ZENworks® 11 Support Pack 4

SSL Management Reference

October 2016

Novell®

Legal Notice

Contents

About This Guide

This *Novell ZENworks 11 SP4 SSL Management Reference* includes information to help you view and configure the certificate authority, and the certificates for ZENworks.

The information in this guide is organized as follows:

Audience

This document is intended for administrators or individuals who are concerned with tasks related to configuring and managing the certificate authority and certificates for ZENworks. To understand and perform the procedures described in this document, you should have a working knowledge of ZENworks, which includes experience in installation, system update and configuration of authentication Satellite Server procedures.

Feedback

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

Additional Documentation

ZENworks 11 SP4 is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 11 SP4 documentation website (http://www.novell.com/documentation/zenworks114/).

1 SSL Management

This chapter provides information on how to view, configure and manage the certificate authority and the certificates used by ZENworks Primary Servers and Authentication Satellite Servers. Based on how the certificate authority is initially installed and configured for ZENworks, the Certificates page will display the active CA. It will also display details of the certificates issued for servers (or other devices) within the zone, who they were issued by, and when they expire. Using the Certificates page, you can also change the certificate authority. This chapter includes the following sections:

Accessing the Certificate Details

To access the certificate details:

1. Log into ZENworks Control Center.
2. Click **Configuration >Certificates**. The following details are displayed:

   Zone Certificate Authority: This pane provides information about the certificate authority, the certificate server details (if the CA is internal), and the expiration date of the CA. It also enables you to perform operations such as Change CA, Move CA Role, Remint CA, Backup CA and Restore CA. For more information, see "Configuring the Certificate Authority" on page 7.

   ZENworks Server SSL Certificates: This pane provides information about the ZENworks Server certificates. Using this pane you can view details of the server certificates and also remint the certificates. For more information, see "Managing the Server Certificates" on page 16.

Configuring the Certificate Authority

When you install ZENworks Configuration Management for the first time, you are prompted to either create an internal Certificate Authority (CA) or provide the appropriate certificate information for an external CA. Based on how the certificate authority is initially installed and configured for ZENworks, the Certificates page will display the active certificate authority (CA). The active CA can be either internal or external.

- Internal Certificate Authority: Certificates are issued by a ZENworks server that is assigned the role of certificate authority.
- External Certificate Authority: Certificates are issued by an external server. The external server certificate can be issued by a subordinate CA or a root CA. ZENworks 11 SP4 and later versions also support the use of wildcard certificates.

This section provides information about the current Certificate Authority and it also provides information about the various operations that can be performed on the CA:

Internal Certificate Authority

Internal certificates are issued by a ZENworks server that has the CA role. ZENworks enables you to perform the following operations for an Internal CA:

- Move CA Role: When using an internal CA, the CA role is given to the first server that you have installed in the zone. This is listed as the Certificate Server. Using the Move Certificate Authority feature, you can move the CA role from one Primary Server to another Primary Server. For more information, see “Moving the CA Role” on page 13.
- Change CA: To change from an internal CA to another internal or external CA, or from an external CA to another external or internal CA. For more information, see “Changing the Certificate Authority” on page 9.
- Backup CA: To backup the certificate authority. For more information, see “Taking a Backup of the Certificate Authority” on page 13.
- Restore CA: To restore the backed up certificate authority. For more information, see “Restoring the Certificate Authority” on page 14.
- Remint CA: To remint the internal certificate authority. For more information, see “Reminting the Certificate Authority” on page 14.

External Certificate Authority

External certificates are issued by an external certificate authority (CA), for example, Verisign. Using ZENworks Control Center, you can change the current external CA to another external or internal CA.For more information, see Changing the Certificate Authority.

NOTE: It is recommended that you remint the certificate before it expires.

Viewing the Certificate Details

To view the certificate details, in the Zone Certificate Authority pane of the Certificates page, click the **View Certificate** button, the following information is displayed:

- Subject: The CA server to whom the certificate is issued.
- Issued by: The CA that issued the certificate.
- Valid from: The date and time from which the certificate is valid.
- Expires: The date and time at which the certificate will expire.
- Key length: The key length that was used to create the certificate.
- MD5 Fingerprint: The MD5 digest of the certificate data.

- SHA1 Fingerprint: The SHA1 digest of the certificate data.
- Certificate Status: Indicates whether the certificate is valid or has expired.

Changing the Certificate Authority

This feature enables you to change the current certificate authority (CA) to another internal or external CA.

- "Changing the CA to Internal" on page 9
- "Changing the CA to External" on page 10

Changing the CA to Internal

Using this feature, you can either change the existing external CA to an internal CA or you can change the existing internal CA to another internal CA.

When you change the CA, the Primary Server and Authentication Satellite Server certificates will get reminted automatically.

To change the CA to Internal:

1. In the Zone Certificate Authority pane, click the **Change CA** button.
2. In the Change Certificate Authority dialog box, confirm that you want to change the CA by selecting **Yes, I want to change the certificate authority**. The remaining fields are then activated.
3. From the drop-down list, select **Change to internal certificate authority**.
4. Specify the following information:
   - Certificate server: Browse and select the Primary Server, which must be the new CA.
   - Subject: Specify a subject name for the CA. By default, the zone name is displayed.
   - Key Length: Specify the key length.
   - Valid for (years): Specify the number of years for which the certificate should be valid. Specify a value between 1 to 10.
5. Select **Include any additional DNS names for each server**, if you want additional DNS names configured for the servers to be part of the Subject Alternative Name of their respective certificates.

   NOTE: The additional DNS names for a server can be configured by selecting the **Settings** tab of the device.

   ---
6. Click **Next**.
7. Specify the Certificate activation date and time. As a part of certificate activation, the new certificates will be effective and from then onwards, the old certificates will not be used for communication between devices.

   You can select any date that is prior to the expiry of the current CA. Ensure that you include adequate time for the associated system update to be applied on all the devices.

   IMPORTANT: If the certificate activation time passes before the system update is applied on the devices, these devices will not be able to communicate with Primary Servers on which the new certificate has already been activated. You will then need to run the Certificate Remint Tool. This tool can be downloaded from the following location `http://<ip of primary server>:<port>/`

`zenworks-setup`. This tool will be available for download on all the Primary Servers after the update is created and assigned. It will not be available when the certificate update is baselined and deleted.

If the CA has already expired, the activation time will be labeled as **Immediate** and you need to run the Certificate Remint Tool on all the devices. On the new CA server, the Certificate Remint Tool will be launched automatically.

8 Click **Finish**.

A message is displayed in the Zone Certificate Authority pane indicating that the Change CA operation has been initiated. As part of the Change CA process, ZENworks will create a system update and the content of the system update will be replicated to all the Primary Servers and Content Satellite Servers in the zone, based on the configured content replication schedule. The CRT will be created on the new CA server. On other Primary Servers, it will be created only after the SU is assigned, to ensure that the content is replicated.

You can click the **current replication status** link to view the list of servers along and their respective content replication statuses. After the replication is complete, the system update will be automatically assigned to all devices in the zone.

At any time before the auto assignment happens, you can assign the system update manually by clicking the **Assign Now** link even though the content is not replicated to all content servers. The system update will get assigned to all devices in the zone. For successful completion, we recommend that you ensure the content is available on the content servers before assigning the system update.

If the system update fails because the content is not available, you need to redeploy the system update on the failed devices.

IMPORTANT: As soon as the SU is assigned, the CRT will run on the new CA server, automatically. You need to remint the certificate on that server first and then all other Primary Servers should be reminted and after that the other devices, in any order.

The system update status for the Primary Servers and Authentication Satellite Servers can be viewed in the ZENworks Server SSL Certificate panel. The future certificate for these servers can be viewed from the **Options** column. The system update status for the other devices can be tracked from the System Updates page.

Changing the CA to External

Using this feature, you can either change the existing internal CA to an external CA or you can change the existing external CA to another external CA.

To change the existing CA to External:

1 In the Zone Certificate Authority pane, click the Change CA button.

2 In the Change Certificate Authority dialog box, confirm that you want to change the CA by selecting **Yes, I want to change the certificate authority**. The remaining fields are then activated.

3 From the drop-down list, select **Change to external certificate authority**.

4 Click **Browse** to select and upload the trusted root certificate provided by the external CA.

NOTE

- If it is an Intermediate CA, you need to provide the complete chain. ZENworks will use the root CA in the chain as the future CA.
- The supported certificate formats are .der, .cer, .crt, .p7b, .pem, .cert

- **IMPORTANT:** Changing a management zone to an intermediate CA can cause security policies and settings to fail for policies and settings originally configured in versions earlier than ZENworks 11 SP4.

  To avoid or resolve this issue when changing to an intermediate CA, see Security policies and security settings fail after changing zone to intermediate CA in the ZENworks 11 SP4 Troubleshooting Policy Deployment reference.

5 Click **Next**. The **Generate CSR** screen is displayed.

6 Select how you want to generate the CSR for each server:

- **I will generate a CSR for each server manually**: If you want to generate the CSR for each server manually, click **Next** and go to Step 7.
- **Let ZENworks generate a CSR automatically for each server**: If you want ZENworks to generate the CSR for all servers automatically, specify the following information and click **Next**:
  - **Organization**: Organization name
  - **Organization Unit**: Organizational unit name, such as a department or division
  - **City/Locality:** City name or location
  - **State/Province**: State or province name
  - **Country/region**: Country or region
  - **Key Length**: Specify the key length
  - **Include any additional DNS names for each server**: Select this option if you want the additional DNS names configured for the servers to be part of the Subject Alternative Name of their respective certificates.

    NOTE: The additional DNS names for a device can be configured by selecting the **Settings** tab of the Primary Server.

7 Specify the **Certificate activation date** and time.

You can select any date that is prior to the expiration date of the current CA. Ensure that you include adequate time for the associated system update to be applied on all the devices.

IMPORTANT: If the certificate activation time passes before the system update is applied on the devices, these devices will not be able to communicate with the Primary Servers on which the new certificate has already been activated. You will then need to run the Certificate Remint Tool on these devices.

If the CA has already expired, the activation time will be labeled as **Immediate,** and you will need to run the Certificate Remint Tool on all the devices, except the server on which the remint was initiated. On this server, the Certificate Remint Tool will be launched automatically.

IMPORTANT: As soon as the SU is assigned, the CRT will run on the new CA server automatically. You need to remint the certificate on that server first and then all other Primary Servers should be reminted and after that the other devices,in any order.

8 Click **Finish**.

A message is displayed in the Zone Certificate Authority pane indicating that the Change CA operation has been initiated. As part of the Change CA process, ZENworks will create a system update whose content will be replicated to all the Primary Servers and Content Satellite Servers in the zone, based on the configured content replication schedule. The Certificate Remint Tool (CRT) will be created on the server on which the remint operation was initiated. On other Primary Servers, it will be created only after the SU is assigned, to ensure that the content is replicated.

You can click the **current replication status** link to view the list of servers along and their respective content replication statuses. After the replication is complete, the system update will be automatically assigned to all devices in the zone.

At any time before the auto assignment happens, you can assign the system update manually by clicking the **Assign Now** link. This is useful if some of the content servers cannot replicate content due to various reasons.The system update will get assigned to all devices in the zone, ignoring the system update stages, if any, in the zone. For successful completion, we recommend that you ensure the content is available on the content servers before assigning the system update.

NOTE: If the system update fails because the content is not available, you need to redeploy the system update on the failed devices.

The system update status for the Primary Servers and Authentication Satellite Servers can be viewed in the ZENworks Server SSL Certificates panel. The **Options** column will enable you to download the CSRs, if any, and also view the future certificates. The system update status for the other devices can be tracked from the System Updates page.

9 If you selected the **I will generate a CSR for each server manually** option in Step 6, you need to generate the certificates for the Primary Servers and Authentication Satellite Servers manually. The certificate (the complete certificate chain) and the private key must then be placed in the remint repository folder of each of these servers:

- **On Windows:** `%zenworks_home%\remint-repo`
- **On Linux:** `/opt/novell/zenworks/remint-repo`

The file name has to be `server` and the extension can have the .der, .cer, .crt, .p7b, .pem, .cert extensions.The certificate can be `der` or `pem` encoded. The private key file name should be `key.der`.

If you selected the **Let ZENworks generate a CSR automatically for each server** option, you have to download the CSR for each server, get them signed by the CA, and import the future certificates using the **Import Certificate** action.

The activator will check the server certificate in the database and if it is imported into the database, it will serialize the server certificate as `server.cer` and place it in the remint repository:

- **On Windows:** `%zenworks_home%\remint-repo`
- **On Linux:** `/opt/novell/zenworks/remint-repo`

The CA certificate will be serialized in the same directory while applying the system update as `ca.cert`.

NOTE: The **Generate CSR** action can be used in the following scenarios:

- You selected the **I will generate a CSR for each server manually** option in Step 6, but you want to use ZENworks to generate CSRs for one or more devices. In this case, you will need to import the certificate for the device using the **Import Certificate** action.
- You selected the **Let ZENworks generate a CSR automatically for each server** option in Step 6, but you want to override the CSR for one or more devices. You can then use the newly generated CSR to request the future certificate from the CA.

To generate CSRs, select one or more servers, then click **Generate CSR** from the **Actions** menu. For more information, see Generating the CSR.

IMPORTANT: If you have 10.3.4 devices in the zone, ensure that all the managed devices are refreshed after all the Primary Servers' future certificates are available in the database. For all other devices, they need to be refreshed if the subject has been changed for any of the Primary Server certificates. If the devices are not refreshed, communication between the managed devices and the Primary Servers will break.

Canceling a Change CA

When you initiate a Change CA, in the Zone Certificate Authority pane, a message is displayed indicating that the Change CA operation has been initiated. This message includes a Cancel button. To cancel the Change CA operation:

1. Click the **Cancel** button. A dialog is displayed asking you to confirm that you want to cancel the operation.
2. After you confirm, a message is displayed indicating the progress of the cancel operation. If the cancel is successful, all the buttons in the Zone Certificate Authority pane are enabled. If the cancel operation fails, a failure message is displayed. You can clear the message and try the Cancel operation again.

   The Change CA operation is canceled successfully. The **Cancel** button will be disabled ten minutes before the activation time.

Moving the CA Role

When hardware has to be upgraded, or when its approaching end-of-life, or for various other reasons, you may need to select a new certificate authority for the zone. To move the certificate authority, you must select a new Primary Server that will serve as the certificate authority, henceforth, for the zone.

To move the certificate:

1. Click **Configuration** > **Certificates**.
2. Click the **Move CA Role** button.
3. In the Move Certificate Authority dialog, click the browse icon to select the Primary Server, which must be the new CA.
4. Select the required server from the list of Primary Servers.
5. Click **OK**.

   The **Certificate server** field in the Zone Certificate Authority panel will reflect the selected server as the new CA.

Taking a Backup of the Certificate Authority

Using the Backup CA feature you can backup the internal certificate authority for ZENworks.

To backup the internal CA certificate:

1. In the Zone Certificate Authority pane. click **Backup CA**.
2. Specify a **Passphrase**.

   This passphrase is required when you want to perform a restore. The passphrase should contain at least 10 characters.
3. Re-type the passphrase in the **Confirm** field.

4 Click **OK**.

   A zip file will be downloaded to the browser's default download directory or the user will be prompted to save the zip file in a particular directory.

Restoring the Certificate Authority

Using the Restore CA feature you can restore the internal certificate authority for ZENworks on to the same server from where you have created a backup or on to another server.

To restore the internal CA certificate:

1 In the Zone Certificate Authority pane, click **Restore CA**.

2 Click **Browse** to navigate to the backup file, then select it.

3 Click the browse icon to select the Primary Server to which you want to restore the backed up CA.

   After the CA is restored, the server will be assigned the CA role.

   If the CA was restored on the server that was used to backup the file, then the CA role will be assigned to the same server. However, if you selected a new server to restore the CA, the role will be moved to the new server.

4 Specify the **Passphrase** that was used while creating the backup.

5 Click **OK**.

   The **Certificate server** field in the Zone Certificate Authority panel will now reflect the chosen server as the new CA.

Reminting the Certificate Authority

If the certificate authority certificate expires, devices will be unable to establish an SSL connection to the server. It is important that before this occurs, you renew or remint the internal CA certificate and distribute this certificate to your managed devices.

When you remint the CA, the Primary Server and Authentication Satellite Server certificates will get reminted automatically.

NOTE: In the case of an internal CA, one of the Primary Servers in the zone will have the CA role. The certificates for all Primary Servers will be issued by the CA Server.

To remint the internal CA certificate:

1 In the Zone Certificate Authority pane, click **Remint CA**.

2 Confirm that you want to remint the CA by selecting **Yes, I want to remint the certificate authority**. The remaining fields are activated.

3 Specify the following information:

- Common name: Specify a common name for the CA. By default, the zone name is displayed.
- Key length: Specify the key length.
- Valid for (years): Specify the number of years for which the certificate should be valid. Specify a value between 1 to 10.

4 Select **Include any additional DNS names for each server**, if you want the additional DNS names configured for the servers to be part of the Subject Alternative Name of their respective certificates.

NOTE: The additional DNS names for a device can be configured by selecting the **Settings** tab of the device.

---

5 Specify the **Certificate activation date** and time.

You can select any date that is prior to the expiration of the current CA. Ensure that you include adequate time for the associated system update to be applied on all the devices.

IMPORTANT: If the certificate activation time passes before the system update is applied on the devices, these devices will not be able to communicate with Primary Servers on which the new certificate has already been activated. You will then need to run the Certificate Remint Tool on these devices.

If the CA has already expired, the activation time will be labeled as **Immediate,** and you will need to run the Certificate Remint Tool on all the devices apart from the new CA server. On the new CA server, the Certificate Remint Tool will be launched automatically.

6 Click **OK**.

A message is displayed in the Zone Certificate Authority pane, indicating that the Remint CA operation has been initiated. As part of the Remint CA process, ZENworks will create a system update, the content of which will be replicated to all the Primary Servers and Content Satellite Servers in the zone, based on the configured content replication schedule. You can click the **current replication status** link to view the list of servers along with their respective content replication statuses. After the replication is complete, the system update will be automatically assigned to all devices in the zone. The CRT will be created on the new CA server. On other Primary Servers, it will be created only after the SU is assigned, to ensure that the content is replicated.

At any time before the auto assignment happens, you can assign the system update manually by clicking the **Assign Now** link. The system update will get assigned to all devices in the zone. For successful completion, we recommend that you ensure that the content is available on the content servers before assigning the system update.

NOTE: If the system update fails because the content is not available, you need to redeploy the system update on the failed devices.

The system update status for the Primary Servers and Authentication Satellite Servers can be viewed in the ZENworks Server SSL Certificate panel. The future certificate for these servers can be viewed from the **Options** column. The system update status for the other devices can be tracked from the System Updates page.

IMPORTANT: If the devices are 10.3.4 make sure all the managed devices are refreshed after all the Primary Servers' future certificates are available in the database. For all other devices, they need to be refreshed if the subject has been changed for any of the Primary Server certificates. If the devices are not refreshed, communication between the managed devices and the Primary Servers will break.

Canceling a CA Remint

When you Initiate a CA remint, in the Zone Certificate Authority pane, a message is displayed indicating that the CA remint operation has been initiated. This message includes a **Cancel** button. To cancel the CA remint:

1. Click the **Cancel** button. A dialog is displayed asking you to confirm that you want to cancel the operation.
2. After you confirm, a message is displayed indicating the progress of the cancel operation. If the cancel is successful, all the buttons in the Zone Certificate Authority pane are enabled. If the cancel operation fails, a failure message is displayed. You can clear the message and try the Cancel operation again.

   The CA remint operation is canceled successfully. The **Cancel** button will be disabled ten minutes before the activation time. Though you cannot cancel the CA Remint, you can cancel the system-update for the device using the **Ignore Device** option from System Update page.

Managing the Server Certificates

The ZENworks Server SSL Certificates pane in ZCC enables you to view information about the SSL certificates that are issued to the ZENworks Primary Servers and Authentication Satellite Servers in the zone. Using this panel, you can view and remint certificates for one or more devices. The information that is displayed includes the following:

- Issued To: The server to which the certificate is issued. Click the server to view its details.
- Subject: The Fully Qualified Domain Name (FQDN) of the server to which the certificate is issued.
- Issued By: The CA that issued the certificate.
- Valid From - The date and time, in the user's time zone, from which the certificate is valid.
- Expires On: The date and time, in the user's time zone, on which the certificate expires.
- MD5 Fingerprint: The MD5 digest of the certificate data.
- SHA1 Fingerprint: The SHA1 digest of the certificate data.
- Certificate Status: Shows the status of the current certificate as active or expired. If a remint is in progress, the certificate-creation status is displayed. For more information, see Certificate Status.
- Options: Provides options to view the future certificate and download the CSR based on the remint operation that is in progress.
- Update Status: If a remint operation is in progress, the status of the associated system update is displayed.
- Version: The version of ZENworks installed on the servers.

This section provides the following information:

- "Certificate Status" on page 17
- "Reminting Server Certificates" on page 17
- "Canceling a Server Remint" on page 22

Certificate Status

When a server certificate remint is in progress, the certificate status can be any of the following:

For Internal Certificates:

- New certificate created - The future certificate is available.
- Creating certificate failed - An error occurred while creating the future certificate.

For External Certificates:

- CSR generated - The Certificate Signing Request (CSR) is generated for the future certificate. This status indicates that CSR is generated for the corresponding server and the administrator has to download the CSR using the download button and then get it signed by the external certificate authority. After receiving the new server certificate that corresponds with the CSR the administrator should import the certificate using ZENworks Control Center.
- CSR generation Failed - An error occurred while generating the CSR. In such a scenario, the administrator can manually select the server for which the CSR generation has failed and generate the CSR again, after correcting the reasons for failure, if any or redeploy the system update for the device.
- New certificate uploaded - The future certificate has been imported in to the database.

Reminting Server Certificates

If your server certificate expires, devices will be unable to establish an SSL connection to the server. It is important that before this occurs, you renew or remint the certificate and distribute this certificate to your managed devices.

- “Remint Server Certificates When the CA Is Internal” on page 17
- “Remint Server Certificates When the CA Is External” on page 19

If a server certificate has already expired, then a dialog box with the following error message is displayed:

```
"The following certificates are about to expire or have expired. You should update
the certificates as soon as possible to avoid a loss of communication between
devices and services.

<Name of the certificate> server certificate has expired".
```

For more information on reminting an expired server certificate, see A server certificate has expired in the Troubleshooting section.

Remint Server Certificates When the CA Is Internal

To renew or remint the internal server certificates, select one or more servers, then click **Remint Certificate**.

NOTE: Based on the operation(s) initiated from the Certificates page, the **Remint Certificate** option might not be enabled until these operations are complete. For example, when a Remint CA or Change CA is in progress, this option will not be available.

1. Confirm that you want to remint the certificate by selecting **Yes, I want to remint the certificate for this server**. The remaining fields are then activated.
2. Specify the **Common name** for the certificate.

   By default, the Fully Qualified Domain Name (FQDN) of the server is displayed. If you have selected multiple servers, or if the selected server has associated satellites, this field will not be displayed.
3. Specify the **Key length**.
4. Select **Include any additional DNS names for each server**, if you want the additional DNS names configured for the servers to be part of the Subject Alternative Name of their respective certificates.

   NOTE: If you selected a single server, the additional DNS names configured for this server are displayed. However, if there are no additional DNS names configured for the server, you cannot select this option. The additional DNS names for the device can be configured by selecting the **Settings** tab of the device.
5. Specify the **Certificate activation date** and time.

   You can select any date that is prior to the expiration of the current CA. Ensure that you include adequate time for the associated system update to be applied on all the devices.
6. Specify a name for the system update that will be created to remint the certificate.
7. Click **OK**.

   A message is displayed in the ZENworks SSL Certificates pane, indicating that the Remint Certificate operation has been initiated. As part of the Remint Certificate process, ZENworks will create a system update, the content of which will be replicated to all the Primary Servers and Content Satellite Servers in the zone, based on the configured content replication schedule. You can click the **current replication status** link to view the list of servers along with their respective content replication statuses. After the replication is complete, the system update will be automatically assigned to the selected devices.

   At any time before the auto assignment happens, you can assign the system update manually by clicking the **Assign Now** link. The system update will get assigned to the selected devices. For successful completion, we recommend that you ensure that the content is available on the content servers before assigning the system update. After clicking the Assign Now link, a warning message is displayed, with a **selected servers** link, when you click on this link, it will display a popup message with a list of the servers for which the remint has been initiated.

   NOTE: If the system update fails because the content is not available, you need to redeploy the system update on the failed devices.

   The system update status for the targeted servers can be viewed in the ZENworks Server SSL Certificate panel. The future certificate for these servers can be viewed from the **Options** column.

Remint Server Certificates When the CA Is External

To remint server certificates when the CA is external, you need to first deploy the Remint system update to the device, then allow ZENworks to generate the CSR, or manually generate the CSR. If you choose to manually generate the CSR, you will need to generate the CSR and then import the certificate to the device.

When you remint the server certificate, you need to get the server certificate issued by the current zone CA (root CA) or any subordinate CA of the current zone CA. If the certificate is issued by a subordinate CA, you need to provide the complete certificate chain.

This section includes the following information:

Reminting the Server Certificate

1. To renew or remint the external server certificates, select one or more servers, then click **Remint Certificate**.
2. Select how you want to generate the CSR for each server:
   - **I will generate a CSR for each server manually**: If you want to generate the CSR for each server manually, click **Next** and go to Step 3.
   - **Let ZENworks generate a CSR automatically for each server**: If you want ZENworks to generate the CSR for all the servers automatically, specify the following information, then click **Next**:
     - **Common name**: The Fully Qualified Domain Name (FQDN) of the server. If you have selected multiple servers, this field will not be displayed.
     - **Organization**: Organization name
     - **Organization unit:** Organizational unit name, such as a department or division.
     - **City/Locality** - City name or location
     - **State/Province**: State or province name
     - **Country/region**: Country or region. For example, US.
     - **Key Length**: Specify the key length
     - **Include any additional DNS names for each server**: Select this option if you want the additional DNS names configured for the servers to be part of the Subject Alternative Name of their respective certificates.

       NOTE: The additional DNS names for a device can be configured by selecting the **Settings** tab of the device.
3. Specify the **Certificate activation date** and time.

   You can select any date that is prior to the expiration of the server that has the earliest expiration date among the selected servers. Ensure that you include adequate time for the associated system update to be applied on all of the devices.
4. Specify a name for the system update that will be created to remint the certificate.
5. Click **Finish**.

A message is displayed in the ZENworks SSL Certificates pane, indicating that the Remint Certificate operation has been initiated. As part of the Remint Certificate process, ZENworks will create a system update which will be replicated to all the Primary Servers and Content Satellite Servers in the zone, based on the configured content replication schedule. You can click the **current replication status** link to view the list of servers along with their respective content replication statuses. After the replication is complete, the system update will be automatically assigned to the selected devices. The CRT will be created on the server on which the remint operation was initiated. On other Primary Servers, it will be created only after the SU is assigned, to ensure that the content is replicated.

At any time before the auto assignment happens, you can assign the system update manually by clicking the **Assign Now** link. The system update will get assigned to the selected devices. For successful completion, we recommend that you ensure that the content is available on the content servers before assigning the system update. After clicking the Assign Now link, a warning message is displayed, with a **selected servers** link, when you click on this link, it will display a popup message with a list of the servers for which the remint has been initiated.

NOTE: If the system update fails because the content is not available, you need to redeploy the system update on the failed devices.

The system update status for the targeted servers can be viewed in the ZENworks Server SSL Certificate panel. The **Options** column will enable you to download the CSRs, if any, and also view the future certificates.

6 If you selected the **I will generate a CSR for each server manually** option in Step 2, you need to generate the certificates for the Primary Servers and Authentication Satellite Servers manually. The certificate (complete certificate chain) and private key must then be placed in the remint repository folder on each of these servers.

- **On Windows:** `%zenworks_home%\remint-repo`
- **On Linux:** `/opt/novell/zenworks/remint-repo`

If you selected the **Let ZENworks generate a CSR automatically for each server** option, you have to download the CSRs for each of the servers, get them signed by the CA, and then import the future certificates using the **Import Certificate** action.

NOTE: The **Generate CSR** action can be used in the following scenarios:

- You selected the **I will generate a CSR for each server manually** option in Step 2, but you want to use ZENworks to generate CSRs for one or more devices. In this case, you will need to import the certificate for the device using the **Import Certificate** action.
- You selected the **Let ZENworks generate a CSR automatically for each server** option in Step 2, but you want to override the CSR for one or more devices. You can use the newly generated CSR to request the future certificate from the CA.

To generate CSRs, select one or more servers, then click **Generate CSR** from the **Actions** menu. For more information, see Generating the CSR.

Based on the operation(s) initiated from the Certificates page, the **Remint Certificate** option might not be enabled until these operations are complete.

After a remint has been initiated, the following **Actions** are enabled:

- **Generate CSR**: If you have selected the **I will generate a CSR for each server manually** option, you can use this action to generate the CSR. However, if you have selected the **Let ZENworks generate a CSR automatically for each server** option, you can use this action to override the CSR that was generated by ZENworks. To generate the CSR, select one or more servers, then click **Generate CSR** from the **Actions** menu. For more information, see Generating the CSR.

- Import Certificate: This option is available after a CSR has been generated for the selected server. After the CSR is submitted to the CA and the CA issues a new certificate, you can import the certificate to ZENworks using this action. To import the certificate, select the relevant server, then click **Import Certificate** from the **Actions** menu. For more information, see Importing the Certificate.
- Download CSRs to Zip File: This option is available if multiple servers are selected and CSRs are available for each of these servers. To download the CSRs, select the required servers, then click **Download CSRs to Zip File** from the **Actions** menu.

Generating the CSR

This feature enables you to generate Certificate Signing Requests (CSRs) for one or more devices.

When moving to an external CA, a CSR must be generated for each Primary Server or Satellite Server in the Zone. You can generate a CSR automatically for all servers in the zone, or you can generate it manually for each server, one at a time.

The Generate CSR action can be used in the following scenarios:

- You have selected the **I will generate a CSR for each server manually** option, but you want to use ZENworks to generate CSRs for one or more devices. In this case, you will need to import the certificate for the device using the Import Certificate action.
- You have selected the Let ZENworks generate a CSR automatically for each server option in Step 1, but you want to override the CSR for one or more devices. You can use the newly generated CSR to request for the future certificate from the CA.

NOTE: This feature is not available for Satellite Server versions that are prior to ZENworks 11 SP4.

To generate a CSR:

1. Log into ZENworks Control Center.
2. Navigate to **Configuration** > **Certificates**.
3. From the ZENworks Server SSL Certificates pane, select one or more servers.
4. Click **Actions > Generate CSR**.
5. Specify the following information:
   - **Common Name (CN):** The Fully Qualified Domain Name of the ZENworks Primary Server. For example, mail.novell.com. If you have selected multiple servers, this field will not be displayed.

     NOTE: This field is not displayed when multiple servers are selected.

   - **Organization (O):** Organization name.
   - **Organizational Unit (OU):** Organizational unit name, such as a department or division.
   - **City or Locality (L):** City name or location.
   - **State or Province (ST):** State or province name.
   - **Country or Region:** Two-letter country code or region. For example, US.
   - **Key length:** Specify the required key length.
6. Click **OK**.

   The CSR is generated and the status of the server is changed to reflect that the CSR is now available to download.

Importing the Certificate

This feature enables you to import the certificates into ZENworks, after you get the CSR signed by the certificate authority (CA).

To import the certificate:

1. Click **Browse**, then select the certificate.
2. Click **OK**.

   The selected certificate is imported to the database.

   The supported certificate formats are .pem, .der, and .p7b.

IMPORTANT: If the devices are 10.3.4 make sure all the managed devices are refreshed after all the Primary Servers' future certificates are available in the database. For all other devices, they need to be refreshed if the subject has been changed for any of the Primary Server certificates. If the devices are not refreshed, communication between the managed devices and the Primary Servers will break.

Canceling a Server Remint

When you initiate a server certificate remint, in the ZENworks SSL Certificates pane, a message is displayed indicating that the Remint Certificate operation has been initiated. This message includes a Cancel button. To cancel a server remint:

1. Click the **Cancel** button. A dialog is displayed asking you to confirm that you want to cancel the operation.
2. After you confirm, a message is displayed indicating the progress of the cancel operation. If the cancel is successful, all the buttons in the Zone Certificate Authority pane are enabled. If the cancel operation fails, a failure message is displayed. You can clear the message and try the Cancel operation again.

   The Remint Server Certificate operation is canceled successfully. The **Cancel** button will be disabled ten minutes before the activation time. Though you cannot cancel the Server Remint, you can cancel the system-update for the device using the **Ignore Device** option from System Update page.

A Troubleshooting

The following sections provide solutions to the problems you might encounter while using the SSL Management feature.

A Windows agent is not able to launch the CertificateActivator executable

Source: ZENworks; SSL Management.

Explanation: When you initiate a remint, a system update is assigned to all devices, and the future security files are created. At the time of activation, the agent launches the `CertificateActivator.exe` to activate the certificate. This executable file is not launching due to an issue with Windows.

Action: You need to apply a hot fix (http://support.microsoft.com/en-us/kb/2701373), and restart the device. During the next agent refresh the CertificateActivator executable will get launched.

When the Certificate Remint Tool is downloaded, the update packages are treated as malicious software

Source: ZENworks; SSL Management.

Explanation: When you download the Certificate Remint Tool, the update packages are treated as malicious software by the anti-virus software. Consequently, the update abruptly stops.

Action: Do the following on the managed device where you want to install the Certificate Remint Tool:

1. Manually add *System_drive*:\windows\novell\zenworks to the exclusion list of the anti-virus software installed on the managed device.
2. Download the Certificate Remint Tool.

Managed device that was re-imaged during remint is not communicating with the Primary Server

Source: ZENworks; SSL Management.

Explanation: After a remint system update is completed on a device, before the activation date, if the device is re-imaged and registered, it will not be able to communicate with the Primary Server, post activation. This is because the new server certificate is already activated on the Primary Server and the device does not have the new certificate because the system update is not sent to the device again.

Action: You need to unregister and re-register the device. If the system update is not yet baselined, you can use the certificate remint tool to run the system update again.

The activator for a failed certificate activation will only be triggered after an agent refresh

Source: ZENworks; SSL Management.

Explanation: When certificate activation fails due to any error, you have to wait till the next agent refresh to happen for the activator to get triggered.

Action: You can trigger the activator before the next refresh by running the zac `refresh` command. For more information, see the Status Commands in the *ZENworks 11 SP4 Command Line Utilities Reference*.

The Certificate Remint Tool fails on a device when the Primary Server to which it is registered, has a certificate chain

Source: ZENworks; SSL Management.

Explanation: If the device is registered with a server whose certificate is signed by an intermedidate CA and you try to download the Certificate Remint Tool from a server which has a certificate with lesser number of chains than the registered server, you will receive the following error: `CA certificate subject from the CA Certificate chain does not match server certificate issuer.`

Action: You need to download the Certificate Remint Tool from the registered Primary Server or from a Primary Server that has the most number of chains.

The Certificate Remint Tool is not created on Primary Servers

Source: ZENworks; SSL Management.

Explanation: The Certificate Remint Tool might not be created on all Primary Servers if the content is not replicated on those servers.

Action: Based on the scenario, the CRT can be downloaded from the following locations:

- During a CA Remint, the CRT will be available on the current CA server.
- During a Change CA to Internal, the CRT will be available on the new CA server.
- During a Change CA to external, the CRT will be available on the server on which the remint is initiated.
- During a Server Remint, if the current CA is internal, the CRT will be available on the current CA server. If the current CA is external, it will be available on the server on which the remint is initiated.

After a Server Remint the managed device is not able to communicate with the server

Source: ZENworks; SSL Management.

Explanation: If we remint a Primary server certificate, the initial web service file on the managed devices that are registered to this Primary Server will not be updated with the new certificate. If the device is not communicating with the server, the agent will not be able to fall back to the initial web service file because the certificate is not updated.

Action: Run the following commands to un-register and register the device:

- **To Unregister the device:** `zac unr`
- **To register the device:** `zac reg https://<server_IP>:<port>`

Certificate Remint Tool fails on the CA Server

Source: ZENworks; SSL Management.

Explanation: If the CA certificate has expired and you perform the Remint operation, the CRT that is launched on the CA server might fail. If you then double-click the CRT, it will fail again.

Action: Perform the following steps:

- **On Windows:** Launch `ZENworks_home\install\downloads\system-update\certificate-update\ZENworks_Certificate_Update_Windows.exe` and run the `-p ZENworks_home\conf\securit\ca.cert` command.
- **On Linux:** Launch `/opt/novell/zenworks/install/downloads/system-update/certificate-update/ZENworks_Certificate_Update_Linux.bin` and run the `-p /etc/opt/novell/zenworks/security/ca.cert command.`

The Agent Version is not getting displayed in the ZENworks Server SSL Certificates panel

Source: ZENworks; SSL Management.

Explanation: The **Version** column in the ZENworks Server SSL Certificates panel might be empty as soon as the server is installed.

Action: None. Once the agent is registered successfully, the **Version** column will get populated.

After a remint, security policy versions are incremented

Source: ZENworks; SSL Management.

Explanation: Security policies (Endpoint Security Management and Full Disk Encryption) are encrypted. After a remint, all published policies are resigned and incremented. Sandbox policies are not incremented.

Action: No action required. The incremented policies are automatically applied to devices during the next device refresh.

A server certificate has expired

Explanation: A server certificate has expired due to which the devices are unable to establish an SSL connection with the server. Certificate remint of an expired server certificate cannot be performed in ZCC.

Action: You need to manually replace the expired server certificate with a new server certificate by performing the following steps:

Replacing an internal server certificate with a new internal server certificate

If the internal server certificate of your Windows or Linux Primary Server has expired you can choose to replace the certificate with a new internal server certificate.

1. Before replacing an internal server certificate with a new internal server certificate, take a reliable backup of the following on all Primary Servers in the Management Zone:
   - **Content-Repo Directory:** The `content-repo` directory is located by default in the *`ZENworks_installation_directory`*`\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

     Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.
   - **Certificate Authority:** For detailed information on how to back up the certificate authority, see Backing Up the Certificate Authority.
   - **Embedded Database:** For detailed information on how to back up the embedded database, see Backing Up a ZENworks Server.
2. Enforce the new certificates on the zone by running the following command on any Primary Server whose certificate has expired:

   ```
   novell-zenworks-configure -c SSL -Z
   ```

   

   Follow the prompts. Do not remint the Certificate authority, just the server certificate.

NOTE: If both the Server Certificate and Certificate Authority (CA) have expired, then use the **Remint CA** option in the ZCC UI to remint the CA, which will remint the expired server certificate as well.

3 Restart all the ZENworks services on all the Primary Servers in the zone by running the following command at the console prompt of each Primary Server in the zone:

`novell-zenworks-configure -c Start`

By default, all the services are selected. You must select **Restart** as the **Action**.

4 Refresh all the devices, including the Primary Servers, in the zone.

If only one Primary Server certificate was changed, and if the CA certificate was not changed, and there is more than one Primary Server in the zone, refreshing the Server, Satellites, and managed devices will allow the agent to trust the new server certificate. Refreshes automatically on the next scheduled refresh.

If there is only one Primary Server in the zone then the Primary Servers, Satellites, and managed devices need to run `zac retr` to reestablish the trust.

If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

`zac retr -u` *`zone_administrator_username`* `-p` *`zone_administrator_password`*

5 Configure the Authentication Satellites with the new certificates by entering the following command at the Satellite's prompt:

On Windows: `zac authentication server reconfigure (asr) -t all`

On Linux: `zac remint-satellite-cert (rsc)`

6 Re-create all the default and custom deployment packages for all the Primary Servers:

- **Default Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the `novell-zenworks-configure -c CreateExtractorPacks -Z` command:

  Custom Deployment Packages: At the console prompt of each Primary Server in the zone, enter the `novell-zenworks-configure -c RebuildCustomPacks -Z` command

Replacing an external server certificate with a new external server certificate

If the external server certificate of your Windows or Linux Primary Server has expired you can choose to replace the certificate with a new external server certificate issued by your current zone CA.

1 Before replacing an external server certificate with a new external server certificate, take a reliable backup of the following on all Primary Servers in the Management Zone:

- **Content-Repo Directory:** The `content-repo` directory is located by default in the *`ZENworks_installation_directory`*`\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.

- **Embedded Database:** For detailed information on how to back up the embedded database, see Backing Up the Embedded Sybase SQL Anywhere Database.

2 Create a certificate signing request (CSR) by providing the hostname (FQDN) of the Primary Server as the subject. Using this CSR, get the new server certificate issued by the external CA.

   For more information on how to create a CSR, see "Creating an External Certificate" in the *ZENworks 11 SP4 Server Installation Guide*.

3 Delete the record of the server whose certificate is being renewed, from the `zCertificate` table in the database by using the query "`delete from zCertificate where SubjectUID = <GUID of the Primary Server whose cert has to be renewed`".

4 At the console prompt of a Primary Server, run the following command with the force (-f, --force) option.

   `zman sacert -f` *`Path_of_the_Primary_Server_in_ZENworks_Control_Center Path_of_Primary_Server_Certificate`*

   For more information about zman, view the zman man page (`man zman`) on the device or see "zman(1)" in the *ZENworks 11 SP4 Command Line Utilities Reference*.

   This adds the certificate of the Primary Server that you specified in the command to the ZENworks database and certificate store.

   NOTE: You must run the command for each server whose certificate you want to replace.

5 Refresh all the devices, including the Primary Servers, in the zone.

   The Primary Server certificates that were imported in Step 4 are sent to the devices as configuration data.

6 Enforce the new certificates on the zone by running the following command on any Primary Server whose certificate has expired:

   `novell-zenworks-configure -c SSL -Z`

   Follow the prompts.

7 Restart all the ZENworks services on the current Primary Server in the zone by running the following command at the console prompt of the Primary Server:

   `novell-zenworks-configure -c Start`

   By default, all the services are selected. You must select **Restart** as the **Action**.

8 Refresh all the devices, including the Primary Servers, in the zone.

   If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

   `zac retr -u` *`zone_administrator_username`* `-p` *`zone_administrator_password`*

9 Configure the Satellites with the new external certificates by entering the following command at the Satellite's prompt:

```
zac iac -pk private-key.der -c signed-server_certificate.der -ca signing-authority-public-certificate.der -ks keystore.jks -ksp keystore-pass-phrase -a signed-cert-alias -ks signed-cert-passphrase -u username -p password  -rc
```

10 Re-create all the default and custom deployment packages for all the Primary Servers:

- **Default Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

  ```
  novell-zenworks-configure -c CreateExtractorPacks -Z
  ```

- **Custom Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

  ```
  novell-zenworks-configure -c RebuildCustomPacks -Z
  ```