

Administration Guide

Data Synchronizer Mobility Pack 1.2.5

January 28, 2013

Legal Notices

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

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

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

Copyright © 2010-2013 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	5
1 Synchronizer Services	7
1.1 Managing the Synchronizer Services Collectively	7
1.2 Managing the Synchronizer Services Individually	7
1.2.1 Managing the Sync Engine	8
1.2.2 Managing the Config Engine	8
1.2.3 Managing the Web Admin Service	8
1.2.4 Managing the Connector Manager	8
2 Synchronizer Web Admin	9
2.1 Accessing Synchronizer Web Admin as an Administrator	9
2.2 Accessing Synchronizer Web Admin as a User	10
2.3 Configuring Synchronizer Web Admin	11
2.3.1 Searching Multiple LDAP Contexts for Users and Groups	12
2.3.2 Setting Up Multiple Synchronizer Administrator Users	13
2.3.3 Adjusting the Synchronizer Web Admin Polling Rate for Groups	14
2.3.4 Adjusting the Synchronizer Web Admin Timeout	15
2.3.5 Changing the Synchronizer Web Admin Port Number	15
2.3.6 Enabling and Disabling SSL for the Synchronizer LDAP Connection	16
2.3.7 Changing the LDAP Server for Authentication	17
2.3.8 Using Synchronizer Web Admin with a Single Sign-On Solution	18
2.3.9 Accessing Synchronizer Web Admin When the LDAP Server Is Inaccessible	18
2.3.10 Configuring Synchronizer Web Admin for a Specific Language	18
3 Synchronizer System Management	21
3.1 Monitoring Your Synchronizer System	21
3.1.1 Enabling the Global Status Monitor	21
3.1.2 Using the Global Status Monitor	22
3.1.3 Disabling the Global Status Monitor	23
3.2 Monitoring the Sync Engine	23
3.3 Monitoring Disk Space Usage	25
3.4 Working with Log Files	25
3.4.1 Log File Overview	26
3.4.2 Log File Rotation	26
3.4.3 Logging Levels	27
3.4.4 Sync Engine Log File	27
3.4.5 Config Engine Log File	28
3.4.6 Web Admin Log File	28
3.4.7 Connector Manager Log File	29
3.4.8 Connector Log Files	29
3.4.9 Synchronizer Log File Management Tools	30
3.4.10 NTS supportconfig Tool	33
3.5 Diagnosing Synchronization Problems	34
3.6 Maintaining the Synchronizer Database	35
3.6.1 Performing General PostgreSQL Database Maintenance	35
3.6.2 Configuring Database Maintenance	36
3.7 Changing the Synchronizer Database Password	36

3.8	Backing Up Your Synchronizer System	37
3.8.1	Understanding What to Back Up	37
3.8.2	Backing Up a Synchronizer System after Stopping It	38
3.8.3	Backing Up a Synchronizer System While It Is Running	38
3.8.4	Restoring Your Synchronizer System	39
3.9	Reconfiguring Your Synchronizer System to Reflect Network Changes	40
3.9.1	Changing the IP Address of the Synchronizer Server	40
3.9.2	Updating the LDAP Password	42
3.10	Managing Anonymous Feedback.	42
3.10.1	Enabling/Disabling Anonymous Feedback	43
3.10.2	Viewing the Collected Feedback	43
3.11	Managing Connectors	43
3.11.1	Connector Startup	44
3.11.2	Connector Logging Level.	44
4	User Management	45
4.1	Managing Users	45
4.1.1	Adding a User in Synchronizer Web Admin.	45
4.1.2	Adding a User through an LDAP Group	46
4.1.3	Customizing a User's Synchronization Settings	47
4.1.4	Setting a User's Application Name	48
4.1.5	Deleting a User	49
4.2	Managing LDAP Groups	50
4.2.1	Adding an LDAP Group	51
4.2.2	Updating an LDAP Group	51
4.2.3	Deleting an LDAP Group	52
4.3	Managing Resources	52
4.4	Auditing User Synchronization Activity.	52
5	Synchronizer System Security	55
5.1	Security Administration	55
5.1.1	Securing Communication with the LDAP Server	55
5.1.2	Securing Communication between the GroupWise Connector and the GroupWise POA	56
5.1.3	Securing Communication between the Mobility Connector and Mobile Devices	56
5.1.4	Selecting a Specific Version of SSL	60
5.2	Security Policies.	61
5.2.1	Securing Your Synchronizer Data	61
5.2.2	Securing Your Synchronizer System	62
A	Synchronizer System Troubleshooting	65
B	Documentation Updates	67
B.1	January 28, 2013 (Mobility Pack 1.2.5)	67

About This Guide

The *Mobility Pack Administration Guide* helps you to manage your Synchronizer system after you have set it up.

- ◆ Chapter 1, “Synchronizer Services,” on page 7
- ◆ Chapter 2, “Synchronizer Web Admin,” on page 9
- ◆ Chapter 3, “Synchronizer System Management,” on page 21
- ◆ Chapter 4, “User Management,” on page 45
- ◆ Chapter 5, “Synchronizer System Security,” on page 55
- ◆ Appendix A, “Synchronizer System Troubleshooting,” on page 65
- ◆ Appendix B, “Documentation Updates,” on page 67

Audience

This guide is intended for network administrators who manage a Synchronizer system to support GroupWise users and their mobile devices.

Feedback

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

Additional Documentation

For additional Data Synchronizer Mobility Pack documentation, see the following documentation provided at the [Novell Data Synchronizer Documentation Web site \(http://www.novell.com/documentation/datasynchronizer1\)](http://www.novell.com/documentation/datasynchronizer1).

- ◆ Mobility Pack Readme
- ◆ *Mobility Pack Installation Guide*
- ◆ *Mobility Pack Administration Guide*

For Mobility Pack connector documentation, see the following documentation provided at the [Novell Data Synchronizer Connectors Documentation Web site \(http://www.novell.com/documentation/datasync_connectors1\)](http://www.novell.com/documentation/datasync_connectors1).

- ◆ Connector Readmes
- ◆ *Mobility Quick Start*
- ◆ *GroupWise Connector Configuration Guide*
- ◆ *Mobility Connector Configuration Guide*

In addition to the Data Synchronizer product documentation, the following resources provide additional information about the Mobility Pack:

- ♦ [Novell Support and Knowledgebase \(http://www.novell.com/support\)](http://www.novell.com/support)
- ♦ [Data Synchronizer Support Forum \(http://forums.novell.com/forumdisplay.php?f=939\)](http://forums.novell.com/forumdisplay.php?f=939)
- ♦ [Data Synchronization Cool Solutions \(http://www.novell.com/communities/cool solutions/datasynchronizer\)](http://www.novell.com/communities/cool solutions/datasynchronizer)
- ♦ [Data Synchronizer Mobility Connector Devices Wiki \(http://wiki.novell.com/index.php/Data_Synchronizer_Mobility_Connector_Devices\)](http://wiki.novell.com/index.php/Data_Synchronizer_Mobility_Connector_Devices)

1 Synchronizer Services

For an overview of the Synchronizer services, see “[Mobility Pack Product Overview](#)” in the *Mobility Pack Installation Guide*. The Synchronizer services are managed on the command line in a terminal window.

IMPORTANT: The Synchronizer services must always run as the Linux `root` user.

- ♦ [Section 1.1, “Managing the Synchronizer Services Collectively,” on page 7](#)
- ♦ [Section 1.2, “Managing the Synchronizer Services Individually,” on page 7](#)

1.1 Managing the Synchronizer Services Collectively

Use the following command as `root` to check the status of the Synchronizer services:

```
rcdatasync status
```

Use the following commands as `root` to manually start and stop all the Synchronizer services:

```
rcdatasync start
rcdatasync restart
rcdatasync stop
```

By default, when you restart the Synchronizer services, all connectors are automatically restarted as well. If you do not want the connectors to restart automatically along with the Synchronizer services, see [Section 3.11.1, “Connector Startup,” on page 44](#). If you choose to manually restart the connectors, always restart the GroupWise Connector first.

1.2 Managing the Synchronizer Services Individually

If you manage the Synchronizer services individually, they should be started in the following order:

- ♦ Config Engine
- ♦ Sync Engine
- ♦ Connector Manager

The Synchronizer services should be stopped in the following order:

- ♦ Connector Manager
- ♦ Sync Engine
- ♦ Config Engine

You can start and stop Web Admin at any time, as long as the other Synchronizer services are running.

Each Synchronizer service has its own set of commands:

- ◆ [Section 1.2.1, “Managing the Sync Engine,” on page 8](#)
- ◆ [Section 1.2.2, “Managing the Config Engine,” on page 8](#)
- ◆ [Section 1.2.3, “Managing the Web Admin Service,” on page 8](#)
- ◆ [Section 1.2.4, “Managing the Connector Manager,” on page 8](#)

1.2.1 Managing the Sync Engine

Use the following command as root to check the status of the Sync Engine:

```
rcdatasync-syncengine status
```

Use the following commands as root to manually start and stop the Sync Engine:

```
rcdatasync-syncengine start  
rcdatasync-syncengine restart  
rcdatasync-syncengine stop
```

1.2.2 Managing the Config Engine

Use the following command as root to check the status of the Config Engine:

```
rcdatasync-configengine status
```

Use the following commands as root to manually start and stop the Config Engine:

```
rcdatasync-configengine start  
rcdatasync-configengine restart  
rcdatasync-configengine stop
```

1.2.3 Managing the Web Admin Service

Use the following command as root to check the status of the Web Admin service:

```
rcdatasync-webadmin status
```

Use the following commands as root to manually start and stop the Web Admin service:

```
rcdatasync-webadmin start  
rcdatasync-webadmin restart  
rcdatasync-webadmin stop
```

1.2.4 Managing the Connector Manager

Use the following command as root to check the status of the Connector Manager:

```
rcdatasync-connectors status
```

Use the following commands as root to manually start and stop the Connector Manager:

```
rcdatasync-connectors start  
rcdatasync-connectors restart  
rcdatasync-connectors stop
```

2 Synchronizer Web Admin

All configuration of your Synchronizer system is done through Synchronizer Web Admin. For a list of supported Web browsers, see “[Web Browser Requirements for Synchronizer Web Admin](#)” in “[Mobility Pack Product Overview](#)” in the *Mobility Pack Installation Guide*.

When you log in as the Synchronizer administrator, you can configure the Sync Engine and connectors. When users log in using their network user names and password, they can control connector-specific aspects of data synchronization.

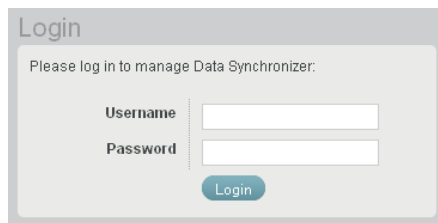
- ♦ [Section 2.1, “Accessing Synchronizer Web Admin as an Administrator,”](#) on page 9
- ♦ [Section 2.2, “Accessing Synchronizer Web Admin as a User,”](#) on page 10
- ♦ [Section 2.3, “Configuring Synchronizer Web Admin,”](#) on page 11

2.1 Accessing Synchronizer Web Admin as an Administrator

- 1 Access Synchronizer Web Admin at the following URL:

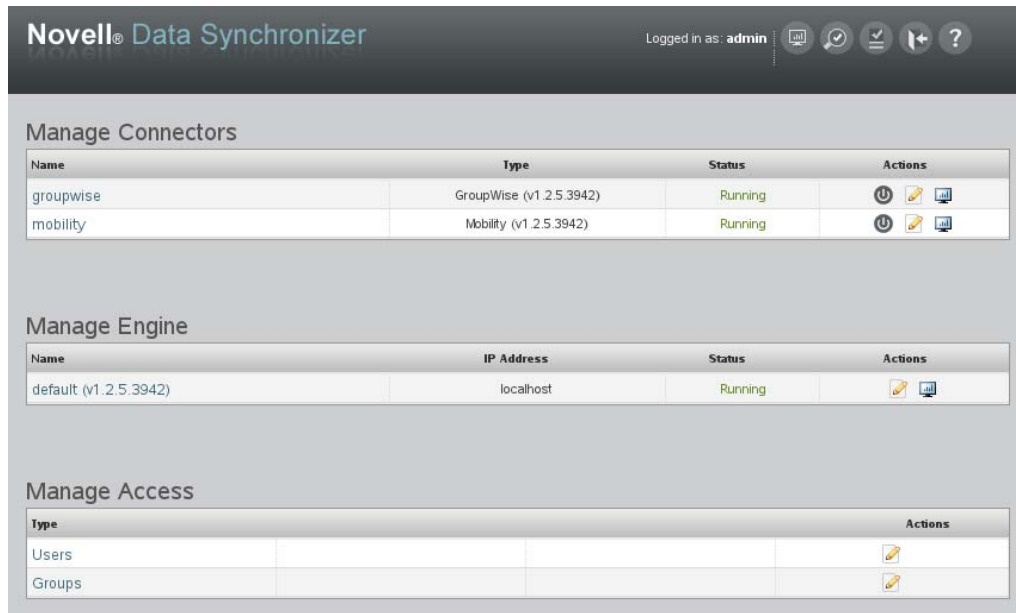
`https://data_synchronizer_server:8120/admin/user/user_name`

Replace `data_synchronizer_server` with the IP address or DNS hostname of the server where you installed the Mobility Pack.



The screenshot shows a web browser window with a login form. The form has a title "Login" and a subtitle "Please log in to manage Data Synchronizer:". Below the subtitle, there are two input fields: "Username" and "Password". A "Login" button is located below the "Password" field.

- Specify the Synchronizer administrator user name (such as admin) and password that were established during installation, then click *Login*.



Synchronizer system configuration and administration is performed using Synchronizer Web Admin.

- ◆ [Chapter 3, “Synchronizer System Management,”](#) on page 21
- ◆ [Chapter 4, “User Management,”](#) on page 45

- Click to log out of Synchronizer Web Admin.

If you want multiple users to be able to access Synchronizer Web Admin, see [Section 2.3.2, “Setting Up Multiple Synchronizer Administrator Users,”](#) on page 13.

2.2 Accessing Synchronizer Web Admin as a User

Users can use the Synchronizer Web Admin URL to access the Synchronizer User Options page by logging in with their network user names and passwords.



IMPORTANT: Even if you have configured your Synchronizer system to use GroupWise authentication for mobile device access, as described in “[Using GroupWise Authentication Instead of LDAP Authentication for Mobile Devices](#)” in “[Mobility Connector Configuration](#)” in the *Mobility Connector Configuration Guide*, users still need to use their network (LDAP) user names and passwords to access the Data Synchronizer User Options page.

GroupWise users who are represented in eDirectory as GroupWise external entities cannot access the User Options page, because GroupWise external entities cannot log in to eDirectory (LDAP).

The *Mobility Quick Start* (http://www.novell.com/documentation/datasync_connectors1/pdfdoc/mobilityconnect12_qs/mobilityconnect12_qs.pdf) explains how to use the Synchronizer Web Admin User Options page.

If you set yourself up as the Synchronizer administrator user, you can access your personal User Options page with the following URL:

```
https://data_synchronizer_server:8120/admin/user/user_name
```

Replace *data_synchronizer_server* with the IP address or DNS hostname of the server where you installed the Mobility Pack.

2.3 Configuring Synchronizer Web Admin


[Synchronizer Web Admin](#) is the management and administration tool for your Synchronizer system.

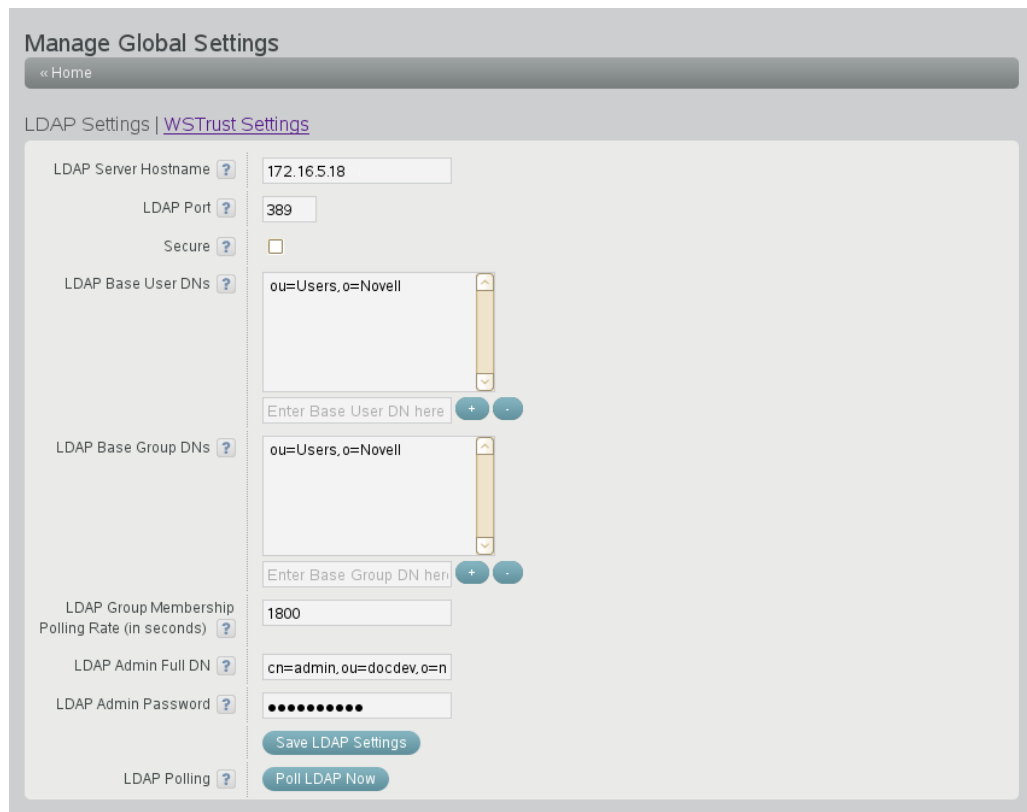
- ♦ [Section 2.3.1, “Searching Multiple LDAP Contexts for Users and Groups,”](#) on page 12
- ♦ [Section 2.3.2, “Setting Up Multiple Synchronizer Administrator Users,”](#) on page 13
- ♦ [Section 2.3.3, “Adjusting the Synchronizer Web Admin Polling Rate for Groups,”](#) on page 14
- ♦ [Section 2.3.4, “Adjusting the Synchronizer Web Admin Timeout,”](#) on page 15
- ♦ [Section 2.3.5, “Changing the Synchronizer Web Admin Port Number,”](#) on page 15
- ♦ [Section 2.3.6, “Enabling and Disabling SSL for the Synchronizer LDAP Connection,”](#) on page 16
- ♦ [Section 2.3.7, “Changing the LDAP Server for Authentication,”](#) on page 17
- ♦ [Section 2.3.8, “Using Synchronizer Web Admin with a Single Sign-On Solution,”](#) on page 18
- ♦ [Section 2.3.9, “Accessing Synchronizer Web Admin When the LDAP Server Is Inaccessible,”](#) on page 18
- ♦ [Section 2.3.10, “Configuring Synchronizer Web Admin for a Specific Language,”](#) on page 18

2.3.1 Searching Multiple LDAP Contexts for Users and Groups

During installation, you specify one LDAP container to search in for user information and another container to in search for group information. After installation, you can add more containers for Synchronizer Web Admin to search in for users and groups when you need to add users and groups to your Synchronizer system.



IMPORTANT: Subcontainers are also searched, so you do not need to add them separately.

- 1 In [Synchronizer Web Admin](#), click *Manage Global Settings* .



The screenshot shows the 'Manage Global Settings' page with a breadcrumb trail '« Home'. Below the title, there are two tabs: 'LDAP Settings' (selected) and 'WSTrust Settings'. The LDAP Settings section contains the following fields and controls:

- LDAP Server Hostname: 172.16.5.18
- LDAP Port: 389
- Secure:
- LDAP Base User DNs: A list containing 'ou=Users, o=Novell' with a scroll bar and a '+ -' button below it.
- LDAP Base Group DNs: A list containing 'ou=Users, o=Novell' with a scroll bar and a '+ -' button below it.
- LDAP Group Membership Polling Rate (in seconds): 1800
- LDAP Admin Full DN: cn=admin, ou=docdev, o=n
- LDAP Admin Password: A masked password field.
- Buttons: 'Save LDAP Settings' and 'Poll LDAP Now'.
- LDAP Polling: A link with a '?' icon.

- 2 To search in an additional container for users, specify the container context in the text entry field under *LDAP Base User DNs*, then click  to add the container to the list of containers to search.
- 3 To search in an additional container for groups, specify the container context in the text entry field under *LDAP Base Group DNs*, then click  to add the container to the list of containers to search.
- 4 Click *Save LDAP Settings*.
- 5 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

Users and groups from the new container contexts are immediately available for adding to connectors.

2.3.2 Setting Up Multiple Synchronizer Administrator Users

During installation, you establish the initial user who can access Synchronizer Web Admin. After installation, you can grant this right to additional users.

1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.

2 Change to the following directory:

```
/etc/datasync/configengine
```

3 Open the `configengine.xml` file in a text editor.

4 Locate the following section:

```
<admins>
  <dn>cn=user_name,ou=organizational_unit,o=organization</dn>
</admins>
```

This section identifies the original Synchronizer user that you established during installation.

5 Copy the line for the original Synchronizer user to a new line between the `<admins>` tags, then modify it as needed to identify an additional Synchronizer administrator user.

6 Save the `configengine.xml` file, then exit the text editor.


7 Restart the Synchronizer services to put the new setting into effect:

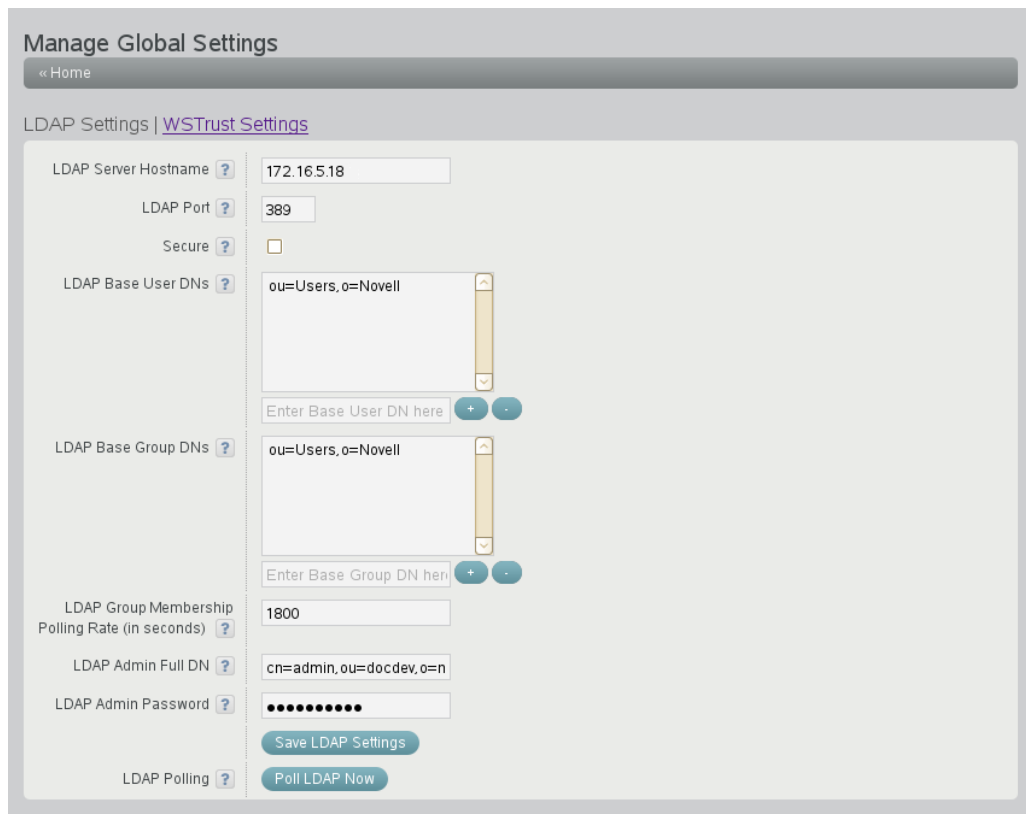
```
rcdatasync restart
```

2.3.3 Adjusting the Synchronizer Web Admin Polling Rate for Groups

When you add an LDAP group to your Synchronizer system in Synchronizer Web Admin, the LDAP group's existing members are added to the group as displayed in Synchronizer Web Admin. Subsequently, Synchronizer Web Admin polls for updates to LDAP group membership, so that the group membership displayed in Synchronizer Web Admin always matches the LDAP group membership.

By default, Synchronizer Web Admin polls the LDAP directory for group membership changes every 30 minutes. It polls only the groups in containers that it has been configured to search, as described in [Section 2.3.1, "Searching Multiple LDAP Contexts for Users and Groups,"](#) on page 12.

- 1 In [Synchronizer Web Admin](#), click *Manage Global Settings* .



The screenshot shows the 'Manage Global Settings' page with a 'LDAP Settings' tab selected. The 'LDAP Group Membership Polling Rate (in seconds)' is currently set to 1800. Other settings include LDAP Server Hostname (172.16.5.18), LDAP Port (389), LDAP Base User DNs (ou=Users, o=Novell), LDAP Base Group DNs (ou=Users, o=Novell), LDAP Admin Full DN (cn=admin, ou=docdev, o=n), and LDAP Admin Password (masked). There are buttons for 'Save LDAP Settings' and 'Poll LDAP Now'.

- 2 Adjust the polling rate as needed to synchronize the group membership in Synchronizer Web Admin with current LDAP group membership to meet the needs of your Synchronizer system.
- 3 Click *Save LDAP Settings*.
- 4 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

2.3.4 Adjusting the Synchronizer Web Admin Timeout

By default, Synchronizer Web Admin times out after one hour. You can adjust the session time by editing the Synchronizer Web Admin configuration file.

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.

- 2 Change to the following directory:

```
/etc/datasync/webadmin
```

- 3 Open the `server.xml` file in a text editor.

- 4 Add the following line between the `<config>` tags:

```
<sessionTimeout>seconds</sessionTimeout>
```

- 5 Replace `seconds` with the number of seconds you want to elapse before Synchronizer Web Admin times out.

The default is 3600 seconds (60 minutes). Increase or decrease the setting as needed to meet your security needs.

- 6 Save the `server.xml` file, then exit the text editor.

- 7 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

2.3.5 Changing the Synchronizer Web Admin Port Number

When you access Synchronizer Web Admin from your Web browser, the default port number is 8210. You can configure Synchronizer Web Admin to use a different port number, such as a port number that is already open through your firewall to provide external access to Synchronizer Web Admin.

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.

- 2 Change to the following directory:

```
/etc/datasync/webadmin
```

- 3 Open the `server.xml` file in a text editor.

- 4 Change 8210 to the desired port number.


- 5 Save the `server.xml` file, then exit the text editor.

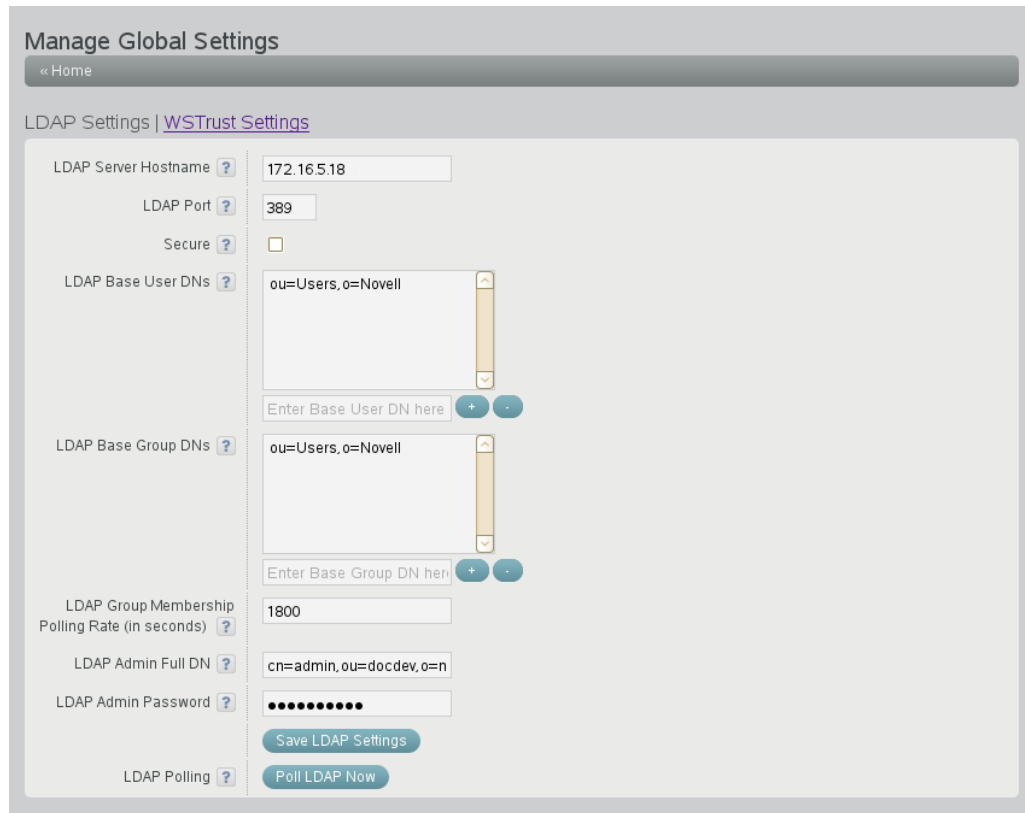
- 6 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

2.3.6 Enabling and Disabling SSL for the Synchronizer LDAP Connection

During Mobility Pack installation, you chose whether to use SSL for the connection between the Synchronizer Web Admin and the LDAP directory. You can change the setting after installation as needed.

- 1 In [Synchronizer Web Admin](#), click *Manage Global Settings* .



The screenshot shows the 'Manage Global Settings' page with a breadcrumb trail: « Home > LDAP Settings | WSTrust Settings. The LDAP Settings section includes the following fields and controls:


- LDAP Server Hostname: 172.16.5.18
- LDAP Port: 389
- Secure:
- LDAP Base User DNs: ou=Users,o=Novell (with a list box and a '+ -' button)
- LDAP Base Group DNs: ou=Users,o=Novell (with a list box and a '+ -' button)
- LDAP Group Membership Polling Rate (in seconds): 1800
- LDAP Admin Full DN: cn=admin,ou=docdev,o=n
- LDAP Admin Password: masked with dots
- Buttons: Save LDAP Settings, Poll LDAP Now
- LDAP Polling: ?

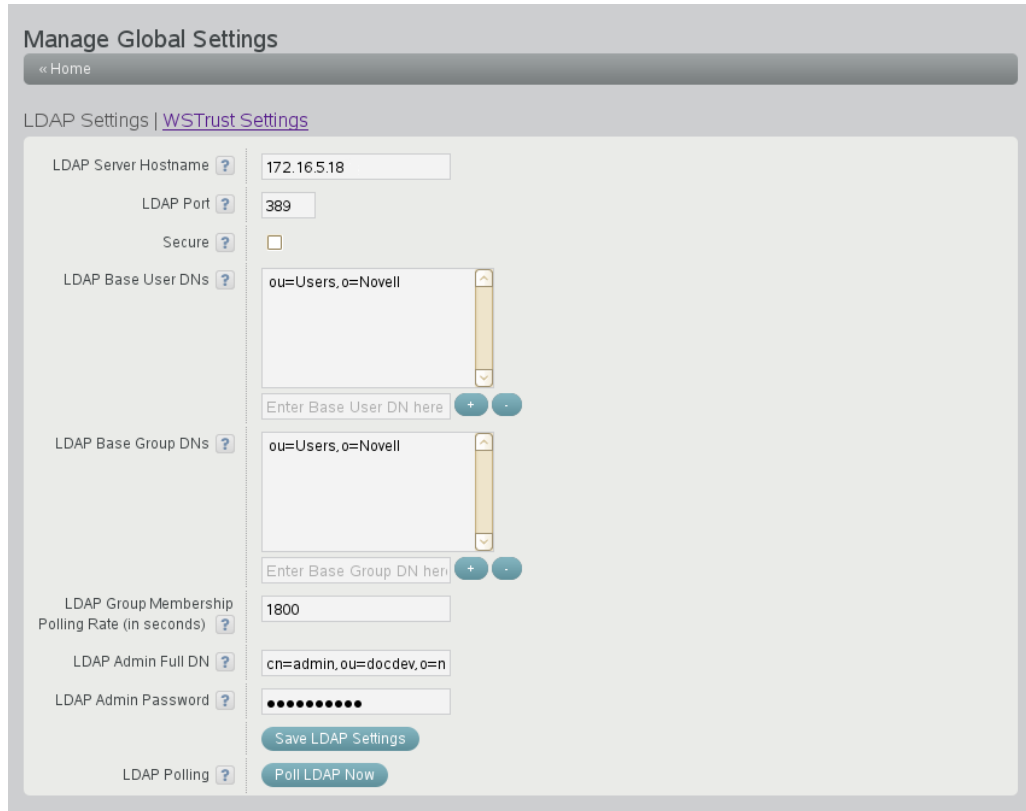
- 2 Select or deselect *Secure* to enable or disable SSL.
- 3 In the *LDAP Port* field, adjust the port number as needed to match the port number used by the LDAP server.
The default secure SSL port is 636. The default non-secure port is 389.
- 4 Click *Save LDAP Settings*.
- 5 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```


2.3.7 Changing the LDAP Server for Authentication

During Mobility Pack installation, you selected an LDAP server for Synchronizer Web Admin to communicate with when authenticating to the LDAP directory. You can change the LDAP server after installation as needed.

- 1 In [Synchronizer Web Admin](#), click *Manage Global Settings* .



The screenshot shows the 'Manage Global Settings' interface. At the top, there is a breadcrumb trail: '<< Home' and 'LDAP Settings | WSTrust Settings'. The main content area is titled 'LDAP Settings' and contains several configuration fields:

- LDAP Server Hostname**: Text input field containing '172.16.5.18'.
- LDAP Port**: Text input field containing '389'.
- Secure**: A checkbox that is currently unchecked.
- LDAP Base User DNs**: A list box containing 'ou=Users,o=Novell'. Below it is a text input field 'Enter Base User DN here' with '+' and '-' buttons.
- LDAP Base Group DNs**: A list box containing 'ou=Users,o=Novell'. Below it is a text input field 'Enter Base Group DN here' with '+' and '-' buttons.
- LDAP Group Membership Polling Rate (in seconds)**: Text input field containing '1800'.
- LDAP Admin Full DN**: Text input field containing 'cn=admin,ou=docdev,o=n'.
- LDAP Admin Password**: Password input field with masked characters '.....'.

At the bottom of the settings area, there are two buttons: 'Save LDAP Settings' and 'Poll LDAP Now'.

- 2 In the *LDAP Server Hostname* field, specify the IP address or DNS hostname of the LDAP server that you want to use for authentication.
- 3 (Conditional) If needed for the new LDAP server, adjust the port number and secure SSL setting. The default secure SSL port is 636. The default non-secure port is 389.
- 4 (Conditional) If needed for the new LDAP server, adjust the LDAP base DN for users and groups.
- 5 (Conditional) If needed for the new LDAP server, adjust the LDAP administrator DN and password.

If you accidentally change any LDAP server information so that you are prevented from logging in to Synchronizer Web Admin using the new LDAP information, you can still log in using the root user name and password, as described in [Section 2.3.9, "Accessing Synchronizer Web Admin When the LDAP Server Is Inaccessible,"](#) on page 18.

- 6 Click *Save LDAP Settings*.
- 7 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

2.3.8 Using Synchronizer Web Admin with a Single Sign-On Solution

If you are using a single sign-on solution such as Novell Access Manager or WSTrust, Synchronizer Web Admin does not require authentication when you are already logged in to the single sign-on solution.

- ♦ For Novell Single Sign-On, no extra configuration is required.
- ♦ For WSTrust, you must provide WSTrust settings in Synchronizer Web Admin. On the Manage Global Settings page, click *WSTrust Settings*. For more information, see [WSTrust \(http://www.wstrust.com/\)](http://www.wstrust.com/).

2.3.9 Accessing Synchronizer Web Admin When the LDAP Server Is Inaccessible

Occasionally, you might need to log in to Synchronizer Web Admin when the LDAP server is unavailable. At all times, you can log in to Synchronizer Web Admin using the `root` user name and password.

After three unsuccessful attempts to log in to Synchronizer Web Admin as `root`, Synchronizer Web Admin is locked against logging in as `root`. To release the lock, you must restart the Web Admin service, as described in [Section 1.2.3, “Managing the Web Admin Service,”](#) on page 8.

2.3.10 Configuring Synchronizer Web Admin for a Specific Language

The Synchronizer Web Admin interface has been translated into the following languages:

- ♦ Dutch
- ♦ French
- ♦ German
- ♦ Spanish
- ♦ Swedish

By default, Synchronizer Web Admin displays in the same language as your Web browser when you are using one of the supported languages. However, if you are using an unsupported language in your Web browser, Synchronizer Web Admin displays in English.

You can configure Synchronizer Web Admin to use the supported language of your choice instead of English.

- 1 In a terminal window on the Synchronizer server, become `root` by entering `su -` and the root password.
- 2 Change to the following directory:

```
/etc/datasync/webadmin
```

- 3 Open the `server.xml` file in a text editor.
- 4 Add the following line between the `<config>` tags:

```
<lang>language_code</lang>
```

- 5 Replace *language_code* with the supported language that you want to use for Synchronizer Web Admin instead of English.

Language	Language Code
Dutch	nl
French	fr
German	de
Spanish	es
Swedish	sv

- 6 Save the `server.xml` file, then exit the text editor.
- 7 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

3 Synchronizer System Management

When you install the Mobility Pack, your initial Synchronizer system is configured with default settings that are generally appropriate. After installation, you can customize your Synchronizer system configuration as your Synchronizer system expands over time.

- ♦ [Section 3.1, “Monitoring Your Synchronizer System,”](#) on page 21
- ♦ [Section 3.2, “Monitoring the Sync Engine,”](#) on page 23
- ♦ [Section 3.3, “Monitoring Disk Space Usage,”](#) on page 25
- ♦ [Section 3.4, “Working with Log Files,”](#) on page 25
- ♦ [Section 3.5, “Diagnosing Synchronization Problems,”](#) on page 34
- ♦ [Section 3.6, “Maintaining the Synchronizer Database,”](#) on page 35
- ♦ [Section 3.7, “Changing the Synchronizer Database Password,”](#) on page 36
- ♦ [Section 3.8, “Backing Up Your Synchronizer System,”](#) on page 37
- ♦ [Section 3.9, “Reconfiguring Your Synchronizer System to Reflect Network Changes,”](#) on page 40
- ♦ [Section 3.10, “Managing Anonymous Feedback,”](#) on page 42
- ♦ [Section 3.11, “Managing Connectors,”](#) on page 43

3.1 Monitoring Your Synchronizer System


Each component of your Synchronizer system can be separately monitored in Synchronizer Web Admin, as described in:

- ♦ [“GroupWise Connector Monitoring”](#) in the *GroupWise Connector Configuration Guide*
- ♦ [“Synchronization Monitoring and Management”](#) in the *Mobility Connector Configuration Guide*
- ♦ [Section 3.2, “Monitoring the Sync Engine,”](#) on page 23

In addition, you can try the new preview feature, the Global Status Monitor, which allows you to monitor many aspects of all three Synchronizer components in one place. The Global Status Monitor is disabled by default.

- ♦ [Section 3.1.1, “Enabling the Global Status Monitor,”](#) on page 21
- ♦ [Section 3.1.2, “Using the Global Status Monitor,”](#) on page 22
- ♦ [Section 3.1.3, “Disabling the Global Status Monitor,”](#) on page 23

3.1.1 Enabling the Global Status Monitor

- 1 In [Synchronizer Web admin](#), click *Global Status Monitor*  to display the instructions for enabling the Global Status Monitor.

Initially, the current section of the documentation displays in your browser so that you can enable the Global Status Monitor.

2 As root in a terminal window, enter the following command:


```
/opt/novell/datasync/previewfeature.sh --monitor --action enable
```

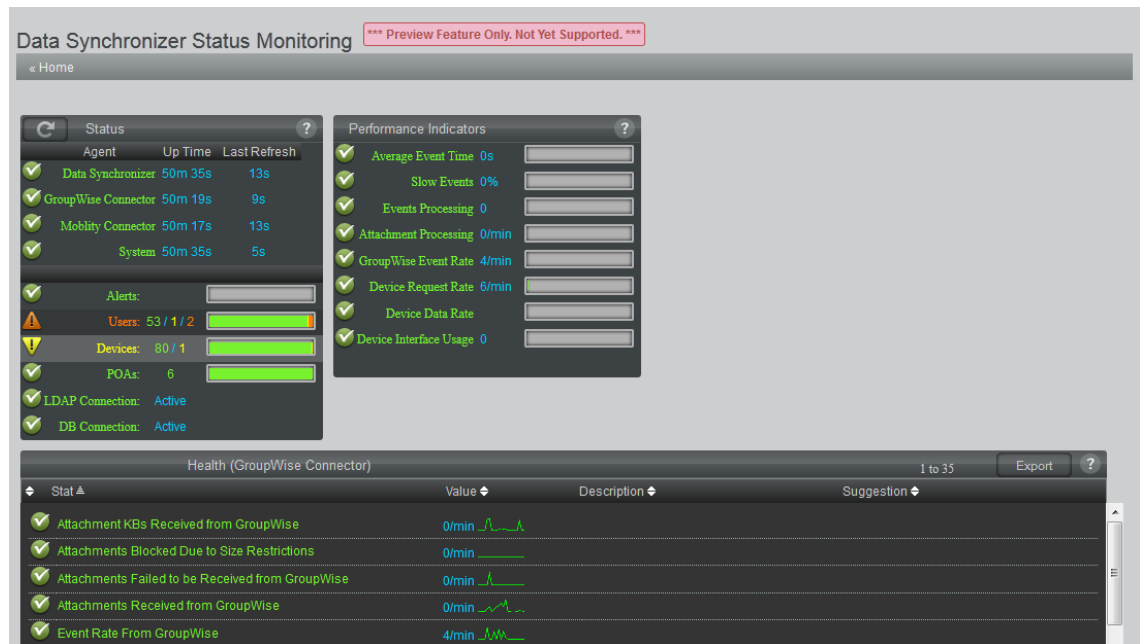
3 Restart the Synchronizer services.

4 Refresh the Synchronizer Web Admin browser window to replace the link to the documentation with the link to the Global Status Monitor.

5 Continue with [Using the Global Status Monitor](#).

3.1.2 Using the Global Status Monitor

1 In Synchronizer Web admin, click *Global Status Monitor*  to display the Global Status Monitor.



The Global Status Monitor provides three types of information:

- ◆ **Status box:** Lists the Synchronizer components (the GroupWise Connector, the Mobility Connector, and the server where they are running) and the participants in the synchronization process (users, devices, POAs, and connections to data sources).

Click a Synchronizer component or synchronization participant to display health or status information in the Listing box.

- ◆ **Performance Indicators box:** Gathers statistics from the Synchronizer components into useful groupings.

Click a performance indicator to display the individual statistics in the Listing box.

- ◆ **Listing box:** Lists the statistics for each Synchronizer component, synchronization participant, or performance indicator.

Click the graph for any statistic to view the statistic over time.

2 Click *Help* in any box for a detailed explanation of the statistics.

3 (Conditional) If necessary, adjust the size of your browser window so that the Help box displays to the right of the Performance Indicators box.

3.1.3 Disabling the Global Status Monitor

Disabling the Global Status Monitor deletes the monitoring data that it has collected.

- 1 As root in a terminal window, enter the following command:

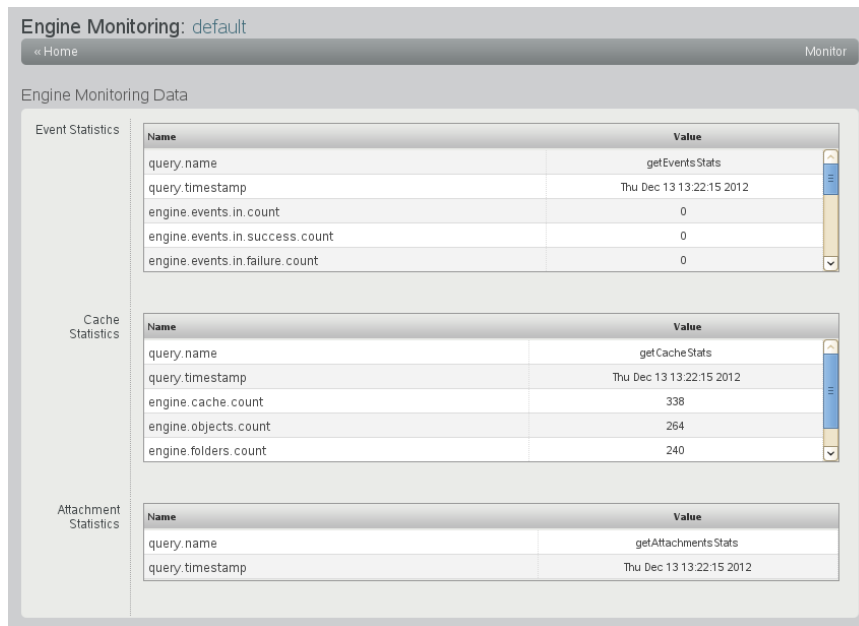
```
/opt/novell/datasync/previewfeature.sh --monitor --action disable
```

- 2 Restart the Synchronizer services.

3.2 Monitoring the Sync Engine

You can assess the functioning of the Sync Engine by checking statistics for events, caching, and attachments.

- 1 In [Synchronizer Web Admin](#), click *Monitoring*  in the *Actions* column for the Sync Engine (default) to display the Engine Monitoring Data page.



Engine Monitoring: default

Engine Monitoring Data

Name	Value
query.name	getEventsStats
query.timestamp	Thu Dec 13 13:22:15 2012
engine.events.in.count	0
engine.events.in.success.count	0
engine.events.in.failure.count	0

Name	Value
query.name	getCacheStats
query.timestamp	Thu Dec 13 13:22:15 2012
engine.cache.count	338
engine.objects.count	264
engine.folders.count	240

Name	Value
query.name	getAttachmentsStats
query.timestamp	Thu Dec 13 13:22:15 2012

- 2 Review the monitoring data in the *Event Statistics* section.

Events are actions that users take on items that are being synchronized. A single **item** can have multiple events associated with it.

Statistic	Description
query.name	The name of the Sync Engine query that is returning the statistics (getEventsStats).
query.timestamp	The date and time when the statistics were gathered. Refresh your browser window to refresh the statistics.
engine.events.in.count	The number of events that the Sync Engine has received from connectors.
engine.events.in.success.count	The number of events that the Sync Engine has received and has successfully stored in its cache for transfer to connectors.

Statistic	Description
engine.events.in.failure.count	The number of events that the Sync Engine has received but has not stored in its cache. Events are not stored when there is an error associated with the event, so that it cannot be successfully processed, or because the event is associated with a user that has not yet been added to any connectors.
engine.events.in.status.count	The total number of status events that the Sync Engine has received from connectors. Status events inform the Sync Engine whether an event was received, dropped, or ignored by a connector. A connector drops an event when the event does not fit within the active policies of the connector. For example, the connector drops events that do not pertain to any users that have been added to the connector. A connector ignores an event when the event cannot be acted on. For example, if the connector receives a delete event for an item that is no longer available for deletion, it drops the event.
events.in.status.success.count	The number of status events received by the Sync Engine that indicate that the events were successfully processed by a connector, so that the Sync Engine does not need to resend those events.
engine.events.in.dq.count	The number of direct queries received by the Sync Engine. A direct query occurs when Synchronizer Web Admin communicates directly with a connected application.
engine.events.out.count	The total number of events that the Sync Engine has sent out to connectors.
engine.events.out.success.count	The number of events that the Sync Engine sent successfully to connectors.
engine.events.out.dq.count	The number of direct queries sent out to connectors.

3 Review the monitoring data in the *Cache Statistics* section.

The Sync Engine caches events until they have been successfully synchronized to all connectors that need the events.

Statistic	Description
query.name	The name of the Sync Engine query that is returning the statistics (<code>getCacheStats</code>).
query.timestamp	The date and time when the statistics were gathered. Refresh your browser window to refresh the statistics.
engine.cache.count	The number of events that are currently cached in the database awaiting synchronization.
engine.objects.count	The number of objects associated with the cached events.
engine.folders.count	The number of folders where synchronized items are stored.
engine.cache.pending.count	The number of events that are waiting in the pending queue because one or more events on which they are depending have not yet been received. For example, if the event for adding an item arrives before the event for adding the folder in which the item must be stored, adding the item must wait until the folder has been added.

- 4 Review the monitoring data in the *Attachment Statistics* section.

Many different types of files can be attached to items. Some types and sizes of attachments are synchronized between applications and some are not, depending on how each connector is configured.

Statistic	Description
query.name	The name of the Sync Engine query that is returning the statistics (getAttachmentsStats).
query.timestamp	The date and time when the statistics were gathered. Refresh your browser window to refresh the statistics.
engine.attachments.count	The number of logical associations between attachments and events that are stored in the cache.
engine.filestore.count	The number of physical attachment files that are stored in the cache. The number of physical attachment files can be less than the number of logical attachments, because a single physical attachment file can be associated with multiple events.

- 5 When you are finished viewing the engine monitoring data, click *Home* in the menu bar to return to the main Synchronizer Web Admin page.

3.3 Monitoring Disk Space Usage

The `datasync-diskcheck.sh` script runs automatically along with the Synchronizer services and monitors disk space usage in the `/var` partition. If disk space usage exceeds 90%, the script shuts down the Synchronizer services normally, to prevent the potential data loss associated with an abnormal shutdown because of insufficient disk space.

The `datasync-diskcheck.sh` script runs every hour. When it detects a low disk space condition, it writes an entry to the `/var/log/datasync/datasync_status` log file. No other notification of the condition is provided before the script shuts down the Synchronizer services.

After a low disk space condition occurs, you can do one or more of the following things to prevent future problems:

- ◆ Improve your database maintenance practices. See [Section 3.6, “Maintaining the Synchronizer Database,” on page 35](#). If you are using the Mobility Connector, see also “[Maintaining the Mobility Connector Database](#)” in “[Mobility Connector Configuration](#)” in the *Mobility Connector Configuration Guide*.
- ◆ Remove old log files. For the location of log files, see [Section 3.4, “Working with Log Files,” on page 25](#). If you are using the Mobility Connector, see also “[Using the Mobility Connector Log File](#)” in “[Mobility Connector Management](#)” in the *Mobility Connector Configuration Guide*.
- ◆ Add more disk space to the Synchronizer server.

3.4 Working with Log Files

Log files provide useful information about the functioning of the various Synchronizer components.

- ◆ [Section 3.4.1, “Log File Overview,” on page 26](#)
- ◆ [Section 3.4.2, “Log File Rotation,” on page 26](#)

- Section 3.4.3, “Logging Levels,” on page 27
- Section 3.4.4, “Sync Engine Log File,” on page 27
- Section 3.4.5, “Config Engine Log File,” on page 28
- Section 3.4.6, “Web Admin Log File,” on page 28
- Section 3.4.7, “Connector Manager Log File,” on page 29
- Section 3.4.8, “Connector Log Files,” on page 29
- Section 3.4.9, “Synchronizer Log File Management Tools,” on page 30
- Section 3.4.10, “NTS supportconfig Tool,” on page 33

3.4.1 Log File Overview

The Synchronizer services generate a set of log files that are created in subdirectories under the following directory:

```
/var/log/datasync
```

The log file subdirectories and file names are:

Synchronizer Component	Log File Subdirectory	Log File Name
Sync Engine	syncengine	engine.log
Config Engine	configengine	configengine.log
Web Admin	webadmin	server.log
Connector Manager	syncengine	connectorManager.log
Connectors	connectors	default.pipeline1.connector_name-AppInterface.log default.pipeline1.connector_name.log

Use the following command to check the most recent additions to a log file:

```
tail -f log_file_name.log
```

3.4.2 Log File Rotation

The Synchronizer log files are automatically compressed and rotated by a `logrotate` cron job. The schedule is set by the `DAILY_TIME="00:30"` line in the `/etc/sysconfig/cron` file, which means that the log files are checked at 12:30 a.m. each night. Any Synchronizer log files that have exceeded 4 MB in size are compressed and rotated at that time. After 99 instances of each log file have accumulated, the oldest log file is deleted when a new log file is created.

Log rotation is controlled by the following files:

```
/etc/logrotate.d/datasync-syncengine
/etc/logrotate.d/datasync-configengine
/etc/logrotate.d/datasync-webadmin
```

By default, `gzip` is used to compress old log files. You can change the compression method by changing the following line in the files listed above:

```
compresscmd /usr/bin/gzip
```

For example, to change from [gzip](http://en.wikipedia.org/wiki/Gzip) (<http://en.wikipedia.org/wiki/Gzip>) compression to [bz2](http://en.wikipedia.org/wiki/Bzip2) (<http://en.wikipedia.org/wiki/Bzip2>) compression, use the following line:

```
compresscmd /usr/bin/bzip2
```

Using bz2 compression produces smaller log files but uses more system resources during compression.

For more information, see the Linux [logrotate](http://linux.about.com/od/commands/l/blcmdl8_logrota.htm) (http://linux.about.com/od/commands/l/blcmdl8_logrota.htm) command.

3.4.3 Logging Levels

All Synchronizer components have log files:

- ♦ [Sync Engine](#)
- ♦ [Config Engine](#)
- ♦ [Web Admin service](#)
- ♦ [Connector Manager](#)
- ♦ [Connectors](#)

All Synchronizer log files use the same logging levels:

- ♦ **Debug:** Logs large quantities of developer-level data. This logging level is appropriate for troubleshooting purposes. It puts a heavy load on the Synchronizer system and should be used only until the troubleshooting activities are completed.
- ♦ **Info:** Logs informational messages about normal synchronization processing. This logging level is suitable for a Synchronizer administrator who wants to observe the functioning of the Synchronizer system.

Info is the default logging level and is strongly recommended because it balances the amount of data logged, the amount of disk space required for log files, and the load on the Synchronizer system.
- ♦ **Warning:** Logs problems that should not adversely affect synchronization processing but should be investigated and resolved for optimum performance. This logging level can be appropriate for a smoothly running Synchronizer system where you only want to be notified of warnings and errors.
- ♦ **Error:** Logs error messages that indicate critical problems in synchronization processing. This logging level puts the least load on the Synchronizer system because it logs only critical errors, but it does not log sufficient data to help resolve any errors that occur.

3.4.4 Sync Engine Log File

The Sync Engine log file ([engine.log](#)) reports on events that pass through the Sync Engine as they transfer from connector to connector. It logs problems with the physical connection to each connector and with communication between connectors. It also logs problems with the event XML files.

You can control the amount of information that is written to Synchronizer log files. The default logging level is Info.

- 1 In [Synchronizer Web Admin](#), click *default* in the *Manage Engine* section to display the Engine Configuration page.
- 2 In the *Logging* section, select a [logging level](#).
- 3 Click *Save Log Settings*.

- 4 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

3.4.5 Config Engine Log File

The Config Engine log file ([configengine.log](#)) reports on configuration setting changes made in Synchronizer Web Admin and on any effects of those changes on the connections between the Sync Engine and connectors. It also logs issues with starting and stopping connectors and tracks the poll cycle for changes in LDAP groups.

You can control the amount of information that is written to Synchronizer log files. The default logging level is Info.

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.
- 2 Change to the following directory:

```
/etc/datasync/configengine
```

- 3 Open the `configengine.xml` file in a text editor.
- 4 Locate the following tag:

```
<log>
  <output>/var/log/datasync/configengine/configengine.log</output>
  <level>info</level>
</log>
```

This section identifies the Config Engine log file and sets the logging level.

- 5 Replace the logging level between the `<log>` tags with the desired [logging level](#).
- 6 Save the `configengine.xml` file, then exit the text editor.
- 7 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

3.4.6 Web Admin Log File

The Web Admin log file ([server.log](#)) reports problems with the Synchronizer Web Admin interface. Typically, you would not see problems here unless you edited the XML source for one of the Configuration pages and introduced invalid XML. If a Configuration page does not display correctly after you edit the XML source, you can check this log file for help resolving the problem with the XML.

You can control the amount of information that is written to Web Admin log file. The default logging level is Info.

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.
- 2 Change to the following directory:

```
/etc/datasync/webadmin
```

- 3 Open the `server.xml` file in a text editor.

- 4 Locate the following tag:

```
<log>
  <output>/var/log/datasync/webadmin/server.log</output>
  <level>info</level>
</log>
```

This section identifies the Web Admin service log file and sets the logging level.

- 5 Replace the logging level between the `<log>` tags with the desired [logging level](#).
- 6 Save the `server.xml` file, then exit the text editor.
- 7 In a terminal window on the Synchronizer server, become `root` by entering `su -` and the root password.

3.4.7 Connector Manager Log File

The Connector Manager log file ([connectorManager.log](#)) reports problems with loading a connector that has the configuration provided on the connector's Configuration page.



The Connector Manager starts one Python thread for itself and an additional Python thread for each connector that it manages. When you list Connector Manager threads or Python threads in a terminal window, you cannot tell which Python thread is associated with the Connector Manager and which Python thread is associated with each connector. The Connector Manager log file lists each component and the PID number associated with each one. This can be very useful for troubleshooting.

3.4.8 Connector Log Files

Each connector has two log files associated with it:

- ♦ The connector application interface log file for each connector (`default.pipeline1.connector_name-AppInterface.log`) reports on problems that occur during event processing by the connector.
- ♦ The connector pipeline log file for each connector (`default.pipeline1.connector_name.log`) reports on problems with the event XML files that transfer back and forth between the Sync Engine and the connector. It logs the results as events pass through the connector.

You can control the amount of information that is written to the connector log file.

- 1 In [Synchronizer Web Admin](#), click the connector that you want to change the setting for.
- 2 In the *Logging* section, select a [logging level](#).
- 3 Click *Save Log Settings*.
- 4 Click *Home* on the menu bar to return to the main Synchronizer Web Admin page.
- 5 In the *Actions* column for the connector, click *Stop*  to stop the connector, then click *Start*  to start the connector with the new setting.

3.4.9 Synchronizer Log File Management Tools

Log files can be an effective window into the functioning of your Synchronizer system. The log file management tools help you to consolidate log files from multiple locations and to gather specific types of information from multiple log files in a single operation.

- ♦ [“Collect Logs Tool” on page 30](#)
- ♦ [“Trace Log Tool” on page 31](#)
- ♦ [“Track Time Tool” on page 32](#)
- ♦ [“Manifest File” on page 33](#)

Collect Logs Tool

As shown in the [Section 3.4.1, “Log File Overview,” on page 26](#), Synchronizer log files are created in a variety of directories. The Collect Logs tool collects the most recent log files into a `.tar.gz` file for convenience when submitting log files to Support. You can collect all of the log files in the following list, or you can collect just the first five, which are the most useful log files:

- ♦ `default.pipeline1.groupwise-AppInterface.log`
- ♦ `default.pipeline1.groupwise.log`
- ♦ `default.pipeline1.mobility-AppInterface.log`
- ♦ `default.pipeline1.mobility.log`
- ♦ `engine.log`
- ♦ `configengine.log`
- ♦ `connectorManager.log`
- ♦ `server.log`

The files are collected into a file named `datasync_logs_YYYY-mm-ddThh.mm.ss.tar.gz`.

To run the Collect Logs tool:

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.
- 2 Change to the following directory:

```
/opt/novell/datasync/tools
```

- 3 Run the following command:

```
python CollectLogs.pyc
```

- 4 Enter `yes` if you want to collect all log files.
or
Enter `no` if you want only the five most useful log files.
- 5 Enter `1` for the GroupWise Connector.
- 6 Enter `1` for the Mobility Connector.

The collected logs are listed in the terminal window and compressed into the `.tar.gz` file.

A `manifest.txt` file that lists the log files in the `.tar.gz` file is also included in the `.tar.gz` file. The `manifest.txt` file can be used as input to the other log file management tools, as described in [“Manifest File” on page 33](#).

Trace Log Tool

The Trace Log tool enables you to trace a specific item or contact through multiple log files.

- 1 In [Synchronizer Web Admin](#), set the logging level to *Debug* for the Sync Engine log file, the GroupWise Connector log file, and the Mobility Connector log file, as described in:
 - ♦ [Section 3.4.4, “Sync Engine Log File,” on page 27](#)
 - ♦ [Section 3.11.2, “Connector Logging Level,” on page 44](#)
- 2 (Conditional) If you want to trace an item (message, appointment, or note), complete this step, then skip to [Step 4](#):
 - 2a In the GroupWise Windows client, send a new item, so that item activity is recorded in the log files.
 - 2b In the Sent Items folder, right-click the item to trace, then click *Properties*.
 - 2c Copy the content of the *Record ID* field to the clipboard of the Windows workstation.
A record ID looks similar to the following example:

```
4C7D1A3C.domain.post_office.100.1686237.1.486FE.1
```
 - 2d Make the content of the *Record ID* field available on the Synchronizer server so that you can paste it into the Trace Log tool in [Step 9](#) below.
- 3 (Conditional) If you want to trace a contact, complete this step, then continue with [Step 4](#):
 - 3a In the GroupWise Windows client, open a personal address book.
 - 3b Right-click the contact to trace, then click *Details*.
 - 3c Click *Advanced*, then scroll down to the *Entry ID* field.
 - 3d Copy the content of the *Entry ID* field to the clipboard of the Windows workstation.
 - 3e Make the content of the *Entry ID* field available on the Synchronizer server so that you can paste it into the Trace Log tool in [Step 9](#) below.
- 4 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.
- 5 Change to the following directory:

```
/opt/novell/datasync/tools
```
- 6 Run the following command:

```
python traceLog.pyc
```

By default, the Trace Log tool accesses log files in the default locations, as listed in [Section 3.4.1, “Log File Overview,” on page 26](#). If you want the Trace Log tool to access log files other than those in the default locations and with the default names, see [“Manifest File” on page 33](#) for additional instructions.
- 7 Enter 1 for the GroupWise Connector.
- 8 Enter 1 for the Mobility Connector.
- 9 Provide the record ID or entry ID that you gathered in [Step 2](#) or [Step 3](#), then press Enter.

The Trace Log tool now creates a file named `trace.out` in the `tools` directory that includes the following sections to help you diagnose the problem:

```
Starting from GroupWise...
=====

From GroupWise Connector into Engine...
=====

Inside Engine...
=====

From Engine to Mobility Connector...
=====

From Mobility Connector to Device...
=====
```

Each section lists the log messages that pertain to the problem item or problem contact for each segment of the synchronization process, enabling you pinpoint the source of the synchronization problem.

- 10 When you are finished tracing items, set the logging level back to its typical setting.

Track Time Tool

The Track Time tool tracks the average time from when an item is created or modified in the GroupWise client to when the item or modification is available in the Mobility Connector and ready for download to your mobile device.

- 1 In [Synchronizer Web Admin](#), set the logging level to *Debug* for the Sync Engine log file, the GroupWise Connector log file, and the Mobility Connector log file, as described in:
 - ♦ [Section 3.4.4, “Sync Engine Log File,” on page 27](#)
 - ♦ [Section 3.11.2, “Connector Logging Level,” on page 44](#)
- 2 In a terminal window on the Synchronizer server, become `root` by entering `su -` and the root password.
- 3 Change to the following directory:

```
/opt/novell/datasync/tools
```

- 4 Run the following command:

```
python trackTime.pyc
```

By default, the Track Time tool accesses log files in the default locations, as listed in [Section 3.4.1, “Log File Overview,” on page 26](#). If you want the Track Time tool to access log files other than those in the default locations and with the default names, see [“Manifest File” on page 33](#) for additional instructions.

- 5 Enter 1 for the GroupWise Connector.
- 6 Enter 1 for the Mobility Connector.

The Track Time tool displays the elapsed time statistics in the terminal window.

- 7 When you are finished gathering elapsed time statistics, set the logging level back to its typical setting.

Manifest File

When you run the Collect Logs tool, it creates a `.tar.gz` file of the collected logs in the `tools` directory. It also includes a `manifest.txt` file that lists the collected log files, for example:

```
{
"GroupWise": "default.pipeline1.groupwise-AppInterface.log",
"Engine": "engine.log",
"Mobility Pipeline": "default.pipeline1.mobility.log",
"Mobility": "default.pipeline1.mobility-AppInterface.log",
"GroupWise Pipeline": "default.pipeline1.groupwise.log"
}
```

The Trace Log tool and the Track Time tool can access the `manifest.txt` file for the list of log files to process. If you want these tools to access archived log files in different locations or with different names from the live log files, you can modify the `manifest.txt` file and make it available to the tools.

- 1 Extract the `manifest.txt` file from the `.tar.gz` file into the same directory with the tools (`/opt/novell/datasync/tools`).
- 2 Edit the `manifest.txt` file with the archived log file locations and file names.
- 3 Use the following commands to run the tools:

```
python traceLog.pyc -i manifest.txt
python trackTime.pyc -i manifest.txt
```

- 4 After you have used the tools to access the log files listed in the `manifest.txt` file, delete or rename the `manifest.txt` file, so that the tools access the live log files, not the archived log files, the next time you run them.

3.4.10 NTS supportconfig Tool

The `supportconfig` tool provided by Novell Technical Services gathers information about your system to help NTS resolve issues with which you require assistance. It is provided as part of the SUSE Linux Enterprise Server 11 operating system. You can also use it for your own troubleshooting activities.

Each component of your Synchronizer system (Sync Engine, connectors, and so on) has a `supportconfig` plug-in that gathers information specific to its functioning. The following information is gathered:

- ◆ The component's configuration file with security information such as passwords stripped out
- ◆ The component's current log file
- ◆ The component-specific script that `supportconfig` ran to collect the information

To run `supportconfig` for your own troubleshooting activities:

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.
- 2 Enter the following command:

```
supportconfig
```

The supportconfig tool examines the server very thoroughly. At the end of its list of findings, it lists the Synchronizer components:

```
Supportconfig Plugins:                6
Plugin: ds_configengine...           Done
Plugin: ds_groupwise_connector...    Done
Plugin: ds_manager_connector...      Done
Plugin: ds_mobility_connector...     Done
Plugin: ds_syncengine...             Done
Plugin: ds_webadmin...               Done
```

The tool zips all the data it collected into the following file:

```
/var/log/nts_servername_yymmdd_hhss.tbz
```

This file name identifies the server and the time stamp for the files that supportconfig has collected.

3 Examine the files that supportconfig collected:

3a Copy the .tbz file to a convenient temporary directory.

3b Use the following command to unzip the compressed file:

```
tar xjf file_name.tzb
```

The following files contain the information about each Synchronizer component:

```
-rw----- 1 root root 14392 Jul 25 21:13 plugin-ds_configengine.txt
-rw----- 1 root root 33965 Jul 25 21:13 plugin-ds_groupwise_connector.txt
-rw----- 1 root root  3644 Jul 25 21:13 plugin-ds_manager_connector.txt
-rw----- 1 root root 20107 Jul 25 21:13 plugin-ds_mobility_connector.txt
-rw----- 1 root root 11538 Jul 25 21:13 plugin-ds_syncengine.txt
-rw----- 1 root root  2256 Jul 25 21:13 plugin-ds_webadmin.txt
```

4 View each .txt file to see the configuration file, current log file, and script file for each Synchronizer component.

For more information, see [supportconfig for Linux \(http://www.novell.com/communities/node/2332/supportconfig-linux\)](http://www.novell.com/communities/node/2332/supportconfig-linux).

3.5 Diagnosing Synchronization Problems

Although log files provide useful information about the functioning of the Synchronizer components, they might not help you determine when data is not synchronizing as expected.

The MCheck utility compares Mobility Connector data with GroupWise data. When a discrepancy is detected, MCheck provides a recommendation for resolving the problem.

MCheck is currently unsupported and is included in the current Synchronizer software for use by Novell Technical Services. However, you can still use MCheck yourself to perform the following actions:

- ♦ Gather configuration settings for your Synchronizer system
- ♦ Verify that the contents of the GroupWise Address Book have synchronized to the Mobility Connector database
- ♦ Verify that the contents of a GroupWise user's mailbox have synchronized to the Mobility Connector database

To run MCheck:

1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.

2 Change to the following directory:

```
/opt/novell/datasync/tools/mcheck
```

3 Run the following command:

```
python mcheck.pyc
```

4 Type the number for the action that you want to perform.

5 (Conditional) If you are verifying a user's mailbox, specify the GroupWise user ID, then press Enter.

6 View the log file for results and recommendations.

Log files are created in the following directory:

```
/opt/novell/datasync/tools/mcheck/logs
```

Action	Log File Name
Gather configuration settings	mobConfiguration_dateTtime.log
Verify the GroupWise Address Book	sab_dateTtime.log
Verify the user's mailbox	username_dateTtime.log

3.6 Maintaining the Synchronizer Database

The Synchronizer database is named `datasync`. The default user for accessing the Synchronizer database is `datasync_user`.

Database maintenance activities for the Synchronizer database ensure satisfactory performance for Synchronizer users.

- ♦ [Section 3.6.1, "Performing General PostgreSQL Database Maintenance,"](#) on page 35
- ♦ [Section 3.6.2, "Configuring Database Maintenance,"](#) on page 36

3.6.1 Performing General PostgreSQL Database Maintenance

The Synchronizer database is a PostgreSQL database. As with any database, the Synchronizer database requires regular maintenance in order to perform reliably. If you are new to managing a PostgreSQL database, see "[Routine Database Maintenance Tasks](http://www.postgresql.org/docs/8.3/interactive/maintenance.html)" (<http://www.postgresql.org/docs/8.3/interactive/maintenance.html>) on the PostgreSQL Documentation Web site for assistance.

3.6.2 Configuring Database Maintenance

The Synchronizer stores Synchronizer system configuration information and pending events when synchronization between the Sync Engine and connectors is interrupted. By default, automatic database maintenance cleans up orphaned and expired records every 2 hours. You can change this interval as needed. For example, you might prefer one-time nightly maintenance.

- 1 In [Synchronizer Web Admin](#), click *default* in the *Manage Engine* section to display the Engine Configuration page.
- 2 Click *Edit XML Source* to display the Engine XML Source window.
- 3 Add the following tags between the `<settings>` and `</settings>` tags:

```
<cacheCleanupInterval>seconds</cacheCleanupInterval>
```
- 4 Replace *seconds* with the time interval for database maintenance.
For example, you could specify 86400 to perform database maintenance once a day, at midnight.
- 5 Click *Save XML* to save your change, then click *Edit Settings Form* to return to the Engine Configuration page.
- 6 In a terminal window, restart the Sync Engine to put the new database maintenance setting into effect.

```
rcdatasync_syncengine restart
```

3.7 Changing the Synchronizer Database Password

To change the Synchronizer database password, you must change the password for `datasync_user` in three places:

- ♦ PostgreSQL (command on the command line)
- ♦ Sync Engine (setting in Synchronizer Web Admin)
- ♦ Config Engine (setting in a configuration file)

- 1 Reset the password for the PostgreSQL database:

1a In a terminal window on the Synchronizer server, become `root` by entering `su -` and the root password.

1b Enter the following command:

```
psql --user datasync_user datasync
```

1c Enter the current password for the Synchronizer database.

1d Enter the following command at the `datasync>` prompt:

```
ALTER USER datasync_user WITH PASSWORD 'password';
```

Replace *password* with the new password for the Synchronizer database.

1e Enter `\q` to quit.

- 2 Reconfigure the Sync Engine to use the new password:

2a In [Synchronizer Web Admin](#), click *default* in the *Manage Engine* section to display the Engine Configuration page.

2b In the *Password* field in the *Database Settings* box, specify the new Synchronizer database password.

2c Click *Save Database Settings*.

- 3 Reconfigure the Config Engine to use the new password.

In the terminal window used for [Step 1](#):

- 3a Change to the following directory:

```
/etc/datasync/configengine
```

- 3b Open the `configengine.xml` file in a text editor.

- 3c In the `<database>` section, replace the existing database password with the new password between the `<password>` tags.

- 3d Save the `configengine.xml` file, then exit the text editor.

- 4 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

- 5 (Conditional) If you want to change the Mobility Connector database password to match the Synchronizer database password, follow the instructions in “[Changing the Mobility Connector Database Password](#)” in “[Mobility Connector Configuration](#)” in the *Mobility Connector Configuration Guide*.

3.8 Backing Up Your Synchronizer System

All of the user data that exists at any time in your Synchronizer system also exists in GroupWise. Therefore, if there is a problem with your Synchronizer system, you can always resynchronize in order to restore your user data to a current working state.

However, you can back up your entire Synchronizer system in order to preserve the Mobility Pack software, configuration files, certificate files, and databases.

- ♦ [Section 3.8.1, “Understanding What to Back Up,”](#) on page 37
- ♦ [Section 3.8.2, “Backing Up a Synchronizer System after Stopping It,”](#) on page 38
- ♦ [Section 3.8.3, “Backing Up a Synchronizer System While It Is Running,”](#) on page 38
- ♦ [Section 3.8.4, “Restoring Your Synchronizer System,”](#) on page 39

For additional details, see TID 7008163, “How to Back Up and Restore the Mobility Pack” in the [Novell Support Knowledgebase \(http://www.novell.com/support\)](http://www.novell.com/support).

3.8.1 Understanding What to Back Up

- ♦ Use your backup software of choice to back up the following directories on your Synchronizer server:

Directory	Description
<code>/opt/novell/datasync</code>	Mobility Pack software
<code>/etc/datasync</code>	Configuration files
<code>/var/lib/datasync</code>	Certificate files

- ♦ Use a PostgreSQL-supported backup solution to back up the Synchronizer database and other connector databases in the following directory:

```
/var/lib/pgsql
```

- ♦ Decide how you want to back up the data:
 - ♦ [Backing Up a Synchronizer System after Stopping It](#)
 - ♦ [Backing Up a Synchronizer System While It Is Running](#)

3.8.2 Backing Up a Synchronizer System after Stopping It

Stopping your Synchronizer system before backing it up is the safest way to ensure a completely consistent backup.

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.
- 2 Create a directory for storing your backup files, for example:

```
mkdir /var/dsbackup
```

- 3 Create a script similar to the following:

```
#!/bin/bash
# back up stopped Synchronizer system
rcdatasync stop
rcpostgresql stop
#
tar -czvpf /var/dsbackup/pgsql.tgz /var/lib/pgsql
tar -czvpf /var/dsbackup/vardatasync.tgz /var/lib/datasync
tar -czvpf /var/dsbackup/optdatasync.tgz /opt/novell/datasync
tar -czvpf /var/dsbackup/etcdatasync.tgz /etc/datasync
#
rcpostgresql start
rcdatasync start
```

For example, you could create a script named `dsbackup.sh` in the `/opt/novell/datasync` directory.

- 4 Add execute permissions to the backup script:


```
chmod +x script_name.sh
```
- 5 Execute the backup script.
- 6 Change to the directory where you backed up the Synchronizer files to verify that the `.tgz` files were successfully created.

3.8.3 Backing Up a Synchronizer System While It Is Running

For convenience, you might want to back up your Synchronizer system while it is still running.

- 1 In a terminal window on the Synchronizer server, become root by entering `su -` and the root password.
- 2 Create a script to back up the Synchronizer database:
 - 2a Create a file named `.pgpass` in the root user's home directory (`/root`).
 - 2b Put the following contents in the `.pgpass` file.

```
*:*:*:datasync_user:database_password
```

The Synchronizer database user is `datasync_user`. The Synchronizer database password was established during installation.

- 2c** Create a database backup script similar to the following, using the `pg_dump` (<http://www.postgresql.org/docs/8.4/static/app-pgdump.html>) command to back up just the Synchronizer database:

```
#!/bin/bash
# back up Synchronizer database
pg_dump -U datasync_user mobility > /tmp/mobility.out
pg_dump -U datasync_user datasync > /tmp/datasync.out
/usr/bin/bzip2 /tmp/mobility.out
/usr/bin/bzip2 /tmp/datasync.out
```

For example, you could create a database backup script named `dsdbbackup.sh` in the `/opt/novell/datasync` directory.

- 2d** Add execute permissions to the backup script:

```
chmod +x script_name.sh
```

- 2e** Execute the backup script.

- 3** Create a script to back up the Synchronizer directories:

- 3a** Create a directory for storing your backup files, for example:

```
mkdir /var/dsbackup
```

- 3b** Use the following script to back up the rest of your Synchronizer system while it is still running:

```
#!/bin/bash
# back up running Synchronizer system
tar -czvpf /var/backup/vardatasync.tgz /var/lib/datasync
tar -czvpf /var/backup/optdatasync.tgz /opt/novell/datasync
tar -czvpf /var/backup/etcdatasync.tgz /etc/datasync
```

For example, you could create a script named `dsdirbackup.sh` in the `/opt/novell/datasync` directory.

- 3c** Add execute permissions to the backup script:

```
chmod +x script_name.sh
```

- 3d** Execute the backup script.

- 3e** Change to the directory where you backed up the Synchronizer files to verify that the `.tgz` files were successfully created.

3.8.4 Restoring Your Synchronizer System

- 1 Change to the directory where you backed up the Synchronizer files.
- 2 Use the following `tar` command to restore the backed-up Synchronizer directories:

```
tar -xzvf file_name.tgz
```

- 3 (Conditional) If you used the `pg_dump` (<http://www.postgresql.org/docs/8.3/static/app-pgdump.html>) command to back up the Synchronizer database separately, use the `psql` (<http://www.postgresql.org/docs/8.3/static/app-psql.html>) command to restore it.

3.9 Reconfiguring Your Synchronizer System to Reflect Network Changes

As time passes, you might make changes to your overall network configuration that affect your Synchronizer system.

- ♦ [Section 3.9.1, “Changing the IP Address of the Synchronizer Server,” on page 40](#)
- ♦ [Section 3.9.2, “Updating the LDAP Password,” on page 42](#)

3.9.1 Changing the IP Address of the Synchronizer Server

- ♦ [“Changing the IP Address for a Small Synchronizer System” on page 40](#)
- ♦ [“Changing the IP Address for a Large Synchronizer system” on page 40](#)

Changing the IP Address for a Small Synchronizer System

For a Synchronizer system with just a small number of users on a single server, the simplest approach is to reinstall the Mobility Pack software.

- 1 Uninstall the Mobility Pack software, as described in [“Uninstalling the Mobility Pack”](#) in [“Mobility Pack Installation”](#) in the *Mobility Pack Installation Guide*.
- 2 Change the IP address of the server.
- 3 Reinstall the Mobility Pack software, as described in [“Running the Mobility Pack Installation Program”](#) in [“Mobility Pack Installation”](#) in the *Mobility Pack Installation Guide*.
- 4 Instruct your mobile device users to delete their accounts from their mobile devices, set them up using the new IP address, then reinitialize their mobile devices.

Changing the IP Address for a Large Synchronizer system

For a Synchronizer system with a large number of users, where having users reinitialize their mobile devices after reinstalling the Synchronizer software could be problematic, you can reconfigure your Synchronizer system with a new IP address, then have users change the IP address that their mobile devices use to access the Synchronizer system.

- 1 Stop the Synchronizer services:

```
rcdatasync stop
```

- 2 Change the IP address of the server.
- 3 Clear event notifications to the POA that refer to the old IP address:

- 3a In the [POA Web console](#), click *Configuration*, then scroll down to the *Internet Protocol Agent Settings* section.

Internet Protocol Agent Settings:	
IMAP Agent	Disabled
SOAP Agent	Enabled
SOAP Port for Incoming SOAP requests:	7191
SOAP over SSL:	Disabled
SOAP Notification List	
Event Configuration List	

- 3b Click *Notification List* to list all Mobility Pack users on that POA.
 - 3c Click each user name to display the Event Configuration page.

GroupWise POA - Sales.Provo2

[Status](#) | [Configuration](#) | [Environment](#) | [Log Files](#) | [Scheduled Events](#) | [MTP Status](#) | [Help](#)

Event Configuration:

UserID	JHarper
Key	default_pipeline1.groupwise_DataSync2_jharper

Add to Notification List
 Show Events
 Delete Events
 Delete Event Configuration

3d Select *Delete Events* and *Delete Event Configuration*, then click *Submit*.

3e Restart the POA.

4 Start the Synchronizer services:

```
rcdatasync start
```

Because the Sync Engine is configured with neutral IP address and hostname information, it starts successfully even though the IP address of the server has changed.

Engine Configuration: default

« Home Monitor

Engine Settings Edit XML Source

IP Address:

Database Settings

Host:
 Port:
 Type:
 Database:
 Username:
 Password:
 ForceConnectionString:


Logging

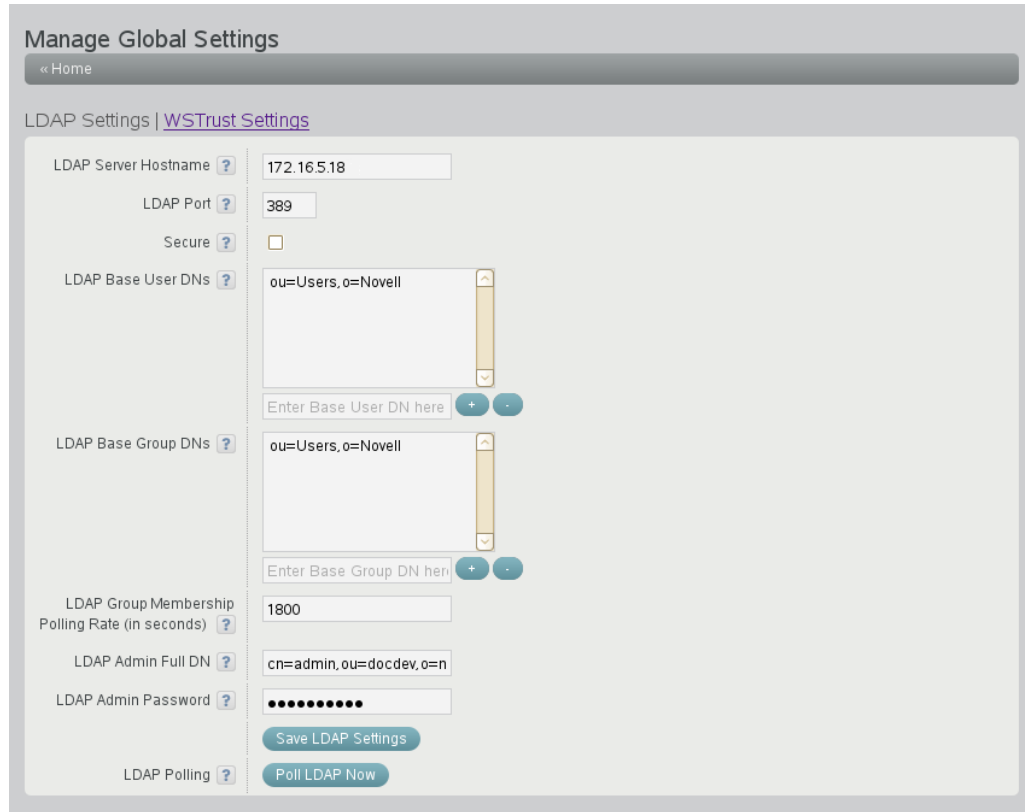
Level:

5 Instruct your mobile device users to reconfigure their accounts with the new IP address.

3.9.2 Updating the LDAP Password

If you change the administrator password on your LDAP server, you must reconfigure your Synchronizer server to match the new password.

- 1 In [Synchronizer Web Admin](#), click *Manage Global Settings* .



The screenshot shows the 'Manage Global Settings' interface for LDAP. The 'LDAP Settings' section includes the following fields and controls:

- LDAP Server Hostname: 172.16.5.18
- LDAP Port: 389
- Secure:
- LDAP Base User DNs: ou=Users,o=Novell
- LDAP Base Group DNs: ou=Users,o=Novell
- LDAP Group Membership Polling Rate (in seconds): 1800
- LDAP Admin Full DN: cn=admin,ou=docdev,o=n
- LDAP Admin Password: [Masked]

Buttons at the bottom include 'Save LDAP Settings' and 'Poll LDAP Now'.

- 2 In the *LDAP Admin Password* field, specify the new password.
- 3 Click *Save LDAP Settings*.
- 4 Restart the Synchronizer services to put the new setting into effect:

```
rcdatasync restart
```

3.10 Managing Anonymous Feedback

Novell is striving to focus engineering efforts around the real-world needs of our Data Synchronizer customers. When you are willing to submit anonymous feedback from your Synchronizer system, you assist in these efforts to improve Synchronizer performance.

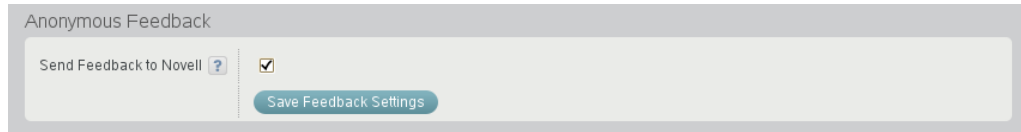
When you enable anonymous feedback, a script runs daily to gather statistics about the usage of your Synchronizer system. The statistics are sent weekly to Novell.

You can enable and disable the sending of feedback at any time. You can review the usage data that has been collected before it is sent to Novell.

- ♦ [Section 3.10.1, “Enabling/Disabling Anonymous Feedback,”](#) on page 43
- ♦ [Section 3.10.2, “Viewing the Collected Feedback,”](#) on page 43

3.10.1 Enabling/Disabling Anonymous Feedback

- 1 In [Synchronizer Web Admin](#), click *Manage Global Settings* , then scroll down to the *Send Feedback to Novell* section.



- 2 Select or deselect *Send Feedback to Novell*, then click *Save Feedback Settings*.

3.10.2 Viewing the Collected Feedback

You can feel comfortable about letting Novell gather usage data from your Synchronizer system. The data is collected by the following script:

```
/opt/novell/datasync/tools/getstats.sh
```

The script is run by the following cron job:

```
/etc/cron.daily/gw-mobility-feedback
```

The cron job runs once a day at midnight. The results are stored in *.gz files in the following directory:

```
/var/log/datasync/configengine
```

The files are saved for 90 days and then deleted.

Use the following command to extract the data from a *.gz file:

```
tar xvfz gwmobility_stats_string_date_time.gz
```

By viewing the gathered usage data, you can assure yourself that no personal data of any kind is being collected by Novell. The following is an example of the type of data that is collected:

```
GWMobilityVersion,SLESVersion,CPUCount,CPUType,SYSKBMemory,SYSType,UserCount,  
DevCount,DevPerUser,GroupWiseEventUserCount,GWAttachmentSize,MCAttachmentSize,  
TotalAttachments,AttachmentCntByMB,BlockedAttachments,MailFromDevice,  
ReadFromFromDevice,DeleteFromFromDevice,MoveFromFromDevice
```

```
1.2.5.190,SLES11SP2,1,Intel(R)Xeon(R)CPUX5550@2.67GHz,1924148,VMwareInc.,  
7,7,"7,0,0,0,0,0",0,500,500,0,"0,0,0,0,0",0,0,7,1,0
```

Thank you in advance for enabling Anonymous Feedback and submitting your Synchronizer system usage data to help improve the Data Synchronizer product.



3.11 Managing Connectors

Some connector configuration settings are the same for both the GroupWise Connector and the Mobility Connector.

- ♦ [Section 3.11.1, “Connector Startup,”](#) on page 44
- ♦ [Section 3.11.2, “Connector Logging Level,”](#) on page 44

3.11.1 Connector Startup

By default, the connectors start automatically whenever you restart the Synchronizer services. You can change this behavior if necessary

- 1 In [Synchronizer Web Admin](#), click the connector that you want to change the setting for.
- 2 In the *Connector Startup* section, select *Manual* so that the connector does not start automatically.
- 3 Click *Save Connector Startup*.
- 4 Click *Home* on the menu bar to return to the main Synchronizer Web Admin page.
- 5 In the *Actions* column for the connector, click *Stop*  to stop the connector, then click *Start*  to start the connector with the new setting.

3.11.2 Connector Logging Level

Each connector writes useful information to two log files, the connector application interface log file and the connector pipeline log file. You can control the amount of information that is written to the connector log file, as described in [Section 3.4.8, “Connector Log Files,”](#) on page 29.

4 User Management

You can add users, groups, and resources to your Synchronizer system.

- ♦ [Section 4.1, “Managing Users,”](#) on page 45
- ♦ [Section 4.2, “Managing LDAP Groups,”](#) on page 50
- ♦ [Section 4.3, “Managing Resources,”](#) on page 52
- ♦ [Section 4.4, “Auditing User Synchronization Activity,”](#) on page 52

4.1 Managing Users

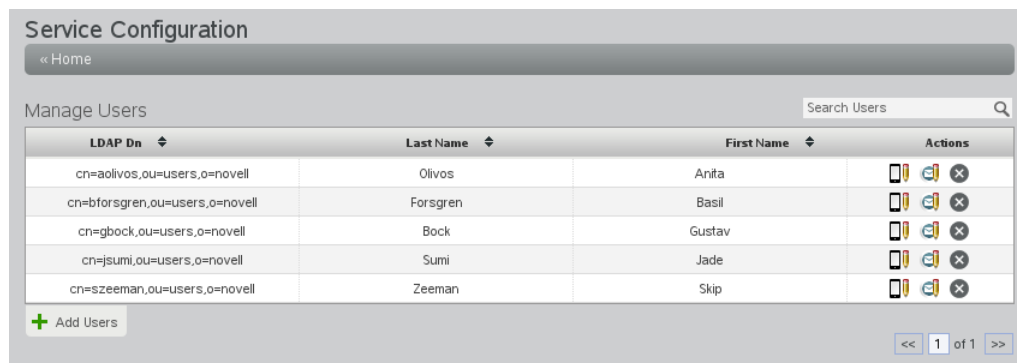
- ♦ [Section 4.1.1, “Adding a User in Synchronizer Web Admin,”](#) on page 45
- ♦ [Section 4.1.2, “Adding a User through an LDAP Group,”](#) on page 46
- ♦ [Section 4.1.3, “Customizing a User’s Synchronization Settings,”](#) on page 47
- ♦ [Section 4.1.4, “Setting a User’s Application Name,”](#) on page 48
- ♦ [Section 4.1.5, “Deleting a User,”](#) on page 49

4.1.1 Adding a User in Synchronizer Web Admin

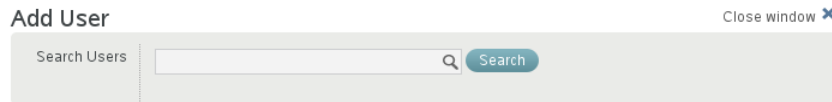
During installation of the Mobility Pack, you specified one LDAP user container and added users from that container. By default, Synchronizer Web Admin searches that LDAP container for users to add. After installation, you can configure Synchronizer Web Admin to search additional LDAP containers for users to add, as described in [Section 2.3.1, “Searching Multiple LDAP Contexts for Users and Groups,”](#) on page 12.

To add a user to your Synchronizer system:

- 1 In [Synchronizer Web Admin](#), click *Users* in the *Manage Access* section.



- 2 Click *Add Users*.



The screenshot shows the 'Add User' window with a search bar labeled 'Search Users' and a 'Search' button. The window title is 'Add User' and there is a 'Close window' button in the top right corner.

- 3 Click *Search* to list the users in LDAP containers that Synchronizer Web Admin has been configured to search.

or

In the *Search Users* field, type the first or last name of a specific user, then click *Search*.



The screenshot shows the 'Add User' window after a search. The search bar contains 'mpalu' and the results are displayed in a table. The table has columns for 'LAST NAME', 'LDAP DN', 'USERNAME', and 'APPLICATION USER NAME'. The first row shows 'Palu' with the LDAP DN 'cn=mpalu,ou=users,o=novell' and the application user name 'mpalu'. There is a 'Click to set' link in the 'APPLICATION USER NAME' column. Below the table is a 'Select All' checkbox and a pagination control showing '<< 1 of 1 >>'. An 'Add' button is at the bottom left.

LAST NAME	LDAP DN	USERNAME	APPLICATION USER NAME
<input type="checkbox"/> Palu	cn=mpalu,ou=users,o=novell	mpalu	Click to set

- 4 Select the user to add to your Synchronizer system.
- 5 (Conditional) If the user's GroupWise user ID is not the same as the user's network login name, in the *Application User Name* column, click *Click to set*, then enter the user's GroupWise user ID in the text box.

Synchronizer uses application user names to match users who have different user names in GroupWise and on the network.

- 6 Click *Add* to add the user to your Synchronizer system.

The user appears on the Manage Users page.

4.1.2 Adding a User through an LDAP Group

As an alternative to adding users in Synchronizer Web Admin, you can add users to any LDAP groups that have already been added to a connector. Users who are added to LDAP groups are added to the Synchronizer system based on the LDAP Group Membership Polling Rate setting, as described in [Section 2.3.3, "Adjusting the Synchronizer Web Admin Polling Rate for Groups,"](#) on page 14. You can also poll immediately, as described in [Section 4.2.2, "Updating an LDAP Group,"](#) on page 51.

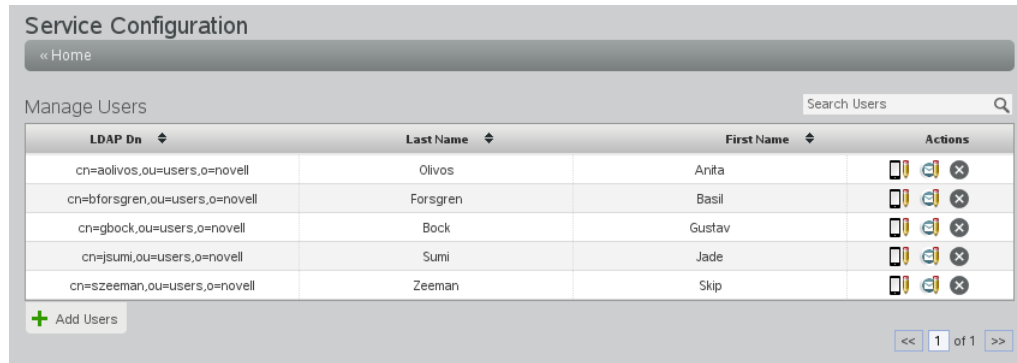
For more information, see [Section 4.2, "Managing LDAP Groups,"](#) on page 50.

4.1.3 Customizing a User's Synchronization Settings

The [Mobility Quick Start](#) describes the synchronization settings that are available to users on the [User Options page](#) of Synchronizer Web Admin. You can also control users' synchronization settings as an administrator.


To change a user's synchronization settings:

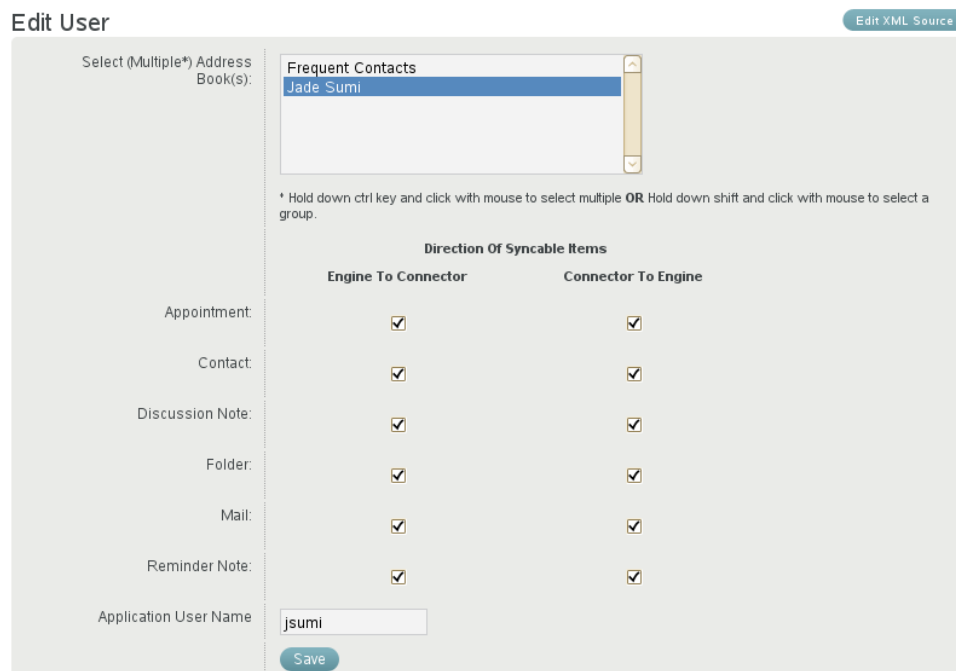
- 1 In [Synchronizer Web Admin](#), click *Users* in the *Manage Access* section.



The screenshot shows the 'Service Configuration' interface for 'Manage Users'. It features a search bar and a table with columns for LDAP Dn, Last Name, First Name, and Actions. The table lists five users: Anifa Olivos, Basil Forsgren, Gustav Bock, Jade Sumi, and Skip Zeeman. Each user has icons for mobile, email, and delete. A '+ Add Users' button is at the bottom left, and a pagination control shows '1 of 1'.


LDAP Dn	Last Name	First Name	Actions
cn=aolivos,ou=users,o=novell	Olivos	Anifa	[Mobile] [Email] [X]
cn=bforsgren,ou=users,o=novell	Forsgren	Basil	[Mobile] [Email] [X]
cn=gbock,ou=users,o=novell	Bock	Gustav	[Mobile] [Email] [X]
cn=jsumi,ou=users,o=novell	Sumi	Jade	[Mobile] [Email] [X]
cn=szeeman,ou=users,o=novell	Zeeman	Skip	[Mobile] [Email] [X]

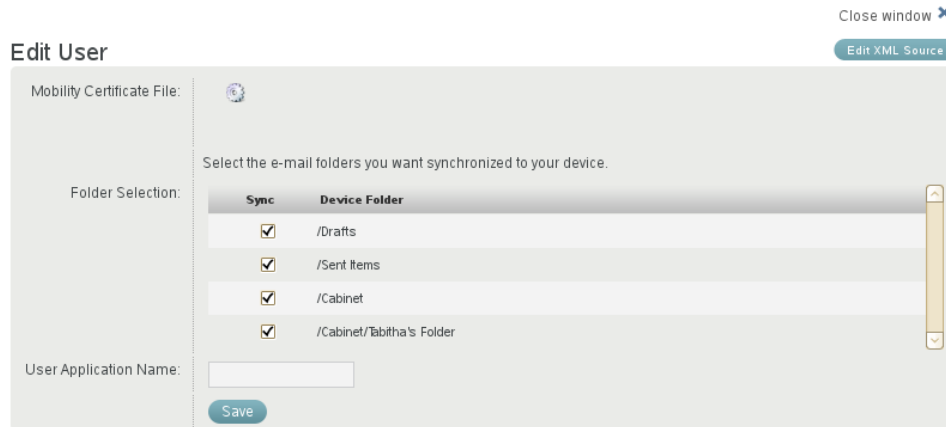
- 2 (Conditional) To set GroupWise settings for users, click *Edit GroupWise Settings* .



The screenshot shows the 'Edit User' interface for GroupWise settings. It includes a 'Select (Multiple*) Address Book(s):' dropdown menu with 'Frequent Contacts' and 'Jade Sumi' selected. Below the menu is a note: '* Hold down ctrl key and click with mouse to select multiple OR Hold down shift and click with mouse to select a group.' The 'Direction Of Syncable Items' section has two columns: 'Engine To Connector' and 'Connector To Engine'. Both columns have checkboxes for Appointment, Contact, Discussion Note, Folder, Mail, and Reminder Note, all of which are checked. The 'Application User Name' field contains 'jsumi' and a 'Save' button is at the bottom.

	Direction Of Syncable Items	
	Engine To Connector	Connector To Engine
Appointment:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Contact:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Discussion Note:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Folder:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mail:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reminder Note:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- (Conditional) To set device settings, click *Edit Device Settings* .



- Select and deselect options as needed to customize the user's data synchronization.
- Click *Save*, then click *Close Window*.

The user's synchronization settings are immediately changed.

4.1.4 Setting a User's Application Name

When you add users to your Synchronizer system during Mobility Pack installation, users are added by specifying their LDAP (network) user names. If LDAP user names are not the same as GroupWise user IDs in your GroupWise system, you must set application names for users in order to map their LDAP user names to their GroupWise user IDs.

IMPORTANT: This task must be done after the users have been added to your Synchronizer system during installation, but before initial synchronization takes place.


When you add users after installation, you provide each user's application name as you add each user, as described in [Section 4.1.1, "Adding a User in Synchronizer Web Admin," on page 45](#). You do not need to add application names as a separate step as described below.

To set a user's application user name:

- In [Synchronizer Web Admin](#), click *Users* in the *Manage Access* section.



LDAP Dn	Last Name	First Name	Actions
cn=aolivos,ou=users,o=novell	Olivos	Anita	
cn=bforsgren,ou=users,o=novell	Forsgren	Basil	
cn=gbock,ou=users,o=novell	Bock	Gustav	
cn=jsumi,ou=users,o=novell	Sumi	Jade	
cn=szeeman,ou=users,o=novell	Zeeman	Skip	

2 Click *Edit GroupWise Settings*  to the right of a user.

Edit User Edit XML Source

Select (Multiple*) Address Book(s):

Frequent Contacts
Jade Sumi

* Hold down ctrl key and click with mouse to select multiple **OR** Hold down shift and click with mouse to select a group.

	Direction Of Syncable Items	
	Engine To Connector	Connector To Engine
Appointment:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Contact:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Discussion Note:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Folder:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mail:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reminder Note:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Application User Name:

Save

3 In the *User Application Name* field, type the GroupWise user ID.

4 Click *Save*, then click *Close Window*.

4.1.5 Deleting a User

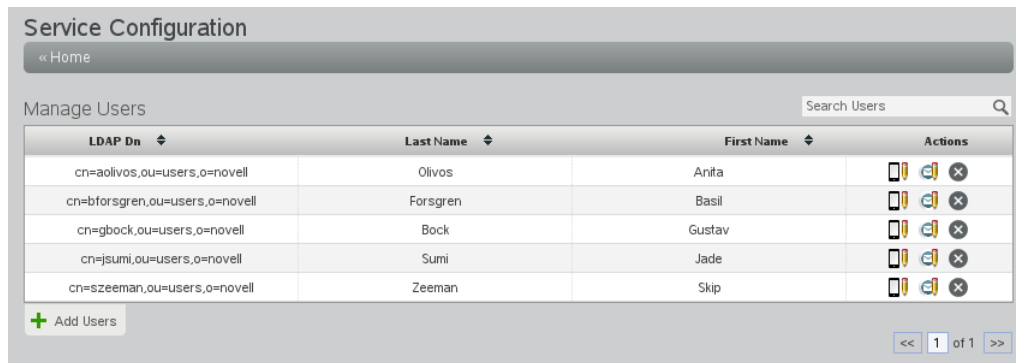
How you delete a user from your Synchronizer system depends on how you added the user.


- ♦ [“Deleting a User Directly” on page 50](#)
- ♦ [“Deleting a User from an LDAP Group” on page 50](#)

Deleting a User Directly

If you added the user during Mobility Pack installation or as described in [Section 4.1.1, “Adding a User in Synchronizer Web Admin,”](#) on page 45, you delete the user in Synchronizer Web Admin.

- 1 In [Synchronizer Web Admin](#), click *Users* in the *Manage Access* section.



- 2 Click *Delete*  to the right of the user, then click *Delete User* to confirm.

Deleting a User from an LDAP Group

If you added the user to your Synchronizer system by adding the user to an LDAP group, you must delete the user from the LDAP group in order to delete the user from your Synchronizer system. For example, you can use ConsoleOne or iManager to delete the user from the LDAP group in eDirectory.

The user is removed from the LDAP group according to the group polling rate, as described in [Section 2.3.3, “Adjusting the Synchronizer Web Admin Polling Rate for Groups,”](#) on page 14. If you do not want to wait for the polling cycle to pass, you can temporarily set the polling rate to a short period of time or you can restart the connector.

4.2 Managing LDAP Groups

During installation of the Mobility Pack, you specified one LDAP group container and added LDAP groups from that container. By default, Synchronizer Web Admin searches that LDAP container for groups to add. After installation, you can configure Synchronizer Web Admin to search additional containers for LDAP groups, as described in [Section 2.3.1, “Searching Multiple LDAP Contexts for Users and Groups,”](#) on page 12.

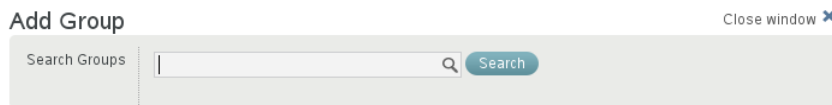
- [Section 4.2.1, “Adding an LDAP Group,”](#) on page 51
- [Section 4.2.2, “Updating an LDAP Group,”](#) on page 51
- [Section 4.2.3, “Deleting an LDAP Group,”](#) on page 52

4.2.1 Adding an LDAP Group

- 1 In [Synchronizer Web Admin](#), click *Groups* in the *Manage Access* section.



- 2 Click *Add Groups*.



- 3 Click *Search* to list the groups in LDAP containers that Synchronizer Web Admin has been configured to search.

or

In the *Search Groups* field, type part of the group name, then click *Search*.




- 4 Select the LDAP group to add to your Synchronizer system.
- 5 Click *Add* to add the LDAP group.

The group is immediately added to the connector.

4.2.2 Updating an LDAP Group

By default, Synchronizer Web Admin polls the LDAP directory for group membership changes every 30 minutes, as described in [Section 2.3.3, “Adjusting the Synchronizer Web Admin Polling Rate for Groups,”](#) on page 14. However, you can poll the LDAP directory immediately to get the latest updates.

- 1 In [Synchronizer Web Admin](#), click *Manage Global Settings* .
- 2 Click *Poll LDAP Now*.

4.2.3 Deleting an LDAP Group

- 1 In [Synchronizer Web Admin](#), click *Groups* in the *Manage Access* section.



- 2 Click *Delete*  for the LDAP group to delete, then click *Yes* to confirm the deletion.

4.3 Managing Resources

You can add resources to your Synchronizer system as if they are users. GroupWise users with rights to the synchronized resource mailboxes can then configure their mobile devices to log in to resource mailboxes just as they can log in to their own mailboxes. This enables GroupWise users to monitor the contents of resource mailboxes from their mobile devices.

Work with GroupWise users to see what resources they want to synchronize to their mobile devices.

Follow the instructions in [Section 4.1, “Managing Users,”](#) on page 45 to add and manage resources in your Synchronizer system.

4.4 Auditing User Synchronization Activity

As your Synchronizer system grows and evolves, you might add a large number of users and groups. As time passes, some users might not need the same synchronization services as when you originally set up your Synchronizer system. You might want to know if there are users in your Synchronizer system who are not currently connecting and synchronizing.

You can check user activity in your Synchronizer system by performing a user audit. You can perform the audit on your entire Synchronizer system or on a specific connector. When you perform a global audit, users are listed based on their most recent activity on any connector. When you perform a connector-specific audit, users are listed based on their most recent activity on that specific connector.

The list includes the following information about each user:

- ♦ Connector name
- ♦ LDAP distinguished name
- ♦ Application user name
- ♦ Type (user or group)
- ♦ Last active

Not all user activities on mobile devices are collected as part of the audit. For example, when users send and delete messages, these activities are captured as part of the audit. However, if users only view their mail and calendar items, these more passive activities are not captured as part of the audit.

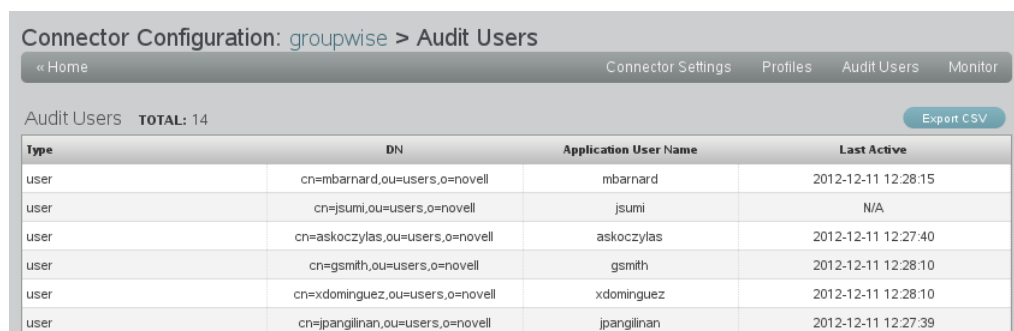
At any time, you can check to see when a specific user last connected to the Synchronizer system, as described in “[Managing Mobile Devices \(Resynchronize, Delete, Block, Reset\)](#)” in “[Synchronization Monitoring and Management](#)” in the *Mobility Connector Configuration Guide*.

To audit Synchronizer users:

- 1 In [Synchronizer Web Admin](#), click *Global Audit*  to list all users in your Synchronizer system.

or

Click a specific connector, then click *Audit Users* to list all users that have been added to the selected connector.



Type	DN	Application User Name	Last Active
user	cn=mbarnard,ou=users,o=novell	mbarnard	2012-12-11 12:28:15
user	cn=jsumi,ou=users,o=novell	jsumi	N/A
user	cn=askoczylas,ou=users,o=novell	askoczylas	2012-12-11 12:27:40
user	cn=gsmith,ou=users,o=novell	gsmith	2012-12-11 12:28:10
user	cn=xdominguez,ou=users,o=novell	xdominguez	2012-12-11 12:28:10
user	cn=jpangilinan,ou=users,o=novell	jpangilinan	2012-12-11 12:27:39

- 2 To save the listed data for use in a spreadsheet:

- 2a Click *Export CSV*.

- 2b Select *Save File*, then click *OK*.

- 2c Browse to and select the directory where you want to save the file.

- 2d (Optional) Change the file name as needed.

- 2e Click *Save* to save the audit report in CSV format for use in a spreadsheet program.

5 Synchronizer System Security

Security administration features help you keep your Synchronizer system and the GroupWise data that it synchronizes secure regardless of where users take their mobile devices. Some initial security policies are recommended. Over time, you can develop additional security policies to meet the needs of your Synchronizer system.

- ♦ [Section 5.1, “Security Administration,” on page 55](#)
- ♦ [Section 5.2, “Security Policies,” on page 61](#)

5.1 Security Administration

It is vital to secure the communication path through which GroupWise data synchronizes from GroupWise mailboxes through your Synchronizer system out to mobile devices and back again.

- ♦ [Section 5.1.1, “Securing Communication with the LDAP Server,” on page 55](#)
- ♦ [Section 5.1.2, “Securing Communication between the GroupWise Connector and the GroupWise POA,” on page 56](#)
- ♦ [Section 5.1.3, “Securing Communication between the Mobility Connector and Mobile Devices,” on page 56](#)
- ♦ [Section 5.1.4, “Selecting a Specific Version of SSL,” on page 60](#)

5.1.1 Securing Communication with the LDAP Server

If your GroupWise system is configured to use LDAP authentication when users access their GroupWise mailboxes, your LDAP server is already set up for a secure SSL LDAP connection with your Synchronizer system. If you are not yet using LDAP authentication in your GroupWise system, but you want to use secure LDAP for communication with your Synchronizer system, the GroupWise documentation provides information to help you set this up. See [“Trusted Root Certificates and LDAP Authentication”](#) in [“Security Administration”](#) in the *GroupWise 2012 Administration Guide*.

You can enable and disable SSL for the LDAP connection on the Global Settings page in Synchronizer Web Admin. For instructions, see [Section 2.3.6, “Enabling and Disabling SSL for the Synchronizer LDAP Connection,” on page 16](#).

5.1.2 Securing Communication between the GroupWise Connector and the GroupWise POA

The GroupWise Connector communicates with the GroupWise POA as a SOAP client. In order to secure communication between the GroupWise Connector and the GroupWise POA, the POA must be configured for secure SSL SOAP, as described in “[Supporting SOAP Clients](#)” in “[Post Office Agent](#)” in the *GroupWise 2012 Administration Guide*.

You can enable and disable SSL for the POA SOAP connections on the GroupWise Connector Configuration page in Synchronizer Web Admin. For instructions, see “[Enabling and Disabling SSL for POA SOAP Connections](#)” in “[GroupWise Connector Configuration](#)” in the *GroupWise Connector Configuration Guide*.

5.1.3 Securing Communication between the Mobility Connector and Mobile Devices

In order to provide a secure SSL connection between the Mobility Connector and mobile devices, you must provide a server certificate on the Synchronizer server.

- ♦ “[Using a Self-Signed Certificate on the Synchronizer Server](#)” on page 56
- ♦ “[Using a Commercially Signed Certificate on the Synchronizer Server](#)” on page 57
- ♦ “[Manually Converting a Certificate to DER Format for Use on Mobile Devices](#)” on page 58
- ♦ “[Manually Downloading a Certificate to a Mobile Device](#)” on page 59
- ♦ “[Enabling and Disabling SSL for Device Connections](#)” on page 60
- ♦ “[Enabling a Password Policy for Device Connections](#)” on page 60

For issues with specific types of certificates, see [Data Synchronizer Mobility Connector SSL Issues](#) (http://wiki.novell.com/index.php/Data_Synchronizer_Mobility_Connector_SSL_Issues).

For SSL issues with specific types of devices, see [Data Synchronizer Mobility Connector Devices](#) (http://wiki.novell.com/index.php/Data_Synchronizer_Mobility_Connector_Devices).

Using a Self-Signed Certificate on the Synchronizer Server

When you have the Mobility Pack Installation program create a self-signed certificate for you, two certificate files are created in the `/var/lib/datasync/device` directory:

```
mobility.pem  
mobility.cer
```

When a mobile device connects to the Mobility Connector, the Mobility Connector passes the self-signed certificate file (`mobility.pem`) to the mobile device. In most cases, the mobile device accepts the self-signed certificate and connects successfully.

Some mobile devices do not automatically accept self-signed certificates in PEM format. If you choose to use a self-signed certificate and if users encounter connection problems with particular mobile devices, explain the procedure in “[Manually Downloading a Certificate to a Mobile Device](#)” on page 59 to the users who are encountering connection problems. This procedure enables users to use the `mobility.cer` file instead of the `mobility.pem` file on their mobile devices.

The self-signed certificate generated by the Installation program is issued to “DataSync Web Admin” rather than to a specific hostname. Some mobile devices require that a self-signed certificate be associated with a specific hostname. You can use YaST to generate a self-signed certificate with a specific hostname. If you need assistance with this task, refer to “[Using YaST on Linux](#)” in “[Security](#)”

Administration” in the *GroupWise 2012 Administration Guide*. Complete Step 1 through Step 4. Do not complete Step 5. By default, YaST generates a single self-signed certificate file as required for use with your Synchronizer system.

Using a Commercially Signed Certificate on the Synchronizer Server

IMPORTANT: You should obtain a commercially signed certificate for use with your Synchronizer system as quickly as possible.

- ♦ “[Selecting a Certificate Authority \(CA\)](#)” on page 57
- ♦ “[Obtaining the Certificate](#)” on page 57
- ♦ “[Removing a Password from a Key File](#)” on page 58
- ♦ “[Combining Files Received from a Certificate Authority](#)” on page 58
- ♦ “[Installing a Commercially Signed Certificate on the Synchronizer Server](#)” on page 58

For more detailed instructions, see TID 7006904, “How to Configure Certificates from a Trusted CA for the Mobility Connector” in the [Novell Support Knowledgebase](http://www.novell.com/support) (<http://www.novell.com/support>).

Selecting a Certificate Authority (CA)

Choose a certificate authority (CA) from the many available on the Web. If you do not want to immediately purchase a certificate, free temporary certificates are available from several Web sites, including:

- ♦ [FreeSSL](http://www.freessl.com) (<http://www.freessl.com>)
- ♦ [Instant SSL](http://www.instantssl.com/ssl-certificate-products/free-ssl-certificate.html) (<http://www.instantssl.com/ssl-certificate-products/free-ssl-certificate.html>)
- ♦ [GlobalSign](http://www.globalsign.com/free-trial/free-ssl-certificate) (<http://www.globalsign.com/free-trial/free-ssl-certificate>)

Obtaining the Certificate

When you have selected a certificate authority, request a certificate in PEM format. If necessary, you can use a chained certificate or a wildcard certificate with your Synchronizer system, although these more complex types of certificates are not recommended.

In order to obtain a certificate, you need to send the certificate authority a certificate signing request (CSR).

For assistance generating a CSR, see “[Generating a Certificate Signing Request](#)” in “[Security Administration](#)” in the *GroupWise 2012 Administration Guide*.

NOTE: Depending on the method that you use to generate the CSR, you might be prompted for the type of Web server where you plan to install the certificate. Synchronizer uses the CherryPy Web server.

The certificate authority returns one or more files to you. These files might require modification for use in your Synchronizer system. Save the files to a convenient location. If the certificate authority included a password, remove the password, as described in “[Removing a Password from a Key File](#)” on page 58. If the certificate authority provided multiple files, combine them into a single file, as described in “[Combining Files Received from a Certificate Authority](#)” on page 58.

Removing a Password from a Key File

If the key file provided by the certificate authority includes a password, you need to remove the password in order to use the key file in your Synchronizer system.

- 1 Check to see if the key file includes a password.

A password-protected key file includes the following line:

```
Proc-Type: 4, ENCRYPTED
```

- 2 Use the following command to remove the password:

```
openssl rsa -in original_file_name.key -out passwordless_file_name.key
```

Combining Files Received from a Certificate Authority

If you receive more than one file from the certificate authority, such as a certificate file and a key file, you must combine the contents into a single file with the following format:

```
-----BEGIN RSA PRIVATE KEY----- several_lines_of_private_key_text
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- several_lines_of_server_certificate_text
-----END CERTIFICATE-----
```

If the certificate authority provided an intermediate certificate, place it at the end of the file after the private key and the actual certificate.

Installing a Commercially Signed Certificate on the Synchronizer Server

- 1 (Conditional) If you have been using a self-signed certificate, rename the existing `/var/lib/datasync/device/mobility.pem` file.
- 2 Copy the certificate file received the certificate authority to `/var/lib/datasync/device`.
- 3 Rename it to `mobility.pem`.
- 4 Restart the Mobility Connector.
- 5 (Conditional) If your particular mobile device does not automatically accept the commercially signed certificate in PEM format, follow the instructions in [“Manually Converting a Certificate to DER Format for Use on Mobile Devices”](#) on page 58.

IMPORTANT: If you uninstall the Synchronizer software, the certificate files associated with your Synchronizer system are also deleted. Back up commercially signed certificates in a location outside of `/var/lib/datasync`.

Manually Converting a Certificate to DER Format for Use on Mobile Devices

Some mobile devices do not automatically accept certificates in PEM format. If users encounter connection problems with particular mobile devices, you can convert the PEM file that you received from the certificate authority into DER format to resolve these connection problems.

- 1 Change to the `/var/lib/datasync/device` directory.
- 2 Execute the following command:

```
openssl x509 -in mobility.pem -inform PEM -out mobility.cer -outform DER
```

IMPORTANT: The output file name with the .cer extension must be in DER (Distinguished Encoding Rules) format.

- 3 Have users with connection problems follow the instructions in “[Manually Downloading a Certificate to a Mobile Device](#)” on page 59 to use the `mobility.cer` file instead of the `mobility.pem` file.

Manually Downloading a Certificate to a Mobile Device

- 1 Access the [Data Synchronizer User Options](#) page on your mobile device at the following URL:

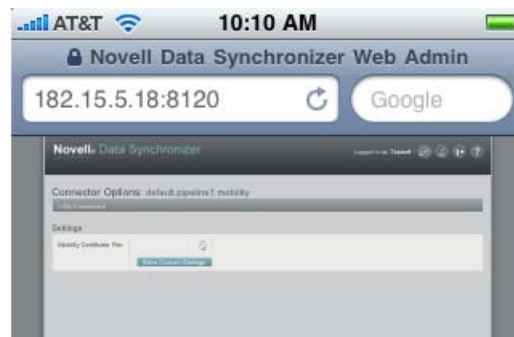
`https://data_synchronizer_server:8120`



Replace `data_synchronizer_server` with the IP address or DNS hostname of the server where you installed the Mobility Pack.

- 2 Log in using your network user name and password.



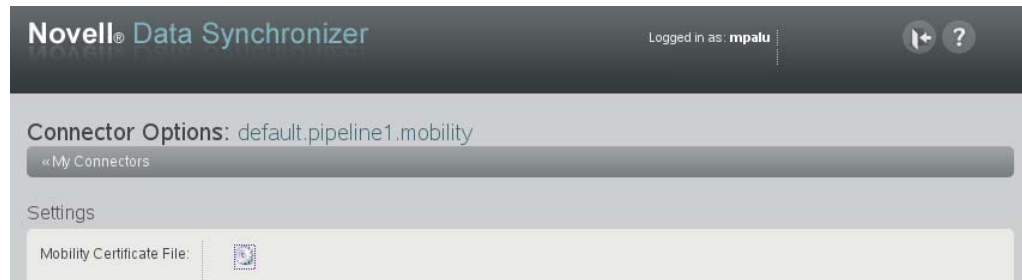
- 3 Click the Mobility Connector.




- 4 (Conditional) If you are the Synchronizer administrator and have associated your mobile device with the Synchronizer administrator account, click *Users*, then click *Edit User*  to display the *Mobility Certificate File* field.
- 5 In the *Mobility Certificate File* field, click *Download Certificate File* .
- 6 Save the `mobility.cer` file to a convenient location on your mobile device.
- 7 Import the certificate file into the certificate store on your mobile device.

For device-specific instructions, see the [Data Synchronizer Mobility Connector Devices Wiki](http://wiki.novell.com/index.php/Data_Synchronizer_Mobility_Connector_Devices) (http://wiki.novell.com/index.php/Data_Synchronizer_Mobility_Connector_Devices).

- 8 (Conditional) If you are not able to access the [Data Synchronizer User Options](#) page from your particular mobile device:
 - 8a Access the [Data Synchronizer User Options](#) page in a Web browser on your Linux or Windows desktop, then click the Mobility Connector.



- 8b Click *Download Certificate File* .
- 8c Save the `mobility.cer` file on your Linux or Windows workstation.
- 8d Set up an IMAP email account on your mobile device, then email the `mobility.cer` file from your workstation to your mobile device.

or

Physically connect your mobile device to your workstation so that it appears as a drive on your workstation, then copy the `mobility.cer` file from your workstation to your device.
- 9 Import the certificate file into the certificate store on your mobile device.

Enabling and Disabling SSL for Device Connections

For instructions, see “[Enabling and Disabling SSL for Device Connections](#)” in “[Mobility Connector Configuration](#)” in the *Mobility Connector Configuration Guide*.

Enabling a Password Policy for Device Connections

For instructions, see “[Enabling a Device Password Security Policy](#)” in “[Mobility Connector Configuration](#)” in the *Mobility Connector Configuration Guide*.

5.1.4 Selecting a Specific Version of SSL

By default, the Mobility Connector accepts connections from mobile devices that use SSLv3 and TLSv1, but rejects connections from mobile devices that use SSLv2. If a user’s mobile device tries to connect using SSLv2, the user receives an error and cannot connect.

You can enable and disable different versions of SSL protocols and also specify the cipher to use with the desired protocol.

- 1 In [Synchronizer Web Admin](#), click the Mobility Connector to display the Mobility Connector Configuration page, then click *Edit XML Source* to display the Connector XML Source window.
- 2 Add the following tags between the `<custom>` and `</custom>` tags:

```
<sslMethod>value</sslMethod>
<sslCiphers>list</sslCiphers>
```

- 3 In the `<sslMethod>` tag, replace *value* with any of the following values:

SSL Version	Value
SSLv2	1 (not recommended)
SSLv3	2
TLSv1	4
All of the above	3 (not recommended)
SSLv3 and TLSv1	5 (default)

- 4 In a terminal window, use the following command to determine the ciphers that are available on your system:

```
openssl ciphers -ssl3
```

- 5 In the `<sslCiphers>` tag in the Connector XML Source window, replace *list* with the desired values as provided by the `openssl` command.
- 6 Click *Save XML* to save your changes, then click *Home* to return to the main Synchronizer Web Admin page.
- 7 Restart the Mobility Connector to put the desired SSL protocol and ciphers into effect.

5.2 Security Policies

Appropriate security policies help you keep users' personal GroupWise data and Synchronizer system information secure.

- ♦ [Section 5.2.1, "Securing Your Synchronizer Data," on page 61](#)
- ♦ [Section 5.2.2, "Securing Your Synchronizer System," on page 62](#)

5.2.1 Securing Your Synchronizer Data

Your Synchronizer server must be kept secure.

- ♦ ["Limiting Physical Access to Synchronizer Servers" on page 61](#)
- ♦ ["Securing File System Access" on page 61](#)

Limiting Physical Access to Synchronizer Servers

Servers where Synchronizer data resides should be kept physically secure, in locations where unauthorized persons cannot gain access to the server consoles.

Securing File System Access

Encrypted file systems should be used on all Synchronizer servers. Only Synchronizer administrators should have direct access to Synchronizer data.

5.2.2 Securing Your Synchronizer System

Locations where GroupWise users' personal data and Synchronizer system information might be obtained must be kept secure.

- ♦ [“Setting Up SSL Connections” on page 62](#)
- ♦ [“Setting Up a Device Password Security Policy” on page 62](#)
- ♦ [“Securing Synchronizer Web Admin” on page 62](#)
- ♦ [“Protecting Synchronizer Configuration Files” on page 63](#)
- ♦ [“Protecting Synchronizer Log Files” on page 63](#)

Setting Up SSL Connections

Secure SSL connections should be used between your Synchronizer system and the following external components:

- ♦ LDAP server
- ♦ GroupWise Post Office Agent (POA)
- ♦ Browser connection for Synchronizer Web Admin
- ♦ Mobile devices

For instructions, see [Section 5.1, “Security Administration,” on page 55](#).

Setting Up a Device Password Security Policy

To increase your control over mobile device access to your Synchronizer system, you should establish a device password security policy to ensure that users set up secure passwords on their mobile devices. For instructions, see [“Enabling a Device Password Security Policy” in “Mobility Connector Configuration” in the *Mobility Connector Configuration Guide*](#).

Securing Synchronizer Web Admin

One Synchronizer administrator is established when you install the Mobility Pack. Additional users can be granted Synchronizer administrator rights, as described in [Section 2.3.2, “Setting Up Multiple Synchronizer Administrator Users,” on page 13](#), but this should be done carefully.

Synchronizer Web Admin can be integrated with a single sign-on solution, as described in [Section 2.3.8, “Using Synchronizer Web Admin with a Single Sign-On Solution,” on page 18](#).

Protecting Synchronizer Configuration Files

The configuration files for all Synchronizer components should be protected from tampering. Configuration files are found in the following default locations:

Synchronizer Component	Configuration File
Sync Engine	<code>/etc/datasync/syncengine/engine.xml</code>
Web Admin	<code>/etc/datasync/webadmin/server.xml</code>
Config Engine	<code>/etc/datasync/configengine/configengine.xml</code>
Connector Manager	<code>/etc/datasync/syncengine/connectors.xml</code>

Protecting Synchronizer Log Files

The log files for all Synchronizer components should be protected against unauthorized access. Some log files contain very detailed information about your Synchronizer system and users. Synchronizer log files are found in the following locations:

Synchronizer Component	Log File
Sync Engine	<code>/var/log/datasync/syncengine/engine.log</code>
Web Admin	<code>/var/log/datasync/webadmin/server.log</code>
Config Engine	<code>/var/log/datasync/configengine/configengine.log</code>
Connector Manager	<code>/var/log/datasync/syncengine/connector-manager.log</code>
Connectors	<code>/var/log/datasync/connectors/ default.pipeline1.connector_name.log default.pipeline1.connector_name-AppInterface.log</code>

A Synchronizer System Troubleshooting

- ♦ [“Synchronizer Web Admin cannot communicate with the LDAP server” on page 65](#)
- ♦ [“The process of adding users does not proceed as expected” on page 65](#)

Synchronizer Web Admin cannot communicate with the LDAP server

Explanation: In order for Synchronizer Web Admin to list users to add to connectors, it must be able to communicate with your LDAP server. If Synchronizer Web Admin cannot list users, it cannot communicate with your LDAP server.

Possible Cause: A firewall is blocking communication between the Web Admin service and the LDAP server.

Action: Make sure that communication through the firewall is allowed on port 636 for a secure LDAP connection or port 389 for a non-secure LDAP connection.

Possible Cause: The LDAP server is not functioning correctly.

Action: Reboot the LDAP server.

The process of adding users does not proceed as expected

Explanation: When you add a large number of users to a connector as a group, Synchronizer Web Admin might not display progress as expected. Refreshing the page might give an invalid server error.

Possible Cause: A timing issue between the add user process and the display of the Synchronizer Web Admin page occasionally causes this problem.

Action: Use a phased approach that avoids occasional timing issues.

1 In Synchronizer Web Admin, stop the GroupWise Connector and the Mobility Connector.

2 In Synchronizer Web Admin, add the LDAP group to the GroupWise Connector.

3 In a terminal window, access the Synchronizer database (datasync):

3a Log in as root.

3b Access the Synchronizer database:

```
psql -U datasync_user datasync
```

3c Enter the Synchronizer database password.

- 4 At the `datasync=>` prompt, verify that all of the users in the LDAP group are successfully added to the GroupWise Connector:
 - 4a List the number of users who have been added to the GroupWise Connector.


```
select count(*) from targets;
```

This number includes the LDAP group.
 - 4b Repeat the `select` command until the number of users that have been added to the GroupWise Connector matches the number of users in the LDAP group.
- 5 In Synchronizer Web Admin, start the GroupWise Connector.
- 6 In Synchronizer Web Admin, add the LDAP group to the Mobility Connector.
- 7 At the `datasync=>` prompt, verify that users have been added to the Mobility Connector:
 - 7a Repeat the `select` command until the number of users has doubled (the same set of users added to two connectors).
 - 7b List all of the users and the connectors to which they have been added:


```
select dn,"connectorID",
        disabled from targets order by dn;
```

All users who have a 0 (zero) in the *Disabled* column have been successfully added to the connector listed in the *Connector ID* column.
- 8 At the `datasync=>` prompt, verify the users in the Mobility database (`mobility`):
 - 8a Change to the Mobility Connector database:


```
\c mobility
```
 - 8b List the number of users who have been added to the Mobility Connector:


```
select count(*) from users;
```

This number includes only the users who have been added to the Mobility Connector.
 - 8c When you have finished, exit from the database.


```
\q
```
- 9 In Synchronizer Web Admin, start the Mobility Connector.

B Documentation Updates

This section lists updates to the *Mobility Pack Administration Guide*, as compared with the *Novell Data Synchronizer 1.2 System Administration Guide*. These updates represent changes made for Mobility Pack 1.2.5. The information helps you to keep current on documentation updates and software updates.

The *Mobility Pack Administration Guide* has been updated on the following dates:

- ♦ [Section B.1, “January 28, 2013 \(Mobility Pack 1.2.5\),” on page 67](#)

B.1 January 28, 2013 (Mobility Pack 1.2.5)

Location	Change
Throughout the guide	Removed references to using other Data Synchronizer connectors with a Synchronizer system that is created by installing the Mobility Pack.
Synchronizer Web Admin	
Section 2.3.7, “Changing the LDAP Server for Authentication,” on page 17	Explained how to configure Synchronizer Web Admin to access a different LDAP server.
Section 2.3.8, “Using Synchronizer Web Admin with a Single Sign-On Solution,” on page 18	Introduced WSTrust as a supported single sign-on solution.
Section 2.3.9, “Accessing Synchronizer Web Admin When the LDAP Server Is Inaccessible,” on page 18	Explained how to log in to Synchronizer Web Admin when the LDAP server is unavailable.
Synchronizer System Management	
Section 3.1, “Monitoring Your Synchronizer System,” on page 21	Introduced the new Global Status Monitor that is available as a preview feature.
Section 3.4.3, “Logging Levels,” on page 27	Explained the improved system of logging levels.
Section 3.5, “Diagnosing Synchronization Problems,” on page 34	Introduced the MCheck utility.
Section 3.10, “Managing Anonymous Feedback,” on page 42	Introduced the opportunity to submit anonymous feedback about your Synchronizer system to Novell to help improve synchronization performance.

Location	Change
User Management	
Chapter 4, "User Management," on page 45	Explained that users are now managed on a Synchronizer system level, rather than being associated with individual connectors.
Section 4.3, "Managing Resources," on page 52	Explained that resources can be added to your Synchronizer system in the same way as users.
System Security	
"Securing Synchronizer Web Admin" on page 62	Suggested that Synchronizer Web Admin can be protected behind a single sign-on solution.
