

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::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?  
Execute? (Y/n or exit)
```

3 KONFIGURACJA ZIMLETU

Answer: Y

```
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 Strings::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::nsgo.....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 Strings::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?
Execute? (Y/n or exit)

instalacji należy archiwum rozpakować w katalogu /tmp/zladpassword/. Następnie uruchomić instalator zimletu:

```
perl ZI-Installer
```

Uruchomił się proces instalacji:

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
```

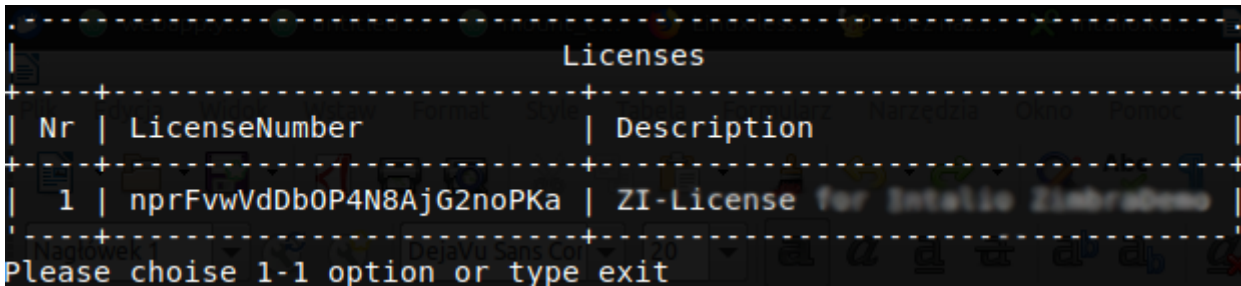
Package	Architektura	Wersja	Repozytorium	Rozmiar
Instalowanie:				
perl-LDAP	noarch	1:0.56-6.el7	base	411 k
Instalowanie, aby rozwiązać zależności:				
perl-Authen-SASL	noarch	2.15-10.el7	base	57 k
perl-Convert-ASN1	noarch	0.26-4.el7	base	54 k
perl-GSSAPI	x86_64	0.28-9.el7	base	59 k
perl-XML-Filter-BufferText	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

Zimlet dostarczany jest w formie archiwum tar.gz. Przed przystąpieniem do instalacji należy archiwum rozpakować w katalogu /tmp/zladpassword/. Następnie uruchomić instalator zimletu:

```
perl ZI-Installer
```

3 KONFIGURACJA ZIMLETU



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          --> CCJgSDeyhwPrhMS8ric6iKTEM8PeoJu
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 menu with options: Home, Tools and Migration, Downloads, Account Migration, Software Updates, Client Upload, ZI-Piler, ZI-LicenseSystem, and ZI-SecurityIncident. The main content area is titled 'Home - Tools and Migration - ZI-SecurityIncident' and contains three configuration sections.

Email settings

From	<input type="text"/>
Internal email address	<input type="text"/>
To	<input type="text"/>
Subject	<input type="text"/>
Names of attachments	<input type="text"/>
This name will be used to create file names such as dangerous_email.7z	
Content	<input type="text"/>

Archive password settings

Password is the current date	<input checked="" type="checkbox"/>
Date format	<input type="text" value="yyyyMMdd"/>
<small>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)</small>	
Static password	<input type="text" value="password"/>
<small>If the password is not a date - enter a static password.</small>	

System for generating message preview

Generate secure message preview	<input checked="" type="checkbox"/>
Delete unsafe code from preview	<input type="checkbox"/>
<small>e.g. executable scripts</small>	
Display images from external sources	<input checked="" type="checkbox"/>
Display images already processed by the system	<input checked="" type="checkbox"/>

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