

بسمه تعالی



سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

نکات امنیتی در مدیریت Adobe Connect

تاریخ نگارش فروردین ۱۳۹۹

مقدمه

با توجه به استفاده گسترده از پلتفرم آموزش و جلسات مجازی Adobe Connect در نظر گرفتن نکات امنیتی در خصوص مدیریت کاربران، محتوای به اشتراک گذاشته شده، اتاق‌های جلسات و کلاس‌های مجازی، حفظ امنیت در برقراری ارتباط و محتوای به اشتراک گذاشته شده ضروری است. بر همین اساس نکات امنیتی لازم همراه با تصاویر بخش‌های مختلف از Adobe Connect v10.6.1 در ادامه بیان شده‌اند.

سیاست‌های امنیتی لاگین و پسورد کاربران

- انقضای پسورد کاربر: بهتر است بسته به نوع استفاده از سرویس، مدت زمانی را به عنوان سقف زمان امکان استفاده از پسورد برای کاربران در نظر گرفت. این کار می‌تواند به دو دلیل انجام شود:
 - تغییر پسورد به صورت دوره‌ای جهت حفاظت از دسترسی
 - عدم امکان دسترسی و سوء استفاده از طریق حساب‌های بدون استفاده کاربرانی که دیگر نیازی به استفاده از این سرویس را ندارد
- اجبار به استفاده از حروف بزرگ، اعداد و کاراکترهای خاص
 - امکان اجبار به وجود یک کاراکتر خاص در پسورد وجود دارد
- تعیین حداقل و حداکثر طول پسورد: توصیه می‌شود حداقل طول پسورد ۸ کاراکتر تعیین شود. به صورت پیش فرض حداقل طول پسورد ۴ کاراکتر و حداکثر ۳۲ کاراکتر است
- اجبار به عدم امکان انتخاب پسورد تکراری: به صورت پیش فرض ۳ مورد در نظر گرفته شده است اما بسته به شرایط استفاده می‌توان عدد بزرگتری را نظر گرفت
- امکان قفل حساب کاربری در صورت ۵ بار تلاش ناموفق برای ورود: بسته به شرایط استفاده می‌توان حساب کاربری را برای ۵ دقیقه معلق کرد و یا گزینه قفل کامل حساب کاربری تا ریست پسورد توسط مدیر را انتخاب نمود
- اجبار به استفاده از کد مخصوص برای ورود به کلاس به جلسه

Home | Content | Meetings | Reports | Administration | My Profile

Account | Users and Groups | Audio Providers | Video Telephony Devices | Customization | Compliance and Control

[Users and Groups](#) | [Customize User Profile](#) | [Edit Login and Password Policies](#) | [Import](#) | [Cost Centers](#) | [SSO Settings](#)

The following set of login and password policies allow administrators to align Adobe Connect with their existing security policies across the Adobe Connect application.

Login Policy

Specify whether or not you wish to use the user's e-mail address as their default login, or another ID (such as network login or employee ID). Note: login credentials must be unique across all users.

Use e-mail address as the login: Yes No

Password Policies

Specify the following password management policies according to your existing best-practices.

Passwords expire after: days
(If blank, passwords do not expire.)

Passwords require the following character:
(Leave blank if not required.)

Passwords must contain a number: Yes No

Passwords must contain a capital letter: Yes No

Password must contain a special character: Yes No

Minimum password length:

Maximum password length:

Prevent reuse of old passwords

Number of old passwords tracked:

Suspend user login after five (5) consecutive incorrect passwords

Suspend user login for five (5) minutes

Suspend user login until password is reset by an Administrator

Room Passcode

Enable Meeting Hosts to enforce passcode for room access

Force passcode for room access

Copyright © 2019 Adobe. All rights reserved.

حفاظت از امنیت کلاس‌ها و جلسات

این تنظیمات برای هر کلاس یا جلسه به صورت جداگانه قابل تعیین است:

- ورود به کلاس و جلسه با حساب کاربری و عدم امکان ورود به عنوان کاربر مهمان.
- کد مخصوص اجباری جهت ورود کاربر را می‌توان به صورت پیچیده تعیین نمود.

Meeting Information

Name: *

Summary:
(max length=4000 characters)

Start Time: 23 ▾ March ▾ 2020 ▾ 01:00 PM ▾

Duration: 00:15 ▾ hours:minutes

Language: * English ▾

- Access:**
- Only registered users may enter the room (guest access is blocked)
 - Only registered users and account members may enter the room
 - Only registered users and accepted guests may enter the room
 - Anyone who has the URL for the meeting can enter the room

Required Passcode Protection (in addition to the Access settings above)

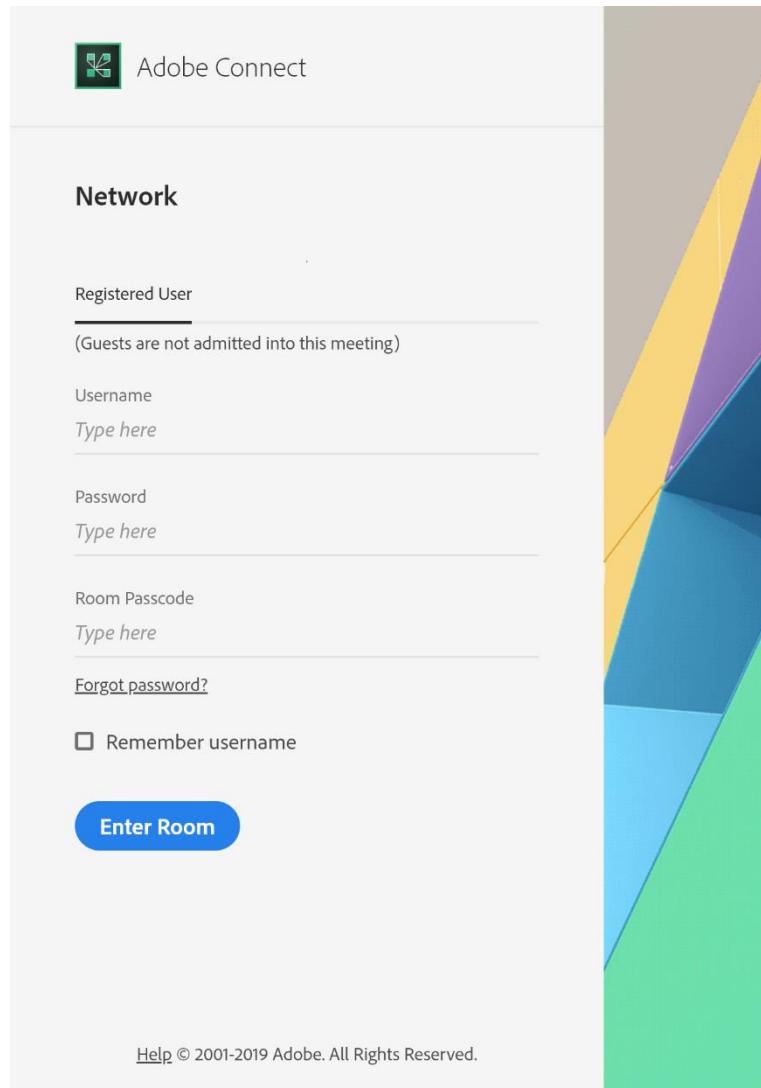
Users must enter room passcode

HTML Client: Enable HTML client for participants

["Learn more about HTML client capabilities and limitations."](#)

(This setting is applicable only if Administrator has NOT enabled 'force launch session in Adobe Connect application' under Advanced Settings. When this setting is enabled, all user sessions for Adobe Connect will be launched in an HTML Client for participants.)

با تنظیمات ذکر شده در بالا، صفحه ورود کاربر به صورت زیر خواهد بود:



Adobe Connect

Network

Registered User
(Guests are not admitted into this meeting)

Username
Type here

Password
Type here

Room Passcode
Type here

[Forgot password?](#)

Remember username

[Enter Room](#)

[Help](#) © 2001-2019 Adobe. All Rights Reserved.

حفاظت از محتوای به اشتراک گذاشته شده

در حفاظت از محتوای به اشتراک گذاشته شده، بسته به شرایط، امکان مشاهده کاربران عضو و یا تعیین انتخابی نوع مجوز دسترسی وجود دارد. انواع مجوزهای قابل تخصیص به کاربران گوناگون شامل `publish`، `manage`، `view` و `denied` است.

ADOBE® CONNECT™

Help | Logout: Sarah :D

Home | Content | Meetings | Reports | Administration | My Profile | Title & Description Search...

Shared Content | User Content | Forced Recordings

Shared Content

Content List | Edit Information | Set Permissions

Reset To Parent

Allow viewing:

- Public
- All Account Members
- Custom

Available Users and Groups	
Search	
Authors	System Group
Meeting Hosts	System Group
Network	Administrator Group
Security	Administrator Group

Add

Remove

Current Permissions For Shared Content		
Search		
test test	Denied	test@ubcert.ir
Sarah :D	Manage	Sarah@ubcert.ir
APA UB	Publish	apa@ubcert.ir
Mahsa :)	View	Mahsa@ubcert.ir

امکان تعیین و استفاده از محدودیت‌هایی خاص برای کاربران مدیر

- در صورت انتخاب تعدادی کاربر به عنوان مدیر، می‌توان بسته به نیاز تعدادی را عضو گروه Administrators-Limited نمود و اختیارات لازم را برای این گروه تعیین کرد:

Home | Content | Meetings | Reports | Administration | My Profile | Title & Description Search...

Account | Users and Groups | Audio Providers | Video Telephony Devices | Customization | Compliance and Control | Administration Dashboard

Users and Groups | Customize User Profile | Edit Login and Password Policies | Import | Cost Centers | SSO Settings

Users and Groups	
Search	
New User New Group Manage Guests View Guests Delete Info Training Groups <input type="checkbox"/> Hide	
Administrators	System Group
Administrators - Limited	System Group
Authors	System Group
Meeting Hosts	System Group

Permissions of Limited Administrators

Users and Groups

- View User Data
 - Reset Password
 - Add users and groups using Web Interface
 - Modify current users and groups
 - Add users and groups using CSV import
 - Delete users and groups
- Modify user profile fields
- Change the login and password policies
- Cost Centers

Account Management

- Edit account information
- Receive Notifications about Account Capacity and Expiration

Customization

- Customization of Account Colors and Images

Reports

- View disk usage and reports
- View System Usage Reports

Compliance and Control

- Compliance

Permissions

- Set content, meeting and seminar permissions
- Allow Limited Administrators to access meeting, content and seminar folders

اجبار به استفاده از SSL

Home | Content | Meetings | Reports | Administration | My Profile

Account | Users and Groups | Audio Providers | Video Telephony Devices | Customization | Compliance and Control | Administration Dashboard

Account Summary | Edit Information | Disk Usage | Reports | Notifications | Session Settings | More Settings

Security Settings

Configure X-Frames/Content-Security-Policy Options

Allow From / Ancestors:

The page can only be displayed in a frame on the same origin as the page itself ▾

Allow From URI / Ancestor Source:

Use the following (different) ALLOW FROM / Ancestor settings for Event modules

Requires SSL Connection (RTMPS)

Enable Enhanced Security

- Force Web Services APIs to use secure (HTTPS) connection
- Generate new session identifier after successful login

It is strongly recommended to check Enhanced Security option unless you have integrations that use session identifier before logging in or use unsecured Web Services APIs. Make sure to update such integrations with session identifier after logging in and use secured Web Services APIs so that the integrations keep working after this option is removed in the near future and enhanced security is enabled by default.

Save

Cancel

Copyright © 2019 Adobe. All rights reserved.