Authentication Integration

VoiceThread provides multiple authentication frameworks allowing your organization to choose the optimal method to implement. This document details the various available authentication implementation methods and includes additional guidelines for each implementation type. The VoiceThread Integration Team is available to collaborate and work with your User and Identity Management department to set up and integrate with these services. The contact email address for our team is: **integration@voicethread.com.**

Please note that our Integration package is included for (K-12) District and (Higher-Ed) Department+ or Site-Wide deployments of VoiceThread and is available as an additional service for all other deployments.

VOICETHREAD AUTHENTICATION AT A GLANCE:

This document addresses the following topics:

Users And Data Security

VoiceThread takes the security of our users and their data quite seriously. Therefore, we require that all authentication information be transmitted over encrypted protocols. We do not support the transport of user information over any communication channel that is not encrypted and require that any service that utilizes direct user authentication (Active Directory and LDAP) must use a security certificate signed by a trusted Certificate Authority (CA). If you need help setting up your system to use a properly signed CA, please contact the VoiceThread Integration Team. VoiceThread does not store any user-credential information and immediately discards direct user authentication credentials upon authentication requests to VoiceThread.

VoiceThread External Authentication

VoiceThread highly recommends that medium and large organizations utilize an External Authentication implementation. This method of authentication is scalable, managed using your existing authentication infrastructure, and provides granular control for end-user authorization. There are several authentication implementations, and VoiceThread works with most standards-based solutions. However, for custom in-house solutions, VoiceThread also provides a method to authenticate users with our application programmers interface (API). Since it is important to select the best authentication implementation for your organization's current system and goals for using VoiceThread, we encourage your implementation team to carefully review this documentation and to contact VoiceThread support regarding any issues not addressed. Please note: The use of external authentication requires a valid VoiceThread-Organizational license. Every authentication implementation presented within this documentation is currently in active use by one or more VoiceThread partners.

Microsoft Windows Active Directory

Microsoft Windows Active Directory provides a centralized user and group management system via the Active Directory User and Computer snap-in module. Administrators can add users, update details, and change passwords via this interface. The end-user will be able to use the same credentials on VoiceThread that they use to authenticate with services that are provided through your Microsoft network. This means that your users only have to remember one user name and password. The diagram below shows the workflow for using Microsoft Active Directory authentication within VoiceThread:

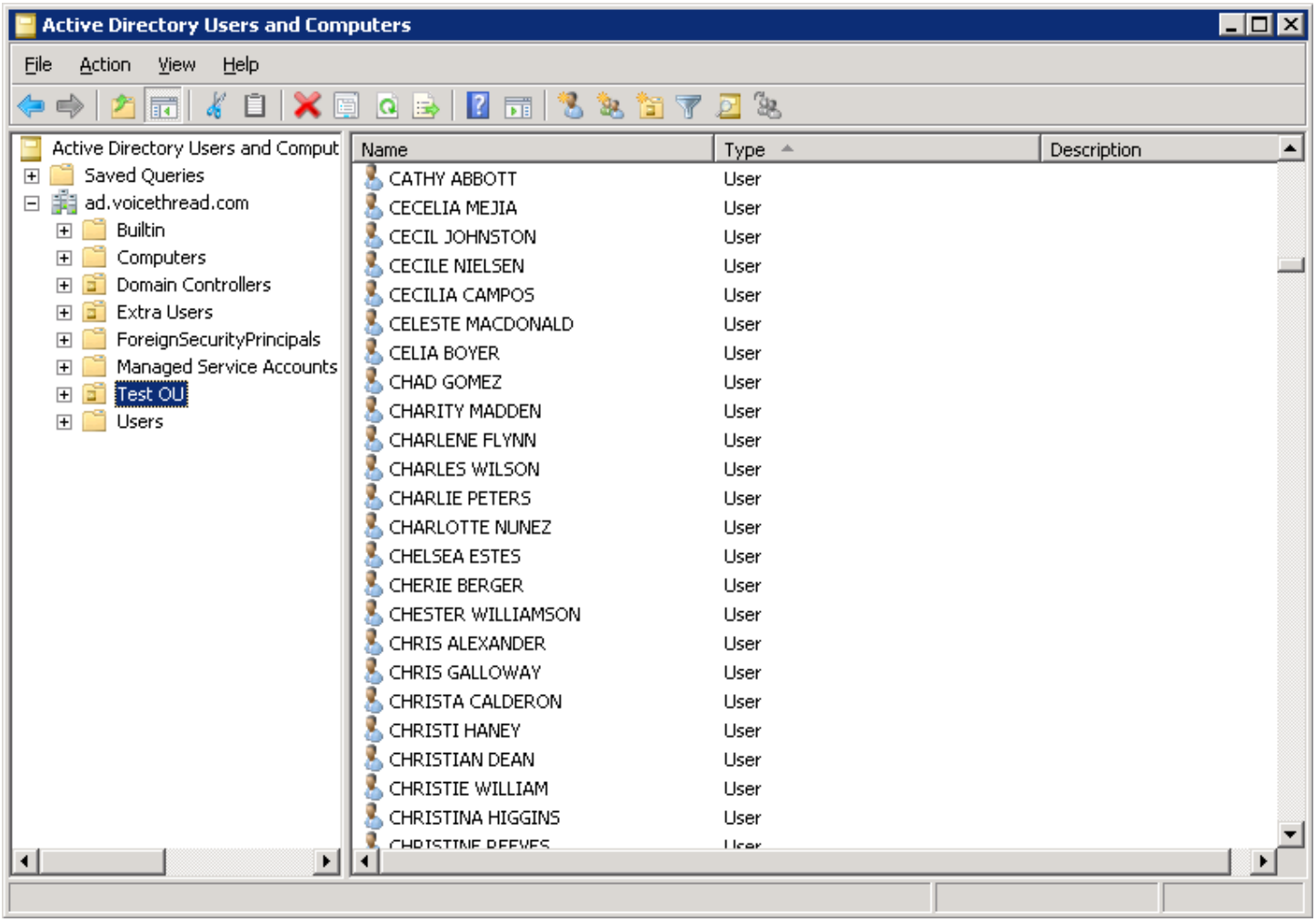
Figure 1: Active Directory/ldap Authentication Workflow

1. A user enters in their credentials to authenticate with VoiceThread. These are the same credentials the user would use to access a service from within their local network.
2. VoiceThread securely transmits these credentials to your Active Directory server via an encrypted connection. As soon as the user credentials are transmitted, VoiceThread immediately discards any and all credential information and awaits a response from your Active Directory server.
3. If authentication is successful, VoiceThread performs a search of the organizational structure to obtain the requested user information (such as their name and email address).
4. If group authorization is used, VoiceThread confirms that the user is a member of an allowed group/organizational unit or is not a member of a restricted group/organizational unit. For new users, VoiceThread creates a new account. For existing users, VoiceThread signs them into their existing account.

VoiceThread requires the following configuration to use Active Directory authentication:

- VoiceThread must have access to an Active Directory controller via port 636. If your organization uses a firewall, you must allow VoiceThread access to this machine on this port. Please speak with the VoiceThread Integration Team for additional information.
- VoiceThread requires that all communication from your Active Directory service be encrypted using either TLS or SSL. Your organization must use a security certificate signed by a trusted Certificate Authority (CA). Please see *http://support.microsoft.com/kb/321051* for additional information.
- VoiceThread must be able to establish an Active Directory bind as an authenticated user. The authenticated bind allows VoiceThread to determine if the user credentials are valid and if the user is authorized to use the service.
- VoiceThread requires a list of base DN (see Figure 2) for users such that VoiceThread can find the user in the system, discover the appropriate details, and collect the correct role information. In the figure below the location of base DN "Test OU" would be located at "dc=server,dc=mydomain,dc=com".
- A valid test account for the VoiceThread Integration Team is required.

Figure 2: Active Directory User and Computer Module



Summary:

For Microsoft environments VoiceThread strongly recommends using this authentication implementation. Using VoiceThread Active Directory Authentication ensures that all of your organizational policies are enforced including requiring the use of strong passwords, restricting usage to a certain time periods, assigning authorized group membership, and enabling password changes to immediately propagate to all services. End users will find this approach simple, familiar, and consistent. However, if your Active Directory server is inaccessible to the Internet or providing the appropriate bind credentials is not possible, then you should strongly consider using the VoiceThread Authentication API *(refer to: API Authentication)*.

Lightweight Directory Access Protocol (LDAP)

LDAP is a standards based method used to store user information, credentials, roles, and group associations. There are many existing standard object class definitions for LDAP including RFC 2798 inetOrgPerson and posixAccount. Additionally, there are various vendor implementations of this standard including Oracle Internet Directory, Novell's eDirectory, and Sun's iPlanet. The VoiceThread LDAP Authentication process is similar to the "Microsoft Windows Active Directory" authentication process, so please read the implementation details above. VoiceThread LDAP Authentication is configurable to work with most of these implementations if they meet the following requirements:

- VoiceThread must have access to the LDAP server via a secure transport protocol (such as via port 636). If your organization uses a firewall, you must allow VoiceThread access to this machine on its secure LDAP port. Please speak with the VoiceThread Integration Team for additional information.
- VoiceThread requires that all communication from your LDAP service be encrypted using either TLS or SSL. Your organization must use a security certificate signed by a trusted Certificate Authority (CA).
- VoiceThread must be able to either bind as an authenticated user using an anonymous bind or have a bind DN and pass word to establish a connection for a search and bind to then authenticate on behalf of the user. The authenticated bind allows VoiceThread to determine if the user credentials are valid and if the user is authorized to use the service.
- VoiceThread requires a base DN (see Figure 2) for users so that VoiceThread can find the user in the system, discover the appropriate details, and collect the correct role information.
- A valid test account for the VoiceThread Integration Team is required.

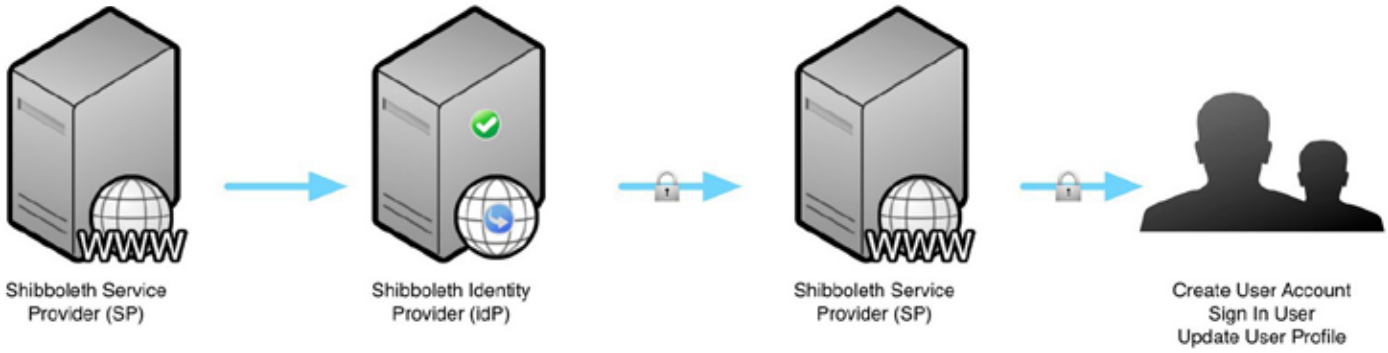
Summary:

VoiceThread recommends using the LDAP Authentication integration for organizations that have a centralized login system based on the LDAP standard. Using VoiceThread LDAP Authentication ensures that all of your organizational policies are enforced including requiring the use of strong passwords, restricting usage to certain time periods, assigning authorized group membership, and enabling password changes to immediately propagate to all services. End users will find this approach simple, familiar, and consistent. However, if your LDAP server is inaccessible to the Internet or providing the appropriate bind credentials is not possible, then you should strongly consider using the VoiceThread Authentication API *(refer to: API Authentication).*

Shibboleth/inCommon

VoiceThread supports organizations that use Shibboleth for user authentication and authorization. VoiceThread has integration options for Shibboleth implementations version 1.3+ and 2.0 and higher (using version 2.0+ is highly recommended). Shibboleth allows large organizations to abstract their internal authentication and records management systems to use a common infrastructure and to provide the appropriate SAML attributes to external providers. VoiceThread works as a Shibboleth Service Provider (Shibboleth SP), requesting authorization information on behalf of the user upon access to VoiceThread. Figure 3 describes the VoiceThread Shibboleth integration process:

Figure 3: Shibboleth Authentication Workflow



1. The end-user requests access to VoiceThread via your organization's VoiceThread domain (e.g. https://yourorg.voicethread.com/) or is redirected from a similar page within the organization.
2. The VoiceThread Service Provider (SP) determines if the user is authorized to view the organization's VoiceThread instance. If the user is authorized, they are allowed to view VoiceThread without further interruption. If the user

has not been authorized, then they are redirected to the organization's Identity Provider (IdP) to request that the user authenticate before accessing VoiceThread.

3. Once the user is authenticated, they are once again redirected to the VoiceThread SP, and the appropriate SAML attributes are released to VoiceThread. If group authorization is used, VoiceThread confirms that the user is a member of an allowed group or is not a member of a restricted group.

4. For new users, VoiceThread creates a new account. For existing users, VoiceThread signs them into their existing account. If an existing account is not yet a member of your organization, VoiceThread will automatically request permission from the user to add their account to your organization (refer to: Existing VoiceThread Accounts and Integration).

The Shibboleth Authentication process is completely transparent to the end-user and allows for a complete Single Sign On (SSO) experience, requiring the end-user to provide their credentials only once for access to all services that support Shibboleth. Many of VoiceThread's larger clients prefer this method of authentication because it reduces many of the complexities of the traditional sign-in experience and provides the end-user with a consistent interface to authenticate to all resources, whether internal or external. VoiceThread's Shibboleth Authentication is configurable to work with most of standard Shibboleth implementations as long as they meet the following requirements:

- If the Shibboleth IdP is not a member of inCommon, VoiceThread must have information about the IdP (including the IdP URI or the URN) and a valid security certificate to establish a secure link between the SP and the IdP.
- The version of Shibboleth in use within the organization (e.g. version 1.3 or 2.0, etc).
- The organization's IdP must expose the following SAML attributes to the VoiceThread SP:
    - A unique identifier (GUID, EPPN, Student ID, mail, or other unique method to identify users)
    - First Name (optional, but highly recommended)
    - Last Name (optional, but highly recommended)
    - Mail (this attribute is used to merge existing account and is hidden from external users. This attribute is only avail able to administrators of the organization. Additionally, this attribute is only used for notification of activity within VoiceThreads of which the end- user is a member, contributor, or editor)
- If the organization's IdP uses a non-standard attribute mapping system, VoiceThread must have the appropriate attribute mapping (preferably in a valid XML document).
- A valid test account for the VoiceThread Integration Team is required.

VoiceThread is a member of the InCommon Federation. This greatly simplifies Shibboleth authentication integration with colleges and universities that are already members of InCommon, which includes the majority of Research-I Universities in the United States. This should allow for faster deployments for Shibboleth authentication, with much less work on the University / Identity Provider's end. For additional information regarding our Participant Operational Practices, please refer the following document:

http:// voicethread.com/support/howto/System_Integration/Auth_Integration/inCommon_POP/

Summary:

Shibboleth is a reliable, robust, single-sign-on solution for medium to large organizations. Shibboleth allows for extremely granular control of user attributes, combining multiple internal authentication systems to use one standard external format, and providing federated access to external resources. VoiceThread has been Shibboleth compliant since 2008 and has several organizations that use this as their preferred option for authentication. Organizations that currently use Shibboleth for their user authentication are encouraged to use this approach to also access VoiceThread. If your organization does not have a public-facing IdP authentication site or if it prefers to serve as both the IdP and SP, we recommend using VoiceThread API Authentication along with your Shibboleth configuration. If you have any question regarding implementing your Shibboleth IdP with VoiceThread, please contact the VoiceThread Integration Team.

Central Authorization Service (CAS)

VoiceThread supports user authorization using the Central Authorization Service (CAS) protocols. The CAS process is analogous to the Shibboleth authentication integration, except there are a few differences in implementing the two protocols (see Figure 3 for a diagram of the authentication workflow). VoiceThread only supports CAS implementations that also expose SAML attributes that can be used to authenticate a user, and thus choosing this option requires that your organization use a version of CAS that supports submitting SAML attributes.

The VoiceThread Integration Team can work with your User and Identity Management department to ensure that these attributes are being successfully captured during the user authentication process. To use CAS with VoiceThread, your organization's implementation must meet the following requirements:

- The organization's CAS instance must expose the following SAML attributes to VoiceThread:
- A unique identifier (GUID, EPPN, Student ID, mail, or other unique method to identify users)
- First Name (optional, but highly recommended)
- Last Name (optional, but highly recommended)
- Mail (this attribute is used to merge existing account and is hidden from external users. This attribute is only available to administrators of the organization. Additionally, this attribute is only used for notification of activity within VoiceThreads in which the end- user is a member, contributor, or editor)
- The version of CAS in use within the organization (e.g. 2.0, 2.1, etc).
- The location of the CAS authorization server and path to access the CAS service.
- A valid test account for the VoiceThread Integration Team is required.

Pearson Learning Studio Authentication

VoiceThread provides integration and authentication integration with Pearson's Learning Studio, a Learning Management System (LMS). If your organization uses Pearson Learning Studio, it is recommended that you use Learning Studio SSO integration and authentication with VoiceThread. As with all VoiceThread authentication options, user information is sent securely to VoiceThread for processing, using Pearson Learning Studio Authentication built-in encryption methods. This type of authentication will require personal communication with the VoiceThread Integration Team, as the Learning Studio authentication process is highly customizable. If you have any question regarding implementing your Learning Studio LMS with VoiceThread, please contact the VoiceThread Integration Team for additional details.

Moodle Authentication

For any organization that uses Moodle as their Learning Management System (LMS), Moodle Authentication is available for authenticating with VoiceThread. The Moodle Authentication module is a version of the API Authentication packaged exclusively for the Moodle LMS. This method of authentication requires installing a "block" (the name for modules within Moodle) on your organization's Moodle instance that will be accessible to those who should have access to VoiceThread. Users will be able to click this block and have their Moodle information encoded and sent to VoiceThread (see Figure 4 below for an overview of the process). To use VoiceThread Moodle Authentication, your organization's implementation must meet the following requirements:

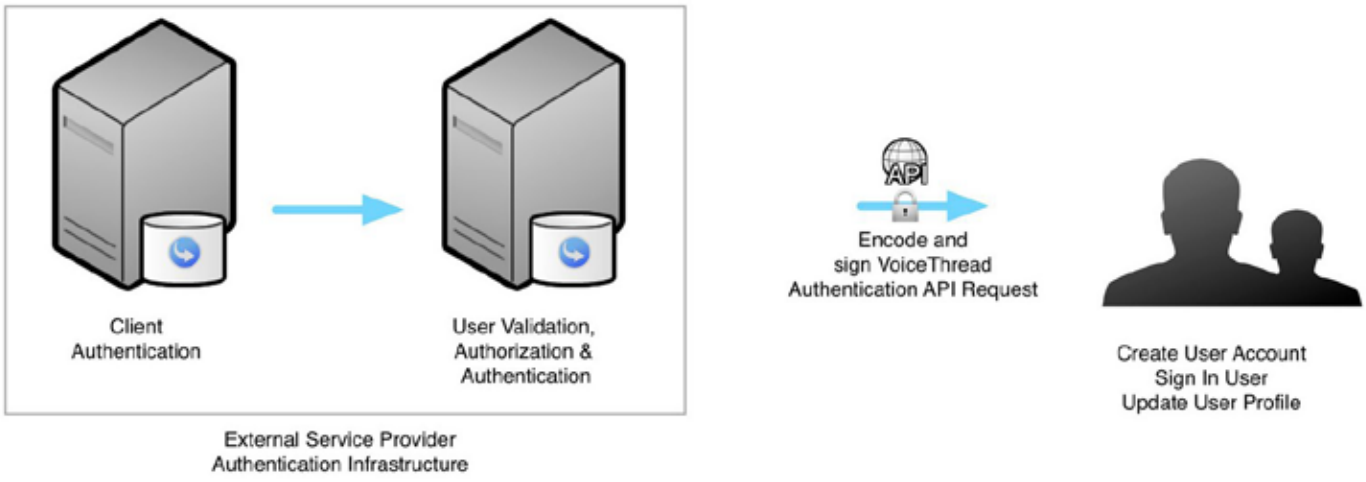
- The organization must be using version 1.9+ or 2.0+ of Moodle.
- Users within your Moodle instance must have a first name, last name, email, and username.
- A server with access to the Internet since the VoiceThread API requires a token be requested from VoiceThread before each authentication request.
- The organization must have an authentication key, organization ID, VoiceThread API key, and custom VoiceThread URL (provided by the VoiceThread Integration Team) to use this service.

API Authentication

VoiceThread recommends using API Authentication for organizations that use custom authentication solutions, are unable to provide VoiceThread with access to its internal authentication system, or wish to streamline their internal authentication process. VoiceThread API Authentication is a very flexible token-based authentication process that allows your organization to determine the validity of its users, package relevant authorization information, and send this information to VoiceThread to enable them to sign in. The API Authentication design is quite flexible, can be written in any programming language of your choice (provided it follows the design specifications), and is designed with security in mind. At no time are user credentials needed or sent, all requests are sent using SSL, and the VoiceThread API Authentication is designed to prevent reply-authentication attacks. The VoiceThread Integration Team can provide your organization with sample source code and documentation that can be used to create its own authentication system. To use VoiceThread API Authentication, your organization's implementation must meet the following requirements:

- The organization must have a programmer who can read through documentation and source code to produce a working authentication solution.
- A unique identifier (GUID, EPPN, Student ID, mail, or other unique method to identify users) and email address for users.
- A server with access to the Internet since the VoiceThread API requires a token be requested from VoiceThread before each authentication request.
- The organization must obtain a secret key (provided by the VoiceThread Integration Team).

Figure 4: VoiceThread Authentication using the API



1. The end-user requests access to VoiceThread via your organization's internal authentication site. This could be a website, portal page, or any other method.
2. Your organization authenticates and authorizes the end-user to use the VoiceThread service.
3. Your organization's internal authentication code assigns the end-user parameters to submit (including unique identifier, email, etc) and r quests an authentication session token from VoiceThread.
4. The end-user transmits these signed credentials securely to VoiceThread, and is either signed in with an existing account or given a new account. If an existing account is not yet a member of your organization, VoiceThread will automati cally request permission from the user to add their account to your organization. For more information, please refer to: *Existing VoiceThread Accounts and Integration.*

VoiceThread Basic Authentication

Voicethread provides a basic way for your organization to allow users to sign in without the use on any external authentication systems. There are two ways for your organization to allow users to sign in: creating a formatted Comma Separate Values (CSV) file with user information and by adding information for users, or one-at-a-time. VoiceThread recommends this system for small organizations with fewer than two hundred users, and for anything larger we strongly recommend using the external authentication methods detailed above. This system is not designed to handle a large number of users and can make managing hundreds of users difficult in the future. This method should not be used in conjunction with any of the other external authentication methods listed above.

Comma Separated Values Upload

The VoiceThread Manager allows your organization to upload a CSV file to populate users within VoiceThread. In the VoiceThread Manager (available at https://voicethread.com/manage/), under the Add Users option is a location to upload a CSV file of users. The CSV file must follow the specifications outlined in the "sample file" format document. If your CSV is not compliant with the sample file, you will be notified of any issues during the upload process. The CSV file must contain the following information (please consult the sample document for additional requirements):

- The first name of the user (will remain private to your administrators).
- The last name of the user (will remain private to your administrators).
- A valid email address for the user (or a unique username if you have a K-12 school or classroom VoiceThread subscription).
- An identity name that will appear with VoiceThread creation or comments (optional).
- Password (six characters or longer).

One-at-a-time user addition

The one-at-a-time user addition system allows your organization to add users on demand. In the VoiceThread Manager (available at https://voicethread.com/manage/), under the Add Users option you are presented with the ability to add a single user. The one-at-a-time user additions must contain the following information (please consult the VoiceThread Manager for additional requirements):

- The first name of the user (will remain private to your administrators).
- The last name of the user (will remain private to your administrators).
- A valid email address of the user (or unique username if you have a school or classroom subscription).
- An identity name that will appear with VoiceThread creation or comments (optional).
- Password (six characters or longer).

VoiceThread Information System Integration (VISI)

The VoiceThread Information System Integration (VISI) enables the automatic synchronization of user, role, and group membership information from your Information Management System to VoiceThread. VISI automatically assigns members into "VISI Groups" based on their current membership in a course or department, and it assigns member roles within these VISI Groups as well as maintains consistency of your member information. VISI is designed to work with most Information Management and Enterprise Resource Planning systems, and is configurable to work with custom in-house solutions. Implementing VISI allows for a seamless experience for the end-user while allowing your organization to leverage the power and flexibility of your current Information Management System infrastructure.

Additional information about VISI is available at http://voicethread.com/about/features/integration/. For more information regarding systems integration, please consult with the VoiceThread Integration Team.

Existing VoiceThread accounts and Integration

If you have users of your organization who were members of VoiceThread before you implemented external authentication, VoiceThread provides a process to ensure that all of their content is migrated successfully. The VoiceThread Account Merger process will identify users based on their email address or unique identifier and ask for their existing VoiceThread.com password before allowing them to continue with the authentication process. Upon successful authentication, VoiceThread will make all of the user's existing content available to your organization so that users can share and collaborate on content seamlessly. The VoiceThread Account Merger process requires that a valid email address be specified for the user of an external authentication system and that the email address matches the address they initially used to register for VoiceThread. If the user originally registered with a different email address than that on record with your organization's information system and their content is not merged upon authentication, they should contact VoiceThread Support with both email addresses to request that their accounts be merged manually.