NotifyMDM
Mobile Device Management

Certificate Management

This guide provides information on . . .

. . . Configuring the *NotifyMDM* server to use a Microsoft Active Directory Certificate Authority

. . . Using Certificates from Outside Sources

. . . Managing Certificates

Table of Contents

Setup and Requirements

Purpose and Description

System administrators can configure the *NotifyMDM* 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 *NotifyMDM* 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 *NotifyMDM* server from the dashboard by an administrator or via the *NotifyMDM* Desktop User Self-Administration portal by a user. Users can then install the certificate on devices using the *NotifyMDM* Mobile User Self-Administration portal. The *NotifyMDM* server supports .cer, .pfx, or .p12 format certificates. Certificates obtained from *VeriSign*^{TM} 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 Managing Users and Resources Guide - User Information: Certificates for more information on uploading certificates from outside sources.

Configuring Certificate Management in NotifyMDM

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

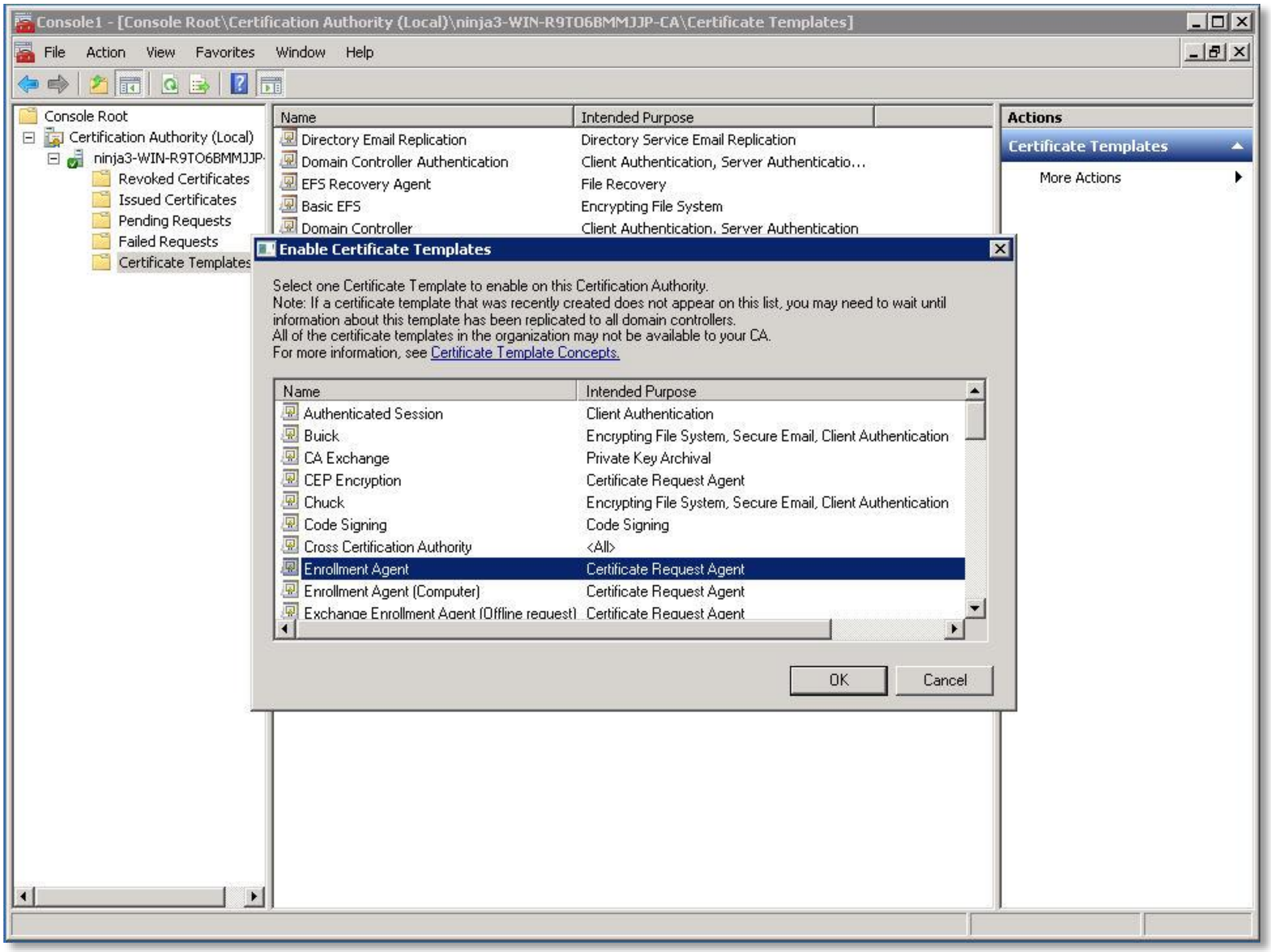
Certificate Templates are created in the *NotifyMDM* dashboard and are associated with the ActiveSync server, Android or iOS Wi-Fi, or iOS VPN corporate resources. When these resources are assigned to a user, the Certificate Authority uses the template to generate a certificate for the user.

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 Management*** > ***Organization Settings*** and remove the mark from the checkbox next to ***Proxy ActiveSync Traffic by Default***.

Requirements

- The NotifyMDM server must be a member of the same Active Directory domain as the Certificate Authority host server.
- NotifyMDM user accounts must have the domain specified in their user record.
- The NotifyMDM 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).

- Make the Enrollment Agent Template available to the Certificate Authority. A signing certificate will be generated from this template, which will be used to request certificates on behalf of Active Directory users without knowing passwords.
    - 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 computer**.
    - 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.



Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Authenticated Session	Client Authentication
Buick	Encrypting File System, Secure Email, Client Authentication
CA Exchange	Private Key Archival
CEP Encryption	Certificate Request Agent
Chuck	Encrypting File System, Secure Email, Client Authentication
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent

- Install the Certificate Authority's trusted root certificate on the *NotifyMDM* machine.
    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.

Recommendation

- On the *NotifyMDM* 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.

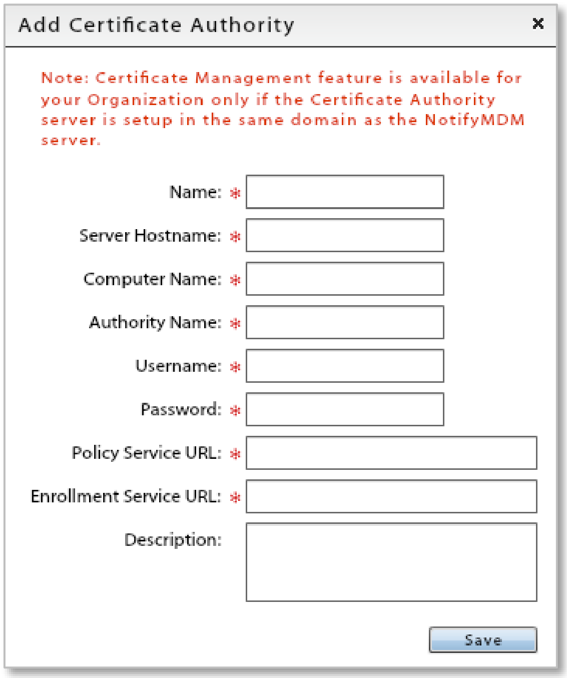
  c. Select Anonymous Authentication and click 'Edit...' from the right hand column.

  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 *NotifyMDM* server. Once CA server setup has been completed, the parameters necessary for the NotifyMDM server to communicate with the Certificate Authority web service must be specified in the dashboard. If the certificate authority configuration is deleted in the *NotifyMDM* dashboard it is deleted on the certificate authority server.

1. From the *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***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 *NotifyMDM* dashboard.



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

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 *My Computer* > *Properties*. 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 task:

   - Change the Application Pool Identity on the NotifyMDM 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.

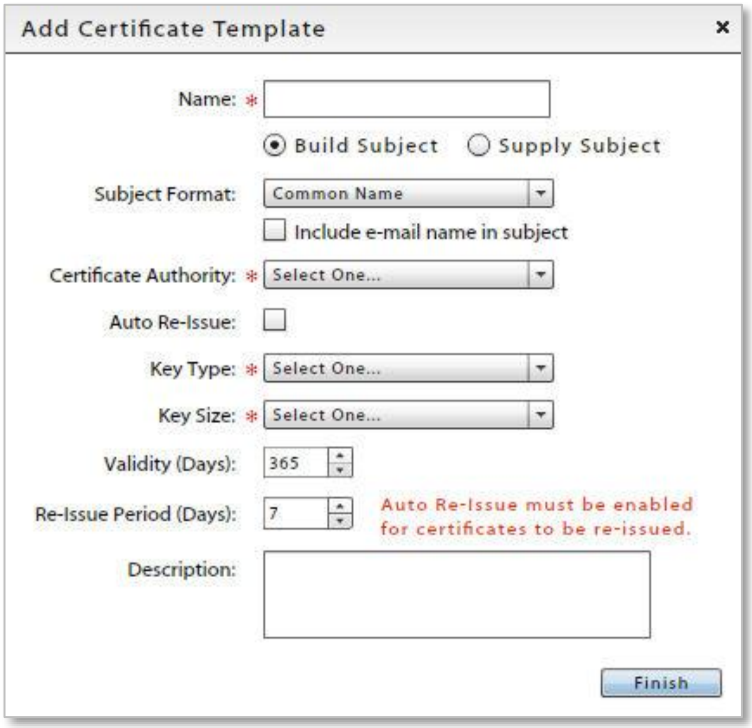
Certificate Templates can be associated with the ActiveSync server, Android or iOS Wi-Fi, or iOS VPN corporate resources. When these resources are assigned to a user, the Certificate Authority uses the template to generate a certificate for the user.

When a certificate template is added/edited/deleted in the *NotifyMDM* 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 *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***Certificate Management*** > ***Certificate Templates***.
2. Click the **Add Certificate Template** button.
3. Enter a **Name** by which to identify the Certificate Template.



Name: *
● Build Subject ○ Supply Subject
Subject Format: Common Name
□ Include e-mail name in subject
Certificate Authority: * Select One...
Auto Re-Issue: □
Key Type: * Select One...
Key Size: * Select One...
Validity (Days): 365
Re-Issue Period (Days): 7 Auto Re-Issue must be enabled for certificates to be re-issued.
Description:

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.

   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 Management*** > ***Organization Settings*** and remove the mark from the checkbox next to **Proxy ActiveSync Traffic by Default**.

When *NotifyMDM* 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 *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***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 *NotifyMDM* 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 *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***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 *NotifyMDM* 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 *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***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**.

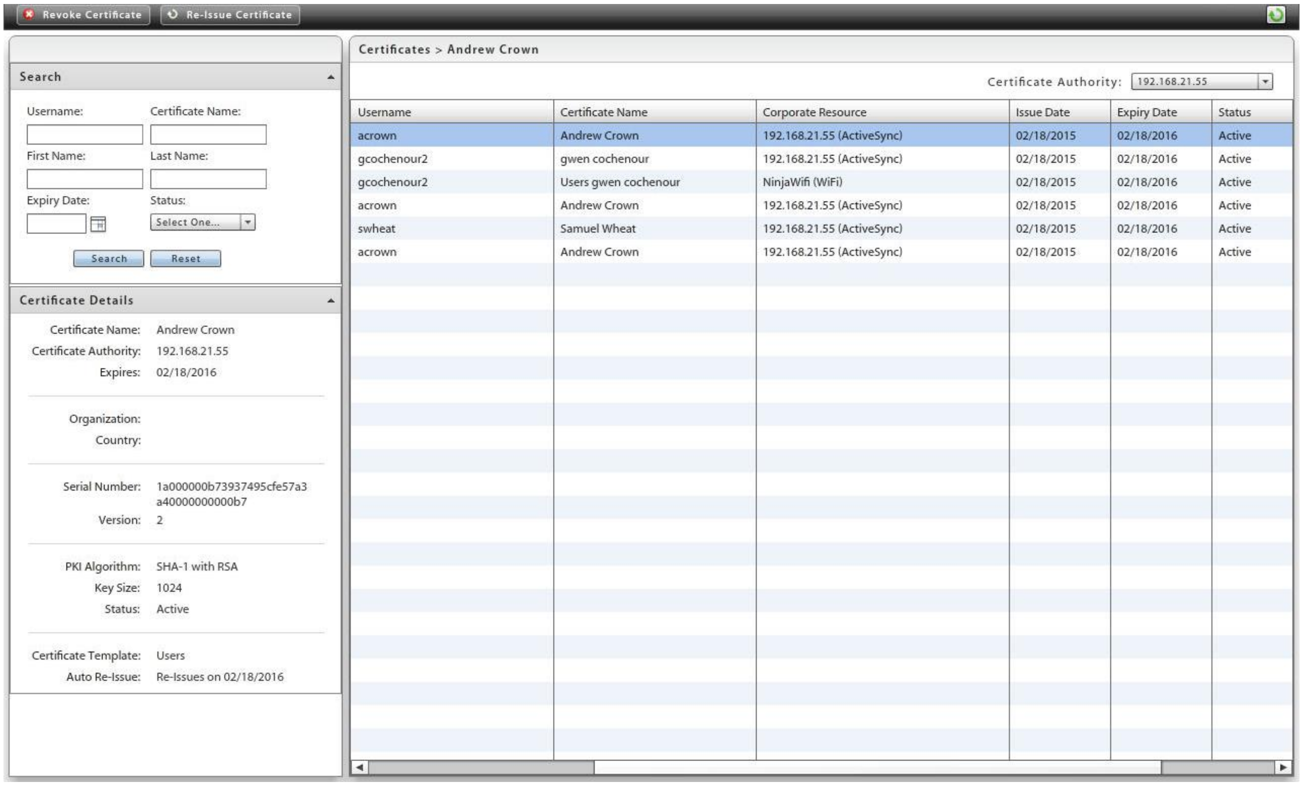
Authenticating iOS Device Users for VPN Access

1. From the *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***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 *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***Certificate Management*** > ***Certificates***.



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

Certificate Name: Andrew Crown
Certificate Authority: 192.168.21.55
Expires: 02/18/2016

Organization:
Country:

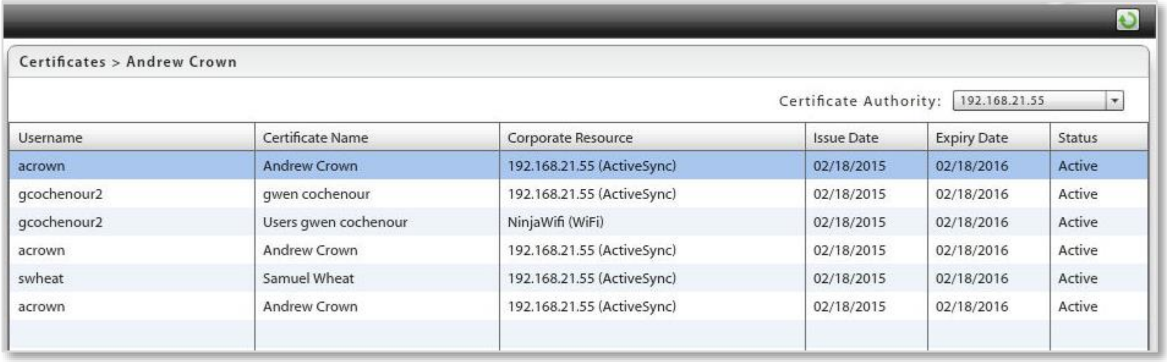
Serial Number: 1a000000b73937495cfe57a3a40000000000b7
Version: 2

PKI Algorithm: SHA-1 with RSA
Key Size: 1024
Status: Active

Certificate Template: Users
Auto Re-Issue: Re-Issues on 02/18/2016

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.



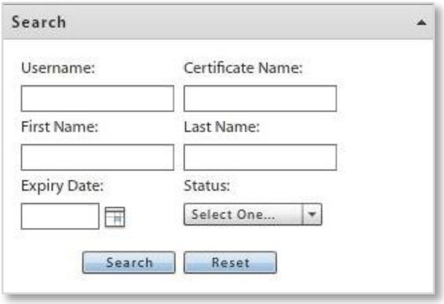
Certificates > Andrew Crown

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:

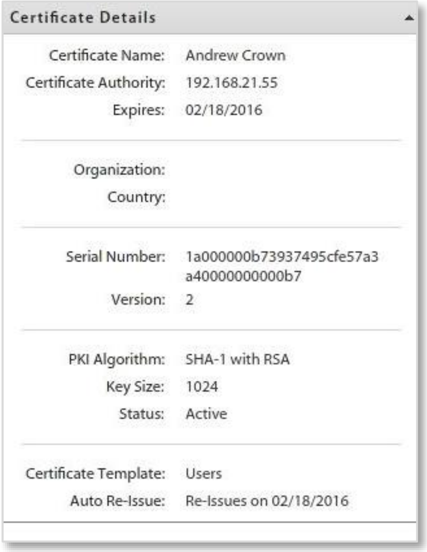
Last Name:

Expiry Date:

Status: Select One...

View 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.



Certificate Details

Certificate Name: Andrew Crown
Certificate Authority: 192.168.21.55
Expires: 02/18/2016

Organization:
Country:

Serial Number: 1a000000b73937495cfe57a3
a40000000000b7
Version: 2

PKI Algorithm: SHA-1 with RSA
Key Size: 1024
Status: Active

Certificate Template: Users
Auto Re-Issue: Re-Issues on 02/18/2016

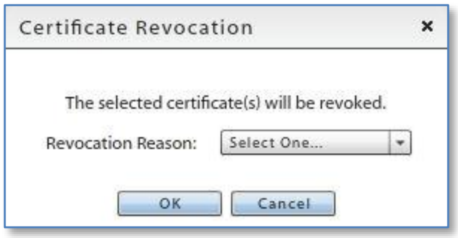
Revoke a Certificate

Certificates issued from the organization's certificate server via *NotifyMDM* can be revoked from the *NotifyMDM* 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.

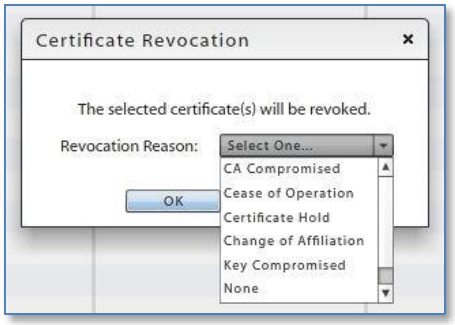
1. From the *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***Certificate Management*** > ***Certificates***.
2. Select a certificate and click the **Revoke Certificate** button.

3. Select a **Revocation Reason**.


Certificate Revocation

The selected certificate(s) will be revoked.

Revocation Reason: Select One...


Certificate Revocation

The selected certificate(s) will be revoked.

Revocation Reason: Select One...

Revocation Reason	Description
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

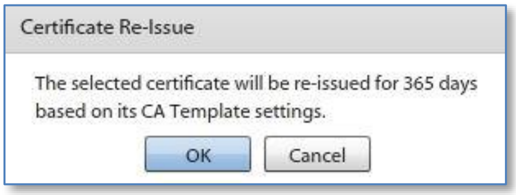
4. Click **OK** to confirm the revocation.

Re-Issue a Certificate

Certificates issued from the organization's certificate server via *NotifyMDM* 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 *NotifyMDM* administrative dashboard, select ***Organization Management*** > ***Certificate Management*** > ***Certificates***.
2. Select a certificate and click the **Re-Issue Certificate** button.


Certificate Re-Issue

The selected certificate will be re-issued for 365 days based on its CA Template settings.

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