Preface

2017 Mozy, Inc. © All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the express written permission of Mozy, Inc.

All other trademarks used herein are the property of their respective owners.

Mozy, Inc.

505 1st Ave S, Suite 600
Seattle, WA 98104
United States

http://www.mozy.com
## CONTENTS

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Implementing Mozy with Federated Identity</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Key Concepts ..................................</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Planning and Preparing for Implementation</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Push Mode vs. Pull Mode..................</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Firewall Requirements ..................</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Managing Directory Service Users in Mozy</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Add a User Group ..........................</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Define a User Group Administrator ....</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Determining Your Organization's Structure</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Configure the LDAP Directory Service ...</td>
<td>15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Installing the Mozy Service</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Logging in to the Admin Console</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Configure Mozy for Federated Identity Authentication</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Enable Directory Services Authentication</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Define the Connection Settings ..................................................................</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Provision Users .........................................................................................</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Deprovision Users ........................................................................................</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Set or Change a Synchronization Schedule ................................................</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Map Mozy and LDAP Attributes ......................................................................</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Enable SSO for Administrators .....................................................................</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Download the LDAP Connector .......................................................................</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Install the LDAP Connector .........................................................................</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Configure the LDAP Connector .....................................................................</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Run the LDAP Connector ..............................................................................</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>LDAP Connector Parameter Reference ..........................................................</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Set Up SAML Authentication ..........................................................................</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Validate SAML Messages ..............................................................................</td>
<td>26</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Deploying the Mozy Clients</th>
<th>29</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Download the Mozy Client ...........................................................................</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>About the Mozy Client ................................................................................</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>About Client Configuration ..........................................................................</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>Backup Software Updates ............................................................................</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Editing Client Versions .............................................................................</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Deploying the Mozy Backup Software .......................................................</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Choosing an Activation Method ...................................................................</td>
<td>50</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix A</th>
<th>Setting Up Active Directory Federation Service for Mozy</th>
<th>55</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Adding Mozy as a Relying Party Trust ......................</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>Editing the Claim Rules for Mozy ............................</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>Edit the Claim Rules for Mozy on Windows Server 2008 ...</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Exporting Token-Signing Certificate ..........................</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Deploy RelayState Settings .......................................</td>
<td>59</td>
</tr>
<tr>
<td>Appendix B</td>
<td>LDAP Error Handling</td>
<td>61</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------</td>
<td>----</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Deployment Worksheet</td>
<td>63</td>
</tr>
</tbody>
</table>
Mozy leverages the user management capabilities of Microsoft Active Directory or any LDAP-enabled directory service to automatically provision and deprovision Mozy users and provides Single Sign On (SSO) support for any identity provider that supports the Security Assertion Markup Language. To integrate with Mozy, your directory service must support LDAP v2.0 or higher and your identity provider needs to include support for SAML v2.0.

**Automated User Management**
When automating user management, everyday actions in the directory service, such as user creates, updates, and deletes, are synchronized to Mozy simplifying administration of the service for IT management. Mozy supports two methods of exchanging information with your directory service.

- **Pull mode:** Mozy queries the directory service for changes and automatically updates the corresponding user accounts. All of the configuration information for connecting to your user directory server and to your identity provider is stored in the Mozy service. The Mozy initiates all connections for synchronization and authentication.
- **Push mode:** Uses the Mozy LDAP Connector installed on a local server to push changes from your directory service to the Mozy service. Authentication information for the user directory is stored on a local server using the LDAP Connector software. The LDAP Connector software will push any changes from your network to the Mozy service.

**Single Sign-On Authentication**
To provide SSO support, Mozy integrates with any enterprise Identity Provider (IdP) using SAML v2.0. The IdP validates the identity of the user, then sends a SAML assertion (message) validating the users' credentials. The assertion is used to gain access to SAML-enabled applications and network services. The SAML assertion is presented to Mozy as proof of identity and eliminates the need for a Mozy-specific username and password. Once the assertion is validated, Mozy issues an access token for access to the service.

Mozy performs ongoing identity provider testing with Active Directory Federation Services (AD FS). Detailed instructions for integrating with AD FS are available in the Appendix. The identity providers listed below have been successfully integrated at customer locations.

- Active Directory Federation Services (AD FS)
- Azure
- Centrify
- LastPass
- Okta
- OneLogin
- OpenAM
Implementing Mozy with Federated Identity

- PingOne
- PingFederate
- RSA Via
- RSA FIM
- Secureauth
- SiteMinder:
  - Key Concepts
**Key Concepts**

Mozy with Directory Services authentication consists of three major components: the Mozy service, an enterprise IdP, and the LDAP directory service. These components together provide a streamlined user experience for user authentication and management. Once configured, users access the Mozy service through Mozy's Web access portal or through the providers application using their network credentials.

**Terms and Definitions**

- **Directory Service**: An authoritative source for enterprise-wide user identity information and management.
- **Lightweight Directory Access Protocol (LDAP)**: LDAP is the protocol used to access the directory service. The directory service must support LDAP 2.0 or higher.
- **Security Assertion Markup Language (SAML)**: An XML-based protocol used for requesting and exchanging the security token required by SSO. The Mozy service requires SAML 2.0.
- **Identity Provider (IdP)**: A provider that creates, maintains, and manages identity information and provides authentication to other service providers within a federation.
It is essential that you take the time to plan your implementation and prepare all of the components before starting the implementation process. You need to consider your network environment, the users you want to provision in Mozy, and how you want to organize those users. This section guides you through some of the information you need to know in order to have a successful deployment. We have provided a worksheet, available in the Appendix, that you can use to track the necessary information for the implementation so it is easily accessible.

- Push Mode vs. Pull Mode ................................................................. 10
- Firewall Requirements ................................................................. 10
- Managing Directory Service Users in Mozy ................................. 11
- Configure the LDAP Directory Service ........................................ 15
Push Mode vs. Pull Mode

Mozy allows you to synchronize your directory service by push changes from your local network to the Mozy service or by pulling changes from the directory services. Pull mode provides a level of convenience by allowing you to define all of your settings in the Mozy directory services configuration. Push mode provides for additional security by keeping authentication information for your directory services within your network.

Pull Mode
In pull mode, the Mozy service queries your user directory for changes on a scheduled basis. You enter your server settings and connection information in the Mozy Admin Console. Your network must be configured to allow incoming and outgoing connections to use directory services authentication in pull mode. At the scheduled time, Mozy connects to your user directory to check for any changes. Changes identified are synchronized to Mozy based on the provisioning and deprovisioning rules you have defined. All of the configuration needed for provisioning your users is done in the Mozy Admin Console.

Push Mode
When using push mode, you install the Mozy LDAP Connector on a server in your organization. The server on which the LDAP Connector is installed must be able to connect to your directory service. The connector can be run manually or you can run it using a scheduling utility. Once you have configured the connector software, it is recommended to use a scheduling utility to ensure your user information is consistently updated. Your network must allow outgoing connections to use directory services authentication in push mode. In addition, you must have an API key enabled for your account. Your Account Manager can assist you in obtaining an API key.

Firewall Requirements

Whether you have chosen to implement Mozy in Pull or Push mode, you may need to make adjustments to your firewall settings to accommodate the communication paths needed for the integration.

Note
For Push mode, only outbound connections from your network are required. Make sure to allow traffic on port 443. If you are using URL filtering in your network, add services.mozy.com. No inbound access is required.

For Pull mode, make sure your network can support the following communication for your Identity Provider and LDAP to the Mozy service. You may need to work with your network administrators to ensure the configuration decisions you made meet the operational requirements of your organization.

Table 1 Required Protocols and Ports

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Standard Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS (for IdP)</td>
<td>443 or 8443</td>
</tr>
<tr>
<td>LDAP (or StartTLS)</td>
<td>389</td>
</tr>
<tr>
<td>LDAPS</td>
<td>636</td>
</tr>
</tbody>
</table>
You can define the ports you want to use on your network. You are not required to use the standard ports.

**Whitelist**
Inbound access to the IP addresses listed below is required when using Pull mode:

- 74.112.148.4-5
- 74.112.148.61-68
- 173.243.52.4-5

---

**Managing Directory Service Users in Mozy**

Mozy allows you to automate the management of your users using your LDAP-enabled directory service. You can provision and deprovision Mozy users using sync rules and by mapping attributes to link the LDAP user to the user record in Mozy. Use the deployment worksheet to capture your decisions for use during installation.

**Mapping User Attributes**
Mapping attributes between Mozy and your user directory enables automatic provisioning and deprovisioning of your users.

<table>
<thead>
<tr>
<th>Mozy Attribute Name</th>
<th>Directory Service Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username*</td>
<td>Any attribute with an email address format; the default is &quot;mail&quot;.</td>
</tr>
<tr>
<td>Name*</td>
<td>Any attribute that contains the user's name; the default is &quot;cn&quot;</td>
</tr>
<tr>
<td>Fixed Attribute</td>
<td>Any immutable attribute. For example, an employee ID.</td>
</tr>
</tbody>
</table>

Mozy requires that Username (in email address format) and Name be mapped. An optional Fixed Attribute setting allows you to define a unique identifier, such as Employee ID. This identifier is used to find a user should the user's email address or name change. These attributes are used when synchronizing the user directory to the Mozy service and are included for each user returned in the query result.

**Note**
If you are using the Deployment Worksheet, you can add this information to it for reference when configuring the service.

**Grouping Users**
Mozy allows you to organize your users into groups to simplify management of the service. You can create configuration files assigned to each user group to customize the Mozy experience for the members of the group. Organize users by type of user, billing plan, or any other factor that makes sense for your organization. When you define your sync rules, you can specify the group into which a user should be added. If you do not specify your own user groups, Mozy adds users to the [default user group] during synchronization.

Most companies opt to keep the structure of their Mozy groups fairly simple using a default user group for most users and then creating a second group for more advanced users. For more information, see Determining Your Organization's Structure on page 14.
Provisioning Users
Mozy queries the user directory using standard LDAP queries. Once you have decided how you want to group users in Mozy, you can start to identify the LDAP attributes needed for the LDAP queries. Mozy processes provisioning rules first and then deprovisioning rules.

Provisioning Rules
LDAP queries allow you to sync users and place them in Mozy groups according to the specific rules you have defined in the query. If you have not defined custom user groups, the users are added to the [default user group].

For a primer on understanding and constructing LDAP queries, see http://technet.microsoft.com/en-us/library/aa996205%28v=exchg.65%29.aspx.

Note
If you are using the Deployment Worksheet, you can add this information to it for reference when configuring the service.

LDAP queries are processed in the order listed in your Sync Rules in Mozy. If a user matches multiple rules in your query, the first matching rule applies. As part of provisioning your users, you can define implied deprovisioning rules as well. To do this, define the number of days that a user must be missing from the sync process before they are suspended or deleted from the Mozy service.

Deprovisioning Rules
In addition to the automatic, or implied, deprovisioning, Mozy allows you to define explicit deprovisioning rules. For example, a terminated user could be placed in a "Terminated" container in your directory service. You can create a sync rule that queries that container and then automatically suspends or deletes users found in that container. As with Provisioning Users, queries are processed in the order in which they are listed. The sync process updates user records regardless of their deprovisioning status.

Note
If you are using the Deployment Worksheet, you can add this information to it for reference when configuring the service.

Add a User Group
Groups define how storage will be managed for users. Every account comes with a single, built-in user group. You can use the Add User Group panel to create your own user groups and define how each group manages storage. If you create at least one user group, you can delete the built-in user group. Once the group is created, you can use the Admin panel to specify an administrator for each group.

This feature is available in MozyEnterprise and for qualified resellers.

Procedure
1. Log in to the Admin Console.
   For additional information, see Logging in to the Admin Console on page 18.
2. Under Quick Links in the left-side pane, click User Group List.
3. Click Add Group.
4. Enter a name for the new group.
5. In **Server Storage Type**, select the type of storage you want server devices to use, and then enter the number of server devices available for this group.

**Note**

Server is available only if a server pass is enabled for your account.

**Table 3 Storage types**

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared</td>
<td>The organization's storage pool is shared among users and their devices, and among user groups if your organization uses them.</td>
</tr>
<tr>
<td>Limited</td>
<td>The organization's storage pool is shared, but the limit you set for any device, user, or user group cannot be exceeded.</td>
</tr>
<tr>
<td>Assigned</td>
<td>A user group can be assigned a portion of storage from the organization's storage pool. The assigned amount is reserved for use only by the users and devices within the user group. This assigned amount cannot be exceeded. This feature is available in MozyEnterprise and for qualified resellers.</td>
</tr>
</tbody>
</table>

6. In **Desktop Storage Type**, select the type of storage you want desktop devices to use, and then enter the number of desktop devices available for this group.

**Table 4 Storage types**

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared</td>
<td>The organization's storage pool is shared among users and their devices, and among user groups if your organization uses them.</td>
</tr>
<tr>
<td>Limited</td>
<td>The organization's storage pool is shared, but the limit you set for any device, user, or user group cannot be exceeded.</td>
</tr>
<tr>
<td>Assigned</td>
<td>A user group can be assigned a portion of storage from the organization's storage pool. The assigned amount is reserved for use only by the users and devices within the user group. This assigned amount cannot be exceeded. This feature is available in MozyEnterprise and for qualified resellers.</td>
</tr>
</tbody>
</table>

7. Click **Save**.

**Define a User Group Administrator**

When you create a user group, the administrator that created the group is responsible for managing the group. If you have created subadministrators, you can assign a different administrator to manage the group. Each user group can have one or more administrators assigned to it.

**Before you begin**

You must have subadministrators created on your account.

This feature is available in MozyEnterprise and for qualified resellers.
Procedure

1. Log in to the Admin Console.
   For additional information, see Logging in to the Admin Console on page 18.
2. Under Admins in the left-side pane, click List Admins.
3. Click the name of the administrator you want to assign as a group administrator.
4. In the User Groups section, click the checkbox next to the name of the user group, or groups this administrator will manage.
5. Click Save Changes.

Determining Your Organization's Structure

Many organizations are divided into logical groups such as business units or functional units. These units may organize members based on geographical location, business type, function, or many other factors.

When managing Mozy, each business or functional unit may have one or more administrators. In addition, each unit might include subordinate departments, each of which might have its own administrators. The Mozy Admin Console provides options for logical groupings to let you support your users using whatever structure best suits your organization.

User groups are the simplest way for an organization to logically group users. The root administrator creates user groups and determines their capabilities with client configurations. The root administrator can also create subordinate administrators, determine which administrative capabilities they have, and then assign them to manage specific user groups.

If your organization does not require a complex structure to use and manage Mozy, you should implement a flat user group structure.

Figure 1 Example of a flat organization with user groups

The root administrator creates sub-administrators and user groups.

Sub-administrators manage storage space and client configuration for users within the user group.

Partners, in conjunction with user groups, are more suited to the logical groupings required by more complex organizations with a deeper hierarchy. This more complex deployment approach requires planning and communication, but it offers benefits to an organization prepared to manage it effectively.
Partners are not available to all types of accounts. Partners are available in MozyEnterprise and for qualified resellers.

In this organizational model, the parent organization has subordinate partners, which can in turn manage their own sub-partners or user groups. In addition to user groups and subordinate administrators, the partner root administrator can also create sub-partners. In turn, administrators of sub-partners may also create their own subordinate partners and user groups.

If your organization has a complex hierarchical structure, you should deploy Mozy using both partners and user groups.

Figure 2 Example of a complex organization with partners and user groups

Configure the LDAP Directory Service

It's important that your directory service meets the requirements below to integrate successfully with Mozy. With the help of the Directory administrator, verify:

- Service Account has access to read from all containers listed in Worksheet Item #11.
- If you are using Pull mode, the firewall permits access to the directory from the Internet when coming from a white-listed IP address.
- All potential Mozy users have a unique email address or an attribute that uses an email address format.
Planning and Preparing for Implementation
CHAPTER 3

Installing the Mozy Service

Before beginning the installation process, make sure your network service has been configured to allow communication to the Mozy service. This section guides you through setting up the Mozy service to communicate with your directory service and identity provider.

Configure the services in the order listed below helps to minimize potential issues.

- Configure your firewall, both inbound and outbound connections
- Configure your identity provider or SAML service. You may return to complete configuration of the IdP, after Mozy is configured.
- Configure your LDAP directory to allow access from the Mozy service or from the LDAP Connector, if you are using push mode.
- Configure the Mozy service to connect to your LDAP user directory.

- Logging in to the Admin Console.................................................................18
- Configure Mozy for Federated Identity Authentication..............................18
- Download the LDAP Connector.................................................................22
- Set Up SAML Authentication....................................................................26
- Validate SAML Messages...........................................................................26
Logging in to the Admin Console

Administrators use the Admin Console to manage their backup environment.

Procedure

1. In a Web browser, enter https://secure.mozy.com/login.
2. Enter the email address and password associated with your administrator account.
3. Click Log In.

The Dashboard page of the Admin Console appears.

Configure Mozy for Federated Identity Authentication

If you have been capturing information in the Deployment Worksheet, use it as a reference when configuring the Mozy integration. Make sure you have reviewed the information for managing your users before you begin to configure Mozy.

Create User Groups
If you have decided to use user groups for organizing your users, create the groups in Mozy before continuing. For more information, see Add a User Group on page 12.

Enable Directory Services Authentication

Procedure

1. Under Configuration in the left-side pane, select Authentication Policy.
2. Next to Provider, select Directory Service.
3. Select the type of integration you want to use.
   - LDAP Pull: Select this option to have Mozy pull user information from your directory service on a scheduled basis.
   - LDAP Push: Select this option to use an on-premise LDAP Connector that will push changes in your directory service to the Mozy service.

After you finish
If you selected to use LDAP Push, you must install and configure the LDAP Connector on a server that has access to both the Internet and to your Identity store. For more information, see LDAP Connector Parameter Reference on page 24.

Define the Connection Settings

Before you begin
Make sure you have enabled directory services authentication for your account and defined whether you are integrating using Pull or Push mode.

Procedure

1. Under Configuration in the left-side pane, click Authentication Policy.
2. Click the Connection Settings tab.
3. Enter the connection settings for your user directory server.
   - Server Host: the hostname or IP address of your user directory server.
   - Protocol: the protocol you want to use for communication with the server. If you are using StartTLS or LDAPS, the field expands to allow you to paste the SSL certificate.
   - Port: the port to use for connections to the user directory.
   - Base DN: the highest point in your directory from which you want to search for users. For example, `dc=example,dc=com`.
   - (LDAP Pull only) Bind Username: the username of the account you want to use to traverse the user directory.
   - (LDAP Pull only) Bind Password: the password associated with the user account.

4. Click **Save Changes**.

5. (LDAP Pull only) Click **Test Connection** to validate the settings entered.
   - It is important that you save the changes to the Connection Settings before testing the connection.

After you finish
- Define the synchronization rules for provisioning and deprovisioning users.
- If you are using LDAP Push, define the Bind credentials in the LDAP Connector software. You can also run the connector in test mode to validate the settings once the software is configured. For more information on setting up the LDAP Connector, see **Configure the LDAP Connector** on page 22.

**Provision Users**

The **Sync Rules** tab allows you to define how users are provisioned, deprovisioned, and the schedule for synchronization.

**Procedure**

1. Under **Configuration** in the left-side pane, click **Authentication Policy**.
2. Click the **Sync Rules** tab.
3. Under Provision Users, click **Add Rule** for each query you need to define.
4. For each query entered, select the **Mozy User Group** users should be added to if they meet the query criteria.
5. If you have more rules to add, click Add Rule to create a new line item.
   Use the arrows to the right of the query to adjust the order in which the queries
   should be processed. Users are processed based on the first query matched.

6. Click the Send Welcome email checkbox to have an email sent to your users
   within information about Mozy and instructions on installing the software.

7. Click Save Changes.

Deprovision Users

You can use implicit or explicit deprovisioning rules to manage your users. The
instructions listed below guide you in creating explicit deprovisioning rules. For implicit
deprovisioning, use the checkboxes in the Provisioning Users section to define the
number of days users can be missing from the sync before they are suspended or
deleted from Mozy.

Procedure

1. In Authentication Policy, click the Sync Rules tab.
2. Under Deprovision Users, click Add Rule for each query you want to define.
3. For each query entered, select the appropriate action to take.
   • Take no action: If a user meets the criteria for the query, do nothing.
   • Suspend: The user account is suspended, but remains in the Mozy system.
   • Delete: The user account is removed from Mozy and all of the data deleted
     from the service.

Set or Change a Synchronization Schedule

You can schedule the frequency that Mozy and your directory service synchronize
user information. Where you define the synchronization schedule depends on whether
you are using directory service authentication in push or pull mode.

• **Push mode:** If you are using the Mozy LDAP Connector to push changes to Mozy,
  use any scheduling utility available on your server to determine how often updates
  are sent.

• **Pull mode:** Use the instructions below to define the synchronization schedule.

Procedure

1. Under Configuration in the left-side pane, click Authentication Policy.
2. Click the Sync Rules tab.
3. You can synchronize daily, hourly, or use both options.
   • For daily synchronization, click the Synchronize Daily At checkbox and
     enter the hour of day during which you want the sync to occur. The hour is
     entered using a 24-hour clock. Synchronization occurs during the hour
     specified.
   • For hourly synchronization, click the Synchronize Hourly checkbox.
     Synchronization occurs at the start of each hour.
4. Click the Enable synchronization safeguards checkbox, if it is not already
   selected, to limit the number of records that can be synchronized at any given
time.
If this option is selected, synchronization will fail if more than 5% of your users are impacted. An email is sent to the administrator of the account with additional information and instructions on how to proceed.

5. Click Save Changes.

Map Mozy and LDAP Attributes

Procedure

1. Click the Attribute Mapping tab and map the LDAP attributes to the Mozy attributes:

<table>
<thead>
<tr>
<th>Mozy Attribute Name</th>
<th>Directory Service Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username*</td>
<td>Any attribute with an email address format; the default is &quot;mail&quot;.</td>
</tr>
<tr>
<td>Name*</td>
<td>Any attribute that contains the user's name; the default is &quot;cn&quot;</td>
</tr>
<tr>
<td>Fixed Attribute</td>
<td>Any immutable attribute. For example, an employee ID.</td>
</tr>
</tbody>
</table>

2. Click Save Changes.

Enable SSO for Administrators

Before you begin

Your account must be configured to use directory services authentication. Contact your Account Manager if you require additional information. For instructions on implementing Mozy with directory services authentication, see the Federated ID Guide.

Mozy allows you to limit single sign-on to your users only or to expand it to administrators in your environment. If using SSO for Administrators, you still need a Mozy administrator account that manages the overall authentication policy for your organization.

Procedure

1. Under Configuration in the left-side pane, click Authentication Policy.
2. Make sure Directory Services is selected next to Providers.
3. At the bottom of the page on any tab, select the Enable SSO for Admins checkbox.
4. Click Save Changes.

Results

An email is sent to your administrators with instructions on how to log in to Mozy using your network credentials.
Download the LDAP Connector

You can download the LDAP Connector when configuring Mozy to use Directory Services authentication in the Authentication Policy panel.

Procedure

1. Log in to the Admin Console.
   For additional information, see Logging in to the Admin Console on page 18.
2. Under Configuration in the left-side pane, click Authentication Policy.
3. Next to Providers, make sure Directory Services is selected.
4. Click Save Changes.
5. Next to Use LDAP Push click Download to download the connector software.

Install the LDAP Connector

The Mozy LDAP Connector allows you to push changes from the LDAP user directory to the Mozy service. You can push these changes on a scheduled basis by initiating the synchronization using your scheduling utility.

Procedure

1. Double-click the LDAPConnector installation file.
2. Click Next.
3. Review and accept the Beta License Agreement, then click Next.
4. Select the directory in which to install the connector. Click Next and then click Install to start the installation.
5. Click Finish to close the installation wizard.

After you finish

Once you have installed the connector software, you need to configure the connector software, including your LDAP Bind username and password, to allow the software to connect to your user directory.

Configure the LDAP Connector

Before you begin

Perform this step only if you have enabled the LDAP Push Directory Service integration in your Authentication Policy. For more information, see Enable Directory Services Authentication on page 18.

The LDAP Connector is command line software that allows you to communicate changes in your user directory to the Mozy service automating user management of the Mozy service. Once you define the server connection settings in the Mozy Admin Console, configure the Mozy login and Bind credentials the LDAP Connector should use to synchronize changes.

Note

You must have your Partner ID and an API key to configure and run the LDAP Connector software. Please contact your Account Manager for this information if you have not yet received it.
The configuration settings for connecting to your LDAP user directory are stored in the registry. You have the option of configuring a proxy server that the connector must use to access the Mozy service. The parameters that are listed below are required to configure the LDAP connector. For more information, see LDAP Connector Parameter Reference on page 24.

- Partner ID
- API Key
- LDAP Username
- LDAP Password
- Test Mode

Use the following examples to guide you in configuring your connection.

**Command Format**

```
LDAPConnector.exe -partner_id partner_id -api_key Your API Key -
ldap_username bind username -ldap_password bind password -test_mode true/false
```

**With Sample Entries:**

```
LDAPConnector.exe -partner_id 123456 -api_key HGgn41ZfhTNs...ybq0bSV5i -ldap_username
"cn=admin,dc=test,dc=mycorp,dc=com" -ldap_password d&ldi82D1 -
test_mode true
```

**Sample Response:**

```
0064FC70 connectEX(400, 10.0.113.44:443) local: 10.0.113.121:62853
0064FC70 close(400)
2014-Jul-22 15:01:40.958452  Begin checking connector version from servers.
00651BA8 connectEX(404, 10.0.113.44:443) local: 10.0.113.121:62855
00651BA8 close(404)
006D6C68 connectEX(384, 10.0.113.44:443) local: 10.0.113.121:62856
{"api":"fedid","rsrc":"sync_config","total":1,"type":"response",
"generated_at":1406012502,"count":1,"items":[{"data":{"_id":"123456,
"rev":"343-2e52e210d7bd6504541439b8f6f6f9f","rules":null,"deprovision":null,"test_mode":false},
"partial_result":false}],
```

**Run the LDAP Connector**

**Before you begin**

- Ensure you have removed the LDAP username and LDAP password parameters to run the LDAP Connector software. The presence of these parameters indicate that the connector is in configuration mode.
Your Partner ID and API Key are required when running the LDAP Connector. For more information on the parameters available for the connector software, see LDAP Connector Parameter Reference on page 24.

Use the following examples to guide you in configuring your connection.

Command Format

```
LDAPConnector.exe -partner_id {partner_id} -ldap_req_timeout {time in seconds} -test_mode {true/false}
```

With Sample Entries:

```
LDAPConnector.exe -partner_id 123456 -ldap_req_timeout 180 -test_mode true
```

Sample Response

```
2014-Jul-22 15:02:27.288085  Starting transfer of LDAP data, test_mode=false
2014-Jul-22 15:02:27.337090  Begin authorization to servers.
006E1D48 connectEX(400, 10.0.113.10:443) local: 10.0.113.121:62860
006E1D48 close(400)
006E1E08 connectEX(412, 10.0.113.10:443) local: 10.0.113.121:62862
006E1E08 close(412)
006E2FC8 connectEX(404, 10.0.113.10:443) local: 10.0.113.121:62863
006E2FC8 close(404)
2014-Jul-22 15:02:33.265682  Beginning connection to LDAP server, host=10.0.113.61, port=389
2014-Jul-22 15:02:33.322688  Beginning query to LDAP server, query=(cn=admin*)
006E1238 connectEX(404, 10.0.113.10:443) local: 10.0.113.121:62865
2014-Jul-22 15:02:34.478804  Data returned from LDAP upload request to servers:
{"api":"fedid","rsrc":"syncjob","total":1,"type":"response","generated_at":1406012554,"count":1,"items": [{"_id":"3d772b24320e31cc60d","description":null,"_rev":"1-0d28443ad6493c32c7027b68f8","_deleted":null,"created_at":"2014-07-22T07:02:34Z","job_id":"3d772b2432021e31cc60d","meta":{"id":"3d772b2432031cc60d","title":null,"deleted":null,"link":"/fedid/syncjob/3d772b2...1cc60d","etag":"91dda499","rsrc":"syncjob"}, "link":"/fedid/syncjobs","query":{"scope":{"partner":123456},"filter":null,"max_limit":1000},"partial_result":false}]
2014-Jul-22 15:02:34.504806  LDAP upload to servers succeeded.
006E1238 close(504)
```

### LDAP Connector Parameter Reference

The LDAP Connector is command line software that allows you to communicate changes in your user directory to the Mozy service automating user management of the Mozy service. The connector can be run using a scheduler to process updates as frequently as needed. Once you define the server connection settings in the Mozy Admin Console, configure the Bind credentials the LDAP Connector should use to...
synchronize changes. If this is the first time you are configuring the LDAP Connector, see the *Federated ID Guide* for information on downloading, installing, and configuring the software.

**Parameters**
The following parameters allow you to configure and then run the software to update the Mozy service. Settings are stored in the registry. If you want to delete any of the settings, specify the parameter followed by empty quotes. For example, `proxy_uri "`.

- **-partner_id**
  The ID of the partner your are synchronizing. If you do not know your partner ID, contact your Account Manager. This parameter is required when running the LDAP Connector software.

- **-api_key**
  The API key for your partner record. The API key is used to authenticate you to the partner record. If you do not know your API Key, contact your Account Manager. This parameter is required when running the LDAP Connector software.

- **-test_mode**
  This parameter is required when running the LDAP Connector software. Use `-testmode True` to test the configuration and validate your settings. Use `-test_mode False` when you want to run the software during normal operations.

- **-ldap_req_timeout**
  This parameter allows you to adjust the timeout value when running the LDAP Connector software. The value is entered in seconds and is not stored in the registry. The default time is 120. Use this parameter if you want to use a timeout value other than the default value of 120 seconds.

- **-ldap_username**
  The account to use to log in to your user directory. This account must have sufficient access to traverse the records defined in the Base DN in the Admin Console. If this parameter exists, the connector is assumed to be running in configuration mode.

- **-ldap_password**
  The password associated with the account you want to use to log in to your user directory. If this parameter exists, the connector is assumed to be running in configuration mode.

- **-show_ldap_config**
  Returns the configuration settings the Mozy service will use to sync with the LDAP user directory. This includes the connecting settings defined in the Mozy Admin Console and the Bind credentials defined for the connector.

- **-proxy_uri**
  If you need to go through a proxy to reach the Mozy service, enter the location of the proxy server. Enter the URI in the format `https://myproxy.example.com:port` or `https://198.51.100.1:port`. This setting are stored in the registry, but you can override the registry entry by specifying the parameter when running the connector.

- **-proxy_logon_name**
  The account to use to log in to the proxy server. The LDAP Connector supports basic proxy authentication only. This setting are stored in the registry, but you
can override the registry entry by specifying the parameter when running the connector.

-\texttt{proxy\_logon\_password}

The password associated with the proxy log in information. This setting are stored in the registry, but you can override the registry entry by specifying the parameter when running the connector.

## Set Up SAML Authentication

### Before you begin

You can find the SAML token-signing certificate in the configuration for your identity provider.

### Procedure

1. Click the \textbf{SAML Authentication} tab and enter the following information:

   - **Authentication URL**: The URL Mozy uses to validate authentication.
   - **SAML Endpoint**: The Mozy server that consumes the assertion: \texttt{https://auth2.mozy.com/your subdomain/saml}
   - **SAML Certificate**: The SAML certificate you want to use to validate the authentication exchange. This is all text between the X.509 tags.

2. Click \textit{Save Changes}.

### After you finish

The SAML Validation tool allows you to ensure authentication requests can be processed successfully and to troubleshoot any potential SAML exchange issues.

## Validate SAML Messages

When configuring your SAML settings, you can validate the SAML assertions that are sent to ensure that your users can log in to the service successfully.

### Procedure

1. Under \textit{Configuration} in the left-side pane, click \textit{Authentication Policy}.
2. Next to \textit{Providers}, make sure \textit{Directory Services} is selected.
3. Click the \textit{SAML Authentication} tab.
4. Make sure you have entered your SAML settings in the available fields.
5. Click \textit{Validate SAML assertions} at the bottom of the page.
6. Copy and paste the SAML assertion into the provided field.
   
   A portion of a SAML assertion is shown below for reference.

   ```xml
   <samlp:Response
       ID="_49722f3c-c36a-42ae-ad63-1f4ec637fb4f"
       Version="2.0"
       Destination="https://auth2.mozy.com/fedidpush/saml"
       Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   SessionIndex="_54044b5c...c2e58">
   
7. Select the format of the assertion you are using.
   
   - Base-64 encoded: Use if the SAML assertion is encoded.
   - Plain text: Use if you are pasting a copy of the SAML assertion in plain text.
     The example in the previous step uses plain text.

8. Click Validate.
   
   The SAML Validation Results window appears with details on the success or failure of each step in the SAML assertion.
Installing the Mozy Service
CHAPTER 4
Deploying the Mozy Clients

Your organization may employ any of these options for how users can obtain and install the backup software on desktops or servers.

Note

Edit Client Versions is available in MozyEnterprise and for qualified resellers.

- Download the client to a network share and direct users to install the client from this location. If you have the ability to edit the client version, be sure the version you download is the same version you have selected in Edit Client Version. If you left the default setting in Edit Client Version, you'll need to download the most recent client.

- Rely on an automated email you can choose to send to users from the Admin Console. This email provides a link to the Mozy Website from which users can download the client.

- Provide the installation instructions from the User Guide, which provides a link to directly download the most recent version of the client from Mozy. If you are managing client versions for your organization and do not typically use the currently available version, do not use this option.

- Download the Mozy Client.......................................................... 30
- About the Mozy Client............................................................. 30
Download the Mozy Client

The Download Mozy Client panel allows you to download the latest version of Mozy as well as older versions. It also includes the MD5 string to validate the file is correct, the date the client was generated, and the release notes.

Note

You can choose for users to receive an email when their account is created. If backup software version 2.22 and later for Windows or version 2.11 and later for Mac are used, your users click the unique link in that email to open a Web page. On that Web page, they create a password, which activates their account. Then they can download and install the backup software and activate it using that same password. If older versions of the backup software are used, the product key is emailed to the user. The user must use that key to activate the backup software. The download link provided depends on the version you have defined in the Edit Client Version panel. You can also save the file you download to a network drive and direct users to install the client from the local network.

Procedure

1. Log in to the Admin Console.
   For additional information, see Logging in to the Admin Console on page 18.
2. Under Resources in the left-side pane, click Download Mozy Client.
3. Click the link for the client you want to download.
   The current releases are listed at the top of the panel. Older releases can be found toward the bottom.
4. Save the file to your hard drive and install the client when you are ready.
5. To view information about the contents of the release, click Release Notes.

About the Mozy Client

About Client Configuration

The Client Configuration panel allows you to customize your Mozy client software configuration. The Mozy client is the software that resides on users’ machines and allows them to configure their backups, restore files, and track their backup histories.

All of the settings below can be cascaded down to your subpartners, administrators, user groups, and users. In order for the settings to be cascaded, the client configuration must be set to use the default user group.

All of the settings in the client configuration can be cascaded down to your users. In addition, you can lock the settings prohibiting users from making changes to the configuration in the client.

You can define many options in the client configuration.

- **Preferences**: set or lock the options available to machines using the local client.
- **Scheduling**: schedule backups to occur at a specific time or on a periodic basis.
- **Bandwidth Throttling**: enable and customize how bandwidth is managed during backups.
- **Windows Backup Sets**: define the types of files that are included in the backups for Windows machines.
- **Mac Backup Sets**: define the types of files that are included in the backups for Mac OS X machines.
- **Linux Backup Sets**: define the types of files that are included in the backups for Linux machines.
- **User Groups**: apply a designated configuration to specific user groups, so each user group has its own default settings.

Create or Change a Client Configuration

On the Client Configuration panel, you can define the default options used by the backup software. You can create an entirely new client configuration, or copy an existing configuration and change it to more quickly make a new configuration. You may also change or delete any existing client configuration.

**Procedure**

1. Log in to the Admin Console.
   For additional information, see Logging in to the Admin Console on page 18.
2. In the left menu, click **Client Configuration**.
3. Create a configuration, copy an existing configuration and modify it, or modify any configuration.
   a. To create a configuration, type its name in the **Name** box under **Create a new client configuration**, select the key type if necessary, and then click **Next**.
   b. To change a configuration, click its name under **Existing Client Configs**.
   c. To copy a configuration, click **Copy** under **Existing Client Configs**.

4. Click the **Preferences** tab to configure your preferences.
   For more information on Preferences, see Setting Preferences on page 35.
5. Click the **Scheduling** tab to configure scheduling options.
   For more information on Scheduling, see Setting Automatic Backups on page 36.
6. Click the **Bandwidth Throttling** tab to configure bandwidth throttling options.
   For more information on controlling bandwidth usage, see Bandwidth Throttling on page 37.
7. Click the **Windows Backup Sets, Mac Backup Sets, or Linux Backup Sets** tab to configure backup sets.
   For more information on defining backup sets, see Backup Sets on page 37.
8. Click the **User Group** tab to select the user groups that are assigned to the client configuration.
9. Click **Save Changes**.
Proxy Server Settings

This feature is available in MozyEnterprise and for qualified resellers. These methods are available for administrators to configure proxy server settings for the Mozy backup software on Windows. These settings apply to Mozy Sync as well.

- Client configuration settings in the Admin Console, at Client Configuration > Configuration Name > Preferences
- Command Line Interface (CLI) switches during automated deployments

Either of these methods allows you to centralize management of the proxy settings, ensuring all clients are up-to-date and accurate.

Note

If you automate deployment of Mozy software, you must ensure the proxy settings defined in the automated deployment and those in the Admin Console do not conflict. Inconsistencies between the locked client settings and those in the Admin Console can prevent the Mozy software from establishing a connection to the Internet and the Mozy service.

Administrators may also choose to permit users to configure proxy server settings on their own, from within the Mozy backup software on Windows. End users may also be permitted to manually configure their own proxy server settings for Mozy Sync on Windows.

Note

There is no means to define proxy server settings for Mozy backup software. There is also no means to define proxy server settings for Mozy Sync on Mac. This is because the proxy server settings defined on each computer are automatically used.

When a proxy is defined for a particular client, if a connection cannot be obtained through the defined proxy, the client reverts to using a direct connection to ensure backups continue, so your data remains secure.

Table 5 Proxy configuration options

<table>
<thead>
<tr>
<th>Option</th>
<th>Admin Console Setting</th>
<th>CLI Switch for Automated Deployments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your organization does not use a proxy, and Mozy software connects directly to the Internet.</td>
<td>No Proxy (Direct Connect)</td>
<td>No switch is necessary</td>
</tr>
<tr>
<td>This is the default setting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You define the proxy server and port number, IP address, host name, or URL the Mozy software must use. Use the format server:port</td>
<td>Use a Specific Proxy</td>
<td>/USEPROXY</td>
</tr>
<tr>
<td>Example: myproxy:80</td>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td>/useproxy:proxyserver:80</td>
<td></td>
<td>/useproxy:url</td>
</tr>
<tr>
<td>/useproxy:url</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use the computer's default proxy defined in the Group Policy Object.</td>
<td>Use Machine Default Proxy</td>
<td>/USEMACHINEDEFAULTPROXY</td>
</tr>
</tbody>
</table>
Table 5 Proxy configuration options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Admin Console Setting</th>
<th>CLI Switch for Automated Deployments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The default proxy is not necessarily the same as the proxy established in the client computer’s Internet Explorer settings.</td>
<td></td>
</tr>
<tr>
<td>Automatically detect an auto-script using Web Proxy Auto Detect (WPAD) settings configured in DHCP or DNS.</td>
<td><strong>Auto-detect Proxy Settings</strong></td>
<td>/AUTODETECTPROXY</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Your DHCP or DNS servers must be configured for auto-detection for this option to work correctly. If auto-detection is not configured, Mozy software reverts to a direct connection.</td>
<td></td>
</tr>
<tr>
<td>Use a proxy auto-configuration (PAC) script located at the URL you specify.</td>
<td><strong>Use a PAC script</strong></td>
<td>/pacurl Example: /pacurl://<a href="https://pacscriptURL">https://pacscriptURL</a></td>
</tr>
<tr>
<td>Retrieve and use the proxy settings defined in Internet Explorer. If a username and password are required, these will need to be provided.</td>
<td>There is no setting for this in the Admin Console.</td>
<td>/GRABUSERIEPROXYSETTIN</td>
</tr>
</tbody>
</table>

Proxy Authentication Command Line Switches

If you are automatically deploying Mozy software, you may use these CLI switches to specify authentication credentials for the proxy server.

Table 6 Proxy authentication switches

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/USEMACHINEPROXYAUTH</td>
<td>Use the authentication credentials on the computer.</td>
</tr>
</tbody>
</table>

Proxy Settings within the Mozy Software

These are the proxy server settings end users see within the Mozy backup software on Windows, if you permit them to configure these settings on their own. These
settings are also available in Mozy Sync for Windows. These settings provide similar
capabilities as those available in the Admin Console or the command line interface.

**Table 7** Mozy proxy settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use a proxy to connect to servers</td>
<td>Indicates that this client is not required to connect through a proxy server or that there is no proxy server on the network. This is the default selection.</td>
</tr>
<tr>
<td>Use this proxy server</td>
<td>Identify a specific proxy server using the port number, the IP address, the host name, or the URL.</td>
</tr>
<tr>
<td>Use this computer's default proxy server</td>
<td>Use the proxy server configured for the machine based on the group policy settings for the user account.</td>
</tr>
<tr>
<td>Automatically detect proxy settings</td>
<td>Find any proxy servers configured for the computer, in this order. 1. DNS or WINS pointer to a PAC script 2. URLs pointing to a PAC script 3. Check for a default proxy in the group policy 4. If no proxy configuration is found, connect to the Internet directly</td>
</tr>
<tr>
<td>Use automatic configuration script</td>
<td>Specify the URL for a PAC script which contains the proxy server configuration.</td>
</tr>
<tr>
<td>Import Windows Proxy Settings</td>
<td>If a proxy server is defined for Internet Explorer, import those settings automatically. If a username and password are required, these will need to be entered manually.</td>
</tr>
</tbody>
</table>

**Configure Proxy Settings for Mozy Backup Software**

In the Admin Console, you can specify proxy server settings for in client configuration,
centralizing management and ensuring all clients are up-to-date and accurate. This feature is available in MozyEnterprise and for qualified resellers.

**CAUTION**

If you automate the deployment of Mozy software, you must ensure the proxy settings defined in the automated deployment and those in the Admin Console do not conflict. Inconsistencies between the locked client settings and those in the Admin Console can prevent the Mozy software from establishing a connection to the Internet and the Mozy service.

**Procedure**

1. Log in to the Admin Console.
   - For additional information, see [Logging in to the Admin Console](#) on page 18.
2. In the left menu, click **Client Configuration**.
3. Create a configuration, copy an existing configuration and modify it, or modify any configuration.
   - To create a configuration, type its name in the **Name** box under **Create a new client configuration**, select the key type if necessary, and then click **Next**.
To change a configuration, click its name under Existing Client Configs.

To copy a configuration, click Copy under Existing Client Configs.

a. Type the name of the new configuration, and then click Submit.

b. Click the name of the configuration you just created.

4. On the Preferences tab, update the Proxy Settings option, selecting Cascade and Lock if appropriate.

5. Click Save Changes.

Proxy Server Advanced Settings

If you manage traffic directly through your firewall or through advanced configuration of your proxy server, you may need to update your configuration to include the following:

Table 8 Advanced proxy settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Required Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports used by Mozy backup software</td>
<td>• Port 80</td>
</tr>
<tr>
<td></td>
<td>• Port 443</td>
</tr>
<tr>
<td>IP Ranges required:</td>
<td>• 74.112.144.0/21</td>
</tr>
<tr>
<td>(if you only allow connections to specific IP</td>
<td>• 74.112.150.0/23</td>
</tr>
<tr>
<td>addresses on ports 80 and 443)</td>
<td>• 173.243.48.0/20</td>
</tr>
<tr>
<td>URLs used by Mozy backup software</td>
<td>• berkeleydata.com</td>
</tr>
<tr>
<td>(if you use URL filtering)</td>
<td>• mozyoem.com</td>
</tr>
<tr>
<td></td>
<td>• mozy.com</td>
</tr>
<tr>
<td></td>
<td>• mozypro.com</td>
</tr>
<tr>
<td></td>
<td>• mozyenterprise.com</td>
</tr>
</tbody>
</table>

Setting Preferences

Procedure

1. Log in to the Admin Console.
   
   For additional information, see Logging in to the Admin Console on page 18.

2. In the left menu, click Client Configuration under Configuration.

3. Select the appropriate settings from the Settings list.
   
   For information about any of the preference settings, click more next to the setting. Additional text displays underneath the setting with a short explanation of what the setting does. To hide the text, click less.

4. (Optional) To override the setting for sub-partners, administrators and users below you, select Cascade.
For the settings to be cascaded, the client configuration must include the default user group.

5. (Optional) To lock a setting, select Lock.
6. Use the slide to increase or decrease the computer speed or backup speed.

**Scheduling Client Backups**

The client configuration settings allow you to define when backups will occur on the client machines.

There are two configuration options.

- Automatic backups automatically backup your data whenever your machine is not in use. See Setting Automatic Backups on page 36 for additional information.
- Scheduled backups backup your data at a specified time. See Setting a Scheduled Backup on page 36 for additional information.

**Setting Automatic Backups**

In the Scheduling tab, you can set the parameters or timing for the backups on all the machines within a designated configuration.

To set an automatic backup schedule (perform backups when the computer is not in use) for each client using this configuration:

**Procedure**

1. Click the Scheduling tab.
2. Select Automatic.
3. Enter the value for Don't back up if the CPU is over this % busy.
   a. Select if you want to Lock this feature so that users cannot change this setting.
4. Enter the Don't back up unless the computer has been idle for at least this many minutes value.
   a. Select if you want to Lock this feature so that users cannot change this setting.
5. Enter the Don't back up more than this many times per day value.
   a. Select if you want to Lock this feature so that users cannot change this setting.
6. Select Force users to use these scheduling options to force the users to use these scheduling options.
7. Select Don't allow users to suspend backups to prevent users from suspending backups.

**Setting a Scheduled Backup**

You can schedule backups to begin at a specified times.

**Procedure**

1. Click the Scheduling tab.
2. Select Scheduled.
3. Select Daily or Weekly.
   If you select Weekly, the Enter (day of the week) parameter displays. Specify
   the day when you want the backup to occur every week.
4. Enter the time of the backup.
5. Enter the frequency of the backups.
   The frequency for the Weekly parameter is set at 1 Week by default. The
   maximum frequency is either 7 days or 7 weeks, depending upon the parameter
   you use. If you select anything longer than 30 days, only the last version is
   retained.
6. Select Force users to use these scheduling options to force the users to use
   these scheduling options.
7. Select Don't allow users to suspend backups to prevent users from
   suspending backups.
   a. Select Cascade if you want this setting applied to all subordinate members.

Bandwidth Throttling
As part of the process of configuring client settings, the Bandwidth Throttling tab
allows you to set how much of your users’ Internet connection is used during a backup
and the days in which throttling will apply. Bandwidth ranges allow for faster backups
during slow bandwidth times.
For information about customizing the client configuration, see Create or Change a
Client Configuration on page 31.

Procedure
1. Click the Bandwidth Throttling tab.
2. Select Enable bandwidth throttle.
3. Enter the number of kilobits per second permitted for backups in the field
   provided.
   The higher the number of kilobits the faster the backup.
4. Select the time frame for the bandwidth throttling.
5. Select the days you want to throttle bandwidth.
   Bandwidth is not throttled on non-selected days.
6. Select Force users to use these bandwidth options to force users to use the
   specified bandwidth throttling options.
7. To hide the use of bandwidth throttling from users, select Enforce hidden
   bandwidth limit.
   a. Enter the number of Kbps allowed for backups. This setting overrides the
      setting above.

Backup Sets
In the Admin Console, you can select or define rules to back up groups of files, called
backup sets. Backup sets are defined separately for the Windows, Mac, and Linux
clients. Backup sets or rules are used to automatically select files on client machines
or to automatically exclude files from backing up.
Changes to a backup set or rule defined for the backup clients are not received by the
clients unless Lock is selected. If a backup set or rule is not locked, the backup client
will not obtain it, and users may be able to modify the backup set or rule themselves.
If a backup client needs to reacquire the backup set rules you have defined in the Admin Console, the client can be uninstalled and then reinstalled. In the case of the Windows client, simply running the Setup Wizard again can also discard the set of backup rules in use and reacquire the rules defined in the Admin Console.

**Procedure**

1. Select each backup set the client should back up.
2. (Optional) To lock any setting, select **Lock** next to the setting.
   
   Locking a backup set ensures that users cannot modify the setting in the client, and that the client can obtain the backup set definition.
3. (Optional) To override the setting for subpartners, administrators, and users below you, select **Cascade** next to the setting.

**Selecting Backup Sets**

**Procedure**

1. Select the **Settings** check box next to the backup set to back up.
2. (Optional) Select the **Lock** check box next to the item.
   
   By locking the backup set, the user cannot edit or turn on or off the backup set.
3. Select one of the following options:
   
   • Click another tab to make further changes.
   
   • Click **Save Changes** to save your changes.

**Viewing and Editing a Backup Set**

**Procedure**

1. Click **View/Edit** next to the backup set you want to view or edit.
2. Click **Done**.

**Creating a Windows Backup Set**

**Procedure**

1. Log in to the Admin Console. For additional information, see [Logging in to the Admin Console](#) on page 18.
2. Click **Client Configuration** under Configuration.
3. Click an existing client config or create a new client config by entering a name, then click **Next**.
4. Click the **Windows Backup Sets** tab.
   
   The Windows Backup Sets tab displays a list of all current backup sets for Windows clients.
5. Click **Create Backup Set**.
6. Enter the name of the new backup set in the **Name** field.
7. (Optional) If you want to exclude the files in the new backup set, select **Files matching this set will be EXCLUDED from the final backup set**.
8. Under **Where to Search**, enter the desired matching criteria. You can use special key words such as `%My Documents%` to search standard file system locations.
   
   You can click one of the predefined special file system keywords to automatically copy it to the location field. You can also enter a drive letter and folder on a local drive or drive share, for example, C:\BACKUP.
9. To add additional search locations, click **Add Search Location**.
10. To delete a search location, click **Delete**.
11. (Optional) Click **Add Rule** to add rules to your backup set. See **Creating Rules** on page 39 for additional information on creating rules.
12. Click **Done**.

**Creating Rules**

There are many possible rule combinations for backup sets. However, they are all based on either including or excluding certain files or folders according to your specifications.

**Procedure**

1. Click the drop-down and select either:
   - **Include** to include data.
   - **Exclude** to exclude data.
2. Use the second drop-down to select a file attribute for the backup set.
3. Click **Done** to save the rule.

**Creating a Mac Backup Set**

You use backup sets to specify types of files to back up on client machines. You decide the folders to search in and what type of files you want to back up.

You can also create exclusionary backup sets that specify files or folders that should not be backed up. You should use exclusionary backup sets carefully because they can have significant negative consequences.

**Procedure**

1. Log in to the Admin Console. For additional information, see **Logging in to the Admin Console** on page 18.
2. Click **Client Configuration** under Configuration.
3. Click an existing client config or create a new client config by entering a name, then click **Next**.
4. Click the **Mac Backup Sets** tab. The Mac Backup Sets tab lists all current backup sets for Mac clients.
5. Click **Create Backup Set**.
6. Enter the name of the new backup set in the **Name** field.
7. (Optional) Select **Files matching this set will be EXCLUDED from the final backup set** checkbox to make an exclusionary backup set.
8. Specify a path where to search for files in the **Where to Search** field. If left blank, this backup set will apply to all folders. For example, `/Users/UserA`. When you select a folder, all its subfolders are included as well.
9. In the **Spotlight Query** field, specify a file type to include (or exclude if you are creating a exclusionary backup set), for example, `.mp3`. You can also use Spotlight Query syntax to search for a file with certain attributes. For more information see: **Using Spotlight Query Syntax** on page 40.
10. Click **Done** to save your new backup set.

The newly-created backup set appears in the list of available backup sets on the Mac Backup Sets window.

**Using Spotlight Query Syntax**

Mozy does not access the Apple Spotlight at the root-level. However, a limited number of Spotlight queries are supported. You can use Spotlight Query syntax to search for a file with certain attributes. For more information, see **Supported Spotlight File Metadata Attributes** on page 40 and the File Metadata Query Expression Syntax article in Apple's Mac Developer Library.

**Supported Spotlight File Metadata Attributes**

The following is a list of supported file metadata attributes searchable in Mozy.

- kMDItemFSName
- kMDItemDisplayName
- kMDItemFileName
- kMDItemContentType
- kMDItemContentCreationDate
- kMDItemContentModificationDate
- kMDItemFSSize

The syntax is defined in the File Metadata Query Expression Syntax article in Apple's Mac Developer Library.

The only change from the official syntax is that Mozy does NOT support the "wcd" string modifiers nor does it support the "InRange()" function.

**Creating a Linux Backup Set**

You use backup sets to select files for backup or exclusion. An inclusion backup set lets you specify files to back up on client machines. You specify the directories to back up.

An exclusionary backup set lets you specify files or directories that should not be backed up. Any files listed in an exclusionary backup set are excluded from all backups, even if they are selected for backup in an inclusion backup set.

When specifying a search location path in a backup set, you can use symbolic links, but a symbolic link cannot be the last directory in a path. When specifying an exclusion search location path in a backup set, you can use wildcards (*) or symbolic links, but you cannot use them at the same time. In this situation, too, a symbolic link cannot be the last directory in a path.

There are no default backup sets for Linux, so you must create all your own custom backup sets.

**Procedure**

1. Log in to the Admin Console.
   
   For additional information, see **Logging in to the Admin Console** on page 18.

2. Click **Client Configuration** under Configuration.

3. Click an existing client config or create a new client config by entering a name, then click **Next**.

4. Click the **Linux Backup Sets** tab.

5. Click **Create Backup Set**.
Figure 3 Linux Backup Set

6. Enter the name of the new backup set in the **Name** field.

7. (Optional) Select **Files matching this set will be EXCLUDED from the final backup set** checkbox to create an exclusionary backup set.

8. Specify a search path for files you want to back up.
   a. In the field below **Where to Search**, enter a search path. For example, `/home`. When you specify a directory, all its subdirectories are also included.
   b. From the drop down menu to the left of the field, select either **Include** to include this path in the backup set or **Exclude** to exclude it.
   c. (Optional) Click **Add Search Location** to add additional paths for this backup set.

---

**Note**

Unlike the other backup clients, if you leave this search path field blank, the Linux client ignores the backup set.

9. (Optional) Create rules that specify the file names or file types you want to include or exclude.

Create rules that specify the file names or file types you want to include or exclude. Some shortcuts are supported for rule creation.

- You can wildcard the file name or file type you specify, for example: "\*file \*" or "log\*".
- When you specify file type, it’s not necessary to prepend a period: for example, you can use "log" instead of ".log".
- If you want to list more than one file name or type in a rule, use whitespace to separate each item in the list. If an individual item in the list uses a space in its name (for example, “file 3”) use double quotes (") to enclose that item.
For example, if you want to back up all of your Microsoft Excel spreadsheet files for Acme Sales that used "2014" in the file name, you can create a rule.

a. In the **File name includes** field, enter *me* *2014*.

b. In the **File type includes** field, enter xls*.

c. Click **Done**.

10. Click **Done** to save your new backup set.

The newly-created backup set appears in the list of available backup sets on the Linux Backup Sets window.

**Deleting a Backup Set**

**Procedure**

1. To delete a backup set, click **Delete** next to the backup set.

**Mobile Rules**

Mobile rules allow you to control when the client can perform backups and restores based upon the type of network the computer is connected to and the speed of the network. When a mobile rule is created, it displays in a list of mobile rules that have been previously created.

Mobile rules can be locked. When a mobile rule is locked, it prevents users from being able to change the mobile rule. When the mobile rule is unlocked it allows the users to change the mobile rule. In addition, a mobile rule can be cascaded. When a mobile rule is cascaded, it means that the sub-partners of the parent partner will have the same rules that the parent partner has created.

**Figure 4 Mobile Rules**

<table>
<thead>
<tr>
<th>Preference</th>
<th>Scheduling</th>
<th>Bandwidth Throttling</th>
<th>Windows Backup Sets</th>
<th>Mac Backup Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Groups</td>
<td>Mobile Rules</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Setting Cascade**

- Make rules tab visible in client

- Create new Mobile Rule

**Locked Mobile Rules**

These mobile rules cannot be changed by the end users.

<table>
<thead>
<tr>
<th>Cascade</th>
<th>Name</th>
<th>Network</th>
<th>Backups Allowed</th>
<th>Restores Allowed</th>
<th>Recorder</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Roaming</td>
<td>Roaming, Slow, Fast</td>
<td>Not Allowed</td>
<td>Not Allowed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Slow Networks</td>
<td>Home, Slow</td>
<td>Manual</td>
<td>Allowed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fast Networks</td>
<td>Home, Fast</td>
<td>Manual &amp; Automatic</td>
<td>Allowed</td>
<td></td>
</tr>
</tbody>
</table>

The order above determines which rules are observed first in the clients.

**Unlocked Mobile Rules**

These mobile rules can be changed by the end users.

There are no unlocked mobile rules configured.

The order above determines which rules are observed first in the clients.

**Creating/Modifying a Mobile Rule**

**To create or modify a mobile rule:**

**Procedure**

1. To create a mobile rule, click **Create a New Mobile Rule**, or to modify a mobile rule, click the name of the mobile rule to modify.

2. Under **Name**, type the name of the mobile rule in the appropriate language text box.
3. Under **Locking**, select the locking mechanism:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lock</strong></td>
<td>Prevents end-users from changing this setting in the client.</td>
</tr>
<tr>
<td><strong>Cascade</strong></td>
<td>Forces the rule to apply to sub-partners, administrators, and end-users of the parent partner.</td>
</tr>
</tbody>
</table>

If you do not select any of the options, then the end-users can change the settings for this rule.

4. Under **Network Type**, select one or more of the following network types:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home Network</strong></td>
<td>Applies the rule when users are connected to their home network.</td>
</tr>
<tr>
<td><strong>Roaming Network</strong></td>
<td>Applies the rule when users are connected to a roaming network. Roaming networks typically incur additional charges compared to a home network.</td>
</tr>
</tbody>
</table>

5. Under **Network Speed**, select one or more of the following network speeds:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Slower Connection:</strong></td>
<td>Applies the rule for slower connection speeds, such as GPRS and Edge.</td>
</tr>
<tr>
<td><strong>Faster Connection:</strong></td>
<td>Applies the rule for faster connection speeds, such as G3 and HSDPA.</td>
</tr>
</tbody>
</table>

6. Under **Backup**, select the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow backups to run</strong></td>
<td>You can select the following options for allowing backups:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Manual</td>
</tr>
<tr>
<td></td>
<td>• Automatic</td>
</tr>
<tr>
<td></td>
<td>• Manual and Automatic</td>
</tr>
<tr>
<td><strong>Backup Size</strong></td>
<td>Select this option to prevent backups from occurring when the backup is larger than the specified size in Megabytes.</td>
</tr>
<tr>
<td><strong>Notification for Manual Backups</strong></td>
<td>Select this option to have the client display a warning message before a manual backup is started.</td>
</tr>
</tbody>
</table>

7. Under **Restore**, select the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow Restores</strong></td>
<td>Allows the users to perform a restore on a mobile network.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restore Size</td>
<td>Select this option to prevent restores from occurring when the restore is larger than the specified size in Megabytes.</td>
</tr>
<tr>
<td>Notify before starting a restore</td>
<td>Select this option to have the client display a warning message before a restore is started.</td>
</tr>
</tbody>
</table>

8. Choose a method to complete the rule modification/creation.

- Click **Done** to save the changes and return to the mobile network rules for the client configuration.
- Click **Save Changes** to save and close the client configuration.

**Example 1** Slower Network Rule

The following example would prevent end-users from performing backups and restores when they are roaming, connected to a slower network (GPRS and Edge), and they are backing up or restoring more than 10 megabytes.

**Figure 5 Mobile Network Rules**

Deleting a Mobile Rule

**Procedure**

1. Click **Client Configuration**.
2. Click the name of the client configuration that contains the mobile rule you want to delete.
3. Click the name of the mobile rule you want to delete.
4. Click **Delete Mobile Rule**, then click **OK** to confirm the deletion.

**Displaying the Mobile Rules Tab**

You can select to display the **Mobile Rules** tab in the client from the **Mobile Rules** tab. You can also select to have the setting cascade to sub-partners as well.

To set the **Mobile Rules** tab display options:

**Procedure**

1. Click the **Mobile Rules** tab.
2. Select **Setting** to have the Mobile Rules tab display in the client.
3. Select **Cascade** to have the rule cascade to sub-partners.
4. Once you have finished configuring the rest of your mobile rules, click **Save Changes**.

**Backup Software Updates**

Mozy uses update rules to update the backup software. The update behavior depends on computer user permissions, whether the automatic update feature is enabled, and the client computer operating system.

Backup software updates are managed through update rules. For MozyEnterprise, the Mozy administrator creates and manages the rules. For MozyPro and qualified resellers, Mozy creates default rules, but the Mozy administrator can override the rules. For more information about update rules, see **Editing Client Versions** on page 46. Organizations can use their own tools to distribute and install updates instead of using Mozy update rules if wanted.

Mozy includes an automatic update feature that allows updates to be installed automatically and silently after they are made available through update rules. This feature can be enabled or disabled through the client configuration settings. For more information, see **Create or Change a Client Configuration** on page 31. The automatic update feature can also be enabled or disabled through the backup software, unless the Mozy administrator has locked the feature. When the feature is disabled, updates can still be made available through update rules, but the installation of the update must be initiated from the client computer. The backup software for Linux does not support update rules or the automatic update feature. Updates are only installed manually.

---

**Note**

If an update rule has the **Required Update** option that is selected, no updates occur, backups in progress stop, and no new backups start on specified computers until the backup software is manually updated to the exact version specified by the rule. For more information, see **Editing Client Versions** on page 46.
Table 9  Backup software update behavior using update rules

<table>
<thead>
<tr>
<th>Platform</th>
<th>Behavior with automatic updates enabled</th>
<th>Behavior with automatic updates disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>For standard rights users, no updates occur and there is no indication of updates being available or an option through the backup software to install updates. For standard users on a computer that is configured for updates in a UAC environment or for a computer administrator, updates are automatically and silently downloaded and installed. For more information about configuring UAC updates, see Configure Backup Software Updates for Non-administrators on page 48.</td>
<td>For standard rights users, no updates occur and there is no indication of updates being available or an option through the backup software to install updates. For administrators, updates are automatically downloaded and an informational box in the computer notification area prompts the administrator to install the update. If the administrator clicks the box, the update is installed. If the box is not clicked, the administrator can right-click the Mozy backup software icon, in the notification area, then select Update Mozy when ready to install the update.</td>
</tr>
<tr>
<td>Mac</td>
<td>Updates are automatically downloaded and silently installed.</td>
<td>The user can click the Mozy backup software icon, in the menu bar, then select Open Mozy Preferences. Next, the user can click the Options tab, then click Check for Updates. If an update is available, a dialog box opens and the user can click Download and Install to install the update. Finally, the user must type the computer administrator password.</td>
</tr>
<tr>
<td>Linux</td>
<td>Update rules are not supported. Updates must be installed manually.</td>
<td>Update rules are not supported. Updates must be installed manually.</td>
</tr>
</tbody>
</table>

Editing Client Versions

Note
This feature is available in MozyEnterprise and for qualified resellers.

This feature allows you to select which backup software client versions are updated automatically. Additionally, you can select the rule to force automatic updates on user machines. By default, clients are set to update automatically without user intervention when forced automatic updates are selected.

There is currently no automatic notification when a new client is available. However, you can see the latest version in both Edit Client Version and Product Release Notes.
Customizing a Default Client Version

Procedure

1. Log in to the Admin Console.
   For additional information, see Logging in to the Admin Console on page 18.

2. Under Configuration in the left-side pane, click Edit Client Version.

3. In the Update To drop-down list, select the appropriate client version.
   This is the version that the backup software client is updated to.

4. In the Current Version drop-down list, select a qualifier.

<table>
<thead>
<tr>
<th>Qualifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any version</td>
<td>Any version of the client that isn't the selected update version</td>
</tr>
</tbody>
</table>
### Qualifier Description

<table>
<thead>
<tr>
<th>Qualifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;=</td>
<td>Any version of the client that is greater than or equal to the selected update version</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Any version of the client that is less than or equal to the selected update version</td>
</tr>
<tr>
<td>Between</td>
<td>Any version of the client that is between the selected versions of the client</td>
</tr>
</tbody>
</table>

5. In the **User Group** drop-down list, select the user group which is subject to this rule.

   You can choose either all user groups (the default) or a single user group.

6. For **Operating System**, select the range of operating systems that will receive the client update.

7. (Optional) Select **Required Update** to force users to update to the client specified in the rule.

8. Click **Submit**.

#### Configure Backup Software Updates for Non-administrators

In organizations where users have standard rights on Windows computers, you can eliminate the need to provide the computer administrator password when installing updates to the backup software.

**Before you begin**

- You must be running version 2.32.4 (or later) of the backup software.
- You must be using MozyEnterprise or be a qualified reseller.

Generally, users with limited rights, such as those in a UAC environment, cannot install backup software updates made available through Mozy update rules without providing the computer administrator password. You, the Mozy administrator, can configure the updates so that updates can be automatically and silently installed without entering the administrator password. This configuration requires that you enable the automatic update feature in the backup software, which can be done through the client configuration file. If you are using version 2.32.4 or 2.32.6 of the backup software, you must also add two registry keys to the client computers.

---

**Note**

If you want to configure backup software activation for users without administrator rights, see [Configuring Backup Software Activation for Non-administrators](#) on page 50.

**Procedure**

1. In the Admin Console, enable and lock the **Install new versions of Mozy silently when they are made available** preference in the client configuration file you use to configure the Windows computers.

   Locking the feature ensures that any manual changes that have occurred to this setting are reset and that this feature cannot be disabled by a user. For more information about client configuration files, see [Create or Change a Client Configuration](#) on page 31.

2. (Version 2.32.4 and 2.32.6 only) Add registry keys to the client computers.
Add a DWORD registry key that is named upgrades_without_uac_prompt with a value of 1 at HKLM\Software \MozyEnterprise\Options.

Add a DWORD registry key that is named autoupdate with a value of 1 at HKEY_CURRENT_USER/software/MozyEnterprise/options. If this key exists, ensure that it is set to 1.

A method for making the registry changes is to push the changes to computers using system management software. If you later decide you do not want to use this feature, set the registry key values to 0 or remove the keys.

Results
Whenever you deploy an update using an update rule (the Edit Client Version feature), the applicable Windows computers are automatically and silently updated. For more information about the Edit Client Version feature, see Editing Client Versions on page 46.

Deploying the Mozy Backup Software
You can deploy the Mozy backup software using a systems management solution (SMS) or by allowing your users to install the software manually.

Table 10 Deployment options for backup software

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Users typically download and install the backup software on their machines, interacting with the available installation options. To use command line switches during a manual installation, the installation program must be started from a command window.</td>
</tr>
<tr>
<td>Automatic</td>
<td>For automatic distribution and installation on users' machines, a systems management solution (SMS) is typically used. Most systems management solutions provide a mechanism to pass command line switches during installation.</td>
</tr>
</tbody>
</table>

Installing the Software Manually
If you choose manual deployment, the Admin Console sends each user an email with the link to download the backup software.

The users are required to download, install, and activate the client. A key might be required.

The Admin Console allows an administrator to type an email address for each user, and to specify the user’s initial storage quota. The system automatically sends an email to the user with the appropriate download link and their product key.

Automate Installation using an SMS
If you choose to deploy using any standard systems management solution (such as SMS, LanDesk, Unicenter, Altiris, and others), the client is delivered to the user’s machine by the package deployment mechanism of the systems management software.

In a typical deployment using this distribution method, the Mozy installer is wrapped in another install script, which passes any relevant command line switches during the installation process.
Configuring Backup Software Activation for Non-administrators

In organizations where users have standard rights on Windows computers, you can eliminate the need to provide the computer administrator password when activating the backup software through the user interface.

Generally, users with limited rights, such as those in a UAC environment, cannot activate the backup software through the user interface without providing the computer administrator password. You, the Mozy administrator, can install the backup software so that the administrator password is not required for activation. To use this feature, you must be running version 2.32.8 (or later) of the backup software.

This configuration requires the installation, but not the activation, of the backup software on the computer using the /nonadminactivation switch with the Mozy installation program (example, Mozysetup.exe /nonadminactivation).

When configuring, you install the backup software on the computer. This installation is usually done through scripts or using SMS software. You do not activate the software. The computer user then logs in to the computer, right-clicks the Mozy backup software icon in the notification area, and selects Continue Setup. If using a script, you can open a window by running C:\Program Files\MozyEnterprise\Mozyenterpriseconf.exe. The user is prompted to provide credentials. The credentials can be Mozy or organization credentials, depending on whether you have integrated your organization authentication system with Mozy.

Choosing an Activation Method

Once you have chosen an installation method, you must decide how you want to activate the Mozy software. The activation process verifies that the user account is valid and that user has the resources to run the Mozy software.

User activation requires users to click a link to activate their account, to create their own passwords, and to manually download and install the Mozy software.

With the automatic and assisted activation methods, your organization must use Microsoft Active Directory. Users are registered based upon their Active Directory domain, which makes it easy to integrate the installation process with a systems management distribution method. Assisted activation is very similar to automatic activation. The main difference is that after the client has been installed, the client displays the username to the user and prompts for a password. This allows users to know their username and password so that they can restore their own files through a Web browser. This also allows a user to have multiple machines associated with a single user account.

User Activation

User activation requires the user to enter a username and password during the activation process.

Procedure

1. From the Admin Console, the administrator creates a new user account with a username and default password.
2. The administrator selects the option to automatically send the user an account activation email.
3. The user clicks the account activation link in the email and creates their own account password which replaces the default password.
4. The user can then download and install the Mozy software using their username and their new password.

Automatic and Assisted Activation

Before you begin
To use either the automatic or assisted activation method, your organization must use Microsoft Active Directory.

Note
When either assisted or automatic activation is used for Mozy on any Mac operating systems, you must first create this user in your AD domain: mozy-mac-autoactivation. If this user does not exist, activation will fail for Mac operating systems.

Note
The Enforce Email Key Match setting is not compatible with automatic or assisted activation.

With the automatic and assisted activation methods, users are registered based upon their Active Directory domain. This makes it easy to integrate the installation process with a systems management distribution method.

Assisted activation is very similar to automatic activation. The main difference is that after the client has been installed, the client displays the username to the user and prompts for a password. This allows users to know their username and password so that they can restore their own files through a Web browser. This also allows a user to have multiple machines associated with a single user account.

Procedure

1. In the Admin Console, the administrator downloads the Mozy Activation Info Utility.
   a. Under Configurations, click Network Domains.
   b. Click Mozy Activation Info Utility.
   c. Save the utility for future use.

2. The administrator provides the Mozy Activation Info Utility to the IT department so they can use it to collect the Domain GUIDs and the Active Directory OU for each machine.

   The GUID and OU are used to determine which user group and partner (if appropriate) the new users are added to when they are created in the account. If an OU is not provided in the Network Domains area of the Admin Console, then that entry will match any OU under that Domain GUID. The administrator can override the active directory OU information with a custom value. If the administrator chooses to use a custom value for the OU, the value needs to be passed to the installation program. To do this, the value needs to be passed using systems management distribution software that can pass command line values to start the installation.

3. In the Admin Console, the administrator creates partners (if appropriate) and user groups, ensuring sufficient storage is available.

4. In the Admin Console, the administrator for each partner or user group creates a Network Domain entry that has the GUID and OU for each user group that has been created.
Users whose machines match the GUID and OU are automatically assigned to this partner or user group.

5. The IT department distributes the client using the preferred application delivery method, such as a systems management solution.

6. The client is installed using the silent installation command line switch. (Optional) The `/OU` command line switch can be used to override Active Directory OU information, which is determined automatically by the client.

<table>
<thead>
<tr>
<th>Automatic Activation</th>
<th>Assisted Activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. The client looks up the domain of the machine and the Active Directory OU of machine if the <code>/OU</code> switch was not used.</td>
<td></td>
</tr>
<tr>
<td>b. The client passes the machine name with the domain and the Active Directory machine OU or custom OU information to the Admin Console.</td>
<td></td>
</tr>
<tr>
<td>a. The client displays the user principal name from Active Directory, and prompts the user to enter a password. Once the user has added a password, the user clicks <strong>Activate</strong> to activate the client.</td>
<td></td>
</tr>
<tr>
<td>b. The client passes the username, password, Active Directory Domain GUID, and the Active Directory OU or custom OU to the Admin Console.</td>
<td></td>
</tr>
</tbody>
</table>

7. Based upon the machine name, domain, and machine OU, the Admin Console determines which user group and partner the account should be created in.

<table>
<thead>
<tr>
<th>Automatic Activation</th>
<th>Assisted Activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user is created with these attributes.</td>
<td></td>
</tr>
<tr>
<td>• Username = machine name @ Active Directory domain name</td>
<td></td>
</tr>
<tr>
<td>• Password = randomly generated and is not provided to user</td>
<td></td>
</tr>
<tr>
<td>The user is created with these attributes.</td>
<td></td>
</tr>
<tr>
<td>• Username = UserPrincipalName</td>
<td></td>
</tr>
<tr>
<td>• Password = specified by user</td>
<td></td>
</tr>
</tbody>
</table>

**Product Key Activation**

**Before you begin**

This activation method is valid only for versions of the Mozy backup software older than version 2.22 for Windows or 2.11 for Mac.

Product key activation requires a username (usually the user’s email address), a password, and a product key.

**Procedure**

1. In the Admin Console, the administrator allocates product keys and storage to the user groups in their account.
2. The administrator assigns a storage quota to product keys in the Admin Console.
3. The administrator distributes the product keys and the download link to users through email.
   (You can either use the Admin Console to send the emails, or you can send them manually through your email system.)
4. The users download the client using the link provided in the email, then install the client on their machines.

5. During the activation process, the users enter the product key that was sent to them in the email message.

6. The client software uses the product keys to create the user accounts in the Admin Console.

7. Once the product key is successfully registered to each user, the user’s machine is also associated with the user account.
Active Directory Federation Service (ADFS) must be set up correctly to integrate your organization Active Directory system with Mozy. Before setting up ADFS for Mozy, you must complete the prerequisites.

- Install and configure ADFS.
- Decide whether you want to use a self-signed certificate or a certificate authority (CA) Issued certificate. A CA Issued certificate is required for mobile access.
  - To use a self-signed certificate, open IIS and create the certificate.
  - To use a CA Issued certificate, ensure that the certificate contains EKU=Server Authentication. Use of the Web Server Certificate is acceptable.

After completing the prerequisites, add Mozy as a relying party trust. For more information, see Adding Mozy as a Relying Party Trust on page 56.

- Adding Mozy as a Relying Party Trust ................................................................. 56
- Editing the Claim Rules for Mozy ................................................................. 56
- Exporting Token-Signing Certificate ........................................................... 58
- Deploy RelayState Settings ........................................................................ 59
Adding Mozy as a Relying Party Trust

Add Mozy as a relying party trust as part of setting up Active Directory Federation Service (ADFS) for Mozy.

**Note**

Before adding Mozy as a relying party trust, you must meet the prerequisites. For more information, see Setting Up Active Directory Federation Service for Mozy on page 55.

You can add Mozy as a relying party trust in a Windows 2008, Windows 2012, or Windows 2016 environment.


When adding the trust, you must supply some Mozy specific information.

<table>
<thead>
<tr>
<th>User Interface Page</th>
<th>Mozy Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Data Source</strong></td>
<td>Select the Import data about the relying party published online or on a local network option. In Federation metadata address (hostname or URL), type auth2.mozy.com/ <code>&lt;subdomain&gt;/saml/metadata/sp.xml</code>, where <code>&lt;subdomain&gt;</code> is the subdomain for your instance of Mozy.</td>
</tr>
<tr>
<td><strong>Issuance Authorization Rules (Windows 2008) or Choose Access Control Policy (Windows 2012 or Windows 2016)</strong></td>
<td>Select users that should have access to Mozy. Mozy recommends selecting Permit All users access (Windows 2008) or Permit everyone (Windows 2012 or 2016). If you select Deny all users access, you must create additional rules to allow your Mozy users to use the service.</td>
</tr>
</tbody>
</table>

The next task is to edit the claim rules for Mozy. For more information, see Editing the Claim Rules for Mozy on page 56.

Editing the Claim Rules for Mozy

Edit the claim rules as part of setting up Active Directory Federation Service (ADFS) for Mozy.

**Note**

Before editing the chain rule, add Mozy as a relying party trust. For more information, see Adding Mozy as a Relying Party Trust on page 56.
Claim rules determine how LDAP values are translated into SAML claims. The claim rules can vary, depending on the LDAP attributes mapped in Mozy.


- (Windows 2008) [Edit the Claim Rules for Mozy on Windows Server 2008](#) on page 57

When editing chain rules, you must supply some Mozy specific information.

Table 12 Mozy specific information for claim rules

<table>
<thead>
<tr>
<th>User Interface Page</th>
<th>Mozy Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Claim Rule Template</strong> (Windows 2008)</td>
<td>Set Claim rule template to Send LDAP attributes as claims.</td>
</tr>
<tr>
<td><strong>Select Rule Template</strong> (Windows 2012 or Windows 2016)</td>
<td></td>
</tr>
<tr>
<td><strong>Chain Rule Name</strong></td>
<td>In the Attribute store drop-down list, select Active Directory. Update the LDAP attribute mapping. If you have defined a Fixed Attribute in Mozy attribute mapping, add it to the claim rules.</td>
</tr>
<tr>
<td></td>
<td>- E-Mail-Addresses (LDAP attribute) - Name ID (Outgoing Claim Type )</td>
</tr>
<tr>
<td></td>
<td>- Given-Name (LDAP attribute) - Given Name (Outgoing Claim Type )</td>
</tr>
</tbody>
</table>

The next task is to export the token signing certificate. For more information, see [Exporting Token-Signing Certificate](#) on page 58.

**Edit the Claim Rules for Mozy on Windows Server 2008**

Claim rules determine how LDAP values are translated into SAML claims. The claim rules can vary depending on the LDAP attributes mapped in Mozy. If you used the default values, can use these steps to guide in creating the claim rules on Windows Server 2008.

**Procedure**

1. In the Edit Claim Rules for Mozy window, click Add Rule.
2. Verify the Claim rule template drop-down list is set to Send LDAP attributes as claims, then click Next.
3. Type a name for the claim rule. You might want to use the same name you typed for the relying party trust. For example, Mozy SSO.
4. In the Attribute store drop-down list, select Active Directory.
5. Update the LDAP attribute mapping. If you defined a Fixed Attribute in Mozy attribute mapping, add it to the claim rules.
Table 13 LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP Attribute</th>
<th>Outgoing Claim Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail-Addresses</td>
<td>Name ID</td>
</tr>
<tr>
<td>Given-Name</td>
<td>Given Name</td>
</tr>
</tbody>
</table>

Figure 7 Add Claim Rules

6. Click Finish, then click Apply.

7. Click OK.

After you finish

The next step is to export the token-signing certificate. For more information, see Exporting Token-Signing Certificate on page 58.

Exporting Token-Signing Certificate

Export the token-sharing certificate as part of setting up Active Directory Federation Service (ADFS) for Mozy.

Note

Before exporting the certificate, edit the claim rules for Mozy. For more information, see Editing the Claim Rules for Mozy on page 56.


When exporting the certificate, you must supply some Mozy specific information.
Table 14 Mozy specific information for exporting a token-sharing certificate

<table>
<thead>
<tr>
<th>User Interface Page</th>
<th>Mozy Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export File Format</td>
<td>Select the Base 64-encoded X.509 (.CER) option. In Windows 2012 or 2016, ensure No, do not export the private key is not selected.</td>
</tr>
</tbody>
</table>

After exporting, add the certificate to the SAML Authentication tab in the Mozy configuration.

The next task is to deploy RelayState settings. For more information, see Deploy RelayState Settings on page 59.

Deploy RelayState Settings

Deploy RelayState settings as part of setting up Active Directory Federation Service (ADFS) for Mozy.

Before you begin

- Export the token-signing certificate. For more information, see Exporting Token-Signing Certificate on page 58.
- If you are using Windows 2008 R2, ensure that you have applied Rollup 2 for AD FS 2.0, which is the minimum version to support RelayState on AD FS. For more information, see Supporting Identity Provider Initiated RelayState at http://technet.microsoft.com/en-us/library/jj127245(v=ws.10).aspx. After applying the updates, restart the server and test the authentication workflow.

RelayState settings identify the specific resource users access after they sign in and are directed to the relying party federation server.

Procedure

1. On the AD FS server, browse to and open the IIS configuration file in notepad.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 R2</td>
<td>%systemroot%\inetpub\adfs\ls\web.config</td>
</tr>
<tr>
<td>Windows 2012 and Windows 2016</td>
<td>%systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config</td>
</tr>
</tbody>
</table>

2. In the `<microsoft.identityServer.web>` section, add `<useRelayStateForIdpInitiatedSignOn enabled="true" />` and save changes.

For Mozy to work on Mac OS X and the web application, the form based authentication method (FBA) must be above everything else. Within the `localAuthenticationTypes` section. The `Forms` code must be first in the list.

```xml
<microsoft.identityServer.web>
    <useRelayStateForIdpInitiatedSignOn enabled="true"/>
    <localAuthenticationTypes>
```

Deploy RelayState Settings
3. (Optional) You might need to restart the service for the changes to take effect.

4. Create an encoded RelayState URL to use as the Authentication URL in Mozy. The encoded URL should contain the URL to the IdP, the Mozy Identifier, and access URL to the Mozy service. The following screenshot shows an example of an encoded URL with the required information.

Microsoft has created a tool to assist you in creating an encoded URL for this purpose. Using this tool ensures that the URL is created correctly. For more information, see https://adfsrelaystate.codeplex.com/.

**Figure 8 RelayState URL Generator**

![RelayState URL Generator](image)

**Results**

You have completed the final step in setting up ADFS for Mozy.
APPENDIX B

LDAP Error Handling

The list of potential errors below provides you with information on resolving some common errors that may occur when configuring or using the directory services authentication feature with Mozy.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory services authentication is not allowed for partner <code>&lt;partner_id&gt;</code></td>
<td>Contact your account manager to ensure your account is enabled for Directory Services authentication.</td>
</tr>
<tr>
<td>Blocked deprovisions.</td>
<td>If a deprovisioning rule will affect more than 5% of your users, Mozy will not execute the rule if Sync Safeguards is enabled. If you have purposely defined a rule that affects more than 5% of your users, you can temporarily disable the Sync Safeguard to allow the deprovisioning rule to take effect. It is recommended that you then re-enable Sync Safeguards.</td>
</tr>
<tr>
<td>There was an error while saving.</td>
<td>A generic message that indicates a loss of connection or some other generic problem. Try saving again.</td>
</tr>
<tr>
<td>API key has not been set up.</td>
<td>Indicates that you have not configured an API key for the LDAP Connector. Add <code>-api_key key value</code> to your configuration. You can remove the <code>key:value</code> pair once configured.</td>
</tr>
<tr>
<td>API key not found.</td>
<td>Indicates the API key entered in the configuration was entered incorrectly. Validate your API key and then enter it in the configuration again.</td>
</tr>
<tr>
<td>Bad parameter.</td>
<td>Verify that all parameters include the leading <code>-</code>. For example, <code>-ldap_username</code>.</td>
</tr>
<tr>
<td>Unknown parameter.</td>
<td>Validate all parameters entered to ensure you have entered them correctly.</td>
</tr>
<tr>
<td>Proxy connection failed.</td>
<td>Validate the username, password, and connection settings for your proxy server. If the settings are valid, make sure you can connect to the proxy server without using the connector.</td>
</tr>
</tbody>
</table>
## Deployment Worksheet

**Table 15 Deployment worksheet**

<table>
<thead>
<tr>
<th>Item #</th>
<th>Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mozy Admin Console Settings</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>URL</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Admin User</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Admin Password</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>LDAP Connection Settings</td>
<td>Your user directory service.</td>
</tr>
<tr>
<td>5</td>
<td>LDAP Server Host</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SSL Certificate</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Base DN</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Bind Username</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Bind Password</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Mozy Provisioning Settings</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>User Groups (to define in Mozy)</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Provisioning Rules (containers to sync)</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Provision Users: suspend after # days (implicit rules for deprovisioning)</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Provision Users: delete after # days (implicit rules for deprovisioning)</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Deprovisioning rules and actions (explicit rules for deprovisioning users)</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Sync Daily At</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attribute Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Username Field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name Field</td>
<td></td>
</tr>
</tbody>
</table>
## Table 15 Deployment worksheet (continued)

<table>
<thead>
<tr>
<th>Item #</th>
<th>Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>Fixed Attribute (optional - supports username (email) changes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAML Authentication Settings</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Authentication URL</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>SAML Endpoint</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>SAML Certificate</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Encrypt SAML</td>
<td></td>
</tr>
<tr>
<td></td>
<td>API Key and Partner ID, make sure to add ID in connector</td>
<td>For Push</td>
</tr>
</tbody>
</table>