CitiDirect® Portal
Security, technical requirements and configuration

CitiService
CitiDirect Helpdesk
tel. 801 343 978, +48 22 690 15 21
Monday to Friday; 8:00 – 17:00
helpdesk.ebs@citi.com

www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

citi handlowy®

Table of Contents

1. Security

We have implemented very high security standards to ensure our Clients are always safe when using CitiDirect, CitiDirect Mobile and CitiDirect Tablet. However, please remember that the security of your funds also depends on you.

1.1 User Identification and Verification

Access to CitiDirect is granted to Users who log into the system with their SafeWord card (token) or mobile token MobilePASS.

Each card is assigned to a particular User. The card generates dynamic, one-time passwords, which significantly reduce the risk of unauthorized access to CitiDirect, for example as a result of password theft or cracking. In addition, the card is protected with a 4-digit PIN code, known only to its holder. Card holders may change their PIN codes at any time.

1.2 User Entitlement Levels

User entitlements are controlled via their access profiles, which determine a specific level of access to functionalities in CitiDirect. Access profiles assigned to Users define:

- access to particular accounts and transaction types
- operations allowed under transactions with a predefined limit
- authorization schemes and limits, etc.

1.3 Multi-level Transaction Authorization

Even the best designed internal processes can prove insufficient, for example when a single person has full control over transactions in the system. That is why we recommend authorization schemes that require transactions to be accepted by at least one additional User.

The Bank offers as many as 9 authorization levels. If a higher authorization level is required when making payments in CitiDirect, the security level can be significantly improved.

We recommend our Clients to define at least one transaction authorization level.

The Bank also offers other risk mitigating functionalities, like blocking manual submission of payment orders by Users, requiring authorization of created payment templates or defining payment limits. In order to configure such additional security mechanisms, please contact your Relationship Manager.

1.4 Encryption session and digital security certificate

All information, from Client identification through the end of a session in CitiDirect, is secured with the TLS (Transport Layer Security) protocol, which ensures the confidentiality of transmitted data with the use of advanced encryption methods.

TLS also protects data integrity. One of its elements is the Message Authentication Code (MAC), which checks verifies whether unauthorized data modification occurred during transmission.

Our electronic banking system https://portal.citidirect.com is secured with a Symantec Class 3 EV SSL CA – G3 digital certificate. This is the digital signature of a site which confirms that the User is using a service owned by Citi Handlowy. The certificate ensures that all confidential transactions executed via CitiDirect are encrypted.

Before you log in to the service, check if the certificate is valid and verify its issuer.

1.5 Automatic Session Expiration

Every session will end automatically after 20 minutes of inactivity to prevent a third party from accessing the accounts if the User forgets to log out.

1.6 Blocking Users

In order to ensure the security of your funds, the SafeWord card and Users are blocked automatically after seven unsuccessful attempts to log in and/or after 12 months since:

- the last login date – for Users who have logged into the system or
- the date of creating the user in the system – for Users who have never logged into the system.

In order to maintain access to the CitiDirect system on a given SafeWord card, we recommend logging into the system at least once every three months. A blocked SafeWord card should be replaced with a new one if a User intends to use the CitiDirect system in the future. This intention should be expressed in a separate application.

If your SafeWord card is lost or damaged, contact CitiService immediately (call **(22) 690 19 81** or **801 24 84 24**) to block access to CitiDirect.

We would like to bring your particular attention to the matter of online security – please read more at www.citidirect.pl/security.

Various aspects of security are presented in ordered sections, constituting an important source of information about the security of online payments and cyber threats related to the everyday use of electronic banking.

Irrespective of the multi-level security scheme implemented by Citi Handlowy:

- protect your personal data using other internet services
- protect tools and data for the registration and authorization of transactions
- use the latest version of your operating system and internet browsers
- use the latest version of your anti – virus software and firewall
- do not install illegal software from untrusted sources
- do not reply to e-mails asking you to provide personal data or access codes
- do not open attachments and do not click on any links in suspicious e-mails or SMS
- log in to the electronic banking system using a trusted computer and network (avoid so-called hot spots) by entering a specific URL – do not search using search engines
- verify that the connection is secure while logging in (https, SSL, TLS).

2. System requirements

2.1 Operating systems

The system is certified to operate on the following operating systems.

Windows® systems:

- Windows® 7 excluding: Arabic OS
- Windows® 10 excluding: Arabic OS.

Apple® macOS:

- Version 10.12 and higher.

2.2 Internet browsers

- Internet Explorer 11.0 (Windows 7)
- Internet Explorer 11.0 (Windows 10)
- Safari: version 10 and higher.

2.3 Java software (optional)

CitiDirect supports the following versions of Java:

- Java 8.

2.4 Adobe Reader

Adobe Reader is used to view reports generated in CitiDirect in PDF format. CitiDirect supports the following versions of Adobe Reader:

- Version 9.0 or higher.

2.5 Network/Internet Access

- transfer to/from external network (for a single station) min. 128 kbs, we recommend 512 kbs
- opened ports http (80) and https (443)
- no scanning, blocking, or caching Java and Active X applets from: https://portal.citidirect.com
- enabled TLS 1.2 protocol in browser and Java settings.

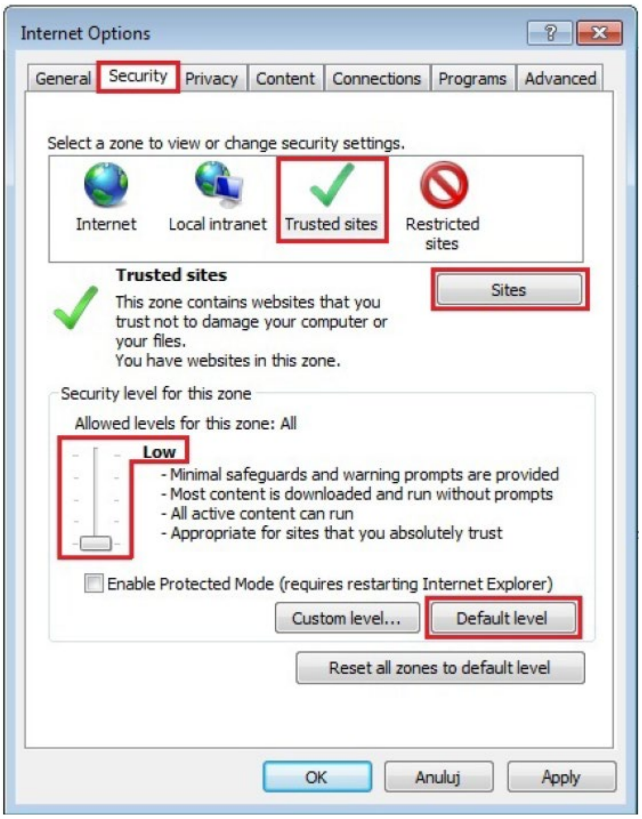
Detailed information about technical system requirements is available on the login page.

3. Configuration

3.1 Internet Explorer

CitiDirect works correctly with default Internet settings. To optimize performance, we recommend using the following settings.

Run the web browser and go to **Tools → Internet options**



Internet Options

Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

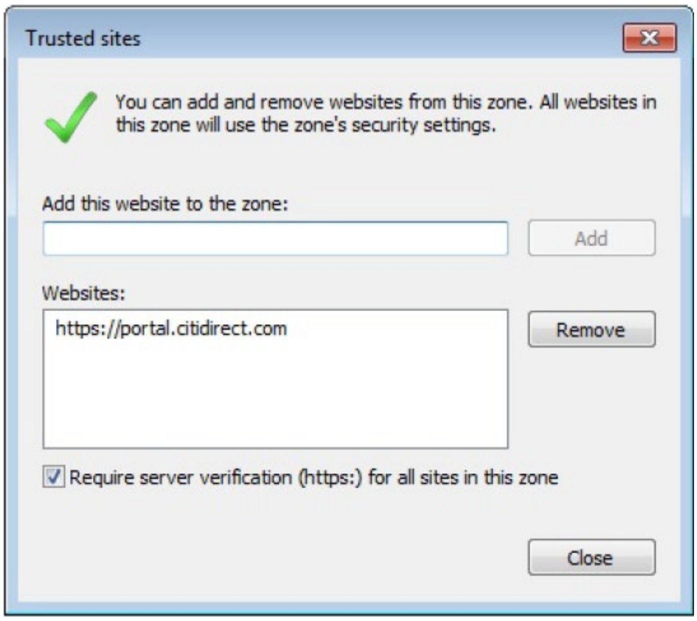
Allowed levels for this zone: All

Low
- Minimal safeguards and warning prompts are provided
- Most content is downloaded and run without prompts
- All active content can run
- Appropriate for sites that you absolutely trust

☐ Enable Protected Mode (requires restarting Internet Explorer)

Security tab

In the select a zone window click **Trusted sites**. The security level for this zone will probably be set as custom. Reset settings by clicking the **Default level** button and move the slide bar to the lowest security setting.



Trusted sites

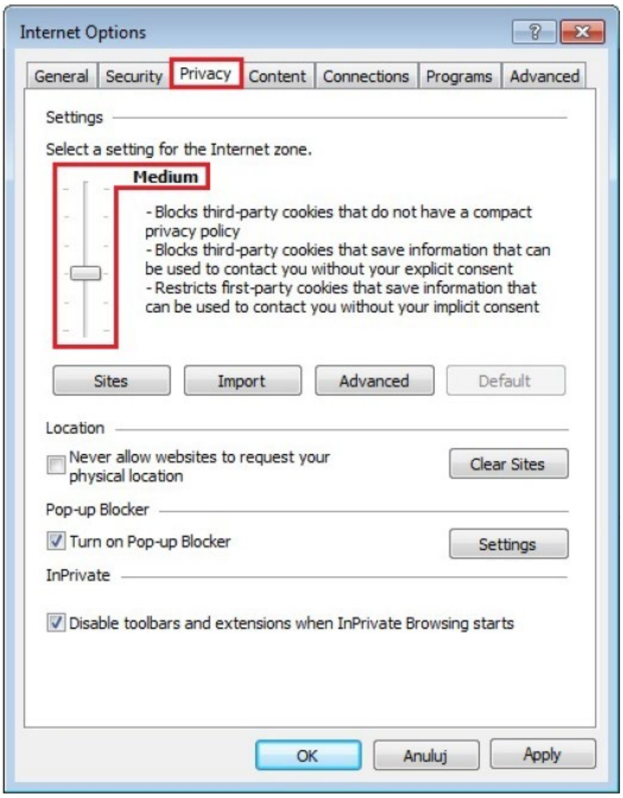
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:
https://portal.citidirect.com

☑ Require server verification (https:) for all sites in this zone

Open the trusted sites list by clicking the **Sites** button and add the CitiDirect system site address: https://portal.citidirect.com.



Internet Options

Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Location

□ Never allow websites to request your physical location

Pop-up Blocker

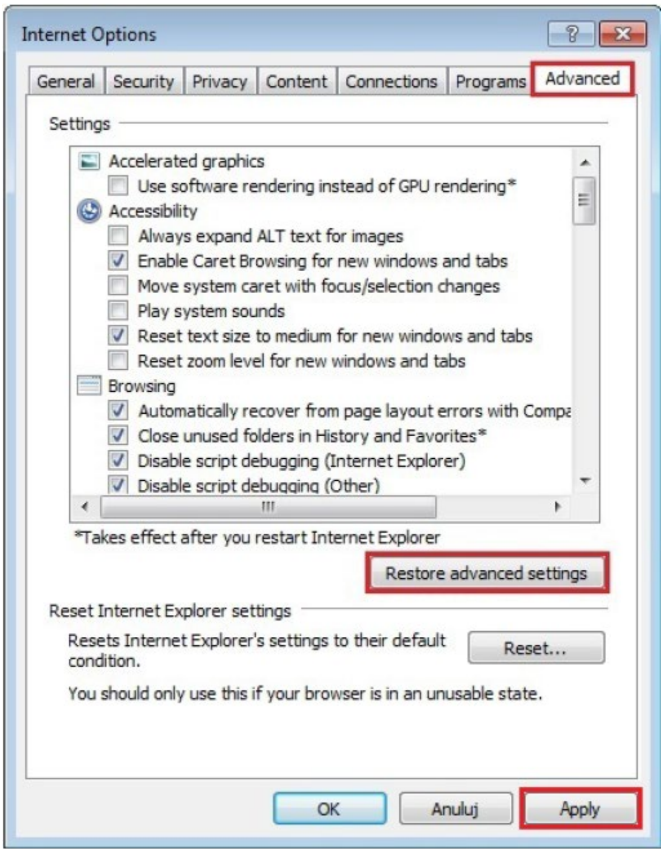
☑ Turn on Pop-up Blocker

InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

Privacy tab

The settings section determines whether the web browser remembers the User created on the login page. Default level – Medium – or lower should be selected here.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

- Accelerated graphics
  - □ Use software rendering instead of GPU rendering*
- Accessibility
  - □ Always expand ALT text for images
  - ☑ Enable Caret Browsing for new windows and tabs
  - □ Move system caret with focus/selection changes
  - □ Play system sounds
  - ☑ Reset text size to medium for new windows and tabs
  - □ Reset zoom level for new windows and tabs
- Browsing
  - ☑ Automatically recover from page layout errors with Compa
  - ☑ Close unused folders in History and Favorites*
  - ☑ Disable script debugging (Internet Explorer)
  - ☑ Disable script debugging (Other)

*Takes effect after you restart Internet Explorer

Restore advanced settings

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

Reset...

You should only use this if your browser is in an unusable state.

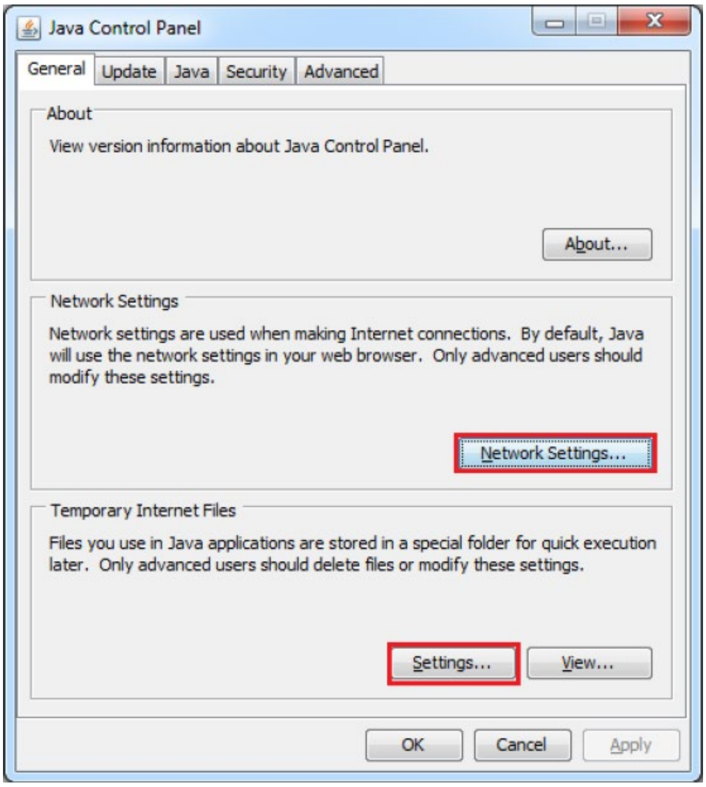
OK | Anuluj | Apply

Advanced tab

We recommend using default settings. If you are not sure if your settings are set to default, click the **Restore advanced settings** button and **Apply**.

3.2. Java Sun

From Windows **START** menu, select **JAVA CONFIGURATION**.



Java Control Panel

General | Update | Java | Security | Advanced

About

View version information about Java Control Panel.

About...

Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Network Settings...

Temporary Internet Files

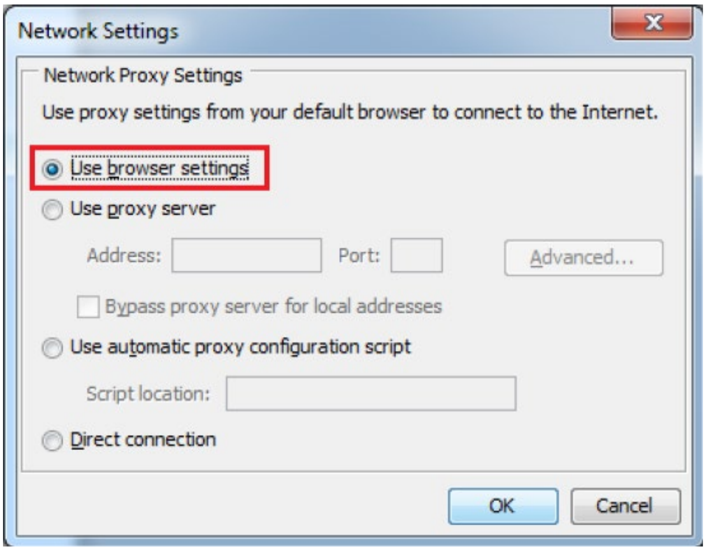
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

Settings... | View...

OK | Cancel | Apply

General tab

Settings affecting CitiDirect are located in the **Network Settings** and **Temporary Internet Files** sections.



Network Settings

Network Proxy Settings

Use proxy settings from your default browser to connect to the Internet.

● Use browser settings

○ Use proxy server

Address: Port: Advanced...

□ Bypass proxy server for local addresses

○ Use automatic proxy configuration script

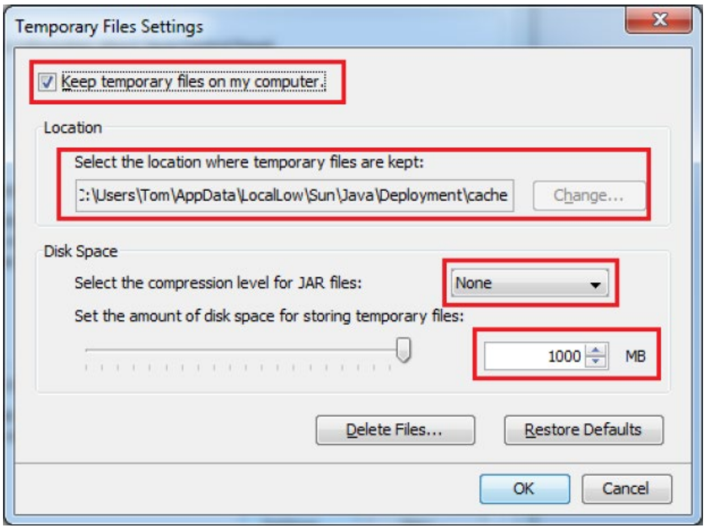
Script location:

○ Direct connection

OK Cancel

Network Settings

Choose the option **Use browser settings**.



Temporary Files Settings

☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

:\Users\Tom\AppData\LocalLow\Sun\Java\Deployment\cache Change...

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files:

1000 MB

Delete Files... Restore Defaults

OK Cancel

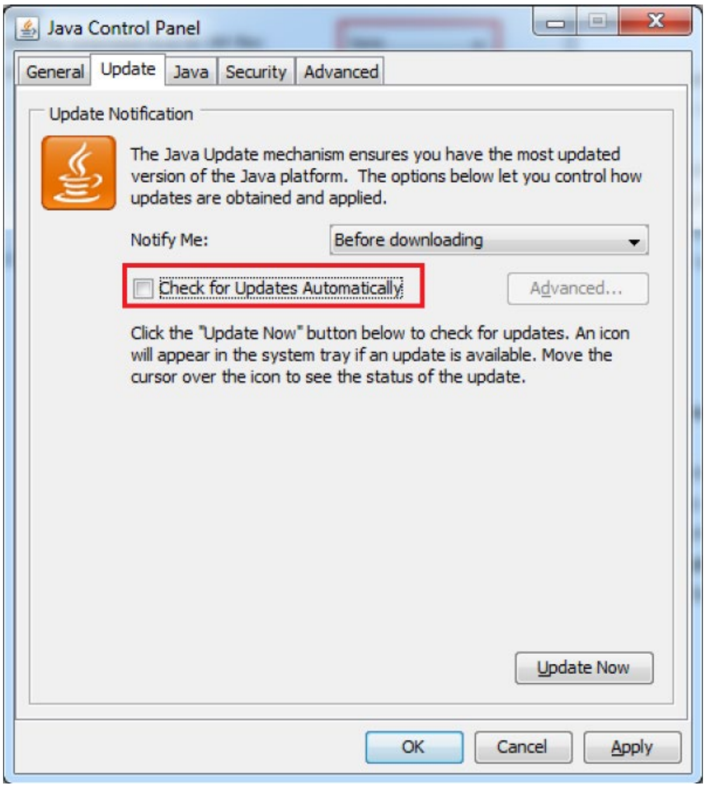
Temporary Internet Files

Keep temporary files on my computer – this option has to be checked.

Location – Windows User needs to have full access to the folder indicated here.

The compression level has to be set at **None**.

The amount of free space on the hard drive should be at least 250 MB. Default setting – **1000 MB**.



Java Control Panel

General | Update | Java | Security | Advanced

Update Notification

The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.

Notify Me: Before downloading

□ Check for Updates Automatically Advanced...

Click the "Update Now" button below to check for updates. An icon will appear in the system tray if an update is available. Move the cursor over the icon to see the status of the update.

Update Now

OK Cancel Apply

Update tab

We recommend turning automatic updates off. In order to do that, uncheck the **Check for updates Automatically** option.

www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

citi handlowy®

Bank Handlowy in Warsaw S.A. with its registered office in Warsaw, ul. Senatorska 16, 00-923 Warsaw, entered into the Register of Entrepreneurs of the National Court Register by the District Court for the Capital City of Warsaw in Warsaw, 12th Commercial Division of the National Court Register, under no. KRS 000 000 1538; NIP 526-030-02-91; share capital of PLN 522,638,400, fully paid up. This material has been published solely for information purposes and it does not constitute an offer within the meaning of Article 66 of the Polish Civil Code.