MICRO FOCUS

Vibe™ 4.0.4

Administration Guide

January 2018

Contents

About This Guide

The *Micro Focus Vibe 4 Administration Guide* provides administration information for Micro Focus Vibe 4.

Audience

This guide is intended for Micro Focus Vibe administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *Micro Focus Vibe 4 Administration Guide* and other documentation, visit the Micro Focus Vibe 4 Documentation website (http://www.novell.com/documentation/vibe4).

Additional Documentation

You can find more information in the Micro Focus Vibe documentation, which is accessible from the Micro Focus Vibe 4 Documentation website (http://www.novell.com/documentation/vibe4).

To access the *Micro Focus Vibe 4 User Guide* from within Vibe, click the **Settings** icon, then click **Help**.

Site Setup

1 Logging In as the Vibe Site Administrator

After logging in to the Micro Focus Vibe site, you should reset the Vibe administrator's password. Also, you might want to create additional Vibe administrators.

- "Logging In" on page 17
- "Changing the Vibe Administrator User ID or Password" on page 17
- "Creating Additional Vibe Administrators" on page 18

Logging In

After installing and configuring Vibe, you need to log in to the Vibe site to perform additional administrative tasks.

1 In your web browser, specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://vibe_hostname
https://vibe_hostname
```

Replace *vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

2 If this is the first time you have logged in to the Vibe site, log in using `admin` as the login name and `admin` as the password.

The Change Password dialog box is automatically displayed when you first log in to the Vibe site.

If this is not your first time logging in, log in using `admin` as the login name and your password.

Changing the Vibe Administrator User ID or Password

When you first install Micro Focus Vibe, the Vibe administrator user name is `admin` and the password is `admin`. When you first log in to the Vibe site as the administrator, you should change the administrator password from the default password to a secure password of your own choosing.

- "Changing the Administrator Password" on page 17
- "Changing the Administrator User ID and Other Profile Information" on page 18

Changing the Administrator Password

You can change your password to a new password at any time:

1 In your web browser, specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://vibe_hostname:8080
https://vibe_hostname:8443
```

Replace `vibe_hostname` with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

2 (Conditional) If this is your first time accessing the site, log in using `admin` as the login name and `admin` as the password.

   The Change Password dialog box is automatically displayed when you first log in to the Vibe site.

3 (Conditional) If this is not your first time accessing the site, log in using the administrator user name and password, then change your password as described in “Changing Your Password” in the *Micro Focus Vibe 4.0.5 User Guide*.

Changing the Administrator User ID and Other Profile Information

You might want to change the administrator User ID in addition to other information on the administrator’s user profile.

- **User ID:** As a security precaution, it might make sense to change the administrator’s user ID from the default `admin`. The administrator user ID is used only when logging in to the Vibe system.

  Changing the administrator user ID requires that you restart each Vibe appliance in the Vibe system in order for the change to take effect.

- **First Name and Last Name:** Providing a first and last name for the administrator changes the name that appears in the upper-right corner of each Vibe page, as well as the name that appears in the administration console under **Administrators**.

To change the Vibe administrator user ID, as well as other profile information, follow the steps in “Modifying Your Profile” in the *Micro Focus Vibe 4.0.5 User Guide*.

Creating Additional Vibe Administrators

Only the original (built-in) Vibe administrator can add or remove site administrator rights for users and groups.

Additional Vibe administrators have rights to administer the following:

- Users
- Groups
- Mobile Devices

Assigning Administrative Rights to a User or Group

1 Log in to Vibe as the Vibe administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://vibe_hostname:8080
https://vibe_hostname:8443
```

Replace `vibe_hostname` with the host name or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 In the **Management** section, click **Administrators**.

4 Click **Add**, then begin typing the name of the user or group for whom you want to grant administrator rights.

5 Click the user or group name when it appears in the drop-down list.

To remove administrator rights from a user or group:

1 Select the users or groups for whom you want to remove administrator rights.

2 Click **Remove**.

Creating an Administration Group

You can create an administration group and assign rights only to that group:

1 Log in to Vibe as the Vibe administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://vibe_hostname:8080
https://vibe_hostname:8443
```

Replace `vibe_hostname` with the host name or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Create an administration group, described in "Creating Groups of Users" on page 97.

3. Assign administrator rights to that group, as described in "Assigning Administrative Rights to a User or Group" on page 19.
4. When you want to grant administrative rights to a user, add that user to the administrator group that you created. (For information about how to add users to a group, see "Modifying Groups" on page 229.)

2 Planning and Controlling User Access to Workspaces and Folders

As the administrator for the Micro Focus Vibe site, you are responsible for setting up and controlling user access across the entire site. Even though workspace and folder owners are responsible for controlling user access in their individual workspaces and folders, you as the Vibe administrator have the ability to create new roles, modify existing roles, and change default access control settings for all types of workspaces and for all types of functions across the Vibe site.

Understanding Access Control

Access control is how you specify which users have the right to perform which tasks in which places. Because your Micro Focus Vibe site is a hierarchy of workspaces and folders and because access control settings can be inherited (or not), access control settings affect a variety of Vibe features

Micro Focus Vibe uses role-based access control. By default, there are seven roles, and each role contains specific rights. If you want a particular user to have certain rights, you can assign that user to the appropriate role.

For example, a user who has been assigned to the Participant role in a workspace or folder can add comments or replies, create entries, delete his or her own entries, modify his or her own entries, and read entries in that folder or workspace.

The following sections help you better understand how access control works in Vibe.

Inheritance

Workspaces can inherit the access control settings of their parent workspaces. You should understand the following facts about access control inheritance:

- If you create a new workspace under an existing workspace that is inheriting its access control settings from its parent, the new workspace continues the inheritance chain. If you change any access control settings above the new workspace at a later time, the access control settings for the new workspace also change. Global workspaces inherit access control settings from the parent workspace by default.
- If you create a new workspace under an existing workspace that is not inheriting its access control settings, the new workspace retains the non-inherited settings of the parent workspace.
- If you move a workspace that is inheriting its access control settings from its original parent workspace, it inherits the access control settings of the new parent workspace into which it is moved. If the new parent workspace has different settings than the original parent workspace, the access control settings for the moved workspace change accordingly.
- Team membership is inherited separately from access control settings. If access control settings are being inherited, this does not necessarily mean that team membership is also being inherited. To edit team membership or to change the team membership inheritance settings for a team workspace, click the **Configure** icon next to the workspace title, then click **Edit Team**.

Navigation

As a best practice, you should not grant users access to sub-workspaces and sub-folders while restricting access for the same users to the higher-level (parent) folders. Ignoring this best practice can be problematic for the following reasons:

- Users cannot navigate to the sub-workspace or sub-folder using the Workspace tree navigation, even though they have appropriate rights to the sub-workspace or sub-folder.

  If you understand this limitation and still have a need to restrict access to a parent workspace or folder while granting access to a sub-workspace or sub-folder, users can still access the hidden sub-workspace or sub-folder by using the Search feature or by accessing the location through WebDAV.
- Users can see the name of a higher-level workspace, even though they do not have appropriate rights.

  Users who use the Search feature or WebDAV to locate the sub-workspace or sub-folder that they have been granted access to are able to see the name of the parent workspace, which they would otherwise not be able to see. However, they can see only the workspace name, not the contents of the workspace.

Default Access Control Behavior in Workspaces

By default, most places inherit the access control settings of their parent. When you establish settings for a primary space, all sub-places automatically apply the same settings, saving administration time. However, unlike other types of workspaces, Team workspaces do not retain the access control settings of the parent workspace by default. This is because the desired access control settings for Team workspaces can vary greatly depending on the objectives of the team.

Also, team membership is inherited separately from access control settings. If access control settings are being inherited, this does not necessarily mean that team membership is also being inherited. To edit team membership or to change the team membership inheritance settings for a team workspace, click **Workspace** > **Edit Team**.

Default User Rights

By default, all Vibe users have rights to perform the following actions:

- Participate in any team workspaces in which they are a member (create folders and entries, make comments, and so forth)
- Create team workspaces (by default, only members of a team can view and participate in team workspaces)
- Visit all personal workspaces (read entries and comment on them)
- Participate in all global workspaces and folders

Default Roles

Vibe includes default roles that you can assign to users and groups. The following sections describe the function of each default role, but does not describe all of the rights associated with each role. For a complete list of rights, click the name of the role in the table on the Configure Access Control page.

(Click the **Configure** icon next to the workspace or folder title, then click **Access Control**.)

For information on how the administrator can assign users to various roles for the Vibe site, see "Controlling User Access throughout the Vibe Site" on page 29. For a detailed description of each right that can be associated with a given role, see "Understanding the Various Rights for Roles" on page 36.

Vibe enables site administrators to create their own custom roles, as described in "Defining a New Role" on page 31.

Understanding Default Roles for Workspaces and Folders

Role	Description
Allow Sharing With Internal Users	Can share workspaces and folders with internal users.
Allow Sharing With External Users	Can share workspaces and folders with external users.

Role	Description
Allow Forwarding of Sharing Rights	When sharing, can allow users to re-share workspaces and folders.
Allow Sharing With The Public	Can share workspaces and folders with the Public.
Allow Sharing File Links	Can share File Links.
Visitor	Has read-only and comment-only access.
Participant	Can create entries and modify those entries, can download folder content as a CSV file, plus perform tasks associated with the Visitor role.
Guest Participant	Can read entries, create entries, and add comments.
Team Member	Has all the rights of a Participant. In addition, can generate reports and manage global tags.
Workspace and Folder Administrator	Can create, modify, or delete workspaces or folders; moderate participation (modify or delete the entries of others); design entries and workflows; set entry-level access controls on entries of others; and perform tasks associated with the Participant and Team Member role.
Workspace Creator	Can create sub-workspaces. In Team Workspace Root workspaces, this role lets users users to create their own team workspaces.

Understanding Default Roles for Entries

Role	Description
Owner Create Entry ACLs	The owner of the entry can create entry-level access controls.
Read	Can read the entry.
Read and Reply	Can read the entry and add comments or replies to the entry.
Write	Can read the entry, add comments or replies, and modify the entry.
Delete	Can read the entry, add comments or replies, modify, and delete the entry.
Change Access Controls	Can read the entry, add comments or replies, modify, and delete the entry. Can also modify the access control settings of the entry.

Understanding Default Administrative Roles

Role	Description
Allow Adding Guest Access	Can make Vibe workspaces and folders available to Guest users in Vibe. By default, Guest users can access only the Guest user personal workspace, as well as any workspace or folder that the Vibe administrator has granted them rights to access. For more information, see “Enabling Individual Users to Grant Guest Access throughout the Vibe Site” on page 107.

Role	Description
Can Only See Members Of Groups I Am In	Removes a user’s ability to view other Vibe users who are not members of a group that he or she belongs to.
Override “Can Only See Members Of Groups I Am In”	Overrides the **Can Only See Members Of Groups I Am In** role. This can simplify the administration of the **Can Only See Members Of Groups I Am In** role. For example, you might assign the **Can Only See Members Of Groups I Am In** role to a group, but at the same time you want to allow certain members of the group to retain their ability to see users that belong to groups outside of their own. In this circumstance, you can assign the **Override “Can Only See Members Of Groups I Am In”** role to the members who you want to retain their ability to see users outside of their own groups.
Token Requester	Can make web service calls on behalf of another Vibe user. This functionality can enable administrators to perform proxy functions for individual Vibe users without logging in as the Vibe user. This means that the web services application does not cache individual users’ credentials in order to perform operations. This role should not be assigned to a Vibe user, but rather to a system-level (agent) account that you want to be responsible for executing web service operations on behalf of one or more regular Vibe users. For more information about the web services operations that support the Token Requester role, see “admin_getApplicationScopedToken” and “admin_destroyApplicationScopedToken” in the *Micro Focus Vibe 4.0.5 Developer Guide*.
Zone Administration	Has all rights associated with access control.

Default Users and Groups

You can assign default or custom access control roles to users and groups for the Vibe site if you are the Vibe administrator, or in your workspaces if you are a workspace owner. In addition to the users and groups that the Vibe administrator creates, Vibe includes four default users and groups to which you can assign roles.

Default User and Group	Description
Owner of a Workspace or Folder	The person who created the workspace, or the person assigned to be the owner of the workspace.
Team Members	The individuals who are designated as team members in a given place. For information about how to add team members, see “Adding Additional Team Members to Your Workspace” in the *Micro Focus Vibe 4.0.5 User Guide*.
All Users	Every person registered within the Vibe site.
Site Administrator	The person who has rights to perform any task in any workspace or folder. Available only to Vibe administrators.

Controlling User Access in Workspaces

The access control settings on each Micro Focus Vibe workspace determine who can see the workspace and how different types of users can participate in each workspace.

- "Controlling User Access to Personal Workspaces" on page 26
- "Controlling User Access to Team Workspaces" on page 27
- "Controlling User Access to Global Workspaces" on page 28

Controlling User Access to Personal Workspaces

- "Default Access Controls" on page 26
- "Restricting Access to Personal Workspaces throughout the Vibe Site" on page 26

Default Access Controls

By default, personal workspaces are created with the following access:

User or Group	Access Role	Role Description
Workspace Owner (user)	Administrator	Can create, modify, or delete workspaces or folders; moderate participation (modify or delete the entries of others); design entries and workflows; and can perform Participant tasks.
All Users group	Visitor	Has read-only and comment-only access.

Restricting Access to Personal Workspaces throughout the Vibe Site

You might want to set up your Vibe site so users' personal workspaces remain hidden and confidential.

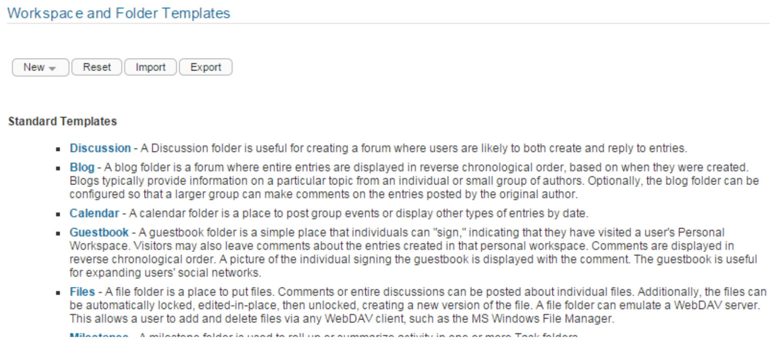
IMPORTANT: If you configure your Vibe site to hide users' personal workspaces as described in this section, the following side effects occur:

- Users cannot follow one another
- Users are not displayed in the Personal Workspaces workspace
- Users are not displayed under Personal Workspaces in the Workspace tree
- User workspaces and user profiles cannot be found when performing a search (this means that users cannot search for and find other Vibe users.)

When you configure your Vibe site as described in this section, you should make these configuration changes before any users are added to your Vibe system. If users are added to your Vibe system before you make these configuration changes, you must manually adjust the access control settings for each user workspace, as described in "Controlling Access" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

2 Under **Management**, click **Workspace and Folder Templates**.



3 Click **User Workspace**.

4 Click **Manage This Target** > **Access Control**.

The Configure Access Control page is displayed.

5 In the access control table, in the **All Users** row, deselect the check box in the **Visitor** column.

6 Click **Save Changes**.

7 Verify access before you start adding users to your Vibe system:

- Create a test user in the Vibe system, navigate to this user's personal workspace, then click **Workspace** > **Access Controls**. Ensure that no check boxes are selected in the **All users** row.
- Navigate to the Personal Workspaces workspace by clicking the Workspace tree icon in the Action toolbar, then clicking **Personal Workspaces**. Click the **Configure** icon next to the workspace title, then click **Access Controls**. Ensure that in the **All users** row the check box is selected in the **Visitor** column. If this check box is not selected, users cannot search for other users in the Vibe system.

For information on how to add users to your Vibe system, see "Adding New Users to Your Vibe Site" on page 97.

Vibe users can adjust the access control for their personal workspaces, as described in "Controlling Access" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Controlling User Access to Team Workspaces

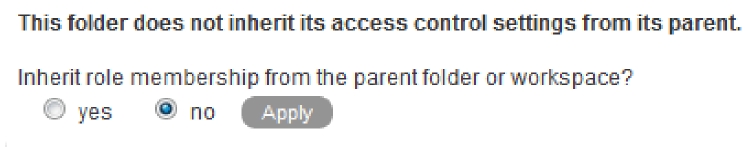
By default, new team workspaces created under the main Team Workspaces directory are visible only to members of the team workspace. Following are the default access control settings for a team workspace:

User or Group	Access Role	Role Description
Workspace Owner (team creator)	Administrator	Can create, modify, or delete workspaces or folders; moderate participation (modify or delete the entries of others); design entries and workflows; and can perform Participant tasks.
Team Members	Team Member	Has all the rights of a Participant. In addition, can generate reports and manage community tags.

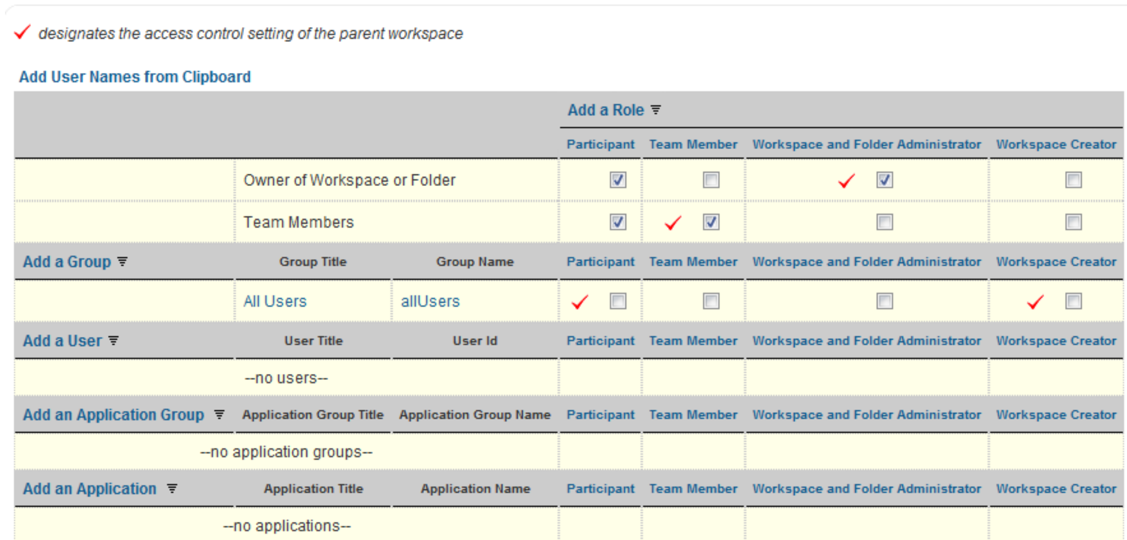
After you create a new team workspace, you can configure different access control settings for it.

1 Navigate to the new team workspace, then click **Workspace > Access Control**.

2 Select **No** in the Inheritance box.



3 Click **Apply** to activate the Access Control table:



4 Adjust the access control settings for the new team workspace as needed, as described in "Controlling Access to Workspaces and Folders" in "Controlling Access" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

5 Click **Save Changes** > **Close**.

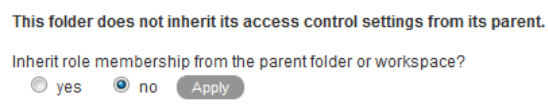
Controlling User Access to Global Workspaces

By default, the Global Workspace directory immediately under the Home Workspace inherits the access control settings of the Home Workspace:

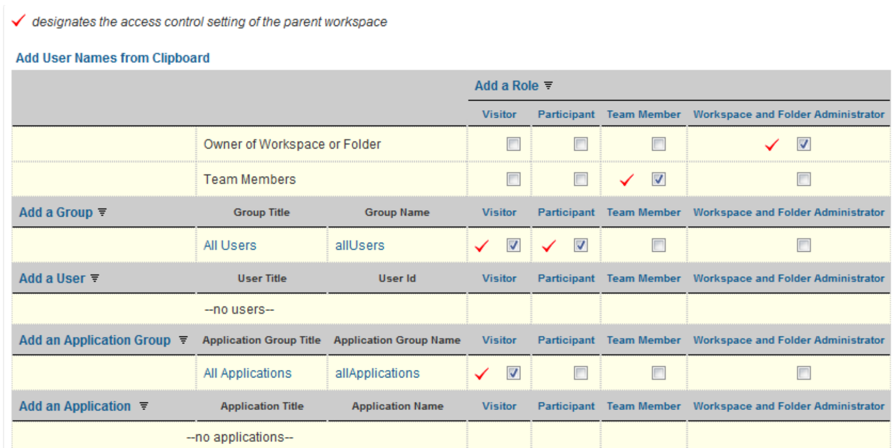
User or Group	Access Role	Role Description
Workspace Owner (admin)	Administrator	Can create, modify, or delete workspaces or folders; moderate participation (modify or delete the entries of others); design entries and workflows; and can perform Participant tasks.
Team Members	Team Member	Has all the rights of a Participant. In addition, can generate reports and manage community tags.
All Users group	Participant	Can create and modify entries, plus perform the Visitor tasks.
	Visitor	Has read-only and comment-only access.
All Applications group	Visitor	Has read-only and comment-only access. For information about application groups, see "Managing Remote Applications" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

When you create a new global workspace under the main Global Workspaces directory, the new global workspace by default inherits the access control settings of the main Global Workspaces directory, as listed above. After you create a new global workspace, you can configure different access control settings for it.

1 Navigate to the new global workspace, then click **Workspace > Access Control**.
2 Select **No** in the Inheritance box.



3 Click **Apply** to activate the Access Control table:



			Add a Role			
			Visitor	Participant	Team Member	Workspace and Folder Administrator
	Owner of Workspace or Folder		☐	☐	☐	✓ ☑
	Team Members		☐	☐	✓ ☑	☐
Add a Group	Group Title	Group Name	Visitor	Participant	Team Member	Workspace and Folder Administrator
	All Users	allUsers	✓ ☑	✓ ☑	☐	☐
Add a User	User Title	User Id	Visitor	Participant	Team Member	Workspace and Folder Administrator
	--no users--					
Add an Application Group	Application Group Title	Application Group Name	Visitor	Participant	Team Member	Workspace and Folder Administrator
	All Applications	allApplications	✓ ☑	☐	☐	☐
Add an Application	Application Title	Application Name	Visitor	Participant	Team Member	Workspace and Folder Administrator
	--no applications--					

4 Adjust the access control settings for the new global workspace as needed, as described in "Controlling Access" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
5 Click **Save Changes** > **Close**.

Controlling User Access throughout the Vibe Site

By assigning users to access control roles for the Micro Focus Vibe site, you can give users additional rights, or restrict current rights.

- "Controlling User Access to Administrative Functions" on page 29
- "Controlling User Access to Workspaces, Folders, and Entries" on page 30

Controlling User Access to Administrative Functions

You can create additional Vibe administrators as described in "Creating Additional Vibe Administrators" on page 18.

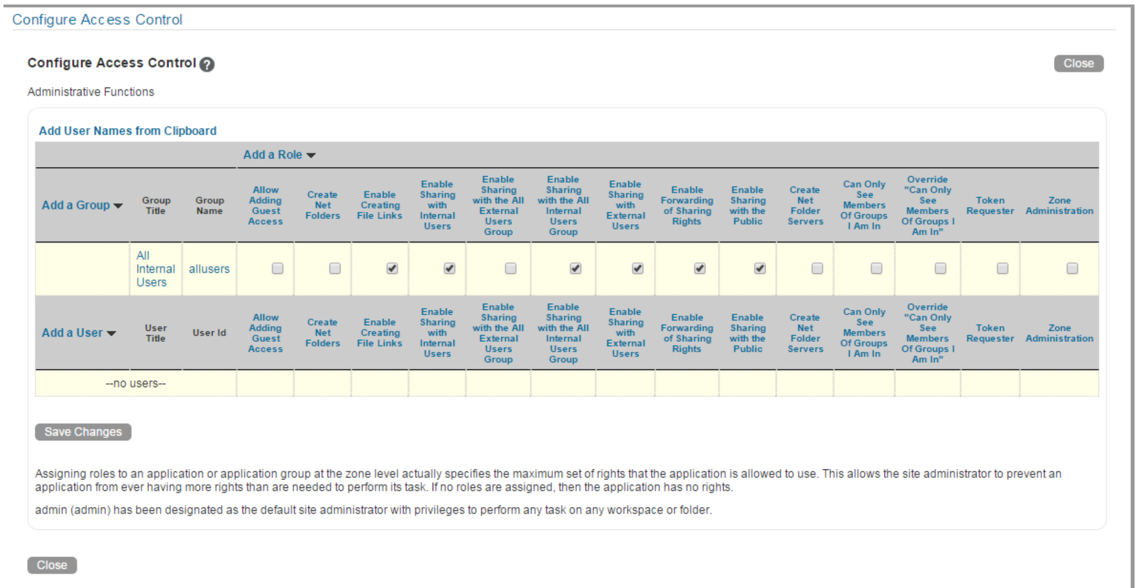
This section describes how you can make more granular access settings.

Administrative roles grant users rights to perform administrative functions throughout your Vibe site. As the Vibe administrator, you can assign users and groups to administrative roles. For a list of default administrative roles, see "Understanding Default Administrative Roles" on page 24.

To assign a user to a particular role for every place on the Vibe site:

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

   The Administration page is displayed.
3. Under **System**, click **Access Control**.



   A basic Vibe site consists of a single zone. Micro Focus Vibe lets you set up multiple zones in a single Vibe site. For more information about creating multiple zones, see Chapter 19, “Setting Up Zones (Virtual Vibe Sites),” on page 195.
4. Add the user to whom you want to grant the site-wide role to the Access Control table.

   For information on how to add users to the Access Control table, see “Adding Users to the Access Control Table” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
5. Add the role that you want to grant to the Access Control table.

   For information on how to add roles to the Access Control table, see “Adding Roles to the Access Control Table” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
6. Click **Save Changes**, then click **Close**.

Controlling User Access to Workspaces, Folders, and Entries

Workspace and folder roles define which rights users have in specific workspaces and folders throughout the Vibe site. Entry roles define which rights users have in specific entries.

Workspace and folder owners (or anyone with administrative rights) can assign workspace and folder roles to specific users and groups by configuring access controls for their workspaces and folders. For more information about how to do this, see “Managing Access Control for Users and Groups” in “Controlling Access” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

As the Vibe administrator, you can modify each default role for workspaces, folders, or entries to suit your organization’s needs. These roles are then made available so that workspace and folder administrators can assign them to users and groups in their workspaces and folders. For information about how to modify existing roles or about how to create new roles, see “Managing Roles to Refine Access Control” on page 31.

Managing Roles to Refine Access Control

Micro Focus Vibe uses role-based access control. Each default role contains specific rights. If you want a particular user to have certain rights, you can assign that user to the appropriate role. For a list of all the default access roles that are included in Vibe, see “Default Roles” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

If you find that the existing roles do not meet the needs of your organization, you can modify them or create new ones. This can be particularly useful if you want to delegate the administration of sub-workspaces and sub-folders, and if you do not want to grant all of the privileges that come with the Workspace and Folder Administration role.

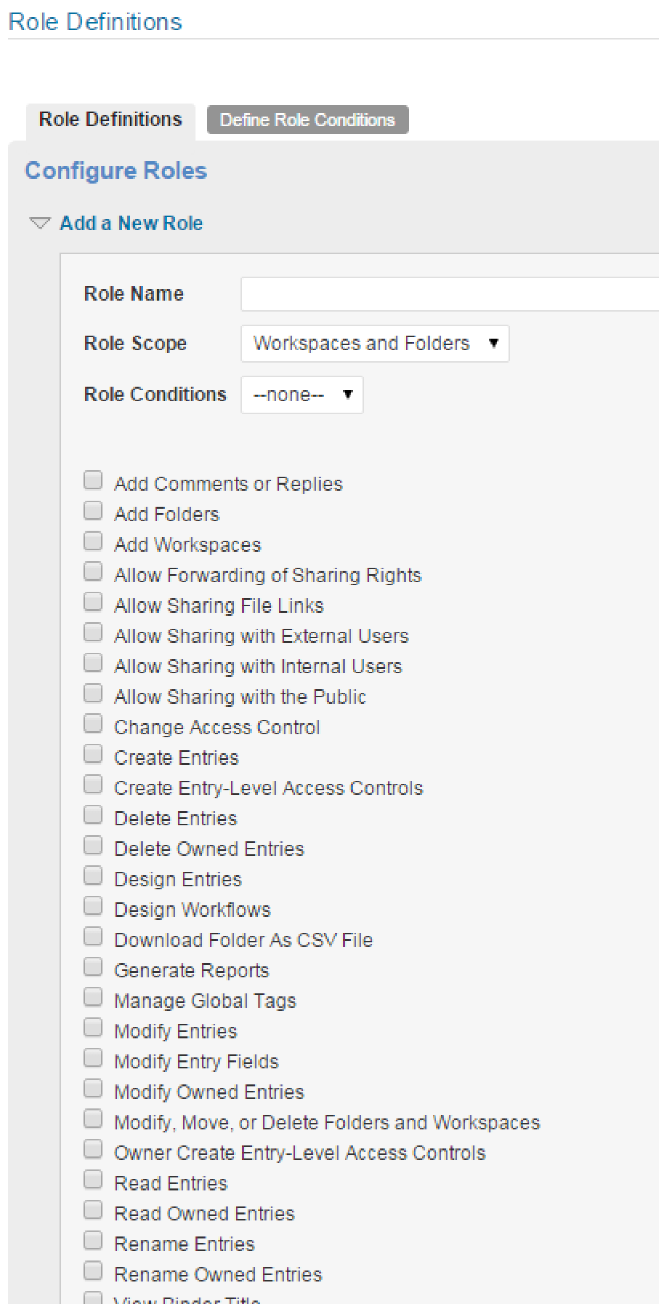
Vibe also lets you delete roles that are no longer useful to your organization.

Defining a New Role

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

   The Administration page is displayed.
3. Under **System**, click **Role Definitions**.

4 Click **Add a New Role**.



5. In the **Role Name** field, specify a name for the new role, then select all of the rights that you want members of this role to be able to perform.
6. In the **Role Scope** drop-down list, select whether you want this new role to be available for workspaces or folders, or for entries.
7. (Optional) In the **Role Conditions** field, select the role condition that you want to associate with this role.

   Role conditions enable you to restrict what information users can access when they are outside your corporate firewall. For more information, see "Restricting Access Rights of Users Outside the Firewall" on page 38.
8. Select the rights that you want to be associated with this role.

For information about each right that you can select, see "Understanding the Various Rights for Roles" on page 36.

9 Click **Add**, then click **Close**.

The role is added to the list of existing roles. If you added this role to control access to entries, the role is automatically made available on the access control page. If you added this role to control access to workspaces and folders, Vibe users can now add this role to the Access Control table, as described in "Adding Roles to the Access Control Table" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Modifying Existing Roles

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

The Administration page is displayed.

3 Under **System**, click **Configure Role Definitions**.

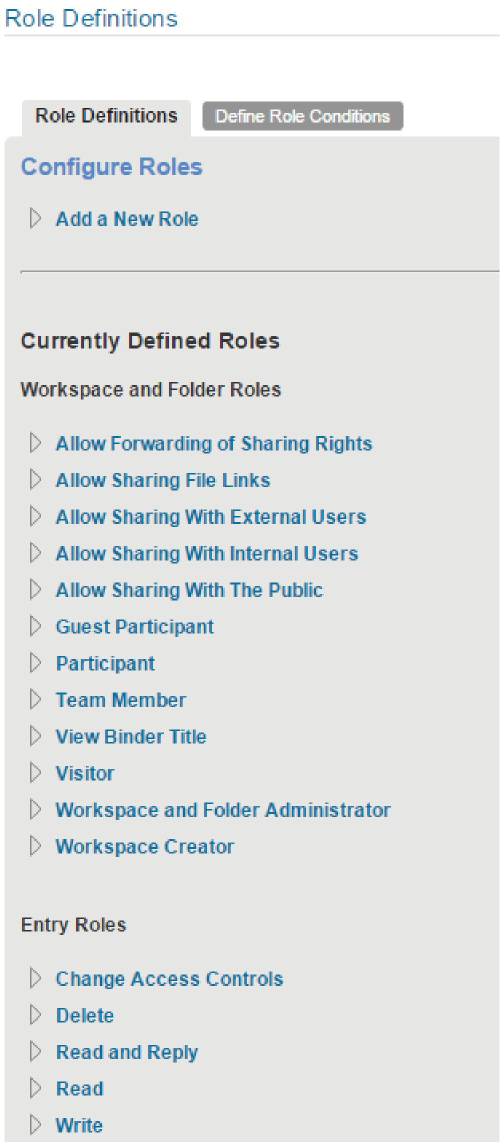
4. In the **Currently Defined Roles** section, click the role that you want to modify.
5. Select the rights that you want members of this role to be able to perform, and deselect the rights that you don't want them to be able to perform.

   For information about each right that you can select, see "Understanding the Various Rights for Roles" on page 36.
6. Click **Apply**, then click **Close**.

Deleting Existing Roles

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

   The Administration page is displayed.
3. Under **System**, click **Configure Role Definitions**.



4 In the **Currently Defined Roles** section, click the role that you want to delete.

5 Click **Delete**, then click **Close**.

Understanding the Various Rights for Roles

Roles are made up of various rights. Default roles have a set of default rights that are associated with them. When you modify a default role, you remove existing rights and add other rights. When you create a custom role, you create a new name for a role and then associate rights with the new role.

Some rights apply only to workspaces and folders, and some apply only to entries. If you associate a right with a role, and then assign users to that role in a workspace, then by default that role applies to all folders and entries in the workspace. For example, if you associate the Delete Entries right with a role in a workspace and assign that role to all users, then all users can delete any entry in the workspace.

Following is the list of rights you can choose from when modifying or creating a role. You cannot create new rights in Vibe.

Right	Function
Add Comments or Replies	Can add comments or replies to entries.
Add Folders	Can add folders to workspaces and folders.
Add Workspaces	Can add workspaces to existing workspaces.
Allow Forwarding of Sharing Rights	Can grant users the ability to re-share items when sharing.
Allow Sharing File Links	Can share File Links.
Allow Sharing with External Users	Can share items with users who are external to the Vibe system.
Allow Sharing with Internal Users	Can share items with users who are internal to the Vibe system.
Allow Sharing with the Public	Can share items to the Public. Items are publicly available if Guest access has been enabled.
Change Access Control	Can modify the access control settings of workspaces, folders, or entries.
Create Entries	Can create entries.
Create Entry-Level Access Controls	Can change access control settings for all entries that are contained in a workspace or folder.
Delete Entries	Can delete entries.
Delete Owned Entries	Users can delete only the entries they own in a workspace or folder.
Design Entries	Users can design their own custom entries by using the Form and View Designers tool, as described in "Designing Custom Folder Entry Forms" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
Design Workflows	Users can design their own custom workflows by using the Form and View Designers tool, as described in "Creating and Managing Workflows" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
Generate Reports	Users can generate reports. For more information about generating reports in Vibe, see "Generating Activity Reports for a Workspace", "Generating an Activity Report on a Folder", and "Generating Reports about a Folder Entry" in the *Micro Focus Vibe 4.0.5 User Guide*.
Manage Global Tags	Users can manage community tags, as described in "Using Tags" in the *Micro Focus Vibe 4.0.5 User Guide*.
Modify Entries	Can modify entries.
Modify Entry Fields	Users can modify only a specific field in an entry. This is useful if you have an entry that is associated with a workflow, and you want only certain users to modify certain fields in the entry.
Modify Owned Entries	Users can modify only the entries they own in a workspace or folder.
Modify, Move, or Delete Folders and Workspaces	Users can modify, move, or delete a folder or workspace.
Owner Create Entry-Level Access Controls	Users can change the access control settings only for the entries they own in a workspace or folder.
Read Entries	Can read entries.

Right	Function
Read Owned Entries	Users can read only the entries they own in a workspace or folder.
Rename Owned Entries	Users can rename only the entries they own in a workspace or folder.
View Binder Title	Enables users who have access to an entry, but do not have access to the parent workspace or folder, to navigate to the entry by using the Workspace tree, as described in "Navigating the Workspace Tree" in the *Micro Focus Vibe 4.0.5 User Guide*. This right is disabled by default, and is not available to assign to any role. For information on how to enable this right and make it available, see "Enabling Users to Access Entries via the Workspace Tree When They Do Not Have Access to the Parent Folder or Workspace" on page 42.

Restricting Access Rights of Users Outside the Firewall

Vibe lets you restrict what information users can access when they are outside your corporate firewall.

If your Vibe site contains sensitive data, and users access the site from non-secure locations, you might want to consider restricting users to certain workspaces and folders when they are not accessing Vibe from inside the corporate firewall.

For example, a user accessing the Vibe system from a public kiosk increases the risk of sensitive data being inappropriately exposed.

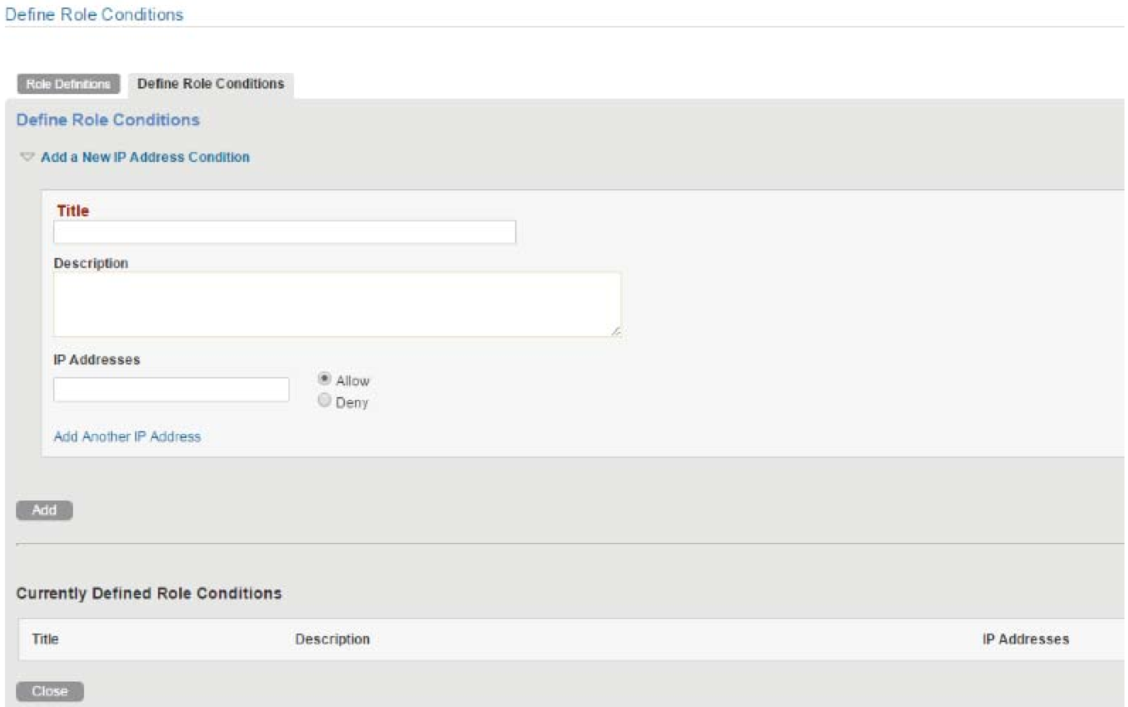
To restrict access for users who are outside the corporate firewall, you must create a condition that contains one or more IP addresses (or range of IP addresses), associate this condition with an existing role, then assign the role to users and groups in the workspaces, folders, or entries where you want to allow access.

- "Creating a New Role Condition" on page 38
- "Associating the Role Condition with a New or Existing Role" on page 40
- "Assigning the Role Condition to Users and Groups" on page 40
- "Example" on page 41

Creating a New Role Condition

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

   The Administration page is displayed.
3. Under **System**, click **Role Definitions**.
4. Click the **Define Role Conditions** tab.
5. Click **Add a New IP Address Condition**.



6 Provide the following information for the new condition:

Title: Specify a title for the condition.

Description: Specify a description for the role condition.

IP Address: Specify the IP address that you want to associate with this condition.

You can mask your IP address by using asterisks. For example, 155.5.*.*

Allow: Select this option to allow access from the specified IP address. There must be at least one **IP Address** field with **Allow** selected.

Deny: Select this option to deny access from the specified IP address. Select this option only if you have multiple **IP Address** fields, and one of these fields has **Allow** selected.

If you are masking an IP address, such as 155.5.*.*, you can exclude an IP address within the range that you are masking. For example, in the first **IP Addresses** field you specify `155.5.*.*`, then select **Allow**. You then add a second **IP Address** field by clicking **Add Another IP Address**, then specifying an IP address that is within the range of your masked IP address. In your second **IP Address** field, you specify `155.5.4.*`, then select **Deny**. This denies access to users who are using an IP address within the range 155.5.4.*, but allows access to users using any other IP address within the range 155.5.*.*.

7 (Optional) Click **Add Another IP Address** to associate multiple IP addresses with this condition. You can also add multiple IP addresses if you want to deny access to a specific IP address that is included within a range of IP addresses that you are allowing.

8 Click **Add**.

9 Continue with "Associating the Role Condition with a New or Existing Role" on page 40.

Associating the Role Condition with a New or Existing Role

You must associate the role condition that you created in "Creating a New Role Condition" on page 38 with a new or existing role.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

   The Administration page is displayed.
3. Under **System**, click **Role Definitions**.
4. On the **Role Definitions** tab, click **Add a New Role**.

   or

   Click an existing role in the **Currently Defined Roles** section.

   For more information about managing roles, see "Managing Roles to Refine Access Control" on page 31.
5. In the **Role Conditions** drop-down list, select the role condition that you want to associate to the role.
6. Click **Apply**.
7. Continue with "Assigning the Role Condition to Users and Groups" on page 40.

Assigning the Role Condition to Users and Groups

After you have completed "Creating a New Role Condition" on page 38 and "Associating the Role Condition with a New or Existing Role" on page 40, you need to assign the role that contains the new role condition to users and groups. You accomplish this in one of two ways, depending on whether you associated the role condition to a new role or an existing role (as described in "Associating the Role Condition with a New or Existing Role" on page 40):

- "Assigning the New Role to Users and Groups" on page 40
- "Assigning an Existing Role to Users and Groups" on page 40

Assigning the New Role to Users and Groups

To assign the role that contains the new role condition to users and groups:

1. Add the role to the Access Control table for the workspaces, folders, or entries where you want to grant users access rights, as described in "Controlling Access to Workspaces and Folders" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
2. Assign the roles to the users and groups who you want to be granted access rights, as described in "Controlling Access to Workspaces and Folders" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Assigning an Existing Role to Users and Groups

If you associated the role condition with an existing role, the role is automatically applied to users and groups in workspaces, folder, and entries where this role is already assigned.

Example

The following example shows how to restrict access to users outside the firewall by using role conditions:

1. Set up a proxy server (such as NetIQ Access Manager) that is external to the firewall.
2. Define a role condition that includes only a range of IP addresses that are internal to the firewall.
3. Associate this role condition to all or some existing Vibe roles.

   If you associate this role condition to all roles except the Workspace and Folder Administrator role, only users who are workspace and folder administrators are able to access workspaces and folders from outside the firewall. Users who are not workspace and folder administrators do not have access.

Enabling Users to Send Messages to All Users

By default, Micro Focus Vibe allows only the Vibe administrator to send email messages to the All Users group. If you want to change this functionality to allow anyone to send messages to the All Users group:

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
mail.allowSendToAllUsers=false
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `mail.allowSendToAllUsers=false` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `false` to `true`, so that the line now reads `mail.allowSendToAllUsers=true`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe to enable users to send messages to the All Users group in your Vibe site.

Enabling Users to Send Messages to All Users

By default, Micro Focus Vibe allows only the Vibe administrator to send email messages to the All Users group. If you want to change this functionality to allow anyone to send messages to the All Users group:

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
mail.allowSendToAllUsers=false
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `mail.allowSendToAllUsers=false` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `false` to `true`, so that the line now reads `mail.allowSendToAllUsers=true`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe to enable users to send messages to the All Users group in your Vibe site.

Enabling Users to Access Entries via the Workspace Tree When They Do Not Have Access to the Parent Folder or Workspace

You can enable users who have access to an entry, but do not have access to the parent workspace or folder, to navigate to the entry by using the Workspace tree, as described in "Navigating the Workspace Tree" in the *Micro Focus Vibe 4.0.5 User Guide*.

Users who do not have this right must either perform a search to locate the entry, or they must have the entry shared with them as described in "Sharing Entries, Folders, and Workspaces" in the *Micro Focus Vibe 4.0.5 User Guide*.

For information about how users can grant other Vibe users access to an entry even when users don't have access to the parent workspace or folder, see "Exposing a Vibe Entry to a Wider Audience Than the Folder Access Controls Allow" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

To enable users to access entries via the Workspace tree when users do not have access rights to the parent folder or workspace:

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
accessControl.viewBinderTitle.enabled=false
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `accessControl.viewBinderTitle.enabled=false` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `false` to `true`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe.

Enabling Folder Administrators to Apply Definition Settings to Sub-Folders and Entries

You can enable folder owners to apply entry definition types to folders or entries that have already been created. This enables users to apply all definition settings of a parent folder to all subfolders. Also, this enables users to change the definition settings to make all folder entries the same. For example, a user might begin a discussion entry in a Discussion folder, then move the entry to the Tasks folder after it is decided that something needs to be done in order to resolve the discussion. After the discussion entry is added to the Tasks folder, the entry can be converted to a task entry. For more information, see "Changing the View Definitions for Existing Folders and Folder Entries" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
ssf.allowFolderDefinitionFixups=false
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the appropriate line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `false` to `true`, so that the line now reads `ssf.allowFolderDefinitionFixups=true`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe.

3 Setting Up Initial Workspaces

Proper organization of workspaces is critical to building an effective Micro Focus Vibe site.

See also Chapter 23, "Managing Workspaces," on page 231.

Understanding Workspaces

Your Micro Focus Vibe site consists of seven types of workspaces:

- **Personal workspaces:** When you add users to your Vibe site, as described in "Adding Users to Your Vibe Site" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*, a personal workspace is established for each user. Users can customize their personal workspaces, as described in "Setting Up Your Personal Workspace" in "Getting Started" in the *Micro Focus Vibe 4.0.5 User Guide*.
- **Team workspaces:** Vibe users, along with you as the Vibe administrator, can create team workspaces for groups of people who work together regularly, as described in "Setting Up Your Personal Workspace" in "Getting Started" in the *Micro Focus Vibe 4.0.5 User Guide*. You, as the Vibe administrator, need to decide how you want to organize team workspaces before you let users start creating them.
- **Team Workspace Root workspaces:** Team Workspace Root workspaces are the optimal type of workspace if you want to create a library of team workspaces as sub-workspaces.

  For more information on Team Workspace Root workspaces, see "Creating and Managing a Team Workspace Root Workspace" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- **Project Management Workspaces:** Project Management workspaces include special accessories that help leaders track the progress of task completion for potentially large projects. Project Management workspaces focus on project completion.

  For more information on Project Management workspaces, see "Creating and Managing a Project Management Workspace" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- **Discussions workspaces:** The Discussions workspace can be the home page for a set of discussion forums. You can also use the Discussions workspace to house other types of folders. Discussions workspaces can be particularly useful for site administrators who are responsible for creating the overall structure of the Vibe site.

  For more information on how you can use Discussions workspaces, see "Creating and Managing a Discussions Workspace" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- **Basic workspaces:** Like other types of Vibe workspaces, basic workspaces in Vibe can be used to organize information inside of existing workspaces, creating different levels of hierarchy within a workspace.

For more information on basic workspaces, see “Creating and Managing a Basic Workspace” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

- **Global workspaces:** Global workspaces contain information that is of interest to all Vibe users. You, as the Vibe administrator, decide what type of information needs to be globally available on your Vibe site.

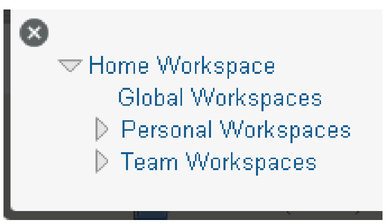
  For more information on Global workspaces, see “Creating Global Workspaces” on page 60.

Setting Up Users’ Personal Workspaces

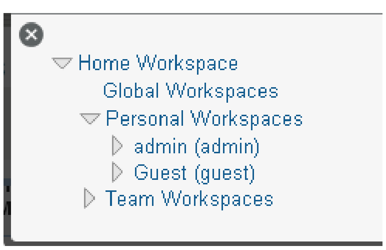
See also “Controlling User Access to Personal Workspaces” on page 26.

Understanding Personal Workspaces

When you create your Micro Focus Vibe site, a workspace named Personal Workspaces is automatically created.



Initially, clicking the **Workspace tree** icon and expanding **Personal Workspaces** lists only two personal workspaces, even after you have created Vibe users, as described in “Adding Users to Your Vibe Site” in “Basic Installation” in the *Micro Focus Vibe 4.0.4 Installation Guide*.



Users’ workspaces appear in the Workspace tree after the users log in for the first time. To see a list of all users in the Vibe system regardless of whether they have logged in, click **Personal Workspaces**.

You can manually add Vibe users from this user list, as described in “Listing Vibe Users” on page 220.

You can also create new Vibe users by using the method described in “Creating a User” in “Basic Installation” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

As the Vibe administrator, you can access any user’s personal workspace by clicking it in the user list.

You cannot access a user’s personal workspace until the user has logged in to the Vibe site one time. After the user has logged in, the user’s personal workspace is ready for the user to personalize.

For information on how users can customize and populate their personal workspaces, see “Setting Up Your Personal Workspace” in the *Micro Focus Vibe 4.0.5 User Guide*.

Customizing the Default Personal Workspace View

As a Vibe administrator, you have the ability to customize the default view for all personal workspaces in your Vibe site.

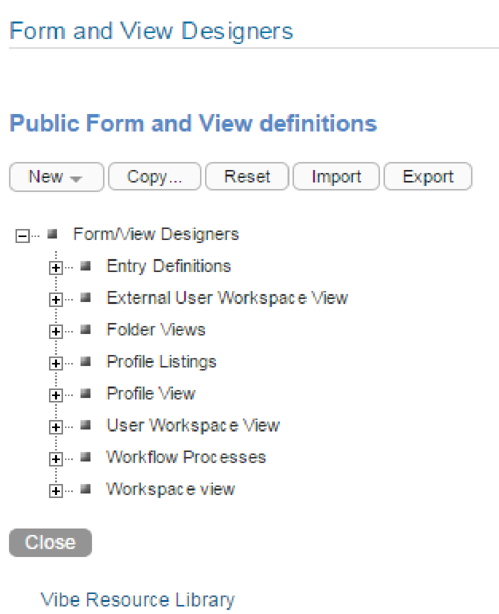
- “Customizing the Default View for Existing and Future Personal Workspaces” on page 47
- “Customizing the Default View for Future Personal Workspaces” on page 48

Customizing the Default View for Existing and Future Personal Workspaces

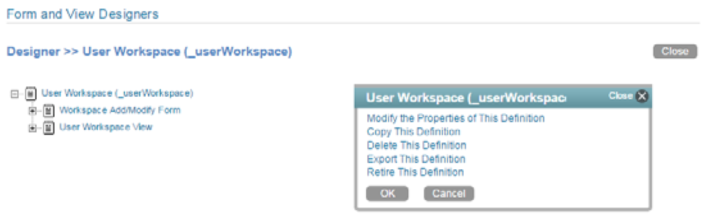
1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

The Administration page is displayed.

2 Under **System**, click **Form/View Designers**.



3 Expand **User Workspace View**, then click **User Workspace**.



4 Add the form and view elements that you want your existing and future personal workspaces to contain by default.

For information on the kinds of elements that you can add and how to add them, see "Adding Elements to the Workspace Add/Modify Form" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Customizing the Default View for Future Personal Workspaces

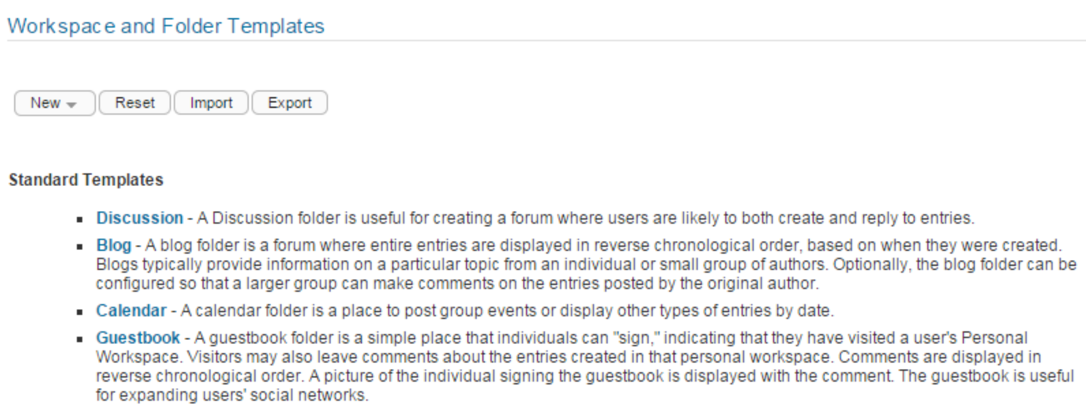
The procedure in this section affects only future personal workspaces (workspaces that have not yet been created). For information on how to change the default view for existing workspaces as well as future workspaces, see "Customizing the Default View for Existing and Future Personal Workspaces" on page 47.

1 Log in as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

The Administration page is displayed.

3 Under **Management**, click **Workspace and Folder Templates**.



4 Click **User workspace**.

5 Modify the settings.

For information on the types of modifications that you can make to the User Workspace template, see "Modifying Workspace and Folder Templates" on page 259.

Enabling Users to Create Landing Pages on Personal Workspaces

By default, Vibe users cannot create a landing page on their personal workspaces. However, as a Vibe administrator, you can enable landing page creation on personal workspaces.

1 Log in as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

   The Administration page is displayed.

3 Under **System**, click **Form/View Designers**.

   The Form and View Designers page is displayed.

4 Click **New** > **User Workspace View**.

5 Specify the following information:

   Caption: Specify a name for the new user workspace landing page view.

   This is the name that appears in the Vibe interface that users see when they use this view. (For example, `User Landing Page`.)

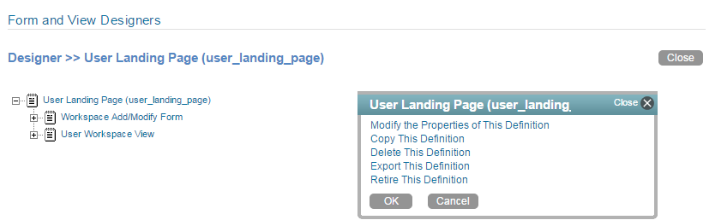
   Name: Specify the internal name for the new user workspace landing page view.

   The name that you enter in this field is not visible to users who use this view. (For example, `user_landing_page`.)

   Family: Ensure **User Workspace** is selected in the drop-down list.

6 Click **OK**.

   The Designer page is displayed.



7 Click **Workspace Add/Modify Form**.

8 Click **Add** in the Workspace Add/Modify Form window.

9 Click **Landing Page Layout** in the **Layout Options** section.

10 Specify the appropriate information, then click **OK**.

11 Click **User Workspace View**.

12 Click **Add** in the User Workspace View window.

13 Click **Landing Page Layout** in the **Standard Form Elements** section.

14 Specify the appropriate information, then click **OK**.

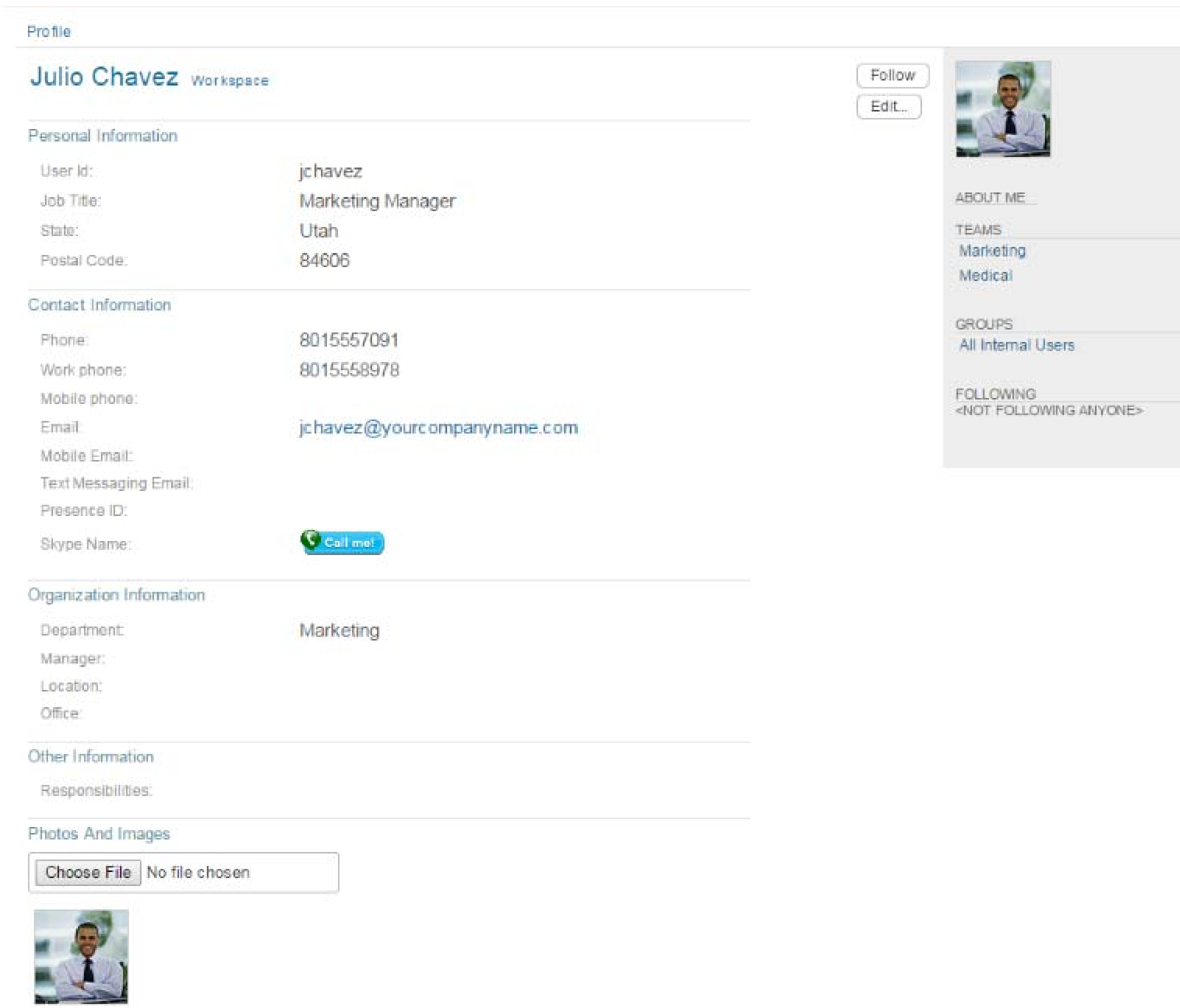
   Vibe users can now enable this landing page on their personal workspaces, as described in "Creating a Landing Page On Your Personal Workspace" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

For information on how to add other elements and layout options to this user workspace landing page view, see "Creating Custom Folder Views" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Customizing the Default User Profile View

The default user profile view is the view that appears in a user's profile in the personal workspace. When you customize the default user profile view, you modify the information that is displayed in all user profiles.

The default user profile view was expanded in Vibe 3 to rival other professional knowledgebases such as LinkedIn. Users can include more information to share with their colleagues, such as education, qualifications, and competencies.



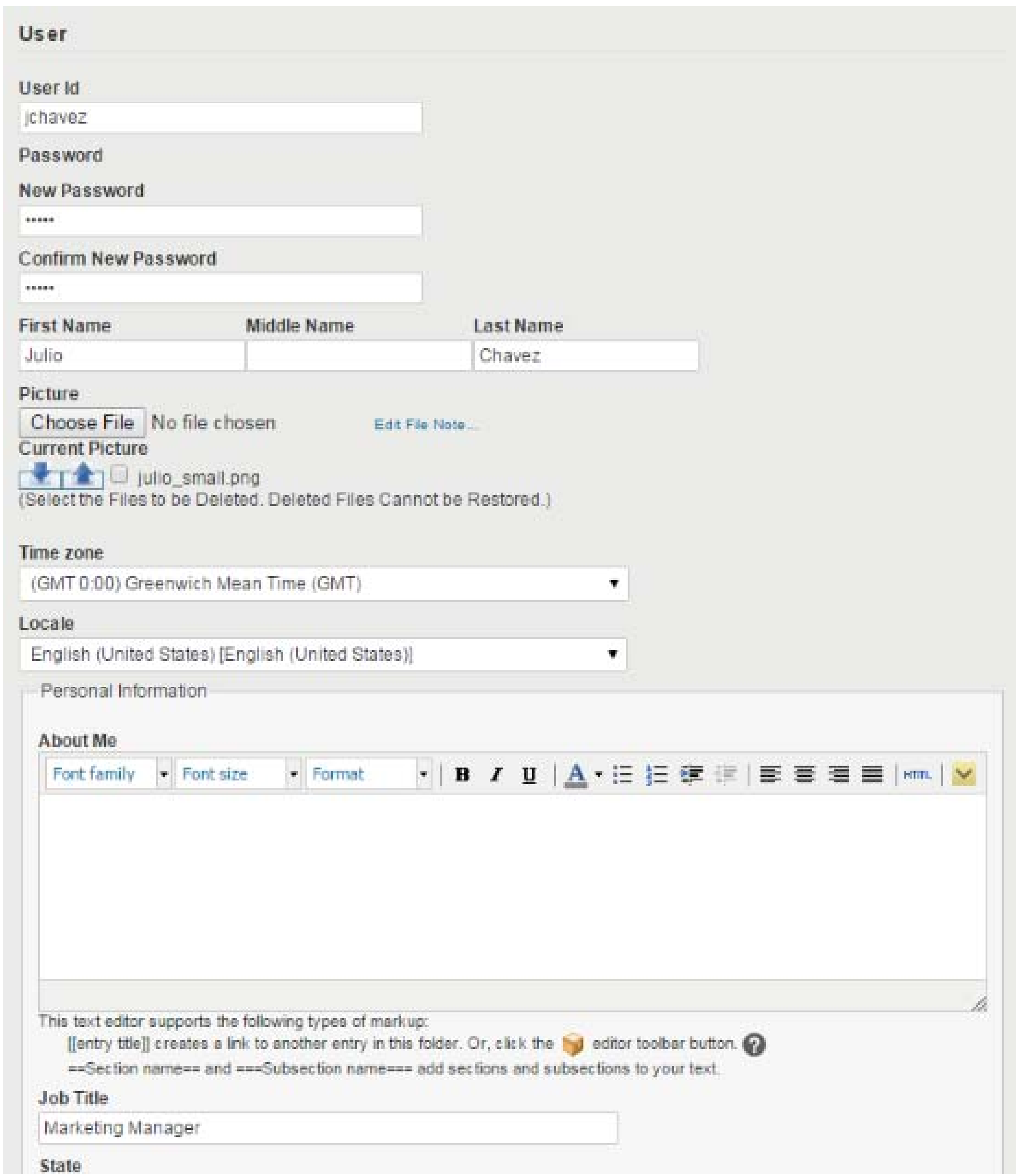
If you are updating your Vibe site from a version prior to Vibe 3 to Vibe 3 or later and you modified the user profile definition in your previous Vibe version, you do not see the new user profile when you upgrade to Vibe 3 or later. In order to see the new user profile, you need to reset your profile user definition. For information about how to reset your definitions, see "Resetting Your Definitions" in "Upgrade" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

You can customize the default user profile view to include custom fields. If you want to customize the user profile view, then you must also customize the user profile form. The view is what users see when they view a user profile; the form is what users fill out when they edit their user profiles. You must design both the form and view of the user profile in order for the elements to be displayed in the user profile view.

- "Designing the User Profile Form" on page 51
- "Designing the User Profile View" on page 53

Designing the User Profile Form

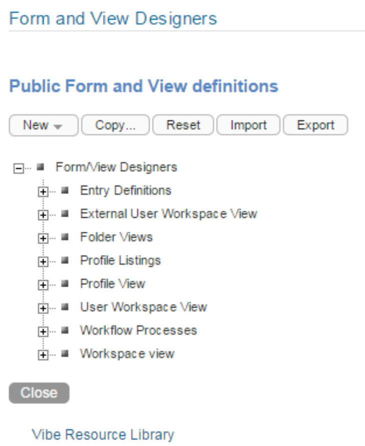
The user profile form is what a users see when they edit their user profile in Vibe. For example:



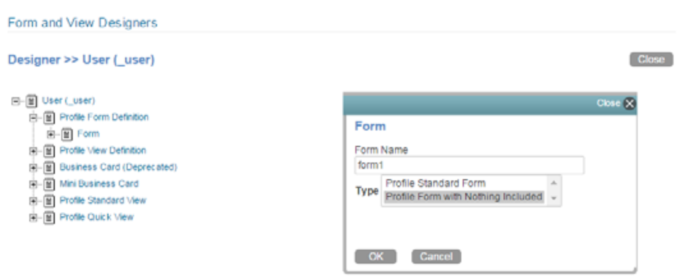
To modify the information that is displayed in the user profile form that users fill out when they edit a user profile:

1. Log in as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration** icon .

   The Administration page is displayed.
3. Under **System**, click **Form/View Designers**.



4. Expand **Profile View**, then click **User**.
5. Expand **Profile Form Definition**, then click **Form**.
6. Click **Modify**.



7. In the **Form Name** field, provide a name for the form.
8. In the **Type** field, select **Profile Form with Nothing Included**.

   This lets you add elements anywhere inside the view. If you do not select this option, you can add elements only after the last element in the default view.
9. Click **OK**.
10. Expand **Profile Form Definition**, then click **Form**.
11. Depending on how you want to modify the profile form, continue with one of the following sections:

- "Adding Elements to the Form" on page 53
- "Modifying Elements within the Form" on page 53

Adding Elements to the Form

1. Expand **Profile Form Definition**, then click **Form**.
2. In the Form dialog box, click **Add** to add an element or layout option to the view.

   You can add any of the elements and layout options that are described in “Workspace Form Elements” and “Understanding Layout Options” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
3. Continue with “Designing the User Profile View” on page 53 to create the user profile view that users will see when they view a user profile.

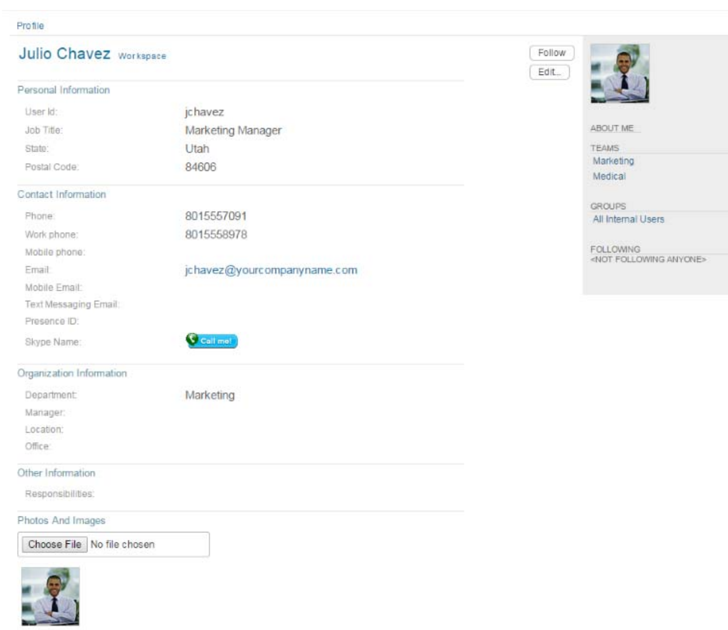
Modifying Elements within the Form

1. Expand **Profile Form Definition**, then expand **Form**.
2. Click the element that you want to modify.

   Depending on the element that you click, you can copy, delete, modify, or move the element. You can also add sub-elements.
3. In the dialog box on the right side of the page, click the action that you want to perform, then follow the on-screen instructions.
4. Continue with “Designing the User Profile View” on page 53 to create the user profile view that users will see when they view a user profile.

Designing the User Profile View

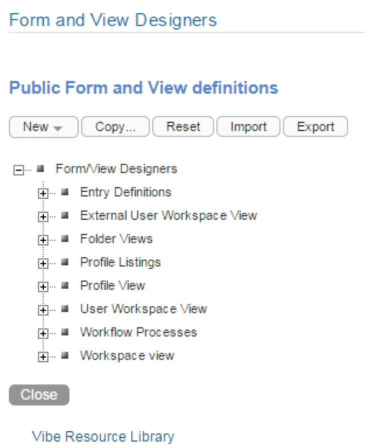
After you have designed the user profile form, as described in“Designing the User Profile Form” on page 51, you can modify the user profile view. The user profile view is what a user sees when the user views a user profile in Vibe. For example:



To modify the information that is displayed in the user profile view that users see when they view a user profile:

1. Log in as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

   The Administration page is displayed.
3. Under **System**, click **Form/View Designers**.



4. Expand **Profile View**, then click **User**.

   The User Designer page is displayed.

5. Expand **Profile Standard View** to view a list of all the elements and layout options that currently exist in the view.
6. Depending on how you want to modify the profile view, continue with one of the following sections:

- "Adding Elements to the View" on page 54
- "Modifying Elements within the View" on page 55

Adding Elements to the View

1. Click **Profile Standard View**.
2. In the Profile Standard View dialog box, click **Add** to add an element or layout option to the view.

   You can add any of the elements and layout options that are described in "Workspace View Elements" and "Understanding Layout Options" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Modifying Elements within the View

1. Click the element that you want to modify.

   You can copy, delete, modify, or move the element. You can also add sub-elements.

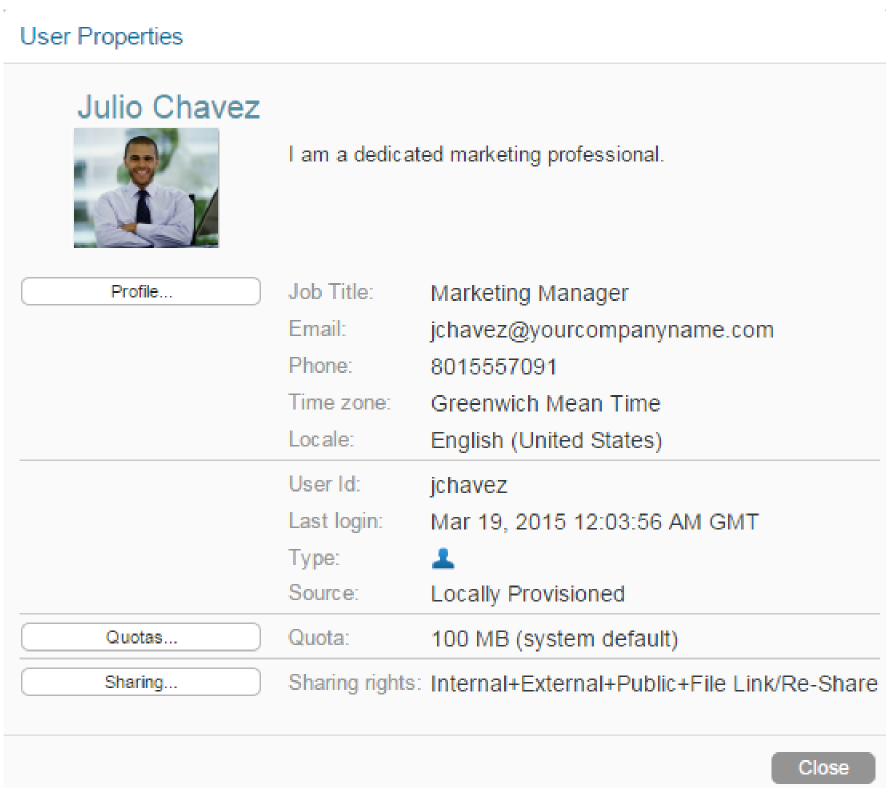
2. In the dialog box on the right side of the page, click the action that you want to perform, then follow the on-screen instructions.

Adding LDAP Elements to the User Profile View

If there is information in your LDAP source that does not have a corresponding element in Vibe, and you want that information to be displayed in the Vibe user profile view, you can create an element in the profile view as described in "Customizing the Default User Profile View" on page 50. After you have created the element, you can synchronize it with the corresponding information from LDAP, as described in "Synchronizing Additional LDAP Attributes" on page 216.

Customizing the Default Profile Quick View

The Profile Quick View is displayed when you click a user's **Presence** icon in Vibe.



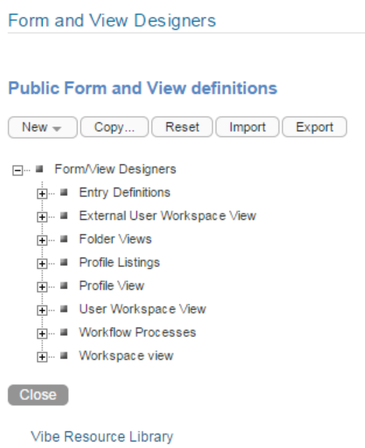
Presence is displayed in the following locations in Vibe:

- In a folder entry next to a user's name
- In a user's profile
- In the home page of a user's personal workspace

To modify the information that is displayed in the Profile Quick View:

1 Log in as the Vibe administrator.
2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

   The Administration page is displayed.
3 Under **System**, click **Form/View Designers**.



4 Expand **Profile View**, then click **User**.

   The User Designer page is displayed.

5 Expand **Profile Quick View**, expand **Conditional by License**, then click **Quick View Elements**.
6 In the Quick View Elements window, click **Modify**.

7 Press and hold the Ctrl key to select and deselect elements that you want to include in the Profile Quick View or exclude from the Profile Quick View.

If the element you want to add is not available in the list, click **Quick View Elements**, then in the Quick View Elements window, click **Add**. Select the element from the list, then click **OK**.

8 Click **OK**.

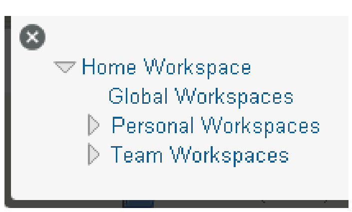
Managing Team Workspaces

- "Understanding Team Workspaces" on page 57
- "Creating a Team Workspace Root Workspace" on page 58
- "Creating a Team Workspace" on page 58
- "Managing Share Rights for Team Workspaces" on page 58
- "Deleting Top-Level Team Workspaces" on page 58
- "Viewing Team Membership of Top-Level Team Workspaces" on page 59

See also Chapter 23, "Managing Workspaces," on page 231.

Understanding Team Workspaces

When you create your Micro Focus Vibe site, a workspace named Team Workspaces is automatically created.



As the Vibe administrator, you are responsible to determine how team workspaces should be organized. Without guidance, Vibe users will inevitably create chaos under the Team Workspaces directory.

You might want to organize team workspaces to parallel your business organization. If appropriate, you might have a level for geographical areas. You would typically want a level for departmental areas, and perhaps even for projects within departments. In addition, you must decide which Vibe users need what kind of access to which teams. Creating groups, as described in "Creating Groups of Users" on page 97, facilitates creating teams because you do not need to individually add users to teams.

In the Team Workspaces directory that is automatically created when you install Vibe, you can create other Team Workspace Root workspaces. A Team Workspace Root workspace is designed to contain multiple team workspaces, so use this type of workspace if you want to create additional team workspaces as sub-workspaces to this workspace.

Creating a Team Workspace Root Workspace

After you have planned the hierarchical organization of the team workspaces for your Vibe site, you can start to implement it by creating Team Workspace Root workspaces, as described in "Creating and Managing a Team Workspace Root Workspace" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Creating a Team Workspace

In the Team Workspaces directory, or in the Team Workspace Root workspaces that you have created:

1. Create each team workspace, as described in "Creating a Team Workspace" in "Getting Started" in the *Micro Focus Vibe 4.0.5 User Guide*.
2. Set the access controls on the team workspace, as described in "Controlling User Access to Team Workspaces" on page 27.

Managing Share Rights for Team Workspaces

For information about how to manage share rights for team workspaces, see "Enabling Sharing for Top-Level Team Workspaces" on page 133.

Deleting Top-Level Team Workspaces

You can easily delete top-level team workspaces:

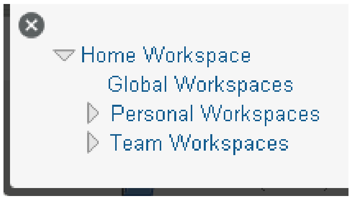
1. Log in to the Vibe site as the Vibe administrator.
   - **1a** Launch a web browser.
   - **1b** Specify one of the following URLs, depending on whether you are using a secure SSL connection:

     ```
     http://Vibe_hostname:8080
     https://Vibe_hostname:8443
     ```

Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **Browse** icon in the Action toolbar, then expand **Home Workspace** in the Workspace tree.



The Home Workspace directory is the highest-level folder in the workspace tree, and might be named something specific to your organization.

3 Click **Team Workspaces**.

The Teams page is displayed.

4 Select the top-level teams that you want to delete by selecting the checkbox next to the team name.

5 Click **Delete**.

6 (Conditional) To move the workspace to the trash, select **Move to trash**, then click **OK**.

Selecting this option removes the workspace from its current location without permanently deleting it from the Vibe system. You can undelete the workspace as described in "Recovering a Workspace from the Trash" in the *Micro Focus Vibe 4.0.5 User Guide*.

7 (Conditional) To permanently delete the workspace, select **Delete**.

IMPORTANT: Deleted items cannot be recovered.

---

8 Click **OK**.

Viewing Team Membership of Top-Level Team Workspaces

You can easily view the team membership of top-level team workspaces:

1 Log in to the Vibe site as the Vibe administrator.

1a Launch a web browser.

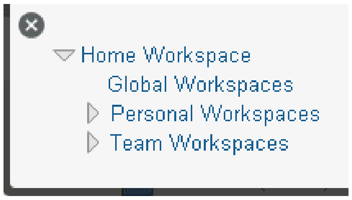
1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **Browse** icon in the Action toolbar, then expand **Home Workspace** in the Workspace tree.



The Home Workspace directory is the highest-level folder in the workspace tree, and might be named something specific to your organization.

3 Click **Team Workspaces**.

The Teams page is displayed.

Team members are listed in the **Team Members** column.

Creating Global Workspaces

A Global workspace is intended to present very high-level information that would be of interest to all Micro Focus Vibe users. It might include a Frequently Asked Questions (FAQ) workspace to help new Vibe users find their way around in the organization of team workspaces that you have set up. It might provide a place to post company-wide news. All Global workspaces must be created under **Home Workspace > Global Workspaces** on the Vibe site.

You might want to use geography to organize your company's global information, and then use departmental categories (**Engineering**, **Human Resources**, **Marketing**) to further organize the information. Or, depending on your organization, you might want to reverse the order (function followed by geography), or use some other organizational scheme.

We strongly recommend that you limit the creation of Global workspaces. First, organic team creation is the more effective use model for this product. Second, we have worked with a significant number of customers who duplicated complex organizational charts in the structure of Global workspaces, and users found them to be confusing and unusable. Instead, populate the global area with a minimal amount of information, and let users guide you in developing a useful structure and content in this area.

Using Workspace and Folder Templates

Templates in Micro Focus Vibe are a powerful way to create consistent custom folders and workspaces. If you are not satisfied with the way default workspaces and folders behave, you can either modify the current templates, or create new templates.

- "Understanding Templates" on page 61
- "Understanding Default Workspace and Folder Templates" on page 62
- "Creating Workspace and Folder Templates" on page 64

Understanding Templates

Workspace and Folder templates are a powerful and efficient way to manage your Vibe site. They enable you to customize the default features, default layout, and default access control settings of the workspaces and folders throughout your Vibe site.

For example, the Team Workspaces template is used when any team workspace is created. By default, the access control settings for the Team Workspaces template specify that only team members are able to view the team workspace. However, if you want to run a more relaxed Vibe site and allow all Vibe users to view any team workspace, you can simply modify the access control settings for the Team Workspaces template.

For information about the specific access control roles that you can assign to various users in Vibe, see "Understanding Access Control" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

- "Creating Templates or Modifying Existing Templates" on page 61
- "Templates vs. Form and View Designers" on page 61

Creating Templates or Modifying Existing Templates

You can modify existing templates, like the Team Workspaces template, or you can create your own custom templates. When you create a new template, all Vibe users have access to that template when they create new workspaces or folders. When you modify existing templates, users who create new workspaces and folders see only the modified template.

For more information on the default templates that are included in Vibe, see "Understanding Default Workspace and Folder Templates" on page 62.

Templates vs. Form and View Designers

Vibe provides two methods of customizing the default features and default layout of workspaces and folders in your Vibe site.

- **Templates:** If users have not yet started using your Vibe site, use templates to create and modify custom folder and workspace views. Typically, templates are easier to work with than the Form and View Designers tool; however, changes that you make to templates affect only those workspaces and folders that are created after the template was modified.
- **Form and View Designers Tool:** If users have already started using your Vibe site, you might want to use the Form and View Designers tool to create and modify folder and workspace views. When you modify folder and workspace views by using the Form and View Designers tool, all modifications are displayed in existing workspaces and folders.

  For information on using the Form and View Designers tool to create new workspace and folder views, see "Creating Custom Workspace Views" and "Creating Custom Folder Views" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Understanding Default Workspace and Folder Templates

By default, Vibe provides basic default templates for various types of workspaces and folders. If the default workspace and folder templates are not sufficient for your needs, you can either modify these templates, as described in "Modifying Workspace and Folder Templates" on page 259, or create new templates, as described in "Creating Workspace and Folder Templates" on page 64.

The following sections outline the default workspace and folder templates that are provided in Vibe:

- "Default Workspace Templates" on page 62
- "Default Folder Templates" on page 63

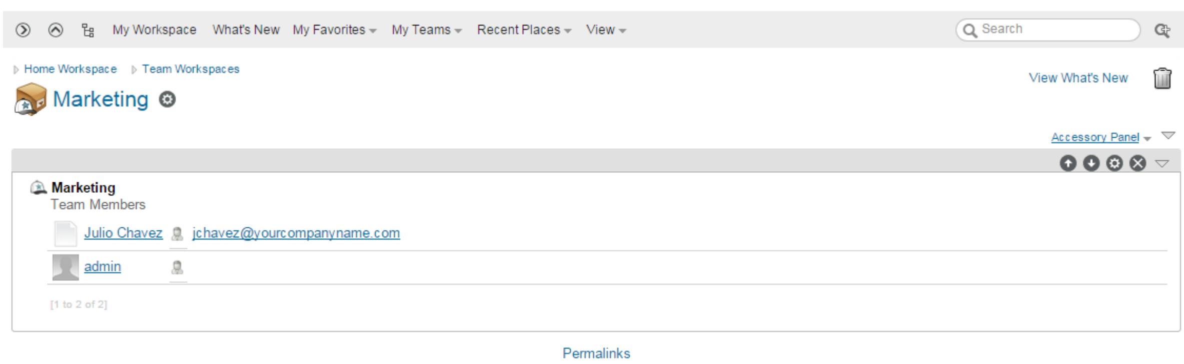
Default Workspace Templates

- Discussions Workspace
- Project Management Workspace
- Team Workspace
- Workspace (Basic)
- Landing Page
- User Workspace

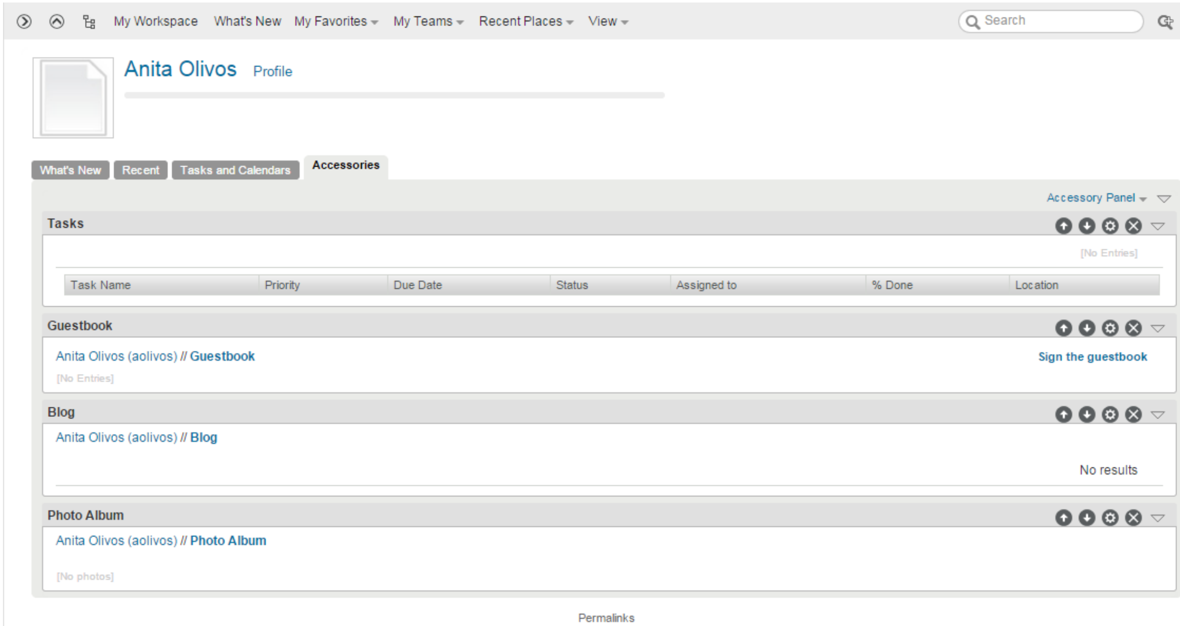
Following are some examples of default workspace templates:

- "Team Workspace" on page 62
- "User Workspace" on page 63

Team Workspace



User Workspace



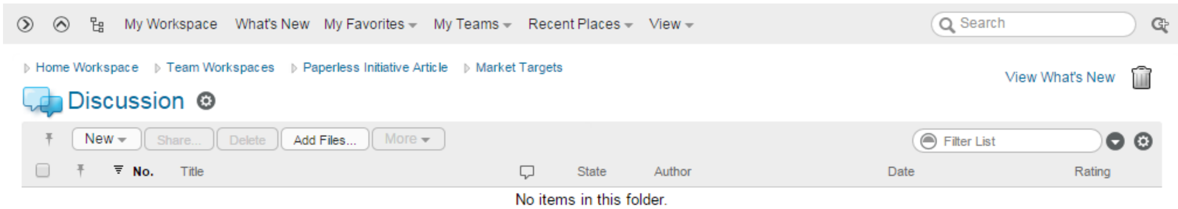
Default Folder Templates

- Discussion
- Blog
- Calendar
- Guestbook
- Files
- Milestones
- Micro-Blog
- Mirrored Files
- Photo Album
- Surveys
- Tasks
- Wiki

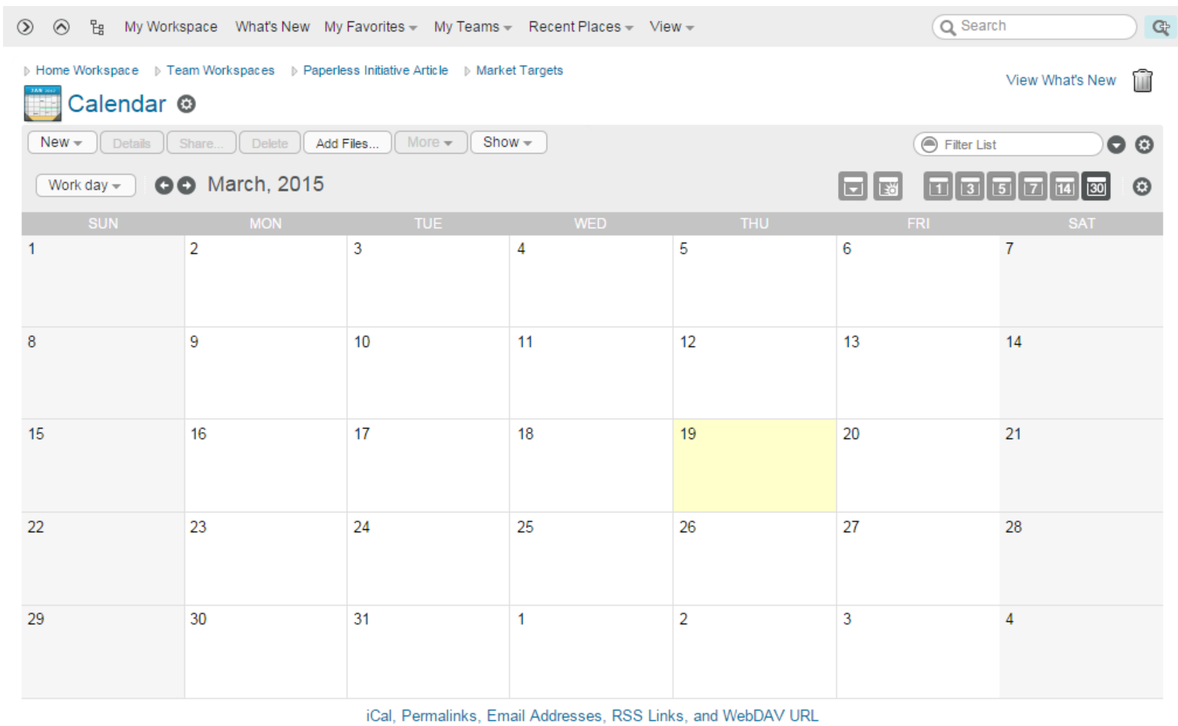
Following are some examples of default folder templates:

- "Discussion Folder" on page 64
- "Calendar Folder" on page 64

Discussion Folder



Calendar Folder



Creating Workspace and Folder Templates

Micro Focus lets you create templates based on existing workspaces and folders; or, you can create new templates. You can also modify existing templates.

- "Creating Templates Based on Existing Workspaces and Folders" on page 64
- "Creating New Templates" on page 66
- "Modifying Existing Templates" on page 67

Creating Templates Based on Existing Workspaces and Folders

You can create templates based on existing workspaces and folders only if the workspaces and folders do not contain local definitions. For example, if a workspace contains a custom form that is being used for the Discussion folder, you cannot create a template based on this workspace.

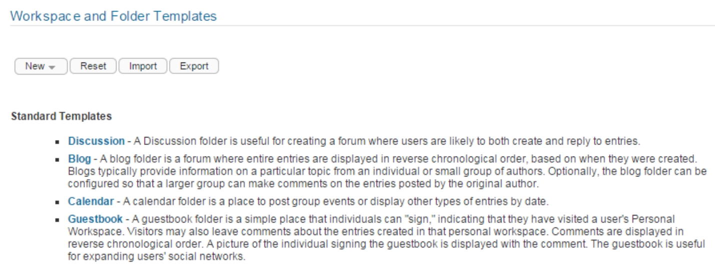
To find out if a workspace or folder contains local definitions, navigate to the workspace or folder, then click **Workspace** > **Form/View Designers** (or **Folder** > **Form/View Designers** if you are in a folder).

To create a template based on an existing workspace or folder:

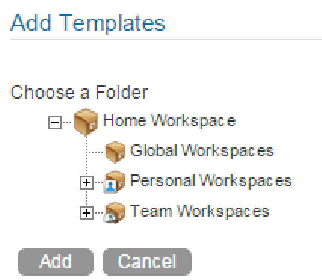
1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

The Administration page is displayed.

2 Under **Management**, click **Workspace and Folder Templates**.

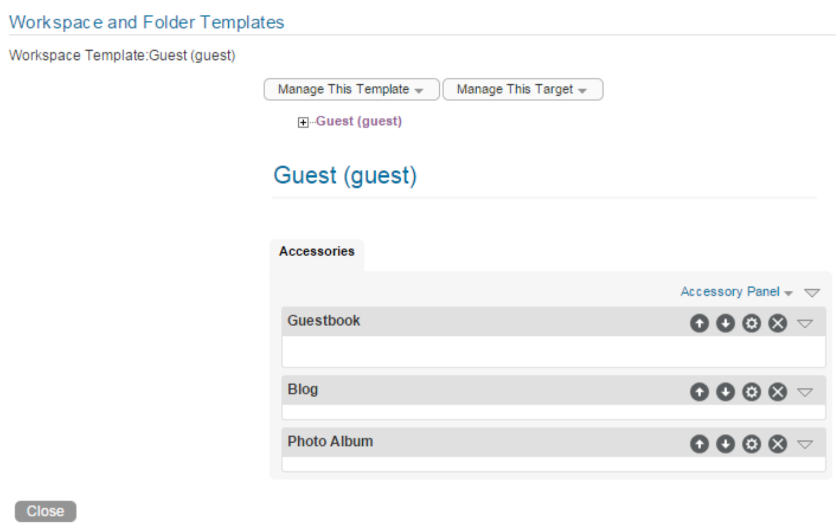


3 Click **New** > **Create a New Template from an Existing Workspace or Folder**.



4 Use the Workspace tree to navigate to and select the folder or workspace whose template you want to modify.

5 Click **Add**.



6 Modify the template as desired.

For information on how to modify a template after you have created it, see "Modifying Workspace and Folder Templates" on page 259.

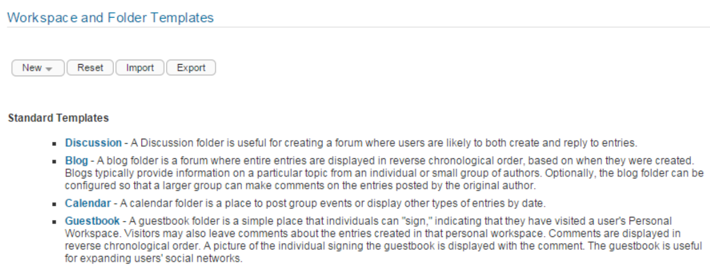
Creating New Templates

Vibe lets you design completely new custom workspace or folder templates.

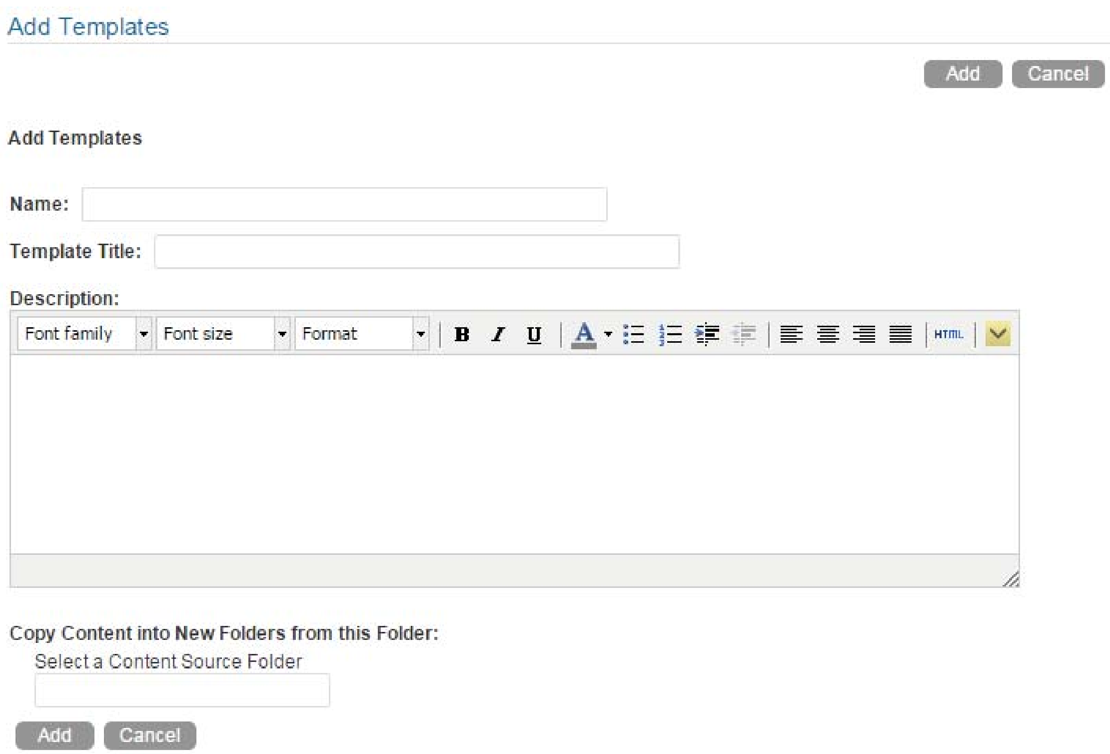
1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

The Administration page is displayed.

2 Under **Management**, click **Workspace and Folder Templates**.



3 Click **New** > **Folder** or **Workspace**, depending on which type of template you want to create.



4 Fill in the following fields:

Name: Internal name of the template

For example, `custom_template`.

Template Title: Visible name of the template.

For example, `Custom Template`.

Description: Description of the template.

5 Click **Add** > **OK**.

The template is created.

6 Set up the template as desired.

For information on how to set up a template after you have created it, see "Modifying Workspace and Folder Templates" on page 259.

Modifying Existing Templates

Vibe lets you modify default templates or custom templates that you have created.

For information on how to modify existing templates, see "Modifying Workspace and Folder Templates" on page 259.

Importing Workspaces

Micro Focus Vibe data can be transferred from one Vibe site to another by exporting it and then importing it. If you have data to import into your Vibe site, see "Exporting/Importing Workspaces, Folders, and Entries" on page 231.

4 Setting Up Site-Wide Customizations

Creating High-Level Landing Pages

Landing pages are a good way to put a custom face on your Micro Focus Vibe site while at the same time providing easier access to your site's most important information.

You might want to create landing pages at high-level workspaces, such as the Home Workspace workspace, which is the default name of the top-level workspace.

For information on how to create a landing page, see "Creating and Managing Landing Pages" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*

Creating a Site-Wide Brand

You can brand your Micro Focus Vibe site to match your corporate brand. When you add a site-wide brand to your Vibe site, the brand is displayed on every Vibe page for authenticated users.

If you have configured Guest access to the Vibe site, the site branding is not displayed for the Guest user. For more information about enabling Guest access to the Vibe site, see "Setting Up Guest Access for the Vibe Site" on page 105.

By default, users can create their own brands for their individual workspaces, team workspaces, and folders. When you create a site-wide brand, you can disable this functionality. For more information, see Branding Rules in Step 4.

1 Sign in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

   The Administration page is displayed.

3 In the **System** section, click **Site Branding**.

   The Site Branding dialog box is displayed.

4 Specify the following information to create your desired brand:

   Use Branding Image: Select this option if you want to use the drop-down list to select an existing image, or click the **Browse** icon to browse to an image on your computer's file system.

   Use Advanced Branding: Select this option, then click **Advanced** if you want to create a brand that includes advanced features in your brand, such as a YouTube video.

   Background Image: Use the drop-down list to select an existing image, or click the **Browse** icon to browse to an image on your computer's file system.

   The background image is displayed behind your regular branding.

   Stretch Image: Stretches the image to occupy the entire branding area.

   If you stretch your background image, the image overrides any background color that you have set.

   Background Color: Adds a background color that occupies the entire branding area. To change the background color, click the color name to the right of this field, select the new color, then click **OK**.

   If you added a background image and stretched the image, the background color is not displayed.

   Text Color: Changes the text color of the workspace name in the upper right corner of the branding area. To change the text color, click the color name to the right of this field, select the new color, then click **OK**.

   Branding Rules: Select from the following:

   - **Display site branding only:** Displays only the site-wide branding on all Vibe pages. Vibe users cannot create their own brands for workspaces and folders.
   - **Display both site and workspace branding:** Enables Vibe users to create their own brands for workspaces and folders. Both the site-wide brand and the workspace or folder brand are displayed.
   - **Workspace branding overrides site branding:** Enables Vibe users to create their own brands for workspaces and folders. Workspace and folder brands override the site-wide brand.

   Sign In Dialog Image: This option lets you change the image that is displayed on the sign-in dialog. For more information, see "Re-Branding the Login Dialog Box" on page 75.

   Clear branding: Click this option to clear all your current branding selections.

5 Click **OK**.

   The Vibe site now displays the brand that you created.

For more information about creating brands in Vibe, see "Branding a Folder or Workspace" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Setting a Default Home Page

By default, all users who log in to the Micro Focus Vibe site are first taken to the What's New page. However, you can change this default behavior to have all users taken to a different home page of your choosing. This might be a corporate landing page that provides links to important places on the Vibe site.

You can also configure Vibe so that users are taken to their personal workspaces when they first log in to the Vibe site. For information on how to configure Vibe in this way, see "Restricting the What's New Page from Being Displayed When Users First Log In" on page 81.

Setting a Default Home Page for All Licensed Vibe Users

1 Log in to the Vibe site as the Vibe administrator.

2 Create a landing page on the workspace that you want to set as the new default home page for all registered users.

For example, you might navigate to the **Global Workspaces** directory and create a landing page on this workspace.

For information on how to create a landing page, see "Creating and Managing Landing Pages" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

3 Set the access control for the workspace to allow all users to be visitors to the workspace, if it is not set already:

3a Click the **Configure** icon next to the workspace title, then click **Access Control**.

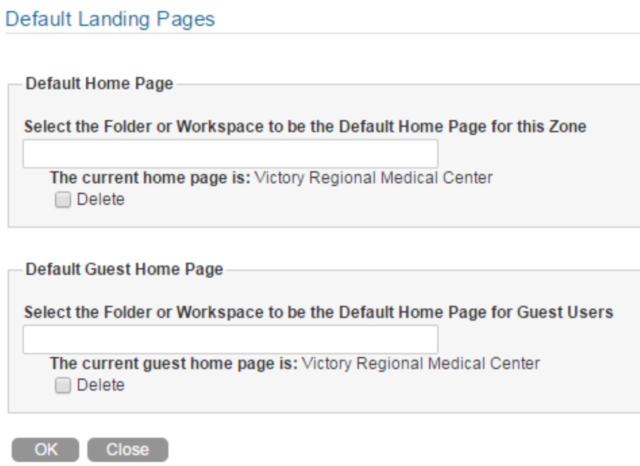
3b In the **Inherit role membership** section, select **no**, then click **Apply**.

3c In the **All Users** row, ensure that the box is selected in the **Visitor** column.

3d Click **Save Changes** > **Close**.

4 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

5 Under **System**, click **Default Landing Pages**.



6 In the **Select the Folder or Workspace to be the Default Home Page for this Zone** field, begin typing the name of the folder or workspace that you want to set as the default home page for all licensed users, then click it when it appears in the drop-down list.

7 Click **OK**.

If you want users to be automatically taken to this page before they log in, and if you want people who do not have a user account to have access to the page, see "Making the Guest User Default Home Page the Same as the Home Page for Licensed Users" on page 72.

Setting a Default Home Page for Guest Users

When you allow people who do not have a user account to access the Vibe site as a guest user, as described in "Allowing Guest Access to Your Vibe Site" on page 104, then by default they are taken to the Guest User workspace when they access Vibe. If you want guest users to be taken to a workspace other than the Guest User workspace, you can set a default home page for guest users that is different from the Guest User workspace. The default home page can be the same default home page that you have set up for your licensed Vibe users, or it can be a different page.

- "Making the Guest User Default Home Page the Same as the Home Page for Licensed Users" on page 72
- "Setting Up a Default Home Page Specifically for Guest Users" on page 73

Making the Guest User Default Home Page the Same as the Home Page for Licensed Users

If you have already set up a default home page for your licensed Vibe users, as described in "Setting a Default Home Page for All Licensed Vibe Users" on page 71, you can configure Vibe to allow guest users who access the Vibe site to be taken to the same home page. If you configure Vibe in this way, everyone who accesses the Vibe site is taken directly to the default home page without logging in.

1 Follow the steps in "Setting a Default Home Page for All Licensed Vibe Users" on page 71.

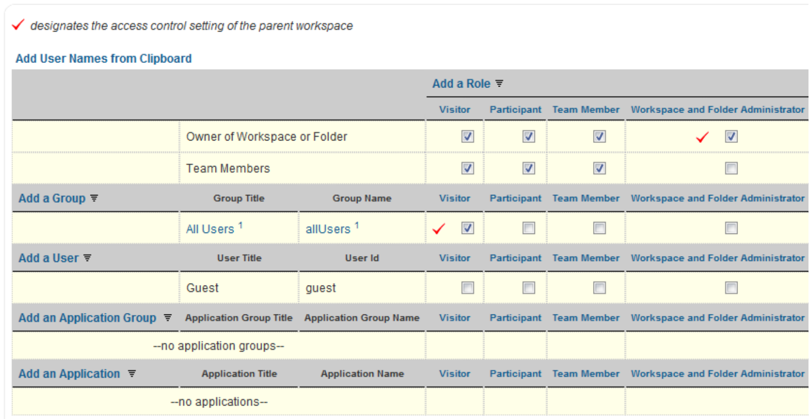
2 Navigate to the workspace that you want to set as the default home page for guest users, which is the workspace that you already set as the default home page for licensed Vibe users in "Setting a Default Home Page for All Licensed Vibe Users" on page 71.

3 Click the **Configure** icon next to the workspace title, then click **Access Control**.

The Configure Access Control page is displayed.

4 Click **Add User,** start typing `Guest` in the **Add a User** field, then click **Guest** when it appears in the drop-down list.

This adds **Guest** as a new row in the Access Control table.



5 In the **Guest** row, ensure that the box is selected in the **Visitor** column.

6 Click **Save Changes** > **Close**.

Setting Up a Default Home Page Specifically for Guest Users

You might want guest users who access the Vibe site to be taken to a workspace that is designated specifically for guest users.

1 Log in to the Vibe site as the Vibe administrator.

2 Create a landing page on the workspace that you want to set as the new default home page for guest users.

For information on how to create a landing page, see "Creating and Managing Landing Pages" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

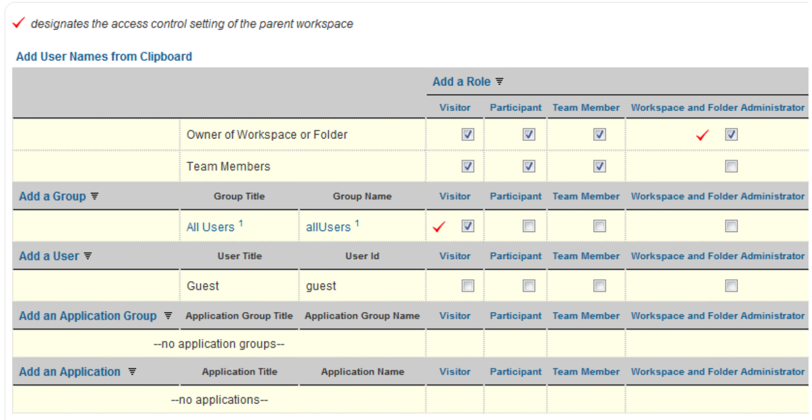
3 Set the access control for the workspace to allow guest users to be visitors to the workspace.

3a Click the **Configure** icon next to the workspace title, then click **Access Control**.

3b In the **Inherit role membership** section, select **no**, then click **Apply**.

3c Click **Add User,** start typing `Guest` in the **Add a User** field, then click **Guest** when it appears in the drop-down list.

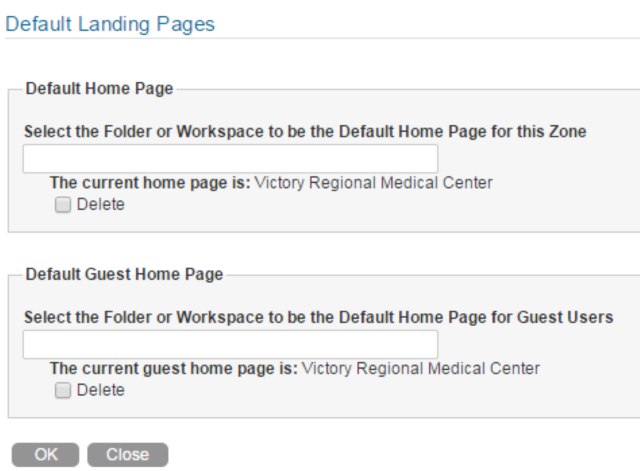
This adds **Guest** as a new row in the Access Control table.



3d In the **Guest** row, ensure that the box is selected in the **Visitor** column.

3e Click **Save Changes** > **Close**.

4. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
5. Under **System**, click **Default Landing Pages**.



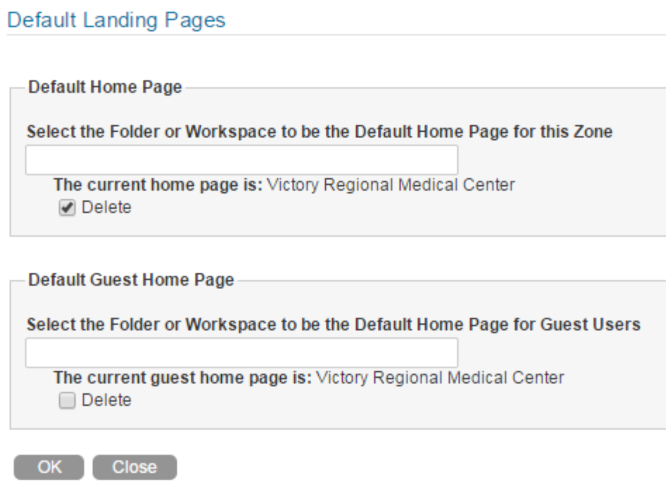
6. In the **Select the Folder or Workspace to be the Default Home Page for Guest Users** field, begin typing the name of the folder or workspace that you want to set as the default home page for guest users, then click it when it appears in the drop-down list.
7. Click **OK**.

Removing the Default Home Page

If you remove the default home page, users are taken to their individual workspaces when they first access the Vibe site.

1. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
2. Under **System**, click **Default Landing Pages**.

3 Beneath **The current home page is**, select **Delete**.



4 Click **OK**.

Re-Branding the Login Dialog Box

You can change the image that is used in the login dialog box that users see before they log in to the Micro Focus Vibe site.

To re-brand the login dialog box to contain a custom image:

1 Sign in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

The Administration page is displayed.

3 In the **System** section, click **Site Branding**.

The Site Branding dialog box is displayed.

4 In the Sign In Dialog Image section, use the drop-down list to select an existing image, or click the **Browse** icon to browse to an image on your computer's file system.

5 Click **OK**.

Enabling User ID Auto-Completion for the Login Dialog Box

You can enable auto-completion for the **User ID** field in the login dialog box for your Micro Focus Vibe site. When you enable auto-completion, each user in your Vibe site can start typing his or her user ID and then select it from a drop-down list when it appears.

To enable auto-completion for your Vibe site:

1 Change to the following directory:

Linux: `/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`

Windows: `c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Open the `ssf-ext.properties` file in a text editor.

3 Scroll to the bottom of the `ssf-ext.properties` file, then add the following line:

```
enable.login.autocomplete=true
```

4 Save and close the `ssf-ext.properties` file.

5 Stop and restart Vibe.

Customizing Vibe Styles

You can customize colors, background images, and fonts throughout the Vibe interface. You might want to do this if you want to change the default Vibe styles to better match your corporate theme.

You must have knowledge of CSS styling to successfully customize styles in your Vibe site. When customizing styles, you need to either add a style, change an existing style, or delete a style.

For information about how to customize icons throughout the Vibe site, see “TID 7007607: Modifying the Default Vibe Icons” in the Novell Support Knowledgebase (http://www.novell.com/support).

IMPORTANT: As you customize styles on the Vibe server, back up the changes you are making and record where you are making them. This is because when you upgrade your Vibe system to a new version, any style changes that you have made could be overwritten. You might need your backups and detailed notes in order to re-create your customized Vibe styles after an upgrade.

Most style customizations in Vibe are accomplished through the modification of CSS style sheets. Some style settings in the Vibe interface are contained within JSP files.

The type of files that you need to modify in order to affect Vibe styles depends on the area of the Vibe interface that you want to customize, as shown in the following table.

Table 4-1 *CSS Style Locations*

Area of Vibe Interface	**Type of File to Modify**	**Location on the Vibe Server**
Masthead	CSS style sheet	apache-tomcat/webapps/ssf/static/*version*/js/gwt/gwtteaming/GwtTeaming.css
Navigation Panel	CSS style sheet	apache-tomcat/webapps/ssf/static/*version*/js/gwt/gwtteaming/GwtTeaming.css
Action Toolbar	CSS Style Sheet	apache-tomcat/webapps/ssf/static/*version*/js/gwt/gwtteaming/GwtTeaming.css
User Profile Page	CSS Style Sheet	apache-tomcat/webapps/ssf/static/*version*/js/gwt/gwtteaming/GwtProfile.css
Content Area	JSP file	apache-tomcat/webapps/ssf/WEB-INF/jsp/common

To customize styles for your Vibe system:

1. Find the CSS selector name for the area of the interface for which you want to customize the style setting.

   For example, suppose you want to modify the color or font of the Action toolbar for your Vibe site. You use Firebug on Firefox to find the selector name for the Action toolbar, which is `mainMenuControl`.

2. On the Vibe server, navigate to the directory where the style that you want to modify is located.

   See Table 4-1 for the file location on the Vibe server.

   For example, Table 4-1 shows that the `mainMenuControl` selector for the Action toolbar is located in the `apache-tomcat/webapps/ssf/static/`*`version`*`/js/gwt/gwtteaming` directory, in the `GwtTeaming.css` file.

3. Open the appropriate file in an editor, then search for the selector name.

   For example, to customize the color of the Action toolbar, open the `GwtTeaming.css` file, then search for `mainMenuControl`.

   If the appropriate file is a `JSP` file, you first need to locate the appropriate `JSP` file.

4. Make your desired style modifications in one of the following ways:

   - In the CSS style sheet, modify the value of the CSS definition that you want to customize, add a new CSS definition, or delete an existing CSS definition.
   - Modify any images that are referenced in the CSS style sheet by navigating to the directory where the images reside and making changes there.

     If you modify an image that is not referenced in the CSS style sheet, your modifications are not reflected in the Vibe interface.

5. Save your changes on the Vibe server, then clear the browser cache and refresh the browser to see the changes.

   Following are examples of color and font changes to the Action toolbar:

   The Action toolbar has been changed to red, and the font has been changed.

Customizing Icons on Your Vibe Site

- "Replacing Existing Icons" on page 77
- "Adding New Icons" on page 78

Replacing Existing Icons

You can customize your Micro Focus Vibe site by replacing standard icons with icons of your own choosing.

1. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/ webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\ webapps\ssf\WEB-INF\classes\config`

2. Open the `ssf.properties` file in a text editor.
3. Search for `icons` in order to move to the section that defines the Vibe icons.

Four types of icons are listed:

```
icons.workspace=
icons.folder=
icons.profileList=
icons.entry=
```

These icons are stored in the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/images/icons`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\images\icons`

4 Replace standard image files with your own image files with the same filenames.

This replaces the standard Vibe icons with your own customized icons. The next time you access the Vibe site, your customized icons display instead of the standard Vibe icons.

Adding New Icons

You can add icons to your Vibe site for use in areas of the Vibe site that you are customizing on a significant scale.

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Open the `ssf.properties` file in a text editor.

3 Search for `icons` in order to move to the section that defines the Vibe icons.

Four types of Vibe icons are listed:

```
icons.workspace=
icons.folder=
icons.profileList=
icons.entry=
```

These Vibe icons are stored in the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/images/icons`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\images\icons`

4 Make a backup copy of the `ssf-ext.properties` file, located in the same directory with the `ssf.properties` file.

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `Icons` section from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 List additional image files for each icon type as needed.

8 Add the new image files to the appropriate subdirectory under the `icons` directory where the existing Vibe icons are stored.

9 Save and close the `ssf-ext.properties` file.

10 Close the `ssf.properties` file without saving it.

11 Stop and restart Vibe to make the new icons available on your Vibe site.

Configuring How Items Are Displayed in the What's New Page

Micro Focus Vibe users can view what's new in Vibe by using the What's New page. Users can quickly see what's new in their teams, favorite places, and more. For more information on how users can view what's new in Vibe, see "Finding What's New" in the *Micro Focus Vibe 4.0.5 User Guide*.

As the Vibe administrator, you can control various aspects of the What's New page by modifying Vibe configuration settings.

- "Understanding the Configuration Settings You Can Customize for the What's New Page" on page 79
- "Changing the Configuration Settings for the What's New Page" on page 81

Understanding the Configuration Settings You Can Customize for the What's New Page

The tables in the following sections describe configuration settings for the What's New page that the Vibe administrator can customize, the system default for the setting, and the line in the `ssf-ext.properties` file that controls the setting:

- "Customizing the Number of Comments That Can Be Displayed for Each Entry on the What's New Page" on page 79
- "Customizing the Number of Words That Are Displayed for Each Item on the What's New Page" on page 80
- "Customizing How Often the What's New Page Is Updated" on page 80
- "Customizing the Number of Items That Are Returned When the What's New Page Is Updated" on page 80
- "Restricting the What's New Page from Being Displayed When Users First Log In" on page 81

Customizing the Number of Comments That Can Be Displayed for Each Entry on the What's New Page

Configuration Setting	System Default	Line in the ssf-ext.properties File
The maximum number of comments that are displayed for any given entry.	2 comments	`activity.stream.active.comments`

Customizing the Number of Words That Are Displayed for Each Item on the What's New Page

Configuration Setting	System Default	Line in the ssf-ext.properties File
The maximum number of words that are displayed for each item on the What's New page.	-1 (The first several lines of an item are displayed)	`activity.stream.display.words`

Customizing How Often the What's New Page Is Updated

Configuration Setting	System Default	Line in the ssf-ext.properties File
How often the What's New page is updated to display the most recent posts.	60 seconds	`activity.stream.interval.refresh.client`

NOTE: Adjusting this setting to update the What's New page more frequently than the system default (60 seconds) can result in inadequate system performance. However, depending on how many users access your Vibe system and your current configuration, a more frequent or less frequent update cycle might be appropriate.

Customizing the Number of Items That Are Returned When the What's New Page Is Updated

Configuration Setting	System Default	Line in the ssf-ext.properties File
The maximum number of new or modified items that are returned by the search (includes entries and comments).	1000 items	`activity.stream.maxhits`

Restricting the What’s New Page from Being Displayed When Users First Log In

Configuration Setting	System Default	Line in the ssf-ext.properties File
Defines whether the What’s New page is displayed when users first log in to the Vibe site. If the value of this line is `true`, the What’s New page is displayed. If the value is `false`, users see their personal workspaces when they first log in to the Vibe site.	true (The What’s New page is displayed when users first log in)	`activity.stream.on.login`

IMPORTANT: If you have specified a default home page for you Vibe site, as described in “Setting a Default Home Page” on page 71, users are taken to that home page when they first log in to the Vibe site, regardless of this setting.

Changing the Configuration Settings for the What’s New Page

To change the configuration settings of the What’s New page:

1 Change to the following directory:

Linux: `/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`

Windows: `c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the appropriate line that represents the configuration setting that you want to customize for the What’s New page.

See the table in “Understanding the Configuration Settings You Can Customize for the What’s New Page” on page 79 to find the line in the `ssf-ext.properties` file that controls the setting that you want to customize.

For example, if you want to change the number of words that are displayed for each item on the What’s New page, search for the line `activity.stream.display.words=-1`, then change the value to the number of words that you want to be displayed. For example, `activity.stream.display.words=25`.

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the appropriate line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change the default value of the line to the value that you want.

8 Save and close the `ssf-ext.properties` file.

9 Stop and restart Vibe.

Sorting Names throughout the Vibe Site by Last Name

By default, where lists of users are displayed in Vibe, names are sorted by first name (for example, Anne Marie Hall), rather than by last name (for example, Hall, Anne Marie).

A list of users in your Vibe system are displayed in the following locations:

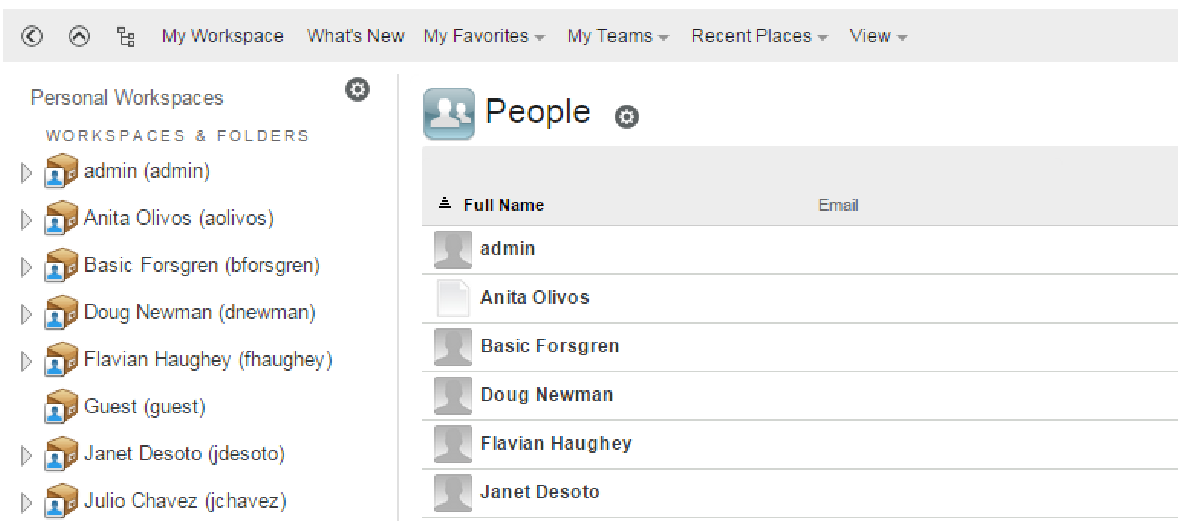
- Navigation Panel in the Personal Workspaces workspace.

  You access the Personal Workspaces workspace by clicking the **Workspace tree** icon, expanding **Home Workspace**, then clicking **Personal Workspaces**.
- Workspace tree in the Action toolbar.

  You access the Workspace tree by clicking the **Workspace tree** icon in the Action toolbar.
- Workspace tree in other areas throughout the Vibe site.

  The workspace tree appears in other locations throughout Vibe, such as in the Search Index.

The following figure shows names in the Navigation panel sorted by first name.



To configure the Vibe site to sort names by last name:

1 Change to the following directory:

Linux: `/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`

Windows: `c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
wsTree.titleFormat=0
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the appropriate line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `0` to `1`, so that the line now reads `wsTree.titleFormat=1`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe.

Managing How Group Names Are Displayed during Name Completion

Certain fields throughout the Vibe site employ name completion (or Type-to-Find) functionality. For example, when you share an item in Vibe and you begin typing the name of a user or group in the Share with field, names of users or groups that match what you have typed so far appear in a drop-down list.

In the Type-to-Find drop-down list, Vibe includes the group name or group title, as well as secondary information about the group (either the group description or the Fully Qualified DN). This secondary information helps distinguish between multiple groups that have the same name.

Vibe allows you to determine the way group names are displayed in this Type-to-Find drop-down list.

1 Log in to the Vibe site as the Vibe administrator.

   1a Launch a web browser.

   1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

   `http://`*`Vibe_hostname`*`:8080`

   `https://`*`Vibe_hostname`*`:8443`

   Replace *Vibe_hostname* with the host name or fully qualified domain name of the Vibe server that you have set up in DNS.

   Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.

3 Under **System**, click **Name Completion Settings**.

   The following options are available:

   Primary display text: Select Name or Title. Name represents the name of the group as it appears in Vibe. Title represents the title as it appears in the LDAP directory.

   Secondary display text: Select Description or Fully Qualified DN. Description represents the description of the group as it appears in Vibe. Fully Qualified DN represents the Fully Qualified Domain Name as it appears in the LDAP directory.

4 Click **OK**.

Changing the Number of Recent Places That Are Displayed

You can modify how many recent places are displayed in the **Recent Places** menu in the Action toolbar. By default, a user's 20 most recently visited places are displayed. (For more information, see "Viewing and Revisiting Recent Places"in the *Micro Focus Vibe 4.0.5 User Guide*.)

To change the number of recently visited places that are displayed for each user:

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
recent-places-depth=20
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `recent-places-depth=20` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `20` to the number that represents how many recent entries you want to be displayed for each user. For example, if you want only 10 recently visited entries to be displayed, the line would now read `recent-places-depth=10`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe.

Configuring File Associations for Edit in Place Applications

When using Edit in Place functionality in Micro Focus Vibe, you can configure Vibe to open specific types of files with non-default applications. You can also configure Vibe to support file extensions that are not supported by default.

For more information about Edit in Place functionality, see "Editing Files Accessed through a Web Browser" in the *Micro Focus Vibe 4.0.5 User Guide*.

- "Changing Global File Associations for Edit in Place Applications" on page 85
- "Configuring Vibe to Support Additional File Types for Edit in Place Applications" on page 85

Changing Global File Associations for Edit in Place Applications

When calling applications with the Edit in Place feature, Micro Focus Vibe uses standard file associations. If your organization uses different file associations, you can reconfigure Vibe to use the preferred file associations.

Individual users can do this for their own user accounts, as described in "Changing the Default Editor Settings for a Single File Type" in the *Micro Focus Vibe 4.0.5 User Guide*.

To reconfigure Vibe to use the preferred file association for all users on the Vibe site:

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for `Edit in place` to move to the block of lines that control the Edit in Place feature.

5 Review the subsequent comment lines to become more familiar with how the Edit in Place feature works.

6 Scroll down to locate the lines for the file associations that you want to change.

7 Copy the lines to the clipboard of your text editor.

8 Open the `ssf-ext.properties` file.

9 Scroll to the end of the `ssf-ext.properties` file, then paste the line you copied in Step 7.

10 Edit the file association as needed.

Use double backslashes for Mac or Linux systems when you need to include a space in the path, as shown in the above example.

11 (Optional) Copy additional lines from the `ssf.properties` file to the `ssf-ext.properties` file as needed.

12 Save and close the `ssf-ext.properties` file.

13 Close the `ssf.properties` file without saving it.

14 Stop and restart Vibe to put the modified file associations into affect for your Vibe site.

Configuring Vibe to Support Additional File Types for Edit in Place Applications

You can configure Vibe to support other document editors to the list of documents that Vibe can edit using Edit in Place.

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/ webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\ webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for `Edit in place` to move to the block of lines that control the Edit in Place feature.

5 Review the subsequent comment lines to become more familiar with how the Edit in Place feature works.

6 Copy the following line to the clipboard of your text editor:

```
edit.in.place.file.applet.extensions=
```

7 Open the `ssf-ext.properties` file.

8 Scroll to the end of the `ssf-ext.properties` file, then paste the line you copied in Step 6.

9 Add the file extension to the comma-delimited list of file extensions.

10 (Optional) Copy additional lines from the `ssf.properties` file to the `ssf-ext.properties` file as needed.

11 Save and close the `ssf-ext.properties` file.

12 Close the `ssf.properties` file without saving it.

13 Stop and restart Vibe.

Understanding and Configuring Search Functionality

Micro Focus Vibe contains various features that control how items are indexed and how searches are executed on the Vibe site. As the Vibe administrator, you can configure the settings for these features. The default configurations are optimal for most Vibe sites.

These features are supported only with Vibe folder entries that contain English or other Western European languages. (For a list of supported languages, see "Supported Languages for Indexing and Searching for the Root Form of Words" on page 92.)

Removing Frequently Used Words That Have No Inherent Meaning

Vibe removes frequently used words that have no inherent meaning when items are indexed and when users perform a search. Examples of such words are `a`, `an`, `the`, `in`, `on`, `the`, and so forth.

This includes when users perform a search with quotation marks. For example, `"sell the products"` would return all of the following: `sell their products`, `sell with products`, `sell the products`, and so forth. However, it would not return `sell products`.

You can customize the words that Vibe considers to have no inherent meaning. For more information, see "lucene.indexing.stopwords.file.path" on page 89.

This functionality is enabled by default. For information on how to modify the default settings, see "Modifying Configuration Settings" on page 88.

Searching for Various Forms of the Same Word

When Vibe indexes a word, it indexes the root form of the word. Likewise, when users perform a search for a word, Vibe searches for the root form of the word and returns all matches. For example, performing a search on the word `research` returns all forms of the word, including `researching`, `researched`, and `researches`. Likewise, searching for the word `researching` returns results for `research`, `researches`, and so forth.

This functionality is enabled by default. For information on how to modify the default settings, see "Modifying Configuration Settings" on page 88.

Searching for Words That Contain Accents

When Vibe indexes a word, it indexes the word without accents, regardless of whether the word originally contains accents. Likewise, when users perform a search for a word, Vibe searches for the word without accents, regardless of whether the user uses accents during the search. This means that when a user performs a search on the word `cliché`, Vibe returns results for the word `cliché` and `cliche`. Vibe also returns both forms of the word if the user performs a search on the word `cliche`.

This functionality is enabled by default. For information on how to modify the default settings, see "Modifying Configuration Settings" on page 88.

Increasing the Number of Words That Are Indexed for Each Document

Vibe indexes all the words (and their variations) in documents that are uploaded to the Vibe site. In most cases, the default settings are sufficient to index documents that contain tens of pages.

If you have very large documents (hundreds or thousands of pages per document) that are stored on your Vibe site, you might encounter problems with parts of the document not being returned in search results. This can be due to the fact that the document is not being indexed in its entirety, because the document is too large. In this case, you might want to increase the number of words that are indexed for each document. Be aware that increasing the number of words that are indexed uses more system resources (RAM and disk space).

You can increase the number of words that are indexed for each document that is added to the Vibe site. For information on how to do this, see "Modifying Configuration Settings" on page 88.

Modifying Configuration Settings

The location of the configuration file on the Vibe server depends on whether you have a single Lucene Index Server that is located on the same server as Vibe, or if your Lucene Index Server is located on a remote server or you have multiple Lucene Index Servers.

For more information about the various ways that you can set up the Lucene Index Server, see "Changing Your Lucene Index Server Configuration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

To modify configuration settings for the Search feature:

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Open the `ssf.properties` file in a text editor if you have a single Lucene Index Server that is located on the same server as Vibe.

or

Open the `lucene-server.properties` file in a text editor if your Lucene Index Server is located on a remote server or you have multiple Lucene Index Servers.

3 Scroll down to locate the line for the search functionality that you want to change.

For information on each configuration setting that you can modify for searching on the Vibe site, see "Configuration Settings for Search Features" on page 88.

4 Copy that line to the clipboard of your text editor.

5 Depending on which file you are modifying (as described in Step 2), make a backup copy of the corresponding `ssf-ext.properties` file or `lucene-server-ext.properties` file, which are located in the same directory as the `ssf.properties` file and the `lucene-server.properties` file.

6 Open either the `ssf-ext.properties` file or the `lucene-server-ext.properties` file.

7 Scroll to the end of the `ssf-ext.properties` file or the `lucene-server-ext.properties` file, then paste the line you copied.

8 Edit the setting for the appropriate search functionality as needed.

9 Save and close the `ssf-ext.properties` file or the `lucene-server-ext.properties` file.

10 Close the `ssf.properties` file or the `lucene-server.properties` without saving.

11 Stop and restart Vibe to put the modified search customizations into affect for your Vibe site.

12 Re-index the Vibe site, as described in "Rebuilding the Lucene Index" on page 281.

Configuration Settings for Search Features

The following tables show the configuration settings that you can modify for the various search features. Each configuration setting has a `lucene.indexing` setting and a corresponding `lucene.searching` setting. Both setting must be configured in order to produce the desired functionality.

- Table 4-2, "Removing Frequently Used Words," on page 89
- Table 4-3, "Searching for Various Forms of the Same Word," on page 90

* Table 4-4, “Searching for Words That Contain Accents,” on page 91
* Table 4-5, “Increasing the Number of Words That Are Indexed for Each Document,” on page 91

***Table 4-2** Removing Frequently Used Words*

Setting	Function
`lucene.indexing.stopwords.enable`	Enables or disables the functionality that removes frequently used words that have no inherent meaning when items are added to the index. For more information, see “Removing Frequently Used Words That Have No Inherent Meaning” on page 87. By default, the value is `true` (enabled).
`lucene.indexing.stopwords.file.charset`	If you have provided your own file that contains frequently used words that you want to be ignored (as described in “lucene.indexing.stopwords.file.path” on page 89), you can change the default character encoding of the file that contains the new words. By default, the value is `UTF-8`.
`lucene.indexing.stopwords.file.path`	Lets you point to a file that you create that contains your own list of words that you want Vibe to ignore when items are added to the index. This file should be in a directory where it does not get overwritten or removed during an upgrade. If you are running Vibe in a clustered environment, this should be a directory that is accessible to and shared by all Vibe nodes. You must specify the full path to the file. Each line of the file should contain only one word. All words in the file must be in lowercase. By default, there is no file path specified, and Vibe defaults to a list of common words that are not normally useful when performing a search, such as a, in, this, and so forth.
`lucene.searching.stopwords.enable`	Enables or disables the functionality that removes frequently used words that have no inherent meaning when users perform a search. For more information, see “Removing Frequently Used Words That Have No Inherent Meaning” on page 87. By default, the value is `true` (enabled).
`lucene.searching.stopwords.file.charset`	If you have provided your own file that contains frequently used words that you want to be ignored (as described in “lucene.indexing.stopwords.file.path” on page 89), you can change the default character encoding of the file that contains the new words. By default, the value is `UTF-8`.

Setting	Function
`lucene.searching.stopwords.file.path`	Lets you point to a file that you create that contains your own list of words that you want Vibe to ignore when performing a search. This file should be in a directory where it does not get overwritten or removed during an upgrade. If you are running Vibe in a clustered environment, this should be a directory that is accessible to and shared by all Vibe nodes. You must specify the full path to the file. Each line of the file should contain only one word. All words in the file must be in lowercase. By default, there is no file path specified, and Vibe defaults to a list of common words that are not normally useful when performing a search, such as a, in, this, and so forth. If you leave all three search features enabled (removing frequently used words, searching for various forms of the same word, and searching for words that contain accents), and you want to specify words to ignore that contain accents, you must specify both forms of the word (with and without the accents).

Table 4-3 *Searching for Various Forms of the Same Word*

Setting	Function
`lucene.indexing.stemming.enable`	Enables or disables the functionality that indexes various forms of the same word. For more information, see "Searching for Various Forms of the Same Word" on page 87. By default, the value is `true` (enabled).
`lucene.indexing.stemming.stemmer.names`	Lets you specify the language that you want Vibe to use when indexing the root form of words. For more information, see "Searching for Various Forms of the Same Word" on page 87. By default, the language is `English`. For information about which languages are available, see "Supported Languages for Indexing and Searching for the Root Form of Words" on page 92.
`lucene.searching.stemming.enable`	Enables or disables the functionality that lets users search for various forms of the same word. For more information, see "Searching for Various Forms of the Same Word" on page 87. By default, the value is `true` (enabled).

Setting	Function
`lucene.searching.stemming.stemmer.names`	Lets you specify the language that you want Vibe to use when searching for the root form of words. For more information, see "Searching for Various Forms of the Same Word" on page 87. By default, the language is `English`. For information about which languages are available, see "Supported Languages for Indexing and Searching for the Root Form of Words" on page 92.

Table 4-4 Searching for Words That Contain Accents

Setting	Function
`lucene.indexing.asciifolding.enable`	Enables or disables the functionality that indexes words with accents as well as the same word without the accents. For more information, see "Searching for Words That Contain Accents" on page 87. By default, the value is `true` (enabled).
`lucene.searching.asciifolding.enable`	Enables or disables the functionality that lets users search for words with accents as well as the same word without the accents. For more information, see "Searching for Words That Contain Accents" on page 87. By default, the value is `true` (enabled).

Table 4-5 Increasing the Number of Words That Are Indexed for Each Document

Setting	Function
`lucene.max.fieldlength`	Designates the maximum number of terms that are indexed for each document that is uploaded to Vibe. Be aware that the number of terms per document can be much higher than the number of words in the document (because stemming and ascii folding capabilities enable various forms of each word in the document to be indexed). Only terms that are indexed appear in search results. For more information, see "Increasing the Number of Words That Are Indexed for Each Document" on page 87. By default, the value is `100000`.

Setting	Function
`doc.conversion.size.threshold`	Depending on your specific environment and need, you might need to modify this setting in addition to the `lucene.max.fieldlength` setting. Designates the size of the document that can be indexed in the Vibe site. For more information, see “Increasing the Number of Words That Are Indexed for Each Document” on page 87. By default, the value is `31457280`.
`doc.max.text.extraction.size.threshold`	Depending on your specific environment and need, you might need to modify this setting in addition to the `lucene.max.fieldlength` setting. Designates the maximum size of a document that can be indexed in the Vibe site after the document has undergone file conversion. For more information, see “Increasing the Number of Words That Are Indexed for Each Document” on page 87. By default, the value is `1048576` (about 1MB).

Supported Languages for Indexing and Searching for the Root Form of Words

By default, when Vibe indexes a word, it indexes the root form of the word. Likewise, when users perform a search for a word, Vibe searches for the root form of the word and returns all matches. (For more information, see “Searching for Various Forms of the Same Word” on page 87.)

The default language of the Vibe site is irrelevant in regards to indexing and searching for the root form of words; Vibe detects the language for each individual entry when it performs the indexing and search.

You can configure Vibe to use any of the following languages when indexing and searching for the root form of words (the default is English):

- Danish
- Dutch
- English
- Finnish
- French
- German
- German2 (This is a modified version of German that handles umlaut characters differently. Appends an `e` after vowels that would otherwise have an umlaut. For example, ä becomes `ae`, ë becomes `oe`, and ü becomes `ue`.)
- Hungarian
- Italian
- Norwegian
- Porter (This is for the English language; this option simply indexes and searches in a different way.)

- Portuguese
- Romanian
- Russian
- Spanish
- Swedish
- Turkish

Understanding and Configuring Document Conversions with Oracle Outside-In Technology

Micro Focus Vibe uses the Oracle Outside-In Technology converter to perform document conversions. Documents undergo two types of conversions:

- Word conversion when they are first added to the Vibe site
- HTML conversion when they are viewed as HTML from the Vibe site

If the Oracle Outside-In Technology converter is crashing with certain file types during the word conversion process, you can exclude the problematic file types from being indexed to the Vibe site.

- "Configuring Which File Formats Can Be Viewed as HTML" on page 93
- "Excluding File Types from Being Indexed" on page 93

Configuring Which File Formats Can Be Viewed as HTML

Many file formats in Micro Focus Vibe can be viewed as HTML by default, as described in "Viewing the File in HTML Format" in the *Micro Focus Vibe 4.0.5 User Guide*. File formats that can be viewed as HTML by default are: `.123`, `.bmp`, `.db`, `.doc`, `.docx`, `.dotm`, `.drw`, `.dxf`, `.htm`, `.html`, `.lwp`, `.odf`, `.odf`, `.odp`, `.ods`, `.odt`, `.pct`, `.ppt`, `.pptx`, `.prz`, `.qpw`, `.rtf`, `.sdw`, `.shw`, `.sxw`, `.tif`, `.txt`, `.vsd`, `.wpd`, `.xls`, `.xlsx`, `.sxi`

Some file formats, such as `.pdf` files, cannot be viewed as HTML by default. This is because the quality of these files is lessened when viewed as HTML. However, if you choose, you can enable non-default file formats, such as `.pdf` files, to be viewed as HTML.

Not all file formats can be enabled to be viewed as HTML in Vibe, but many can be. If you are unsure whether Vibe supports a particular file format to be viewed as HTML, try it and see.

You can enable additional file formats to be viewed as HTML during the Vibe installation, as described in "Installing and Setting Up a Basic Vibe Site" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Excluding File Types from Being Indexed

If the Oracle Outside In Technology converter is crashing with certain file types during indexing, you can restrict the problematic file types from being indexed.

- "Excluding File Types from Being Indexed to the Vibe Site" on page 94
- "Excluding File Types from Being Displayed in HTML" on page 94

Excluding File Types from Being Indexed to the Vibe Site

IMPORTANT: Performing the following procedure causes the file types that you specify to be excluded from searches performed in Vibe.

---

1. Change to the following directory:

   Linux: `/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`

   Windows: `c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2. Open the `ssf.properties` file in a text editor.
3. Search for the following line:

   ```
   exclude.from.stellent.indexing.extensions=
   ```

   ```
   exclude.from.openoffice.indexing.extensions=
   ```

4. Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.
5. Open the `ssf-ext.properties` file in a text editor.
6. Copy the `exclude.from.stellent.indexing.extensions=` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.
7. Add the file types that are causing OpenOffice to crash to be the value of this property. For example, `exclude.from.stellent.indexing.extensions=.pptx,.odf`
8. Save and close the `ssf-ext.properties` file.
9. Close the `ssf.properties` file without saving it.
10. Stop and restart Vibe.

Excluding File Types from Being Displayed in HTML

You can display files in HTML view as described in "Viewing the File in HTML Format" in "Working with Folder Entries" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*. If OpenOffice crashes during this HTML conversion process with certain files, you can exclude the problematic file types from being converted. These file types can then no longer be viewed in HTML. For information on how to exclude file types from displaying in HTML, see "Configuring Which File Formats Can Be Viewed as HTML" on page 93.

Customizing the Simple URL Prefix

When users create user-friendly URLs that point to their workspaces or folders, by default, the name they specify is preceeded by the text string `/novl/`. For more information, see "Defining a User-Friendly URL for a Workspace or Folder" in the Micro Focus Vibe 4.0.5 User Guide

Some Vibe 3.*x* administrators configured their systems to not use a prefix, but "empty prefixes" are no longer supported in Vibe 4.*x* because that would preclude WebDAV support.

Other Vibe 3.*x* administrators customized the prefix by including a simpleurl.ctx parameter in the ssf-ext.properties file. In Vibe 4.x, this action alone is no longer sufficient.

To configure Vibe to prepend a different text string, you must do the following:

1. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2. Make a copy of the `ssf-ext.properties` file then open the file in a text editor.
3. Insert the following line at the bottom of the `ssf-ext.properties` file.

   ```
   simpleurl.ctx=/new-prefix
   ```

   where *new-prefix* is the text string that you want prepended.
4. Save and close the `ssf-ext.properties` file.
5. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/conf`
Windows:	`c:\Program Files\Novell\teaming\apache-tomcat\conf`

6. Make a copy of the `server.xml` file then open the file in a text editor.
7. Search for the string `/vibe`.
8. Insert a new line before the line containing `/vibe` as follows:

   ```
   <Context path="/new-prefix" reloadable="false" docBase="novl"
   crossContext="true"/>
   ```

   where *new-prefix* is the text string you that you also specified in Step 3.
9. Save the `server.xml` file.
10. Stop and restart Vibe to enable the simple URL configuration change.

5 Setting Up User Access to the Vibe Site

Adding New Users to Your Vibe Site

You can add new users to your Vibe site in any of the following ways:

- Synchronizing from an LDAP directory, as described in "Synchronizing Users and Groups from an LDAP Directory" on page 205.
- Manually adding local users, as described in "Creating a New Local User" on page 220.
- Importing profile files for local users, as described in "Managing Local Users and Groups by Importing Profile Files" on page 226.

Creating Groups of Users

This section describes how to create groups within Vibe. You can also synchronize groups of users from your LDAP directory to your Micro Focus Vibe site, as described in "Synchronizing Users and Groups from an LDAP Directory" on page 205.

You can use existing groups or create additional groups within Vibe to facilitate access control on your Vibe site. For background information on access control, see "Controlling Access" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

In addition to creating groups to assist with access control, you might want to create groups for any of the following reasons:

- To facilitate team creation, as described in "Creating a Team Workspace" in "Getting Started" in the *Micro Focus Vibe 4.0.5 User Guide*.
- To facilitate managing data quotas, as described in "Managing User Data Quotas" on page 244.
- To facilitate user visibility restrictions, as described in "Restricting Groups of Users from Seeing One Another" on page 103.
- To create multiple Vibe administrators, as described in "Creating Additional Vibe Administrators" on page 18.

Users are responsible for access control in their personal workspaces and any team workspaces that they create. As the Vibe site administrator, you are responsible for access control in public locations such as global workspaces. By creating groups of users who have attributes in common, you and other Vibe users can set access controls and create teams without listing users individually. Groups can be nested within groups, so create small groups first, then build larger groups from your smaller groups.

You can create either static or dynamic groups.

- “Creating Static Groups” on page 98
- “Creating Dynamic Groups” on page 99

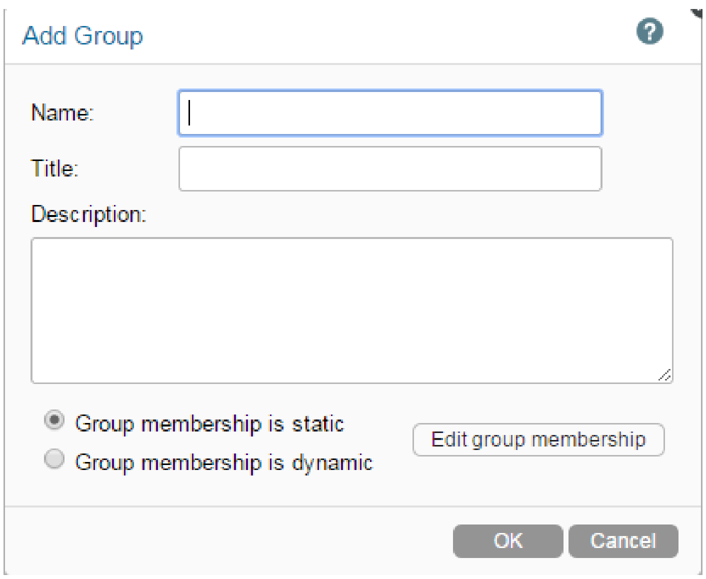
Creating Static Groups

Static groups are groups whose membership does not change based on LDAP queries.

This section describes how to create static groups directly from Vibe. You can synchronize static groups to Vibe from your LDAP directory as described in “Synchronizing Users and Groups from an LDAP Directory” on page 205.

To create static groups in Vibe:

1. Log in to the Vibe site as the Vibe administrator.
2. Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.
3. Under **Management**, click **Groups**, then click **New**.



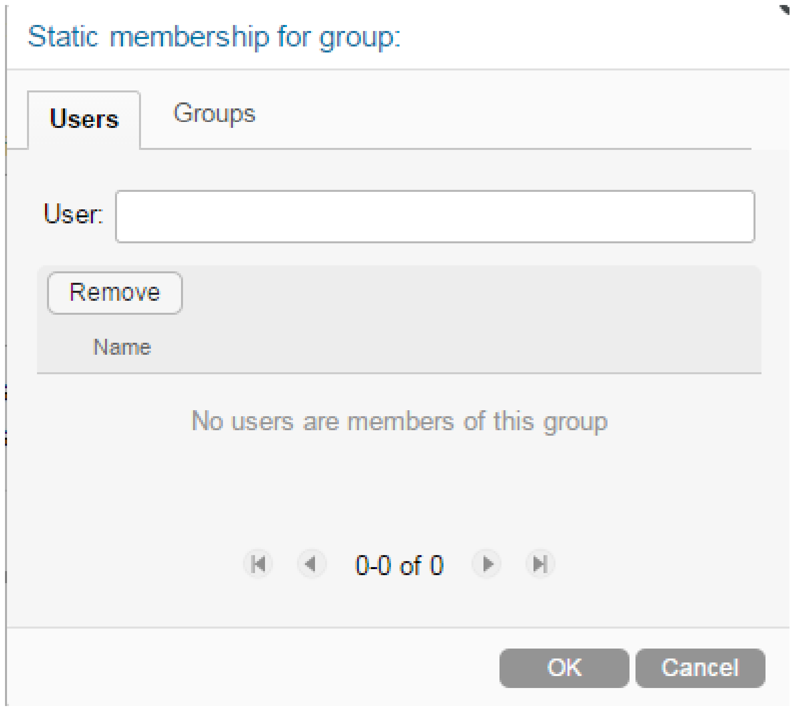
4. Fill in the following fields:

   Name: Specify the unique name under which the group is stored in the Vibe database. You can use alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_).

   Title: Specify the group name that displays to users on the Vibe site. This string can include any characters that you can type.

   Description: Describe what the members of this group have in common.
5. Select **Group membership is static**.

   This means that group membership does not change based on LDAP queries.
6. Click **Edit group membership**.



7 Click the **Users** or **Groups** tab, depending on whether you want to add users or groups to the group that you are creating.

8 In the **User** or **Group** field, specify the name of the user or group that you want to add to the group that you are creating, then click the name of the user or group when it appears in the drop-down list.

9 Repeat Step 7 and Step 8 to add multiple users and groups to the group that you are creating, then click **OK** when you have finished adding users and groups.

10 Click **OK** to create the group.

After you have created one or more small groups, you can use the **Groups** field to create larger groups from smaller groups.

Creating Dynamic Groups

Groups based on LDAP queries are dynamic in that they can be configured to have their membership updated when the information in the LDAP directory changes.

Creating groups based on LDAP queries is a quick way to create Vibe groups that consist of users who match specific criteria. You can create dynamic groups as described in the following sections:

- “Creating Dynamic Groups within LDAP” on page 100
- “Creating Dynamic Groups within Vibe” on page 100

Creating Dynamic Groups within LDAP

Depending on the LDAP directory that you are using, you might be able to create dynamic groups within your LDAP directory. For example, you can create dynamic group objects in eDirectory with Novell iManager (for more information, see the iManager Documentation (http://www.novell.com/documentation/imanager27/index.html)).

Dynamic groups created within LDAP are stored in your LDAP directory and can then be synchronized to Vibe, as described in "Synchronizing Users and Groups from an LDAP Directory" on page 205

Creating Dynamic Groups within Vibe

You can create dynamic groups in Vibe by querying the LDAP directory.

Prerequisites

- Users must already have existing Vibe user accounts in order for them to be added to a Vibe group as described in this section. If your LDAP query includes users who are not already Vibe users, the users are not added to the Vibe group
- When configuring your LDAP connection, you must specify the GUID name (LDAP attribute that uniquely identifies the user), because the value of this attribute never changes. For eDirectory, this value is `GUID`. For Active Directory, this value is `objectGUID`. For GoupWise, this value is `entryUUID`. For more information about this attribute, see "Server Information" on page 207.

  The Vibe process that creates a dynamic group uses the LDAP configuration settings in Vibe to authenticate to the LDAP directory server. The credentials that are used are the LDAP server URL, user DN, and password. For more information on how to configure these and other LDAP configuration settings in Vibe, see "Synchronizing Users and Groups from an LDAP Directory" on page 205.

Advantages

Advantages to creating dynamic groups within Vibe rather than within your LDAP directory include:

- Allows the Vibe administrator to control group membership without having direct access to the group object in the LDAP user store.
- Your LDAP directory might not support dynamic groups.
- You do not want dynamic groups to sync to applications other than Vibe that are leveraging your LDAP directory.

Considerations with Multiple LDAP Sources

Consider the following if your Vibe site is configured with multiple LDAP sources:

- You should not create dynamic groups in Vibe if the base dn that you define for the dynamic group does not exist in each LDAP source. This is because the membership of the dynamic group might not get updated correctly.
- If your Vibe site is configured with multiple LDAP sources and the base dn that you define for the dynamic group exists in each LDAP source, the membership of the dynamic group contains users from each LDAP source that match the dynamic group's filter.

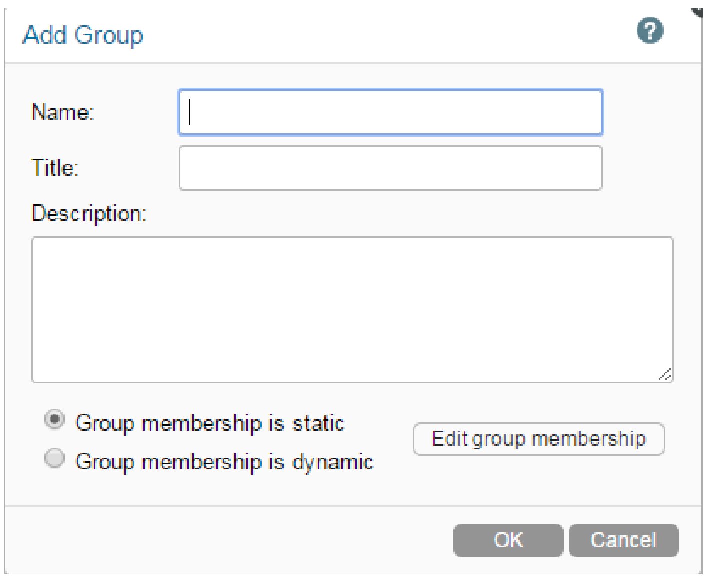
Creating the Group

To create the dynamic group within Vibe:

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under **Management**, click **Groups**, then click **Add**.



4 Fill in the following fields:

Name: Specify the unique name under which the group is stored in the Vibe database. You can use alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_).

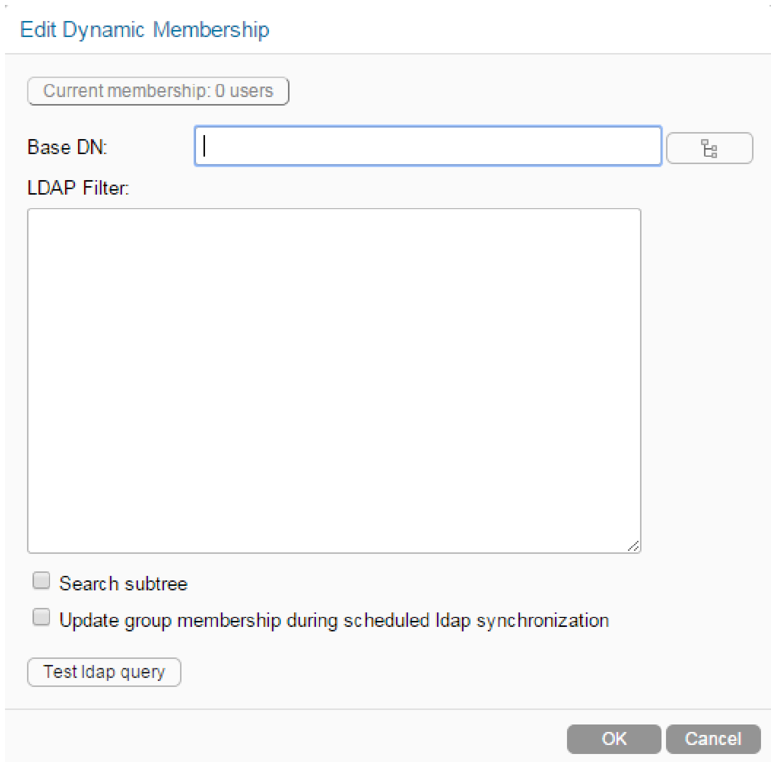
Title: Specify the group name that displays to users on the Vibe site. This string can include any characters that you can type.

Description: Describe what the members of this group have in common.

5 Select **Group membership is dynamic**.

This means that group membership is based on an LDAP query that you will define in this procedure.

6 Click **Edit group membership**.



7 Specify the following options:

Base DN: Specify the base DN where you want to start your search.

If you have multiple LDAP sources, see "Considerations with Multiple LDAP Sources" on page 101 before proceeding.

LDAP Filter: Specify the filter criteria.

For example, to search for all users located in Utah, specify `(st=Utah)`.

Search subtree: Select this option if you want to also search for matches in subtrees of the base dn you are currently searching.

Update group membership during scheduled ldap synchronization: Select this option to update the membership of this group during each scheduled LDAP synchronization. Group membership is updated based on changes that might have occurred in the LDAP directory.

For information on how to set the LDAP synchronization schedule, see "Configuring the Synchronization Schedule" on page 215.

8 (Optional) Click **Test ldap query** to test the results of your LDAP query.

This process can take several minutes, depending on the size of your LDAP directory.

9 Click **OK** > **OK** to create the group.

Restricting Groups of Users from Seeing One Another

If your Micro Focus Vibe site has multiple sets of users who need to remain hidden from each other, you can use access controls to restrict users who belong to a specific group from seeing users who do not belong to the group. For example, you might want to do this if your Vibe site contains users from more than one company and you want users to see only the users who belong to the same company.

You accomplish this by setting zone-level access controls on individual users or groups of users, limiting them to seeing only those users with whom they share a common group.

When you restrict groups of users from seeing one another in your Vibe site, you see the following behaviors:

- When users search for people in the Vibe site, they do not see the users they are restricted from seeing.
- By default, users cannot see the personal workspaces of users they are restricted from seeing. However, individual users can modify the access control settings of their personal workspaces to grant access to users who are restricted from seeing them. Users can do this by granting access to other groups.
- The Vibe site might contain folders and entries that are open to a wider audience, such as in a global workspace. If a restricted user has access to one of these folders, and an entry is posted by someone the user is not allowed to see, the name of the entry creator is hidden. The name is also hidden from the restricted user wherever else it might appear, such as in the Left Navigation pane or on the Search Results page.

  For example, User B is restricted from seeing User A. when User A posts an entry in a global workspace, User B can see the entry but cannot see User B's name on the entry.

To restrict groups of users from seeing one another:

1. Create a group for each set of users that you want to keep separate. For example, create groups called Company A, Company B, and Company C.

   For information about how to create a group, see "Creating Groups of Users" on page 97.

2. Populate each group with the appropriate users.

   For information about how to populate groups with users, see "Creating Groups of Users" on page 97.

3. Navigate to the Administration page and add the groups to the **Can Only See Members of Groups I Am In** role or use the **Limit User Visibility** option as explained in "Limiting User Visibility" on page 225.

   If you want to allow certain members of a group to retain their ability to see users that belong to groups outside of their own, you can add these specific users to the **Override "Can Only See Members of Groups I Am In"** role.

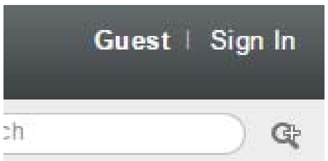
   For more information about these roles as well as other roles, see "Controlling User Access to Administrative Functions" on page 29.

   For information about how to add users and groups to a specific role, see "Controlling User Access to Administrative Functions" on page 29.

IMPORTANT: Do not create a group that contains users who you want to hide from each other. For example, if your Vibe site has users from Company A and Company B, you should not create a single group that contains users from both Company A and Company B. Users who belong to a common group are able to see each other, regardless of any access controls that are set on other groups. If you must create a single group of users from multiple companies, first create a sub-group for each company so you can keep users' names separate from each other.

Allowing Guest Access to Your Vibe Site

When a person arrives at the Micro Focus Vibe site URL, the person is considered to be a Guest user on the site, as indicated by the user name displayed in the upper right corner of the page:



This page is also the main Vibe login page. Users with Vibe user names can log in to their personal workspaces, and from there they can access any other locations where they have been granted access.

- "Guest Access Limitations" on page 104
- "Understanding the Guest User" on page 105
- "Setting Up Guest Access for the Vibe Site" on page 105
- "Configuring Any Workspace to Be the Default Home Page for Guest Users" on page 107
- "Enabling Individual Users to Grant Guest Access throughout the Vibe Site" on page 107
- "Monitoring Guest User Access" on page 108

Guest Access Limitations

Guest access to the Vibe site is not possible in the following situations:

- If you are using NetIQ Access Manager to provide single sign-on functionality.

  For more information about NetIQ Access Manager, see "Configuring Single Sign-On with Novell Access Manager" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

- If users are accessing the Vibe mobile interface. For guest users to access the Vibe site, they must access the full user interface from a browser.

  For more information about accessing the Vibe mobile interface, see the *Micro Focus Vibe Mobile Quick Start (https://www.novell.com/documentation/vibe4/vibe4_qs_mobile/data/vibe4_qs_mobile.html)*.

Understanding the Guest User

As the administrator, you can choose whether you want people who do not have Vibe user names to be able to access information on the Vibe site as the Guest user.

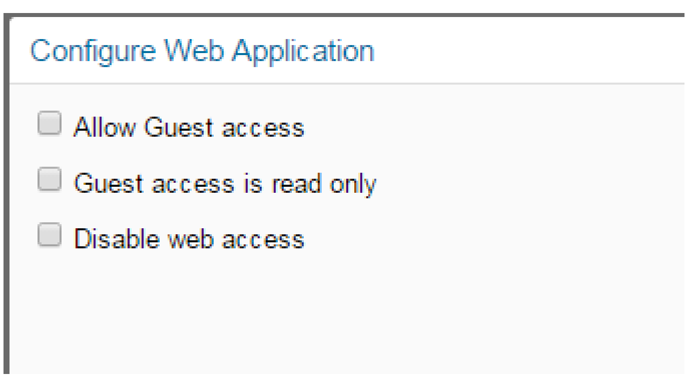
For example, a government organization such as a city might give Vibe user accounts only to key city knowledge workers. However, it is critical that other city workers and regular citizens also access the site to see a listing of upcoming events, read city news, report complaints, and so forth. As a Vibe administrator, you can use the Guest User workspace as a place to present information to non-registered Vibe users.

When people visit your Vibe site as the Guest user, they can have some or all of the following experiences, depending on the access controls that you set for the Guest user:

- Any user who knows the Vibe site URL can access the Guest workspace.
- The Relevance Dashboard in the Guest workspace displays only the information that the Guest user has been specifically granted access to see.
- A Guest user can find out what is accessible on the Vibe site by clicking the **Search Options** icon, selecting **Places**, then pressing the Spacebar.
- If a Guest user uses the Search feature, the only information returned is information that the Guest user has been granted access to see.
- When a Guest user adds a folder entry, the entry form requests the user's name and email address. This information is displayed like a signature when the folder entry is viewed. Providing the name and email address is optional.
- If you grant Participant rights to the Guest user, people who access the Vibe site as the Guest user can modify and delete entries and comments posted by other people who have accessed the Vibe site as the Guest user.

Setting Up Guest Access for the Vibe Site

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. Under **System**, click **Web Application**.



4. Under **System**, click **Configure Guest Access and Self Registration**.
5. Make sure that **Allow Guest Access** is selected, then click **Close**.

Even though this option is selected by default, the Guest workspace is initially inaccessible because the default user access control settings do not allow access.

6 (Optional) Select **Guest access is read only** if you do not want the Guest user to be allowed to add files or make comments on files.

7 Click **Close** again to close the Administration page.

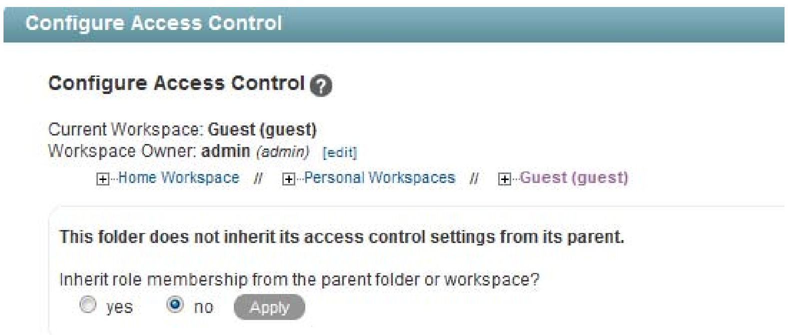
8 Click the Workspace tree icon, expand **Home Workspaces**, then click **Personal Workspaces**.

9 Begin typing `Guest` in the **Entry** field, then click it in the drop-down list.

The Guest user's personal workspace is displayed.

10 Click the **Configure** icon next to the workspace title, then click **Access Control**.

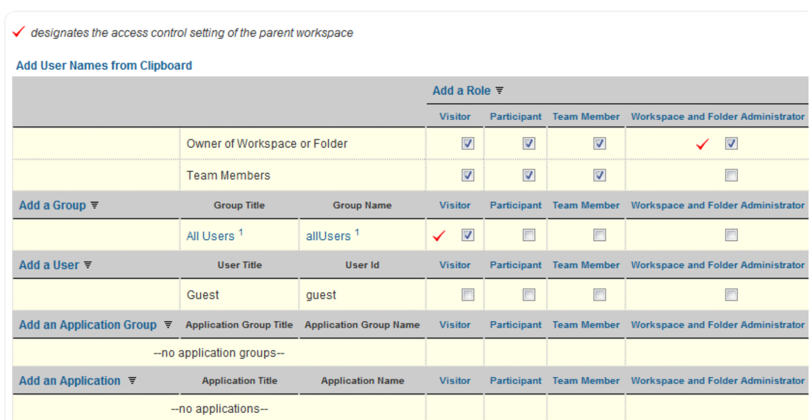
11 Ensure that **no** is selected in the Inherit role membership section. If it is not, select **no** then click **Apply**.



12 Add the roles that you want the Guest user to be able to perform in the Guest workspace:

12a Click **Add a User,** start typing `Guest` in the **Add a User** field, then click **Guest** when it appears in the drop-down list.

This adds **Guest** as a new row in the Access Control table.



12b Select one or more roles that you want the Guest user to be able to perform on the Guest User workspace. For example:

Visitor: The Guest user can read entries and add comments or replies in folders in the Guest user workspace.

Participant: In addition to Visitor activities, the Guest user can also create new entries, and modify or delete his or her own entries.

For more information about the additional access control options, see “Controlling Access” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

12c Click **Save Changes**, then click **Close**.

Now, when people access the Vibe site who do not have user names, they are admitted as a Guest user and see the What’s New page (only items that the Guest user has access to see are visible).

13 (Conditional) If you want the Guest user to be able to access content throughout the Vibe site, add the Guest user to the Configure Access Control page for those workspaces or folders.

You can also enable specific Vibe users in addition to the Vibe administrator to grant Guest access to locations in your Vibe site, as described in “Enabling Individual Users to Grant Guest Access throughout the Vibe Site” on page 107.

14 Notify people who might be interested in accessing your Vibe site about your Vibe site URL.

15 (Conditional) If you want information on your Vibe site to be searchable on the Internet, see “Allowing Web Crawler Access to Your Vibe Site” on page 108.

Configuring Any Workspace to Be the Default Home Page for Guest Users

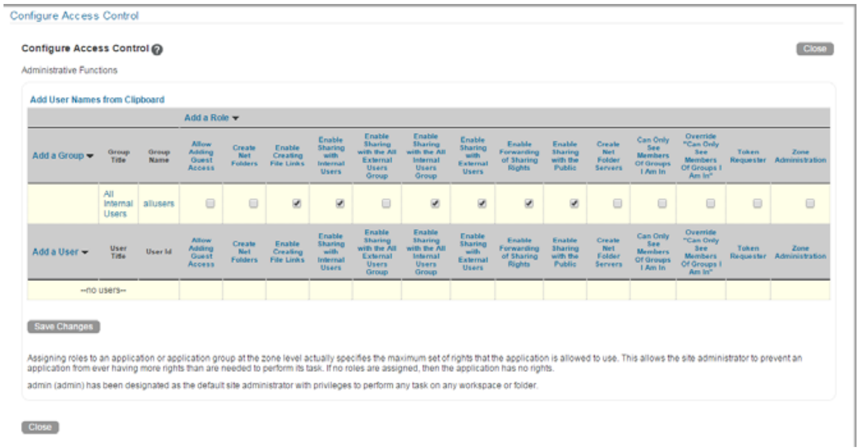
If you’re not satisfied with the What’s New page being the default home page for guest users, you can configure the Guest User workspace or a different workspace to be the default home page, giving you complete control over what guest users see when they first access the Vibe site.

For information on how to change the default home page for guest users, see “Setting a Default Home Page for Guest Users” on page 72.

Enabling Individual Users to Grant Guest Access throughout the Vibe Site

If you want users in addition to the Vibe administrator to be able to grant Guest access to locations in your Vibe site:

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. Under **System**, click **Access Control**.



A basic Vibe site consists of a single zone. Micro Focus Vibe lets you set up multiple zones in a single Vibe site. For more information about zones, see Chapter 19, “Setting Up Zones (Virtual Vibe Sites),” on page 195.

4. Click **Add a User**, start typing the user’s name, then select the user from the drop-down list to add the user to the Access Control table.
5. Select the check box in the **Allow Adding Guest Access** column.
6. Repeat Step 4 and Step 5 for each user who you want to be able to grant Guest access to locations on your Vibe site.
7. Click **Save Changes**, then click **Close**.
8. Notify the users who are allowed to grant Guest access.

Monitoring Guest User Access

As the Vibe site administrator, you can create a report of all locations on the Vibe site that the Guest user can access. For instructions, see “User Access Report” on page 298.

Allowing Users Limited External Access to Your Vibe Site

Vibe lets you restrict what information users can access when they are outside your corporate firewall. For more information, see “Restricting Access Rights of Users Outside the Firewall” on page 38.

Allowing Web Crawler Access to Your Vibe Site

If you allow Guest access to your Micro Focus Vibe site, as described in “Setting Up Guest Access for the Vibe Site” on page 105, you can provide Internet search engines (such as Google) with the Vibe permalinks for workspaces and folders that you want to make publicly available on the Internet. A

Vibe permalink is the complete URL that someone outside of your Vibe site and outside of your organization, such as a web crawler (http://en.wikipedia.org/wiki/Web_crawler), could use to access a specific location on your Vibe site.

1 To determine the permalink of a workspace or folder, click **Permalinks** at the bottom of a workspace or folder page.

Disabling User Access to the Vibe Site on the Web

If you want users to have access to the Vibe system only through the Vibe desktop application, you can disable users' ability to access the Vibe site via a web browser.

You can restrict access to the Vibe site on the web for all users, or for specific users and groups. Alternatively, you can disable access to the site for all users and then enable access for specific users and groups.

- "Disabling Access for All Users" on page 109
- "Disabling or Enabling Access for Individual Users" on page 110
- "Disabling or Enabling Access for Individual Groups" on page 111

Disabling Access for All Users

Disabling access as described in this section disables access to Vibe on the web for all users in the Vibe system, except for the Vibe administrator.

1 Log in to the Vibe site as the Vibe administrator.

   1a Launch a web browser.

   1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

   Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

   Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 Under **System**, click **Web Application**.

4 Select **Disable web access**.

5 Click **OK**.

Disabling or Enabling Access for Individual Users

1 Log in to the Vibe site as the Vibe administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

Replace *`Vibe_hostname`* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 Under **Management**, click **Users**.

The Manage Users page is displayed.

4 (Conditional) If you have not disabled access for all users (as described in "Disabling Access for All Users" on page 109), you can disable access for an individual user by clicking the drop-down arrow next to the user's name and then clicking **Disable Web Access for this User**.

or

To disable access for multiple users, select the users whose access you want to disable, then click **More** > **Disable Web Access**.

5 (Conditional) If you have disabled access for all users, you can enable access for an individual user by clicking the drop-down arrow next to the user's name and then clicking **Enable Web Access for this User**.

or

To enable access for multiple users, select the users whose access you want to enable, then click **More** > **Enable Web Access**.

Disabling or Enabling Access for Individual Groups

1 Log in to the Vibe site as the Vibe administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 Under **Management**, click **Groups**.

The Manage Groups page is displayed.

4 (Conditional) If you have not disabled access for all users (as described in "Disabling Access for All Users" on page 109), you can disable access for users who belong to an individual group by clicking the drop-down arrow next to the group name and then clicking **Disable Web Access for Users in this Group**.

or

To disable access for multiple users, select the users whose access you want to disable, then click **More** > **Disable Web Access**.

5 (Conditional) If you have disabled access for all users, you can enable access for users who belong to an individual group by clicking the drop-down arrow next to the group name and then clicking **Enable Web Access for Users in this Group**.

or

To enable access for multiple users, select the users whose access you want to enable, then click **More** > **Enable Web Access**.

Managing Mobile Device Access to Your Vibe Site

By default, your Micro Focus Vibe site allows mobile device access at one of the following URLs, depending on whether or not you are using a secure SSL connection:

```
http://vibe_hostname/mobile
https://vibe_hostname/mobile
```

In these URLs, *vibe_hostname* is the hostname or fully qualified domain name of the Vibe server that you have set up in DNS.

For a list of supported mobile devices, see "Mobile App Requirements" in the *Micro Focus Vibe Mobile Quick Start (https://www.novell.com/documentation/vibe4/vibe4_qs_mobile/data/vibe4_qs_mobile.html)*.

For instructions on using the mobile device interface to the Vibe site, see the *Micro Focus Vibe Mobile Quick Start (https://www.novell.com/documentation/vibe4/vibe4_qs_mobile/data/vibe4_qs_mobile.html)*.

- "Restricting Mobile Device Access to Your Vibe Site" on page 112
- "Changing the Default View for Tablets" on page 112
- "Configuring Mobile Device Access with NetIQ Access Manager" on page 114

Restricting Mobile Device Access to Your Vibe Site

As the Vibe administrator, you can prevent mobile device access to your Vibe site if necessary.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. Under **System**, click *Mobile Access*.
4. Deselect **Enable Mobile Access**.
5. Click **Apply**, then click **Close**.

Changing the Default View for Tablets

When users access the Vibe site through a browser (not through the mobile app), some tablets (such as the iPad and Kindle Fire) display the full UI by default (the same UI that is displayed when you access Vibe from your workstation). Other tablets (such as Android-based tablets) display the mobile UI by default.

For a better user experience, users should use the Vibe mobile app. For more information about accessing Vibe by using the mobile app, see the *Micro Focus Vibe Mobile Quick Start (https://www.novell.com/documentation/vibe4/vibe4_qs_mobile/data/vibe4_qs_mobile.html)*.

- "Changing the Default View for the iPad" on page 112
- "Changing the Default View for Android Tablets" on page 113
- "Changing the Default View for All Other Tablets" on page 114

Changing the Default View for the iPad

To change the default view for the iPad to display the mobile UI rather than the full UI:

1. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2. Open the `ssf.properties` file in a text editor.
3. Search for the following line:

   ```
   tablet.userAgentRegexp=(?:ipad)
   ```

   ```
   exclude.from.openoffice.indexing.extensions=
   ```

4. Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.
5. Open the `ssf-ext.properties` file in a text editor.
6. Copy the `tablet.userAgentRegexp=(?:ipad)` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.
7. If you want the iPad to display the mobile UI, delete the value of this property (`(?:ipad)`), so that it now reads as follows:

   ```
   tablet.userAgentRegexp=
   ```

   ```
   exclude.from.openoffice.indexing.extensions=
   ```
8. Save and close the `ssf-ext.properties` file.
9. Close the `ssf.properties` file without saving it.
10. Stop and restart Vibe.

Changing the Default View for Android Tablets

To change the default view for all tablets that are running the Android operating system to display Vibe in the Full UI rather than the mobile UI:

1. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2. Open the `ssf.properties` file in a text editor.
3. Search for the following line:

   ```
   tablet.useDefaultTestForAndroidTablets=false
   ```

   ```
   exclude.from.openoffice.indexing.extensions=
   ```
4. Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.
5. Open the `ssf-ext.properties` file in a text editor.
6. Copy the `tablet.useDefaultTestForAndroidTablets=false` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.
7. Change the value of this property from `false` to `true`, so that it now reads as follows:

   ```
   tablet.useDefaultTestForAndroidTablets=true
   ```

   ```
   exclude.from.openoffice.indexing.extensions=
   ```
8. Save and close the `ssf-ext.properties` file.
9. Close the `ssf.properties` file without saving it.
10. Stop and restart Vibe.

Changing the Default View for All Other Tablets

To change the default view for all tablets that are not the iPad or Android-based (Kindle, Xoom, Playbook, etc.) to display Vibe in the mobile UI rather than the full UI:

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Open the `ssf.properties` file in a text editor.

3 Search for the following line:

```
tablet.userAgentRegexp=(?:ipad)
```

```
exclude.from.openoffice.indexing.extensions=
```

4 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `tablet.userAgentRegexp=(?:ipad)` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 If you want to change the default view of a specific kind of tablet to display the full UI rather than the mobile UI, add the name of the tablets to the value, as follows:

```
tablet.userAgentRegexp=(?:ipad|xoom|playbook|tablet|kindle|schi800)
```

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe.

Configuring Mobile Device Access with NetIQ Access Manager

To allow mobile device access to Vibe through NetIQ Access Manager, you need to modify your protected resource in NetIQ Access Manager to allow a non-redirected login and to redirect the identity server when no authentication header is provided.

Follow the steps in "Configuring an Authentication Procedure for Non-Redirected Login" in "Protecting Web Resources Through Access Gateway" in the *NetIQ Access Manager Administration Guide*.

When specifying the method for obtaining credentials, ensure that **Non-Redirected Login** and **Redirect to Identity Server When No Authentication Header Is Provided** are selected.

6 Configuring Single Sign-On to the Vibe Site

Configuring Single Sign-On with NetIQ Access Manager

For more information about configuring single sign-on with NetIQ Access Manager, see “Configuring Single Sign-On with Novell Access Manager” in “Advanced Installation and Reconfiguration” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Configuring Single Sign-On with KeyShield

Use the information and instructions in the following sections to configure Vibe to work with an existing KeyShield installation.

Prerequisites

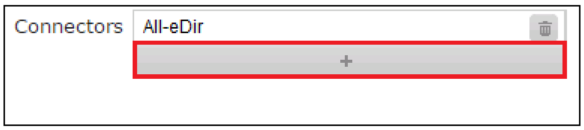
For Vibe to work with an existing KeyShield installation, you must have the following already in place.

- A KeyShield SSO server that is registered with DNS and provides single sign-on services to your network users.
- An API Key that is displayed in a defined API Authorization configuration.
- One or more Authentication Connectors (defined on the KeyShield server) that are allowed to be used with the API Key.
- Administrative Access to the KeyShield server for obtaining the following:
  - The API Authorization Key associated with the KeyShield Connectors you are leveraging for Vibe
  - The SSL certificate, downloadable as a `.CER` file for importing into the Vibe keystore.

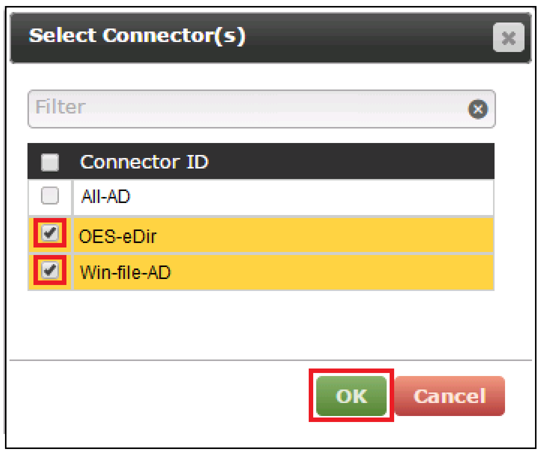
(Conditional) Allowing the Authorization Connectors to Access the API Key

Continuing in the **General** tab (accessed in the previous section), if access to the KeyShield SSO APIs is restricted to users on specific connectors, ensure that the connectors that your Vibe users will be connecting through are listed by doing the following:

1 If the connectors your users will use are not listed, click the bar below the already-allowed connectors.



2 Select the connectors for your users, then click **OK**.



Configuring Vibe for KeyShield SSO Support

1 Open a new tab or a new browser session to access Vibe on port 8443:

`https://Vibe-ip-address-or-dns-name:8443`

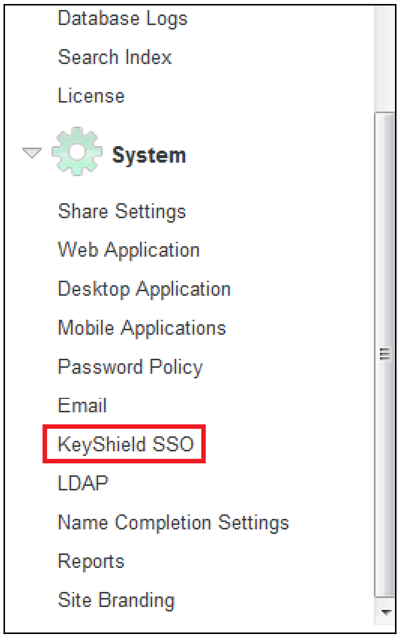
For example `https:192.168.30.150:8443`

Having a new session will let you easily switch between the KeyShield administration console and the Vibe Administration console.

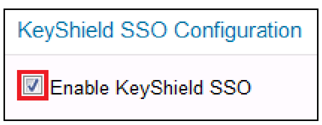
2 In the new browser session, log in to Vibe as an administrator.

3 Click the admin link in the upper-right corner of the page, then click the Administration Console icon .

4 In the left frame, click **KeyShield SSO**.



5 In the KeyShield SSO Configuration dialog, click **Enable KeyShield SSO**.



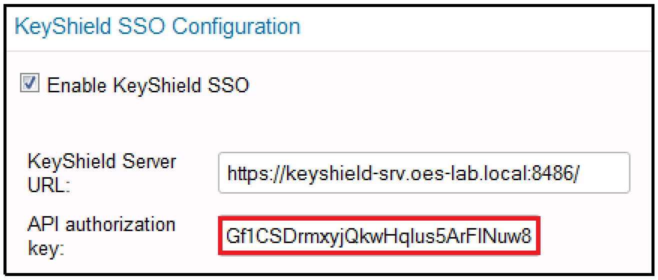
6 In the **KeyShield Server URL** field, type the access URL for the KeyShield server:

`https://`*`ks-server-dns-name_or_ip-address`*`:`*`ks-server-https-port/`*

For example,

7 Switch to the KeyShield browser-based console, toggle open the API Key, then select and copy the key to your clipboard.

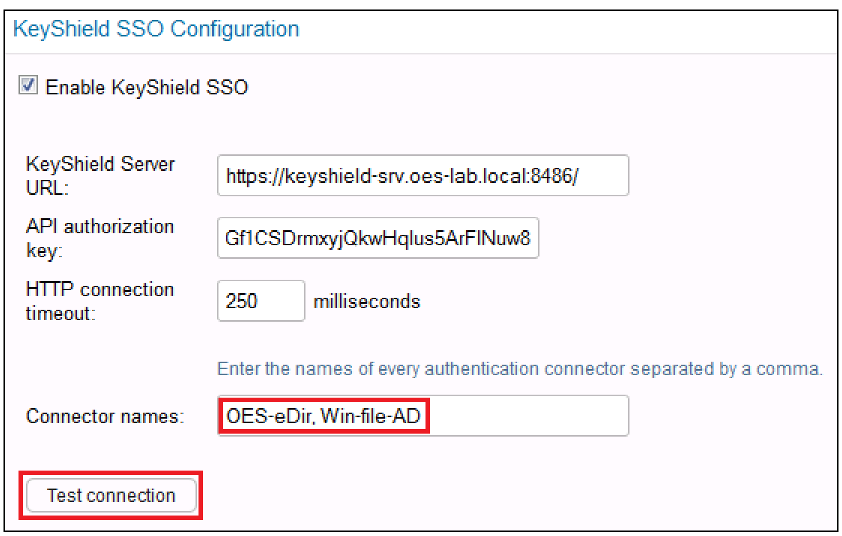
8 Switch to the Vibe Administration panel and paste the API Key into the **API Authorization** field.



9 The **HTTP Connection Timeout** controls how long the Vibe Appliance will wait for a response from the KeyShield server before prompting users for their login credentials.

Micro Focus doesn't recommend changing this value unless the connection between the Vibe Appliance and the KeyShield SSO server doesn't facilitate a quick response. For example the appliance and server are connected over a WAN.

10 In the Connector Names field, type the names of each KeyShield SSO connector that Vibe users will connect through.



11 Continue with the next section, "KeyShield Attribute Alias Support."

KeyShield Attribute Alias Support

Vibe lets administrators provision users from different LDAP sources, such as eDirectory and Active Directory. It also allows for flexibility in specifying which LDAP attribute will be imported as the Vibe username.

In addition to Vibe, organizations have email applications, RADIUS clients, and so on, that use different LDAP attributes for their usernames.

KeyShield 6 includes support for ***Attribute Aliases***. These let KeyShield match username validation requests from each application with the LDAP attribute that the application uses for its usernames.

A Vibe Example

1. Jane Smith logs in through KeyShield's SSO service using jsmith (her UID in LDAP) as her Username.
2. Jane then launches Vibe.

   Unfortunately, the Vibe administrator who configured the LDAP import, specified CN as the LDAP username attribute and JaneSmith was imported as Jane's Vibe username.
3. When Vibe tries to authenticate Jane Smith, KeyShield doesn't find her as an authenticated user and the attempt fails.

   Jane is then prompted to log in to Vibe.
4. To fix the mismatch of LDAP attributes, Jane's KeyShield administrator adds `x-Vibe = cn` as an **Attribute Alias** in Keyshield.
5. Jane's Vibe administrator adds `x-Vibe` as the **Username Attribute Alias** in Vibe.
6. The next time Jane launches Vibe after signing in through KeyShield' SSO service, KeyShield verifies to Vibe that JaneSmith is authenticated and no additional login is required.

Configuring Attribute Alias Support

1 In Keyshield, specify the appropriate **Attribute Alias** for each Authentication Connector.

For example, if your Vibe deployment uses the CN attribute as the username for an eDirectory server that is defined as an Authentication Connector in KeyShield, then in the Attribute Alias field in the connector configuration, you would specify

```
x-Vibe = cn
```

This means that for this Authentication Connector, when authentication verification requests arrive with the Attribute Alias `x-Vibe`, KeyShield needs to request a match in the CN attributes in the targeted eDirectory Authentication Connector.

2 By default, the Vibe 2.0 KeyShield SSO Configuration dialog, the Username Attribute Alias is set to `x-Vibe`.

We strongly recommend that you not change this value. However, if you do, be sure that the name is changed in each KeyShield Authentication Connector configuration as well.

3 Continue with “Configuring Two-Factor Authentication.”

Configuring Two-Factor Authentication

KeyShield 6.1 adds the ability to require a hardware token in addition to usernames and passwords for LDAP users seeking access through a web browser or WebDAV.

NOTE: Two-factor authentication doesn’t apply to desktop or mobile device applications.

Vibe 2.0 supports KeyShield’s two-factor authentication capability through two new options in the KeyShield SSO Configuration dialog:

- **Require Hardware Token:** Requires a physical token, such as an access card, for access to Vibe.

  You can also specify the error messages that you want displayed when the required token is either not presented or not recognized by KeyShield for web browser or WebDAV access.
- **Allow Username/Password based Fallback Authentication (non-SSO) for LDAP Users:**

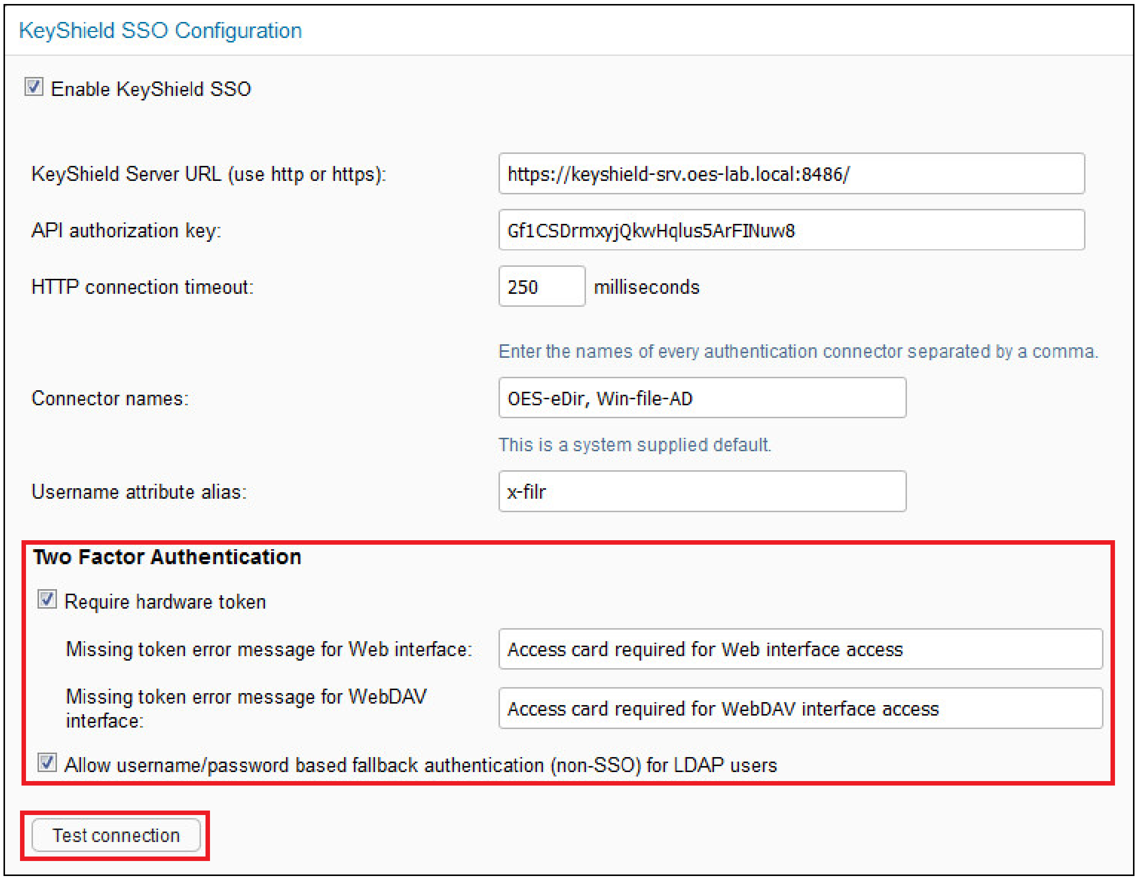
  Allows authentication by entering a username and password as an alternative to the hardware token.

  Use this option if you want users to be able to effectively bypass the hardware token requirement by typing in their username and password.

1 If you want to configure two-factor authentication for your KeyShield 6.1 SSO service, select the options and specify the text accordingly.

2 Click **Test Connection**.

Because the Vibe appliance doesn’t yet have the KeyShield SSO SSL certificate in its keystore, the test fails.



3 Continue with "Downloading and Installing the KeyShield SSO SSL Certificate" on page 121

Downloading and Installing the KeyShield SSO SSL Certificate

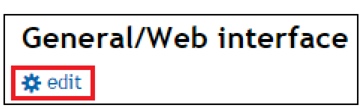
1 Open a third browser session and access the Vibe appliance on port 9443:

`https://`*`Vibe-ip-address-or-dns-name`*`:9443`

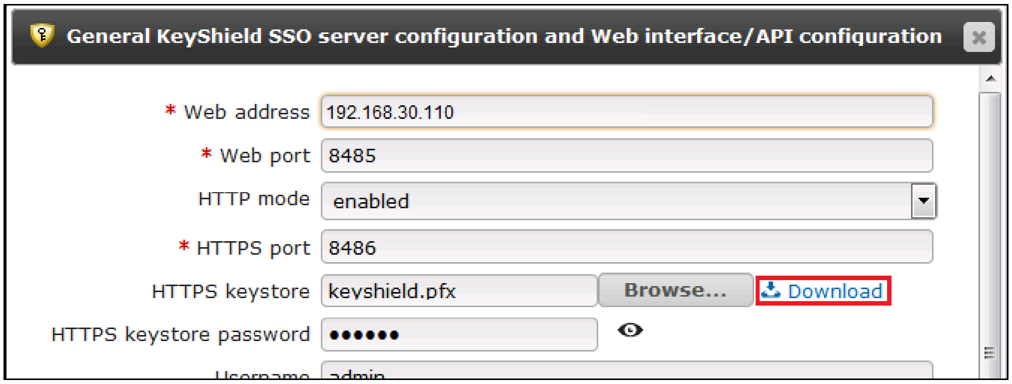
For example `https:192.168.30.150:9443`

2 Log in as `vaadmin`.

3 Switch to the KeyShield browser-based console and under General/Web Interface, click Edit.



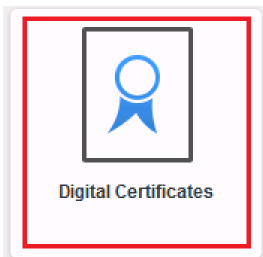
4 Click the **Download** button for the **HTTPS Keystore**.



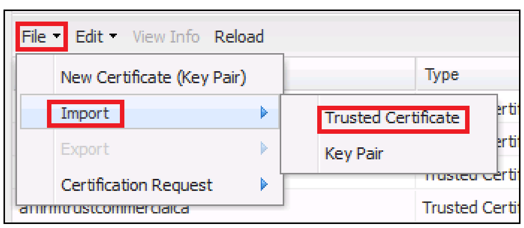
5 Save the `Keyshield.cer` file on the workstation running the browser.

6 Switch to the browser session opened in Step 1 on page 121 and click the **Appliance Configuration** icon.

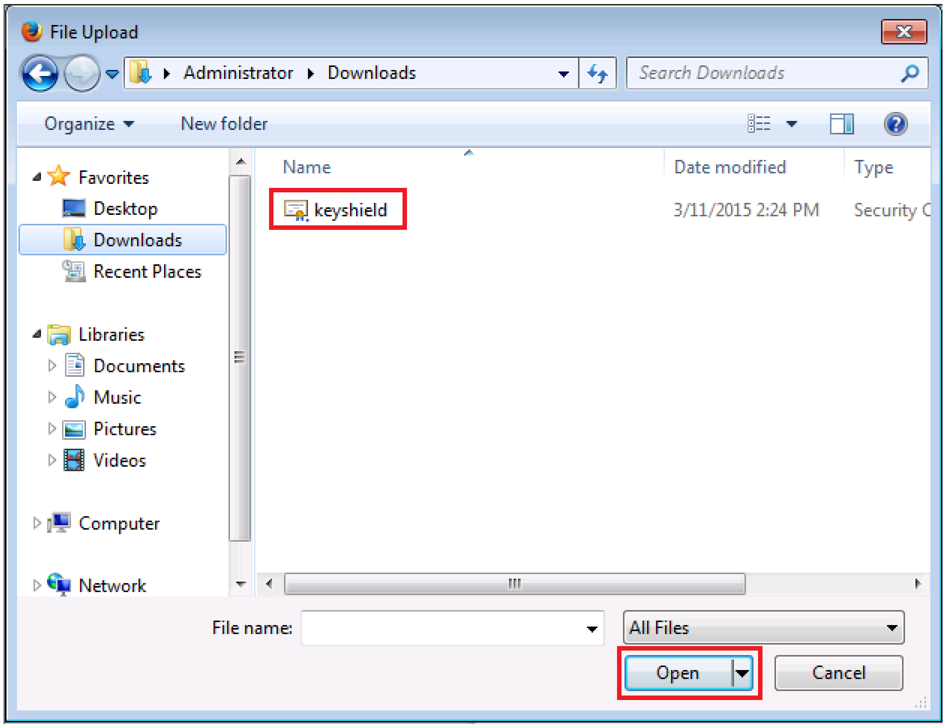
7 Click the **Digital Certificates** icon.



8 Click **File > Import > Trusted Certificate**.



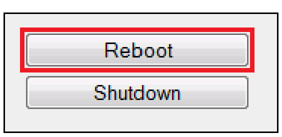
9 Click **Browse**, then browse to the location where you saved the `Keyshield.cer` file and click **Open**.



10 Click **OK** to import the certificate file.

11 Acknowledge the message about restarting the appliance by clicking **OK**.

12 Click the back arrow in the browser, then select **Reboot**.

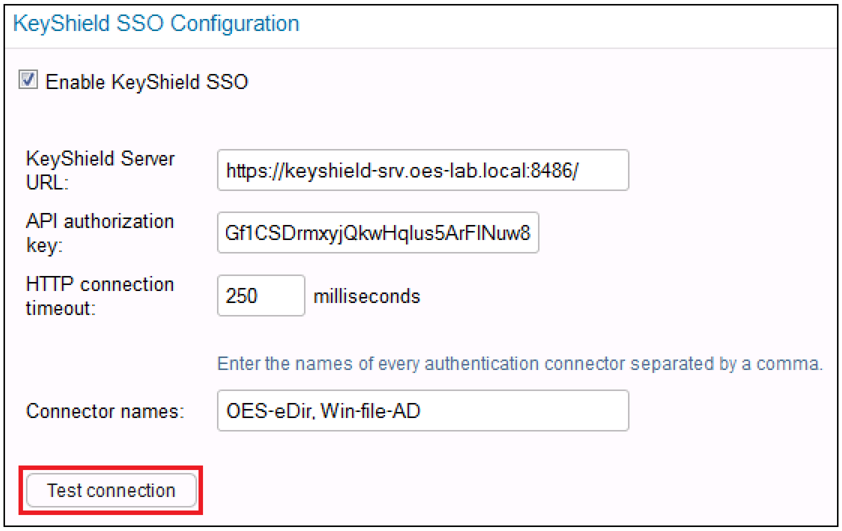


13 After the system restarts, continue with the next section, Testing the KeyShield SSO Configuration.

Testing the KeyShield SSO Configuration

1 Switch back to the Vibe administration console (port 8443).

2 Click **Test Connection**.



The test should succeed.

3 Click **OK** to finalize the configuration and complete the Keyshield SSO integration.

7 Setting Up Sharing

As the Vibe administrator, you need to enable sharing privileges for users on your Vibe site before users are able to share files and folders from their personal workspace. You then need to enable sharing for the top-level Global and Team workspaces in order for users to be able to share content from those workspaces. You or workspace owners can then enable sharing on lower-level workspaces on an individual basis.

There are various sharing privileges that you can grant.

Understanding Sharing

Sharing in Vibe enables users to grant access to entries, folders, and workspaces to other users, either internal or external to the organization.

If multiple users share the same item with a single user, the user who receives the share is granted the highest level of access that was shared with the user. For example, User B shares a file with User A and grants User A Read rights to the file. Then User C shares the same file with User A and grants Read and Write rights to the file. As a result, User A has Read and Write rights to the file.

Understanding External Users

Users external to your organization can access your Vibe site at no additional cost. External users in Micro Focus Vibe do not count as a licensed Vibe user, but they have their own individual user account (unlike the Guest user) and can participate in Vibe workspaces like any other user.

An example of an external user might be a contractor who interacts with the corporation for only a couple months a year, who needs access to the system as a defined user but does not need consistent access to the system.

External users are added to the Vibe system when a workspace, folder, or entry is shared with them. You as the Vibe administrator, determine whether users can share externally. For information about how to enable this functionality, see "Enabling Users to Share" on page 126.

Users Can't Grant Share Roles That They Don't Have

Users with Contributor rights on folders or workspaces can grant Viewer, Editor, and Contributor rights to other users as Vibe system share settings allow.

On the other hand, Users with Viewer rights on folders or workspaces can grant only Viewer rights to other users with whom they are allowed to share.

Enabling Users to Share

IMPORTANT: You must enable the sharing feature before any sharing can take place on the Vibe system.

After you enable the sharing feature, the default behavior for whether users can share files from their personal workspace differs depending on whether the user is new to the Vibe system after Vibe 4, or if the user existed in the Vibe system prior to Vibe 4:

- **New users:** Users who are new to the Vibe system after Vibe 4 are able to share items from their personal workspace by default.
- **Existing users:** Users who existed in the Vibe system prior to Vibe 4 do not automatically have rights to share items from their personal workspace.

For users to be able to share files that are located outside of their personal workspace (such as their team workspaces, etc.), sharing must be enabled on the individual workspace. For information about how to enable sharing for the top-level Global and Team workspaces, see "Enabling Sharing on Workspaces" on page 131.

When you enable users to share, it is best to keep the share rights fairly unrestricted (for example, give the All Internal Users group the ability to share whatever they want). You can then restrict sharing of files in the personal workspace on a per-user basis.

When you set up sharing for your Vibe site, complete the necessary steps in the following order:

1. Set up sharing for the entire Vibe site (as described in "Enabling Sharing for All Users" on page 127).
2. Configure sharing for individual users (as described in "Modifying Share Rights on a User Basis" on page 130).

   After you have enabled sharing for the entire Vibe system, you can fine-tune share rights throughout the site on the user level.

   You might need to do this for the following reasons:

   - If you want only certain users to be allowed to share files from their personal workspace. After you have enabled sharing for the entire site (as described in "Enabling Sharing for All Users" on page 127), then you can restrict sharing privileges at the user level.

     For example, if you want only a few groups of users to be allowed to share with external users, you first need to enable sharing to external users at the site level. After you have enabled it at the site level, you can then remove this ability from the users who you do not want to have this ability.
   - If there are users who existed in your Vibe system prior to Vibe 4, and you want these users to be able to share items from their personal workspace, you must modify the workspace share rights for these users at the user level.

Enabling Sharing for All Users

1 Log in to the Vibe site as the Vibe administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

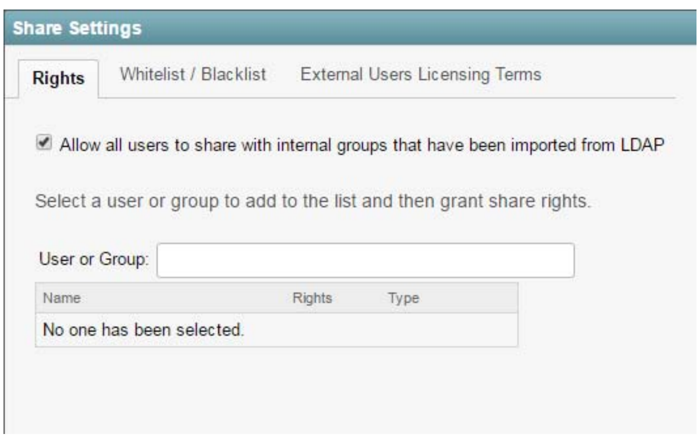
Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 Under **System**, click **Share Settings**.

The Share Settings page is displayed.



4 Select **Allow all users to share with groups that have been imported from LDAP** to enable users to share with LDAP groups.

If you select this option, groups that were imported from the LDAP directory are displayed in the **Share with** field when users are sharing an item (as described in "Sharing Entries, Folders, and Workspaces" in the *Micro Focus Vibe 4.0.5 User Guide*). All users in the LDAP group then have access to the item that was shared.

5 To enable sharing for all internal users on the Vibe site, go to the **User or Group** field, begin typing `All Internal Users`, then select it when it appears in the drop-down list.

or

To enable sharing on a per-user or per-group basis, go to the **Select user/group** field, begin typing the name of the user or group for whom you want to grant share rights, then select the name when it appears in the drop-down list.

The Edit Share Rights dialog box is displayed. Select from the following options:

Re-share items: When users share a file or folder, they can give the users they are sharing with the ability to re-share the file or folder. The user receiving the share can share the file only if that user has been given administrative rights to share the file or folder.

IMPORTANT: When selecting this option, be aware that if one user's access rights to an item are removed, it does not remove the access rights of the user with whom the item was re-shared.

For example, suppose User A shares an item with User B and grants re-share rights. User B then shares the item with User C. If User A revokes User B's access rights to the item, User C continues to have access to the shared item.

Share with Internal users: lets users share items with internal users.

Share with "All Internal Users" group: lets users perform a mass share to all internal users by sharing with the `All Internal Users` group.

Share with External users: lets users share items with users external to the organization.

Users external to the organization receive an email notification with a link to the shared item, and they can then log in to the Vibe site. For more information, see "Sharing with People Outside Your Organization" in the *Micro Focus Vibe 4.0.5 User Guide*.

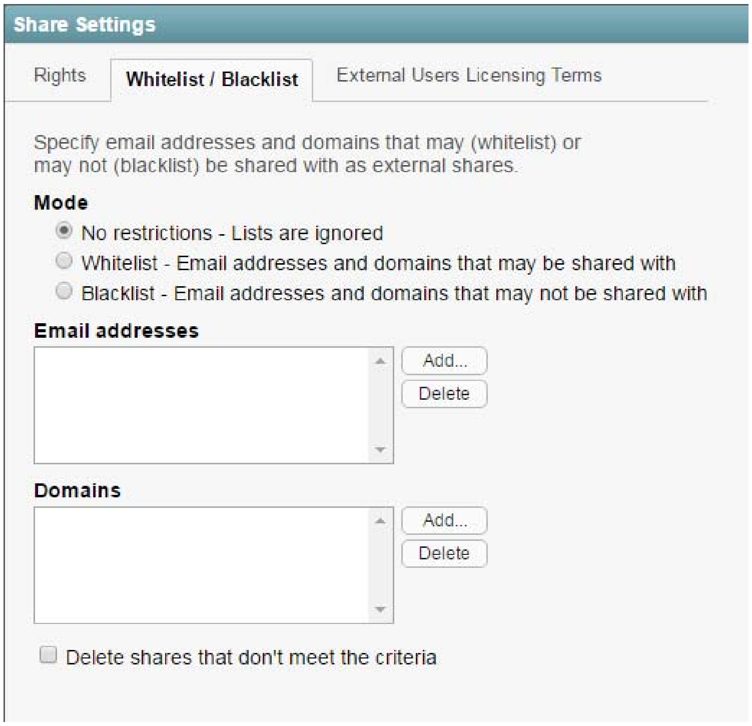
Share with Public: lets users make items publicly available. This means that anyone with the correct URL to the shared item can access the shared item without logging in to the Vibe site.

In addition to selecting this option, you also need to enable Guest access to the Vibe site if you want to allow users to share items with the public. For information about how to enable Guest access to the Vibe site, see "Setting Up Guest Access for the Vibe Site" on page 105.

Share using File Link: lets users share a link to a file in Vibe. Any user with the link can then access the file. However, the file is not displayed in the Public area, so users must have direct access to the link in order to access the file.

For more information about File Links, see "Distributing a Link to a File" in the *Micro Focus Vibe 4.0.5 User Guide*.

6 (Optional) Click the **Whitelist / Blacklist** tab to configure which email addresses and domains users can share with when sharing externally.



The following options are available when configuring a whitelist or blacklist for sharing:

No restrictions: Select this option to disregard any email addresses or domains that might already exist in the **Email addresses** and **Domains** fields. Selecting this option means that users can share with any email address.

Whitelist: Select this option to allow sharing only with email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.

Blacklist: Select this option to disallow sharing with any email addresses and domains that have been specified in the **Email addresses** and **Domains** fields.

Email addresses: Click **Add**, specify the email address that you want to add to the whitelist or blacklist, then click **OK**.

Repeat this process to add multiple email address.

Domains: Click Add, specify the domain that you want to add to the whitelist or blacklist (for example, `yahoo.com`), then click **OK**.

Repeat this process to add multiple domains.

Delete shares that don't meet the criteria: Select this option to delete all existing shares in the Vibe system that do not match the criteria you set.

For example, if you selected **Blacklist** and then specified **yahoo.com** in the **Domains** field, selecting this option would delete all Vibe shares made to Yahoo email addresses.

7. Click **OK**.
8. Modify individual user share rights as described in "Modifying Share Rights on a User Basis" on page 130.

Modifying Share Rights on a User Basis

After you have enabled sharing of files for the entire Vibe system (as described in “Enabling Sharing for All Users” on page 127), you can modify share rights throughout the site on the user level.

You might need to do this for the following reasons:

- If you want only certain users to be allowed to share files from their personal workspace. After you have enabled sharing for the entire site (as described in “Enabling Sharing for All Users” on page 127), then you can restrict sharing privileges at the user level.

  For example, if you want only a few groups of users to be allowed to share with external users, you first need to enable sharing to external users at the site level. After you have enabled it at the site level, you can then remove this ability from the users who you do not want to have this ability.
- If there are users who existed in your Vibe system prior to Vibe 4, and you want these users to be able to share items from their personal workspace, you must modify the workspace share rights for these users at the user level.

You cannot grant individual users more rights than are currently defined for the site-wide setting.

To modify share rights for specific users:

1 Log in to the Vibe site as the Vibe administrator.

  1a Launch a web browser.

  1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

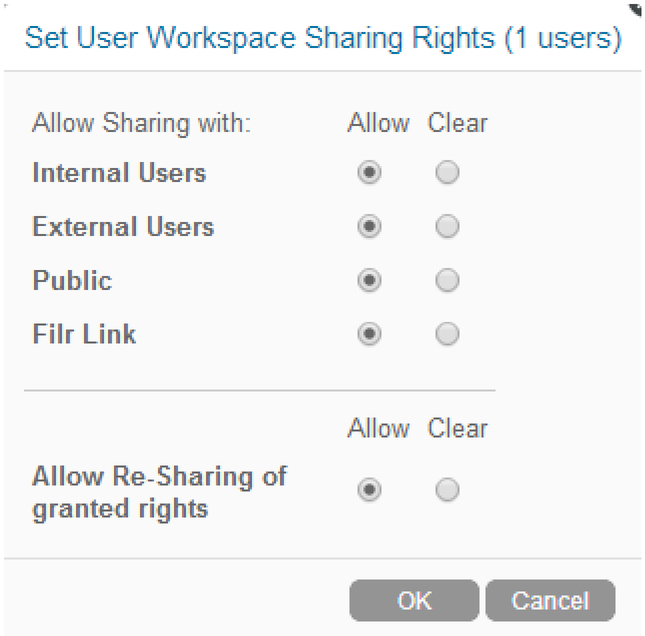
  Replace *`Vibe_hostname`* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

  Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Users**.

4 Select the users whose sharing rights you want to manage, then click **More** > **Workspace Share Rights**.



5 Select the radio button in the **Clear** column next to the sharing right that you want to remove from the user or group, then click **OK**.

or

If you have already removed a share right and you want to add it again, select the radio button in the **Allow** column next to the sharing right that you want to add to the user or group, then click **OK**.

Enabling Sharing on Workspaces

After sharing has been enabled for users on your Vibe site (as described in "Enabling Users to Share" on page 126), you can enable sharing for the top-level Global and Team workspaces in order for users to be able to share content from those workspaces. You or workspace owners can then enable sharing on lower-level workspaces on an individual basis.

- "Enabling Sharing for Top-Level Global Workspaces" on page 131
- "Enabling Sharing for Top-Level Team Workspaces" on page 133

Enabling Sharing for Top-Level Global Workspaces

1 Log in to the Vibe site as the Vibe administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **Workspace Tree** icon in the Action toolbar, expand **Home Workspace**, then click **Global Workspaces**.

3 Select all top-level workspaces by selecting the checkbox in the column header.

4 When all the top-level workspaces are selected, click **Workspace Share Rights**.

The Set Workspace Sharing Rights dialog box is displayed.

Select **Allow** next to any share rights that you want to grant to all the selected workspaces, and select **Clear** next to any share rights you do not want to grant. Select **No Change** to maintain any share rights that might already exist on any workspaces.

The following share rights are available:

Internal Users: lets users share items with internal users.

External Users: lets users share items with users external to the organization.

Users external to the organization receive an email notification with a link to the shared item, and they can then log in to the Vibe site. For more information, see "Sharing with People Outside Your Organization" in the *Micro Focus Vibe 4.0.5 User Guide*.

Public: lets users make items publicly available. This means that anyone with the correct URL to the shared item can access the shared item without logging in to the Vibe site.

In addition to selecting this option, you also need to enable Guest access to the Vibe site if you want to allow users to share items with the public. For information about how to enable Guest access to the Vibe site, see "Setting Up Guest Access for the Vibe Site" on page 105.

File Link: lets users share a link to a file in Vibe. Any user with the link can then access the file. However, the file is not displayed in the Public area, so users must have direct access to the link in order to access the file.

For more information about File Links, see "Distributing a Link to a File" in the *Micro Focus Vibe 4.0.5 User Guide*.

Allow Re-Sharing of granted rights: When users share a file or folder, they can give the users they are sharing with the ability to re-share the file or folder. The user receiving the share can share the file only if that user has been given administrative rights to share the file or folder.

IMPORTANT: When selecting this option, be aware that if one user's access rights to an item are removed, it does not remove the access rights of the user with whom the item was re-shared.

For example, suppose User A shares an item with User B and grants re-share rights. User B then shares the item with User C. If User A revokes User B's access rights to the item, User C continues to have access to the shared item.

---

5 Click **OK**.

Enabling Sharing for Top-Level Team Workspaces

1 Log in to the Vibe site as the Vibe administrator.

  1a Launch a web browser.

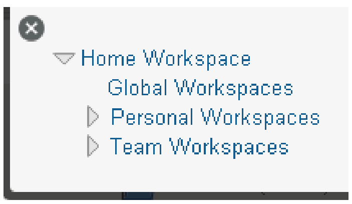
  1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://Vibe_hostname:8080
https://Vibe_hostname:8443
```

  Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

  Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **Browse** icon in the Action toolbar, then expand **Home Workspace** in the Workspace tree.



The Home Workspace directory is the highest-level folder in the workspace tree, and might be named something specific to your organization.

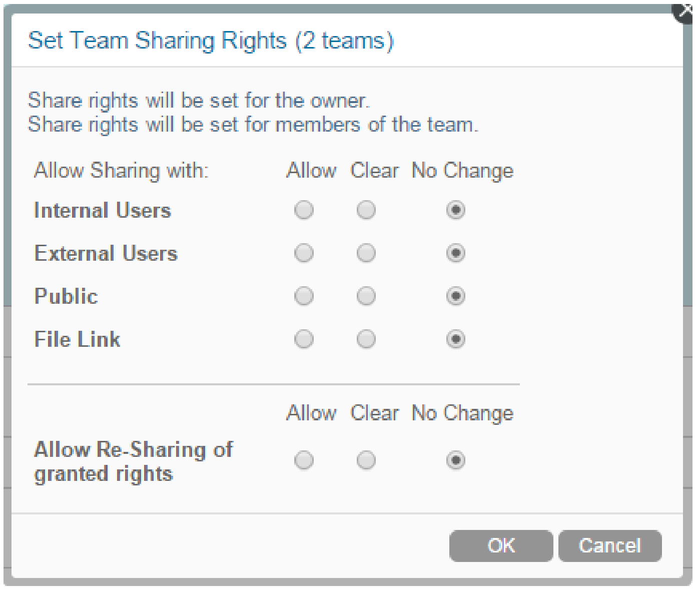
3 Click **Team Workspaces**.

The Teams page is displayed.

4 Select the top-level teams that you want to grant share rights by selecting the checkbox next to the team name.

5 Click **Team Share Rights**.

The Set Team Sharing Rights dialog box is displayed.



Select **Allow** next to any share rights that you want to grant to all the selected workspaces, and select **Clear** next to any share rights you do not want to grant. Select **No Change** to maintain any share rights that might already exist on any workspaces (this option is displayed only when multiple teams are selected).

The following share rights are available:

Internal Users: lets users share items with internal users.

External Users: lets users share items with users external to the organization.

Users external to the organization receive an email notification with a link to the shared item, and they can then log in to the Vibe site. For more information, see“Sharing with People Outside Your Organization” in the *Micro Focus Vibe 4.0.5 User Guide*.

Public: lets users make items publicly available. This means that anyone with the correct URL to the shared item can access the shared item without logging in to the Vibe site.

In addition to selecting this option, you also need to enable Guest access to the Vibe site if you want to allow users to share items with the public. For information about how to enable Guest access to the Vibe site, see “Setting Up Guest Access for the Vibe Site” on page 105.

File Link: lets users share a link to a file in Vibe. Any user with the link can then access the file. However, the file is not displayed in the Public area, so users must have direct access to the link in order to access the file.

For more information about File Links, see “Distributing a Link to a File” in the *Micro Focus Vibe 4.0.5 User Guide*.

Allow Re-Sharing of granted rights: When users share a file or folder, they can give the users they are sharing with the ability to re-share the file or folder. The user receiving the share can share the file only if that user has been given administrative rights to share the file or folder.

IMPORTANT: When selecting this option, be aware that if one user's access rights to an item are removed, it does not remove the access rights of the user with whom the item was re-shared.

For example, suppose User A shares an item with User B and grants re-share rights. User B then shares the item with User C. If User A revokes User B's access rights to the item, User C continues to have access to the shared item.

6 Click **OK**.

Managing Shares

As the Vibe administrator, you are in control of all shared items in the Vibe system. You can view who has shared items, what items have been shared, what access rights have been granted via the share, and so forth. Furthermore, you can modify share rights for existing shares or delete existing shares.

You can manage shares through a management interface, where you can filter by user, file, folder, or all shares. Or, you can manage shares for individual folders and files as you encounter them in the Vibe site.

Users are not notified about changes that you make to shared items.

- "Managing Shares for the Vibe Site" on page 135
- "Managing Individual Shares" on page 136

Managing Shares for the Vibe Site

You can manage all active shares in the Vibe system with the Manage Shares dialog box in the administration console. You can filter shares by individual users, files, or folders. Or, you can view all active shares in the Vibe system.

1 Log in to the Vibe site as the Vibe administrator.

   1a Launch a web browser.

   1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

   ```
   http://Vibe_hostname:8080
   https://Vibe_hostname:8443
   ```

   Replace *Vibe_hostname* with the hostname or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

   Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Shares**.

   The Manage Shares dialog box is displayed.

4 In the **Find share items by** drop-down list, select one of the following options by which you want to manage shares:

   User: Begin typing the name of a user in the **User** field, then select the user name when it appears in the drop-down list. All active shares from that user are displayed in the table.

   File: Begin typing the name of a file in the **File** field, then select the file name when it appears in the drop-down list. All active shares associated with that file are displayed in the table.

   Folder: Begin typing the name of a folder in the **Folder** field, then select the folder name when it appears in the drop-down list. Or click the **Browse** icon next to the **Folder** field and browse to the folder. All active shares associated with that folder are displayed in the table.

   Find all shares: Displays all active shares in the Vibe system.

5 (Optional) Change the access control settings, expiration date, and note for a shared item.

For more information about these options, see "Sharing Entries, Folders, and Workspaces" in the *Micro Focus Vibe 4.0.5 User Guide*.

6 (Optional) Remove a user or group's access to a shared item by selecting the share that you want to remove, then clicking **Delete**.

7 Click **OK**.

Managing Individual Shares

As the administrator, you can manage shares for individual entries, folders, or workspaces as you encounter them in the site.

1 In a workspace or folder, click the **Configure** icon next to the workspace or folder title, then click **Manage Shares**.

or

In a folder or an area such as your Shared with Me area, click the drop-down arrow next to the entry, then click **Manage Shares**

The Manage Shares dialog box is displayed.

2 (Optional) Change the access control settings, expiration date, and note for a shared item.

For more information about these options, see "Sharing Entries, Folders, and Workspaces" in the *Micro Focus Vibe 4.0.5 User Guide*.

3 (Optional) Remove a user or group's access to a shared item by selecting the share that you want to remove, then clicking **Delete**.

4 Click **OK**.

8 Allowing Access to the Vibe Site through NetIQ Access Manager

To allow access to the Vibe site through NetIQ Access Manager, you need to make configuration changes in NetIQ Access Manager to configure a protected resource for a Micro Focus Vibe server as described in "Configuring a Protected Resource for a Micro Focus Vibe Server" on page 137.

IMPORTANT: When NetIQ Access Manager (or another single sign-on tool) is used in conjunction with your Vibe system, external users and the Guest user cannot access your Vibe site.

For more information about external users in Vibe, see "Understanding External Users" on page 125.

Configuring a Protected Resource for a Micro Focus Vibe Server

The following sections explain how to configure the Access Gateway with a domain-base multi-homing service. The instructions assume that you have a functioning Micro Focus Vibe server on Linux and a functioning Access Manager system (3.1 SP1 IR1 or higher) with a reverse proxy configured for SSL communication between the browsers and the Access Gateway.

The Vibe server needs to be configured to trust the Access Gateway to allow single sign-on with Identity Injection and to provide simultaneous logout. You also need to create an Access Gateway proxy service and configure it.

For information on other possible Access Gateway configurations, see "Teaming 2.0: Integrating with Linux Access Gateway" (http://www.novell.com/communities/node/9580/teaming-20-integration-linux-access-gateway).

Configuring the Micro Focus Vibe Server to Trust the Access Gateway

To use Micro Focus Vibe as a protected resource of an Access Gateway and to use Identity Injection for single sign-on, the Vibe server needs a trusted relationship with the Access Gateway. With a trusted relationship, the Vibe server can process the authorization header credentials. The Vibe server accepts only a simple user name (such as user1) and password in the authorization header.

This section explains how to set up the trusted relationship and how to enable simultaneous logout, so that when the user logs out of Vibe, the user is also logged out of the Access Gateway.

To configure the trusted relationship:

1. Log in to the Vibe server.
2. Stop the Vibe server with the following command:

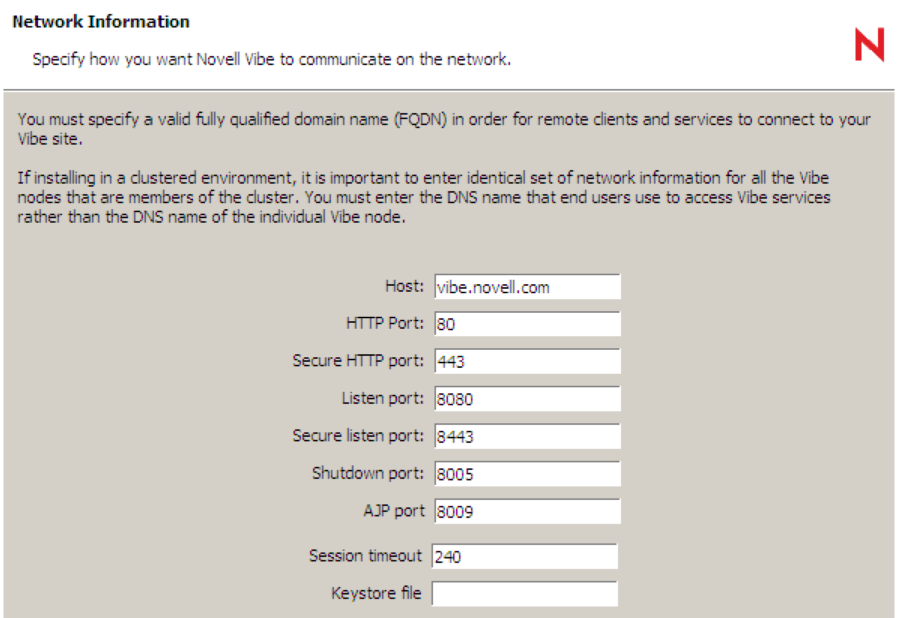
```
/etc/init.d/teaming stop
```

3 Run the `installer-teaming.linux` script.

4 Accept the license agreement, then select **Reconfigure settings**, then click **Next**.

5 Confirm that your Vibe server is shut down, then select **Advanced installation**, then click **Next**.

6 Continue through the installation program until you reach the Network Information page. Ensure that you have a valid Host name specified. You will need this later in the installation.



7 Continue through the installation program until you reach the Reverse Proxy Configuration page. Specify the following configuration options:

Enable Access Gateway: Select this option to enable the reverse proxy access gateway.

Access Gateway address(es): Specify the IP address of the Access Gateway that is used for the connection to the Vibe server.

If the Access Gateway is part of a cluster, add the IP address for each cluster member. Wildcards such as 164.99.*.* are allowed.

When you specify IP addresses in this option, Vibe logins are allowed only from the specified addresses. Also, if Authorization header credentials are not present or are incorrect, the user is prompted for login using Basic Authentication.

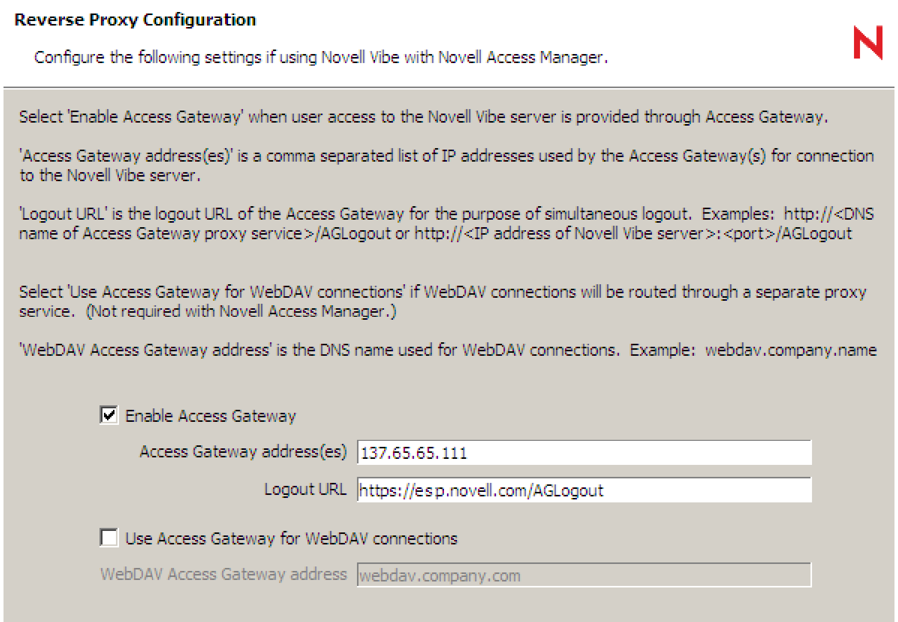
Logout URL: Specify the URL of the published DNS name of the reverse proxy that you have specified for the ESP, plus `/AGLogout`.

You can find the domain used for the ESP by editing the LAG/MAG cluster configuration, then clicking **Reverse Proxy / Authentication**.

For example, if the published DNS name of the proxy service that you have specified for the ESP is esp.*yoursite*.com, specify the following URL:

```
https://esp.yoursite.com/AGLogout
```

Use Access Gateway for WebDAV connections: Leave this option unselected.



8 Continue through the installation program to complete the reconfiguration process.

9 Start the Vibe server with the following command:

```
/etc/init.d/teaming start
```

10 Continue with "Configuring a Reverse-Proxy Single Sign-On Service for Micro Focus Vibe" on page 139.

Configuring a Reverse-Proxy Single Sign-On Service for Micro Focus Vibe

To configure a reverse-proxy single sign-on service for Vibe, complete the following tasks:

- "Creating a New Reverse Proxy" on page 139
- "Configuring the Domain-Based Proxy Service" on page 139
- "Creating Policies" on page 140
- "Configuring Protected Resources" on page 141
- "Disabling a Rewriter Profile" on page 143

Creating a New Reverse Proxy

Before you can configure the domain-based proxy service, you need to create a new reverse proxy. For information on how to create a reverse-proxy, see "Managing Reverse Proxies and Authentication" in the *NetIQ Access Manager Administration Guide.*

Configuring the Domain-Based Proxy Service

1 In the Administration Console, click **Devices** > **Access Gateways** > **Edit**, then click the name of the reverse proxy that you created in "Creating a New Reverse Proxy" on page 139.

2 Click the reverse proxy link that you have previously created. In the **Reverse Proxy List**, click **New**, then fill in the following fields:

Proxy Service Name: Specify a display name for the proxy service that the Administration Console uses for its interfaces.

Published DNS Name: Specify the DNS name you want the public to use to access your site. This DNS name must resolve to the IP address you set up as the listening address. For example, `vibe.doc.provo.Novell.com`.

Web Server IP Address: Specify the IP address of the Vibe server.

Host Header: Select the **Forward received host name**.

Web Server Host Name: Because of your selection in the **Host Header** field, this option is dimmed.

3 Click **OK**.

4 Click the newly added proxy service, then select the **Web Servers** tab.

5 Make sure that **Enable Session Stickiness** is selected.

Otherwise, users will get `Invalid RPC token` errors when two or more Vibe servers are online.

6 Change the **Connect Port** to 8080.

If the Linux Vibe server has port forwarding enabled, you do not need to change from the default port 80.

IMPORTANT: Vibe uses the requesting hostname and port to generate the URL in the `DO.JNLP` file. In order for this to work with a reverse proxy, such as Access Manager, the proxy needs to preserve both the hostname and the port when it forwards the HTTP request to the Vibe server.

We strongly recommend that you preserve the HTTP and HTTPS ports.

---

7 Click **TCP Connect Options**.

8 Click **OK**.

9 Continue with "Configuring Protected Resources" on page 141.

Creating Policies

There are two policies that you need to create, LDAP Identity Injection, and X-Forwarded-Proto:

- "Creating the LDAP Identity Injection Policy" on page 140
- "Creating the X-Forwarded-Proto HTTP Header Policy" on page 141

Creating the LDAP Identity Injection Policy

1 In the Administration Console, click **Policies > Policies**.

2 Select the policy container, then click **New**.

3 Specify `ldap_auth` as the name for the policy, select **Access Gateway: Identity Injection** for the type, then click **OK**.

4 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple policies to be used by multiple resources.

5 In the **Actions** section, click **New**, then select **Inject into Authentication Header**.

6 Fill in the following fields:

User Name: Select **Credential Profile** > **LDAP User Name**.

Password: Select **Credential Profile** > **LDAP Password**.

7 Leave the default value for the Multi-Value Separator, which is comma.

8 Click **OK**.

9 To save the policy, click **OK**, then click **Apply Changes**.

For more information on creating such a policy, see "Configuring an Authentication Header Policy" in the *NetIQ Access Manager Appliance 4.2 Administration Guide.*

Creating the X-Forwarded-Proto HTTP Header Policy

When communicating over HTTPS from the browser to Access Manager, and over HTTP from Access Manager to Vibe, the X-Forwarded-Proto is a best practice. Vibe 3.3 was enhanced to take advantage of the HTTP header X-Forwarded-Proto.

1 In the Administration Console, click **Policies > Policies**.

2 Select the policy container, then click **New**.

3 Specify `x-forwarded` as the name for the policy, select **Access Gateway: Identity Injection** for the type, then click **OK**.

4 (Optional) Specify a description for the injection policy. This is useful if you plan to create multiple policies to be used by multiple resources.

5 In the **Actions** section, click **New**, then select **Inject into Custom Header**.

6 Fill in the following fields:

Custom Header Name: Specify `X-Forwarded-Proto` as the name.

Value: Select **String Constant** in the drop-down, then specify `https`.

7 Leave the other settings at the defaults.

8 Click **OK**.

9 To save the policy, click **OK**, then click **Apply Changes**.

For more information on creating such a policy, see "Configuring an Identity Injection Policy" in the *NetIQ Access Manager Appliance 4.2 Administration Guide.*

Configuring Protected Resources

You need to create three protected resources, one for HTML content, one for WebDAV content, and a public:

1 Create a protected resource for HTML content:

1a In the **Protected Resource List**, click **New**, specify `Basic auth with redirection` for the name, then click **OK**.

1b (Optional) Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.

1c Specify a value for **Authentication Procedure.** For example, select the **Secure Name/ Password - Form** contract.

1d Click the Edit icon.

1e In the dialog box that is displayed, fill in the following fields.

Contract: Select the **Secure Name/Password - Form** contract, which is same contract that you selected for the HTML content protected resource.

Non-Redirected Login: Select this option.

Realm: Specify a name that you want to use for the Vibe server. This name does not correspond to a Vibe configuration option. It appears when the user is prompted for credentials.

Redirect to Identity Server When No Authentication Header is Provided: Select this option.

1f Click **OK** twice.

2 Create a public protected resource for web Services:

2a In the **Protected Resource List**, click **New**, specify `public` for the name, then click **OK**.

2b (Optional) Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.

2c For the **Authentication Procedure**, select **None**.

2d Click **OK**.

2e In the **URL Path List**, remove the `/*` path and add the following paths:

```
/ssf/atom/*
/ssf/ical/*
/ssf/ws/*
/ssf/rss/* - enables non-redirected login for RSS reader connections.
/ssf/s/readFile/share/*
/ssr/*
/rest/*
/ssf/applets/fileopen/* - enables Edit this file functionality
/downloads/* - enables Client Downloads page
/dave/*
```

The `/ssf/rss/*` path enables non-redirected login for RSS reader connections. Vibe provides authentication for all of the paths listed above.

2f Click **OK**.

3 Create a protected resource for WebDAV content:

3a In the **Protected Resource List**, click **New**, specify `Basic auth without redirection` for the name, then click **OK**.

3b (Optional) Specify a description for the protected resource. You can use it to briefly describe the purpose for protecting this resource.

3c Specify a value for **Authentication Procedure.** For example, select the **Secure Name/ Password - Basic** contract.

3d Click the Edit icon.

3e In the dialog box that is displayed, fill in the following fields.

Contract: Select the **Secure Name/Password - Form** contract, which is same contract that you selected for the HTML content protected resource.

Non-Redirected Login: Select this option.

Realm: Specify a name that you want to use for the Vibe server. This name does not correspond to a Vibe configuration option. It appears when the user is prompted for credentials.

Redirect to Identity Server When No Authentication Header is Provided: Do not select this option.

3f In the **URL Path List**, remove the `/*` path and add the following path:

```
/dav/*
/davs/*
```

3g Click **OK** twice.

4 Assign the X-Forward-Proto Header policy to all three protected resources that you created:

   4a Click **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service] > Protected Resources**.

   4b For each Vibe protected resource, click the **Identity Injection** link, select the **x-forward** policy that you created, click **Enable**, then click **OK**.

   4c Click **OK.**

5 Assign the Identity Injection policy to two of the protected resources that you created, specifically **Basic auth with redirection** and **Basic auth without redirection**. Do not assign this policy to the **public** protected resource.

   5a Click **Access Gateways** > **Edit** > **[Name of Reverse Proxy]** > **[Name of Proxy Service] > Protected Resources**.

   5b For each Vibe protected resource, click the **Identity Injection** link, select the **ldap_auth** policy that you created, click **Enable**, then click **OK**.

   5c Click **OK.**

6 To save the configuration changes, click **Devices** > **Access Gateways**, then click **Update**.

7 In the **Protected Resource List**, ensure that the protected resources you created are enabled.

8 To apply your changes, click **Devices** > **Access Gateways**, then click **Update**.

9 Continue with "Disabling a Rewriter Profile" on page 143.

Disabling a Rewriter Profile

In the Proxy Service List, ensure that the HTML Rewriter is disabled.

Forwarding Cache Control Headers

The recommended configuration for Micro Focus Vibe is to configure Access Manager to forward cache control headers to the browser. For information on how to forward cache control headers to the browser, see "Controlling Browser Caching" in the *NetIQ Access Manager Appliance 4.2 Administration Guide.*

9 Configuring Vibe Desktop and the Microsoft Office Add-In

Micro Focus Vibe Desktop and the Vibe Add-in for Micro Focus Vibe enable you to work with Vibe files on your personal computer. Vibe Desktop lets you manage Vibe files from the file system on your computer, and the Vibe Add-in lets you edit Vibe documents directly from Microsoft Office. For more information about Vibe Desktop, see the Micro Focus Vibe Desktop for Windows Quick Start (http://www.novell.com/documentation/vibe33/vibe33_qs_desktop/data/vibe33_qs_desktop.html) and the Micro Focus Vibe Desktop for Mac Quick Start (http://www.novell.com/documentation/vibe33/vibe33_qs_desktopmac/data/vibe33_qs_desktop.html). For more information about the Vibe Add-in, see the Micro Focus Vibe Add-In Quick Start (http://www.novell.com/documentation/vibe33/vibe33_qs_office/data/vibe33_qs_office.html).

As a Vibe administrator, you must enable file synchronization for Vibe Desktop in order for users to take advantage of this functionality. There are also optional administrative procedures that you might want to perform when configuring Vibe Desktop.

Configuring Vibe Desktop to Synchronize Files between Vibe and Users' Computers

You can allow users to synchronize their Micro Focus Vibe files with their personal computers. Users can modify files without accessing the Vibe site directly; additions and modifications are synchronized between Vibe and users' personal computers. By default, this functionality is not enabled.

Configuring the Vibe Desktop Application for All Users

To enable this functionality for the Vibe site:

1 In Vibe, click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

2 Under **System**, click **Desktop Application**.

3 In the Configure Desktop Application dialog box, specify the following information:

Access Vibe: lets users access the Vibe site through the Vibe desktop application.

NOTE: Depending on the amount of anticipated load that the Vibe desktop application will put on your Vibe system, you might want to make the application available to users in a staged process.

Allowing access to the Vibe site through the Vibe desktop application can be changed on a per-user basis, as described in "Configuring Vibe Desktop for Individual Users and Groups" on page 147.

Cache the user's password: lets users enable the **Remember password** option on the **Account Information** page in the Micro Focus Vibe Console.

This option can be changed on a per-user basis, as described in "Configuring Vibe Desktop for Individual Users and Groups" on page 147.

Be deployed: Select this option to make the Vibe desktop application available to users. If this option is selected, users can download the Vibe desktop application as described in "Downloading and Installing Vibe Desktop (https://www.novell.com/documentation/vibe4/vibe4_qs_desktop/data/vibe4_qs_desktop.html#bwrk0ll)" in the *Micro Focus Vibe Desktop Quick Start for Windows* (https://www.novell.com/documentation/vibe4/vibe4_qs_desktop/data/vibe4_qs_desktop.html) or the *Micro Focus Vibe Desktop Quick Start for Mac* (https://www.novell.com/documentation/vibe4/vibe4_qs_desktopmac/data/vibe4_qs_desktopmac.html). If this option is not selected, the link to download the Vibe desktop application is not visible to users.

NOTE: You might want to leave the **Be deployed** option deselected if you plan to deploy Vibe Desktop to user workstations by using client management software such as Novell ZENworks. The `.msi` file is available to you if you are planning to deploy Vibe Desktop by using ZENworks.

For more information about how to deploy Vibe by using the `.msi` file, see "Managing the Vibe Desktop Application" on page 153.

Auto-update URL: Specify the HTTP server where Vibe Desktop can check for Vibe Desktop updates.

You can configure your Vibe server to be the HTTP server that provides auto-update information, or you can configure a separate web server to provide the auto-update information.

If you configure the Vibe server for this purpose, the auto-update URL is `https://`*`vibe_hostname`*`:8443/downloads`.

For information about how to set up a separate web server to deploy the application, see "Configuring a Separate Web Server to Deploy the Vibe Desktop Application" on page 149. Select this option if your Vibe system is clustered or fronted by an L4 or L10 switch.

If this option is selected, the available field must be populated with the URL of the web server that you configure for deploying the desktop application.

Synchronization every *xx* Minutes: Specify the interval (in minutes) for how often the Vibe Desktop checks Vibe for changes to files. The default is every 15 minutes. This means that 15 minutes after one synchronization ends, another begins. This lets you control the amount of load Vibe Desktop puts on the Vibe server.

Changes made in the desktop application are automatically synchronized to the server regardless of this setting.

Maximum file size that can be synchronized: Specify the maximum file size (in MB) that can be synchronized between the Vibe desktop application and the Vibe server.

4 Click **OK**.

Users need to download, install, and configure Vibe Desktop on their personal computers. For more information, see the *Micro Focus Vibe Desktop Quick Start for Windows* (https://www.novell.com/documentation/vibe4/vibe4_qs_desktop/data/vibe4_qs_desktop.html) or the *Micro Focus Vibe Desktop Quick Start for Mac* (https://www.novell.com/documentation/vibe4/vibe4_qs_desktopmac/data/vibe4_qs_desktopmac.html).

Configuring Vibe Desktop for Individual Users and Groups

Individual user and group settings override global settings. This section describes how to customize the desktop application experience for individual users and groups on your Vibe system.

To make the desktop application available to only a subset of users in your system, configure the application for all users, as described in "Configuring the Vibe Desktop Application for All Users" on page 146, then restrict access to the users and groups who should not have access to the application, as described in this section.

1 In Vibe, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.

2 Under **Management**, click **Users**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the users or groups for whom you want to configure Vibe Desktop, then click **More** > **Desktop Application Settings**.

The **Configure Desktop Application** page is displayed.

4 To change the desktop application settings for the selected users to be different from the global settings, select **Use user settings to allow the desktop application to**, then choose from the following options:

Access Vibe: lets users access the Vibe site through the Vibe desktop application.

Cache the user's password: lets users enable the **Remember password** option on the **Account Information** page in the Micro Focus Vibe Console.

5 Click **OK**.

If you have set individual and group settings for Vibe Desktop, you can change those settings back to the global settings for the individual users and groups.

1 In Vibe, click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.

2 Under **Management**, click **User Accounts**.

The Manage Users page is displayed.

3 Select the check boxes next to the names of the users or groups for whom you want to configure Vibe Desktop, then click **More** > **Desktop Application Settings**.

The **Configure Desktop Application** page is displayed.

4 To change the desktop application settings back to the global settings for the selected users, select **Use global settings**.

5 Click **OK**.

Configuring the Vibe Server as an HTTP Server to Provide Auto-Update Information for Vibe Desktop

You can configure your Vibe server as an HTTP server to provide auto-update information for Vibe Desktop. This section describes how to configure Vibe as an HTTP server when Vibe is running on a single server. If you want to configure Vibe as an HTTP server when Vibe is running in a clustered environment, you must configure each Vibe node. If Vibe is running in a clustered environment, it is probably more convenient to use an external web server or the reverse-proxy server as the HTTP server.

To configure your single-server Vibe server as an HTTP server to provide auto-update information for Vibe Desktop:

1 Download the `MicroFocusVibeDesktopAutoUpdate.tgz` file from the Vibe downloads page on the Novell Downloads site (https://download.novell.com) to the `/apache-tomcat/webapps/downloads` directory. (If the `downloads` directory does not already exist, you need to create it.)

2 With the `MicroFocusVibeAutoUpdate.tgz` file in the `/apache-tomcat/webapps/downloads` directory, extract it:

```
tar -xvf MicroFocusVibeAutoUpdate.tgz
```

Linux: 32-bit	`/opt/novell/teaming/apache-tomcat/webapps/downloads /novellvibedesktop/windows/x86`
Linux: 64-bit	`/opt/novell/teaming/apache-tomcat/webapps/downloads /novellvibedesktop/windows/x64`
Windows: 32-bit	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\downloads \Novellvibedesktop\windows\x86`
Windows: 64-bit	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\downloads \Novellvibedesktop\windows\x64`

3 Change the ownership:

```
chown -R vibe:vibe downloads
```

4 From a browser, ensure that you can access the following file:

`http://`*`vibe_hostname:8443`*`/downloads/novellvibedesktop/`*`windows/x64`*`/version.json`

5 Configure the auto-update URL for Vibe Desktop in the Vibe Administration Console, as described in "Configuring Vibe Desktop to Synchronize Files between Vibe and Users' Computers" on page 145.

Configuring a Separate Web Server to Deploy the Vibe Desktop Application

By default, the Vibe server is configured to deploy the Vibe desktop application and to provide the auto-update information. As a best practice to minimize load on the Vibe server, we recommend that you set up a separate web server and configure it to deploy the desktop application and provide the auto-update information.

1 Set up a web server as a host for the Vibe desktop application auto-update information.

   This web server must be set up so that it does not require authentication.

   NOTE: If you are using secure HTTP, the web server must have a certificate signed by a trusted certificate authority.

   ---

2 Download and extract the `MicroFocusVibeDesktopAutoUpdate.tgz` file into a location on the web server so the files are available to download via the http server. (You can download the `MicroFocusVibeDesktopAutoUpdate.tgz` file from the Vibe downloads page on the Novell Downloads site (https://download.novell.com).)

   This compressed file contains all of the files required for installing the Vibe desktop application.

3 From a browser, ensure that you can access the following file:

   `http://`*`web_server_address/path_to_download_directory/`*`novellvibedesktop/`*`windows/x64/`*`version.json`

   For example:

   `http://`*`web_server_address/`*`downloads/novellvibedesktop/`*`windows/x64/`*`version.json`

4 Configure the Vibe desktop application as described in "Configuring the Vibe Desktop Application for All Users" on page 146.

   In the **Auto-update URL** field:

   `http://`*`web_server_address/path_to_download_directory/`*

5 Click **OK**.

Configuring the Maximum File Size Limit for Vibe Desktop

By default, Vibe Desktop does not upload or download any file that exceeds 1 GB.

If a file size limit has already been set for uploading files to the Vibe site (as described in "Setting a File Upload Size Limit for Individual Users and Groups" on page 256), whichever limit is more restrictive is honored by Vibe Desktop.

For example, if you set a file size limit in Vibe of 500 MB and the maximum file size limit for Vibe Desktop is set at 2 GB, users cannot upload files bigger than 500 MB to the Vibe site either by accessing the Vibe site directly or by uploading files through Vibe Desktop.

- "Configuring the Maximum File Size Limit for Uploading Files" on page 150
- "Configuring the Maximum File Size Limit for Uploading and Downloading Files" on page 150

Configuring the Maximum File Size Limit for Uploading Files

To restrict the size of files that are uploaded to the Vibe site outside of Vibe Desktop (such as by accessing Vibe through a browser, through the Vibe Add-in, or through WebDAV), as well as through Vibe Desktop (while keeping the default 1 GB file size limit for files that are downloaded through Vibe Desktop), use the Vibe administration console to modify this setting, as described in "Managing the File Upload Size Limit" on page 255.

Configuring the Maximum File Size Limit for Uploading and Downloading Files

You can increase or decrease the file size limit for files that are both uploaded and downloaded to and from the Vibe site through Vibe Desktop.

Modifying the property as described in this section does not affect a user's ability to upload documents to Vibe outside of Vibe Desktop (such as by accessing Vibe through a browser, through the Vibe Add-in, or through WebDAV).

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
fsa.max.file.size=
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `fsa.max.file.size=` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change the value of this property to the file size (in bytes) that represents the maximum file size that you want Vibe Desktop to upload to the Vibe site and download from the Vibe site. For example, if you want Vibe Desktop to be able to upload and download only 500 MB files, the line would read `fsa.max.file.size=536870912`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe.

Prepopulating Vibe Desktop with Your Vibe URL

If you use application management software, such as Novell ZENworks, to deploy Vibe Desktop to user workstations, you can also prepopulate Vibe Desktop with your organization's Vibe server URL. This saves users from specifying the Vibe server URL when they are configuring Vibe Desktop on their individual workstations.

To configure Vibe Desktop in this way, you must accomplish the tasks in either of the following sections as part of the deployment process of Vibe Desktop to user workstations with your application management software:

- "Setting the VIBEURL Windows Installer Property" on page 151
- "Writing the Vibe Server URL to the Registry" on page 151

Setting the VIBEURL Windows Installer Property

You can prepopulate Vibe Desktop with the URL of your organization's Vibe server by specifying the VIBEURL Windows Installer property when Vibe Desktop is installed.

The exact steps for specifying the Windows Installer property differ depending on the application management software you are using to deploy Vibe Desktop to user workstations; however, the following command illustrates how to perform a silent installation of Vibe Desktop and prepopulate Vibe Desktop with the URL of your organization's Vibe server:

```
msiexec /i NovellVibeDesktop.msi /quiet VIBEURL=https://vibe.mycompany.com
```

Writing the Vibe Server URL to the Registry

You can prepopulate Vibe Desktop with the URL of your organization's Vibe server by writing the Vibe server URL directly to the registry after Vibe Desktop is installed.

The exact steps for writing the Vibe server URL to the registry differ depending on the application management software you are using to deploy Vibe Desktop to user workstations; however, in `\\HKEY_LOCAL_MACHINE\Software\Novell\Vibe Desktop` you must set the `Default Server URL` string value to your organization's Vibe server URL.

Distributing Vibe Desktop and Vibe Add-In Synchronization Traffic

Vibe Desktop and Vibe Add-in can cause a large amount of traffic on the Vibe servers. To prevent the Vibe Desktop and the Vibe Add-in synchronization process or the Vibe site from becoming slow, you can distribute Vibe Desktop and Vibe Add-in traffic among dedicated Vibe servers with your load balancer or reverse proxy server.

For example, if you have a Vibe installation with five servers, you could dedicate one server to handle Vibe Desktop traffic, one server to handle Vibe Add-in traffic, and use the remaining three servers to serve the main Vibe web application. This configuration prevents an unusual spike in Vibe Desktop traffic or Vibe Add-in traffic from impacting the Vibe site.

You can distribute Vibe Desktop traffic and Vibe Add-in traffic differently, depending on whether you want traffic from all applications (not just Vibe Desktop and Vibe Add-in) that are accessing Vibe to be handled in the same way, or whether you want Vibe Desktop traffic and Vibe Add-in traffic to be handled independently from each other and from other applications that are accessing Vibe.

- "Distributing Vibe Desktop Traffic Separately from Other Applications" on page 152
- "Distributing Vibe Add-In Traffic Separately from Other Applications" on page 152
- "Distributing Vibe Desktop and Vibe Add-In Traffic in Conjunction with Other Applications" on page 153
- "Load Balancer and Reverse Proxy Server Configuration" on page 153

Distributing Vibe Desktop Traffic Separately from Other Applications

You can configure your load balancer or reverse proxy server to distribute Vibe Desktop synchronization traffic among multiple Vibe servers. Vibe Desktop traffic is independent of traffic from other applications that are accessing Vibe.

NOTE: Your load balancer or reverse proxy server must be able to make routing decisions based on the request headers.

---

1 Configure your load balancer or reverse proxy server to use the user agent request header. For Vibe Desktop, the request header begins with `NovellVibeDesktop`. For example: `User-Agent: NovellVibeDesktop/1.0 (Windows NT 6.1; Python/2.7.0; en_US) suds/0.4`.

  For specific information on how to configure the load balancer or reverse proxy server, see "Load Balancer and Reverse Proxy Server Configuration" on page 153.

Distributing Vibe Add-In Traffic Separately from Other Applications

You can configure your load balancer or reverse proxy server to distribute Vibe Add-in synchronization traffic among multiple Vibe servers. Vibe Add-in traffic is independent of traffic from other applications that are accessing Vibe.

NOTE: Your load balancer or reverse proxy server must be able to make routing decisions based on the request headers.

---

1 Configure your load balancer or reverse proxy server to use the user agent request header. For Vibe Add-in, the request header begins with `NovellVibeDesktop`. For example: `User-Agent: NovellVibeMsoAddin/1.0 (Windows NT 6.1.7601.65536; .NET Framework 4.0.30319.239; en_US)`

  For specific information on how to configure the load balancer or reverse proxy server, see "Load Balancer and Reverse Proxy Server Configuration" on page 153.

Distributing Vibe Desktop and Vibe Add-In Traffic in Conjunction with Other Applications

You can configure your load balancer or reverse proxy server to distribute Vibe Desktop and Vibe Add-in synchronization traffic (along with traffic coming from all other applications that use the Vibe web service interface) among multiple Vibe servers.

Examples of other applications that use the Vibe web service interface are:

- GroupWise client SOAP requests
- All other SOAP requests from third-party applications

NOTE: Your load balancer or reverse proxy server must be able to make routing decisions based on the HTTP URL path.

---

1 Configure your load balancer or reverse proxy server to send all Vibe Desktop HTTP requests (designated by the following paths `/ssf/ws/TeamingServiceV1` and `/rest/*`) to one pool of Vibe servers.

   All other requests are sent to another pool of Vibe servers.

   For specific information on how to configure the load balancer or reverse proxy server, see "Load Balancer and Reverse Proxy Server Configuration" on page 153.

Load Balancer and Reverse Proxy Server Configuration

For information on how to configure a load balancer for your Vibe site, see any of the following sections, depending on the type of load balancer you want to use:

- "Configuring Apache as a Load Balancer" in "Running Vibe on Multiple Servers" in the *Micro Focus Vibe 4.0.4 Installation Guide*.
- "Configuring Linux Virtual Server as a Load Balancer" in "Running Vibe on Multiple Servers" in the *Micro Focus Vibe 4.0.4 Installation Guide*.
- "Configuring IIS to Load Balance in a Clustered Environment" in "Configuring Single Sign-On with Internet Information Services for Windows" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

For information on how to configure a reverse-proxy server for your Vibe site, see "Configuring Single Sign-On with Novell Access Manager" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Managing the Vibe Desktop Application

You can manage the Vibe desktop application on users' workstations with client management software such as Novell ZENworks.

When following the instructions in this section, you must use the `.msi` file, which is bundled in the `NovellVibeAutoUpdate.tgz` file, and is available at the Novell Downloads site (https://download.novell.com/).

If you use the `.msi` file to distribute the Vibe desktop application to user workstations, you need to install the following items to each user workstation, independent of the Vibe software:

- Microsoft .NET Framework 4.5 (Applies to 64-bit Windows and Mac workstations.)

You can download Microsoft .NET Framework 4.5 from the Microsoft .NET Downloads page (http://www.microsoft.com/net/downloads).

- Microsoft Visual C++ 2013 Redistributable Package (Applies to all workstations)

  You can download the redistributable package from the Microsoft Download Center (https://www.microsoft.com/en-us/download/details.aspx?id=40784).

NOTE: The ability to manage the Vibe desktop application is available only with Vibe desktop 1.0.2 and later.

You can customize the installation and control whether Windows Explorer is restarted.

- "Customizing the Installation for the Vibe Desktop Application" on page 154
- "Controlling Windows Explorer Restart" on page 157

Customizing the Installation for the Vibe Desktop Application

You can customize the installation process of the Vibe desktop application for your organization in the following ways:

- Configure default values for each installation option of the Vibe desktop application. (Users can change these default values when configuring the Vibe desktop application.)
- Auto-configure all values for each installation option of the Vibe desktop application. (Users specify only their user name and password when configuring the Vibe desktop application; users cannot change the default values during initial configuration.)
- Disallow users from modifying configuration options in the Vibe desktop application. (Users cannot change the default values during initial configuration, and cannot modify the values via the Vibe console after initial configuration.)

  NOTE: This does not prevent users from manually modifying configuration settings in the registry or file system.

The following sections describe how to make these customizations.

- "Configuring Default Values" on page 154
- "Enabling Auto-Configuration" on page 155
- "Disallowing User Configuration" on page 156
- "Modifying the Vibe Desktop Configuration" on page 156

Configuring Default Values

You can configure the default values for each installation option of the Vibe desktop application. Users can change these default values when configuring the Vibe desktop application.

You accomplish this on Windows by creating registry values, and on Mac by adding properties to the application's `Info.plist` file.

1 **Windows:** Access the following location where you will create registry values:

```
\\HKLM\Software\Novell\Vibe
```

Mac: Access the `Info.plist` file where you will add properties. This file is usually in the following location:

`/Applications/Novell Vibe/Contents/Info.plist`

2 Create Windows registry values and add properties to the `Info.plist` file for the values for which you want to configure defaults.

The following table displays the available options for configuring default values.

Table 9-1 *Default Value Configuration Options*

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Default Server URL	REG_SZ	VibeDefaultServerURL	string	No	https://
Default Username	REG_SZ	VibeDefaultUsername	string	Yes	%USERNAME% or $USER
Default Account Name	REG_SZ	VibeDefaultAccountName	string	No	Hostname in server URL
Default Remember Password	REG_SZ (“true” or “false”)	VibeDefaultRememberPassword	<true/> or <false/>	No	false
Default Sync Dir	REG_SZ	VibeDefaultSyncDir	string	Yes	%USERNAME%\Vibe or $USER\Vibe
Default Start On Login	REG_SZ (“true” or “false”)	VibeDefaultStartOnLogin	<true/> or <false/>	No	true
Default Folder List	REG_MULTI_SZ	VibeDefaultFolderList	Array of strings	No	My Files Shared with Me

Enabling Auto-Configuration

After you have configured default values for the Vibe desktop application installation, you can enable auto-configuration. When auto-configuration is enabled, users cannot change the default values during initial configuration. (Users specify only their user name and password when configuring the Vibe desktop application.)

You accomplish this on Windows by creating registry values, and on Mac by adding properties to the application’s `Info.plist` file.

1 **Windows:** Access the following location where you will create registry values:

`\\HKLM\Software\Novell\Vibe`

Mac: Access the `Info.plist` file where you will add properties. This file is usually in the following location:

`/Applications/Novell Vibe/Contents/Info.plist`

2 Create Windows registry values and add properties to the `Info.plist` file for the values for which you want to configure defaults.

The following table displays the available options for auto-configuration.

Table 9-2 *Auto-Configuration Options*

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Auto Configure	REG_SZ (“true” or “false”)	VibeAutoConfigure	<true/> or <false/>	No	false

Disallowing User Configuration

You can disallow users from modifying configuration options in the Vibe desktop application. This means that users cannot change the default values during initial configuration, and they cannot modify the values via the Vibe console after initial configuration.

NOTE: This does not prevent users from manually modifying configuration settings in the registry or file system.

You accomplish this on Windows by creating registry values, and on Mac by adding properties to the application’s `Info.plist` file.

1 **Windows:** Access the following location where you will create registry values:

`\\HKLM\Software\Novell\Vibe`

Mac: Access the `Info.plist` file where you will add properties. This file is usually in the following location:

`/Applications/Novell Vibe/Contents/Info.plist`

2 Create Windows registry values and add properties to the `Info.plist` file for the values for which you want to configure defaults.

The following table displays the available options for disallowing user configuration.

Table 9-3 *Disallow User Configuration Options*

Windows Registry Value Name	Value Type	Mac Property Name	Value Type	Supports Env Variables	Default Value
Allow User Configuration	REG_SZ (“true” or “false”)	VibeAllowUserConfiguration	<true/> or <false/>	No	true

Modifying the Vibe Desktop Configuration

If you have configured the Vibe desktop application with auto-configuration (as described in “Enabling Auto-Configuration” on page 155), you can modify the configuration settings:

1 Change the options in the registry or `.plist` file, then restart the Vibe desktop application.

When the Vibe desktop application starts, it detects that the default settings have changed and applies the new settings.

NOTE: The one exception is that the synchronization directory cannot be changed after the Vibe desktop application has been configured.

Controlling Windows Explorer Restart

The Vibe desktop application for Windows includes overlay icons that do not appear until Windows Explorer is restarted. In previous versions of the Vibe desktop application, the Windows `.msi` always restarted Windows Explorer during the installation (except when using the `No UI` option). Because restarting Explorer might not always be desirable, the Vibe desktop application lets you override the default.

The Windows installer supports four basic user interface levels for installing `MSI` files:

- No UI (“msiexec /qn”)

  Windows Explorer is never restarted when using this option.
- Basic UI (“msiexec /qb”)
- Reduced UI (“msiexec /qr”)
- Full UI (“msiexec /qf” or simply “msiexec”, since this is the default)

For example, use the following command to install the `MSI` with basic UI and without restarting Windows Explorer:

```
msiexec /qb /i NovellVibe-version.msi RESTARTEXPLORER=no
```

Enabling Users to Edit Vibe Documents with Microsoft Office

Users can edit Vibe documents with the Micro Focus Vibe Add-in for Microsoft Office by simply installing and configuring the Vibe Add-in. Users can browse to documents, edit them, save them to Vibe, and much more, all directly from Microsoft Office. For more information, see the Micro Focus Vibe Add-In Quick Start (http://www.novell.com/documentation/vibe33/vibe33_qs_office/data/vibe33_qs_office.html).

To allow users to co-edit documents, you must modify the access control settings for the Team Member role to allow team members to edit entries that were created by other team members:

1. In Vibe, click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
2. Under **System**, click **Configure Role Definitions**.
3. On the **Configure Role Definitions** tab, in the **Currently Defined Roles** section, expand **Team Member**.
4. Select **Modify Entries**, then click **Apply**.

   This adds the Modify Entries right to the Team Member role. For more information about roles and the rights that are associated with them, see “Managing Roles to Refine Access Control” on page 31.

Configuring Integrated Windows Authentication to Support Vibe Desktop and the Vibe Add-In

If your Vibe server is configured with Integrated Windows Authentication, Vibe Desktop cannot synchronize files on your Vibe site because of a port conflict.

To work around this issue:

1 Configure Vibe Desktop and the Vibe Add-in to point directly to Tomcat's secure port (by bypassing port 80 and port 443) in the Vibe Desktop and Vibe Add-in installation programs.

For more information about configuring Windows Authentication for your Vibe site, see "Configuring Single Sign-On with Internet Information Services for Windows" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

10 Configuring Vibe to Support WebDAV on Windows 7

WebDAV is a standard collaborative editing and file management protocol. Micro Focus Vibe relies on the WebDAV protocol to operate two key features:

- Edit-in-Place functionality for files by using tools such as OpenOffice and Microsoft Office, as described in "Using WebDAV to Edit Individual Files" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- Map Vibe folders as a web folder on the client computer, which allows access to Vibe files from a WebDAV-compliant file navigation tool such as Windows Explorer or Nautilus, as described in "Creating a Mapped Drive to the Vibe Folder" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

If your Vibe users are running a supported client operating system other than Windows 7, features that are supported by WebDAV already work as described in "Setting Up and Using WebDAV" in the *Micro Focus Vibe 4.0.5 Advanced User Guide* without any additional configuration.

The information in this section assumes that your environment requires the use of Microsoft Office. If your environment does not require the use of Microsoft Office, see "Using OpenOffice as Your Document Editor for WebDAV" on page 161.

Planning Your WebDAV Implementation

Understanding the Different Types of WebDAV Authentication Methods

Micro Focus Vibe supports the following WebDAV authentication methods:

- **Basic Authentication:** User name and password are encoded with the Base64 algorithm. The Base64-encoded string is unsafe if transmitted over HTTP, and therefore should be combined with SSL/TLC (HTTPS).

  For more information, see "Choosing Basic Authentication" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

If you plan to use Basic authentication over a non-secure connection (HTTP), you need to modify the registry on each Windows 7 client workstation, as described in "Allowing Basic Authentication over an HTTP Connection on Windows 7" on page 163. The registry modification lets users use WebDAV with Microsoft Office 2007. However, Microsoft Office 2010 is not supported.

- **Digest Authentication:** Applies MD5 cryptographic, one-way hashing with usage of nonce values to a password before sending it over the network. This option is more safe than Basic Authentication when used over HTTP.

  For more information, see "Choosing Digest Authentication" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

- **Windows Authentication:** Provides Windows users with a single sign-on experience, enabling users to automatically authenticate to Vibe after they are logged in to their individual workstations. Internet Information Services (IIS) provides this capability.

  For more information, see "Choosing Windows Authentication" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Using WebDAV When Vibe Is Fronted by NetIQ Access Manager or IIS

If your Vibe system is fronted by either NetIQ Access Manager or Internet Information Services (IIS), you must use the designated WebDAV authentication method:

Product Fronting Vibe	Designated Authentication Method
NetIQ Access Manager	If your Vibe installation is fronted by NetIQ Access Manager, as described in "Configuring Single Sign-On with Novell Access Manager" in the *Micro Focus Vibe 4.0.4 Installation Guide*, you must use basic authentication for your WebDAV implementation In the Vibe installation program, select **basic** on the WebDAV Authentication Method page.
Internet Information Services (IIS)	If your Vibe installation is fronted by IIS, as described in "Configuring Single Sign-On with Internet Information Services for Windows" in the *Micro Focus Vibe 4.0.4 Installation Guide*, you must use Windows authentication for your WebDAV implementation.

Meeting Vibe Certificate Requirements on Windows 7

If you are using WebDAV functionality (either Edit-in-Place or mapping a Vibe folder) with Vibe on Windows 7 with a secure (HTTPS) connection, you need to ensure that the Vibe server certificate requirements are met. If all of the requirements are not met, various Windows 7 services fail.

The Vibe server certificate requirements are:

- You must use a trusted server certificate that is accepted by Windows 7. This server certificate must be signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

  NOTE: You can use a self-signed certificate only if the certificate is imported into the Trusted Root Certification Authorities store on each Windows 7 client computer. For specific information on how to accomplish this, see "Configuring Windows 7 to Use a Self-Signed Certificate with Vibe" on page 162

- The trusted server certificate must be issued to a name that exactly matches the domain name of the URL that you are using it for. This means that it must match the URL of your Vibe site.
- The date range for the trusted server certificate must be valid. You cannot use an expired server certificate.
- The Windows 7 system must be adjusted to enable FIPS-compliant algorithms for encryption, hashing, and signing.
  1. From the Start menu, type **Local Security Policy**, then press Enter.
  2. Expand **Local Policies**, then select **Security Options**.
  3. Enable the following setting:

     System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

Using OpenOffice as Your Document Editor for WebDAV

If your environment does not require the use of Microsoft Office, you might consider migrating users to OpenOffice 3.1 or later as their document editor. Using OpenOffice 3.1 or later provides seamless integration between the WebDAV server and Vibe, regardless of which operating system is being used.

Editing Files with Edit-in-Place Functionality

You can leverage Edit-in-Place functionality to edit files by using tools such as OpenOffice and Microsoft Office. For information on how to edit files in Vibe with Edit-in-Place functionality, see "Using WebDAV to Edit Individual Files" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

If you are using Edit-in-Place functionality over HTTP, no additional setup is required. However, if you are using Edit-in-Place functionality over HTTPS on Windows 7, ensure that you have met the Vibe server certificate requirements, as described in "Meeting Vibe Certificate Requirements on Windows 7" on page 160.

For more information about editing Vibe documents in Microsoft Office with Windows 7, see "TID 7006717: Document editing failure with Windows 7 and Microsoft Office" in the Novell Support Knowledgebase (http://www.novell.com/support/kb/).

Mapping a Vibe Folder as a WebDAV Folder

Mapping a Micro Focus Vibe folder as a WebDAV folder on the client computer allows access to Vibe files from a WebDAV-compliant file navigation tool such as Windows Explorer or Nautilus. For information on how to map a Vibe folder, see "Creating a Mapped Drive to the Vibe Folder" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

When you map a Vibe folder as a WebDAV folder on Windows 7, consider the following:

- Successfully mapping a Vibe folder does not ensure that the Edit-in-Place feature on single files also works, as described in "Using WebDAV to Edit Individual Files" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

  For example, if you map a Vibe folder using Basic Authentication over HTTP (with the required registry change to the client computer), then attempt to edit a file in Microsoft Office 2010, it fails to open the file because Microsoft Office 2010 does not work with Basic Authentication over HTTP.

* When you map a Vibe folder and your Vibe server is configured with Windows Authentication, you expect the client computer to automatically supply your Windows login credentials to the server. However, because of a problem in Windows 7, users might be prompted to enter their credentials when accessing the Vibe server.

  To fix this problem, modify the registry on each Windows 7 client computer, as instructed in an article on the Microsoft Support Page (http://support.microsoft.com/Default.aspx?id=943280).
* When you map a Vibe folder and your Vibe server is configured with Windows Authentication, an error might occur saying that there's been a problem with Windows Shell web services, and the process fails.

  To fix this problem, modify the registry on each Windows 7 client computer, as instructed in an article on the Microsoft Support Page (http://support.microsoft.com/Default.aspx?id=943280).
* When mapping a Vibe folder over HTTPS, you must ensure that all Vibe server certificate requirements are met, as described in "Meeting Vibe Certificate Requirements on Windows 7" on page 160.

Configuring Windows 7 to Use a Self-Signed Certificate with Vibe

Configuring Windows 7 to use a self-signed certificate with Micro Focus Vibe is a two-step process. The first step is accomplished by the Vibe administrator on the Vibe server, and the second step is accomplished by each Vibe user on his or her Windows 7 workstation.

Administrator Configuration Responsibilities

1. Ensure the following prerequisites are met in order to configure Windows 7 to use a self-signed certificate with Vibe:
   * The self-signed server certificate must be issued to a name that exactly matches the domain name of the URL that you use it for. This means that it must match the URL of your Vibe site. If you are generating a self-signed certificate using the keytool, as described "Importing the Certificate Files into the Vibe Keystore" on page 337, you must enter the Vibe domain name when prompted for your first and last name.
   * The date range for the trusted server certificate must be valid. You cannot use an expired server certificate.

User Configuration Responsibilities

Each user on his or her Windows 7 workstation must import the self-signed certificate of the Vibe server into the **Trusted Root Certification** Authorities store.

In a controlled corporate environment where the system administrator sets up each client workstation before use, this certificate can be pre-installed on each Windows 7 workstation. This can minimize end-user error and frustration.

1. Launch the Internet Explorer browser.
2. Click **Tools** > **Internet Options** to display the Internet Options dialog box.
3. Click the **Security** tab, then select **Trusted sites**.

4 Click **Sites**.

5 In the **Add this website to the zone** field, specify the URL of the Vibe web site, then click **Add** > **Close**.

6 Browse to your Vibe site.

7 (Conditional) If a prompt displays indicating that there is a problem with this web site's security certificate, complete the following steps:

7a Click **Continue to this website (not recommended)**.

7b Click **Certificate Error** at the right of the address bar, then click **View certificates**.

7c Click **Install Certificate**, then click **Next** in the wizard.

7d Select **Place all certificates in the following store**.

7e Click **Browse**, browse to and select **Trusted Root Certification Authorities**, then click **OK**.

7f In the wizard, click **Next**, then click **Finish**.

7g (Conditional) If a Security Warning dialog box displays, click **Yes**.

7h Click **OK** to close the Certificate Import Wizard.

7i Click **OK** to close the Certificate window.

7j Shut down all instances of the Internet Explorer browser, then restart the browser.

7k Browse to the Vibe site. You should no longer see the certificate error message.

If you continue to see the certificate error message, the server's self-signed certificate might not match the site URL, as described in "Administrator Configuration Responsibilities" on page 162.

Allowing Basic Authentication over an HTTP Connection on Windows 7

You can modify the Windows registry to allow Basic authentication to WebDAV over an HTTP connection. This registry change lets users use Microsoft Office 2007 on the Windows 7 operating system, but does not allow them to use Microsoft Office 2010. Microsoft Office 2010 is not supported with Basic Authentication over an HTTP connection.

To modify the Windows registry:

1 On each Windows 7 workstation, click **Start** > **Run**, then specify `regedit` in the **Open** field.

2 Click **OK**.

3 In the Registry Editor window, navigate to the following registry entry:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\services\WebClient\Parameters\Bas
icAuthLevel
```

4 Change the value of this registry entry to `2`.

5 Navigate to the Services interface, then restart the **WebClient** service.

11 Configuring Email Integration

Initial email configuration is performed when you install Micro Focus Vibe. Additional aspects of email handling are configured on the Vibe site. For information about how to further configure email settings beyond what is covered in this section, see Chapter 28, “Managing Email Configuration,” on page 271.

Enabling/Disabling Outbound Emailing of Folder Digests

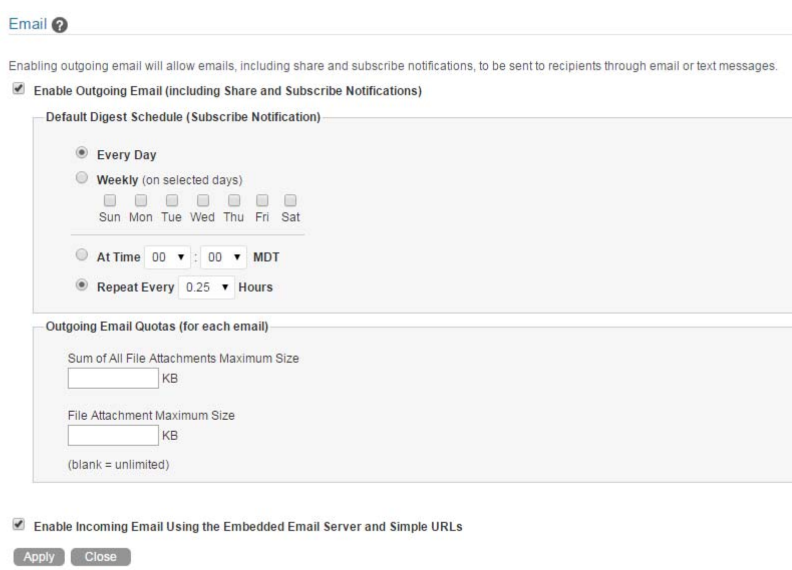
During installation, you configured Micro Focus Vibe to communicate with your email system, as described in “Gathering Outbound Email Information” in “Basic Installation” in the *Micro Focus Vibe 4.0.4 Installation Guide*. As a result, Vibe users can send email messages to other Vibe users and to anyone whose email address they know. They can also send email notifications when they create workspaces, add folder entries, and so on.

In addition to this basic email functionality, you can configure your Vibe site so that users can receive folder digests of site activity that are created and sent to the users who have subscribed to the folders.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the Vibe page, then click the **Administration** icon .

3 Under **System**, click **Email**.



4 Select **Enable Outgoing Email**.

By default, folder digests are compiled and sent daily at fifteen minutes after midnight.

5 Adjust the schedule as needed to meet the needs of the majority of your Vibe users.

   Users can turn the digests on and off for individual folders, but they cannot change the email schedule that you establish.

6 (Optional) To set a data quota on outgoing mail messages, specify the quota limit in the **Sum of All File Attachments Maximum Size** and the **File Attachment Maximum Size** fields.

   By default, there is no limit to the size of attached files. You can leave the fields blank to retain the default of no limit.

   To restrict any attachments from being sent, specify `0` in each field.

7 Click **Apply** to save the settings, then click **Close**.

For information about the options that users have for receiving email notifications, see "Subscribing to a Folder or Entry" in "Getting Informed" in the *Micro Focus Vibe 4.0.5 User Guide*.

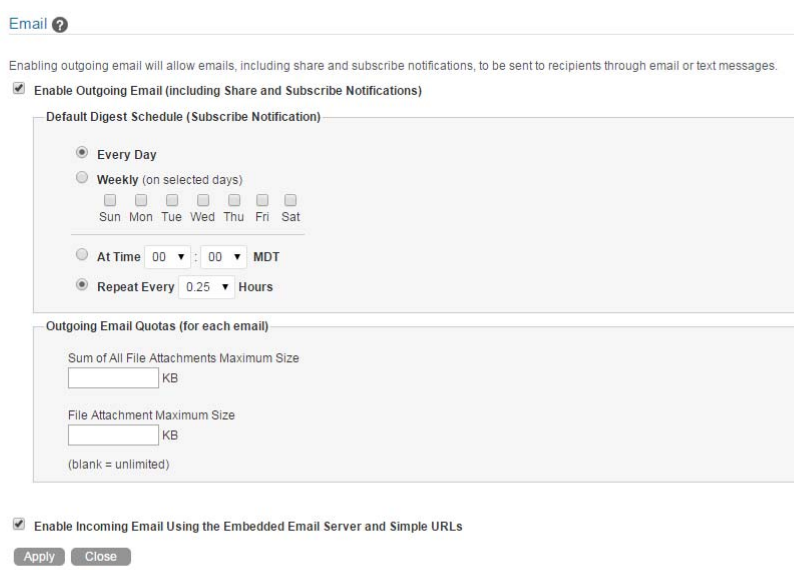
Disabling/Enabling Inbound Email Postings

During installation, you configured Micro Focus Vibe to include an internal SMTP mail host for receiving email postings to folders, as described in "Enabling Inbound Email" in "Basic Installation" in the*Micro Focus Vibe 4.0.4 Installation Guide*. Your selection during installation carries over into the configuration of your Vibe site. Therefore, you can disable incoming email if necessary, and then enable it again on the Vibe site. Relaying is permanently disabled on the internal SMTP mail host.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under **System**, click **Email**.



4 Select or deselect **Enable Incoming Email Using the Embedded Email Server and Simple URLs**.

5 Click **Apply > Close** to save the setting.

For information about how to configure folders to receive email postings, see "Enabling Folders to Receive Entries through Email" in "Managing Folders" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*. Failed email postings are listed in the Tomcat log file. For background information about the Tomcat log file, see "Tomcat Log File" on page 309.

12 Configuring Weekends and Holidays

You can configure Micro Focus Vibe to recognize weekends and holidays. Currently, the weekend and holiday schedule is used by default only in relation to task durations. It can also be leveraged by users when configuring workflow transitions.

* "Configuring Vibe to Recognize Weekends and Holidays" on page 169
* "Using Weekend and Holiday Information in Tasks and Workflows" on page 170

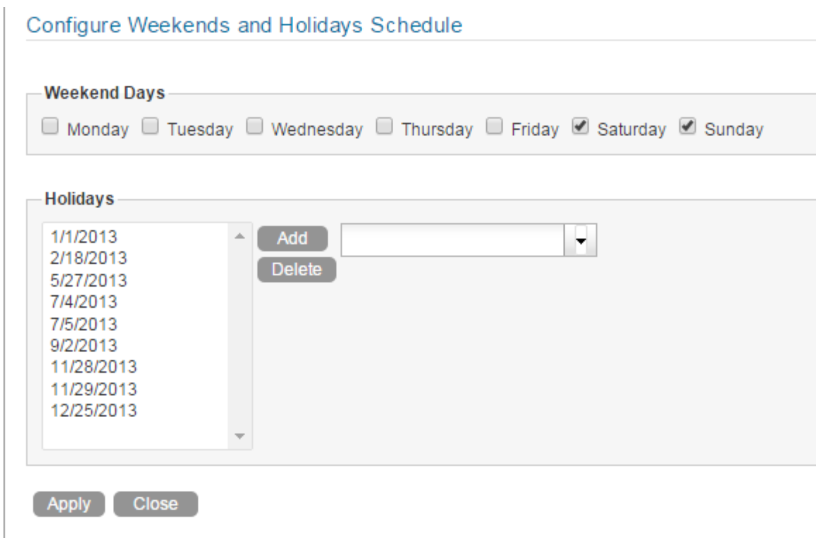
Configuring Vibe to Recognize Weekends and Holidays

To configure weekends and holidays for your Vibe site:

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **System**, click **Weekends and Holidays**.



4 In the **Weekend Days** section, select the days that you want to designate as the weekend.

Days left unselected are considered regular workdays.

5 In the **Holidays** section, click in the field on the right, select the date that you want to make a holiday, then click **Add**.

To remove a date as a holiday, select the date in the field on the left, then click **Delete**.

6 Click **Apply** > **Close**.

Using Weekend and Holiday Information in Tasks and Workflows

When Calculating Task Durations

If you have configured weekends and holidays, task durations exclude these days when calculating task due dates. For example, a task with a duration of 10 days translates into two full weeks (assuming a two-day weekend for each week). For more information about task durations, see "Working with Tasks Folders" in the *Micro Focus Vibe 4.0.5 User Guide*.

NOTE: Configuring a weekend and holiday schedule or changing an existing weekend and holiday schedule does not immediately affect the due dates of existing tasks. Existing tasks are affected only after the due dates are recalculated, such as when a new task (that includes a task duration) is added to the Tasks folder where the existing tasks are located.

When Configuring Workflow Transitions

If you have configured weekends and holidays, the weekend and holiday schedule can be leveraged by users when configuring workflows to transition after a specified number of days, as described in "Transition After Time Elapsed" in "Creating and Managing Workflows" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

13 Configuring Real-Time Communication Tools

From the Micro Focus Vibe site, Vibe users can communicate with each other in various ways.

- "Integrating Messenger with Vibe" on page 171
- "Integrating Skype with Vibe" on page 172

Integrating Messenger with Vibe

Vibe 3 and later lets you integrate with Novell Messenger 2.2 and later. This integration displays a user's Messenger presence information within Vibe. For information about where presence information is displayed in Vibe, see "Sending an Instant Message from within Vibe" in the *Micro Focus Vibe 4.0.5 User Guide*.

When you click a user's presence icon, the Profile Quick View is displayed, which lets you send an instant message to the user, view the user's personal workspace, follow the user, and more.

To successfully integrate Novell Messenger with Micro Focus Vibe, you must complete the following tasks:

- "Defining an Allowed Service User in ConsoleOne" on page 171
- "Configuring Messenger Integrations in the Vibe Installation Program" on page 171
- "Configuring Presence" on page 172

Defining an Allowed Service User in ConsoleOne

The Allowed Service User's function is to log in to the Messenger system and retrieve presence information, which is then displayed in Vibe.

For information about how to create an Allowed Service User in ConsoleOne, see "Integrating Micro Focus Vibe with GroupWise Messenger" in the *GroupWise Messenger 18 Administration Guide*.

Configuring Messenger Integrations in the Vibe Installation Program

After you have defined an Allowed Service User in ConsoleOne, as described in "Integrating Micro Focus Vibe with GroupWise Messenger" in the *GroupWise Messenger 18 Administration Guide*, you need to run the Vibe installation program and configure Messenger.

For information about the presence configuration page in the Vibe installation program, see "Configuring Presence" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Configuring Presence

You should use LDAP to sync users with a directory service such as eDirectory in order to populate the **Presence ID** field in Vibe.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. Under **System**, click **LDAP**.
4. On the **Users** tab, map the identifier `presenceID` to the LDAP attribute that identifies the user. For example, `presenceID=cn`.
5. Click **OK**.

Integrating Skype with Vibe

Micro Focus Vibe enables Vibe users to use Skype to contact other Vibe users directly from the Vibe interface.

This functionality is enabled on a system level by default. For more information on how Vibe users can use Skype to contact other Vibe users from inside Vibe, see “Using Skype from within Vibe” in “Connecting With Your Co-Workers” in the *Micro Focus Vibe 4.0.5 User Guide*.

14 Enabling Custom JSPs to Be Used on Your Vibe Site

Micro Focus Vibe supports the use of custom JavaServer Pages (JSP) files. As a Vibe administrator, you can work with Vibe developers to write custom JSP files that enhance the appearance and functionality of your Vibe site.

Before you can enable a JSP file to be used in your Vibe site, the file must first be created. For information on how to create a custom JSP file, see "Creating JavaServer Pages (JSPs)" in the *Micro Focus Vibe 4.0.5 Developer Guide*.

Enabling JSP Files to Be Used on Your Vibe Site

After a JSP file has been created, you need to make it available to users in your Vibe site.

1. On the Vibe server, locate the JSP file that you want to make available to users.
2. Place the JSP file in the `/WEB-INF/jsp/custom_jsps` directory.

   Users need to reference this file by name in order to use it, so make sure that the name of the file is intuitive and easy to remember.

   TIP: You might want to create separate folders for each custom JSP file inside the `custom_jsps` directory. This can make managing your custom JSP files more simple. However, users who leverage these sample JSP files from the Vibe site will need to enter the relative path to the file. For example: *`new_folder`*`/custom_jsp_landing_page_entry.jsp`.

   ---

3. Stop and Restart the Vibe server.

   or

   If you are running Vibe in a non-production environment, you can configure Vibe to automatically update a all JSP changes that you make on the Vibe server, without stopping and restarting the Vibe server. For more information, see "Dynamically Updating JSP Files by Running Vibe in Development Mode" on page 173.

Dynamically Updating JSP Files by Running Vibe in Development Mode

---

WARNING: Running Vibe in development mode is not supported in production environments, significantly decreases Vibe performance, and is offered only as a convenience for developers.

If you are testing JSP files on a non-production system and you want all JSP changes that you make on the Vibe server to be automatically available on the Vibe server without stopping and restarting the Vibe server, you can run Vibe in development mode.

To run Vibe in development mode:

1 Open the `web.xml` file in a text editor.

The `web.xml` file is located in the following directory:

Platform	Default Location
Linux:	`/opt/novell/teaming/apache-tomcat/conf`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\conf`

2 Search for the `development` parameter, then change the value of this parameter from `false` to `true`.

3 Save and close the `web.xml` file.

Using Sample Custom JSPs to Modify the Behavior of a Landing Page

NOTE: While the information in this section is still valid, users can achieve the same results (and more) with Vibe 3.1 and later by adding an Enhanced View element to the landing page. For more information, see "Enhanced View:" in "Adding Content to Your Landing Page" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Micro Focus Vibe includes sample custom JSP files that enable you to modify the behavior of Vibe landing pages. Before you implement the sample JSP files that are described in this section, you might want to further customize them to suit your specific needs, as described in "Creating JavaServer Pages (JSPs)" in the *Micro Focus Vibe 4.0.5 Developer Guide*.

For information on how users can add these custom JSP files to their individual landing pages after the JSP files have been enabled for use, see "Adding Content to Your Landing Page" in "Creating and Managing Landing Pages" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

- "Listing Folder Entry Titles in a Bulleted List" on page 174
- "Displaying Entry Replies on a Landing Page" on page 175
- "Enabling Users to Take a Survey Directly from a Landing Page" on page 175

Listing Folder Entry Titles in a Bulleted List

To activate the sample JSP file that enables Vibe users to list entries in a bulleted list for any given folder:

1 In the Vibe source files, navigate to the `\WEB-INF\jsp\custom_jsp\samples` directory.

2 Select and copy the `custom_jsp_landing_page_folder_list.jsp` file, then paste it into the `\WEB-INF\jsp\custom_jsp` directory.

TIP: You might want to create separate folders for each custom JSP file inside the `custom_jsps` directory. This can make managing your custom JSP files more simple. However, users who leverage these sample JSP files from the Vibe site need to enter the relative path to the file. For example: *`new_folder`*`/custom_jsp_landing_page_entry.jsp`.

Displaying Entry Replies on a Landing Page

You can display replies for a single entry, or for all entries that are contained in a folder.

- "Displaying Entry Replies for a Single Entry" on page 175
- "Displaying Entry Replies for All Entries in a Folder" on page 175

Displaying Entry Replies for a Single Entry

To activate the sample JSP file that lets Vibe users display entry replies on a landing page when referencing a folder entry:

1. In the Vibe source files, navigate to the `\WEB-INF\jsp\custom_jsp\samples` directory.
2. Select and copy the `custom_jsp_landing_page_entry.jsp` file, then paste it into the `\WEB-INF\jsp\custom_jsp` directory.

TIP: You might want to create separate folders for each custom JSP file inside the `custom_jsps` directory. This can make managing your custom JSP files more simple. However, users who leverage these sample JSP files from the Vibe site need to enter the relative path to the file. For example: *`new_folder`*`/custom_jsp_landing_page_entry.jsp`.

Displaying Entry Replies for All Entries in a Folder

To activate the sample JSP file that lets Vibe users display entry replies on a landing page when referencing a folder:

1. In the Vibe source files, navigate to the `\WEB-INF\jsp\custom_jsp\samples` directory.
2. Select and copy the `custom_jsp_landing_page_folder.jsp` file, then paste it into the `\WEB-INF\jsp\custom_jsp` directory.

TIP: You might want to create separate folders for each custom JSP file inside the `custom_jsps` directory. This can make managing your custom JSP files more simple. However, users who leverage these sample JSP files from the Vibe site need to enter the relative path to the file. For example: *`new_folder`*`/custom_jsp_landing_page_entry.jsp`.

Enabling Users to Take a Survey Directly from a Landing Page

To activate the sample JSP file that enables Vibe users to participate in a survey directly from a landing page:

1. In the Vibe source files, navigate to the `\WEB-INF\jsp\custom_jsp\samples` directory.
2. Select and copy the `custom_jsp_landing_page_survey_entry.jsp` file, then paste it into the `\WEB-INF\jsp\custom_jsp` directory.

15 Enabling Custom JAR Files to Be Used on Your Vibe Site

Micro Focus Vibe supports the use of custom Java Archive (JAR) files. JAR files are one way that you can incorporate custom functionality to Vibe workflows.

As a Vibe administrator, you can work with Vibe developers to write custom JAR files that enhance the functionality of workflows on your Vibe site.

Before you can enable a JAR file to be used in a workflow, the file must first be created. (The Vibe documentation does not describe how to create a JAR file.)

After the code has been written to accomplish a specific workflow action and then packaged into a JAR file, you need to make that JAR file available to Vibe users who are creating workflows.

When you customize workflows by using JAR files as described in this section, the JAR file can be referenced from any zone within your Vibe system. If you want customizations to be available to only one particular zone, you can instead add the customizations by adding an extension, as described in Chapter 16, “Adding Software Extensions to Your Vibe Site,” on page 179. (For more information about zones in Vibe, see Chapter 19, “Setting Up Zones (Virtual Vibe Sites),” on page 195.)

To make the custom JAR file available to Vibe users:

1 Place the JAR file in the following directory. If the directory does not yet exist, create it.

Linux:	`/opt/novell/teaming/apache-tomcat/lib/custom-ext`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\lib\custom-ext`

Users can now reference this JAR file by adding a Custom Action element to a workflow, as described in “Adding On-Entry or On-Exit Events” in “Creating an Advanced Workflow” in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

16 Adding Software Extensions to Your Vibe Site

You can customize your Micro Focus Vibe site through the use of software extensions. Vibe administrators or Vibe developers can create custom extensions (add-ons) that enhance the power and usefulness of the Vibe software. For example, you might have an extension that enables Flash video support in Vibe.

When you customize your Vibe site through the use of software extensions, as described in this section, the customizations are available only for the zone where the software extension is deployed. If you are creating customizations for workflows, and you want to make the customizations available to multiple zones, you can instead add the customizations as JAR files, as described in Chapter 15, "Enabling Custom JAR Files to Be Used on Your Vibe Site," on page 177. (For more information about zones in Vibe, see Chapter 19, "Setting Up Zones (Virtual Vibe Sites)," on page 195.)

This section discusses how to add software extensions that have already been created.

If you want Vibe to communicate with a third-party application and display related information inside of Vibe, you can set up a remote application, as described in Chapter 17, "Using Remote Applications on Your Vibe Site," on page 183.

Creating a Software Extension

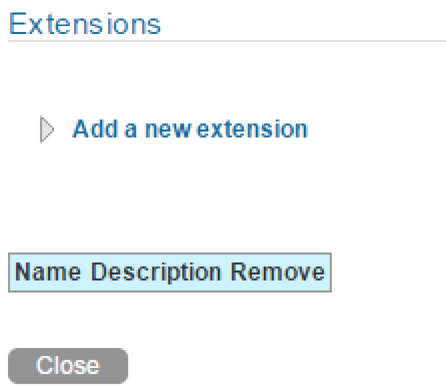
For information on how to create a custom software extension for Micro Focus Vibe, see "Creating and Packaging Extensions for Deployment" in the *Micro Focus Vibe 4.0.5 Developer Guide*.

Deploying the Extension in Your Vibe Site

1 Log in to the Micro Focus Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under **Management**, click **Extensions**.



4 Click **Add a new extension**.

5 In the **Choose a File** section, click **Browse**, then browse to the extension that you want to deploy.

The extension is a `zip` file that can contain definition `xml` files, custom JSP files, Java classes, `html` files, `css` files, JavaScript, and other third-party files.

6 Click **Add**.

The extension is now installed and is displayed in a table on the Manage Extensions page.

You might need to configure an extension after it has been installed. For information on how to configure extensions, see the installation instructions on the web site where you obtained the extension.

Installation instructions are specific for each extension, and should be written by the extension creator.

Viewing Your Vibe Extensions

1 Log in to the Micro Focus Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under **Management**, click **Extensions**.

The Extensions page is displayed.

The table lists all extensions that are currently available in the Vibe site.

Removing an Extension from Your Vibe Site

An extension cannot be removed from the Micro Focus Vibe site if the extension is being referenced by a binder or entry. If an extension is being referenced somewhere in the Vibe site, you must first manually delete the files and definitions that are referencing the extension before you can remove the extension itself. When an extension is removed, it does not remove any actual data from the Vibe site.

To remove an extension from your Vibe site:

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. Under **Management**, click **Extensions**.

   The Manage Extensions page is displayed.
4. In the table, click the (x) in the **Remove** column for the extension that you want to delete.
5. Click **OK**.

   The extension is removed from the Vibe site and can no longer be used.

17 Using Remote Applications on Your Vibe Site

A remote application is a program that runs on a remote server and delivers data for use on your Micro Focus Vibe site (such as data from a remote database). For example, you could set up a remote application for Twitter that displays all of your Twitter entries in Vibe.

Unlike creating an extension for Vibe, creating a remote application does not modify the Vibe software in any way.

If you want to make modifications to the Vibe software itself, you can add a software extension, as described in Chapter 16, "Adding Software Extensions to Your Vibe Site," on page 179.

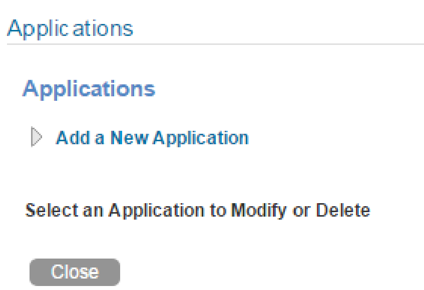
Adding a Remote Application to Your Vibe Site

After you or a developer have created a remote application, you need to make it available on your Micro Focus Vibe site.

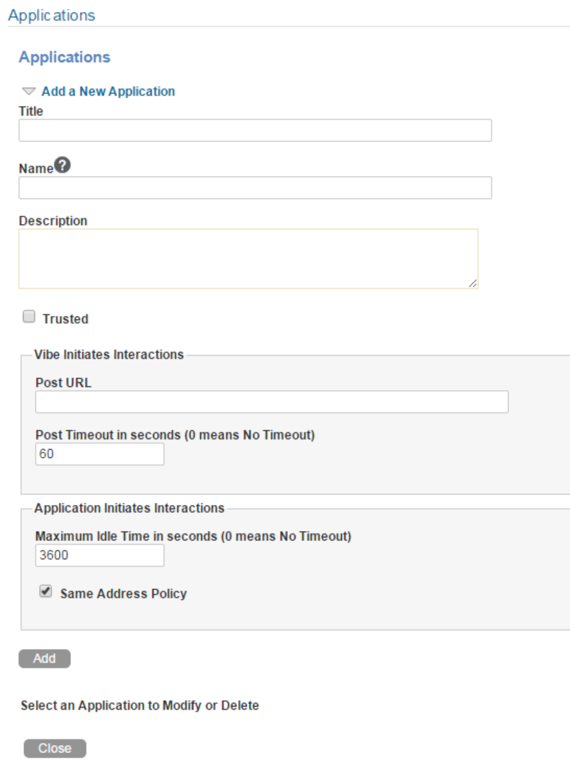
1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under **Manage**, click **Applications**.



4 Click **Add a New Application**.



5 Fill in the following fields:

Title: Specify a unique title for the remote application. For example, `Hello World`.

Vibe site users who add the remote application to a form or view can select the title from the list of available remote applications.

Name: Specify a unique name for the remote application. The name is for internal use in the Vibe database. The first character must be an alphabetic character (a-z, A-Z). For the rest of the name, you can use alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_). For example, `helloworld`.

Description: Provide a description of what the remote application does.

Trusted: Select **Trusted** if the application is extremely trustworthy (for example, if you write, maintain, and run the application on the same server that runs Vibe). If you select **Trusted**, Vibe applies access control according to the viewing user's access control settings. For complete information about access control, see "Managing Remote Applications" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Post URL: Specify the URL of the remote application. Vibe posts requests for information, along with the requesting user and a security token for use by Vibe web services, to this URL, then waits to receive the requested HTML snippets for posting on the Vibe site. For example, `http://localhost:8080/remoteapp/helloWorld`.

Post Timeout: Specify the number of seconds that Vibe should wait for a response from the remote application before it assumes that the remote application is not available. The default is 60 (1 minute). If Vibe does not receive a response from the remote application, it displays the page requested by the user without any input from the remote application.

Maximum Idle Time: Specify the number of seconds that Vibe maintains idle connections through Vibe web service with a remote application. The default is 3600 (1 hour). After the maximum idle time elapses, Vibe closes idle connections.

Same Address Policy: Select this option if interactions with the Vibe site are initiated by the remote application, and if the remote application must communicate with Vibe through the Vibe web services machine by using the same security token for the entire communication.

6 Click **Add** to add the remote application to the list of remote applications that are available on your Vibe site, then click **Close**.

Users now see the new remote application in the list of tools within the designers and within the tool used to create accessories.

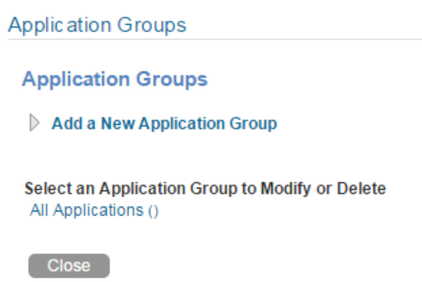
Creating an Application Group

If you create a number of remote applications for your Micro Focus Vibe site, you can create application groups for remote applications so they can all be assigned the same roles in the Access Control table. For example, you might have a group of remote applications that are allowed to perform administrative tasks and another group of remote applications that are granted only read access.

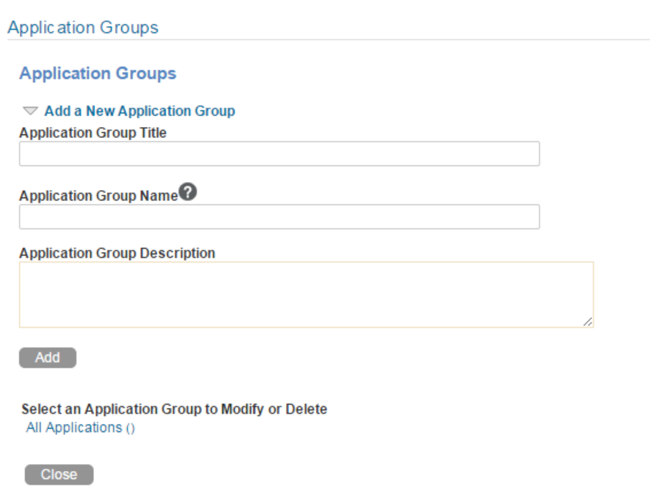
1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Manage**, click **Application Groups**.



4 Click **Add a New Application Group**.



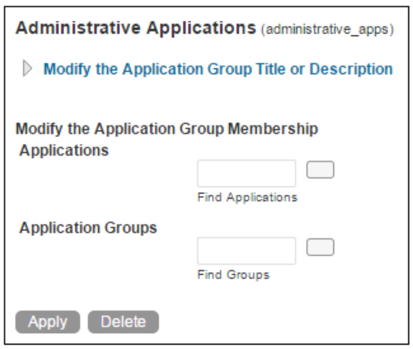
5 Fill in the following fields:

Application Group Title: Specify a unique title for the remote application group. Vibe site users who need to set access controls for a remote application can select the title from the list of available remote application groups.

Application Group Name: Specify a unique name for the remote application group. The name is for internal use in the Vibe database. The first character must be an alphabetic character (a-z, A-Z). For the rest of the name, you can use alphanumeric characters (a-z, A-Z, 0-9), hyphens (-), and underscores (_).

Application Group Description: Provide a description of the types of remote applications that the application group includes.

6 Click **Add** to add the application group to the list of application groups that are available on your Vibe site, then select the new application group to add remote applications to it.



7 Fill in the following fields:

Applications: Start typing the title of a remote application, then select the remote application. Repeat for each application that you want to add to the application group.

Application Groups: Start typing the title of an existing application group that you want to nest in the new application group, then select the application group. Repeat for each application group that you want to nest in the application group.

8 Click **Apply** to save the application group, then click **Close**.

Managing Access Controls for Remote Applications

Because not all remote applications can be completely trusted, it is often a good idea to limit the privileges of the remote application. This section describes how you can accomplish this.

If you are running a trusted remote application, such as an application that you are maintaining on the same server as Micro Focus Vibe, then you do not need to set access controls on it.

When an application is restricted to a specific role, the application can use web services to perform only those tasks that are allowed for that role. For example, the Participant role can create new entries, modify entries that the user created, add comments to entries, and so on. Participants cannot perform system administration tasks and cannot modify other users' entries.

Because workspace and folder owners can change the access control for places they own, you should communicate to your users about registered applications in the system and recommended access-control settings.

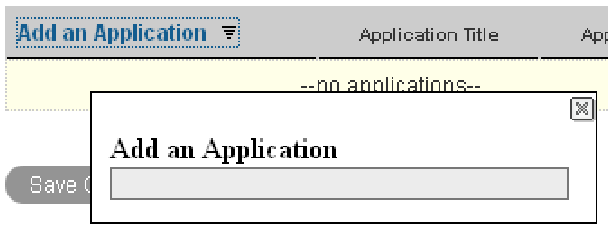
To limit the remote application to privileges assigned to a specific role:

1 Log in to the Vibe site as the Vibe administrator.

2 Access the top workspace in the hierarchy by clicking the workspace tree icon, then clicking **Home Workspace** (this is the default name for the top workspace).

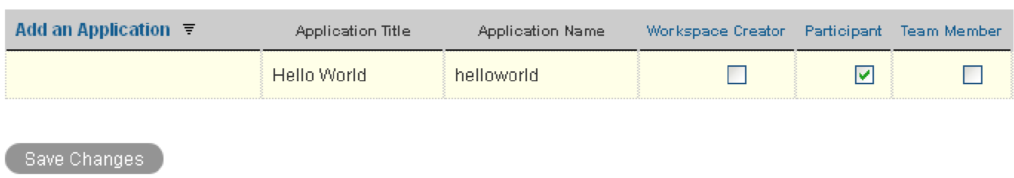
3 Click **Workspace** > **Access Control**.

4 On the Configure Access Control page, click **Add an Application**.



5 In the **Add an Application** field, use the type-to-find to specify and select the application that you want to add.

6 In the access control table, select the check box that is located in the row of the remote application that you just added, and the column of the role that you want to assign to the application.



7 Click **Save Changes** > **Close**.

The application that you added is now restricted to those operations allowed for the role that you selected. For example, if you assigned the Participant role to the remote application, then the inheritance of workspace and folder access controls means that it is very likely that most workspaces and folders inherit this setting. Assuming that all places inherited this setting, the most powerful role the remote application can assume within the installation is that of a Participant.

You can assign access-control roles to groups of applications instead of assigning roles to one application at a time if you have enabled multiple applications for your site and have grouped them together in an application group, as described in "Creating an Application Group" on page 185.

Implementing Remote Applications on Your Vibe Site

After you as the Micro Focus Vibe administrator have added remote applications to the Vibe site, users can implement them in custom forms and views, in workspaces, and as accessories. For instructions, see "Managing Remote Applications" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

18 Setting Up Mirrored Folders

A mirrored folder is a library folder within Micro Focus Vibe that is synchronized with a folder located on a system drive outside of Vibe. When you perform basic actions (adding subfolders and files, modifying files, deleting folders and files) by using the Vibe interface or by accessing the file on the drive, the change is reflected in the other interface. The advantage to using mirrored files is that you can apply Vibe tools to files on a drive, including tools such as text search, workflow, and discussion (in the form of comments applied to the entry in the library folder).

Initial setup of mirrored folder resource drivers is done during Micro Focus Vibe installation, as described in "Configuring Mirrored Folder Resource Drivers" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

The Vibe Installation program lets you set up as many as three mirrored folder resource drivers. If you need more than three, you must manually edit the `installer.xml` file, then update your Vibe installation.

After you set up the mirrored folder resource drivers by using the Installation program, you must perform additional mirrored folder configuration on the Vibe site.

- "Manually Setting Up More Than Three Mirrored Folder Resource Drivers" on page 189
- "Creating a Mirrored Files Folder for a Mirrored Folder Resource Driver" on page 192

Manually Setting Up More Than Three Mirrored Folder Resource Drivers

- "Editing the installer.xml File" on page 189
- "Updating Your Vibe Site Configuration" on page 191

Editing the installer.xml File

The Micro Focus Vibe Installation program lets you set up three mirrored folder resource drivers. However, there is no limit to the total number of mirrored folder resource drivers that you can set up after installation. A useful strategy is to set up resource drivers for root directories, then set up Mirrored File folders for root directories and subdirectories as needed, as described in "Creating a Mirrored Files Folder for a Mirrored Folder Resource Driver" on page 192.

When you run the Vibe Installation program, it creates the `installer.xml` file in the directory where you run it. The `installer.xml` file stores the information you provided during installation. You can also edit it manually, then update your Vibe installation.

1. Make a backup copy of your existing `installer.xml` file.
2. Open the `installer.xml` file in a text editor.
3. Search for `mirrored`.
4. Scroll down until you reach the three existing mirrored folder resource drivers.
5. Copy the mirrored folder resource driver that is most like the one you want to create, then paste it between the `<MirroredFolder>` and `</MirroredFolder>` tags.

The Vibe Installation program displays only the first three mirrored folder resource drivers, so you might want to place new resource drivers at the top of the list in order to double-check the information when you run the Vibe Installation program to implement your changes.

6 Set the parameters as needed for the file system location that you want to mirror in your Vibe site:

Tag	Setting
`enabled=`	`true`
`type=`	`file` or `webdav`
`id=`	The unique internal name for the mirrored folder resource driver. Use only alphanumeric characters. Do not include spaces, extended characters, or double-byte characters.
`title=`	The name of the mirrored folder resource driver that displays on the Vibe site. The title can include any characters.

`rootPath=`	For the `file` mirrored folder type, the absolute path to the directory from the point of view of the Vibe server.
	
	For the `webdav` mirrored folder type, the path to the directory after the WebDAV server hostname, and optionally, the port number, as specified by the `hostUrl=` parameter. The path should start with a slash (/), because it is appended to the setting of the `hostUrl=` parameter. For example, if the full WebDAV server location is:
	
	`http://webdavserver/archive/docs`
	
	the `rootPath=` setting would be:
	
	`/archive/docs`

`readonly=`	`true` or `false`
`zoneId=`	For a multi-zone Vibe site, this is the ID of the zone where you want the mirrored folder resource driver to be available. For information about Vibe zones, see Chapter 19, “Setting Up Zones (Virtual Vibe Sites),” on page 195. For a single-zone Vibe site, leave this parameter empty.--
`AllowedUsers idList=`	A list of Vibe user IDs that can access the mirrored folder resource driver and create mirrored folders. Use a semicolon (;) between user IDs.
`AllowedGroups idList=`	A list of Vibe groups that can access the mirrored folder resource driver and create mirrored folders. Use a semicolon (;) between group IDs.

7 (Conditional) If you are setting up a `webdav` mirrored folder, set the following additional parameters:

Tag	Setting

`hostUrl=`	The hostname, and optionally, the port number for the WebDAV server. For example:
	`http://`*`webdav_hostname`*`[:`*`port`*`]`
	`https://`*`webdav_hostname`*`[:`*`port`*`]`
	Do not include the directory path to the data. Use the `rootPath=` parameter to specify the path to the directory on the WebDAV server. For example, if the full WebDAV server location is:
	`http://`*`webdav_hostname`*`/archive/docs`
	the `hostUrl=` setting would be:
	`http://`*`webdav_hostname`*

`user=`	The user name that Vibe can use to connect to the WebDAV server. The WebDAV server must support HTTP Basic authentication (http://en.wikipedia.org/wiki/Basic_access_authentication).
`password=`	The password for the user name specified by the `user=` parameter.

8 Repeat Step 5 and Step 6 for each mirrored folder resource driver that you want to create.

9 Save the `installer.xml` file, then exit the text editor.

Updating Your Vibe Site Configuration

After you edit the `installer.xml` file, you must run the Micro Focus Vibe Installation program to update the configuration of your Vibe site. If you need assistance with any of the following steps, refer to the appropriate platform-specific instructions in “Installing and Setting Up a Basic Vibe Site” in “Basic Installation” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

1 Stop Vibe.

2 Start the Vibe Installation program.

The Vibe Installation program reads the updated `installer.xml` file. If your edits inadvertently changed the syntax of the file, the Installation program cannot start. If this happens, correct the problem in the `installer.xml` file, or return to your backup copy and try your edits again.

3 Accept the License Agreement, then click **Next**.

4 Select **Reconfigure Settings**, then click **Next**.

5 Select **Advanced**, then click **Next**.

6 Click **Next** until you reach the Mirrored Folder Resource Driver Configuration page.

The Vibe Installation program displays the first three mirrored folder resource drivers listed in the `installer.xml` file.

7 (Conditional) If you placed the new resource drivers at the top of the list, review the information that you added, and make corrections if necessary.

8 Click **Next**.

9 Click **Install** to implement the new mirrored folder resources.

10 Start Vibe.

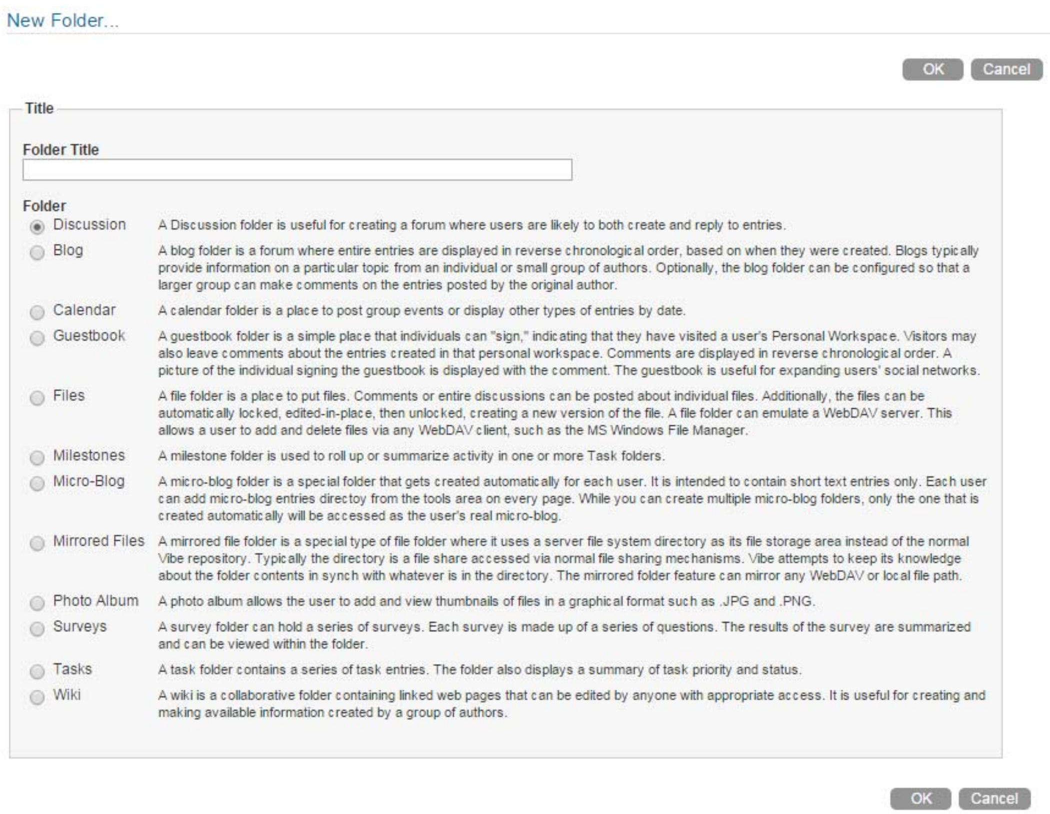
Creating a Mirrored Files Folder for a Mirrored Folder Resource Driver

After you have set up one or more mirrored folder resource drivers in the Micro Focus Vibe Installation program, you need to create a Mirrored Files folder for each resource driver in order to make the data accessible to users on your Vibe site.

1 Navigate to the workspace where you want to create a mirrored folder.

2 Create a new File folder:

2a Click the **Configure** icon next to the workspace title, then click **New Folder**.



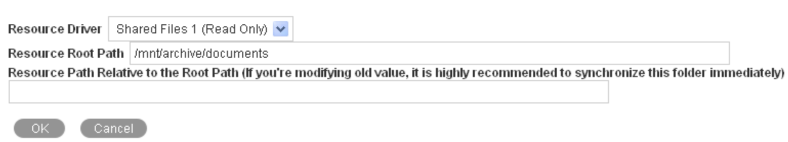
2b Specify a name for the folder that reflects the type of data that is available in the mirrored location.

2c Select **Mirrored Files**, then click **OK**.

3 Configure the new Mirrored Files folder to access the resource driver:

3a Click the **Configure** icon next to the folder title, then click **Edit Folder**.

3b Scroll down to the mirrored folder options at the bottom of the page.



3c Set the mirrored folder options as needed:

Resource Driver: Select the name of the mirrored folder resource driver, as specified in the **Title** field on the Mirrored Folder Resource Driver Configuration page in the Vibe Installation program or using the `title=` tag in the `installer.xml` file.

Resource Root Path: Displays the pathname you specified in the Vibe Installation program or the `installer.xml` file.

Resource Path Relative to the Root Path: (Optional) Add a subdirectory path to restrict the scope of the files available in the Mirrored File folder.

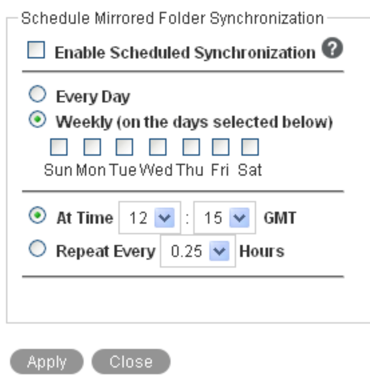
IMPORTANT: After you configure a Mirrored Files folder with a resource driver, you cannot edit any of the mirrored folder settings except for the subdirectory path. If you need to change other settings, you can delete the Mirrored File folder and create a new one with different settings.

3d Click **OK** to save the mirrored folder settings.

4 Display the Mirrored Files folder, click the **Configure** icon next to the folder title, then click **Manually Synchronize** to create the initial metadata for the mirrored folder.

5 Set up a synchronization schedule to keep the metadata current:

5a Click the **Configure** icon next to the folder title, then click **Schedule Synchronization**.



6 Select **Enable Scheduled Synchronization.**

7 Set schedule options as needed.

You can choose to have mirrored folder synchronization performed every day, or you can select specific days of the week (for example, on Monday, Wednesday, and Friday). You can choose to have synchronization performed once a day at a specified time (for example, at 2:00 a.m.), or you can set a time interval, so that it is performed multiple times each day (for example, every four hours). The smallest time interval you can set is .25 hours (every 15 minutes).

8 Click **Apply > Close** to save the synchronization schedule options for the mirrored folder.

9 Click the new Mirrored Files folder to display the directories and files in the mirrored location.

IMPORTANT: If you set up multiple Mirrored Files folders that point to the same files, and if Vibe users have been granted write access to those files, multiple Vibe users can gain write access to the same mirrored file at the same time. File locking is associated with each Mirrored File folder entry, not with the physical source files. Make sure that all Vibe users have access to mirrored files through the same Mirrored File folder.

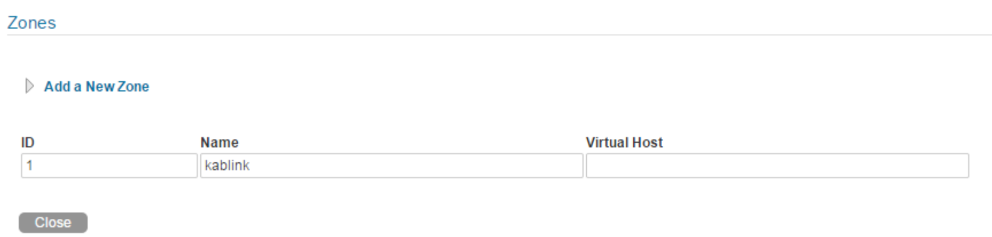
10 Set appropriate access controls on the Mirrored Files folder, as described in Chapter 2, "Planning and Controlling User Access to Workspaces and Folders," on page 21.

19 Setting Up Zones (Virtual Vibe Sites)

You can set up multiple virtual Micro Focus Vibe sites within a single physical Vibe site by setting up Vibe zones. Each Vibe zone is completely independent. Each zone has its own unique URL, and data files for each zone are stored in a separate subdirectory of the Vibe file repository, so that no searching across zones is possible.

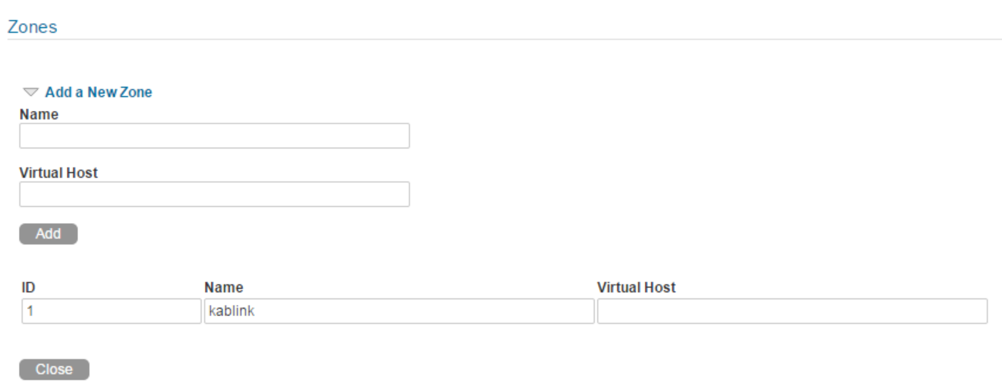
Creating a New Vibe Zone

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. Under **Management**, click **Zones**.



The default zone name is `kablink`. It represents your initial Vibe site, from which all other zones can be managed.

4. Click **Add a New Zone**, then fill in the fields.



Name: Specify a unique name to describe the zone. The name can include alphanumeric characters, periods, and underscores. Do not include spaces, extended characters, or double-byte characters.

Virtual Host: Specify the hostname for the zone. You can use any hostname that does not conflict with an existing hostname.

5 Click **Add**, then click **Close** to create the zone.

Configuring DNS to Support the New Zone

The new zone URL has the following format:

`http://`*`virtual_hostname`*`[:`*`port`*`]`

where *`virtual_hostname`* is the hostname or fully qualified domain name of the Micro Focus Vibe zone that you have set up in DNS.

All zones use the same port number as the physical Vibe site. If you have the Vibe site configured to listen on your browser default port, you do not need to include the port number in the zone URL. How you configure your Vibe site to listen on the browser default port varies by platform.

Linux:	See "Setting Up Port Forwarding" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*.
Windows:	Specify the desired port numbers when you run the Vibe Installation program, as described in "HTTP/HTTPS Ports" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

1 To perform an initial test of the Vibe zone, add the zone URL to the `hosts` file on your local workstation where you run your browser. The location of the `hosts` file and the format of the line to add vary by platform:

Linux	`/etc/hosts`			
		`ip_address` `172.16.5.18`	*`vibe_zone_url`* `www.myvibesite.com`	*`hostname`* `vibe1`
Windows	`C:\Windows\system32\drivers\etc\hosts`			
		`ip_address` `172.16.5.18`	*`vibe_zone_url`* `www.myvibesite.com`	

2 Specify the zone URL in your web browser.

`http://www.myvibesite.com`

3 Log in to the new zone by using the default administrator user name (`admin`) and password (`admin`).

From this, you can see that each zone has its own site administrator who has administrative rights only within that particular zone.

4 Immediately change the site administrator password to a secure password of your own choosing, as described in "Accessing Your Basic Vibe Site as the Site Administrator" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

5 After you can access the new zone successfully following the instructions in Step 1, have your network administrator make comparable changes to DNS so that the zone URL is recognized across your company or across the Internet as needed.

Accessing the New Zone

As with your original Micro Focus Vibe site, the Vibe administrator user name is `admin`, and the password is `admin`. For the security of the new zone, you should immediately change the zone's administrator password.

1. In your web browser, specify one of the following URLs, depending on whether or not you are using a secure SSL connection:

   `http://`*`zone_hostname`*
   `https://`*`zone_hostname`*

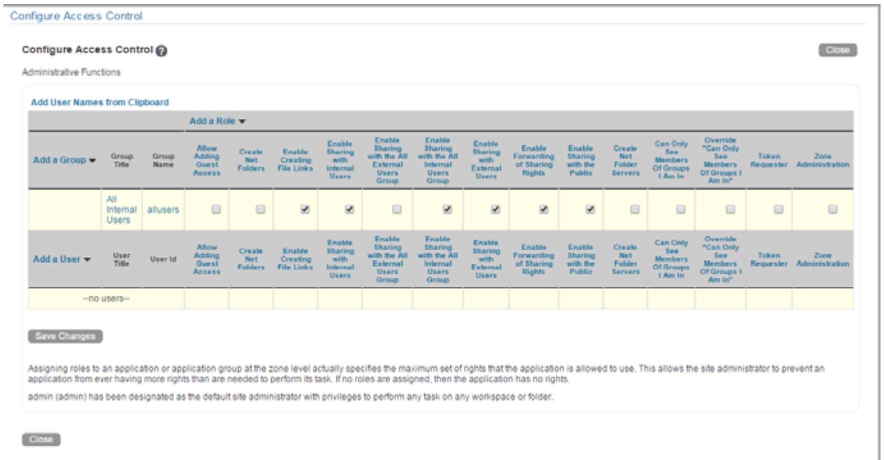
   Replace *`zone_hostname`* with the zone hostname or fully qualified domain name that you set up in DNS.
2. Log in using `admin` as the login name and `admin` as the password.
3. Change the default zone administrator password to a secure password:
   - **3a** Navigate to the personal workspace of the Vibe administrator.
   - **3b** Click **Profile**, then click **Edit** on the Profile page.
   - **3c** Specify a new password for the zone administrator in the **New Password** and **Confirm New Password** fields.
   - **3d** (Optional) Provide useful information in the additional fields of the zone administrator's profile.
   - **3e** Click **OK** to return to the zone administrator's profile.

IMPORTANT: The zone can only be administered by accessing the zone URL and by logging in through the zone administrator password. The zone cannot be administered from the main Vibe site, even when you are logged in as the main Vibe administrator.

Setting Up Access Control for the New Zone

After you log in to the zone as the zone administrator, you can set access controls for the zone.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. Under **System**, click **Access Control**.



4 (Conditional) If you want to have more than one zone administrator:

4a Click **Add a User**, start typing the user's name, then select the user from the drop-down list.

4b Select the check box in the **Zone Administration** column.

4c Click **Save Changes**.

5 (Optional) Add roles, as described in "Managing Roles to Refine Access Control" on page 31.

6 (Optional) Set other access controls for the zone, as described in "Controlling Access" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

20 Managing a Multiple-Language Vibe Site

Accommodating Multiple Languages

Understanding the Vibe Site Default Language

There can be only one default language for the entire Micro Focus Vibe site. You select the default language when you install Vibe, as described in "Accommodating Multiple Languages" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

When you create Vibe users, you can select a locale for each user, which determines the language of each personal workspace. However, when users who speak various languages work together on a Vibe site, they can often see interface text that is not in their preferred language. Examples include:

- Standardized text such as **Home Workspace**, **Global Workspaces**, **Personal Workspaces**, and **Team Workspaces** in the Workspace tree
- Standardized group names, such as All Users
- Login page

Although you cannot change standardized group names, such as All Users, you can rename the standardized workspaces to include multiple languages. Although the Vibe login page can be displayed in only one language, you can change the page's default language.You must be logged in as the Vibe administrator in order to perform these tasks.

Setting Up a Multilingual Workspace Name

1. Browse to the workspace.
2. Click the **Configure** icon ⚙ next to the workspace title, then click **Edit Workspace**.
3. In the **Title** field, add text in another language, then click **OK**.

Changing the Default Language on the Login Page

The language of the Vibe login page is decided by the Guest user account. Because of this, you can display only one language for your entire Vibe site in the login page.

To change the language of the Guest user account, and therefore change the language that is displayed on the Vibe login page:

1. Navigate to the Guest workspace.
2. On the Profile page click **Edit**.

   The User page is launched.
3. In the **Locale** drop-down list, select the language that you want to be displayed on your login page.

   Users who log in as Guest view the Vibe site in the language that you select.
4. Click **OK**.

Adding a New Language

- "Current Language Availability" on page 200
- "Text to Translate" on page 201
- "New Language Implementation" on page 201

Current Language Availability

Micro Focus Vibe is currently translated into 15 languages. Each language is identified by a language code in the Vibe software. Directory names and filenames include the language codes to identify the languages of directories and files.

- Chinese-Simplified (zh_TW)
- Chinese Traditional (zh_CN)
- Danish (da)
- Dutch (nl)
- English (en)
- French (fr)
- German (de)
- Hungarian (hu_HU)
- Italian (it)
- Japanese (ja)
- Polish (pl)
- Portuguese (pt_BR)
- Russian (ru_RU)
- Spanish (es)
- Swedish (sv)

Kablink Vibe is an open source project where additional languages can be contributed by interested members of the open source community.

Text to Translate

You can translate the software interface text and pop-up text.

The files that contain the text strings in the Vibe interface (`messages_`*`language_code`*`.properties`) and in mouse-over pop-ups (`help-messages_`*`language_code`*`.properties`) are located in the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/messages`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\messages`

1. Identify the file in the language that you want to translate from.
2. Identify the language code for the language that you want to translate into.

   Lists of standard language codes (http://en.wikipedia.org/wiki/Language_code) are available on the Internet.
3. Create a copy of the file that you want to translate, and name it with the appropriate language code.
4. Edit the file to translate in a text editor.

   Useful information for translators is provided at the top of each file (in English).
5. Locate the following line:

   ```
   Teaming.Lang=
   ```
6. Replace the existing language code with the language code for the language that you want to translate into.

   The lines in the file have the following format:

   `tag=string`
7. In each line, replace the text after the equal sign (=) with your translation for the string.
8. Save your translated file along with the other translated files.
9. Configure Vibe to recognize the new language, as described in "New Language Implementation" on page 201.

New Language Implementation

1. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes/config`
2. Make a backup copy of the `ssf-ext.properties` file, located in the same directory with the `ssf.properties` file.
3. Open the `ssf.properties` file in a text editor.
4. Locate the following line:

```
i18n.locale.support=en,da,de,es,fr,hu_HU,it,ja,nl,pl,pt_BR,ru_RU,sv,
                                                                zh_CN,zh_TW
```

5. Copy that line to the clipboard of your text editor.
6. Open the `ssf-ext.properties` file.
7. Scroll to the end of the `ssf-ext.properties` file, then paste the line you copied.
8. Type a comma (,) at the end of the line, followed by your language code.
9. Save and close the `ssf-ext.properties` file.
10. Close the `ssf.properties` file without saving it.
11. Stop and restart Vibe.

II Site Maintenance

21 Managing Users

As time passes on your Novell Vibe site, users come and go, resulting in the need for periodic maintenance activities.

Synchronizing Users and Groups from an LDAP Directory

Unless you are planning a very small Novell Vibe site, the most efficient way to create Vibe users is to synchronize initial user information from your network directory service (eDirectory, GroupWise, or Active Directory directory service) after you have installed the Vibe software. Over time, you can continue to synchronize user information from the LDAP directory to your Vibe site.

IMPORTANT: The following limitations apply when synchronizing user information to Vibe from an LDAP directory service:

- Vibe performs one-way synchronization from the LDAP directory to your Vibe site. If you change user information on the Vibe site, the changes are not synchronized back to your LDAP directory.
- If your LDAP directory contains a multi-value attribute, Vibe recognizes only one of the values. For example, if your LDAP directory contains multiple email addresses for a given user, only one of the email address is synchronized to Vibe.
- Users that are imported to Vibe via LDAP are always authenticated to Vibe via the LDAP source. If the LDAP source is unavailable for any reason, the LDAP-imported users cannot log in to Vibe.

For information about known issues with LDAP synchronization in Vibe, see "LDAP Synchronization Issues" in the *Micro Focus Vibe 4.0.5 Beta Release Notes*.

Table 21-1 shows user synchronization rates based on samples from test labs at Novell. Results may vary depending on hardware, LDAP server, database, and network topology.

Table 21-1 LDAP Synchronization Performance Rate Samples

Number of Users Synchronized	Time Required to Complete Synchronization
1,000	20 seconds
2,500	44 seconds
10,000	2 minutes
20,000	5 minutes
50,000	13 minutes

To synchronize users and groups from LDAP:

1 Log in to Vibe as the Vibe administrator.

1a Launch a web browser.

1b Specify one of the following URLs, depending on whether you are using a secure SSL connection:

```
http://vibe_hostname:8080
https://vibe_hostname:8443
```

Replace *vibe_hostname* with the host name or fully qualified domain name of the Vibe server that you have set up in DNS. If you configured the HTTP ports correctly during installation, you do not need to include the port number in the Vibe URL.

Depending on how you have configured your Vibe system, you might not be required to enter the port number in the URL. If you are using NetIQ Access Manager, the Vibe login screen is not used.

2 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

3 Under **System**, click **LDAP**.

Configuring an LDAP Connection

You can configure one or more LDAP connections to your directory.

You should never configure multiple LDAP connections to point to the same location on the same LDAP directory. If you need a failover solution, you should use a load balancer.

To configure an LDAP connection:

1 On the LDAP Configuration page, click the **LDAP Servers** tab.

2 To create a new LDAP connection, click **Add**.

or

To modify an existing LDAP connection, click the URL of the connection in the **Server URL** column of the provided table.

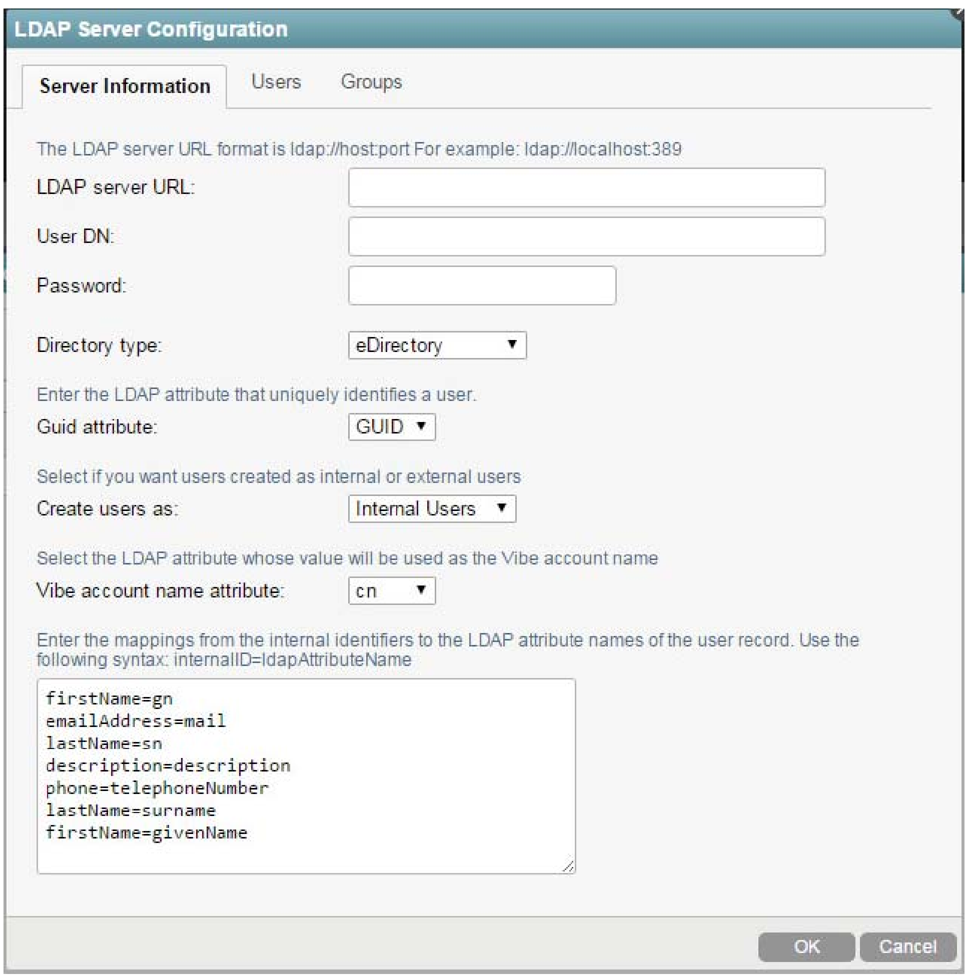
3 On the LDAP Server Configuration dialog box, specify the information on each tab, as described in the following sections:

- "Server Information" on page 207
- "Users" on page 210
- "Groups" on page 211

Server Information

1 On the **LDAP Servers** tab, click Add.

The LDAP Server Configuration dialog box is displayed.



2 Specify the following information on the **Server Information** tab:

IMPORTANT: When modifying an existing LDAP connection, do not modify the LDAP server URL. Doing so can lead to synchronized users being disabled or deleted.

LDAP Server URL: In order to synchronize initial user information, Vibe needs to access an LDAP server where your directory service is running. You need to provide the host name of the server, using a URL with the following format:

ldap://*hostname*

If the LDAP server requires a secure SSL connection, use the following format:

ldaps://*hostname*

If the LDAP server is configured with a default port number (389 for non-secure connections or 636 for secure SSL connections), you do not need to include the port number in the URL. If the LDAP server uses a different port number, use the following format for the LDAP URL:

ldap://*hostname*:*port_number*
ldaps://*hostname*:*port_number*

If the LDAP server requires a secure SSL connection, additional setup is required. You must complete the steps in "Securing LDAP Synchronization" on page 332 to import the root certificate for your LDAP directory into the Java keystore on the Vibe server before you configure Vibe for LDAP synchronization.

User DN (proxy user for synchronizing users and groups): Vibe needs the user name and password of a user on the LDAP server who has sufficient rights to access the user information stored there:

Directory Service	Required Rights
eDirectory	◆ [All Attribute Rights] - Compare & Read ◆ [Entry Rights] - Browse (on the container containing the users that need to be imported into Vibe)
Active Directory	Any authenticated user can be used as the proxy user as long as there are no read restrictions in place on the Organizational Unit (OU) that contains the users Required rights if OU read restrictions are in place: ◆ Read (on the Organizational Unit containing the users that need to be imported into Vibe) Ensure that **This object & all descendant objects** is selected in the **Security** tab under the advanced options.
GroupWise	GroupWise requires an Admin App user for this. See "Creating an Admin App in GroupWise" in the *GoupWise Mobility Service 2014 R2 Administration Guide.*

You need to provide the fully qualified, comma-delimited user name, along with its context in your LDAP directory tree, in the format expected by your directory service.

Directory Service	Format for the User Name
eDirectory	cn=*username*,ou=*organizational_unit*,o=*organization*
Active Directory	cn=*username*,ou=*organizational_unit*,dc=*domain_component*
GroupWise	cn=*admin_app_user*,o=*system_name*

Password: Password for the User DN.

Directory Type: The directory type that you are connecting to. Select **eDirectory**, **Active Directory**, or **GroupWise**.

GUID attribute: Depending on the directory type that you chose, this field is populated with the name of the LDAP attribute that uniquely identifies a user or group. For eDirectory, this value is `GUID`. For Active Directory, this value is `objectGUID`. For GroupWise, this value is `entryUUID`. This attribute always has a unique value that does not change when you rename or move a user in the LDAP directory. It ensures that Vibe modifies the existing user instead of creating a new user when the user is renamed or moved in the LDAP directory.

If this attribute is not set and you rename or move a user in the LDAP directory, Vibe assumes that the new name (or the new location of the same name) represents a new user, not a modified user, and creates a new Vibe user.

For example, suppose you have a Vibe user named William Jones. If William changes his name to Bill, and you make that change in the LDAP directory, Vibe creates a new user named Bill Jones.

If you want to map users to a different attribute, select **Other** in the drop-down list, specify the name of the LDAP attribute, then click **OK**. Before you do this, ensure that the attribute that you use is a binary attribute. For example, the cn attribute cannot be used because it is not a binary attribute.

Create Users As: Specify whether you want Vibe to treat the users as Internal or External. If you choose **External**, then the **Vibe Account Name** attribute will change from `cn` to `mail`. All external users use their email address as their login.

Vibe account name attribute: The attribute you choose here depends on the directory type you selected in the **Directory type** drop-down list. If you selected **eDirectory** in the **Directory type** drop-down list, you see **cn** and **Other** as options for this attribute. If you selected **GroupWise** in the **Directory type** drop-down list, you see only **cn** as an option for this attribute.If you selected **Active Directory** or **Other** in the **Directory type** drop-down list, you see **sAMAccountName**, **cn**, and **Other** as options for this attribute. If you select **Other** as the value for this attribute, you are prompted to enter the name of the LDAP attribute. The value of the attribute that you enter is used for the Vibe account name.

The Vibe account name attribute has two purposes:

- Used as the Vibe user name when the user is first provisioned from LDAP. The value of this attribute must be unique.
- During Vibe login, Vibe uses this attribute to locate the user in the LDAP directory and then tries to authenticate as that user.

LDAP directories differ in the LDAP attribute used to identify a User object. Both eDirectory and Active Directory might use the cn (common name) attribute. A more sure alternative for Active Directory is to use the sAMAccountName attribute. Other LDAP directories might use the uid (unique ID) attribute, depending on the structure and configuration of the directory tree.

You might need to consult with your directory administrator in order to determine which attribute is best to use. In some cases where not all users are imported successfully, you might need to set up two LDAP sources pointing to the same LDAP server and have each source use a different value for the **LDAP Attribute Used for Vibe Name**. For example, set up one LDAP source and use cn as the **Vibe account name attribute**. Then set up a separate source to the same LDAP server and use sAMAccountName as the **Vibe account name attribute**.

In addition to the attributes already mentioned in this section, other LDAP attributes can be used for the **Vibe account name attribute**, as long as the attribute is unique for each User object. For example, the mail LDAP attribute on User objects could be used to enable Vibe users to log in to the Vibe site by using their email addresses.

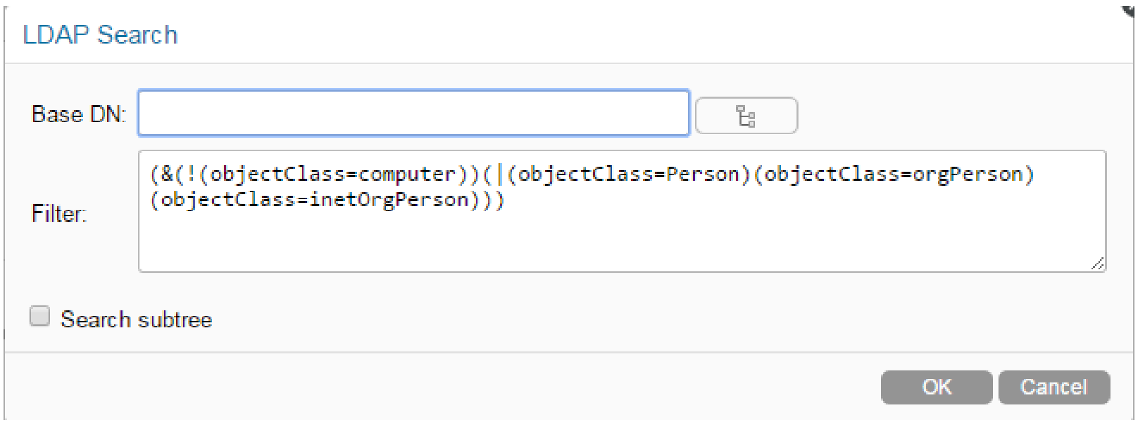
NOTE: Because the login name becomes part of the user's workspace URL, the at sign (@) in the email address is replaced with an underscore (_) in the workspace URL because @ is not a valid character in a URL.

3 Continue with "Users" on page 210.

Users

1 On the LDAP Server Configuration page, click the **Users** tab, then click **Add**.

The LDAP Search dialog box is displayed.



2 Specify the following information n the LDAP search dialog box:

Base DN: Vibe can find and synchronize initial user information from User objects located in one or more containers in the LDAP directory tree. A container under which User objects are located is called a base DN (distinguished name). The format you use to specify a base DN depends on your directory service.

Directory Service	Format for the User Container
eDirectory	`ou=`*organizational_unit*`,o=`*organization*
Active Directory	`ou=`*organizational_unit*`,dc=`*domain_component*
GroupWise	`cn=`*admin_app_user*`,o=`*system_name*

Container names cannot exceed 128 characters. If the container name exceeds 128 characters, users are not provisioned.

TIP: You can use the **Browse** icon  next to the **Base DN** field to browse the LDAP directory for the base DN that you want to use.

Filter: If you are using GroupWise, accept the default as is.

To identify potential Vibe users, Vibe by default filters on the following LDAP directory object attributes:

- `Person`
- `orgPerson`
- `inetOrgPerson`

You can add attributes to the user or group filter list if necessary. You can use the following operators in the filter:

- | OR (the default)
- & AND
- ! NOT

You might find it convenient to create a group that consists of all the users that you want to set up in Vibe, regardless of where they are located in your LDAP directory. After you create the group, you can use the following filter to search for User objects that have the specified group membership attribute:

IMPORTANT: If you create a filter to search for a specific group to find users, users that are located in any sub-groups to that group are not synchronized.

When synchronizing against Active Directory, you can create a filter that synchronizes users in sub-groups by using the following rule object identifier (OID):

```
<attribute name>:<matching rule OID>:=<value>
```

Be sure to include the parentheses in your filter.

Directory Service	Filter to search for User objects
eDirectory	(groupMembership=cn=*group_name*,ou=*organizational_unit*,o=*organization*)
Active Directory	(memberOf=cn=*group_name*,ou=*organizational_unit*,dc=*domain_component*)
GroupWise	Use the default.

Search subtree: Select whether you want Vibe to search for users in containers underneath the base DN (that is, in subtrees).

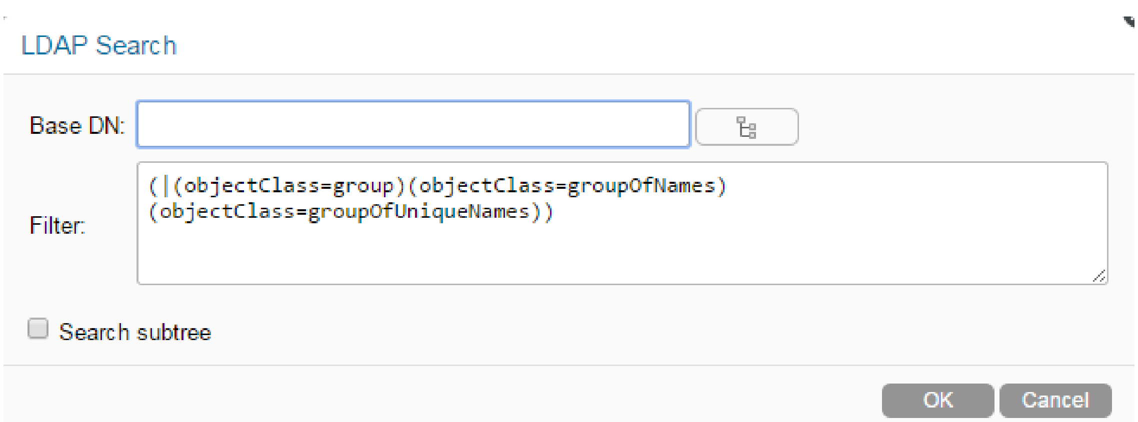
3 Click **OK**.

4 Continue with "Groups" on page 211.

Groups

1 On the LDAP Server Configuration page, click the **Groups** tab, then click **Add**.

The LDAP Search dialog box is displayed.



2 Specify the following information on the LDAP Search dialog box:

Base DN: Vibe can find and synchronize initial user information from group objects located in one or more containers in the LDAP directory tree. A container under which User objects are located is called a base DN (distinguished name). The format you use to specify a base DN depends on your directory service.

Directory Service	Format for the Group Container
eDirectory	`ou=organizational_unit,o=organization`
Active Directory	`ou=organizational_unit,dc=domain_component`
GroupWise	`cn=admin_app_user,o=system_name`

Container names cannot exceed 128 characters. If the container name exceeds 128 characters, users are not provisioned.

TIP: You can use the **Browse** icon  next to the **Base DN** field to browse the LDAP directory for the base DN that you want to use.

Filter: For GroupWise, use the default.

To import groups based on information in your LDAP directory, Vibe filters on the following LDAP directory object attributes:

- `group`
- `groupOfNames`
- `groupOfUniqueNames`

You can add attributes to the group filter list if necessary. You can use the following operators in the filter:

- | OR (the default)
- & AND
- ! NOT

IMPORTANT: Be sure to include the parentheses in your filter.

TIP: For information about how to import GroupWise distribution lists to be used in Vibe, see the following Cool Solutions article: "Using GroupWise Distribution Lists in Novell Vibe" (https://www.novell.com/communities/coolsolutions/using-groupwise-distribution-lists-novell-vibe/)

Directory Service	Filter to search for Group objects
eDirectory	`(groupMembership=cn=group_name,ou=organizational_unit,o=organization)`
Active Directory	`(memberOf=cn=group_name,ou=organizational_unit,dc=domain_component)`
GroupWise	Use the default.

Search subtree: Select whether you want Vibe to search for groups in containers beneath the base DN (that is, in subtrees).

3 Click **OK**, then click **OK** again to save the LDAP server configuration.

4 Continue with “Configuring LDAP Synchronization” on page 213.

Configuring LDAP Synchronization

When you configure LDAP synchronization, you configure user synchronization options, groups synchronization options, and the synchronization schedule.

NOTE: Because the synchronization options apply to all LDAP configurations within the same zone, you cannot have customized synchronization settings for each LDAP configuration. However, the Micro Focus Vibe site can have multiple zones. For more information about zones, see Chapter 19, “Setting Up Zones (Virtual Vibe Sites),” on page 195.

- “Configuring User Synchronization Options” on page 213
- “Configuring Group Synchronization Options” on page 214
- “Configuring the Synchronization Schedule” on page 215

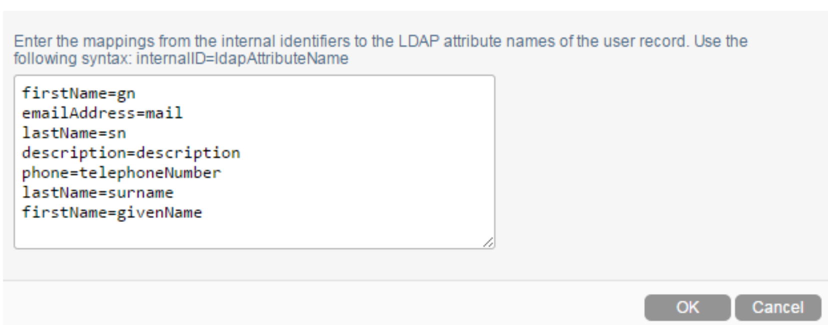
Configuring User Synchronization Options

1 On the LDAP Configuration page, click the **User Settings** tab.

2 Specify the following information for enabling and configuring user synchronization from your LDAP directory to your Vibe site:

Register LDAP user profiles automatically: Select this option to automatically add LDAP users to the Vibe site. However, workspaces are not created until users log in to the Vibe site for the first time.

Synchronize user profiles: Select this option to synchronize user information whenever the LDAP directory information changes after initial Vibe site setup. The attributes that are synchronized are the attributes that are found in the map box on the **Server Information** tab on the LDAP Server Configuration page.



By default, Vibe synchronizes the following attributes from the LDAP directory:

- First name
- Last name
- Phone number
- Email address
- Description

For information about how to add additional attributes to be automatically synchronized, see “Synchronizing Additional LDAP Attributes” on page 216.

For user accounts provisioned from LDAP that are no longer in LDAP: Because deleting user accounts cannot be undone, Novell recommends that you leave **Disable account** selected.

For more information about disabled users in Vibe, see "Disabling Vibe User Accounts" on page 224.

Select **Delete account** only if you are certain that you want to delete users that exist on the Vibe site but do not exist in your LDAP directory. If you do decide to delete user accounts, you can select the option **Also delete associated user workspaces and content** to remove obsolete information along with the user accounts.

IMPORTANT: A deleted user cannot be undeleted; deleting a user is permanent and is not reversible.

If you are sure that you want to automatically delete users that are not in LDAP, this option is designed to be used under the following conditions:

- You have deleted users from your LDAP directory and you want the LDAP synchronization process to also delete them from Vibe.
- In addition to the users synchronized from LDAP, you create some Vibe users manually, as described in "Creating a New Local User" on page 220, and you want the LDAP synchronization process to delete the manually created users.
- In addition to the users synchronized from LDAP, you allow Guest users to self-register, as described in ""Allowing Guest Access to Your Vibe Site" on page 104," and you want the LDAP synchronization process to delete the self-registered users.

Use the following time zone when creating new users: Select this option to set the time zone for user accounts that are synchronized from the LDAP directory into your Vibe site. The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city.

Common selections for United States time zones:

Time Zone	Continent/City
Pacific Time	America/Los Angeles
Mountain Time	America/Denver
Central Time	America/Chicago
Eastern Time	America/New York

Use the following locale when creating new users: Select this option to set the locale for user accounts that are synchronized from the LDAP directory into your Vibe site. The locale list is sorted alphabetically by language.

3. Continue with "Configuring Group Synchronization Options" on page 214.

Configuring Group Synchronization Options

1. On the LDAP Configuration page, click the **Group Settings** tab.
2. Specify the following information for enabling and configuring user and group synchronization from your LDAP directory to your Vibe site:

   Register LDAP group profiles automatically: Select this option to automatically add LDAP groups to the Vibe site.

   Synchronize group profiles: Select this option to synchronize group information, such as the group description, to the Vibe site whenever this information changes in LDAP.

Synchronize group membership: Select this option so that the Vibe group includes the same users (and possibly groups) as the group in your LDAP directory. If you do not select this option, and you make changes to group membership in the LDAP directory, the changes are not reflected on your Vibe site.

If users have rights to files on your OES or Windows file systems through group membership, you must select this option to synchronize group membership to Vibe. If you do not synchronize group membership, users who have access rights to files through membership in a group might not have the appropriate access rights in Vibe.

Delete groups that were provisioned in LDAP but are no longer in LDAP: Select this option to delete groups that exist on the Vibe site but do not exist in your LDAP directory. Use this option under the following conditions:

- You have deleted groups from your LDAP directory and you want the LDAP synchronization process to delete them from Vibe as well.
- In addition to the groups synchronized from LDAP, you create some Vibe groups manually, as described in "Creating Groups of Users" on page 97, and you want the LDAP synchronization process to delete the manually created groups.

3 Continue with "Configuring the Synchronization Schedule" on page 215.

Configuring the Synchronization Schedule

This section describes how to set a schedule for the LDAP synchronization.

When planning the schedule, take into account how often your LDAP directory user (and, optionally, group) information changes and the server resources required to perform the synchronization for the number of users (and, optionally, groups) that you have.

1. On the LDAP Configuration page, click the **Synchronization Schedule** tab.
2. Select **Enable schedule** to enable a schedule for the LDAP synchronization to occur.
3. Select whether to run the LDAP synchronization every day, or select specific days of the week when you want it run (for example, on Monday, Wednesday, and Friday).

   You can choose to have it run once a day at a specified time (for example, at 2:00 a.m.), or you can set a time interval, so that it is run multiple times each day (for example, every four hours). The smallest time interval you can set is .25 hours (every 15 minutes).
4. (Conditional) If you want to restrict local users from logging in to the Vibe site, continue with "Restricting Local User Accounts from Logging In" on page 215.
5. Continue with "Previewing and Running the LDAP Synchronization" on page 218.

Restricting Local User Accounts from Logging In

By default, Vibe allows locally created users to log in the Vibe site. This section describes how to configure Vibe to allow only users that are synchronized via LDAP to log in.

1. On the LDAP Configuration page, click the **Local User Accounts** tab.
2. Leave **Allow log in for local user accounts (i.e. user accounts not in LDAP)** to allow users who you have created locally to log in to the Vibe site.

   For more information about creating users, see "Creating a New Local User" on page 220.
3. Continue with "Previewing and Running the LDAP Synchronization" on page 218.

Synchronizing Additional LDAP Attributes

By default, Vibe synchronizes the following attributes from the LDAP directory:

- First name
- Last name
- Phone number
- Email address
- Description

This information displays on each user's personal user profile.

To synchronize additional LDAP attributes, complete the following sections:

- "Identifying or Creating a Vibe Field for the LDAP Attribute" on page 216
- "Copying the Data Name of the Vibe Field" on page 216
- "Mapping the Vibe Field to the LDAP Attribute" on page 217

Identifying or Creating a Vibe Field for the LDAP Attribute

Before you can synchronize Vibe user profiles with additional attributes from your LDAP directory, you first need to ensure that there is a corresponding Vibe field for the LDAP attribute that you want to synchronize.

To view the existing fields in the user profile:

1. Navigate to a user profile and see if there is an existing field that corresponds to the LDAP attribute that you want to synchronize.
2. If the appropriate field already exists, continue with "Copying the Data Name of the Vibe Field" on page 216.

   If the appropriate field doesn't already exist, you must create it, as described in "Customizing the Default User Profile View" on page 50.

Copying the Data Name of the Vibe Field

Each field in Vibe has an internal data name, which is added when the field is created. When you create a field by using the Form and View Designers tool, Vibe requires that you enter a data name. This name is how Vibe identifies the field.

To map an LDAP attribute to a Vibe field, you must find the data name for the field.

The following procedure shows how to find the data name for a particular field in the user profile:

1. Log in to the Vibe site as the Vibe administrator.
2. Click the **Administrator** link in the upper right corner of the page, then click the **Administration Console** icon.
3. In the **System** section, click **Form/View Designers**.
4. Expand **Profile View**, then click **User**.
5. Expand **Profile Form Definition**, expand **Form**, then locate the Vibe field that you want to synchronize with an LDAP attribute.

6 Click the name of the field, then click **Modify** in the dialog box on the right side of the page.

7 Copy the text in the **Data Name** field, then continue with "Mapping the Vibe Field to the LDAP Attribute" on page 217.

Mapping the Vibe Field to the LDAP Attribute

After you have copied the data name of the Vibe field that you want to synchronize with an LDAP attribute as described in "Copying the Data Name of the Vibe Field" on page 216, you can map the Vibe field to the LDAP attribute that you want to synchronize.

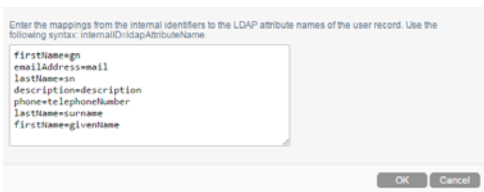
1 Log in to the Vibe site as the Vibe administrator.

2 Click the **Administrator** link in the upper right corner of the page, then click the **Administration Console** icon.

   The Administration page is displayed.

3 In the **System** section, click **Configure LDAP**.

   The map box in the **Users** section lists the LDAP attributes that are currently being synchronized.



   The items in the list have the following format:

   vibe_field_name=ldap_attribute_name

4 Add a new line to the list, specifying the Vibe field name to the left of the equal sign (=) and the LDAP attribute name to the right of the equal sign.

   The *vibe_field_name* is the data name that you copied in "Copying the Data Name of the Vibe Field" on page 216, and *ldap_attribute_name* is the name of the LDAP attribute in your LDAP directory.

5 Repeat Step 4 for each LDAP attribute that you want to add to the user profile.

6 Select **Run Immediately**, then click **Apply**.

   The status box shows the LDAP attribute information being added to Vibe users.

Allowing Users to Log In When the LDAP Server is Down

You can configure the Vibe server to allow users who are being synchronized through LDAP to still have access to the Vibe server when the LDAP server is down.

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
portal.password.auto.synchronize=false
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the portal.password.auto.synchronize=false line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `false` to `true`, so that the line now reads `portal.password.auto.synchronize=true`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe to enable users to log in to the Vibe site when the LDAP server is down.

Previewing and Running the LDAP Synchronization

Before you run the LDAP synchronization, it is a good idea to preview the synchronization so that you are aware what changes will occur when you run the live synchronization.

- "Previewing LDAP Synchronization" on page 218
- "Running the LDAP Synchronization" on page 218

Previewing LDAP Synchronization

After you have configured the LDAP connection, you can see a preview of what the synchronization results will be. This allows you to see beforehand the users and groups that will be added or deleted, as well as the users that will be disabled, before you run the actual synchronization.

To preview the LDAP synchronization:

1 On the LDAP Configuration page, click the **LDAP Servers** tab, then click **Preview sync**.

Users and groups that will be modified by running the LDAP sync are shown, along with information about how they will be modified (whether they will be added, modified, deleted, or disabled).

2 (Optional) Specify a user or group in the **Filter List** field to filter the list of users and groups to be synchronized.

or

Click the drop-down arrow next to the **Filter List** field, then select the type of users or groups that you want to display, then click **OK**. (For example, select to display added users, modified users, modified groups, and so forth.)

3 After you review the results of the synchronization, click **Close**, then continue with "Running the LDAP Synchronization" on page 218.

Running the LDAP Synchronization

After you have run the preview of the LDAP synchronization (as described in "Running the LDAP Synchronization" on page 218), you are ready to run the live synchronization.

1 On the LDAP Configuration page, click the **LDAP Servers** tab, then click **Sync All**.

Users and groups that have been modified by running the LDAP sync are shown, along with information about how they have been modified (whether they were added, modified, deleted, or disabled).

2 (Optional) Specify a user or group in the **Filter List** field to filter the list of users and groups to be synchronized.

   or

   Click the drop-down arrow next to the Filter List field, then select the type of users or groups that you want to display. (For example, select to display added users, modified users, modified groups, and so forth.)

3 Click **Close**.

Viewing Synchronization Results

You can view the synchronization results of the most recent LDAP synchronization for the current browser session. If you perform a synchronization, log out of Vibe, and then log in again, you cannot view the results of the LDAP synchronization for your previous session.

To view the results for a previous synchronization:

1 On the LDAP Configuration page, click the **LDAP Servers** tab.

2 Click **Show sync results**.

Deleting an LDAP Configuration

IMPORTANT: If you delete an LDAP configuration and you have selected the option to delete user accounts that are provisioned from LDAP that are no longer in LDAP, all users that were synchronized to the Vibe site through that LDAP configuration are deleted from the Vibe site. (For more information about the configuration option concerning user accounts provisioned from LDAP, see "Configuring User Synchronization Options" on page 213.)

---

1 On the LDAP Configuration page, click the **LDAP Servers** tab.

2 Select the LDAP configuration that you want to delete, then click **Delete**.

Setting a Default Time and Locale for Non-LDAP and External Users

Path to Configuration Dialog: **Vibe Administration Console > Management > Default User Settings**

By default, the locale setting for newly created local users is English (US) and the time zone is set to Greenwich Mean Time (GMT).

This dialog lets you change the defaults for newly created local users.

You specify the default locale and time zone for LDAP users when you configure LDAP synchronization.

Creating a New Local User

You can manually create users on the Vibe site, rather than synchronizing user information from an LDAP directory. Users created in this way are local users, and are not added to your LDAP directory. Local users are not authenticated through NetIQ Access Manager when Access Manager is fronting the Vibe system.

You can create local users from the Administration Console:

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, and then click the **Administration Console** icon.
3. In the **Management** section, click **Users**.
4. Click **New**.

   The User page is displayed.
5. Provide the user's information in the User page, then click **OK**.

Listing Vibe Users

On the Novell Vibe site, you can view a comprehensive list of all the Vibe users.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. In the **Management** section, click **Users**.

   All users in the Vibe site are displayed.

You can use this page in the following ways:

- "Filtering Users" on page 220
- "Navigating to a User's Individual Workspace" on page 221
- "Adding Local Users" on page 221

Filtering Users

You can filter the user list in the following ways: by specifying a name in the **Filter List** field in the upper-right corner.

- Specify a name in the **Filter List** field in the upper-right corner, then press Enter.
- Click the drop-down arrow next to the **Filter List** field, then select from the following options (by default, all options are selected):
  - **Show Internal Users:** Shows internal Vibe users.
  - **Show External Users:** Shows external Vibe users.
  - **Show Disabled Users:** Shows users that have been disabled.
  - **Show Enabled Users:** Shows users that are enabled.
  - **Show Administrators:** Shows users that have Administrative rights.

* **Show Users That Are Not Administrators:** Shows users that do not have Administrative rights.

Navigating to a User's Individual Workspace

You can use the user list to navigate to a user's individual workspace.

1 In the user list, in the **Full Name** column, click the name of the user whose workspace you want to navigate to, then click **Workspace**.

If you have deleted a user workspace but have not yet purged the workspace, the user workspace is still displayed in the user list, but you are unable to navigate to the workspace.

If you want the user workspace to be removed from the user list, you must purge the workspace, as described in "Making Disk Space Available by Deleting Items from the Trash" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

If you want to restore the workspace, see "Restoring Items from the Trash" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Adding Local Users

A local user is a Vibe user who is not added to your LDAP directory. You can use the Users page to add new local users to your Vibe site.

For information about how to add local users, see "Creating a New Local User" on page 220.

Modifying a User's Profile Information

You can modify the following information in a user's profile directly from Vibe, unless the information is being synchronized from an external directory via LDAP:

* Password
* Name
* Email addresses
* Time zone
* Locale
* Personal information, including job title, state, and postal code
* Contact information, including phone numbers
* Organization information, including department and manager
* Job responsibilities
* Profile picture

To modify a user's profile information:

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 In the **Management** section, click **Users**.

All users in the Vibe site are displayed.

4 Click the name of the user whose profile information you want to change.

5 If the user has logged in to the Vibe site at least one time, click **Profile**.

or

If the user has never logged in to the Vibe site, click **Modify**.

6 Modify the user's profile information as desired, then click **OK**.

Renaming a Vibe User

Novell Vibe users are identified by name (first, middle, last) and by user ID. User names are used to identify personal workspaces. User IDs are used for logging in. You can change users' names, but not their user IDs. How you change users' name depends on how you created the user.

- "Renaming a Vibe User from LDAP" on page 222
- "Renaming a Local Vibe User" on page 222

Renaming a Vibe User from LDAP

If you are synchronizing user information from an LDAP directory, as described in "Adding Vibe Users from Your LDAP Directory" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*, you change a user's first, middle, or last name by updating it in the LDAP directory. The updated information then synchronizes to the Vibe site according to the schedule you have established for LDAP synchronization. If you change a user's first, middle, or last name by updating information on the Vibe site, the change is not synchronized back to the LDAP directory, so the two sources of user information can be out of sync.

Renaming a Local Vibe User

If you manually create Vibe users on the Vibe site, rather than synchronizing user information from an LDAP directory, you can change users' names (first, middle, last) on the Vibe site.

When a user logs in to the Vibe site for the first time, the user's personal workspace is created. Before a user logs in, he or she does not have a personal workspace. Vibe enables site administrators to manually rename both types of users.

NOTE: Vibe does not allow you to change a user ID after the user account has been created.

To rename a local Vibe user:

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 In the **Management** section, click **Users**.

All users in the Vibe site are displayed.

4 Click the name of the user who you want to rename.

5 If the user has logged in to the Vibe site at least one time, click **Profile**.

or

If the user has never logged in to the Vibe site, click **Modify**.

6 Modify the **First Name**, **Middle Name**, and **Last Name** fields as desired.

7 Click **OK**.

Deleting a Vibe User

When users no longer need access to your Novell Vibe site, you have two options to revoke their access to the Vibe site: disabling or deleting their Vibe user accounts.

IMPORTANT: Novell recommends that you disable user accounts instead of deleting them. When you delete a user account, the account can never be re-activated. If there is the slightest possibility that the user might return to your Vibe site, disable the user account rather than deleting it. Disabled accounts do not count as a licensed user. For information on how to disable a user, see "Disabling Vibe User Accounts" on page 224.

When you delete a user, the following user information is deleted and cannot be recovered:

- All profile information, including profile pictures
- Access controls to workspaces and folders

Entries and information that the user contributed are preserved even after the user is deleted.

How you delete a user depends on how you originally created the user.

Deleting a Local User

Any user account that has been created manually (not created by the LDAP synchronization process) can be deleted as described in this section. To delete a user account that was created by the LDAP synchronization process, see "Deleting an LDAP User" on page 224.

IMPORTANT: If you delete user accounts that were created by the LDAP synchronization process without following the instructions in "Deleting an LDAP User" on page 224, new users with the same name are created the next time the users log in or the next time the LDAP synchronization occurs.

---

1. Log in to Vibe as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. In the **Management** section, click **Users**.
4. Select the users whose accounts you want to delete, then click **Delete**.

   The Delete Users dialog box is displayed.
5. Select **Move user workspaces to trash** if you want the workspaces to be recoverable.

   or

   Select **Delete user workspaces** to permanently delete the workspaces. You then have an additional option to **Delete user object**.

   The first option deletes only the user's personal workspace. The user account remains on the system, and the user can still log in, create a new workspace, and so on.

   The second option also removes the user account from the system, so that the user no longer exists on the system, can't log in, and so on.
6. Click **OK**.

Deleting an LDAP User

User accounts can be synchronized to the Vibe site with an LDAP directory. While you can delete Vibe user accounts, Novell recommends that you disable them, as described in "Disabling Vibe User Accounts" on page 224.

If you decide to delete Vibe user accounts, it is safer to manually delete them rather than deleting them through the LDAP synchronization process.

- "Manually Deleting User Accounts That Are Being Synchronized through LDAP" on page 224
- "Configuring LDAP to Automatically Delete User Accounts" on page 224

Manually Deleting User Accounts That Are Being Synchronized through LDAP

Following is the preferred method for deleting user accounts from the Vibe site that are being synchronized from an LDAP directory:

1. In your LDAP directory, modify the User objects that you want to delete from the Vibe site so that the User objects no longer match the LDAP synchronization criteria that you previously set.

   For information about setting LDAP synchronization criteria, see "Synchronizing Users and Groups from an LDAP Directory" on page 205.
2. In Vibe, manually delete the user accounts, as described in "Deleting a Local User" on page 223.

   Because user accounts that are deleted cannot be recovered, you should make sure you know exactly which users you are deleting, and the only way to be sure is by manually deleting them.

Configuring LDAP to Automatically Delete User Accounts

IMPORTANT: While it is possible to configure LDAP synchronization to automatically delete Vibe users and workspaces, this should be avoided because it might result in unwanted deletion of users. For example, if the LDAP context is entered incorrectly and none of the users match the incorrect LDAP context, all of the users would be permanently deleted.

For more information about how to configure the LDAP synchronization to automatically delete Vibe users and workspaces, see "Configuring LDAP Synchronization" on page 213.

Disabling Vibe User Accounts

Novell recommends that you disable user accounts instead of deleting them. When you delete a user account, the account can never be re-activated. If there is the slightest possibility that the user might return to your Vibe site, disable the user account rather than delete it. Disabled accounts do not count as a licensed user.

This section describes how to disable local user accounts as well as accounts that are being synchronized with an LDAP directory.

To disable user accounts:

1. Log in to Vibe as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 In the **Management** section, click **Users**.
4 Select the users whose accounts you want to disable, then click **More** > **Disable User Account**.

   The user accounts are disabled

To re-enable user accounts:

1 Log in to Vibe as the Vibe administrator.
2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3 In the **Management** section, click **Users**.
4 Select the users whose accounts you want to re-enable, then click **More** > **Enable User Account**.

   The user accounts are enabled

Limiting User Visibility

Path to Configuration Page: Vibe Administration Console > **Management** > **Limit User Visibility**

By default, each Vibe user can see all other Vibe users on the site.

Vibe lets you restrict the users that appear in Vibe dialogs and so on, to only those within groups to which a user belongs.

For additional information and instructions on limiting user visibility, see “Restricting Groups of Users from Seeing One Another” on page 103.

- “Creating User Visibility Limitations” on page 225

Creating User Visibility Limitations

For administrative efficiency and as a best practice, user-visibility limitations are usually applied to one or more groups.

Most organization choose to limit visibility at the group level and then manage exceptions by creating overrides for individual users. However, limitations can be applied to individual users if needed.

1 Identify the groups whose users require and/or will benefit from having user-visibility limitations set.
2 Identify group users who will need to be able to collaborate and share on a system-wide basis and will therefore need overrides.
3 Log in as an administrator, open the Vibe Administration Console > **Management** > **Limit User Visibility**.
4 Use the **Add Limitation** button to add user-visibility limitations to the groups (or users) identified.
5 Use the **Add Override** as needed.
6 If you need to remove a limitation, select the line to be removed and use the **Remove Visibility Settings** button to remove the setting from the list.

Managing Local Users and Groups by Importing Profile Files

You can manage local users and groups by importing profile files that contain user or group information in XML format. This is a good way to simultaneously perform multiple actions when you are not using LDAP.

You can perform the following actions:

- Create or modify users
- Delete users
- Create or modify groups

To manage local users and groups by importing profile files:

1. Log in to Vibe as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. In the **Management** section, click **Users**.
4. Click the **Import Profiles** tab.
5. Click **Choose File**, then navigate to and select the file that contains user or group profile information in XML format.

   Ensure that the format of your file matches the format that is shown in the provided sample file. To view the provided sample file, click **View a Sample File** in the **Import Files** tab.
6. Click **OK**.

Enabling Users to Bypass the XSS Security Filter

Cross-site scripting (XSS) is a client-side computer attack that is aimed at web applications. Because XSS attacks can pose a major security threat, Novell Vibe contains a built-in security filter that protects against XSS vulnerabilities. This security filter is enabled by default.

The XSS security filter protects the Vibe site from XSS in two key areas:

- Text and HTML fields in entries and folders
- Uploaded HTML files

Specific users might need to add some of the content described in "Understanding What Content Is Not Permitted" on page 355. If you trust these users, you can enable them to bypass the XSS security filter by adding JavaScript and other restricted content.

IMPORTANT: We do not recommend that you turn off the XSS security filter for the entire site. For more information about keeping your Vibe site secure from XSS, see "Securing the Vibe Site against XSS" on page 355.

Enabling a group to bypass the XSS filter is more efficient than enabling individual users because it requires you to modify the configuration file only once, when you initially authorize the group. After the initial setup, you can easily modify group membership.

- "Enabling Groups to Bypass the XSS Security Filter" on page 227
- "Enabling Individual Users to Bypass the XSS Security Filter" on page 227

Enabling Groups to Bypass the XSS Security Filter

The most efficient way to enable users to bypass the XSS security filter is to set up a group in Vibe, add users to this group who you trust, then authorize this group to bypass the XSS security filter. Only group members have the authority to bypass the XSS security filter.

1 Create a group in Vibe and add only users who you trust to this group.

   Members of this group will be allowed to bypass the XSS security filter.

   For information on how to create a group and add users to the group, see "Creating Groups of Users" on page 97.

2 On the Vibe server, change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

3 Open the `zone-ext.cfg.xml` file in a text editor.

4 Add the following information to the `xml` file, inside the `<zoneConfiguration>` tags:

```
<zone name="kablink">
 <xssConfiguration>
  <trustedGroups>
   <group name="trusted"/>
  </trustedGroups>
 </xssConfiguration>
</zone>
```

   The `group name` value should contain the group ID for the group you want to be able to upload HTML files to the Vibe site.

   If your Vibe system began as Teaming version 1, the `zone name` value is `liferay.com` instead of `kablink`

5 Stop and restart Vibe.

Enabling Individual Users to Bypass the XSS Security Filter

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Open the `zone-ext.cfg.xml` file in a text editor.

3 Add the following information to the `xml` file, inside the `<zoneConfiguration>` tags:

```
<zone name="kablink">
 <xssConfiguration>
  <trustedUsers>
   <user name="jchavez"/>
  </trustedUsers>
 </xssConfiguration>
</zone>
```

The `user name` value should contain the user ID for the user you want to be able to upload HTML files to the Vibe site.

If your Vibe system began as Teaming version 1, the `zone name` value is `liferay.com` instead of `kablink`

To enable multiple users to add HTML content to the Vibe site, create a group and enable the group to add content, as described in "Enabling Groups to Bypass the XSS Security Filter" on page 227. Or, you can enable multiple users on an individual basis by using multiple `<user name>` elements. For example:

```
<user name="jchavez"/>
<user name="ahall"/>
<user name="cjones"/>
```

4 Stop and restart Vibe.

22 Managing Groups

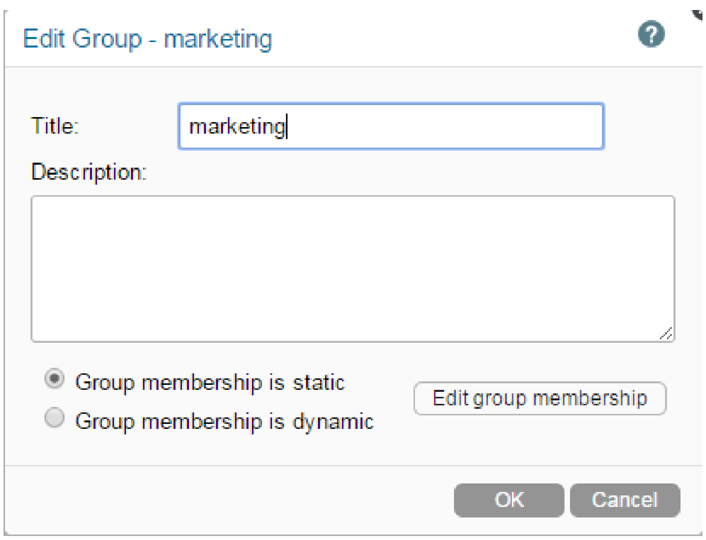
Group creating and maintenance is an useful way to manage users throughout your Vibe site. For more information about why it is important to create groups, see "Creating Groups of Users" on page 97.

Creating Groups

For information on how to create groups, see "Creating Groups of Users" on page 97.

Modifying Groups

1 Log in to the Vibe site as the Vibe administrator.
2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3 Under **Management**, click **Groups**.
4 Click the name of the group that you want to modify.



5 Modify the title, description, and group membership, then click **OK**.

For more information about editing static and dynamic group membership, see "Creating Groups of Users" on page 97.

Deleting Groups

1 Log in to the Vibe site as the Vibe administrator.
2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3 Under **Management**, click **Groups**.
4 Select the group that you want to delete, then click **Delete**.

23 Managing Workspaces

As an administrator for Novell Vibe, you can perform management functions on all Vibe workspaces. For information on how to perform general workspace management functions, such as creating a workspace, deleting a workspace, moving a workspace, and so forth, see "General Workspace Management" in the *Micro Focus Vibe 4.0.5 User Guide*.

You can perform additional workspace management tasks as the Vibe administrator:

- "Exporting/Importing Workspaces, Folders, and Entries" on page 231
- "Managing Workspace Disk Space Usage" on page 237
- "Modifying the Title, Description, and Branding of the Personal Workspaces Workspace" on page 237

Exporting/Importing Workspaces, Folders, and Entries

You can transfer data from one Novell Vibe site to another by exporting it from the source Vibe site and importing it into the destination Vibe site. When you export data, it remains in the source Vibe site and a copy of the exported data is imported into the destination Vibe site.

A user has to be a Vibe administrator in order to export and import workspaces, folders, and entries.

- "Understanding the Export and Import Process" on page 231
- "Exporting Workspaces" on page 234
- "Importing Workspaces" on page 234
- "Exporting Folders" on page 235
- "Importing Folders" on page 235
- "Exporting Folder Entries" on page 236
- "Importing Folder Entries" on page 236

If you want to simply move or copy data within a single Vibe site, see "Copying a Workspace" and "Moving a Workspace", "Copying a Folder" and "Moving a Folder", or "Copying a Folder Entry" and "Moving a Folder Entry" in the *Micro Focus Vibe 4.0.5 User Guide*.

Understanding the Export and Import Process

The export process creates a `.zip` file named `export.zip` that you can save to any convenient location on disk. The `.zip` file contains all the workspaces, folders, folder entries, and attachments that you elected to export.

When you export and import a workspace, folder, or folder entry, not all types of data are preserved.

- "Data That Is Preserved" on page 232
- "Data That Is Not Preserved" on page 233

Data That Is Preserved

- Hierarchical structure of the workspace

  If you are selecting specific folders within the workspace to export, the hierarchical structure to the selected folders must be preserved. For example, if you select to export a sub-folder but not the parent folder, the parent folder is also included in the export as a blank folder in order to keep the structure.
- All folders in the workspace (unless they are specifically excluded)
- All content in exported folders
- Access control information

  User and group IDs are also preserved and are matched to the same users and groups if they exist on the Vibe system where the workspace, folder, or entry is imported.

  Access control settings are not preserved if the workspace, folder, or entry is inheriting its access control settings from the parent folder or workspace in the original Vibe system. When you import a workspace, folder, or entry that is inheriting its access control settings, the workspace, folder, or entry assumes the access control settings of the higher-level workspace or folder where it is being imported. For more information on access control, see Chapter 2, "Planning and Controlling User Access to Workspaces and Folders," on page 21.
- Landing pages for workspaces or folders

  For more information on landing pages, see "Creating and Managing Landing Pages" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- Entry definitions associated with any folder content

  Entry definitions are custom entry forms that have been created in your folder or workspace. Entry definitions that are being used in any exported content are preserved, even if the definition is saved at a higher level in the workspace hierarchy. For more information on entry definitions, see "Designing Custom Folder Entry Forms" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- Workflows associated with any workspace content

  Workflows that are being used in any exported content are preserved, even if the workflow is saved at a higher level in the workspace hierarchy.

  NOTE: If your workflow contains an On Entry condition that starts a parallel workflow thread, as described in "Adding On-Entry or On-Exit Events" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*, the parallel workflow is automatically restarted when the workflow is imported.

  For more information on workflows, see "Creating and Managing Workflows" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- Custom forms associated with any workspace content

  Custom forms that are being used in any exported content are preserved, even if the custom form is saved at a higher level in the workspace hierarchy.For more information on custom forms, see "Designing Custom Folder Entry Forms" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- Wiki links

  For more information on wiki links, see "Linking to a Folder or Folder Entry" in the *Micro Focus Vibe 4.0.5 User Guide*.

- Content in Mirrored Files folders

  When you export a Mirrored Files folder, the files from the mirrored folder are written in the export file. However, when the folder is imported, the resulting folder becomes a Vibe library folder where all the files are added as regular file entries that are no longer mirrored. There is no way to export a mirrored folder and import it back into Vibe as a mirrored folder.

Data That Is Not Preserved

The following types of data are not included in the export and import processes:

- Profile information for user workspaces

  When a user workspace is exported and imported, the profile information for the user is not preserved. To move user workspaces from one Vibe site to another, add users to the target Vibe server in one of the ways described in "Adding New Users to Your Vibe Site" on page 97. You can then export the folders within the workspace from the source Vibe site, then re-import the folders into the target Vibe site to the user workspace for each appropriate user.
- Accessories

  For more information on accessories, see "Managing Accessories" in the *Micro Focus Vibe 4.0.5 User Guide*.
- Custom JSP files

  Custom JSP files must be exported as part of an extension. (For more information on extensions, see Chapter 16, "Adding Software Extensions to Your Vibe Site," on page 179.) However, if you have a workspace that leverages custom JSP files, the workspace still retains the settings that point to the custom JSP files. Therefore, if you export a workspace or folder that is referencing custom JSP files, and the Vibe site where you import the workspace has the same custom JSP files, the imported workspace or folder points to the correct custom JSP files.
- Permalinks

  Entries that are exported receive new permalinks when they are imported. However, if an entry description contains a permalink to another entry that was also imported, then the permalink is preserved.
- Activity data, such as who visited the place, edit history, and workflow history

  For more information about activity data, see "Generating Activity Reports for a Workspace", "Generating an Activity Report on a Folder", and "Generating Reports about a Folder Entry" in the *Micro Focus Vibe 4.0.5 User Guide*.
- Entry ratings

  For more information on entry ratings, see "Rating a Folder Entry" in the *Micro Focus Vibe 4.0.5 User Guide*.
- Entry definitions that are not associated with folder content

  Entry definitions are custom entry forms that have been created in your folder or workspace. For more information on entry definitions, see "Designing Custom Folder Entry Forms" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- Workflows that are not associated with workspace content

  For more information on workflows, see "Creating and Managing Workflows" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- Email notification settings
- Default folder columns
- Global filters

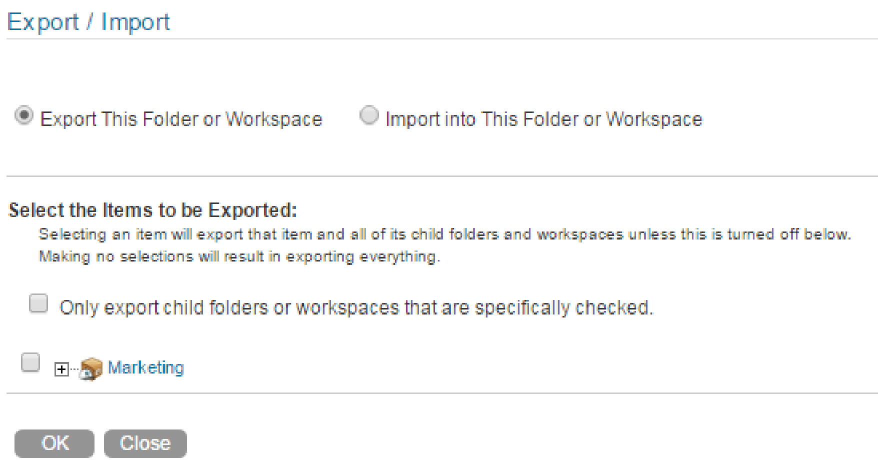
Exporting Workspaces

1 Log in to the Vibe site as the Vibe administrator.

2 Navigate to the workspace that you want to export.

3 Click the **Configure** icon next to the workspace title, then click **Import/Export Workspace**.

The Export/Import page is displayed.



4 Select **Export This Folder or Workspace**.

5 To export all contents of the folder or workspace, click **OK**.

or

To export only individual workspaces and folders, select **Only export child folders or workspaces that are specifically checked**, then expand the workspace tree and select the workspaces and folders that you want to export. Then click **OK**.

Importing Workspaces

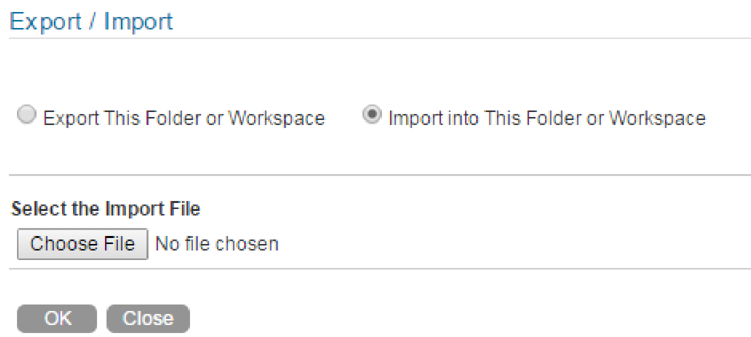
1 Log in to the Vibe site as the Vibe administrator.

2 Navigate to the workspace where you want the imported workspace to reside.

3 Click the **Configure** icon next to the workspace title, then click **Import/Export Workspace**.

The Export/Import page is displayed.

4 Select **Import into This Folder or Workspace**.



5 Browse to and select the workspace that you want to import, then click **OK**.

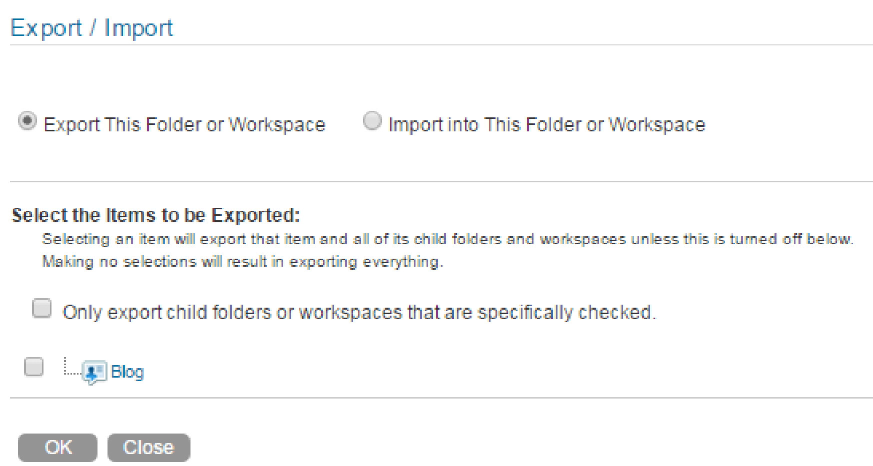
Exporting Folders

1 Log in to the Vibe site as the Vibe administrator.

2 Navigate to the folder that you want to export.

3 Click the **Configure** icon next to the folder title, then click **Import/Export Folder**.

The Export/Import page is displayed.



4 Select **Export This Folder or Workspace**.

5 To export all contents of the folder or workspace, click **OK**.

or

To export only individual workspaces and folders, select **Only export child folders or workspaces that are specifically checked**, then expand the workspace tree and select the workspaces and folders that you want to export. Then click **OK**.

Importing Folders

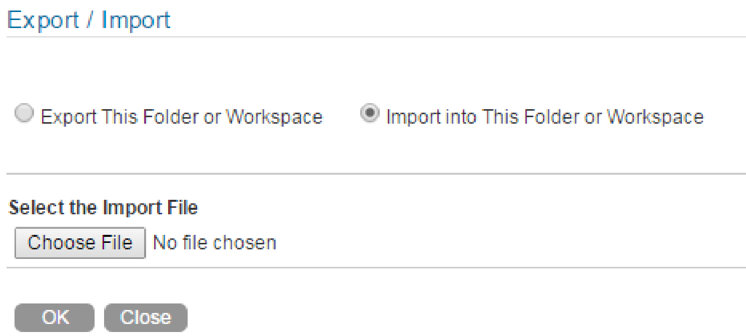
1 Log in to the Vibe site as the Vibe administrator.

2 Navigate to the folder or workspace where you want the imported folder to reside.

3 Click the **Configure** icon next to the folder or workspace title, then click **Import/Export Folder** if you are importing into a folder.

The Export/Import page is displayed.

4 Select **Import into This Folder or Workspace**.



5 Browse to and select the folder that you want to import, then click **OK**.

Exporting Folder Entries

1 Log in to the Vibe site as the Vibe administrator.

2 Navigate to and select the folder entry that you want to export.

3 In the entry footer, click **Export this entry**.

You can now download the entry to your computer's file system.

Importing Folder Entries

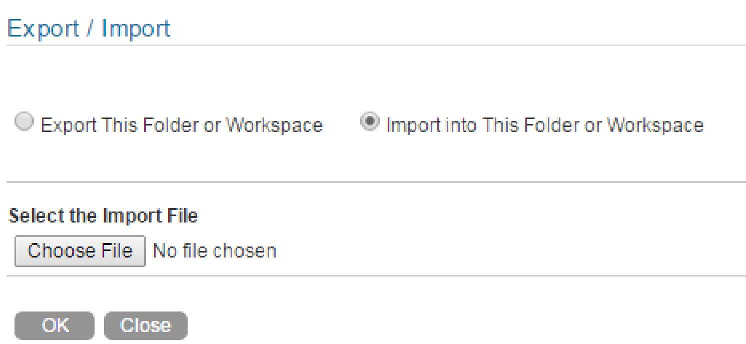
1 Log in to the Vibe site as the Vibe administrator.

2 Navigate to the folder where you want the imported folder entry to reside.

3 Click the **Configure** icon next to the folder title, then click **Import/Export Folder**.

The Export/Import page is displayed.

4 Select **Import into This Folder or Workspace**.



5 Browse to and select the folder entry that you want to import, then click **OK**.

Managing Workspace Disk Space Usage

Disk space usage is managed on both a folder and workspace basis as well as an individual user or group basis.

You can enforce one or both of these types of data quotas. See "Managing the File Upload Size Limit" on page 255.

Modifying the Title, Description, and Branding of the Personal Workspaces Workspace

By default, the workspace that contains all of the personal workspaces is named **Personal Workspaces**. (This is an alternate way of viewing users in your Vibe system.) The brand for this workspace is inherited from the parent workspace, and there is no workspace description. However, Vibe lets you modify the name, description, and brand of the workspace.

- "Modifying the Title and Description" on page 237
- "Modifying the Brand" on page 237

Modifying the Title and Description

1 Navigate to the Personal Workspaces workspace by clicking the **Workspace Tree** icon in the Action toolbar, expanding **Home Workspace**, then clicking **Personal Workspaces**.

2 Click the **Configure** icon next to the workspace title, then click **Edit Workspace**.

Use this page to change the title and description of the workspace.

Modifying the Brand

1 Navigate to the Personal Workspaces workspace by clicking the **Workspace Tree** icon in the Action toolbar, expanding **Home Workspace**, then clicking **Personal Workspaces**.

2 Click the **Configure** icon next to the workspace title, then click **Brand Workspace**.

Use the Workspace/Folder branding dialog box to modify the workspace brand. For more information about how to brand a workspace, see "Branding a Folder or Workspace" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

24 Managing Disk Space Usage with Data Quotas and File Restrictions

As time passes, your Novell Vibe site occupies more and more disk space as users post folder entries, attach files, create new versions of files, and so on. As the Vibe administrator, you can impose limits on the amount of data that is uploaded into the Vibe site.

Only files and attachments count toward the data quota. Workspaces, folders, and entries that do not contain files and attachments do not count toward the data quota.

You can limit the amount of files and attachments for individual users and groups as well as individual workspaces and folders.

- "Understanding the Types of Data Quotas" on page 239
- "Understanding Data Quota Behavior and Exclusions" on page 240
- "Managing Workspace and Folder Data Quotas" on page 241
- "Managing User Data Quotas" on page 244
- "General Data Quota Management" on page 254
- "Managing the File Upload Size Limit" on page 255
- "Setting a Maximum Number of Versions for Each File" on page 257
- "Automatically Deleting Old File Versions" on page 257

Understanding the Types of Data Quotas

You as the Novell Vibe administrator can enable two kinds of data quotas:

- User data quotas
- Workspace and folder data quotas

You can enable one of these quotas, or both of them.

- "Understanding User Data Quotas" on page 239
- "Understanding Workspace and Folder Data Quotas" on page 240

Understanding User Data Quotas

User data quotas limit the amount of data individual users can add to the Vibe site. Any files and attachments that a user adds to the Vibe site counts toward his or her data quota, regardless of the folders or workspaces where the user adds them.

Understanding Workspace and Folder Data Quotas

Workspace and folder quotas limit the amount of data that can be stored in individual workspaces and folders.

Sub-workspaces and sub-folders that have a data quota are subject to their own data quota as well as any data quotas that exist on parent folders and workspaces. For example, consider a workspace that has a data quota of 50 MB. The workspace contains two sub-workspaces: Workspace A and Workspace B. Users cannot upload data that is in excess of 50 MB into either of these sub-workspaces. Furthermore, users cannot upload data into both of these sub-workspaces that is in excess of 50 MB (for example, users cannot upload data that is in excess of 30 MB into both sub-workspace, because the amount of combined data for both sub-workspaces is greater than 50 MB).

Understanding Data Quota Behavior and Exclusions

- "Understanding Default Data Quota Behavior" on page 240
- "Understanding Data Quota Exclusions" on page 241

Understanding Default Data Quota Behavior

The following sections describe the default behavior for how user data quotas work after they have been enabled. (For information on how to enable data quotas for your Vibe site, see "Enabling Workspace and Folder Data Quotas" on page 241 and "Managing Workspace and Folder Data Quotas" on page 241.)

- "Exceeding the Data Quota" on page 240
- "Exceeding the High-Water Mark" on page 240

Exceeding the Data Quota

By default, Vibe users are strictly held to the data quota that you set. If a user who is approaching his or her data quota tries to upload a file to the Vibe site and that file exceeds the user's data quota, Vibe rejects the upload attempt and the entry is lost. This is also true with data quotas that are set on workspaces and folders.

For user data quotas (not for workspace and folder data quotas), you can allow users to post a final entry to the Vibe site even if the entry exceeds the user data quota. This approach is less strict and does not guarantee that users won't exceed the data quota; however, it is more forgiving because it allows users to post one final upload to the Vibe site and does not erase the entry and attached file that they are trying to upload.

For information on how to configure your Vibe data quotas to be less strict by allowing users one final upload to the Vibe site, see "Configuring Data Quotas to Be Less Strict" on page 254.

Exceeding the High-Water Mark

When users exceed the data quota high-water mark, they are notified that they are approaching the data quota. Vibe informs them how many kilobytes of disk space are still available.

For more information on selecting an appropriate high-water mark, see "Selecting an Appropriate High-Water Mark" on page 245.

Understanding Data Quota Exclusions

Files stored in mirrored folders do not count against data quotas because they are not uploaded into the Vibe site.

Managing Workspace and Folder Data Quotas

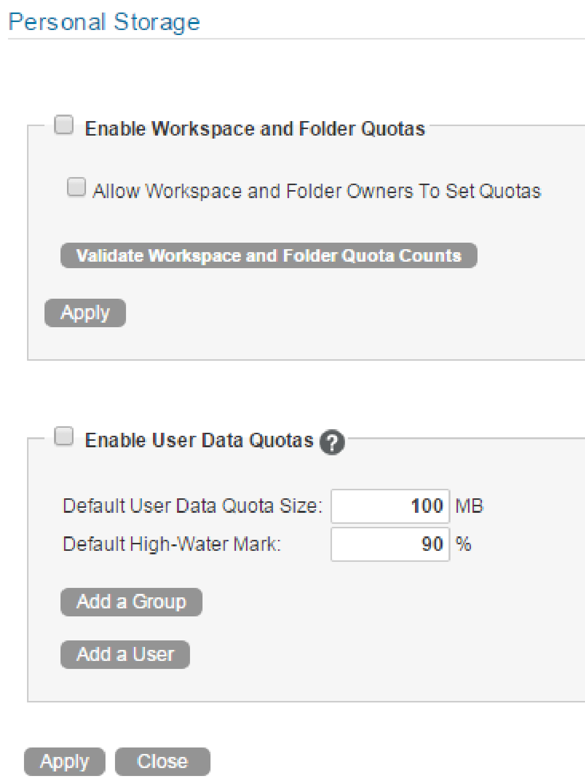
- "Enabling Workspace and Folder Data Quotas" on page 241
- "Setting Quotas on Workspaces and Folders" on page 242
- "Validating Workspace and Folder Quotas" on page 243

Enabling Workspace and Folder Data Quotas

Before you can set data quotas on workspaces and folders, you must first enable them. You can enable data quotas so that only you as the Vibe administrator can manage workspace and folder quotas, or you can enable data quotas so that all users can manage the data quotas for their own workspaces and folders.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. Under **Management**, click **Personal Storage**.
4. Click **Initialize Workspace and Folder Quota Counts**.

   This sets up the workspace and folder data quota for your Vibe site. This operation can take a significant amount of time (10 to 20 minutes).



5 Select **Enable Workspace and Folder Quotas**.

6 (Optional) If you want to allow users to manage the data quotas for their own workspaces and folders, select **Allow Workspace and Folder Owners To Set Quotas**.

7 Click **Apply** > **Close**.

8 Set data quotas on workspaces and folders as described in "Setting Quotas on Workspaces and Folders" on page 242.

Setting Quotas on Workspaces and Folders

Before you can set data quotas on workspaces and folders, you need to enable them, as described in "Enabling Workspace and Folder Data Quotas" on page 241.

You can set quotas on individual workspaces and folders, or you can set quotas on all workspaces and folders of a certain type. For example, you can configure all Photo Album folders in your Vibe site to have a data quota of 10 MB.

- "Setting Quotas on Individual Workspaces and Folders" on page 242
- "Setting Quotas on All Workspaces and Folders of a Certain Type" on page 243

Setting Quotas on Individual Workspaces and Folders

1 Navigate to the workspace and folder where you want to set the quota.

2 Click the **Configure** icon next to the workspace or folder title, then **Configure Views, URLs and Controls**.

3 Click the **Quotas** tab.

4 In the **Set a Quota** field, specify the new data quota, then click **OK**.

Setting Quotas on All Workspaces and Folders of a Certain Type

When you set data quotas on all workspaces or folders of a certain type, the quota applies only to workspaces or folders that are created after you set the quota. Workspaces and folders that were created before the quota was set do not automatically have a data quota assigned to them.

To set a data quota on all workspaces and folders of a certain type, you need to modify the template for the workspace or folder where you want to set the data quota. For information on how to modify the template for workspaces and folders, see "Modifying Workspace and Folder Templates" on page 259.

Validating Workspace and Folder Quotas

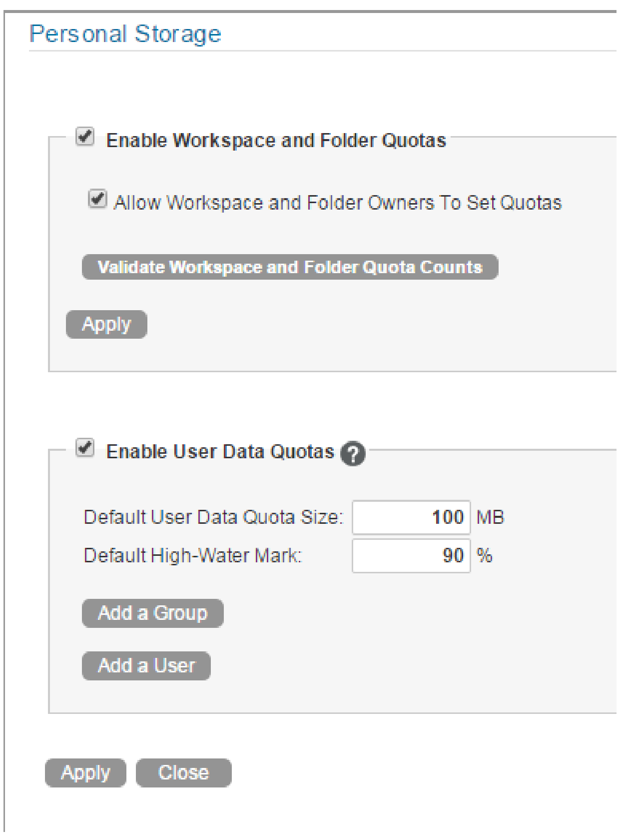
Quota counts for workspaces and folders can become marginally inaccurate over time if multiple users are frequently adding and deleting files in a workspace or folder where a data quota has been set.

You can repair any data quota inaccuracies by validating the data quota:

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Personal Storage**.



4 Click **Validate Workspace and Folder Quota Counts**.

5 Click **Apply** > **Close**.

Managing User Data Quotas

Each user's data quota establishes how much disk space the user's attached files and file versions can occupy in the Vibe site. Workspaces, folders, and entries that do not contain files or attachments do not count toward a user's data quota.

By default, users are not limited in the disk space that their attached files and file versions occupy in the Vibe site. As the Vibe administrator, you can decide when limiting users' disk space usage becomes appropriate.

- "Planning User Data Quotas" on page 244
- "Setting User Data Quotas" on page 245
- "Modifying User Data Quotas" on page 248
- "Removing User Data Quotas" on page 251
- "Managing Your Personal Data Quota" on page 253
- "Monitoring User Data Quotas" on page 254

Planning User Data Quotas

- "Understanding User Data Quota Priority" on page 244
- "Selecting the Default User Data Quota for All Users" on page 245
- "Selecting an Appropriate High-Water Mark" on page 245
- "Determining Data Quotas for Specific Users" on page 245
- "Determining Data Quotas for Specific Groups" on page 245

Understanding User Data Quota Priority

Because users can have multiple data quotas assigned to them, either individually, through group membership, or through the site-wide default, Vibe prioritizes the existing data quotas and uses only one for each individual Vibe user. If users have multiple data quotas that pertain to them, the priority level is as follows:

1. **User Quota:** A quota that is set for an individual user overrides the site-wide default quota and any other quotas that are associated with any groups where the user is a member.
2. **Group Quota:** A quota that is set for an individual group overrides the site-wide default quota. This pertains to all users who are members of that group.

   When a user is a member of multiple groups that have data quotas associated with them, the user is given the highest data quota. For example, if a Vibe user is a member of Group A, Group B, and Group C, and the data quotas for each of these groups is 10, 20, and 30, the Vibe user's data quota is 30.
3. **Site-Wide Default:** The site-wide default quota is used for all Vibe users who have not been assigned individual quotas, and who are not associated with any groups where a quota has been set.

Selecting the Default User Data Quota for All Users

When you enable the data quota feature, the initial default data quota is 100 MB. This means that each Vibe user can upload 100 MB of files and attachments to the Vibe site. There is one default data quota for each Vibe zone.

When you select the default data quota for your Vibe site, consider the size of your Vibe site, the number of Vibe users, the amount of available disk space, and so on. You can override the default data quota on a per-user and per-group basis, as described in "Managing Workspace and Folder Data Quotas" on page 241.

As described in "Exceeding the Data Quota" on page 240, when a user adds enough files and attachments to exceed the data quota, the user can no longer attach files or create versions until existing files have been deleted and purged to free up storage space.

For information about purging deleted files to make storage space available, see "Permanently Deleting Files from the Trash" on page 255.

For information about the user experience when nearing or exceeding a data quota, see "Adding Files and Attachments to the Vibe Site When You Are Over Your Quota" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

For information about which data quota is used when users have multiple data quotas that pertain to them, see "Understanding User Data Quota Priority" on page 244.

Selecting an Appropriate High-Water Mark

The high-water mark is the percentage of the data quota when users are notified that they are approaching their data quotas. The default high-water mark is 90% of a user's data quota.

This high-water mark also applies to data quotas that are set on workspaces and folders.

Determining Data Quotas for Specific Users

If there is a user in your Vibe site who needs either a higher or lower data quota than the site-wide default, you can assign that user an individual user data quota.

When you set data quotas for specific users, remember that individual user data quotas override the default user data quota, as well as quotas that are assigned to any groups where the user is a member, as described in "Understanding User Data Quota Priority" on page 244.

Determining Data Quotas for Specific Groups

When you set data quotas for specific groups, remember that group data quotas override the default site-wide data quota, but do not override individual user quotas, as described in "Understanding User Data Quota Priority" on page 244.

Setting User Data Quotas

You can set data quotas for the entire Vibe site, for individual groups, and for individual users.

- "Setting a Default Data Quota" on page 246
- "Setting Data Quotas for Individual Groups" on page 246

- “Setting Data Quotas for Individual Users” on page 247
- “Setting Data Quotas on Outgoing Email Messages” on page 248

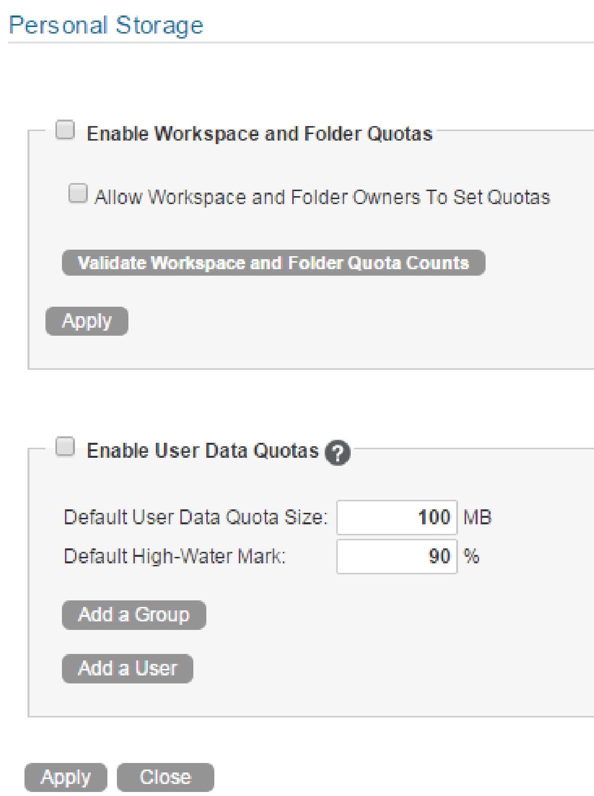
Setting a Default Data Quota

When you set a default data quota, the quota applies to all Vibe users who have not been assigned individual quotas, and who are not associated with any groups where a quota has been set.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Personal Storage**.



4 Select **Enable User Data Quotas**.

5 Set the **Default Data Quota Size** and **Default High-Water Mark** options as determined in “Planning User Data Quotas” on page 244.

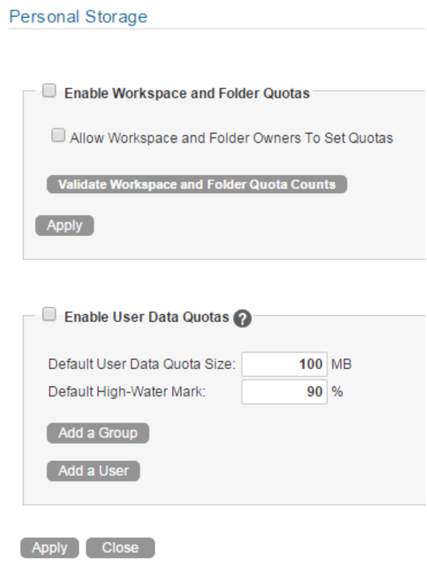
6 Click **Apply** > **Close** to save the user data quota settings.

Setting Data Quotas for Individual Groups

1 Log in to the Vibe site as the Vibe administrator.

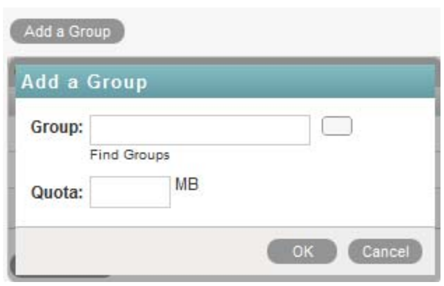
2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Data Quotas and File Upload Limits**.



4 Select **Enable User Data Quotas**.

5 Click **Add a Group**.



6 In the **Group** field, start typing the name of the group for which you want to set a quota, then click the group name when it appears in the drop-down list.

Repeat this process to add additional groups for which you want to assign the same data quota.

7 In the **Quota** field, specify the disk space limit for the group.

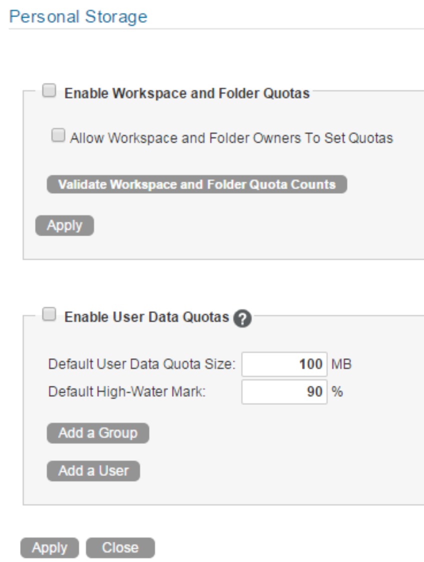
8 Click **OK**, then click **Apply** > **Close** to save the user data quota settings.

Setting Data Quotas for Individual Users

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Data Quotas and File Upload Limits**.



4 Select **Enable User Data Quotas**.

5 Click **Add a User**.

6 In the **User** field, start typing the name of the user for which you want to set a quota, then click the user's name when it appears in the drop-down list.

Repeat this process to add additional users for which you want to assign the same data quota.

7 In the **Quota** field, specify the disk space limit for the user.

8 Click **OK**, then click **Apply** > **Close** to save the user data quota settings.

Setting Data Quotas on Outgoing Email Messages

You can set a maximum file size on individual email messages that are sent from the Vibe system. For more information, see "Enabling/Disabling Outbound Emailing of Folder Digests" on page 165.

Modifying User Data Quotas

Vibe lets you modify data quotas that you have previously set. You can modify data quotas for your entire Vibe site, or modify data quotas for individual groups and users.

- "Modifying User Data Quotas for the Entire Vibe Site" on page 249
- "Modifying User Data Quotas for Individual Groups and Users" on page 250

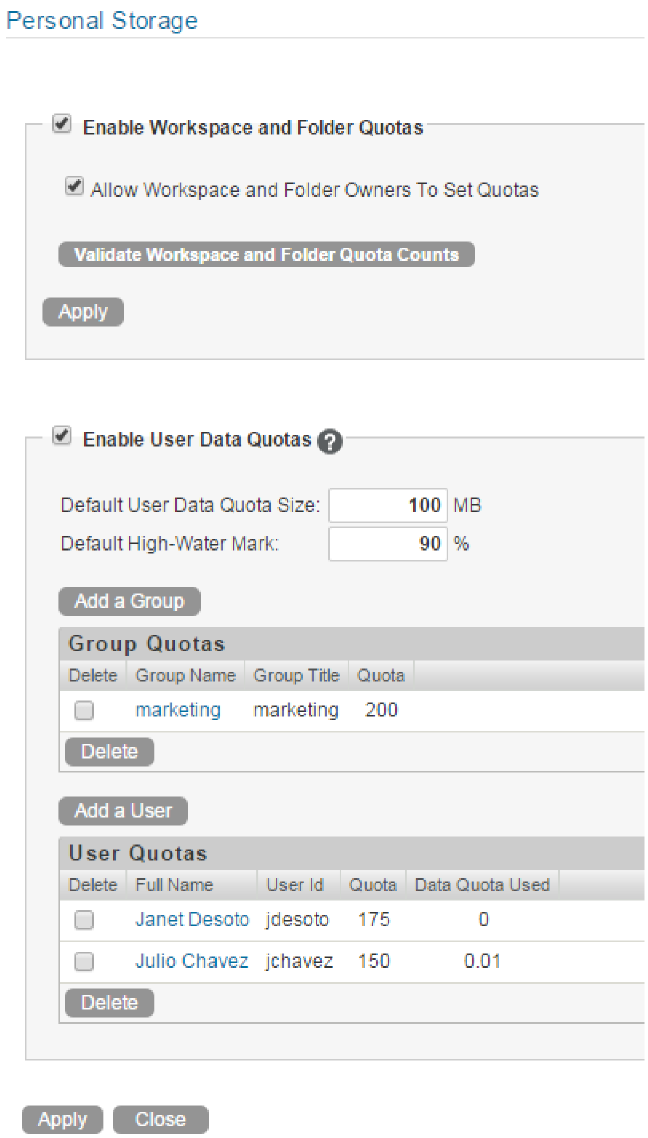
Modifying User Data Quotas for the Entire Vibe Site

Vibe lets you easily modify the site-wide default user data quota.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Personal Storage**.



4 In the **Default User Data Quota Size** field, delete the existing quota and specify the new quota.

You can also modify the default high-water mark in the **Default High-Water Mark** field. For more information about the high-water mark, see "Selecting an Appropriate High-Water Mark" on page 245.

5 Click **Apply** > **Close** to save the user data quota settings.

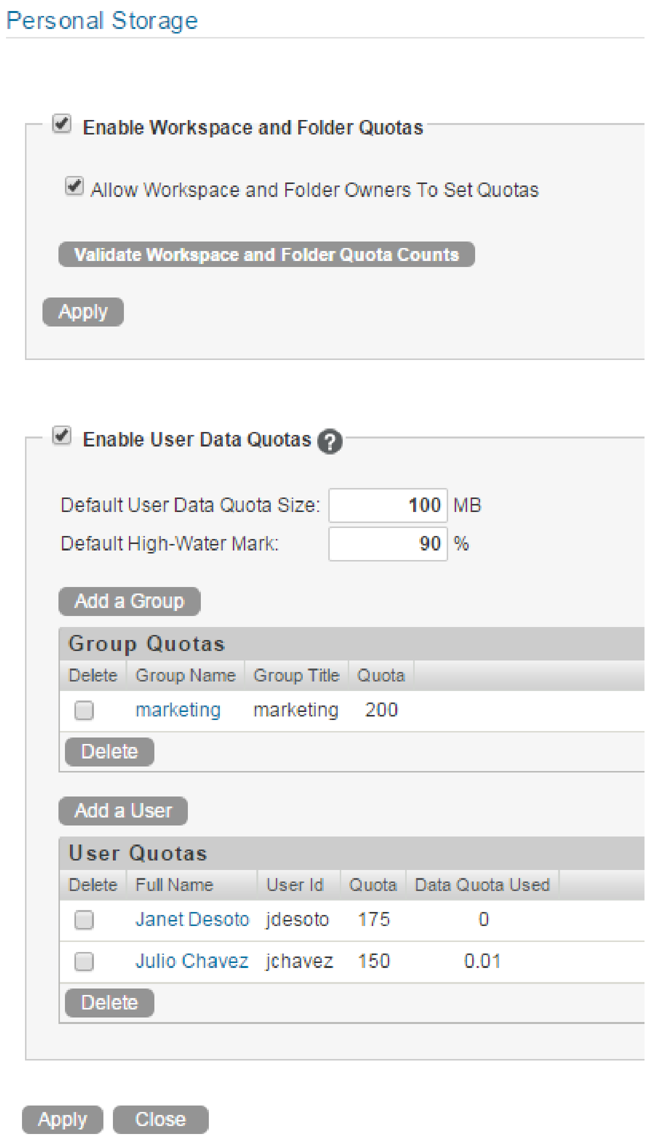
Modifying User Data Quotas for Individual Groups and Users

Vibe lets you easily modify individual group and user data quota settings that you have previously set.

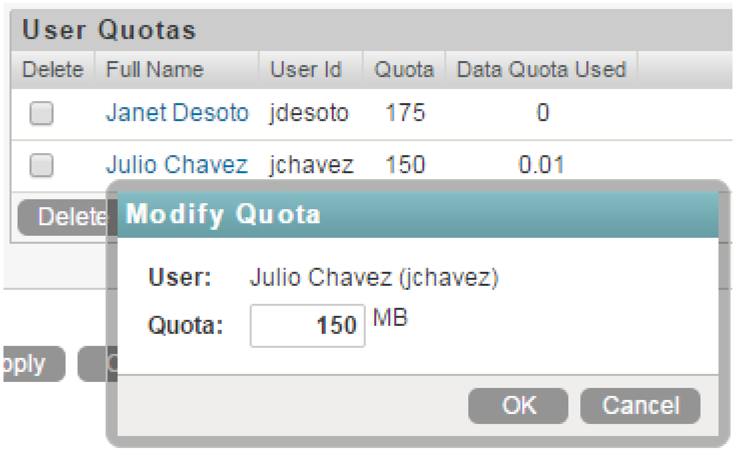
1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Personal Storage**.



4 In the **Group Quotas** table or **User Quotas** table, click the group name or user name that represents the group or user whose quota you want to modify.



5 In the **Quota** field, delete the existing quota and specify a new quota.

6 Click **OK**, then click **Apply** > **Close** to save the user data quota settings.

Removing User Data Quotas

Vibe lets you disable data quotas that you have previously set. You can disable data quotas for your entire Vibe site, or remove data quotas from individual groups and users.

- "Disabling User Data Quotas for the Entire Vibe Site" on page 251
- "Removing User Data Quotas from Individual Groups and Users" on page 252

Disabling User Data Quotas for the Entire Vibe Site

If you decide that you no longer need to impose limits on the amount of data that users are permitted to upload into the Vibe site, you can disable the data quota feature. Disabling the data quota feature enables all Vibe users to upload as much data to the Vibe site as they want.

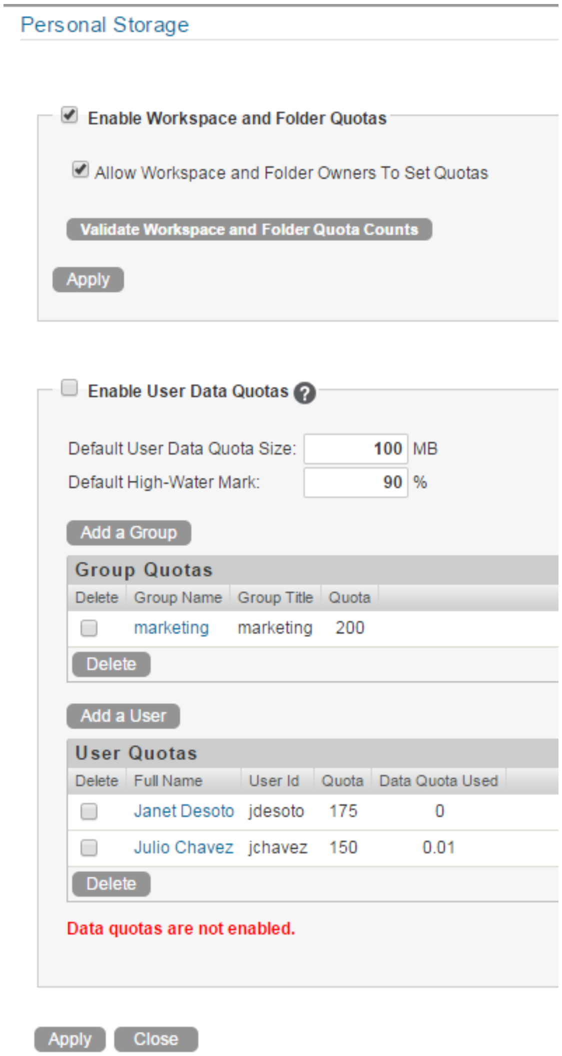
1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Personal Storage**.

The Data Quotas and File Upload Limits page is displayed.

4 Deselect **Enable User Data Quotas**, then click **Apply**.



Data quotas are no longer enabled for your Vibe site.

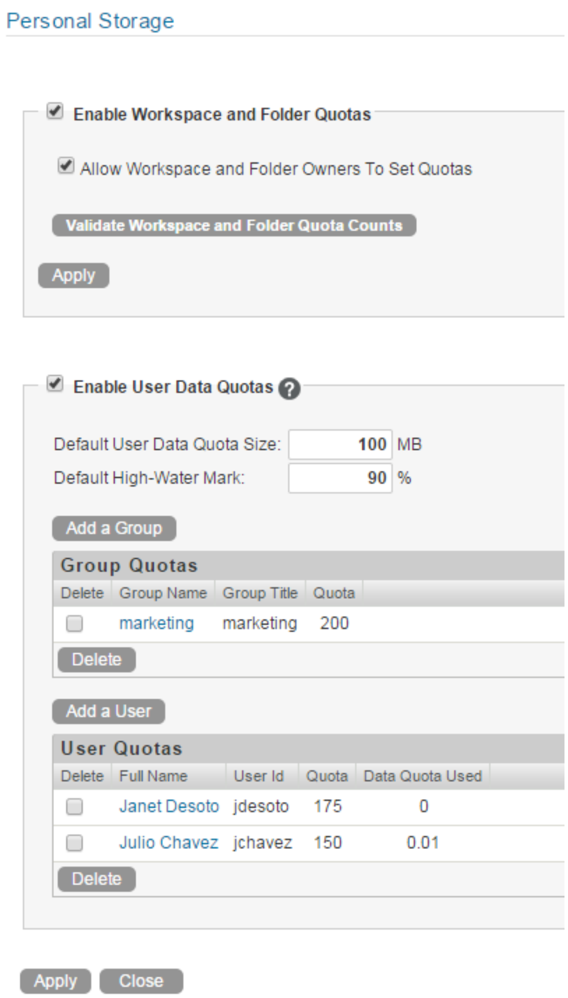
Removing User Data Quotas from Individual Groups and Users

You can remove data quotas that you have previously set for individual groups and users. Users are held to the site-wide data quota default setting if they do not have an individual quota defined for them and they are not members of any groups where a group quota has been assigned.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under **Management**, click **Personal Storage**.



4 In the **Group Quotas** table or **User Quotas** table, select the check box next to the group or user whose quota you want to remove, then click **Delete**.

5 Click **Apply** > **Close** to save the user data quota settings.

Managing Your Personal Data Quota

NOTE: As a Vibe administrator, you are also held to a data quota. If you want to assign yourself a larger quota than the site-wide default, you can add an individual quota for yourself, as described in "Setting Data Quotas for Individual Users" on page 247.

All Vibe users need to manage their personal data quotas. When you have a limited allocation of disk space, you need to be aware of the amount of disk space that you have available, know how to make more disk space available as you approach your quota, and know what counts against your quota and what doesn't.

For information on how to accomplish these and other important tasks as you manage your data quota, see "Managing Your Data Quota" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Monitoring User Data Quotas

You can monitor which users in the Vibe site have exceeded or are close to exceeding their data quotas by generating the following reports:

- "Data Quota Exceeded Report" on page 302
- "Data Quota Highwater Exceeded Report" on page 303

General Data Quota Management

This section describes tasks that are common to both types of data quotas: workspace and folder data quotas and user data quotas.

- "Configuring Data Quotas to Be Less Strict" on page 254
- "Permanently Deleting Files from the Trash" on page 255

Configuring Data Quotas to Be Less Strict

This section applies only to user data quotas. You cannot configure workspace and folder quotas to be less strict, as described in this section.

As a Vibe administrator, you can decide how strictly you want to enforce user data quota adherence. You can maintain the default behavior, or you can be less strict by allowing users to post a final entry that exceeds the data quota.

For more information about the default behavior for a data quota, see "Understanding Default Data Quota Behavior" on page 240.

To configure Vibe to allow users to post a final entry that exceeds the data quota:

1. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config

2. Make a backup copy of the `ssf-ext.properties` file.
3. Open the `ssf-ext.properties` file in a text editor.
4. Add the following line to the `ssf-ext.properties` file:

   ```
   data.quota.strict.conformance=false
   ```

5. Save and close the `ssf-ext.properties` file.
6. Stop and restart Vibe.

Permanently Deleting Files from the Trash

When users delete files or file versions, the disk space occupied by the deleted files and versions counts against the data quotas until users permanently delete the files and versions from the Trash, as described in "Making Disk Space Available by Deleting Items from the Trash" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

As a Vibe administrator, you can permanently delete files and versions anywhere on the Vibe site in order to recover disk space.

IMPORTANT: After items have been permanently deleted, they cannot be recovered except through a tedious manual process from the archive store with the help of Novell Technical Support. For more information, see "Manually Restoring Individual Entries" on page 289.

To permanently delete files and file versions from the Trash:

1. Log in to the Vibe site as the Vibe administrator.
2. Click the **Workspace tree** icon, then click **Home Workspace**.

   All global workspaces, team workspaces, and personal workspaces are located under the Home Workspace.
3. Click **Trash** at the bottom of the Left Navigation pane to display a list of all deleted files and versions.

   By default, the list is ordered alphabetically by title.
4. (Optional) Click a column heading to sort the list by when items were deleted, who deleted the items, or where the items were deleted on the Vibe site.
5. Select items to permanently delete, then click **Delete**.

Managing the File Upload Size Limit

The file upload size limit conserves disk space on your Novell Vibe site because it prevents users from uploading large files to the Vibe site. The default size limit for uploading files into your Vibe site is 2 GB.

Browsers also impose limits on the size of files that can be uploaded. This limit differs depending on which browser you are using to run Vibe.

If you are using Vibe Desktop to upload and download files between user workstations and the Vibe site, see "Configuring the Maximum File Size Limit for Vibe Desktop" on page 149 for more information about controlling maximum file size limits.

Modifying the File Upload Size Limit for the Vibe Site

You as the Vibe administrator can increase or decrease this size limit for the Vibe site. Workspace and folder owners can set a file upload size limit for their own workspaces and folders, but the limit in individual workspaces and folders cannot exceed what you set for the Vibe site.

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
2 Under **Management**, click **File Upload Limits**.
3 In the **File Upload Size Limits** section, specify the new file upload size limit.
4 Click **Apply** > **Close**.

Setting a File Upload Size Limit for Individual Users and Groups

You can assign a file upload size limit to individual users and groups that is different from the site-wide file upload size limit. For example, if the file upload size limit for your Vibe site is 2 GB, but your Marketing team often uploads large files, you can give the `Marketing` group a file upload size of 3 GB.

- "Setting a Limit for a Group" on page 256
- "Setting a Limit for a User" on page 256

Setting a Limit for a Group

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
2 Under **Management**, click **File Upload Limits**.
3 In the **File Upload Size Limits** section, click **Add a Group**.
4 Specify the following information:

   Group: Begin typing the group name for which you want to set a file upload size limit, then click the name when it appears in the list.

   File Size Limit: Specify the new file size limit for the group.
5 Click **OK**.

Setting a Limit for a User

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
2 Under **Management**, click **File Upload Limits**.
3 In the **File Upload Size Limits** section, click **Add a User**.
4 Specify the following information:

   User: Begin typing the user name for which you want to set a file upload size limit, then click the name when it appears in the list.

   File Size Limit: Specify the new file size limit for the user.
5 Click **OK**.

Setting a File Upload Size Limit for Individual Workspaces and Folders

Workspace and folder owners can set a file upload size limit on individual workspaces and folders. If a site-wide limit has been set by the Vibe administrator, the limit on the workspace or folder must be less than the site-wide limit. For more information, see "Limiting the File Upload Size for Folders and Workspaces" in "Managing Folders" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Setting a Maximum Number of Versions for Each File

Because a significant amount of data can be consumed by old versions of files, you can configure the Vibe site to allow only a certain number of file versions for each file version set within the folder or workspace. (A file version set includes the major file version and all minor file versions. For more information about major and minor file versions, see "Incrementing the Major Version Number of a File" in "Working with Files in a Folder Entry" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.)

To configure the Vibe site in this way, navigate to the top-level workspace (which by default is called **Home Workspaces**), then follow the instruction in "Automatically Deleting Minor File Versions That Exceed the Allowed Maximum" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Automatically Deleting Old File Versions

Because a significant amount of data can be consumed by old versions of files, you can configure all minor versions of each file to be automatically deleted after a specified number of days on the Vibe site. When you configure your Vibe site in this way, all minor versions of each document are deleted after the specified number of days (major versions are never deleted).

Workspace and Folder owners can remove this setting for their workspaces and folders, or specify a different number of days, as described in "Automatically Deleting Minor File Versions after a Specified Number of Days" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

2 Under **System**, click **File Version Aging**.

3 Specify the number of days to wait before each lower-level version is automatically deleted, then click **Apply** > **Close**.

25 Managing Workspace and Folder Templates

Workspace and Folder templates are a powerful and efficient way to manage your Novell Vibe site. They enable you to customize the default features, default layout, and default access control settings of the workspaces and folders throughout your Vibe site.

For example, the Team Workspaces template is used when any team workspace is created. By default, the access control settings for the Team Workspaces template specify that only team members are able to view the team workspace. However, if you want to run a more relaxed Vibe site and allow all Vibe users to view any team workspace, you can simply modify the access control settings on the Team Workspaces template.

Changes that you make to templates affect only those workspaces and folders that are created after the template was modified.

For more information about templates, see "Understanding Templates" on page 61.

Creating Workspace and Folder Templates

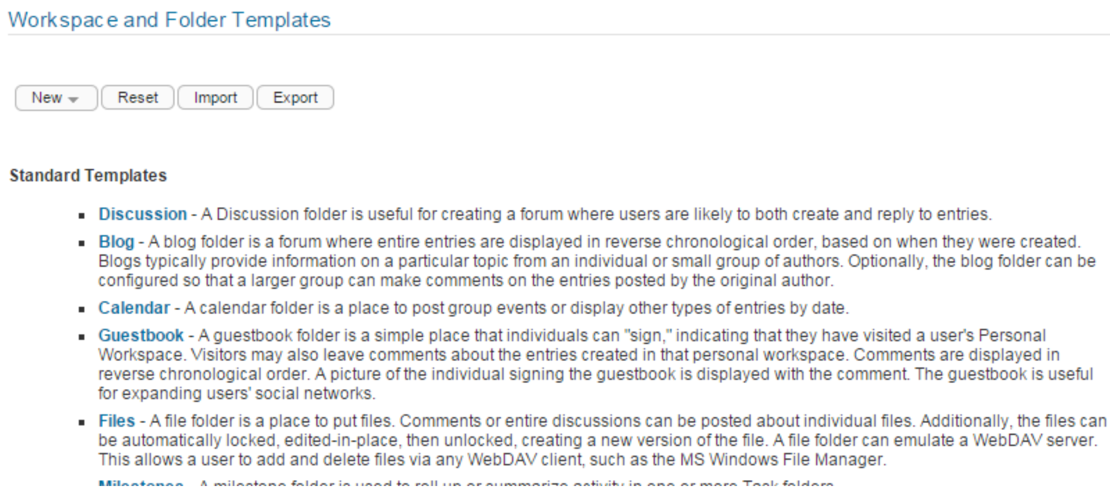
For information on how to create new workspace and folder templates, see "Creating Workspace and Folder Templates" on page 64.

Modifying Workspace and Folder Templates

Novell Vibe lets you modify default templates as well as custom templates that you have already created.

For information on how to create custom templates, see "Creating Workspace and Folder Templates" on page 64.

1. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
2. Under **Management**, click **Workspace and Folder Templates**.



3 Click the workspace or folder template that you want to modify.

From this page you can do any of the following:

- "Deleting the Template" on page 260
- "Exporting the Template" on page 260
- "Renaming the Template" on page 261
- "Adding an Existing Workspace Template" on page 261
- "Adding an Existing Folder Template" on page 261
- "Removing a Folder Template or Workspace Template from the Template" on page 262
- "Adding Access Controls to the Template" on page 262
- "Adding a Data Quota to the Template" on page 262
- "Changing the Default View for the Template" on page 262
- "Changing the Title, Description, Brand, and Icon for the Template" on page 263
- "Modifying the Accessory Panel for the Template" on page 263

Deleting the Template

Deleting a template deletes the template and all sub-templates.

1 Click **Manage This Template**.

2 Click **Delete This Template** > **OK**.

Exporting the Template

1 Click **Manage This Template**.

2 Click **Export This Template** > **OK**.

For information on how to export multiple templates simultaneously, see "Exporting Multiple Templates" on page 264.

Renaming the Template

You can change the information that is displayed on the Add New Workspace page (or Add New Folder page), when users select which type of workspace they want to add.

1 Click **Manage This Template**.

2 Click **Modify This Template**.

3 Specify the following information:

   Name: This is the internal database name.

   Template Title: This name appears in the Add New Workspace page (or Add New Folder page) when users select which type of workspace they want to add.

   Description: This description appears in the Add New Workspace page (or Add New Folder page) when users select which type of workspace they want to add.

4 Click **Modify**.

Adding an Existing Workspace Template

You can add a workspace template to the template that you are currently modifying. The workspace template that you add becomes a sub-workspace to the main workspace. All template sub-workspaces and sub-folders that you add are preserved when the template is used in your Vibe site.

1 Click **Manage This Template**.

2 Click **Add Workspace Template**.

3 In the Currently Defined Templates section, select the workspace template that you want to add.

4 Click **Add**.

   A cloned copy of the workspace template is added as a sub-folder to the main workspace.

Adding an Existing Folder Template

You can add a folder template to the template that you are currently modifying. The folder template that you add becomes a sub-folder to the main workspace or folder. All template sub-workspaces and sub-folders that you add are preserved when the template is used in your Vibe site.

You can add a folder template to the template that you are currently modifying.

1 Click **Manage This Template**.

2 Click **Add Folder Template**.

3 In the Currently Defined Templates section, select the folder template that you want to add.

4 Click **Add**.

   A cloned copy of the folder template is added as a sub-folder to the main folder or workspace.

Removing a Folder Template or Workspace Template from the Template

You can also remove folder or workspace templates that you previously added to the template that you are modifying (as described in "Adding an Existing Workspace Template" on page 261 and "Adding an Existing Folder Template" on page 261.) Or you can remove folder or workspace templates that exist by default in the template that you are modifying. For example, you can remove the Files folder template from the User Workspace template.

1. Expand the workspace tree on the Workspace and Folder Templates page.
2. Select the workspace or folder template that you want to remove.
3. Click **Manage This Template**.
4. Click **Delete This Template** > **OK**.

Adding Access Controls to the Template

1. Click **Manage This Target**.
2. Click **Access Control**.

   The Configure Access Control page is displayed.

   For information on how to use this page, see Chapter 2, "Planning and Controlling User Access to Workspaces and Folders," on page 21.
3. After you have made your access control modifications, click **Close**.

An example of adding access controls to a template is described in "Restricting Access to Personal Workspaces throughout the Vibe Site" on page 26.

Adding a Data Quota to the Template

1. Click **Manage This Target**.
2. Click **Configure Views, URLs, and Controls**.
3. Click the **Quotas** tab.
4. Specify the quota in the **Set a Quota** field, then click **OK**.

   For information on data quotas for workspaces and folders, see "Managing Workspace and Folder Data Quotas" on page 241.

Changing the Default View for the Template

1. Click **Manage This Target** > **Configure Views, URLs and Controls**.

   A page with various configuration options is displayed.
2. In the **Default View** section, select the default view that you want the template to have.
3. Click **Apply** > **Close**.

Changing the Title, Description, Brand, and Icon for the Template

You can change the attributes of the template that are displayed in the workspace after the workspace is created.

1. Click **Manage This Target**.
2. Click **Modify**.
3. Change the title, description, brand, and icon as desired, then click **OK**.

Modifying the Accessory Panel for the Template

Vibe lets you modify the Accessory Panel in a template.

If the Accessory Panel already contains accessories, you can modify them; or, you can create new accessories. For information on how to modify and create accessories, see “Managing Accessories” in the *Micro Focus Vibe 4.0.5 User Guide*.

Exporting Templates

You might want to export templates for the following reasons:

- To import the template into another system.

  For information on how to import a template, see “Importing Templates” on page 265.
- To back up the template.

  This can be useful if you want to edit a template, so you can restore the original if your edits don’t go according to plan.

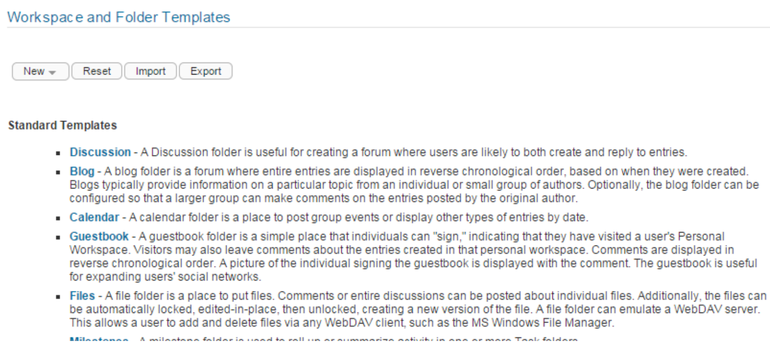
Novell Vibe lets you export individual templates, or export multiple templates simultaneously.

Exporting a Single Template

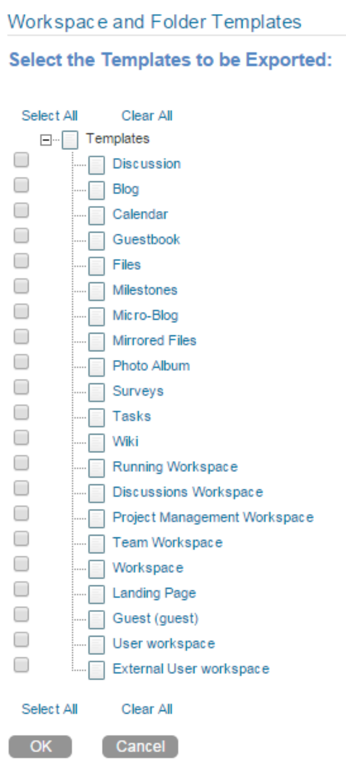
1. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
2. Under **Management**, click **Workspace and Folder Templates**.
3. Click the workspace or folder template that you want to export.
4. Click **Manage This Template**.
5. Click **Export This Template**.
6. Click **OK**.

Exporting Multiple Templates

1. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
2. Under **Management**, click **Workspace and Folder Templates**.



3. Click **Export**.



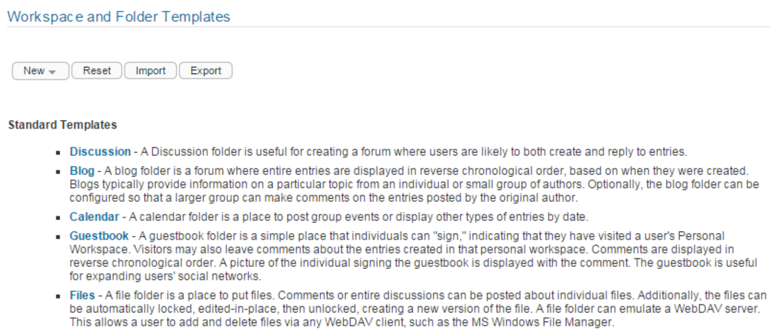
4. In the **Select the Templates to be Exported** section, select the template or templates that you want to export, then click **OK**.

Importing Templates

You can import a template after you have exported it. For information on how to export a template, see "Exporting Templates" on page 263.

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

2 Under **Management**, click **Workspace and Folder Templates**.



3 Click **Import**.

The **Import Templates** page is displayed.

4 Browse for and select the templates that you want to import, then click **OK**.

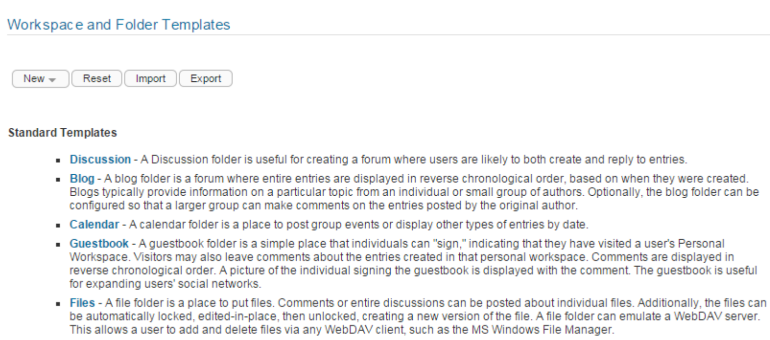
The imported templates are displayed in the Manage Workspace and Folder Templates page.

Reverting All Templates to the Factory Default

When you revert all templates to the factory default, you lose any modifications that you have made to existing templates, as well as any custom templates that you might have created.

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

2 Under **Management**, click **Workspace and Folder Templates**.



3 Click **Reset**, then click **OK**.

26 Creating and Managing Workflows

Workflows can improve efficiency in your organization by automating common business processes.

As an administrator for Novell Vibe, you have the ability to create workflows and make them available to all Vibe users. You can also import existing workflows and then tailor them to your specific organization.

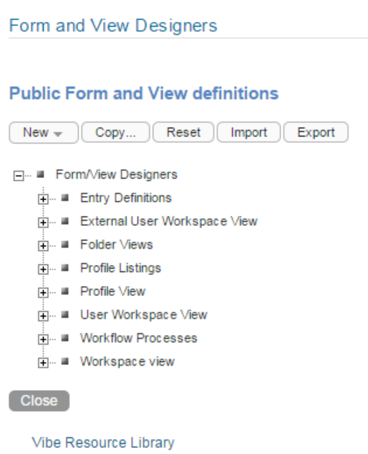
Examples of workflows include approving documents, ordering supplies, hiring new employees, requesting paid time off, and getting expense reimbursements.

Creating Global Workflows

You can create workflows that are accessible to all Novell Vibe users.

1 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

2 Under **System**, click **Form/View Designers**.



3 Follow the steps for creating and managing a workflow, as described in "Creating and Managing Workflows" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Remember that when you create workflows at the Administration level, the workflows that you create can be leveraged by all users in your Vibe site.

Downloading Existing Custom Forms and Workflows

The Micro Focus Vibe Resource Library provides a collection of existing Novell Vibe folder entry forms and workflows that have been designed to solve specific business problems. You can easily download the custom forms and workflows, then import them into your Vibe environment. You can further customize these forms and workflows to suit your individual business needs.

1. Visit the Micro Focus Vibe Resource Library (http://www.novell.com/products/vibe/resource-library/).
2. Select the custom form or workflow that you want to use in your Vibe environment.
3. In the **Attachment** section, click the `zip` file to download it.
4. Import the file into your Vibe environment and deploy it for use.

   For information on how to do this, follow the Micro Focus Vibe Resource Library Deployment Instructions (http://www.novell.com/products/vibe/resource-library/demos/form_workflow_deployment.html).

27 Viewing and Updating the Vibe License

Viewing the Vibe License

1 Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon .

2 Under **Management**, click **License**.

   The Vibe license is displayed.

3 (Conditional) If you have updated your Vibe license and the contents of the new license are not being displayed, click **Reload Vibe License**.

Updating the Vibe License

You update the Vibe license as described in “Updating Your Vibe License” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

28 Managing Email Configuration

After you enable email integration for the Vibe site as described in Chapter 11, "Configuring Email Integration," on page 165, you can further modify the way emails are managed on the Vibe site.

Configuring Outbound Email with TLS over SMTP

Depending on how your email application is configured, it may require that Vibe outbound email be configured with TLS over SMTP for secure email. Micro Focus GroupWise, for example, can be configured to require this. If you are using GroupWise or another email application that requires this type of configuration, you can configure Vibe with TLS over SMTP by using STARTTLS.

NOTE: In the Vibe installation program, on the Outbound Email Configuration page, ensure that you have selected **SMTP** in the **Protocol** drop-down list. For more information about outbound email configuration in the Vibe installation program, see "Gathering Outbound Email Information" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

To configure outbound email with TLS over SMTP:

1 Import the certificate from the email server into the Vibe Java keystore file (`cacerts`).

The default location for the Java keystore file is:

Linux:	`/usr/java/jdk`*`version`*`/jre/lib/security`
Windows:	`c:\Program Files\Java\jdk`*`version`*`\jre/lib/security`

2 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/ conf/Catalina/localhost`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\ conf\Catalina\localhost`

3 Open the `ssf.xml` file in a text editor.

4 Add the following attribute to the resource node that begins with `<Resource name="mail/SiteScapePool"` (this is the first resource node in the list):

```
mail.smtp.starttls.enable="true"
```

5 (Optional) To enable tracing of sent email to assist with debugging mail issues, add the following attribute to the same resource node:

```
mail.debug="true"
```

6 Stop and restart Vibe.

Customizing Email Templates

- "About Vibe's Email Templates" on page 272
- "Tips and Documentation" on page 272
- "Modifying the Template Files" on page 273
- "A Video Walkthrough" on page 273

About Vibe's Email Templates

Vibe generates email notifications using Apache Velocity version 1.5 templates.

You can customize the following templates, beginning with the Vibe 4.0.1 release:

Template Name	Purpose
footer.vm	Text or images applied at the end of each email
header.vm	Text or images applied at the beginning of each email
passwordChangedNotification.vm	Notification that user's password changed
publicLinkNotification.vm	Notification of a publicly available link to a file
selfRegistrationRequired.vm	Shared item notification to user who must register with Vibe in order to view it
sharedEntryInvite.vm	Shared file invitation to an existing Vibe user
sharedEntryNotification.vm	Shared file notification of change to existing Vibe user
sharedFolderInvite.vm	Shared folder invitation to existing Vibe user
sharedFolderNotification.vm	Shared folder notification of change to existing Vibe user
style.vm	CSS style sheet for email notifications
teaming.vm	Macros that get applied to all emails

Tips and Documentation

The following are tips about the template files in Vibe.

- Each template contains a brief explanation about what you can customize.

- Vibe system-generated emails contain both text and HTML MIME parts. You can customize these independently.
- You can customize by language to localize the emails your Vibe system generates.
- You can revert back to the default template by selecting a customize template in the list and then clicking the Delete button.
- Make sure you use the Velocity documentation (https://velocity.apache.org/engine/releases/velocity-1.5/user-guide.html).

  For example, one user assumed that the hash marks (#) indicated comments, when in fact they are part of many scripting languages, including Velocity.

Complete information and instructions for the Apache Velocity version 1.5 template language are available on the Apache Velocity Project website (https://velocity.apache.org/engine/releases/velocity-1.5/).

Modifying the Template Files

The default email templates that reside on the Vibe 4.0.4 system cannot be changed or deleted, but you can create and deploy customized copies of them by doing the following:

1. Download a template to your local disk by clicking it in the Email Templates dialog
2. Open it in a text editor
3. Save it on your local disk.
4. Upload the customized file by dragging and dropping it into the Email Templates dialog.

   The **Type** then changes to **Customized**.

A Video Walkthrough

To see a demonstration of the email template customization process for the Filr product, view the following video:

http://www.youtube.com/watch?v=AA4A-nG3dIY

The same principles apply to Vibe.

Configuring the Field that Vibe Uses When Sending Emails

By default, emails that are sent from Vibe are sent with the recipients in the **BCC** field. You can configure Vibe to use the **To** field rather than the **BCC** field for all sent messages.

Configuring Vibe in this way makes it so message recipients can see other message recipients in the email notification. For information about how to configure Vibe to send individual messages to each user rather than including multiple users on the same message, see "Configuring the Number of Users Who Can Be Included in the Same Email Notification" on page 274.

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Open the `ssf.properties` file in a text editor.

3 Search for the following line:

```
mail.notifyAsBCC=true
```

4 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the mail.notifyAsBCC=true line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `true` to `false`, so that the line now reads `mail.notifyAsBCC=false`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe to configure Vibe to use the **To** field rather than the **BCC** field when sending messages.

Configuring the Number of Users Who Can Be Included in the Same Email Notification

By default, Vibe imposes a limit of 500 message recipients for each email notification that Vibe sends. You might want to change this limit to 1 if you have configured Vibe as described in "Configuring the Field that Vibe Uses When Sending Emails" on page 273.

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
mail.rcpt.limit=500
```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `mail.rcpt.limit=500` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Change `500` to `1`, so that the line now reads `mail.rcpt.limit=1`.

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe to configure Vibe to include only one user in each email notification that is sent.

Configuring Vibe to Send Email Messages and Notifications from a Custom Address

For security reasons, your corporation's email system might be set up to automatically delete messages from internal users that are not sent from the corporate email system. If your corporate email system is configured in this way, email messages and notifications sent from Novell Vibe are automatically deleted.

You can configure Vibe to send email messages directly from the Vibe server, rather than from internal users. These are messages that are sent when a user performs an action that creates a message. For example, when a user shares a workspace with another Vibe user, a message is sent to the receiving user's email mailbox. By default, this message is sent from the internal user. However, you can configure Vibe to send such messages from the Vibe server itself. Configuring Vibe in this way enables email messages to be sent from Vibe, while maintaining the same level of security for your corporation.

By default, Vibe is configured to send messages from individual users in the following scenarios:

- When sending a workflow notification, as described in "Adding On-Entry or On-Exit Events" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.
- When sharing an entry, folder, or workspace, as described in "Sharing Workspaces, Folders, and Entries" in the *Micro Focus Vibe 4.0.5 User Guide*.
- When creating an entry, as described in "Creating a Folder Entry" in the *Micro Focus Vibe 4.0.5 User Guide*.

You can configure Vibe to send email messages from an external address for an individual zone or for the entire Vibe site:

- "Configuring a Zone-Specific Email Address for Sent Messages" on page 275
- "Configuring a Site-Wide Email Address for Sent Messages" on page 276

Configuring a Zone-Specific Email Address for Sent Messages

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2 Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.

3 Open the `ssf.properties` file in a text editor.

4 Search for the following line:

```
ssf.outgoing.from.address.<zone name>=zoned@company.com
```

5. Open the ssf-ext.properties file in a text editor.
6. Copy the ssf.outgoing.from.address.<zone name>=zoned@company.com line from the ssf.properties file to the bottom of the ssf-ext.properties file.
7. Replace <zone name> with the name of the Vibe zone that you want email messages to be addressed from and edit the email address to reflect your company's email.

   For example, if the name of your Vibe zone is kablink, and the name of your company is greenergy, the line would read:

   ```
   ssf.outgoing.from.address.kablink=zone@greenergy.com
   ```
8. Save and close the ssf-ext.properties file.
9. Close the ssf.properties file without saving it.
10. Stop and restart Vibe.

Configuring a Site-Wide Email Address for Sent Messages

1. Change to the following directory:

Linux:	/opt/novell/teaming/apache-tomcat/ webapps/ssf/WEB-INF/classes/config
Windows:	c:\Program Files\Novell\Teaming\apache-tomcat\ webapps\ssf\WEB-INF\classes\config

2. Make a backup copy of the ssf-ext.properties file, which is located in the same directory as the ssf.properties file.
3. Open the ssf.properties file in a text editor.
4. Search for the following line:

   ```
   ssf.outgoing.from.address=global@company.com
   ```
5. Open the ssf-ext.properties file in a text editor.
6. Copy the ssf.outgoing.from.address=global@company.com line from the ssf.properties file to the bottom of the ssf-ext.properties file.

   Edit the email address to reflect your company's email.

   For example, if the name of your company is greenergy, the line would read:

   ```
   ssf.outgoing.from.address=global@greenergy.com
   ```
7. Save and close the ssf-ext.properties file.
8. Close the ssf.properties file without saving it.
9. Stop and restart Vibe.

Enabling Users to Configure a Folder or External Email Address to Receive Sent Emails

Like a personal email Outbox for the Vibe site, users can configure a folder or external email address to receive all email messages that they send from the Vibe site. This can help users better track their activity.

To enable users to set up a folder or external email address in this way, Vibe administrators must ensure that the following prerequisites are met:

- Enable the Vibe site to allow incoming email.

  For information on how to enable Vibe to allow incoming email, see "Disabling/Enabling Inbound Email Postings" on page 166.

- Reset definitions on the Vibe site if the Vibe site was upgraded from a version of Vibe prior to 3.1. If you are installing Vibe 3.1 or later as a new installation, you do not need to reset the definitions.

  For information on how to reset the definitions, see "Resetting Your Definitions" in "Upgrade" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

NOTE: If you have made customizations to definitions throughout the Vibe site and you do not want your customizations to be overwritten, you can manually add a field to the User Profile form, rather than resetting the definitions for the Vibe site. To do this, add the **BCC Email Address** element to the **Contact Information** section of the **Profile Form Definition** for the User Profile. For more information on how to modify the User Profile definition, see "Customizing the Default User Profile View" on page 50.

For more information on how users can configure folders to receive sent emails, see "Setting Up a Folder or External Email Address to Receive All Sent Email Messages" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

Displaying the User's Profile Picture in Email Notifications

By default, a user's profile picture (avatar) is no longer included in email notifications sent from Vibe. This is because Micro Focus GroupWise does not always display the profile picture correctly.

To configure Vibe to always include the profile picture in email notifications:

1. Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes\config`

2. Make a backup copy of the `ssf-ext.properties` file, which is located in the same directory as the `ssf.properties` file.
3. Open the `ssf.properties` file in a text editor.
4. Search for the following line:

   ```
   email.showAvatarInHeader=false
   ```

5 Open the `ssf-ext.properties` file in a text editor.

6 Copy the `email.showAvatarInHeader=false` line from the `ssf.properties` file to the bottom of the `ssf-ext.properties` file.

7 Replace `false` with `true` so that the line now reads

```
email.showAvatarInHeader=true
```

8 Save and close the `ssf-ext.properties` file.

9 Close the `ssf.properties` file without saving it.

10 Stop and restart Vibe.

29 Managing the Lucene Index

For background information about the Lucene index, see "Understanding Indexing" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Starting and Stopping the Lucene Index Server

On Linux

Use the following commands to manually start and stop the Lucene Index Server:

```
/etc/init.d/indexserver start
/etc/init.d/indexserver stop
```

On Windows

Use the following command at a DOS command prompt to manually start the Lucene Index Server:

```
c:\Program Files\Novell\Teaming\luceneserver\indexserver\bin\
                                                    indexserver-startup.bat
```

To stop the Lucene Index Server, close the command prompt window where you started the Lucene Index Server.

Changing Your Lucene Configuration

The default Lucene Index Server configuration is appropriate for a medium-sized Novell Vibe site. If you have a larger Vibe site, you can change its Lucene Index Server configuration by rerunning the Vibe Installation program, selecting **Reconfigure Settings**, then selecting **Advanced**. For instructions, see "Changing Your Lucene Index Server Configuration" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Optimizing the Lucene Index

If you notice that search performance in Novell Vibe is becoming slower over time, you might want to optimize your Lucene index.

For a medium to large Vibe system, it is recommended that you run the optimization once a week. You should run the optimization during off hours or on weekends when the Vibe system is not being heavily used.

Optimizing the Lucene index does not repair a damaged or out-of-date index. To repair a damaged or out-of-date index, you must rebuild the index, as described in "Rebuilding the Lucene Index" on page 281.

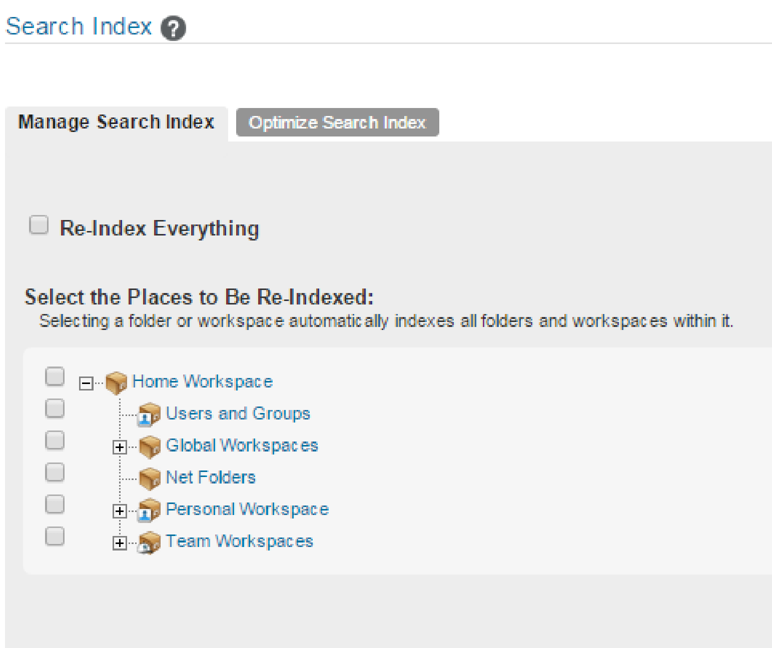
- "Optimizing a Single Search Index" on page 280
- "Optimizing the Search Index with Multiple Index Servers" on page 281

Optimizing a Single Search Index

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **Management**, click **Search Index**.



4 Click the **Optimize Search Index** tab.

5 Select **Run Immediately** if you want to run the optimization right now.

6 Select **Run at Scheduled Time**, then specify the days and times that you want the optimization to occur.

7 Click **OK**.

Optimizing the Search Index with Multiple Index Servers

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. In the **Search Index** section, click **Index**.
4. Click the **Optimize Search Index** tab.
5. Select **Run Immediately** if you want to run the optimization right now.
6. Select **Run at Scheduled Time**, then specify the days and times that you want the optimization to occur.
7. Select each node that you want to optimize.
8. Click **OK**.

Rebuilding the Lucene Index

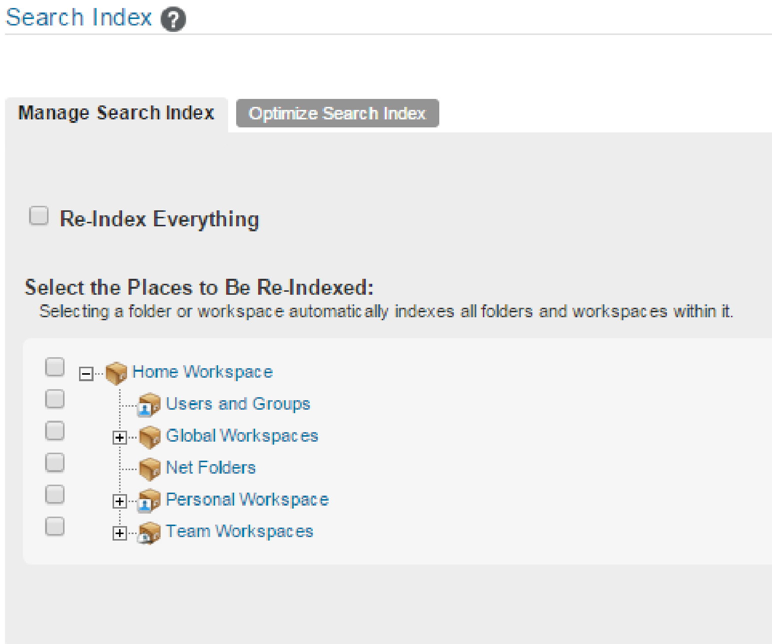
The Lucene index provides access to all data in your Novell Vibe site. If it becomes damaged or out-of-date for some reason, you can rebuild it. Users might first notice a problem with the Lucene index if they cannot find information that they know should be available on the Vibe site. If you are running multiple Lucene Index Servers, follow the instructions in "Performing Maintenance on a High Availability Lucene Index" on page 283.

The steps to reset the search index differ depending on whether you have multiple Lucene Index servers.

- "Rebuilding a Single Search Index" on page 281
- "Rebuilding the Search Index with Multiple Index Servers" on page 282

Rebuilding a Single Search Index

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. In the **Management** section, click **Search Index**.



4 To reindex the entire Vibe site, select **Re-Index Everything**.

Depending on the size of your Vibe site, this can be a very time-consuming process.

or

Select one or more parts of your Vibe site to reindex.

5 Click **OK** to start the indexing.

Users can still access the Vibe site during the indexing process, but search results might not be accurate until the index has been completely rebuilt.

A message notifies you when indexing is complete.

Rebuilding the Search Index with Multiple Index Servers

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 In the **Search Index** section, click **Index**.

4 To reindex the entire Vibe site, select **Re-Index Everything**.

Depending on the size of your Vibe site, this can be a very time-consuming process.

or

Select one or more parts of your Vibe site to reindex.

5 Select each node that you want to re-index.

6 Click **OK** to start the indexing.

Users can still access the Vibe site during the indexing process, but search results might not be accurate until the index has been completely rebuilt.

A message notifies you when indexing is complete.

Performing Maintenance on a High Availability Lucene Index

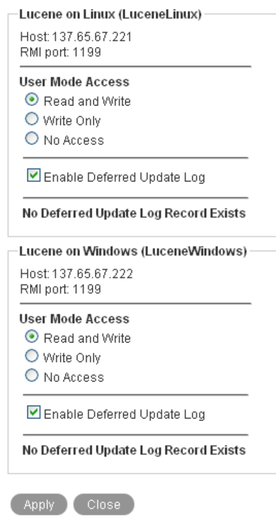
If you have a high availability Lucene configuration, you can take one Lucene node out of service for maintenance while other Lucene nodes continue to operate. Then you can synchronize the out-of-date Lucene node with the current indexing data.

1 Log in to the Micro Focus Vibe site as the Vibe administrator.

2 Take the Lucene node that needs maintenance out of service:

  2a Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

  2b Under **Search Index**, click **Nodes**.



  2c In the list, locate the node that needs maintenance.

  2d Make sure that **Enable Deferred Update Log** is selected.

  2e In the **User Mode Access** box, change **Read and Write** to **Write Only**.

  2f Click **Apply**, then click **Close**.

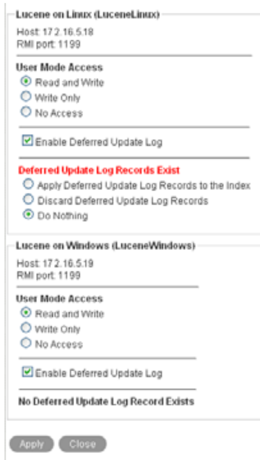
  The new setting is put into effect immediately, so that the Lucene node is no longer accessible to Vibe users.

3 Perform the needed maintenance on the Lucene server, then start the Lucene Index Server again.

4 Return the out-of-date Lucene node to full service:

  4a Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

  4b Under **Search Index**, click **Nodes**.



The out-of-date Lucene node is flagged with **Deferred Update Log Records Exist**.

The **User Mode Access** option shows **Read and Write** because this is the last selected setting. If you are checking the Tomcat `catalina.out` file, as described in "Observing Lucene Node Activity" in "Multi-Server Configurations and Clustering" in the *Micro Focus Vibe 4.0.4 Installation Guide*, Vibe is not actually accessing the out-of-date Lucene node because it is out of sync with the Vibe site.

4c Select **Apply Deferred Update Log Records to the Index**, then click **Apply**.

The Deferred Update Log options disappear if the update is successful.

4d Click **Close**.

The Lucene node that was out of service has now been updated with current indexing data.

30 Managing Database Logs and File Archives

Vibe allows you to manage the frequency in which database logs are deleted, as well as whether deleted files are archived.

- "Managing Database Logs" on page 285
- "Managing File Archiving" on page 285

Managing Database Logs

You can determine the frequency with which database logs (audit trail entries and change log entries) are deleted from the Vibe system.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Click **Database Logs and File Archiving**.

4 In the **Manage Database Logs** section, the following options are available:

   Automatically Delete Audit Trail Entries Older Than *xx* Days: Specify the maximum number of days to keep audit trail log entries before they are deleted. The default is 183 days (6 months). The allowed minimum is 30 days.

   Audit trail entries are used to build the Activity and Login reports. Removing older entries limits the possible time span for these reports. (For more information about these reports, see "Generating Reports" on page 294.)

   The Vibe desktop application relies on audit trail data when doing full synchronizations.

   Enable the Change Log: Select this option to enable users to track the edit history of folders, files, and entries. This includes:

   - Adding, modifying, deleting, and moving of entries, folders, and workspaces.
   - Changes to access control settings for entries, folders, and workspaces.
   - Changes to workflows, including starting, stopping, changing states, and timeouts.

   Automatically Delete Change Log Entries Older Than *xx* Days: Specify the maximum number of days to keep change log entries before they are deleted.

   Removing older log entries will limit how far back changes to an item can be traced.

5 Click **OK**.

Managing File Archiving

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Click **Database Logs and File Archiving**.

4 In the **Manage File Archiving** section, the following options are available:

   Enable Archiving of Deleted Files: Select this option to move files to the Vibe archive when they are deleted.

   Files in Mirrored Files folders cannot be archived.

5 Click **OK**.

31 Backing Up Vibe Data

Reliable backups are critical to the stability of your Novell Vibe site.

Locating Vibe Data to Back Up

In order to keep adequate backups of your Novell Vibe data, you must back up the following types of data.

Vibe File Repository

Platform	Default Location
Linux:	`/var/opt/novell/teaming`
Windows:	`c:\Novell\Teaming\filerepository`

For more information, see "Distributing Different Data Types to Different Locations" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Vibe Database

Database Server	Default Linux Location	Default Windows Location
MySQL	`/var/lib/mysql`	`c:\Program Files\MySQL\ MySQL Server` *`version`*`\Data`
Microsoft SQL	N/A	`c:\Program Files\Microsoft SQL Server\ MSSQL\Data`
Oracle	N/A	N/A
PostgreSQL	`/var/lib/pgsql`	`c:\Program Files\PostgreSQL\ PostgreSQL Server` *`version`*`\Data`

For more information, see "Creating the Vibe Database on a Remote Server" and "Running Multiple Database Servers" in "Multi-Server Configurations and Clustering" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Lucene Index

Platform	Default Location
Linux:	`/var/opt/novell/teaming/lucene/`*`zone_name`*
Windows:	`c:\Novell\Teaming\lucene\kablink`

For more information, see "Installing the Lucene Index Server on a Remote Server" and "Running Multiple Lucene Index Servers" in "Multi-Server Configurations and Clustering" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Certificates

If you have changed your password in the `server.xml` when creating a new keystore file (as described in "Do Not Change the Password for the Keystore File" on page 336), be aware that these changes are not preserved when you upgrade Vibe. You should make these changes again after upgrading Vibe rather than backing up the `server.xml` file.

- "Linux Locations" on page 288
- "Windows Locations" on page 288

Linux Locations

Certificate Type	Default Location
Tomcat:	`/opt/novell/teaming/apache-tomcat/conf/.keystore`
Java:	`/usr/lib/jvm/java-`*`version`*`/jre/lib/security/cacerts`

Windows Locations

Certificate Type	Default Location
Tomcat:	`c:\Program Files\Novell\Teaming\apache-tomcat\conf\.keystore`
Java:	`c:\Program Files\Java\jre`*`version`*`\lib\security\cacerts`

Scheduling and Performing Backups

You do not need to bring your Novell Vibe site down in order to perform backups. You might want to back up the Vibe file repository and the Vibe database every night, perhaps doing a full backup once a week and incremental backups on other days. You can back up the Lucene index whenever it is convenient. You can always reindex the Vibe site in order to re-create the Lucene index, but being able to restore one from backup can save time in case of an outage.

Restoring Vibe Data from Backup

If you need to restore your Novell Vibe site from a backup, restoring the same backup version for both the file repository and the database creates a Vibe site that is consistent within itself but might be missing information that was added after the backups were created. If you lose the file repository but not the database, you can restore the backed-up file repository and keep the more current database, but some entries then have files that are missing from the file repository. If you lose the database but not the file repository, you can run a report to identify entries created since the last database backup, as described in "Content Modification Report" on page 300. You can then notify the affected Vibe users that they need to re-create the entries that are not available in the backup.

Manually Restoring Individual Entries

All Vibe users can restore individual entries and attached files if the entry has been deleted but not yet purged. For information on how to do this, see "Restoring Items from the Trash" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*.

If an entry has been deleted and also purged from the Vibe site, it can usually be recovered from the archive store with the help of Novell Technical Support, but this is not an easy process. If an entry can be restored, it is not identical to the original entry in that the original entry ID is lost, the original creation and modification dates are lost, and some entry metadata is lost. Contact Novell Support (http://www.novell.com/support) for assistance.

32 Monitoring the Vibe Site

You can monitor activity on your Novell Vibe site by using Vibe reports and log files. You can also use JMX to monitor Vibe and to perform certain management functions.

- "Using JMX to Monitor the Vibe Site" on page 291
- "Generating Reports" on page 294
- "Using Log Files" on page 308
- "Checking the Vibe Site Software Version" on page 310

Using JMX to Monitor the Vibe Site

Java Management Extensions (JMX) is a Java technology for managing and monitoring applications, system objects, devices, and services. It is a lightweight, non-intrusive mechanism for gathering and monitoring useful runtime statistics. You can use JMX in addition to other tools that are included in the Vibe product to monitor your Vibe site.

- "Installing and Configuring JMX for Vibe" on page 291
- "Requiring Authentication When Accessing Vibe through JMX" on page 292
- "Using JConsole to Monitor the Vibe Site" on page 293

Installing and Configuring JMX for Vibe

1 Install Vibe as described in the *Micro Focus Vibe 4.0.4 Installation Guide*.

2 Navigate to the following directory on the Vibe server:

Linux:	`/opt/novell/teaming/apache-tomcat/conf`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\conf`

3 Open the `vibe.management.properties` file in a text editor.

4 Uncomment the following line:

```
#com.sun.management.jmxremote.port=8642
```

If this port is already in use on your server, change the port number to a port that is not in use.

5 (Recommended) To require authentication when accessing Vibe remotely through JMX, change the value of the following property to `true`:

```
com.sun.management.jmxremote.authentication=false
```

IMPORTANT: If you require authentication when accessing Vibe remotely through JMX, you must specify a password and restrict access to the password file in order for JMX to run, as described in "Requiring Authentication When Accessing Vibe through JMX" on page 292.

6 By default, SSL is not enabled when accessing Vibe through JMX. If the JMX user is accessing Vibe from within the firewall (which is recommended), there is no reason to require an SSL connection. If SSL is required by your organization, you can enable it.

   To require an SSL connection when accessing Vibe remotely through JMX, change the value of the following property to `true`:

   ```
   com.sun.management.jmxremote.ssl=false
   ```

   If you require an SSL connection when accessing Vibe through JMX, you must also set up a certificate and configure SSL as instructed in the online JMX documentation (http://download.oracle.com/javase/6/docs/technotes/guides/management/agent.html).

7 Save your changes, then close the text editor.

8 Stop and restart the Vibe server.

Requiring Authentication When Accessing Vibe through JMX

For security reasons, you must configure JMX to require authentication when accessing Vibe. In a clustered environment where a firewall is protecting your entire system but where there is no firewall running between individual nodes (which is the recommended configuration), it is extremely important that authentication is required when accessing Vibe through JMX in order to prevent an unauthorized entity from gaining access to the Vibe system.

After you have required authentication for the JMX user as discussed in "Installing and Configuring JMX for Vibe" on page 291, you need to finish setting up the authentication:

- "Specifying a Password for One or Both JMX User Types" on page 292
- "Restricting Access to the Password File" on page 293

Specifying a Password for One or Both JMX User Types

The properties discussed in this section represent JMX user types that can have access to Vibe through JMX. These are not Vibe users, but rather are JMX users. These users are not reflected anywhere in your Vibe system.

1 Navigate to the following directory on the Vibe server:

Linux:	`/opt/novell/teaming/apache-tomcat/conf`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\conf`

2 Open the `jmxremote.password` file in a text editor.

3 Uncomment one or both of the user types, depending on whether you want the JMX user to have Read Only access or Read/Write access through JMX. If you plan to use only one user type (for example, Read/Write), leave the other one commented out.

   Read Only access: Allows the JMX user to monitor or view Vibe data through JMX.

   To configure the JMX user to have Read Only access, uncomment the following user type:

   ```
   # monitorVibeRole XYZ
   ```

   Read/Write access: Allows the JMX user to perform state-changing actions such as initiating garbage collection of the JVM, changing an attribute of an MBean, or executing an operation on an MBean, as well as monitoring and viewing Vibe data through JMX.

To configure the JMX user to have Read/Write access, uncomment the following user type:

```
# controlVibeRole A&B
```

4 Replace the `XYZ` and/or `A&B` values to a secure password. For example, if you want to change the password for Read/Write access to `Novell`, the line would look like the following:

```
controlVibeRole Novell
```

Passwords are case-sensitive.

5 Save the `jmxremote.password` file and close the text editor.

Restricting Access to the Password File

The `jmxremote.password` file displays the user names of the JMX users who can access the Vibe site through JMX, together with the passwords for these users, in plain text. For this reason it is important that you restrict access to this file to only the file owner, which is the operating system account where the Vibe server is running.

- "Restricting Access to the Password File on Linux" on page 293
- "Restricting Access to the Password File on Windows" on page 293

Restricting Access to the Password File on Linux

If your Vibe server is running on a Linux operating system, the file permissions are changed automatically when Vibe is installed. (The Vibe program runs this command: `chmod 600 vibe.jmxremote.password`.)

Restricting Access to the Password File on Windows

If your Vibe server is running on a Windows operating system, you must change the permissions manually after Vibe is installed. For instructions on how to set file permissions on Windows, see How to Secure a Password File on Microsoft Windows Systems (http://download.oracle.com/javase/6/docs/technotes/guides/management/security-windows.html).

Using JConsole to Monitor the Vibe Site

JConsole is a Java monitoring tool that comes with JDK. You can use JConsole to monitor your Vibe site through JMX.

- "Starting JConsole" on page 293
- "Using JConsole to Monitor Vibe" on page 294
- "Using Zenoss Core to Supplement JConsole Monitoring" on page 294

Starting JConsole

Because JConsole requires a considerable amount of system resources in order to run, you should not run JConsole from the same machine where Vibe is running. The section describes how to connect JConsole to Vibe from a remote machine.

The machine that you run JConsole from must have a JDK installed.

1 Navigate to the location where your JDK is installed, then in the `bin` directory launch following file appropriate for your operating system:

Linux: `jconsole`

Windows: `jconsole.exe`

The New Connection dialog box is displayed.

2 Select **Remote Process**, then specify the hostname and port number of the server where Vibe is running.

3 In the **Username** and **Password** fields, specify the user name and password that you created in "Specifying a Password for One or Both JMX User Types" on page 292.

4 Click **Connect**.

The Java Monitoring & Management Console is displayed.

Using JConsole to Monitor Vibe

JConsole contains several tabs that help you monitor various aspects of your server. Information specific to Vibe is found in the **MBeans** tab in the **Vibe** folder. For specific information about the other tabs in JConsole, see Using JConsole (http://download.oracle.com/javase/6/docs/technotes/guides/management/jconsole.html).

Using Zenoss Core to Supplement JConsole Monitoring

Zenoss Core is not a replacement for JConsole, but it can provide additional monitoring functionality. Zenoss provides the following capabilities:

- Define alerts on an MBean attribute based on the attribute's acceptable value range, without relying on the JMX notification mechanism.
- Display performance graphs to view how data points change over time (JConsole displays only the current snapshot).

For more information about Zenoss, see Zenoss Core - Enterprise IT Monitoring (http://sourceforge.net/projects/zenoss/).

Generating Reports

Most Novell Vibe reports are created in CSV format, so that you can import them into a spreadsheet and easily manipulate the data to suit your needs. The default CSV filename is `report.csv`. If you create multiple reports without manually renaming them, the default filename is incremented (`report-`*`n`*`.csv`). The default location to save the report varies by platform:

Linux: `/tmp`

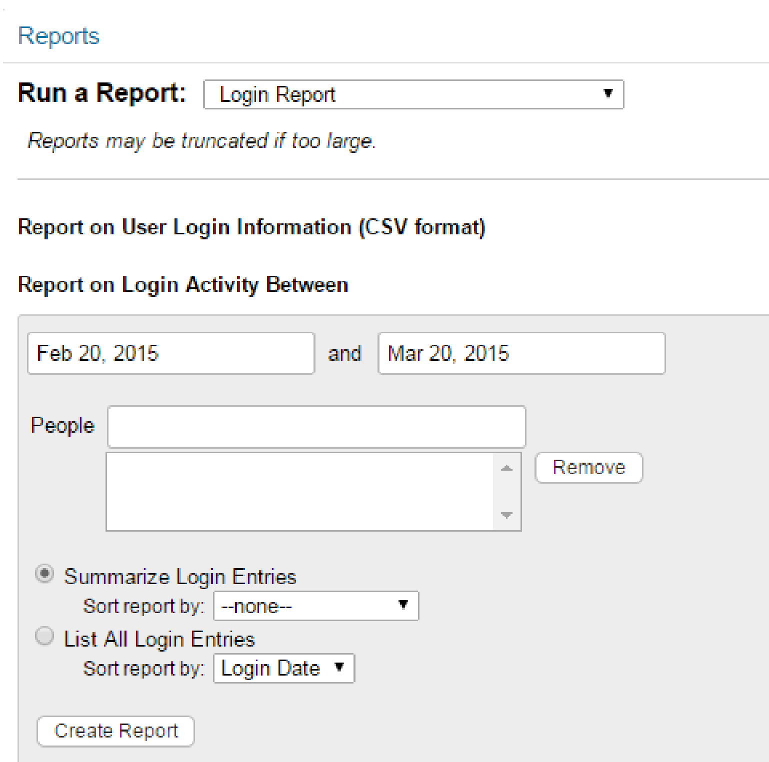
Windows: Your current Windows default directory

- "Login Report" on page 295
- "User Activity Report" on page 296
- "User Access Report" on page 298
- "Content Modification Report" on page 300
- "Data Quota Exceeded Report" on page 302

Login Report

The Login report lists the Vibe users who have logged in to the Vibe site during a specified period of time. In addition, it can include a dated list of every login by each user.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. Under **System**, click **Reports**.
4. In the **Run a Report** drop-down list, select **Login Report**.



5. Specify the date range for the Login report.
6. Leave the **People** field blank to list all user logins.

   or

   In the **People** field, begin typing the first name of a Vibe user, then in the drop-down list of names that match what you have typed, select a user whose logins you want to be reported. Repeat this process to include multiple users in the report.
7. Select the type of Login report that you want to generate.

Summarize Login Entries: Lists how many times the selected users have logged into the Vibe site. In the **Sort Report By** drop-down list, select **User**, **Last Login**, or **Number of Logins** to organize the data.

List All Login Entries: Lists each individual user login and includes the following data about the action:

- First name
- Last name
- User name
- Date
- Time

In the **Sort report by** drop-down list, select **Login Date** or **User** to organize the data most helpfully.

8 Click **Create Report** to generate the Login report.

9 Select a text editor to view the report in, then click **OK**.

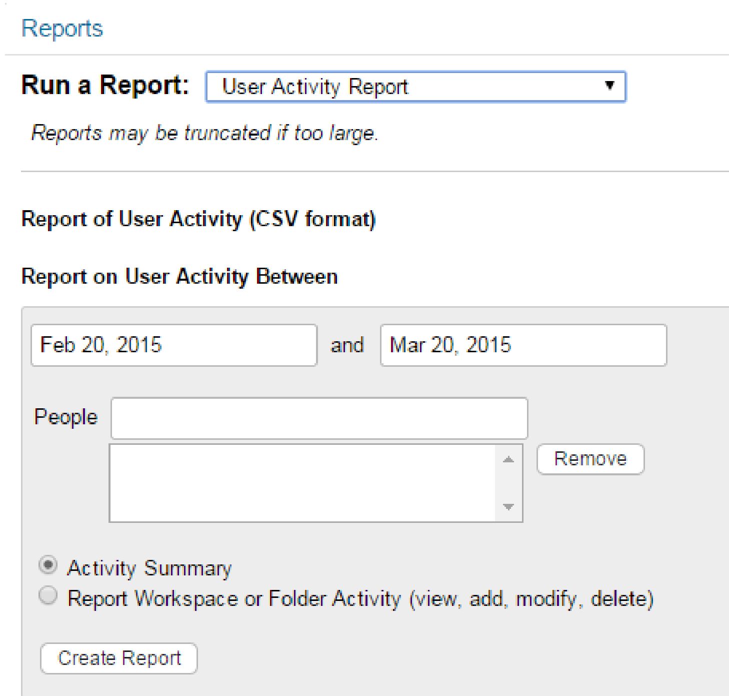
For a short report, you might obtain the information you need by viewing the CSV file.

10 (Optional) Save the CSV file with a meaningful name in a convenient location, then retrieve it into a spreadsheet program for further examination.

User Activity Report

The User Activity report lists how many times specified users have viewed, added, modified, or deleted content on the Vibe site during a specified period of time. In addition, it can include the date and time of each action, along with the location of the action.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. Under System, click **Reports**.
4. In the **Run a Report** drop-down list, select **User Activity Report**.



5 Specify the date range for the User Activity report.

6 Leave the **Select User** field blank to list all user activity.

or

In the **Select User** field, start typing the first name of a Vibe user.

In the drop-down list of names that match what you have typed, select a user whose activity you want to be reported. Repeat this process to include additional users.

7 Select the type of User Activity report that you want to generate.

Activity Summary: Lists how many times the selected users have performed the following actions in the Vibe site:

- View
- Add
- Edit
- Delete (purge)
- Pre-Delete (delete but not purge)
- Restore (restore a deleted item that has not been purged)

Report Workspace or Folder Activity: Lists each individual user action and includes the following data about the action:

- User
- Activity
- Date
- Time
- Folder
- Entry title
- Entry type

8 Click **Create Report** to generate the User Activity report.

9 Select a text editor to view the report in, then click **OK**.

For a short report, you might obtain the information you need by viewing the CSV file.

10 (Optional) Save the CSV file with a meaningful name in a convenient location, then retrieve it into a spreadsheet program for further examination.

User Access Report

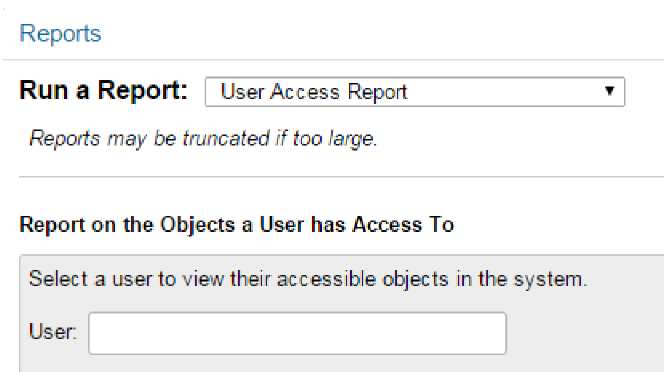
The User Access report lists the locations on the Vibe site where a specified user has access rights. In addition, you can view, and if necessary, change or remove the access rights for any location. This report is especially useful on Vibe sites where Guest user access has been granted, as described in "Setting Up Guest Access for the Vibe Site" on page 105.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

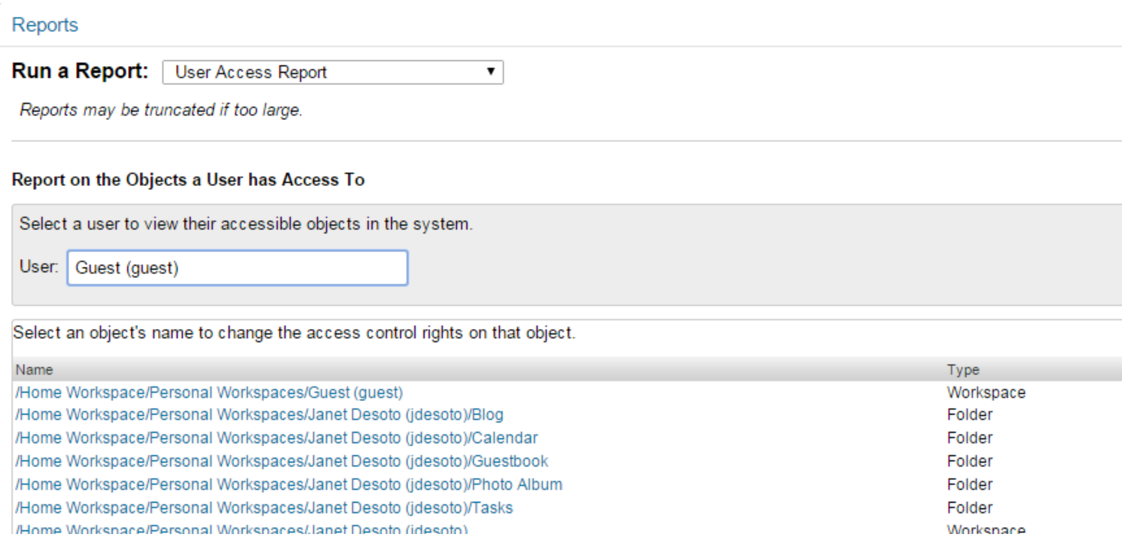
3 Under System, click **Reports**.

4 In the **Run a Report** drop-down list, select **User Access Report**.



5 In the **User** field, begin typing the first name of a Vibe user.

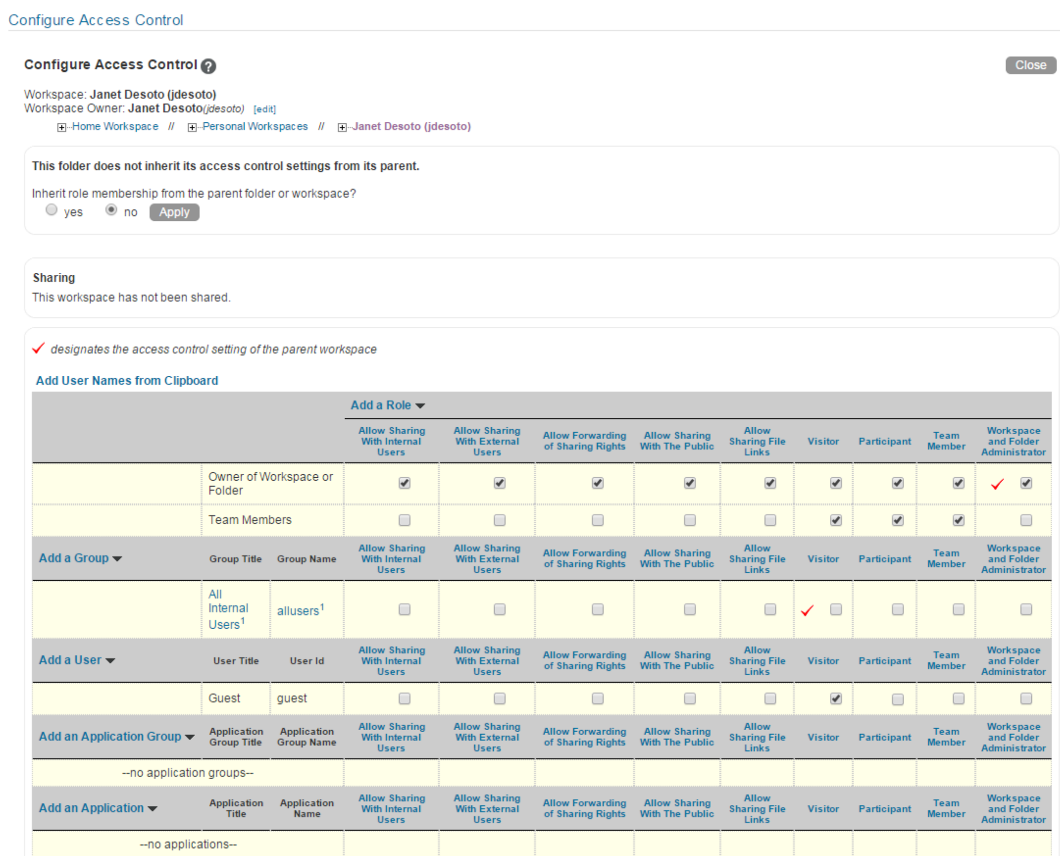
6 In the drop-down list of names that match what you have typed, select the user whose site access you want to be reported.



In this example, the Guest user has access to the Guest workspace and also to Janet DeSoto's personal workspace. This could be appropriate if Janet DeSoto's job is to maintain a publicly available workspace, but would not be appropriate if the Guest access has been granted in error.

7 (Conditional) If you want to change the current access:

7a Click the name of a location to display the Configure Access Control page for that location.



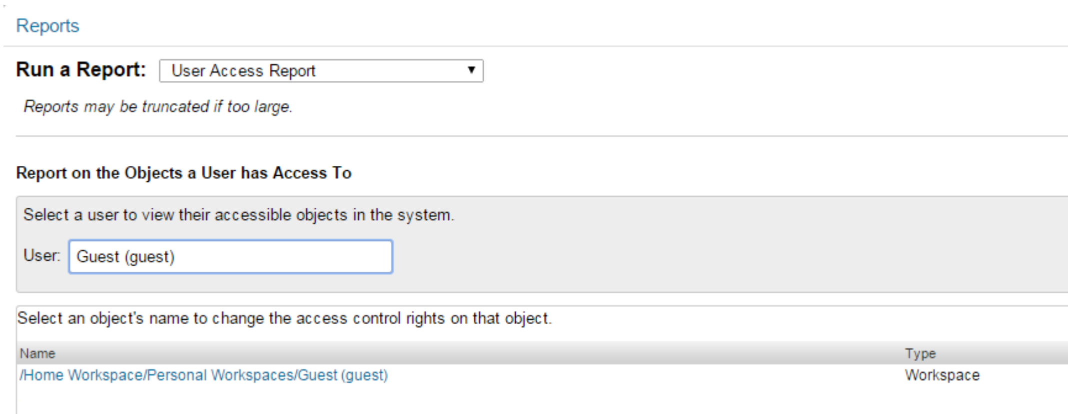
In this example, the Guest user has been granted Visitor access to Janet DeSoto's personal workspace.

7b Select or deselect access rights as needed.

7c Click **Save Changes**, then click **Close** to return to the User Access Report page

7d Rerun the report to view the results of your changes.

For example, if you removed the Guest access rights from Janet DeSoto's personal workspace, her workspace is no longer listed in the User Access report for the Guest user.



8 (Conditional) If you want to save the user access information, select it and copy it into a text editor.

9 Click **Close** when you are finished checking user access rights.

Content Modification Report

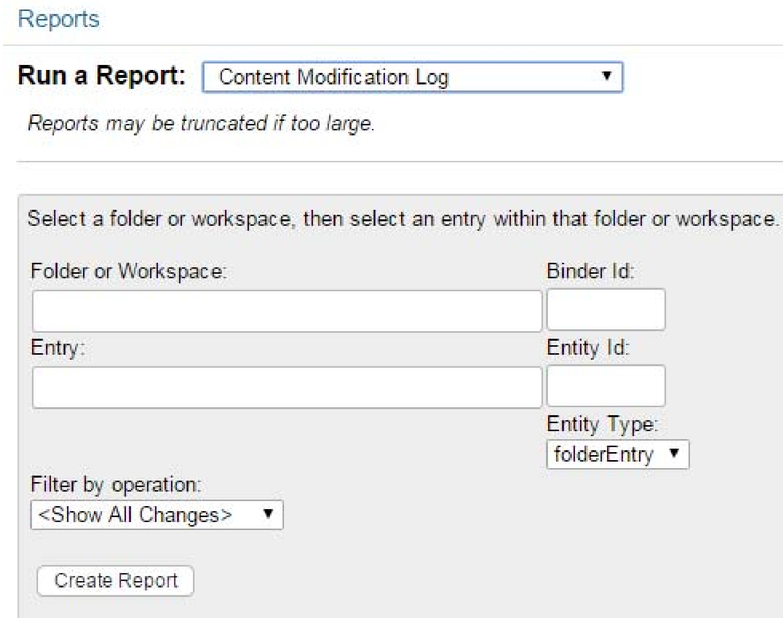
The Content Modification report lists changes to workspaces, folders, and folder entries, as well as users, groups, access rights, and workflows. By generating a Content Modification report, you can determine who has performed any of the following actions:

- Added, modified, moved, or deleted a workspace
- Added, modified, moved, or deleted a folder
- Added, modified, renamed, or deleted a file or one of its versions
- Added, modified, moved, or deleted an entry

  For purposes of this report, users and groups are handled as if they are folder entries.
- Started or modified a workflow
- Modified or deleted access rights

The Content Modification report can also help you recover data that has been accidentally deleted.

1. Log in to the Vibe site as the Vibe administrator.
2. Determine the exact name of the workspace, folder, file entry, and so on where you want to check for content modifications.
3. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
4. Under System, click **Reports**.
5. In the **Run a Report** drop-down list, select **Content Modification Log**.



6 Fill in the fields to specify where to check for content modifications and the type of modifications to check for:

Folder or Workspace: Start typing the name of a folder or workspace. In the drop-down list of names that match what you have typed, select the folder or workspace where you want to check for content modifications. The internal ID of the folder or workspace is displayed for reference.

Entry: (Optional) To restrict the content modification check to a specific entry in a folder, start typing text in the title of the entry. In the drop-down list of entry titles that match what you have typed, select the entry where you want to check for content modifications. The internal ID of the entry is displayed for reference.

Entity Type: (Optional) To further restrict the content modification check, select one of the following:

- Workspace (not the contents of the workspace, but the workspace itself)
- Folder (not the contents of the folder, but the folder itself)
- Folder entry (the contents of the folder entry)
- Profiles (the contents of the Personal Workspaces folder where there is a personal workspace for each user)
- User (the contents of a user's personal profile, such as the user's name, email address, and locale)
- Group (the contents of the group)

Filter by Operation: Further restrict the content modification check by selecting a specific action performed on the selected workspace, folder, or entry (add, modify, rename, delete, and so on).

7 Click **Create Report** to generate the Content Modification report.

The results are displayed as an XML file.

```
<folder databaseId="59" logVersion="1" operation="addBinder" modifiedBy="jchavez"
modifiedOn="Fri Feb 18 16:14:16 GMT 2011">
  <_entryAcl>all</_entryAcl>
  <_folderAcl>2 own team</_folderAcl>
  <_teamAcl>xx</_teamAcl>
  <historyStamp author="8" when="18 Feb 2011 16:14:16 GMT" name="created"/>
  <historyStamp author="8" when="18 Feb 2011 16:14:16 GMT" name="modified"/>
  <property name="parentBinder">58</property>
  <property name="entryDef">402883c6115753d8011157619e35000b</property>
  <attribute name="iconName" type="string">/icons/folder_blue_blog.gif</attribute>
  <attribute name="title" type="string">Blog</attribute>
  <property name="library">false</property>
  <property name="inheritFunctionMembership">true</property>
  <property name="inheritDefinitions">false</property>
  <property name="inheritTeamMembers">true</property>
  <property name="uniqueTitle">false</property>
  <property name="teamMembers"/>
</folder>
```


8. (Conditional) If the results are too extensive, restrict the scope of the content modification check until you locate the modification that you are seeking.
9. Click **Close** when you are finished checking for content modifications.

A specialized use of the Content Modification report is to restore accidentally deleted data. For example, you can use the following steps to recover an accidentally deleted folder entry:

1. Run the Content Modification report to list all entry deletions in the folder where the entry was accidentally deleted.
2. Record the entry ID of the deleted entry.
3. Run the Content Modification report on the entry ID, selecting **folderEntry** in the **Entity Type** field.
4. Use the modification history of the entry to reconstruct the accidentally deleted entry.

Data Quota Exceeded Report

The Data Quota Exceeded report lists individual users who have exceeded the data quota. The report provides a spreadsheet with the following information for each user:

- **Data Quota Used (MB):** Displays the amount of disk space the user is currently using.
- **Data Quota:** Displays the user’s individual quota if one has been set.

  For information on how to set a quota for individual users, see “Managing Workspace and Folder Data Quotas” on page 241.
- **Max Group Quota (MB):** Displays the largest data quota for any group that the user is a member of. Users are assigned the highest of all data quotas for any group for which they are a member.
- **Default Data Quota (MB):** Displays the site-wide default quota.

  For information on how to set a default data quota, see “Managing Workspace and Folder Data Quotas” on page 241.

To generate the Data Quota Exceeded report:

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.
3. Under **System**, click **Reports**.
4. In the **Run a Report** drop-down list, select **Data Quota Exceeded Report**.

5 Click **Create Report** to generate the report.

The report is launched in a spreadsheet.

Data Quota Highwater Exceeded Report

The Data Quota Highwater Exceeded report lists individual users who have exceeded the data quota high-water mark. The report provides the following information for each user:

- **Data Quota Used (MB):** Displays the amount of disk space the user is currently using.
- **Data Quota:** Displays the user’s individual quota if one has been set.

  For information on how to set a quota for individual users, see “Managing Workspace and Folder Data Quotas” on page 241.
- **Max Group Quota (MB):** Displays the largest data quota for any group that the user is a member of. Users are assigned the highest of all data quotas for any group for which they are a member.
- **Default Data Quota (MB):** Displays the site-wide default quota.

  For information on how to set a default data quota, see “Managing Workspace and Folder Data Quotas” on page 241.

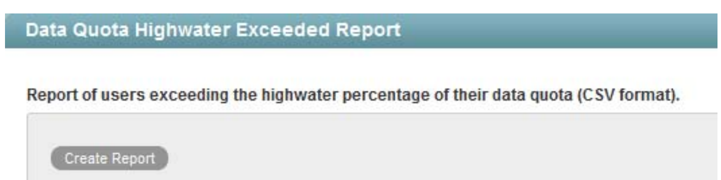
To generate the Data Quota Highwater Exceeded report:

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under System, click **Reports**.

4 In the **Run a Report** drop-down list, select **Data Quota Highwater Exceeded Report**.



5 Click **Create Report** to generate the report.

The report is launched in a spreadsheet.

Disk Usage Report

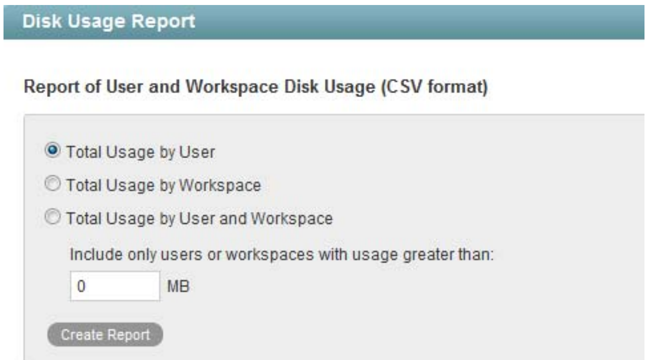
The Disk Usage report lists the amount of disk space for workspaces on the Vibe site by user, by workspace, or by both. In addition, you can restrict the reporting to only those workspaces that exceed a specified number of megabytes.

1 Log in to the Vibe site as the Vibe administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .

3 Under System, click **Reports**.

4 In the **Run a Report** drop-down list, select **Disk Usage Report**.



5 Select the type of Disk Usage report that you want to generate.

Total Usage by User: Lists all Vibe users whose disk space usage is above the amount specified in the **Usage Greater Than** field.

Total Usage by Workspace: Lists all workspaces where disk space usage is above the amount specified in the **Usage Greater Than** field. Disk space usage for each folder in each workspace is listed separately. The data is organized by workspace and folder ID.

Total Usage by User and Workspace: Combines the user and workspace data into a single report.

Include only users or workspaces with usage greater than: Specify the number of megabytes above which you want to list disk space usage. This eliminates smaller disk space usages from the report.

6 Click **Create Report** to generate the Disk Usage report.

7 Select a text editor to view the report in, then click **OK**.

For a short report, you might obtain the information you need by viewing the CSV file.

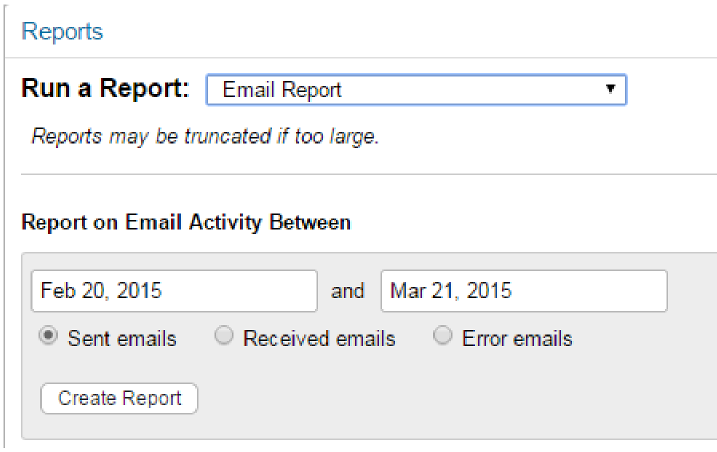
8 (Optional) Save the CSV file with a meaningful name in a convenient location, then retrieve it into a spreadsheet program for further examination.

9 Click **Close** when you are finished checking disk space usage.

Email Report

The Email Report lists mail messages that have been sent from and into the Vibe site. It also lists email errors that have been encountered.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. Under System, click **Reports**.
4. In the **Run a Report** drop-down list, select **Email Report**.



5. Specify the date range for the Email report.
6. Select whether you want a report on email that was sent from Vibe, email that was sent into Vibe, or email errors that occurred.
7. Click **Create Report**.

   The report contains the following information:

   Send Date: Date when the email was sent.

   From Address: Address that the email was sent from.

   This is the email address that the user has defined in his or her user profile.

   To Address: Address that the email was sent to.

   This is the email address if the message was sent from Vibe, or it is the folder or workspace if the message was sent into Vibe.

   Type: For messages that are sent from Vibe, this is the action that caused the message to be sent. For example, `workflowNotification` indicates that the email message was sent as a result of a workflow notification. For messages that are sent into Vibe, this is `emailPosting`, which indicates that the email message was converted to a Vibe entry via the internal Email Posting Agent.

   Status: Status of the message, such as Sent or Received.

   Subject Line: Subject line of the message.

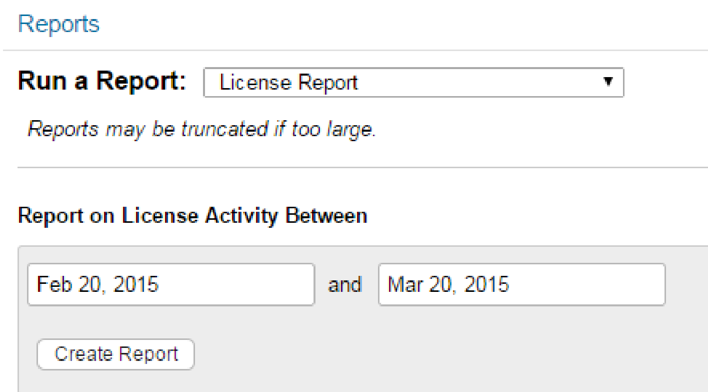
   Attached Files: Filename of any attachments that were included in the email message.

   Errors: Any errors that are associated with the email message.

License Report

The License report lists information about your Vibe license, as well as information about the number of users in your Vibe site and how many of those users have accessed the site.

1 Log in to the Vibe site as the Vibe administrator.
2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3 Under System, click **Reports**.
4 In the **Run a Report** drop-down list, select **License Report**.



5 Specify the date range for the License report, then click **Create Report**.

The License report lists the following information:

- Vibe version
- User access information
  - **Current Number of Local Users:** Number of local users accessing the system at the precise moment when you view the license report
  - **Current Number of External Users:** Number of external users accessing the system at the precise moment when you view the license report
  - **Current Number of LDAP Synchronized Users:** Number of LDAP-synchronized users accessing the system at the precise moment when you view the license report
  - **Current Active User Count:** Number of users who have accessed the Vibe system in the past 365 days.
  - **Guest Access Enabled:** Displays whether Guest access is currently enabled on the Vibe site.
- License information
  - License key type
  - Date the license key was issued
  - Date range when the license key is valid
- Allowed number of registered users during the date range
- Allowed number of external users during the date range

- List of dates in the date range with the following user license information:
  - **Local and External Users:** The user account was created within Vibe, and is not being synchronized from an LDAP directory.
  - **Users Synchronized from LDAP:** The user account was created from an LDAP source. (Only synchronized accounts that are not marked as Deleted or Disabled are counted.)
  - **Users Who Used Vibe During the Previous 365 Days:** Users who have logged in at least once in the past 365 days.

    User logins are counted only after your Vibe system is upgraded to Vibe 3 or later. The number of users who have logged in is always `0` for dates prior to the upgrade to Vibe 3 or later.

    To see how many people accessed the Vibe site prior to the upgrade to Vibe 3 or later, or just for more detailed information in this area, run the Login report. For more information about the Login report, see "Login Report" on page 295.

   The Vibe software does not limit the number of Vibe users that you can create, but sites where Vibe licenses have been purchased and the Vibe software installed are periodically audited against their purchased number of licenses.

6. Click **Close** when you are finished reviewing the License report.

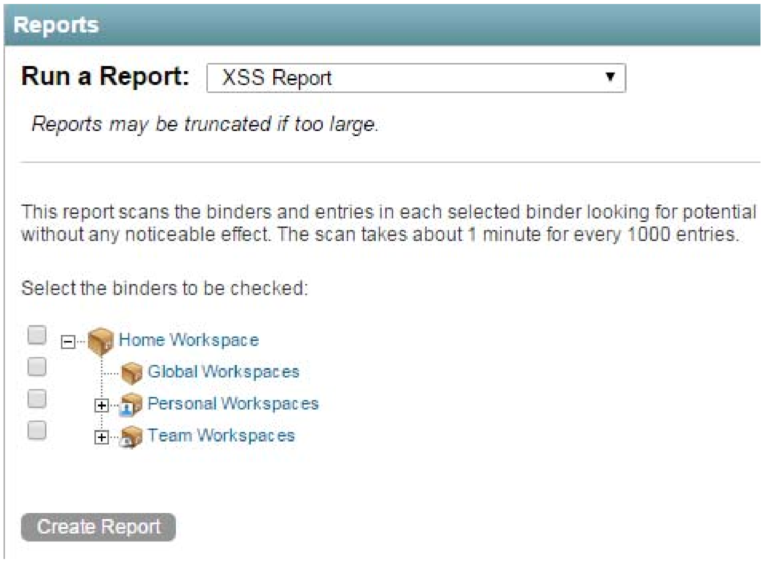
For information on how to install a new Vibe license, see "Updating Your Vibe License" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

XSS Report

Cross-site scripting (XSS) is a client-side computer attack that is aimed at web applications. Because XSS attacks can pose a major security threat, Novell Vibe contains a built-in security filter that protects against XSS vulnerabilities. For more general information about XSS, see "Securing the Vibe Site against XSS" on page 355.

The XSS report in Vibe lets you remove potentially harmful XSS threats from your Vibe site.

1. Log in to the Vibe site as the Vibe administrator.
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon .
3. Under System, click **Reports**.
4. In the **Run a Report** drop-down list, select **XSS Report**.



5 Select the workspace or folder where you want to run the report. Any sub-workspaces or sub-folders of the workspace or folder that you select are included in the report.

6 Click **Create Report**.

IMPORTANT: Because XSS attacks often are designed to wait for users with extra privileges (such as the administrator) to view the page where the attack was set, it is important that you don't navigate to the page after you run the report.

For information about how to run the XSS report and safely remove XSS threats, see "TID 7007381: Running the XSS Report in Micro Focus Vibe" in the Novell Support Knowledgebase (http://www.novell.com/support).

Using Log Files

Vibe Log File

The Novell Vibe log file (`ssf.log`) is available from the Vibe site.

1 Log in as the Vibe site administrator.

2 Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

3 Under **System**, click **Reports**, click **System Error Logs**.

4 In the **Run a Report** drop-down list, select **System Error Logs**.

5 Click **Download Log**.

You are prompted to open or save a file named `logfiles.zip`, which contains the current `appserver.log` file. This file contains any stack traces or warning messages because of unexpected events encountered by the Vibe program.

6 Save the `appserver.log` file to a convenient location on the Vibe server.

   This file is helpful when you need assistance resolving a problem with your Vibe site.

If you are unable to start Vibe and therefore cannot retrieve the log file as described above, the Vibe log file is also available in the following directory of your Vibe installation:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/logs`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\ webapps\ssf\WEB-INF\logs`

Tomcat Log File

In addition to the Novell Vibe error log file (`ssf.log`), the Tomcat error log file (`catalina.out` on Linux and `stdout_*.log` on Windows when Vibe runs as a service) is also useful. The Tomcat log file contains more information than the Vibe log file, because it includes problems encountered by Tomcat outside of the Vibe application itself. The location of the Tomcat log file varies by platform:

Linux:	`/opt/novell/teaming/apache-tomcat/logs`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\logs`

NOTE: When Vibe and Tomcat run as a Windows application, rather than as a Windows service, the information displayed in the command prompt window where you started Vibe is your only source of information. The data displayed in the command prompt window is not logged by Tomcat on Windows.

The Tomcat log file provides the following useful information:

- At the top, the Tomcat log file lists Tomcat startup messages.
- The System Properties section lists information about the supporting software packages that Tomcat relies on (for example, Java) and information about their current location and configuration.
- The System Environment section lists the currently set environment variables (for example, `HOSTNAME`, `PATH`, and `JAVA_HOME`).
- Exception and error data includes sufficient information for you to determine what user was trying to perform what action in what location on the Vibe site, to help you isolate and reproduce the problem.

  NOTE: The Novell Vibe product name prior to version 3 is Novell Teaming. If your Vibe site was originally installed as a Teaming 2.0 or Vibe site, the root of your site is referred to as `org.kablink` in the Tomcat error log. If you updated from a Teaming 1.0 site or a Teaming 2.0 beta site, the root of your site is referred to as `com.liferay`.

This file is helpful when you need assistance resolving a problem with your Vibe site.

Adjusting the Log Level for the Tomcat Log File

The log levels for various Tomcat functions are set in the `log4j.properties` file. Each type of information that is logged can have a log level of INFO, WARN, ERROR, FATAL, or DEBUG, depending on the type and quantify of information that you want logged. Some lines in the log4j.properties file are commented out with a pound sign (#), so that no information of that type is gathered. You can change the log level for each type of information and comment or uncomment lines to adjust the information gathered in the Tomcat log file to meet your troubleshooting needs.

1. Open the log4j.properties file in a text editor.

   The location of the log4j.properties file varies by platform.

Linux:	/opt/novell/novell/teaming/apache-tomcat/conf
Windows:	c:\Program Files\Novell\Teaming\apache-tomcat\conf

2. Change log level settings as needed for the type of information you want to gather.
3. Comment or uncomment lines, depending on the type of information you want to gather.
4. Save the log4j.properties file, then exit the text editor.
5. Stop Vibe, then start Vibe to put the new logging level into effect.

Checking the Vibe Site Software Version

To display the version number and software date of the Novell Vibe software:

1. Log in to the Vibe site as the Vibe administrator
2. Click your linked name in the upper right corner of the page, then click the **Administration Console** icon.

   The Vibe software version and date are displayed.

33 Reconfiguring the Vibe Site

Many aspects of your Novell Vibe site can be changed when you are logged in to the Vibe site as the Vibe administrator. Some aspects of reconfiguring the Vibe site require you to rerun the Vibe installation program, as described in “Setting Configuration Options after Installation” in “Advanced Installation and Reconfiguration” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

- “Basic Installation” on page 311
- “Advanced Installation” on page 312

Basic Installation

The configuration settings that can be changed using a Basic installation are:

Location of TrueType Fonts for Stellent Converters
Default Locale for Novell Vibe
Network Information
- Host
- HTTP Port and Secure HTTP Port
- Listen Port and Secure Listen Port
- Shutdown Port and AJP Port

WebDAV Authentication Method
Database Selection
- Database Type
- JDBC URL
- Credentials

Java JDK Location
- Java Heap Size

Outbound Email Configuration
- Protocol
- Host, Port, and Time Zone
- User name, Password, and Authentication
- Allow Sending Email to All Users

Inbound Email Configuration
- Internal SMTP Email Server
- SMTP Bind Address
- SMTP Port
- Announce TLS

For information about these basic configuration options, see “Planning a Basic Vibe Installation” in “Basic Installation” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Advanced Installation

An Advanced installation includes the options available in a Basic installation, as well as the following additional options:

- Web Services
  - Enable WSS Authentication
  - Enable Basic Authentication
  - Enable Token-Based Authentication
  - Enable Anonymous Access
- Lucene Configuration
- RSS Configuration
  - Max Elapsed Days
  - Max Inactive Days
- Presence Configuration
- Reverse Proxy Configuration
  - Access Gateway Address
  - Logout URL
  - WebDAV Access Gateway Address
- Integration with IIS for Windows Authentication
- Mirrored Folder Resource Driver Configuration
- Vibe Cluster Configuration

For information about these advanced configuration options, see “Planning an Advanced Vibe Installation” in “Advanced Installation and Reconfiguration” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

III Interoperability

Novell Vibe can be used in conjunction with various other software products. By incorporating these products into your Vibe system, you can add functionality, increase security, and maximize the value of Vibe.

34 NetIQ Access Manager

Using Micro Focus Vibe in conjunction with NetIQ Access Manager adds enterprise-level security to your Vibe system.

Only a version of Access Manager that supports Transport Layer Security (TLS) can be used when using Access Manager with Vibe. For information about which versions of Access Manager support TLS and how to enable it, see *Enabling Transport Layer Security 1.1 and 1.2 for Access Manager* (https://www.netiq.com/documentation/netiqaccessmanager4/enable_tls_nam40/data/enable_tls_nam40.html#).

IMPORTANT: When NetIQ Access Manager (or another single sign-on tool) is used in conjunction with your Vibe system, external users and the Guest user cannot access your Vibe site.

For more information about external users in Vibe, see "Understanding External Users" on page 125.

Before you can access your Vibe site through NetIQ Access Manger, you must first configure specific protected resources in Access Manager to be public, as described in Chapter 8, "Allowing Access to the Vibe Site through NetIQ Access Manager," on page 137.

Furthermore, you can configure NetIQ Access Manager to work with Micro Focus Vibe in the following ways:

- Configure NetIQ Access Manager to provide single sign-on access to the Vibe site.

  For more information, see "Configuring Single Sign-On with Novell Access Manager" in the *Micro Focus Vibe 4.0.4 Installation Guide*.
- Configure NetIQ Access Manager to allow access to iOS and Android mobile applications for Vibe.

  For more information, see "Configuring Mobile Device Access with NetIQ Access Manager" on page 114.

When you set up NetIQ Access Manager to work with Vibe, ensure that you specify the correct HTTP/HTTPS port numbers during the Vibe installation, as described in "HTTP/HTTPS Ports When You Use Novell Access Manager with Vibe" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

35 Internet Information Services (IIS)

You can integrate Micro Focus Vibe with Internet Information Services (IIS) to achieve Integrated Windows Authentication functionality. For more information about IIS and Integrated Windows Authentication with Vibe, see “Configuring Single Sign-On with Internet Information Services for Windows” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

36 Micro Focus GroupWise

When you use Micro Focus Vibe with GroupWise, some configuration steps are required to integrate the applications, as described in "Configuring GroupWise for Use with Micro Focus Vibe" in the *GroupWise 18 Interoperability Guide*:

- "Configuring GroupWise for Use with Micro Focus Vibe"
- ""Enabling GroupWise/Vibe Integration for GroupWise Client Users
- ""Accessing Your Vibe Site from the GroupWise Client

37 Novell Messenger

Micro Focus Vibe lets you integrate with Novell Messenger 2.2 and later. This integration displays users' Messenger presence information within Vibe. For information about how to configure Vibe to work with Messenger, see "Integrating Messenger with Vibe" on page 171.

38 Skype

Novell Vibe lets you integrate with Skype, so Vibe users can easily set up instant Skype meetings with other Vibe users, as described in "Using Skype from within Vibe" in the *Micro Focus Vibe 4.0.5 User Guide*.

Before users can use Skype from within Vibe, Vibe administrators must enable this functionality. For instructions on how to set up Vibe to work with Skype, see "Integrating Skype with Vibe" on page 172.

39 Twitter and Other Remote Applications

Novell Vibe lets you incorporate third-party products such as Twitter into Vibe, through the use of remote applications.

For information on how to incorporate existing remote applications into your Vibe site, see Chapter 17, “Using Remote Applications on Your Vibe Site,” on page 183.

40 YouTube

Novell Vibe lets you display YouTube videos directly from the Vibe site. This functionality is enabled by default and does not need to be activated by a Vibe administrator.

For more information about how to display YouTube videos on the Vibe site, see “Displaying YouTube Videos in a Folder Entry” in the *Micro Focus Vibe 4.0.5 User Guide*.

IV Site Security

41 Security Administration

SSL (Secure Socket Layer) and TLS (Transport Layer Security) can be used to secure the connections between your Novell Vibe site and other network services.

Dealing with Security Scan Results

Running regular security scans on your network is critical to security administration. As exemplified in Chapter 42, “Security Policies,” on page 351, security is a top priority for the Vibe development team.

Occasionally, reputable security scanning software reports risks that the Vibe team considers to be less significant than reported. The following are specific examples:

- **PHP as a Security Vulnerability:** Although in many cases the presence of PHP scripts is a legitimate concern, in the case of Vibe, there is no PHP access without first authenticating through port 9443. Since access through port 9443 is secure by definition, Vibe’s PHP implementation is secure.
- **Diffie-Hellman 1024 Keys:** If you run a Nessus or equivalent security scan, you might receive a report of “Medium Risk” associated with Diffie-Hellman 1024-bit keys.

  The Vibe team is aware of this and is considering increasing the key size in a future release. At this time, however, the team does not feel that this is a significant threat to Vibe installations; breaking 1024-bit keys requires computing resources that only a nation-state would have at its disposal.

  If you are concerned or feel that your organization might be vulnerable to nation-state attacks, you can specify a stronger key through the Java security policy.

Securing LDAP Synchronization

If your LDAP directory service requires a secure LDAP connection (LDAPS), you must configure Novell Vibe with a root certificate. The root certificate identifies the root certificate authority (CA) for your Vibe site, which lets you generate a self-signed root certificate based on your eDirectory tree.

Understanding How Vibe Uses the Root Certificate for Your eDirectory Tree

You can generate a root certificate for your eDirectory tree by using either ConsoleOne or iManager, then import the root certificate into the Java keystore file (`cacerts`) on the Vibe server to make it accessible to Vibe. The default location for the Java keystore file is:

Linux:	`/usr/lib64/jvm/java-`*`version`*`-ibm-`*`version`*`/jre/lib/security`
Windows:	`c:\Program Files\Java\jdk`*`version`*`\jre/lib/security`

NOTE: For iManager instructions, see "TID 3176104: How to Enable SSL for Teaming LDAP Synchronization and Authentication" in the Novell Support Knowledgebase (http://www.novell.com/support). If you are using Active Directory rather than eDirectory, consult your Active Directory documentation for a procedure comparable to the one provided in "Generating a Root Certificate in ConsoleOne" on page 332.

Generating a Root Certificate in ConsoleOne

1. On Linux or Windows, start ConsoleOne and authenticate to your eDirectory tree.
2. Expand the Security container, right-click the *Tree_Name* CA object, then click **Properties**.
3. Click **Certificates > Self Signed Certificate**.
4. Click **Validate** to update the certificate status, then click **OK** to close the Certificate Validation dialog box.
5. Click **Export** to export your eDirectory root certificate into a file that can be imported into the Java keystore file.
6. Click **Next** to accept the default of `No` for exporting a private key file along with the root certificate.
7. Select the output format for the root certificate file.

   Either DER or Base64 format can be imported into the Java keystore file.
8. In the **Filename** field, specify the location where you want to create the root certificate file and the filename to use, such as `SelfSignedRootCert.der`.

   IMPORTANT: You need to be able to access this file from the Vibe server. Specify an accessible location or copy it to the Vibe server after you create it.

   ---
9. Click **Next** to display a summary of the options you have selected, then click **Finish** to generate the root certificate file.
10. Click **Cancel** to close the Self Signed Certificate properties page of the *Tree_Name* CA object.

11 Exit ConsoleOne.

12 (Conditional) If necessary, copy the root certificate file to a convenient location on the Vibe server.

Importing the Root Certificate into the Java Keystore

1 On the Vibe server, make sure that you have access to the root certificate file.

2 Make sure that you can access the `keytool` tool:

SLES 11:	`/usr/lib64/jvm/java-`*`version`*`-ibm-`*`version`*`/bin/keytool`
SLES 12:	`/usr/java/java-`*`version`*`-ibm-`*`version`*`/bin/keytool`
Windows:	`c:\Program Files\Java\jdk`*`version`*`\bin\keytool.exe`

For convenient use, you might need to add its location to the PATH environment variable.

3 Use the following command to import the root certificate into the Java keystore:

```
keytool -import -alias ldap_server_dns_name
        -keystore path_to_java_keystore_file
        -file root_certificate_file
```

For example:

```
keytool -import -alias ldapserver.yourcompanyname.com
        -keystore /usr/java/jdkversion/jre/lib/security/cacerts
        -file /certs/SelfSignedRootCert.der
```

4 When prompted, enter `changeit` as the password for the Java keystore.

5 Enter `yes` to accept the certificate import.

6 Use the following command to verify that the root certificate has been imported into the Java keystore:

```
keytool -list -keystore path_to_java_keystore_file
```

7 Enter the root certificate password to list the root certificate information.

8 Restart Vibe so that Tomcat rereads the updated Java keystore file.

You are now ready to configure your Vibe site for secure LDAP synchronization, as described in "Adding Vibe Users from Your LDAP Directory" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Securing Email Transfer

When you install Novell Vibe, you can choose whether or not the Vibe internal mail host uses TLS (Transport Layer Security) when it communicates with other SMTP mail hosts. For more information, see "Inbound Email Security" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

If your Vibe site needs to send email messages to an email system that requires secure SMTP (SMTPS), the Vibe site must have the same type of root certificate that is required for secure LDAP (LDAPS). If you have not already set up secure LDAP for your Vibe site, follow the instructions in "Securing LDAP Synchronization" on page 332 to set up secure SMTP for communications with your email system.

Securing HTTP Browser Connections

Using secure HTTP (HTTPS) improves the security of your Novell Vibe site. During installation, you can choose to configure your Vibe site for HTTP or HTTPS. After installation, you can force secure HTTP connections.

Preparing for Secure HTTP Connections

If you want users to access the Vibe site with a secure HTTP connection, you must configure Vibe with a root certificate and a server certificate. The root certificate identifies the root certificate authority (CA) for your Vibe site. The server certificate is customized for the specific server where Vibe is installed.

Understanding How Vibe Handles Certificates

Vibe uses a keystore to store certificates. The default keystore file that is installed along with Vibe is:

Linux:	`/opt/novell/teaming/apache-tomcat/conf/.keystore`
Windows:	`c:\Program Files\Novell\Teaming\ apache-tomcat\conf\.keystore`

The original certificate in the default keystore is sufficient for you to set up secure HTTP connections during initial installation, but it is self-signed and has an expiration date, so you cannot use it permanently. Soon after installation, you must obtain a permanent certificate. You can use a commercially signed certificate or a self-signed certificate. There are advantages and disadvantages to each approach.

- **Commercially Signed Certificate:** The advantage to using a certificate signed by a commercial certificate authority (CA) is that browsers automatically accept these certificates. The disadvantage is that an additional step is required, with some wait time while you obtain the commercially signed certificate.
- **Self-Signed Certificate:** The advantage to using a self-signed certificate is that it is quick and easy for you to do as the Vibe administrator. The disadvantage is that users receive a warning in the browser about the self-signed certificate the first time they access the Vibe site using secure HTTP. Users must manually accept the self-signed certificate, then the warning never occurs again.

After you obtain your permanent certificate, you can store it in the default Vibe keystore, or in a location of your own choosing. Vibe reads the location of its keystore from the following file:

Linux:	`/opt/novell/teaming/apache-tomcat/conf/server.xml`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\conf\server.xml`

If you do not want to use the default keystore location, you must update the `server.xml` file to match the location you choose for your keystore.

Creating a New Keystore File

Rather than updating the Vibe `.keystore` file that is provided during installation, it is easier to create a new `.keystore` file, then import your signed certificate into it.

1 Create a new directory where you want to create the new `.keystore` file, such as a `certs` directory in a convenient location.

2 Change to the new `certs` directory.

3 Make sure that you can access the `keytool` tool:

Linux:	`/usr/lib64/jvm/java-`*`version`*`-ibm-`*`version`*`/bin/keytool`
Windows:	`c:\Program Files\Java\jdk`*`version`*`\bin\keytool.exe`

For convenient use, you might need to add its location to the PATH environment variable.

4 Use the following command to create a new `.keystore` file:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore .keystore
```

5 When prompted, specify and confirm `changeit` as the password for the new `.keystore` file.

6 When you are prompted for your first and last name, specify the fully qualified DNS name of the Vibe server, such as `vibe.yourcompanyname.com`.

You are then prompted for additional information about your organization:

- Organizational unit
- Organization
- City or locality
- State or province
- Two-letter country code

7 (Conditional) If you are planning to obtain a your certificate from a commercial certificate authority (CA), respond to the additional information prompts with accurate information appropriate to your organization.

or

(Conditional) If you are planning to generate a self-signed certificate, press Enter to skip through the prompts.

8 When you are prompted whether the information you provided is correct, enter `yes`.

9 Press Enter to use the same password that you specified in Step 5 as the key password for Tomcat.

10 List the files in the `certs` directory to see that a new `.keystore` file has been created.

Do Not Change the Password for the Keystore File

The password for the `.keystore` file is hard coded and should not be changed.

The password adds no additional protection because the keystore is secured by being located in a root-owned directory, not by the password.Port 9443 Vibe and Filr Cert management are hard coded to expect the password as it is created on the system.

Changing the password breaks 9443 certificate management.

Generating a Certificate Signing Request

1 Use the following command to create a certificate signing request (CSR):

```
keytool -certreq -alias tomcat -keyalg RSA
        -file certreq.csr -keystore .keystore
```

2 Enter the keystore password (`changeit`) to create the CSR.

3 List the files in the `certs` directory to see that a new `certreq.csr` file has been created along with the existing `.keystore` file.

4 Use the `certreq.csr` file to obtain a signed certificate.:

4a To use a commercial certificate authority (CA), continue with "Submitting the Certificate Signing Request to a Certificate Authority (CA)" on page 336.

or

4b To use a self-signed certificate, skip to "Using the Certificate Signing Request to Generate a Self-Signed Certificate" on page 337.

Submitting the Certificate Signing Request to a Certificate Authority (CA)

You can find a commercial certificate authority (CA) on the Internet by searching for "certificate authority." The process of obtaining a signed certificate varies from company to company. Each company provides instructions to assist you.

The certificate authority sends you a set of certificate files that you import into the Vibe keystore. Import these files into the same keystore that you used to create the original certificate request. You must import all of the files that you receive.

The following procedure is a guideline for importing the certificate into the Vibe keystore. Instructions might vary depending on the certificate authority.

1 Change to the `certs` directory where you created the root certificate file and the server certificate file.

2 Use the following command to import the root certificate file:

```
keytool -import -alias root -trustcacerts -keyalg RSA -keystore .keystore
        -file CertificateAuthorityCert.der
```

3 Enter the keystore password (`changeit`) to add the root certificate to the Vibe keystore.

4 Use the following command to import the SSL certificate file that you received from the certificate authority:

```
keytool -import -alias tomcat -keyalg RSA -keystore .keystore
        -file certificate_name.cer
```

5 Enter the keystore password (`changeit`) to add the server certificate to the Vibe keystore.

Using the Certificate Signing Request to Generate a Self-Signed Certificate

If you do not want to wait to receive your signed certificate from a commercial certificate authority (CA), you can generate your own self-signed certificate using iManager. You must generate both a self-signed eDirectory root certificate file and a server certificate file.

For help, refer to "Understanding the Certificate Server" in the *NetIQ eDirectory Administration Guide*.

NOTE: If you are using Active Directory rather than eDirectory, consult your Active Directory documentation for comparable procedures.

Importing the Certificate Files into the Vibe Keystore

After you have obtained or generated a signed certificate, you must import the certificate files into the Vibe keystore. This section describes how to import the files associated with a self-signed certificate. For information about how to import the files for a certificate that you receive from a certificate authority, see "Submitting the Certificate Signing Request to a Certificate Authority (CA)" on page 336.

1 Change to the `certs` directory where you created the root certificate file and the server certificate file.

2 Use the following command to import the root certificate file:

```
keytool -import -alias root -keyalg RSA -keystore .keystore
        -file SelfSignedRootCert.der
```

3 Enter the keystore password (`changeit`) to add the root certificate to the Vibe keystore.

4 Use the following command to import the server certificate file:

```
keytool -import -alias tomcat -keyalg RSA -keystore .keystore
        -file SelfSignedServerCert.der
```

5 Enter the keystore password (`changeit`) to add the server certificate to the Vibe keystore.

The new `.keystore` file is now ready to be added to your Vibe system.

6 Use the following command to verify that the server certificates have been imported into the Vibe keystore:

```
keytool -list -keystore .keystore
```

7 Enter the keystore password (`changeit`), then verify that the certificates have been imported.

You should see the text `Your keystore contains 2 entries`, followed by information about each certificate that you imported.

8 Continue with "Replacing the Original Vibe Keystore File with Your Permanent Keystore File" on page 338.

Replacing the Original Vibe Keystore File with Your Permanent Keystore File

1 Change to the following directory on the Vibe server:

Linux:	`/opt/novell/teaming/apache-tomcat/conf`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\conf`

2 Rename the existing `.keystore` file to `keystorebackup`.

3 Copy your new `.keystore` from the `certs` directory to the `conf` directory.

4 Adjust the ownership and permissions of the new `.keystore` file to match those of the backed-up keystore file.

5 Restart Vibe so that Vibe rereads the updated keystore file.

Implementing Secure HTTP Connections

When you run the Vibe installation program, you can choose between non-secure and secure HTTP connections, as described in "HTTP/HTTPS Ports" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Forcing Secure HTTP Connections

With additional configuration, you can force users from a non-secure HTTP connection to a secure HTTPS connection.

- "Using NetIQ Access Manager to Force Secure HTTP Connections" on page 338
- "Configuring Tomcat to Redirect to Secure HTTP Connections" on page 338
- "Adding the Apache Web Server to Force Secure HTTP Connections" on page 340

Using NetIQ Access Manager to Force Secure HTTP Connections

With Micro Focus Vibe, you can use NetIQ Access Manager to force secure HTTP connections. For more information, see "Configuring Single Sign-On with Novell Access Manager" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Configuring Tomcat to Redirect to Secure HTTP Connections

To reconfigure Tomcat, you must update two configuration files (both named `web.xml`) under two different directories (`ssf` and `ROOT`). The `ssf` directory name refers to SiteScape Forum, a legacy product name. The `ssf` directory contains the main Vibe web application that you use when you interact with your browser. The `ROOT` directory name refers to SiteScape File System. The `ROOT` directory contains the Vibe WebDAV application that you use to access files on a remote WebDAV server from the Vibe site.

1 Log in to the Vibe server with sufficient rights to edit the `web.xml` files (`root` on Linux, `Administrator` on Windows).

2 Modify the `web.xml` file under the `ssf` directory:

   2a Change to the directory where the `web.xml` file is located.

Linux: `/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF`

Windows: `c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF`

2b Make a backup copy of the `web.xml` file, then open the `web.xml` file in a text editor.

2c Add the following security constraint at the bottom of the file, immediately above the `</web-app>` tag.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Entire Application</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

2d (Conditional) If users access the Vibe site with Internet Explorer, find the following single line in the security constraint you just added:

```
 <url-pattern>/*</url-pattern>
```

2e Replace it with the following set of lines:

```
  <!-- Patterns from web.xml.tmpl. -->
  <url-pattern>/a/*</url-pattern>
  <url-pattern>/ws/*</url-pattern>
  <url-pattern>/rss/*</url-pattern>
  <url-pattern>/atom/*</url-pattern>
  <!-- Patterns from subdirectories of webapps/ssf. -->
  <url-pattern>/applets/*</url-pattern>
  <url-pattern>/css/*</url-pattern>
  <url-pattern>/help/*</url-pattern>
  <url-pattern>/help_doc/*</url-pattern>
  <url-pattern>/i/*</url-pattern>
  <url-pattern>/images/*</url-pattern>
  <url-pattern>/js/*</url-pattern>
```

For Internet Explorer, this list of URL patterns forces secure HTTP connections for everything except the `/s/*` pattern (document files with extensions such as `.odt` and `.doc`) and the `/ical/*` pattern (calendar `.ics` files).

2f Save the modified `web.xml` file, then exit the text editor.

3 Modify the `web.xml` file under the `ROOT` directory:

3a Change to the directory where the `web.xml` file is located.

Linux: `/opt/novell/teaming/apache-tomcat/webapps/ROOT/WEB-INF`

Windows: `c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ROOT\WEB-INF`

3b Make a backup copy of the `web.xml` file, then open the `web.xml` file in a text editor.

3c Add the following security constraint at the bottom of the file, immediately above the `</web-app>` tag.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Entire Application</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

3d Save the modified `web.xml` file, then exit the text editor.

Adding the Apache Web Server to Force Secure HTTP Connections

You can set up the Apache web server to front your Vibe site and use a meta refresh (http://en.wikipedia.org/wiki/Meta_refresh) to redirect users to a secure URL.

1. Install the Apache web server on one server.
2. Configure Apache to listen on port 80.
3. Create an `index.html` file similar to the following example:

```
<html>
<head>
  <meta http-equiv="refresh" content="0;url=https://vibe_url" />
  <title>Redirected to Secure Vibe</title>
</head>
<body>
  This page is used to redirect to the Secure Vibe server. If your
  browser does not automatically redirect you in a few seconds, click
  <a href="https://vibe_url">here</a> to go to the secure page.
</body>
</html>
```

4. Replace *vibe_url* with the URL to your Vibe site.
5. Place the `index.html` file in the document root directory of the Apache web server.

Linux:	`/srv/www/htdocs`
Windows:	`c:\Program Files\Apache Software Foundation\Apache2.2\htdocs`

6. Restart the Apache web server.

Defaulting to Secure HTTP URLs

- “Defaulting to Secure HTTP URLs in Vibe Links” on page 341
- “Defaulting to Secure HTTP URLs in Email Notifications” on page 341

Defaulting to Secure HTTP URLs in Vibe Links

Vibe includes URLs to locations on the Vibe site in various links throughout the Vibe system. By default, the URLs are formed with HTTP rather than HTTPS. You can reconfigure Vibe to default to HTTPS for Vibe site URLs.

1 Log in to the Vibe server with sufficient rights to edit the `ssf-ext.properties` file (`root` on Linux, `Administrator` on Windows).
2 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/ webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\ webapps\ssf\WEB-INF\classes/config`

3 Open the `ssf.properties` file in a text editor.
4 Locate and copy the following lines:

```
adapter.web.protocol=context-http
servlet.web.protocol=context-http
rss.web.protocol=context-http
ical.web.protocol=context-http
ssfs.web.protocol=context-http
simpleurl.web.protocol=context-http
```

5 Make a backup copy of the `ssf-ext.properties` file, located in the same directory with the `ssf.properties` file.
6 Open the `ssf-ext.properties` file in a text editor.
7 Paste the lines that you copied in Step 4 to the bottom of the file.
8 Change `http` to `https`.

```
adapter.web.protocol=context-https
servlet.web.protocol=context-https
rss.web.protocol=context-https
ical.web.protocol=context-https
ssfs.web.protocol=context-https
simpleurl.web.protocol=context-https
```

9 Close the `ssf.properties` file without saving.
10 Save the `ssf-ext.properties` file, then exit the text editor
11 Restart Vibe to put the change into effect.

Defaulting to Secure HTTP URLs in Email Notifications

When an email notification is sent from Vibe, Vibe includes a URL to the location on the Vibe site where the notification was sent. By default, the URLs in email notifications are formed with `http` rather than `https`. You can reconfigure Vibe to default to `https` for Vibe site URLs.

1 Log in to the Vibe server with sufficient rights to edit the `ssf-ext.properties` file (`root` on Linux, `Administrator` on Windows).
2 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes/config`

3. Open the `ssf.properties` file in a text editor.
4. Locate and copy the following line:

   ```
   ssf.secure.links.in.email=false
   ```

5. Close the `ssf.properties` file without saving.
6. Make a backup copy of the `ssf-ext.properties` file, located in the same directory with the `ssf.properties` file.
7. Open the `ssf-ext.properties` file in a text editor.
8. Paste the line that you copied in Step 4 to the bottom of the file:

   ```
   ssf.secure.links.in.email=false
   ```

9. Change `false` to `true` so that the line now looks like this:

   ```
   ssf.secure.links.in.email=true
   ```

10. Save the `ssf-ext.properties` file, then exit the text editor
11. Restart Vibe to put the change into effect.

All system-generated email notifications now default to secure HTTP URLs. However, all user-generated emails from the Vibe system follow the current user's context. For example, if a user is logged in as HTTP and chooses to share an entry with another user, the link in the email notification uses HTTP.

Securing against Brute-Force Attacks with CAPTCHA

CAPTCHA (http://en.wikipedia.org/wiki/CAPTCHA) provides additional security against brute-force attacks on the Vibe web application.

Brute-force attack monitoring is enabled on the Vibe system by default.

By default, Vibe considers a brute-force attack to be taking place if any user has 5 failed login attempts to the Vibe system within a 30-minute timeframe. During the time that Vibe believes that a brute-force attack is occurring, Vibe requires all users to specify the CAPTCHA response when logging in to the Vibe web application. Vibe considers the system to be safe from the brute-force attack as soon as there have been fewer than 5 failed login attempts within the past 30 minutes. At that time, specifying a CAPTCHA response is no longer required.

To change the default configuration settings for CAPTCHA for the Vibe web application:

1. Log in to the Vibe server with sufficient rights to edit the `ssf-ext.properties` file (`root` on Linux, `Administrator` on Windows).
2. Change to the following directory:

Linux: `/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/classes/config`

Windows: `c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssf\WEB-INF\classes/config`

3 Open the `ssf.properties` file in a text editor.

4 Locate and copy the following lines:

```
#failed.user.authentication.history = true
#failed.user.authentication.history.max.user.size = 5
#brute.force.attack.in.last.num.seconds = 30
#brute.force.attack.num.failed.logins = 5
```

5 Close the `ssf.properties` file without saving.

6 Make a backup copy of the `ssf-ext.properties` file, located in the same directory with the `ssf.properties` file.

7 Open the `ssf-ext.properties` file in a text editor.

8 Paste and uncomment the lines that you copied in Step 4 to the bottom of the file:

```
failed.user.authentication.history = true
failed.user.authentication.history.max.user.size = 5
brute.force.attack.in.last.num.seconds = 30
brute.force.attack.num.failed.logins = 5
```

9 Change the values to match your desired functionality. The function of each setting is as follows:

failed.user.authentication.history: When this option is set to `true` it enables tracking of failed login attempts on a per-user basis. The subsequent settings allow you to further customize the functionality.

failed.user.authentication.history.max.user.size: The number of failed login attempts per user of which Vibe keeps a history.

brute.force.attack.in.last.num.seconds: The number of seconds for which Vibe will look for the number of failed login attempts. The default value for this setting is 30 seconds.

brute.force.attack.in.last.num.failed.logins: The number of failed login attempts allowed per user (within the specified number of seconds) before Vibe requires all users to specify the CAPTCHA response. The default of failed login attempts allowed per user is 5.

For example, suppose `brute.force.attack.in.last.num.seconds` is set to 300 (5 minutes) and `brute.force.attack.num.failed.logins` is set to 4. If user A unsuccessfully attempts to log in to the Vibe web application 4 times within a 5-minute period, the next time any user in the Vibe system attempts to log in he or she will be required to enter a CAPTCHA response.

10 Save the `ssf-ext.properties` file, then exit the text editor

11 Restart Vibe to put the change into effect.

Securing User Passwords

You can require that user passwords to the Vibe site meet certain criteria by enabling password complexity checking. Only locally created users and external users are affected by this setting; users whose accounts are synchronized to Vibe via LDAP are not affected.

Users’ existing passwords are not forced to comply with the password policy; only when a user changes his or her password is the password policy put into effect.

When you enable password complexity checking in Vibe, Vibe requires that passwords:

- Are at least 8 characters in length
- Do not contain the user's first name, last name, or user ID (these restrictions are not case-sensitive)
- Contain at least 3 of the following:
  - A lower-case character
  - An upper-case character
  - A number
  - One of the following symbols: `~ @ # $ % ^ & * ( ) - + { } [ ] | \ ? / , . < >`

To enable password policy checking on the Vibe site:

1. Log in to the Vibe site as the Vibe administrator.
2. Click the **admin** link in the upper-right corner of the page, then click the **Administration Console** icon.
3. Under **System**, click **Password Policy**.
4. Select **Enable Password Complexity Checking for Local and External Users**, then click **OK**.

Securing Web Service Connections

Web Services in Vibe allow third-party applications to integrate with your Vibe system. To increase the security of your Vibe site, you can configure Vibe to allow only secure applications to integrate with Vibe. This section does not attempt to describe how to write a third-party application that supports HTTPS. Instead, this section describes how to configure your Vibe system to prevent non-secure third-party applications from connecting with Vibe.

To prevent non-secure third-party applications from connecting with your Vibe system:

1. Log in to the Vibe server with sufficient rights to edit the `web.xml` files (`root` on Linux, `Administrator` on Windows).
2. Modify the `web.xml` file under the `ssr` directory:

   2a Change to the directory where the `web.xml` file is located.

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssr/WEB-INF`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\webapps\ssr\WEB-INF`

   2b Make a backup copy of the `web.xml` file, then open the `web.xml` file in a text editor.

   2c Add the following security constraint at the bottom of the file, immediately above the </web-app> tag.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Entire Application</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

2d Save the modified `web.xml` file, then exit the text editor.

Securing Tomcat

In order to support a wide variety of browsers, Vibe (Tomcat) allows the full range of SSL and TLS key cipher methods. Over time, some of the cipher methods have proven vulnerable to attack. To harden Tomcat and eliminate the server acceptance of vulnerable ciphers, you can specify which ciphers the server should not accept:

NOTE: Because cipher lists are constantly changing, we can't provide an up-to-date list of vulnerable ciphers. Consult with your risk management department or security manager for your organization's list.

---

1 Change to the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/conf`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\conf`

2 Open the `server.xml` file in a text editor.

3 Locate the `sslProtocol` attribute.

4 Disable the weak ciphers supplied by your risk management department or security manager by adding a list to the `server.xml` file, after the `sslProtocol` attribute:

`ciphers="`*`example_cipher_1, example_cipher_2, etc.`*`"`

5 Save and close the `server.xml` file.

Requiring That External Users Accept Terms and Conditions

You can require that any external (guest) users who access the Vibe site accept terms and conditions before being granted access.

Path: Vibe Administration Console > System > Share Settings > External Users Licensing Terms tab

1. Enter your access terms in the Terms and Conditions for External Users window.
2. Enable Display Terms and Condition.

   External users are now required to accept the terms and conditions before being granted access.

Vibe Sanitizes HTML to Prevent Security Risks

Vibe 4.0.2 and later uses the OWASP HTML Sanitizer to allow or remove HTML elements, attributes, and CSS Style properties that Micro Focus regards as “safe” or “unsafe,” as explained in the following sections:

- “HTML Elements” on page 346
- “HTML Element Attributes” on page 346
- “Conditional HTML Element Attributes” on page 347
- “CSS Style Properties” on page 348

HTML Elements

The following HTML Elements are considered “safe.”

a	dfn	h4	ol	table
abbr	dir	h5	p	tbody
area	div	h6	pre	td
b	dl	hr	q	textarea
big	dt	i	s	tfoot
blockquote	em	img	samp	th
br	figcaption	input	small	thead
caption	figure	ins	span	tr
center	font	kbd	strike	tt
cite	h1	li	strong	u
code	h2	map	sub	ul
dd	h3	o	sup	var
del				

You can configure your Vibe site to regard additional HTML elements as “safe” by doing the following:

1. Using a text editor, add the following parameter with the elements you are adding, to the `ssf-ext.properties` file.

   `html.safe.elements=`*`Element1`*`,`*`Element2`*`,`*`Element3`*
2. After adding or modifying the file, you must restart Apache Tomcat for your configuration changes to take effect.

IMPORTANT: Additions to the default OWASP HTML Sanitizer settings are not supported and are regarded as unsafe by Micro Focus Support.

If you want Micro Focus to consider supporting your additions in a future Vibe release, you must submit them for consideration to Micro Focus via Customer Care.

HTML Element Attributes

The following HTML Element Attributes are considered safe by default

abbr	compact	rowspan
acronym	coords	rules
align	dir	scope
alt	face	size
axis	frame	sortable
bgcolor	haling	sorted
border	headers	style
cellpadding	height	summary
cellspacing	href (on `area` elements)	target
char	hspace	title
charoff	id	type
class	lang	usemap
color	longdesc	valign
colspan	name	vspace
	nowrap	width
	rel	

You can configure your Vibe site to regard additional HTML attributes as “safe” by doing the following:

1. Using a text editor, add the following parameter with the attributes you are adding, to the `ssf-ext.properties` file.

   `html.safe.attributes=`*`Attribute1`*`,`*`Attribute2`*`,`*`Attribute3`*

2. After adding or modifying the file, you must restart Apache Tomcat for your configuration changes to take effect.

IMPORTANT: Additions to the default OWASP HTML Sanitizer settings are not supported and are regarded as unsafe by Micro Focus Support.

If you want Micro Focus to consider supporting your additions in a future Vibe release, you must submit them for consideration to Micro Focus via Customer Care.

Conditional HTML Element Attributes

Vibe limits the following HTML elements as indicated.

href

- Allowed on `<a/>` tags
- Allowed URL protocols are `http`, `https` and `mailto`

src

- Allowed on <img/> tags
- Allowed URL protocols are `http`, `https`, `mailto` and `data`
- For embedded images, allowed mime-types are:
  - `data:image/jpeg`;
  - `data:image/png`;
  - `data:image/gif`;

CSS Style Properties

The following is a list of CSS style properties in “style” attributes are considered “safe.”

-moz-border-radius
-moz-border-radius-bottomleft
-moz-border-radius-bottomright
-moz-border-radius-topleft
-moz-border-radius-topright
-moz-box-shadow
-moz-outline
-moz-outline-color
-moz-outline-style
-moz-outline-width
-o-text-overflow
-webkit-border-bottom-left-radius
-webkit-border-bottom-right-radius
-webkit-border-radius
-webkit-border-radius-bottom-left
-webkit-border-radius-bottom-right
-webkit-border-radius-top-left
-webkit-border-radius-top-right
-webkit-border-top-left-radius
-webkit-border-top-right-radius
-webkit-box-shadow
azimuth
background
background-attachment
background-color
background-image
background-position
background-repeat
border
border-bottom
border-bottom-color
border-bottom-left-radius
border-bottom-right-radius
border-bottom-style
border-bottom-width
border-collapse
border-color
border-left
border-left-color
border-left-style
border-left-width
border-radius
border-right
border-right-color
border-right-style
border-right-width
border-spacing
border-style
border-top
border-top-color
border-top-left-radius
border-top-right-radius
border-top-style
border-top-width
border-width
box-shadow
caption-side
color
cue
cue-after
cue-before
direction
display
elevation
empty-cells
float
font
font-family
font-size
font-stretch
font-style
font-variant
font-weight
height
image()
letter-spacing
line-height
linear-gradient()
list-style
list-style-image
list-style-position
list-style-type
margin
margin-bottom
margin-left
margin-right
margin-top
max-height
max-width
min-height
min-width
outline
outline-color
outline-style
outline-width
padding
padding-bottom
padding-left
padding-right
padding-top
pause
pause-after
pause-before
pitch
pitch-range
quotes
radial-gradient()
rect()
repeating-linear-gradient()
repeating-radial-gradient()
rgb()
rgba()
richness
speak
speak-header
speak-numeral
speak-punctuation
speech-rate
stress
table-layout
text-align"
text-decoration
text-indent
text-overflow
text-shadow
text-transform
text-wrap
unicode-bidi
vertical-align
voice-family
volume
white-space
width
word-spacing
word-wrap
z-index

You can configure your Vibe site to regard additional CSS Style Properties as “safe” by doing the following:

1. Using a text editor, add the following parameter with the properties you are adding, to the `ssf-ext.properties` file.

   css.safe.properties=*Property1*,*Property2*,*Property3*

2. After adding or modifying the file, you must restart Apache Tomcat for your configuration changes to take effect.

IMPORTANT: Additions to the default OWASP HTML Sanitizer settings are not supported and are regarded as unsafe by Micro Focus Support.

If you want Micro Focus to consider supporting your additions in a future Vibe release, you must submit them for consideration to Micro Focus via Customer Care.

---

42 Security Policies

Securing the Vibe Data

Limiting Physical Access to Vibe Servers

Servers where Novell Vibe data resides should be kept physically secure, so unauthorized persons cannot gain access to the server consoles.

Protecting the Vibe File Repository

The Novell Vibe file repository contains unencrypted data. See "Distributing Different Data Types to Different Locations" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide* for details about how Vibe uses the local file system for data storage. These directories contain uploaded information in various formats (both native file formats and potentially a number of rendered formats (such as cached HTML versions of files, thumbnails, and RSS feeds) as well as archived data. These files are managed exclusively by the Vibe application software.

For data security, encrypted file systems should be used on servers where Vibe data resides. Only Vibe administrators should have direct access to Vibe data.

Protecting the Vibe Database

During installation, you select the encryption method that you want to use for the Vibe database, as described in "Database Encryption Algorithm" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*. Three levels of encryption strength are available. The encryption algorithm cannot be changed after you have started using the Vibe database, so be sure to select the level of encryption appropriate for your Vibe site during initial installation.

Depending on your local security guidelines, you might want to encrypt the database connections between the Vibe software and the Vibe database. SSL-encrypted data between the Vibe application and the database server imposes a performance penalty because of the increased overhead of encrypting and decrypting the retrieved data.

Support for this is highly dependent on the database client drivers and JDBC connector support, and on how you are configuring your database client and server certificates. You should check with your database vendor on how to set up SSL connections on both the client and server sides of the connection. You might need to modify the JDBC URL during installation, as described in "Database Location" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*. For example, for MySQL, you might add `useSSL=true&requireSSL=true` to the `options` part of the JDBC URL.

Securing the Vibe Software

- "Protecting the Vibe Configuration Files" on page 352
- "Protecting the Vibe Properties File" on page 352
- "Protecting Log Files" on page 352
- "Protecting the Vibe Process on Linux" on page 353

Protecting the Vibe Configuration Files

The Novell Vibe configuration file (`installer.xml`) for the Vibe software should be protected from tampering. It contains user name and password information for Vibe features that interact with other programs.

The initial `installer.xml` is created in the same directory where the Vibe Installation program is run. Backup copies are stored in:

Linux:	`/opt/novell/teaming/teaming-config`
Windows:	`c:\Program Files\Novell\Teaming\teaming-config`

Protecting the Vibe Properties File

The Vibe properties file (`ssf.properties`) should be protected from tampering. Like the Vibe configuration file, it contains user name and password information, as well as many other details about your Vibe site configuration. The Vibe properties file (`ssf.properties`) is located in the following directory:

Linux:	`/opt/novell/teaming/apache-tomcat/` `webapps/ssf/WEB-INF/classes/config`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\` `webapps\ssf\WEB-INF\classes/config`

Protecting Log Files

The log files for Vibe and Tomcat should be protected against access by unauthorized persons. Log files contain very detailed information about your Vibe system and Vibe users.

The Vibe log file is available in the following directory of your Vibe installation:

Linux:	`/opt/novell/teaming/apache-tomcat/webapps/ssf/WEB-INF/logs`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\` `webapps\ssf\WEB-INF\logs`

The Tomcat log file is available in the following directory of your Vibe installation:

Linux:	`/opt/novell/teaming/apache-tomcat/logs`
Windows:	`c:\Program Files\Novell\Teaming\apache-tomcat\logs`

Protecting the Vibe Process on Linux

On Linux, Vibe is installed to run as a user other than the Linux `root` user. See “Linux User ID for Vibe” in “Basic Installation” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Securing the Vibe Site

Configuring a Proxy Server

Your Novell Vibe system should be located behind your firewall. If Vibe users want to access the Vibe site from outside your firewall, you should set up a proxy server outside your firewall to provide access. You can use NetIQ Access Manager to protect your Vibe site, as described in “Configuring Single Sign-On with Novell Access Manager” in “Advanced Installation and Reconfiguration” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Setting the Vibe Administrator Password

The Vibe site is initially installed to allow administrator access by using the user name `admin` and the password `admin`. The Vibe administrator password should be changed immediately after installation, as described in “Accessing Your Basic Vibe Site as the Site Administrator” in “Basic Installation” in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Setting Up SSL Connections

All communication with the Vibe site should be configured to use SSL connections, as described in:

- “Securing Email Transfer” on page 333
- “Securing LDAP Synchronization” on page 332
- “Securing HTTP Browser Connections” on page 334

Shortening the Vibe Session Timeout

By default, if a user's Vibe session is idle for four hours (240 minutes), Vibe logs the idle user out. For increased security for your Vibe site, you can make the session timeout shorter, as described in "Changing the Vibe Session Timeout" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Using Role-Based Access Control

Vibe controls all access to folders and entries by using role-based access controls. Vibe is intended to be used primarily for the sharing of information, so many default access rights tend toward allowing at least universal read access. For information on setting access controls for your Vibe site, see:

- Chapter 2, "Planning and Controlling User Access to Workspaces and Folders," on page 21 in this guide
- "Controlling Access" in the *Micro Focus Vibe 4.0.5 Advanced User Guide*

Monitoring Inbound Email

You can configure Vibe to receive email and post the messages as entries in a folder, as described in "Enabling Inbound Email" in "Basic Installation" in the *Micro Focus Vibe 4.0.4 Installation Guide*. Because email is inherently non-secure, there is no way to be sure that the senders are who they claim to be. Entries posted by email include the email address of the sender to alert Vibe users about the origin of the postings.

Preventing Web Services Access

The default Vibe installation allows authenticated access via web services, as described in "Configuring Web Services" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*. If you are not using web services, you can disable them.

Controlling RSS Feeds

Because RSS readers are outside of the authentication Vibe system, the URL provided by Vibe for an RSS feed embeds some authentication information about the user. This means that the RSS URL must be protected and not shared between users. For this reason, RSS is not recommended for use on highly sensitive data. If necessary, you can disable RSS feeds for your Vibe site, as described in "Managing RSS Feeds" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*.

Securing Mirrored Folders

Mirrored folders make files that are stored on a file system available to users on the Micro Focus Vibe site. Two levels of security are provided for mirrored folder access:

- When you create mirrored folder resource drivers, as described in "Configuring Mirrored Folder Resource Drivers" in "Advanced Installation and Reconfiguration" in the *Micro Focus Vibe 4.0.4 Installation Guide*, you can choose read-only access or read/write access. In addition, you can identify specific Vibe users and groups that are allowed access to the mirrored folder resource drivers.
- When you set up the mirrored folders on the Vibe site, as described in Chapter 18, "Setting Up Mirrored Folders," on page 189 in this guide, you can set access controls on the Mirrored File folder.

Securing the Vibe Site against XSS

Cross-site scripting (XSS) is a client-side computer attack that is aimed at web applications. Because XSS attacks can pose a major security threat, Novell Vibe contains a built-in security filter that protects against XSS vulnerabilities. This security filter is enabled by default.

The following sections describe the types of content that the security filter blocks from the Vibe site, where exactly it blocks it from entering, and how you can disable the security filter or enable specific users to bypass the security filter.

- "Understanding What Content Is Not Permitted" on page 355
- "Understanding Where the Content Is Not Permitted" on page 355
- "Listing All XSS Threats in Your System" on page 356
- "Disabling the XSS Security Filter" on page 356

Understanding What Content Is Not Permitted

By default, the XSS security filter in Vibe is very strict, and does not allow users to add certain types of content. For example, the following content is not permitted:

- HTML that contains JavaScript
- Forms
- Frames
- Objects
- Applets

Understanding Where the Content Is Not Permitted

The type of content discussed in "Understanding What Content Is Not Permitted" on page 355 is filtered by Vibe in the following areas:

- Text and HTML fields in entries and folders
- Uploaded HTML files

Listing All XSS Threats in Your System

Vibe lets you run an XSS report that lists XSS threats that are contained in your Vibe system. For more information, see "XSS Report" on page 307.

Disabling the XSS Security Filter

IMPORTANT: Because of the serious nature of XSS attacks, we strongly recommend that you do not disable the XSS security filter for the entire site. If there are certain users who need to upload information to the Vibe site, you can grant those users access to bypass the XSS security filter, as described in "Enabling Users to Bypass the XSS Security Filter" on page 226.

It is possible to disable the XSS security filter for the entire site for each of these areas by copying the appropriate lines from the `ssf.properties` file, pasting them into the `ssf-ext.properties` file, then changing the values of the lines to `false`. The lines in the `ssf.properties` file that are responsible for enabling and disabling the XSS security filter are:

- `xss.check.enable`
- `xss.content.filter.file.extensions`

V Appendixes

A Managing Product Improvement

Path to Configuration Dialog: Vibe Administration Console > **Management > Product Improvement**

The first time you log in to Vibe, after changing the admin user's password, a dialog displays that explains that the purpose of the Vibe data collection system is to help improve the Vibe product.

IMPORTANT: Micro Focus collects nothing that identifies your organization, your data, or your users.

Accessing the Product Improvement Dialog

You can see what is collected, and you can modify, disable, or re-enable the data collection system by using the Product Improvement dialog.

1. Open the Vibe Administration Console as the Admin user.
2. Click **Product Improvement**.

The data collection process runs for the first time when a Vibe server has been running for 24 hours. Thereafter, it runs weekly.

After the initial run, a **View the information collected** link displays in the dialog that lets you download the `.json` file created by the collection process.

To see the information collected, open the downloaded file in an application such as WordPad.

About the Data That Is Collected for Product Improvement

As already mentioned, Micro Focus collects nothing that identifies your organization, your data, or your users.

The items in the `.json` file are mostly self-explanatory, but the following points might be helpful to understanding file content.

The data is divided in three sections:

- **Installation Identifier:** This is a unique string generated for each appliance. Its sole purpose is to let Micro Focus track usage and statistics for a specific appliance over time.
- **Tier 1:** This section includes the product, version and build, license type, and number of users.
- **Tier 2:** This section includes additional information about the installation, most of which is self-explanatory.
  - The **user** information doesn't include the LDAP user count because that is already available under the Tier1.
  - The user count numbers do not include system user accounts, such as `admin`, `_filesyncagent`, and so on.
  - The group count numbers do not include system groups, such as `allusers`, `allextusers`, and so on.

- `workspaceCount` does not include system workspaces, such as the `/Home` workspace and so on.
- The mobile device type is derived from the value of the description field associated with the device information captured in the system. Any descriptions that don't match one of the pre-defined keywords are included as `other`.

How Micro Focus Receives Product Improvement Data

After the weekly data collection process concludes, the system creates a `.json` data file and sends it to `ftp://productfeedback.Novell.com/stats/Vibe`.

If the FTP transfer is unsuccessful, the system attempts to send it again during the next weekly cycle. No send attempts are made outside of the weekly cycles.

Data files are sent through a regular non-secure FTP connection. File contents are not encrypted because no sensitive or identifying information is included.

B Documentation Updates

Changes made to this guide since the initial release of Vibe 4.0 are listed below.

Date	Sections Changed	Summary of Changes
April 2017	"Vibe Database" on page 287	Added to document new features and address confusion regarding user-friendly URL generation.
August 19, 2016	Various	Fixed broken help links from the administrative utilities.
March 28, 2016	"Dealing with Security Scan Results" on page 331	New section.
March 2016	"Customizing Email Templates" on page 272 "Limiting User Visibility" on page 225 "Configuring Single Sign-On with KeyShield" on page 115 "Synchronizing Users and Groups from an LDAP Directory" on page 205	New and updated sections for Vibe 4.0.1.
February 2016	"Configuring Protected Resources" on page 141	Added /ssf/s/readFile/share/* as a required URL path.
December 2015	"Configuring Tomcat to Redirect to Secure HTTP Connections" on page 338	Corrected file path to show `ROOT` rather than `ssfs` as it was in version 3.4.