Bitrix Platform 9.x

Proactive Protection Guide

Phone/Fax: +1 (703) 740-8301; e-mail: info@bitrixsoft.com, http://www.bitrixsoft.com

Introduction

A web site owner should keep vigilant watch over protection of their web resources from hacks, hijacking and data theft. Bitrix has developed the **Proactive Protection** module embracing the main aspects of the site and third party application security.

The level of security provided by the standard distribution package is sufficiently high. However, the implementation of a web project usually requires component customization and developing custom tools whose security is not always tested and thus cannot be trusted. The **Proactive protection** module is an important part of the security subsystem and significantly strengthens web project security.

The guide describes general operations required on an administrator's side to configure the **Proactive protection** module. The document has been developed for the Bitrix Site Manager administrators and the IT security specialists.

A **Proactive Protection** is a complex of hardware and software solutions and organizational measures within the concept of security aimed to broaden the idea of web application threat immunity and possible reaction to threats.

The module offers the following protection features:

- one time password technology;
- session protection technology;
- proactive filter;
- system integrity control;
- phishing protection;
- data encryption.

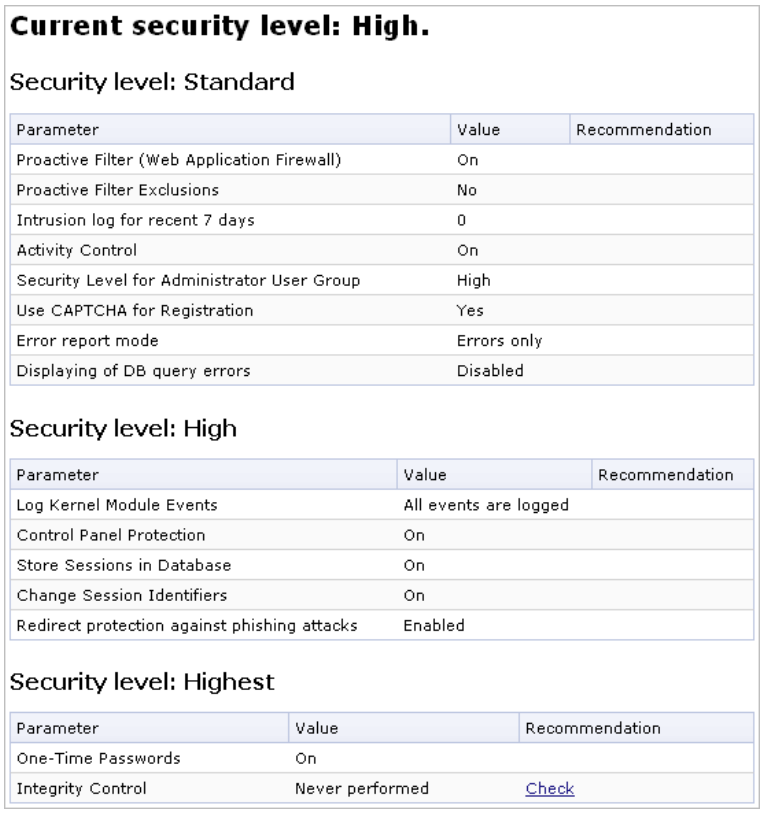
Chapter 1. Proactive Protection Configuration

Any Bitrix Framework based web site is always preconfigured for the use of the basic protection level. However, you can improve the site security significantly by selecting one of the **Proactive Protection** module presets:

- standard;
- high;
- highest.

Remember that all the security levels are inclusive, which effectively means that you have to set the parameters of the standard level prior to configuring the higher protection levels.

The **Security Control Panel** page (*Settings* > *Proactive Protection* > *Security Panel*, fig. 1.1) shows information on a current security level. For each level, there is a table of parameters and values. **Security Control Panel** shows recommendations on changing parameters to the recommended values, if necessary.



Current security level: High.

Security level: Standard

Parameter	Value	Recommendation
Proactive Filter (Web Application Firewall)	On	
Proactive Filter Exclusions	No	
Intrusion log for recent 7 days	0	
Activity Control	On	
Security Level for Administrator User Group	High	
Use CAPTCHA for Registration	Yes	
Error report mode	Errors only	
Displaying of DB query errors	Disabled	

Security level: High

Parameter	Value	Recommendation
Log Kernel Module Events	All events are logged	
Control Panel Protection	On	
Store Sessions in Database	On	
Change Session Identifiers	On	
Redirect protection against phishing attacks	Enabled	

Security level: Highest

Parameter	Value	Recommendation
One-Time Passwords	On	
Integrity Control	Never performed	Check

Fig. 1.1 Security control panel

If an incorrect value has been specified for a parameter, the **Recommendation** field will show a useful hint about it.

Standard security level

Entirely all parameters of the standard security level should be configured properly so that a web site runs well protected (fig. 1.2).

Security level: Standard

Parameter	Value	Recommendation
Proactive Filter (Web Application Firewall)	On	
Proactive Filter Exclusions	No	
Intrusion log for recent 7 days	0	
Activity Control	On	
Security Level for Administrator User Group	High	
Use CAPTCHA for Registration	Yes	
Error report mode	Errors only	
Displaying of DB query errors	Disabled	

Fig. 1.2 Standard security level settings

Note. If you fail to configure the standard level properly, the basic protection level takes effect with respect to parameters of other protection levels.

Proactive Filter and Exceptions

The proactive filter (Web Application Firewall) protects the system from most known web attacks. The filter recognizes dangerous treats in the incoming requests and blocks intrusions. Proactive Filter is the most effective way to guard against possible security defects in the web project implementation. The filter analyzes entirely all data received from visitors in variables and cookies.

You can enable or disable the Proactive filter at *Settings* > *Proactive Protection* > *Proactive Filter* using the **Enable Proactive Protection** button (or **Disable Proactive Protection**, fig. 1.3).

Fig. 1.3 The proactive filter

If required, you can set the proactive filter exceptions; this will cause the proactive filter to not be applied to pages matching the wildcards on the **Exceptions** tab.

Note. The standard protection level implies that the proactive filter is enabled and no filter exception is defined.

The actions the system undertakes in response to the intrusion attempts are configured on the **Active Reaction** tab (fig. 1.4).

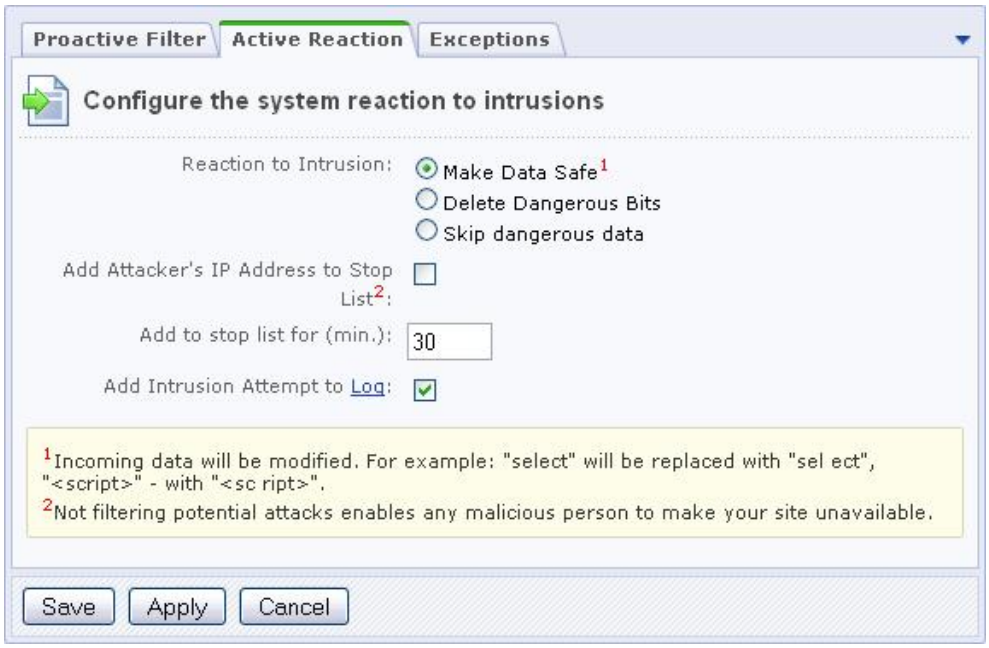


Fig. 1.4 The active reaction parameters

- Select the required action to respond to attacks:
  - **Make Data Safe** – dangerous data will be modified; for example: "**sel ect**" will replace "**select**".
  - **Delete Dangerous Bits** – dangerous data will be removed.
  - **Skip dangerous data** – no action will be performed.
- **Add Attacker's IP Address to Stop List** – dangerous data will be altered and a visitor will be blocked for the period specified (**Add to stop list for (min.)** parameter).
- To log the intrusion attempt events, enable the corresponding option.

Note that some harmless actions a visitor may perform can be suspicious and cause the filter to react.

Note. The proactive filter will not be applied to user groups whose operation set (in fact, permissions) includes the **Bypass Proactive Filter** option (see the description of access permission levels, fig. 1.5).

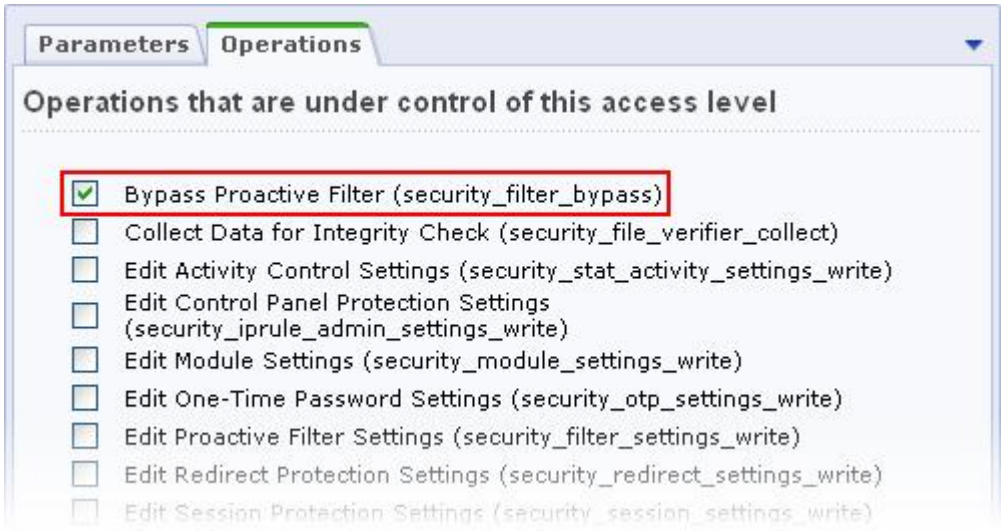


Fig. 1.5 Operations for the Proactive Protection module

Intrusion Log

An **Intrusion Log** (*Settings* > *Proactive Protection* > *Intrusion Log*) registers any events relating to potential security threats. The log lifetime can be defined in the kernel module settings. The log includes the following information on an event (fig. 1.6):

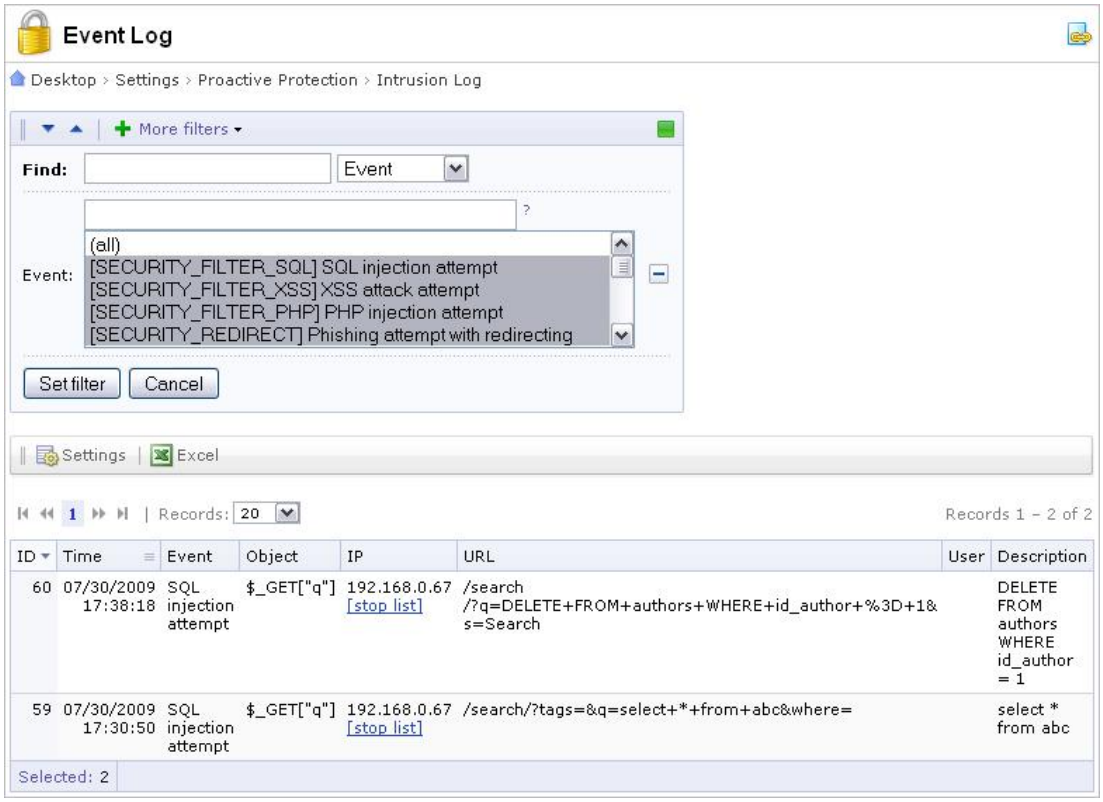


Fig. 1.6 The intrusion log

- the event date and time;
- the event name;
- severity (SECURITY or WARNING);
- an event source;
- an event object;
- the source IP. The "**stop list**" adds the URL to the **Web Analytics** module stop list.
- the client User Agent;
- the URL of an offended page;
- an offended site;
- the user name (if an event originates from a registered user), or a visitor ID. This field exists if the **Web Analytics** module is installed;
- the event description.

The log registers the following events.

- The **Web Analytics** module: exceeding the activity limit.
- The **Proactive protection** module: SQL and PHP injection attempts, XSS attacks and phishing attempts with redirecting.
- The **Kernel** module: successful log in and log out; password change request; stored authorization errors; new user registration; user registration and deletion errors.

Activity Control

User activity control is build around the **Web Analytics** module mechanisms and requires this module to be installed. Activity Control allows to protect the system from profusely active visitors, obtrusive bots, some DDoS attacks, and to prevent password brute force attempts.

You can enable or disable the activity control here: *Settings* > *Proactive Protection* > *Activity Control* using the **Enable Activity Control** (or **Disable Activity Control**, fig. 1.7) option.

Fig. 1.7 Activity Control

The visitor maximum activity is regulated by the **Parameters** tab settings (fig. 1.8).

Fig. 1.8 Configuring the activity parameters

If a user makes more requests than allowed within the time specified, they are automatically blocked for the specified period showing a special page to them. The **edit template** link allows to edit the template of the error page. Check the **Add entry to event log** option to register the limit exceeding in the intrusion log (*Settings > Proactive Protection > Intrusion Log*).

Note. The standard protection level implies that the activity control is enabled.

Special Security Settings for Administrators

The standard protection level implies that the **Administrators** user group has the highest security level, which is the default setting. If this security level is different from the highest for some reason, do the following:

- Click **Set to High** on the **Security panel**. The **Security** tab of the group properties form will open (fig. 1.9).

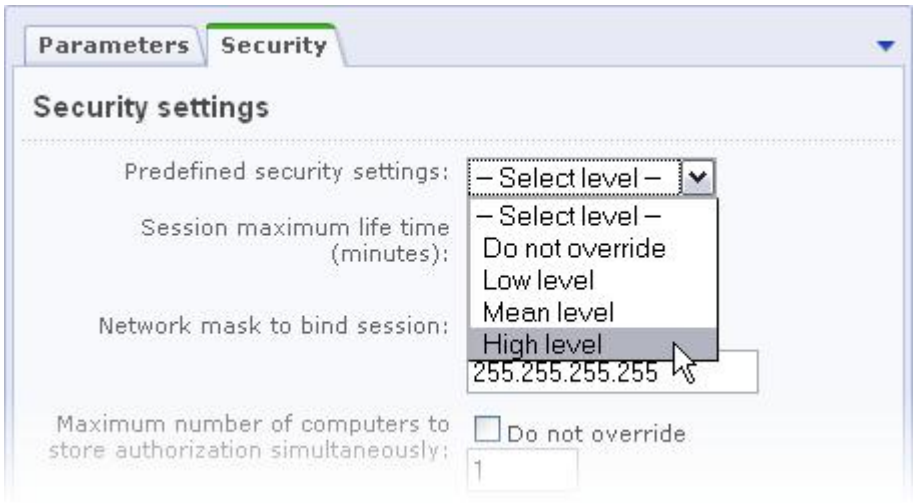


Fig. 1.9 Setting the user group security level

- Specify **High level** in the **Predefined security settings** field.
- Save changes.

The CAPTCHA-Aware Registration Procedure

A requisite condition for the standard protection level is the use of CAPTCHA for user registration. This option can be enabled in the **Main** module settings on the **Authorization** tab (fig. 1.10):

Fig. 1.10 Enabling CAPTCHA for use registration

You can alter the CAPTCHA look and feel is configured at *Settings* > *System settings* > *CAPTCHA*.

Error Report Mode

In order to protect the site at the standard protection level, there is another Kernel module parameter that is to be configured - **Error report mode**.

- Open the **Kernel** module settings (*Settings* > *System settings* > *Module settings* > *Main module*).
- Select either **Errors only** or **None** in the **Error report mode** field (fig. 1.11).

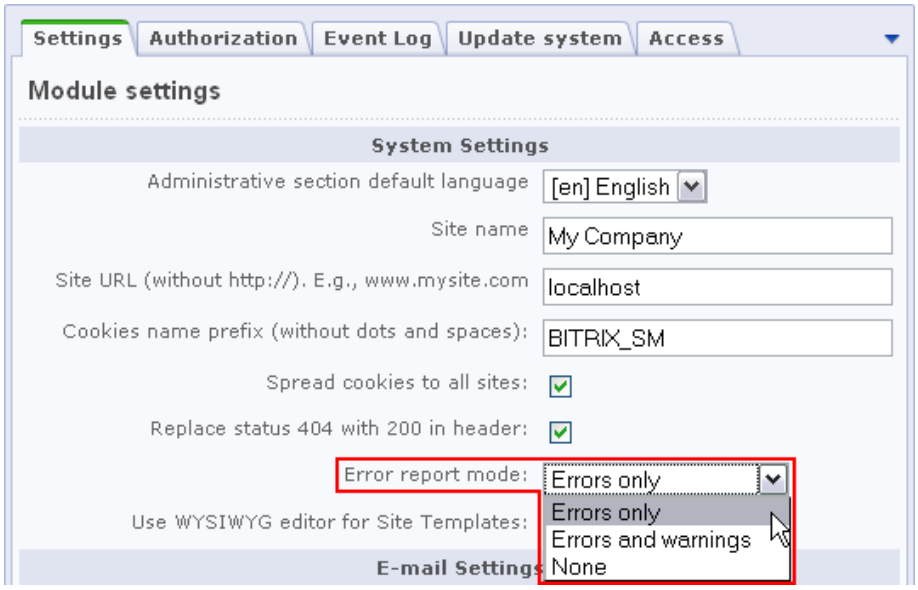


Fig. 1.11 Setting the error report mode

Note: selecting the **Errors and warnings** mode automatically switches the security level to basic.

- Save changes.

Showing Database Request Errors

The standard protection level does not require showing database error messages to common users which means the **$DBDebug** variable is to be set to **false**. Here, when a database error occurs, only the administrator will see the full error description. However, setting this variable to **true** causes the error messages to be shown to all the site visitors.

You can change the **$DBDebug** variable value by editing the **/bitrix/php_interface/dbconn.php** file.

High Security Level

Remember that you have to set the parameters of the standard level prior to configuring the higher protection levels (fig. 1.12).

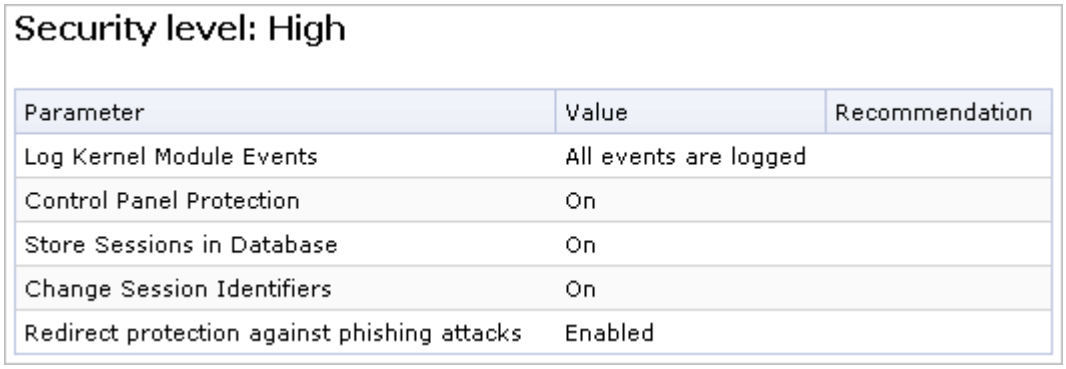


Fig. 1.12 The parameters of the high protection level

Note: if some of the high protection level parameters are incorrect, the **standard** protection level takes effect with respect to parameters of other protection levels, or **basic** if the standard level have been configured incorrectly.

Logging the Kernel Events

The **Log Kernel Module Events** parameter embraces a number of the kernel module options:

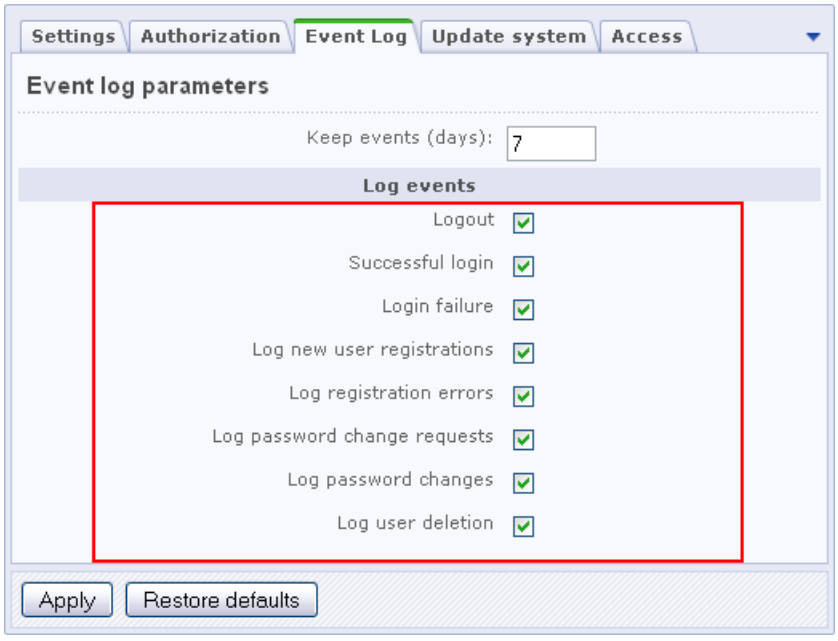


Fig. 1.13 The Kernel event log configuration sheet

Enable all the events on this sheet (fig. 1.13) for the site to be protected at the high security level. Even if one of the options is not checked, the **Log Kernel Module**

Events parameter is considered to be taking a mismatching value which causes the site to be protected at the standard (or basic) security level.

Protection for the Site Control Panel

The site control panel is protected by denying access from all IP addresses except for those specified in the settings. You can enable or disable the protection at *Settings > Proactive Protection > Control Panel Protection* using **Enable Protection** (or **Disable Protection**, fig. 1.14).

Fig. 1.14 Control Panel protection

Note. Before enabling the Control Panel protection, specify here the IP addresses or address range of clients allowed to access Control Panel.

Secure web projects must have the Control panel protection enabled.

Note. To remove the IP address restrictions, create a special flag file and specify the file pathname in the **Proactive Protection** module settings (fig. 1.15). The default name format is **ipcheck_disable_cef<*32_random_characters*>**.

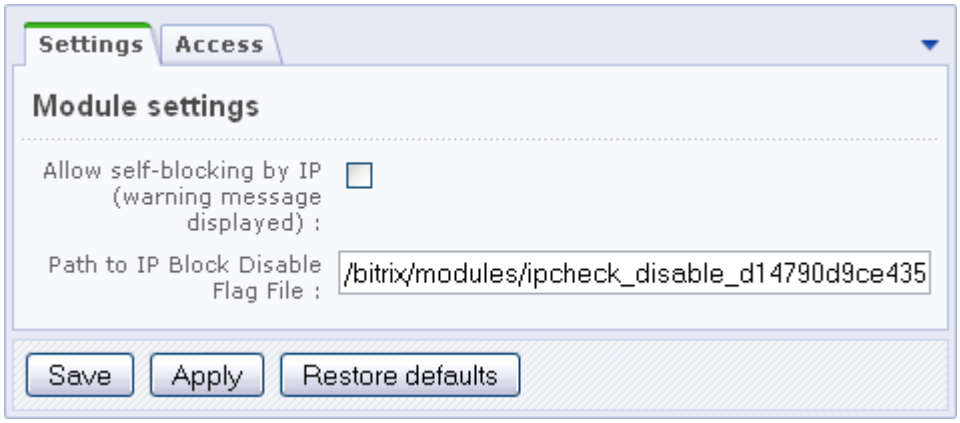


Fig. 1.15 The Proactive Protection module parameters

The Session Storage and Session ID Change

Most web attacks are purposed to steal the session data of an authorized user or, what is more valuable for attackers, of an administrator. The standard Bitrix Site Manager package controls the following session protection parameters, for each user group individually:

- Session lifetime (min.);
- Session Network Mask.

However, it is often impossible to restrict access because users may use dynamic IP addresses. The following two protection techniques of the **Proactive protection** module significantly add to the standard protection mechanisms:

- storing sessions in the **Security** module database;
- changing session ID's after specified intervals.

In order to enable or disable storing the user session in the database, click the big button, the only control on the *Settings* > *Proactive Protection* > *Session Protection* page (fig. 1.16).

Fig. 1.16 Session storage control

Storing session data in the module database prevents data from being stolen by running scripts on other virtual servers which eliminates virtual hosting configuration errors, bad temporary folder permission settings and other operating system related problems. It also reduces file system stress by offloading operations to the database server.

Note. Switching the session store mode causes all the logged-in users to lose authorization because this erases the user session data.

You can configure the session ID change mechanism on the **Change ID's** tab of the session protection settings form (fig. 1.17).

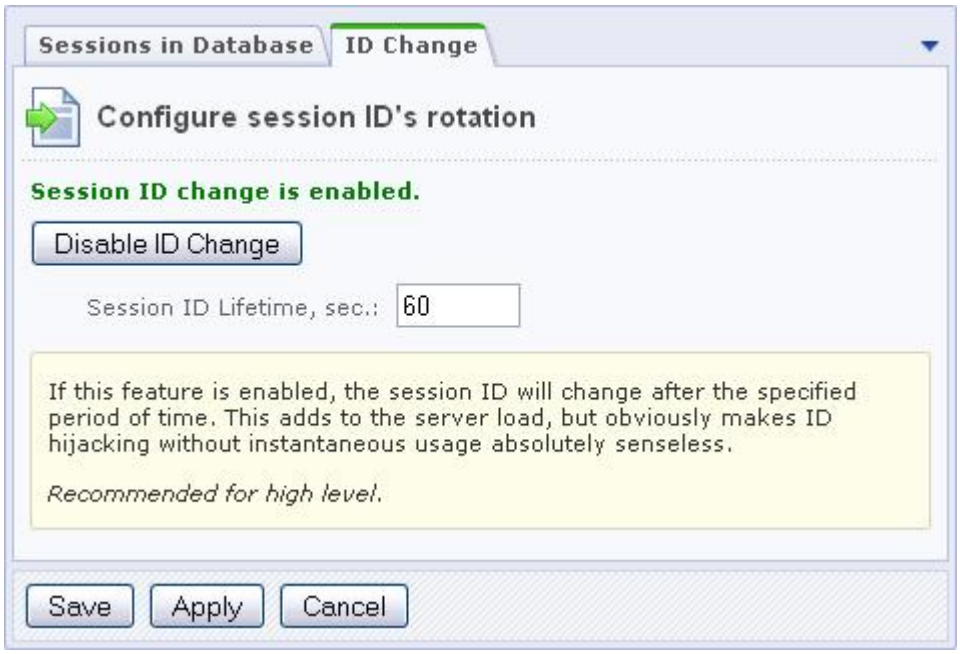


Fig. 1.17 Session ID change

Do the following to activate the ID change:

- specify the **Session ID Lifetime** (in seconds), which is the interval between two consecutive session ID changes;
- click **Enable ID Change**.

Changing the identifier increases the server load but makes the authorized session hijacking ineffective.

Note. The high protection level requires that you enable both of these protection mechanisms.

Redirect Phishing Protection

You can enable or disable the phishing protection at *Settings* > *Proactive Protection* > *Redirect protection* by clicking the big button fig. 1.18.

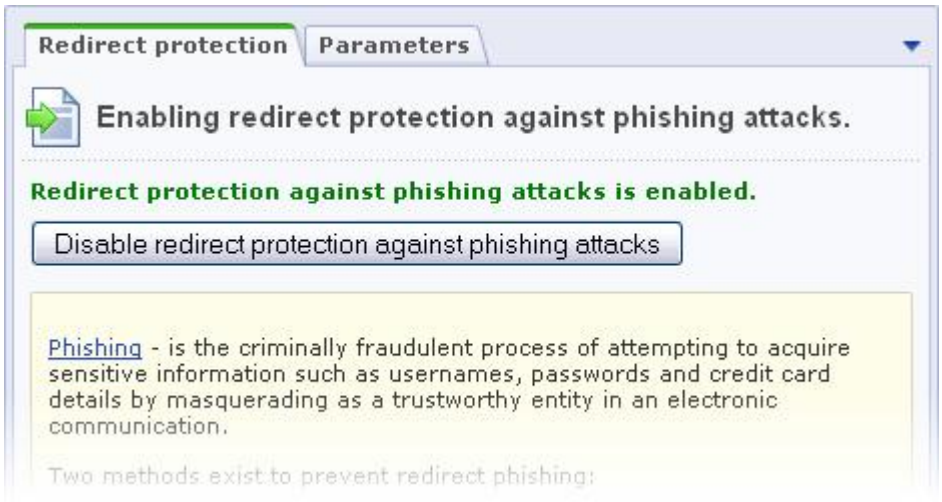


Fig. 1.18 The redirect phishing protection form

The following picture illustrates the phishing protection parameters (fig. 1.19):

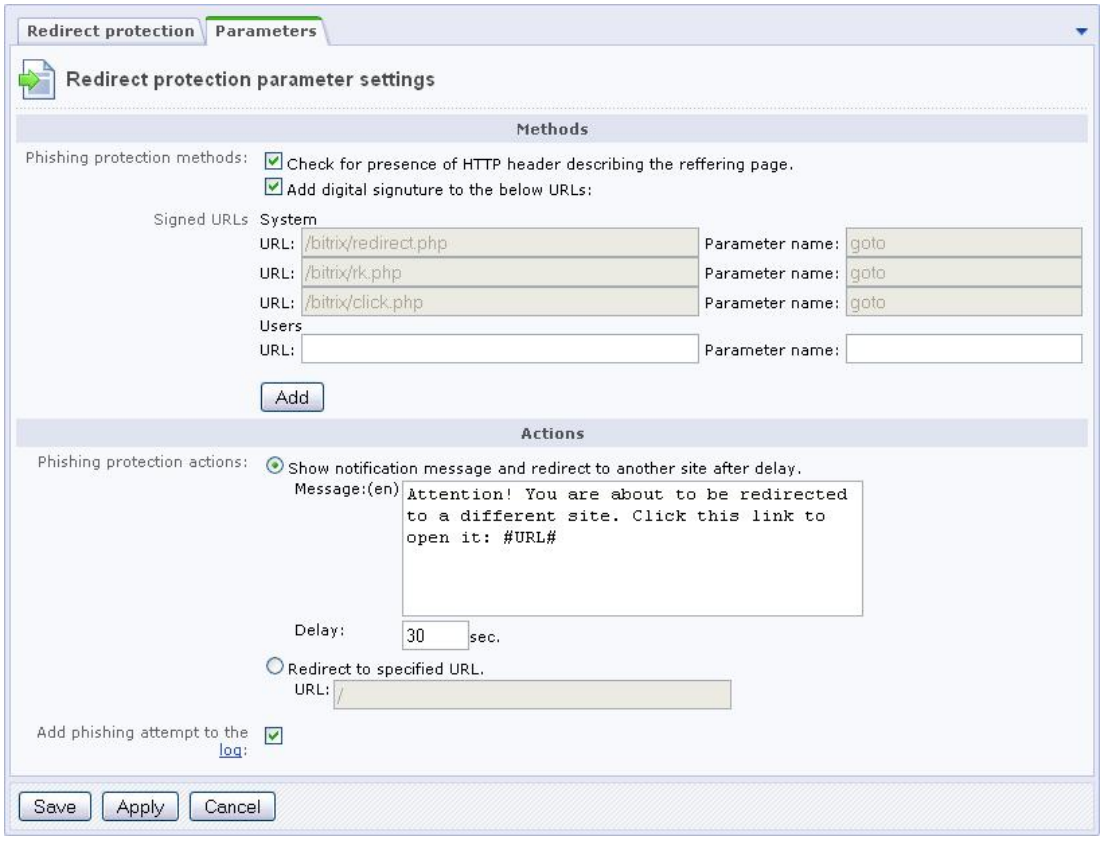


Fig. 1.19 The redirect protection settings sheet

You can protect your redirects by:

- checking a page for the presence of the HTTP header;
- signing the site links with a digital signature. This option specifies to add a special parameter which uniquely identifies the site and the transition to the system links. However, administrators can add their own links they want to protect.

The redirect protection can react in either of the following ways:

- redirect to a link URL showing a warning message and making a seconds delay. The message text and the delay duration are entered in the fields below;
- redirect to a fully, admittedly safe address. This can be the index page, for example.

Note: the standard protection level requires active phishing protection.

Highest Security Level

Remember that you first have to configure the parameters of the standard and high levels prior to configuring the highest protection (fig. 1.20):

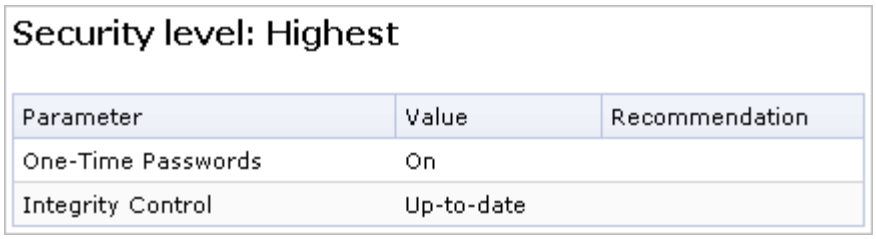


Fig. 1.20 Highest protection level

Note: if at least one parameter of the highest protection level takes an invalid value, the protection level whose parameters are completely configured takes effect with respect to parameters of other protection levels.

One-Time Passwords

The concept of one-time passwords empowers the standard authorization scheme and significantly reinforces the web project security. The one-time password system requires a physical hardware token (device) (e.g., Aladdin eToken PASS) or special OTP software. These passwords are especially recommended for use by the site administrators since they significantly improve security of the "Administrators" user group.

Note. You have to enable the one-time password system for the site to be protected at the highest protection level.

You can enable (or disable) one-time passwords on the *Settings* > *Proactive Protection* > *One-time passwords* form by clicking **Enable one-time passwords** (or **Disable one-time passwords**, fig. 1.21).

Fig. 1.21 One-time passwords

For the one-time password scheme, a corresponding tab is shown in the user profile form (fig. 1.22). The one-time password mechanism is configured for each user individually.

Fig. 1.22 User authentication settings

To enable users to authenticate using one-time passwords:

- Check **Enable Compound Passwords**.
- Enter the **Secret key** supplied with your OTP software.
- Initialize the device by entering two one-time passwords generated by the device consequently (for example: 111111 and 222222, see fig. 1.22).
- Save changes.

Now a user can authorize using their login and a compound password - a combination of the standard password and a one-time device password (6 digits). The one-time password (see item 2 on fig. 1.23) must be entered in the **Password** field after the standard password (item 1 on fig. 1.23) without space.

Fig. 1.23 The authorization form

The OTP authorization system was developed by the Initiative for Open Authentication OATH. The implementation is based on the HMAC algorithm and the SHA-1 hash function. To calculate the OTP value, the system takes the two parameters on input: the secret key (initial value for the generator) and the counter current value (the required cycles of generation). Upon initialization of the device, the initial value is stored in the device as well as on the site. The device counter increments each time a new OTP is generated, the server counter - upon each successful OTP authentication.

Hence, if a device button was pushed more than once (f.e. accidentally) but no successful OTP authentication took place, and the push count exceeds the **Password Check Window Size** value, the generator counter will become desynchronized making a user unable to authorize.

Fig. 1.24 The OTP password threshold parameter

In this case, a device and a user must be resynchronized by resetting the server value to that stored in a device. This procedure requires that a system administrator (or a user owning sufficient permission) generates two consequent OTP values and enters them in the user parameters form (fig. 1.22).

To avoid desynchronization, you can increase the **Password Check Window Size** value to, say, 100 or 1000.

Integrity Control

The **File integrity control** form (*Settings* > *Proactive Protection* > *Integrity Control*) serves to check the integrity of the system kernel, system area and public files.

Check the system integrity on a regular basis (at least weekly) for the site to be protected at the highest level. Perform the integrity control check before updating the system and collect the new file data afterwards.

Note. Some module updates may require the control script to be signed anew.

Running the Integrity Check

- Enter and remember your password. A strong password should have at least 10 characters containing letters and digits.
- Confirm the password in the corresponding field.

- Specify and remember a keyword. It must differ from the password.

Fig. 1.25 Signing the control script

- Click **Next**.

If you made no mistake with the password confirmation, the following message will appear (fig. 1.26):

Fig. 1.26 A successful signing message

Now you can collect the file information in order to check the system integrity.

Gathering the File Information

- Click the **Actions** tab and check the **Collect File Information** option (fig. 1.27):

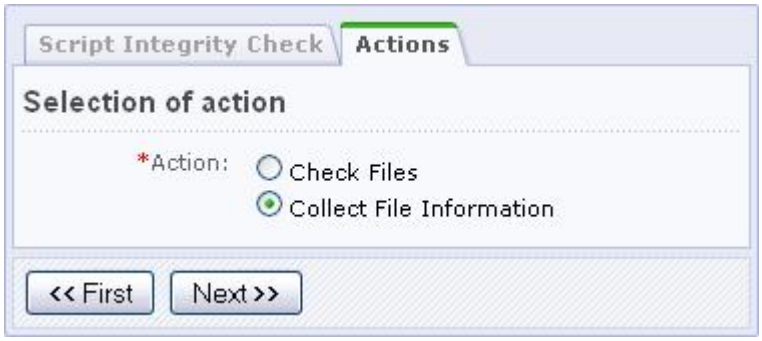


Fig. 1.27 Choosing the integrity control action

- Click **Next**. The following form will open (fig. 1.28):

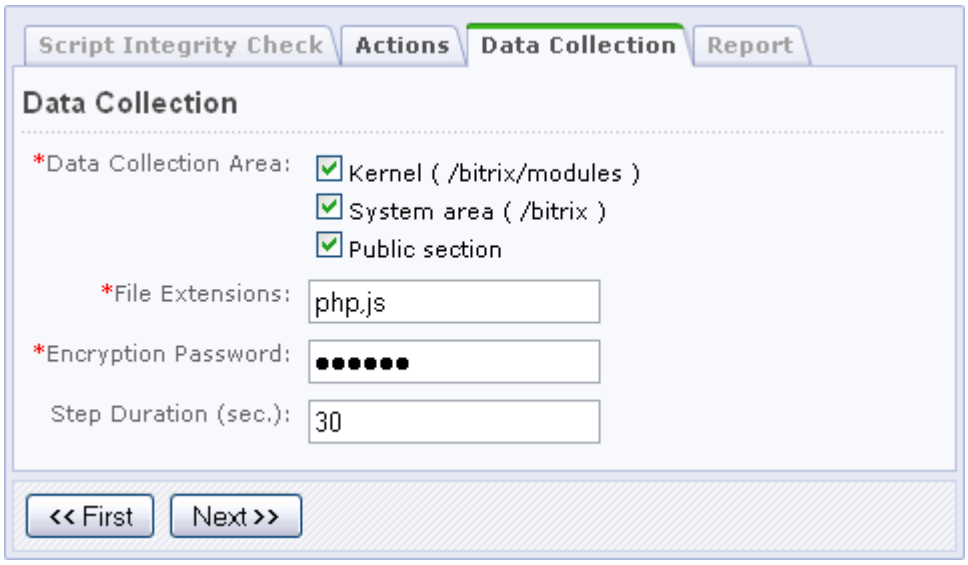


Fig. 1.28 Collecting the file data

- Set the data collection parameters:

  - **Data Collection Area** – select the system folders you want to process.
  - **File Extensions** – specify extensions of files whose information is to be collected. Separate multiple extensions with comma, without space.
  - **Encryption Password** – type here and remember the password which will be used to encrypt and decrypt the verification file.
  - **Step Duration** – specify the duration of a single data collection step, in seconds.

- Click **Next** to start data collection. Upon completion, download the data file to your local computer for better security (fig. 1.29).

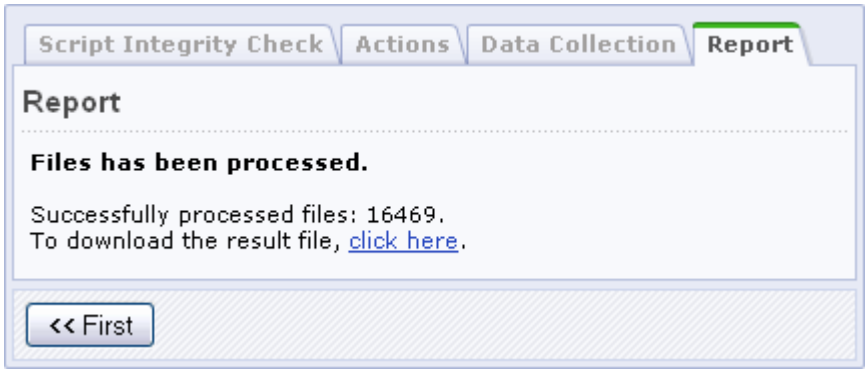


Fig. 1.29 File processing has finished

The verification data file is now ready, you can check the system integrity.

Checking the System Integrity

Every (except the first) time you start the system integrity check, the verification script is checked for unintentional or malicious changes.

- Enter the password (fig. 1.30) you have used to sign the verification script (fig. 1.25) and click **Next**.

Fig. 1.30 Checking the verification script

Ensure the verification script prints the keyword you have specified for signing (fig. 1.31).

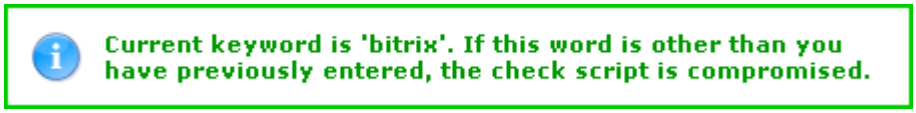


Fig. 1.31 A check result message

Note: if the keyword differs from the one you have previously entered, the integrity control script is compromised which means it has been modified and

cannot be trusted. In this case, you have to supersede the control script (for example, rollback to version 8.0.0).

- Click the **Actions** tab and activate the **Check Files** option (fig. 1.32).

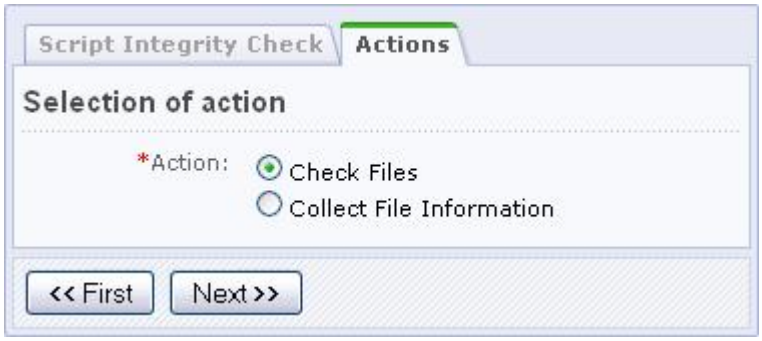


Fig. 1.32 Selecting the action

- Click **Next** to open the verification data file selection form (fig. 1.33):

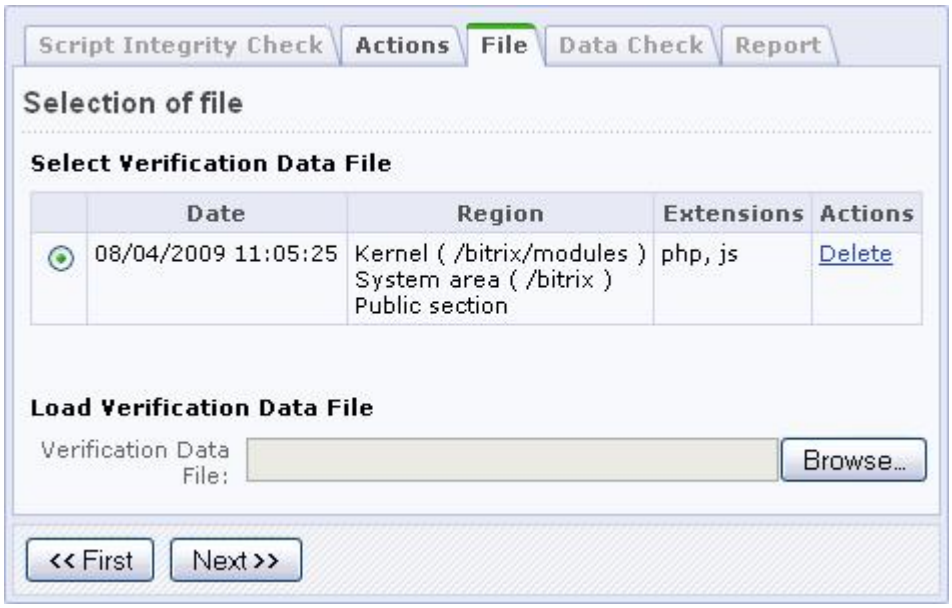


Fig. 1.33 Selecting the verification data file

- Select one of the existing log files or upload the log file from your machine using **Browse**. The following form will open (fig. 1.34).

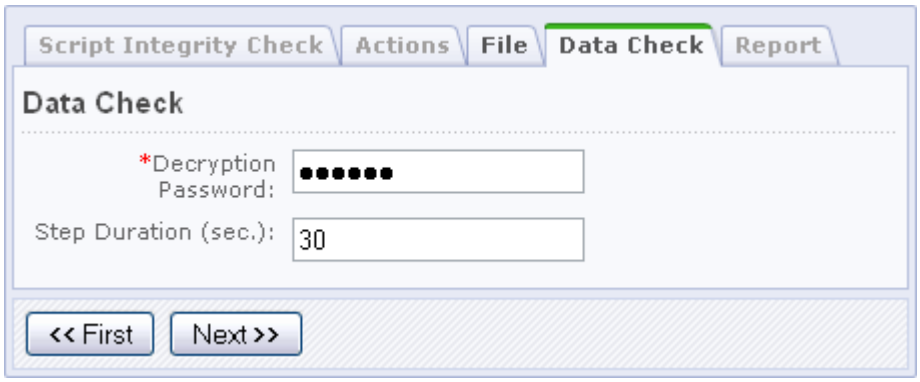


Fig. 1.34 Checking the data

- In the appropriate filed, type in the decryption password you specified when creating the verification data file.
- Specify the duration of a single check step (less times give more server stress).
- Click **Next** to start checking the system integrity. On completion, the following report will be displayed (fig. 1.35):

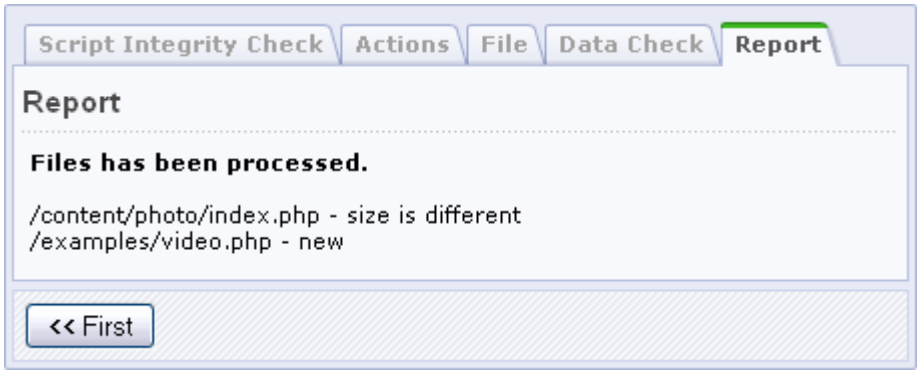


Fig. 1.35 System files verification report

Chapter 2. Additional Configuration Options

The Stop List

The **Proactive Protection** module has a private stop list (*Settings* > *Proactive protection* > *Stop List*, fig. 2.1). This feature is different from the **Web analytics** module stop list.

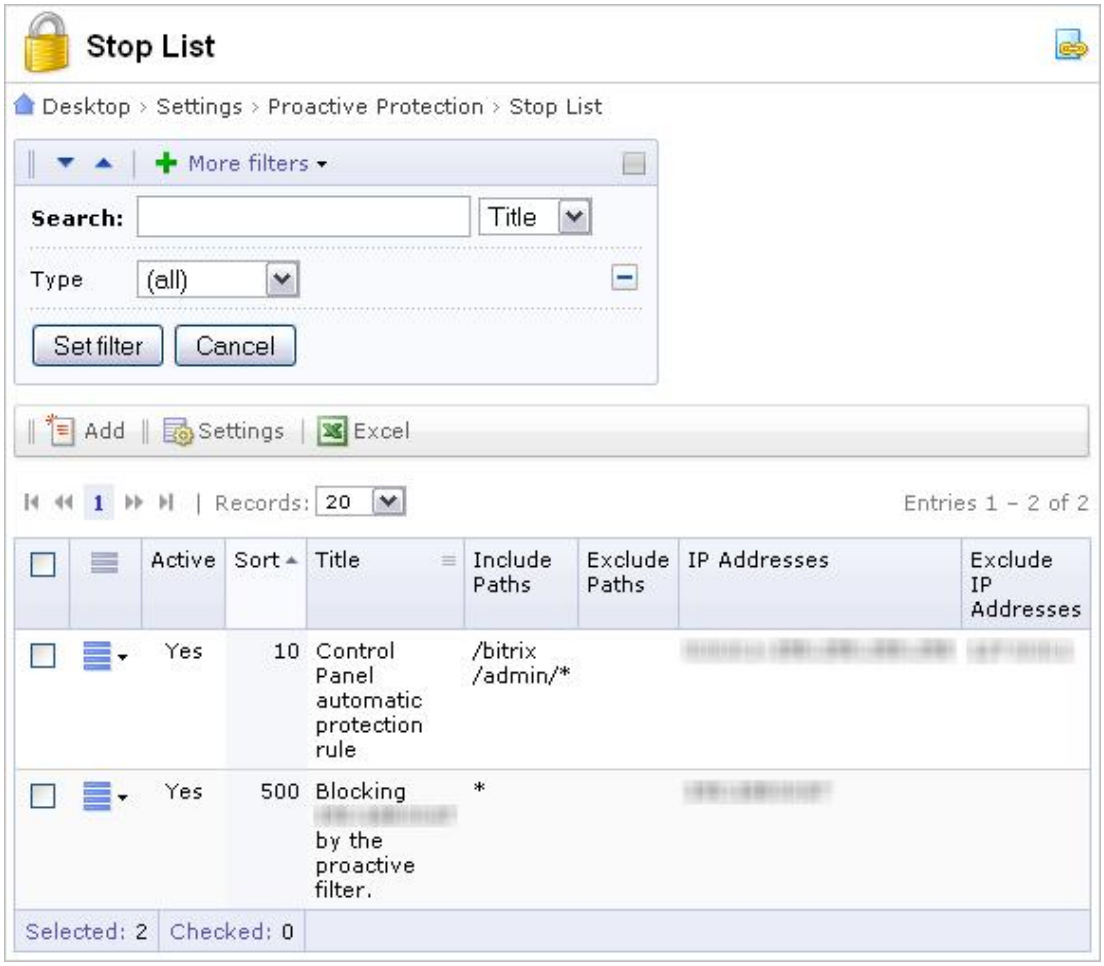


Fig. 2.1 The proactive protection stop list

The **Stop List** page shows existing rules aimed to restrict access to your site (as a whole or individual areas) from IP addresses listed in the rules. If **Active** is green, the rule is valid; if red – the rule is expired.

The access restriction records can be created manually or automatically. The rule will be created automatically if:

- the Control Panel protection mechanism is enabled;

§ the proactive filter responds to an intrusion attempt (if the **Add Attacker's IP Address to Stop List** option is selected as the attack response action, fig. 1.4).

You may want to add restriction rule manually, for example, when analyzing the intrusion logs. To do so:

q click **Add** on the context toolbar in the stop list page. The rule editor form will open (fig. 2.2).

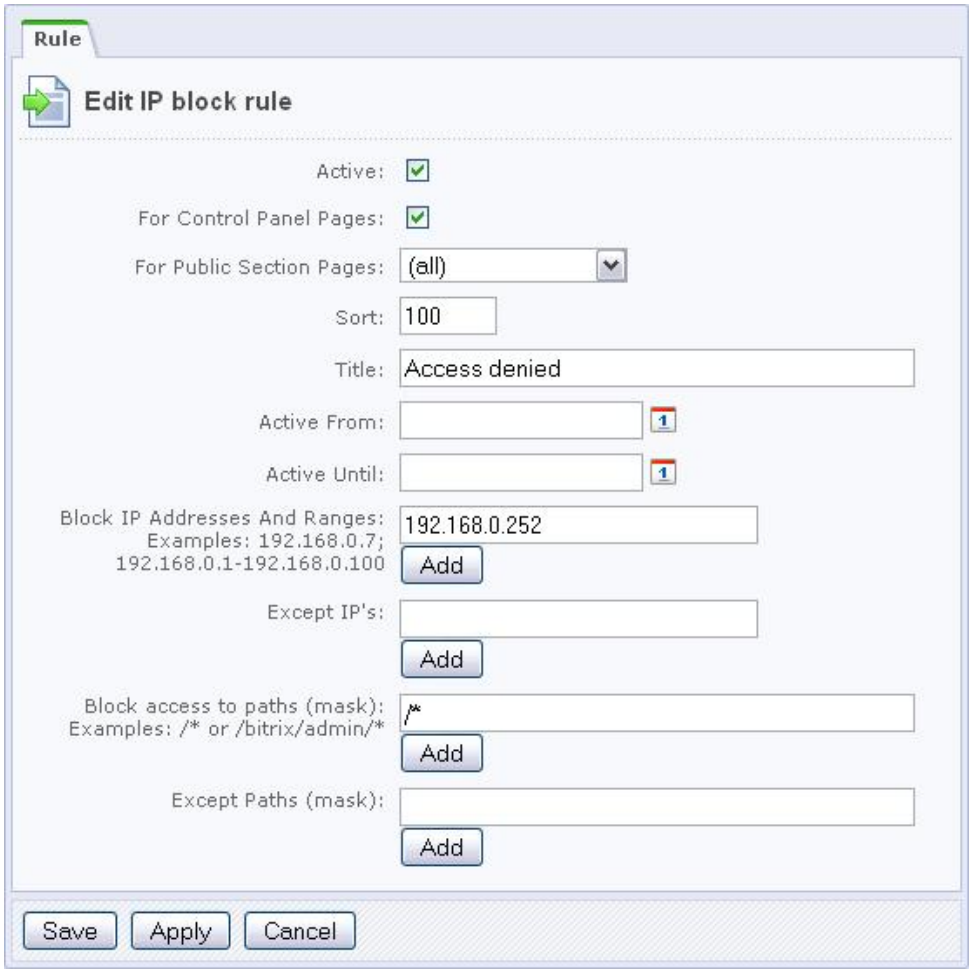


Fig. 2.2 Creating a stop list rule

q Fill in the form fields as required.

You can restrict access to the Control Panel or public pages for certain IP addresses or address ranges. Any rule can have one or more exceptions which can be set by IP or paths wildcards.

Note. Each IP address or path wildcard is typed in a separate field. Click **Add** to reveal more fields. Specify IP ranges using dashes, for example: 192.168.0.1-192.168.0.100.

- Save changes.

Now, if a user whose IP address matches the rule attempts to access your site, they will see a HTTP 403 error message, which effectively means that access is denied.

Final Notes

This manual has given you some insight of using the **Proactive protection** module to provide better security for your web site.

You can ask your questions at the Bitrix corporate forum:

http://www.bitrixsoft.com/support/forum/,

Should you have any difficulty using Bitrix Site Manager, do not hesitate to send a request to the technical support service:

http://www.bitrixsoft.com/support/