Advanced Configuration

Administration Guide

Active Learning Platform

October 2015

Table of Contents

Configuring Authentication

User authentication can be very basic, having users enter their credentials on the main Active Learning Platform login screen.

Alternately, you can configure single sign-on through PingOne or have users access Active Learning Platform content through your configured LMS.

PingOne

PingOne is a cloud-based identity management system used by the Active Learning Platform for its external authentication solution. There are three aspects to PingOne configuration:

- Setting up a PingOne account
- Configuring the IdP system for use with PingOne
- Enabling PingOne communication in ALP

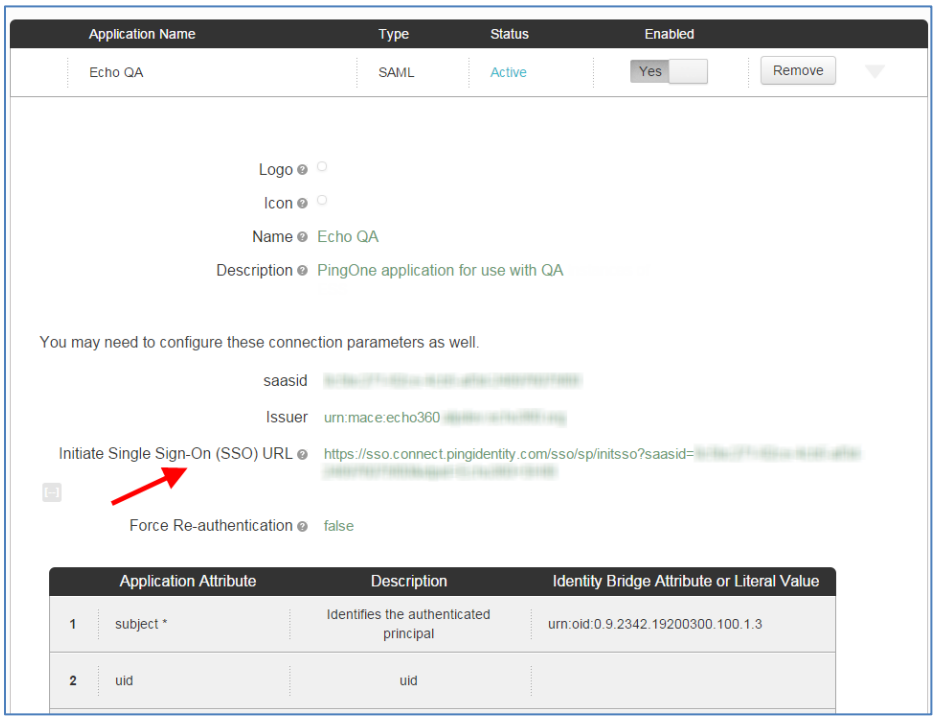
These three aspects are addressed in the topic Configuring PingOne Authentication.

Beyond the initial setup, the **Admin workflow for establishing SSO** (single sign-on) for users through PingOne is as follows:

1. Configure PingOne based on the user authentication method you're already using (see link above).
2. Add users into ALP, assigning them to sections as appropriate. BE SURE the email address in ALP ***exactly matches*** the email address in your system, and is unique to each user.
3. Distribute or post the PingOne SSO URL for your ALP integration, shown in the below figure.
   This is the link users will click to enter ALP using their institution credentials. It can be found on the Application Details page of your PingOne account.

   Alternately, users can navigate to the EchoALP Website (echo360.org) and click Login with Student ID to use their institution's credentials.

TIP: If you post this link in a location where a user has already logged into your network (the institution's student portal, or other secured site) the URL will pass them directly through to ALP, as your system has already authenticated them.



IMPORTANT NOTE: Users will receive email inviting them to register for the Echo360 system, and notifying them of their enrollment in sections/courses. **Users can ignore these email**.
However, if they choose to complete the ALP registration process, it does no harm. They ***must*** be sure the email and password they provide matches the institution information. After that, their ALP registration simply allows them to access ALP directly via the ALP website, authenticating through ALP instead of the institution's network. They can still also authenticate through the institution network by using the SSO URL.

LMS

If you are using a Learning Management System (LMS), Active Learning Platform allows you to configure integration with the LMS for course integration and assessment purposes.

Because the LMS and Active Learning Platform establish authenticated communication between them, students who log into the LMS automatically receive the appropriate Active Learning Platform content through the LMS interface, without having to log in again.

For information on configuring integration between Active Learning Platform and your LMS, see Configuring the Active Learning Platform with an LMS.

Configuring PingOne Authentication

PingOne is a cloud-based identity management system that provides secure authentication and integrated single sign-on (SSO) for the Active Learning Platform.

Before You Begin

The PingOne integration offers the following single sign-on methods for customers:

- Active Directory (requires IIS and AD Connect software from PingOne)
- SAML Identity Providers
- GoogleApps

Echo360 recommends that you select which option to implement *in advance* of performing the procedures on this page. To use Active Directory, understand that it requires software installation as noted above, and that the system must reside outside the firewall.

Workflow

The following workflow, and the instructions on this page, identify the steps necessary to set PingOne up to provide SSO services to ALP through your network. For information on the subsequent steps needed to add and configure users to access ALP content, see Configuring Authentication.

1. Register for a PingOne one account.
2. Register the Active Learning Platform configuration with PingOne.
3. Select the desired authentication method.
4. Configure the authentication method in PingOne, and exchange the required metadata with the authentication source.
5. Create or import the desired user accounts into the Active Learning Platform.

When a user logs in through the Active Learning Platform, the authentication request is sent through PingOne to the selected authentication system, then back to the Active Learning Platform for access.

Creating PingOne account credentials

You must register in PingOne first and create your account credentials, then enable PingOne in the Active Learning Platform.

To register PingOne

1. Go to **https://admin.pingone.com/web-portal/register**.

2. Under Account Type, select **PingOne for Enterprise**.
3. Under Profile setup, complete all details.

   NOTE: Your email address will become your username.

4. In the Registration key field, enter **PingForEcho360_FP**.
5. Enter and confirm your account password.
6. Click **Register**.

After registering, you receive a confirmation email at the address entered on the form. Click the link in the email to complete the account registration process.

Configure authentication method in PingOne

PingOne needs to know which authentication method you want to use, and then you must configure that authentication method through PingOne.

NOTE: The procedures below are provided as guidelines to the PingOne authentication setup process. Refer to the PingOne documentation for additional details, or contact PingOne support if you need further assistance.

Configuring SAML authentication

Configuring SAML authentication involves sharing identity key and certification information between PingOne and a SAML identity provider (IdP), allowing the two to communicate securely and provide appropriate user authentication.

To configure SAML authentication

1. Log in to PingOne.
2. Select the **Setup** tab.
3. Select appropriate **SAML identity bridge**.
4. Click **View/Edit**.
5. Select to **Download the PingOne metadata** to exchange with your identity provider (IdP). This tells PingOne to generate all of the necessary field parameters, then generates a downloadable file for you to upload into the IdP.
6. Once you have uploaded the PingOne metadata and configured the IdP, you must enter the provider's configuration information back into PingOne. You have the following choices:
   - **Upload a metadata file** obtained from your identity provider into PingOne. This populates the PingOne configuration with the proper information from the provider.

- **Manually enter the appropriate field information**. You may have received this data from the identity provider, or you may need to re-type the data into the corresponding fields for the identity provider.

7. When finished, click **Save Configuration**.

Configuring active directory (AD) authentication

Using Active Directory authentication with PingOne requires that you have IIS installed and configured and AD Connect installed and configured.

PingOne provides a download of the AD Connect installer to user if needed. AD Connect requirements include:

- One of the following platforms:
  - Microsoft Windows Server® 2012 with IIS 8.0 (32-bit/64-bit)
  - Microsoft Windows Server 2008 R2 with IIS 7.5 (32-bit/64-bit)
  - Microsoft Windows Server 2008 with IIS 7.0 (32-bit/64-bit)
- Administrator privileges on the Windows Server IIS host.
- The Windows Server IIS host must reside in an Active Directory domain, but for security reasons, must not be a domain controller (DC).
- Port 443 (HTTPS) must be open to your organization.
- Time synchronization must be set up on the Windows Server IIS host.
- Microsoft Net 4.0 Framework installed. The framework installation file is packaged with the AD Connect distribution.
- IIS Server role service installed.
- Windows Authentication role service installed for IIS.

To install and configure IIS

NOTE: The installation instructions linked below are for Windows 2008 server with IIS 7.0. If you are using a different operating version, please find the Technet articles that relate to your specific supported environment.

1. **Install and Configure IIS:** http://technet.microsoft.com/en-us/library/cc771209(WS.10).aspx
2. **Create a Certificate Request:** http://technet.microsoft.com/en-us/library/cc732906(v=ws.10).aspx
3. **Complete the Certificate Request:** http://technet.microsoft.com/en-us/library/cc771816(v=ws.10).aspx
4. **Import an existing certificate:** http://technet.microsoft.com/en-us/library/cc732785(v=ws.10).aspx
5. **Add HTTPS protocol and port 443 binding to IIS:** By default, IIS may not be configured to support the HTTPS protocol. To implement HTTPS on 443, follow

these instructions to create the binding: http://technet.microsoft.com/en-us/library/cc771438(v=ws.10).aspx

To install and configure AD Connect

1. Log on to your PingOne account.
2. Download the AD Connect software.
3. Extract the zipped file and launch the installation package by double-clicking the "run-as-administrator.cmd" file in the extracted folder.
4. Click **Next** to proceed with the installation.
5. Select **Full with IIS** to install the full AD connect package in IIS.
6. Click **Next**. The AD Connect installer checks that the prerequisites are in place. If all prerequisites are in place, the installation proceeds to the activation tab.
7. The installer checks whether the .Net 4.0 framework is installed. If the .Net 4.0 framework isn't installed, you can install it using the .Net 4.0 distribution located in the AD Connect installation directory. When the .Net 4.0 framework installation is complete, return to this AD Connect screen, and click **Verify Install**.
8. Click **Next**. The installer then checks whether the IIS Server role is installed. If it isn't, install this role service using Windows Server Manager, return to this dialog and click Verify Install to proceed.
9. Click **Next**. The installer then checks whether the Windows Authentication role is installed for IIS. If it isn't, install this role service for IIS using Windows Server Manager, then return to this screen and click Verify Install to proceed.
10. Click **Next**. The AD Connect activation screen appears. The Organization ID and the Product Key values are on the setup screen in PingOne.
11. In the AD Connect activation screen, enter the Organization ID and Product Key, then click **Activate** and **Next**.

    NOTE: If the product is activated properly, you will see the following acknowledgement: "AD Connect has been activated"

12. Select the IIS web site that you want the AD Connect software installed to.
13. Enter the installation location for the AD connect software and click **Next**.
14. Click **Install** to complete the installation process of AD Connect.
15. Click **Finish** to complete the installation process.

Enabling PingOne authentication in the Active Learning Platform

To enable PingOne

1. Log on as administrator.
2. Click the Settings icon and select **Configurations** from the list.

3. Select **PingOne Configuration**.
4. In the **Identify Provider ID** field, enter a descriptive value for your identity provider.
5. Click **CONNECT TO PINGONE**.
6. A pop-up box appears on the screen with a checkbox. Click a check in this **Enable Single-Sign on** checkbox.
7. A link to PingOne appears below the checkbox. Click this link.
8. Log in to PingOne.
9. Complete the PingOne application configuration by adding the proper **identity bridge attribute** for the application.
10. **Continue to Next Step**, then add your institution **Logo**, **Icon**, **Name** and **Description** as needed.
11. When finished click **Save and Publish**.

Once PingOne is configured for Active Learning Platform, users can select to Log in with their school ID. See Configuring Authentication for the process steps needed to allow users to access ALP content through their institutional login.

Configuring Closed Captioning

Closed captioning is the process of transcribing audio/video from captured material and presenting the transcribed text in a readable format for end users during playback. Originally developed as an aid for the hearing-impaired, it is also useful for reinforcing lesson materials for all students.

The capture material (audio/video) is sent to a transcription and captioning service and then retrieved by the platform to integrate with the capture material. Echo360 uses Cielo24 to provide captioning service for the Active Learning Platform.

Obtain Cielo24 credentials

Cielo24 provides a variety of services to Active Learning Platform customers. For these services to provide closed captioning for your content, you must establish an account with Cielo24.

To obtain Cielo24 account credentials

1. Send an email to echo360@cielo24.com. The message should include:
    - Company or institution name
    - Contact name
    - Contact email address
    - Phone number
2. Cielo24 will process the request for a trial account and contact you with details.

Be sure to discuss your captioning turnaround time and accuracy requirements with Cielo24 when establishing your account. Faster turnaround times with higher accuracy will affect costs.

Configure closed captioning in the Active Learning Platform

Once an account is established with Cielo24, they will provide the necessary items for configuring closed captioning in the Active Learning Platform. This configuration tells the Active Learning Platform to submit the captures you identify to Cielo24, and provides the necessary account information and service requirements for the captioning.

To configure closed captioning in the Active Learning Platform

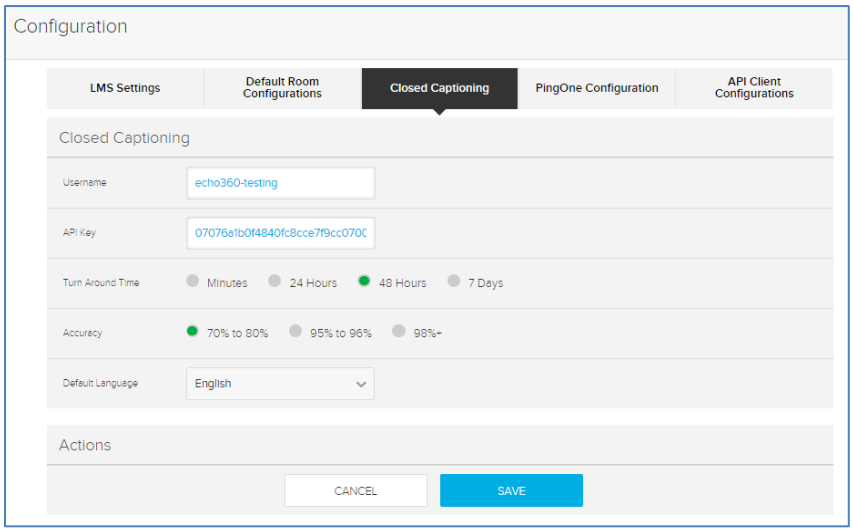
1. Log on as administrator.
2. Click the **Settings** icon and select **Configurations** from the list.
3. Select **Closed Captioning**.
4. Enter the following information:

- **Username** - This is your Cielo24 account username.
- **API Key** - This key is provided by Cielo24 to provide secure API communication between the Active Learning Platform and their system.
- **Turn Around Time** - Identify how quickly you require the captioning to be completed after submission to Cielo24.
- **Accuracy** - Identify the required minimum accuracy of the captioning.

NOTE: Selecting a Turn Around time of less than 24 Hours limits the Accuracy selections available. For example, if you want a turnaround time of Minutes, the only Accuracy selection available is 70% - 80%.

- **Default Language** - Select the language for the caption text.

5. When finished, click **SAVE**.



Apply captioning to a capture

Closed captioning can be applied to individual captures or to all captures in a scheduled series, such as for a section. Closed Captioning is enabled through the capture options.

To apply captioning to scheduled section captures

1. From the main menu, click **COURSES**.
2. Find the course containing the sections with captures you want to caption.
3. Expand the course to show the sections.
4. Click the **calendar** icon to view the current capture schedule for the section.
5. Expand the **Options** section of the capture configuration dialog box.
6. Enable the **Closed Captioning** slider.

NOTE: This option will not appear if closed captioning is not configured for your institution.

7. Click **SAVE**.

To apply captioning to an individual capture

1. From the main menu, click **CAPTURES**.
2. Find the capture you want to caption and hover over it to show the menu arrow in the upper-right corner of the capture block.
3. Select **Edit**.
4. Expand the **Options** section of the capture configuration dialog box.
5. Enable the **Closed Captioning** slider.

   NOTE: This option will not appear if closed captioning is not configured for your institution.

6. Click **SAVE**.

Device Communication in an Active Learning Platform Environment

The information on this page addresses the communication methods used by Echo360 capture devices. These devices need to communicate externally with the Active Learning Platform as well as internally to other servers via the local area network (LAN).

NOTE: The information on this page applies to ***all*** capture devices (exceptions noted):
-- First generation Capture Appliance
-- SafeCapture HD (SCHD)
-- Classroom Capture (DHCP and NTP do not apply; handled by computer OS)
-- Personal Capture (DHCP and NTP do not apply; handled by computer OS)

External Device Communication and Firewall Port Requirements

Capture devices require only two external communication ports; one to the Active Learning Platform server, and one to the default network time server.

If you use an internal time server, the external NTP server connection is not needed.

Port Description	Default Port	Port Direction	Protocol
HTTPS (Secure Hypertext Transfer Protocol) *Outbound required to Active Learning Platform server*	443	outbound	TCP
NTP (Network Time Protocol) to ***.pool.ntp.org** (default ALP time server) *(If you use an internal time server, this does not apply.)*	123	outbound	UDP
RTP (Real-time Transport Protocol) to Active Learning Streaming Servers *(Applies only to LIVE streaming; see Port Configuration for LIVE Streaming for details.)*	49152-65535	outbound	UDP

Internal Network Device Communication Ports and Methods

Device communications through the internal network or LAN are defined in the below table.

Port Description	Default Port	Port Direction	Protocol
DHCP (Dynamic Host Configuration Protocol) *(Appliance may be set to static addressing later but requires DHCP initially.)*	67, 68	both	UDP
DNS (Domain Name Service)	53	outbound	UDP
HTTPS (Secure Hypertext Transfer Protocol) *(Optional, for device web interface access, including ad-hoc capture UI)*	443	inbound	TCP
HTTP (Hypertext Transfer Protocol) *(Optional, for device web interface access, including ad-hoc capture UI)*	80	inbound	TCP
RTMP (Real-time Messaging Protocol) to users *(For LIVE streaming to users)*	80	inbound	TCP
Internal NTP Time Server (if used) *(If you use the default Echo NTP server, see table in section above.)*	123	outbound	UDP

Configuration Requirements for Live Streaming

Live streaming simply means that users can remotely watch a class as it is happening. For Live streamed classes, the input being captured by the capture device is webcast in real-time to those users viewing the classroom through ALP.

For live streaming to work properly, there are a few configuration requirements. Don't worry; they're pretty straightforward.

Live streaming is only available for section captures

When you schedule a capture for a *section*, the Options available include a **Live stream** toggle. When you try to add or schedule a capture outside of a section (Captures page > Add Capture), you don't get this option.

Why?

Well, it has to do with the fact that users (students) can only access media that exists in a class. The view it by clicking GO TO CLASSROOM. So if you want people to view LIVE streams, it has to go into a class, in a section.

Remember also that to get into a section, you have to be assigned to the section. Meaning a user who isn't assigned to the section can't see the classes for the section, so they can't GO TO CLASSROOM.

So, while we could let you configure a live stream for a capture that isn't associated with a section, how would users get there? How would they find the "GO TO CLASSROOM" button for the live class?

What you CAN do, however, is configure a dedicated course and section for holding special events or other happenings that you want to stream live to a larger institutional audience. Then assign all of the users you want to that section.

Live streaming requires an SCHD

Only classes that occur in rooms where a SafeCapture HD (SCHD) is configured to capture can be used for live streaming. Keep this in mind when you are scheduling captures for the section. Be sure to select a room that uses an SCHD for capture.

Check and configure outbound port communications

Live streaming is provided through hosted streaming (Wowza) servers. These servers receive the separate input streams from the SCHD devices via RTP (real-time transfer protocol), then deliver the consolidated media stream back to users.

In order to make this work, the SCHD devices need to be able to communicate with the streaming servers through the appropriate ports, and those ports need to be configured, via wildcard DNS entries, to point to the cloud-based Wowza servers.

For details on this, see Port Configuration for LIVE Streaming.

Port Configuration for Live Streaming

Live streaming for the Active Learning Platform (ALP) is provided through a carefully orchestrated combination of:

- Dynamically scaled hosted streaming servers that support live streaming
- An SCHD appliance that sends live video and audio feeds to a hosted streaming server
- Users that stream a class live from a hosted streaming server via the ALP classroom in their browser

What do I need to do?

Your network must be configured to send and receive streams to and from the hosted streaming servers using the ports and protocols outlined below.

- For *sending* live video streams each **SCHD** requires the outbound **UDP** port range **64936-65535** be open to the hosted streaming servers using the Real-time Transport Protocol (**RTP**).
- For *playback*, ALP supports Flash on desktop browsers and Safari on iOS for receiving live video streams in the classroom environment.
    - For desktop playback, Flash must be able to make **outbound** requests to the hosted streaming servers and receive the **inbound** stream via the Real Time Messaging Protocol (**RTMP**) using **TCP** over port **80**.
    - For Safari on iOS the HTTP Live Streaming (**HLS**) protocol is used to make both the outbound requests to the hosted streaming server and for receiving the inbound stream. All of these outbound and inbound communications use **HTTP TCP** over port **80**.

Important Details

- The IP addresses used by the hosted streaming servers fluctuate, so a * firewall rule is required.
- Proxy servers are **not** supported for:
    - The **SCHD** sending **RTP** via **UDP outbound** to the hosted streaming server.
    - **Flash** (for **desktop** browser playback) making **outbound** requests and receiving the **inbound** live stream from the hosted streaming server using **RTMP**.
- Safari on iOS ***does support*** proxy servers, as these requests use HTTP direct from the browser.

Why?

- Live streaming in ALP requires an SCHD to send its streams to the exact same hosted streaming server as the users connect to for that particular live streamed class coming from that SCHD.
- Because the SCHD and users for a live class must connect to the exact same hosted streaming server it is not possible to load balance behind a single IP.
- The Active Learning Platform is a multi-tenant SaaS platform; streaming servers are scaled up and down dynamically based on demand, spreading client load across servers.
- Dynamically scaling these servers prevents the need to specify a single or small set of IP addresses for all streaming SCHDs to send live streams to and subsequently for all those users to request live streams from.