



# **Optimal Biz Windows Client Reference Manual**

Last update date October 16, 2022  
(Website ver.9.13.1)  
OPTiM Corporation

---

# Getting Started

## Purpose of this manual

This manual explains operation of Windows device.

## How to read this manual

The following two methods are available for managing Windows devices. Refer to individual pages for operation procedure.

- Device management by installed Windows agent

- ☞ "Agent Basic Operations" Page 13

- ☞ "Stop Agent Use" Page 66

- Device management by Optimal Biz with MS-MDM function


- 📖 "MS-MDM Authentication" in <Windows Kitting Manual>

In addition, this manual is written when installing on Windows 10 Mobile device. When operating on a tablet device, read "click" as "tap", "double click" as "double tap", "right click" as "press & hold" or "press & tap".

The meanings of symbols and marks used in the explanation of this manual, the types of screens used in manuals, and notes are as follows.

### ◆ About the symbol ·mark

The marks and symbols used in the manual are as follows.

Symbols / Mark	Description
[ ]	Represents menu name, button name, and link name.
“ ”	Represents the name you want to emphasize, such as tab name, function name, item name, reference destination in the manual.
< >	Represents the manual name or the document name.
⇒	Represents the result of the operation.
📖	Represents the manual or document to be referenced.
☞	Represents the reference in the manual and the link to the website.
⚠	Explains what to watch out for.
📝	Explains points of handling and operation and what is convenient to know.
Operation	In the explanation of the screen, describes the menu operation for displaying the corresponding screen. Ex.) Operation [Settings]→[iOS]→[Applications]→[Application Distribution]→ 

### ◆ About the screen

- The version notation on the screen may differ from the actual one.

---

## About website URL

---

URLs of websites other than our company described in the manual are subject to change without notice.

## About trademark

---

- Company names and product names mentioned are trademarks and registered trademarks of each company.

---

## Table of contents

<b>1 About Windows client.....</b>	<b>6</b>
1.1 Overview .....	7
1.2 OS support policy .....	7
1.3 Agent System Requirement.....	8
1.4 Agent System Requirement (Windows Server) .....	9
1.5 System Requirement for MS-MDM.....	9
1.6 Roles for Agent and MS-MDM .....	10
1.7 Agent and MS-MDM collecting information .....	10
<b>2 Agent Basic Operations .....</b>	<b>13</b>
2.1 Install Agent.....	14
2.2 Screen Layout .....	14
2.2.1 How to use agent .....	14
2.2.2 Details of tray icon.....	14
2.2.3 Display task tray icon menu .....	15
2.2.4 Description on tray icon menu .....	16
2.2.5 Show Toolbar.....	17
2.2.6 Details of toolbar .....	17
2.2.7 Open control panel.....	18
2.2.8 Details of control panel.....	19
2.3 Confirm information of a Windows device or the agent.....	20
2.4 Sync with management site.....	22
2.5 Register Asset Information .....	23
<b>3 Proxy authentication .....</b>	<b>26</b>
3.1 Proxy authentication .....	27
3.2 Change the settings of proxy authentication .....	28
<b>4 Remote Support.....</b>	<b>29</b>
4.1 Receive Remote Support .....	30
<b>5 Remove remote lock.....</b>	<b>32</b>
5.1 How to use remote lock screen.....	33
5.2 Remove remote lock.....	34
5.3 Sync with management site on lock screen .....	37
<b>6 Update agent.....</b>	<b>39</b>
6.1 Update agent .....	40
<b>7 Drive Encryption .....</b>	<b>43</b>
7.1 Drive Encryption .....	44

---

<b>8 SIM Monitoring</b>	<b>47</b>
<b>8.1 Timing of operation and release method</b>	<b>48</b>
8.1.1 Timing of registered as regular SIM	48
8.1.2 Timing of released from regular SIM	48
8.1.3 Timing of displayed the lock screen	49
8.1.4 Release the lock screen	49
<b>9 SaaS ID Federation</b>	<b>50</b>
<b>10 Windows Information Protection (WIP)</b>	<b>51</b>
<b>10.1 Target file</b>	<b>52</b>
10.1.1 Create a new file to be protected	53
10.1.2 Set as protected file	54
10.1.3 Check the management status of protected files	55
10.1.4 Remove protection from a file	56
10.1.5 Verify ownership	57
10.1.6 How it looks in a shared folder	60
<b>10.2 Message displayed when data is shared</b>	<b>62</b>
10.2.1 Messages for each protection level	62
<b>10.3 Operation using USB</b>	<b>63</b>
10.3.1 To copy protected files created on a WIP-adaptive terminal to USB	63
10.3.2 When the file to be protected exists in the USB and is opened on a different device under different conditions	64
10.3.3 Recovering data via USB	65
<b>11 Stop Agent Use</b>	<b>66</b>
<b>11.1 Finish agent</b>	<b>67</b>
11.1.1 Finish agent	67
11.1.2 Re-Launch agent	69
<b>11.2 License activation</b>	<b>70</b>
11.2.1 Deactivate agent	70
11.2.2 Activate Agent	72
<b>11.3 Delete agent</b>	<b>74</b>

---

# 1 About Windows client

Describes the following items.


Item	Page
<a href="#">Overview</a>	<a href="#">7</a>
<a href="#">OS support policy</a>	<a href="#">7</a>
<a href="#">Agent System Requirement</a>	<a href="#">8</a>
<a href="#">Agent System Requirement (Windows Server)</a>	<a href="#">9</a>
<a href="#">System Requirement for MS-MDM</a>	<a href="#">9</a>
<a href="#">Roles for Agent and MS-MDM</a>	<a href="#">10</a>
<a href="#">Agent and MS-MDM collecting information</a>	<a href="#">10</a>

## 1.1 Overview

Optimal Biz (hereinafter referred to as this product) is a support service that manages and operates devices without requiring expert knowledge. By installing the application "Optimal Biz Agent (hereinafter referred to as agent)" on the Windows device, or by using Optimal Biz via MS-MDM (MDM function incorporated in Windows) (\*1) You can manage the device from Optimal Biz management site (hereinafter referred to as the management site).

\*1: Refer to the following for target OS.


 "System Requirement for MS-MDM" Page 9

 This manual is the operation manual of Windows devices. For operation of the management site, refer to the following.

 <Management Site Reference Manual>




## 1.2 OS support policy






In this product, OS support policy was established with the aim of ensuring product operation and security functions. We will end support of lower OS version on a regular basis, so customers who use OS and devices that are not subject to support will be requested to update OS or change model.

Support policy	Example of support
<ul style="list-style-type: none"> <li>● Compliant with Microsoft's OS support policy.</li> <li>● With the addition of the latest supported OS, as for the OS version that became out of support, we respond to inquiries as much as possible only for one year from the date the support period expires as transition period. Operation guarantee and trouble correspondence are not performed.</li> </ul>	<ul style="list-style-type: none"> <li>● Windows 8.1 : Support until 2023/01/09</li> <li>● Windows 10 : Support until the deadline stipulated in each edition, version</li> <li>● Windows 11 : Support until the deadline stipulated in each edition, version</li> <li> Windows 8 and Windows 7 are no longer supported.</li> </ul>

## 1.3 Agent System Requirement

Windows client system requirement is as follows.




OS	Windows 8.1 Windows 8.1 Pro Windows 8.1 Enterprise Windows 10 Home (2004 or later) Windows 10 Pro (2004 or later) Windows 10 Enterprise (1909 or later) Windows 10 Enterprise 2015 LTSC Windows 10 Enterprise 2016 LTSC Windows 10 Enterprise 2019 LTSC Windows 10 Education (1909 or later) Windows 11 Home (21H2 or later) Windows 11 Pro (21H2 or later) Windows 11 Education (21H2 or later) Windows 11 Enterprise (21H2 or later)  Windows RT and RT 8.1 are not supported.  Supports 32 bit and 64.  For Windows 10 Home/Pro, 64-bit ARM is supported.
CPU	Greater than 1GHz
Memory	1GB (32bit) / 2GB (64bit) or greater in RAM
HDD	1GB or greater free space
Network Connection	Enable to connect to the internet via 3G, Wi-Fi or wired network connection. Available to communicate HTTPS (port 443) to the management site with / without proxy.


-  Support for agent: Optimal Biz supports the agent for 180 days after release. Also supported are two newest generations of released agents.
-  If group policy is set by the system, group policy takes precedence and functions may not be available. Contact your administrator about group policy.
-  Windows agents may become slow or syncing may take time immediately after the PC starts up or during virus scanning. Add the Windows agent to the antivirus software safelist and check the status.
-  The ARM 64-bit version cannot collect device information within the same network.
-  Only available in Japan.



## 1.4 Agent System Requirement (Windows Server)

The system requirement for using Windows Server as Windows client is as follows.

OS	Windows Server 2012 Windows Server 2012 R2  Supports 32bit and 64bit versions.  Also supports Windows Small Business Server 2011.  Only supports Windows Servers with X86 architecture. Itanium-based Systems OS are not supported.
CPU	Greater than 1GHz
Memory	System environment for Windows Server is compliant with Window Server's own system requirements.
HDD	1GB or greater free space
Network Connection	Able to connect to the Internet via Wi-Fi or a wired network connection. Able to communicate HTTPS (port 443) to management site with and without proxy.

 Support for agent: Optimal Biz supports the agent for 180 days after release. Also supported are two newest generations of released agents.

 Only available in Japan.

## 1.5 System Requirement for MS-MDM



The system requirement when using the MS-MDM function is as follows.

OS	Windows 8.1 Windows 8.1 Pro Windows 8.1 Enterprise Windows RT 8.1
Network Connection	Able to connect to the internet via 3G, Wi-Fi or a wired network connection. Able to communicate HTTPS (port 443) to the management site with and without proxy.

 Only available in Japan.

## 1.6 Roles for Agent and MS-MDM

On the Windows client, agent and MS-MDM do the followings.

General	Function	Agent	MS-MDM
Collect Windows device information	Periodically collects Windows device information and sends the information to the server.	○	○
Windows device setting	Periodically collects setting information from the server and applies to Windows devices.	○	×
Collect device information within same network	<p>Periodically collects information from the network which the Windows agent belongs to. Device information of this network is sent to the server.</p> <p> Information may not be collected depending on the management site setting. For details on the settings, contact your administrator.</p> <p> The ARM 64-bit version cannot collect device information within the same network.</p>	○	×

## 1.7 Agent and MS-MDM collecting information

Information collected by agents and MS-MDM is as follows.

Category	Items	Agent	MS-MDM
Asset Information	OS version	○	○
	Computer Name	○	○
	Workgroup	○	○
	Windows Version	○	○
	System Manufacturer	○	○
	System Model	○	○
	Serial Number	○	○
	Type	○	×
	Location data	○	×
	Default Web Browser Name	○	×
	Default Web Browser Version	○	×
	Default Mailer Name	○	×
	Default Mailer Version	○	×
	Default Printer Name	○	×
	Default Printer Port	○	×
	List of apps	○	×
	Windows automatic update	○	×
	Firewall	○	×
	Anti-virus	○	×
	Anti-spyware	○	×
	Screen saver	○	×

Category	Items	Agent	MS-MDM
	Drive Encryption	○	×
	Password Policy	○	×
	Password Expiration Period	○	×
	Number of Password History	○	×
	Period in Which Password Change Is Prohibited	○	×
	Require complex password	○	×
	Remote Lock Status	○	×
	Remote Desktop	○	×
	SIM Monitoring Registered SIM List	○	×
	Microsoft Update Program	○	×
Hardware Information	CPU	○	×
	Memory	○	×
	Motherboard	○	×
	Video Card	○	×
	TPM Version	○	×
	BIOS manufacturer	○	×
	BIOS Version	○	×
	BIOS Release Date	○	×
	Total Drive Space	○	×
	Drive Free Space	○	×
	User Name	○	×
	SID	○	×
Network information	Global IP Address	○	○
	NIC Name	○	○
	Connection Type	○	○
	MAC Address	○	○
	IP Address	○	○
	Default Gateway	○	○
	DHCP	○	○
	DHCP Server	○	○
	DNS Server	○	○
	DNS Suffix	○	○
	Network	○	○
Agent Information	Agent Version	○	○
	Communication Date	○	○
	Authentication Date / Time	○	○

Category	Items	Agent	MS-MDM
Optimal Biz Information	Zone	○	×
	Policy	○	×
	Log	○	×

- ✎ Since the above information is collected directly from the OS, information not recognized by the OS is not reflected on the management site.
- ✎ Even when device is communicating via mobile communication such as 3G/LTE, MAC address information (such as Wi-Fi and LAN board info.) will be utilized for agent activation.

---


## 2 Agent Basic Operations

Describes the following items.

Item	Page
<a href="#">Install Agent</a>	<a href="#">14</a>
<a href="#">Screen Layout</a>	<a href="#">14</a>
<a href="#">Confirm information of a Windows device or the agent</a>	<a href="#">20</a>
<a href="#">Sync with management site</a>	<a href="#">22</a>
<a href="#">Register Asset Information</a>	<a href="#">23</a>


## 2.1 Install Agent


This product manages Windows devices via agents. For details, refer to the following.

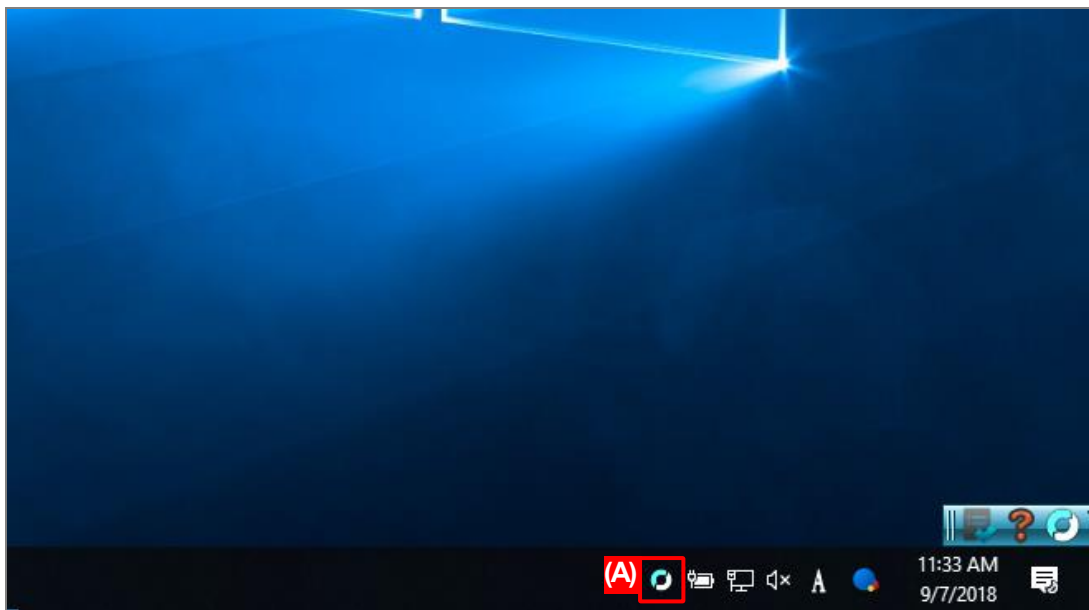
 "Install Agent" - "Install Agent" in <Windows Kitting Manual>

## 2.2 Screen Layout

### 2.2.1 How to use agent






**[1] Check the  (tray icon)(A) to confirm the status of agent.**

 When location information retrieval is changed to either enabled or disabled, a confirmation balloon is displayed on the screen.




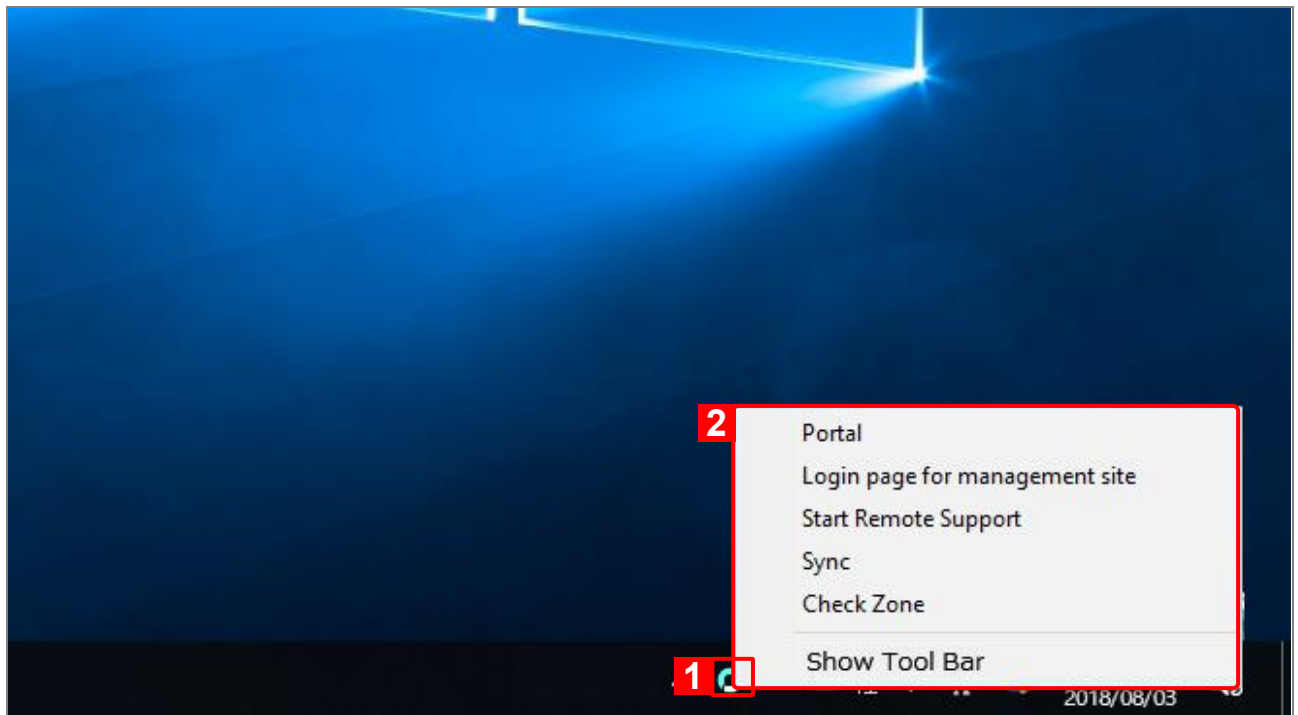
### 2.2.2 Details of tray icon

The tray icon shows you the status of the agent.

Status	Function
Normal  (Color display)	The agent is operating normally.
Failed to connect to the server  (Gray display)	The agent is not connected to the management server. Your PC is not connected to the internet, or the agent is paused. If the agent is paused and you want to start the agent again, see the following.  "Re-Launch agent" Page 69
Inactivated  (Color display with icon of red "!")	The agent is not activated. Refer to the following and activate license.  "Activate Agent" Page 72

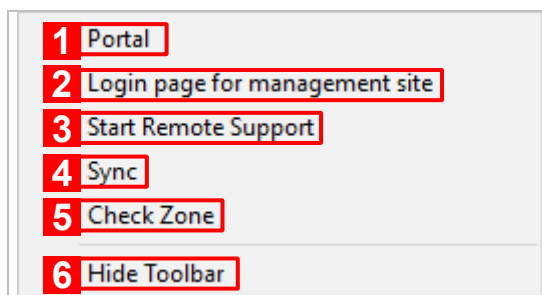
### 2.2.3 Display task tray icon menu

- [1]** Right-click  (task tray icon).
- [2]** The task tray icon menu is displayed.



## 2.2.4 Description on tray icon menu


To use the function of this product, open a menu of the tray icon and click the function you want to use.

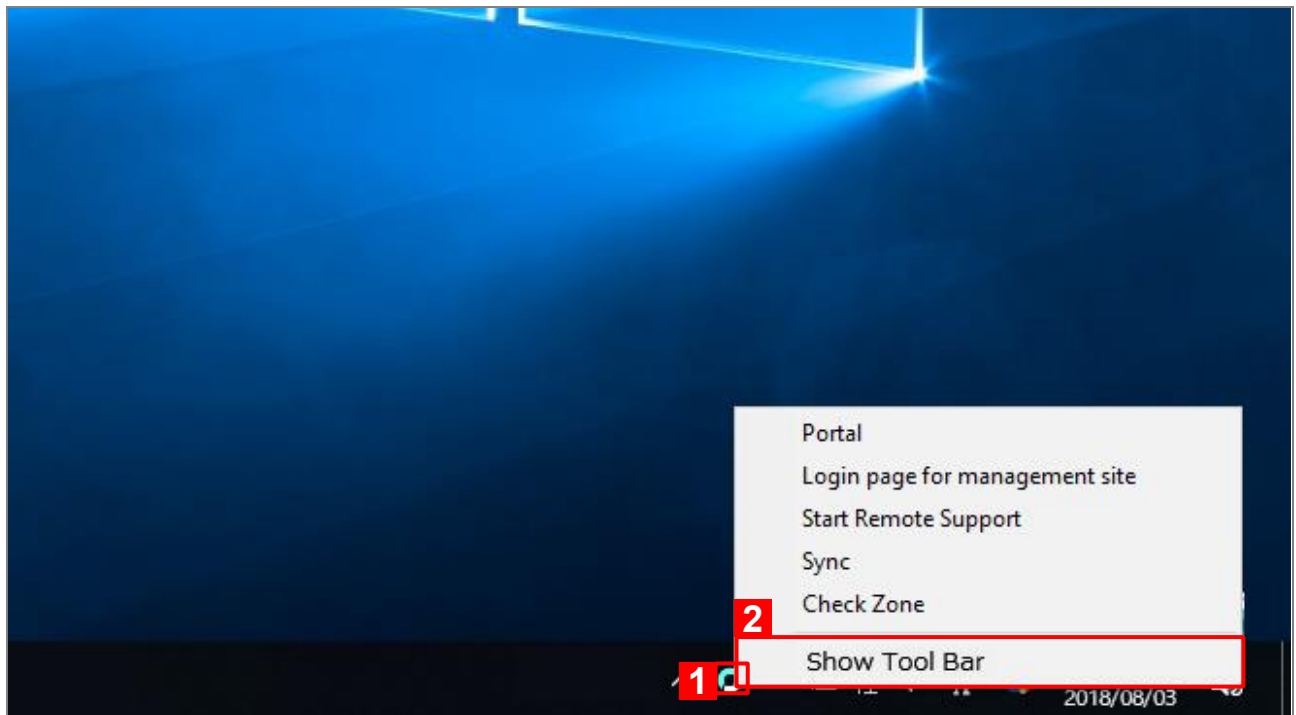


No.	Object	Function
1	Portal	Portal screen appears. You can register and edit asset information. For details, refer to the following. "Register Asset Information" Page 23
2	Login page for management site	Opens a login page for the management site. Available only for administrators. For details, refer to the following. <Management Site Reference Manual> This menu may not be displayed depending on the administrator's settings.
3	Start Remote Support	Starts remote support. For details, refer to the following. "Receive Remote Support" Page 30
4	Sync	Sync with the management server to reflect the latest configuration in the Windows devices. Sync is used whenever the changes on the management site need to be applied to the devices. For details, refer to the following. "Sync with management site" Page 22
5	Check Zone	Display the current zone information.
6	Show Toolbar Hide Toolbar	Switch the display of the toolbar. If the toolbar is displayed, "Hide Toolbar" is displayed on the menu. For details, refer to the following. "Show Toolbar" Page 17



## 2.2.5 Show Toolbar

- [1] Right-click  (task tray icon).
- [2] Click [Show Tool Bar].



## 2.2.6 Details of toolbar

By clicking each button, you can use the following functions in this product.



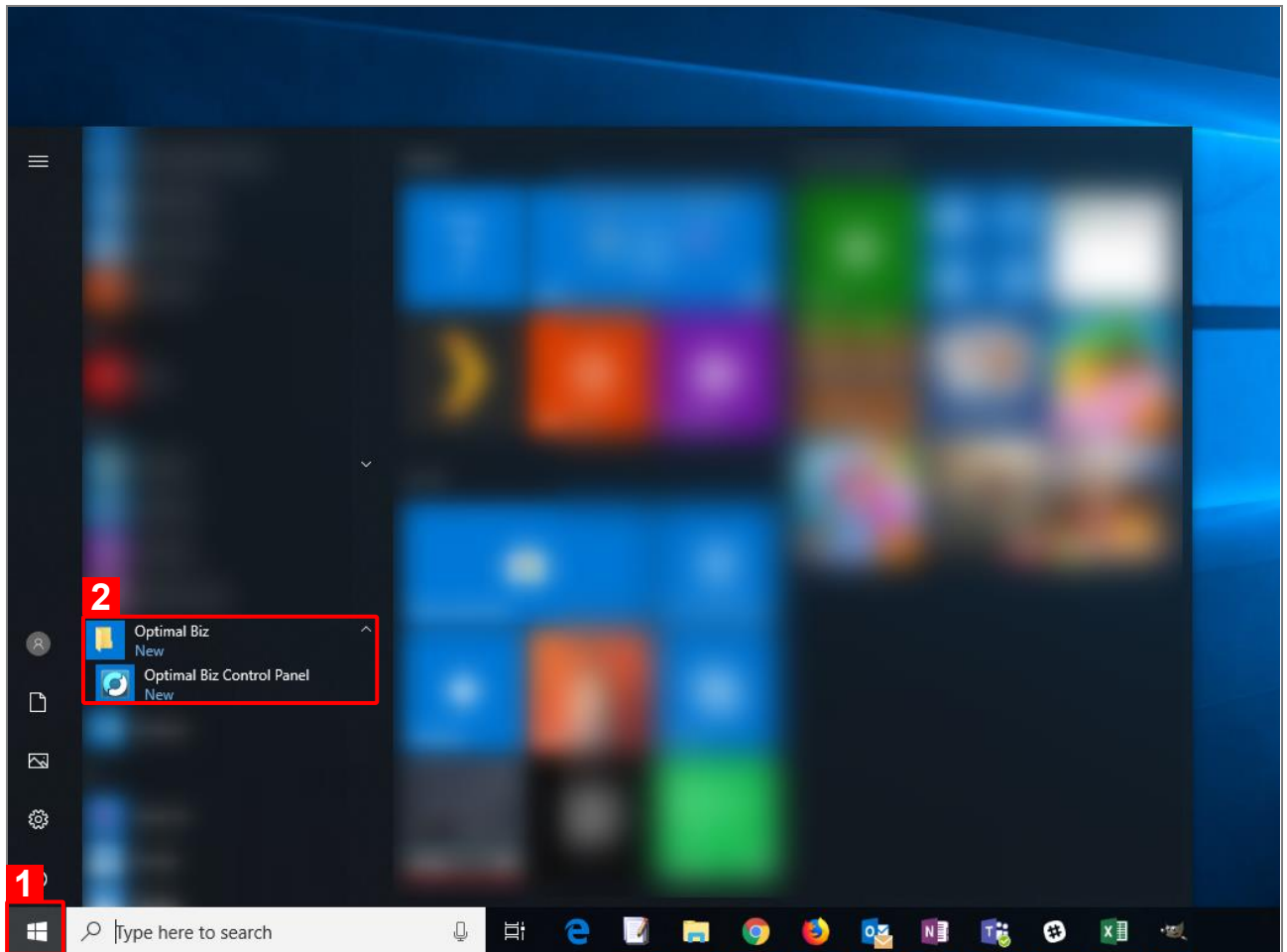
No.	Object	Function
1	[Grip]	Drag to move the toolbar.
2	[Portal]	Portal screen appears. You can register and edit asset information. For details, refer to the following. ☞ "Register Asset Information" Page 23
3	[Start Remote Support]	Starts Remote Support. For detail. For details, refer to the following. ☞ "Receive Remote Support" Page 30
4	[Sync]	Sync with the management server to reflect the latest configuration in the Windows devices. Sync is used whenever the changes on the management site need to be applied to the devices. For details, refer to the following. ☞ "Sync with management site" Page 22
5	[Check Zone]	Display Zone information.
6	[Minimize Icon]	Hide toolbar from the desktop. You can display it again from the menu of the tray icon.

## 2.2.7 Open control panel

Click the start menu to open the control panel.

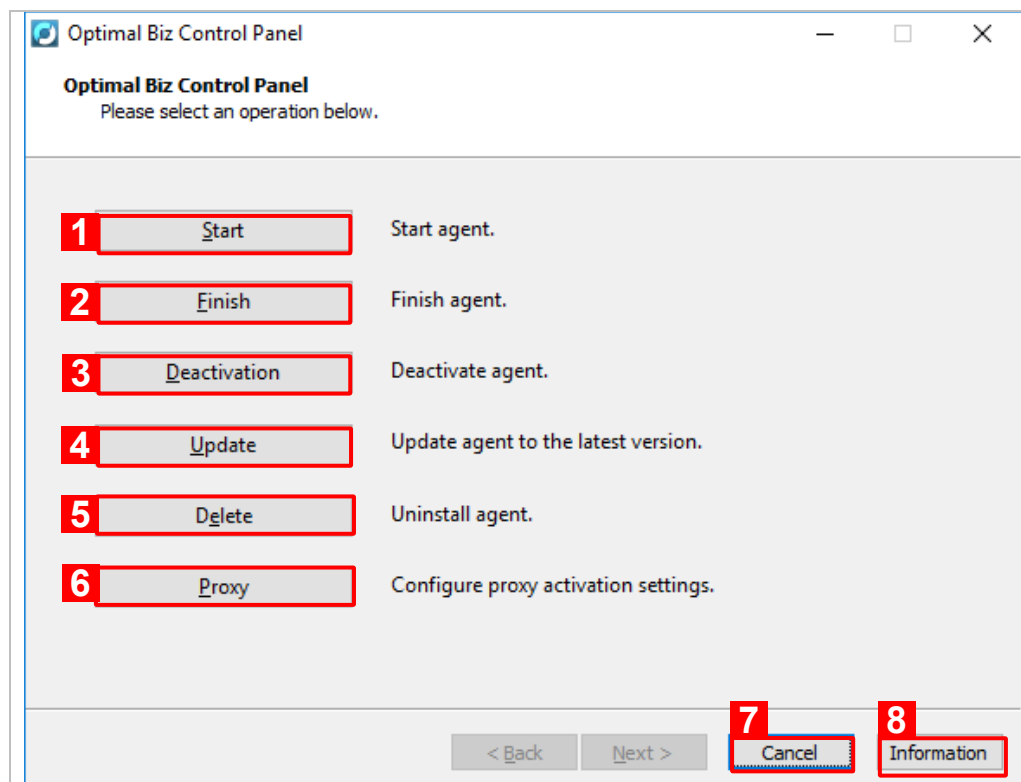
**[1]** Click the start button on the bottom-left corner of the screen.

**[1]** Click [Optimal Biz]-[ Optimal Biz Control Panel].



## 2.2.8 Details of control panel

The control panel is used when controlling the agent.

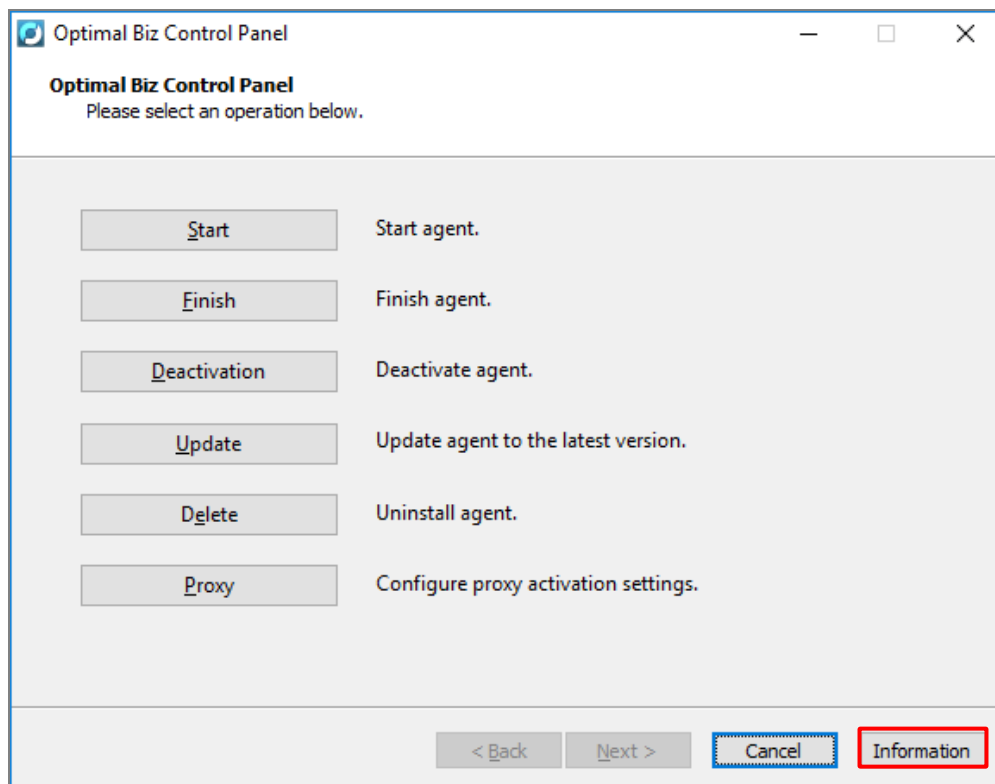


No.	Object	Function
1	[Start]	Launch the agent and start the management of a Windows device. For details, refer to the following. ☞ "Re-Launch agent" Page 69
2	[Finish]	Finish the agent. Click [Launch] to launch the agent again. For details, refer to the following. ☞ "Finish agent" Page 67
3	[Deactivation]	Once you deactivate the agent, you can no longer use this product. For details, refer to the following. ☞ "Deactivate agent" Page 70
4	[Update]	The agent is updated automatically. If you want to update the agent manually, click this button. For details, refer to the following. ☞ "Update agent" Page 40
5	[Delete]	Uninstall the agent. For details, refer to the following. ☞ "Delete agent" Page 74
6	[Proxy]	Set the user name and password of proxy authentication. For details, refer to the following. ☞ "Proxy authentication" Page 27
7	[Cancel]	Close the control panel.
8	[Info]	Display the information of a Windows device or the agent. For details, refer to the following. ☞ "Confirm information of a Windows device or the agent" Page 20

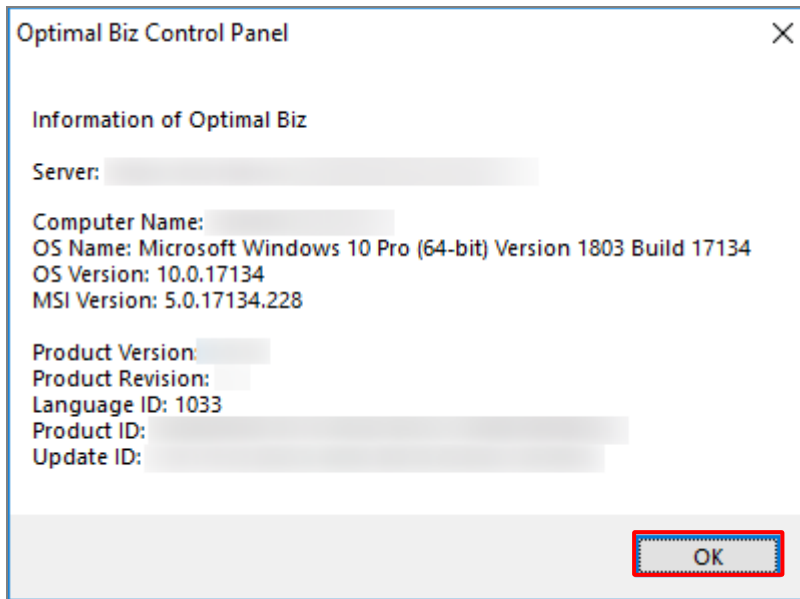
## 2.3 Confirm information of a Windows device or the agent

You can confirm the information of a computer name or version of the agent.

**[1] Open the control panel and click [Information].**



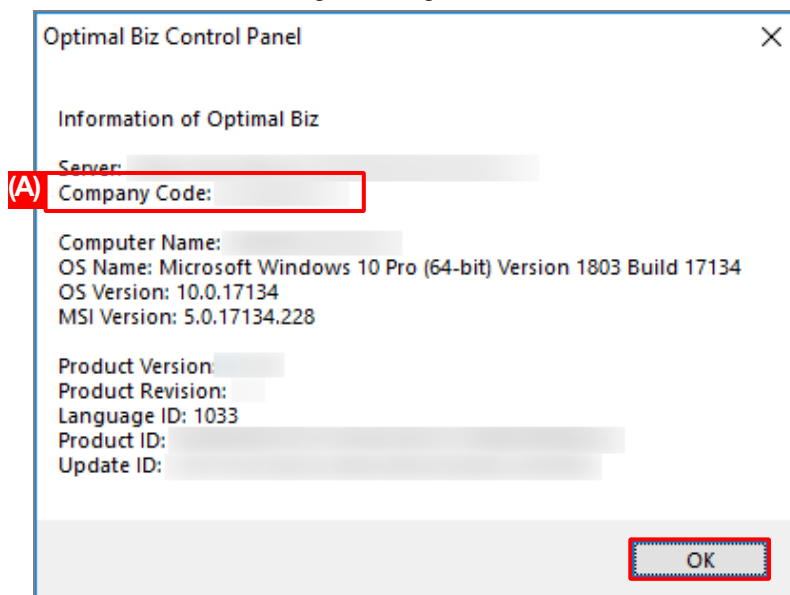
**[2]** The information screen is displayed. Click [OK] to close the screen.



If activated, company code(A) will be displayed.

For details, refer to the following, "Activate Agent" for activation.

"Activate Agent" Page 72




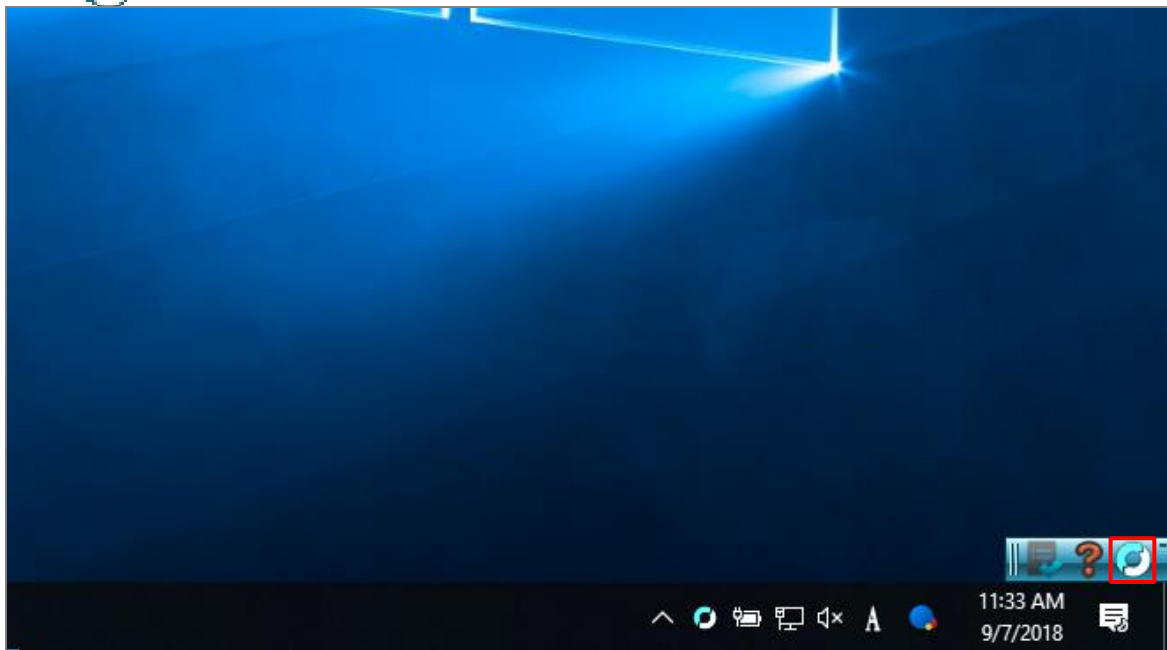
## 2.4 Sync with management site

The settings of Windows devices are reflected in Windows devices regularly, but if you want to reflect the settings set on the management site immediately, follow the steps below.

- ✍ When the Windows device is deleted on the management site, the license authentication on the Windows device is automatically canceled at the next synchronization.

<<From the icon in the toolbar>>

- Click  "Sync" icon in the toolbar.

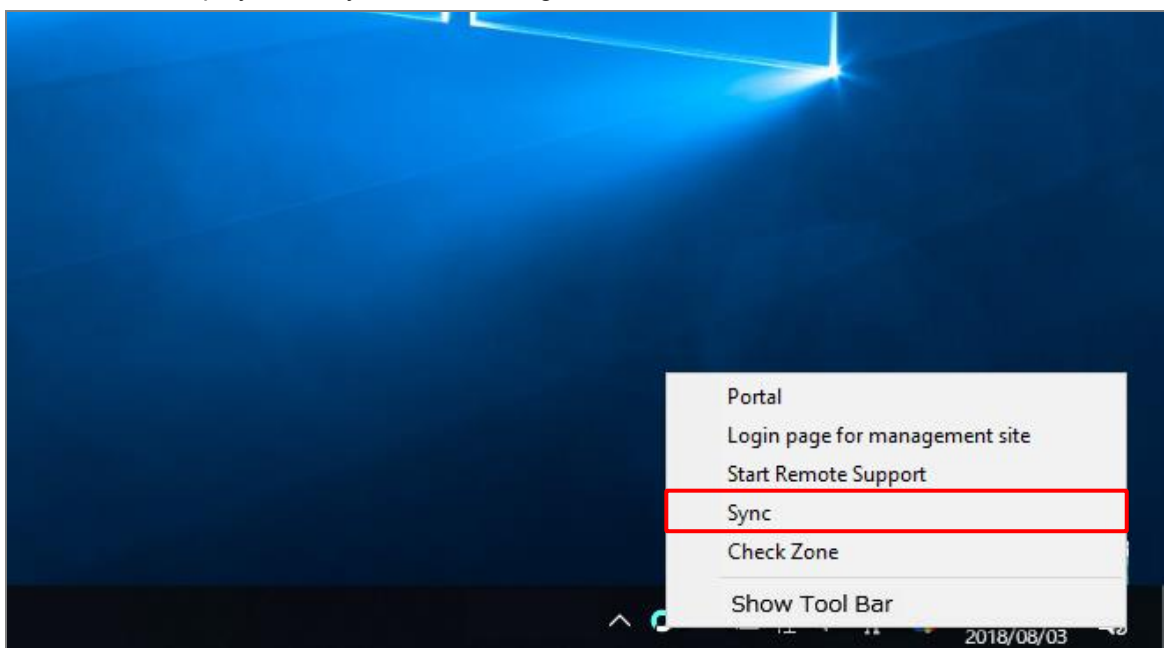


<<From the menu of the tray icon>>

- Click [Sync] in the menu of the tray icon.

✍ "Display menu of the tray icon" on how to display the menu of the tray icon.

👉 "Display task tray icon menu" Page 15



## 2.5 Register Asset Information

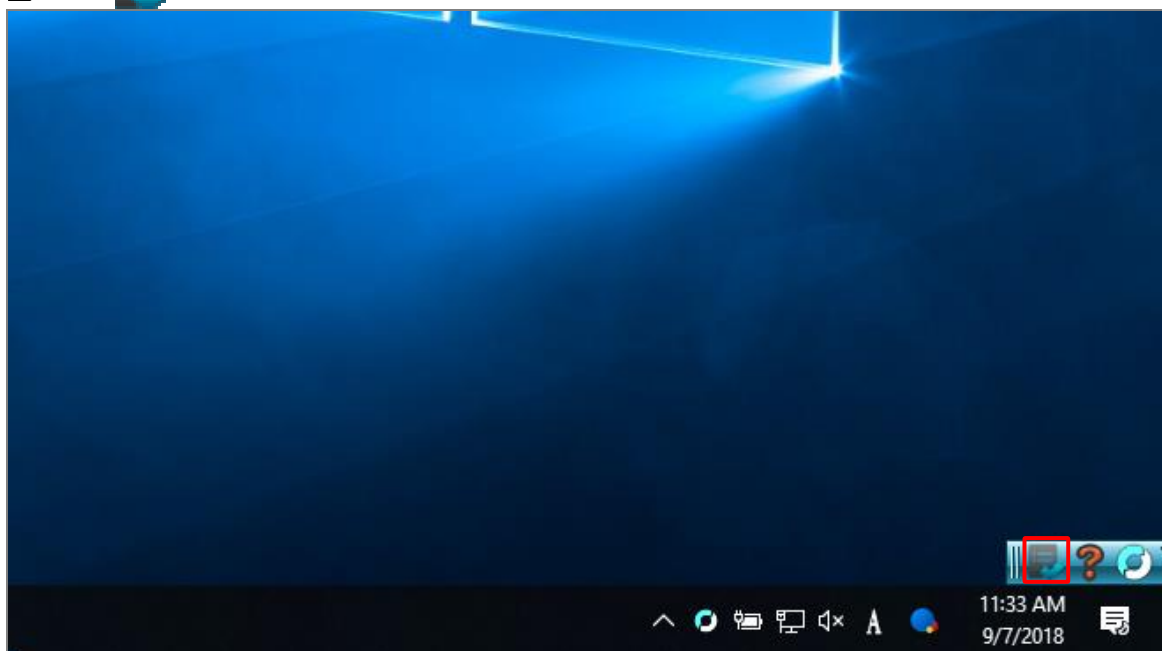
To register asset information, follow the steps below.

- ✎ If an additional asset item is not registered on the management site, the setting page is not displayed. An asset item depends on the settings on the management site.

### [1] Access the portal.

<<From the icon in the toolbar>>

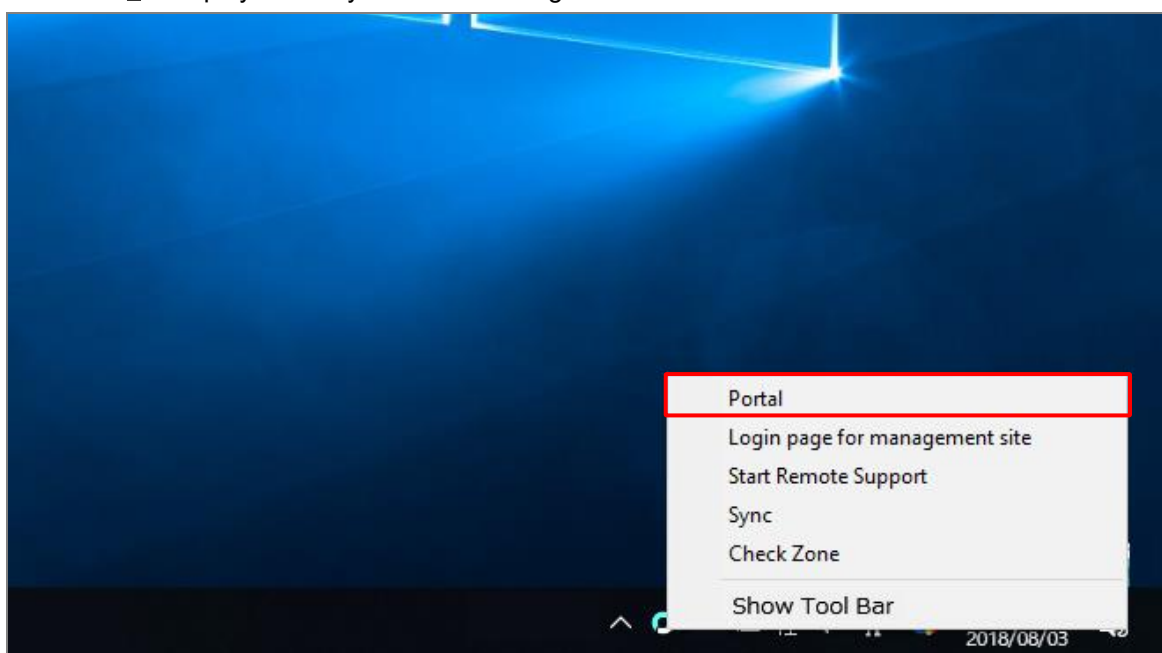
- ✎ Click  "Portal" in the toolbar.



<<From the menu of the tray icon>>

- ✎ Click [Portal] in the menu of the tray icon. For details, refer to the following.

☞ "Display task tray icon menu" Page 15



**[2]** The portal screen is displayed. Click [Change asset information].

The screenshot shows the 'Portal Home' interface. At the top, there is a green header bar with the text 'Portal Home'. Below this, there is a white bar with a blurred logo. The main content area has a light gray background. On the left side, there are two labels: 'Classification (None)' and 'Free input (None)'. In the center, there is a green button with a white plus icon and the text 'Change asset information', which is highlighted with a red rectangular border. At the bottom, there is a green footer bar with the text 'Optimal Biz Optimal Biz' and '©2017 OPTIM | Terms of Service | Privacy Policy'.

**[3]** Enter the required information and click [Register].

The screenshot shows the 'Asset Information Registration' interface. At the top, there is a green header bar with the text 'Asset Information Registration'. Below this, there is a white bar with a blurred logo. The main content area has a light gray background. On the left side, there are two labels: 'Asset Information Registration' and 'Classification'. Below 'Classification', there is a green dropdown menu with the text '(Uncategorized)' and a white checkmark icon. Below this, there is a label 'Free input' and a white text input field. At the bottom, there are two green buttons: 'Back' and 'Register'. The 'Register' button is highlighted with a red rectangular border. At the bottom, there is a green footer bar with the text 'Optimal Biz Optimal Biz' and '©2017 OPTIM | Terms of Service | Privacy Policy'.



**【4】 Registration is completed. Click [OK].**

Asset Information Registration

Completed device information registration.

Classification  
(None)

Free input  
Test input

☒ OK

Optimal Biz Optimal Biz  
©2017 OPTIM | [Terms of Service](#) | [Privacy Policy](#)

---

## 3 Proxy authentication

You can set a user name and password for proxy authentication.


Describes the following items.

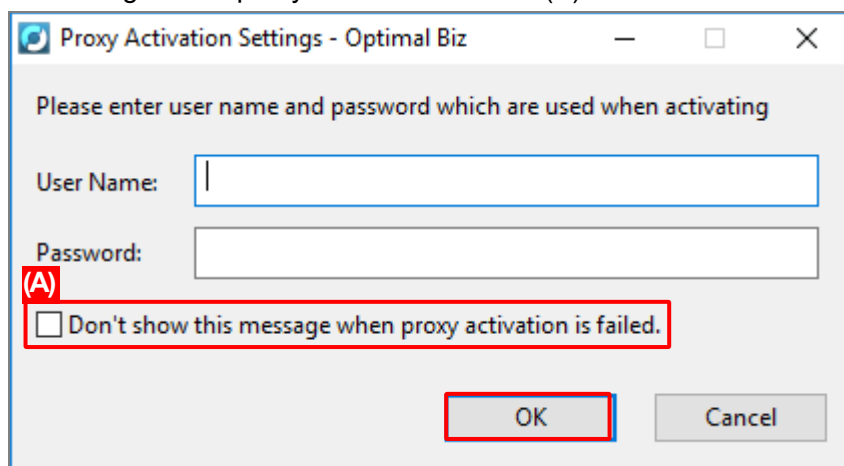
Item	Page
<a href="#">Proxy authentication</a>	<a href="#">27</a>
<a href="#">Change the settings of proxy authentication</a>	<a href="#">28</a>

## 3.1 Proxy authentication

The following proxy authentication screen appears if the agent tries to connect to the management site in the area that requires proxy authentication.

**[1] Enter "User Name" and "Password" for proxy authentication and click [OK].**

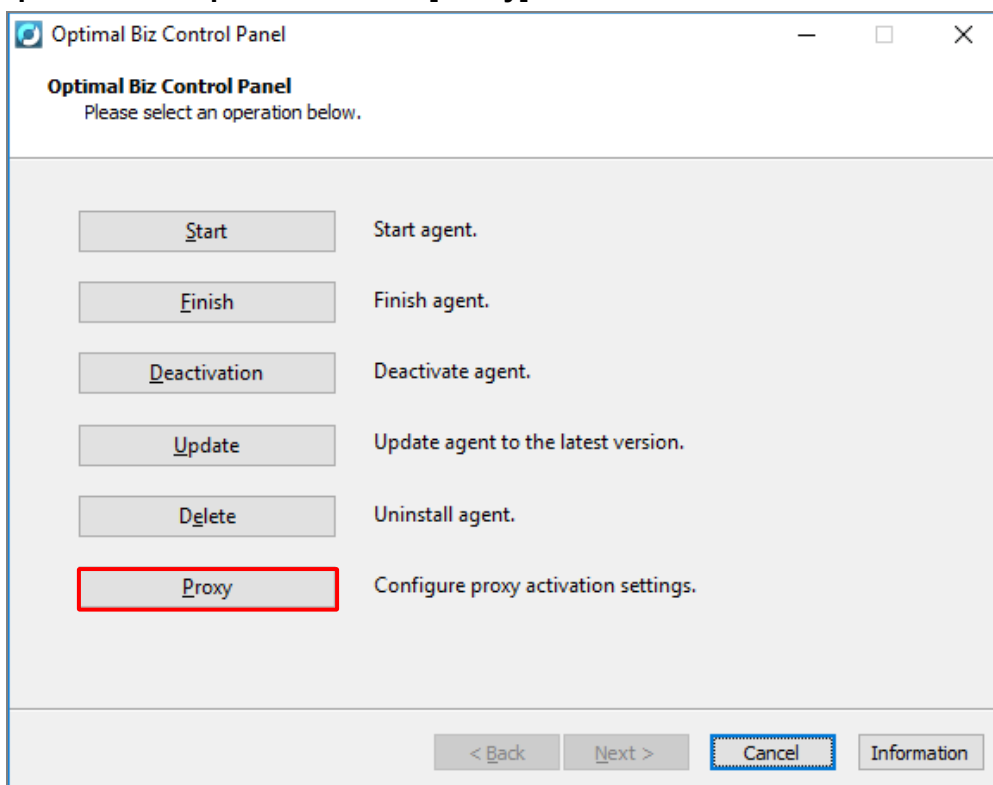
 If you don't want to see this window when proxy authentication has failed, check "Don't show this message when proxy activation is failed"(A).




The image shows a Windows-style dialog box titled "Proxy Activation Settings - Optimal Biz". The dialog has a standard title bar with minimize, maximize, and close buttons. The main content area contains the text "Please enter user name and password which are used when activating". Below this text are two input fields: "User Name:" and "Password:". The "User Name:" field has a cursor in it. Below the "Password:" field is a checkbox labeled "(A) Don't show this message when proxy activation is failed.". The checkbox is currently unchecked. At the bottom right of the dialog are two buttons: "OK" and "Cancel". The "OK" button is highlighted with a red rectangle.

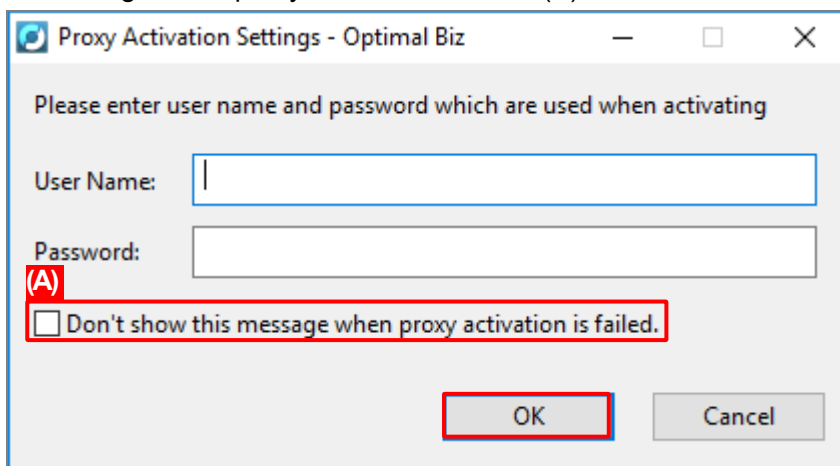
## 3.2 Change the settings of proxy authentication

**[1] Open a control panel and click [Proxy].**



**[2] Enter "User Name" and "Password" for proxy authentication and click [OK].**

 If you don't want to see this window when proxy authentication has failed, check "Don't show this message when proxy activation is failed"(A).




---

## 4 Remote Support

"Remote Support" allows you to share your Windows screen with the help desk operator. By sharing your screen, the operator will be able to provide more flexible troubleshooting. Operator can also remotely operate on your device. To receive remote support, contact your help desk operator.

 Contact your administrator for how to get in touch with the help desk.

Follow the instructions from the operator and start remote support. The receipt number will be displayed. Provide this number to the operator. Look further into this section for further instructions.

 Note that remote support requires an Internet connection.

Describes the following items.

Item	Page
<a href="#">Receive Remote Support</a>	<a href="#">30</a>

## 4.1 Receive Remote Support

### [1] Start remote support.

<<From the icon in the toolbar>>

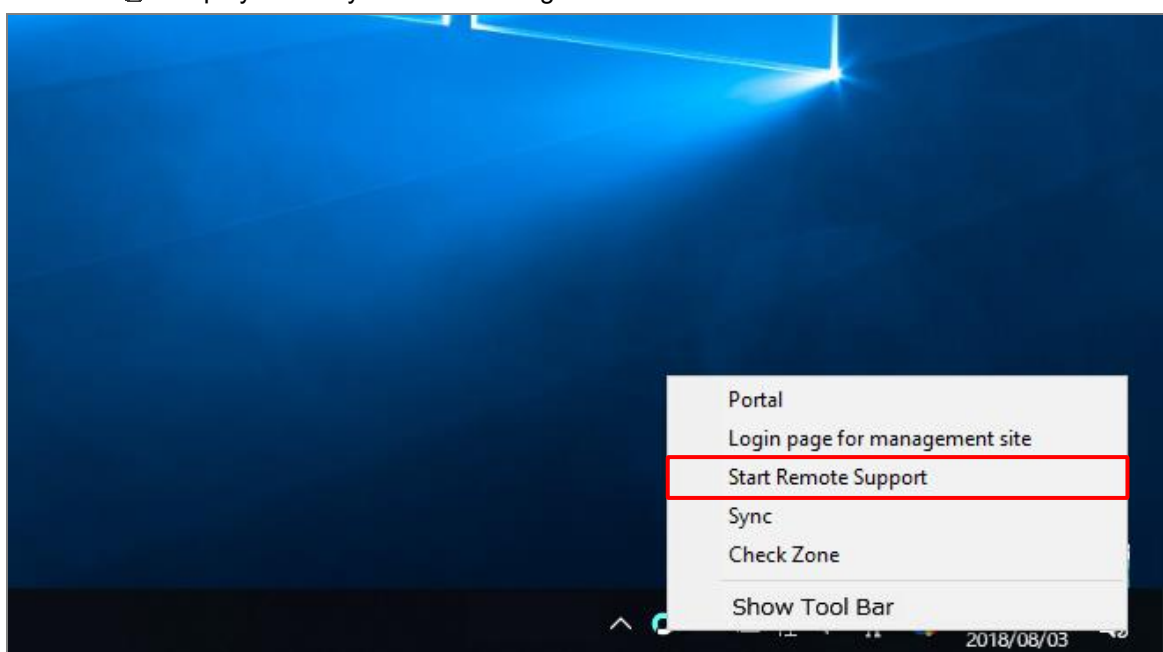
✎ Click on the “ ? ” icon on the Toolbar.



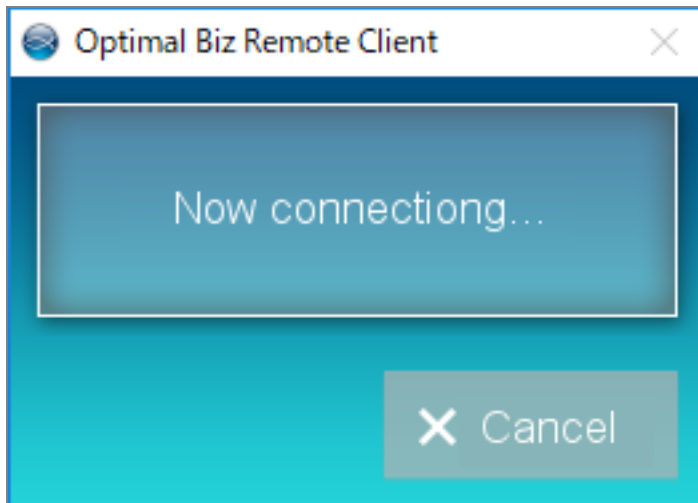
<<From the menu of the tray icon>>

✎ Click on "Start Remote Support" in the task tray icon. For details, refer to the following.

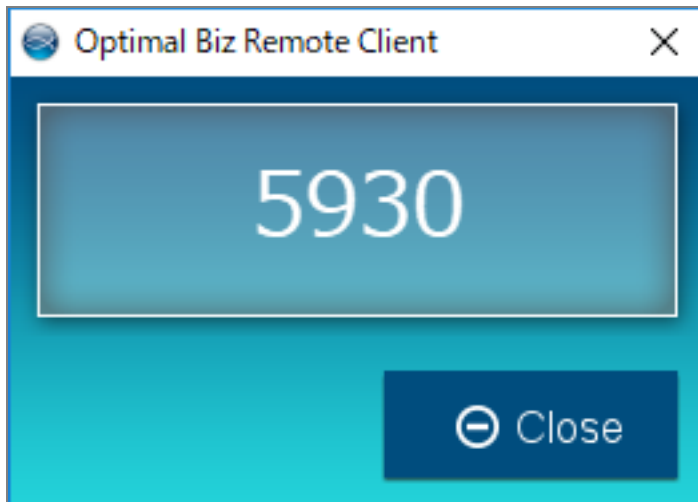
☞ "Display task tray icon menu" Page 15



**[3]** After installation, check the connection status of the remote client. Wait.



**[4]** The receipt number will be displayed. Provide this number to the operator.



---

## 5 Remove remote lock

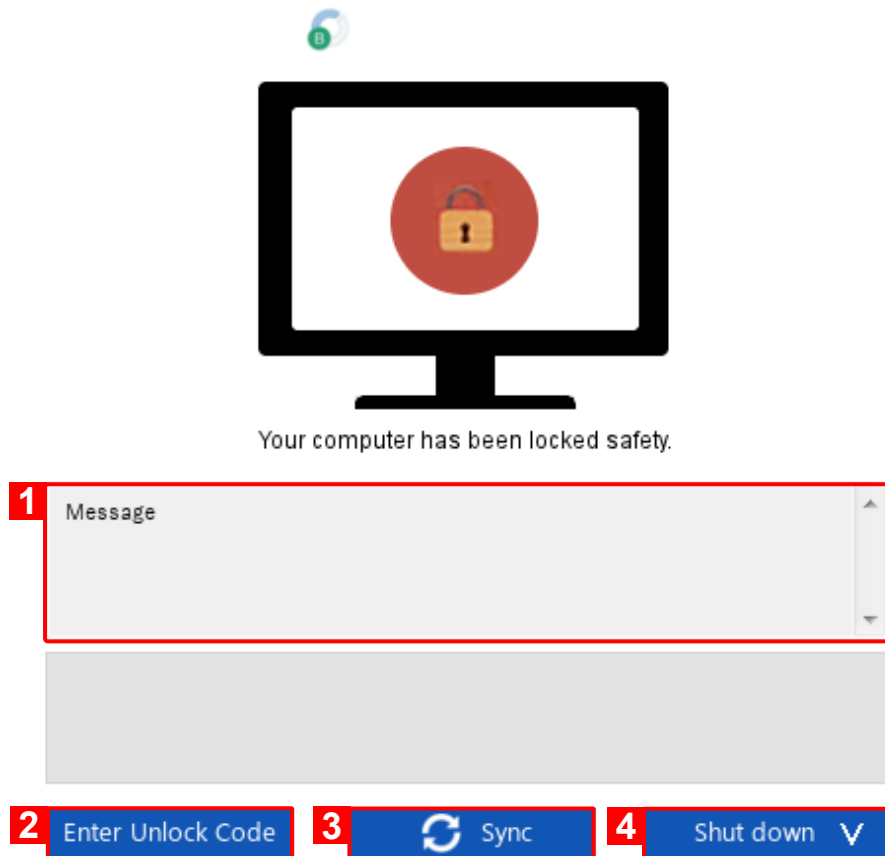
When the remote lock is applied from the management site or the device is locked due to offline devices detection, you can remove the lock according to the procedure described in this section.

Describes the following items.

Item	Page
<a href="#">How to use remote lock screen</a>	<a href="#">33</a>
<a href="#">Remove remote lock</a>	<a href="#">34</a>
<a href="#">Sync with management site on lock screen</a>	<a href="#">37</a>



## 5.1 How to use remote lock screen

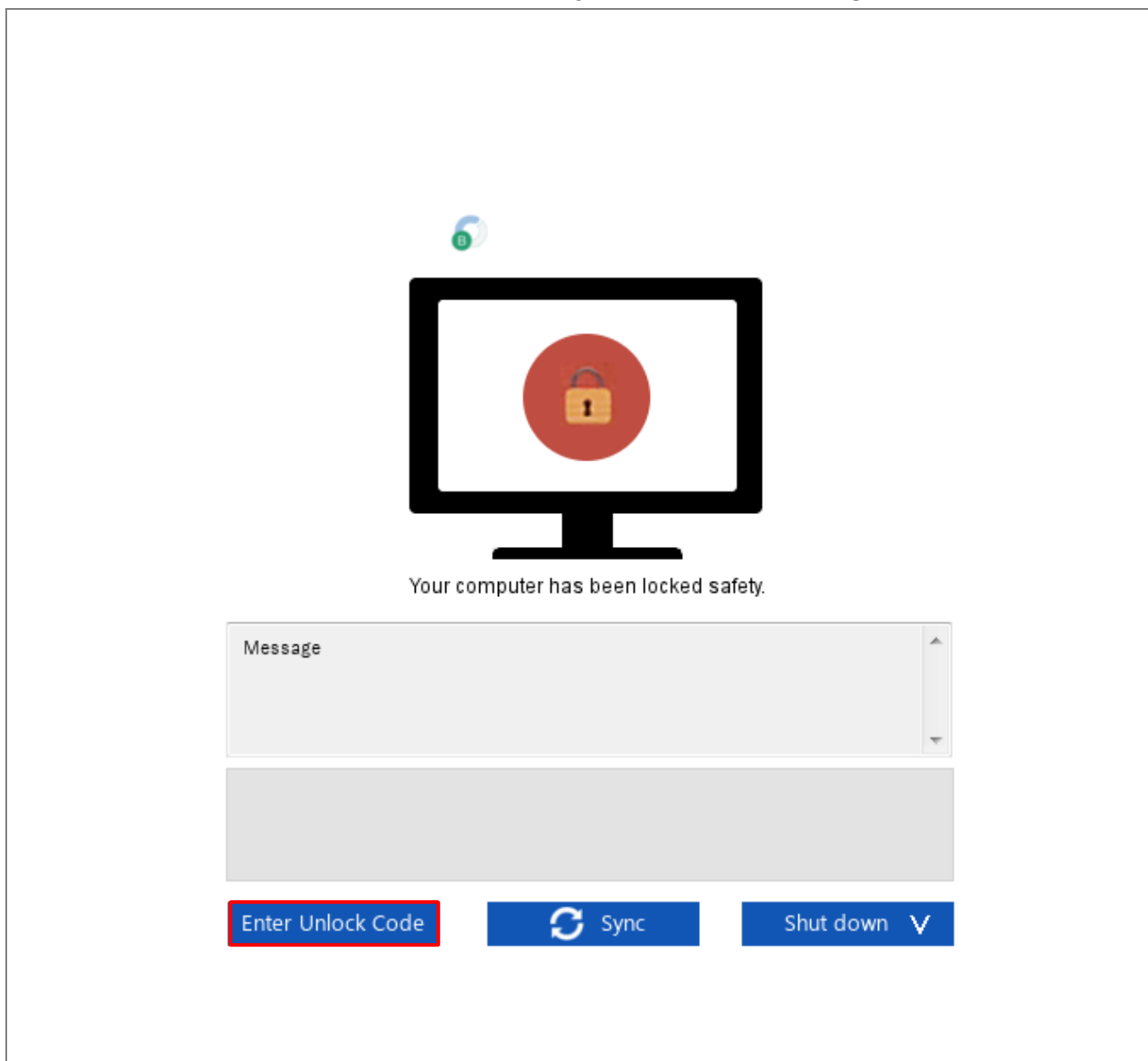


No.	Obbect	Description
1	Message	Displays lock message set to the device user at the management site. When no message is set, a blank field is displayed.
2	[Enter Unlock Code]	Click to unlock remote lock.
3	[Sync]	Click to sync with the management site.
4	[Shut down]	Click to access the shutdown menu. You can sleep, reboot or shut down the computer.

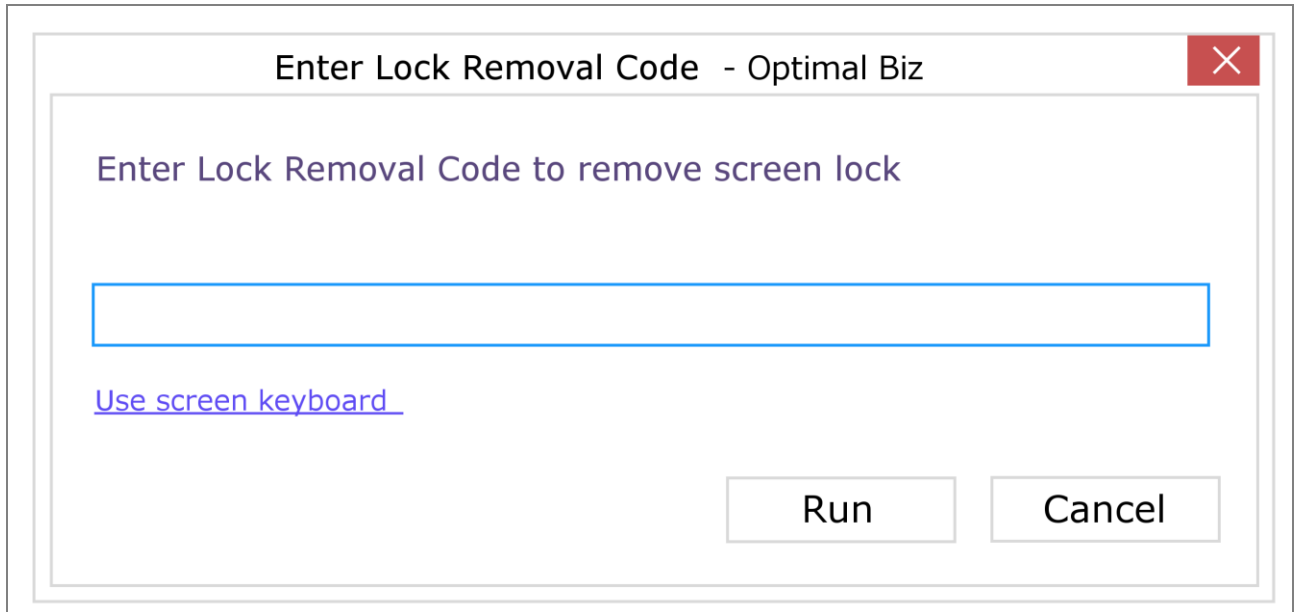
## 5.2 Remove remote lock

When the remote lock is applied from the management site or the device is locked due to offline devices detection, you can remove the lock according to the procedure described in this page.

**[1]** Click on the [Enter Unlock Code] button displayed under the "message" field.

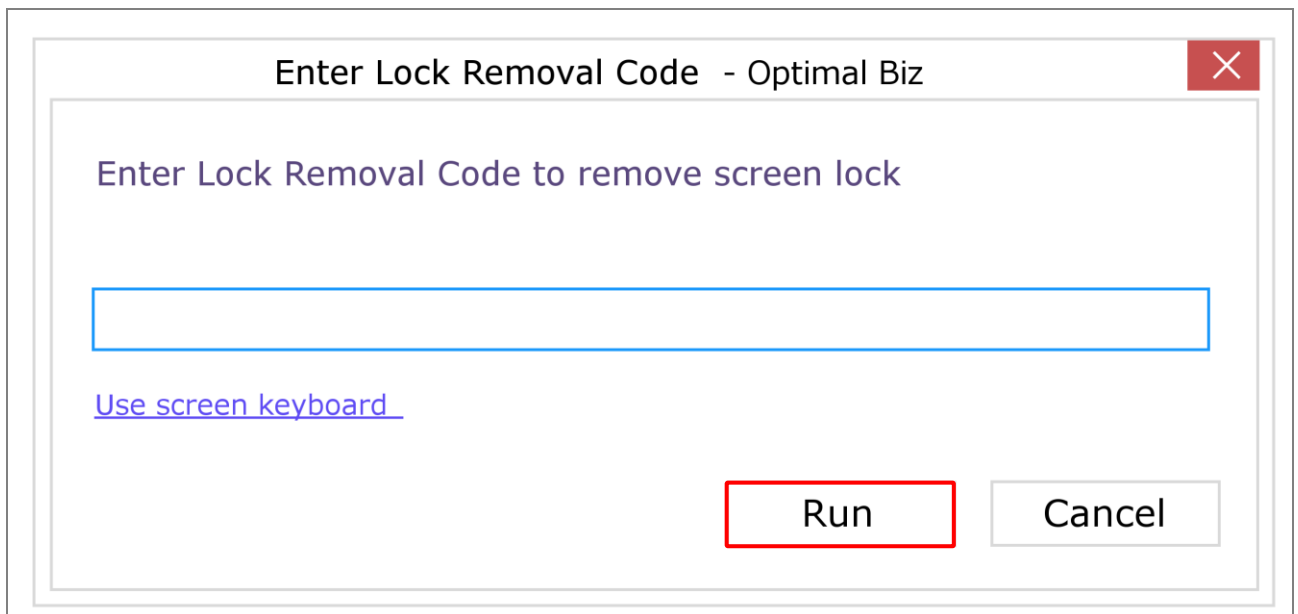


**[2]** The "Enter Lock Removal Code" dialog is displayed.



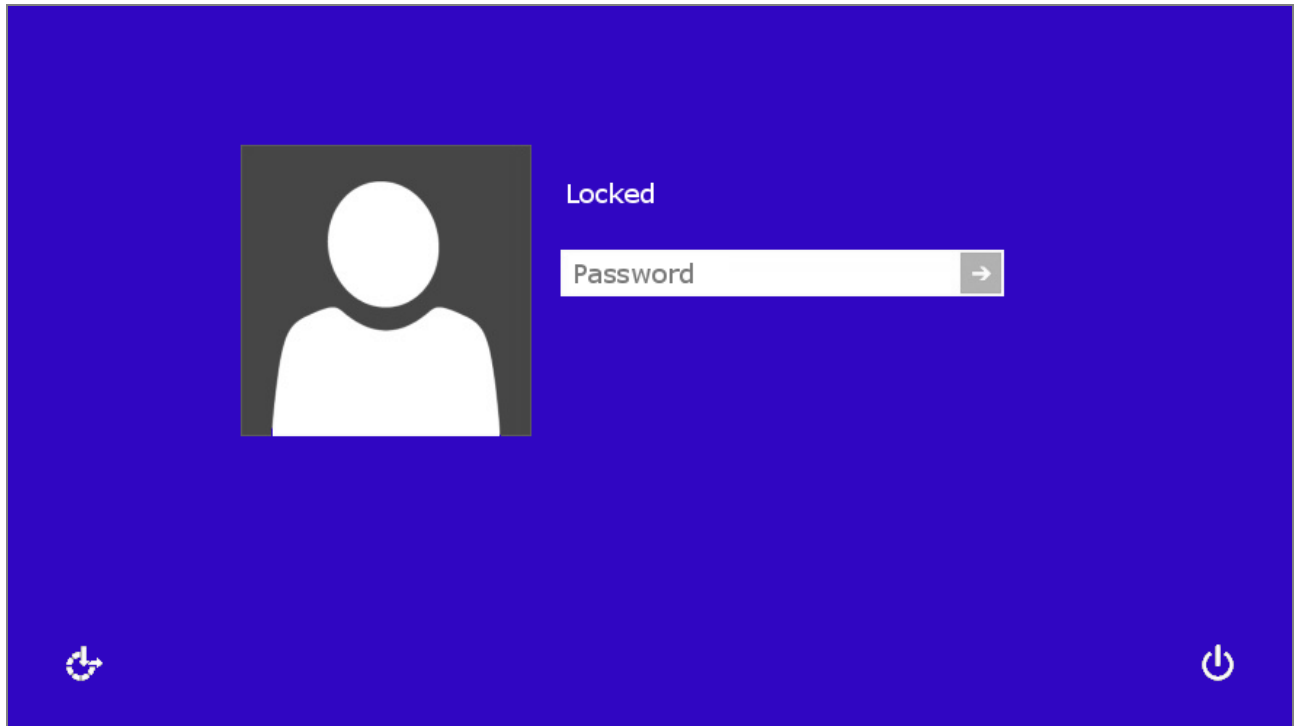
The screenshot shows a dialog box titled "Enter Lock Removal Code - Optimal Biz" with a red close button in the top right corner. The main text inside the dialog reads "Enter Lock Removal Code to remove screen lock". Below this text is a long, empty rectangular input field. Underneath the input field is a blue underlined link that says "Use screen keyboard". At the bottom right of the dialog are two buttons: "Run" and "Cancel".

**[3]** Enter "Lock Removal Code" and press the [Run] button.



This screenshot is identical to the one above, showing the "Enter Lock Removal Code - Optimal Biz" dialog box. However, the "Run" button at the bottom right is now highlighted with a red rectangular border, indicating it is the next step in the process.

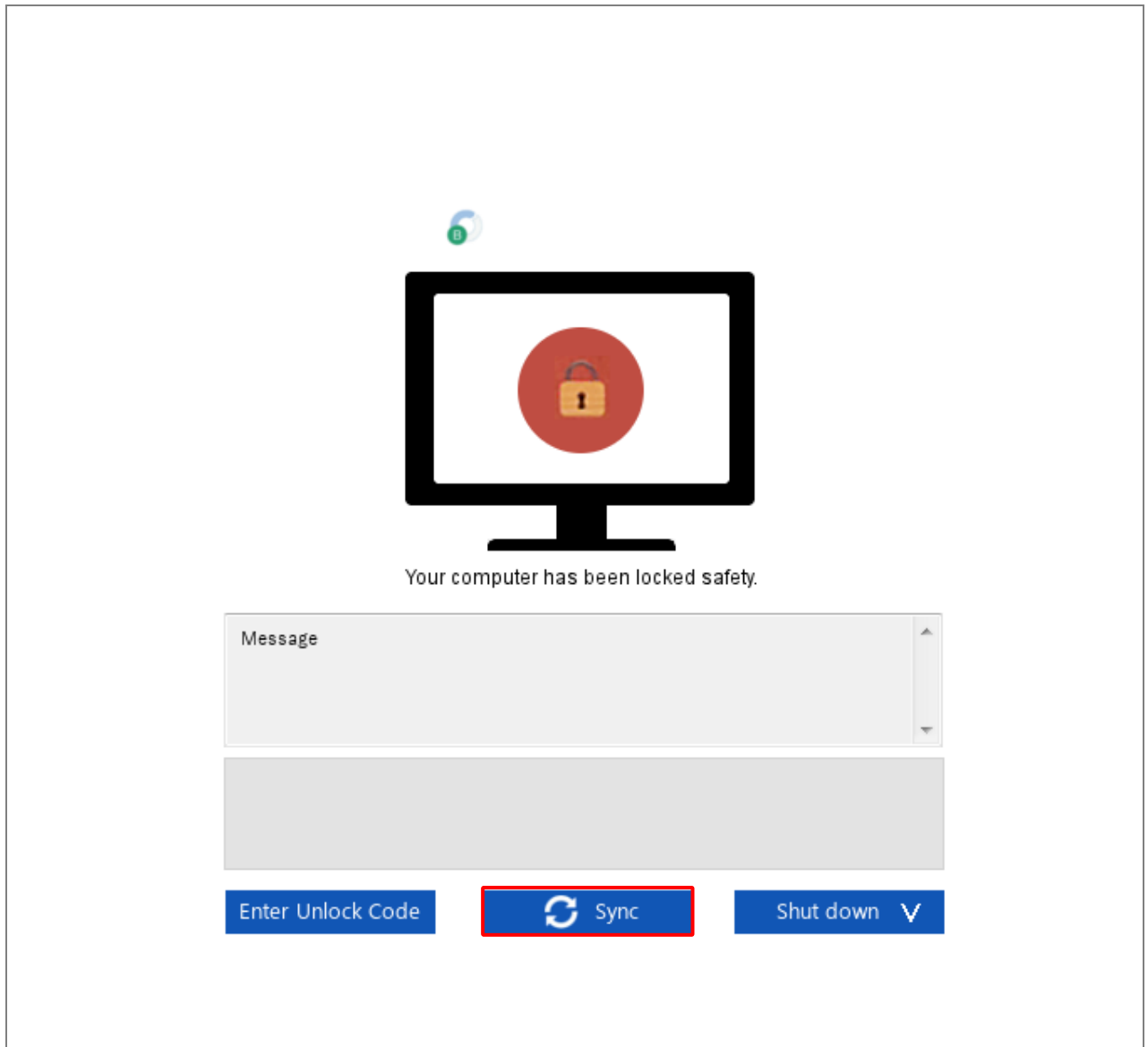
**【4】 When the remote lock is removed, the Windows standard lock screen is displayed.**



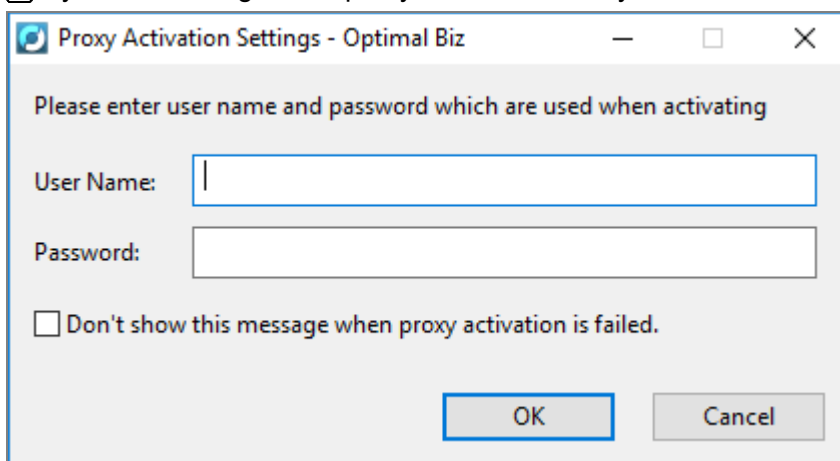
### 5.3 Sync with management site on lock screen

If the lock removal code has been altered after the lock is applied, you need to sync with the management site on the lock screen.

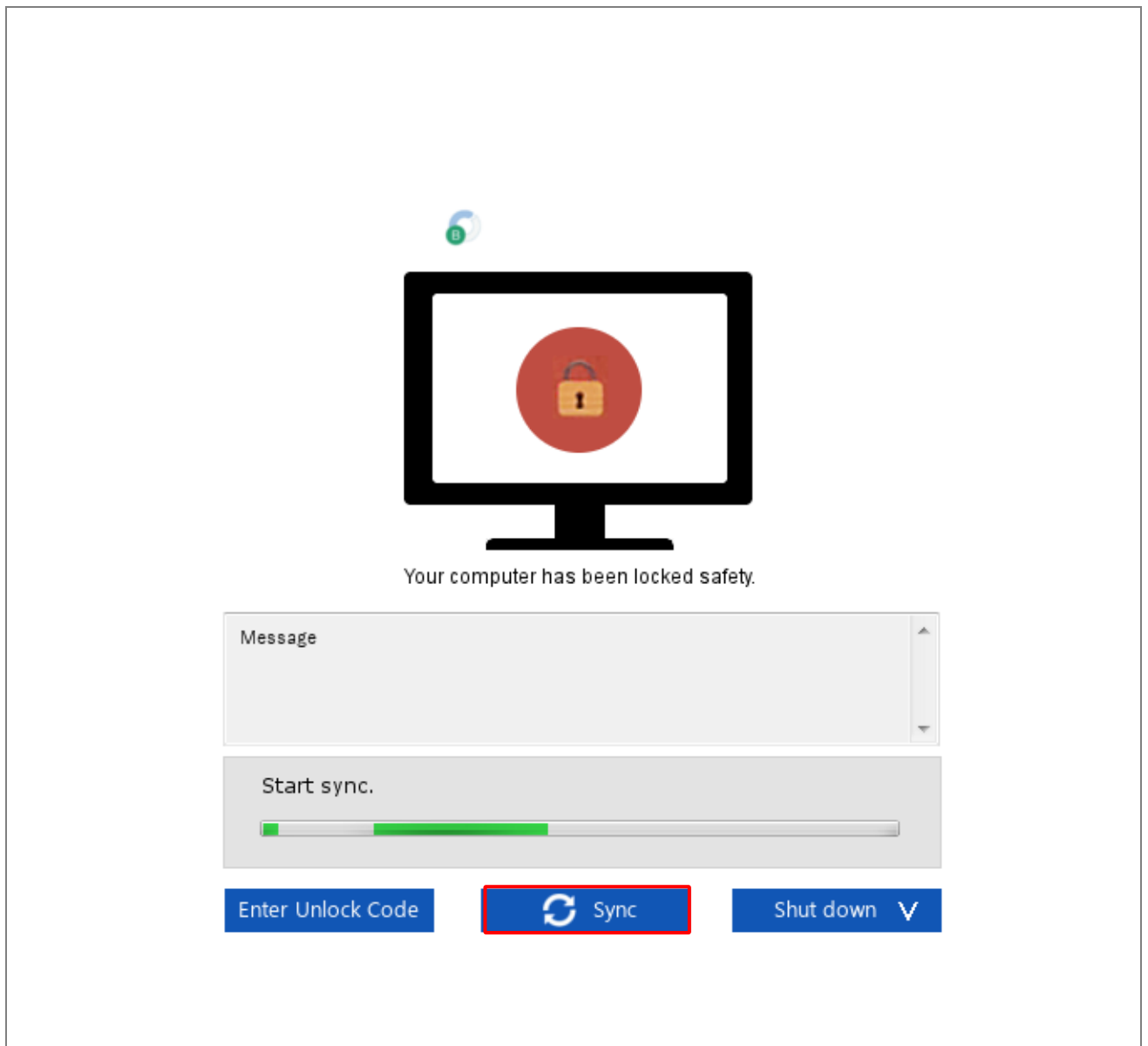
- [1]** Click on the [Sync] button displayed under the "message" field.



 If you need to log in to a proxy server, the Proxy Activation Settings dialog is displayed.



**[2]** Wait until sync with the management completes and the [Sync] button becomes active again.



---

## 6 Update agent

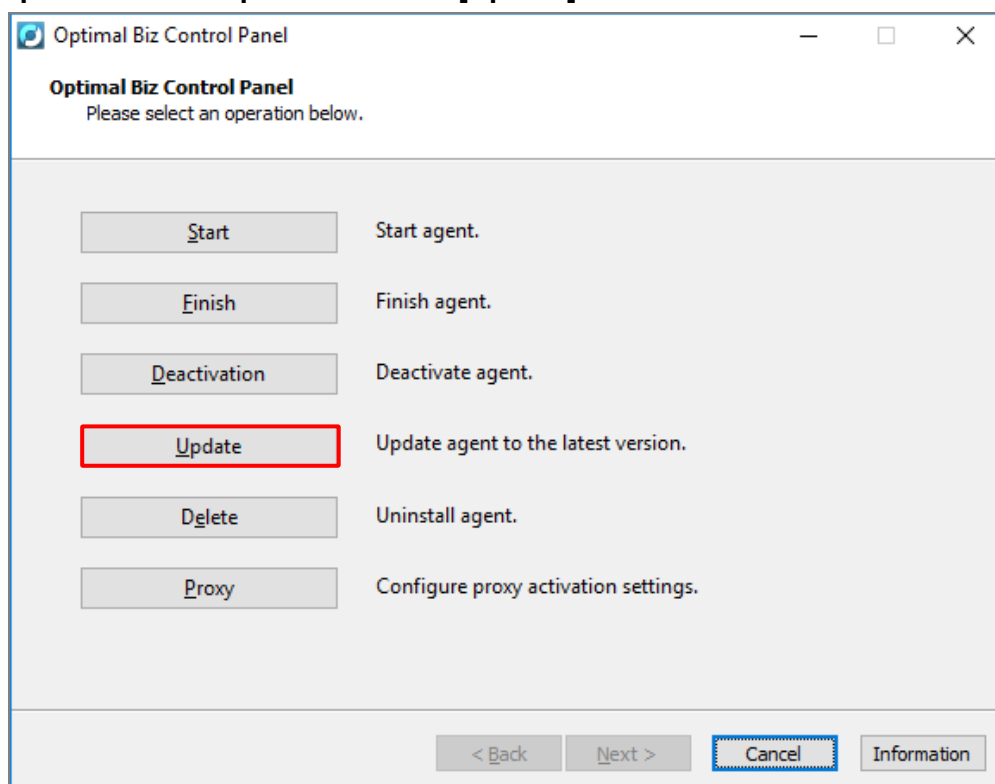
The agent is automatically updated to the latest version, but you can update it manually.  
When using proxy authentication, manual upload is unavailable.

Describes the following items.

Item	Page
<a href="#">Update agent</a>	<a href="#">40</a>

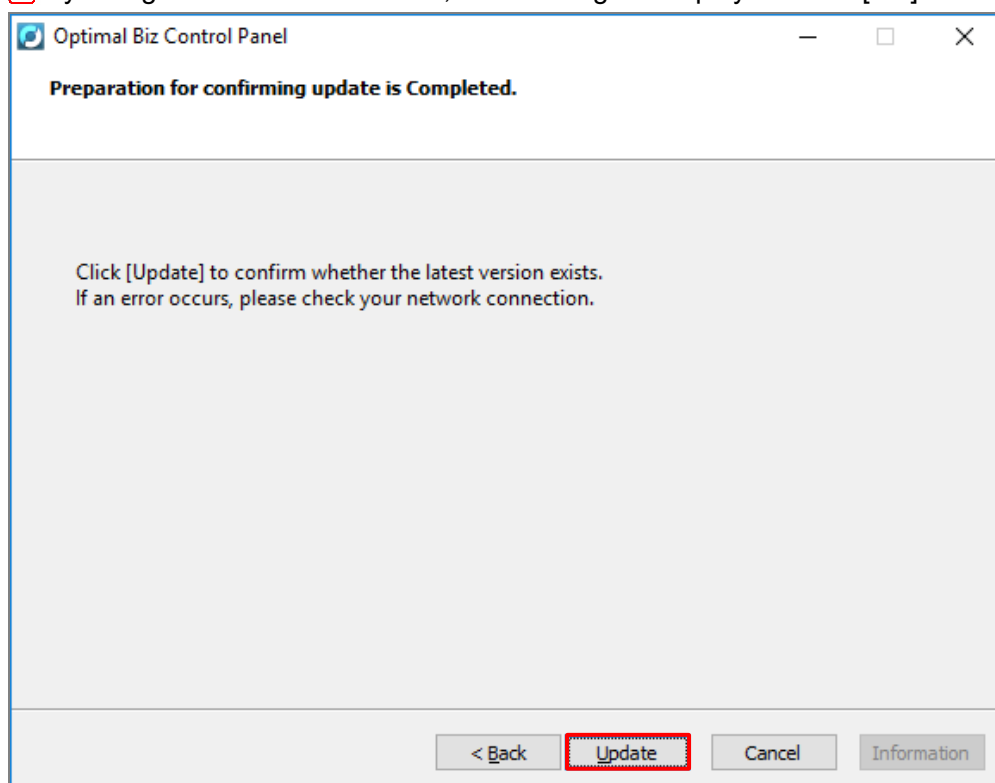
## 6.1 Update agent

**[1]** Open the control panel and click [Update].

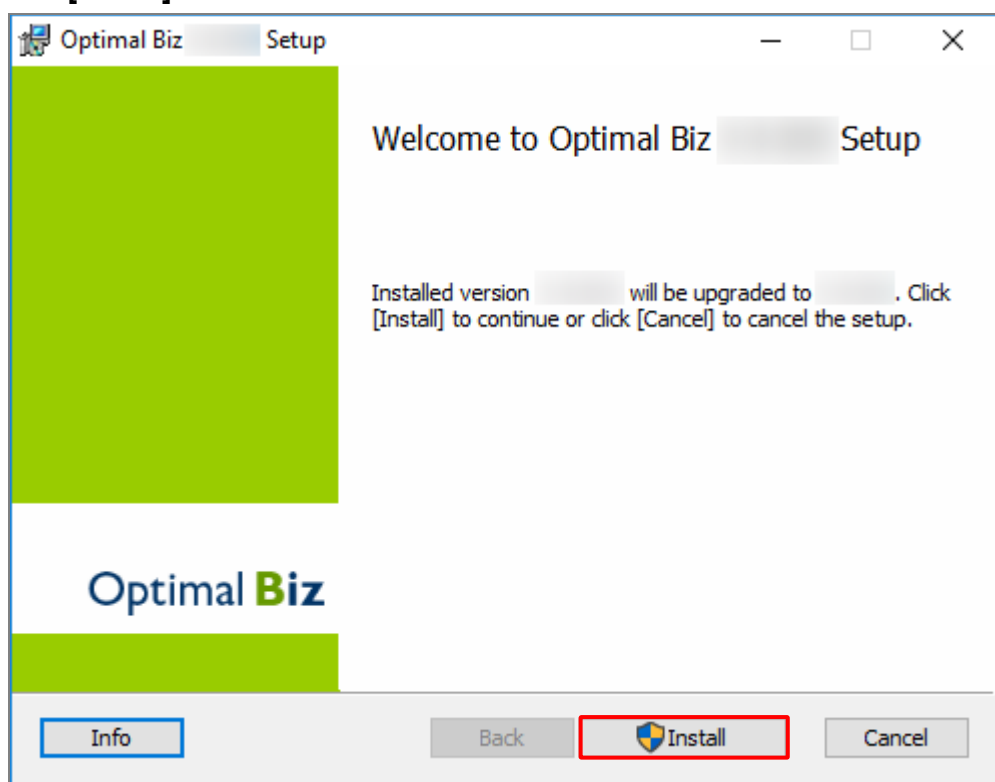
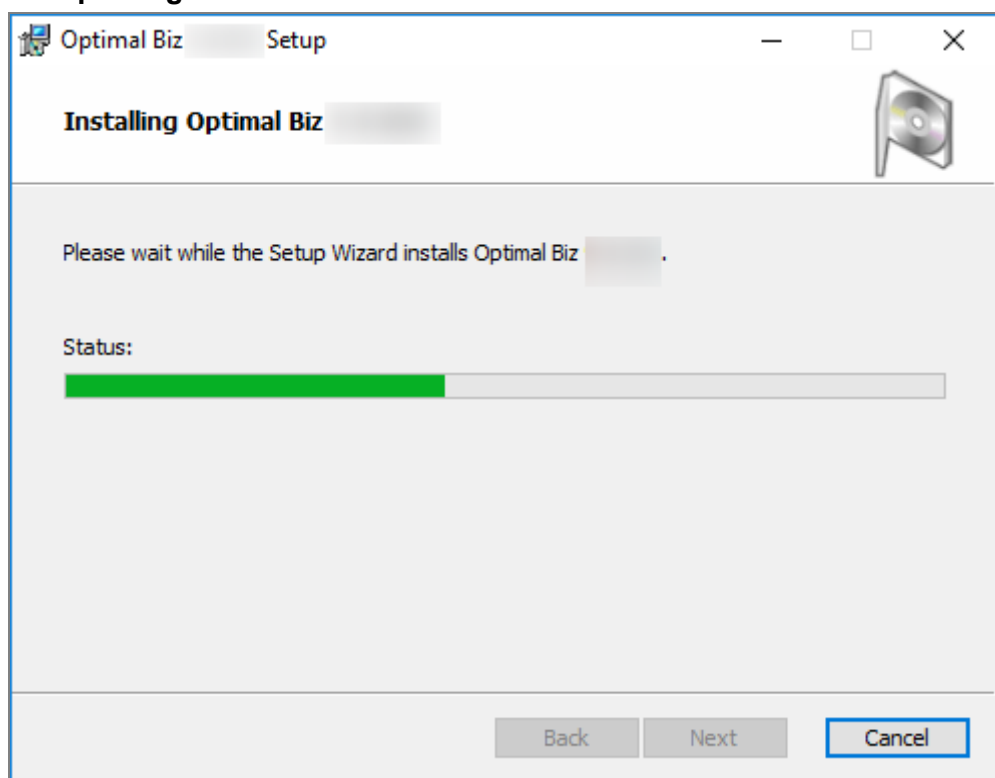


**[2]** Click [Update].

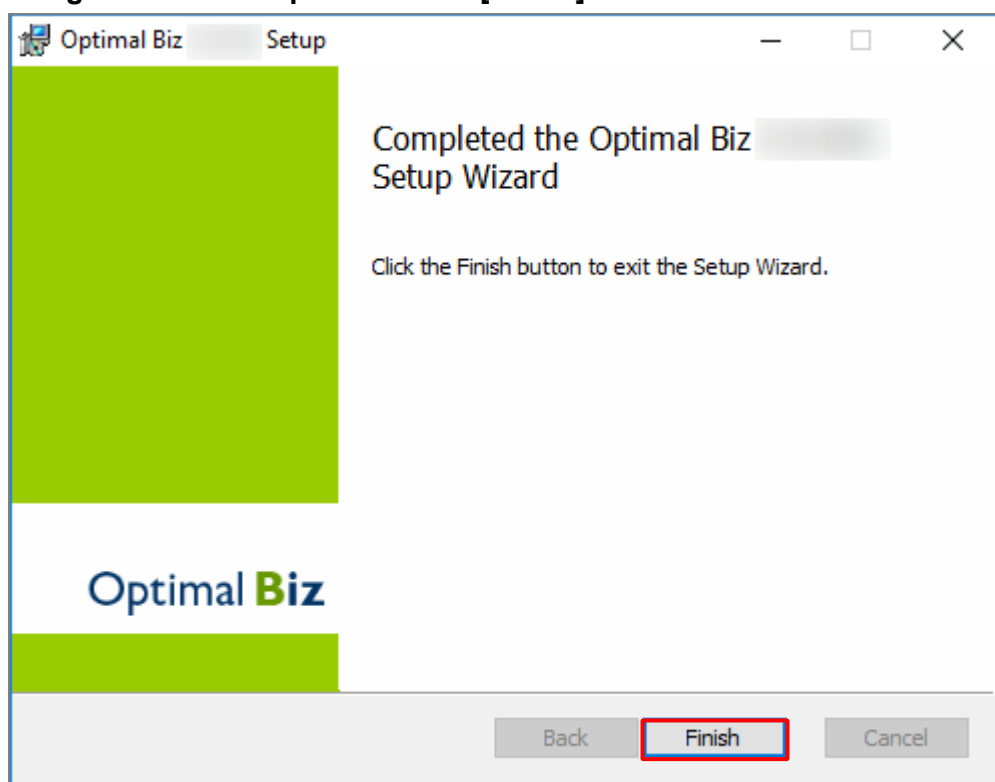
✓ If your agent is the latest version, this message is displayed. Click [OK].





**[5] Click [Install].****[6] Now updating. Wait.**

**[7]** The agent has been updated. Click [Finish].



---

## 7 Drive Encryption

When the drive encryption is set from the management site, a password is set on the Windows device.

Describes the following items.

Item	Page
<a href="#">Drive Encryption</a>	<a href="#">44</a>

## 7.1 Drive Encryption

Encryption is set from the management site. After encryption is set, the following screen is displayed. Set the password if your device doesn't include a TPM chip(\* 1).

\* 1: TPM chip is the IC chip that supports software encryption.

✎ The encryption target is system drive and data drive. Removable disk is not included.

✎ Manually encrypt the removable disk. For details, refer to the Microsoft website.

👉 [Microsoft - BitLocker Drive Encryption](#)

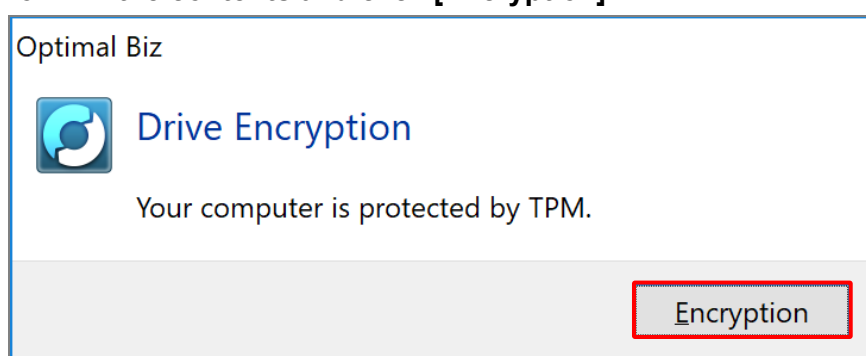
✎ Depending on the type of Windows OS, BitLocker encryption may not work properly. In this case, another encryption method needs to be employed. Keep in mind that, when choosing not to use BitLocker for a specific drive, the remote wipe function utilizing BitLocker will no longer be available for the drive.

✎ The password you set on this screen is needed to launch your Windows device. This product does not keep track of passwords used for encryption. Make sure to remember it, otherwise you cannot launch your Windows device.

✎ After encryption, if you connect an external USB hard disk and your environment of the computer is changed, you may need to enter a recovery key before you launch your computer. Contact your administrator to get 48 digit recovery password and unlock it.

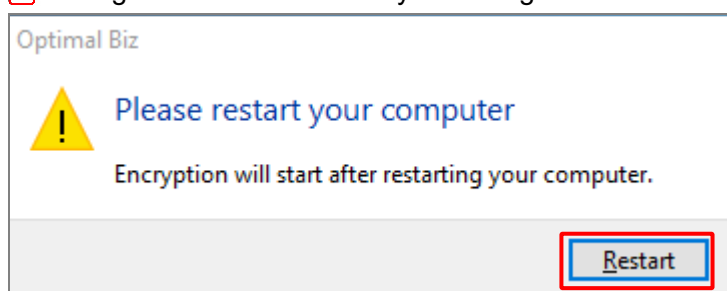
<<Device with TPM chip>>

**[1] Confirm the contents and click [Encryption].**



**[2] A dialog prompting to restart is displayed. Click [Restart].**

✎ The agent will be launched by restarting the Windows device.



## &lt;&lt;Device without a TPM chip&gt;&gt;

**[1] Enter the password and click [Encryption].**

- ✎ The password must be alphanumeric characters (Case sensitive) and be 8 or more characters.
- ✎ The password is not saved in this product. This product does not keep track of passwords used for encryption.



Drive Encryption - Optimal Biz

**Drive Encryption**

Please enter password for encryption:

Please enter password for encryption again:

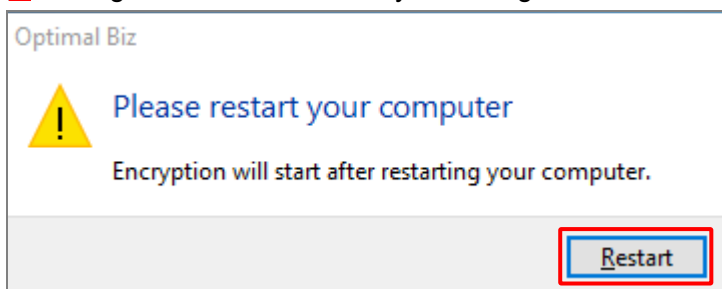
Password must be alphanumeric characters and 8 characters or more. It is case sensitive.

⚠ Attention: Password is needed when launching your computer.

**Encryption**

**[2] A dialog prompting to restart is displayed. Click [Restart].**

- ✎ The agent will be launched by restarting the Windows device.



Optimal Biz

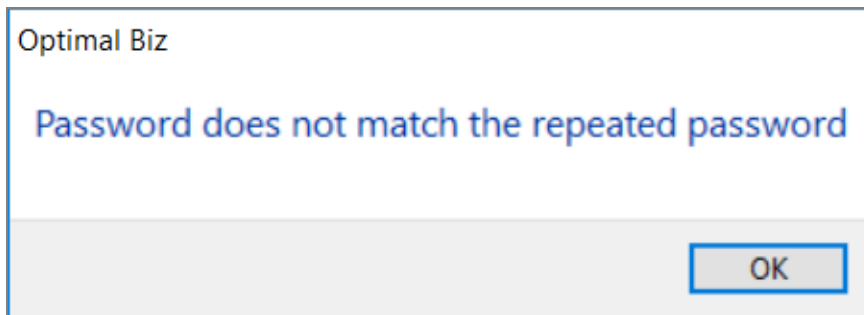
⚠ Please restart your computer

Encryption will start after restarting your computer.

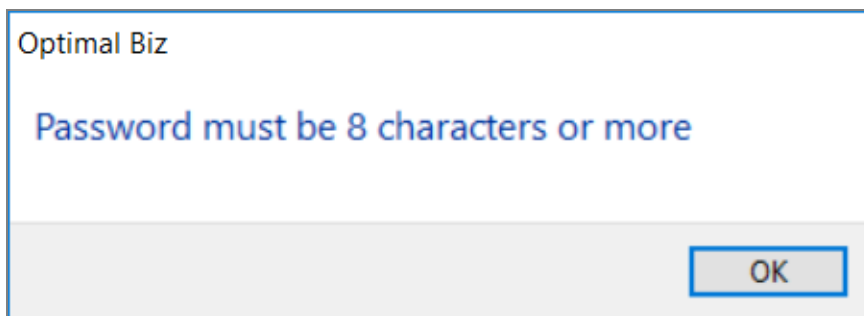
**Restart**

✎ If the password requirements are not fulfilled, the following error will be displayed.

- When the password and the re-entered password do not match



- When the password length is less than 8 characters



## 8 SIM Monitoring

We prohibit insertion of anything other than regular SIMs paid by the company to the Windows device, display the lock screen when the regular SIM is pulled out, and make the Windows device unoperatable.

You can also register another SIM as a regular SIM.

Describes the following items.

Item	Page
<a href="#">Timing of registered as regular SIM</a>	<a href="#">48</a>
<a href="#">Timing of released from regular SIM</a>	<a href="#">48</a>
<a href="#">Timing of displayed the lock screen</a>	<a href="#">49</a>
<a href="#">Release the lock screen</a>	<a href="#">49</a>



### Attention

- We do not recommend the use of USB-connected SIM (hereinafter referred to as USB-SIM) due to the following reasons.
  - USB-SIM connection can be detected but lock screen cannot be displayed because removal cannot be detected.
    - ⇒ When an unregistered USB-SIM is connected with the regular SIM inserted, the lock screen will be displayed. However, it is not possible to release the lock screen because you cannot detect removal of USB-SIM. Release from the management site.
      - ☞ "Release the lock screen" Page 49
  - When USB-SIM is registered as regular SIM, lock screen cannot be displayed because removal of USB-SIM cannot be detected.
    - ⇒ Because removal of USB-SIM cannot be detected, the record cannot be saved in the log. If you repeat USB - SIM connection -> Disconnect -> Connection -> Disconnect, logs will be recorded as "Insertion" -> "Insertion" continuously.
- Notes on using eSIM

If you are using external SIM on your device on a PC with both external SIM and eSIM, external SIM will be registered as regular SIM.

However, at the timing when the external SIM is removed, the device automatically switches to using eSIM, so eSIM may be recognized as an irregular SIM and the lock screen may be displayed. If the lock screen is displayed, cancel the lock screen from the management site and re-register the SIM.

  - ☞ "Release the lock screen" Page 49
  - 🔍 "(Setting - Windows) Setting allocation" - "Assets setting" - "List" - "Asset" in  
<Management Site Reference Manual>
- "ICCID" of unique identification number is used for each SIM in order to register as regular SIM. When SIM is lost or reissued, the ICCID will be changed even if the phone number does not change. Therefore, it will not be detected as regular SIM, re-register again.

## 8.1 Timing of operation and release method

---

### 8.1.1 Timing of registered as regular SIM

---

Register as regular SIM at the following timing.

- When "SIM Monitoring" is enabled during agent authentication
  - With SIM  
Register the SIM detected at the time of synchronization after authentication as regular SIM.
  - Without SIM  
Register SIM that was detected for the first time as regular SIM.
- When "SIM Monitoring" changes from "Disabled" to "Enabled" after agent authentication
  - With SIM  
Register SIM inserted at the timing when "Enabled" setting is accepted as regular SIM.
  - Without SIM  
Register SIM that was detected for the first time as regular SIM.

### 8.1.2 Timing of released from regular SIM

---

Released from regular SIM at the following timing.

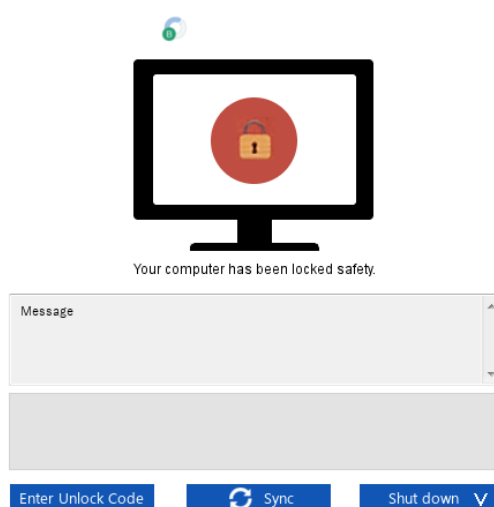
- Switch "SIM Monitoring" from "Enabled" to "Disabled" or "(None)"
- Release the agent authentication
- Uninstall the agent
  - 🔪 There is no effect even if you upgrade the agent version.



### 8.1.3 Timing of displayed the lock screen

Display the lock screen at the following timing.

- If a regular SIM is removed
  - Regular SIM is pulled out
  - If a non-regular SIM is inserted
  - If a non-regular SIM has been inserted
  - If no SIM is inserted
  - SIM other than regular SIM is inserted
- ☑ The connection status to the Internet can be online or offline.



### 8.1.4 Release the lock screen

When the lock screen is displayed on the Windows device, you can unlock in the following way.

- Insert regular SIM
- If regular SIM is inserted and irregular SIM is inserted, remove irregular SIM.
- If a non-regular SIM is inserted, remove the non-regular SIM
- Unlock from management site (\*1)

🔍 "(Operation - Windows) Unlock" - "Operation of Assets" - "List" - "Asset" in <Management Site Reference Manual>

👉 Enter unlock code to unlock(\*1)

☑ Contact administrator for unlock code.

\*1 : If "SIM Monitoring" switches from "Enabled" to "Disabled" or "(None)" while the lock screen is being displayed, the lock screen will continue to be displayed. In that case, perform the corresponding operation and release the lock screen.

---

## 9 SaaS ID Federation

If SaaS ID Federation is set on the management site, you can login to the SaaS application (Office 365 or Google Workspace (formerly G Suite)) with the ID of Optimal Biz.

For the login method with SaaS ID Federation method, For details, refer to the following.


 <SaaS ID/Access Control Operation Manual>

---

## 10 Windows Information Protection (WIP)

Windows Information Protection (hereafter referred to as WIP) is a feature introduced in Windows 10 version 1607 or later to prevent the leakage of corporate data.

For more information on enabling protection, please refer to the Administration Site Reference Manual.

 "Windows Information Protection" -<Management Site Reference Manual>.


The following items are explained.

Item	Page
<a href="#">Target file</a>	<a href="#">52</a>
<a href="#">Message displayed when data is shared</a>	<a href="#">60</a>
<a href="#">Operation using USB</a>	<a href="#">63</a>



### Attention

- For more information about WIP, please refer to the official Microsoft website.

 <https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/protect-enterprise-data-using-wip>

---

## 10.1 Target file

### ◆ Function purpose

You can set WIP on the management site and make files created by the target application as protected files. By making it a protected file, you can prevent the leakage of corporate data.






### ◆ Terms of Use

It is compatible with both 32-bit and 64-bit versions of the Windows operating system (Windows10 Pro (1803 or later), Windows10 Enterprise (1709 or later), Windows10 Education (1709 or later) and Windows 11 Pro/Enterprise/Education.


 Specifications may vary depending on the device you use.

### ◆ Level of Windows information protection

The following are the levels of Windows information protection (hereafter referred to as protection levels) that can be set at the management site. The behavior differs depending on the protection level set.

Item	Description
Invalid	No data protection or monitoring is provided.  Set to disabled when disabling protected apps.
Record	Record inappropriate data sharing.  Get a log of the data sharing status of the protected application. For more information, please refer to the following.  Windows Information Protection Event Log" - <Management Site Reference Manual>
Warnings and Records	Detects, warns and records inappropriate data sharing.  Inappropriate data sharing of protected apps will result in a warning screen being displayed.
Prohibition	Detects inappropriate data sharing and prohibits app operations.  Prohibits the manipulation of data in protected applications.

 Inappropriate data sharing includes copying data from a protected file and pasting it into an unprotected file.

 Please contact your administrator for more information about the settings.

### ◆ Scope of files to be protected

Covered	Not covered
<ul style="list-style-type: none"> <li>• Inside the device</li> <li>• USB</li> <li>• External device</li> <li>• Within the local network</li> </ul>	Not listed in the left Ex.) <ul style="list-style-type: none"> <li>• cloud</li> <li>• proxy</li> </ul>

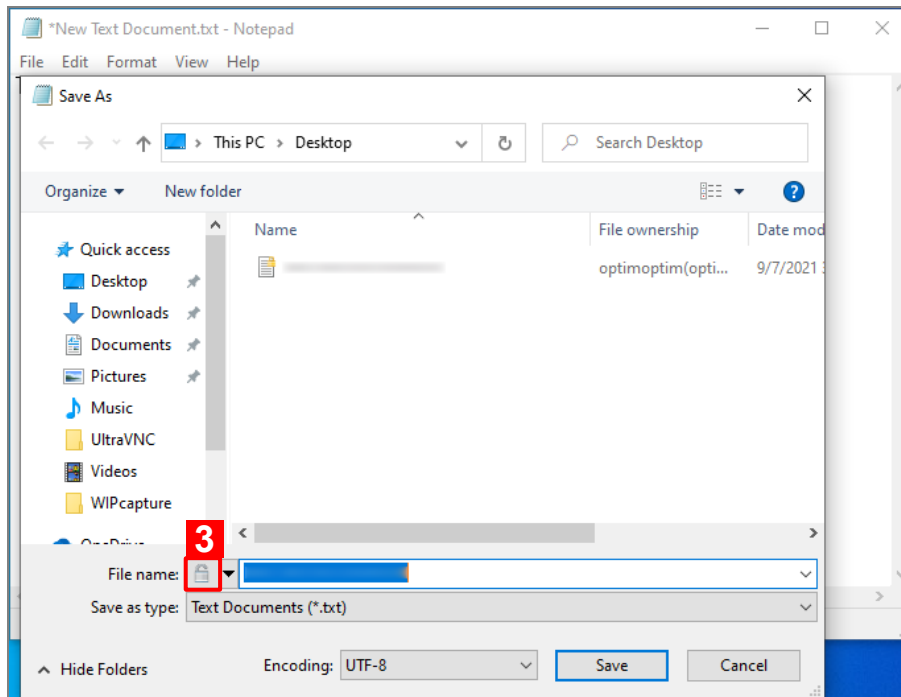
### 10.1.1 Create a new file to be protected.

To create a new file to be protected, perform the following.

- ✎ On Windows 11 or later, you cannot create a new file to be protected. After you create a file, set it as a protected file. Refer to the following for details.

👉 "Set as protected file" Page 54

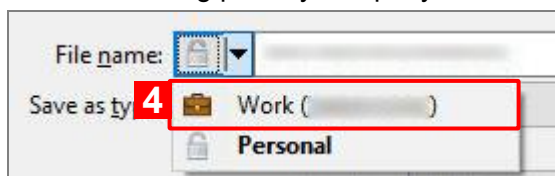
- [1] Create a file that you want to protect.**
- [2] Select [Save As...].**
- [3] Select the pull-down next to File name (N):.**



- [4] Select [Work (Primary Company ID)] from the list that appears.**

✎ If you do not select "Work (Primary Company ID)", the file will not be protected.

✎ Even if you add a primary company ID other than the primary company ID in the administration site, the existing primary company ID will be displayed.



- [5] Set any file name and save it.**

### 10.1.2 Set as protected file

To set an existing file created by a protected application as a protected file, perform the following operations.

✎ Even if you configure the settings on the management site, existing files cannot be made protected files without this operation.

**[1] Select the file you want to set as the protected file.**

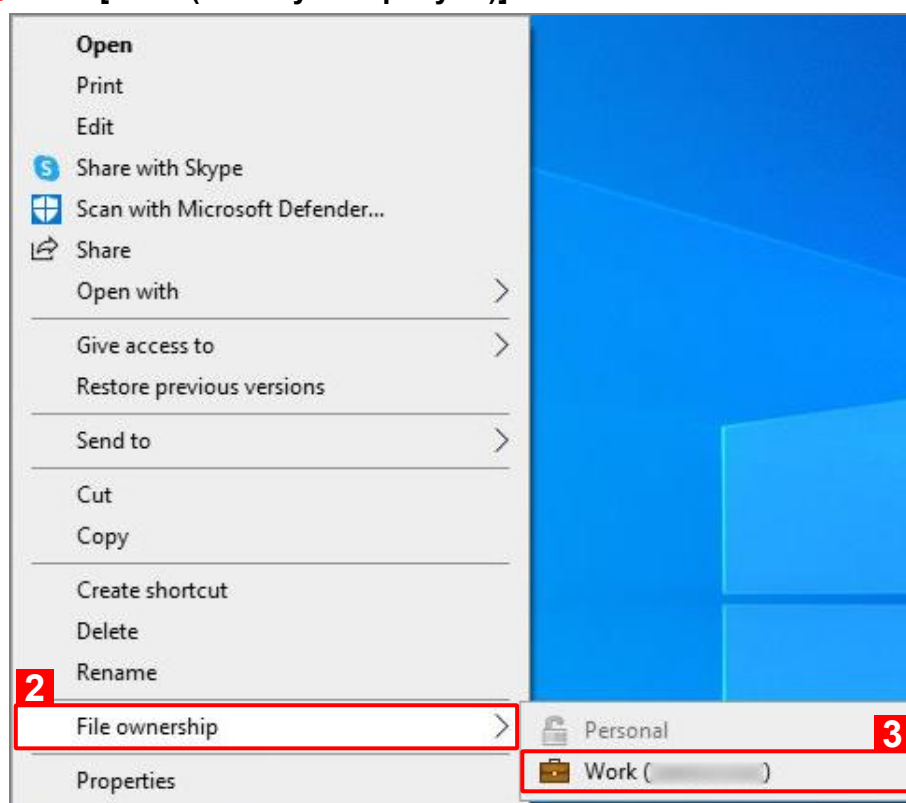
**[2] Right-click on the selected file and select [File Ownership].**

✎ Not displayed when the protection level is set to [Disabled].

To enable it, please contact your administrator.

✎ If the settings are not reflected in the currently running application, close the application and start it again.

**[3] Click [Work (Primary Company ID)].**



**[4] In the upper right corner of the target file will be displayed in the upper right corner of the target file, and it will be set as a protected file.**


✎ Due to the specifications of your device, the may be displayed as is displayed in some cases.


✎ If the file is set to the protection level [Prohibited] on the administration site, it cannot be removed once it is set as a protected file.


### 10.1.3 Check the management status of protected files.

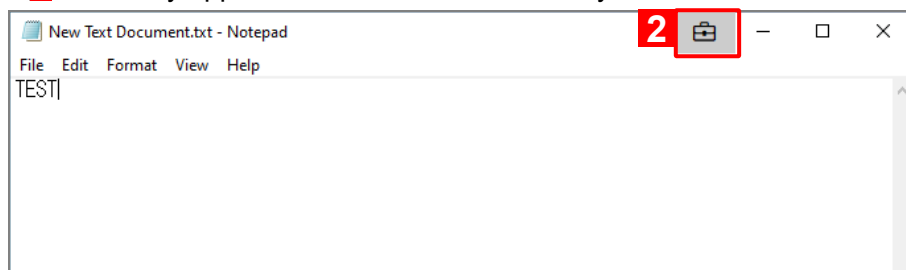
Displayed in the upper right corner of the file icon  The following is how to check the file except

**[1] Open the protected file you want to check.**

**[2] In the title bar  will be displayed in the title bar.**

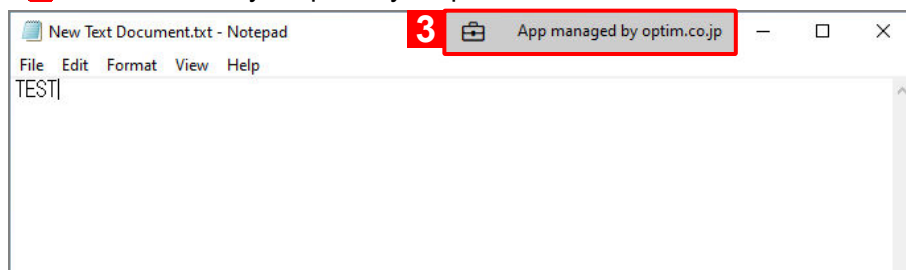
 It is displayed for files that have been set as protected files.

 It will only appear when the mouse is nearby.





**[3] Click  .**


 You can check your primary corporate ID information.

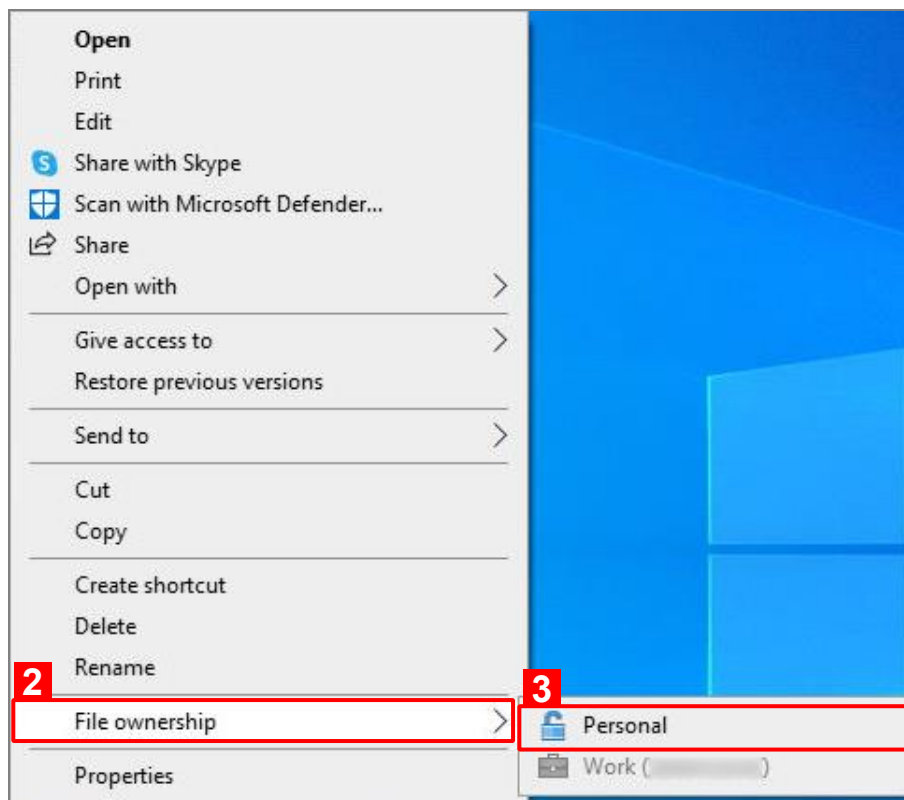


### 10.1.4 Remove protection from a file

To remove protection from a file, perform the following.

- ✎ If the protection level is set to "Prohibited", the protection cannot be removed.
- ✎ Due to the specifications of your device, the  may be displayed as  is displayed in some cases.

- [1] Select the file to be protected that is marked with .**
- [2] Right-click on the selected file and select [File Ownership].**
- [3] Click [Personal Use].**



- [4] The upper-right corner of the target file  in the upper right corner of the target file will disappear and the protection will be removed.**



### 10.1.5 Verify ownership

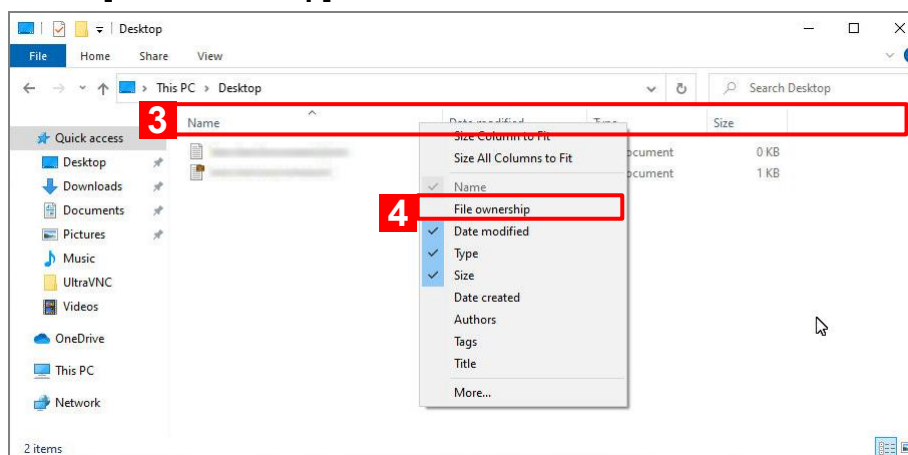
To check the ownership, check with the following procedure.

✎ Specifications may vary depending on the device you use.

#### Check with Explorer

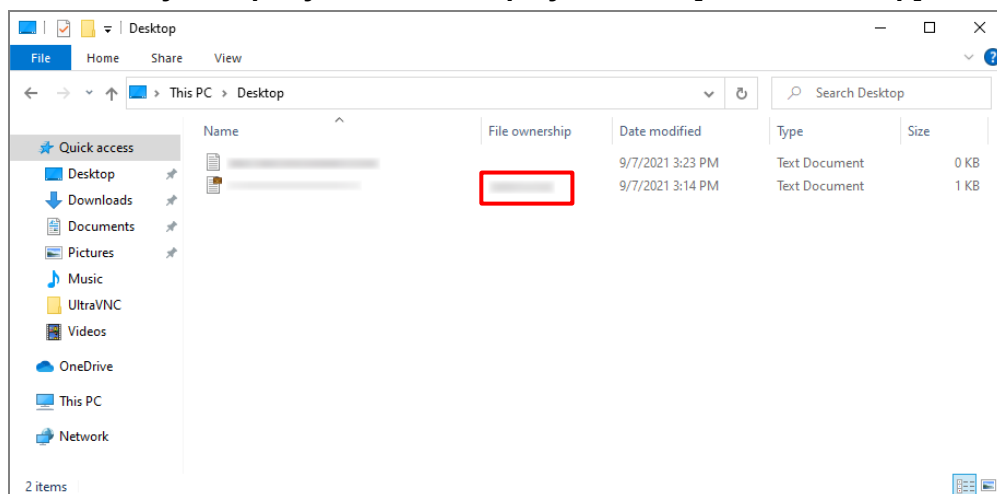
You can check the ownership of the protected files.

- [1] Open Explorer.**
- [2] On the [View] tab under [Layout], select [Details] to change the view.**
- [3] Right-click on the tab that appears.**
- [4] Select [File Ownership].**



✎ If you do not see [File Ownership], click [Other] and select [File Ownership] from the list that appears.

- [5] The Primary Company ID will be displayed in the [File Ownership] field.**




✎ The primary company ID is only displayed for protected files.

✎ The ownership of files other than those to be protected will be displayed as blank.

## Check in Task Manager.

You can check the WIP target apps.

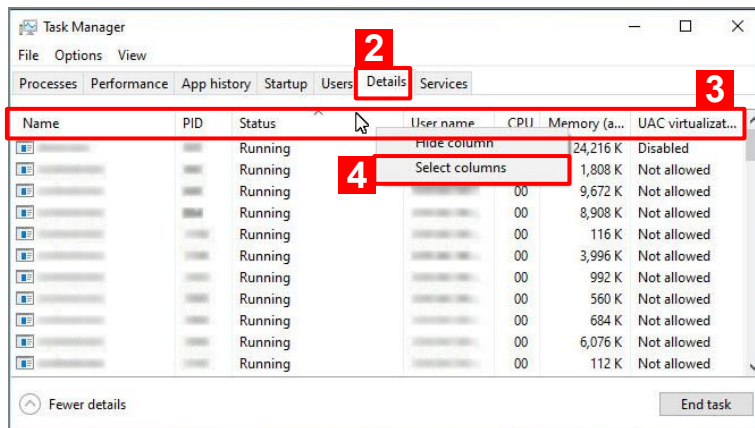
**[1] Launch the Task Manager.**

 If you are using the simple view, please change it to the detailed view.

**[2] Click on the [Details] tab.**

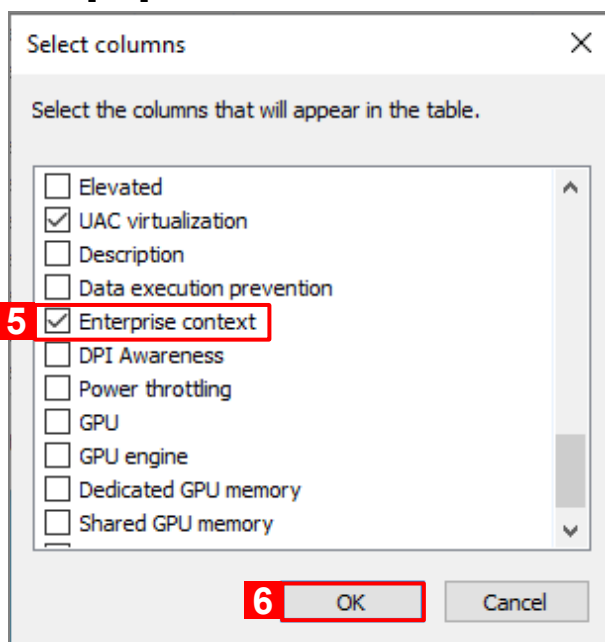
**[3] Right-click on the tab that appears.**

**[4] Click [Select Column].**

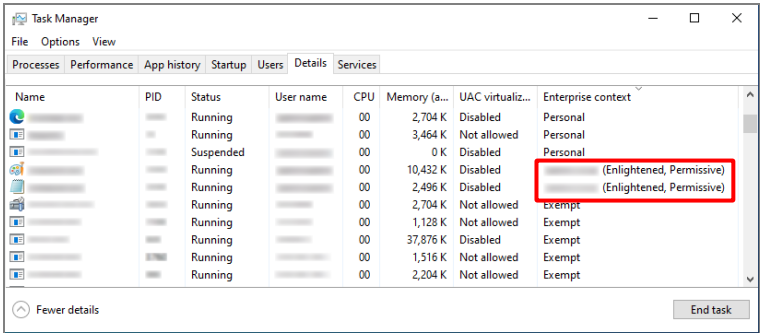


**[5] Select [Enterprise Context] from the table that appears.**

**[6] Click [OK].**



**[7] A row for the enterprise context will be added.**  
**The WIP target app will display the primary company ID.**



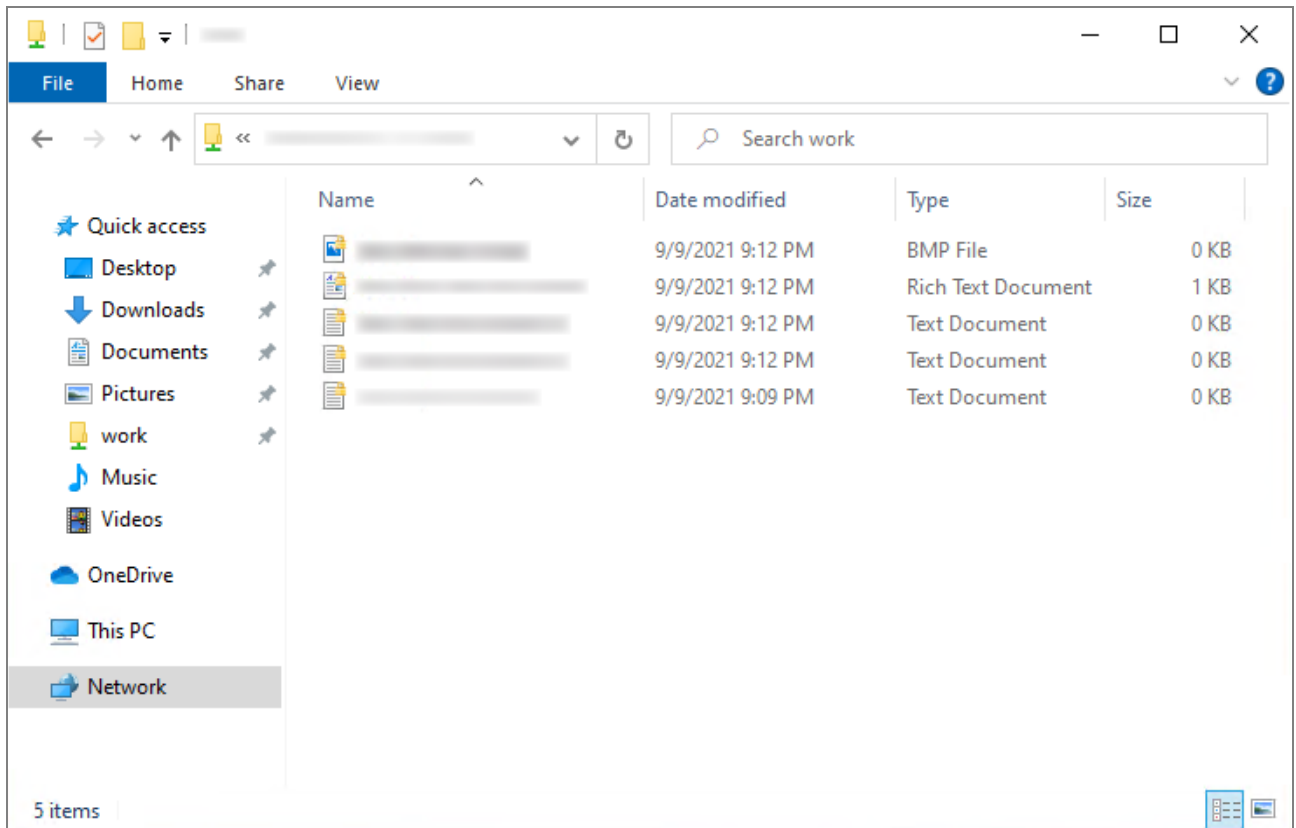
- ✚ Apps that do not support WIP will be labeled as personal use.
- ✚ Apps that are not WIP compliant will be marked as exceptions.

### 10.1.6 How it looks in a shared folder

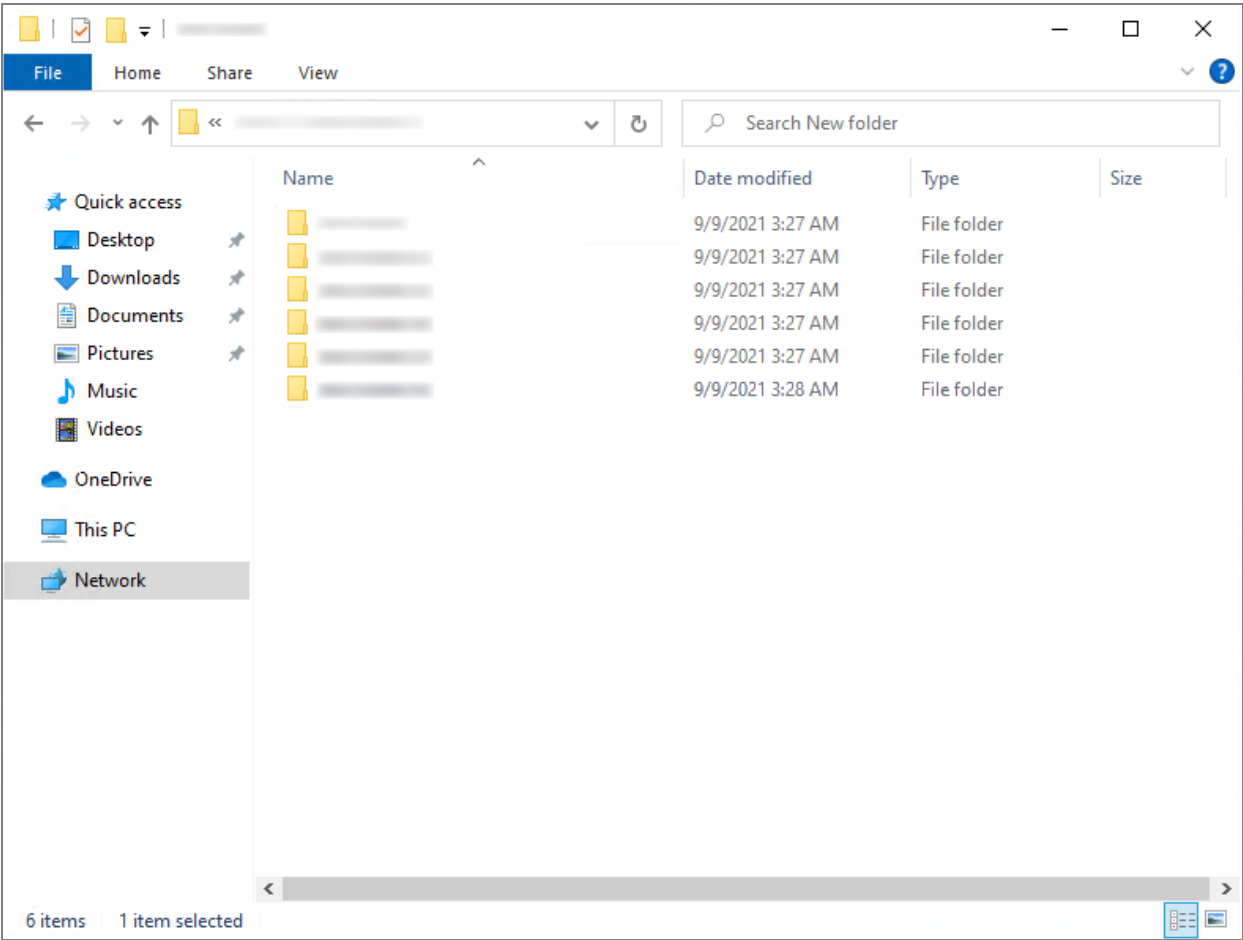
It will look different on the shared folder.

#### ◆ Shared folders with the same network domain name

- ✍ It will have an encryption icon, but it is not encrypted.
- ✍ It will be encrypted when copied from the shared folder to the local terminal.



◆ Shared folders with different network domain names



## 10.2 Message displayed when data is shared

The following message will be displayed.

- ✎ If you receive a message that is not listed below, please contact Microsoft.
- ✎ The message may be displayed differently depending on the OS version.

### 10.2.1 Messages for each protection level

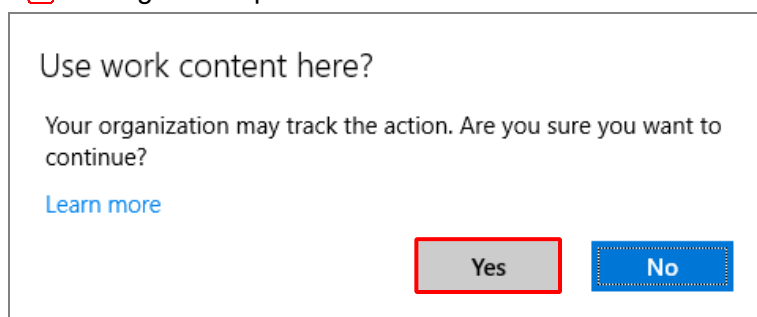
- ✎ When the protection level is set to [Disable] or [Record], the message will not be displayed.

#### When [Warning and Recording] is set

##### ● When [Yes] is clicked

⇒ You can ignore the warning and perform the operation.

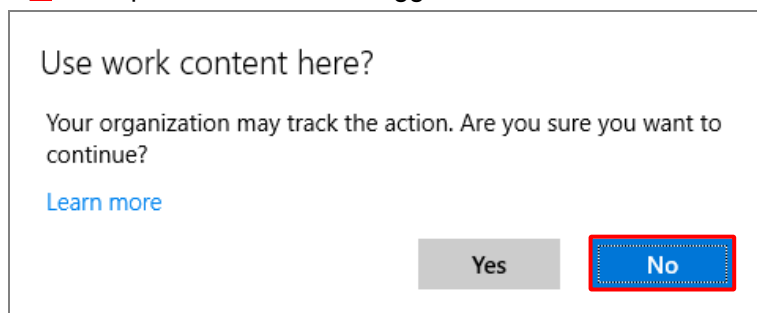
- ✎ The log of the operation will be retrieved.



##### ● When [No] is clicked

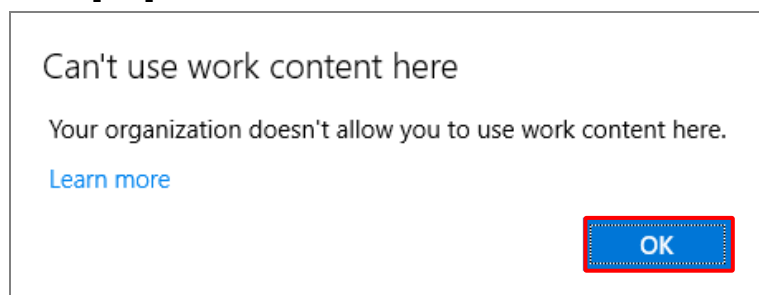
⇒ The warning will close and the operation will not be performed.

- ✎ The operation will not be logged.



#### When [Prohibited] is set

##### [1] Click [OK].



- ✎ If you click [OK], the operation will not be executed.
- ✎ The log will not be obtained.

## 10.3 Operation using USB

If you perform the following operations, the behavior will vary depending on the conditions.

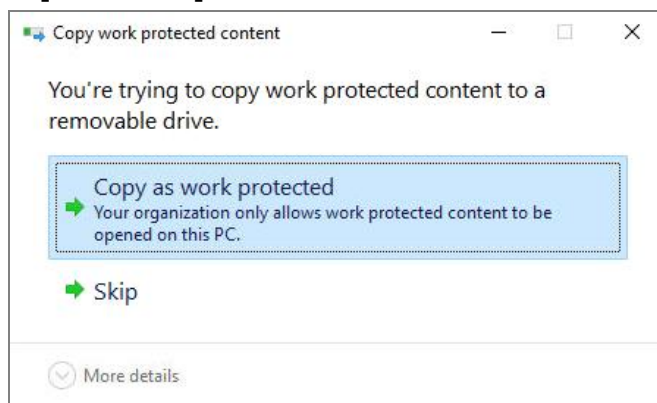
- ✎ Specifications may vary depending on the device you use.
- ✎ If your problem is not listed below, please contact Microsoft.

### 10.3.1 To copy protected files created on a WIP-adaptive terminal to USB

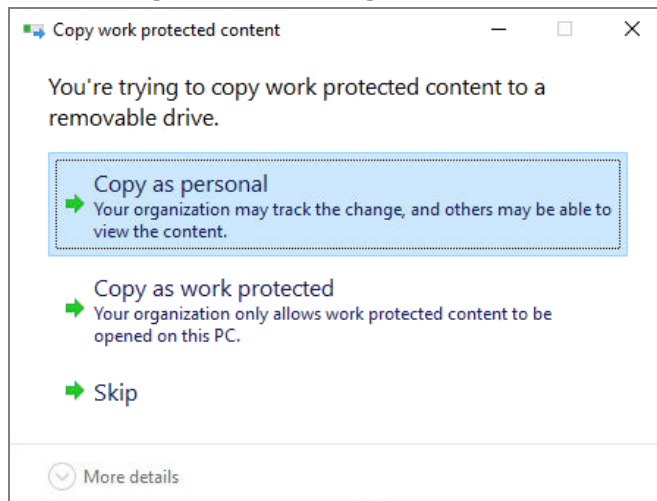
Different messages will be displayed depending on the protection level.

- ✎ If you set [Record] or [Disable], no message will be displayed and the file will not be saved as a protected file.

#### ◆ When [Prohibited] is set



#### ◆ When [Warning and Recording] is set



### 10.3.2 When the file to be protected exists in the USB and is opened on a different device under different conditions

The behavior varies depending on the conditions of the device you are trying to open.

#### When opening on a device where WIP has been applied at least once

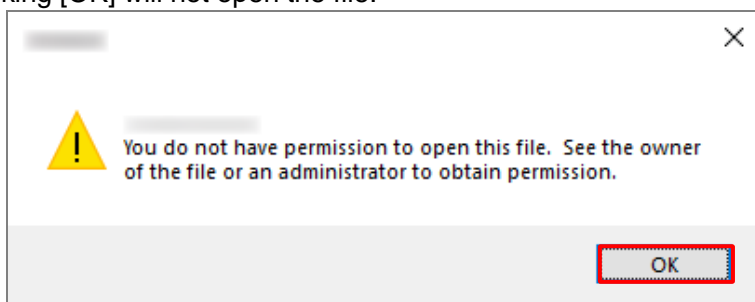
**[1] Double-click the file to be protected.**

- You have set [Prohibit], [Warn and Record] or [Record].  
⇒ Open as a protected file.
- • [Disabled] is set.  
⇒ The file will be opened with the protection removed.

#### When opening on a device that has never applied WIP (WIP-enabled OS)

The protected file cannot be opened on a device that has never applied WIP.

✂ Clicking [OK] will not open the file.



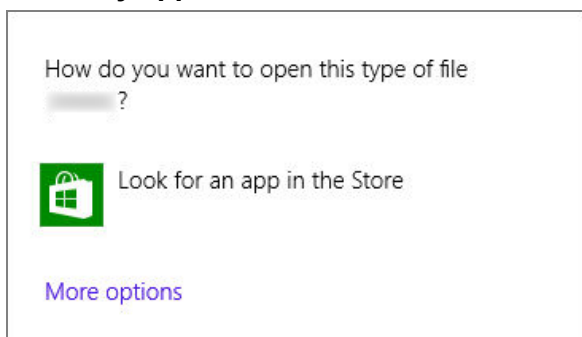
✂ For more information on WIP-supported operating systems, please refer to the following  
👉 “Terms of Use” Page 52

#### When opening on an OS that does not support WIP

If you open the file on an OS that is not WIP-compatible, such as Windows 7, the following behavior will occur.

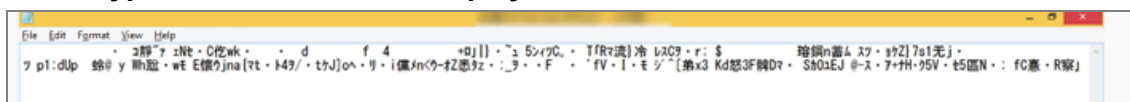
**[1] Double-click the file to be protected.**

**[2] Select any app.**



✂ Select an application that can display the contents of the protected file.

**[3] The encrypted contents will be displayed.**





### 10.3.3 Recovering data via USB

---

If you want to recover data via USB, refer to the following.

 <https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-and-verify-an-efs-dra-certificate>

 Please refer to the link [Recover WIP-protected after unenrollment].

---

## 11 Stop Agent Use

Describes the following items.

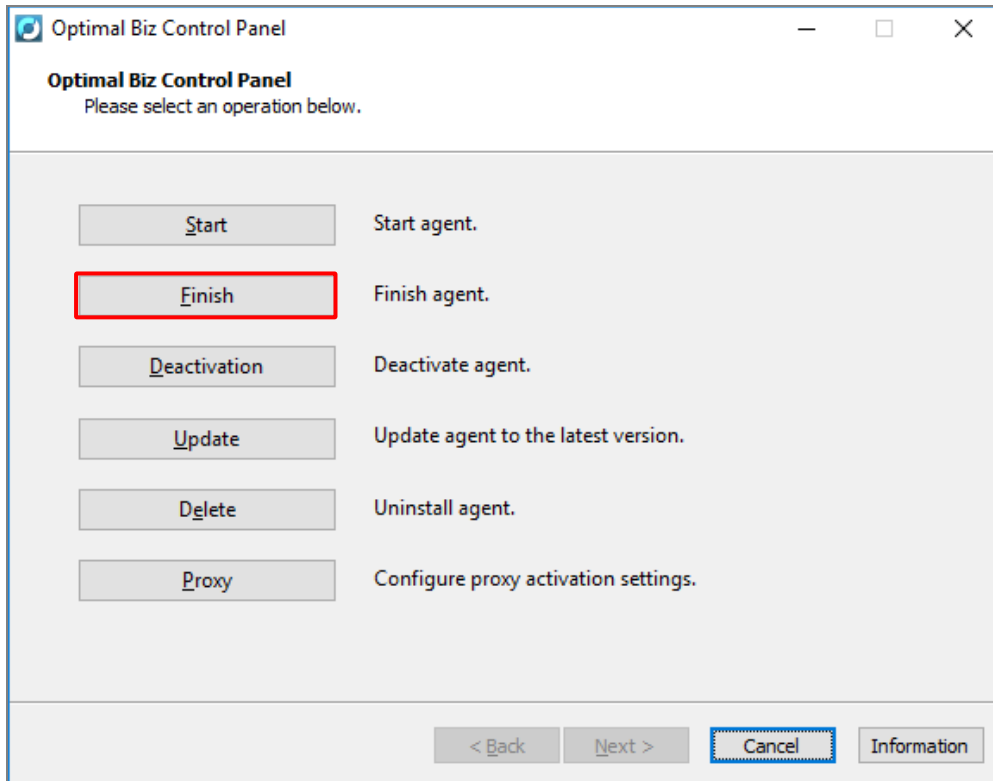
Item	Page
<a href="#">Finish agent</a>	<a href="#">67</a>
<a href="#">License activation</a>	<a href="#">70</a>

## 11.1 Finish agent

### 11.1.1 Finish agent

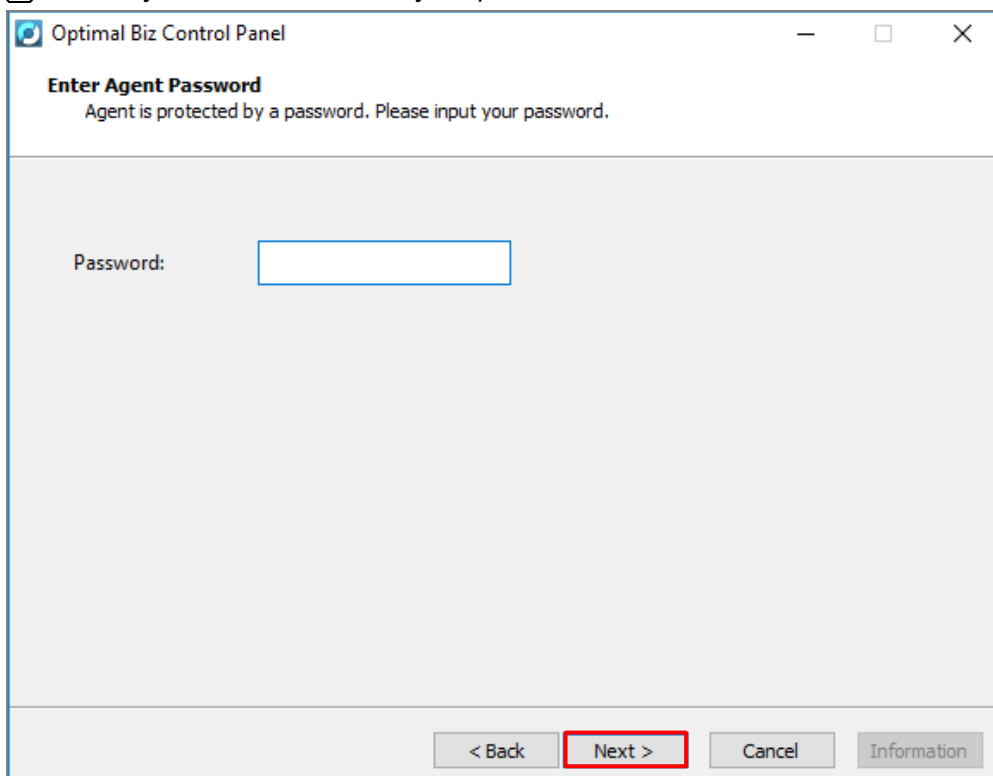
To finish the agent and temporarily stop managing the device, follow the steps below.

**[1] Open control panel and click [Finish].**



**[2] Enter "Password" and click [Next].**

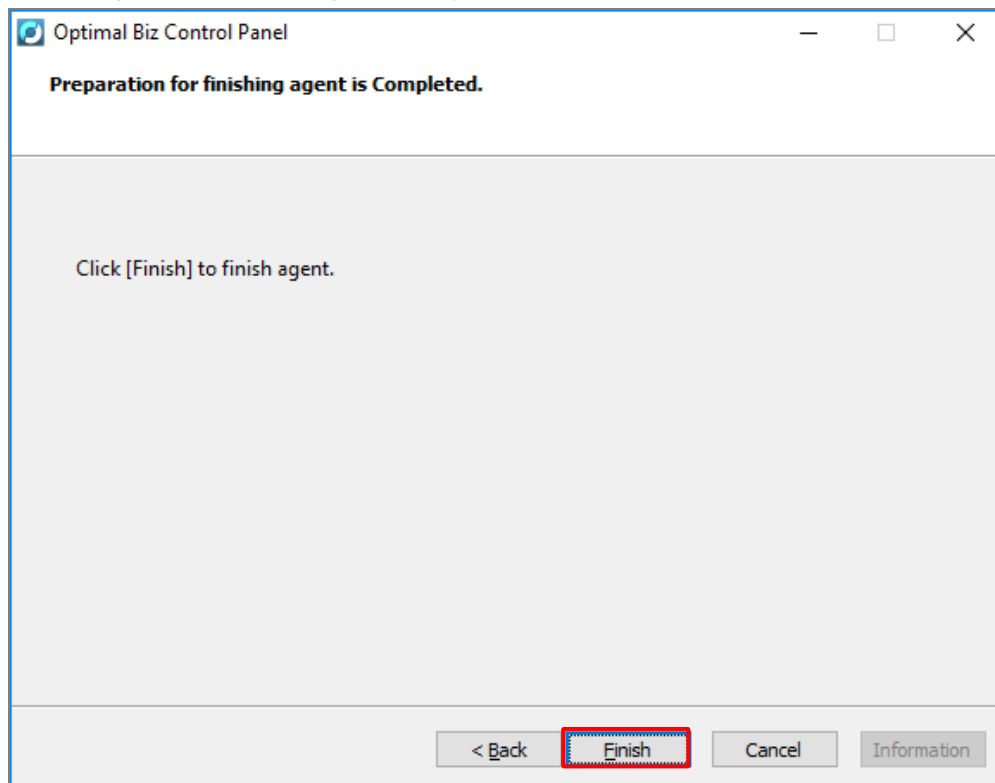
 Contact your administrator for your password.



**[3] Click [Finish].**

⇒ finish the agent.

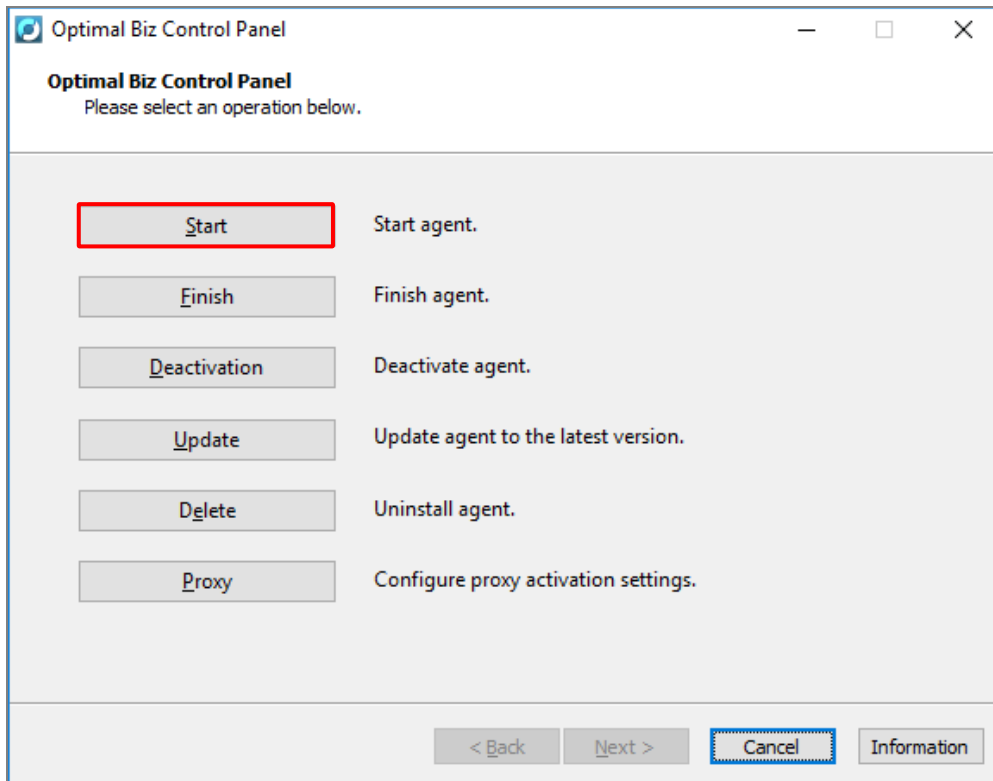
✎ The agent will launch again after you reboot the device.



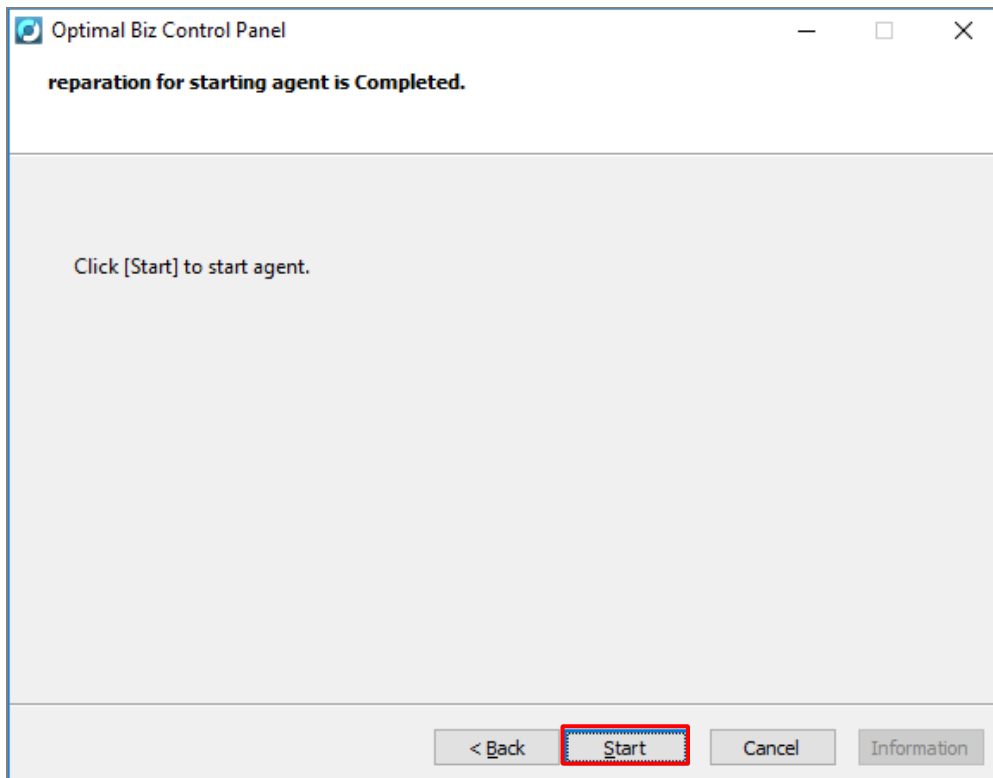
### 11.1.2 Re-Launch agent

To launch the agent again after you quit it, follow the steps below.

**[1] Open control panel and click [Start].**



**[2] Click [Start].**



## 11.2 License activation

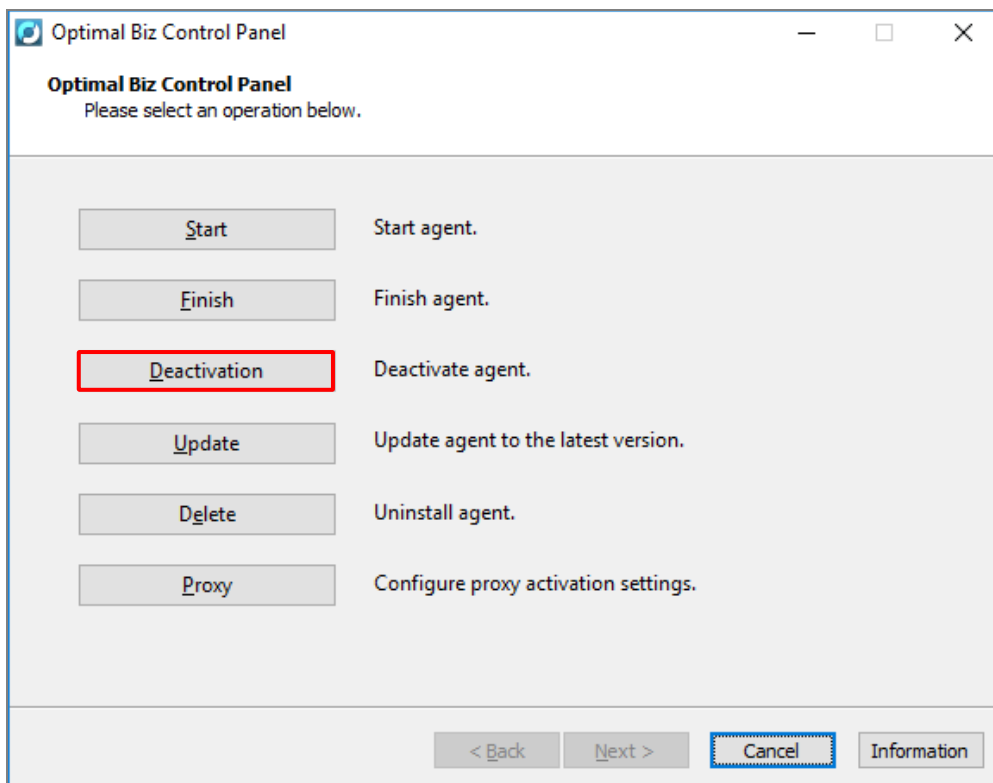
### 11.2.1 Deactivate agent

To deactivate the agent, follow the steps below. Deactivating the agent does not uninstall the agent from the device. For details, refer to the following.

☞ "Delete agent" Page 74

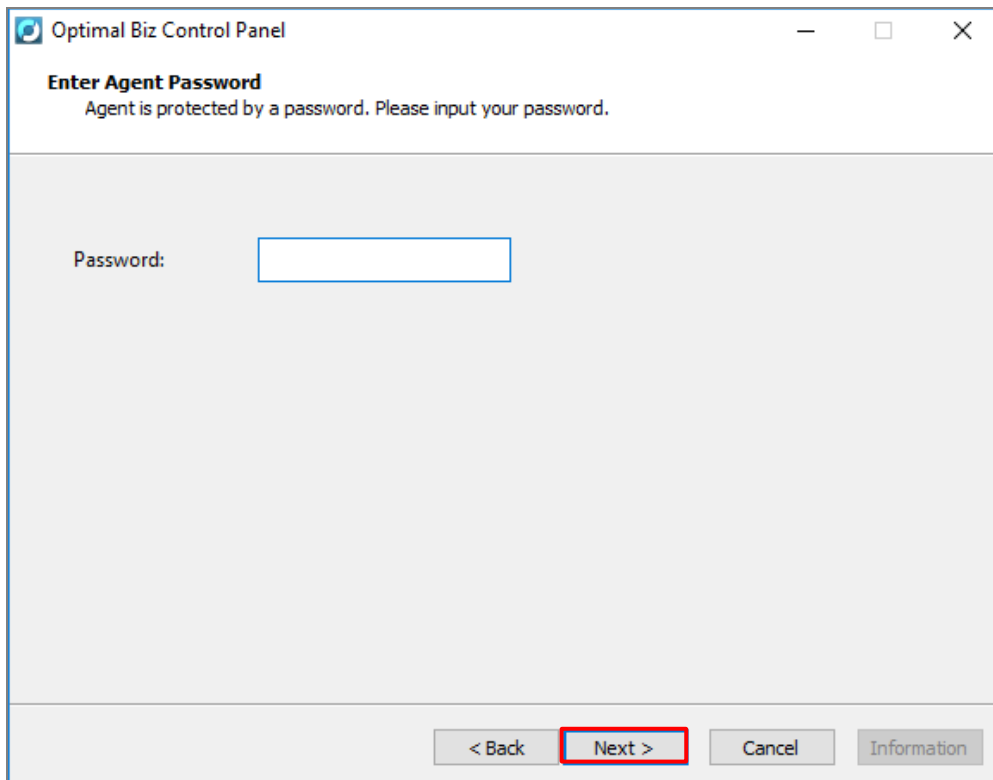
☑ When the Windows device is deleted on the management site, the license authentication on the Windows device side is automatically canceled at the next synchronization, so manual cancellation is unnecessary.

**[1] Open the control panel and click [Deactivation].**

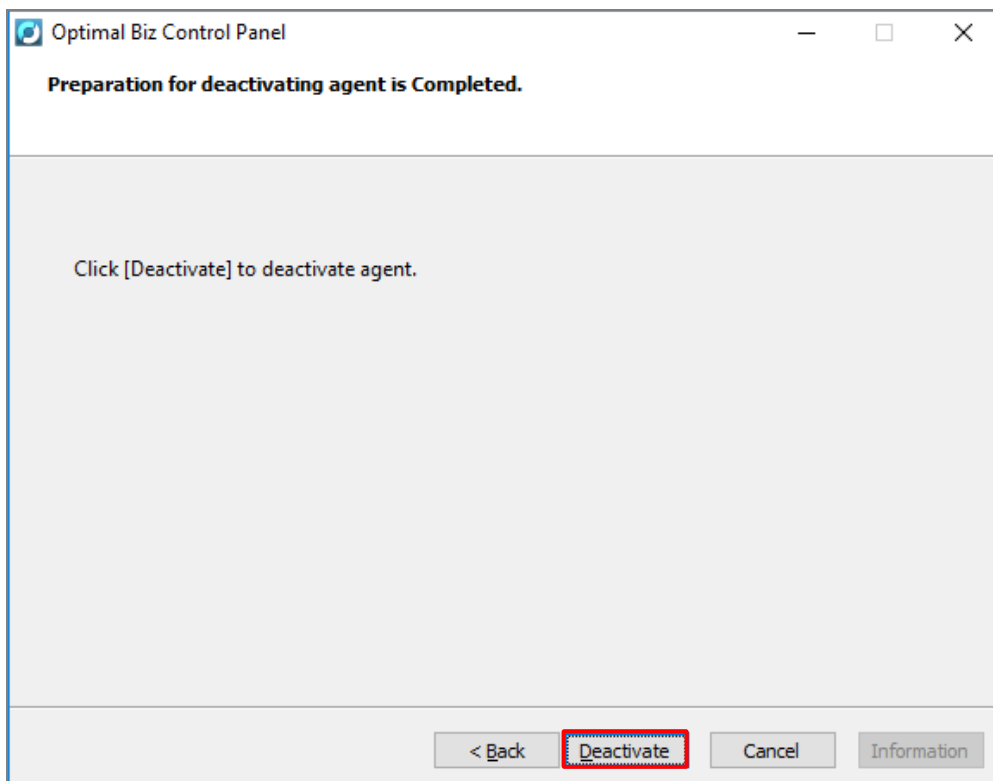


**[4] Enter "Password" and click [Next].**

 Contact your administrator for your password.



The dialog box is titled "Optimal Biz Control Panel" and "Enter Agent Password". It contains the text "Agent is protected by a password. Please input your password." Below this is a label "Password:" followed by a text input field. At the bottom, there are four buttons: "< Back", "Next >" (highlighted with a red box), "Cancel", and "Information".

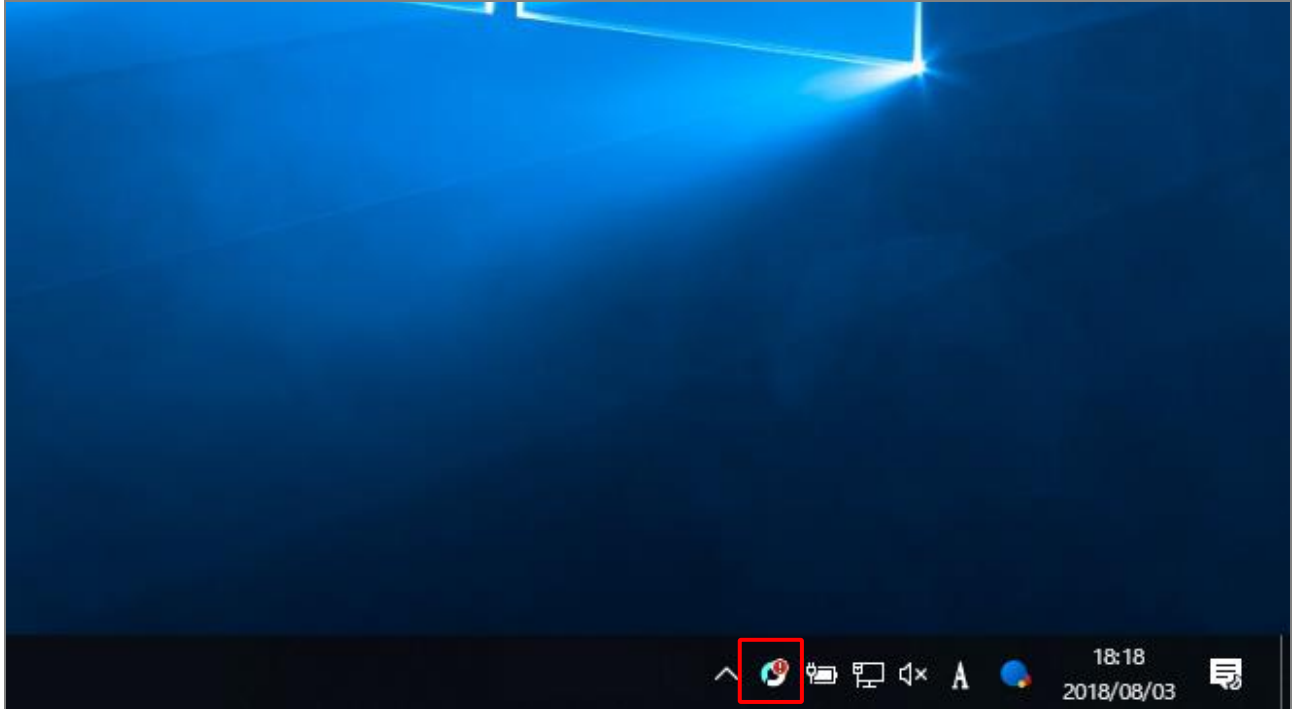
**[5] Click [Deactivate].**

The dialog box is titled "Optimal Biz Control Panel" and "Preparation for deactivating agent is Completed." It contains the text "Click [Deactivate] to deactivate agent." Below this is a large empty space. At the bottom, there are four buttons: "< Back", "Deactivate" (highlighted with a red box), "Cancel", and "Information".

## 11.2.2 Activate Agent

In the case you do not activate the agent yet or you want to activate the agent again after you deactivate the agent, follow the steps below.

**[1]** Double-click on  (the tray icon).

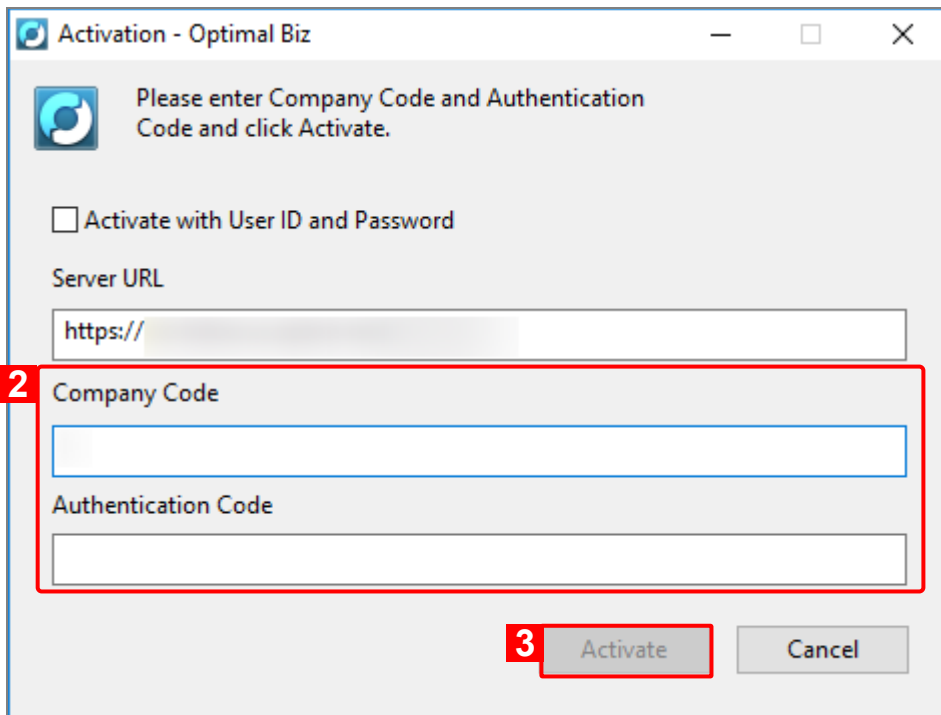




**[2] Activation screen is displayed. Enter "Company Code" and "Authentication Code".**

**[3] Click [Activate].**

 Contact your administrator for the "Company Code" and "Authentication Code".



Activation - Optimal Biz

Please enter Company Code and Authentication Code and click Activate.

☐ Activate with User ID and Password

Server URL

https://

**2** Company Code

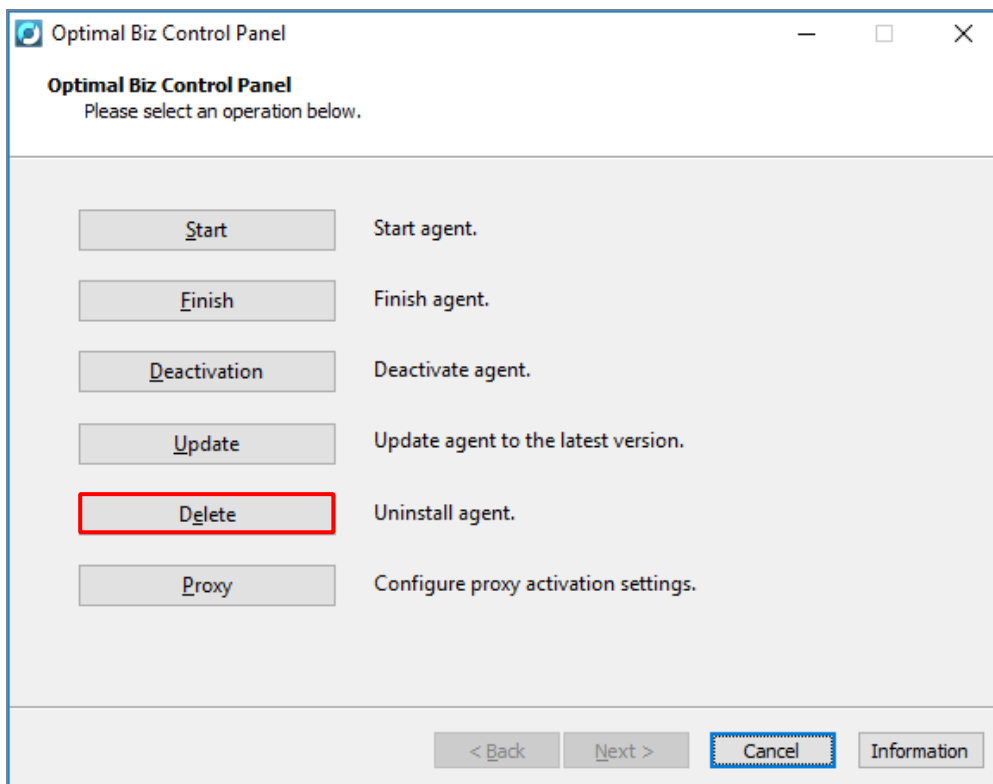
Authentication Code

**3** Activate Cancel

## 11.3 Delete agent

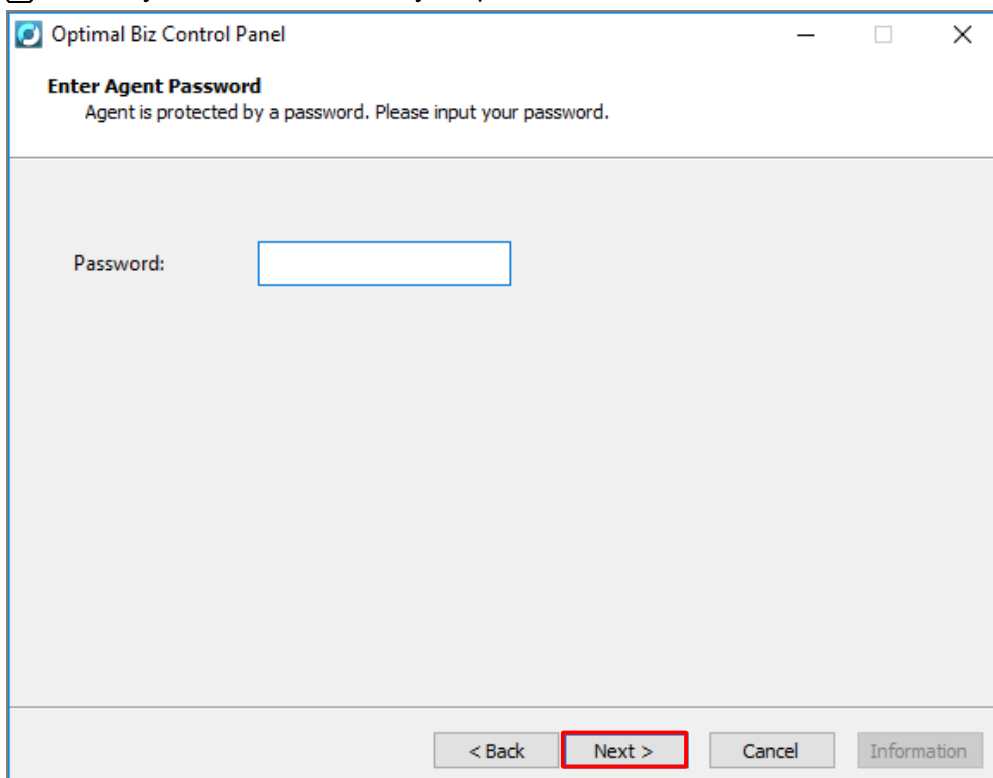
To delete the agent from the device, follow the uninstallation steps below.

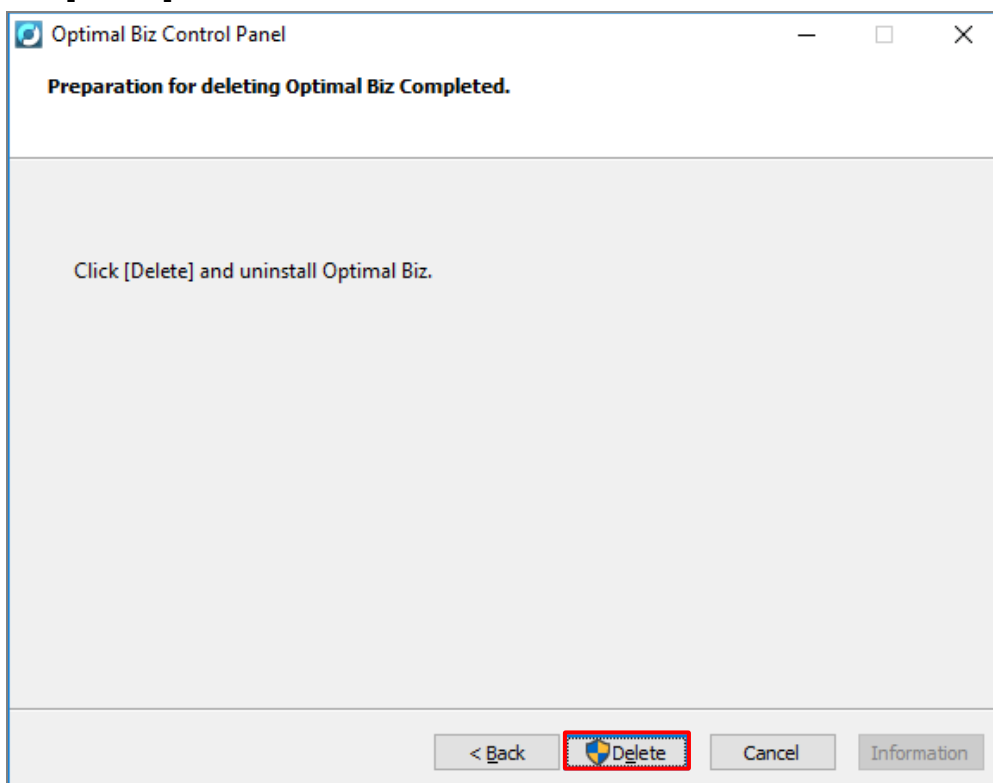
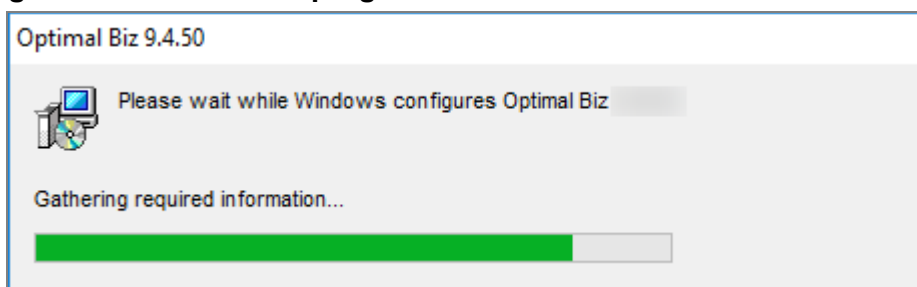
**[1] Open control panel and click [Delete].**



**[2] Enter your password and click [Next].**

 Contact your administrator for your password.



**[3] Click [Delete].****[4] Agent uninstallation in progress. Wait.****[5] The agent has been deleted. Click [OK].**