

Organization Setup, Device Connection Schedules, and Policy Suites

ZENworks® Mobile Management 2.6.x

January 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 © 2012-13 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 latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Table of Contents

| | |
|---|-----------|
| Accessing the Dashboard | 4 |
| Configuring the Organization | 5 |
| Organization Setup Wizard | 5 |
| Creating an Organization by using the Organization Setup Wizard | 6 |
| Enter Organization Information and Set Parameters | 6 |
| Defining the Organization's Default Servers | 7 |
| Creating the Organization's Default Policy Suite | 9 |
| Creating the Organization's Default Device Connection Schedule | 10 |
| Managing SMTP, ActiveSync, and Administrative LDAP Servers | 11 |
| Configuring the Organization for Hands-Off Enrollment | 13 |
| Policy Suites | 14 |
| Creating a New Policy | 15 |
| Policy Suite Editor | 16 |
| Components of the Policy Suite | 17 |
| Tips on Customizing and Using Policy Suites | 23 |
| Device Connection Schedules | 25 |
| Create a Device Connection Schedule | 25 |
| Editing Device Connection Schedules | 27 |
| Tips on Using Device Connection Schedules | 28 |

Accessing the Dashboard

Accessing the Dashboard

ZENworks Mobile Management dashboard requirements:

- Microsoft Internet Explorer or Firefox
- Adobe Flash Player 10.1.0
- Minimum screen resolution: 1024 x 768
- Desktop computer running Windows OS

In your Web browser, enter the server address of the *ZENworks Mobile Management* server, followed by ***/dashboard***

Example: <https://my.ZENworks.server/dashboard>

Login

Log in to the *ZENworks Mobile Management* dashboard by using the email address and password you designated as administrative login credentials when installing the *ZENworks Mobile Management Web/Http Server Component*.

You can create additional logins to the dashboard with system administrator, organization administrator, or support administrator privileges. See the [System Administration Guide](#) for details.



The screenshot shows the login interface for Novell ZENworks Mobile Management. At the top left is the Novell logo, and at the top right is the word "Novell". The main heading is "Novell. ZENworks Mobile Management" in a large, bold font. Below this, it says "Version 2.6.1" and "© 2012 Novell, Inc. All Rights Reserved". The login form consists of two input fields: "Username" and "Password". The "Username" field has a cursor in it. Below the "Password" field is a "Login" button with a right-pointing arrow.

Configuring the Organization

Organization Setup Wizard

The Organization Setup Wizard is a tool used to create an organization on the *ZENworks Mobile Management* server. The organization might be a company or a distinct group of individuals within a company. Each organization consists of:

- Its users/devices
- One or more policy suites that enforce functionality settings and security settings for an organization's fleet of mobile devices
- One or more device connection schedules that govern when devices synchronize policy setting updates and send device statistics

A single application of *ZENworks Mobile Management* software can accommodate just one organization or host multiple organizations.

Organization tasks:

- Entering organization information.
- Defining a default ActiveSync Server (if applicable) for the purpose of user authentication and hands-off enrollment.
- Defining a default Administrative LDAP Server (optional) for the purpose of importing user information to the *ZENworks Mobile Management* server in batches.
- Defining a default SMTP Server for email communication to and from the *ZENworks Mobile Management* server.
- Creating a default policy suite or for the organization
- Creating a default Device Connection Schedule or schedules for the organization
- Setting up a Welcome letter to be emailed to new users (optional).
- Adding users.

The Organization Setup Wizard steps you through each of the above items. You can then proceed with configuring the Compliance Manager and adding users.

See the following guides:

[Compliance Manager](#)

[Adding Users and Enrolling Devices](#)

Creating an Organization by using the Organization Setup Wizard

The Organization Setup Wizard displays automatically when you log in to *ZENworks Mobile Management* for the first time. Before you create the first organization, you must enter your Customer Care Center credentials. You only have to enter these credentials when using the wizard for the first time.

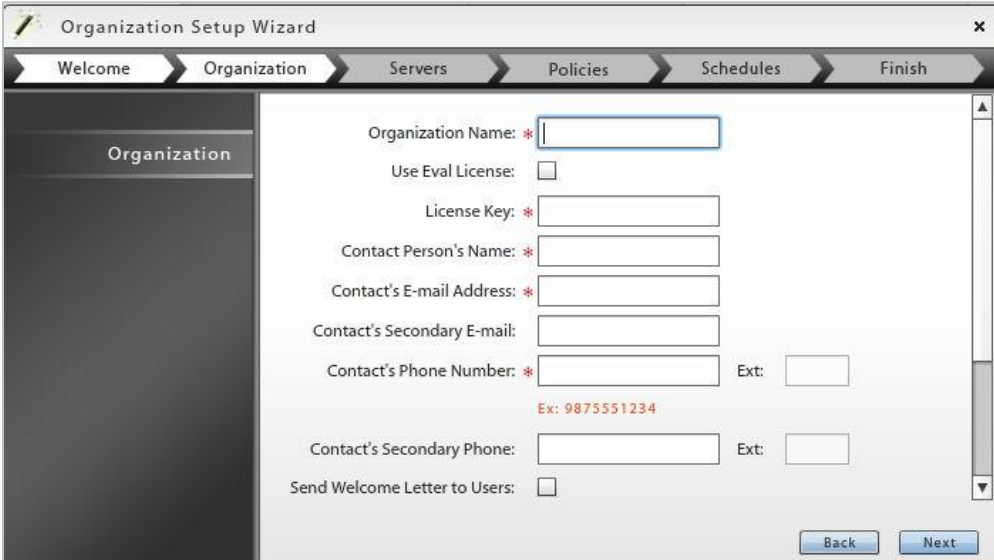
You can also access the wizard via the dashboard.

1. From the *ZENworks Mobile Management* dashboard header, select **System**
2. From the menu panel, select **System Administration > Organizations**.
3. Click the **Add Organization** button.
4. Click **Next** to begin creating a new organization.

Enter Organization Information and Set Parameters

Enter the following:

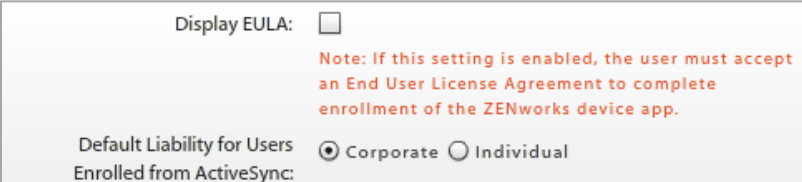
- Organization name
- Contact Name
- Enable Use Eval License or enter a License Key for the organization
- Contact's primary and secondary email address
- Contact's primary and secondary phone number



The screenshot shows the 'Organization Setup Wizard' window with the 'Organization' step selected. The wizard has a progress bar at the top with steps: Welcome, Organization, Servers, Policies, Schedules, and Finish. The 'Organization' step is currently active. The form contains the following fields and options:

- Organization Name: * [Text Input]
- Use Eval License:
- License Key: * [Text Input]
- Contact Person's Name: * [Text Input]
- Contact's E-mail Address: * [Text Input]
- Contact's Secondary E-mail: [Text Input]
- Contact's Phone Number: * [Text Input] Ext: [Text Input]
Ex: 9875551234
- Contact's Secondary Phone: [Text Input] Ext: [Text Input]
- Send Welcome Letter to Users:

At the bottom right of the form are 'Back' and 'Next' buttons.



This section shows two options for configuration:

- Display EULA:
- Default Liability for Users Enrolled from ActiveSync: Corporate Individual

A red note is displayed below the EULA option: "Note: If this setting is enabled, the user must accept an End User License Agreement to complete enrollment of the ZENworks device app."

- Choose whether you want to send an email Welcome Letter to users when they enroll their devices. The letter is associated with the policy suite assigned to the user. Compose or edit the letters via **Organization > Policy Suites**.

- Choose whether to display the **ZENworks Mobile Management End User License Agreement (EULA)** when users enroll their *ZENworks Mobile Management* app (recommended).
- Select the **Default Liability for Users Enrolled from ActiveSync**. Select **Corporate** when liability for data on device rests with the corporation. Select **Individual** when liability rests with the individual carrying the device.
- Click **Next**.

Defining the Organization's Default Servers

Define the following server credentials for the organization:

ActiveSync Server (optional)

An ActiveSync server is not required, but for systems utilizing the ActiveSync protocol, ZENworks Mobile Management can act as a gateway server. An ActiveSync server allows hands-off enrollment of devices, reducing the amount of manual user configuration. In addition, users are authenticated via their ActiveSync server credentials. ActiveSync Email and PIM traffic are relayed to and from devices by ZENworks Mobile Management.

ActiveSync servers using protocol version 12.0 or greater should be configured to enable *Autodiscover* so that actual server address information can be discovered as users enroll.

- ActiveSync server name
- ActiveSync server address
- ActiveSync server port
- Use SSL
- Allow Hands-Off Enrollment
- ActiveSync server domain (*required for hands-off enrollment*)

Defining ActiveSync Server Credentials for Hands-Off Enrollment

Enabling the *Hands-Off Enrollment* option when defining an ActiveSync server provides a method of auto-provisioning users on the *ZENworks Mobile Management* server. You must enter a domain configured on this server. Hands-off enrollment requires users to enroll with the domain in one of the following formats: domain\username or user@domain.

With hands-off enrollment users are automatically added to the *ZENworks Mobile Management* server, as long as their credentials are recognized by the ActiveSync server. *ZENworks Mobile Management* creates the new account by using the ActiveSync user account credentials and the default servers, policy suite, and device connection schedule specified for the organization.

See also [Configuring the Organization for Hands-Off Enrollment](#) and [Managing SMTP, ActiveSync, and Administrative LDAP Servers](#)

LDAP Server (optional)

Defining an LDAP server allows an administrator to add users in batches, import user information into custom column fields, and authenticate administrators via the LDAP server.

- LDAP server name
- LDAP server address
- LDAP server port
- LDAP E-mail Attribute
- Use SSL
- Use TLS
- LDAP username
- LDAP password
- LDAP Base DN
- LDAP Object Class

SMTP Server

ZENworks Mobile Management uses the SMTP server defined here to send administrative email and to send email generated from Group Emailing, Welcome Letters, security command confirmations, etc.

- SMTP server name
- SMTP server address
- SMTP server port
- Use SSL
- Use TLS
- Use Authentication
- Username
- Password
- Automatic Email Address
- Automatic Email Display Name

The screenshot shows the 'Organization Setup Wizard' window at the 'Servers' step. The 'ActiveSync Server' option is selected in the left sidebar. The main area contains the following fields and options:

- ActiveSync Server Name: *
- ActiveSync Server Address: *
- ActiveSync Server Port: *
- Use SSL:
- Allow Hands-Off Enrollment:
- ActiveSync Server Domain: [Text Box] [Add] [Remove]
- Domain: [Table with 1 column and 1 row]

At the bottom, there are 'Back' and 'Next' buttons. A checkbox on the left sidebar is checked: I Have An ActiveSync Server.

ActiveSync Server

The screenshot shows the 'Organization Setup Wizard' window at the 'Servers' step. The 'LDAP Server' option is selected in the left sidebar. The main area contains the following fields and options:

- LDAP Server Name: *
- LDAP Server Address: *
- LDAP Server Port: *
- LDAP E-mail Attribute: *
- Use SSL:
- Use TLS:
- LDAP Username: [Text Box]
- LDAP Password: [Text Box]
- LDAP Base DN: [Text Box]
- LDAP Object Class: [Text Box]

At the bottom, there are 'Back' and 'Next' buttons. A checkbox on the left sidebar is checked: I Have An LDAP Server.

Administrative LDAP Server

The screenshot shows the 'Organization Setup Wizard' window at the 'Servers' step. The 'SMTP Server' option is selected in the left sidebar. The main area contains the following fields and options:

- SMTP Server Name: *
- SMTP Server Address: *
- SMTP Server Port: *
- Use SSL:
- Use TLS:
- Use Authentication:
- User Name: [Text Box]
- Password: [Text Box]
- Automatic Email Address: *
- Automatic Email Display Name: *

At the bottom, there are 'Back' and 'Next' buttons.

SMTP Server

Creating the Organization's Default Policy Suite

You need to create a default policy suite for the organization. Other policy suites can be created later to accommodate different groups of users. The default policy suite is automatically assigned to users added to the system via hands-off enrollment. For additional information, see [Policy Suites](#).

Define a policy name for the organization's default policy suite.

Set corporate policy strength (policy for devices that the company is responsible for).

Set individual policy strength (policy for devices that individuals are responsible for).

- **Low** - No options are restricted on the device. Passwords can be simple.
- **Moderate** - No options are restricted on the device. Passwords are strong and password expiration is enforced.
- **Strict** - Requires an alphanumeric password and encryption on the device and storage card.
- **High** - Browser and camera are disabled. Requires alphanumeric password and encryption on the device and storage card.



To customize the default policy or create additional policies, use the **Policy Suites** option on the *Organization* page.

Creating the Organization's Default Device Connection Schedule

You need to create a default device connection schedule for the organization. Other schedules can be created later to accommodate different groups of users. Device connection schedules dictate peak and off-peak times for devices to synchronize. Times can overlap days to cover different work shift situations and special case employees. The default device connection schedule is automatically assigned to users added to the system via hands-off enrollment. For additional information, see [Device Connection Schedules](#).

Define a schedule name for the organization's default schedule.

Set a corporate device connection schedule (schedule for devices that the company is responsible for).

Set an individual device connection schedule (schedule for devices that individuals are responsible for).

Define the following settings:

Corporate

Monday through Sunday peak connect times

Peak Connect Interval

Require Direct Push for Peak Times

Off-peak Connect Interval

Require Direct Push for Off-peak Times

Individual

Monday through Sunday peak connect times

Peak Connect Interval

Require Direct Push for Peak Times

Off-peak Connect Interval

Require Direct Push for Off-peak Times

Regulating the interval at which devices synchronize should be considered carefully to minimize the device battery depletion.

The times you define in the schedule grid designate peak connection times.

Anything that falls outside the peak schedule is off-peak connection time.

Organization Setup Wizard

Welcome Organization Servers Policies Schedules Finish

Assign a Name

Corporate Schedule

Individual Schedule

Times extending into next day are allowed, but the next day's start time must be after the preceding day's end time.

Define Corporate Peak Connection Times

Monday 8:00 AM to 5:00 PM

Tuesday 8:00 AM to 5:00 PM

Wednesday 8:00 AM to 5:00 PM

Thursday 8:00 AM to 5:00 PM

Friday 8:00 AM to 5:00 PM

Saturday 8:00 AM to 5:00 PM

Sunday 8:00 AM to 5:00 PM

Peak Connect Interval: 30 minutes

Off-peak Connect Interval: 60 minutes

Require Direct Push for Peak Times

Require Direct Push for Off-peak Times

Back Next

To edit the default schedule or create additional schedules, use the **Device Connection Schedules** option on the Organization page.

Managing SMTP, ActiveSync, and Administrative LDAP Servers

You can define multiple administrative LDAP or ActiveSync servers for an organization, in addition to the servers you defined through the Organization Wizard.

You can also edit information for the administrative LDAP, ActiveSync, or SMTP servers defined through the Organization Wizard.

Server Function in the ZENworks Mobile Management Environment

SMTP Server – *ZENworks Mobile Management* uses this server to send administrative email and to send email generated from group emailing, welcome letters, security command confirmations, etc.

ActiveSync Servers – (Optional) With an ActiveSync server defined, *ZENworks Mobile Management* acts as a gateway server relaying email and PIM traffic to and from devices. Users are authenticated via their ActiveSync server credentials. The system accommodates hands-off enrollment. ActiveSync servers using protocol version 12.0 or greater should be configured to enable Autodiscover.

Administrative LDAP Servers defined here are for the purpose of adding users in batches, importing user information into custom column fields, and authenticating administrators via an LDAP server. See these guides for further information:

- [Adding Users, Enrolling Devices: Adding Users via LDAP and Custom Columns](#)
- [System Administration Guide: Creating Administrative Logins](#)

LDAP servers defined under *Corporate Resources* are for the purpose of configuring LDAP settings to make available to iOS device users. When users synchronize the settings, the device is automatically enabled for accessing corporate directory information.

Defining Additional Administrative LDAP or ActiveSync Servers

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the menu panel, select **LDAP Servers** or **ActiveSync Servers**.
3. Click the **Add LDAP Server** or **Add ActiveSync Server** option.
4. Enter the server credentials.

TIP: To limit the number of users pulled from the LDAP server, edit the LDAP Base DN to include a group when you are batch importing users from the LDAP server. This limits the users returned from the query to only those in the group.

Editing Information for Administrative LDAP, ActiveSync, or SMTP Servers

To edit credentials for an existing LDAP, ActiveSync, or SMTP server:

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the menu panel, select **LDAP Servers**, **ActiveSync Server**, or **SMTP Servers**.
3. For LDAP or ActiveSync servers, select the server you want to edit from the table.
4. Edit the information and click **Save Changes**.

Server Connection Testing

Use the **Test Now** button on the server editing screens to test the connection from *ZENworks Mobile Management* to an Administrative LDAP, ActiveSync, or SMTP server after you have initially added it or if you suspect there is a connection problem.

| Server | Tests: | Credentials entered for the test |
|----------------------------|--|---|
| Administrative LDAP Server | -Connectivity between the <i>ZENworks Mobile Management</i> server and the Administrative LDAP server | None – uses the credentials on file |
| ActiveSync Server | -Connectivity between the <i>ZENworks Mobile Management</i> server and the ActiveSync server; -Accessibility by an authorized user; -Autodiscover | A set of active user credentials in the format required by the ActiveSync server. |
| SMTP Server | -Connectivity between the <i>ZENworks Mobile Management</i> server and the SMTP server; -Authentication if <i>Use Authentication</i> is enabled; -Email delivery | None Optional email delivery test: Provide a test email address, subject, and message body |

Configuring the Organization for Hands-Off Enrollment

Enabling the *Hands-Off Enrollment* option when defining an ActiveSync server provides a method of auto-provisioning users on the *ZENworks Mobile Management* server, thus freeing the administrator from the task of adding users either manually or by batch import.

You must also enter a domain that is configured on this server. Hands-off enrollment requires users to enroll with the domain in one of the following formats: domain\username or user@domain.

With hands-off enrollment, users are automatically added to the *ZENworks Mobile Management* server, as long as their credentials are recognized by the ActiveSync server. *ZENworks Mobile Management* creates the new account by using the ActiveSync user account credentials and the default servers, policy suite, and device connection schedule specified for the organization.

Requirements for Novell GroupWise DataSync and Other ActiveSync 2.5 Mail Servers

Systems where iOS users are interfacing with a Novell GroupWise DataSync server must use DataSync Update 4 (Mobility 1.2.4) to fully utilize the hands-off enrollment functionality. Users need to enroll using their entire email address in lieu of their username if they are enrolling by the hands-off method. Similar processes must be followed to use hands-off enrollment when users interface with Exchange 2003 or any other mail server running ActiveSync 2.5 protocol. A user's username and the string of characters to the left of the @ sign in their email address must be the same.

Enabling Hands-Off Enrollment for an ActiveSync Server

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the menu, select **ActiveSync Servers**.
3. From the left panel, select an existing ActiveSync server or create a new ActiveSync server by choosing **Add ActiveSync Server**.
4. Select the box labeled **Allow Hands-Off Enrollment** and make sure you have specified at least one **Domain** for the server. You can enter multiple domains if necessary for your configuration.
5. Click **Finish** or **Save Changes**.

The screenshot shows a dialog box titled "Add Organization ActiveSync Server". The main area contains the following fields and controls:

- ActiveSync Server Name: * ex2007
- ActiveSync Server Address: * 123.456.78.9
- ActiveSync Server Port: * 80
- Use SSL:
- Allow Hands-Off Enrollment:
- ActiveSync Server Domain:
- Domain:
-

Policy Suites

A policy suite is a set of rules and permissions that enforce an organization's security and usage standards for mobile devices in the enterprise. The policy suite is a key element of the *ZENworks Mobile Management* system. It enables administrators to manage users operating on a variety of device platforms and to enforce policies across those device platforms as consistently as possible.

ZENworks Mobile Management currently supports mail/PIM servers operating with ActiveSync protocol versions 2.5, 12.0, 12.1, 14.0, or 14.1. A handful of the *ZENworks Mobile Management* policies, however, are not supported on systems with less than version 12.0. This information, descriptions of individual policy settings, and functionality of settings across device platforms can be found in the [Device Platform Functionality](#) tables. Information about the policies is also available via the tool tips in the dashboard user interface.

The Policy Wizard guides you through setup of an organization's policy suites, which includes settings for both corporate and individual users/devices. The Wizard allows an administrator to quickly create a new policy suite either by copying an existing policy suite or by choosing from a number of pre-defined policy suite templates which reflect four levels of security strength. The administrator can start with one of these templates and use the Policy Suite Editor to customize the settings associated with any of the policy rules.

Multiple policy suites can be created to accommodate different groups of users. Each user/device can be assigned the policy that best suits their role. See the [Default Policy Settings](#) document for a comprehensive list of the policy suite rules and their default settings.

ActiveSync Policies. For enterprises utilizing the ActiveSync protocol, *ZENworks Mobile Management* acts as a gateway server. *ZENworks Mobile Management* intercepts policy updates sent from the ActiveSync server and instead enforces ActiveSync policy settings that have been defined in *ZENworks Mobile Management*. When an ActiveSync server is not part of the enterprise, *ZENworks Mobile Management* itself acts as an ActiveSync server and enforces ActiveSync policies.

Welcome Letter. You can also draft a Welcome Letter that is emailed to users associated with a particular policy suite. In the organization setup, you can enable a setting that issues the letter automatically when the user is added to the system. You can leave this setting disabled and issue the letter manually for each user from the user's profile.

Policy rules are categorized into the following groups:

- Audit Tracking
- Device Control
- File Share Permission
- iOS Devices
- Mobile Apps Permissions
- Security Settings
- S/MIME Settings
- TouchDown Settings

Creating a New Policy

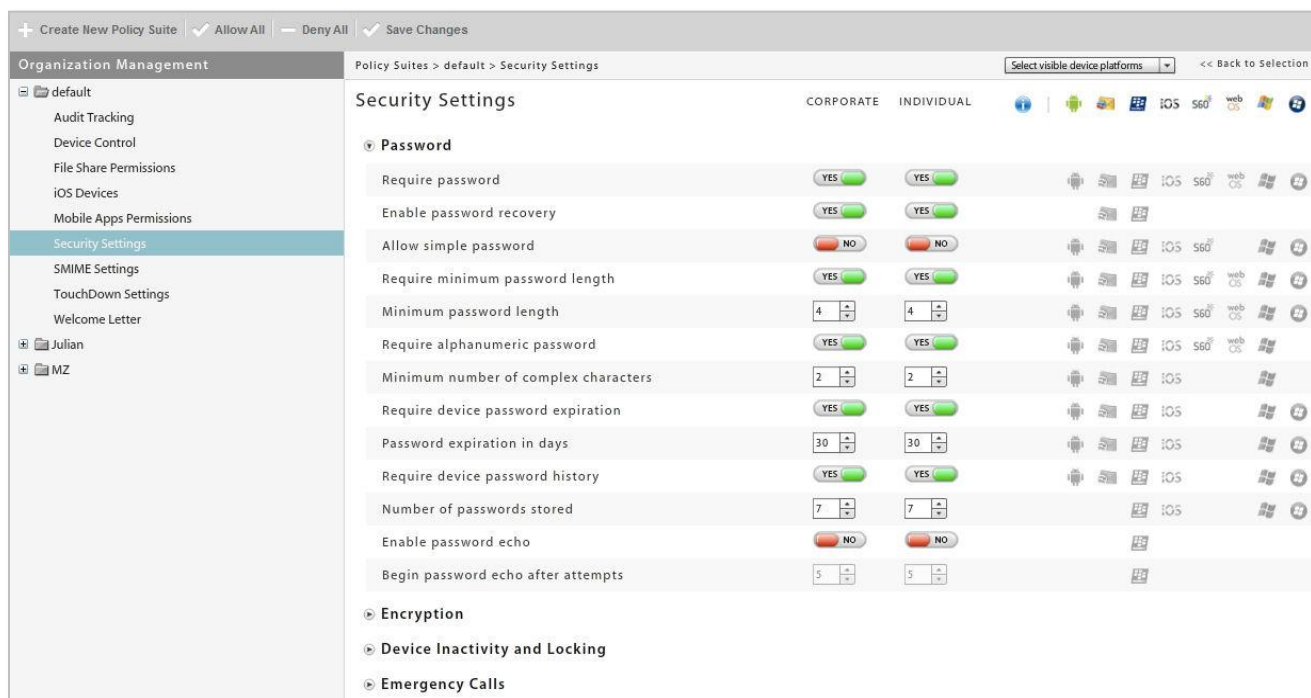
1. From the *ZENworks Mobile Management* dashboard header, select **Organization**
2. Select the **Policy Suites** icon.
3. Click the **Create New Policy** option.
4. Choose a method for creating a policy suite:
 - Create the initial policy suite by using sliders to determine its general policy strength (low, recommended, strict, high security).
 - Create the initial policy suite by copying the settings of an existing policy suite.
5. Use the Policy Suite Editor to customize the new policy.



Policy Suite Editor

To edit an existing policy suite:

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. Select the **Policy Suites** icon.
3. From the menu panel, select the policy you want to change.
4. Edit the Welcome Letter. Enter information that you want to email to new users when they are added to the *ZENworks Mobile Management* system. This can include a welcome to the system, information about policies, links to resources, etc.
 - To have the letter sent automatically when users are added, enable the setting in *Organization Settings*. From the dashboard, select **System > Organization** and select the **Send Welcome Letter to Users** option.
 - To issue the letter as needed for each user, leave the *Organization Settings* option disabled. Then, select **Users** and highlight a user. Click the **Send Welcome Letter** option in the *User Detail* panel.
5. Select the category you want to edit.
6. Edit the settings and click **Save Changes**.



See the [Default Policy Settings](#) document for a comprehensive list of the policy suite rules and their default settings.

Descriptions of individual policy settings and functionality of the settings across device platforms can be found in the [Device Platform Comparison](#) tables.

Components of the Policy Suite

The Welcome Letter

For each policy you create, you can compose a new user Welcome letter that can communicate information to users when they are added to the *ZENworks Mobile Management* system. You might include information about:

- Links to resources, such as the device app downloads, user documentation, and the user self-administration portal
- Details of policies that may change device functionality
- New features that make devices more secure

Welcome Letters can be configured to email automatically or you can manually email them as needed.

To configure the organization so that *Welcome Letters* are automatically emailed to every user that is added to the *ZENworks Mobile Management* server: Select **System** > **Organization** and select the **Send Welcome Letter to Users** option.

To manually send the letter on an individual basis: Select **Users** and highlight a user. Click the **Send Welcome Letter** option in the *User Detail* panel.

To edit the letter: Select **Organization** > **Policy Suites**, highlight a policy, and select the **Welcome Letter** option in the left panel.

The screenshot shows a web interface for configuring a welcome letter. The breadcrumb path is 'Policy Suites > Default Policy > Welcome Letter'. The page title is 'Welcome Letter'. Below the title is a descriptive sentence: 'This is the welcome letter that will be sent to a new user belonging to this policy suite.' There are four input fields: 'Sender Name' with the value 'ZENworks Mobile Management Admin', 'Sender Address' with 'admin@novell.com', and 'Subject' with 'Welcome to ZENworks Mobile Ma'. The 'Body' field is a large text area containing the following text: 'Welcome to the ZENworks Mobile Management service. All links to device applications and documentation for setting up your device can be found at www.novell.com/documentation/zenworksmobile2. Device applications can be found under the "Downloads" section, "Device Application Downloads." Device documentation can be found under the "Documentation" section, "ZENworks Mobile Management Device Apps."'.

Policy Suite Description and Notes

Use the **Description** field to provide more details about the purpose of the policy.

Use the **Notes** field for keeping a record of changes made to a policy.



Policy Suites > Default Policy

Default Policy

Policy Suite Description

Notes for Policy Suite

Save Description and Notes

Policy Settings by Category

Descriptions of individual policy settings and functionality of the settings across device platforms can be found in the [Device Platform Comparison](#) tables.

See the [Default Policy Settings](#) document for a comprehensive list of the policy suite rules and their default settings.

Audit Tracking

This option provides rules that enable tracking of information about device usage (phone and text message logs, file archive) and location.

Examples: Phone and text message logs, GPS tracking statistics

Recording the location of devices can increase battery consumption. Administrators can adjust GPS location accuracy to offset this.

There are six accuracy levels with 1 being the least accurate and consuming the least battery power and 6 being the most accurate and consuming the most battery power. The function of these levels varies based on the device platform, as described in the table below. The accuracy level can be customized by choosing the positioning method and distance. Distance denotes the distance traveled before the device synchronizes a new location.

Symbian S60,3 devices do not support location accuracy; however, users can choose the positioning technology on the device by selecting **Settings > General > Positioning > Positioning Methods**. Choices are Bluetooth GPS, Assisted GPS, Integrated GPS, or Network Based (Cell Towers). Windows Mobile devices partially support location accuracy. The positioning method can be set, but distance requirements are not supported.

Android devices differ across models in how often they detect location. *ZENworks Mobile Management* regulates this by updating at least once per device connection interval with a minimum of ten minutes.

Location Accuracy Functionality by Device Platform

| Level | Android | BlackBerry (w/ NotifySync) | iOS Devices | Windows Mobile 6 |
|--------|---|---|---|---|
| 1 | Cell towers only; approximate location, low power, 1000 meters distance | Cell towers only; low power, no set accuracy | Cell towers only (Levels 1, 2, 3 are the same) | Cell towers only (Levels 1-4 are the same) |
| 2 | Cell towers only; approximate location, low power, 800 meters distance | Cell towers and GPS; no set accuracy | Cell towers only | Cell towers only |
| 3 | Cell towers only; Approximate location, low power, 600 meters distance | Cell towers and GPS; 100 meters | Cell towers only | Cell towers only |
| 4 | GPS; approximate location, low power, 400 meters distance | Cell towers and GPS; 50 meters | GPS; 500 meters to 1 kilometer | Cell towers only |
| 5 | GPS; fine location, high power, 200 meter distance <i>Note:</i> Device constantly checks, even in situations where it is not moving. | Cell towers and GPS; 25 meters | GPS; 100 meters | GPS (Levels 5-6 are the same) |
| 6 | GPS; fine location, high power, 1 meter distance | GPS only; 5 meters | GPS; best to 5 meters Device checks location only when it is moving. | GPS |
| Custom | Location source: Use GPS or Use Cellular Triangulation . Distance in meters: (1-1000) | Location source: Use GPS or Use Cellular Triangulation . Distance in meters: (1-1000) | Location source: Use GPS or Use Cellular Triangulation . Distance in meters: (1-1000) | Location source: Use GPS or Use Cellular Triangulation . WM devices support the positioning technology chosen, but do not support distance requirements. |

Device Control

This option allows you to use different rules to control devices:

- Allow or block the use of device features
- Allow, block, or limit types of email
- Limit the amount of email or calendar items synchronized
- Allow or block the enrollment of multiple devices per user

Examples: Allow Camera. Allow HTML formatted email, Maximum calendar age for synchronization

File Share Permissions

This option provides permissions for whether or not users can access the File Share list. Permissions are granted per folder or subfolder.

iOS Devices

This option provides settings and controls specifically for iOS devices. These rules govern iOS device features and applications, Safari browser settings, ratings controls, configuration profile controls, and iCloud usage.

This category also includes policies that enable you to record the installed applications and manage mobile apps on iOS devices.

Mobile App Permissions

This option provides permissions for whether or not users can access the Mobile App list. Permissions are granted per application.

Permissions for iOS mobile apps for iOS 5 devices include a **Force Push** option. When it is enabled for a policy, Force Push automatically installs the app on all iOS 5 devices associated with the policy.

Security Settings

This option provides rules that enforce compliance with a company's policies for securing mobile devices. Examples: Require Password, Require Encryption, Wipe Device on failed unlock attempts

All Security Settings are dependent on whether you have enabled Require Password.

SMIME Settings

Provides Secure/Multipurpose Internet Mail Extensions settings to add an additional layer of encryption for email messages.

TouchDown Settings

This option provides settings and controls specifically for Android or iOS devices that use the TouchDown application (v7.3.00052 or greater). These rules govern Android and iOS functionality and user access to many TouchDown settings that are configurable on the device. Subcategories include: Installation, General, Signature, Widgets, Phone Book, User Configurable Settings, and Suppressions.

About User Configurable Settings

Users can configure these policies according to preference. Administrators choose the setting for initial device configuration. Changes to these settings do affect existing TouchDown users.

About Suppressions

Suppressions are a specific category of policies that can actually remove the configurable TouchDown setting from the device view. They control whether users have access to settings that configure email, calendar, contacts, tasks, security, synchronization, and device capabilities.

An enabled suppression policy gives the user control of the setting. The policy is enabled when set to YES.



A disabled suppression removes the setting from user devices.

If the disabled suppression has a control setting, the administrator can configure it.

An example of a suppression with a control setting is:



When a disabled suppression does not have a control setting, the setting is locked as it was previously set on the device.

An example of a suppression without a control setting is:



If you plan to disable suppression policies that do not have a control setting, thereby removing it from a device, the setting on the device must be configured accurately before the suppression is imposed.

When suppression policies without control settings will be disabled, the best practices for deploying devices entail the following:

- Create two policy suites – one that does not disable suppressions policies and the policy suite you will ultimately assign to the user.
- Initially, assign to the user the policy that does not disable suppression policies.
- Install and register the TouchDown and *ZENworks Mobile Management* apps on devices.
- Configure the TouchDown settings on the device in accordance with your company policies.

- Change the policy assignment for the user from the dashboard (assign the policy with the suppressions disabled) and allow the changes to synchronize.
- Issue the device to the user.

Welcome Letter

Allows you to create a Welcome letter that is sent to users when they are added to the organization. See [Adding Users, Enrolling Devices](#): Welcome New Users to *ZENworks Mobile Management*.


Tips on Customizing and Using Policy Suites

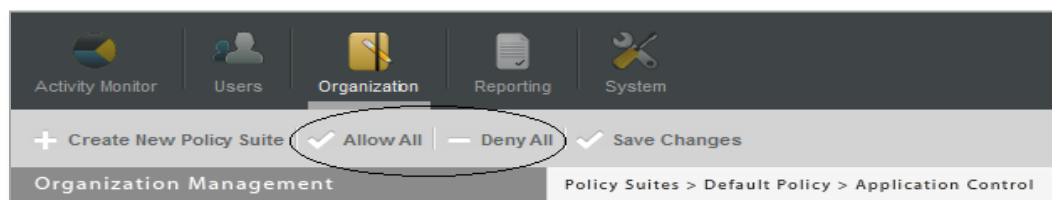
- The Policy Suite configuration pages can display the device platforms that support the policy. Select device platforms to view from the drop-down list.



- The symbols displayed next to a policy represent the device platforms that support the policy. Hover over a symbol to view help text.

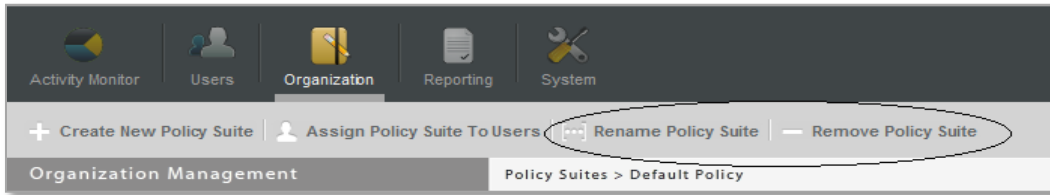


- Click the  symbol to access the Device Platform Functionality table from the dashboard. This table gives descriptions of each policy and details the functionality across each device platform. The document is also available via the ZENworks Mobile Management documentation portal. [Device Platform Functionality](#)
- You can use **Allow All** and **Deny All** buttons in a category to easily allow or deny all settings for corporate and individual devices simultaneously.

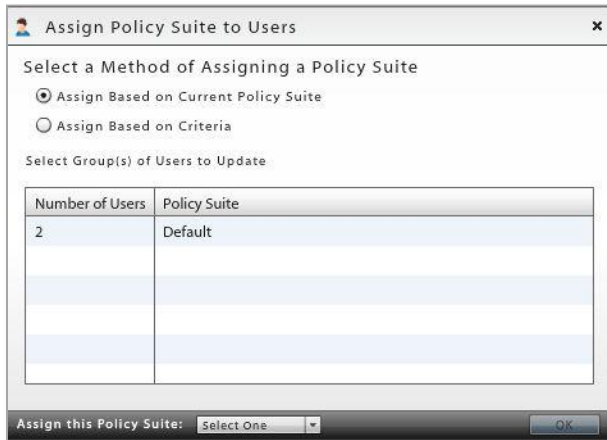
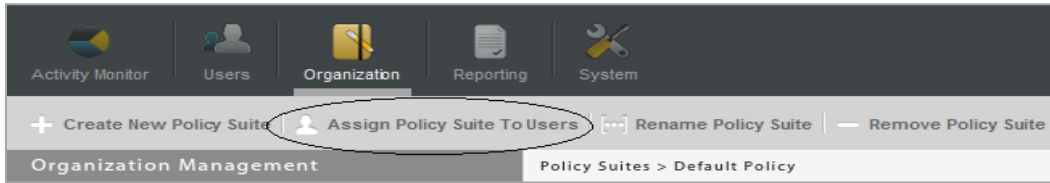


- Some policies determine the options available for other policies. For example, Allow Browser in the Device Control section must be enabled if you plan to enable Allow Safari for iOS devices.
- You must specify a policy suite when you add a user. Users added by import methods all have the same policy suite. Users added to the system via hands-off enrollment are assigned the default policy suite.
- You can change an individual user's policy suite in his or her *User Profile*.

- You can rename or remove a Policy Suite.



- You can select users by criteria and assign or change the group's policy suite by using the **Assign Policy Suite To Users** option. Selection criteria includes policy suite, device connection schedule, device model, ownership, device platform, and custom columns.



Device Connection Schedules

The device connection schedule determines the frequency at which devices connect with the *ZENworks Mobile Management* server. The schedule controls when the devices send statistics and can also control when the server sends updates (if the direct push setting is disabled). Regulating the interval at which devices connect should be considered carefully to minimize the device battery depletion.

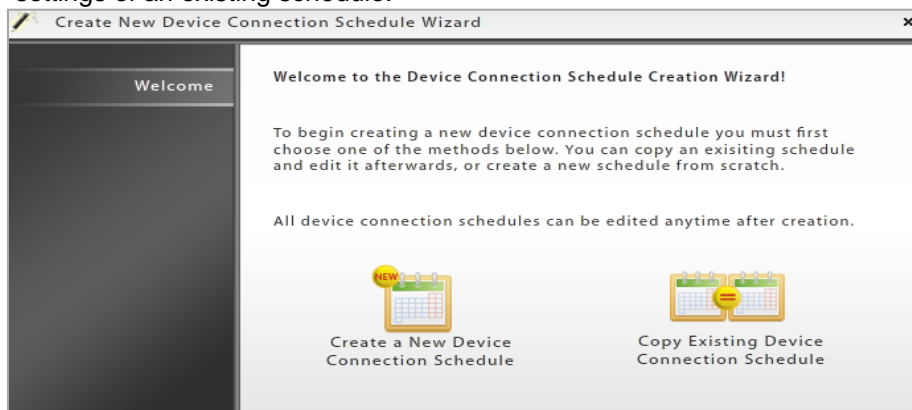
Schedules defined here do not affect ActiveSync synchronization of email/PIM. The device connection schedule controls only the synchronization frequency of *ZENworks Mobile Management* data, such as device statistics, location, and audit tracking data.

Creating Device Connection Schedules

- A wizard guides you through setting up of an organization's connection schedules.
- Multiple schedules can exist and each user (device) can be assigned the appropriate schedule.
- The wizard allows an administrator to quickly create a new device connection schedule or copy an existing schedule. If a schedule is copied, the administrator can use the *Device Connection Schedule Editor* to customize the settings associated with the new schedule.
- Each schedule can be customized for corporate and individual users.

Create a Device Connection Schedule

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. Select the **Device Connection Schedules** icon.
3. Click the **Create New Device Connection Schedule** option.
4. Choose a method for creating a connection schedule:
 - **Create a New Device Connection Schedule** - Create the initial schedule by using the system defaults.
 - **Copy Existing Device Connection Schedule** - Create the initial policy suite by copying the settings of an existing schedule.



5. Define the following settings for Corporate and Individual devices:

- Monday through Sunday Peak Connect Times
- Peak Connect Interval
- Require Direct Push for Peak Times
- Off-peak Connect Interval
- Require Direct Push for Off-peak Times

Define Corporate Peak Connection Times

| | | | | |
|-----------|-------------------------------------|---------|----|---------|
| Monday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Tuesday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Wednesday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Thursday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Friday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Saturday | <input type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Sunday | <input type="checkbox"/> | 8:00 AM | to | 5:00 PM |

Peak Connect Interval: 30 Minutes Off-peak Connect Interval: 60 Minutes

Require Direct Push for Peak Times Require Direct Push for Off-peak Times

Back Next

Peak Connection Times - The times you define in the schedule grid designate *Peak Connection Times*. Anything that falls outside the peak schedule is off-peak connection time.

Peak and Off-peak Connect Intervals - A schedule's *Peak and Off-peak Connect Intervals* define the frequency at which devices connect with the *ZENworks Mobile Management* server. Peak time are periods during which device usage is consistently higher than average. Conversely, off-peak times are periods during which device usage is consistently lower than average. Consider the following:

- To accommodate the higher traffic, set peak connect intervals at lower values (initiating more frequent connections) than off-peak connect intervals.
- Lower connect intervals increase the efficiency of the *ZENworks Mobile Management* Compliance Manager, since devices report device statistics more frequently allowing the server to detect non-compliance sooner.
- Avoid setting intervals so low that they significantly affect device battery depletion.

Require Direct Push - The *Require Direct Push* setting determines whether updates from the server, such as security commands, are synchronized immediately or during the next scheduled connection. If this setting is enabled, commands from the server sync to the device as soon as they are issued. Synchronizations from the device still occur according to the scheduled connect interval and are not affected by this setting.

When user devices are in Direct Push mode, remote Wipe commands sent from the server sync immediately, regardless of whether or not *Require Direct Push* is enabled.

Editing Device Connection Schedules

To edit an existing device connection schedule:

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. Select the **Device Connection Schedules** icon.
3. From the menu panel, select the schedule you want to change.
4. Select the **Corporate** or **Individual** schedule.
5. Edit the settings and click **Save Changes**.

Corporate Peak Device Connection Schedule

Device Connection Schedules Govern ZENworks App Connections Only

| | | | | |
|-----------|-------------------------------------|----------|----|----------|
| Monday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Tuesday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Wednesday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Thursday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Friday | <input checked="" type="checkbox"/> | 8:00 AM | to | 5:00 PM |
| Saturday | <input type="checkbox"/> | 12:00 AM | to | 12:00 AM |
| Sunday | <input type="checkbox"/> | 12:00 AM | to | 12:00 AM |

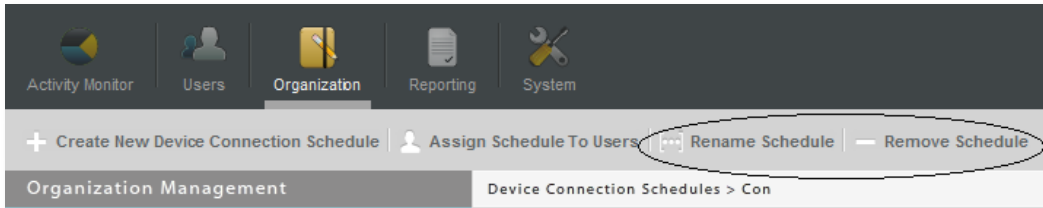
Peak Connect Interval: Minutes Off-peak Connect Interval: Minutes

Require Direct Push for Peak Times Require Direct Push for Off-peak Times

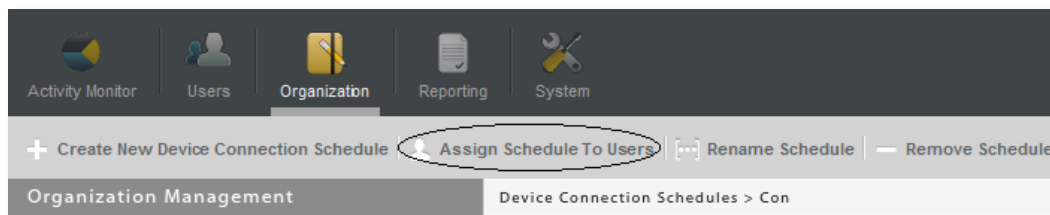
Note: Times extending into next day are allowed, but the next day's start time must be after the preceding day's end time.

Tips on Using Device Connection Schedules

- You must specify a device connection schedule when you add a user. Users added by import methods all have the same device connection schedule. Users added to the system via hands-off enrollment are assigned the default device connection schedule.
- You can rename or remove a device connection schedule.



- You can change an individual user's device connection schedule in his or her *User Profile*.
- You can select users by criteria and assign or change the group's device connection schedule by using the **Assign Schedule To Users** option.



Assign Device Connection Schedule to Users

Select a Method of Assigning a Device Connection Schedule

Assign Based on Current Device Connection Schedule

Assign Based on Criteria

Select Group(s) of Users to Update

| Number of Users | Device Connection Schedule |
|-----------------|----------------------------|
| 3 | Default Connection |
| | |
| | |
| | |
| | |

Assign This Schedule: Select One OK

Assigning a Device Connection Schedule