

Administration Guide

Novell® Vibe™ Cloud

April 5, 2011

www.novell.com



Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2010-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the [Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Managing Users and Groups	9
1.1 Viewing Users	9
1.2 Adding Users	9
1.2.1 Adding Individual Users	9
1.2.2 Adding Multiple Users	10
1.3 Editing a User's Information	10
1.4 Resetting a User's Password	11
1.5 Making a User an Organization Administrator	11
1.6 Disabling a User	12
1.7 Viewing Groups	13
1.8 Creating Groups	13
1.9 Modifying a Group	13
1.9.1 Editing a Group's Information	13
1.9.2 Making Users Followers of a Group	14
1.9.3 Removing Users as Followers of a Group	14
1.9.4 Granting Administrator Rights to Group Members	15
1.9.5 Removing Administrator Rights from Group Members	16
1.9.6 Modifying Group Preferences	16
1.10 Displaying Administrators	17
1.10.1 Displaying Administrators in Your Organization	17
1.10.2 Displaying Administrators for a Group	17
1.11 Filtering Lists	18
1.11.1 Using the Basic Filter	18
1.11.2 Using the Advanced Filter	18
2 Controlling Privacy Settings for Your Organization	21
2.1 Setting the Organization Visibility	21
2.2 Setting Group Creation Privileges	22
2.3 Setting Messaging Privileges	22
2.4 Setting Group Follower Privileges	23
2.5 Setting User Follower Privileges	24
3 Controlling Federation Settings for Your Organization	27
3.1 Configuring the Identity Provider to Trust Vibe	27
3.2 Configuring Federated Authentication in Vibe	28
4 Managing Information about Your Organization	31
4.1 Managing Your Organization's Profile	31
4.2 Viewing License and Entitlement Information for Your Organization	31
4.3 Viewing User Entitlements for Your Organization	32
5 Reviewing Audit Log Files for the Web Admin Console	35

About This Guide

Novell Vibe Cloud is a real-time collaboration Web application that unites common communication, authoring, and social messaging tools. Vibe Cloud administrators can manage users and groups in their organizations.

- ◆ Chapter 1, “Managing Users and Groups,” on page 9
- ◆ Chapter 2, “Controlling Privacy Settings for Your Organization,” on page 21
- ◆ Chapter 3, “Controlling Federation Settings for Your Organization,” on page 27
- ◆ Chapter 4, “Managing Information about Your Organization,” on page 31
- ◆ Chapter 5, “Reviewing Audit Log Files for the Web Admin Console,” on page 35

Audience

This guide is intended for Novell Vibe Cloud organization 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, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of this manual, visit the [Novell Vibe Cloud Documentation Web site](http://www.novell.com/documentation/vibe_cloud/) (http://www.novell.com/documentation/vibe_cloud/).

Additional Documentation

You can find more Novell Vibe documentation at the [Novell Vibe Cloud Documentation Web site](http://www.novell.com/documentation/vibe_cloud/) (http://www.novell.com/documentation/vibe_cloud/).

Managing Users and Groups

1

- ♦ Section 1.1, “Viewing Users,” on page 9
- ♦ Section 1.2, “Adding Users,” on page 9
- ♦ Section 1.3, “Editing a User’s Information,” on page 10
- ♦ Section 1.4, “Resetting a User’s Password,” on page 11
- ♦ Section 1.5, “Making a User an Organization Administrator,” on page 11
- ♦ Section 1.6, “Disabling a User,” on page 12
- ♦ Section 1.7, “Viewing Groups,” on page 13
- ♦ Section 1.8, “Creating Groups,” on page 13
- ♦ Section 1.9, “Modifying a Group,” on page 13
- ♦ Section 1.10, “Displaying Administrators,” on page 17
- ♦ Section 1.11, “Filtering Lists,” on page 18

1.1 Viewing Users

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.



1.2 Adding Users

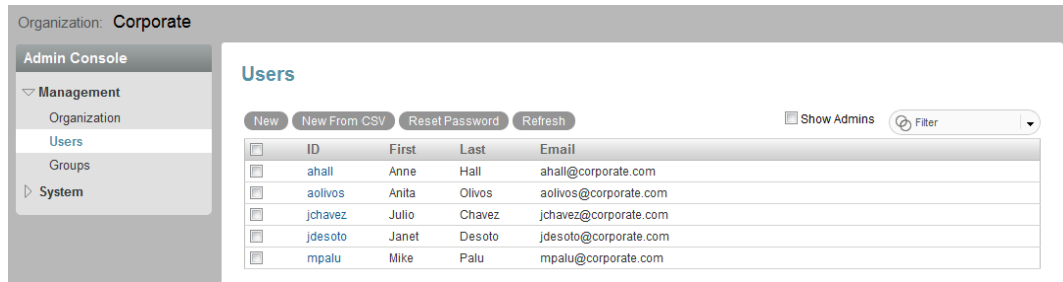
You can individually add users, or you can simultaneously add multiple users.

- ♦ Section 1.2.1, “Adding Individual Users,” on page 9
- ♦ Section 1.2.2, “Adding Multiple Users,” on page 10

1.2.1 Adding Individual Users

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.



3 Click *New*.

The New User dialog box is displayed.

4 Specify the appropriate information for the user, then click *OK*.

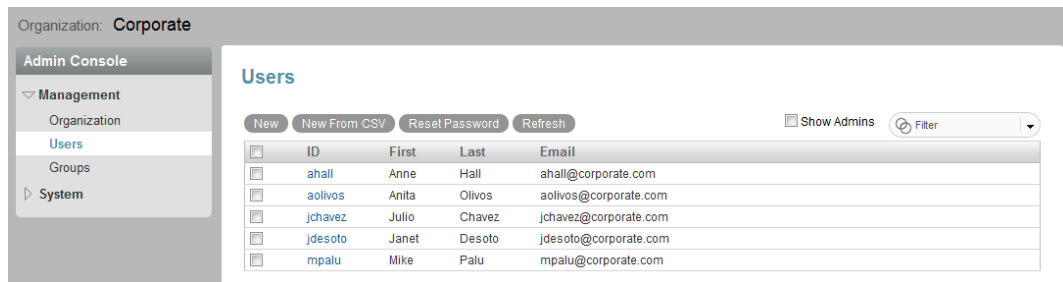
1.2.2 Adding Multiple Users

You can simultaneously add multiple users through the use of CSV files.

1 Log in to the Web Admin Console.

2 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.



3 Click *New From CSV*.

The *Add Users From CSV* dialog box is displayed.

4 Click *Browse*, then browse to the CSV file that contains the users that you want to add.

The CSV file must contain the following fields: *User ID*, *First Name*, *Last Name*, and *Email Address*. Optional fields are *Title*, *Office Phone*, *Mobile Phone*, *Fax Number*, *Address*, *City*, *State*, *Postal Code*, and *Country*.

5 Click *Preview*, then click *Start*.

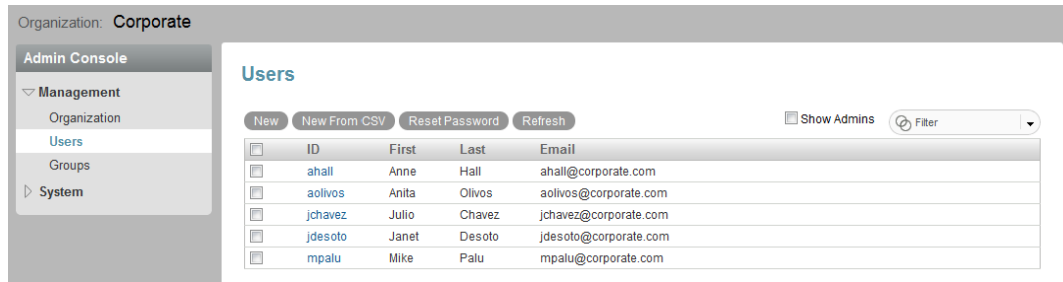
1.3 Editing a User's Information

You can edit a user's e-mail address, name, contact information, address, and more.

1 Log in to the Web Admin Console.

2 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.

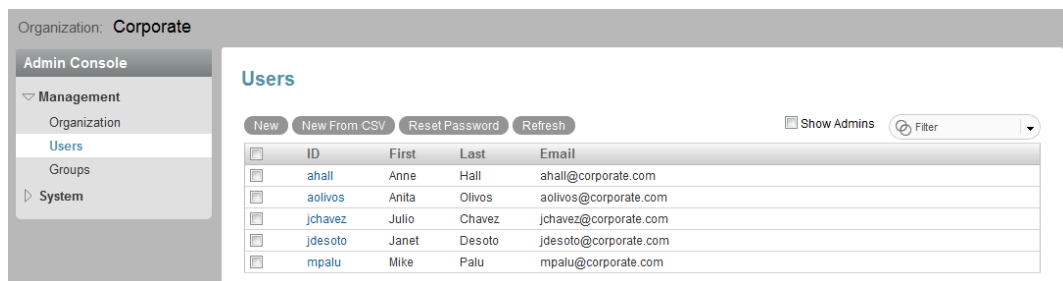


- 3 Click the name of the user whose information you want to edit.
The user's profile information is displayed.
- 4 Click *Edit*.
- 5 Make the desired modifications to the user's information, then click *Save*.

1.4 Resetting a User's Password

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.



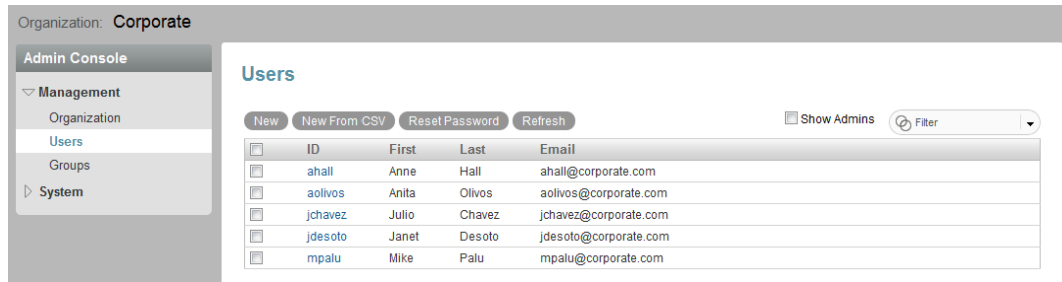
- 3 Select the user whose password you want to reset, then click *Reset Password*.
You can select multiple users.
- 4 Click *OK*.
A dialog box is displayed stating that the password was successfully reset.
The user receives an e-mail notification.

1.5 Making a User an Organization Administrator

Organization administrators have access to the Web Admin Console, and are responsible for managing users, groups, and all other aspects that deal with the organization.

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.

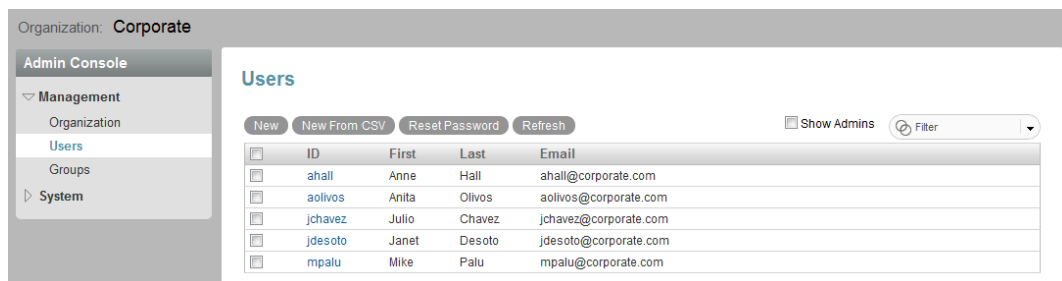


- 3 Click the name of the user you want to make an administrator for the organization.
- 4 Click *Edit*.
- 5 In the *Roles* section, select *Enable Organization Admin Privileges*.
- 6 Click *Save > Close*.

1.6 Disabling a User

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.

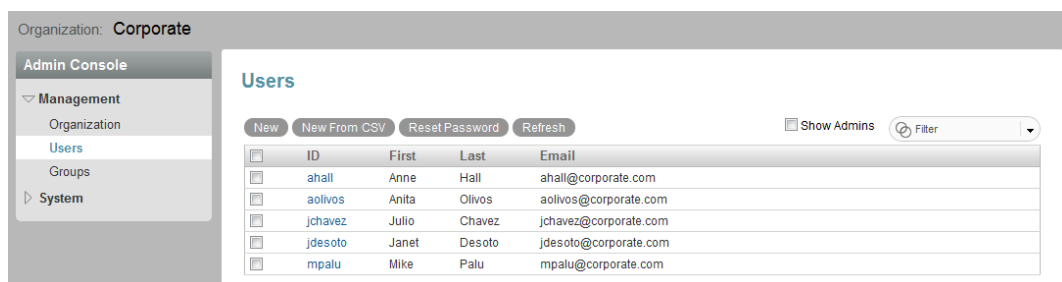


- 3 Click the name of the user you want to disable.
- 4 Click *Edit*.
- 5 Deselect *Enable user*, then click *Save > Close*.

To enable the user:

- 1 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.

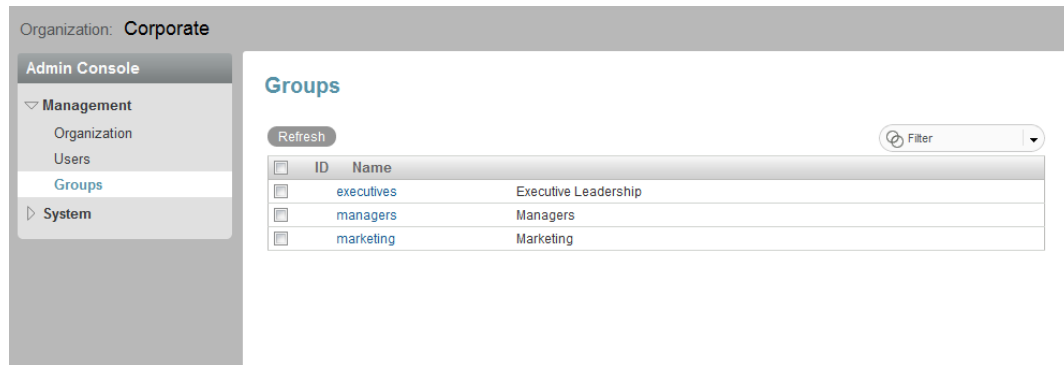


- 2 Click the name of the user who you want to enable.
- 3 Click *Edit*.
- 4 Select *Enable user*, then click *Save > Close*.

1.7 Viewing Groups

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Groups*.

The Groups page is displayed, listing all the groups that are currently in your organization.



1.8 Creating Groups

You cannot create groups within the Web Admin Console. To create a group, you must access the Vibe site. For more information on how to create a group within Vibe, see “[Creating a Group](#)” in “[Managing Groups](#)” in the *Novell Vibe Cloud User Guide*.

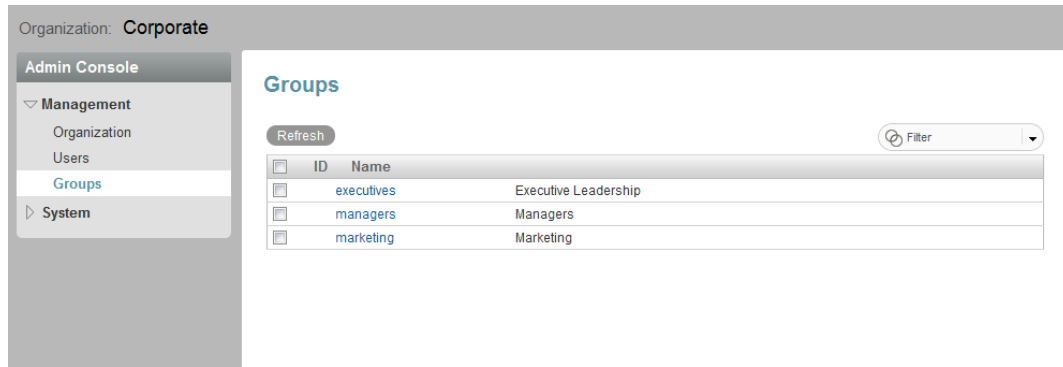
1.9 Modifying a Group

- ◆ [Section 1.9.1, “Editing a Group’s Information,” on page 13](#)
- ◆ [Section 1.9.2, “Making Users Followers of a Group,” on page 14](#)
- ◆ [Section 1.9.3, “Removing Users as Followers of a Group,” on page 14](#)
- ◆ [Section 1.9.4, “Granting Administrator Rights to Group Members,” on page 15](#)
- ◆ [Section 1.9.5, “Removing Administrator Rights from Group Members,” on page 16](#)
- ◆ [Section 1.9.6, “Modifying Group Preferences,” on page 16](#)

1.9.1 Editing a Group’s Information

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Groups*.

The Groups page is displayed, listing all the groups that are currently in your organization.



- 3 Click the name of the group whose information you want to edit.
- 4 Click *Edit*.
- 5 Make your desired modifications to the user's information, then click *Save*.

1.9.2 Making Users Followers of a Group

You can make users followers (members) of a group.

- 1 Expand *Management*, then click *Groups*.
The Groups page is displayed, listing all the groups that are currently in your organization.

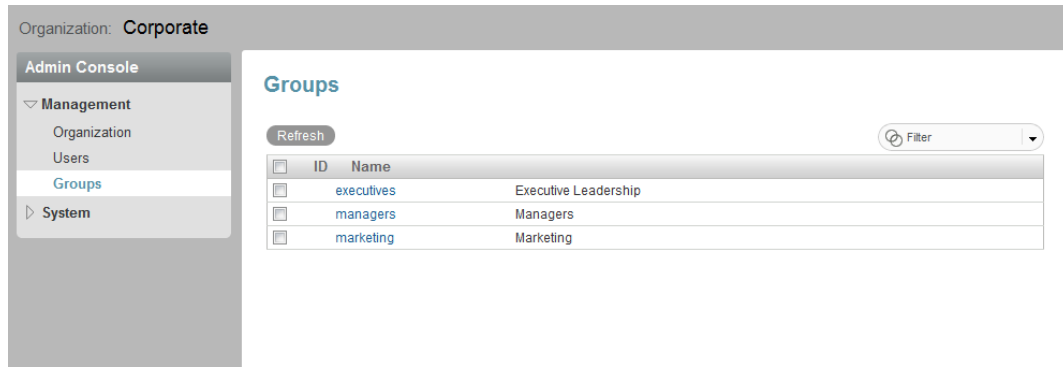


- 2 Click the name of the group for which you want to add or remove users.
- 3 Click the *Members* tab, then click *Add Member*.
The Select Members dialog box is displayed.
- 4 Select the users you want to make followers of the group, then click *OK*.

1.9.3 Removing Users as Followers of a Group

You can remove users as followers (members) of a group.

- 1 Expand *Management*, then click *Groups*.
The Groups page is displayed, listing all the groups that are currently in your organization.



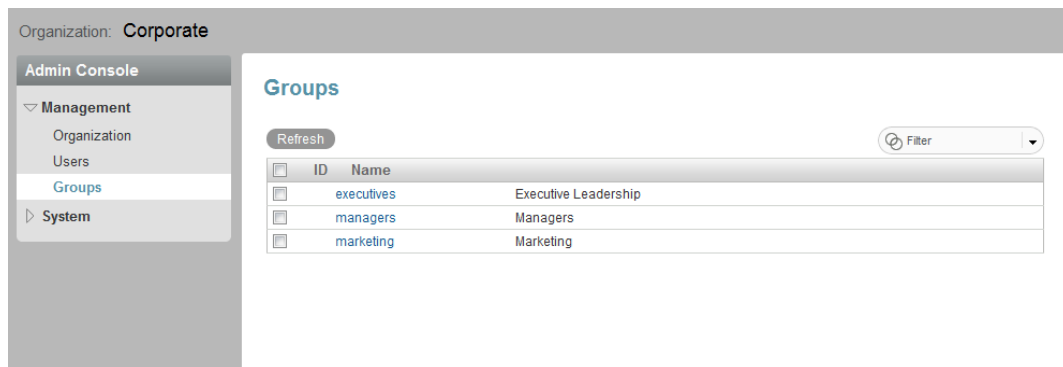
- 2 Click the name of the group for which you want to add or remove users.
- 3 Click the *Members* tab.
- 4 Select the users you want to remove from the group, then click *Remove Member*.
A message is displayed informing you that the member has been removed from the group.

1.9.4 Granting Administrator Rights to Group Members

You can grant administrator rights for users who are followers (members) of a group.

- 1 Expand *Management*, then click *Groups*.

The Groups page is displayed, listing all the groups that are currently in your organization.



- 2 Click the name of the group for which you want to grant administrator rights for group members.
- 3 Click the *Members* tab.
- 4 Select the users you want to grant administrator rights in the group, then click *Grant Admin*.
The user is granted administrator privileges.

For information about how to display all the administrators of a group, see [Section 1.10.2, “Displaying Administrators for a Group,”](#) on page 17.

1.9.5 Removing Administrator Rights from Group Members

You can remove administrator rights for users who are followers (members) of a group.

- 1 Expand *Management*, then click *Groups*.

The Groups page is displayed, listing all the groups that are currently in your organization.



- 2 Click the name of the group for which you want to revoke administrator rights for group members.
- 3 Click the *Members* tab.
- 4 Select the users you want to remove administrator rights in the group, then click *Remove Admin*.

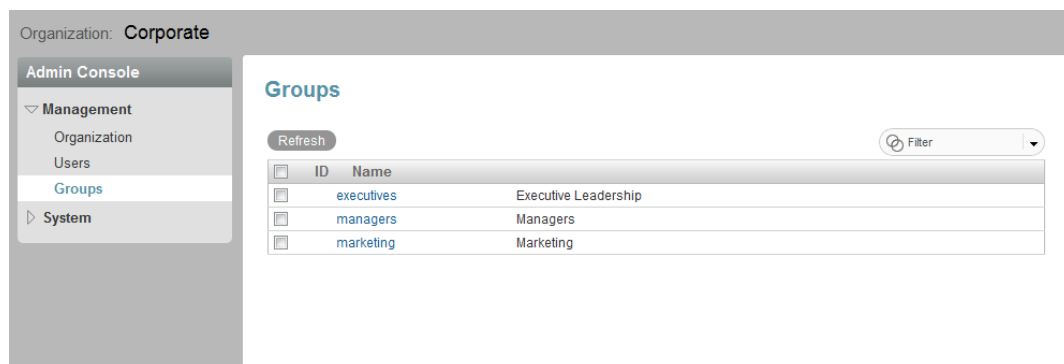
Administrator rights are removed from the user.

For information about how to display all the administrators of a group, see [Section 1.10.2, “Displaying Administrators for a Group,”](#) on page 17.

1.9.6 Modifying Group Preferences

- 1 Expand *Management*, then click *Groups*.

The Groups page is displayed, listing all the groups that are currently in your organization.



- 2 Click the name of the group for which you want to modify group preferences.
- 3 Click the *Preferences* tab.
- 4 Click *Edit*.

5 You can modify the following group preferences:

Follow Requesting/Message Visibility: Select one of the following options:

- ♦ Any user can follow the group without needing to make a request
- ♦ Users must request approval from the group leader before they are admitted to the group
- ♦ Users cannot make requests for group membership

Contribution: Select one of the following options:

- ♦ Any follower can add messages and replies
- ♦ Any follower can add replies; only group administrators can add messages
- ♦ Only group administrators can add messages and replies

Allowed to Email Group: Select one of the following:

- ♦ Any follower can e-mail the group
- ♦ Only group administrators can e-mail the group
- ♦ No one can e-mail the group

6 Click *Save*.

1.10 Displaying Administrators

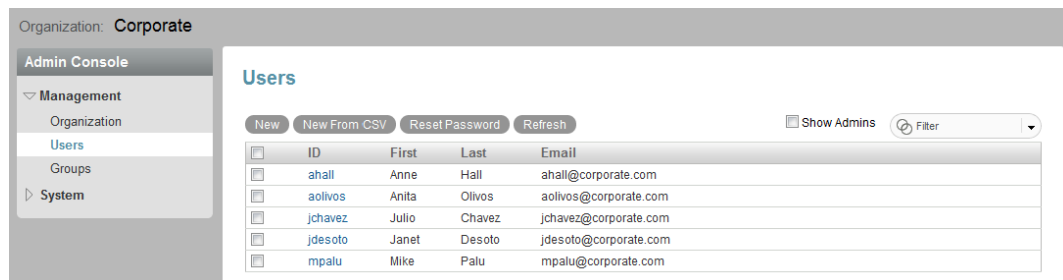
You can display the administrators for your organization or for a specific group.

- ♦ [Section 1.10.1, “Displaying Administrators in Your Organization,” on page 17](#)
- ♦ [Section 1.10.2, “Displaying Administrators for a Group,” on page 17](#)

1.10.1 Displaying Administrators in Your Organization

1 Expand *Management*, then click *Users*.

The Users page is displayed, listing all the users who are currently in your organization.

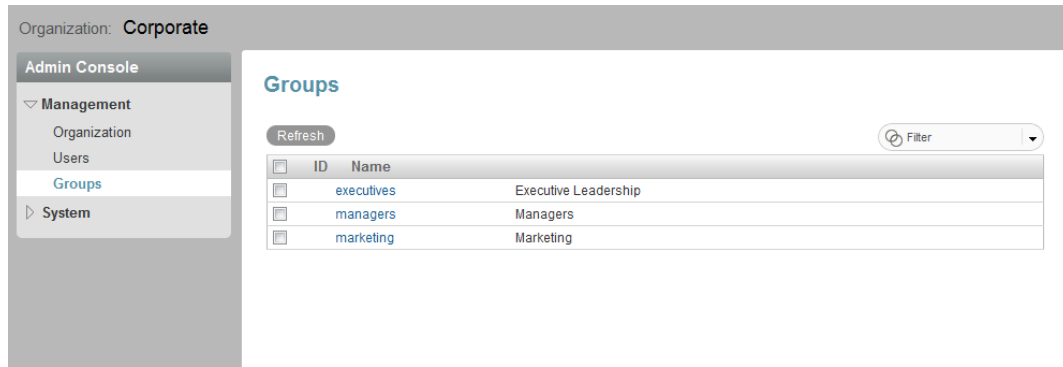


2 Select *Show admins*.

1.10.2 Displaying Administrators for a Group

1 Expand *Management*, then click *Groups*.

The Groups page is displayed, listing all the Groups that are currently in your organization.



- 2 Click the name of the group for which you want to display the group administrators.
- 3 Click the *Members* tab.
- 4 Select *Show admins*.

1.11 Filtering Lists

You can filter lists of users, groups, and more. The Filter is located in the upper-right corner of most pages of the Web Admin Console.

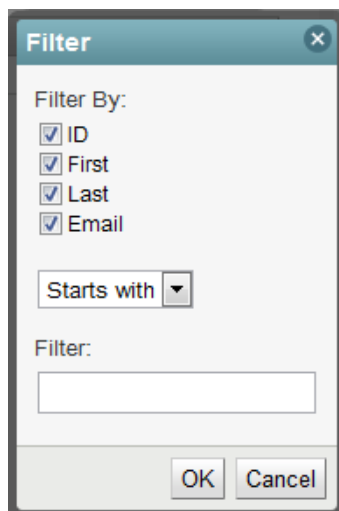
- ♦ [Section 1.11.1, “Using the Basic Filter,” on page 18](#)
- ♦ [Section 1.11.2, “Using the Advanced Filter,” on page 18](#)

1.11.1 Using the Basic Filter

- 1 In the *Filter* field, specify how you want to filter the list, then press Enter.

1.11.2 Using the Advanced Filter

- 1 Click the drop-down arrow next to the *Filter* field to display the Filter dialog box.



Different options are available, depending on the page you are currently viewing.

ID: Filter by the User ID.

First: Filter by the user's first name.

Last: Filter by the user's last name.

Email: Filter by the user's e-mail address.

Name: Filter by the group or user name.

Starts with: Filter by the first letters of the text in the *Filter* field.

Contains: Filter by the text in the *Filter* field.

Ends with: Filter by the last letters of the text in the *Filter* field.

Filter: Specify text that you want to filter for.

2 Click *OK*.

Controlling Privacy Settings for Your Organization

2

- ♦ Section 2.1, “Setting the Organization Visibility,” on page 21
- ♦ Section 2.2, “Setting Group Creation Privileges,” on page 22
- ♦ Section 2.3, “Setting Messaging Privileges,” on page 22
- ♦ Section 2.4, “Setting Group Follower Privileges,” on page 23
- ♦ Section 2.5, “Setting User Follower Privileges,” on page 24

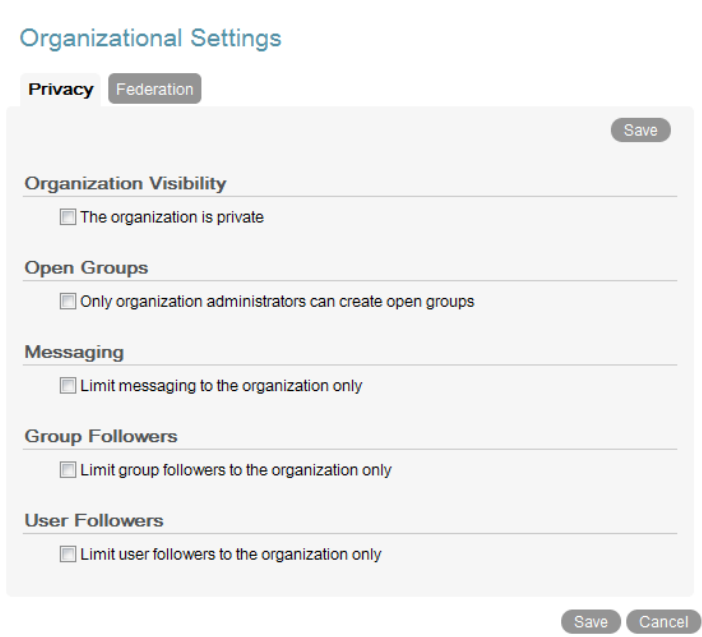
2.1 Setting the Organization Visibility

By default, users who belong to the organization can be seen by users who do not belong to the organization.

You can configure your organization to make users who belong to your organization invisible to users who do not belong to your organization. When users are invisible to users outside the organization, users can no longer follow or send messages to users outside the organization.

To restrict visibility for users outside the organization:

- 1 Log in to the Web Admin Console.
- 2 Expand *System*, then click *Settings*.
- 3 On the *Privacy* tab, click *Edit*.



The screenshot shows the 'Organizational Settings' interface. At the top, there are two tabs: 'Privacy' (selected) and 'Federation'. A 'Save' button is located in the top right corner of the settings panel. The 'Organization Visibility' section is expanded, showing a checkbox labeled 'The organization is private' which is currently unchecked. Below this are four other sections, each with a checkbox: 'Open Groups' (checkbox: 'Only organization administrators can create open groups'), 'Messaging' (checkbox: 'Limit messaging to the organization only'), 'Group Followers' (checkbox: 'Limit group followers to the organization only'), and 'User Followers' (checkbox: 'Limit user followers to the organization only'). At the bottom right of the settings panel, there are 'Save' and 'Cancel' buttons.

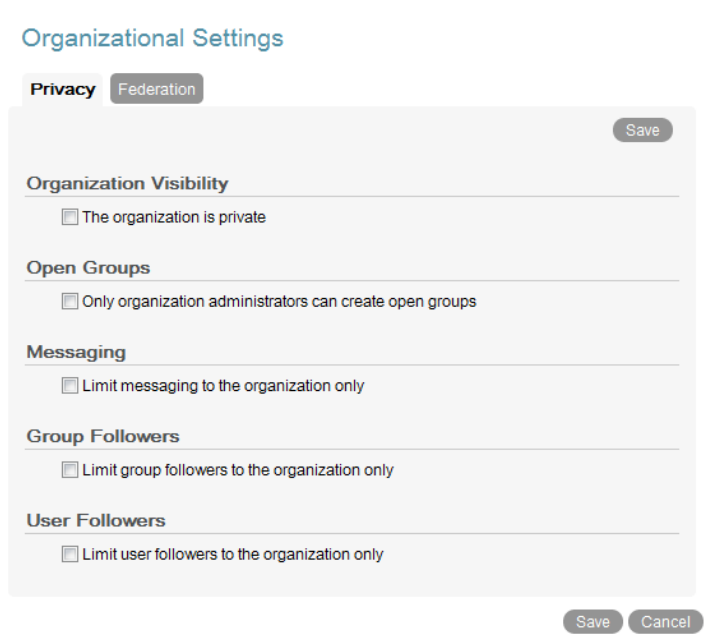
- 4 In the *Organization Visibility* section, select *The organization is private*.

2.2 Setting Group Creation Privileges

By default, any user can create an open group that can be seen by all users, regardless of the organization to which they belong.

You can configure your organization so only administrators of the organization have the ability to create open groups. Regular users can create only groups that are restricted to the organization or that are restricted to specified users within the organization.

- 1 Log in to the Web Admin Console.
- 2 Expand *System*, then click *Settings*.
- 3 On the *Privacy* tab, click *Edit*.



The screenshot shows the 'Organizational Settings' interface. At the top, there are two tabs: 'Privacy' (selected) and 'Federation'. A 'Save' button is located in the top right corner. Below the tabs, there are several sections with checkboxes:

- Organization Visibility**: The organization is private
- Open Groups**: Only organization administrators can create open groups
- Messaging**: Limit messaging to the organization only
- Group Followers**: Limit group followers to the organization only
- User Followers**: Limit user followers to the organization only

At the bottom right, there are two buttons: 'Save' and 'Cancel'.

- 4 In the *Open Groups* section, select *Only organization administrators can create open groups*.

2.3 Setting Messaging Privileges

By default, users can send and receive messages without organizational barriers.

You can configure your organization to restrict users from exchanging messages between users who do not belong to the same organization. However, users can reply to messages from users outside the organization if the messages were sent before messaging privileges were restricted. Furthermore, if users who are external to the organization were included on messages sent before messaging privileges were restricted, the user or group names are displayed as “Vibe User,” “Vibe User’s feed,” and “Vibe Group’s feed”.

To restrict messaging privileges for your organization:

- 1 Log in to the Web Admin Console.
- 2 Expand *System*, then click *Settings*.
- 3 On the *Privacy* tab, click *Edit*.

The screenshot shows the 'Organizational Settings' page with the 'Privacy' tab selected. The 'Federation' tab is also visible. The settings are organized into sections: 'Organization Visibility' with a checkbox for 'The organization is private'; 'Open Groups' with a checkbox for 'Only organization administrators can create open groups'; 'Messaging' with a checked checkbox for 'Limit messaging to the organization only'; 'Group Followers' with a checkbox for 'Limit group followers to the organization only'; and 'User Followers' with a checkbox for 'Limit user followers to the organization only'. There are 'Save' buttons at the top right and bottom right, and a 'Cancel' button at the bottom right.

- 4 In the *Messaging* section, select *Limit messaging to the organization only*.

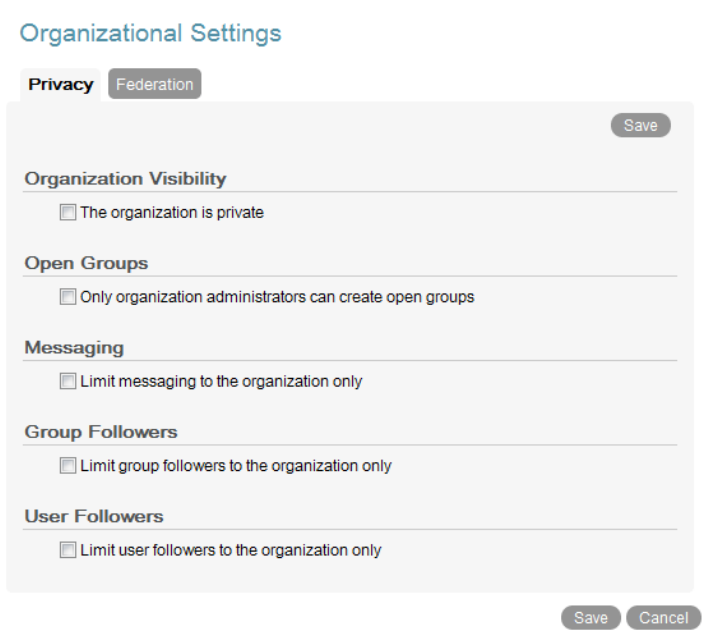
2.4 Setting Group Follower Privileges

By default, users can follow groups that are both inside and outside their organization.

You can configure your organization to restrict users from following groups that are outside of their organization.

- 1 Log in to the Web Admin Console.
- 2 Expand *System*, then click *Settings*.

- 3 On the *Privacy* tab, click *Edit*.



The screenshot shows the 'Organizational Settings' interface with the 'Privacy' tab selected. The 'Federation' tab is also visible. The settings are organized into sections: 'Organization Visibility' with a checkbox for 'The organization is private'; 'Open Groups' with a checkbox for 'Only organization administrators can create open groups'; 'Messaging' with a checkbox for 'Limit messaging to the organization only'; 'Group Followers' with a checkbox for 'Limit group followers to the organization only'; and 'User Followers' with a checkbox for 'Limit user followers to the organization only'. There are 'Save' buttons at the top right and bottom right, and a 'Cancel' button at the bottom right.

- 4 In the *Group Followers* section, select *Limit group followers to the organization only*.

2.5 Setting User Follower Privileges

By default, users can follow users who are both inside and outside their organization.

You can configure your organization to restrict users from following users who are outside of their organization. However, if users from another organization are already following users from your organization, they will continue to follow the users from your organization. Furthermore, users from your organization can follow users who were already following them.

To restrict following privileges for your organization:

- 1 Log in to the Web Admin Console.
- 2 Expand *System*, then click *Settings*.
- 3 On the *Privacy* tab, click *Edit*.

Organizational Settings

Privacy **Federation**

Save

Organization Visibility

The organization is private

Open Groups

Only organization administrators can create open groups

Messaging

Limit messaging to the organization only

Group Followers

Limit group followers to the organization only

User Followers

Limit user followers to the organization only

Save Cancel

- 4 In the *User Followers* section, select *Limit user followers to the organization only*.

Controlling Federation Settings for Your Organization

3

Federated authentication allows a source other than the Vibe server to handle user authentication to Vibe Cloud. To perform federated authentication, your organization must have its own identity provider that supports the SAML 2.0 protocol. The identity provider then passes user attributes (such as users' names and e-mail addresses) to Vibe.

For example, when a user specifies the Vibe URL in a browser, Vibe redirects the user to the identity provider for login rather than to the Vibe login screen. The user specifies his or her login credentials, then the identity provider verifies the user's credentials and redirects the user back to Vibe, which allows the user access to Vibe without requiring additional authorization. Vibe never sees the user login credentials because of the trusted relationship between Vibe and the identity provider.

You can leverage federated authentication for the following two purposes when configuring Vibe users:

- ♦ **User Authentication:** Your corporation's identity provider authenticates the user and passes the user's credentials to Vibe.
- ♦ **User Provisioning:** Vibe automatically creates an account for a user who is not in the Vibe system when the user authenticates through federated authentication.

To set up federation between Vibe and the identity provider, you must configure your identity provider to trust Vibe, and you must configure Vibe to trust the identity provider, as described in the following sections:

- ♦ [Section 3.1, “Configuring the Identity Provider to Trust Vibe,” on page 27](#)
- ♦ [Section 3.2, “Configuring Federated Authentication in Vibe,” on page 28](#)

3.1 Configuring the Identity Provider to Trust Vibe

Vibe currently supports only Novell Access Manager as an identity provider.

- 1 Configure the identity provider to trust Vibe.

How you configure your identity provider to trust Vibe differs depending on the identity provider that you are using.

For information on how to configure Novell Access Manager to trust a service provider such as Vibe, see “Configuring User Identification Methods for Federation” in the *Novell Access Manager 3.1 SP3 Identity Server Guide* (<http://www.novell.com/documentation/novellaccessmanager31/identityserverhelp/data/b65ogn0.html>).

- 2 Import Vibe metadata into your identity provider.

The metadata that you need to import is located at: <https://vibe.novell.com/saml/metadata> (<https://vibe.novell.com/saml/metadata>).

- 3 Configure the user attributes that you want the identity provider to share with Vibe.

User attributes are displayed on the user profile page in Vibe. Vibe accepts most user attributes that you want to configure the identity provider to send, but Vibe requires that at least the following user attributes are shared:

- ♦ E-mail address
- ♦ First name
- ♦ Last name

4 Continue with [Section 3.2, “Configuring Federated Authentication in Vibe,”](#) on page 28.

3.2 Configuring Federated Authentication in Vibe

- 1 Log in to the Web Admin Console.
- 2 Expand *System*, then click *Settings*.
- 3 Click the *Federation* tab.

Organizational Settings

Privacy Federation Save

Federated Authentication

Use federated authentication for user authentication

Use federated provisioning for new user creation

SAML 2.0 Metadata (copy and paste xml data here):

```
<?xml version="1.0" encoding="UTF-8" ?>
- <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="#idrP28ETi7J-jkVgFUwf01fH-p9-Y"
entityID="http://www.myidp.com:8080/nidp/saml2/metadata">
- <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:SignedInfo>
  <CanonicalizationMethod xmlns="http://www.w3.org/2000/09/xmldsig#"
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
- <ds:Reference URI="#idrP28ETi7J-jkVgFUwf01fH-p9-Y">
- <ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue
xmlns="http://www.w3.org/2000/09/xmldsig#">KR1U34lwIEzKAs2+i1wX7Df7kec=
</DigestValue>
  </ds:Reference>
</ds:SignedInfo>
  <SignatureValue
xmlns="http://www.w3.org/2000/09/xmldsig#">Jl/BbwfMDO+ZrGyTqElxymGL3+S3KZ
ULoQSlxDUq7pr9s7WdJgqgC2BSGR4WhOkD8nlhRu+mINNF
Pj3I5W2u1kqU11xauy4s77Z2L+xDqUTXJ6I7JFbfgvLE6QnPuT5jRt2vs6VSQ+SZfesUghDw6
tbt
+WC2MxcC7DTaptbrwzqjyY3ojMrygPGk6W5HCoEA+RDVTYhz1I4H8yI4vDMXetr1QN1jF3KYq
9fi
```

Save Cancel

- 4 Select *Use federated authentication for user authentication* if you want
- 5 Select *Use federated provisioning for new user creation* if you want Vibe to automatically create accounts for users who are not in the Vibe system.

- 6 In the *SAML 2.0 Metadata* field, paste the XML federation information that is generated by your identity provider.

Security Assertion Markup Language (SAML) 2.0, as shown in the following example, is the protocol that federation is based on.

```
SAML 2.0 Metadata (copy and paste xml data here):
<?xml version="1.0" encoding="UTF-8" ?>
- <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="#idrPZ8ETi7J-jkVgFUwf01fH-p9-Y"
entityID="http://www.myidp.com:8080/nidp/saml2/metadata">
- <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:SignedInfo>
<CanonicalizationMethod xmlns="http://www.w3.org/2000/09/xmldsig#"
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
- <ds:Reference URI="#idrPZ8ETi7J-jkVgFUwf01fH-p9-Y">
- <ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue
xmlns="http://www.w3.org/2000/09/xmldsig#">KR1U34lwIEzKAs2+i1wX7Df7kec=
</DigestValue>
</ds:Reference>
</ds:SignedInfo>
<SignatureValue
xmlns="http://www.w3.org/2000/09/xmldsig#">Jl/BbwfMDO+ZrGyTqElxymGL3+S3KZ
ULoQSlxDJq7pr9s7WdJgqgC2BSGR4WhOkD8n1hRu+mINNF
Pj3I5W2u1kqU11xauy4s7722L+xDqUTXJ6I7JFbfgvLE6QnPuI5jRt2vs6VSQ+SZfesUghDw6
tbt
+WC2MxcC7DTaptbrwzqjyY3ojMrygPGk6W5HCoEA+RDVTYhz1I4H8yI4vDMXEt+r1QN1jF3KYq
9fi
```

- 7 Click *Save*.

Managing Information about Your Organization

- ◆ Section 4.1, “Managing Your Organization’s Profile,” on page 31
- ◆ Section 4.2, “Viewing License and Entitlement Information for Your Organization,” on page 31
- ◆ Section 4.3, “Viewing User Entitlements for Your Organization,” on page 32

4.1 Managing Your Organization’s Profile

Your organizational profile contains various information about your organization, such as the organization ID, display name, description, contact information, and address. Some of this information can be edited.

To display your organization’s profile information and make changes:

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Organization*.

The screenshot displays the 'Organization: Corporate' profile page in the Web Admin Console. The left sidebar shows the 'Admin Console' menu with 'Management' expanded to 'Organization'. The main content area has tabs for 'Profile', 'License', and 'User Entitlements', with 'Profile' selected. The 'Profile' tab includes an 'Edit' button. The profile information is organized into sections: 'Organization' (Organization ID: 2612bc65-efe3-4ae1-a248, Description), 'Contact Information' (First Name, Last Name, Email, Office Phone, Mobile Phone, Fax), and 'Address' (Street, City, State, ZIP, Country).

- 3 On the *Profile* tab, click *Edit*.
- 4 Modify your organization’s profile information, then click *Save*.

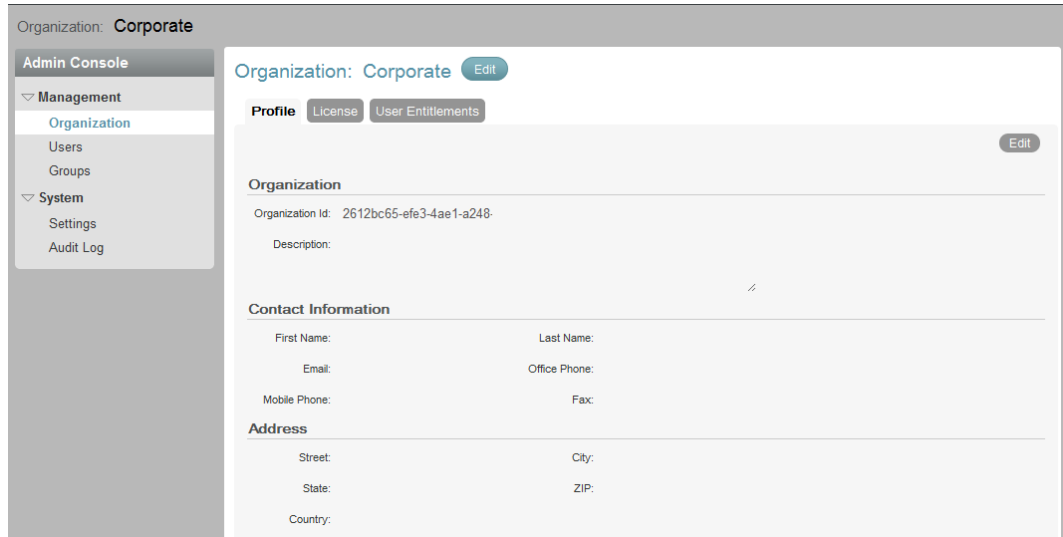
4.2 Viewing License and Entitlement Information for Your Organization

You can view your Vibe license to see the type of license you have, the number of users you are allowed to have, and the date your license expires.

Entitlements are privileges that can be specific to your organization. Examples of entitlements are the number of groups that each user is allowed to follow, the number of groups your organization is allowed to create, or the amount of bandwidth you are allowed to use.

To view your organization's license and entitlement information:

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Organization*.



- 3 Click the *License* tab.

In the *License Information* section, you see the following information about your license:

Type: The type of Vibe license that you currently have.

Expires: The date that your license expires. There is no expiration date for the Default Free license.

of Users: The number of users allowed in your organization.

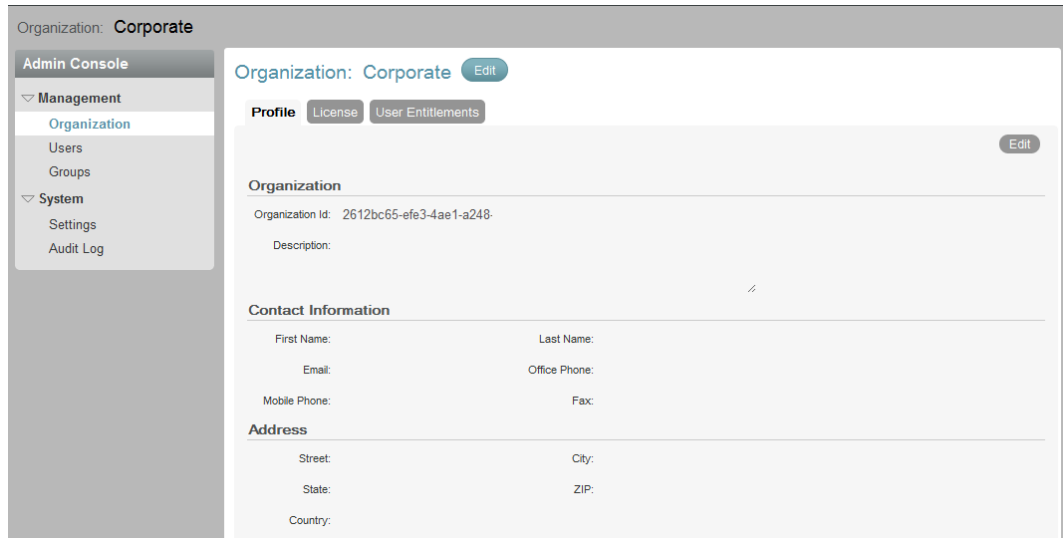
In the *Entitlements* section, you see entitlements that are associated with your license. For example, the total number of disk space that your organization is entitled to.

4.3 Viewing User Entitlements for Your Organization

User entitlements are privileges that are specific to users in your organization. An example of a user entitlement is the number of groups that each user is allowed to follow.

To view your organization's user entitlement information:

- 1 Log in to the Web Admin Console.
- 2 Expand *Management*, then click *Organization*.



3 Click the *User Entitlements* tab.

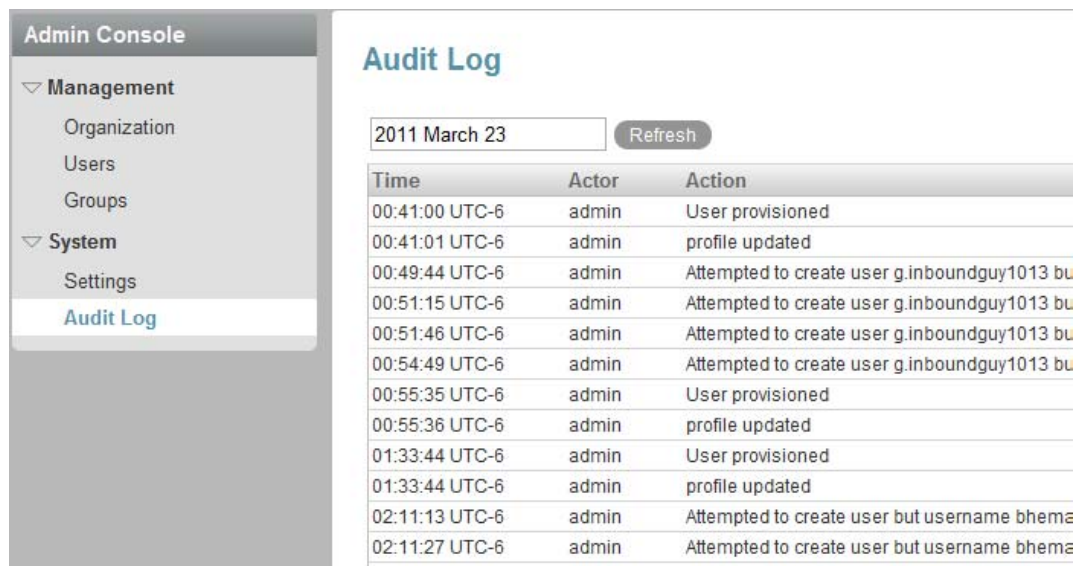
You see entitlements that exist for your organization, such as the number of groups that each user is allowed to follow.

Reviewing Audit Log Files for the Web Admin Console

5

You can view activity that has occurred in the Web Admin Console for your organization. Any user who has administrative privileges can make changes in the Web Admin Console. These changes can be tracked by reviewing the audit log files.

- 1 Log in to the Web Admin Console.
- 2 Expand *System*, then click *Audit Log*.
- 3 Click in the date field, then select the date for which you want to view activity.



Time	Actor	Action
00:41:00 UTC-6	admin	User provisioned
00:41:01 UTC-6	admin	profile updated
00:49:44 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:51:15 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:51:46 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:54:49 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:55:35 UTC-6	admin	User provisioned
00:55:36 UTC-6	admin	profile updated
01:33:44 UTC-6	admin	User provisioned
01:33:44 UTC-6	admin	profile updated
02:11:13 UTC-6	admin	Attempted to create user but username bhema
02:11:27 UTC-6	admin	Attempted to create user but username bhema

- 4 Click *Refresh* to obtain the most recent log information.

The following information is displayed:

Time: The time that the action was performed.

Actor: The user who performed the action.

Action: The action that was performed.

Target: The user who is the object of the action.

