

# ZI-SecurityIncident - Installation and Administration Guide

- [Installation](#)
- [Configuration](#)

# Installation

## Requirements

- Zimbra 8.8.15
- ZI-LicenseSystem

## ZI-LicenseSystem

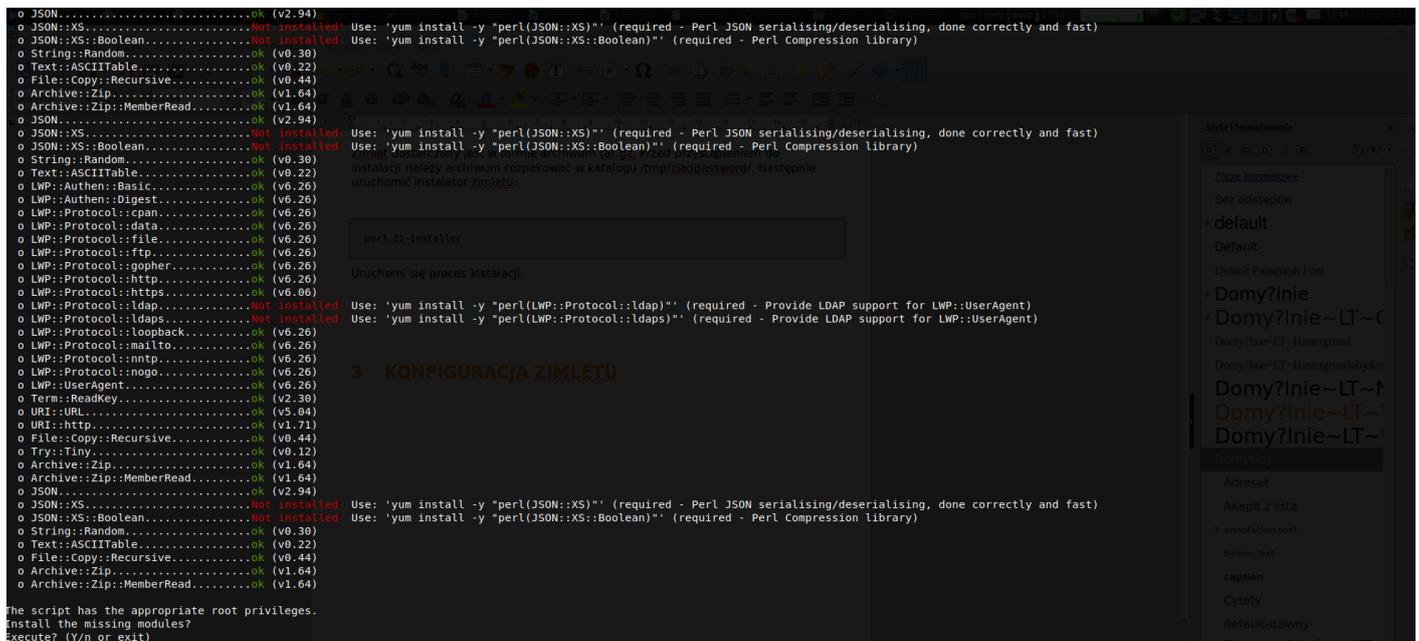
Unpack installer archive file \*.tar.gz in /var/tmp/ (as root):

```
mv /root/ZI-LicenseSystem-x.x.tar.gz /var/tmp/  
cd /var/tmp/  
tar xzvf ZI-LicenseSystem-x.x.tar.gz  
cd /var/tmp/ZI-LicenseSystem-x.x
```

Run installation script (as root):

```
perl ZI-Installer --instal-deps
```

At the beginning required perl packages will be installed:



```
o JSON.....ok (v2.94)  
o JSON:XS.....Not installed Use: 'yum install -y "perl(JSON:XS)"' (required - Perl JSON serialising/deserialising, done correctly and fast)  
o JSON:XS:Boolean.....Not installed Use: 'yum install -y "perl(JSON:XS:Boolean)"' (required - Perl Compression library)  
o String:Random.....ok (v0.30)  
o Text:ASCIITable.....ok (v0.22)  
o File:Copy:Recursive.....ok (v0.44)  
o Archive:Zip.....ok (v1.64)  
o Archive:Zip:MemberRead.....ok (v1.64)  
o JSON.....ok (v2.94)  
o JSON:XS.....Not installed Use: 'yum install -y "perl(JSON:XS)"' (required - Perl JSON serialising/deserialising, done correctly and fast)  
o JSON:XS:Boolean.....Not installed Use: 'yum install -y "perl(JSON:XS:Boolean)"' (required - Perl Compression library)  
o String:Random.....ok (v0.30)  
o Text:ASCIITable.....ok (v0.22)  
o LWP:Authen:Basic.....ok (v6.26)  
o LWP:Authen:Digest.....ok (v6.26)  
o LWP:Protocol:cpan.....ok (v6.26)  
o LWP:Protocol:data.....ok (v6.26)  
o LWP:Protocol:file.....ok (v6.26)  
o LWP:Protocol:ftp.....ok (v6.26)  
o LWP:Protocol:gopher.....ok (v6.26)  
o LWP:Protocol:http.....ok (v6.26)  
o LWP:Protocol:https.....ok (v6.06)  
o LWP:Protocol:ldap.....Not installed Use: 'yum install -y "perl(LWP:Protocol:ldap)"' (required - Provide LDAP support for LWP:UserAgent)  
o LWP:Protocol:ldaps.....Not installed Use: 'yum install -y "perl(LWP:Protocol:ldaps)"' (required - Provide LDAP support for LWP:UserAgent)  
o LWP:Protocol:loopback.....ok (v6.26)  
o LWP:Protocol:mailto.....ok (v6.26)  
o LWP:Protocol:nntp.....ok (v6.26)  
o LWP:Protocol:nogo.....ok (v6.26)  
o LWP:UserAgent.....ok (v6.26)  
o Term:ReadKey.....ok (v2.30)  
o URI:URL.....ok (v5.04)  
o URI:http.....ok (v1.71)  
o File:Copy:Recursive.....ok (v0.44)  
o Try:Tiny.....ok (v0.12)  
o Archive:Zip.....ok (v1.64)  
o Archive:Zip:MemberRead.....ok (v1.64)  
o JSON.....ok (v2.94)  
o JSON:XS.....Not installed Use: 'yum install -y "perl(JSON:XS)"' (required - Perl JSON serialising/deserialising, done correctly and fast)  
o JSON:XS:Boolean.....Not installed Use: 'yum install -y "perl(JSON:XS:Boolean)"' (required - Perl Compression library)  
o String:Random.....ok (v0.30)  
o Text:ASCIITable.....ok (v0.22)  
o File:Copy:Recursive.....ok (v0.44)  
o Archive:Zip.....ok (v1.64)  
o Archive:Zip:MemberRead.....ok (v1.64)  
The script has the appropriate root privileges.  
Install the missing modules?  
[recute? (Y/n or exit)]
```

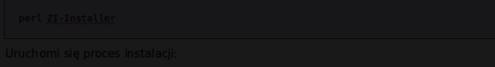
Answer: Y

```

o JSON:XS:Random.....ok (v0.30)
o Text::ASCIITable.....ok (v0.22)
o File::Copy::Recursive.....ok (v0.44)
o Archive::Zip::MemberRead.....ok (v1.64)
o JSON:XS:Random.....ok (v0.30)
o JSON:XS:Boolean.....Not installed Use: 'yum install -y "perl(JSON:XS)"' (required - Perl JSON serialising/deserialising, done correctly and fast)
o String::Random.....ok (v0.30)
o Text::ASCIITable.....ok (v0.22)
o LWP:Authen:Basic.....ok (v6.26)
o LWP:Authen:Digest.....ok (v6.26)
o LWP:Protocol:cpan.....ok (v6.26)
o LWP:Protocol:data.....ok (v6.26)
o LWP:Protocol:file.....ok (v6.26)
o LWP:Protocol:ftp.....ok (v6.26)
o LWP:Protocol:gopher.....ok (v6.26)
o LWP:Protocol:http.....ok (v6.26)
o LWP:Protocol:https.....ok (v6.66)
o LWP:Protocol:ldap.....Not installed Use: 'yum install -y "perl(LWP:Protocol:ldap)"' (required - Provide LDAP support for LWP:UserAgent)
o LWP:Protocol:loopback.....Not installed Use: 'yum install -y "perl(LWP:Protocol:loopback)"' (required - Provide LDAP support for LWP:UserAgent)
o LWP:Protocol:mailto.....ok (v6.26)
o LWP:Protocol:nntp.....ok (v6.26)
o LWP:Protocol:nogo.....ok (v6.26)
o LWP:UserAgent.....ok (v6.26)
o Term::ReadKey.....ok (v2.30)
o URI::URL.....ok (v5.04)
o URI::http.....ok (v1.71)
o File::Copy::Recursive.....ok (v0.44)
o Try::Tiny.....ok (v0.12)
o Archive::Zip::MemberRead.....ok (v1.64)
o JSON:XS:Random.....ok (v0.30)
o JSON:XS:Boolean.....Not installed Use: 'yum install -y "perl(JSON:XS)"' (required - Perl JSON serialising/deserialising, done correctly and fast)
o String::Random.....ok (v0.30)
o Text::ASCIITable.....ok (v0.22)
o File::Copy::Recursive.....ok (v0.44)
o Archive::Zip::MemberRead.....ok (v1.64)

```

The script has the appropriate root privileges.  
Install the missing modules?  
Execute? (Y/n or exit)



### 3 KONFIGURACJA ZIMLETU

Press: Y

```

Install module 2 of 4
Wczytane wtyczki: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.icm.edu.pl
 * epel: ftp.icm.edu.pl
 * extras: ftp.icm.edu.pl
 * updates: ftp.icm.edu.pl
Nie ma pakietu perl(JSON:XS:Boolean).
Błąd: Nie ma niczego do zrobienia

Install module 3 of 4
Wczytane wtyczki: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.icm.edu.pl
 * epel: ftp.icm.edu.pl
 * extras: ftp.icm.edu.pl
 * updates: ftp.icm.edu.pl
Rozwiązywanie zależności
--> Wykonywanie sprawdzania transakcji
--> Pakiet perl-LDAP.noarch 1:0.56-6.el7 zostanie zainstalowany
--> Przetwarzanie zależności: perl(Convert:ASN1) >= 0.2 dla pakietu: 1:perl-LDAP-0.56-6.el7.noarch
--> Przetwarzanie zależności: perl(Authen:SASL) >= 2.00 dla pakietu: 1:perl-LDAP-0.56-6.el7.noarch
--> Przetwarzanie zależności: perl(XML:SAX:Writer) dla pakietu: 1:perl-LDAP-0.56-6.el7.noarch
--> Przetwarzanie zależności: perl(XML:SAX:Base) dla pakietu: 1:perl-LDAP-0.56-6.el7.noarch
--> Wykonywanie sprawdzania transakcji
--> Pakiet perl-Authen-SASL.noarch 0:2.15-10.el7 zostanie zainstalowany
--> Przetwarzanie zależności: perl(GSSAPI) dla pakietu: perl-Authen-SASL-2.15-10.el7.noarch
--> Pakiet perl-Convert-ASN1.noarch 0:0.26-4.el7 zostanie zainstalowany
--> Pakiet perl-XML-SAX-Base.noarch 0:1.08-7.el7 zostanie zainstalowany
--> Pakiet perl-XML-SAX-Writer.noarch 0:0.53-4.el7 zostanie zainstalowany
--> Przetwarzanie zależności: perl(XML:NamespaceSupport) dla pakietu: perl-XML-SAX-Writer-0.53-4.el7.noarch
--> Przetwarzanie zależności: perl(XML:Filter:BufferText) dla pakietu: perl-XML-SAX-Writer-0.53-4.el7.noarch
--> Wykonywanie sprawdzania transakcji
--> Pakiet perl-GSSAPI.x86_64 0:0.28-9.el7 zostanie zainstalowany
--> Pakiet perl-XML-Filter-BufferText.noarch 0:1.01-17.el7 zostanie zainstalowany
--> Pakiet perl-XML-NamespaceSupport.noarch 0:1.11-10.el7 zostanie zainstalowany
--> Ukończono rozwiązywanie zależności
Rozwiązano zależności

```

Package	Architektura	Wersja	Repozytorium	Rozmiar
Instalowanie:				
perl-LDAP	noarch	1:0.56-6.el7	base	411 k
Instalowanie, aby rozwiązać zależności:				
perl-Authen-SASL	noarch	2.15-10.el7	base	57 k
perl-Convert-ASN1	noarch	0.26-4.el7	base	54 k
perl-GSSAPI	x86_64	0.28-9.el7	base	59 k
perl-XML-Filter-BufferText	noarch	1.01-17.el7	base	11 k
perl-XML-NamespaceSupport	noarch	1.11-10.el7	base	18 k
perl-XML-SAX-Base	noarch	1.08-7.el7	base	32 k
perl-XML-SAX-Writer	noarch	0.53-4.el7	base	25 k
Podsumowanie transakcji				

Style (Formatowanie)

Złóż Intencje

Bez odstępów

default

Default

Default Paragraph Font

Domy?Inie

Domy?Inie~LT~C

Domy?Inie~LT~H

Domy?Inie~LT~H

Domy?Inie~LT~H

Domy?Inie~LT~H

Adresat

Akapit z listą

Annotation text

Annotation text

caption

Cyfaty

default-dzwiny

```

Instalowanie:
perl-LDAP                                noarch                1:0.56-6.el7                base                411 k
Instalowanie, aby rozwiązać zależności:
perl-Authen-SASL                         noarch                2.15-10.el7                base                57 k
perl-Convert-ASN1                        noarch                0.26-4.el7                 base                54 k
perl-GSSAPI                              x86_64               0.28-9.el7                 base                59 k
perl-XML-Filter-BufferText               noarch                1.01-17.el7                base                11 k
perl-XML-NamespaceSupport                noarch                1.11-10.el7                base                18 k
perl-XML-SAX-Base                        noarch                1.08-7.el7                 base                32 k
perl-XML-SAX-Writer                      noarch                0.53-4.el7                 base                25 k

Podsumowanie transakcji
Zimlet dostarczany jest w formie archiwum tar.gz. Przed przystąpieniem do
uruchomienia instalatora zimletu:
Instalacja 1 Pakiet (+7 Zależne pakiety)
Całkowity rozmiar pobierania: 667 k
Rozmiar po zainstalowaniu: 1.6 M
Downloading packages:
(1/8): perl-Authen-SASL-2.15-10.el7.noarch.rpm
(2/8): perl-Convert-ASN1-0.26-4.el7.noarch.rpm
(3/8): perl-GSSAPI-0.28-9.el7.x86_64.rpm
(4/8): perl-LDAP-0.56-6.el7.noarch.rpm
(5/8): perl-XML-Filter-BufferText-1.01-17.el7.noarch.rpm
(6/8): perl-XML-NamespaceSupport-1.11-10.el7.noarch.rpm
(7/8): perl-XML-SAX-Base-1.08-7.el7.noarch.rpm
(8/8): perl-XML-SAX-Writer-0.53-4.el7.noarch.rpm

Razem
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Instalowanie      : perl-XML-SAX-Base-1.08-7.el7.noarch
Instalowanie      : perl-XML-Filter-BufferText-1.01-17.el7.noarch
Instalowanie      : perl-XML-NamespaceSupport-1.11-10.el7.noarch
Instalowanie      : perl-XML-SAX-Writer-0.53-4.el7.noarch
Instalowanie      : perl-GSSAPI-0.28-9.el7.x86_64
Instalowanie      : perl-Authen-SASL-2.15-10.el7.noarch
Instalowanie      : perl-Convert-ASN1-0.26-4.el7.noarch
Instalowanie      : 1:perl-LDAP-0.56-6.el7.noarch
Sprawdzanie       : perl-Convert-ASN1-0.26-4.el7.noarch
Sprawdzanie       : perl-XML-Filter-BufferText-1.01-17.el7.noarch
Sprawdzanie       : 1:perl-LDAP-0.56-6.el7.noarch
Sprawdzanie       : perl-GSSAPI-0.28-9.el7.x86_64
Sprawdzanie       : perl-XML-NamespaceSupport-1.11-10.el7.noarch
Sprawdzanie       : perl-XML-SAX-Base-1.08-7.el7.noarch
Sprawdzanie       : perl-XML-SAX-Writer-0.53-4.el7.noarch
Sprawdzanie       : perl-Authen-SASL-2.15-10.el7.noarch

Zainstalowano:
perl-LDAP.noarch 1:0.56-6.el7

Zainstalowano zależności:
perl-Authen-SASL.noarch 0:2.15-10.el7  perl-Convert-ASN1.noarch 0:0.26-4.el7  perl-GSSAPI.x86_64 0:0.28-9.el7  perl-XML-Filter-BufferText.noarch 0:1.01-17.el7  perl-XML-NamespaceSupport.noarch 0:1.11-10.el7
perl-XML-SAX-Base.noarch 0:1.08-7.el7  perl-XML-SAX-Writer.noarch 0:0.53-4.el7

ukończono.

```

```

Installer must be located in zimbra directory!
Do you want copy to /opt/zimbra/.tmp/IntalioZiADPassword?
Execute? (Y/n or exit)
Y

```

Answer: Y

```

ZI-Installer: "installationType" is not specified, use local installation instead
ZI-Installer: "NoDatabase" was set. Database configuration will be ignored

----- CONFIG -----
DatabaseConfigFormat      -->
DatabaseConfigLocation   -->
help                      -->
installationType          --> local
installConfigPath        -->
InstallDeps               -->
mysqlHost                 -->
mysqlNewDatabaseName     -->
mysqlNewPassword         -->
mysqlNewUser              -->
mysqlPort                 -->
NoActivate                --> 1
NoAsk                     -->
NoDatabase                --> 1
PostinstallCommand       -->
RestartZimbra            -->
SqlFile                   -->
Update                    --> 0
version                   -->
zimbraPath                --> /opt/zimbra
zimletDirName             --> IntalioZiLicenseSystem

Mailboxd service won't be restarted automatically.
Proceed?
(Y/n or exit):

```

Answer: Y

```

Please enter your login:

```

Enter login and password received with the license.

```
-----
                        Licenses
-----+-----+-----+
| Nr | LicenseNumber | Description |
-----+-----+-----+
| 1 | nprFvwVdDb0P4N8AjG2noPKa | ZI-License for Intalio Zimbra |
-----+-----+-----+
Please choose 1-1 option or type exit
```

Choose: 1

```
Installation starting....
Creating zimlet directory...
Removing earlier version...
Copying Extensions...
Copying script libs...
Setting permissions...
Looking for zip files in Zimlets directory...
Found 1 files
Starting deploy...
[ ] INFO: Deploying Zimlet intalio_zi_license_system in LDAP.
[ ] INFO: Installing Zimlet intalio_zi_license_system on this host.
[ ] INFO: Deploying on service node test-zmbox2.int.intalio.pl
[ ] INFO: post to server test-zmbox2.int.intalio.pl, data size 176531
[ ] INFO: Deploy initiated. Check the server test-zmbox2.int.intalio.pl's mailbox.log for the status.
Deploy complete
Restart zimbra?
(Y/n or exit): y
```

Choose: Y

If You answer Y, the zimbra mailbox will be restarted

After the mailbox restart, zimlet should be installed. Now, ZI-SecurityIncident can be installed.

ZI-LicenseSystem must be installed on all mailboxes

## Zi-SecurityIncident

Unpack installer archive file \*.tar.gz in /var/tmp/ (as root):

```
mv /root/ZI-SecurityIncident-x.x.tar.gz /var/tmp/
cd /var/tmp/
tar xzvf ZI-SecurityIncident-x.x.tar.gz
cd /var/tmp/ZI-SecurityIncident-x.x
```

Run installation script (as root):

```
perl ZI-Installer --instal-deps
```

```
-----CONFIG-----
DatabaseConfigFormat      --> CS
DatabaseConfigLocation   --> ./Extensions/db.properties
help                      -->
InstallationType         --> local
installConfigPath        -->
InstallDeps              -->
mysqlHost                -->
mysqlNewDatabaseName     --> IntalioZiSecurityIncident
mysqlNewPassword         --> CCJgSDeyhwPrhMS8ric6IKMTEM8PeoJu
mysqlNewUser             --> intaliozisecurityincident_user
mysqlPort                --> 7306
NoActivate               -->
NoAsk                    -->
NoDatabase               -->
PostinstallCommand       -->
RestartZimbra            -->
SqlFile                  -->
Update                   --> 1
version                  -->
zimbraPath               --> /opt/zimbra
ZimletDirName            --> IntalioZiSecurityIncident
-----

Mailboxd service won't be restarted automatically.
Proceed?
(Y/n or exit): █
```

Type: Y

# Configuration

Log in to the Zimbra Administration Console. The ZI-SecurityIncident configuration panel is available on **Main Page -> Migration and tools -> ZI-SecurityIncident**

The screenshot shows the Zimbra Administration console interface. The left sidebar contains a navigation menu with the following items: Home, Tools and Migration, Downloads, Account Migration, Software Updates, Client Upload, ZI-Piler, ZI-LicenseSystem, and ZI-SecurityIncident (which is currently selected). The main content area is titled 'Home - Tools and Migration - ZI-SecurityIncident' and contains three configuration sections:

- Email settings:** This section includes input fields for 'From' (Internal email address), 'To', 'Subject', and 'Names of attachments' (with a note: 'This name will be used to create file names such as dangerous\_email.7z'). There is also a large text area for 'Content'.
- Archive password settings:** This section includes a checkbox for 'Password is the current date' (checked), a 'Date format' field with a legend (y = year (yy year yyyy), M = month (MM), d = day in month (dd), h = hour (0-12) (hh), H = hour (0-23) (HH), m = minute (mm), z = timezone (e.g. Pacific Standard Time...), Z = timezone (e.g. -0800)) and a value of 'yyyyMMdd', and a 'Static password' field with a value of 'password'.
- System for generating message preview:** This section includes four checkboxes: 'Generate secure message preview' (checked), 'Delete unsafe code from preview' (unchecked, with a note: 'e.g. executable scripts'), 'Display images from external sources' (checked), and 'Display images already processed by the system' (checked).

## Email settings

- **From** - sender of the notification email
- **To** - recipient of the notification email
- **Subject** - subject of the notification email
- **Names of attachments** - names of the unsafe attachments
- **Content** - content of the message

## Archive password settings

- **Password is the current date** - password of the zipped attachment is the date of the received message
- **Date format**
- **Static password** - password of the zipped attachment when option **Password is the current date** is unchecked

## System for generating message preview

- **Generate secure message preview** - if set, unsafe message is converted to pdf
- **Delete unsafe code from preview** - if set, unsafe code is removed from preview
- **Display images from external sources** - if set, images from external sources will be included in the processed message
- **Display images already processed by the system** - if set, images in message will be processed