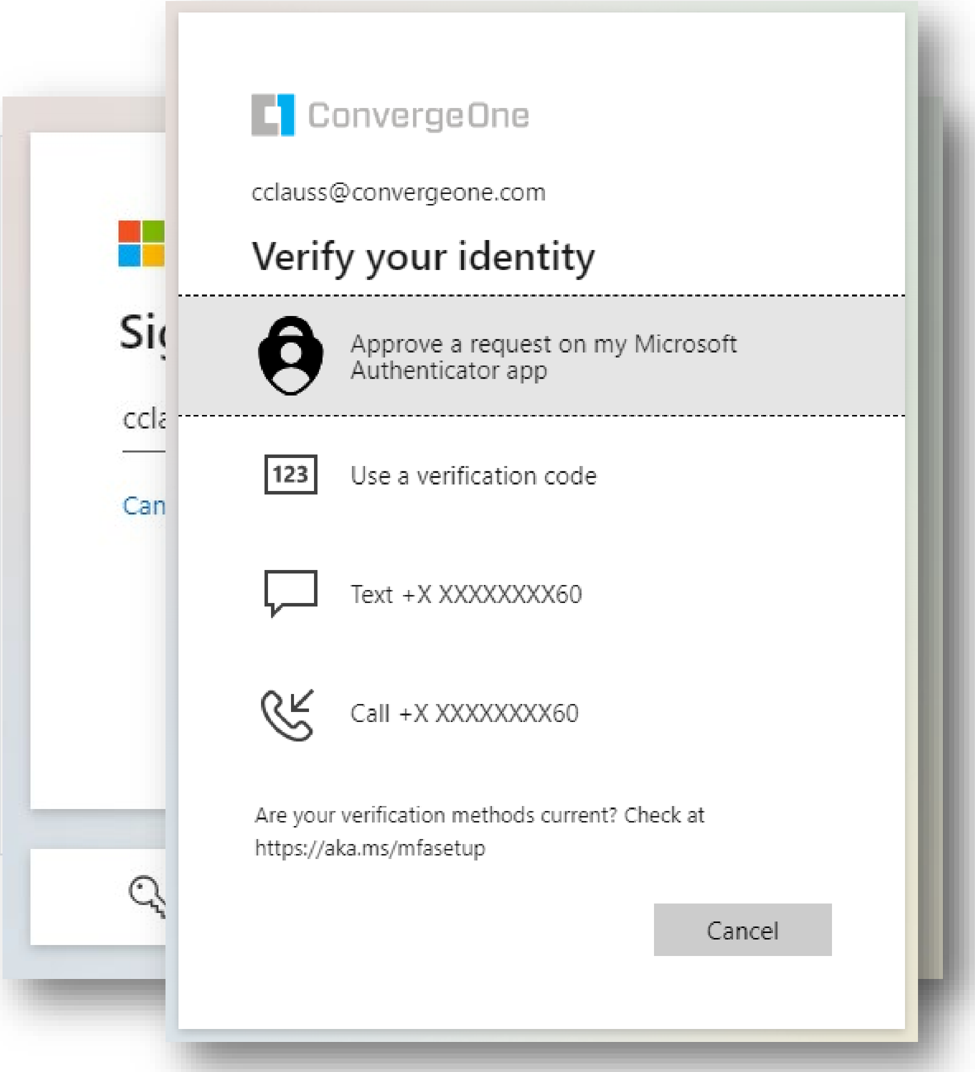
AADS matches user email to SMGR

SIP station login sent back to AADS

AADS builds config based on group membership and sends SIP login back to user to login

SAML Authentication on Workplace Client

- A web screen is popped on the device to have the user authenticate to the identity provider.
- Once complete, the provider sends back a token with the user's information.
- AADS matches that user to System Manager and pulls the station login and password.
- AADS sends that information back to workplace to login the user.



ConvergeOne

cclauss@convergeone.com

Verify your identity

Approve a request on my Microsoft Authenticator app

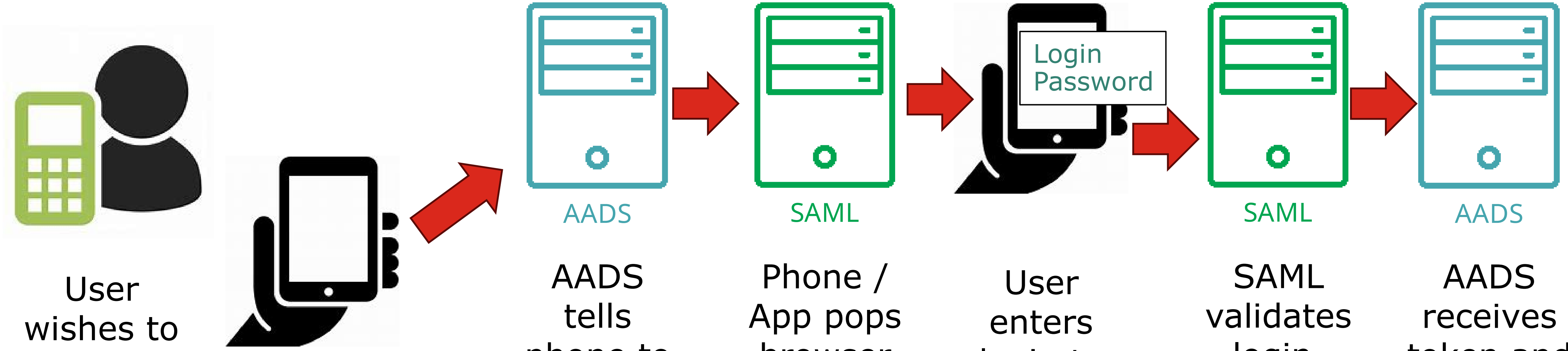
Use a verification code

Text +X XXXXXXXX60

Call +X XXXXXXXX60

Are your verification methods current? Check at https://aka.ms/mfasetup

Single Sign On - SAML



User wishes to login to phone

Phone / App asks AADS to login

AADS tells phone to use SAML

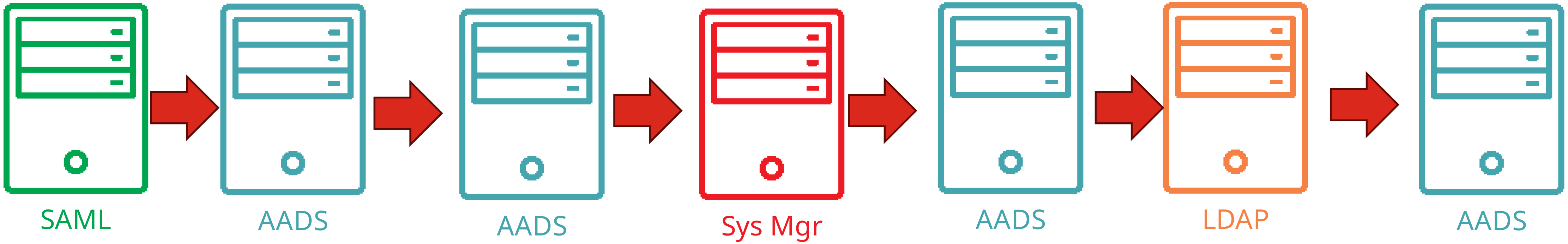
Phone / App pops browser

User enters login to browser. not the app

SAML validates login. Sends token to AAD

AADS receives token and pulls email address*

Single Sign On – SAML - Continued



SAML validates login. Sends token to AAD

AADS receives token and pulls email address*

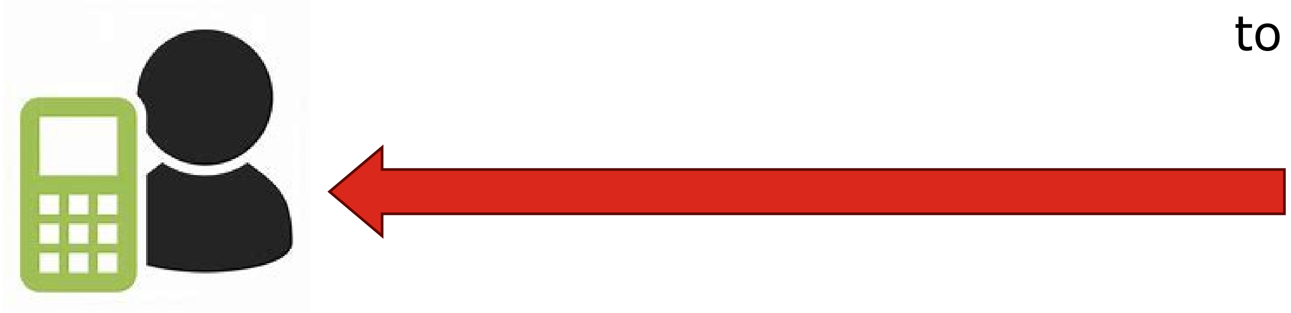
AADS matches user email to SMGR

SIP station login sent back to AADS

AADS matches user with LDAP server to get group membership

LDAP groups information looked up by AADS

AADS builds config based on group membership and sends SIP login back to user to login



SAML Easily supports MFA (Multi Factor Authentication)

Extends security beyond password.

Something you know…

- Your Login and Password

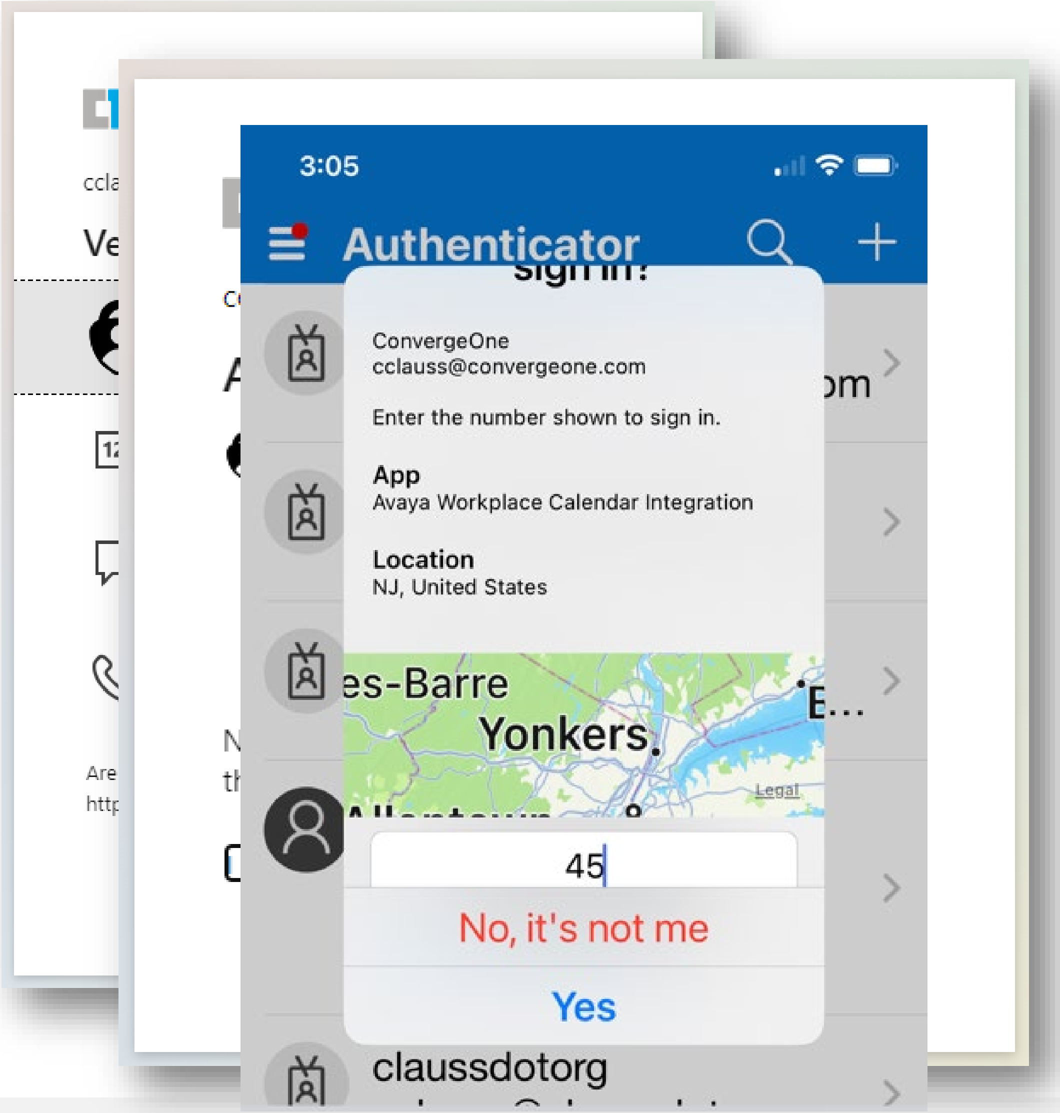
Something you have

- A cell phone app or token ID card

Something you are

- Face recognition on a cell phone

Successful login will send a token to AADS to validate the login.



ConvergeOne
cclauss@convergeone.com

Enter the number shown to sign in.

App
Avaya Workplace Calendar Integration

Location
NJ, United States

45

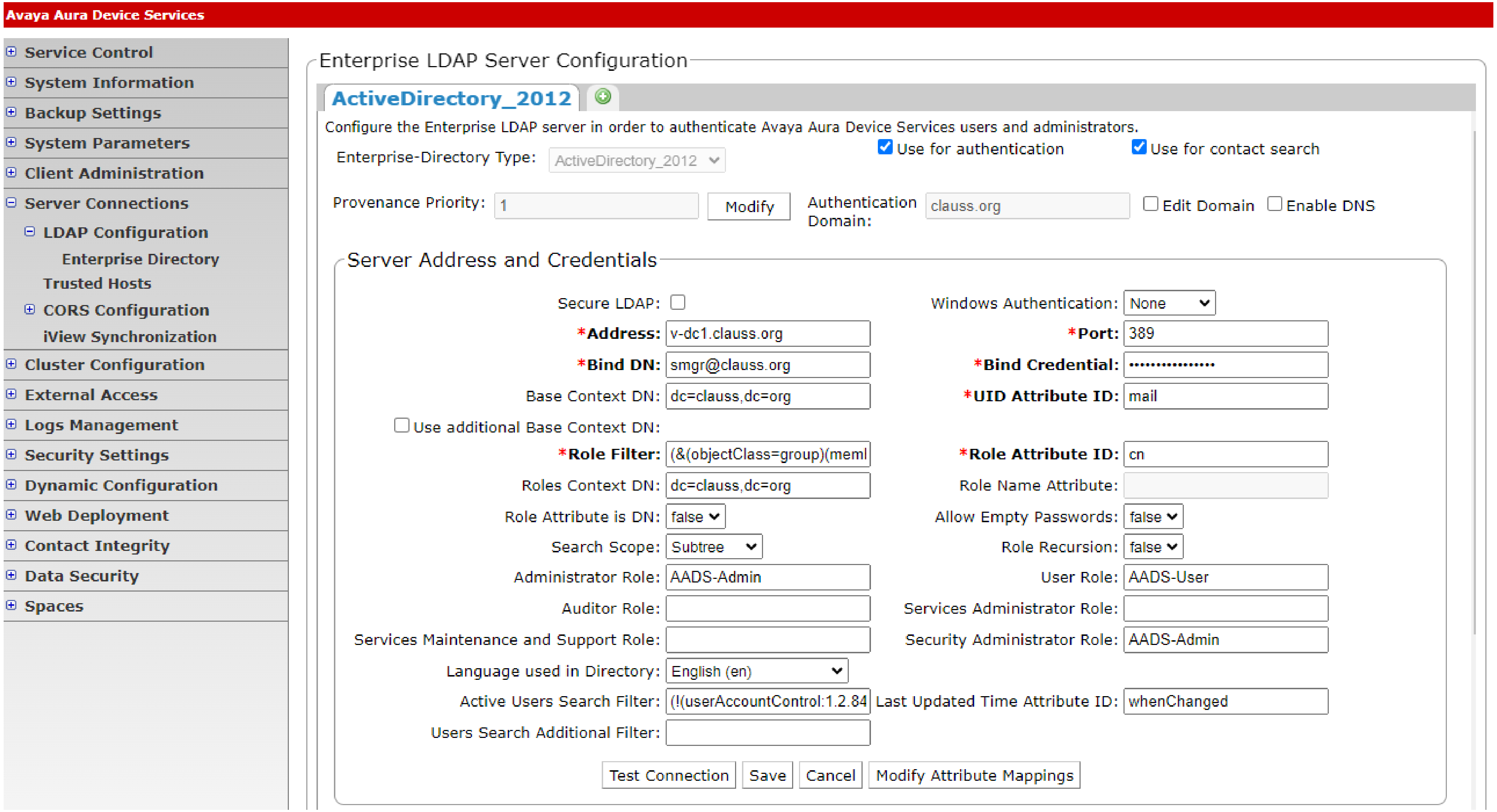
What is a SAML token?

Contains information the software can use.

Token will return information we can use to allow the application to work.

- Name of the user
- Groups / Permissions
- Some type of “matching” field – usually email address.
  - Match a user from SAML to a user in Avaya systems.
- Has an expiry time – user must reauthenticate.

AADS LDAP Authentication



Enterprise LDAP Server Configuration

Configure the Enterprise LDAP server in order to authenticate Avaya Aura Device Services users and administrators.

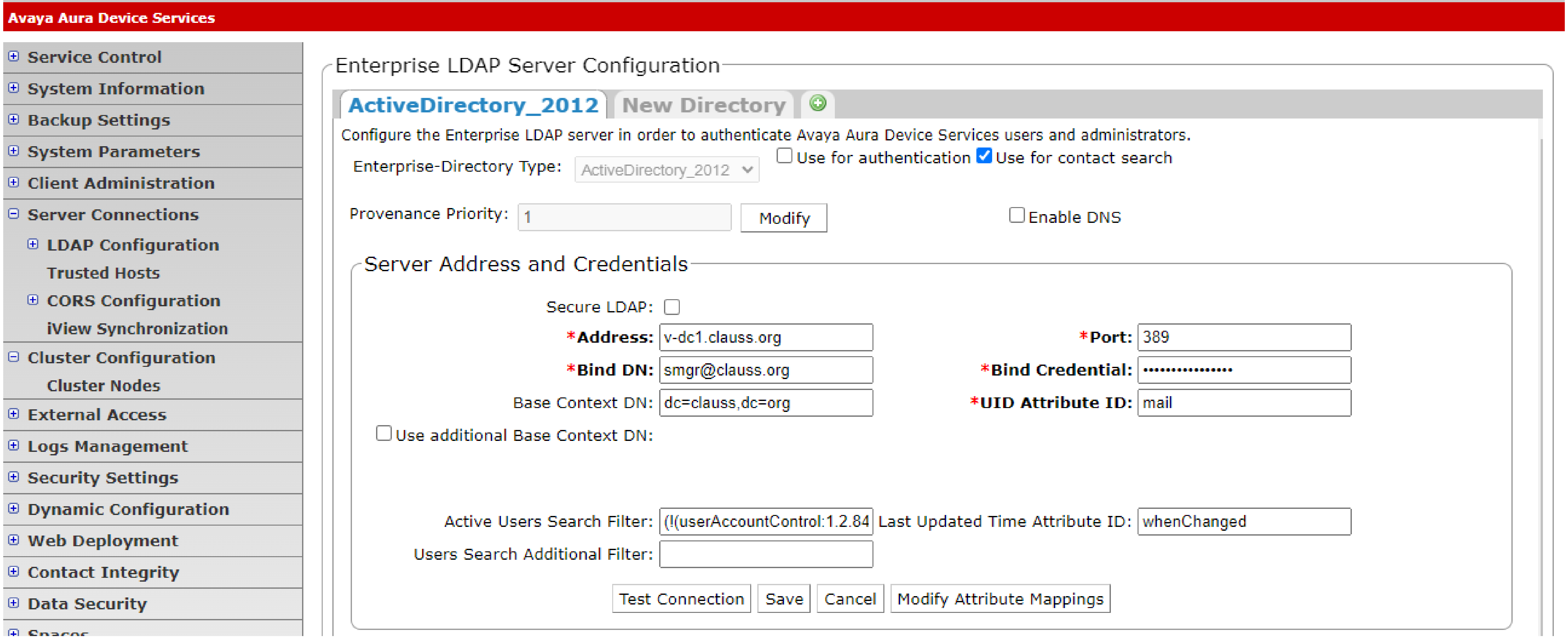
Enterprise-Directory Type: ActiveDirectory_2012 ☑ Use for authentication ☑ Use for contact search

Provenance Priority: 1 Authentication Domain: clauss.org ☐ Edit Domain ☐ Enable DNS

Server Address and Credentials

Secure LDAP:	☐	Windows Authentication:	None
*Address:	v-dc1.clauss.org	*Port:	389
*Bind DN:	smgr@clauss.org	*Bind Credential:	•••••••••••••••••
Base Context DN:	dc=clauss,dc=org	*UID Attribute ID:	mail
☐ Use additional Base Context DN:			
*Role Filter:	(&(objectClass=group)(meml	*Role Attribute ID:	cn
Roles Context DN:	dc=clauss,dc=org	Role Name Attribute:	
Role Attribute is DN:	false	Allow Empty Passwords:	false
Search Scope:	Subtree	Role Recursion:	false
Administrator Role:	AADS-Admin	User Role:	AADS-User
Auditor Role:		Services Administrator Role:	
Services Maintenance and Support Role:		Security Administrator Role:	AADS-Admin
Language used in Directory:	English (en)		
Active Users Search Filter:	(!(userAccountControl:1.2.84	Last Updated Time Attribute ID:	whenChanged
Users Search Additional Filter:			

AADS SAML Authentication



Enterprise LDAP Server Configuration

Configure the Enterprise LDAP server in order to authenticate Avaya Aura Device Services users and administrators.

Enterprise-Directory Type: ActiveDirectory_2012 ☐ Use for authentication ☑ Use for contact search

Provenance Priority: 1 ☐ Enable DNS

Server Address and Credentials

Secure LDAP: ☐

*Address: v-dc1.clauss.org *Port: 389

*Bind DN: smgr@clauss.org *Bind Credential: ••••••••••••••••

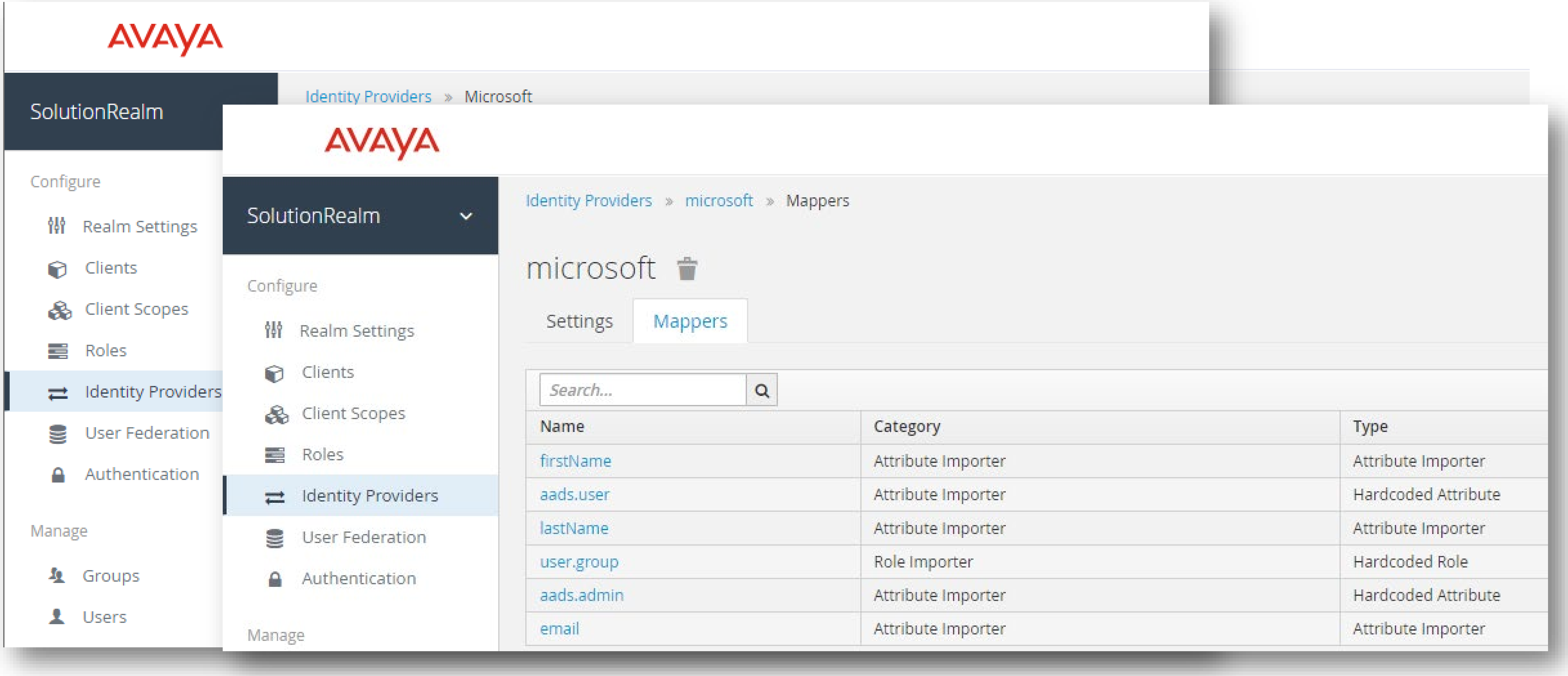
Base Context DN: dc=clauss,dc=org *UID Attribute ID: mail

☐ Use additional Base Context DN:

Active Users Search Filter: (!(userAccountControl:1.2.84 Last Updated Time Attribute ID: whenChanged

Users Search Additional Filter:

AADS SAML Authentication



Name	Category	Type
firstName	Attribute Importer	Attribute Importer
aads.user	Attribute Importer	Hardcoded Attribute
lastName	Attribute Importer	Attribute Importer
user.group	Role Importer	Hardcoded Role
aads.admin	Attribute Importer	Hardcoded Attribute
email	Attribute Importer	Attribute Importer

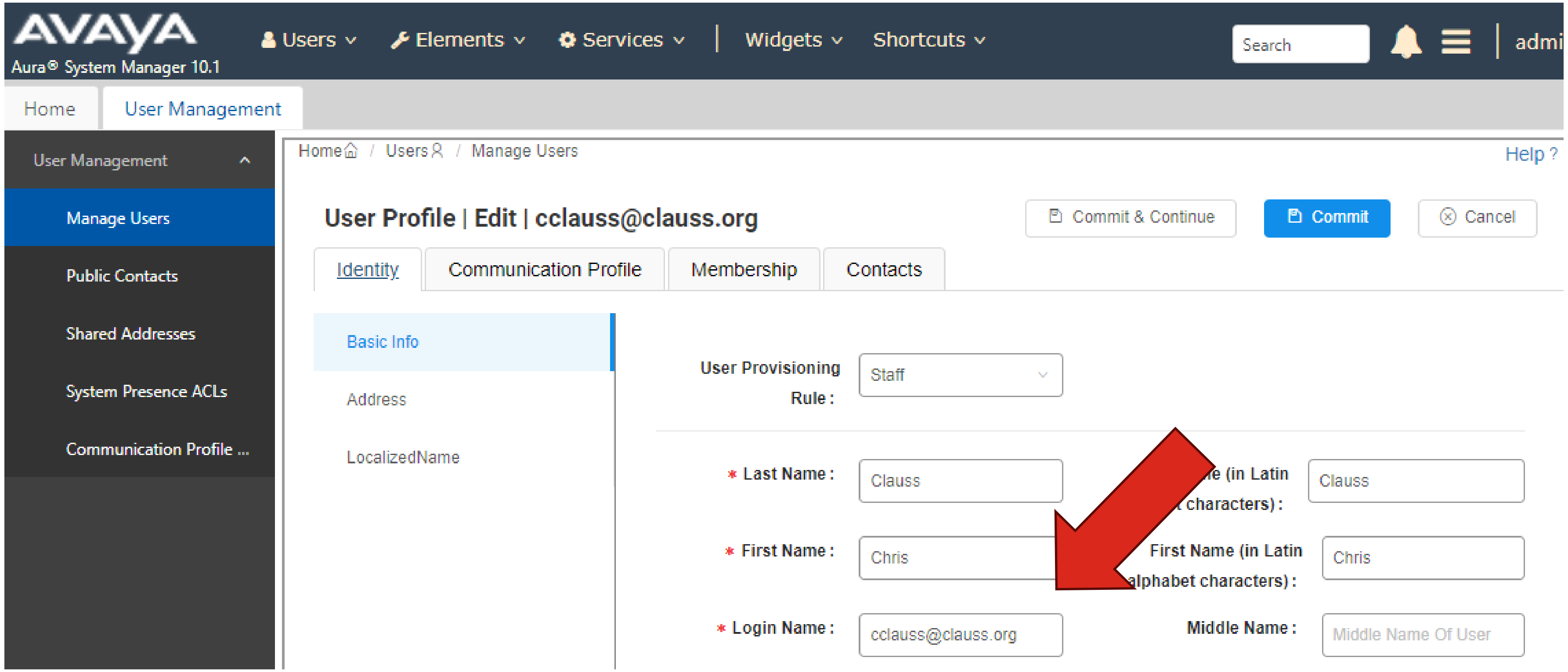
Now that a user is authenticated?

How do we get the settings for a station?

Once LDAP or SAML authentication has been completed, we get a matching field.

AADS matches that to a System Manager user profile (usually by email address)

Once we know what Avaya user we need to login, we can pull the SIP username and password.



User Profile | Edit | cclauss@clauss.org

User Provisioning Rule : Staff

* Last Name : Clauss

…e (in Latin …characters) : Clauss

* First Name : Chris

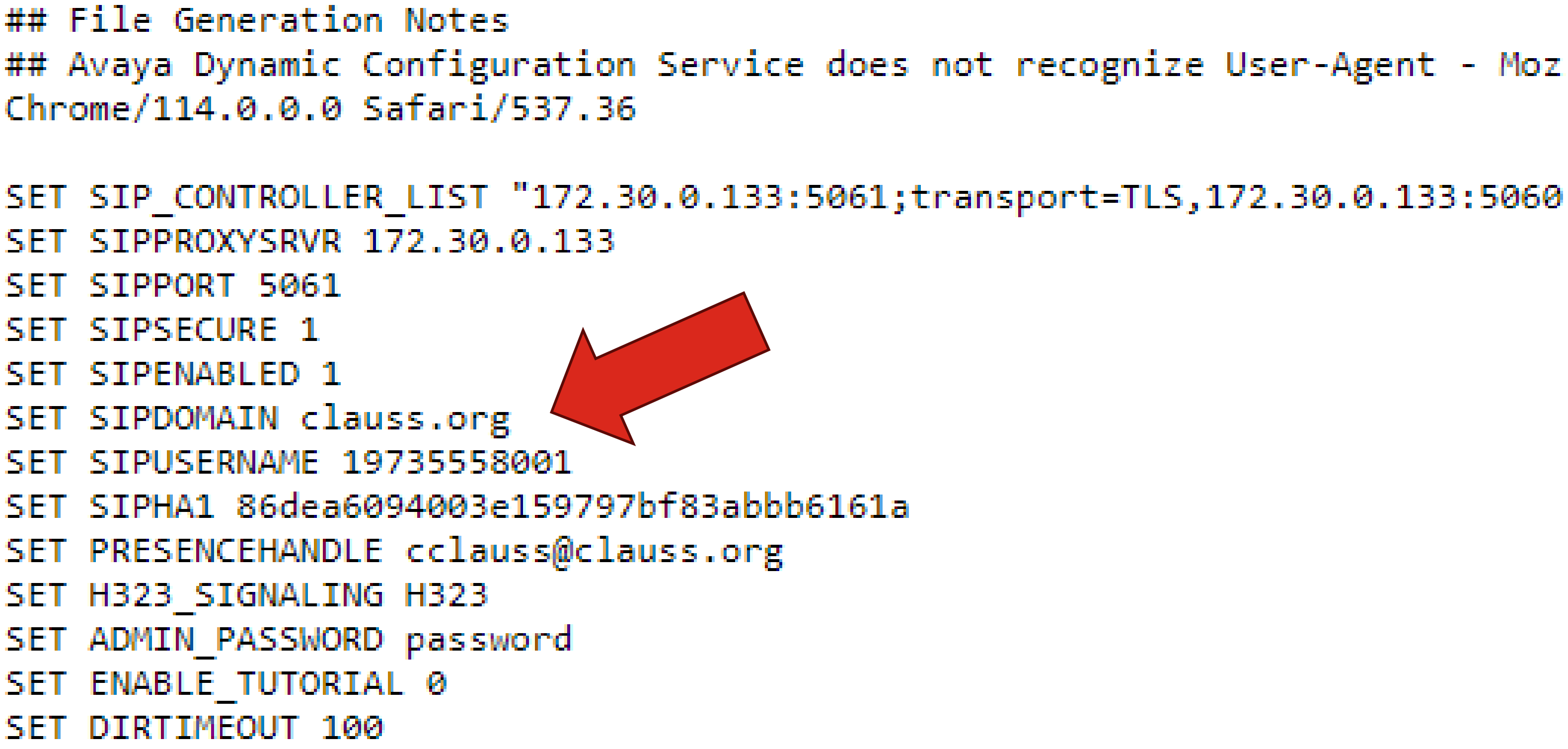
First Name (in Latin alphabet characters) : Chris

* Login Name : cclauss@clauss.org

Middle Name : Middle Name Of User

AADS uses this information to build a config…

AADS grabs the SIP login, encrypts it, checks the group memberships, then builds a custom config (46xxsettings) file and sends it to the endpoint.



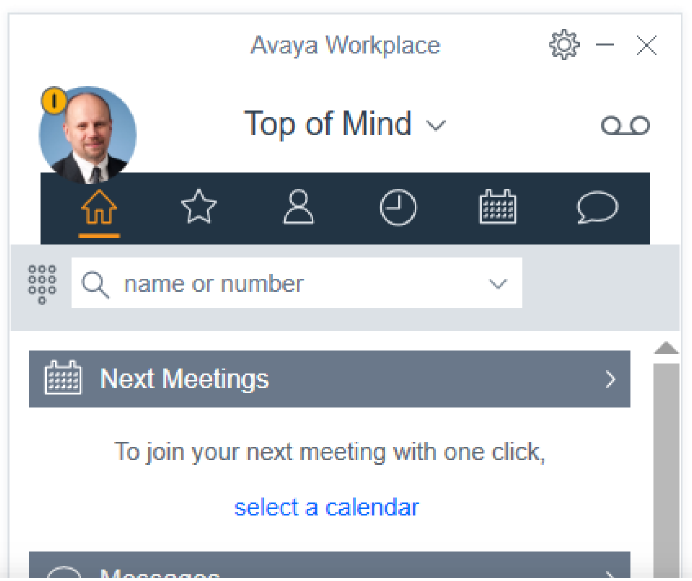
```
## File Generation Notes
## Avaya Dynamic Configuration Service does not recognize User-Agent - Moz
Chrome/114.0.0.0 Safari/537.36

SET SIP_CONTROLLER_LIST "172.30.0.133:5061;transport=TLS,172.30.0.133:5060
SET SIPPROXYSRVR 172.30.0.133
SET SIPPORT 5061
SET SIPSECURE 1
SET SIPENABLED 1
SET SIPDOMAIN clauss.org
SET SIPUSERNAME 19735558001
SET SIPHA1 86dea6094003e159797bf83abbb6161a
SET PRESENCEHANDLE cclauss@clauss.org
SET H323_SIGNALING H323
SET ADMIN_PASSWORD password
SET ENABLE_TUTORIAL 0
SET DIRTIMEOUT 100
```

What clients are supported by AADS?

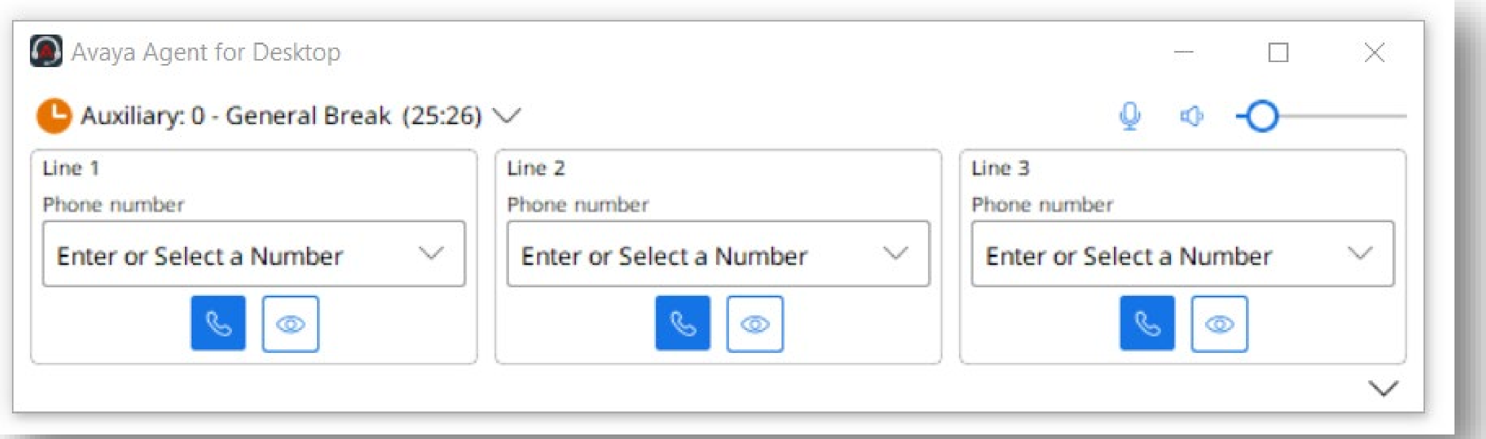
AADS send the config to the endpoint with SIP login

- Avaya Workplace
- Avaya Workplace (Call Center)
- Agent for Desktop
- J1XX physical endpoints



To join your next meeting with one click,

select a calendar



Auxiliary: 0 - General Break (25:26)

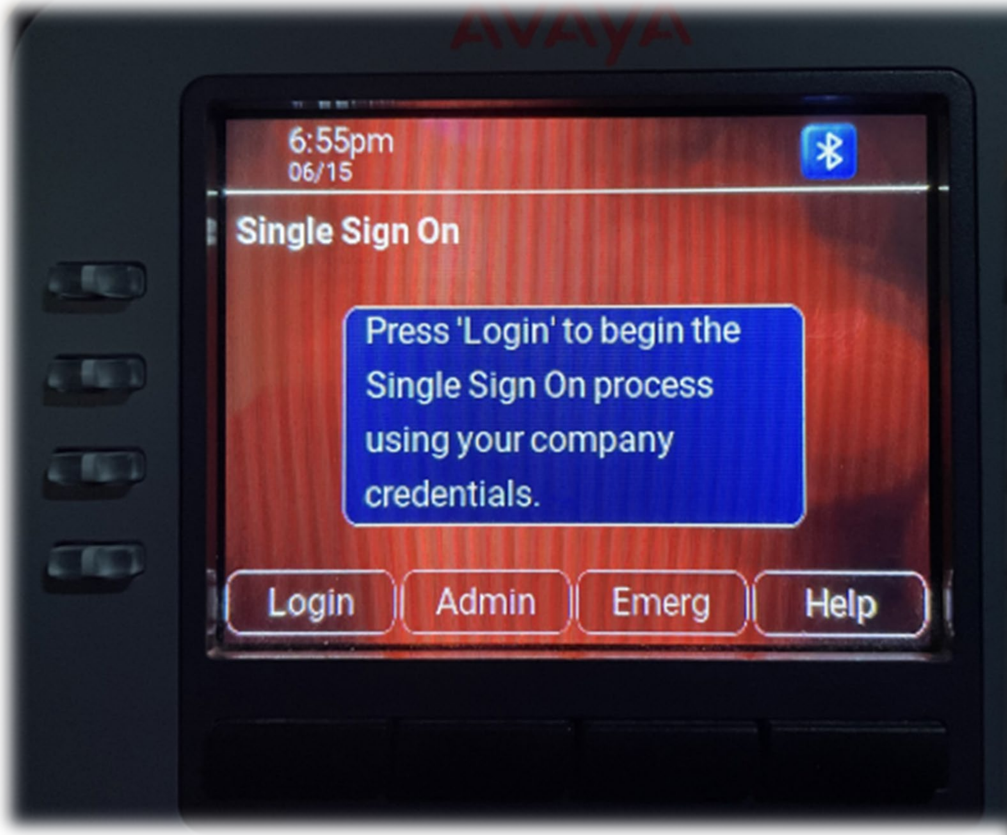
Line 1	Line 2	Line 3
Phone number	Phone number	Phone number
Enter or Select a Number	Enter or Select a Number	Enter or Select a Number

What about support for physical phones?

J100 Series sets support SSO staring in 2023

- AADS is required
- Requires AADS 10.1.1 and later
  - SMGR / ASM 8.1.3 or 10.0
- Latest SIP firmware 4.1.x (April 5, 2023)
  - Supports TLS 1.3
- Only supports Avaya IAM (Identity and Access Management)
- IAM can cascade logins to another Identity Provider
- Future – direct authentication with another identity provider.

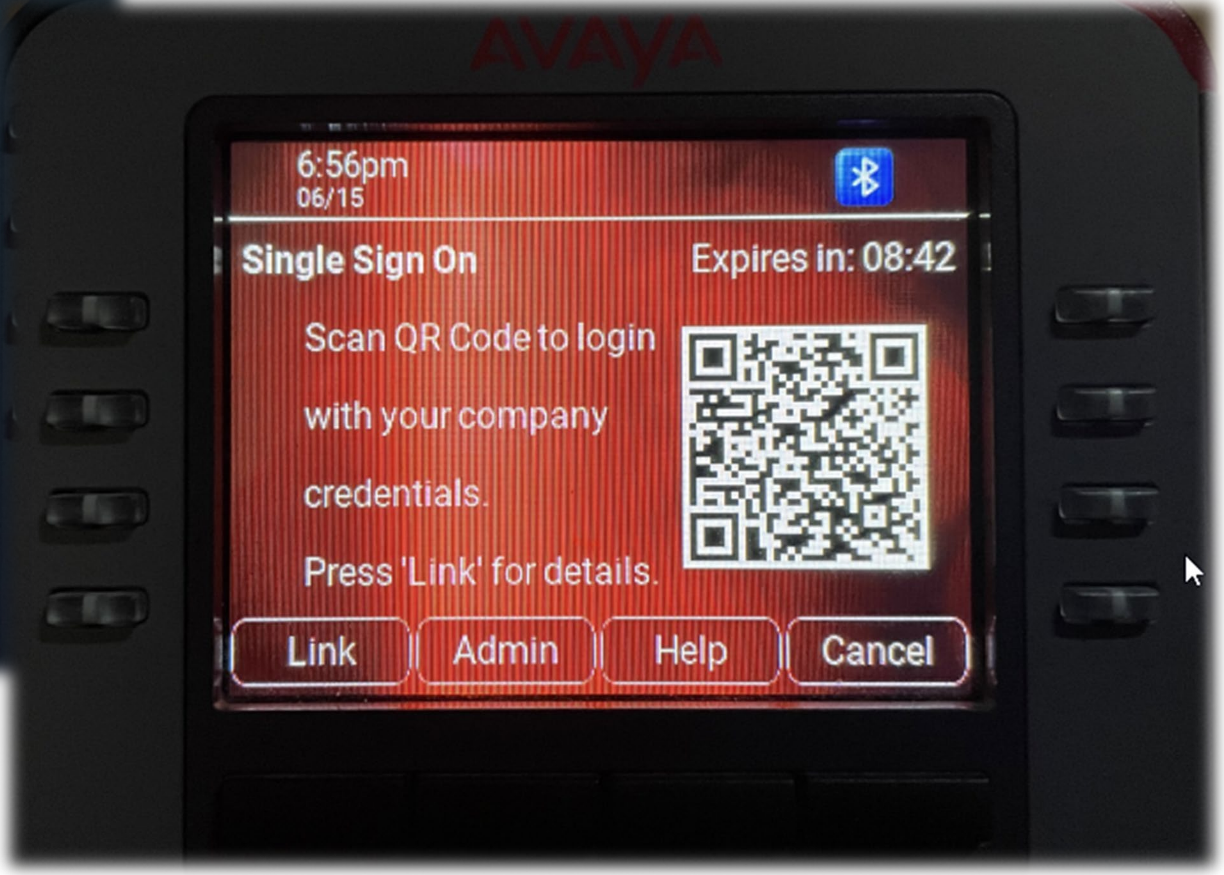
How do I type my password into a phone?



6:55pm
06/15

Single Sign On

Press 'Login' to begin the Single Sign On process using your company credentials.



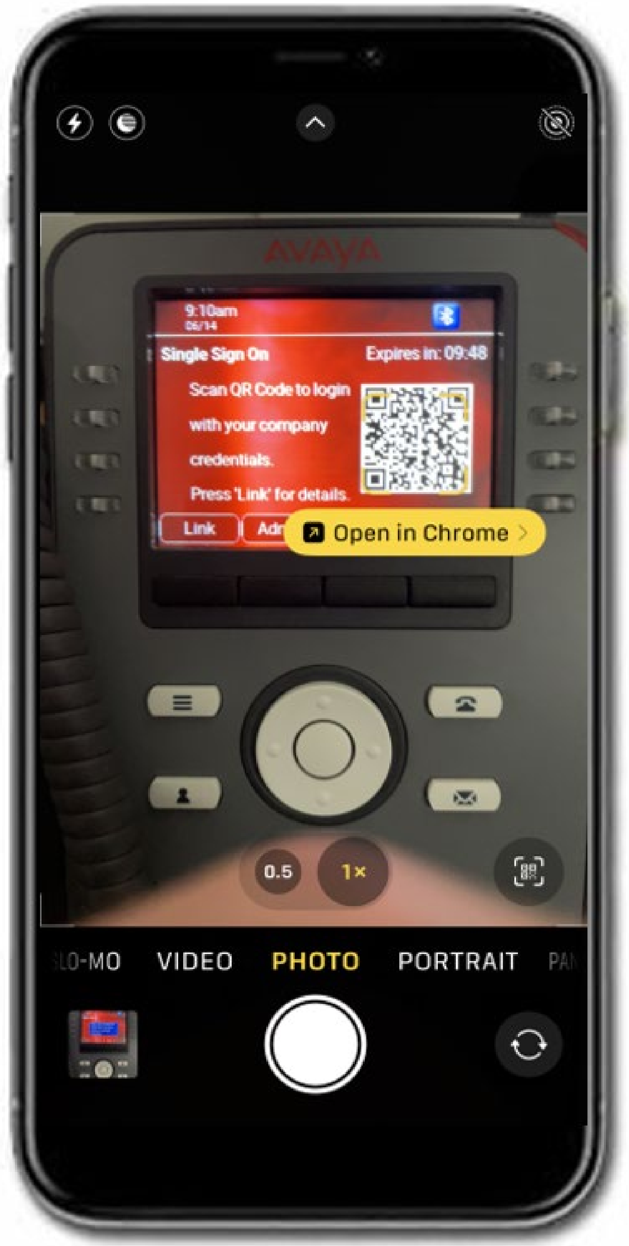
6:56pm
06/15

Single Sign On

Expires in: 08:42

Scan QR Code to login with your company credentials.

Press 'Link' for details.



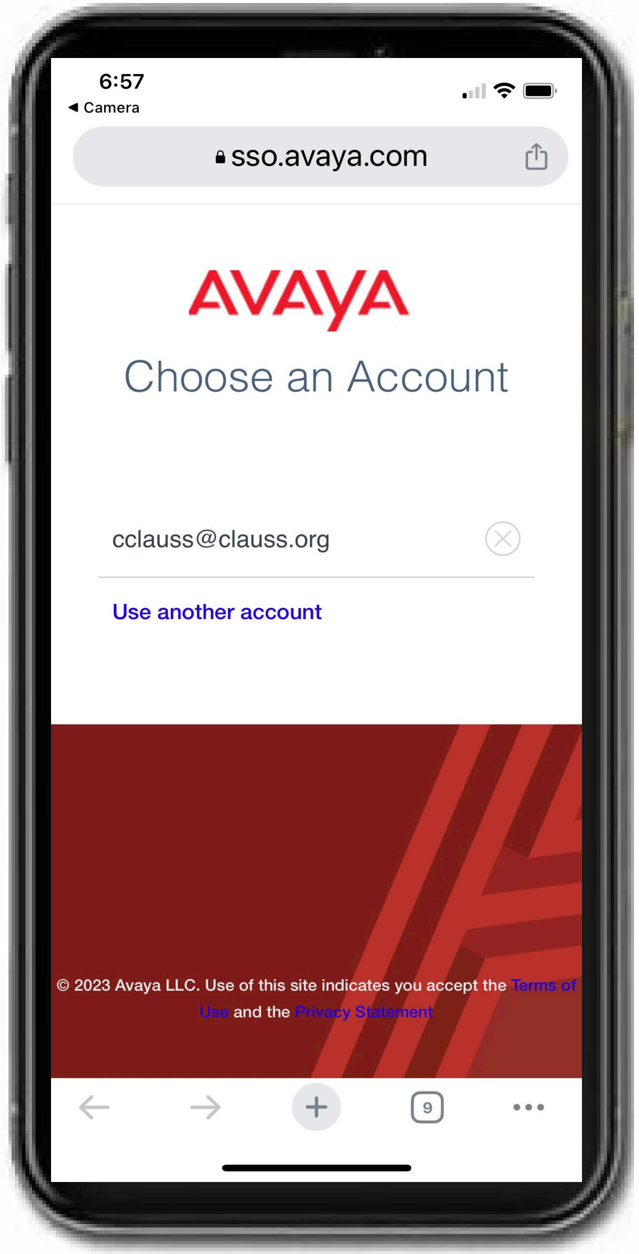
Single Sign On

Expires in: 09:48

Scan QR Code to login with your company credentials.

Press 'Link' for details.

Open in Chrome



sso.avaya.com

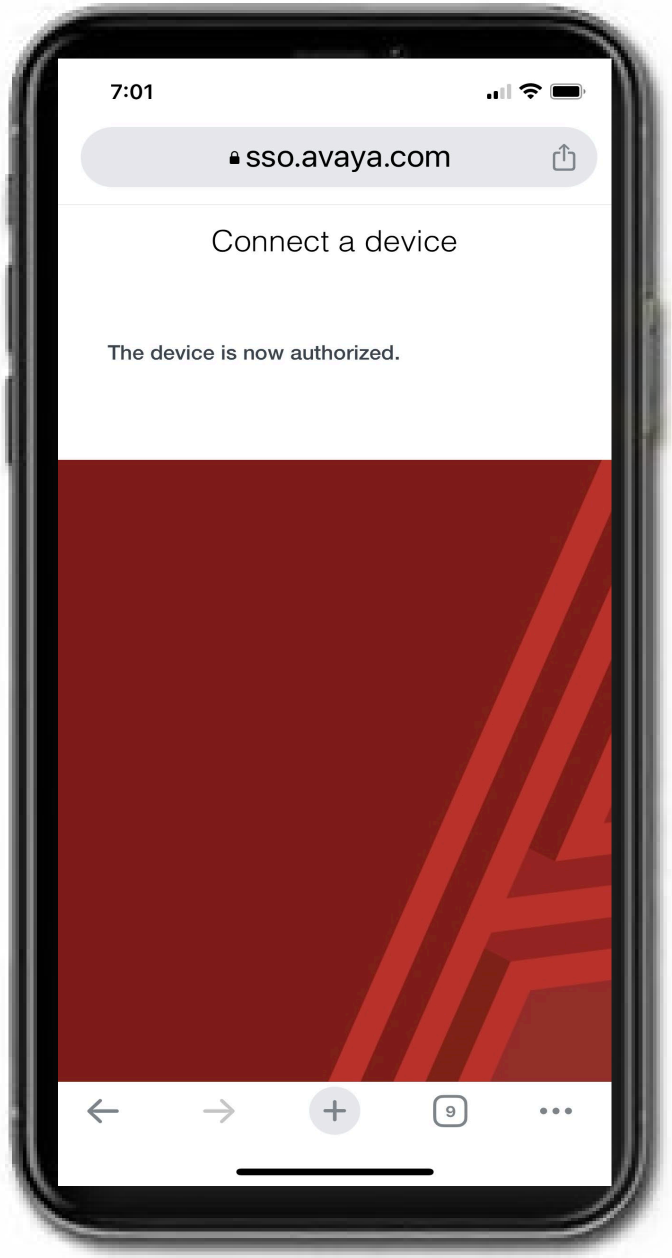
AVAYA

Choose an Account

cclauss@clauss.org

Use another account

© 2023 Avaya LLC. Use of this site indicates you accept the Terms of Use and the Privacy Statement

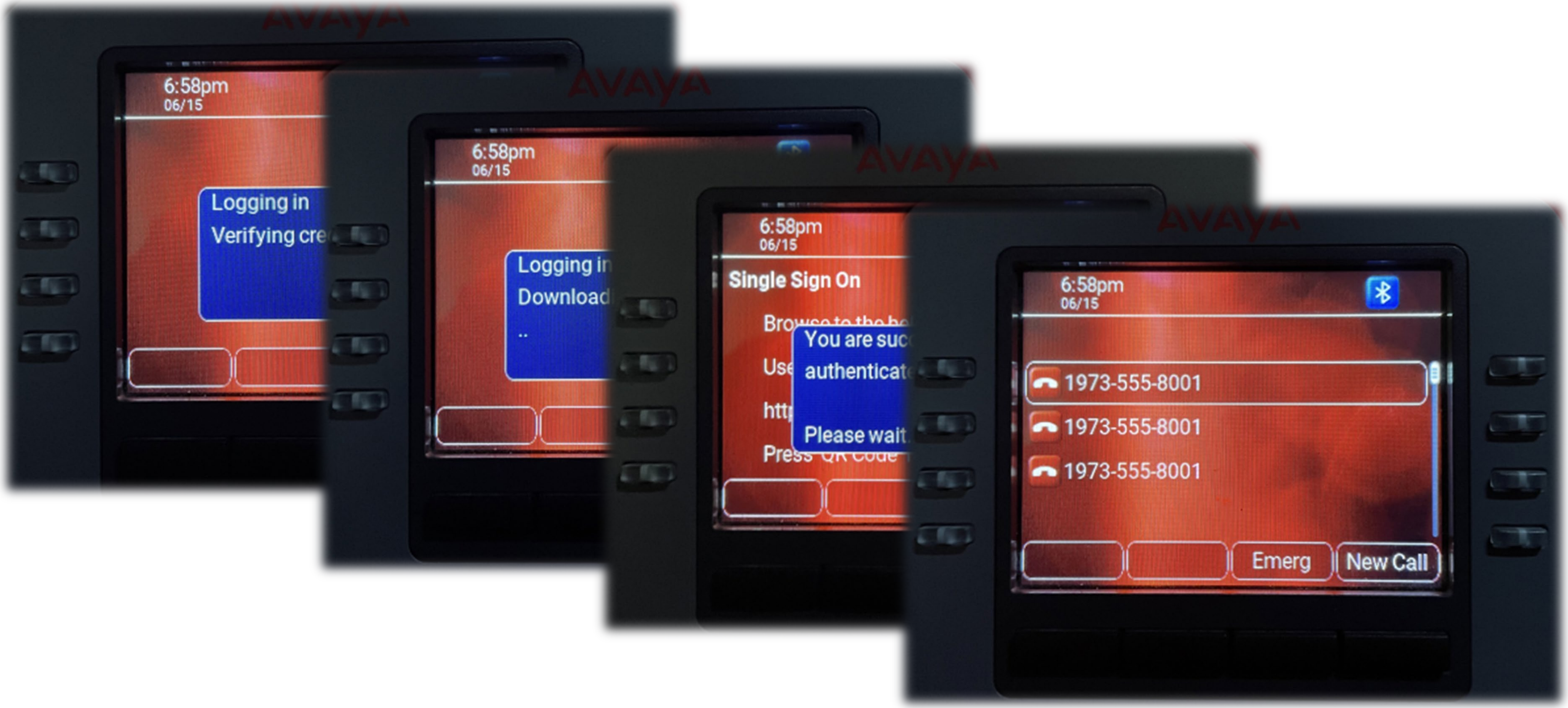


sso.avaya.com

Connect a device

The device is now authorized.

How do I type my login on a phone?



6:58pm
06/15

Logging in
Verifying cre

6:58pm
06/15

Logging in
Download
..

6:58pm
06/15

Single Sign On

Browse to the ho
Use
http
Press QR Code

You are suc
authenticat

Please wait.

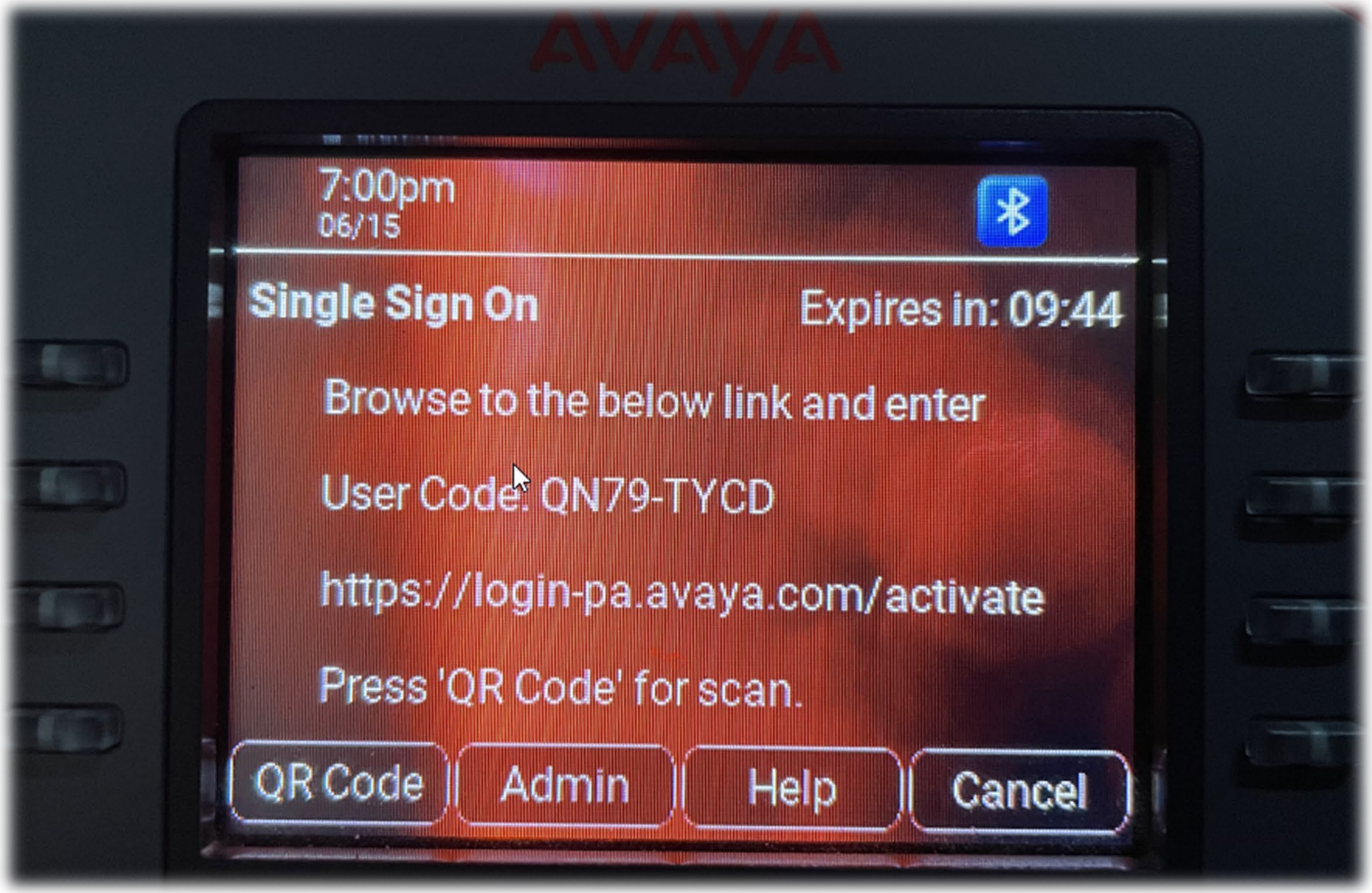
6:58pm
06/15

1973-555-8001

1973-555-8001

1973-555-8001

Emerg | New Call



7:00pm
06/15

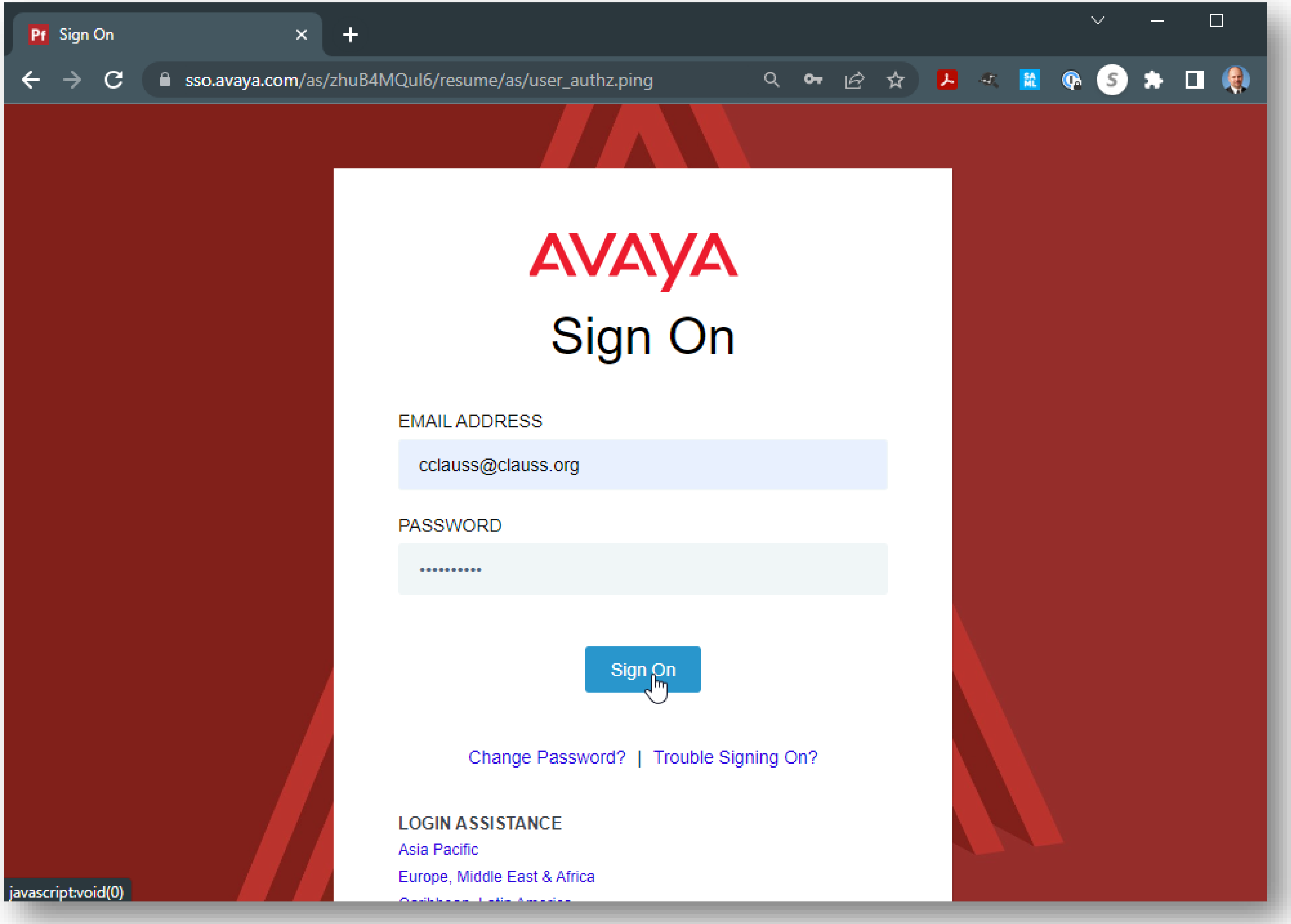
Single Sign On Expires in: 09:44

Browse to the below link and enter

User Code: QN79-TYCD

https://login-pa.avaya.com/activate

Press 'QR Code' for scan.



Sign On
sso.avaya.com/as/zhuB4MQul6/resume/as/user_authz.ping
AVAYA

Sign On

EMAIL ADDRESS

cclauss@clauss.org

PASSWORD

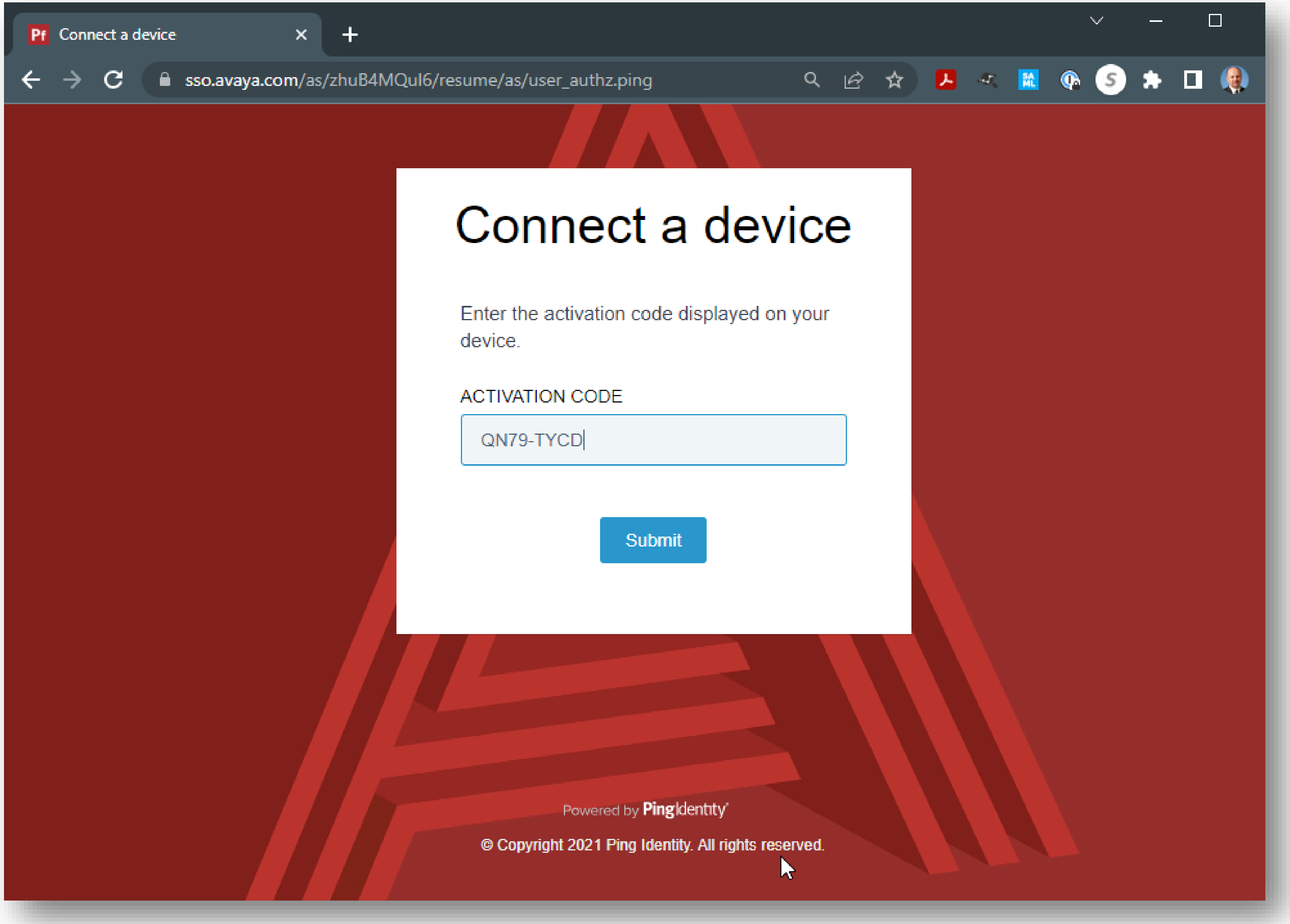
••••••••••

Sign On
Change Password? | Trouble Signing On?

LOGIN ASSISTANCE

Asia Pacific

Europe, Middle East & Africa



Connect a device

Enter the activation code displayed on your device.

ACTIVATION CODE

QN79-TYCD

Configuring Set SSO…

Edit 46xxsettings.txt

Need 1 line…

SET AADS_URL https://aads.customer.com/acs/resources/configurations

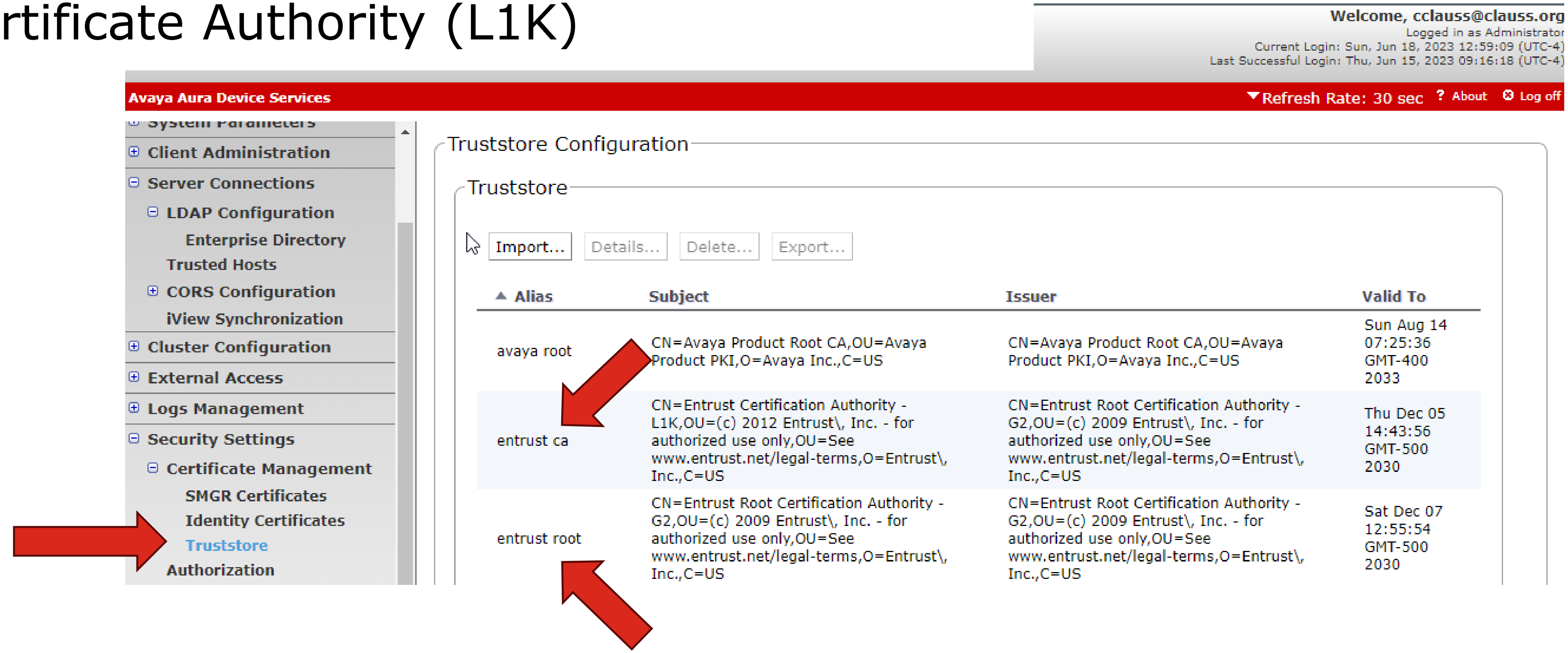
All other settings will be pulled from AADS when the station login completes.

On AADS, several configuration items…

Add root certs for Avaya SSO to AADS Trust Store

Entrust Root Certificate Authority (G2)

Entrust Certificate Authority (L1K)



Welcome, cclauss@clauss.org
Logged in as Administrator
Current Login: Sun, Jun 18, 2023 12:59:09 (UTC-4)
Last Successful Login: Thu, Jun 15, 2023 09:16:18 (UTC-4)

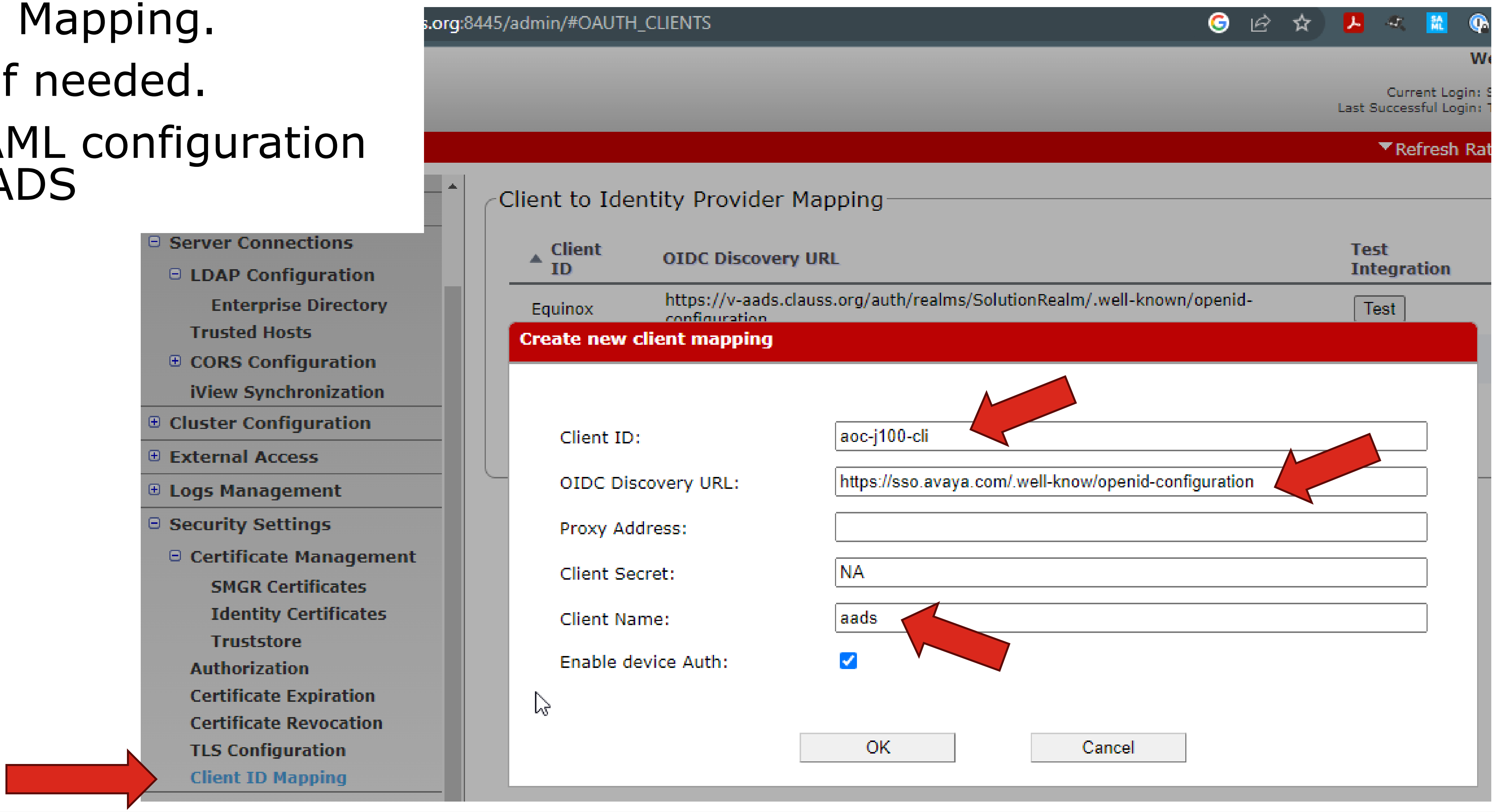
Alias	Subject	Issuer	Valid To
avaya root	CN=Avaya Product Root CA,OU=Avaya Product PKI,O=Avaya Inc.,C=US	CN=Avaya Product Root CA,OU=Avaya Product PKI,O=Avaya Inc.,C=US	Sun Aug 14 07:25:36 GMT-400 2033
entrust ca	CN=Entrust Certification Authority - L1K,OU=(c) 2012 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US	CN=Entrust Root Certification Authority - G2,OU=(c) 2009 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US	Thu Dec 05 14:43:56 GMT-500 2030
entrust root	CN=Entrust Root Certification Authority - G2,OU=(c) 2009 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US	CN=Entrust Root Certification Authority - G2,OU=(c) 2009 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US	Sat Dec 07 12:55:54 GMT-500 2030

On AADS, several configuration items…

Add Client ID Mapping.

Add a proxy if needed.

Note – No SAML configuration needed on AADS



Client to Identity Provider Mapping

Client ID	OIDC Discovery URL	Test Integration
Equinox	https://v-aads.clauss.org/auth/realms/SolutionRealm/.well-known/openid-configuration	Test

Create new client mapping

Client ID: aoc-j100-cli

OIDC Discovery URL: https://sso.avaya.com/.well-know/openid-configuration

Proxy Address:

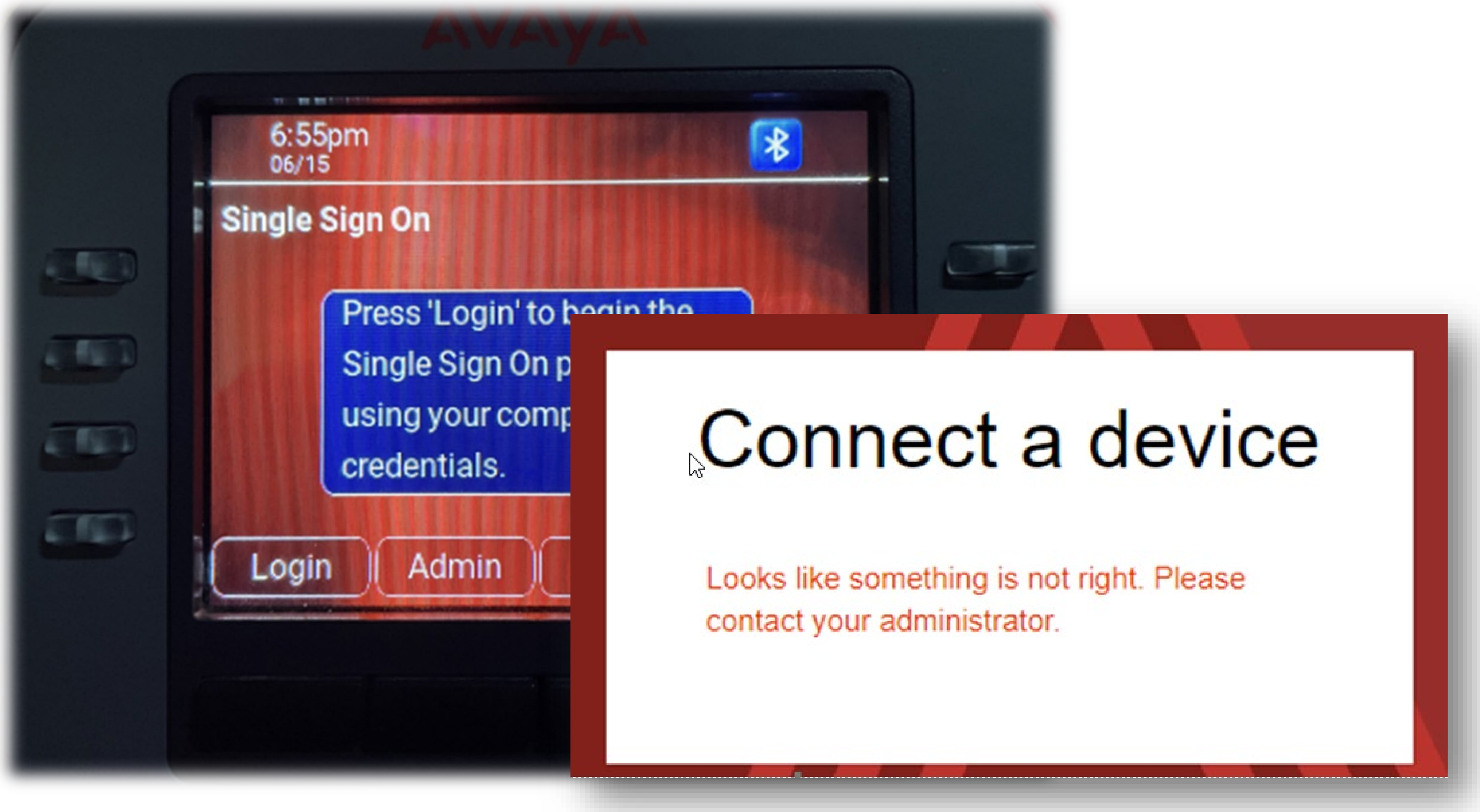
Client Secret: NA

Client Name: aads

Enable device Auth: ☑

Last but not least… – test login…

If the login process works, but comes up with a something is not right error, open a case with Avaya to fix the backend SSO to allow your domain.



Press 'Login' to begin the Single Sign On p using your comp credentials.

Connect a device

Looks like something is not right. Please contact your administrator.

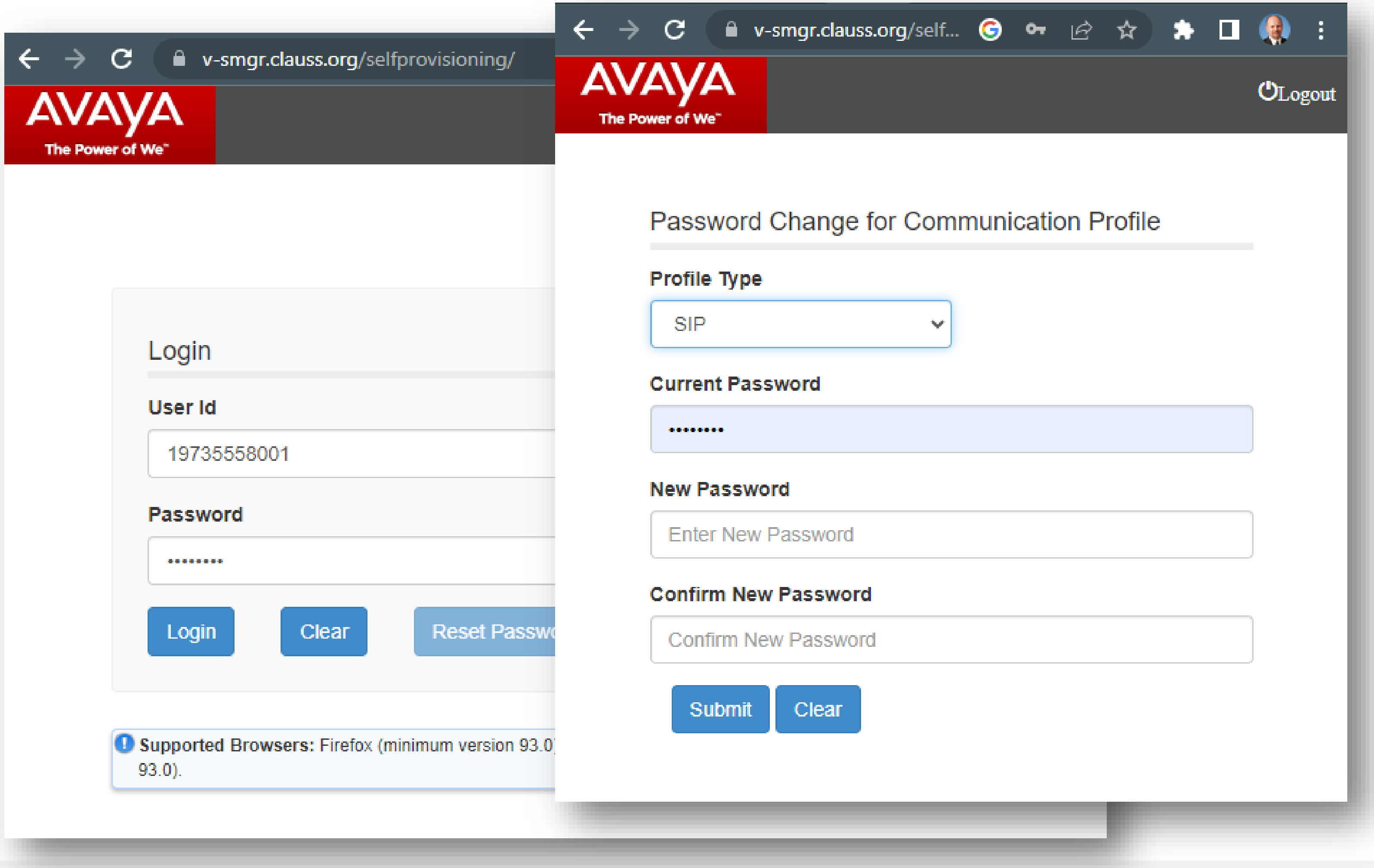
So back to password management...

Really Important!

- A phone or soft client always uses SIP station login and SIP station password to connect to Session Manager or SBC.
- An attacker can use this information to login a station, even if you are using other authentication techniques.
- The best way to protect against this – leverage the tools Avaya and C1 provide so that SIP station passwords can be impossible to guess.
- Never give a user a station password. Use single sign on.

System Manager self provisioning tool https://smgr/selfprovisioning

Allows basic services for a user to change station login and password and reset passwords.



v-smgr.clauss.org/selfprovisioning/

Login

User Id: 19735558001

Password: ••••••••

Supported Browsers: Firefox (minimum version 93.0) 93.0).

v-smgr.clauss.org/self...

Password Change for Communication Profile

Profile Type: SIP

Current Password: ••••••••

New Password: Enter New Password

Confirm New Password: Confirm New Password

System Manager for password management

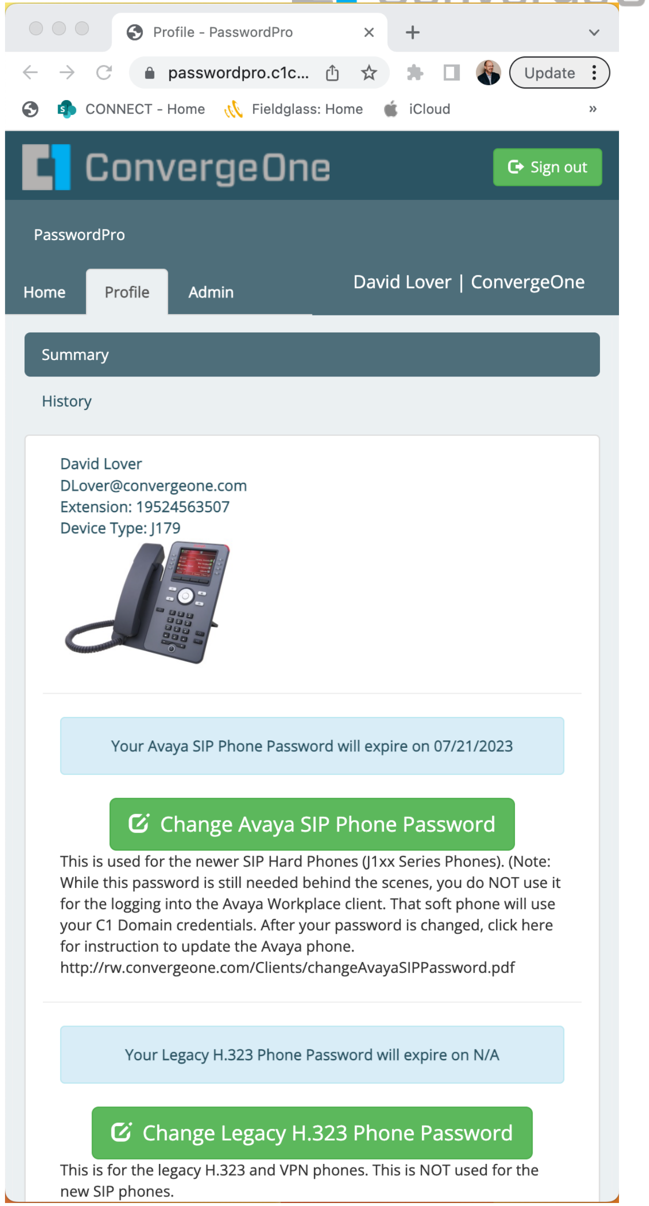
System Manager can provide user self service, but…

- URL runs on System Manager
  - Not good to place on public web
- Has limited capabilities
- Allows users to know their SIP station passwords
  - Bad as they can be set to poor password
- Problematic for single sign on integration.
- Another solution….

ConvergeOne

C1CX PasswordPro

- Simple and easy to use end-user portal
- Admin Dashboard provides at a glance view
- Flexible LDAP Configuration
- Securely connect to Communication Manager & System Manager via premises-based PasswordPro Gateway application
- Single or bulk-user actions
- Customizable expiration notification emails with Rich Text
- Cloud-based service
    - Regular updates, new features, and zero maintenance



David Lover
DLover@convergeone.com
Extension: 19524563507
Device Type: J179

Your Avaya SIP Phone Password will expire on 07/21/2023

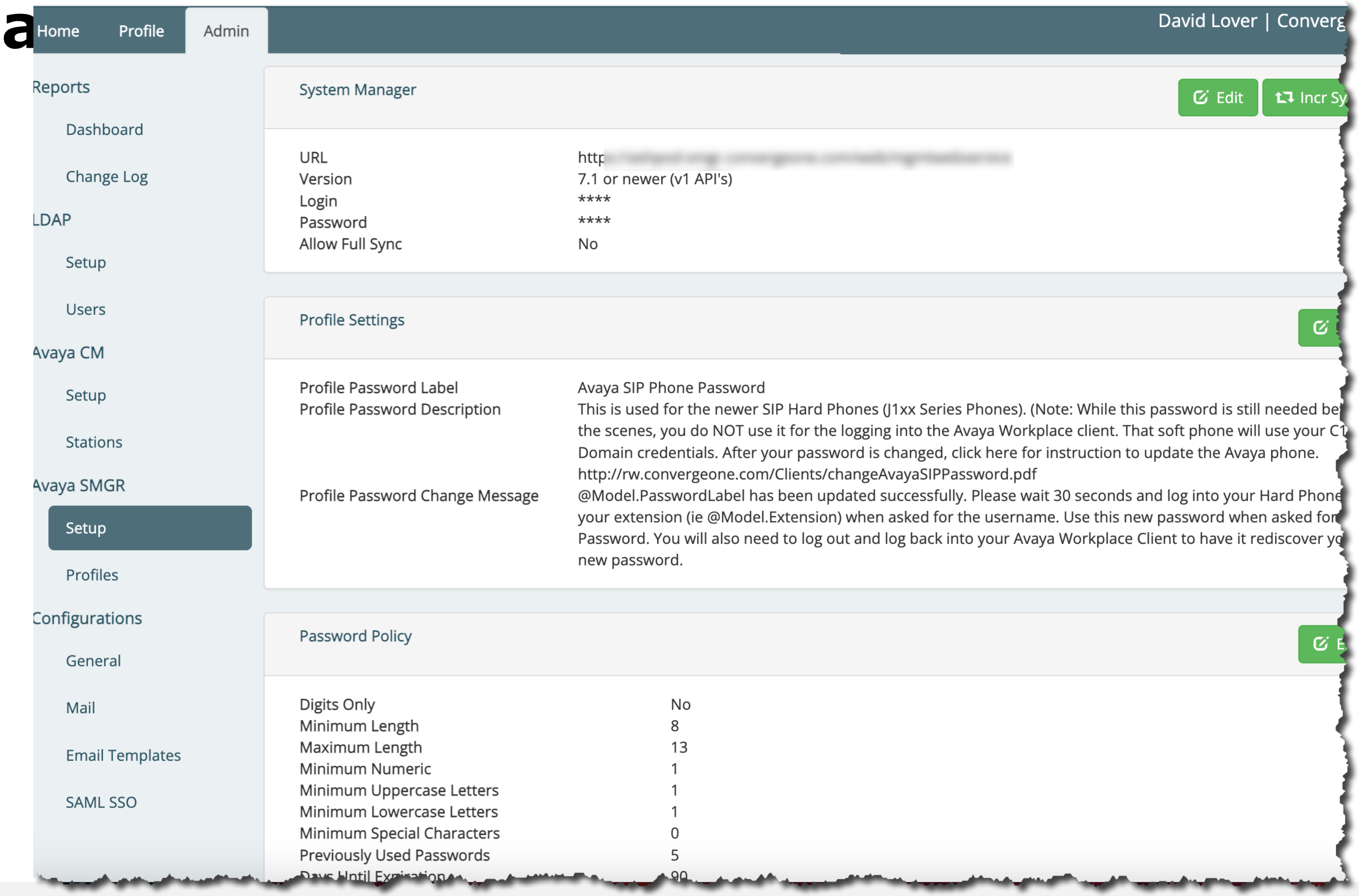
This is used for the newer SIP Hard Phones (J1xx Series Phones). (Note: While this password is still needed behind the scenes, you do NOT use it for the logging into the Avaya Workplace client. That soft phone will use your C1 Domain credentials. After your password is changed, click here for instruction to update the Avaya phone.
http://rw.convergeone.com/Clients/changeAvayaSIPPassword.pdf

Your Legacy H.323 Phone Password will expire on N/A

This is for the legacy H.323 and VPN phones. This is NOT used for the new SIP phones.

System Ma

PasswordPro accesses customer’s Avaya Aura System Manager via the premises based PasswordPro Gateway through HTTPS based API.



System Manager

URL	http[redacted]
Version	7.1 or newer (v1 API's)
Login	****
Password	****
Allow Full Sync	No

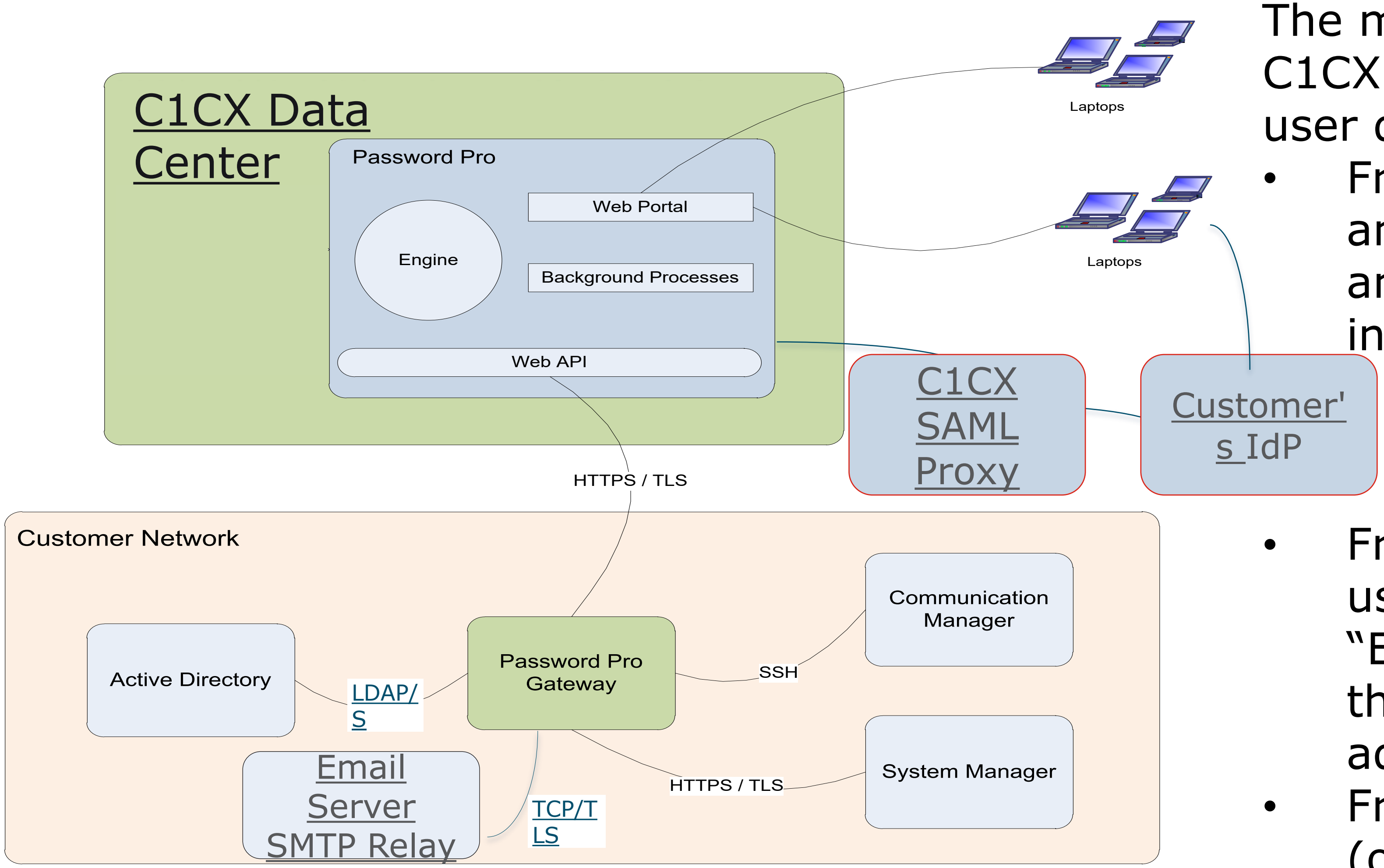
Profile Settings

Profile Password Label	Avaya SIP Phone Password
Profile Password Description	This is used for the newer SIP Hard Phones (J1xx Series Phones). (Note: While this password is still needed be the scenes, you do NOT use it for the logging into the Avaya Workplace client. That soft phone will use your C1 Domain credentials. After your password is changed, click here for instruction to update the Avaya phone. http://rw.convergeone.com/Clients/changeAvayaSIPPassword.pdf
Profile Password Change Message	@Model.PasswordLabel has been updated successfully. Please wait 30 seconds and log into your Hard Phone your extension (ie @Model.Extension) when asked for the username. Use this new password when asked for Password. You will also need to log out and log back into your Avaya Workplace Client to have it rediscover yo new password.

Password Policy

Digits Only	No
Minimum Length	8
Maximum Length	13
Minimum Numeric	1
Minimum Uppercase Letters	1
Minimum Lowercase Letters	1
Minimum Special Characters	0
Previously Used Passwords	5
Days Until Expiration	90

C1cx PasswordPro
High Level Architecture and Data Collection



The main PasswordPro servers in the C1CX Data Center will pull the following user data, via the on-prem gateway:

- From LDAP, it will pull the user's first and last name, the email address, and phone number (generally stored in the telephoneNumber field).
- From System Manager, it will pull the user's first and last name, their "E.164" communication address, and the "Avaya SIP" communication address.
- From Communication Manager (optional), it will pull the username and the station extension.

C1CX PasswordPro Benefits

- A critical component in protection of user's telephony accounts
- Enforces compliance to password complexity and expiration policies
- Provides 24x7 availability for password resets without the need for additional headcount
- Fully automate your password reset process and free up help-desk resources

Questions / Comments / Applause / Boos…

What's the best way for you to get help with password and single sign on?

Find the best partner – here at the show!
Please fill out your session survey! Session 1050

- Come ask us questions
- Call us – 888-777-7280
- Check us out online – www.convergeone.com
- Thanks for attending!

Dave Lover
dlover

Chris Clauss
cclauss

@convergeone.com

AVAYA ENGAGE®

BUILDING a WORLD ONE EXPERIENCE AT a time!

THANK YOU