IBM Connections 5.0

Deployment Scenarios

Deploying External Collaboration

by

Morten Kristiansen
Paddy Barrett
Mustansir Banatwala
Mark Curran
Jay Boyd

Trademarks

Contents

Figures

Foreword

IBM Connections introduced External Collaboration in version 5.0, released in June 2014. With this feature, you can add external users from *outside your firewall* to your own internal IBM Connections deployment. Once registered, external users can be added to Communities and Files, enabling them to collaborate with your internal users but with a refined user experience, limited access to content, and special identifiers that alert internal users when content is visible to external users.

About the authors

Morten Kristiansen is a Test Architect for Systems Test on IBM Connections.

Mustansir Banatwala is an IBM Connections architect and an IBM Senior Technical Staff Member (STSM).

Paddy Barrett writes technical documentation about IBM Connections.

Mark Curran is a senior software tester on the IBM Connections System Verification Test (SVT) team.

Jay Boyd is a senior software engineer on the IBM Connections team.

Introducing IBM Connections External Collaboration

IBM Connections v5.0 introduced the ability to invite your external partners, suppliers, and customers to collaborate with you inside IBM Connections.

Instead of sharing information with external users through email, meetings, and phone calls, you can now invite them to join a community where they interact with your internal users, helping you improve communications and productivity, and enhance business results.

External users can work with all the content of a community; they can also work with files that have been shared with them. However, external users cannot see content that has not been explicitly shared with them. For example, they can see communities only if they are members of them, and they can only see files that have been shared with them.

Setting up a community and inviting an external user

To collaborate with external users in a community, an authorized internal user creates a community and selects the option to allow external users. Authorization is enabled by your IBM Connections administrator.

When a community is defined as an external community, and when external users are registered in your directory, you can invite them to join the community by typing their name or email address in the **Invite Member** typeahead field. The external user then receives a notification email inviting them to become a member of the community.

Working with external users in Communities

In communities, external users have all the same rights as internal users – they can interact with community activities, blogs, forums, wikis, and so on, but they cannot access data outside the community (except for files that you explicitly shared with them).

Communities that are shared externally are clearly identified as such in the UI with a yellow banner across the top of the community page, as shown below:

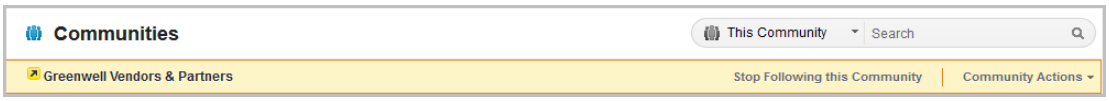

Figure 1. The yellow banner indicates that this community is shared with external users.

Note: External users cannot be community owners.

Sharing a file with an external user

You can share files with external users by using the IBM Connections Files application. Only authorized internal users can allow a file to be shared with an external user. Authorization is enabled by your IBM Connections administrator.

When you share a file externally, the external user receives a notification email with a link to the file. The external user's activity stream also shows that the file has been shared with them.

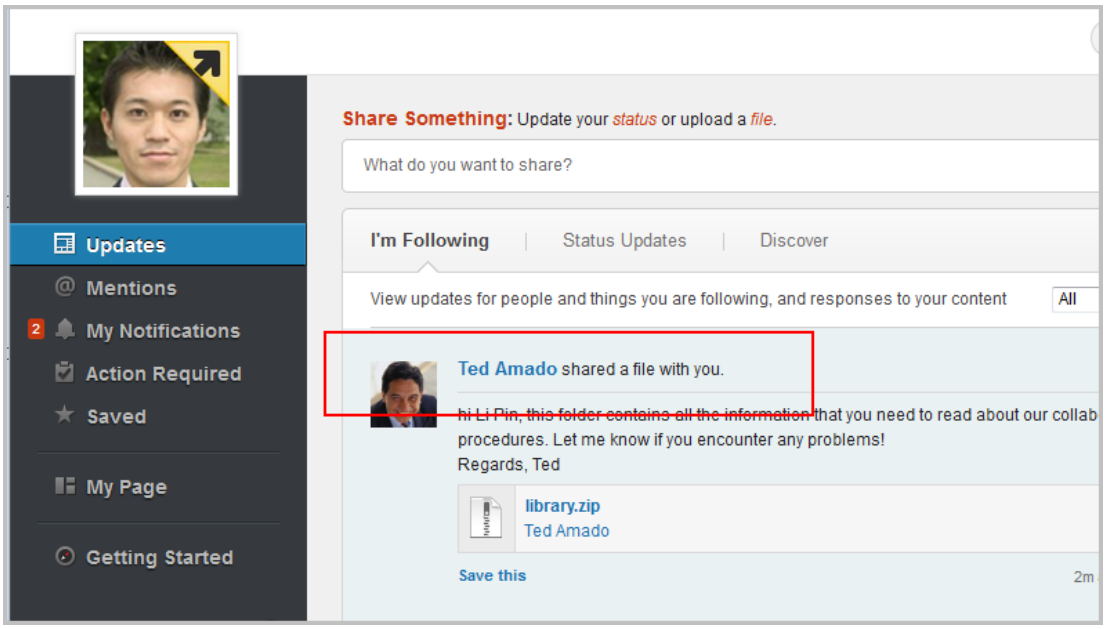

Figure 2. Files shared with an external user.

How to work with external users

You can interact with external users just like you do with internal users, except that you can easily identify content that is shared with external users. External users are identified by a yellow indicator in their profile photo and text on their name. This image and naming convention is consistent throughout Connections:

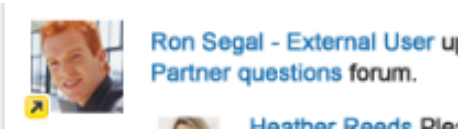

Figure 3. External users are differentiated with graphical and textual highlighting.

Similarly, files that are shared with external users are also identified as such – a special yellow icon beside the file name indicates that it is shared externally:

In addition, you will see a warning message whenever you are about to post content that would be visible to an external user:

Figure 4. External-facing content is always differentiated.

The External User perspective

External users can see only the content that is shared with them – no other content is visible to them. They can view only those files that are shared with them and the communities to which they have been invited. They can collaborate fully in communities where they are members, but they cannot create or own communities.

As an external user, you can perform the following tasks:

- Collaborate fully as members in communities.
- View and download files that are shared with you
- Edit files in IBM Docs
- See an activity stream to which you have access
- Edit your profile by clicking your picture and selecting My Profile
- View business cards of users who share content with you
- Share files with people
- Search inside content shared with them

External users cannot see the following IBM Connections items:

- Public microblogs
- Public or moderated communities
- Public files
- The organization's directory
- Recommended content or people
- The Profiles menu.
- Users' profiles

- Community metrics

Nor can external users perform the following tasks:

- Create or own a community
- Follow people
- Search the organization's directory

For more information, see the Using Connections V5 topics in the IBM Connections Knowledge Center or watch the IBM Connections 5 - External Collaboration video.

Enabling External Collaboration in IBM Connections

Choosing a User Directory Topology

In IBM Connections, all user identities are stored in one or more user directories. These user directories are configured in the Security section of the IBM WebSphere Application Server Integrated Solutions Console. Typically, such user directories are LDAP directories although it is possible to implement other types of user directories through custom integration activities that are supported by the capabilities of WebSphere Federated Repositories.

Additional information about users in the organization is stored in a relational database that serves the Profiles application. Content such as address, division, telephone, job role, skills, responsibilities and professional network is managed by the Profiles application and stored in the Profiles (PEOPLEDB) database. During the implementation phase of a Connections-based solution, many of these attributes are extracted from a variety of (HR-related) data sources and pushed into Profiles by using the Tivoli Directory Integrator (TDI) solution that is provided with IBM Connections or built by IBM Services engagements. Subsequently, a scheduled process that uses the TDI solution synchronizes Profiles with any changes in the LDAP directory or other data sources.

For more information about using TDI with Profiles, see the Populating the Profiles database topic in the IBM Connections Knowledge Center and the Understanding IBM Tivoli Directory Integrator for IBM Lotus Connections 3.0 whitepaper. While the whitepaper was originally created for IBM Connections V3, many of the concepts and technologies still apply to IBM Connections V5.

During the authentication process, when a user accesses a Connections application, WebSphere Application Server issues a bind request to the LDAP server to establish the identity of the user who is logging in to IBM Connections. The relevant unique identifiers are returned to the Directory Services Integration application code which in turn uses these unique identifiers to bind the user principal to the additional information stored in the Profiles database.

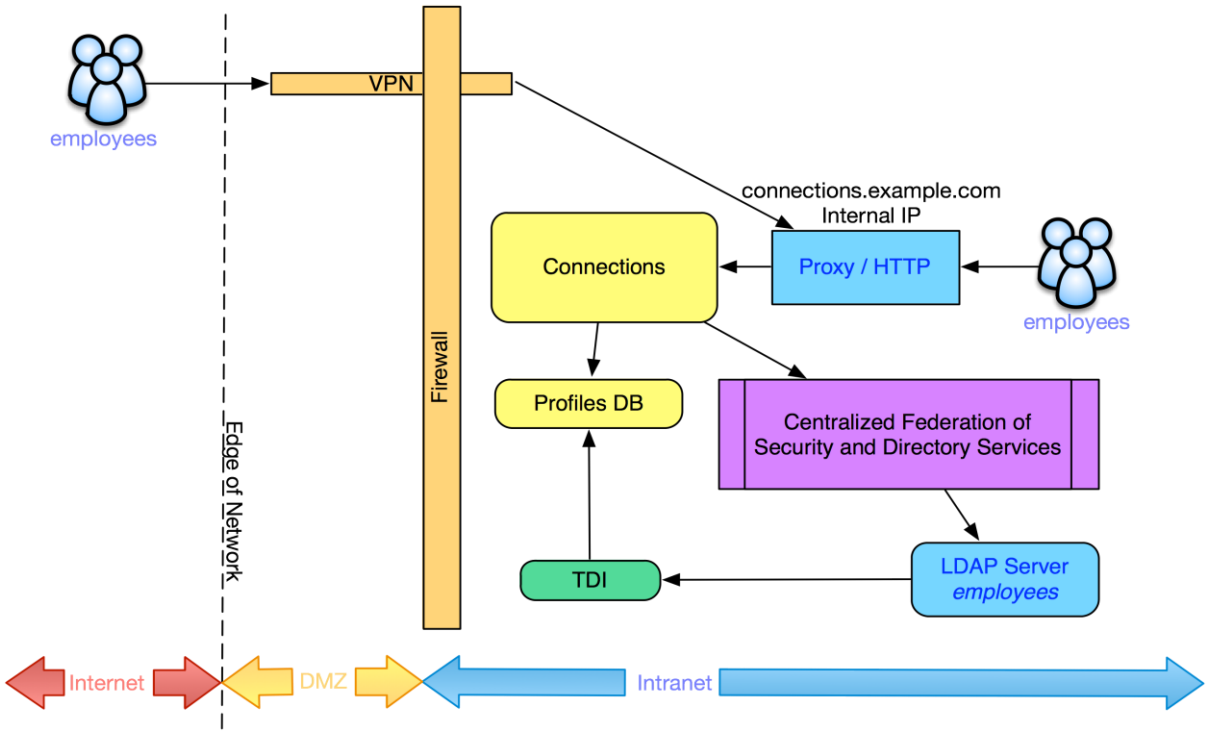

Figure 5. Standard deployment topology for internal use

Note: There is no functional difference in how the attributes of internal or external users are stored.

Tip: To prevent external users from being able to authenticate with other applications within your organization, IBM strongly discourages adding external users to an existing LDAP directory that is used by other applications. IBM recommends creating a separate LDAP directory specifically for external users and ensuring that this directory is used only by IBM Connections. If, for instance, external users are added to the corporate LDAP directory, then it could be possible for external users who visit your premises to log on to intranet systems that use this directory for authentication.

Caution: Groups

Some groups in your LDAP directory might contain external users. If an internal user adds this type of group to the membership of an internal community, external users will have access to the content of that community, and the community will not indicate that external users have access.

To avoid this risk, take one or more of the following steps:

- Ensure that the LDAP directory that is used for external users does not contain groups.
- If the LDAP directory that is used for external users already contains groups, configure the security settings in WebSphere Application Server so that it cannot find these groups.
- If the LDAP directory that is used for external users is the same one that is used for internal users, ensure that no external users are added to any groups

in the directory. If external users are already present in groups in the directory, remove them.

- If none of the preceding steps is possible, advise your users to add only those groups to communities that do not contain external users.

A user's authentication credentials, username, and password/certificate, are typically stored in an LDAP directory and registered in Profiles through the TDI solution provided with IBM Connections.

Depending on an organization's preferences and other constraints, it is possible to store internal and external users in the same LDAP branch, separate branches in the same LDAP directory, or in completely separate LDAP directories. External users' records in LDAP are subject to the same requirements as internal users' records in that they must have an immutable unique identifier.

For more information on how LDAP directories are configured, see the **Setting up federated repositories** topic in the IBM Connections Knowledge Center.

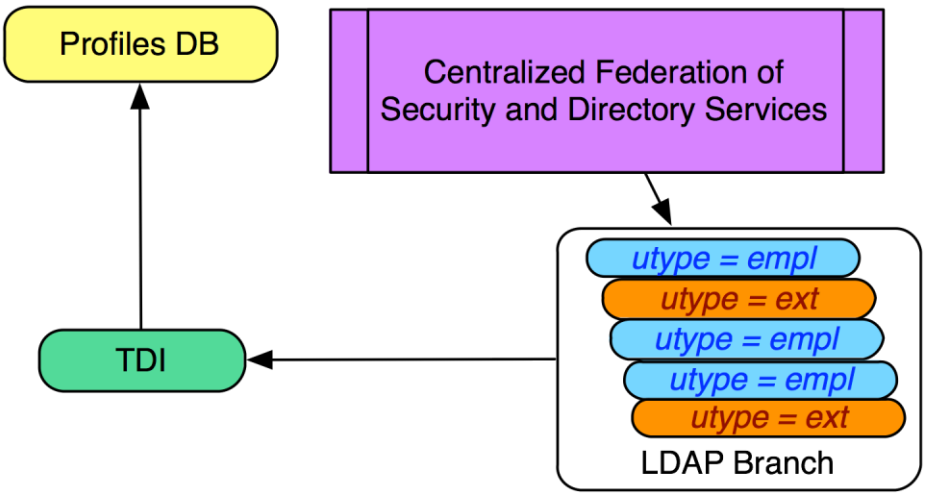

Figure 6. Internal and External Users in the same LDAP branch.

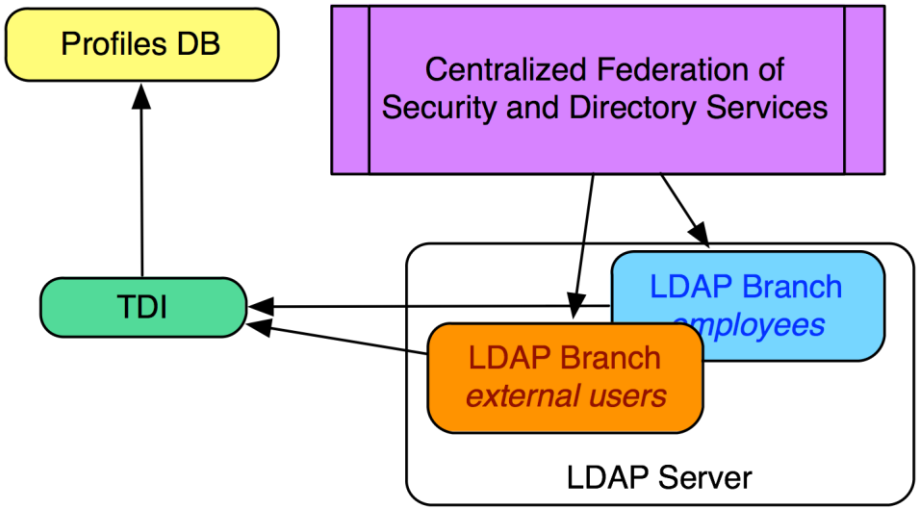

Figure 7. Internal and External Users in separate branches of the same LDAP directory.

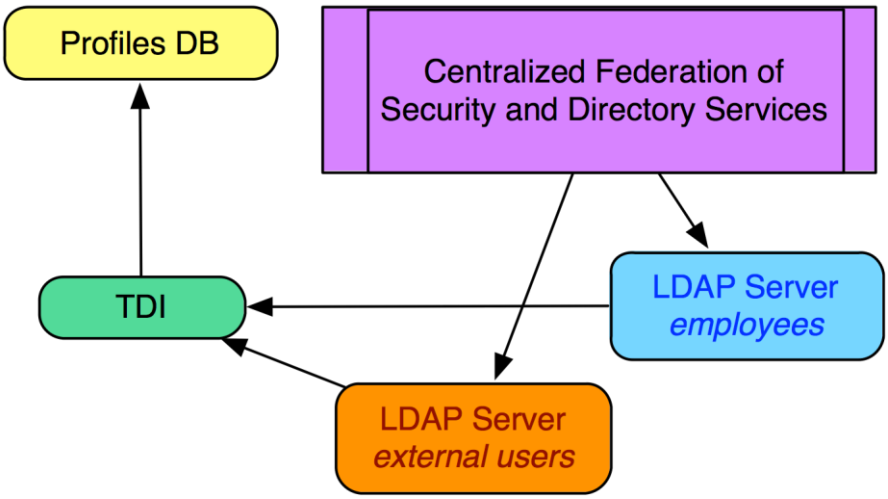

Figure 8. Internal and External Users in separate LDAP directories.

If external users are stored in the same LDAP directory as internal users, we recommend using a separate branch for external users. This can help to ensure that there is sufficient logical distinction between the user types. However, if external users are stored in the same LDAP branch as internal users, you must ensure that they can be distinguished from internal users by using one or more immutable attributes.

Regardless of which approach for storing internal and external users is chosen, we recommend that separate TDI Solution directories are maintained for internal and external users. This strategy will help you to:

- Support separate schedules for synchronizing the LDAP directory with the Profiles database.

- Support different rules for managing attributes and attribute mappings for internal and external users.
- Eliminate potential failure scenarios where the settings for external users could be used to synchronize internal users, and vice versa.

Configuring IBM Connections to enable External Users

When a user directory topology for external users has been chosen and the appropriate infrastructure created, you might need update the repository definition of your WebSphere Federated Repositories configuration. This is the case for User Directory Topologies 2 and 3 that were outlined in the previous section

For more information, see the Setting up federated repositories topic in the IBM Connections Knowledge Center.

Subsequently, you must synchronize identity information and other attributes of external users with the Profiles database.

For more information, see the Populating the Profiles database and Registering external users with Profiles topics in the IBM Connections Knowledge Center. The instructions vary according to your User Directory Topology.

Once external users have been added to Profiles, their photos appear with special styling to clearly distinguish them from internal users, as illustrated in Figure 3.

Authorizing internal users to create externally-accessible content

Now that we have added external users to the Profiles database, we need to authorize internal users to share content with external users. Only internal users with the `EMPLOYEE_EXTENDED` role can share files with external users or create Communities which accept external users as members. Any members of those Communities can interact with external members.

Only internal users who are registered with the Profiles database can be assigned to the `EMPLOYEE_EXTENDED` role. There are two approaches to configuring roles for internal users.

Using administrative commands to configure internal user roles

The Profiles application provides administrative commands for configuring users roles. You can set a user's role either by external ID or by email address. A batch option is also available where a list of email addresses or external IDs is input from a text file.

To remove the privileges to share content externally from a user, you can reset a user's role to either the `EMPLOYEE` or `DEFAULT` role.

Note: *External ID* refers to the attribute in the user directory by which the directory services integration module of IBM Connections binds the user principal to the additional user information in the Profiles database.

For more information about using Profiles administrative commands to set the internal user role, see the Setting user roles for external collaboration topic.

Administrative commands are available by default in IBM Connections and can be integrated into an end-to-end solution through the scripted administration facility in WebSphere Application Server. Generic sample administration scripts are available on developerWorks.

Making External Collaboration available outside the firewall

Conceptual Topology

Now that we understand the technical aspects of enabling External Collaboration in a deployment from a feature-function perspective, we can review how to make the capability available outside the firewall.

On the right side of the firewall in Figure 9, we see the standard Connections deployment elements as they relate to External Collaboration. A number of the Connections components require server to sever communication, which commonly is routed through the internal Proxy / HTTP service. If we opened firewall access to the internal HTTP service, we would compromise the safety of this traffic as it would be exposed to the Internet.

Standard practice for enabling access to systems behind a firewall is to introduce a Reverse Proxy to service the clients and effectively hide the identity (hostname, IP address, and so on) of the internal systems. However, the email digest capability in IBM Connections requires a single DNS hostname to be available to internal as well as external users. This capability is handled by registering the DNS hostname in external, Internet-facing DNS servers, with the IP address of the Internet-facing Reverse Proxy host. Meanwhile, the same DNS hostname is registered in an internal-facing DNS service with the IP address of the internal Proxy / HTTP host.

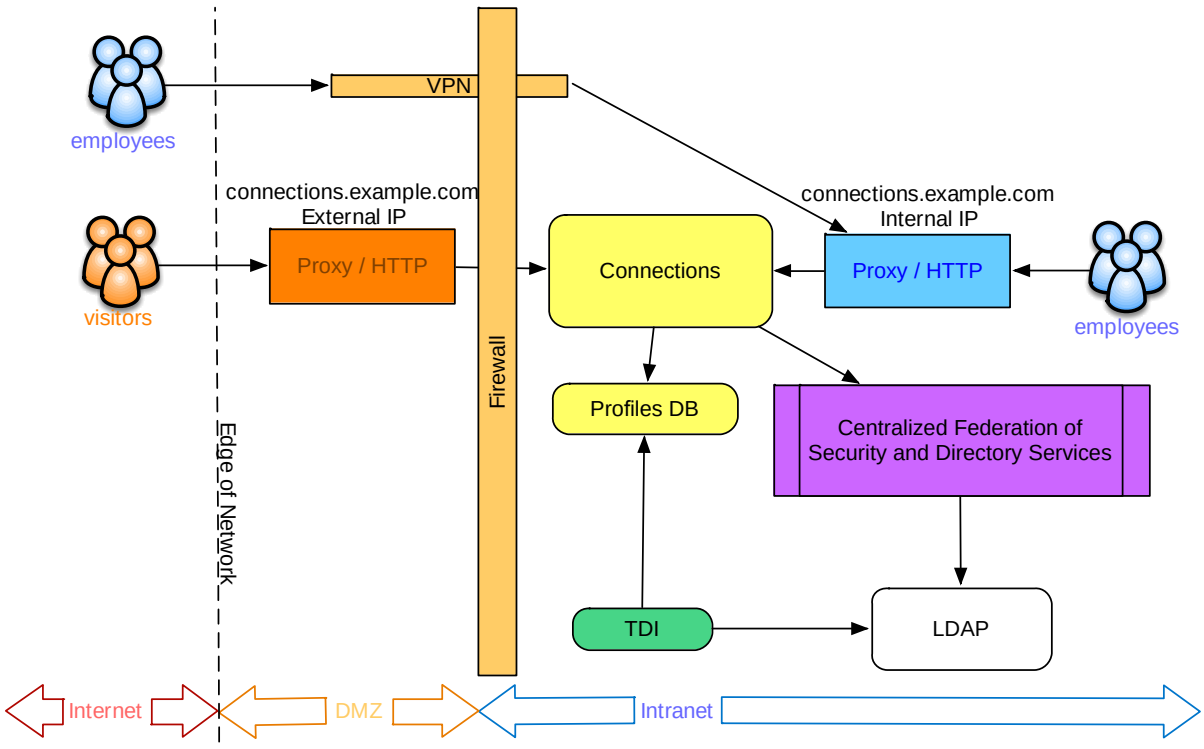

Figure 9. A simple conceptual topology accessible outside the company firewall.

There are many ways to configure and protect an IBM Connections deployment both for internal, behind the firewall use, and for providing access to external users through a firewall. In the following sections, we cover the most commonly-used technologies to show how this can be achieved.

Using 'simple' Single Sign-On methods

The simplest scenario with which to make External Collaboration available outside the firewall is based on a standard deployment that uses Forms-Based Authentication and LTPA tokens for Single Sign-On.

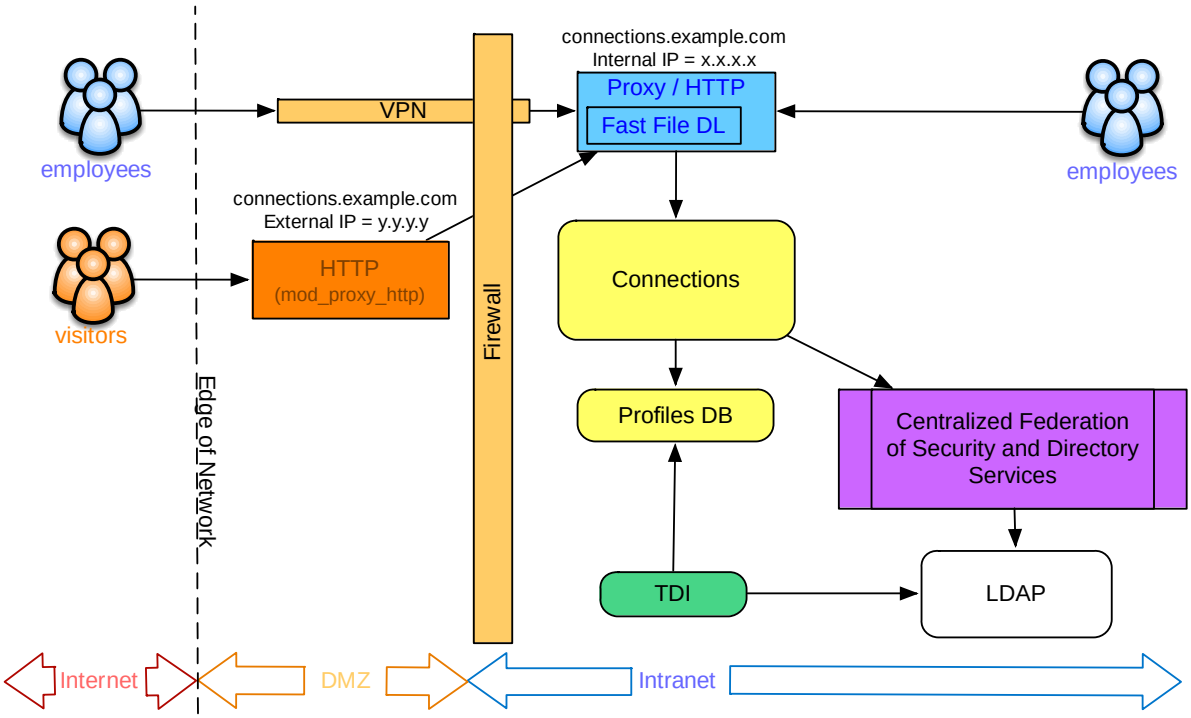

Figure 10. Using Forms-Based Authentication and LTPA Tokens for SSO.

Here, we augment an existing Connections deployment with the external HTTP service. This service is typically an Apache or IBM HTTP Server configured with the mod_proxy_http and ProxyPass rules to proxy incoming traffic to the internal HTTP service. Ideally, this server will use only SSL/TLS protected network connections when routing traffic through the firewall to IBM Connections.

Key aspects of this scenario are:

1. The IP address of the external HTTP service is registered in Internet-facing DNS services with the same hostname as that of the internal HTTP service (eg: connections.example.com).
2. The Fast File Download module is configured only in the internal HTTP service.

3. No changes are required to the configuration of the deployment components inside the firewall.
4. The External HTTP Service needs to be configured to trust the SSL certificate presented by the Internal HTTP Service, preferably through the addition of the appropriate signer certificates in the security key store.
5. It is necessary to enforce authentication on all access to the deployment. Otherwise, external users would be able to see content which is considered public to the company but that should not necessarily be accessible to external users.

For more information about configuring IHS to act as a reverse proxy, see the Setting up a reverse proxy configuration with SSL topic in the IBM Knowledge Center.

Technologies and services like F5 and Akamai can also be configured in a similar manner.

Using IBM Security Access Manager

In this scenario, we augment an existing Connections deployment with a delegated security model that uses IBM Security Access Manager (ISAM).

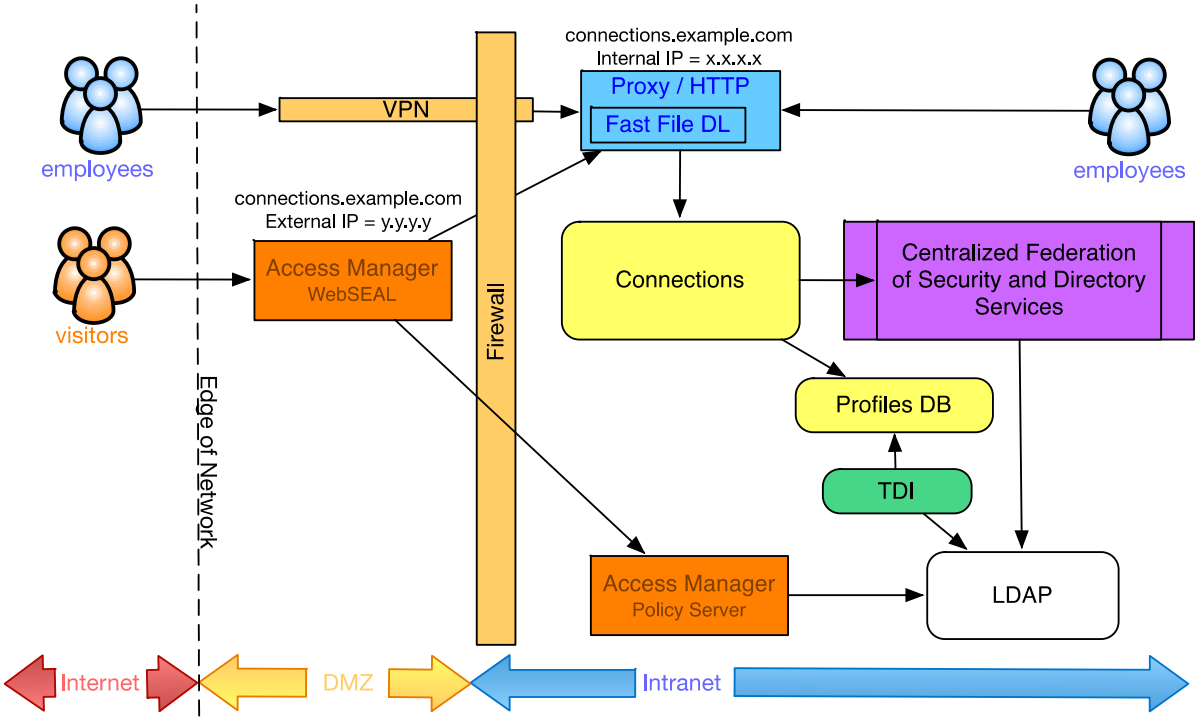

Figure 11. Using Forms-Based Authentication and IBM Security Access Manager for SSO.

By using WebSEAL as a reverse proxy, the authorization of users and access control of resources is delegated to the Policy Server. WebSEAL will obtain access control and authorization information from the Policy Server before it passes the request on to the internal HTTP service.

For more information on configuring IBM Connections with IBM Security Access Manager, see the Configuring single sign-on topic in the IBM Connections Knowledge Center.

Unlike the scenario outlined in Figure 10, it is possible to configure the WebSEAL/Policy Server to enforce authentication while allowing anonymous access to public content for (Internal) users who access the HTTP service directly.

Key aspects of this scenario are:

1. The IP address of the external HTTP service is registered in Internet-facing DNS services with the same hostname as that of the internal HTTP service (eg: connections.example.com).
2. The Fast File Download module is configured only in the internal HTTP service.
3. No changes are required to the configuration of the deployment components inside the firewall – with the exception of the additional Access Manager Policy Server. However, it is necessary to configure a WebSEAL server outside the firewall.
4. It is also possible to configure a WebSEAL reverse proxy inside the firewall to take advantage of the capabilities provided by ISAM across other internal IT systems.
5. This solution is not necessarily any more secure than other security topologies but is easier to administer, is more flexible, and has more customization options.

Note: IBM Security Access Manager was formerly known as IBM Tivoli Access Manager.

Using SiteMinder

In this scenario, we augment an existing Connections deployment with a delegated security model using the SiteMinder product by Computer Associates International, Inc.

Note: SiteMinder is now named CA Single Sign-On, and Computer Associates International, Inc. is now named CA, Inc.

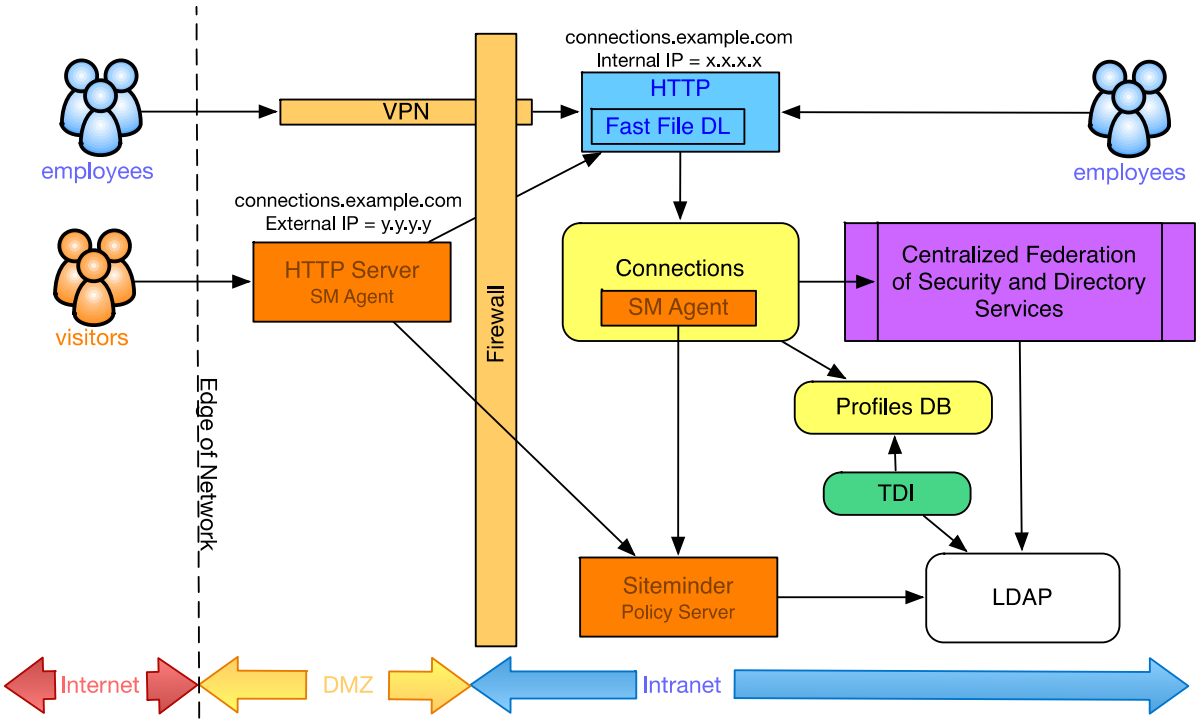

Figure 12. Using Forms-Based Authentication and CA Siteminder for SSO.

Through the use of additional agents installed on the HTTP Server (as well as the WebSphere Application Server that hosts Connections), the authorization of users and the access control of resources is delegated to the Siteminder Policy Server. As user requests are passing through the HTTP Server, the SM Agent will obtain access control and authorization information from the Policy Server before it passes the request to the internal HTTP service.

For more information on configuring IBM Connections with SiteMinder, see the Configuring single sign-on topic in the IBM Connections Knowledge Center.

Unlike the scenario outlined in Figure 10, it is possible to configure Siteminder to enforce authentication while allowing anonymous access to public content for (Internal) users who access the HTTP service directly.

Key aspects of this scenario are:

1. The IP address of the external HTTP service is registered in Internet-facing DNS services with the same hostname as that of the internal HTTP service (eg: connections.example.com).
2. The Fast File Download module is configured only in the internal HTTP service.
3. Agents are installed on the Connections server and (optionally) the external HTTP Server.
4. It is possible to also configure an SM Agent on the HTTP Server inside the firewall to take advantage of the capabilities provided by ISAM across other internal IT systems.

5. This solution is not necessarily any more secure than other security topologies but provide greater administration, flexibility, and more customization options.

Automated on-boarding of external users

At present, IBM Connections does not provide any specific or generic solutions for automated registration of external users. It is, however, possible to build a self-registration service or “Registration Portal” that leverages some of the capabilities that are delivered as part of the product.

Note: the IBM Software Services team has created an asset to provide automated on-boarding of external users. Customers can purchase the "IBM Connections Invite" plugin to implement the Internal Request with Verification scenario described in this section. Contact isscapps@us.ibm.com or your local IBM Software Services for Collaboration representative to learn more. http://www-01.ibm.com/software/lotus/services/contact.html

The topology diagram in Figure 13 illustrates conceptually what is required. The diagram shows all users, internal as well as external, stored in a single LDAP branch, but either of the three user directory topologies referenced earlier will work equally well.

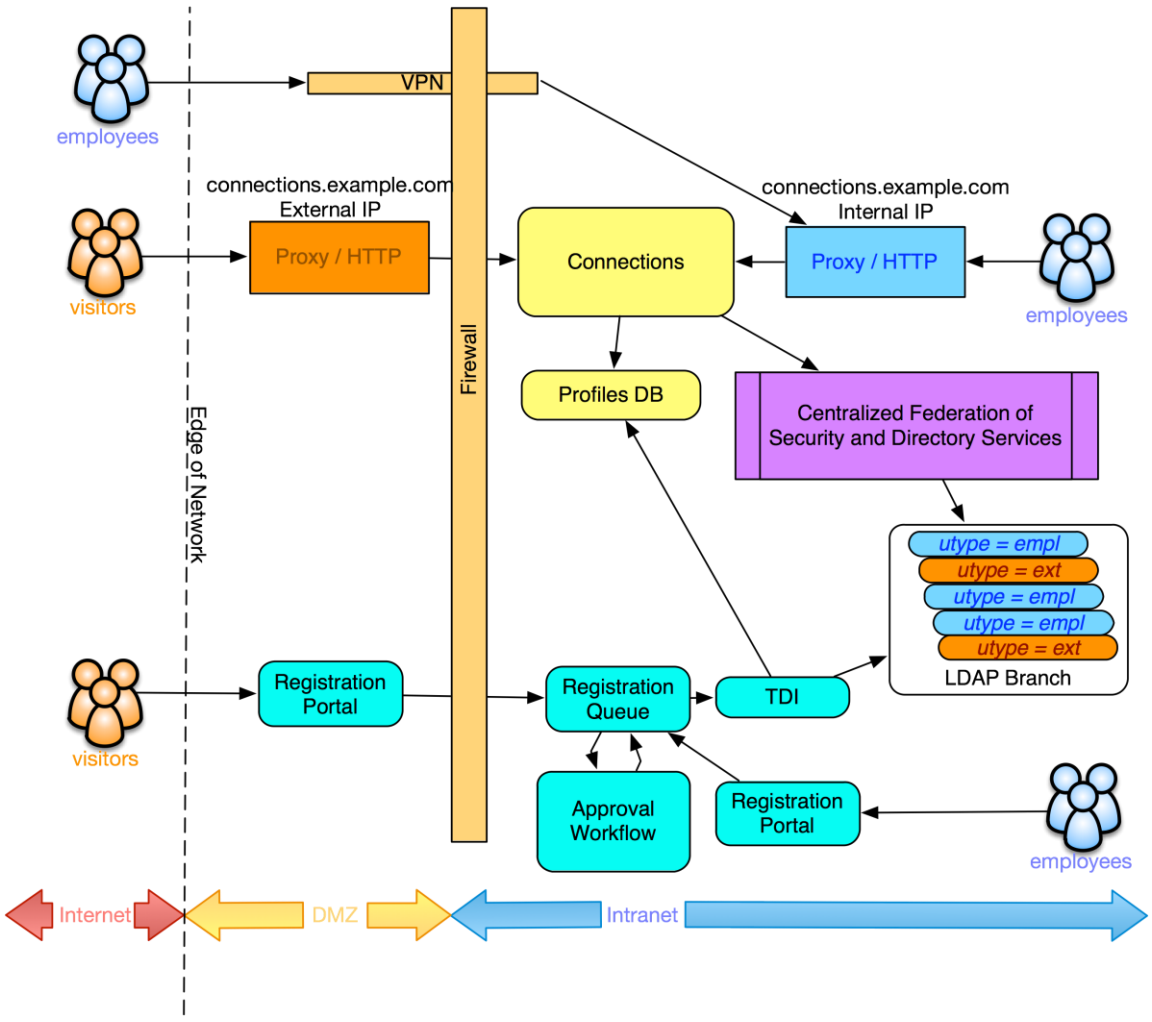

Figure 13. Automated on-boarding of external users.

Registration portal scenarios

- Internal Request

  An internal user, authorized to share content with external collaboration partners, uses the Registration Portal to generate an invitation to a person they want to collaborate with. The invitation is sent by email and includes authentication details such as a login ID and password. For additional control, the approval workflow may be invoked.

- Internal Request with Verification

  As above, but the external user receives a verification URL which takes them to the Registration Portal (where additional details can also be requested).

- External Request with Verification

  An external user requests to join and provides contact details along with business sponsor information. The business sponsor is provided with a verification URL which takes them to the Registration Portal to approve or reject the request.

In each of the above scenarios, the registration request is recorded in the Registration Queue along with information about the state of the request.

Registration queue

- Active Invitation. Any invitations that have not yet expired and have not yet been completed by the invitee.
- Registration Pending Approval. Optional, depending on business process rules. The invitee has completed a registration form and approval is required before the invitee can be registered in the user directory as an external user.
- Registration Approved. The registration and approval are completed but the user has not yet been registered in the user directory and the Profiles database.

Approval Workflow and Invitation Expiration

A business process application is required to approve registration requests. This application can also purge any outstanding, non-activated invitations which are older than a pre-defined period of time.

Tivoli Directory Integrator

IBM Tivoli Directory Integrator (TDI) uses a custom assembly line which reads entries from the Registration Queue and adds users to the LDAP directory as well as to the Profiles database. Once this has been done, the entry is removed from the Registration Queue. The external user can now log on to IBM Connections and can be invited to collaborate with internal users.

Security Considerations

When introducing External Collaboration, and making it available outside the firewall, additional considerations are necessary to help an IT department to choose and implement the protection that is applicable to their particular business environment.

Protecting against malicious content in attachments

It is a generally accepted practice that any IT system can be protected at the 'edge of network' boundary. For standard, behind the firewall, deployments of IBM Connections, this is normally achieved by virus-scanning of content on internal workstations as well as the content that passes through email gateways.

Because the IT organization is not in control of the workstation or device used by external users to access IBM Connections, it is necessary to consider additional protection against the propagation of viruses through attachments that are uploaded to or downloaded from IBM Connections. To facilitate this, IBM Connections supports ICAP compliant virus scan engines. While in theory it should be possible to make IBM Connections work with multiple different open source or commercial scan engines, our internal Quality Assurance process has validated this scenario only with the Symantec Scan Engine.

For more information on supported hardware and software, see the System Requirements for IBM Connections 5 support document.
For more information about enabling virus scanning, see the Enabling virus scanning topic in the IBM Connections Knowledge Center.

In addition to ICAP compliant virus scan engines, other technologies are available that can be injected into the network layer in front of IBM Connections and act as a reverse proxy, conducting virus scanning on the fly as attachments are uploaded to or downloaded from the deployment.

Protecting against malicious content in text entry

Any software that displays user-authored content can be vulnerable to cross-site scripting (XSS) attacks. Attackers can introduce JavaScript™ into their content that can, among other things, steal a user's session. Session-stealing in a single sign-on (SSO) environment poses particular challenges because any vulnerability to XSS attacks can render the entire single sign-on domain vulnerable.

One of the ways that IBM Connections provides a defense against this type of attack is by implementing an active content filter. This filter removes potentially harmful text content, such as JavaScript, from user input added to a post or entry before saving the post or entry to an application. Note that it does not filter file attachments. You can turn off the active content filter if you determine that your network is safe from

the threat of malicious attacks. You can also change the content that is filtered per application by editing the configuration properties.

Because these security measures can also limit the flexibility of the applications, the system administrator must evaluate the security of your network and determine whether you need to implement them. The security measures outlined below will be applied to both internal as well as external users.

Text-based fields

When active content filtering is enabled, users cannot add certain types of content to text-based fields. IBM Connections provides a set of sample active content filter configuration files which specify which types of content are allowed. The configuration files used by default by the product allow users to edit styles and add forms to entries in each of the applications. They also allow users of the Blogs and Wikis applications to add Flash content to entries. You can use the default filter settings or you can choose to apply other, more restrictive settings.

For more information about configuring more restrictive active content filter settings, see the Configuring the active content filter for Blogs, Wikis, and Forums and Configuring the active content filter for Activities, Communities, and Bookmarks topics in the IBM Connections Knowledge Center.

.

Custom Blogs templates

The Blogs application supports the use of custom templates, which allow a blog owner to change the look and feel of a blog. A custom template page is not filtered by the active content filter. Allowing custom templates in Blogs can potentially expose the IBM Connections deployment and its users to XSS exploits. As a consequence, custom Blogs templates are disabled by default.

Introducing External Collaboration to an IBM Connections deployment does not represent any additional security risk in relation to custom templates in the Blogs application because external users cannot manipulate the template even when this feature is enabled.

Protecting against possible Firewall bypass

IBM Connections include a rich set of extension points that support integration with other IBM applications such as FileNet, Sametime, and Portal, as well as third party applications from other vendors.

Some of these extension points can, if not configured correctly, expose internal data or systems to external parties. By default, the IBM Connections AJAX proxy is configured to allow cookies, headers, or mime types, and for all HTTP actions to be exchanged among the IBM Connections applications. Explicit configuration is required to allow traffic between IBM Connections applications and third party

applications.
When configuring the AJAX proxy to allow users access only to websites that contain information that is appropriate to both internal and external users,

For more information see the Configuring the AJAX proxy topic in the IBM Connections Knowledge Center.

Public Caching

In some deployment configurations, both internal and external users can access IBM Connections through a single caching proxy server. In this case, you must disable the public cache to avoid serving public content to external users. To disable the public cache, edit the LotusConnections-config.xml file and add the following directive to the `<properties>..</properties>` section at the end of the file:

```
<genericProperty name="publicCacheEnabled">
    false
</genericProperty>
```

For more information, see the Changing common configuration property values topic in the IBM Connections Knowledge Center.

Desktop Plugins

Before you collaborate with external users, consider whether your internal users use the IBM Connections Desktop Plug-in for Microsoft Windows. Support for external users is limited in the current version of the desktop plug-ins. There are no indicators or warnings to inform users that content they access from Connections and add from their desktop might be visible to external users and there is no ability to control external sharing when creating content.

CCM Libraries

With versions of IBM Connections 5.0 earlier than v5.0 CR2, if Connections Content Manager (CCM) is used in your deployment and external user access is enabled, the URL to FileNet® Collaboration Services (by default /dm/*) must be blocked from external users.

You can block external users by setting rules in a security proxy such as Tivoli® Access Manager. You can also block external users by giving them access only to a separate HTTP server that lacks a mapping for the Library or FileNet Collaboration Services (/dm/*). Test your block by browsing to your FileNet Collaboration Services URL (for instance, http://example.com/dm/) from the network that is used by your external users. This network can be a VPN for your external users or the Internet. If the server returns a valid response, you did not correctly block external users from accessing CCM.

If the URL to FileNet Collaboration Services (/dm) is unblocked, external users might be able to directly access Libraries content in public Communities. When external users are configured for IBM Connections and CCM is enabled, you cannot add CCM Libraries or Linked Libraries to communities to which external users have access. These widgets are not available in those communities.

Starting with IBM Connections 5.0 CR2, CCM will correctly determine if a user is internal or external and respond appropriately.

Connections Mobile

When using the Connections mobile app, external users and externally-facing content are clearly identified as such.

External users cannot currently log in to Connections from the mobile app, but this capability will be supported with IBM Connections 5.0 CR2.

Disable anonymous access

If external users are not forced to authenticate through a mechanism such as Tivoli Access Manager (TAM), you must disable anonymous access for all Connections users. If anonymous access is enabled, external users could anonymously access all public data in IBM Connections, including profiles and public files and communities that were not intended to be shared externally.

For more information about restricting anonymous access, see the Forcing users to log in before they can access an application topic in the IBM Connections Knowledge Center.

Single Sign On

If IBM Connections is enabled with Single Sign On, it is important to recognize and review the potential security implications. While we discussed earlier the importance of ensuring that the firewall only allows external users to interact with IBM Connections and not with other applications, we encourage you to also consider if there could be ramifications if the external user has access to your organization's intranet. For instance, if an external user attends a meeting on-site and Internet access is provided, you could potentially expose the organization's resources to the external user because of their ability to authenticate with SSO.

We encourage you to carefully examine your specific authentication model and determine what an external user could access when they are allowed to authenticate with the IBM Connections deployment.

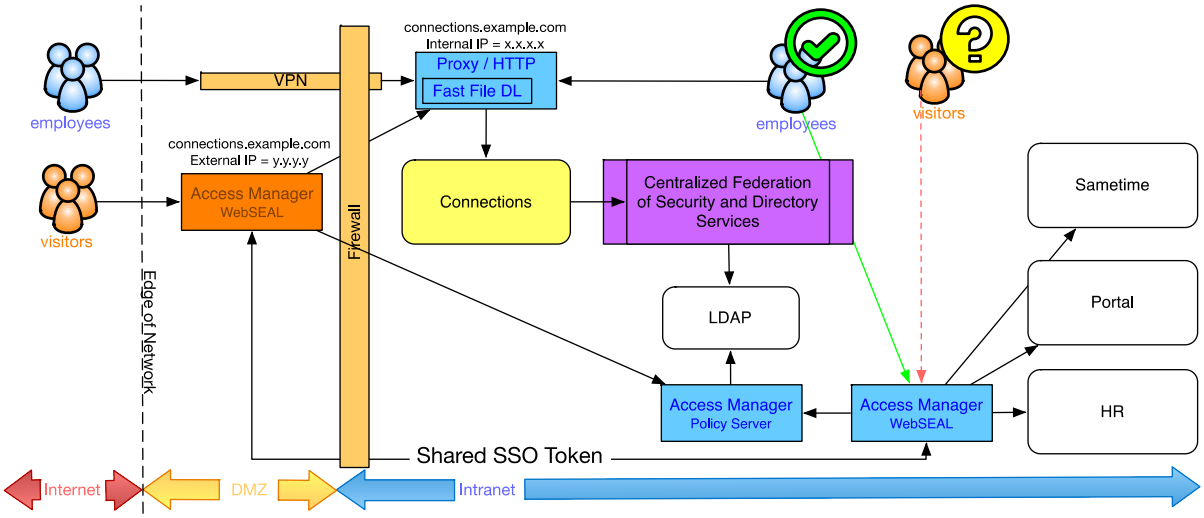

Figure 14. Scenarios exist where additional configuration is required to prevent external users who are present on your organization's premises from gaining access to intranet systems. This example shows how sharing SSO tokens between an internal and an external WebSEAL can allow external users to have inappropriate access to Sametime, Portal, and a HR system.