

Certificate Management

ZENworks® Mobile Management 3.2.x

September 2015

Novell.



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 © 2012-15 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

Setup and Requirements	4
Establishing a Certificate Authority	7
Creating a Certificate Template	9
Issuing Certificates	11
Authenticating Users for ActiveSync Server Access	11
Authenticating Android Device Users for Wi-Fi Access	11
Authenticating iOS Device Users for Wi-Fi Access	12
Authenticating iOS Device Users for VPN Access	12
The Certificate Grid	13
Customize the Certificates Grid	14
Search the Certificates Grid.....	14
View the Certificate Details	15
Revoke a Certificate.....	15
Re-Issue a Certificate	16

Setup and Requirements

Purpose and Description

System administrators can configure the *ZENworks Mobile Management* server to use a Microsoft Active Directory Certificate Authority. Enterprise certificates generated with this method can be used for:

- Authentication of users with Android KNOX and iOS devices accessing ActiveSync servers - when *ZENworks* is configured so that it does not proxy ActiveSync traffic, devices that retrieve email can be assigned a certificate for authenticating against the ActiveSync Server.
- Authentication of users with Android and iOS devices for Wi-Fi access.
- Authentication of users with iOS devices for access through a virtual private network (VPN).

Certificates from Outside Sources

Certificates for resources other than those listed above can be uploaded to the *ZENworks Mobile Management* server from the dashboard by an administrator or via the *ZENworks Mobile Management* Desktop User Self-Administration portal by a user. Users can then install the certificate on devices using the *ZENworks Mobile Management* Mobile User Self-Administration portal. The *ZENworks Mobile Management* server supports .cer, .pfx, or .p12 format certificates. Certificates obtained from *VeriSign™* have been tested and verified as functional. Certificates obtained from other certificate authorities can be functional if the device platform recognizes the certificate authority as trusted. See the [User Management Guide - User Information: Certificates](#) for more information on uploading certificates from outside sources.

Configuring Certificate Management in ZENworks Mobile Management

ZENworks Mobile Management can be configured to act as an enrollment agent in conjunction with an existing enterprise deployment of Microsoft Active Directory Certificate Services. When you configure a Certificate Authority in the administration dashboard, the ZENworks server is able to establish a connection with the Active Directory Certificate Authority through which it can obtain an enrollment agent certificate, create certificate templates, and submit requests for certificates on behalf of Android or iOS users.

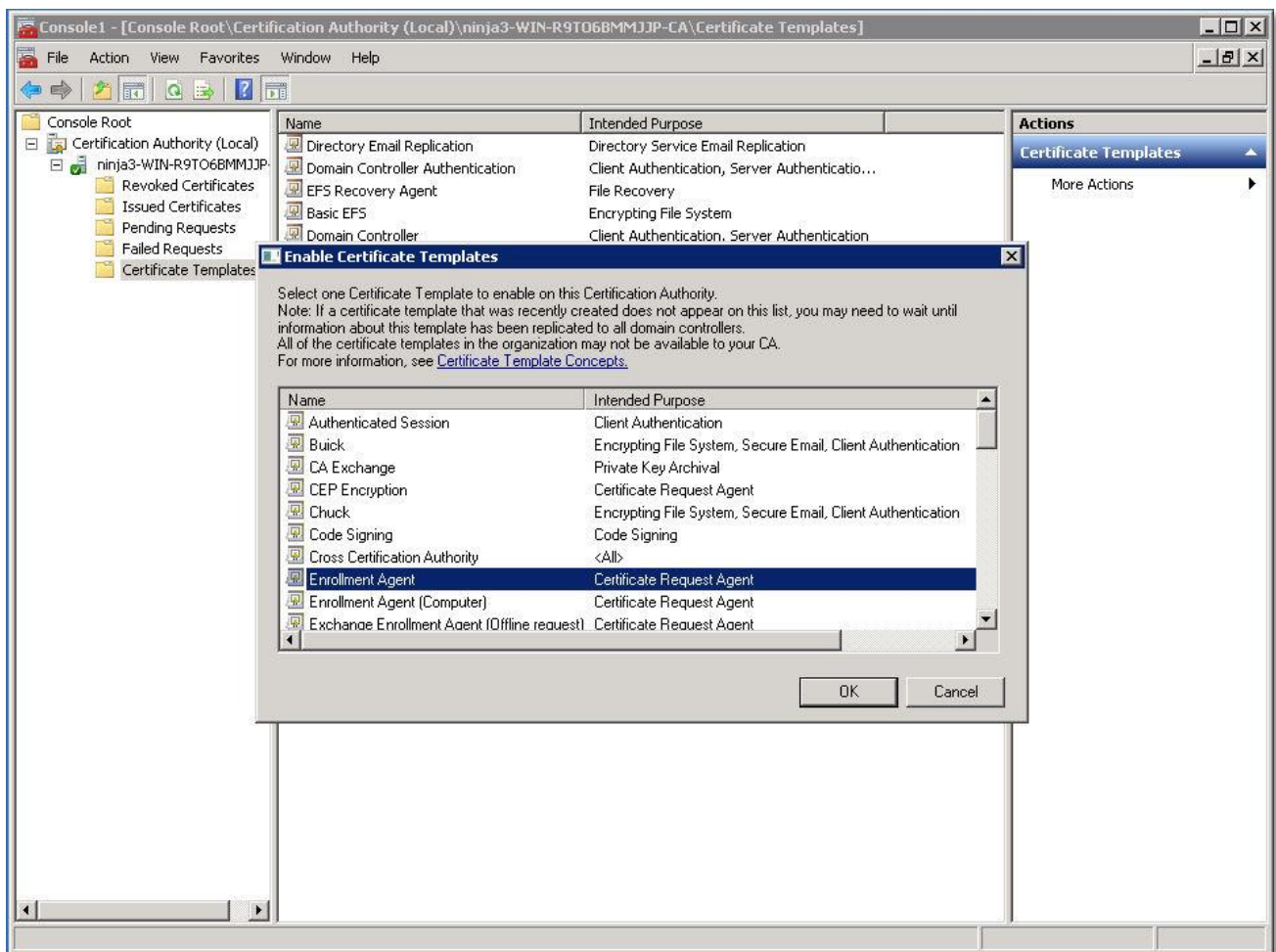
Certificate Templates are created in the *ZENworks* dashboard and are associated with the ActiveSync server, iOS or Android Wi-Fi, or iOS VPN corporate resources. When these resources are assigned to a user, the Certificate Authority uses the template to generate a certificate for the user.

In order to apply a Certificate Template to the ActiveSync server resource, the ActiveSync proxy option must be disabled. From the dashboard navigate to **System > Organization Settings** and remove the mark from the checkbox next to **Proxy ActiveSync Traffic by Default**.

Requirements

- The *ZENworks Mobile Management* server must be a member of the same Active Directory domain as the Certificate Authority host server.
- *ZENworks Mobile Management* user accounts must have the domain specified in their user record.
- The *ZENworks Mobile Management* server communicates with the Certificate Enrollment Policy Web Service and the Certificate Enrollment Web Service features. These features must be configured to use the Username and Password. (aka Basic Authentication).

- When configured to perform certificate management tasks, *ZENworks Mobile Management* acts as an enrollment agent on behalf of the Active Directory users in your domain. In order for *ZENworks Mobile Management* to do so, it must first have an Enrollment Agent certificate provisioned. This certificate is requested when saving the Certificate Authority definition in the administration dashboard. In order for this to succeed, you need to make sure that the Enrollment Agent certificate template is enabled and available for issuing by the Certificate Authority. To do this:
 - Open the Microsoft Management Console (MMC) on the CA server (Windows + r). Type *mmc* in the pop-up.
 - Add the Certificate Authority snap-in by selecting **File > Add/Remove Snap-in**. Select **Certification Authority** and choose **Local**.
 - From there navigate to the **Certificate Templates** portion. Right clicking will allow you to add a template to issue. Select the **Enrollment Agent** template and confirm that it is added to the list.
 - Administrators should wait approximately 10 minutes before adding the CA to the dashboard.



- Additionally, because the Certificate Authority is the issuer of the Enrollment Agent certificate, you need to ensure that the Certificate Authority's trusted root certificate is installed on the *ZENworks Mobile Management* machine. To do so:
 - a. Go to https://<CA_ServerAddress>/certsrv/certcarc.asp
 - b. Select **Download CA Certificate** and save the .cer file.
 - c. Run Microsoft Management Console (Windows + r) as Administrator.
 - d. In MMC, select **File > Add/Remove Snap-in**.
 - e. Add **Certificates** snap-in for local computer account.
 - f. Expand the *Certificates* tree.
 - g. Right click on **Third-Party Root Certificate** and select **All Tasks > Import**.
 - h. Import the downloaded certificate.

- If the certificate authority is known by different names, ensure that the IIS server's default HTTPS binding is configured to use the certificate minted for the full DNS name of the device in the domain.

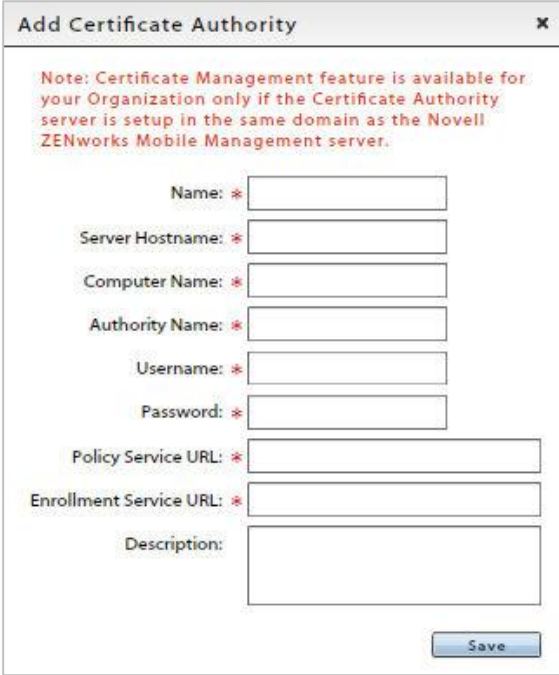
Recommendation

- On the *ZENworks Mobile Management* server, set Application Pool as your Anonymous Logon user.
 - a. Open IIS Manager and select Default Web Site.
 - b. Select Authentication in the IIS section.
 - c. Select Anonymous Authentication and click 'Edit...' from the right hand column.
 - d. Verify that the Application Pool Identity radio button is selected.

Establishing a Certificate Authority

The Certificate Authority (CA) server must be set up in the same domain as the *ZENworks Mobile Management* server. Once CA server setup has been completed, you can create a Certificate Authority object in the dashboard that contains the necessary parameters for the *ZENworks Mobile Management* server to communicate with the Certificate Authority web service.

1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > Certificate Management > Certificate Authorities**.
2. Click the **Add Certificate Authority** button.
3. Enter a **Name** by which to identify the certificate authority. This will display in the *ZENworks* dashboard.



Add Certificate Authority [X]

Note: Certificate Management feature is available for your Organization only if the Certificate Authority server is setup in the same domain as the Novell ZENworks Mobile Management server.

Name: *

Server Hostname: *

Computer Name: *

Authority Name: *

Username: *

Password: *

Policy Service URL: *

Enrollment Service URL: *

Description:

Save

4. Enter the connection parameters for the certificate authority server.

Server Hostname	Host name of the Windows server where the certificate authority is set up. In most environments communications with the certificate web services use TLS, so this must be configured to use the same DNS name as the subject name for the certificate that is bound to the IIS site hosting these services.
Computer Name	Name of the machine running the Certificate Authority; found under <i>My Computer > Properties</i> . In some cases, this is identical to the Server Hostname.
Authority Name	Name of the certificate authority specified during configuration in the Windows server. In a default installation, this is <DOMAIN>-<SERVER>-CA.
Username/Password	Authentication credentials required by the Windows server hosting the certificate authority. (Use Domain Admin credentials or credentials created for a user in the Domain Admin group.)
Policy Service URL	The URL of the installed Certificate Enrollment Policy Web Service. Example: https://<HostName>/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP.
Enrollment Service URL	The URL of the installed Certificate Enrollment Web Service. Example: https://<HostName>/<AuthorityName>_CES_UsernamePassword/service.svc/CES.

5. In the **Description** field, enter information describing the certificate authority.
6. Click **Save**. A test connection will run to verify the connection to the certificate authority server. An enrollment agent certificate is generated.

Note: If you see a message regarding an error while adding your certificate authority to the MDM server, you may need to perform the following tasks:

- a. Change the Application Pool Identity on the *ZENworks Mobile Management* server.
 - a. Verify that the Application Pool has been set as your Anonymous Logon user. See the [Recommendation](#) above.
 - b. Open IIS Manager and select Application Pools.
 - c. Select DefaultAppPool and click 'Advanced Settings...' from the right hand column.
 - d. Under Process Model select Identity and click the '...' button to edit.
 - e. Under Built-in Account, select LocalSystem and click 'Ok.'
 - f. Click 'Ok' again to close the Advanced Settings dialog.

Creating a Certificate Template

The Certificate Template is used by the Certificate Authority to generate certificates.

Certificate Templates can be associated with the ActiveSync server, iOS or Android Wi-Fi, or iOS VPN corporate resources. When these resources are assigned to a user, the Certificate Authority uses the template to generate a certificate for the user.

When a certificate template is added/edited/deleted in the *ZENworks* dashboard it is added/updated/deleted on the certificate authority server. Additionally, it is configured as a template that the Certificate Authority can issue.

Helpful Information:

- A Certificate Authority must be set up before you create a template, as every template must be associated with a CA.
 - When a template has been newly created or updated, administrators should wait approximately 10 minutes before associating the template with a corporate resource so that the certificate authority has sufficient time to process it.
1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > Certificate Management > Certificate Templates**.
 2. Click the **Add Certificate Template** button.

3. Enter a **Name** by which to identify the Certificate Template.

The screenshot shows the 'Add Certificate Template' dialog box. It includes the following fields and options:

- Name:** A text input field with a red asterisk indicating it is required.
- Subject:** Radio buttons for 'Build Subject' (selected) and 'Supply Subject'.
- Subject Format:** A dropdown menu currently set to 'Common Name'.
- Include e-mail name in subject:** An unchecked checkbox.
- Certificate Authority:** A dropdown menu showing 'Select One...'.
- Auto Re-Issue:** An unchecked checkbox.
- Key Type:** A dropdown menu showing 'Select One...'.
- Key Size:** A dropdown menu showing 'Select One...'.
- Validity (Days):** A spin box set to 365.
- Re-Issue Period (Days):** A spin box set to 7.
- Description:** A large text area.

A red warning message is displayed: "Auto Re-Issue must be enabled for certificates to be re-issued." A "Finish" button is located at the bottom right of the dialog.

4. Supply the **Subject** value information that goes in to the certificate.

Choose **Build Subject** (recommended) and select Common Name or Fully Distinguished Name from the drop-down list. Choose whether or not to include the email name in the subject. If you choose Build Subject, then ZENworks Mobile Management will submit certificate requests using the <DOMAIN>\<USERNAME> format so that certificates are issued on behalf of the Active Directory user.

OR

Choose **Supply Subject** and enter the subject value, usually in the form O=Company Name, CN={username}, CN={emailaddress}

5. From the drop-down list, select a **Certificate Authority** with which to associate this template.
6. Mark the **Auto Re-Issue** checkbox if you want certificates generated from this template to be re-issued when the validity expires.
7. Select the **Key Type:** *Signing Key* or *Signing and Encryption Key*
8. Select the **Key Size:** *1024* or *2048*
9. Enter the **Validity** (in days) for the certificates generated from this template.
10. Enter the **Re-Issue Period** (in days). The certificate will be re-issued within this period of days prior to the end of the certificate's validity when *Auto Re-Issue* is enabled.
11. In the **Description** field, enter information describing the template.
12. Click **Finish**.

Issuing Certificates

Certificate Templates are associated with the ActiveSync server, iOS Wi-Fi, or Android Wi-Fi corporate resources. When these resources are assigned to a user, the certificate authority uses the template to generate a certificate for the user. When the certificate is synchronized to the device, the user must accept the certificate or trust the certificate authority.

Authenticating Users for ActiveSync Server Access

Note: In order to apply a Certificate Template to the ActiveSync server resource, the ActiveSync proxy option must be disabled. From the dashboard navigate to **System > Organization Settings** and remove the mark from the checkbox next to **Proxy ActiveSync Traffic by Default**.

When *ZENworks* is configured so that it does not proxy ActiveSync traffic, users with Android KNOX and iOS devices that retrieve email can be assigned a certificate for authenticating against the ActiveSync Server.

1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > Administrative Servers > ActiveSync Servers**.
2. Select an existing ActiveSync server from the left panel or add one by clicking *Add ActiveSync Server*.
3. Select a **Certificate Authority** and a **Certificate Template** from the drop-down lists.
4. Click **Save Changes**.

When *ZENworks* configures ActiveSync settings on an Android KNOX or iOS device, the user's certificate is deployed based on the certificate template selection.

Authenticating Android Device Users for Wi-Fi Access

1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > Android Corporate Resources > Wi-Fi Networks**.
2. Select an existing Android Wi-Fi network from the left panel or add one by clicking *Add New Android Wi-Fi Network*.
3. **Security Type** for the network must be *802.1x*.
4. For **EAP Method**, select *PEAP*, *TTLS*, or *TLS*.
 - a. For TLS, select a **Certificate Authority** and a **Certificate Template** from the drop-down lists. If a CA server is selected, but a certificate template is not, the CA server certificate is provided so that the device can trust it.
 - b. For PEAP or TTLS, select the **Certificate Authority** from the drop-down list.
5. Click **Save Changes**.

When *ZENworks* app configures the Wi-Fi settings on an Android or iOS device, the user's certificate is deployed based on the PEAP, TTLS, TLS EAP method settings.

Authenticating iOS Device Users for Wi-Fi Access

1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > iOS Corporate Resources > Wi-Fi Networks**.
2. Select an existing iOS Wi-Fi network from the left panel or add one by clicking *Add New iOS Wi-Fi Network*.
3. **Security Type** for the network must be *WEP Enterprise*, *WPA Enterprise*, or *Any Enterprise*.
4. Select a **Certificate Authority** and a **Certificate Template** from the drop-down lists.
If a CA server is selected, but a certificate template is not, the CA server certificate is provided so that the device can trust it.

Note: User name for Enterprise Wi-Fi authentication is set only for LDAP users. The user information is obtained from LDAP group assignment for the Wi-Fi resource.

5. Click **Save Changes**.

Authenticating iOS Device Users for VPN Access

1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > iOS Corporate Resources > VPNs**.
2. Select an existing iOS VPN from the left panel or add one by clicking *Add New VPN*.
3. **User Authentication** (or *Machine Authentication*) for the VPN must be *Certificate*.
4. Select a **Certificate Authority** and a **Certificate Template** from the drop-down lists.
If a CA server is selected, but a certificate template is not, the CA server certificate is provided so that the device can trust it.
5. Click **Save Changes**.

The Certificate Grid

The Certificate Grid lists all certificates generated using the Microsoft Active Directory Certificate Authorities, the users to whom they were issued, and the corporate resources for which the certificates were issued. A certificate can be re-issued or revoked from this grid.

From the *ZENworks Mobile Management* administrative dashboard, select **Organization > Certificate Management > Certificates**.

The screenshot displays the 'Certificates > Andrew Crown' page. At the top, there are buttons for 'Revoke Certificate' and 'Re-issue Certificate'. Below these is a search panel with fields for Username, Certificate Name, First Name, Last Name, Expiry Date, and Status. The main area shows a table of certificates with columns for Username, Certificate Name, Corporate Resource, Issue Date, Expiry Date, and Status. A 'Certificate Authority' dropdown is set to '192.168.21.55'. The 'Certificate Details' panel on the left shows information for the selected certificate: Andrew Crown, issued by 192.168.21.55, expires on 02/18/2016. The details include Organization, Country, Serial Number (1a00000b73937495cfe57a3a4000000000b7), Version (2), PKI Algorithm (SHA-1 with RSA), Key Size (1024), Status (Active), Certificate Template (Users), and Auto Re-Issue (Re-issues on 02/18/2016).

Username	Certificate Name	Corporate Resource	Issue Date	Expiry Date	Status
acrown	Andrew Crown	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
gcochenour2	gwen cochenour	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
gcochenour2	Users gwen cochenour	NinjaWifi (WiFi)	02/18/2015	02/18/2016	Active
acrown	Andrew Crown	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
swheat	Samuel Wheat	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
acrown	Andrew Crown	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active

Customize the Certificates Grid

- Select the Certificate Authority list you want to view from the drop-down list in the top right corner of the grid.
- Drag and drop column headings to reorder the columns.
- Click the heading of any column to sort the list by the information in that column. Sort in ascending or descending order.



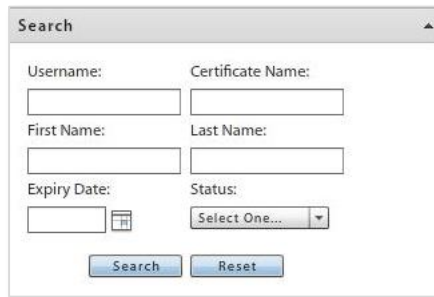
Certificates > Andrew Crown

Certificate Authority: 192.168.21.55

Username	Certificate Name	Corporate Resource	Issue Date	Expiry Date	Status
acrown	Andrew Crown	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
gcochenour2	gwen cochenour	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
gcochenour2	Users gwen cochenour	NinjaWifi (WiFi)	02/18/2015	02/18/2016	Active
acrown	Andrew Crown	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
swheat	Samuel Wheat	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active
acrown	Andrew Crown	192.168.21.55 (ActiveSync)	02/18/2015	02/18/2016	Active

Search the Certificates Grid

Search the list by Username, Certificate Name, First Name, Last Name, Expiry Date, or Status (select Active/Expired/Revoked from the drop-down list).



Search

Username: Certificate Name:

First Name: Last Name:

Expiry Date: Status:

View the Certificate Details

Select a certificate or user from the grid and view the details of the certificate from the panel to the left of the grid.

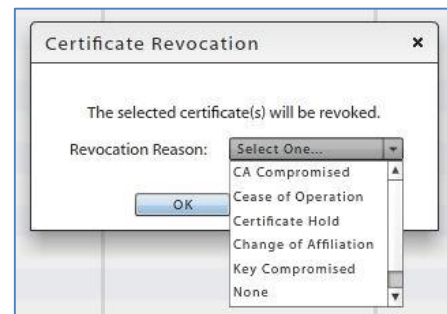


Revoke a Certificate

Certificates issued from the organization's certificate server via *ZENworks Mobile Management* can be revoked from the *ZENworks Mobile Management* dashboard via the Certificate Grid or the user's profile.

Once the Certificate Authority publishes a certificate revocation list, any resource (ActiveSync email, Wi-Fi, etc.) that uses the certificate for authentication will be inaccessible. Please note that in most cases, this does not occur immediately after an administrator has revoked the certificate. A user may still have access to resources for a short time after a certificate has been revoked.

1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > Certificate Management > Certificates**.
2. Select a certificate and click the **Revoke Certificate** button.
3. Select a **Revocation Reason**.



CA Compromised	Certificate authority (CA) that issued the certificate has been compromised
Cease of Operation	Client no longer qualifies for the certificate
Certificate Hold	Certificate has been placed on hold
Change of Affiliation	Subject value associated with the certificate has been modified
Key Compromised	Certificate's key has been compromised
None	No reason specified
Superseded	Certificate is no longer valid for the intended purpose or has been superseded by another certificate

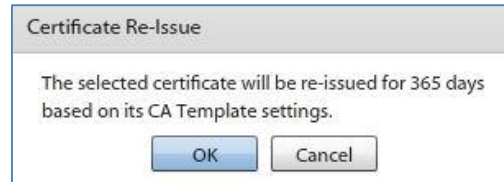
4. Click **OK** to confirm the revocation.

Re-Issue a Certificate

Certificates issued from the organization's certificate server via *ZENworks Mobile Management* can be re-issued from the Certificate Grid or from the user's profile.

When a certificate is re-issued it is valid for the number of days specified on the template from which the certificate was generated.

1. From the *ZENworks Mobile Management* administrative dashboard, select **Organization > Certificate Management > Certificates**.
2. Select a certificate and click the **Re-Issue Certificate** button.



3. Click **OK** to confirm the action.