FUJITSU Software
Systemwalker Desktop Patrol

Installation Guide

Windows

Preface

Purpose of this guide

This guide describes necessary setting and operating procedures to install the following products.

- Systemwalker Desktop Patrol V15.1.0

Systemwalker is a generic name for the distributed system operation management products provided by Fujitsu Limited.

Intended readers

This guide is for those responsible for constructing asset management systems using Systemwalker Desktop Patrol as well as operating and managing asset management systems.

To understand the contents of this guide, the following knowledge is essential.

- General knowledge regarding Internet Information Services(IIS)

- General knowledge regarding personnel computers

- General knowledge regarding Windows

- General knowledge regarding the Internet

- General knowledge regarding smart devices

Structure of this guide

The structure of this guide is as follows:

Chapter 1 Design

This chapter describes the design required to install Systemwalker Desktop Patrol.

Chapter 2 Installation

This chapter describes how to install Systemwalker Desktop Patrol.

Chapter 3 Maintenance

This chapter describes how to back up and restore the processing data via Systemwalker Desktop Patrol.

Chapter 4 Version Upgrade

This chapter describes how to perform version update for Systemwalker Desktop Patrol.

Chapter 5 Uninstallation

This chapter describes how to uninstall Systemwalker Desktop Patrol.

Appendix A Server Silent Installation

This appendix describes files, commands, and messages used in silent installation of the Systemwalker Desktop Patrol server.

Location of this guide

In Systemwalker Desktop Patrol manual, location of this guide is shown as follows.

Manual Name	Contents
Systemwalker Desktop Patrol Release Information	Functions modified and added to Systemwalker Desktop Patrol, and items that become incompatible after a version upgrade.
Systemwalker Desktop Patrol User's Guide	Basic knowledge of Systemwalker Desktop Patrol, such as overview, features, functions, etc.

Manual Name	Contents
Systemwalker Desktop Patrol Installation Guide (this guide)	How to install Systemwalker Desktop Patrol, change the operation environment, and perform maintenance.
Systemwalker Desktop Patrol Operation Guide: for Administrators	How to collect PC information, install security patches, distribute software, license management, management ledger, and environment setup of Systemwalker Desktop Keeper.
Systemwalker Desktop Patrol Operation Guide: for Clients	How to install, operate and change the settings of the client side. In addition, it explains how to handle error messages output from client side.
Systemwalker Desktop Patrol Reference Manual	Commands, files and port numbers used in Systemwalker Desktop Patrol. In addition, it explains how to handle error message output from Systemwalker Desktop Patrol.

Also, the following manuals are enclosed as Systemwalker Live Help manuals. Refer to them when you use the remote operation function (Systemwalker Live Help Function).

Manual Name	Contents
Systemwalker Live Help User's Guide	It explains how to install Systemwalker Live Help, how to use the hardware and software and set the support center. In addition, it also explains how to manage by Live Help Connection Manager.
Systemwalker Live Help Client Guide	It explains how to install, use and set Systemwalker Live Help Client.

Symbols used in this guide

This guide uses the following names, symbols and abbreviations for explications.

Symbols used in commands

This subsection describes the symbols used in the examples of commands.

Meaning of symbols

Symbol	Meaning
[ ]	Indicates that the items enclosed in these brackets can be omitted.
l	Indicates that one of the items separated by this symbol should be specified.
{ }	Indicates that one of the items enclosed in these symbols should be specified.

Symbols used in this guide

The following symbols are used in this guide.

Meaning of symbols

Symbol	Meaning
n	Indicates variable value.

Note

Indicates an item requires special attention.

Point

....

Indicates useful information.

....

DTP installation directory

The directory in which Systemwalker Desktop Patrol CS, Systemwalker Desktop Patrol DS, Systemwalker Desktop Patrol AC, Systemwalker Desktop Patrol ADT, Systemwalker Desktop Patrol CT or Systemwalker Desktop Patrol SS is installed is indicated as the DTP installation directory.

Abbreviations

In this guide, the product names are abbreviated as follows.

Product Name	Abbreviation
Systemwalker Desktop Patrol CS	CS
Systemwalker Desktop Patrol DS	DS
Systemwalker Desktop Patrol AC	AC
Systemwalker Desktop Patrol ADT	ADT
Systemwalker Desktop Patrol CT	CT
Systemwalker Desktop Patrol SS	SS
Systemwalker Desktop Patrol Client	Smart device CT

In this guide, the operating system names are abbreviated as follows.

Abbreviation	Full Name
Windows Server(R) 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Datacenter
Windows Server(R) 2012	Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Essentials Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Datacenter
Windows Server(R) 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise
Windows Server(R) 2008	Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise

Abbreviation	Full Name
Windows(R) 8.1	Windows(R) 8.1 Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise
Windows(R) 8	Windows(R) 8 Windows(R) 8 Pro Windows(R) 8 Enterprise Windows(R) 8.1 Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise
Windows(R) 7	Windows(R) 7 Enterprise Windows(R) 7 Ultimate Windows(R) 7 Professional Windows(R) 7 Home Premium
Windows Vista(R)	Microsoft(R) Windows Vista(R) Ultimate Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Home Premium Microsoft(R) Windows Vista(R) Home Basic Microsoft(R) Windows Vista(R) Ultimate 64-bit Edition Microsoft(R) Windows Vista(R) Enterprise 64-bit Edition Microsoft(R) Windows Vista(R) Business 64-bit Edition Microsoft(R) Windows Vista(R) Home Premium 64-bit Edition Microsoft(R) Windows Vista(R) Home Basic 64-bit Edition
Windows	Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Essentials Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Windows(R) 8.1 Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise Windows(R) 8 Windows(R) 8 Pro Windows(R) 8 Enterprise Windows(R) 7 Enterprise Windows(R) 7 Ultimate Windows(R) 7 Professional Windows(R) 7 Home Premium Microsoft(R) Windows Vista(R) Ultimate Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Home Premium Microsoft(R) Windows Vista(R) Home Basic

Abbreviation	Full Name
	Microsoft(R) Windows Vista(R) Ultimate 64-bit Edition Microsoft(R) Windows Vista(R) Enterprise 64-bit Edition Microsoft(R) Windows Vista(R) Business 64-bit Edition Microsoft(R) Windows Vista(R) Home Premium 64-bit Edition Microsoft(R) Windows Vista(R) Home Basic 64-bit Edition
IIS	Internet Information Services 6.0 Internet Information Services 7.0 Internet Information Services 7.5 Internet Information Services 8.0 Internet Information Services 8.5
IE	Microsoft(R) Internet Explorer(R) 6.0 Windows(R) Internet Explorer(R) 7 Windows(R) Internet Explorer(R) 8 Windows(R) Internet Explorer(R) 9 Windows(R) Internet Explorer(R) 10 Windows(R) Internet Explorer(R) 11
Android	Android(TM) 3.0 - Android(TM) 5.0
iOS	iOS 5.0 - iOS 8.1

Shortcuts in the Start window of Windows(R) 8 and Windows Server(R) 2012

To check which product a shortcut in the **Start** window is for, right-click the shortcut and click **Open File Location** from the menu at the bottom of the screen. This will open the file location in **Windows Explorer**, where the product name can be checked.

Halfwidth characters

In this guide, the "halfwidth characters to be handled" refer to the following ASCII characters, except in places where limitations for the halfwidth characters that can be used are described.

- Halfwidth spaces

- Halfwidth symbols

   ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

- Halfwidth numbers

   0 1 ... 9

- Halfwidth alphabetic characters

   A B ... Z

   a b ... z

Characters other than the above are treated as fullwidth characters.

Version notation

The following versions of this product do not have an English version - ignore references to them.

- Systemwalker Desktop Patrol V12.0L10

- Systemwalker Desktop Patrol V13.3.0

- Systemwalker Desktop Patrol V14.0.0

- Systemwalker Desktop Patrol V14.0.1

- Systemwalker Desktop Patrol V14.1.0

- Systemwalker Desktop Patrol V14.3.0

- Systemwalker Desktop Patrol V14.3.1

- Systemwalker Desktop Patrol V15.0.0

- Systemwalker Desktop Patrol V15.0.1

For example, read "V15.0.1 or later" as "V14.2.0 or later", because V15.0.1 does not have an English version.

Likewise, read "V14.0.0 or earlier" as "V13.2.0 or earlier", because V14.3.1 does not have an English version.

The table below shows the available versions:

Japanese version	English version
V11.0L10	V11.0L10
V12.0L10	V11.0L10
V13.0.0	V13.0.0
V13.2.0/V13.2.1	V13.2.0
V13.3.0	V13.2.0
V14.0.0/V14.0.1	V13.2.0
V14.1.0	V13.2.0
V14.2.0	V14.2.0
V14.3.0	V14.2.0
V14.3.1	V14.2.0
V15.0.0	V14.2.0
V15.0.1	V14.2.0
V15.1.0	V15.1.0

Export management regulations

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Trademark

Intel, Intel vPro and Centrino are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows NT, Windows Vista, Windows Server, Active Directory and names or product names of other Microsoft's products are registered trademarks of Microsoft Corporation in the United States and other countries

Oracle is the registered trademark of Oracle Corporation.

Symantec, the Symantec logo, and Norton AntiVirus are registered trademarks of Symantec Corporation in the United States.

VirusBuster is registered trademark of Trendmicro Ltd.

VirusScan and NetShield are trademarks or registered trademarks of Network Associate, Inc. or its affiliates.

Google, the Google logo, Android, the Android logo, Google Play, the Google Play logo, Gmail, and the Gmail logo are trademarks or registered trademarks of Google Inc.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

Apple, the Apple logo, and Mac OS are trademarks of Apple Inc., registered in the United States and other countries.

All other trademarks are the property of their respective owners.

Screen shots are used in accordance with Microsoft Corporation's guidelines.

July 2015

Contents

Chapter 1 Design

This chapter describes the design required for installation of Systemwalker Desktop Patrol.

1.1 Determine System Configuration

This section explains how to design the deployment of the following components in the system of Systemwalker Desktop Patrol. For details on the components, refer to *Systemwalker Desktop Patrol User's Guide*.

Among these components, some may not be compatible with the others. Refer to "Products Unavailable for Combined Application" in the *Systemwalker Desktop Patrol User's Guide* for conformation prior to the design of system configuration.

The following important points shall be noticed when installing the components according to the design of system configuration:

CS

    CS is a server which defines operation polices of software distribution and collection policies for inventory information, and distributes service to each proxy.

    This server provides security patch distribution, security auditing, power saving monitoring and license management service through a web browser according to a database containing IT asset information (IT policy) and organization information (human resources and section information). Usually, one CS is installed in a company.

DS

    DS is a server which transfers or saves operation policies, collects or distributes inventory information or distributed software.

    The server is installed for load sharing. It is effective when a CT is remote, the speed of network line is low, or the capacity of the distributed software is larger.

AC

    AC is a management console for report output, asset information registration and alteration, and Location Map creation and browse.

    It is not necessary to install an AC if the above functions are not used.

CT

    The CT is installed in a PC that manages assets by collecting inventory information. It provides distributed software download and security patch reception service.

    CT is installed together with CS and DS.

ADT

    ADT is installed in each network segment and can automatically detect the devices connecting to the network in the same segment. Also, it notifies the detected device information to CS.

Web GUI

    Web GUI is an operation view of operation of Systemwalker Desktop Patrol which is carried out through the web browser in order to make use of services provided by CS.

    Additionally, operation policies of CT can be set.

    Main menu and download menu are included in Web GUI.

SS

    SS is a server that relays the inventory information between the CS and smart device CT to manage smart devices.

Smart device CT

    It is installed on smart devices that manage the assets through inventory information collection.

Live Help Expert

    This software is used for remote operation on Live Help Client. With this software, the CT user can directly connect to the PC of the CT user and provide assistance when the CT user is in trouble with operation of the PC.

Live Help Client

This software is installed on the PC of a client user who needs help or on a server you wish to operate remotely. The CT user can be helped by remote operation of Live Help Expert when he/she does "not know how to respond to the message on the screen" or "not know how to operate the application".

Systemwalker Support Center

Systemwalker Support Center is a Fujitsu-managed system Support Center. This center distributes the "Software Dictionary" which defines inventory information collected from Systemwalker Desktop Patrol CT, provides relevant information and answers questions about Systemwalker Desktop Patrol.

Example of system configuration

When one CS is installed

For example, suppose that there are 3 sections in a certain company; a Systemwalker Desktop Patrol CS is installed to manage PCs of each section. The components of Systemwalker Desktop Patrol to be installed in the company are shown below:

- Systemwalker Desktop Patrol CS: 1 unit

- Systemwalker Desktop Patrol CT: Same as the number of PCs of each section

According to the above case, its configuration system view is shown as follows:
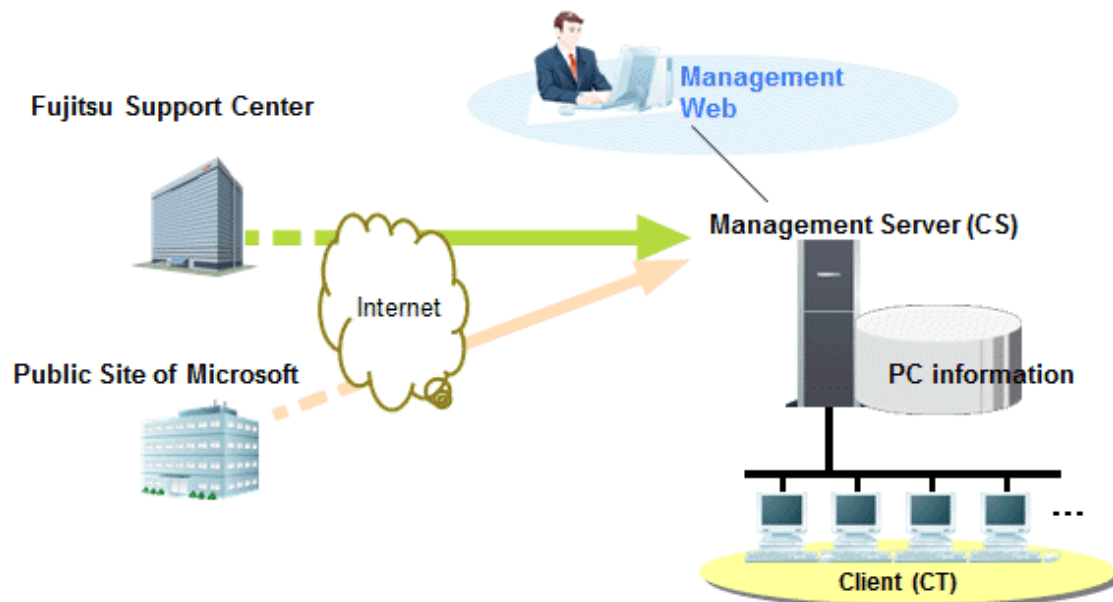
When DS are installed

For example, suppose that there are three sections in a certain company. It is required to install a DS in each section to share load due to the large capacity of distributed software. The components of Systemwalker Desktop Patrol to be installed in the company are shown as follows:

- Systemwalker Desktop Patrol CS: 1 unit

- Systemwalker Desktop Patrol DS: 3 units

- Systemwalker Desktop Patrol CT: Same as the number of PCs of each section

According to the above case, its configuration system view is shown as follows:
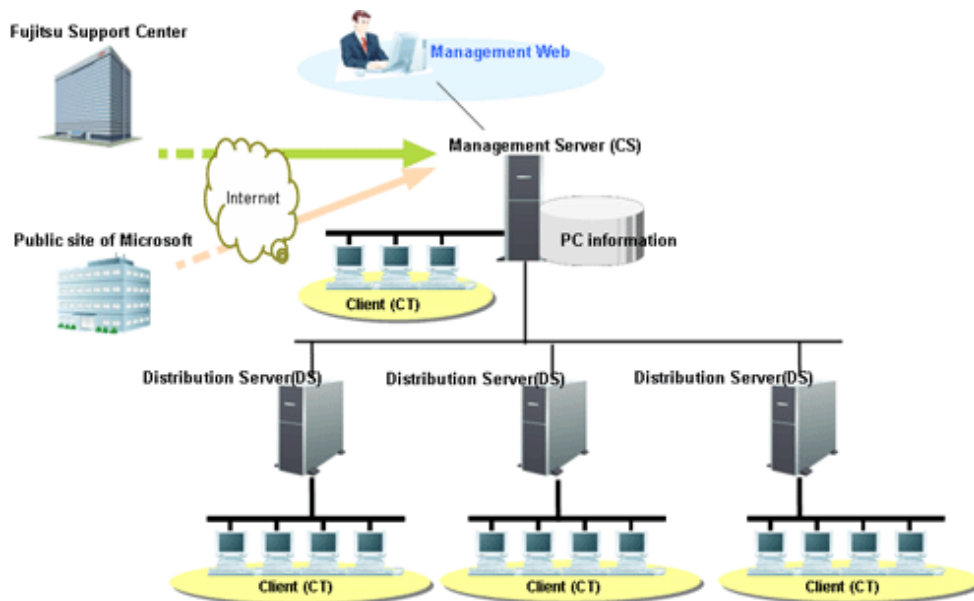
When ADT is installed

Suppose that a company has a section where devices other than PCs are installed, ADT can automatically detect the devices connecting to the network. Additionally, AC can be used to output reports. The components of Systemwalker Desktop Patrol to be installed in the company are shown below:

- Systemwalker Desktop Patrol CS: 1 unit

- Systemwalker Desktop Patrol DS: 2 units

- Systemwalker Desktop Patrol AC: 1 unit

- Systemwalker Desktop Patrol ADT:3 units

- Systemwalker Desktop Patrol CT: Same as the number of PCs of each section

According to the above case, its configuration system view is shown as follows:
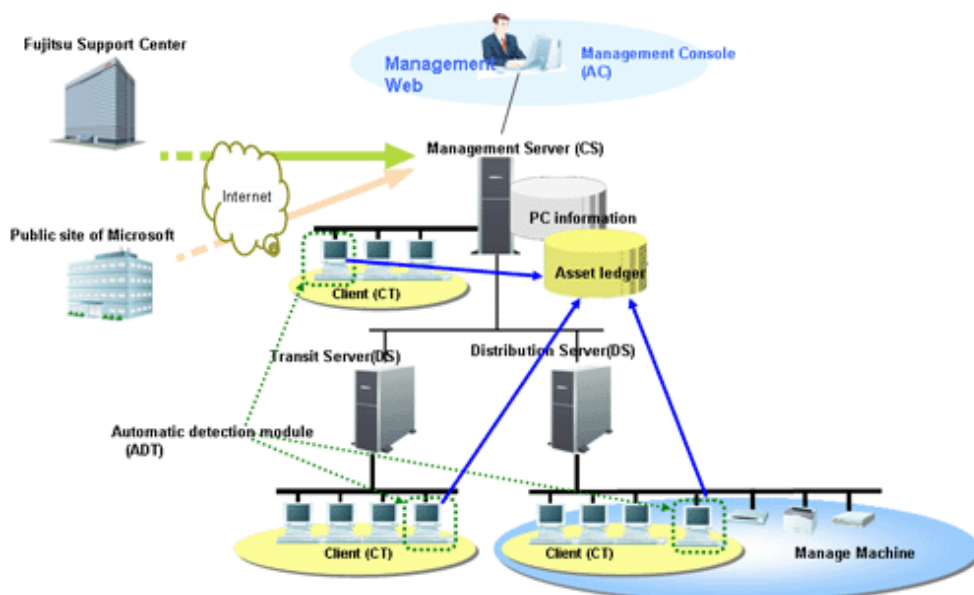
When SS is installed

Suppose that a company has a section where smart devices are used in the company's intranet. SS can collect and manage inventory information, not only for PCs but also for smart devices. The components of Systemwalker Desktop Patrol to be installed in the company are shown below:

- Systemwalker Desktop Patrol CS: 1 unit

- Systemwalker Desktop Patrol DS: 2 units

- Systemwalker Desktop Patrol SS: 1 unit

- Systemwalker Desktop Patrol CT: Same as the number of PCs of each section

- Smart device CT: Same as the number of smart devices

According to the above case, its configuration system view is shown as follows:
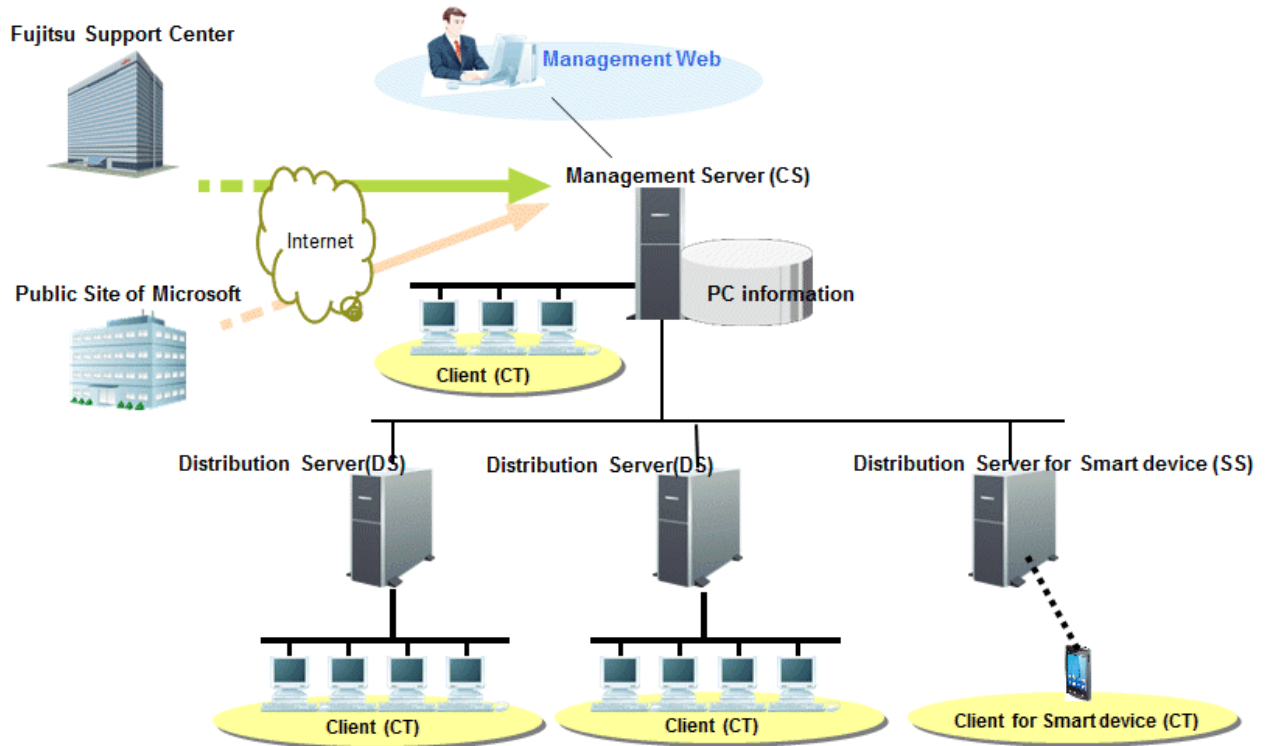
Note

If both Systemwalker Desktop Patrol and Systemwalker Desktop Keeper manage iOS, the Systemwalker Desktop Patrol SS and the Systemwalker Desktop Keeper Smart Device Relay Server must coexist.

1.2 Determine Administrator Configuration

This section describes the type and function of Systemwalker Desktop Patrol administrator.

Administrator is classified as the following two types.

System administrator

System administrator defined in this product refers to those who construct, operate and maintain the system installed with Systemwalker Desktop Patrol over the whole company.

System administrator can operate "Desktop Patrol Main Menu (browse and setup authority)".

Section administrator

Unlike system administrator, a section administrator only has an authority to access a specific section. A section administrator must be endowed with necessary authority and can not browse or operate the information of other sections that he/she is unauthorized to access.

The section management account can construct, operate and maintain the system installed with Systemwalker Desktop Patrol in his/her section by the section administrator account and operation authority.

The system administrator may have such a heavy burden if he/she controls the whole system.

Therefore, the system administrator can appoint section administrators and give them corresponding authority to manage the information of his/her section to reduce his or her own burden.

Section administrators can be appointed after the system installed with Systemwalker Desktop Patrol is put into application.

Section administrators can operate "Desktop Patrol Main Menu (browse and setup authority)".

Additionally, the "user" of this product is defined as follows:

User

Users are those who use the managed target PCs during assets management operation by means of Systemwalker Desktop Patrol. Usually, it is not necessary to pay attention to the operation. The user can operate "Desktop Patrol Main Menu (only browse the PC)" by the operation authority of user account to browse hardware, software or security information of the PC.

1.3 Determine How to Create Master Data

This section describes the structural information as managed object in Systemwalker Desktop Patrol.

Structural information has three types:

- User management information

- Section management information

- Building management information

The following three methods can be used to create structural information during first installation, decide which method shall be selected to create structural information during the design.

- Linking with Active Directory

- Importing from Systemwalker Desktop Keeper

- Registration in the main menu

1.3.1 Linking with Active Directory

The information can be imported in Systemwalker Desktop Patrol through linking with Active Directory server managing organizational structure, user information and computer information.

The structural information of Systemwalker Desktop Patrol is created automatically based on the organizational structure, user information and computer information of Active Directory, so the installation or alteration work of Systemwalker Desktop Patrol can be reduced thereof.

Additionally, Active Directory can collectively manage the organizational structure, user information and computer information, even though the system administrator of Systemwalker Desktop Patrol needs to make modifications in organization or personnel, he/she can only import the information from Active Directory without the need to recreate the structural information.

For details about linkage methods, refer to "Creation of Master Data" in *Systemwalker Desktop Patrol Operation Guide: for Administrators*.

1.3.2 Importing from Systemwalker Desktop Keeper

The structural information saved by Systemwalker Desktop Keeper shall be imported in Systemwalker Desktop Patrol in the form of CSV file.

Linkage with the structural information of Systemwalker Desktop Keeper can not be realized when Systemwalker Desktop Patrol links with Active Directory.

For details about linkable Systemwalker Desktop Keeper products, refer to "Relevant Softwares" in the *Systemwalker Desktop Patrol User's Guide*.

For details about linkage method, refer to "Create Master Data" in the *Systemwalker Desktop Patrol Operation Guide: for Administrators*.

1.3.3 Registration in main menu

Structural information can be recreated through registering "Section Management Information" and "User Management Information" in the main menu.

For details about registration method, refer to "Create Master Data" in the *Systemwalker Desktop Patrol Operation Guide: for Administrators*.

1.4 Determine How to Install Client (CT)

The following two methods can be used to install the client (CT) of Systemwalker Desktop Patrol.

- Single computer installation

- Installation by Kitting of CT.

Select an installation method according to the desired quantity of CTs.

Single computer installation

The user can use the setup boot disk of Systemwalker Desktop Patrol to install the CT in PCs one by one using one of the installation procedures below:

- Wizard installation

- Silent installation

- Installation in an Active Directory environment
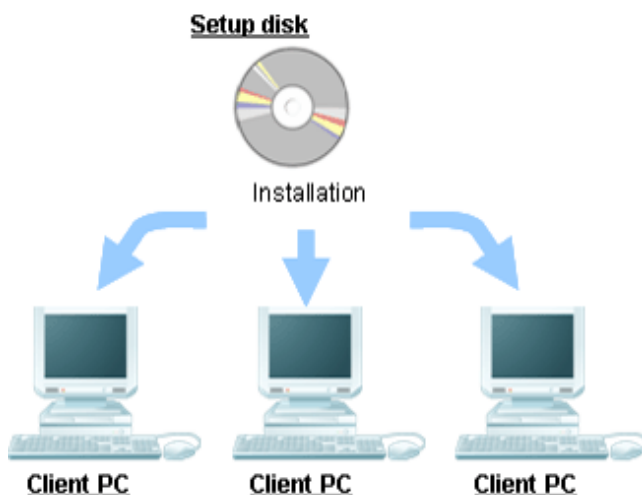
Installation by Kitting of CT

Install the client (CT) in the host PC and create a main mapping and distribute the main mapping to all PCs to be installed with a CT of Systemwalker Desktop Patrol.
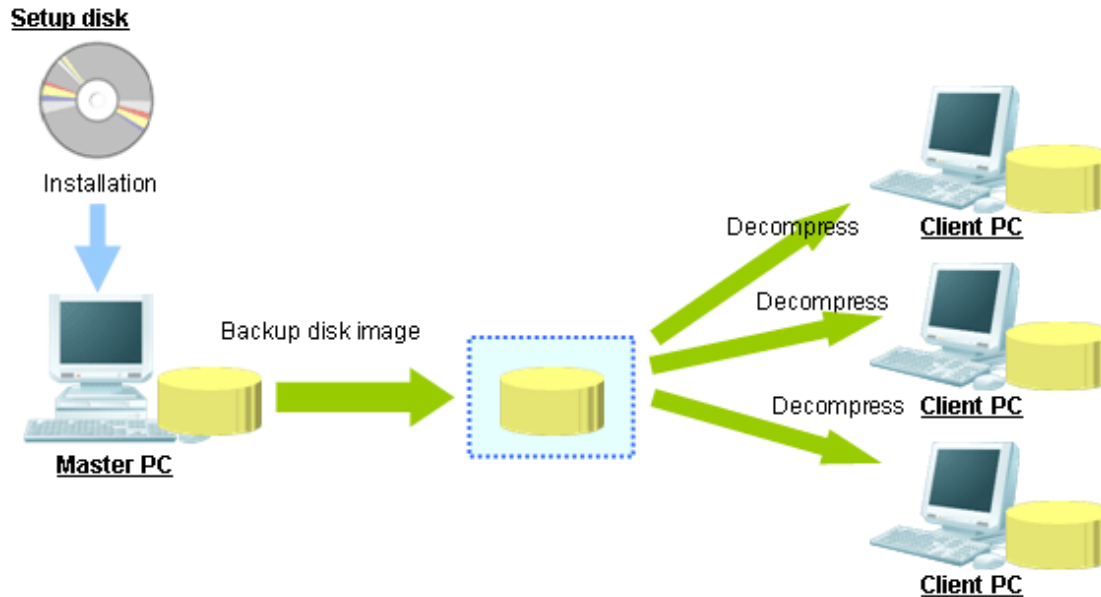
1.5 Port Number Confirmation

Confirm whether the port number used in Systemwalker Desktop Patrol is problematic or usable or not at the design stage.

Refer to "Port Number and Service" in the *Systemwalker Desktop Patrol Reference Manual* to confirm the port number used in Systemwalker Desktop Patrol.

Modify the port number if the port number used in Systemwalker Desktop Patrol has been used in the system.

Considerations for AC and SS construction

The port number between CS and AC, and between CS and SS, is 10104 during operation.

Therefore, if other applications use the port number 10104, corresponding applications have to be closed, or the port number for Systemwalker standard database has to be modified before constructing the environment in the **Operation Environment Maintenance Guide** window to prevent repeated use of port number.

The same port number shall be set in CS and AC, and between CS and SS. If the port number in AC and SS is modified, ensure the port number in CS has been modified.

For the method to modify the port number of CS, AC, and SS, refer to "Modify Method of Applied Port Number" in the *Systemwalker Desktop Patrol Reference Manual*.

If the environment has been constructed in the CS, "Expand Applied Environment" through the "Operation Environment Maintenance Guide" after changing the port number. It is not necessary to make special modifications in the setting value in the **Expand Applied Environment** window.

When starting up the **Managed Ledger Setting** window after changing the port number in AC, the "Connection Fails" message will be displayed. Confirm the **Connected Target Server Name** and click the **OK** button.

In the SS, change the port number, and restart the Systemwalker Desktop Patrol SS services.

Chapter 2 Installation

This chapter describes how to install Systemwalker Desktop Patrol.

2.1 Procedures for Installation

The procedures for installing Systemwalker Desktop Patrol are as follows.

For the procedures marked "Option", refer to "1.1 Determine System Configuration" for installation.

1. Advance preparation (Optional)

2. Construct Systemwalker Desktop Patrol CS (Required)

3. Install Systemwalker Desktop Patrol DS (Optional)

4. Install Systemwalker Desktop Patrol AC (Optional)

5. Install Systemwalker Desktop Patrol ADT (Optional)

6. Install Systemwalker Desktop Patrol CT (Required)

7. Install Systemwalker Desktop Patrol SS and smart device CT (Optional)

8. Settings for remote operation (Optional)

2.1.1 Notes during Installation

This section describes the notes during installation.

Notes on the network environment

- About firewall function settings

  If firewall is enabled in an environment on which CS, DS, and SS are installed, exceptional programs need be set to allow the connections from DS, SS, AC, ADT and CT respectively.

  For details of how to set, refer to "Port Number List" of *Systemwalker Desktop Patrol Reference Manual*.

- In PC with dual network card, if automatically getting IP address as PC name when installing CT has been set, which IP address to get cannot be specified.

About DTP installation directory of 64-bit OS

Take the example of 32-bit OS default "C:\Program Files" to record DTP installation directory.

If installing the following on a 64-bit operating system, view after converting to "C:\Program Files (x86)" by default.

- 32-bit version CS

- DS, CT, SS and ADT

About User ID and PC Name in the Environment Setup

In the same system, "User ID+PC Name" should be unique.

Setting real-time scan of anti-virus software

Set the following folders as non-targets for the real-time scan of anti-virus software.

- Systemwalker Desktop Patrol installation directory

- *iisInstallDirOnCs*\Scripts\DTP

- *iisInstallDirOnCs*\Scripts\DTPA

- *iisInstallDirOnCs*\wwwroot\DTP

- Software distribution storage directory on the CS/DS

2.2 Advance Preparation

2.2.1 Advance Preparation for Managing iOS Devices

To manage iOS devices, Systemwalker Desktop Patrol uses the Apple Push Notification Service provided by Apple. For this reason, the MDM certificate issued by Apple must be obtained by following the steps shown below. The MDM certificate must be set to Systemwalker Desktop Patrol SS during its installation.

Note

Execute the following steps on a Mac OS.

1. Register in the iOS Developer Enterprise Program

   Access the following URL (as of February, 2015), and register in the "iOS Developer Enterprise Program".

   https://developer.apple.com/jp/programs/ios/enterprise/

2. Obtain the signing certificate (MDM Signing Certificate)

   Contact Apple via phone or email, and request an MDM vendor registration. Once Apple is informed that you want to be registered as an MDM vendor, they will start the registration process.

   Follow Apple's instructions to create a signing certificate. The private key created in this step will later be required in the step 3.

3. Export the private key

   Export the private key used to create the signing certificate in PKCS#12 format. It can be exported using Keychain Access. The passphrase specified in this step will also be required in step 6.

4. Obtaining the Apple Inc. intermediate certificate

   Obtain the intermediate certificate (Worldwide Developer Relations) from the following URL (as of February, 2015):

   http://www.apple.com/certificateauthority/

5. Obtain the Apple Inc. Root Certificate

   Obtain the root certificate (Apple Inc. Root Certificate) from the following URL (as of February, 2015):

   http://www.apple.com/certificateauthority/

6. Create the MDM certificate request file

   Using the certificate and private key obtained in steps 2 to 5, create the MDM certificate private key and MDM certificate request file.

   These can be created automatically by executing the sign_csr.sh (creating MDM certificate request file) script stored in the Systemwalker Desktop Patrol DVD-ROM. Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on how to use this script.

   This script is stored in:

   systemwalkerDesktopPatrolDvdRomDrive:\utilities\tool\iOS\sign_csr.sh

7. Create the MDM certificate

   Obtain the MDM certificate from the Apple Inc. website (as of February, 2015). By uploading the request file created in step 6, the MDM certificated will become available for download.

   https://identity.apple.com/pushcert/

8. Convert the certificate format

   Convert the format of the downloaded MDM certificate.

   Open **Terminal**, and execute the command shown below. The MDM certificate will be converted into PKCS#12 format. The converted file must be set for the SS.

   ```
   openssl pkcs12 -export -in mdmCertificate -inkey mdmCertificatePrivateKey -out outFile
   ```

   For *mdmCertificate*, specify the downloaded MDM certificate (required).

   For *mdmCertificatePrivateKey*, specify the private key output in step 6 (required).

   For *outFile*, specify the file name of the converted certificate, with the p12 extension (required).

2.2.2 Preparation on the PC in Which the Web Browser will be Used

📌 Note
. . . .
For Windows(R) 8, start Internet Explorer from desktop.
. . . .

Settings for Internet Explorer

On PCs where the main menu or download menu is used, set the security level settings of Internet Explorer as required.

If the security level set for the zones to which the web browser site (URL) belongs is higher than the level indicated below, it may not behave properly.

- Security level - **Medium**

If the browser does not work properly because of the reason described above, you must either have the web browser site (URL) belong to a zone whose security level is the same as or less than the level mentioned above, or lower the security level of the zone to which the web browser site (URL) currently belongs.

Normally, the security level is set **Medium-low** for the **Intranet** zone, and **Medium** for the **Trusted sites** zone as default, and therefore, registering the web console site (URL) in **Sites** in either zone is recommended.

Note that, when the web browser is displayed, the zone to which that browser currently belongs (**Intranet**, **Internet**, for example) is displayed in the right-bottom.

For Internet Explorer 7.0 and Internet Explorer 8.0, if **Intranet settings are now turned off by default** is output to the information bar, turn on the intranet settings.

The browser may not work properly during DTP version upgrade even if the above settings are completed. If this happens, delete the Internet Explorer Internet temporary files, and re-execute it.

If using the web browser on Windows Server(R) 2008, or Windows Server(R) 2012

If using a web browser on Windows Server(R) 2008, or Windows Server(R) 2012, register "about:blank" in the **Trusted sites** zone, or configure the following settings.

- For Windows Server(R) 2008

   Follow the steps below:

   1. Click **Administrative Tools** > **Server Manager**.

2. Click **Server Summary** > **Security Information**, and click **Configure IE ESC**.
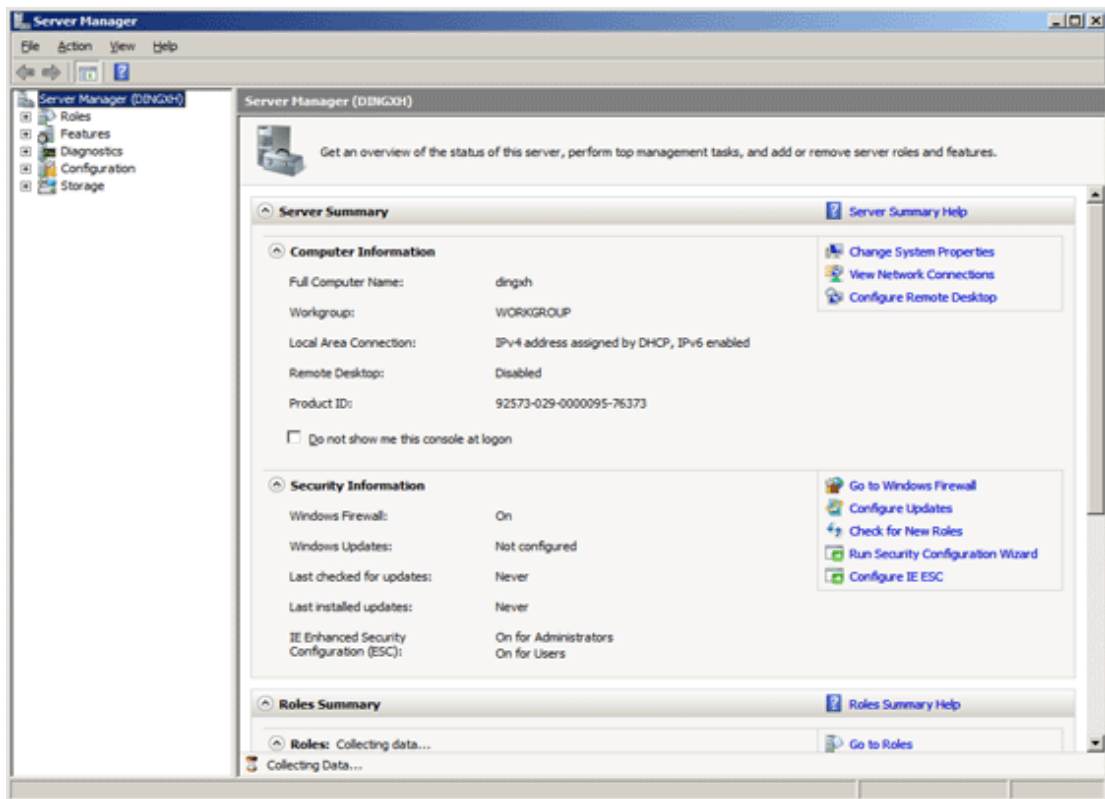
3. The window below will be displayed.
   Select **Off** for both **Administrators** and **Users**, and click **OK**.
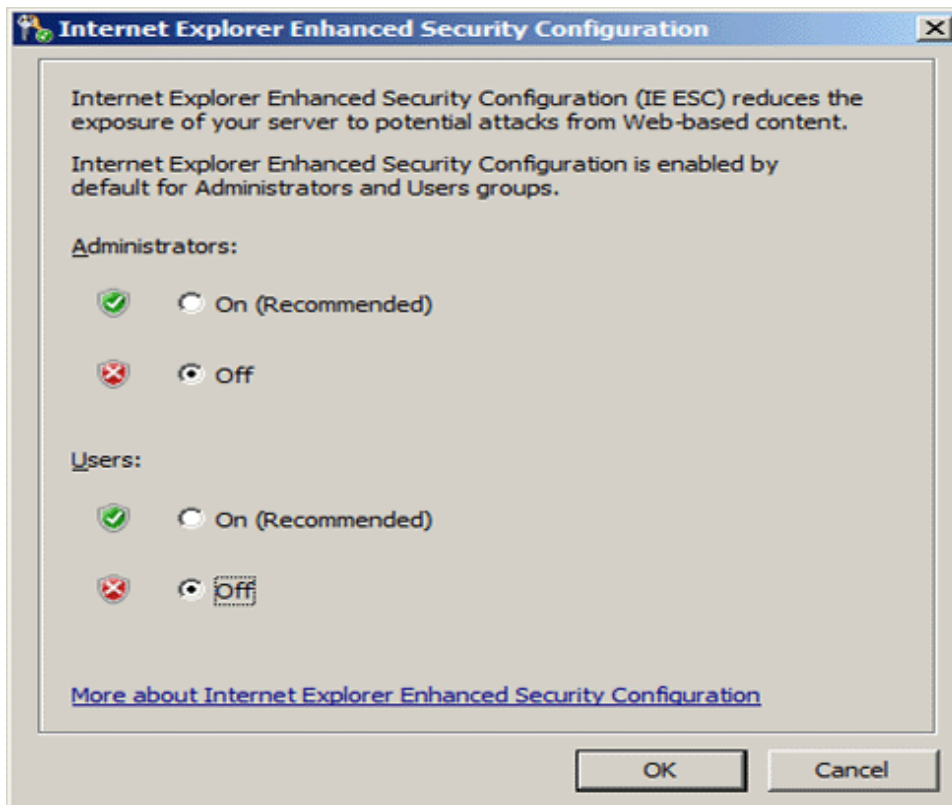
- For Windows Server(R) 2012

  Follow the steps below:

  1. Click **Server Manager**.

  2. Click **Local Server**.
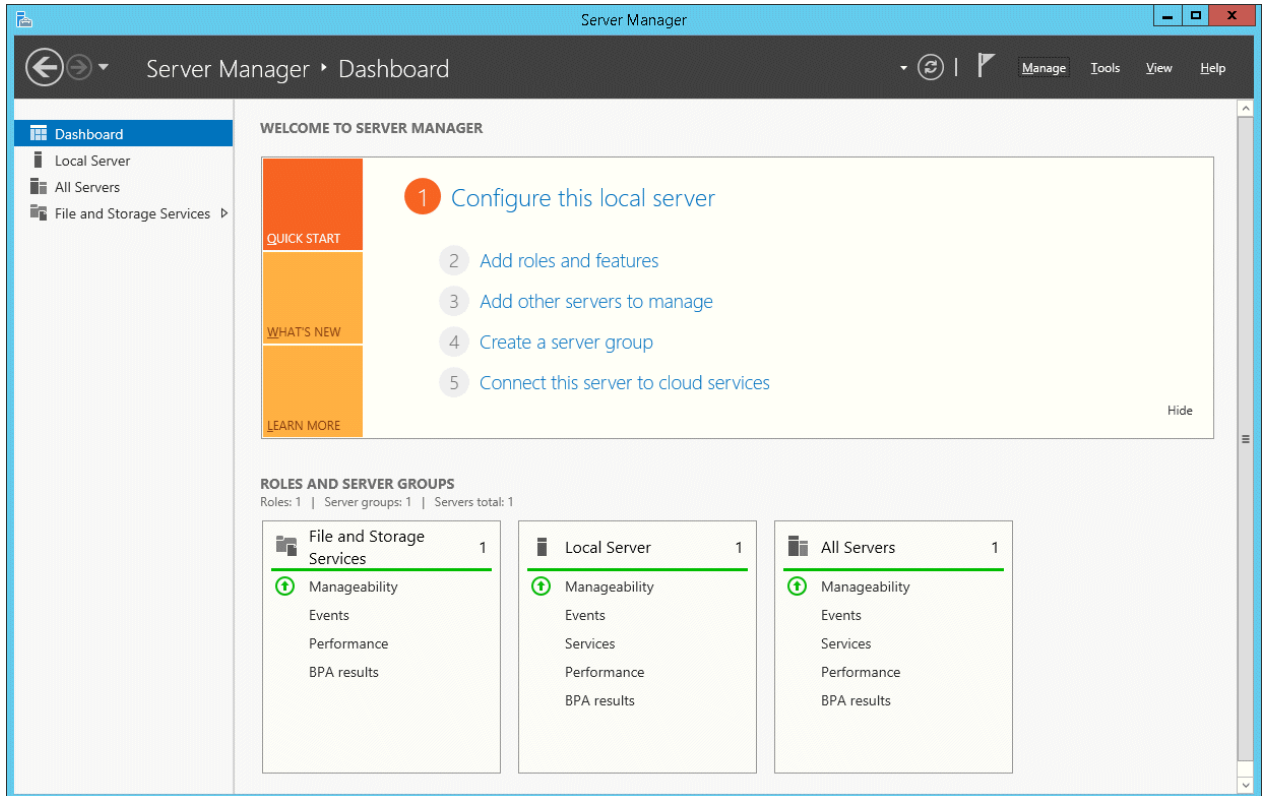
3. In **Properties**, click **On** for **IE Enhanced Security Configuration**.
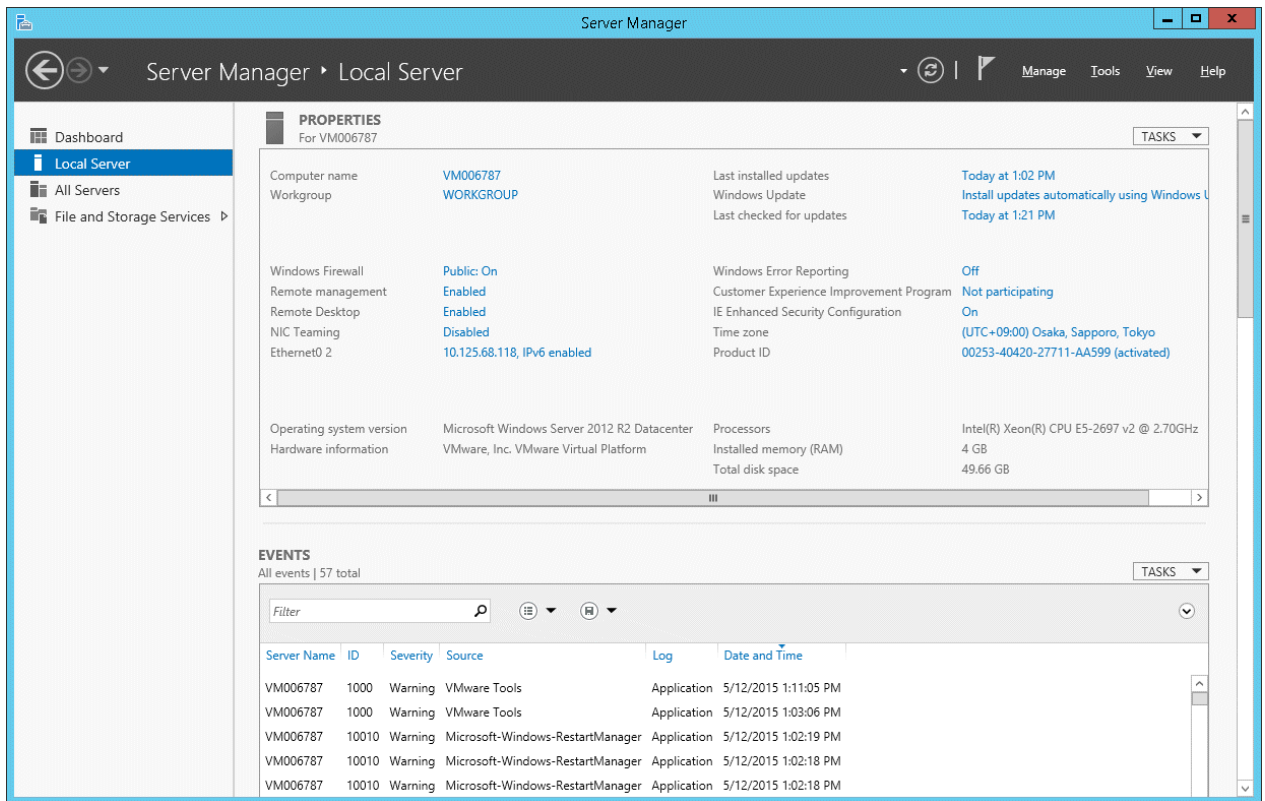
4. As is the case on Windows Server(R) 2008, the **Internet Explorer Enhanced Security Configuration** window will be displayed.
Select **Off** for both **Administrators** and **Users**, and click **OK**.

Settings for linking with Systemwalker Desktop Keeper

To link with Systemwalker Desktop Keeper, and use Internet Explorer 8.0 or higher, configure the following settings.

1. On Internet Explorer, select **Tools** > **Internet options**, and select the **Security** tab.

2. Select the zone to which the Systemwalker Desktop Patrol and Systemwalker Desktop Keeper sites (URL) belong, and click **Custom level** to open the **Security Settings** window.

3. In **Settings**, select **Miscellaneous** > **Navigate windows and frames across different domains** > **Enable**.

4. In the **Security Settings** window, click **OK**.

5. In the **Security** tab, click **Apply** or **OK**.

2.3 Construct CS

In Systemwalker Desktop Patrol, Systemwalker Desktop Patrol CS is constructed as the server performing PC information collection, management or software distribution processing.

2.3.1 IIS Installation and Settings

Systemwalker Desktop Patrol manages by using Web browser.

Procedures for installing ISAPI extension when newly installing IIS

1. Select **Administrative Tools** > **Server Manager** from **Control Panel**.

2. The **Server Manager** window is displayed, click **Add Roles**.
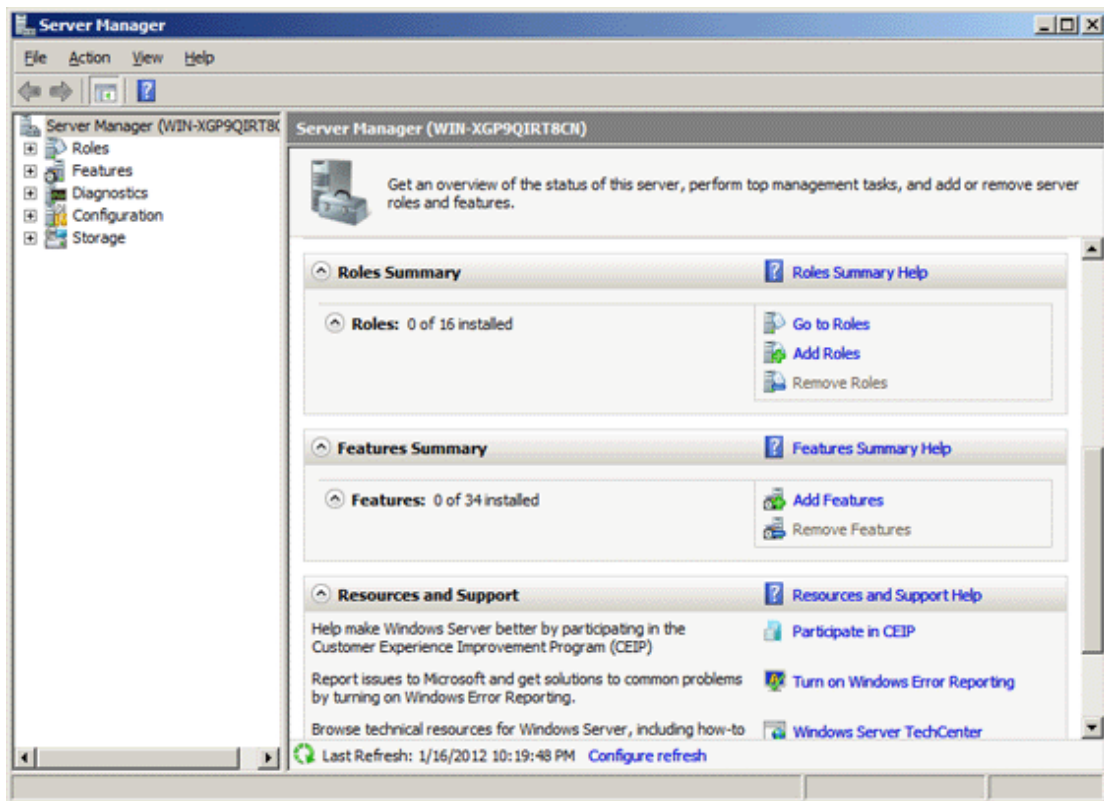
3. The **Before You Begin** window of **Add Roles Wizard** is displayed, click the **Next** button.
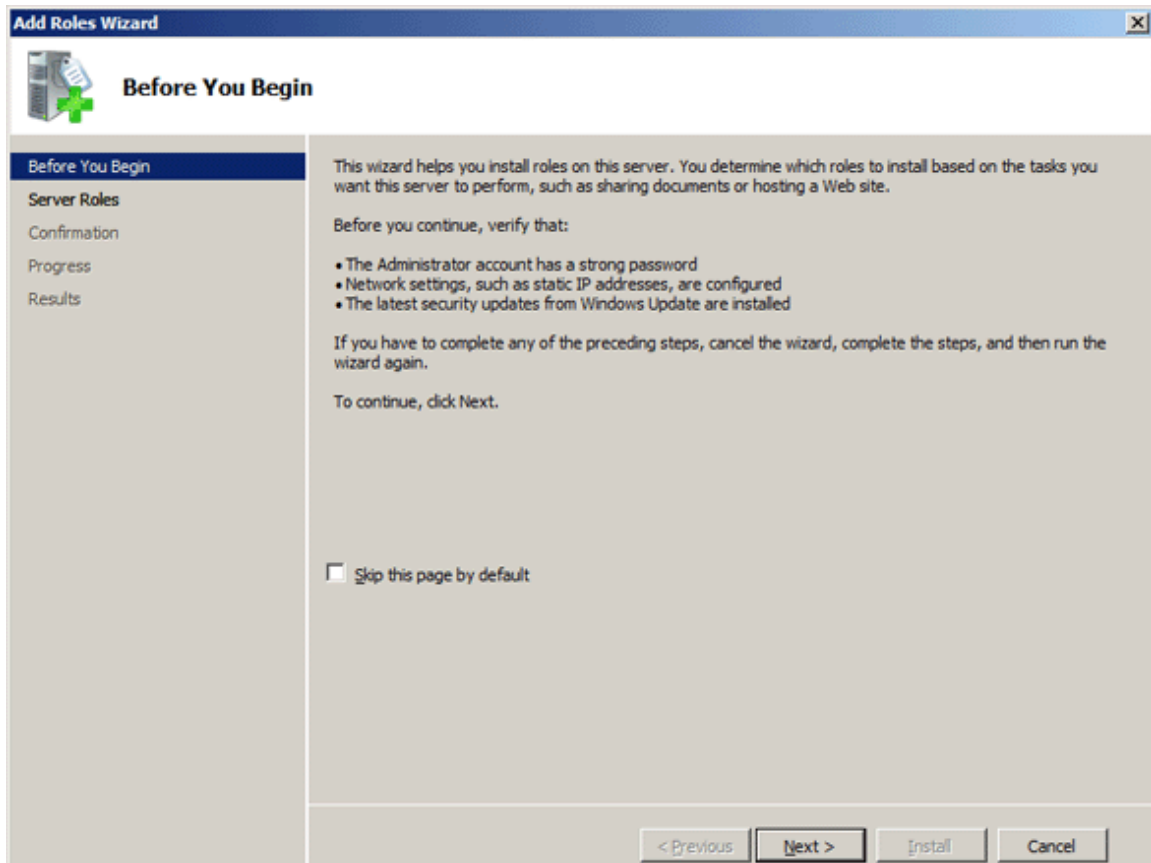
4. The **Select Server Roles** window of **Add Roles Wizard** is displayed, select **Web Server (IIS)** and click the **Next** button.
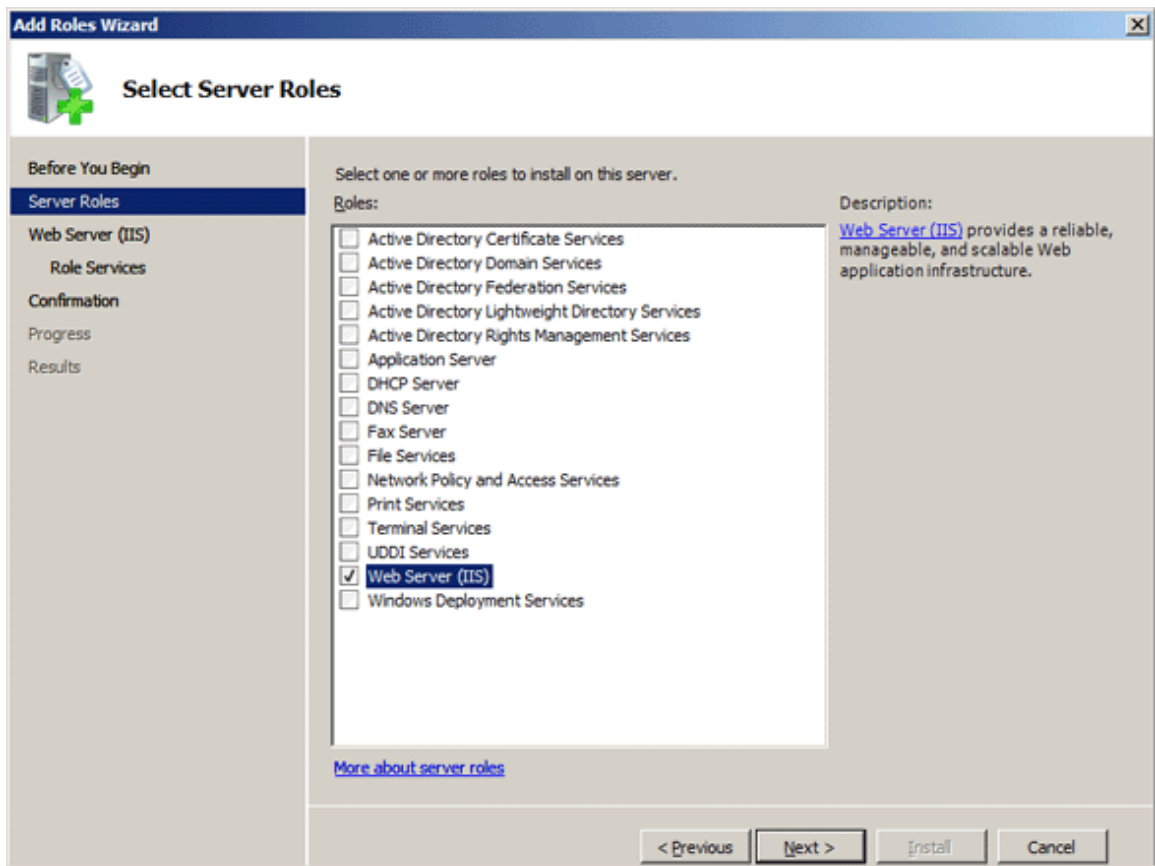
5. The **Web Server (IIS)** window of **Add Roles Wizard** is displayed, click the **Next** button.
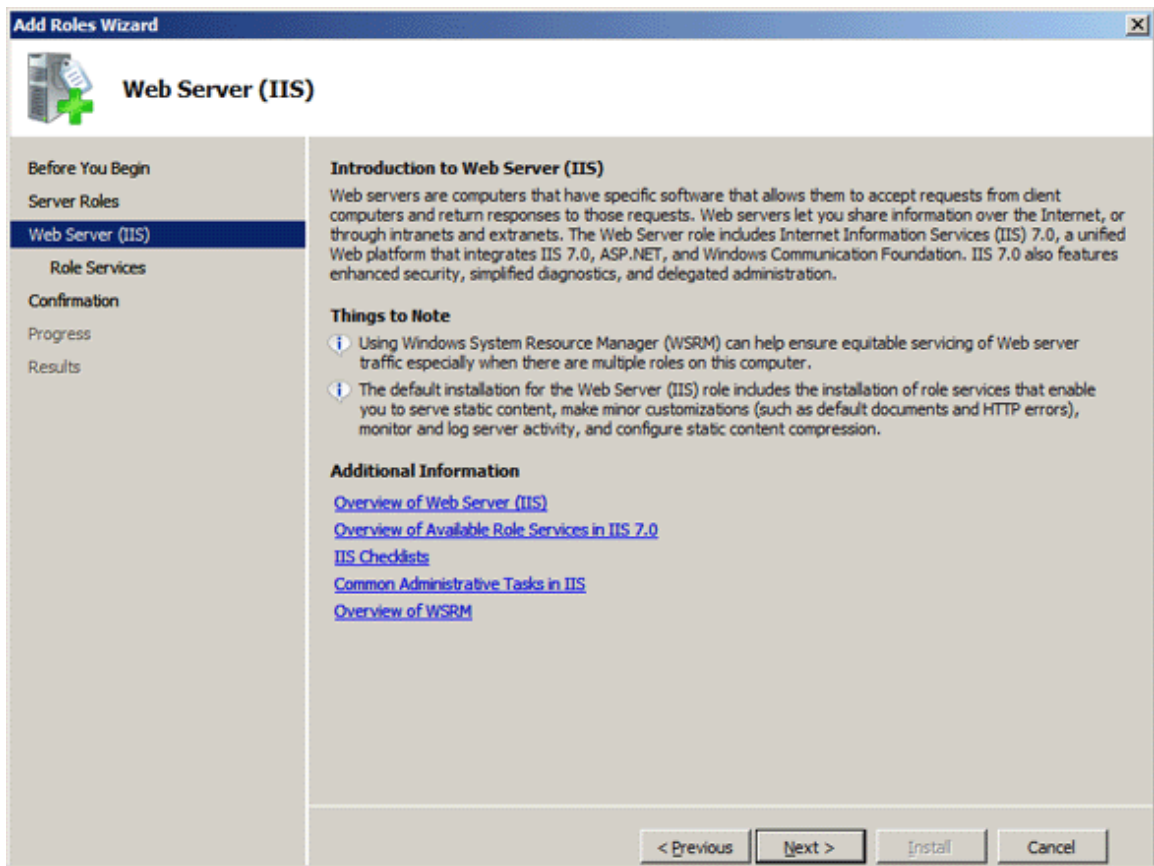
6. The **Select Role Services** window of **Add Roles Wizard** is displayed, select the following items and click the **Next** button.

    -   **Application Development** > **ISAPI Extensions**

    -   **Management Tools** > **IIS 6 Management Compatibility**

    Besides, if the following items have not been selected, select them.

    -   **Common HTTP Features** > **Static Content**

    -   **Common HTTP Features** > **Default Document**

    -   **Common HTTP Features** > **Directory Browsing**

- **Common HTTP Features** > **HTTP Errors**

7. The **Confirm Installation Selections** window of **Add Roles Wizard** is displayed. Click **Install**.
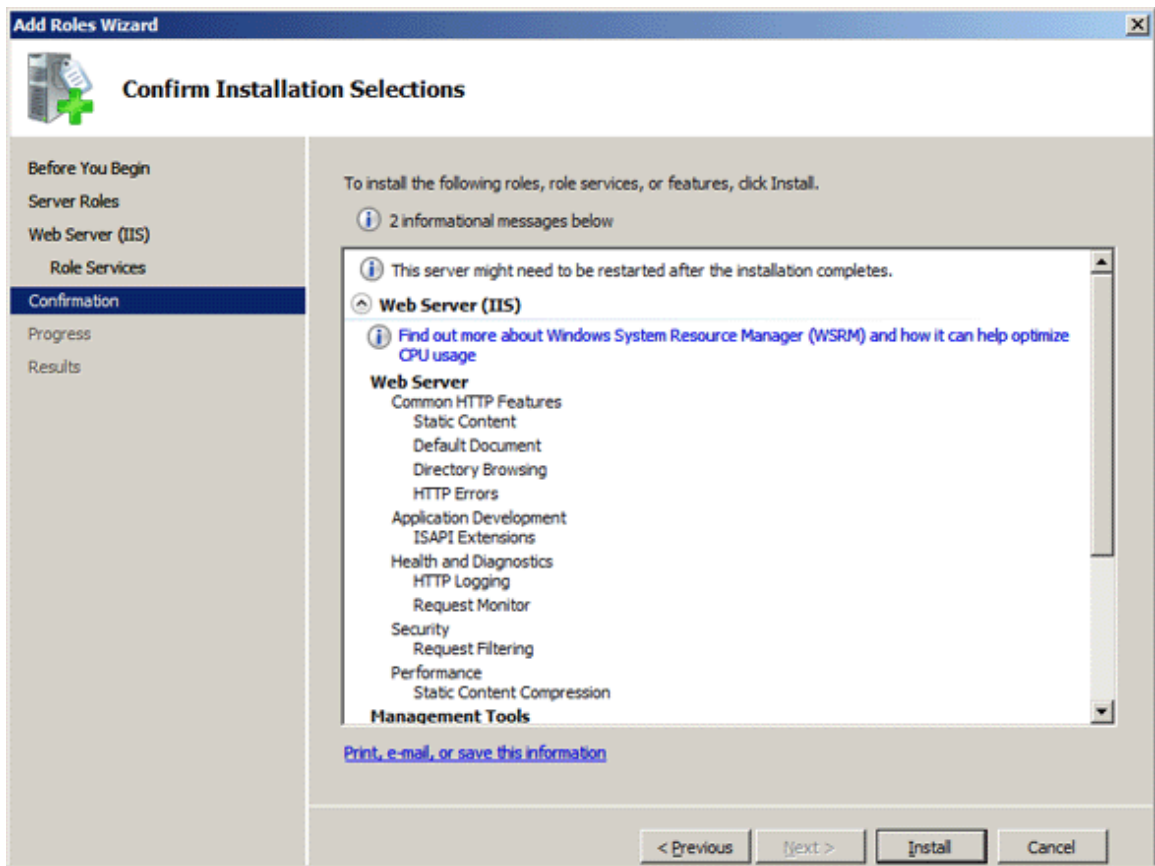
8. After installation has completed, click **Close**.

Procedure of installing ISAPI extension when IIS has been installed

1. Select **Administrative Tools** > **Server Manager** from **Control Panel**.

2. The **Server Manager** window is displayed, select **Roles** > **Web Server (IIS)** in the tree view.
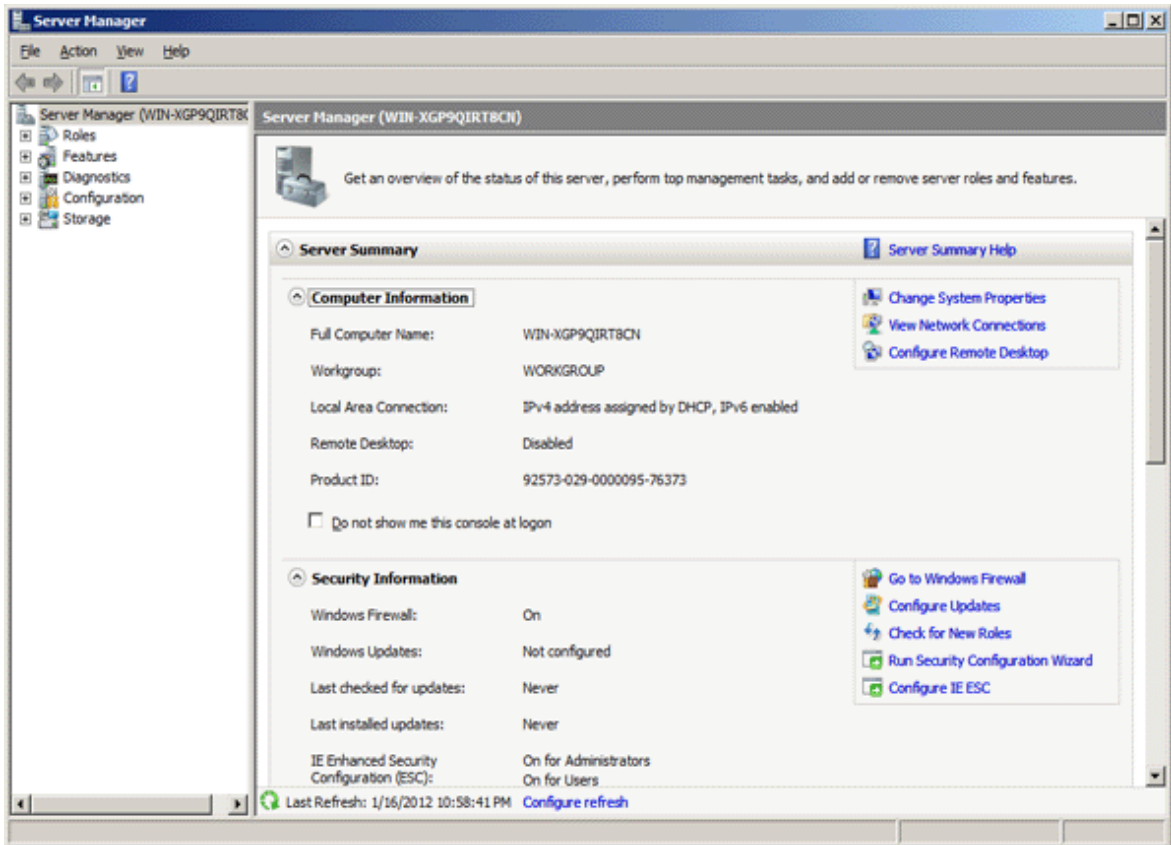
3. The **Web Server (IIS)** window is displayed. Click **Add Role Services**.
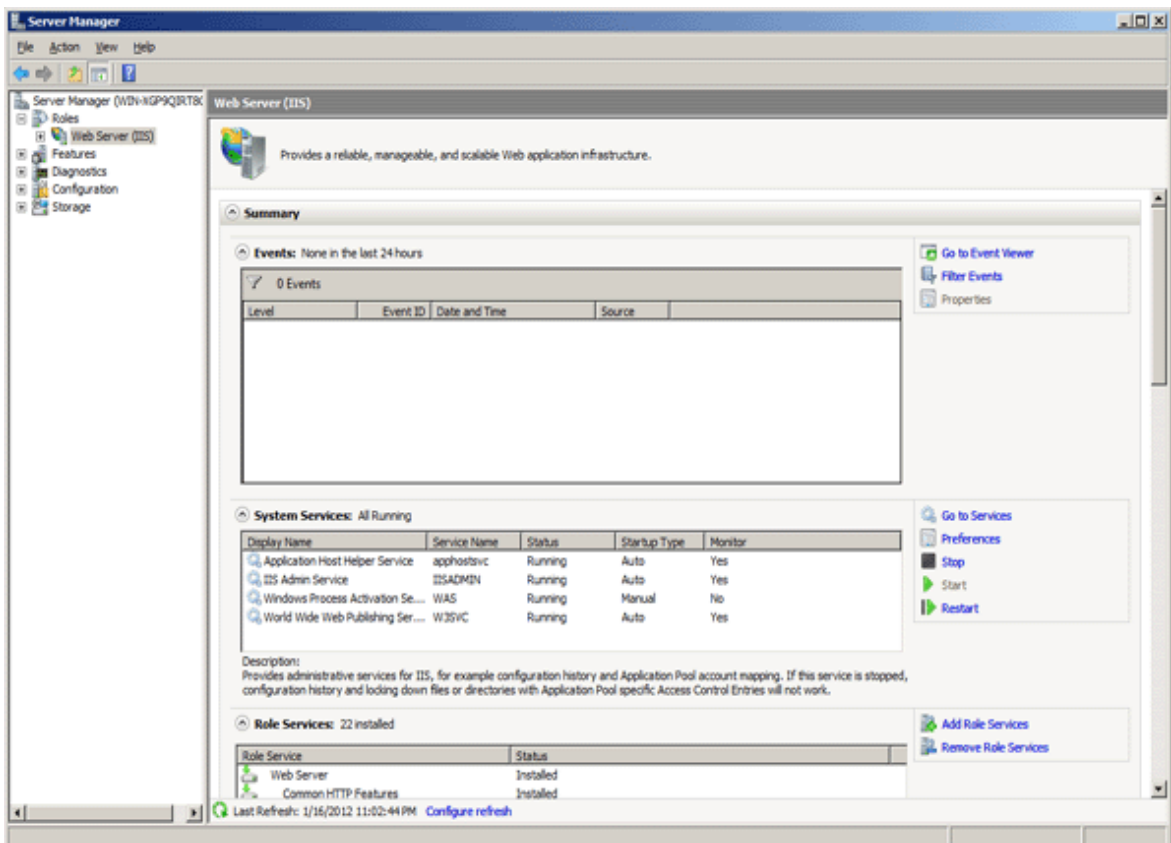
4. The **Select Role Services** window of **Add Role Service** is displayed, select when the following items have not been selected and click the **Next** button.

- **Application Development** > **ISAPI Extensions**.

- **Management Tools** > **IIS6 Management Compatibility**

Besides, if the following items have not been selected, select them.

- **Common HTTP Features** > **Static Content**

- **Common HTTP Features** > **Default Document**

- **Common HTTP Features > Directory Browsing**

- **Common HTTP Features > HTTP Errors**
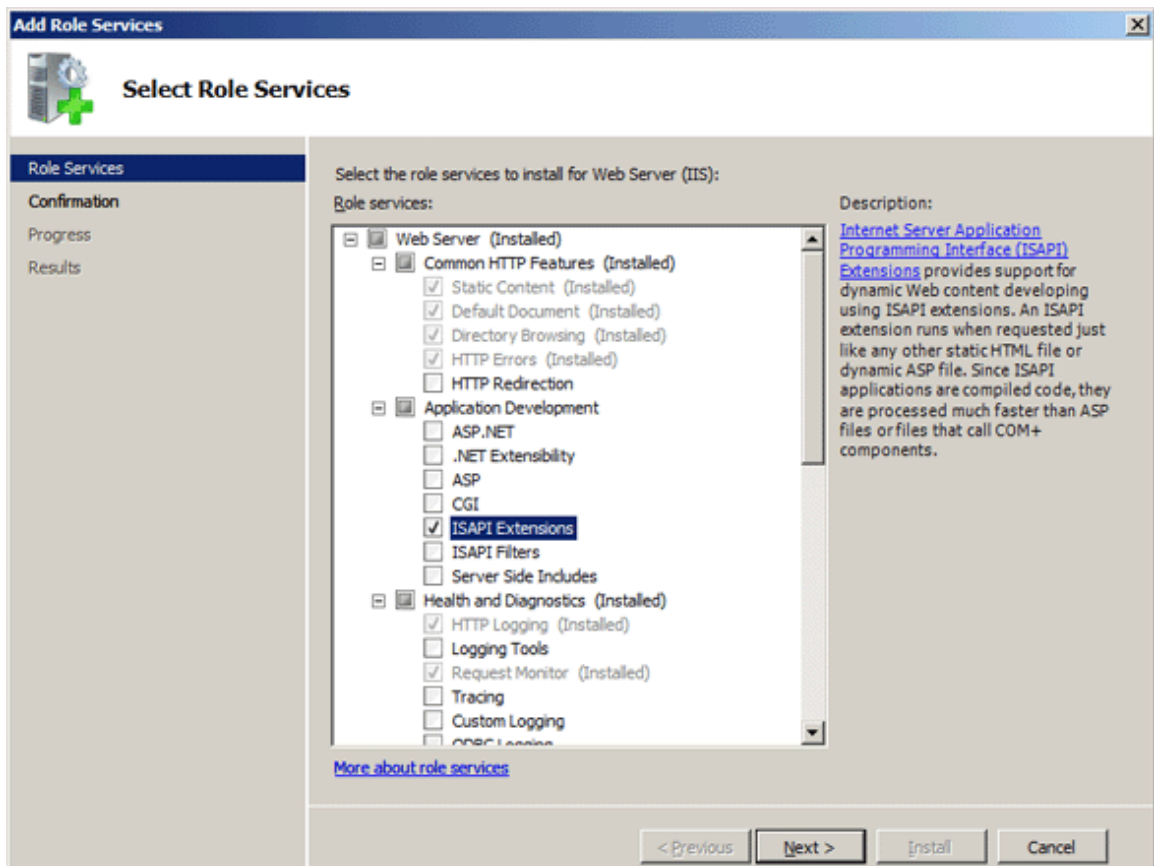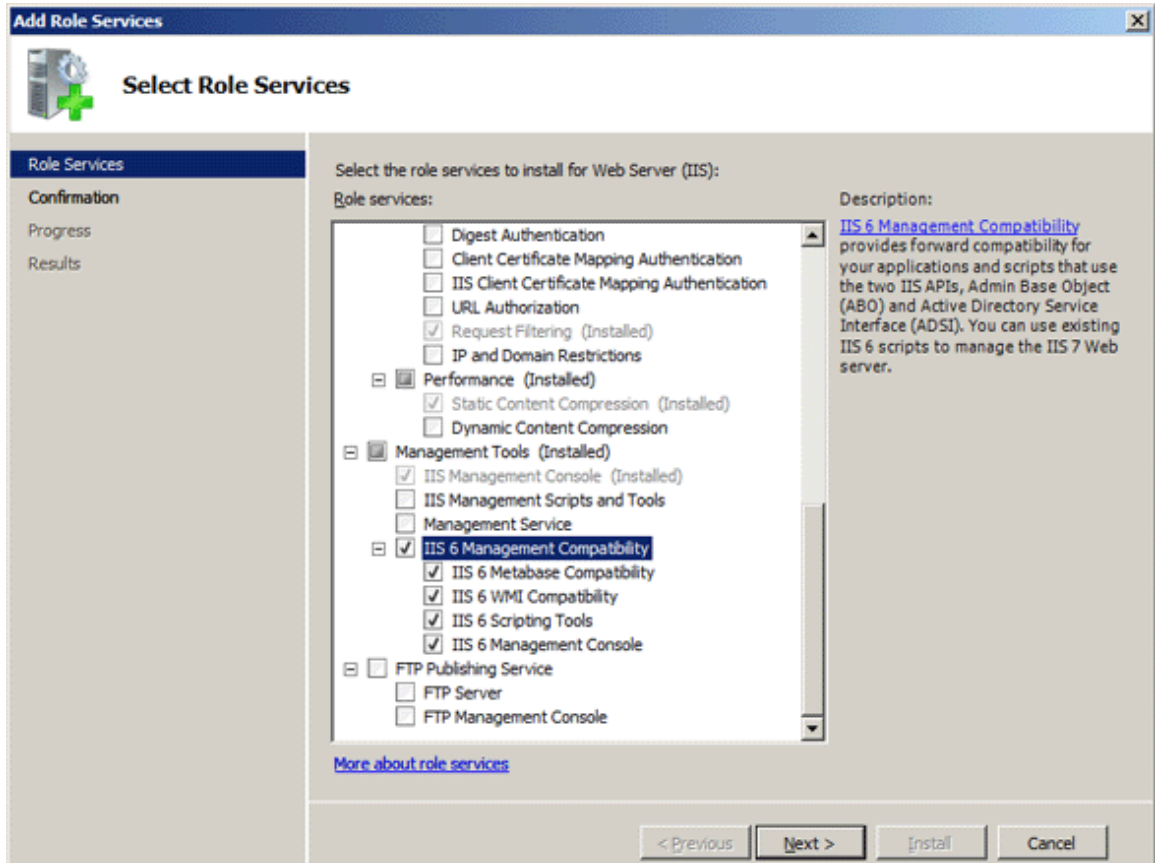
5. The **Confirm Installation Selections** window is displayed. Click **Install**.
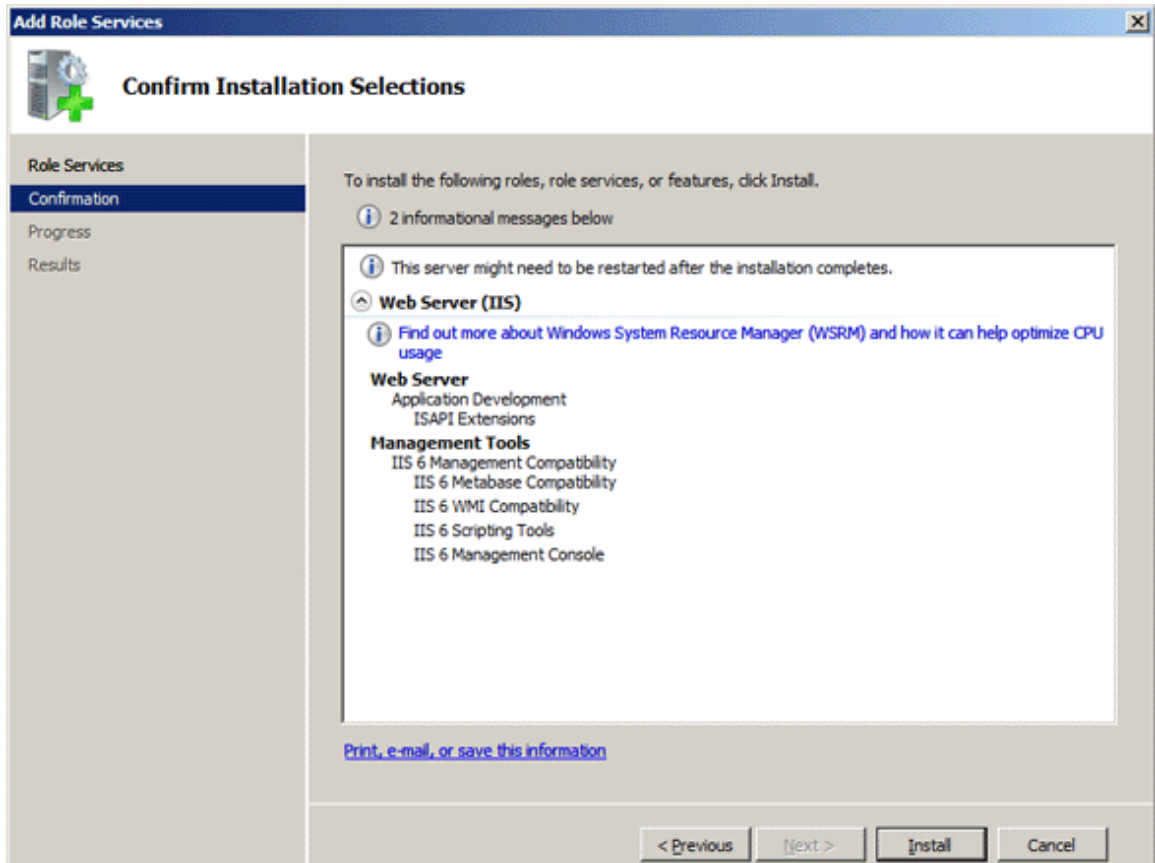
6. After the installation has completed, click **Close**.

Installation procedure for the ISAPI extensions when IIS is installed for the first time

1. When Windows Server(R) 2012 starts, it automatically starts **Server Manager**.
   If this does not happen, click the **Server Manager** icon at the bottom left of the window to start it.

   The **Server Manager** window will be displayed. In the **Manage** menu at the top-right of the window, click **Add Roles and Features**.
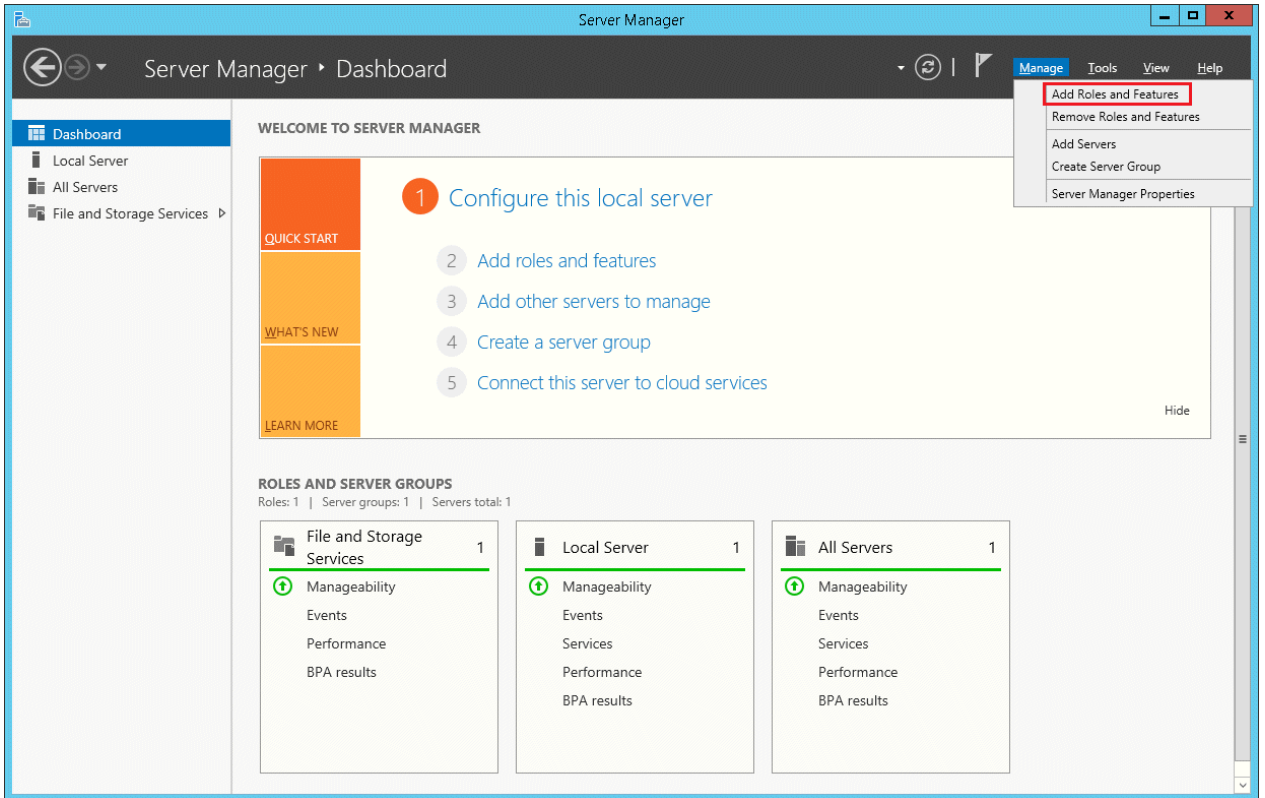
2. The **Add Roles and Features Wizard** will be displayed. In **Installation Type**, select **Role-based or feature-based installation**, and click **Next**.
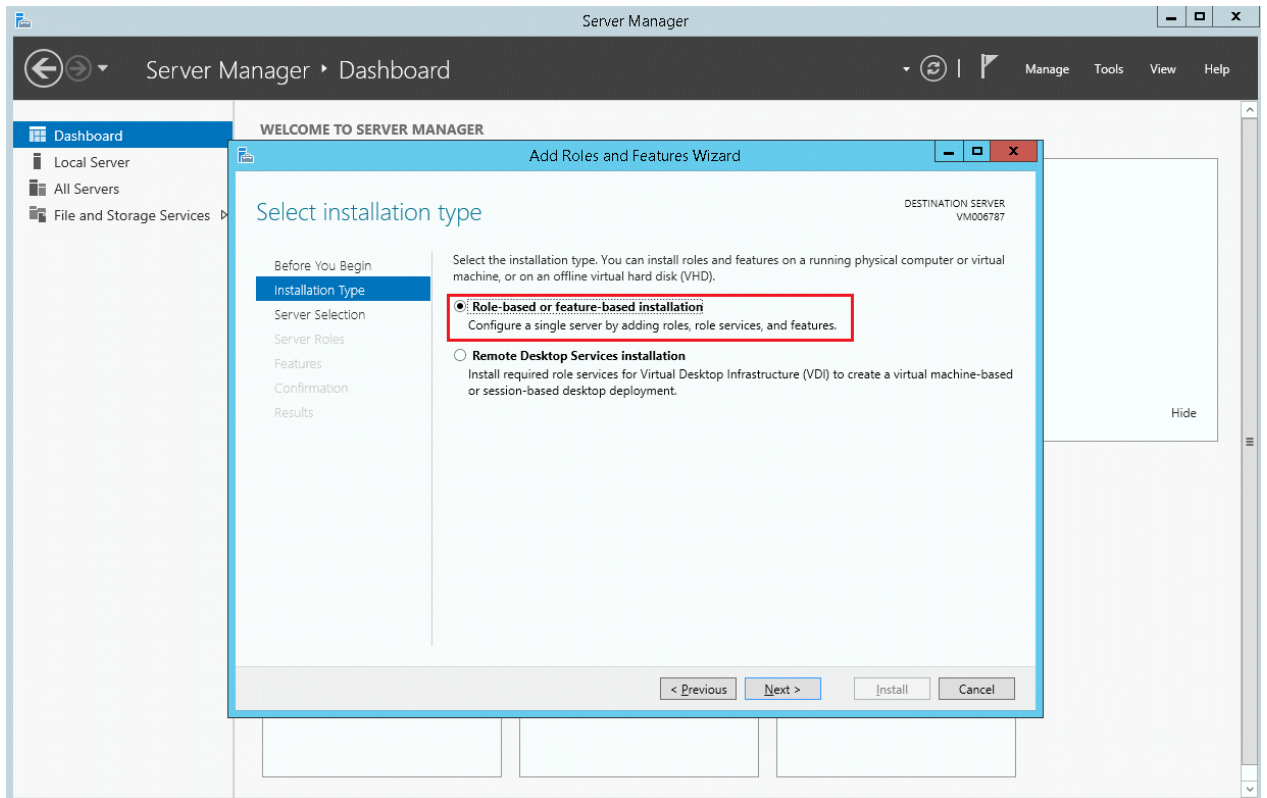
3. In **Server Selection**, select **Select a server from the server pool**. Select the server to be installed from **Server Pool**, and click **Next**.
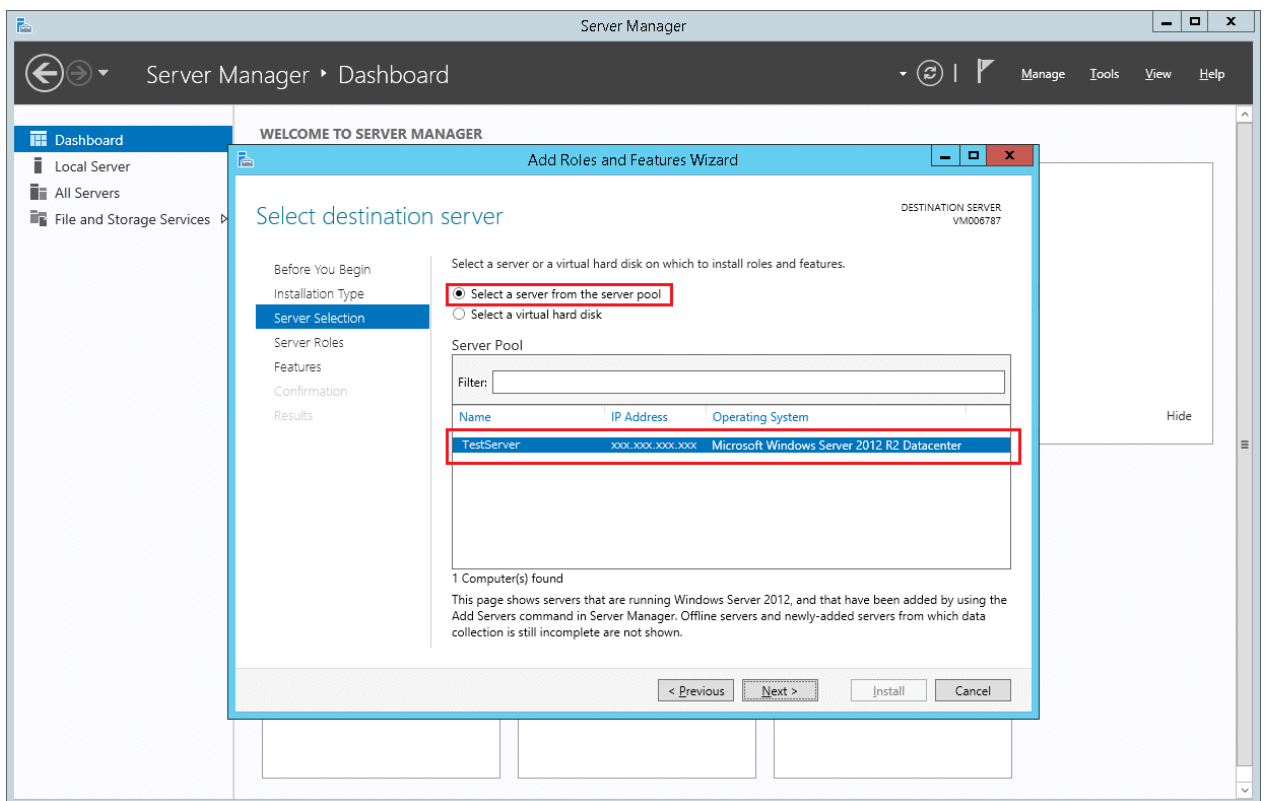
4. In **Server Roles** > **Roles,** ensure that **Web Server (IIS)** is selected.
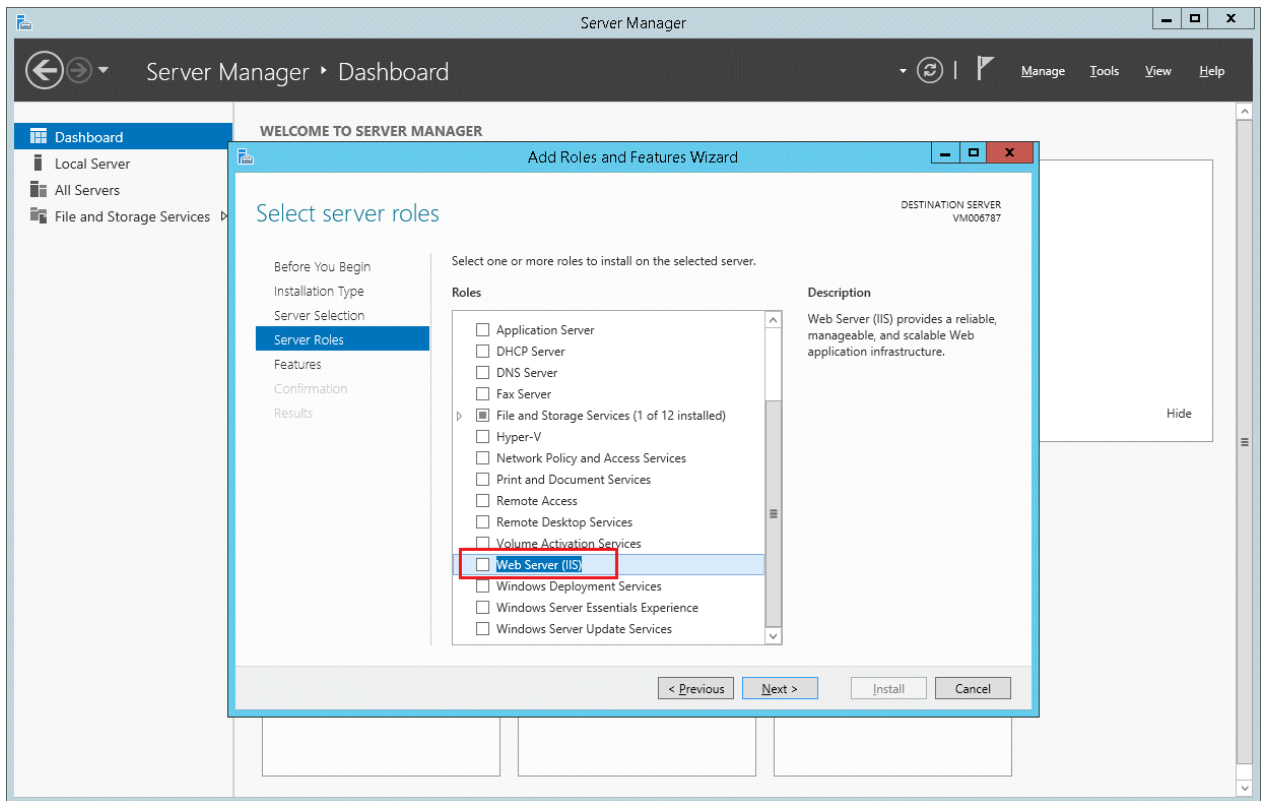
5. A confirmation window will be displayed. Click **Add Features**.
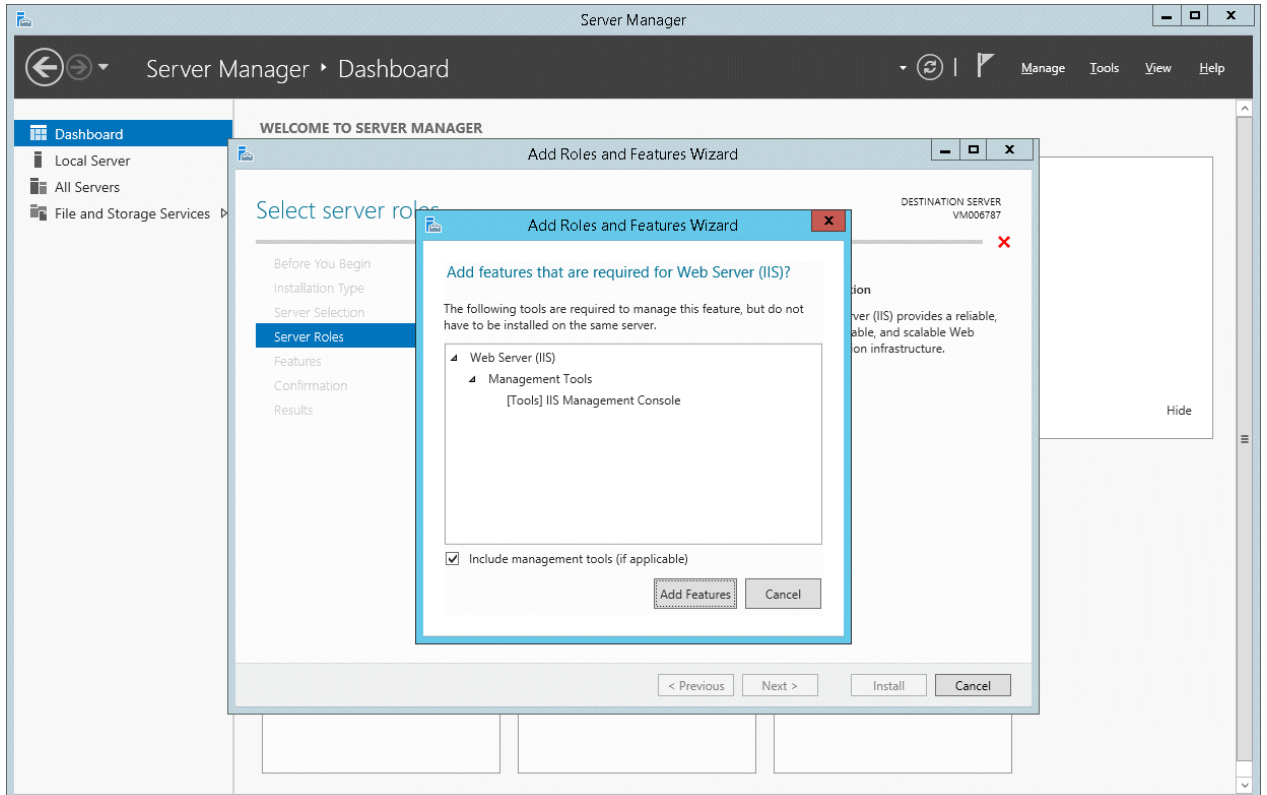
6. In **Select server roles**, click **Next**.
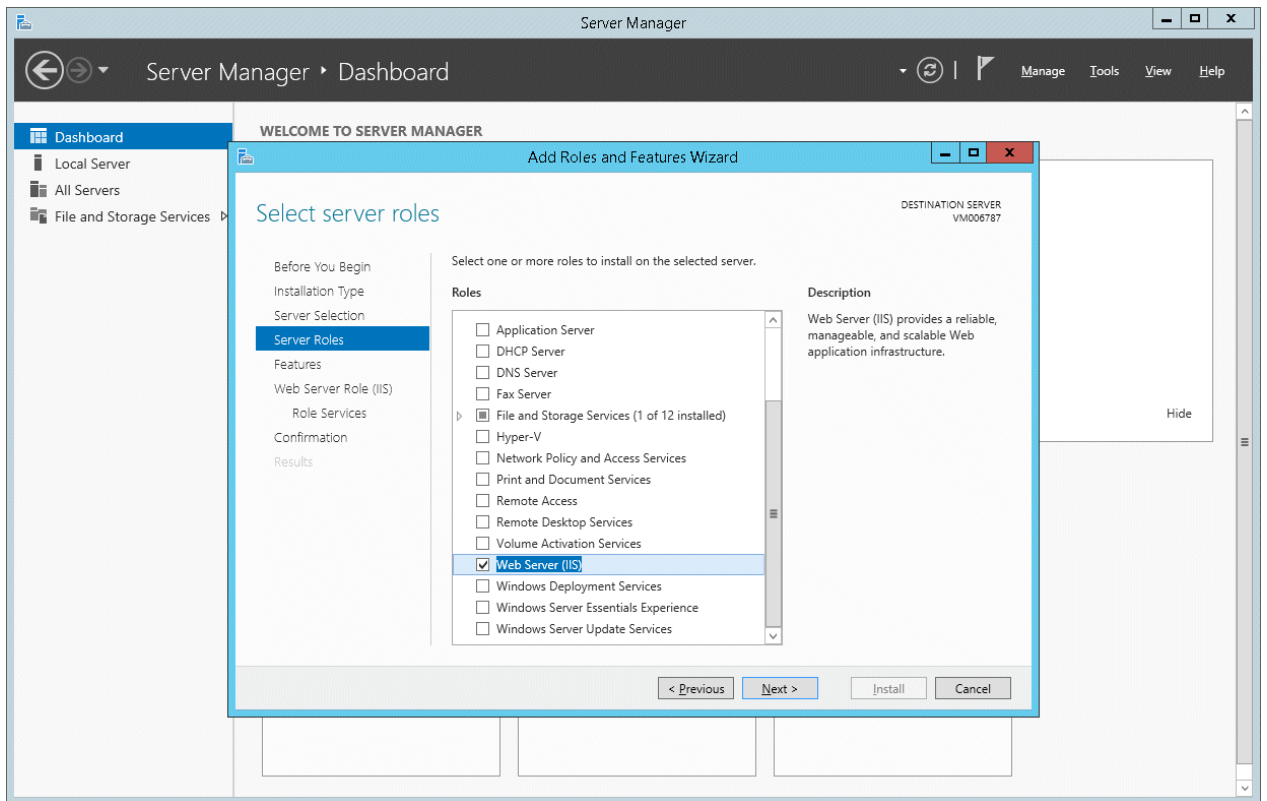
7. In **Select features**, click **Next**.
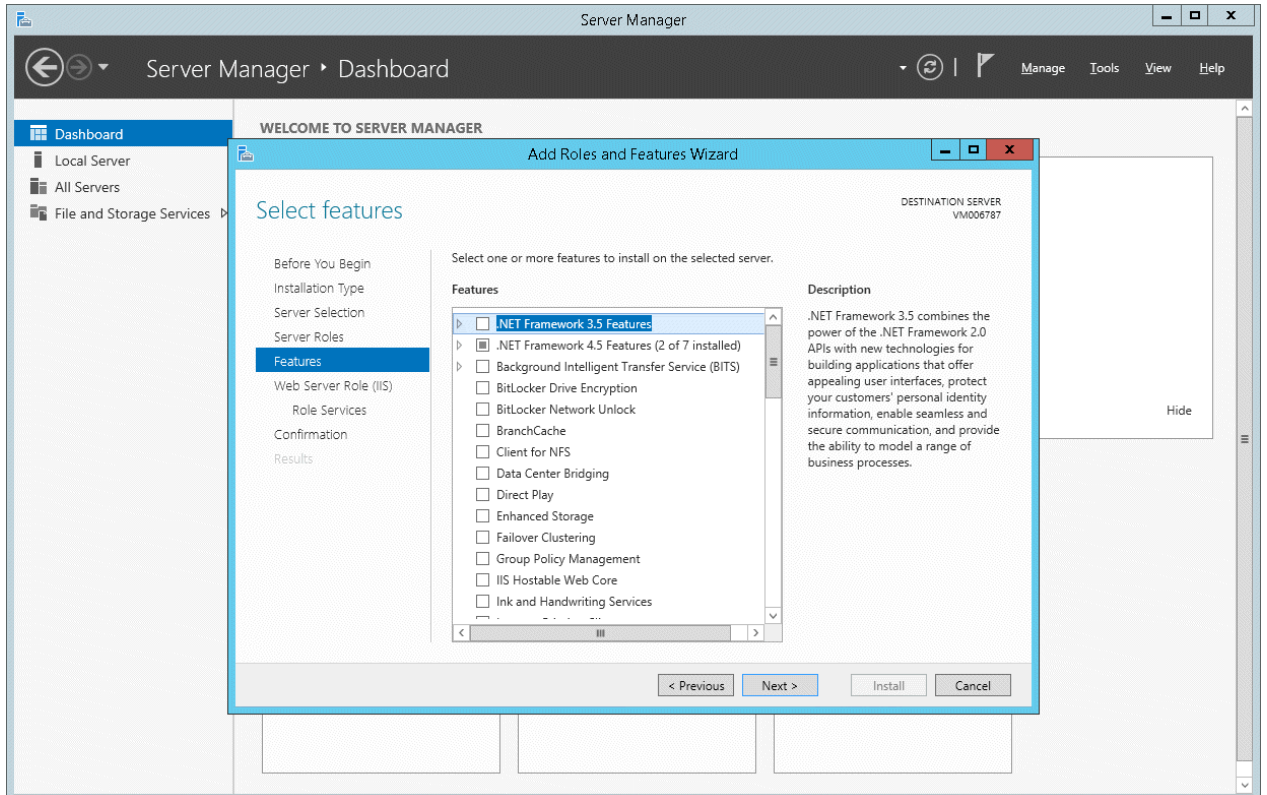
8. In **Web Server Role (IIS),** click **Next**.
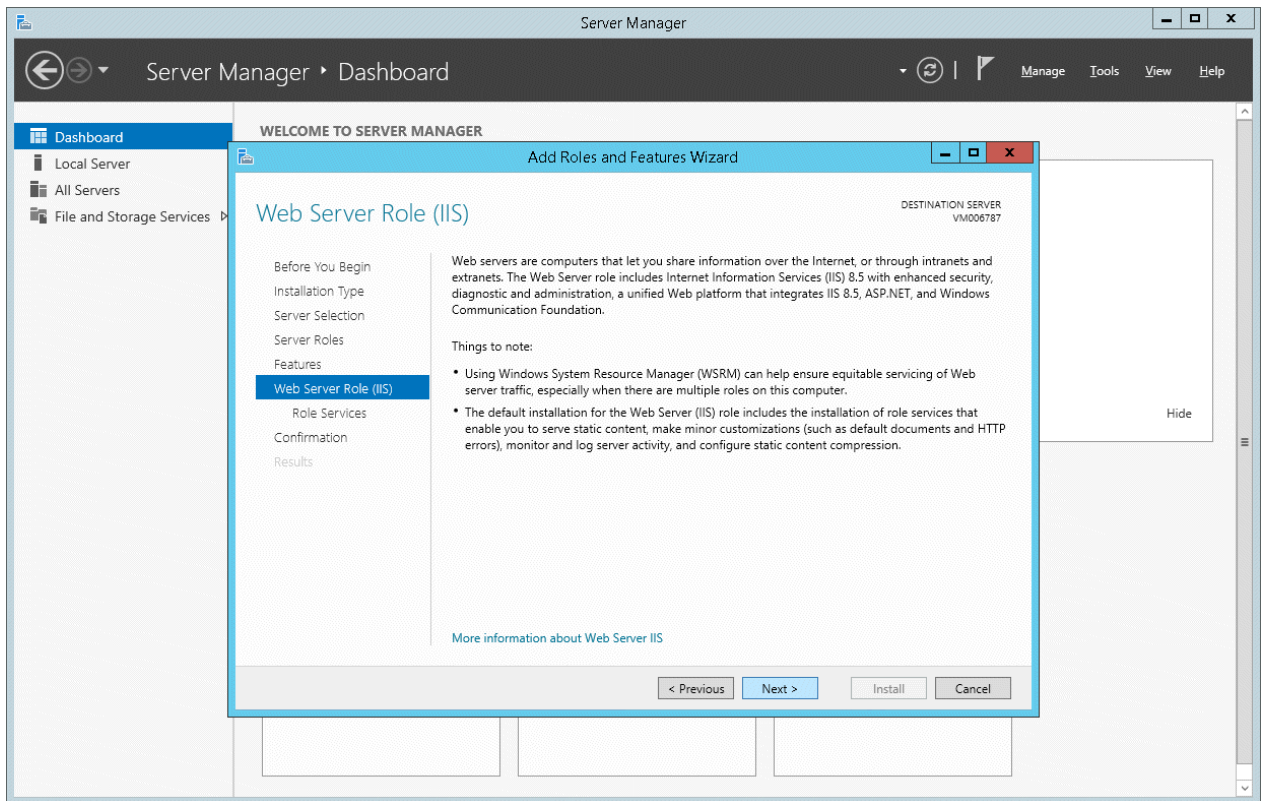
9. In **Select role services**, ensure that **Web Server** > **Application Development** > **ISAPI Extensions** is selected.
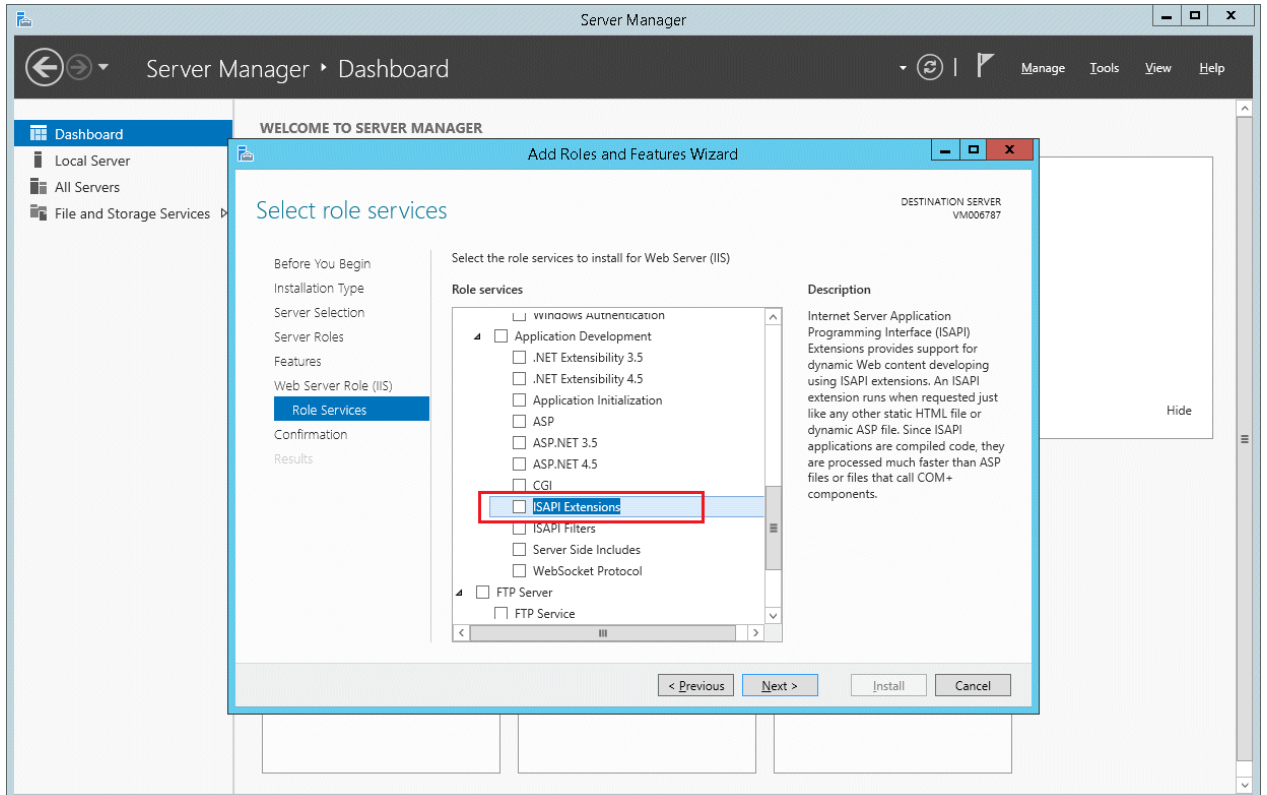
10. Ensure that the four features listed under **Management Tools** > **IIS 6 Management Compatibility** are selected, and click **Next**.

![Note icon] **Note**
. . . .

Ensure that the following items are selected.

- **Web Server** > **Common HTTP Features** > **Static Content**

- **Web Server** > **Common HTTP Features** > **Default Document**

- **Web Server** > **Common HTTP Features** > **Directory Browsing**

- **Web Server** > **Common HTTP Features** > **HTTP Errors**

. . . .
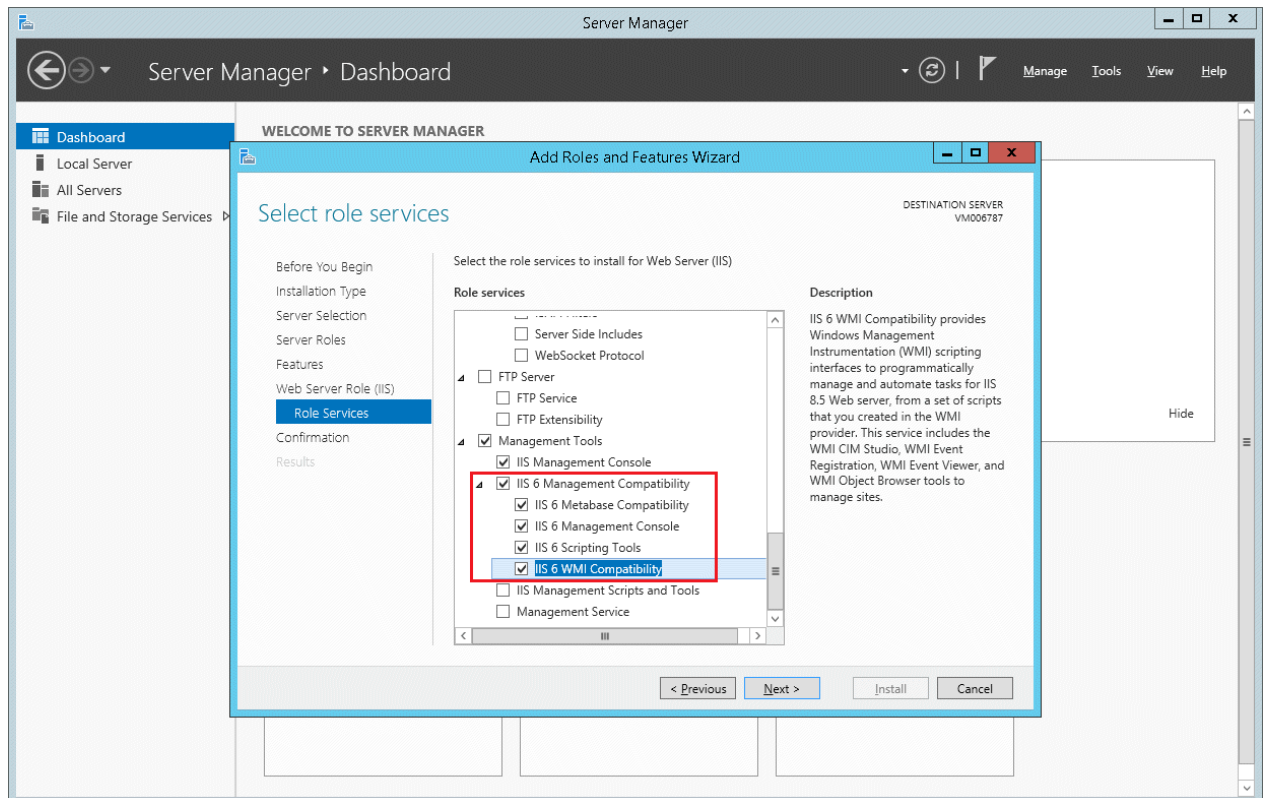
11. A confirmation window will be displayed. Click **Install**.
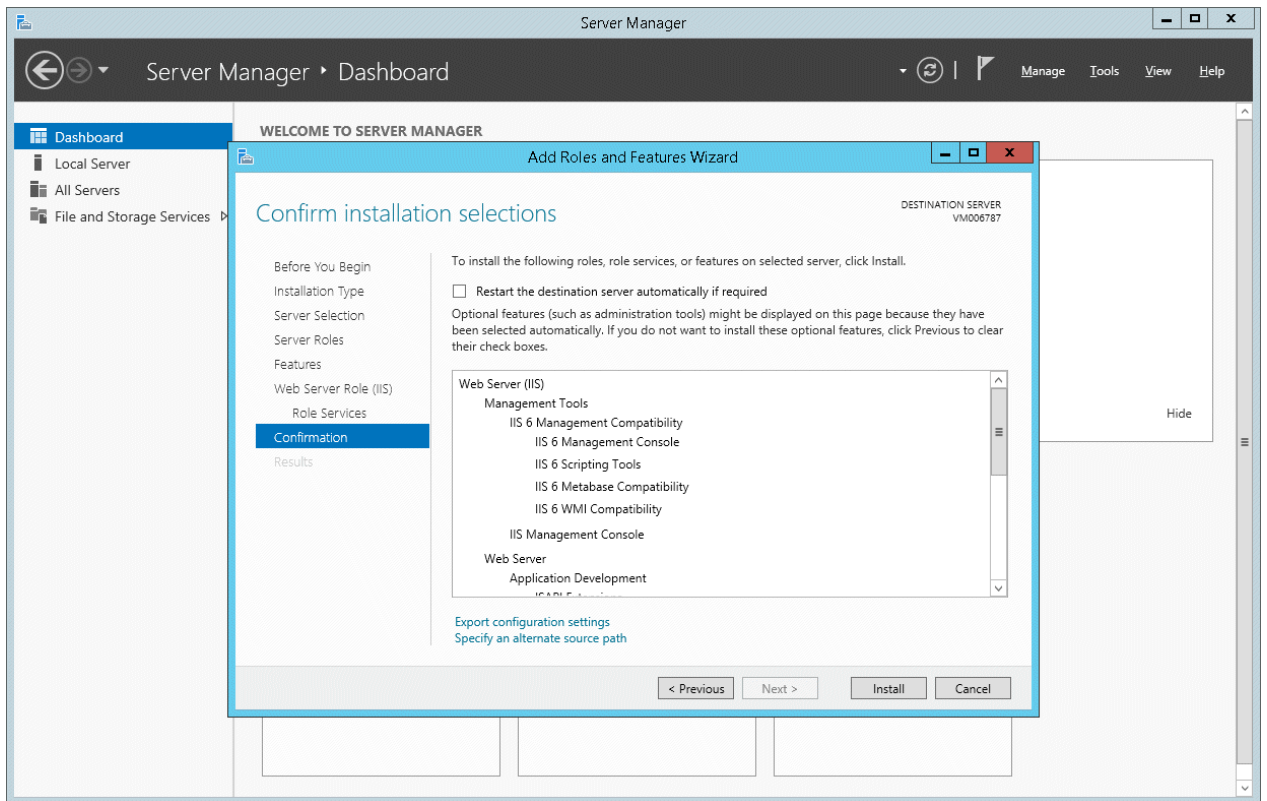
12. Once installation is completed, click **Close**.

Installation procedure for the ISAPI extensions when IIS is already installed

1. Click the **Server Manager** icon in the bottom-left of the window to start it.

2. The **Server Manager** window will be displayed. In the **Manage** menu in the top-right of the window, click **Add Roles and Features**.
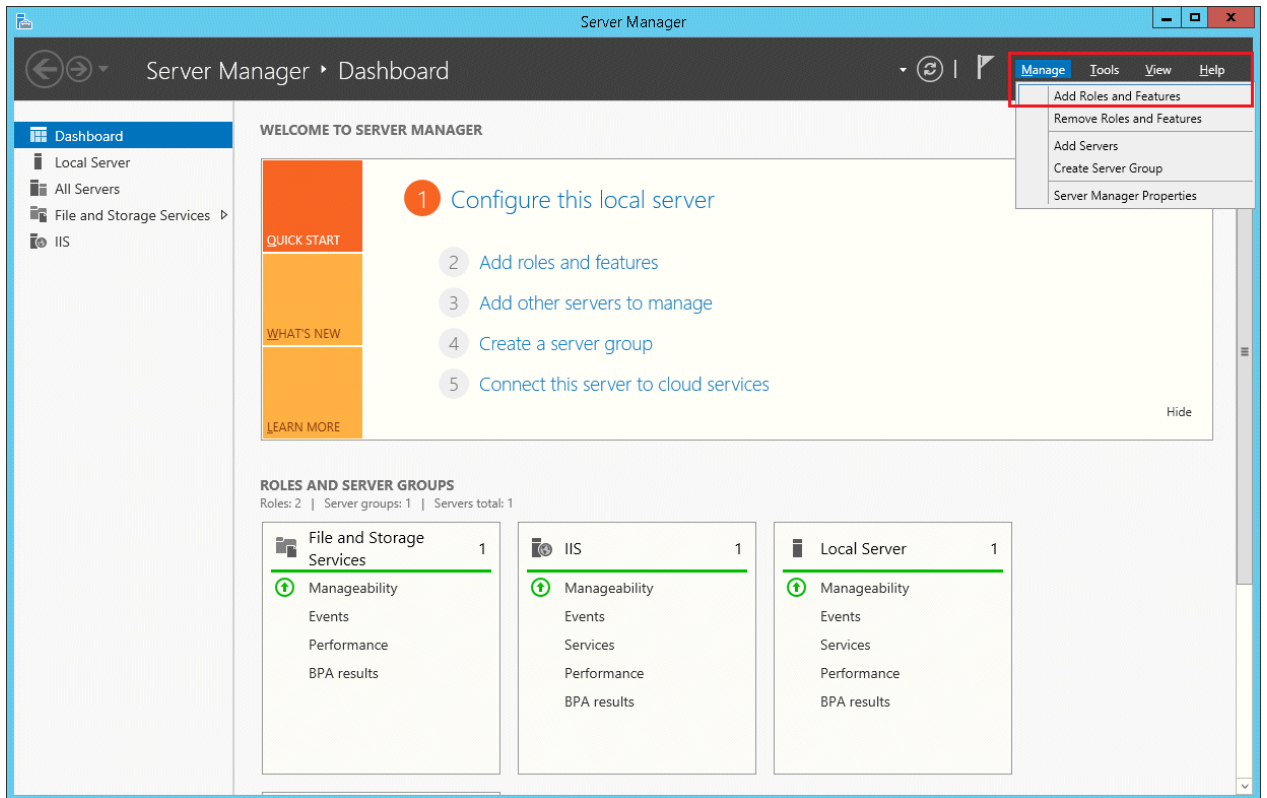
3. The **Add Roles and Features Wizard** will be displayed. In **Installation Type**, click **Next**.
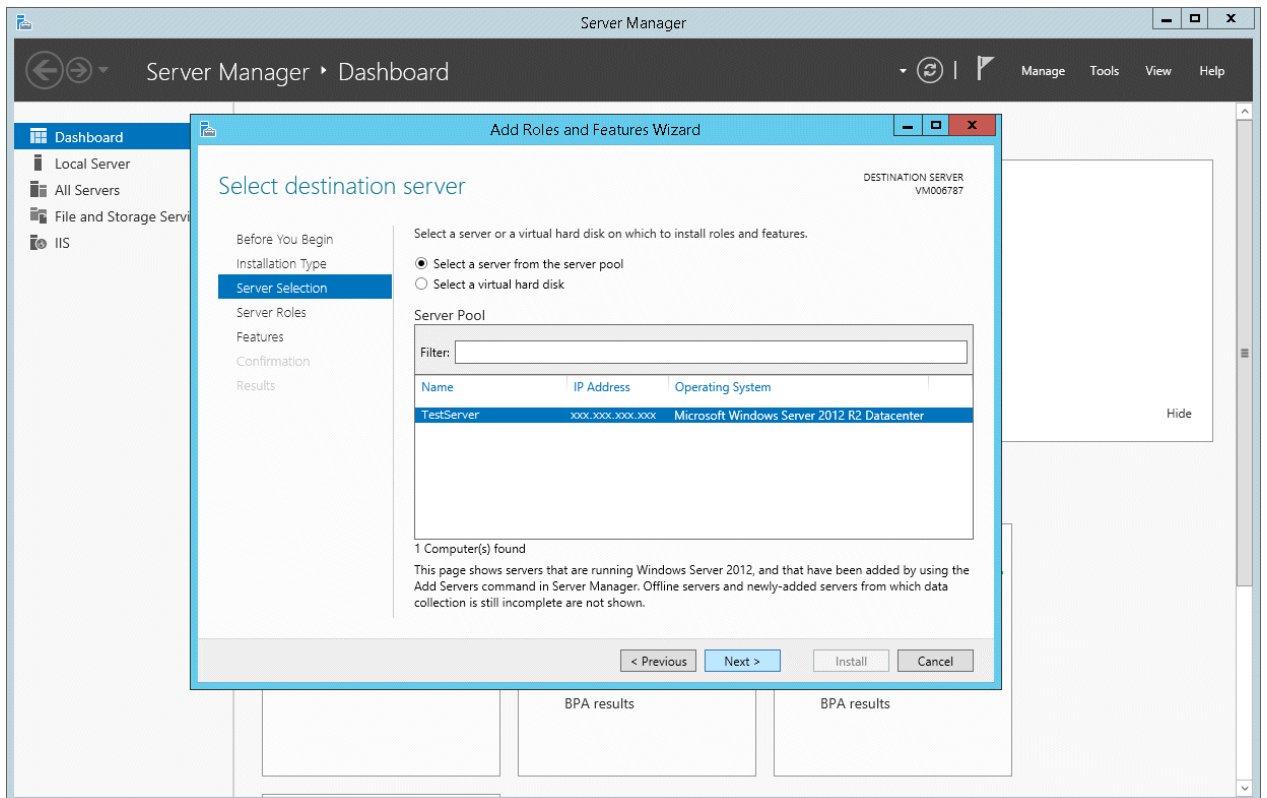
4. In **Server Selection**, click **Next**.
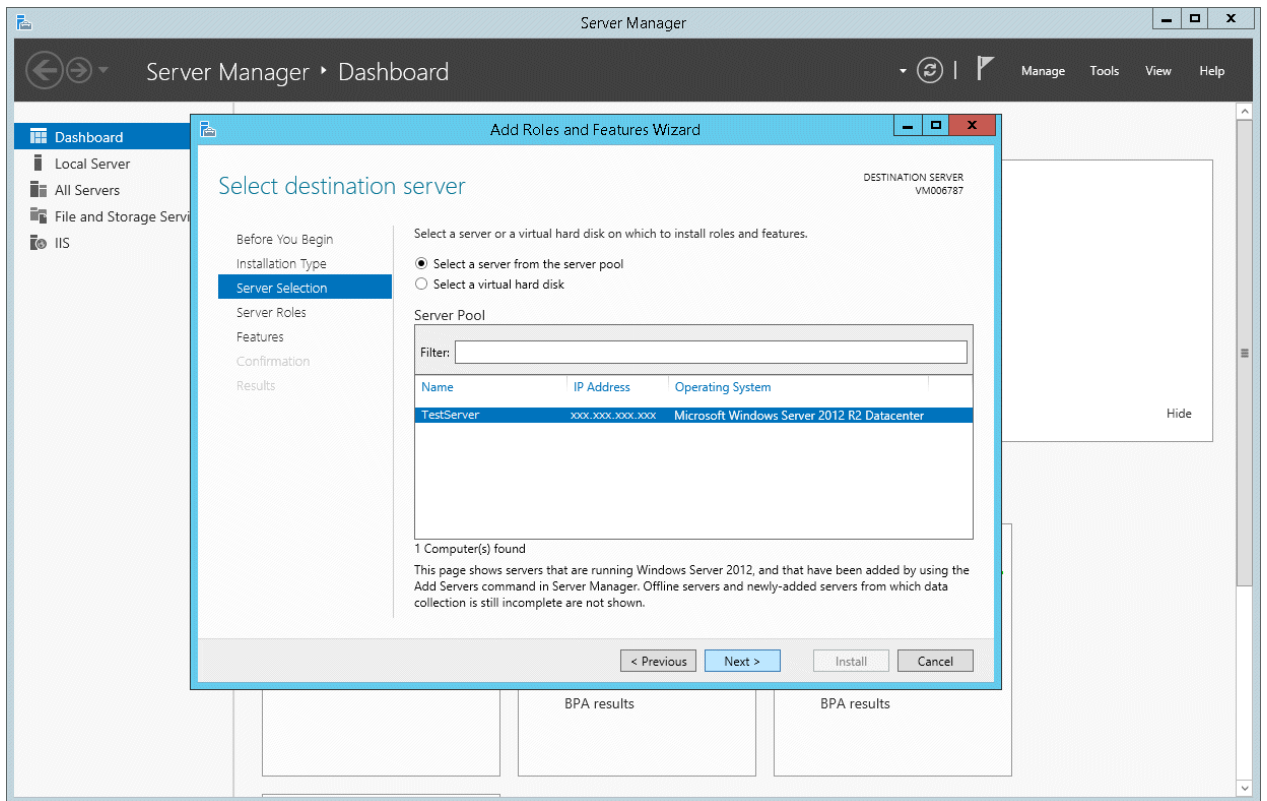
5. In **Select role services**, ensure that **Web Server** > **Application Development** > **ISAPI Extensions** is selected.
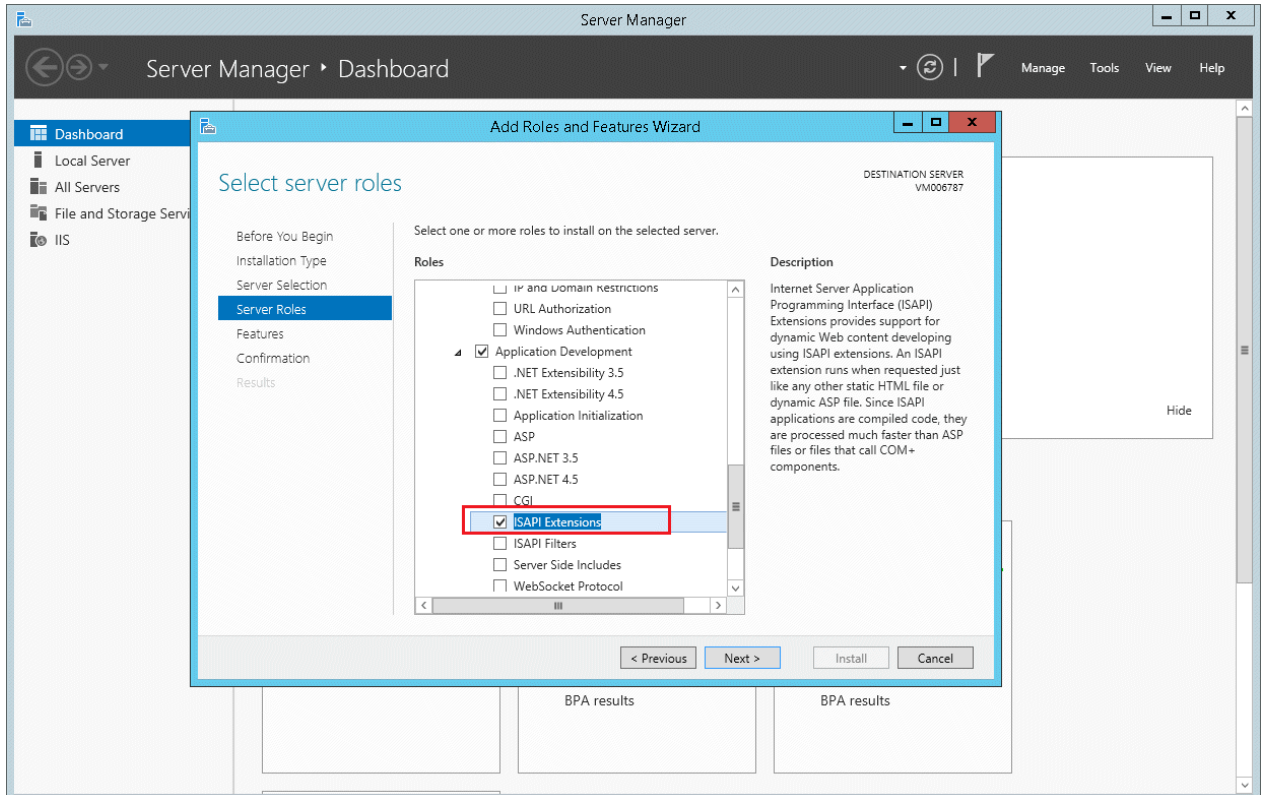
6. Ensure that the four features listed under **Management Tools** > **IIS 6 Management Compatibility** are selected, and click **Next**.

![Note icon] **Note**

· ·

Ensure that the following items are selected.

-   **Web Server** > **Common HTTP Features** > **Static Content**

-   **Web Server** > **Common HTTP Features** > **Default Document**

-   **Web Server** > **Common HTTP Features** > **Directory Browsing**

-   **Web Server** > **Common HTTP Features** > **HTTP Errors**

· ·
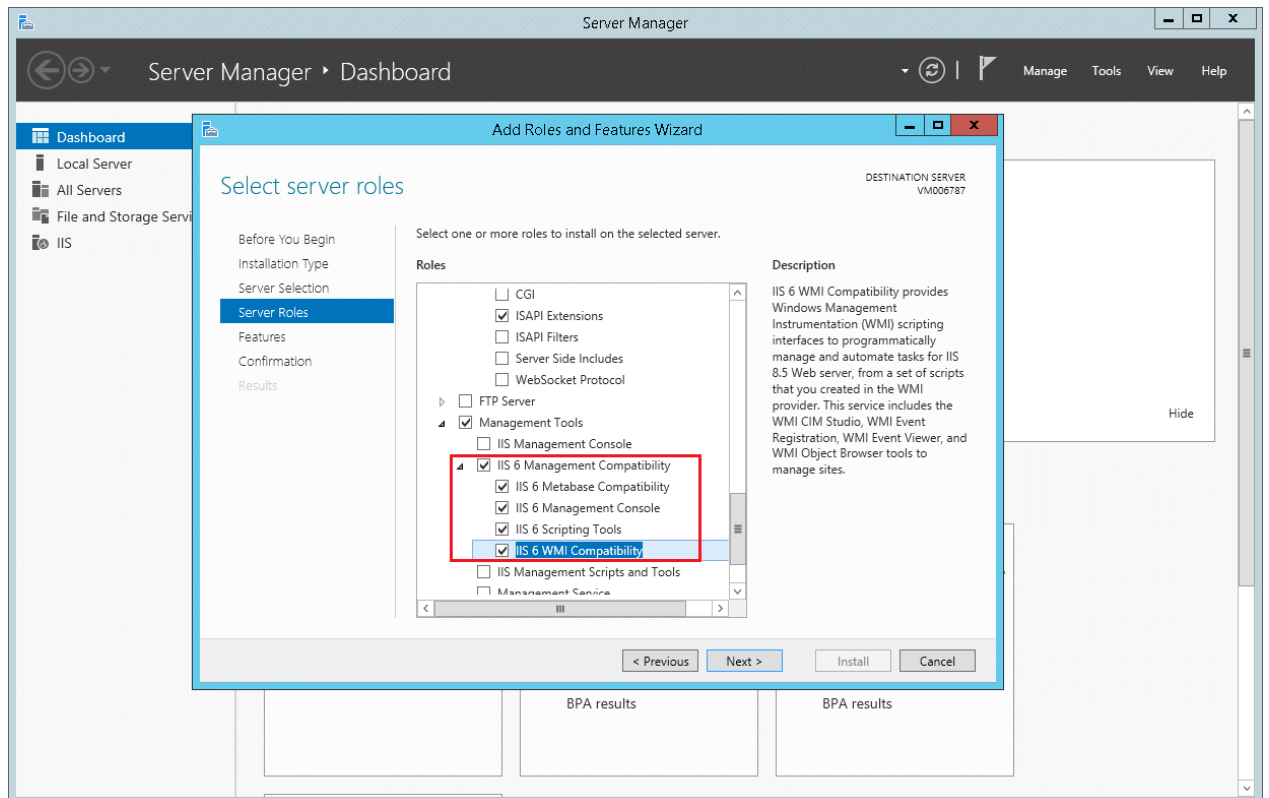
7. In **Select features**, click **Next**.
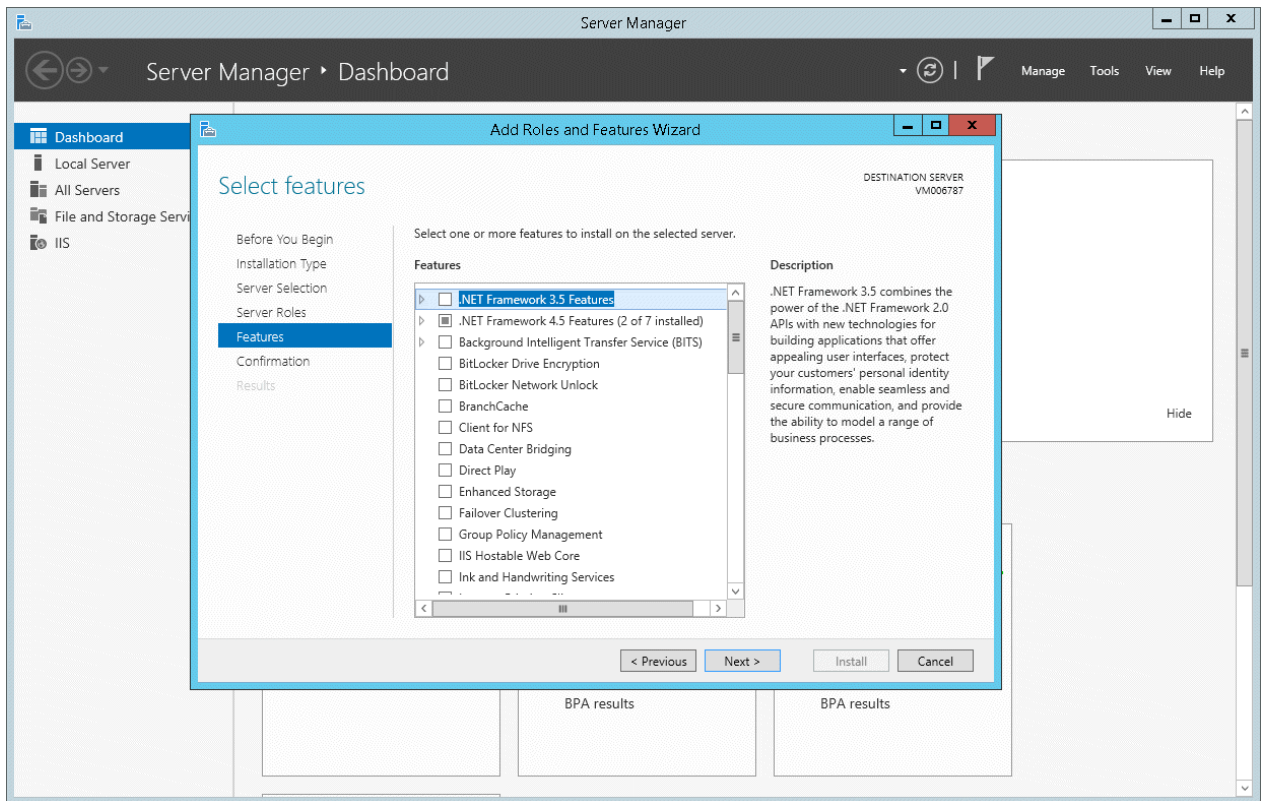
8. A confirmation window will be displayed. Click **Install**.
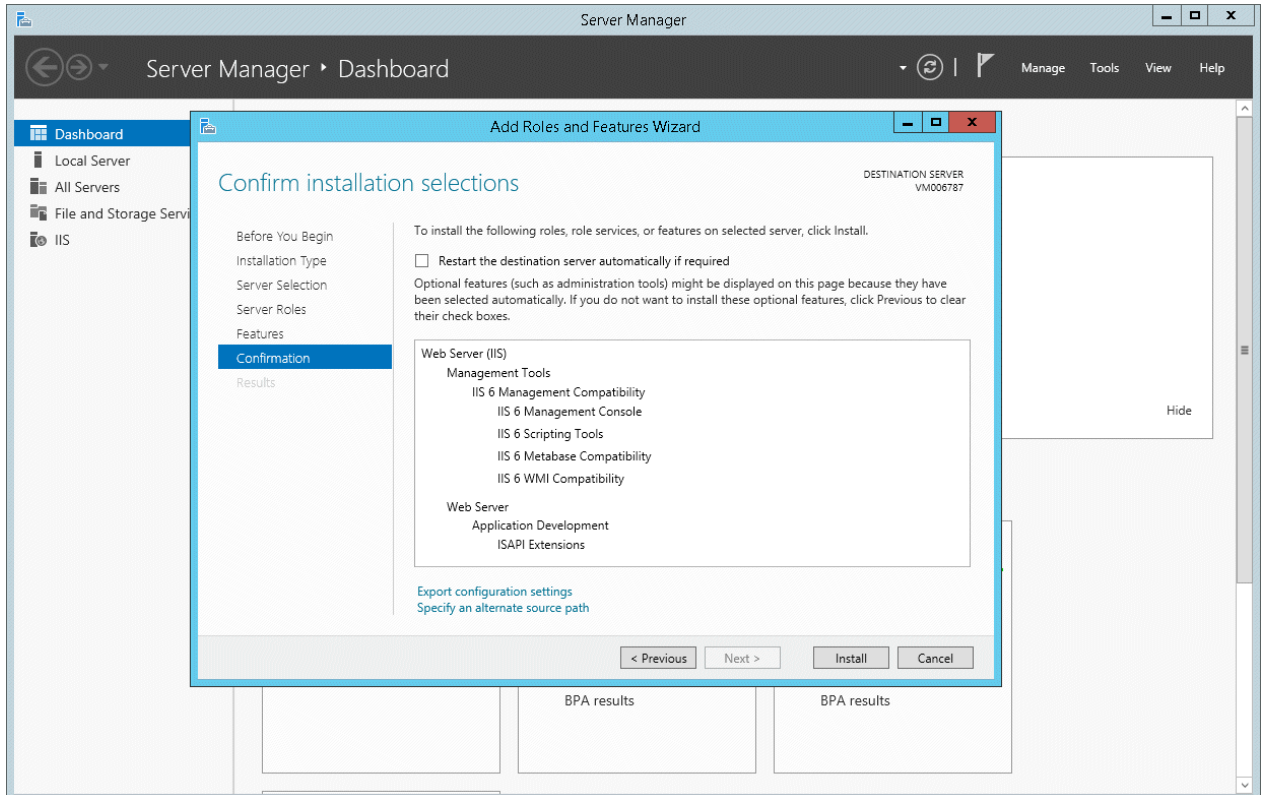
9. Once installation is completed, click **Close**.

2.3.2 Install CS

This section describes how to install CS.

If Systemwalker Desktop Patrol CS is installed, the Systemwalker Desktop Patrol CT function will be installed at the same time. It can be managed as other CTs do.

The CT function of CS cannot be uninstalled alone.

There are three ways to install CS:

Standard installation should be performed if 300 or less CTs are to be managed on one CS, and default installation setting values are to be used. Custom installation should be performed if more than 300 CTs are to be managed on one CS, and values other than the default are to be used.

Note
. . . .

CT registration password

- To use a CT registration password, ensure that the server administrator uses CustomPolicy.exe (policy for modifying custom setup command) to enable it. CT registration passwords can be set per target server (CS and DS). Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on the command.

  It is recommended to change the CT registration password using CustomPolicy.exe (policy for modifying custom setup command) once the CT is extracted.

- If a CT registration password is enabled, it must be set on the CT.
. . . .

Issues to be confirmed before installation

- Stop the following programs before installation.

    - Resident program included virus check program.

    - The **Service** window of Windows

- Confirm whether the disk capacity required for the drive specified in the installation target of the database installation folder has been ensured by referring to "Operation Environment" of *Systemwalker Desktop Patrol User's Guide*.

- Confirm "Products that cannot be Used in Mixture" by referring to "Operation Environment" of *Systemwalker Desktop Patrol User's Guide*.

- Confirm the port number in use by referring to "List of Port Numbers" of *Systemwalker Desktop Patrol Reference Manual*.

- When specifying "FQDN" or "Windows Host Name" in **Host Name** of the **Server Environment Setup** window set at installation, the address of this "FQDN" or "Windows Host Name" should be analyzed through Systemwalker Desktop Patrol CT, so confirm before installation.

- If you install Systemwalker Desktop Patrol to an environment where Systemwalker Desktop Keeper is installed, the service managing iOS devices will be stopped automatically. In this case, the service managing iOS devices will not be available for use until the system is restarted.

Note
. . . .

If the address of host name cannot be analyzed, install it again

When the address cannot be analyzed, it is likely that patch installation, software distribution and Inventory collection cannot be performed in Systemwalker Desktop Patrol CT. Systemwalker Desktop Patrol CS should be installed again.
. . . .

2.3.2.1 Standard Installation

The table below lists the default values used in standard installation.

Refer to the appropriate sections in "2.3.2.2 Custom Installation" or "2.3.3 Construct Database" for the details on item names.

📌 **Note**

. . . .

Standard installation uses fixed values for the system administrator user ID and initial password.

For security reasons, change the initial password when you log in the main menu for the first time.

Until the initial password is changed, a warning message prompting you to change the password will be displayed when you log in the main menu.

. . . .

Setting context	Item and referenced section	Default value	Can be updated?
Folder settings	**Install folder** (step 5 in "2.3.2.2 Custom Installation")	If installing a 32-bit version of CS on a 32-bit version of the operating system or installing a 64-bit version of CS on a 64-bit version of the operating system: C:\Program Files\Fujitsu\Systemwalker Desktop Patrol If installing a 32-bit version of CS on a 64-bit version of the operating system: C:\Program Files (x86)\Fujitsu\Systemwalker Desktop Patrol	Y
	IIS (Internet Information Services) home directory (step 6 in "2.3.2.2 Custom Installation")	(IIS home directory)	
Server environment setup	**Server name** (step 8 in "2.3.2.2 Custom Installation")	Corporate server	
	Host name (step 8 in "2.3.2.2 Custom Installation")	(Obtained automatically.)	Y
	Software distribution port number (step 8 in "2.3.2.2 Custom Installation")	2922	Y
	Port number for inventory transmission (step 8 in "2.3.2.2 Custom Installation")	2856	Y
	Directory for saving distributed software (step 8 in "2.3.2.2 Custom Installation")	"*dtpInstallDir*\FJSVsbtrs\data\swc"	

Setting context		Item and referenced section	Default value	Can be updated?
		Maximum size (step 8 in "2.3.2.2 Custom Installation")	5000 MB	
Environment setup for Systemwalker Desktop Patrol CT	**Identification**	**User ID** (step 9 in "2.3.2.2 Custom Installation")	systemadmin (user ID for system administrator)	
		PC name (step 9 in "2.3.2.2 Custom Installation")	First 20 characters of host name	
	User	**Content** (step 9 in "2.3.2.2 Custom Installation")	(No default value)	
	Server	**Connection Server** (step 9 in "2.3.2.2 Custom Installation")	(Obtained automatically.)	
Database construction	**Register the system account**	**User ID** (step 5 in "2.3.3 Construct Database")	systemadmin (user ID for system administrator)	
		Password (step 5 in "2.3.3 Construct Database")	systemadmin (initial password for system administrator)	
	Enter database information	**Database Storage Location** (step 6 in "2.3.3 Construct Database")	C:\DESKTOPPATROL_DBSP	
		Number of PC(s) (step 6 in "2.3.3 Construct Database")	300	
		Number of smart devices (step 6 in "2.3.3 Construct Database")	0	
		Number of managed non-PC(s) (step 6 in "2.3.3 Construct Database")	0	
		Collection of EXE Information (step 7 in "2.3.3 Construct Database")	Not checked.	
		Collection of Software Operation Information or Control of Execution File (step 7 in "2.3.3 Construct Database")	Not checked.	

Follow the steps below to perform standard installation (refer to the *Systemwalker Desktop Patrol User's Guide* for details on the operating environment):

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. After inserting DVD-ROM of Systemwalker Desktop Patrol into PC, the following window is displayed.

   Select **CS Installation**.
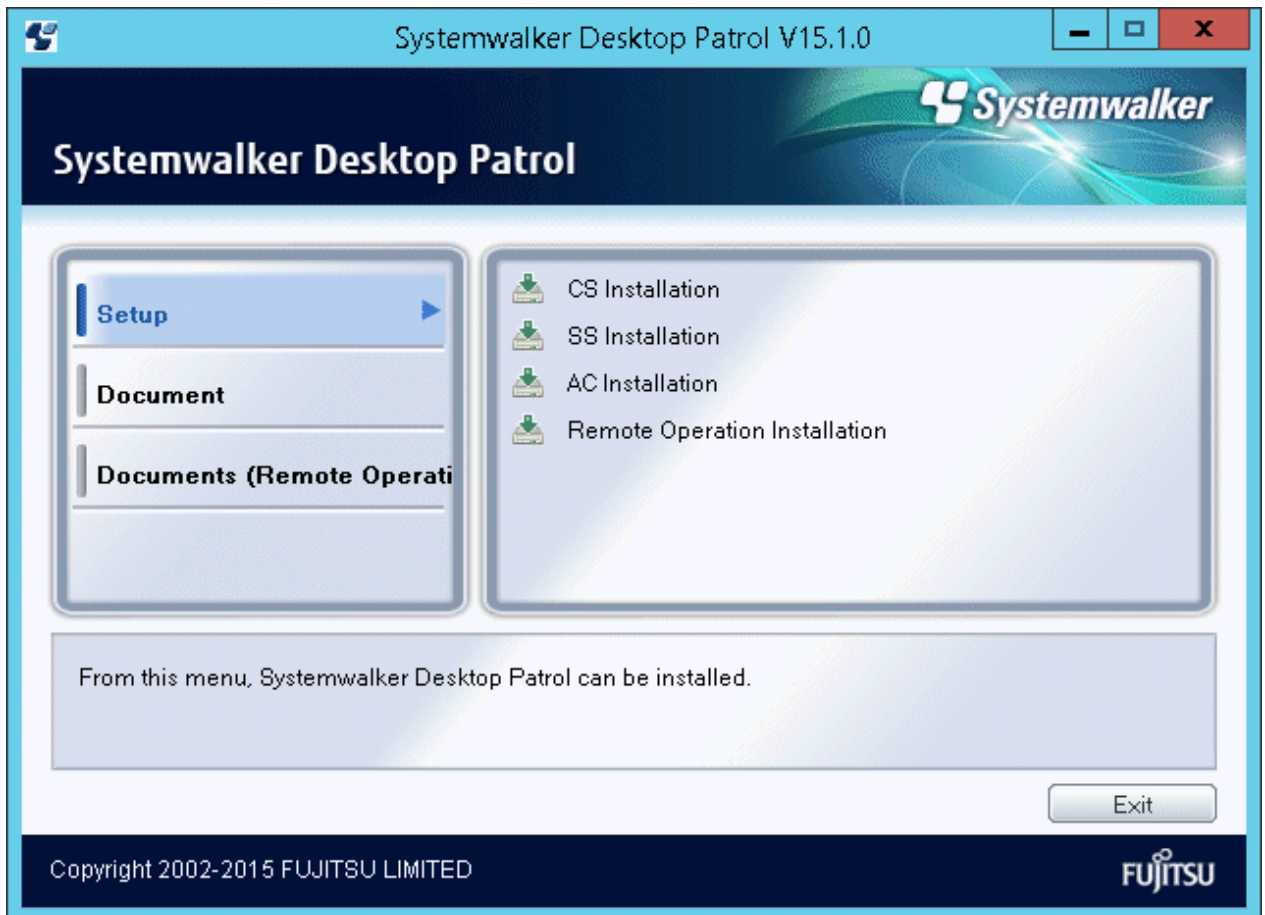
If the above installer is not started, start "swsetup.exe" of DVD-ROM drive.

Note

If the operating system in use is Windows Server(R) 2008 or later, execute this as administrator.

4. The **Welcome to setup Systemwalker Desktop Patrol** window is displayed, select **Standard Installation**, and click the **Next** button.
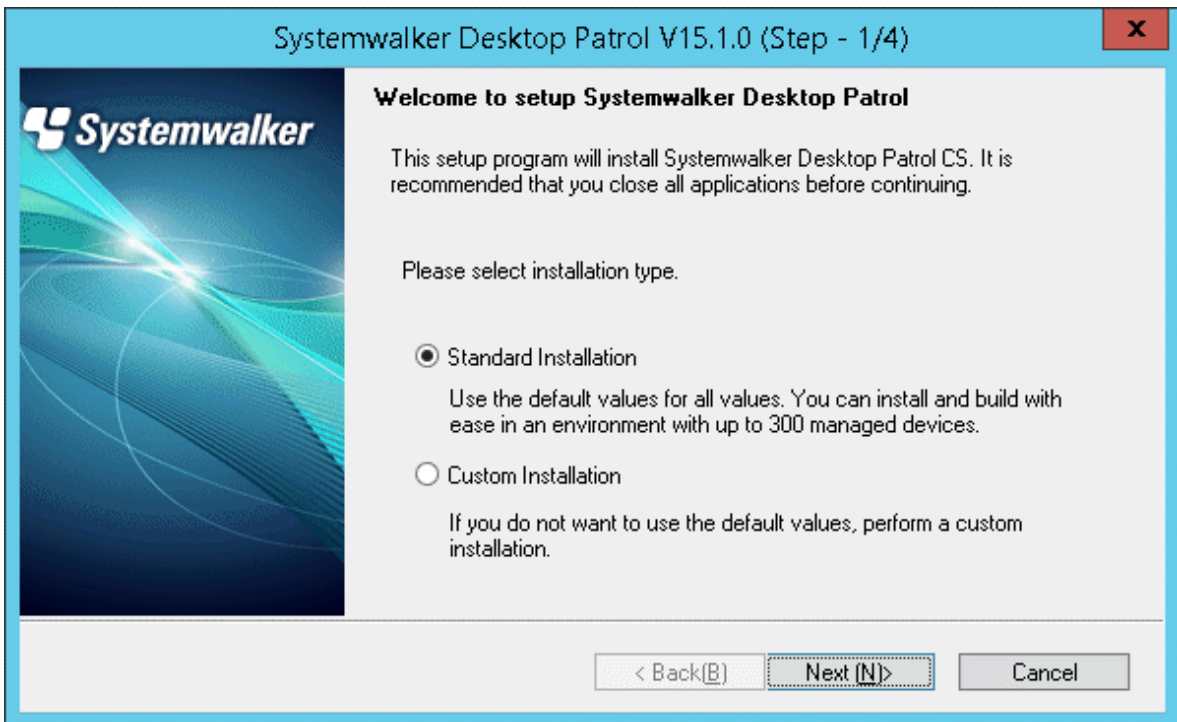
5. The **Installation Parameter Settings** window will be displayed.
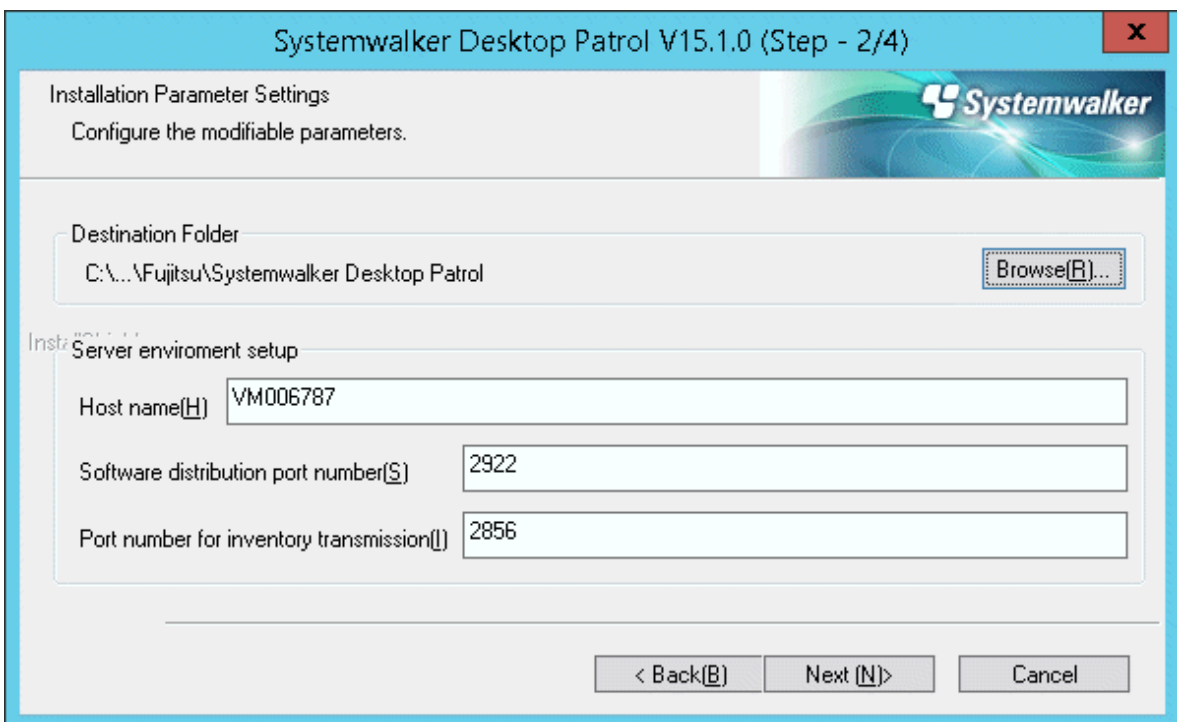
If you want to use the displayed item values, click **Next**.

If you want to modify the displayed item values, change according to the table below, and click **Next**.

Item	Description
Destination Folder	CS installation folder.

Item		Description
		To change the value, click **Browse** and specify a different folder.
		Specify a folder not used by other programs. This product must not coexist with other programs in the same folder. For this reason, do not install other programs under the installation folder after this product is installed.
		📛 **Note**
		Invalid characters
		Do not specify fullwidth characters or halfwidth Japanese characters for **Destination Folder,** otherwise client policy will not be distributed.
Server environment setup	**Host name** (this value cannot be changed after installation)	Change the value as required.
		If the default value is not displayed, consider the following conditions and enter the host name.
		Specify the FQDN format, IP address, or Windows host name of the PC on which Systemwalker Desktop Patrol CS will be installed. Specify up to 50 characters, using alphanumeric characters, hyphens ("-") and periods ".".
		Example: cs.example.com
		Specify an environment that can be resolved using the Systemwalker Desktop Patrol DS/CT that will be connected.
		📛 **Note**
		Communication in IPv6 environments
		IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name:
		- Register the CS and DS host name and IP address in the DNS server.
		- Register the CS and DS host name and IP address in the communication source PC hosts file.
	Software distribution port number (this value cannot be changed after installation)	Port number used for software distribution.
		The default value is 2922.
		Specify a value from 5001 to 65535 that does not conflict with other systems.
	Port number for inventory transmission (this value cannot be changed after installation)	Port number to be used for inventory transfer.
		The default value is 2856.
		Specify a value from 5001 to 65535 that does not conflict with other systems.

6. In the **Confirm Installation** window, ensure that the information displayed is correct, and click **Install** to start installation. If you need to revise the parameters, click **Back**.
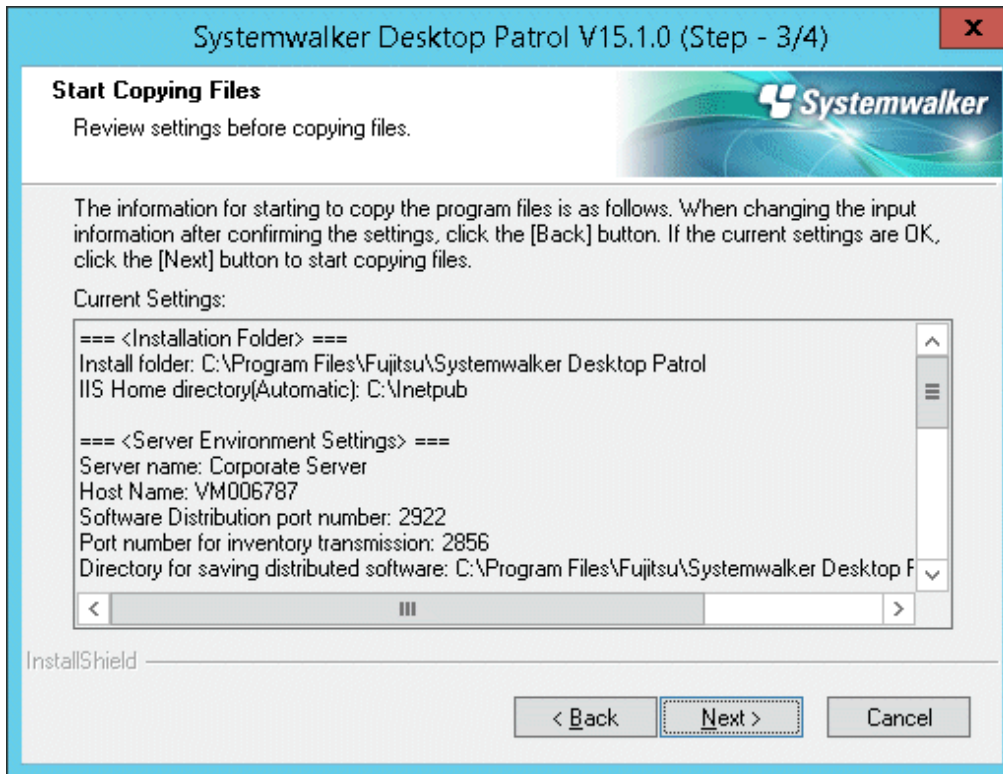
7. Once installation is completed, the window below will be displayed.

    Click **Finish**.

8. To use the program, the system must be restarted.

    Click **Yes**.
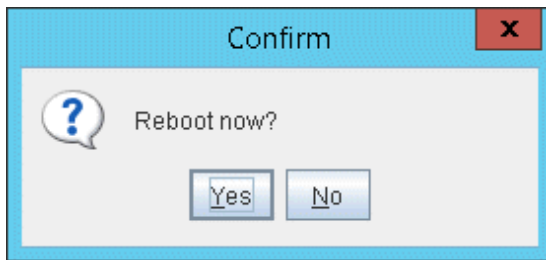
After installation, perform the tasks described in "2.3.4 Construct an iOS Management Database" and later sections.

2.3.2.2 Custom Installation

Follow the steps below to perform custom installation (refer to the *Systemwalker Desktop Patrol User's Guide* for details on the operation environment):

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. Insert the Systemwalker Desktop Patrol DVD-ROM in the PC.

    In the window below, select **CS Installation**.
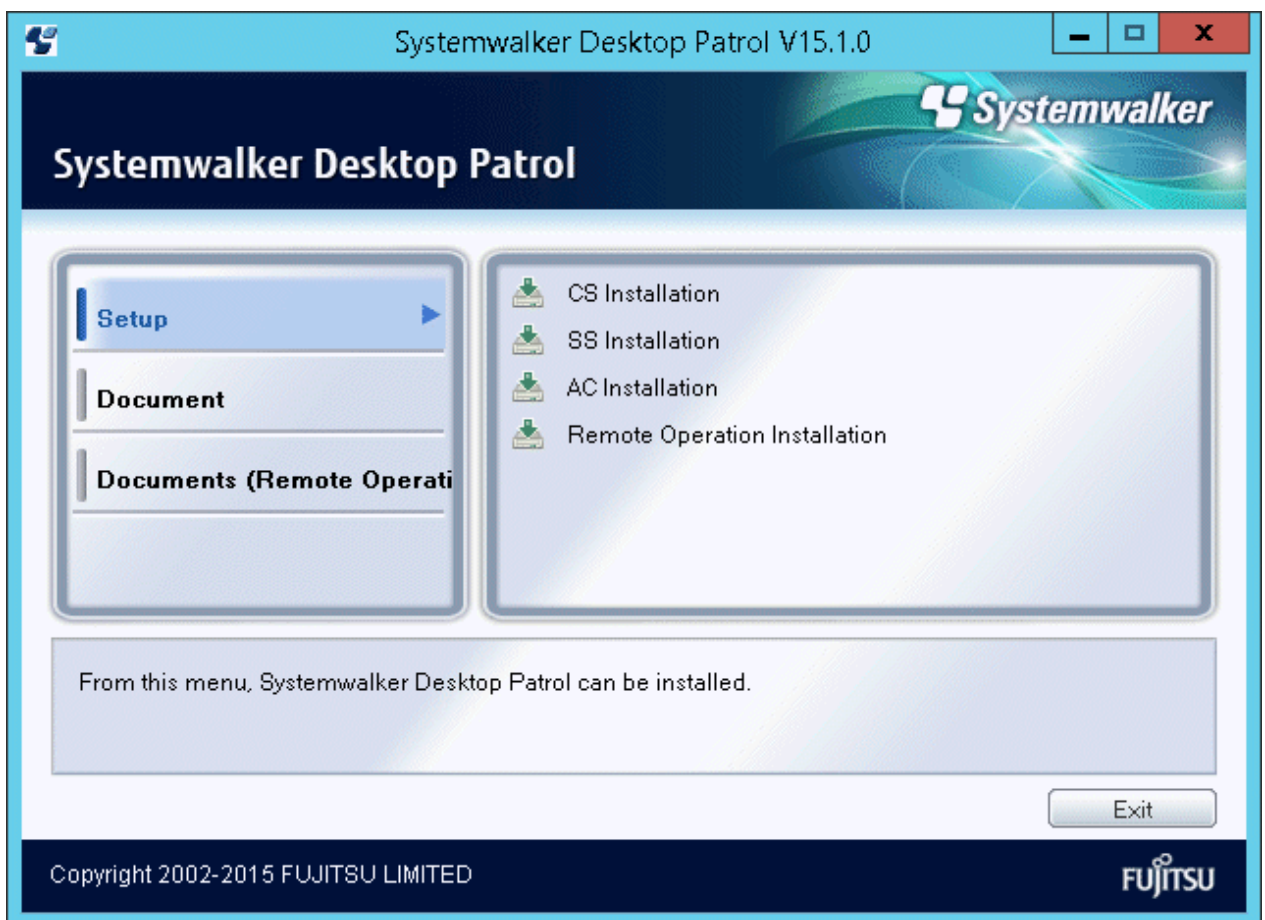
If the above installer window is not displayed, start "swsetup.exe" in the DVD-ROM drive.

Note

. . . .

In Windows Server(R) 2008 or later, execute this as administrator.

. . . .

4. The **Welcome to setup Systemwalker Desktop Patrol** window will be displayed. Click **Custom Installation**, and then **Next**.
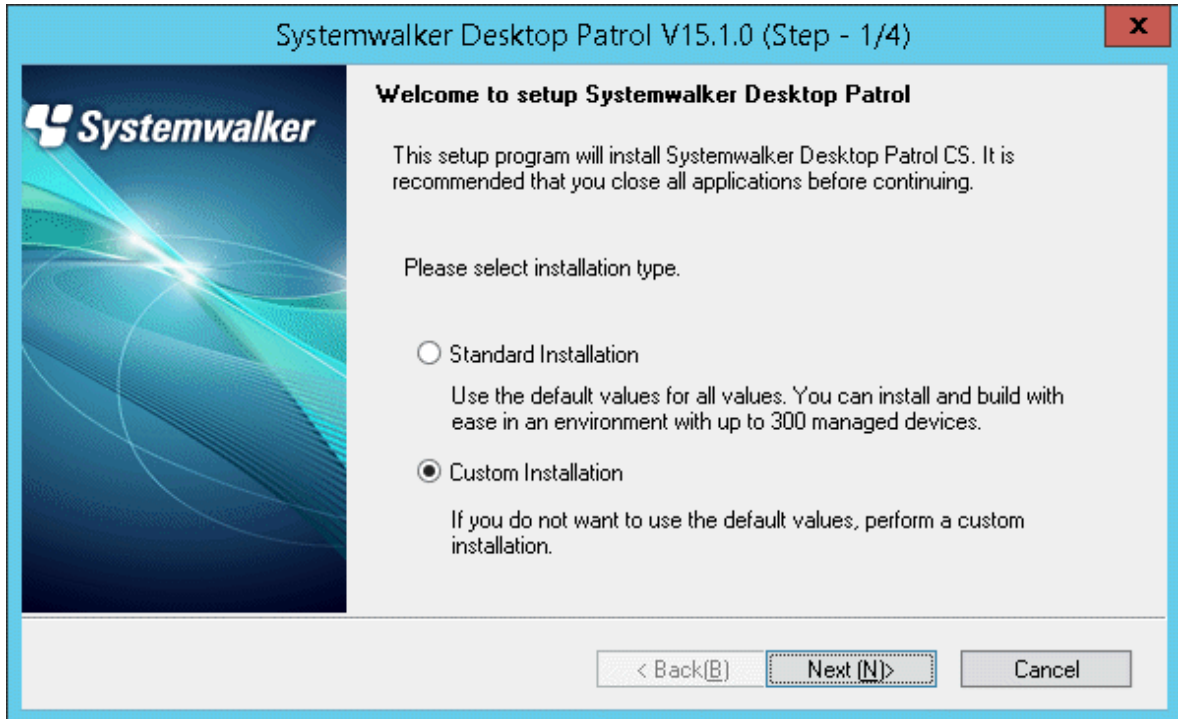
5. The **Please Read** window is displayed, confirm the content and click the **Next** button.

6. The **Select Installation Folder** window is displayed.

   If you do not want to modify the displayed installation target, click the **Next** button.

   To modify the displayed installation target, click the **Browse** button of the folder to be modified, and click the **Next** button after the folder is modified.

   When installing this product, create a folder different from that of other programs and install to this folder. Do not install this product to the folder same as other programs. Besides, after installing this product, do not install other programs to the installation target folder of this product.

   Besides, the capacity required for installation and the available capacity of the selected **Installation Target Folder** will also be displayed in the window. To confirm the capacity of other disks, click the **Disk Capacity** button.

 Note

. . . .

About characters that cannot be specified

Do not specify directory containing Multi-byte in **Installation Target Folder**. If characters not allowed have been set in the directory, client policy cannot be distributed.

. . . .

7. The "Select IIS (Internet Information Services) Home Directory" window is displayed.

   If you do not want to modify the displayed home directory, click the **Next** button.

   To modify the displayed home directory, click the **View** button of the folder to be modified, click the **Next** button after the home directory is modified.

8. The **Start to Copy File** window is displayed, confirm whether the content displayed in the window is incorrect, and click the **Next** button.

The **Installation Status** window is displayed, start installation.

9. The **Server environment setup** window will be displayed during installation.

📌 Note

. . . .

The **Server environment setup** window will be displayed behind the background window during installation sometimes.

Display this window by switching the window through the taskbar or Alt+TAB key.

. . . .

Enter the following information, and click the **Next** button after confirmation.

It is unable to return to this window after the following **Environment Setup** window is displayed.

Item	Description
Server name (Required)	Specify "Company Name" for installing Systemwalker Desktop Patrol CS. Any characters within 50 characters which contain single-byte letters and numerals, special character "-", "@" and "." can be specified. Example) Fujitsu Company
Host name (Required) (cannot be modified once set here)	Display the initial value, modify it as required. If the initial value has not been displayed, input the host name according to the following conditions. Specify "FQDN Format", "IP Address" or "Windows Host Name" of PC with Systemwalker Desktop Patrol CS installed. Specify up to 50 alphanumeric characters, "-"(hyphen) or "." (period). Example) cs.example.com This host name should be set in the environment where the name can be analyzed through the connected Systemwalker Desktop Patrol DS/CT. 📌 **Note** . . . . **Communication in IPv6 environments**

Item	Description
	IPv6 addresses cannot be specified. For communication in an IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name: - Register the CS and DS host name and IP address in the DNS server. - Register the CS and DS host name and IP address in the communication source PC hosts file.
Software distribution port number (Required) (cannot be modified once set here)	Specify a port number for software distribution. The initial value is set as "2922". To modify, specify it as a value within 5001-65535 that is not in conflict with other numbers in system.
Port number for inventory transmission (Required) (cannot be modified once set here)	Specify a port number for Inventory transmission. The initial value is set as "2856". To modify, specify it as a value within 5001-65535 that is not in conflict with other numbers in system.
Directory for saving distributed software (Required) (cannot be modified once set here)	Specify a directory for saving distributed software. Specify an absolute path using up to 128 characters, except for the following symbols: / * ? \ " < > | The initial value is set as "*dtpInstallDir*\FJSVsbtrs\data\swc". To modify, specify a directory with sufficient available capacity. In addition, when automatically applying security patches, specify a directory other than Windows installation drive, which has sufficient available capacity. **P** Point . . . . **To prevent OS damage, it is recommended to specify the space excluding the Setup disk** To prevent insufficient disk space due to registering/distributing software or automatically applying security patches, it is recommended to specify distribution software saving directory as other space excluding OS Setup disk . . . .
Maximum size	Specify the maximum disk capacity of **Directory for saving distributed software** in "MB". The maximum size can be specified within 1-999999. If this value is omitted, the available capacity of the specified directory is assumed to be the maximum. A value larger than the available capacity of the drive specified in **Directory for saving distributed software** can be set. Set the maximum combining with the PC environment design.

10. The **Environment Setup** window is displayed.
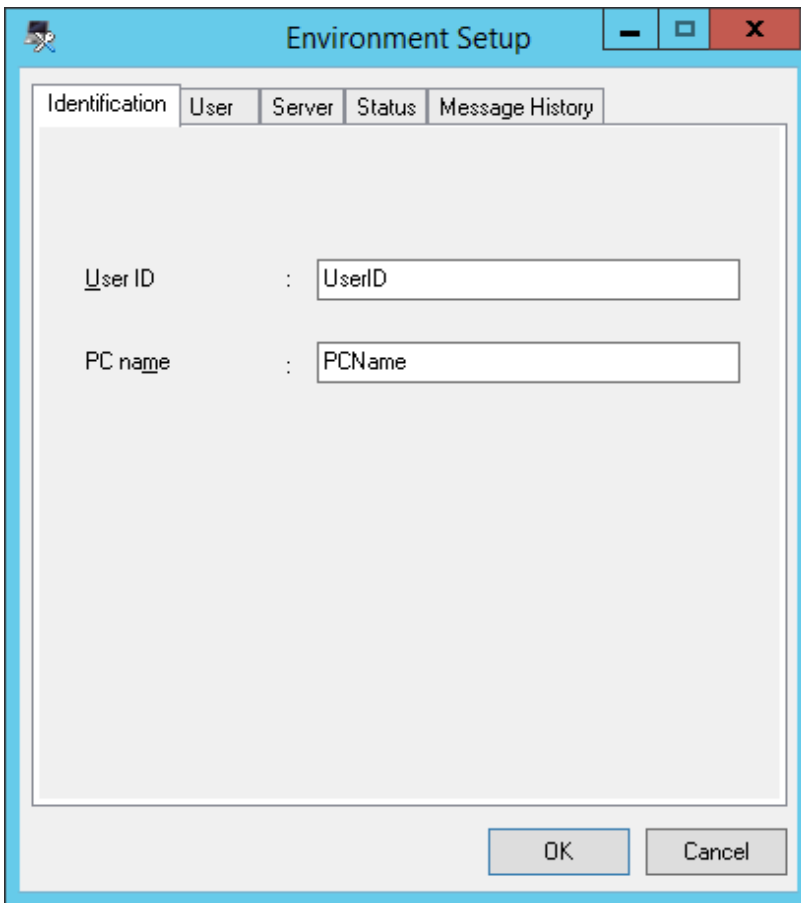
Enter the following information, and click the **OK** button after confirmation to continue installation.

 Point
....

- During installation, specify the appropriate items in **Identification** and **User**. Some items are required.

- To perform this setting later, click the **Cancel** button. At this time, the installation will be continued as well. When performing the settings later, click **Start** > **Program** > **Systemwalker Desktop Patrol CT** > **Environment Setup** or **Apps** > **Systemwalker Desktop Patrol CT** > **Environment Setup**.

....

Environment Setup Tab	Item	Description
Identification	**User ID** (Required)	Specify the user ID to manage as Systemwalker Desktop Patrol CT. It must be specified.
		The user ID set here will be displayed in the main menu for identifying a certain user.
		You can specify up to 20 halfwidth alphanumeric characters and the following symbols: - @ . _
		Alphabetic characters are case-sensitive.
	PC name (Required)	Specify the name to manage as Systemwalker Desktop Patrol CT.
		You can specify up to 20 halfwidth alphanumeric characters. You cannot specify fullwidth characters, spaces and the following symbols: + * ? < > , ; : \ / " |

Environment Setup Tab	Item	Description
User	**Content**	Enter when it is indicated to input in "System Administrator". You can specify up to 256 fullwidth characters, halfwidth alphanumeric characters, halfwidth spaces, and the following symbols: - @ . ( ) [ ] < > : ; / { }
Server	**Connection server**	Specify the host name of the connection server in FQDN format or with IP address. If it has been set at installation, there is no need to input/modify. You can specify up to 256 characters, and the following symbols: - . 📖 **Note** . . . . **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name: - Register the CS and DS host name and IP address in the DNS server. - Register the CS and DS host name and IP address in the communication source PC hosts file. . . . .
Status	**Policy received on**	After operation is started, this item displays the operation status of each CT item.
	Inventory collection	
	Patch installation status	
Message History	None	After operation is started, the history of the messages sent from the administrator is displayed.

11. The **Operation Environment Maintenance Guide** window for constructing the CS database will be displayed.

12. Refer to "2.3.3 Construct Database", and execute tasks to construct the database.

13. Once installation is completed, the window shown below will be displayed.

   Click **Finish**.

14. Reboot the system to use the program.

   Click **Yes**.
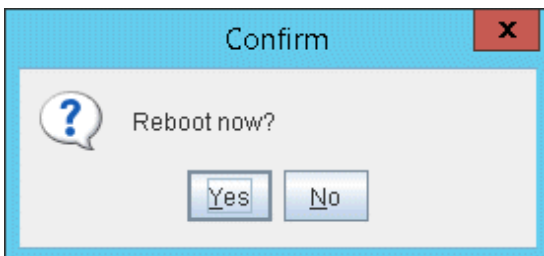
2.3.2.3 Silent Installation

📝 **Note**

....

- Silent installation can only be performed when you are performing custom installation for the first time.

- Installation process must not be interrupted during silent installation.

- Define a non-encrypted password in the installation parameter CSV file and in the response file.
  It is the responsibility of the user to manage the installation parameter CSV file and the response file.

....

Follow the steps below to perform silent installation:

1. Create an installation parameter CSV file.

   Refer to "A.1.1 Installation Parameter CSV File" for details.

   If you are performing installation using the default values for all parameters, this step is not required.

2. Use the parameter setup command to create a response file.

   Refer to "A.1.2 Parameter Setup Command" for details.

   If you did not create an installation parameter CSV file in step 1, this step is not required.

3. Execute the silent installation command.

   Refer to "A.1.4 Silent Installation Command" for details.

4. Check the installation result in the returned value and message from the silent installation command.

Refer to "A.1 Silent installation of CS" for details on the files and commands used, and messages output, in silent installation.

After installation, perform the tasks described in "2.3.4 Construct an iOS Management Database" and later sections.

2.3.2.4 Register the license key

If you already have a license key, register it using the license key input command after the product is installed. This will make you an official user of the product. Official use of the product will start once you start it after becoming an official user.

If you are not yet an official user of the product, you will not be able to start the product.

The license key is registered using the fjlic register command (license key input command). The command can be executed either by specifying the license key in the parameter directly or by specifying the license key file. Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on the command.

- Specifying the license key in the fjlic register command directly

```
fjlic.exe register -k <license key>
```

- Specifying the license key file in which the license key is stored in the fjlic register command

```
fjlic.exe register -f <license key file full path>
```

2.3.3 Construct Database

This section describes how to construct Systemwalker Desktop Patrol database.

Note

When constructing the database, pay attention to the following restrictions and notes

[About the Database Creation Target]

- Do not set compression and encryption for the drive and folder for constructing the database.

- If the Systemwalker Centric Manager database has already been constructed, specify a different database directory to the Systemwalker Centric Manager database.

[About the User for Constructing the Database]

For the logon user name of Windows, specify within 18 characters, which has Administrator authority and begins with English letters. Do not delete the Windows logon user for constructing database. After installation, when executing the operating environment extension, SWDTP_dbbk.exe (DTP data backup) command, SWDTP_dbrs.exe (DTP data restoration) command, dtplook.exe (log collection) command and dtpctlusr.exe (standard database user modification) command, Windows logon user for constructing operating environment or Windows logon user added through dtpctlusr.exe (standard database user modification) command is required.

Upgrading from V11.0L10 or earlier

If a database (SQL Server/Oracle) used in V11.0L10 or earlier has not been started, or is being started, the number of PCs may fail to be retrieved.
Wait a few moments, and re-execute after the old database (SQL Server/Oracle) is started.

Database capacity

Refer to "Required Hardware" in the *Systemwalker Desktop Patrol User's Guide* for details on a rough estimate of the database capacity.

The procedures for constructing Systemwalker Desktop Patrol database are as follows:

If executing custom installation, then execute from step 3.

1. Log on to Windows with the user that belongs to the Administrators group and the user that belongs to the Administrators group of domain or Domain Admins group in local computer.

2. If you are using other applications, close them.

3. Select **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Operation Environment Maintenance Guide**, or **Apps** > **Systemwalker Desktop Patrol** > **Operation Environment Maintenance Guide**.

4. The **Operation Environment Maintenance Wizard** window is displayed. Click the **Next** button.
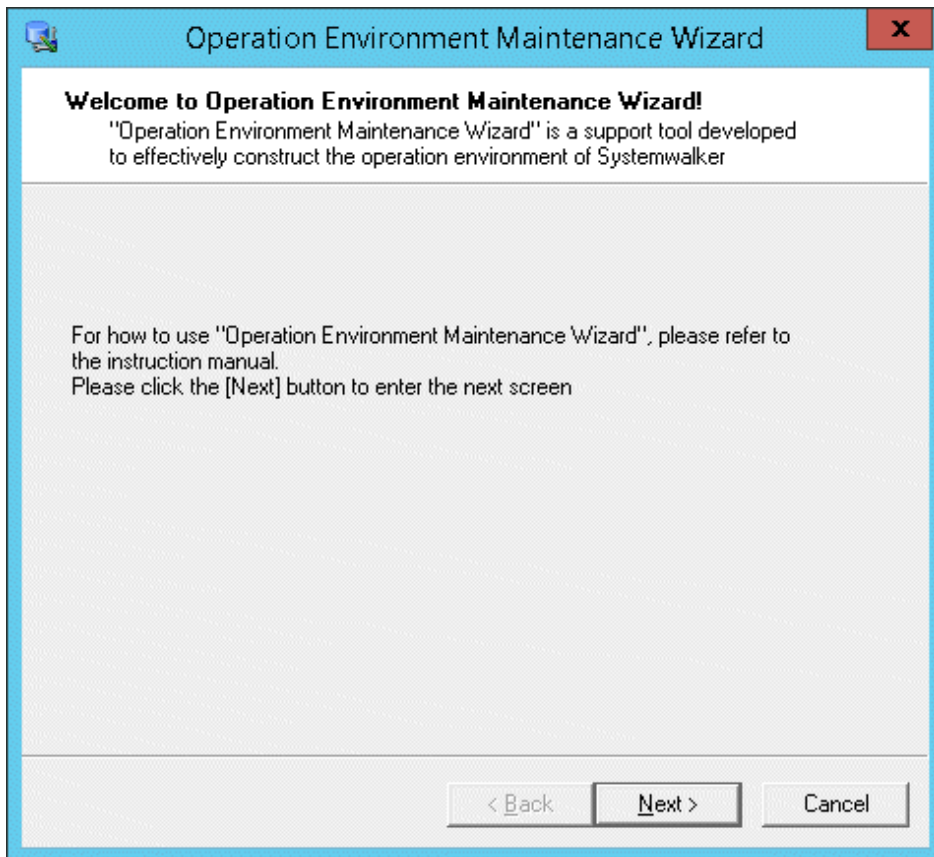
5. The **Select Process** window is displayed. Set **Operation** and click the **Next** button.

Here, select **Construction of Operation Environment** in **Operation**.
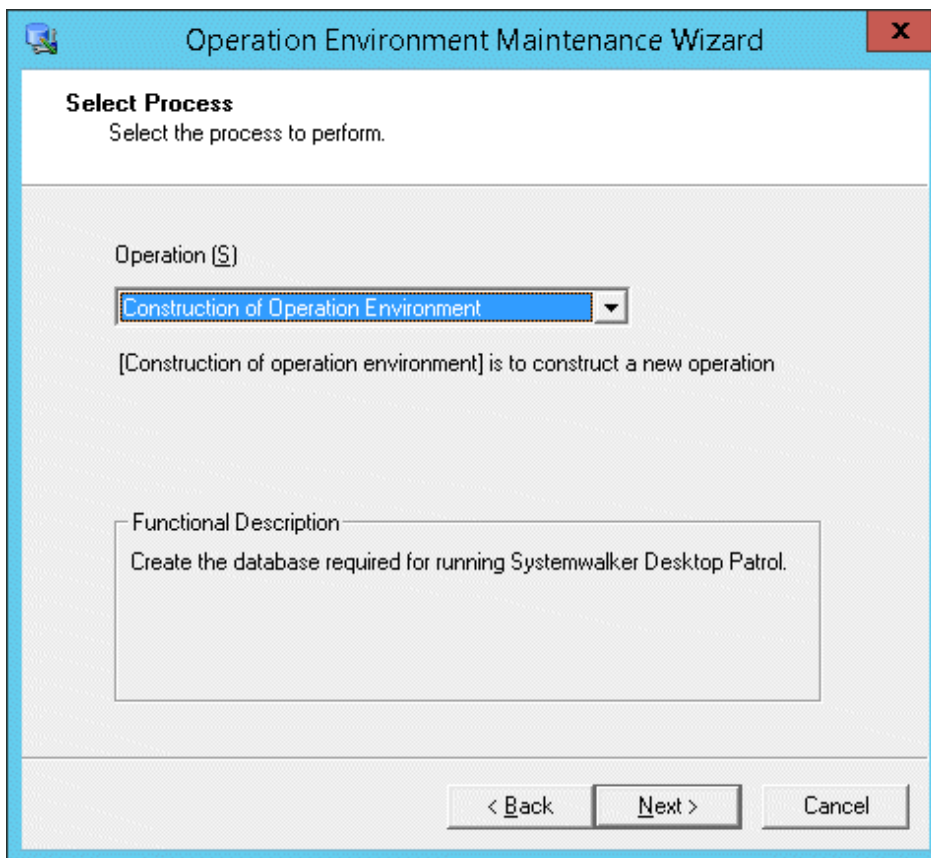
6. The **Register the system account** window is displayed, input system account information and click the **Next** button.

Item	Description
User ID	Single-byte alphanumeric characters within 4-20 characters and the following single-byte symbols. Besides, it is case sensitive for English alphabets. "-", "@", ".", "_"
Password	Single-byte alphanumeric characters within 4-12 characters, single-byte space and the following single-byte symbols. Besides, it is case sensitive for English letters. "-", "=", "*", "+", """, "@", "~", "(", ")", "&", "$", "#", "'", "!", "?", "%", "\", ".", ",", "/", ":", ";", "`", "[", "]", "|", "<", ">", "{", "_", "}"
Confirm Password	Enter the password set above for confirmation.

The system account registered here is the one for operating the main menu.

For system account, refer to the instructions in "Authority for Operation" of *Systemwalker Desktop Patrol Operation Guide: for Administrators*.

7. The **Enter database information** window is displayed. Set **Database Storage Location** and **Database Settings**.

Item	Description
Database Storage Location	Path name of 64 characters at most can be specified in the database saving target. You cannot specify fullwidth characters, halfwidth spaces, tabs, and the following symbols: , ; ' # If the directory name specified in the database saving target is different from "DESKTOPPATROL_DBSP", "DESKTOPPATROL_DBSP" directory will be automatically created under the specified directory, and the database will be saved in it.
Number of PC(s)	Select the correspondent number of PC(s). When specifying an arbitrary number, enter within 100-100,000. For the standard of database capacity, refer to "Hardware" of *Systemwalker Desktop Patrol User's Guide*. ![Note icon] **Note** . . . . **Number of PC**(s) **is a standard of number of PC**(s) **that can be managed** **Number of PC(s)** is a standard of the number of PC(s) that can be managed in Systemwalker Desktop Patrol. According to the situation, it might be smaller than the specified number of PC(s). At this time, the capacity of Systemwalker standard database can be extended by performing "Extend Operation Environment". . . . .

Item	Description
	🅿 Point . . . . **About version upgrade from V11.0L10** When performing version upgrade from V11.0L10, the approximate number in use currently will be displayed in number of PC(s). Modify the number of PC(s) as required. . . . .
Number of smart device(s)	Specify the estimated number of smart devices to be managed by Systemwalker Desktop Patrol. You can specify a number from 0 to 100000.
Number of managed non-PC(s)	Set the devices (devices) managed in Systemwalker Desktop Patrol. Number within 0-100000 can be set.

8. To perform **Collection of EXE Information** and **Collection of Software Operation Information or Control of Execution File**, click the **Detailed Settings** button. Access the next procedure if not to set.
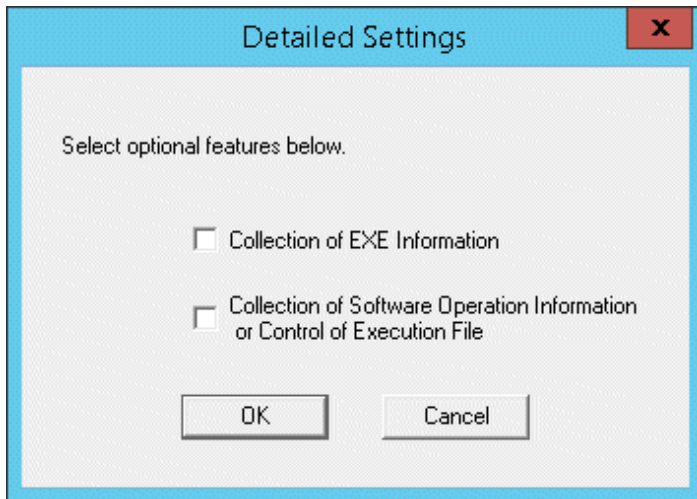
Select the collected information and click the **OK** button.

9. Click the **Next** button, the **Confirmation of Settings** window is displayed, confirm whether the content displayed in the confirmation window is correct, and click the **Next** button.

Display the **Execute Processing** window and start to create the database.

Besides, if **Cancel** is clicked to interrupt **Construct Operation Environment**, the interrupted **Construct Operation Environment** can be restarted by executing again **Operation Environment Maintenance Guide**.
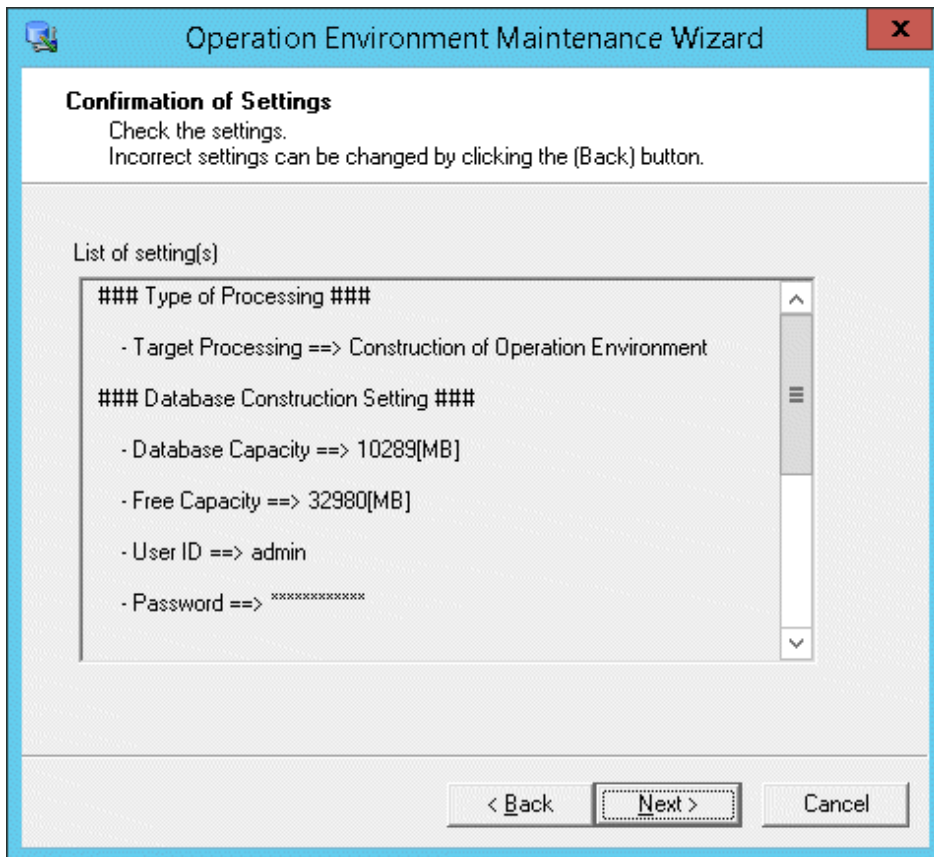
10. The **Process Competed** window is displayed after the processing has been completed normally. Click the **Finish** button.

2.3.4 Construct an iOS Management Database

Constructing an iOS management database

To manage iOS devices, an iOS management database must be constructed using swss_MDMDB_ENV.exe (constructing/deleting iOS management database environment command) with the /C option.

If managing iOS devices in both Systemwalker Desktop Patrol and Systemwalker Desktop Keeper, the constructing/deleting iOS management database environment command for both products must be executed.

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on swss_MDMDB_ENV.exe.

The building iOS management database environment command will set the port in which the iOS management database waits with the initial value (55432). If this value needs to be modified, refer to "How to Modify the Port Number" in the *Systemwalker Desktop Patrol Reference Manual*.

🛠 Note
．．

If the operating system is to be restarted after an iOS management database is constructed, the PostgreSQL_swdtmdm service must be stopped first. Open the Windows **Services** window, select the **PostgreSQL_swdtmdm** service, and click **Action** > **Stop**.

If the operating system is restarted before stopping the service, the following message may be output to the event log.

ERROR: canceling statement due to user request

This is a message displayed when the operating system stops the service, and does not cause any problem to the operation.
．．

Deleting an iOS management database

To stop managing iOS devices, the iOS management database can be deleted with the following procedure:

1. On the SS, use SWDTP_ctrl.exe (batch starting/stopping services) to stop the SS services.

2. On the SS, use swss_config.exe (SS environment setup command) with the /iOS.enabled:false option to disable iOS device management.

3. On the CS, use swss_MDMDB_ENV.exe (constructing/deleting iOS management database environment command) with the /D option to delete the iOS management database.

4. On the SS, use SWDTP_ctrl.exe (batch starting/stopping services) to start the SS services.

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on swss_config.exe and swss_MDMDB_ENV.exe.

> 📝 **Note**
> ....
>
> - If Systemwalker Desktop Patrol and Systemwalker Desktop Keeper coexist and iOS device management is to be stopped in both, then the deleting iOS management database environment command must be executed in both products.
>
> - If Systemwalker Desktop Patrol and Systemwalker Desktop Keeper coexist and iOS devices are managed by both products, they can be changed to be managed by one product only. Follow the steps below to delete the iOS management database no longer managed.
>
>   1. Use swss_config.exe (SS environment setup command) to check the host name of the iOS management database connected with SS. Perform backup on the server that matches the iOS management database host name displayed in "iOSmgr.host".
>
>   2. Execute the deleting iOS management database environment command in both products.
>
>   3. Execute the building iOS management database environment command in the product that manages iOS devices.
>
>   4. In the iOS management database constructed in step 3, restore the data backed up in step 1.
> ....

2.3.5 Set CS Operating Environment

This section describes how to set CS operating environment.

2.3.5.1 Set the Saving Target of CT Operation Status Log

CT operation status log collected in CT is saved in CS.

To reduce the disk consumption, the saving target folder of CT operation status log will be performed the compressed folder settings automatically at CS installation.

The default settings of CT operation status log saving target of CS are as follows:

```
Desktop Patrol CS Installation Directory\FJSVsbinv\ct_trace
```

And for saving CT operation status log, the following disk capacity is required.

```
Size of CT Operation Status Log = 30KB * Number of Users * Number of days to save (Default: 30 Days)
```

The saving target of this CT operation status log can be modified by using SVPolicy.exe (server environment setup) command.

For command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

To modify the saving target, set the compressed folder as follows.

1. Start the command prompt.

2. Start the following command.
   compact.exe /c /s:<Saving Folder of CT Operation Status Log>

2.3.5.2 Set CS Operation Log Collection

This section describes how to set CS operation log collection.

Refer to "CS Operation Log File" and "CS Operation Details Log File" in the *Systemwalker Desktop Patrol Reference Manual* for details on output log format.

Edit the definition file

When modifying the number of days to save and the output target for the log, edit the following definition file of CS.

- Saving target: DTP Installation Directory\common\etc

- Definition file name: dtpaudit

Field/Key Name	Description	Configuration Value
AUDIT	Field name	-
FUNCTION	Enable/disable CS operation log collection	Set either of the following. 0: collect 1: not collect (default)
FUNCTION_DETAIL	Enable/disable CS operation details log collection	Specify one of the following: 0: Do not collect 1: Collect (default value)
DATE	Number of days to save for the log	Set the following numbers. Default value: 30. 0: no limit for number of days 1-366: number of days When a value out of the range of 1-366 has been set, it will be the default value (30). *When updating the log file, log file in those days before the specified number of days, so delete the unnecessary log file manually. *After the number of days to save has been modified, logs before the number of days to save might be collected when collecting logs before updating log files. *If 0 is specified, log file will increase infinitely, delete unnecessary log file regularly.
PATH	Log output target	Specify the log output folder with an absolute path using up to 100 fullwidth characters or 200 halfwidth characters. If not specified, the default is the folder under CS. DTP Installation Directory\common\dtpaudit *When an invalid path has been specified, it will be output to the default folder. *When the capacity of log output target folder is insufficient, auditing log cannot be output.

Example for recording the definition file:

```
[AUDIT]
FUNCTION=1
FUNCTION_DETAIL=1
DATE=30
PATH=D:\auditlog
```

2.3.5.3 Set Server Information

The following content can be set as server information.

- Modify server name

  "CS Name" set here will be used in the following window.

  - **CS Name** of **Environment Setup** > **CS/DS Settings and Status** of the main menu

  - **CS Name** of **CT Downloading** of the download menu

The procedure is as follows.

1. Enter the following URL in the **Address** bar of Web Browser.

```
http://Server Information (FQDN Name or Host Name or IP Address of CS)/DTP/index.html
```

   The logon window is displayed.
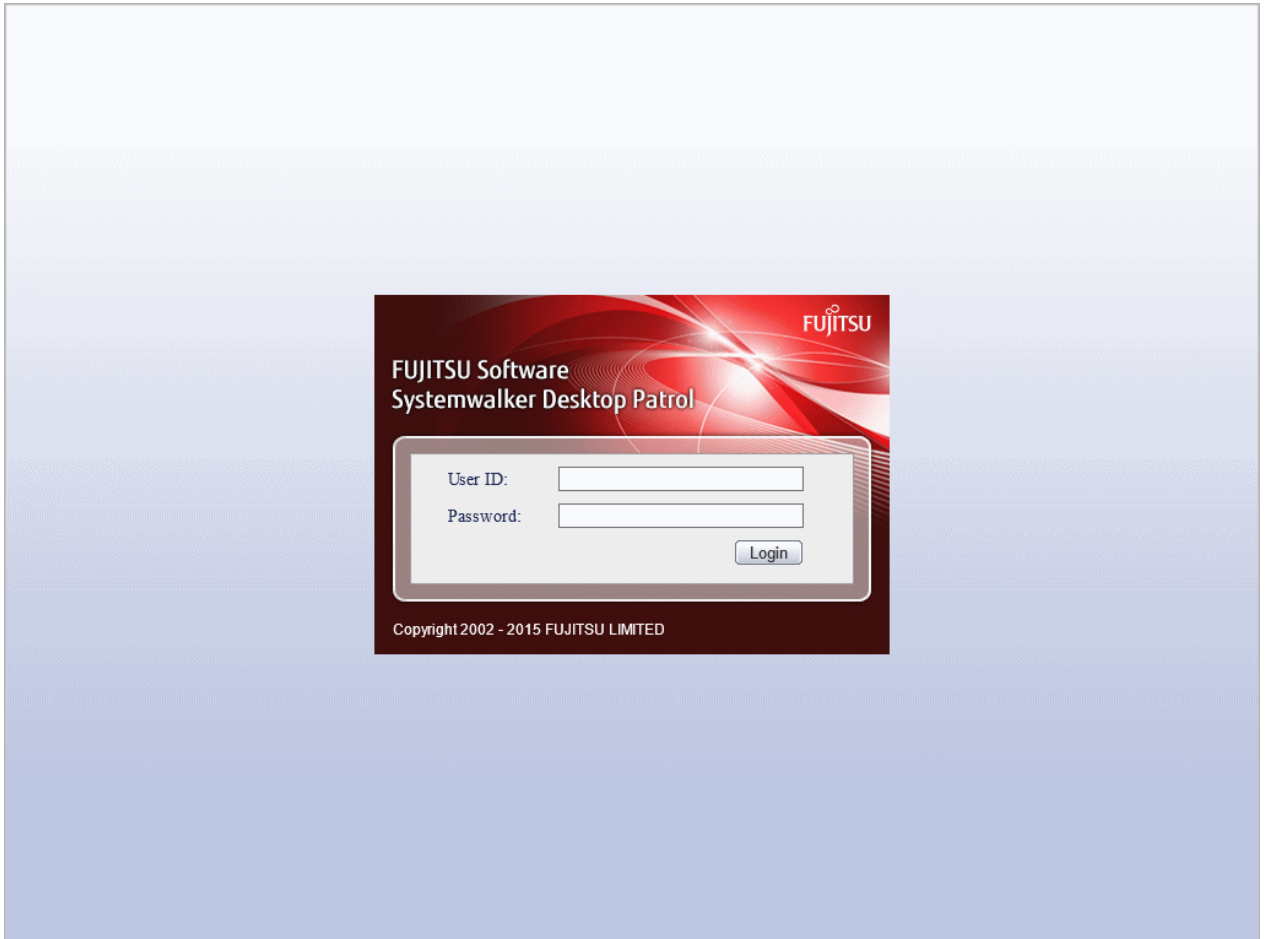
2. Enter the following information, and click the **Login** button.

   - **User ID** textbox

   - **Password** textbox

   The main menu is displayed.
   If standard installation was performed, the initial value for both user ID and password is "systemadmin". Refer to "2.3.2.1 Standard Installation" for details.

   After the initial login, the password must be changed.

If custom installation was performed, the value specified in step 5 of "2.3.3 Construct Database" will be used.

The server information can also be set using the user ID of the system account in which the master data was registered after installation.

3. Click **Environment Setup**.

   The **Environment Setup** window is displayed.

4. Click **CS/DS Settings and Status.**

   The following window is displayed.

5. Click the link of CS/DS Name.

The following window is displayed.

6. Set the following item.

Item	Content
CS Name	Display the common name of CS to be installed.
	Specify CS name as characters within 50 characters included single-byte alphanumeric characters and special characters "-", "@", ".". Blank cannot be specified.
	Cannot be omitted.

7. Click the **OK** button.

2.3.5.4 Transmission Settings

This section describes the settings performed when transmitting information from Systemwalker Desktop Patrol CS to downstream server or Systemwalker Desktop Patrol CT.

The transmitted information contains the following.

- Registered Software

- Security Patches

- Client Policy/Server Properties

And as transmission settings, the following item can be set.

- Number of simultaneously connected devices

The procedure is as follows.

1. Log on to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **CS/DS Settings and Status**.

   The following window is displayed.

3. Click the link of the CS/DS name.

   The following window is displayed.

4. Enter the following item from the communication settings of the downstream DS/Client.

Item	Content
Maximum number of connections(1-999)	Specify the total number of downstream DS/CT communicating simultaneously with CS/DS within 1-999.
	Default: 30, cannot be omitted.
	Set the following values according to the total number of the actually connected downstream server and client.
	1000 or less: 30
	2000 or less: 40
	2000 above: 50

5. Click the **OK** button.

2.3.5.5 Set Proxy

Proxy can be used when communicating with the public server of Microsoft Company.

 Note

About proxy settings

[Proxy Server and Setting Conditions Not Allowed]

The following proxy server is not allowed.

- Software of other companies WEBGUARDIAN

And if the following settings have been performed, the proxy server cannot be used.

- Windows authentication has been enabled in ISA Server

Proxy can be used when security patches are acquired from Microsoft Company to CS.

The procedure is as follows.

1. Log on to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **CS/DS Settings and Status**.

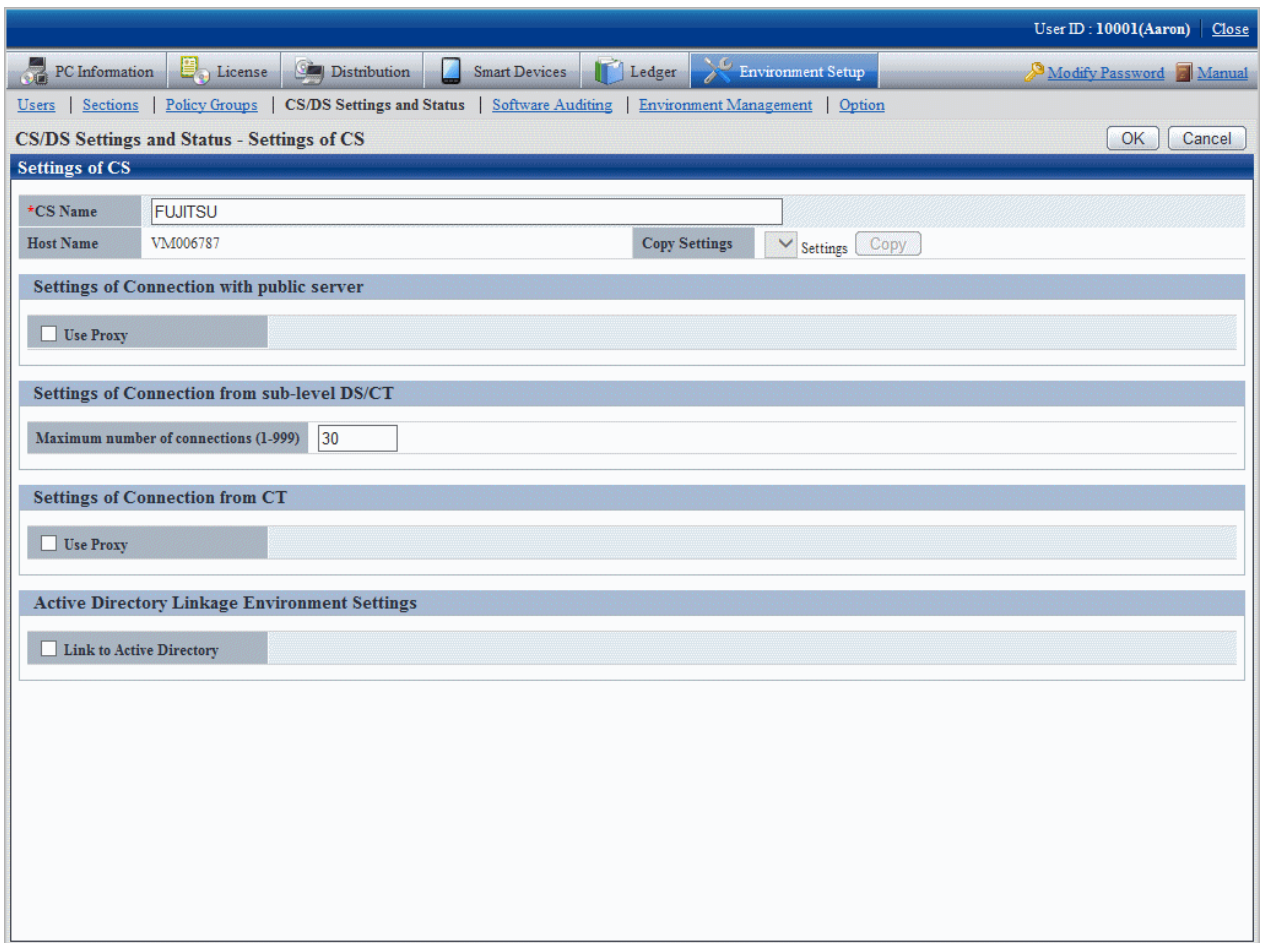   The following window is displayed.

3. Click the link of CS/DS.Name

The following window is displayed.

4. Enter items of **Settings of Connection with public server**.

Item	Content

Use Proxy	Selected when using proxy.
	
	The following items can be specified when using proxy.
	
	  - **Proxy Server Name**
	
	    Specify the name of proxy server.
	
	    Specify FQDN or IP address with single-byte alphanumeric characters within 64 characters, "-" and ".".
	
	    Note
	    ·
	    Communication in IPv6 environments
	
	    IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name:
	
	      - Register the CS and DS host name and IP address in the DNS server.
	
	      - Register the CS and DS host name and IP address in the communication source PC hosts file.
	    ·
	
	  - **Port Number**
	
	    Specify the port number for proxy server.

Item	Content
	Specify a number within 1-65535. Cannot be omitted. - **User Name** Specify the user name of proxy server within 256 halfwidth characters. - **Password** Specify the password of proxy server within 256 halfwidth characters. - **Bypass proxy server for these domains (Use a blank to specify multiple domain names)** Specify the domain name not using proxy server. When specifying multiple domain names, separate them with space. Specify within 2064 halfwidth characters. Specify the domain name with single-byte alphanumeric characters, "-" and ".".

5. Enter the following items from **Settings of Connection from CT**.

Item	Content
Use Proxy	Selected when using proxy. The following item can be specified when using proxy. - **Proxy Server Name** Specify the name of proxy server.

Item	Content
	Specify FQDN or IP address with single-byte alphanumeric characters within 64 characters, "-" and ".". Cannot be omitted. - **Port Number** Specify the port number for proxy server. Specify a number within 1-65535. **Note** . . . . **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name: - Register the CS and DS host name and IP address. - Register the CS and DS host name and IP address in the communication source PC hosts file. . . . . - **User Name** Specify the user name of proxy server within 256 halfwidth characters. - **Password** Specify the password of proxy server within 256 halfwidth characters. - **Bypass proxy server for these domains (Use a blank to specify multiple domain names)** Specify the domain name not using proxy server. When specifying multiple domain names, separate them with space. Specify within 2064 halfwidth characters. Specify the domain name with single-byte alphanumeric characters, "-" and ".".

When the proxy server name cannot be analyzed through the PC that connect to the proxy server, set IP address of proxy server in **Proxy Server Name**.

6. Click the **OK** button.

2.3.5.6 Software Dictionary Update

Software dictionary update

A Software Dictionary will be sent from the Systemwalker Support Center to the administrator by E-mail.

To receive a Software Dictionary from the Systemwalker Support Center, select Registration.text in Systemwalker Desktop Patrol CD-ROM\Utilities\Supportcenter folder, and then apply to receive the Software Dictionary through the Systemwalker Support Center service.

To update the Software Dictionary:

1. Store Software Dictionary attached to the E-mail in an appropriate file on the PC that contains Systemwalker Desktop Patrol CS. For example, suppose that the Software Dictionary is stored in "c:\tmp".

2. Execute the command below following the command prompt. Specify a folder that contains "Software Dictionary" in the parameter.

```
DTP Installation Directory\FJSVsbtrs\bin\AtoolETPGT.exe C:\tmp
```

Set auditing software

The auditing software should be selected when starting to use according to the Support Center definition.

For how to select, refer to *Systemwalker Desktop Patrol Operation Guide: for Administrators*.

2.3.5.7 Perform the Settings of Linking with Active Directory

When applying the linkage with Active Directory, set the operation environment according to one of the following procedures.

Besides, in case of changing from the environment of linking with Active Directory to the one of not linking with Active Directory, to change the operating environment, the settings should be performed according to one of the following procedures as well.

- Settings procedure using the command
- Settings procedure using the main menu

Settings procedure using the command

Follow the steps below in CS.

1. Use dtpadset.exe (Active Directory linkage environment setup) command to set or change the linkage environment with Active Directory.

   For dtpadset.exe (Active Directory linkage environment setup) command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

Settings procedure using the main menu

Follow the steps below:

1. Log in to the main menu and click **Environment Setup**.

   The **Environment Setup** window will be displayed.

2. Click **CS/DS Settings and Status**.

The window below will be displayed.

3. Click the link for the server name whose server type is CS.

   The window below will be displayed.

4. Select **Link to Active Directory** and enter the appropriate fields.

   The window below will be displayed.

Alternatively, to change to an environment not linking to Active Directory, clear **Link to Active Directory**.
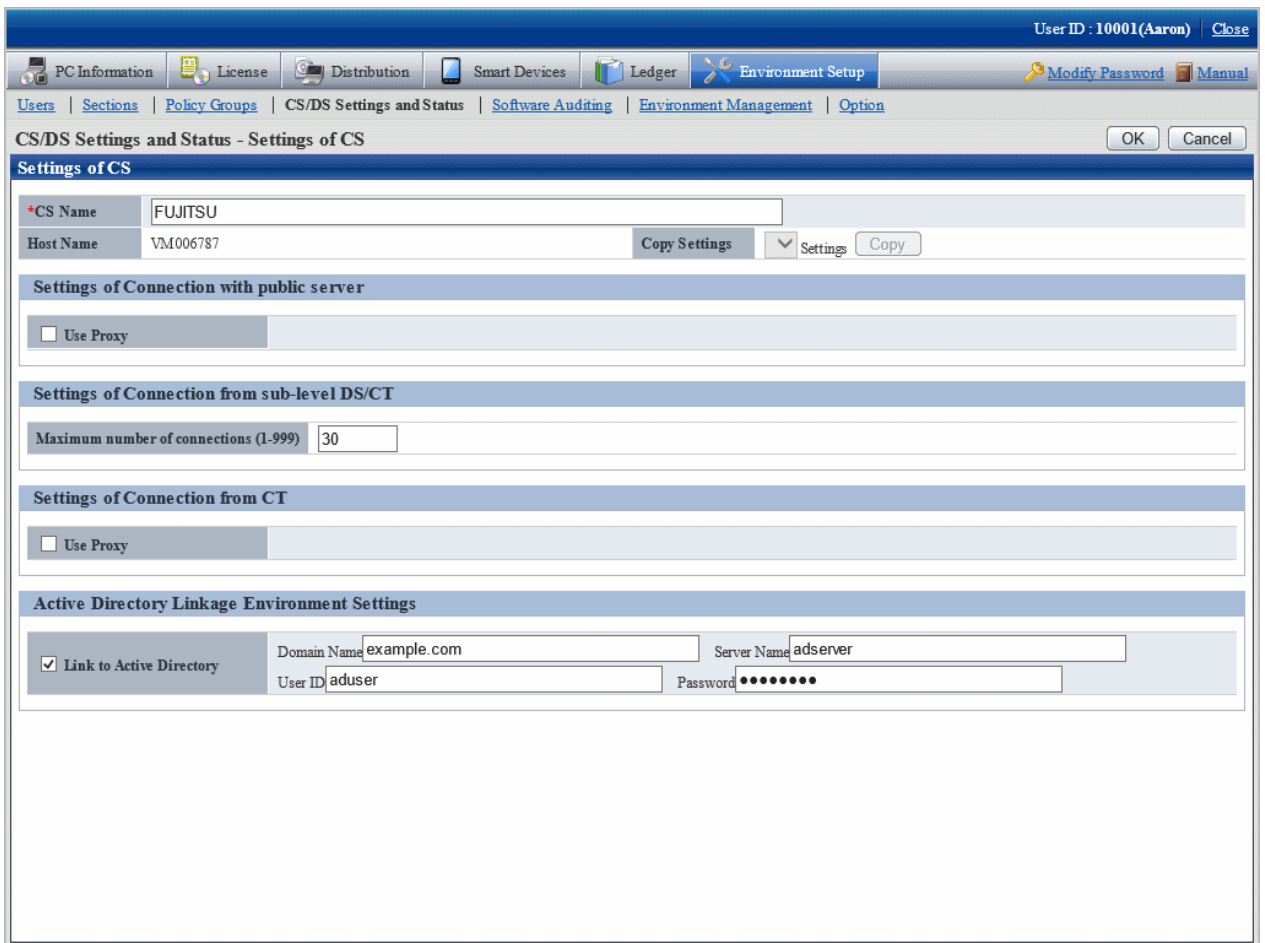
5. Configure the settings for the following items:

Item	Description
Domain Name	Domain name for the Active Directory domain server.
	Specify the domain name using 4 to 36 halfwidth alphanumeric characters, and the following halfwidth symbols: . - _
	This item is required.
Server Name	Name of the Active Directory server connection target.
	Specify up to 128 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - = * + ' @ ~ ( ) & $ # " ! ? % \ . , / : ; ` [ ]	< > { _ }
	Halfwidth spaces at the beginning and end of the value will be ignored.
	This item is required.
User ID	User ID of the administrator of the Active Directory server connection target.
	Specify up to 128 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - = * + ' @ ~ ( ) & $ # " ! ? % \ . , / : ; ` [ ]	< > { _ }
	Halfwidth spaces at the beginning and end of the value will be ignored.
	This item is required.
Password	Login of the administrator of the Active Directory server connection target.
	Specify up to 128 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - = * + ' @ ~ ( ) & $ # " ! ? % \ . , / : ; ` [ ]	< > { _ }

Item	Description
	This item is required.

6. Click **OK**.

P Point

. . . .

When setting as the environment of linking with Active Directory, but in the information of CT **User Identification Information** tab, by using the timing for logging on to Windows domain again, the following values are set automatically only during the first logon.

- **User ID**: logon name of Windows domain

- **PC name**: computer name

. . . .

Timing for automatically setting user ID and PC name is as follows:

- When performing Active Directory Linkage after the environment construction

  Timing for first logon to Windows after distributing the policy with Active Directory linkage set to CT and DS

- When performing Active Directory Linkage in case the environment construction has not been performed

  Timing for first logon to Windows after CT and DS are installed

Automatic settings of user ID and PC name are only for the time above during the first logon.

2.3.5.8 Customize the Environment Setup Window of CT

The administrator can set the **Environment Setup** window of CT collectively as follows.

- Message displayed to user

  Information required for environment setup can be set as message.

- Limit as not being able to modify client settings

  Set as not being able to modify user ID and PC name after installation.
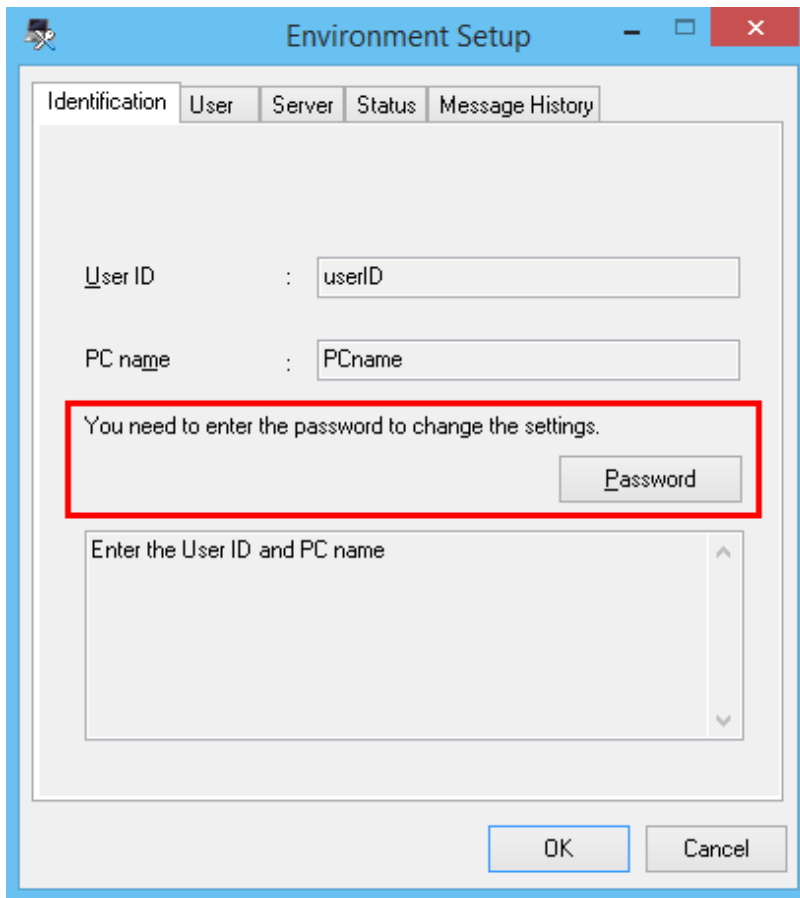
- Prompt to modify the settings if the environment is changed

  Message prompting the modifications can be displayed to PC user when the environment setup (user identification information and user information) need to be modified.
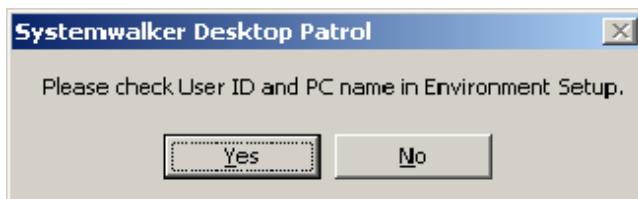
The procedure is as follows.

1. Log on to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **Policy Groups**

The following window is displayed.

3. Click the **Customize Various Policies** button.

The following window is displayed.

4. Click the **Basic Operation Policy** tab.

Click the link of policy name, and the following window is displayed.

5. Click **CT Environment Setup** of the **Common Settings** tab, the following item will be displayed.

Enter the following item.

Operations during CT installation

Item	Content
Set the initial value	Select **Yes** if you hope to set the initial value as operation during CT installation. Specify user ID/PC name. Select one of user ID/PC name as the item for initial value setting. - **User ID** Selected when to set initial value for user ID. - **Login user ID** Set the logon user ID of Windows. - **As Specified Bits of 9** Fill the digit specified in "Digit" with 9 from the beginning. - **PC Name** Selected when to set initial value for PC name. - **Computer Name** Set the computer name. If the computer name has exceeded 20 characters, characters following the 20th character will be deleted.

Item	Content
	- **IP Address**
	Note
	· ·
	If there is no IPv4 address, no value will be set for the PC name.
	· ·
	- **As Specified Bits of A**
	Fill the digit specified in "Digit" with A from the beginning.
	- **Serial NO**
	Set the serial number.
	- **Domain Name**
	Set the domain name.
	- **Specify the beginning character for PC Name**
	The beginning character of PC name can be specified after being selected. Specify with alphanumeric characters within 10 characters. The characters specified here will be added as the beginning character of PC name.
	If selected, cannot be omitted.
	If "Beginning Character of PC Name + PC Name" has exceeded 20 characters, the characters following the 20th character of the initial PC name displayed in the CT environment setup window will be deleted.
	When selecting the beginning character and "As Specified Bits of 9", the format will be "Beginning Character+AAAAAAAAA". The part in total exceeding 20 characters will be deleted.

Actions during CT installation and settings after installation

Item	Content
Modification restricted	Selected when to restrict modifying CT environment setup.
	- **User ID**
	Selected when modifying user ID is not allowed.
	- **PC Name**
	Selected when modifying PC name is not allowed.
	- **Allow CT to change User ID and PC Name by specifying the password**
	Selected when it is allowed to modify environment information through the password. Specify the password in **Password** and **Confirm the Entered Password**. Specify the password using 6 to 32 halfwidth alphanumeric characters.
	If selected, it cannot be omitted.
The Environment Setup window is displayed only once during login	Selected when it is required to enter the CT environment setup window.
	To display message in CT, the message should be specified using 2048 fullwidth characters or 4096 halfwidth characters. The following message will appear if omitted.
	"Confirm 'User ID' and 'PC Name' of 'Environment Setup'."
	When it is required to update the message and enter again, click the **Display again** button.

Display information

Item	Content
Display Message	Selected when displaying message in the **User Identification Information** tab of the CT environment setup window. Specify the message displayed in CT using up to 2048 fullwidth characters or 4096 halfwidth characters. The message body cannot be omitted.

6. Confirm the settings and click the **Apply** button.

    Set the set assets management information.

7. To cancel, click the **Logout** button to log out from the main menu.

Point

About the user ID and PC name of CT installed in the virtual desktop environment

In the virtual desktop environment, desktop mapping (virtual PC) is copied through system mapping.

The user identification information (user ID and PC name) of the system mapping cannot be inherited in this copied virtual PC, Systemwalker Desktop Patrol will initialize the user identification information and reset automatically after detecting the copy of system mapping.

To automatically reset this user identification information, set the policy through the main menu according to the following procedures.

1. In **Environment Setup** > **Policy Groups** > **Basic operation policy** > **CT environment setup** of the main menu, set **Set the initial value** as **Yes** and select **User ID** and **PC Name**, select the item from the drop-down menu.

2. Create policy group through **Policy Groups** and register **Basic operation policy** and PC created in Procedure 1.

3. Download CT Package from the download menu to install CT.

Note

- When getting the initial value of user ID and PC name, it will become the following action. Try using the initial value to make the combination of user ID and PC name different from other PC.

    - When characters not allowed are contained in the user ID and PC name, this character will be replaced as "." (period).

    - When the upper limit (20 characters) for characters of user ID and PC name has been exceeded, the exceeding part will be deleted.

- When failing to get the initial value of PC name, perform the following action.

    - Get "Computer Name" if getting "Domain Name" failed.

2.3.5.9 Set Client Prohibition

This section describes how to set client prohibition.

How to set prohibition function

Client prohibition function is disabled by default.

The procedure of setting is as follows.

1. Execute the (client environment setup) command in Systemwalker Desktop Patrol CS CTPolicy.exe.

2. Systemwalker Desktop Patrol CT will activate the settings after receiving the policy.

For command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

When disabling the prohibition function temporarily

To disable client prohibition function temporarily in the maintenance and so on operations of Systemwalker Desktop Patrol CT, perform the following operation.

1. Execute the Control.exe (disable client prohibition function) command in Systemwalker Desktop Patrol CT.

2. Stop CT service, uninstall CT or modify the connection server of CT.

3. Systemwalker Desktop Patrol CT will enable the client prohibition function again after receiving the policy.

For command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

2.3.5.10 Set Automatic Detection Schedule (Create ADT Module)

ADT collects the device information within the network segment, and notifies the collected device information to CS.

This section describes how to set the schedule of notifying device information automatically detected in ADT.

Besides, if ADT function will not be used,, no need to perform the settings.

The procedures for setting automatic detection schedule are as follows:

1. Click **Start** > **Programs** (or **All Programs**) > **Systemwalker Desktop Patrol** > **Environment Setup** > **Scheduling of Automatic Detection**. Alternatively, select **Apps** > **Systemwalker Desktop Patrol** > **Environment Setup** > **Scheduling of Automatic Detection** in PC with CS installed.

   The **Schedule Setup of Auto Detection** window is displayed.

   Enter the following information and click the **Create** button.

- **Setup of Detection to Segment** tab

Item		Description
On Demand Device Information Notification		Selected when not using Scheduler to modify the device information detected through ADT.
Scheduled Device Information Notification		Selected when using Scheduler to modify the device information detected through ADT.
Notification Target Settings	**Connect Server**	📋 **Note** ••• **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name:

Item		Description
		- Register the CS and DS host name and IP address.
		- Register the CS and DS host name and IP address in the communication source PC hosts file.
		. . . .
	Port Number	Set the port number for notification target. Set in case it is not the initial value port 80.
	Set(S)	Used when setting proxy.
Collect Devices Not Registered in Ledger (Detailed Collection)		Select this option to perform automatic detection and information collection of devices for maintaining the management ledger.
		This option cannot be selected if **Collect Devices Connected to without Permission (Simple Collection)** is selected.
Scheduler Setting	Daily	Selected when notifying the device information every day.
	Weekly	Selected when notifying the device information weekly. Set as that Monday to Sunday can be selected.
	Monthly	Selected when notifying the device information monthly. Select the execution date in **Execution Date**.
		Besides, as **Execution Date**, if the date not existing in the set month has been specified, automatic detection cannot be performed in this month. Thus, to execute at the end of a month, consider executing at 00:00 on the first day of the month.
	Start Time	Set the time for starting to notify the device information.
		When using ADT module on server PC which does not operate around the clock, if time late at night has been set, then the power for PC performing automatic detection might be cut off, so pay attention to the time settings.
Collect Devices Connected to without Permission (Simple Collection)		Select this option to perform automatic detection and information collection of devices connected to without permission.
		This option cannot be selected if **Collect Devices Not Registered in Ledger (Detailed Collection)** is selected.
	Collection interval	Specify the interval for collecting device information when detecting devices connected to without permission. Device information will be repeatedly collected at this interval.
		Select one of the following intervals:
		- **30 minutes**
		- **1 hour**
		- **2 hours**
		- **6 hours**
Creation Status of ADT Module		Display the creating status of ADT module.
		If ADT module has been created, the following message will appear.
		MM/DD/YYYY hh:mm:ss.
	Create	Create ADT module.

Besides, if ADT module has not be started in the set aggregating timing (due to PC power not switched on, etc.), the device information will be notified at the start time for scheduler settings after ADT module is started.

When connecting Systemwalker Desktop Patrol CS by using proxy, click the **Set** button of connection target server to set the connection information for proxy.

The following window is displayed.

Item		Description
Use Proxy in the Communication with Connection Target Server		Selected when notifying the device information detected by ADT via proxy.
Set Proxy	**Proxy Server**	**Note** **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand one of the following patterns, and then enter the host name: - Register the proxy server host name and IP address in the DNS server. - Register the proxy server host name and IP address in the communication source PC hosts file.
	Port Number	Set proxy server user port number. The initial value is 8080. Set a value within 1-65536.
	Proxy User ID	Set the user ID for proxy.
	Proxy Password	Set the password for proxy.

Click the **Apply** button and create "ADT Module" in the following location.

[Save Directory]

<*IIS Home Directory*>\wwwroot\DTP\ADT

[File Name]

ADTSetup.exe

- **Setup of Collective Detection** tab
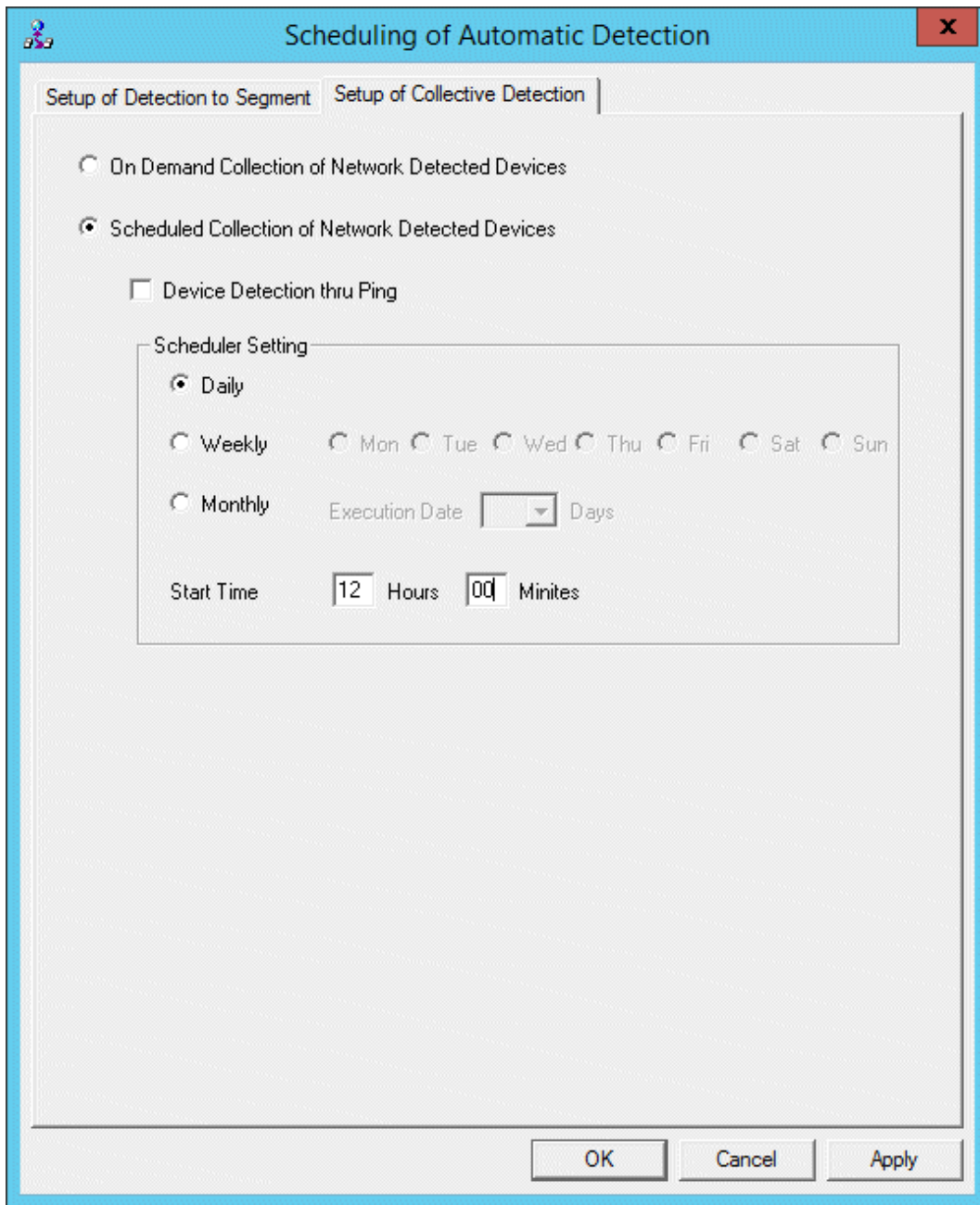
Item		Description
On Demand Collection of Network Detected Devices		Selected when not performing Batch Network Check by schedule.
Scheduled Collection of Network Detected Devices		Selected when performing Batch Network Check by schedule.
Device Detection thru Ping		Selected when the devices only responding to Ping are detected as unregistered ones.
		If selected, devices which cannot get MAC address will also be output to the **List of Unregistered Devices** window.
Scheduler Setting	**Daily**	Selected when notifying the device information every day.

Item		Description
	Weekly	Selected when notifying the device information weekly. Set as that Monday to Sunday can be selected through option button.
	Monthly	Selected when notifying the device information monthly. Select the execution date in **Execution Date**. Besides, as **Execution Date**, if the date not existing in the set month has been specified, automatic detection cannot be performed in this month. Thus, to execute at the end of a month, study the execution use at 00:00 on the first day of the month. When selecting **Monthly**, the initial value is **1 Day** and the start time is the current time.
	Start Time	Set the time for starting to collectively detect device information.

2. Click the **OK** button to restart the system. The settings will take effect after starting the system next time.

2.4 Construct DS

In Systemwalker Desktop Patrol, due to higher server and network load resulting from collection and distribution such as PC information collection, management and software distribution, etc., construct Systemwalker Desktop Patrol DS to reduce the load.

2.4.1 Install DS

This section describes how to install DS.

After installing Systemwalker Desktop Patrol DS, Systemwalker Desktop Patrol CT can be installed at the same time. And it can manage as other CTs do.

CT function of DS cannot be uninstalled alone.

Systemwalker Desktop Patrol DS is installed after the installation of Systemwalker Desktop Patrol CS is completed and the environment has been constructed.

There are two ways to install DS:

- 2.4.1.1 Installation using the Wizard

- 2.4.1.2 Silent Installation

 Note

CT registration password

- To use a CT registration password, ensure that the server administrator uses CustomPolicy.exe (policy for modifying custom setup command) to enable it. CT registration passwords can be set per target server (CS and DS). Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on the command.

  It is recommended to change the CT registration password using CustomPolicy.exe (policy for modifying custom setup command) once the CT is extracted.

- If a CT registration password is enabled, it must be set on the CT.

Issues to be confirmed before installation

- End the following programs after the installation is completed.

  - Resident programs containing virus scanning program.

  - The **Service** window of Windows.

- By referring to "List of Port Numbers" of *Systemwalker Desktop Patrol Reference Manual*, confirm the port number in use.

- When specifying "FQDN" or "Windows Host Name" in **Host Name** of the **Server Environment Setup** window set at installation, the address of this "FQDN" or "Windows Host Name" should be analyzed through Systemwalker Desktop Patrol CT, so confirm that before installation.

![Note icon] Note

If the address of host name cannot be analyzed, reinstall it

If the address cannot be analyzed, patches application, software distribution and Inventory collection may not be performed through Systemwalker Desktop Patrol CT, Systemwalker Desktop Patrol DS should be reinstalled.

2.4.1.1 Installation using the Wizard

The procedures for installing DS are as following. Besides, for the operating environment, refer to *Systemwalker Desktop Patrol User's Guide*.

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. Enter the following URL in the **Address** bar of Web Browser.

```
http://server information (FQDN name or host name or IP address of [Systemwalker Desktop Patrol
CS])/DTP/index.html
```

4. The login window is displayed, enter **User ID** and **Password**, click the **Login** button. Consult the user ID and password to "System Administrator".

Item	Description
User ID	Enter the user ID of "System Administrator" or "Department Administrator".
Password	Enter the password of "System Administrator" or "Department Administrator".

5. The main menu is displayed. Click **CS/DS Settings and Status** of the **Environment Setup** window. The following window is displayed.

6. Click **Download** of CS/DS as the higher server with DS installed.

7. The **Download Files** dialog box is displayed and the message for confirming saving appears, click the **Open** button.

8. The **Welcome** window is displayed, click the **Next** button.

> 📋 **Note**
>
> Before the **Welcome** dialog box above is displayed, the following message window might be displayed, click the **Run** button to start installation.
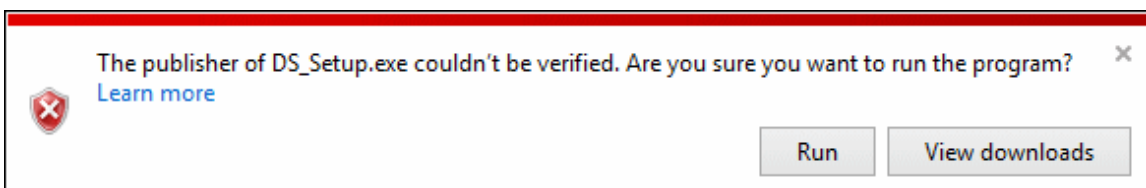
9. The **Select Installation Target** window is displayed.

If you do not want to modify the displayed installation target, click the **Next** button.

To modify the installation target, click the **View** button of the folder to be modified and click the **Next** button after the folder is modified.

Do not specify the directory containing Multi-byte /single-byte characters (Chinese) in **Installation Target Folder**.

10. The following **Server environment setup** window is displayed.

Note
. . . .

Server environment setup window will be displayed behind the background window during installation.

Display the window by switching the window through the task bar or Alt+TAB key.
. . . .

Enter the following information and click the **Next** button after confirmation.

Item	Description
Server name (Required)	Specify "Section Name" for installing Systemwalker Desktop Patrol DS. Specify it as characters within 50 characters included single-byte alphanumeric characters and special characters "-", "@", ".". Example) Fujitsu Company
Host name (Required) (cannot be modified once set here)	Display the initial value, modify it as required. If the initial value has not been displayed, input the host name according to the following conditions. Specify "FQDN Format", "IP Address" or "Windows Host Name" of PC with Systemwalker Desktop Patrol DS installed. Specify it within 50 characters with alphanumeric characters, - (hyphen) and . (period). Example) ds.example.com This host name should be set under the environment where the name can be analyzed through the connected Systemwalker Desktop Patrol DS/CT. ![Note icon] **Note** . . . . **Communication in IPv6 environments**

Item	Description
	IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name: - Register the CS and DS host name and IP address in the DNS server. - Register the CS and DS host name and IP address in the communication source PC hosts file. ·
Software distribution port number (Required)	Display the port number for software distribution specified at CS installation. Here, it can be viewed instead of being modified.
Port number for inventory transmission (Required)	Display the port number for Inventory transmission specified at CS installation. Here, it can be viewed instead of being modified.
Directory for saving distributed software (Required) (cannot be modified once set here)	Specify the directory of the software distribution saving target with absolute path. Set the initial value as "*dtpInstallDir*\FJSVsbtrs\data\swc". To modify, specify a directory with sufficient available capacity. Besides, when applying the security patches automatically, specify a directory with sufficient available capacity excluding Windows Installation Drive. 📘 **Point** · **To prevent OS damage, it is recommended to specify the space excluding the Setup disk** To prevent insufficient disk space due to registering/distributing software or automatically applying security patches, it is recommended to specify distribution software saving directory as other space excluding OS Setup disk ·
Maximum size	Specify in "MB" the maximum disk capacity of the software distribution saving directory. Specify a number within 1-999999 in the maximum size. If omitted, the maximum size is the available capacity of the specified directory. A value larger than the available capacity of the specified drive in **Software Distribution Saving Directory** can be set. Set the maximum size combining with PC environment design.

11. The following **Server environment setup** window is displayed, confirm that the **Use a proxy server for connections to an upstream server** checkbox is not selected and click the **Next** button.

Here, the "Upstream Server" refers to the server selected and downloaded in the **DS Downloading** window.

The proxy cannot be set at installation. For proxy setting, refer to "2.3.5.5 Set Proxy".

This window cannot be returned after the following **Server environment setup** window is displayed.

12. The **Environment Setup** window is displayed.
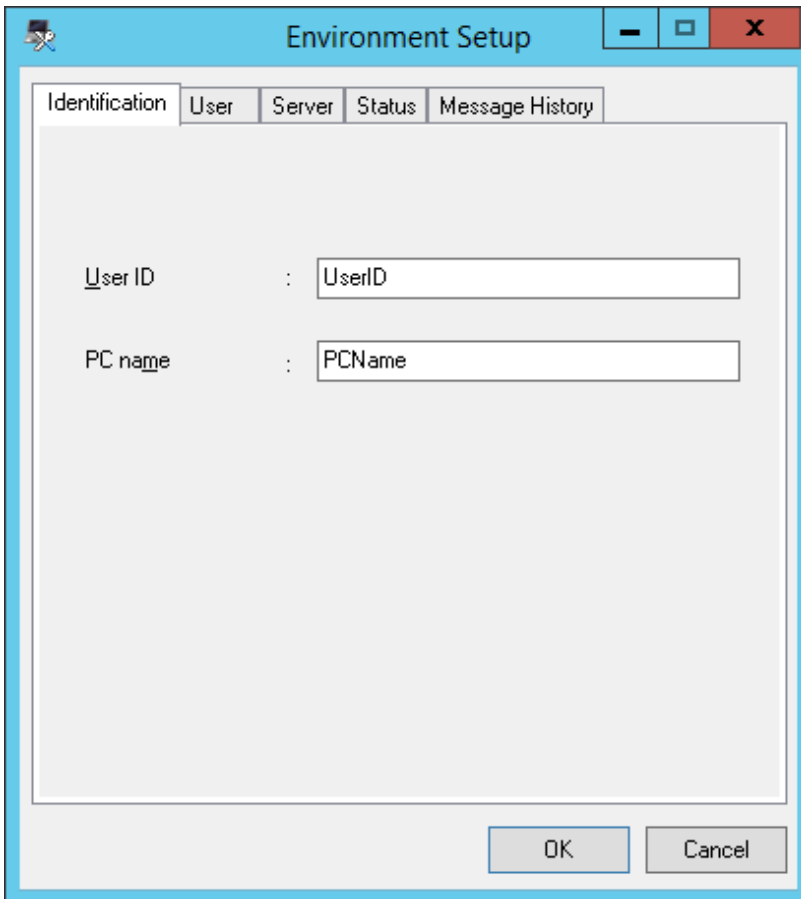
Enter the following information and click the **OK** button after confirming the content.

Environment Setup Tab	Item	Description
Identification	**User ID** (Required)	Specify the user ID to manage as CT. Make sure to specify. The user ID set here will be displayed through the main menu for identifying the user.

Environment Setup Tab	Item	Description
		You can specify up to 20 halfwidth alphanumeric characters. Single-byte alphanumeric characters and single-byte symbols "-", "@", "." are allowed. It is case sensitive for English letters.
	PC name (Required)	Specify the name to manage as Systemwalker Desktop Patrol CT. You can specify up to 20 halfwidth alphanumeric characters. Besides, fullwidth characters, space and the following special characters cannot be specified. "+", "*", "?", "<", ">", ",", ";", ":", "\", "/", """, "|"
User	**Content**	Enter when it is prompted to enter in "System Administrator". Characters of 256 characters at most can be specified. Multi-byte characters, single-byte letters and numbers, single-byte space and the following special characters can be specified. "-", "@", ".", "(", ")", "[", "]", "<", ">", ":", ";", "/", "{", "}"
Server	**Connection server**	Specify the host name of the connection server in FQDN format or with IP address. If it has been set at installation, there is no need to input/modify. If this value needs to be changed after installation, you can specify up to 256 alphanumeric characters, and the following symbols: - . ⚐ Note ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯ **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name: - Register the CS and DS host name and IP address in the DNS server. - Register the CS and DS host name and IP address in the communication source PC hosts file. ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

Continue installation.

Besides, when performing Active Directory linkage, do not set the following value in **User Identification Information** tab.

- **User ID**: the logon name of Windows domain

   (In case of "user@domain.jp", "domain\user", set the "user" part.)

- **PC name**: computer name

13. The **Installation Completed** window is displayed after the processing is completed normally, click the **Finish** button.

2.4.1.2 Silent Installation

 Note

. . . .

- Silent installation can only be performed when you are performing installation for the first time.

- Installation process must not be interrupted during silent installation.

. . . .

Installation procedure

Follow the steps below to perform silent installation:

1. Create an installation parameter CSV file.

   Refer to "A.2.1 Installation Parameter CSV File" for details.

   If you are performing installation using the default values for all parameters, this step is not required.

2. Use the parameter setup command to create a response file.

   Refer to "A.2.2 Parameter Setup Command" for details.

   If you did not create an installation parameter CSV file in step 1, this step is not required.

3. Prepare the resources required for silent installation.

   Copy the following resources to the folder in the TMP environment variable.

   - DS installer (DSSetup.exe)

     The DS installer is located under the following folder on the CS.

     iisHomeDir\wwwroot\DTP\DS

   - Server environment setup file (ATOOL_policy_ds.zip)

     The server environment setup file is located under the following directory on the CS.

     - If the upstream server is the CS:
       iisHomeDir\wwwroot\DTP\DS

     - If the upstream server is the DS:
       iisHomeDir\wwwroot\DTP\DS*upstreamServerHostName*

4. Execute the silent installation command.

   Refer to "A.2.4 Silent Installation Command" for details.

5. Check the installation result in the returned value and message from the silent installation command.

Refer to "A.2 Silent Installation of DS" for details on the files and commands used, and messages output, in silent installation.

2.4.2 Set DS Operation Environment

This section describes how to set DS operating environment.

2.4.2.1 Set Server Information

The following content can be set in the server information.

- Modify the server name

  The "DS Name" set here will be used in the following window.

  - **DS Name** of **Environment Setup** > **CS/DS Settings and Status** in the main menu

  - **DS Name** of **CT Downloading** in the download menu.

The procedure is as follows.

1. Log on to the main menu, click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **CS/DS Settings and Status**.

   The following window is displayed.

3. Click the link of server name.

The following window is displayed.

4. Enter the following item.

Item	Content
DS Name	Display the common name of DS to be installed.
	Specify DS name within 50 characters included single-byte alphanumeric characters and special characters "-", "@", ".". Blank cannot be specified.
	Cannot be omitted.

5. Click the **OK** button.

2.4.2.2 Set Transmission

This section performs the settings when transmitting information from Systemwalker Desktop Patrol DS to higher server and transmitting information from Systemwalker Desktop Patrol DS to downstream server or Systemwalker Desktop Patrol CT.

The transmitted information contains the following information.

- Inventory Information

- Registered Software

- Security Patches

- Client Policy/Server Properties

And as transmission settings, the following items can be set.

- Transmission Interval

- Number of Simultaneously connected devices

The procedure is as follows.

1. Log on to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **CS/DS Settings and Status**.

   The following window is displayed.

3. Click the link of the server name.

   The following window is displayed.

4. Enter items of **Settings of Connection with Higher CS/DS**

Item	Content
Connection Interval with Higher CS/DS (1-1440)	Specify in minute the period for downloading software from the higher server within 1-1440. Default: 5, cannot be omitted.
Specify hour(s) of receiving distribution software	Selected when specifying the time frame for downloading software. Specify the time frame for downloading software from higher server. If not selected, the time frame for downloading will be under the status of being able to download in 24 hours at will. Specify a number from 0 to 23 for the hour, a number from 0 to 59 for the minute. The start time cannot be specified the same as the end time.

5. Enter the following item from settings of communication with downstream DS/Client.

Item	Content
Maximum number of connections (1-999)	Specify the total number of downstream DS or CT communicating simultaneously within 1-999. Default: 30, cannot be omitted. Set the following values according to the total number of actually connected downstream server or client.

Item	Content
	1000 or less: 30
	2000 or less: 40
	2000 above: 50

6. Click the **OK** button.

2.4.2.3 Set Proxy

Proxy server can be used when the higher server or mobile PC communicating with DS set in the company.

📗 Note

. . . .

Proxy server and setting conditions not allowed

The following proxy server is not allowed.

 - Software of other company WEBGUARDIAN

And if the following settings are performed, it cannot used.

 - Windows authentication has been enabled in ISA Server

. . . .

1. Log on to the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

2. Click **CS/DS Settings and Status**.

The following window is displayed.

3. Click the link of server name.

The following window is displayed.

4. Enter the following item of **Settings of Connection with Higher CS/DS**.

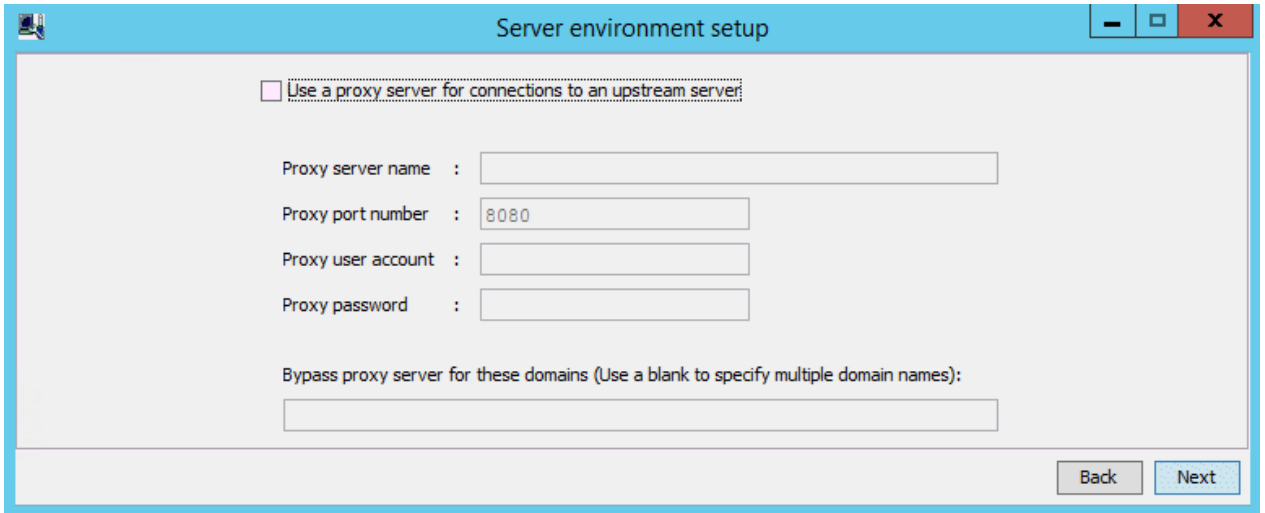| Item	Content
Use Proxy	Selected when using proxy.
	The following items can be specified when using proxy.
	- **Proxy Server Name**
	Specify the name of proxy server.
	Specify within 64 characters FQDN or IP address with single-byte alphanumeric characters, "-", ".".
	Cannot be omitted.
	![Note] **Note**
	Communication in IPv6 environments
	IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name:
	- Register the CS and DS host name and IP address in the DNS server.
	- Register the CS and DS host name and IP address in the communication source PC hosts file.
	- **Port Number**

Item	Content
	Specify a port number for proxy number.
	Specify a number within 1-65535.
	Cannot be omitted.
	- **User Name**
	Specify the user name of proxy server within 256 halfwidth characters.
	- **Password**
	Specify the password of proxy server within 256 halfwidth characters.
	- **Bypass proxy server for these domains (Use a blank to specify multiple domain names)**
	Specify the domain name not using proxy server. When multiple domain names are specified, separate them with space.
	You can specify up to 2064 halfwidth characters, including the following symbols: - .

5. Enter the following items from **Settings of Connection from CT**.

Item	Content
Use Proxy	Selected when using proxy.
	The following item can be specified when using proxy.
	- **Proxy Server Name**

Item	Content
	Specify the name of proxy server.
	Specify within 64 characters FQDN or IP address with single-byte alphanumeric characters, "-", ".".
	Cannot be omitted.
	- **Port Number**
	Specify a port number for proxy number.
	Specify a number within 1-65535.
	Cannot be omitted.
	Note
	Communication in IPv6 environments
	IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name:
	- Register the CS and DS host name and IP address in the DNS server.
	- Register the CS and DS host name and IP address in the communication source PC hosts file.
	- **UserName**
	Specify the user name of proxy server within 256 halfwidth characters.
	- **Password**
	Specify the password of proxy server within 256 halfwidth characters.
	- **Bypass proxy server for these domains (Use a blank to specify multiple domain names)**
	Specify the domain name not using proxy server. When multiple domain names are specified, separate them with space. Specify within 2064 halfwidth characters.
	Specify the domain name with single-byte characters, "-", ".".

If the name of proxy server cannot be analyzed by connecting PC of proxy server, set IP address of proxy server in **Proxy Server Name**.

6. Click the **OK** button.

2.4.2.4 Set Operation Environment for Mobile PC

When connecting into the company from external by using VPN (Virtual Private Network) for mobile use, the following operation policy can be set for Systemwalker Desktop Patrol CT on the mobile PC. Even if in the mobile PC not connecting the network usually, assets management can also be performed through Systemwalker Desktop Patrol.

Class	Settings
Settings for Mobile PC Assets Management	Icon displayed in task tray (task bar)
	Send Inventory information which has not been sent
Settings for Reducing Mobile PC Load	Send CT operation status log
	Search method for patch installation in the **Start** menu (**Apps** screen)

Class	Settings
	Message displayed when automatically starting to download software

The settings above are for setting DS for mobile connection use.

By connecting this DS, the mobile PC operates according to the set operation policy.

In case the mobile PC has not be connected network when the new confirmation arrives, detect the later LAN connection and get client policy, apply security patches (*) and perform Inventory collection during LAN connection.

　　* When the settings are for applying security patches

The figure for using the mobile PC is as follows:
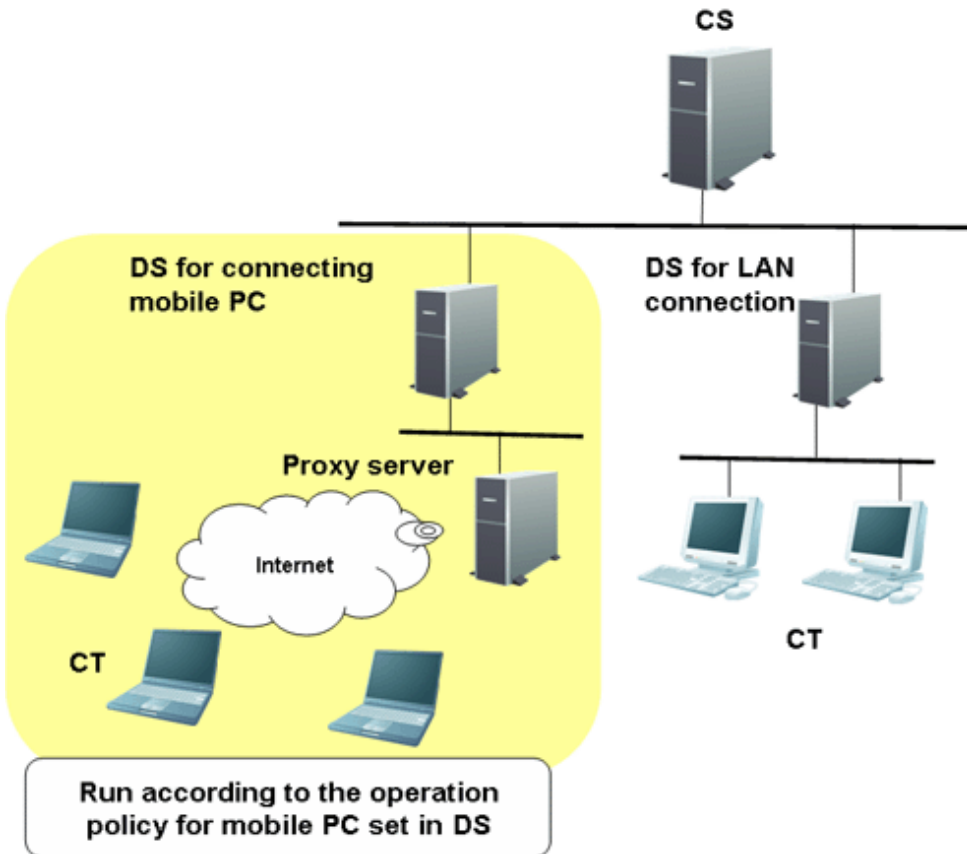
Items to be set

Icon displayed in task tray (task bar)

CT icon is displayed in the task tray and the balloon is displayed when starting/ending Inventory collection.

The user can master the status of Inventory collection to determine the timing for disconnecting the network.

In case of Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 R2 or Windows Server(R) 2012, CT icon is displayed in the task bar after starting Inventory collection and the operating status is displayed. (Notes)

Notes) When the operating status is displayed in Windows Server(R) 2008 R2 or Windows Server(R) 2012, enable it after installing the following function.

　- Desktop Experience

- The following icon is displayed in the task tray (task bar) of the mobile PC.

    - In case of not Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 R2 or Windows Server(R) 2012

    The following icon is displayed in the task tray.

    - In case of Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 R2 or Windows Server(R) 2012

    The following icon is displayed in the task bar.

- In case of not Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 R2 or Windows Server(R) 2012, the balloon will be displayed when starting/ending Inventory collection. The balloon will be closed automatically in about 10 seconds.

    The displayed content is as follows:

    [When Starting Inventory Collection]

    ```
    Systemwalker Desktop Patrol
    Inventory Collection Started
    ```

    [When Ending Inventory Collection]

    ```
    Systemwalker Desktop Patrol
    Inventory Collection Completed
    ```

- The tool prompt will be displayed after moving the cursor behind the icon.

    The displayed content is as follows:

    - In case of not Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 R2 or Windows Server(R) 2012

    [Normal]

    ```
    Systemwalker Desktop Patrol
    ```

    [During Inventory Collection]

    ```
    Systemwalker Desktop Patrol
    Collecting Inventory
    ```

    - In case of Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 R2 or Windows Server(R) 2012

    [During Inventory Collection]

    ```
    Collecting Inventory - Systemwalker Desktop Patrol
    ```

Send Inventory information which has not been sent

   When the network is connected, Inventory information which cannot be sent to the connection server due to the following reasons in the previous Inventory collection is sent for the first time, thus, it can be used for assets management more reliably in the mobile PC which has not been connected the network for a short time.

- When it cannot be sent because the network is not connected, though Inventory collection has been performed

- When it cannot be sent because the network is cut off during sending Inventory information

Send CT operation status log

   In general, CT operation status log will be sent to the connection server along with Inventory information.

   Because the network traffic has been cut down, whether to send CT operation status log to the connection server can be selected.

Search method for patch installation in the Start menu (Apps screen)

In general, after selecting **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Patch Installation**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Patch Installation**, to detect security patch which has not been installed in PC, the registry and files in the whole drive will be searched.

Because file search will cause increasing battery consumption in case of the mobile PC performing patch installation, select the resolution for search during patch installation from the following methods.

a. Perform patch Installation after searching all the drives (common search method)

Perform file search for all drives of Systemwalker Desktop Patrol CT. The user can detect the software installed in any folder, but the battery consumption will increase due to file search for all drive.

b. Perform patch installation after searching the system folders.

Perform file search for the following folders only. Though file search time can be shortened, security patches cannot be detected when installing software to non search object folder.

   - System folders Example) c:\windows

   - Program folders Example) c:\Program Files

c. Perform security patch installation according to the "Unapplied Patch Information" detected in Systemwalker Desktop Patrol CS.

Apply security patches according to the "Unapplied Patch Information" detected in Systemwalker Desktop Patrol CS.

Because security patches can be installed immediately in case it won't cause any load on Systemwalker Desktop Patrol CT if file search has not been performed, but situation where security patches of the new installed software cannot be applied according to the timing for Inventory collection exists.

Message displayed when starting to download software automatically

The window for confirmation is displayed before automatically downloading software, you can select to perform or cancel automatic downloading.

Thus, patches can be downloaded when the mobile PC use won't be affected.

Setting method

Set the operation policy of the mobile PC by using the following command.

   - MBPolicy.exe (mobile environment setup) command

Execute the command above on Systemwalker Desktop Patrol CS for setting Systemwalker Desktop Patrol DS for mobile PC connection use.

For MBPolicy.exe (mobile environment setup) command, refer to *Systemwalker Desktop Patrol Reference Manual*.

For how to use proxy in the communication between Systemwalker Desktop Patrol CT and Systemwalker Desktop Patrol DS, refer to "2.4.2.3 Set Proxy".

2.5 Construct AC

Systemwalker Desktop Patrol AC is constructed for managing the report output function and assets information registration function of Systemwalker Desktop Patrol.

2.5.1 Install AC

This section describes how to install AC.

Issues to be confirmed before installation

- End the following programs before installation.

    - Resident programs included virus scanning program.

- By referring to "Operation Environment" of *Systemwalker Desktop Patrol User's Guide*, confirm "Products That Cannot be Used in Mixture".

- By referring to "List of Port Numbers" of *Systemwalker Desktop Patrol Reference Manual*, confirm the port numbers in use.

    To modify the port number used between Systemwalker Desktop Patrol CS and Systemwalker Desktop Patrol AC, start the **Environment Setup** window after modifying the port number. Message indicating connection failed appears. To confirm the settings of **Setup of Host Name of CS**, click the **OK** button.

- Microsoft(R) Excel is required in AC. Confirm whether Microsoft(R) Excel has been installed. For the available Microsoft(R) Excel, refer to "Required Software" of *Systemwalker Desktop Patrol User's Guide*.
  Besides, when installing Microsoft(R) Excel, Visual Basic for Applications (installed by default) of Setup option is also required.

Installation

The procedures for installing AC are as follows. Besides, for the operating environment, refer to *Systemwalker Desktop Patrol User's Guide*.

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. After inserting DVD-ROM of Systemwalker Desktop Patrol into PC, the following window is displayed.

4. Select **AC Installation**.

If the Setup above has not been started, start "swsetup.exe" of DVD-ROM drive.

Note that the following message may be output depending on the environment, however, this is not a problem. Click **OK** to continue the installation.

"The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 2803"

5. The **Welcome to Install Systemwalker Desktop Patrol** window is displayed, click the **Next** button.

6. The **Select Installation Folder** window is displayed. If you are performing reinstallation, this step is not required.

   If you do not want to modify the displayed installation target, click the **Next** button.

   To modify the displayed installation target, click the **View** button of the folder to be modified, and click the **Next** button after the folder has been modified.

   You must specify a valid folder name in Windows using up to 64 halfwidth characters.

   Specify a folder not used by other programs. This product must not coexist with other programs in the same folder. For this reason, do not install other programs under the installation folder after this product is installed.

7. The **Start to Copy Files** window is displayed, confirm whether the content displayed in the window is incorrect and click the **Next** button.

   The **Installation Status** window is displayed, start installation.

8. The **Setup has been completed normally.** window is displayed, click the **Finish** button.

9. The **Setup of Host Name of CS** window will be displayed.

   Set **CS Host Name** and click the **OK** button.

   When it takes time to connect the database, the window prompting canceling the processing will be displayed. At this time, wait or after canceling the processing, execute again after resetting. As cause for time consuming connection, it might be higher CPU load of connection target server or the port number of connection target server being used by other product.

   Besides, the settings can be modified after installation. For modification, refer to "Modify the settings of connection target server after installation".

Item	Description
CS Host Name	Set the "IP Address" or "Windows Host Name" of PC with Systemwalker Desktop Patrol CS installed.
	Characters within 18 characters included single-byte alphanumeric characters and single-byte symbols can be set.
	Besides, the specified "Host Name of CS" should be set in the environment where the name can be analyzed through Systemwalker Desktop Patrol AC.

Item	Description
	![Note icon] **Note** **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using the following pattern, and enter the host name: - Values with 18 characters or more cannot be specified, therefore register the CS IPv6 address in the hosts file beforehand, and then specify that host name.

Modify the settings of connection target server after installation

The connection target server is set when installing AC. Execute this procedure when hoping to confirm the settings at installation or modify the settings.

1. Start the window for setting connection target server.

   Select **Start** > **All Programs** > **Systemwalker Desktop Patrol AC** > **Management Ledger Settings**, or **Apps** > **Systemwalker Desktop Patrol AC** > **Management Ledger Settings** of PC with AC installed.

   The following window is displayed.
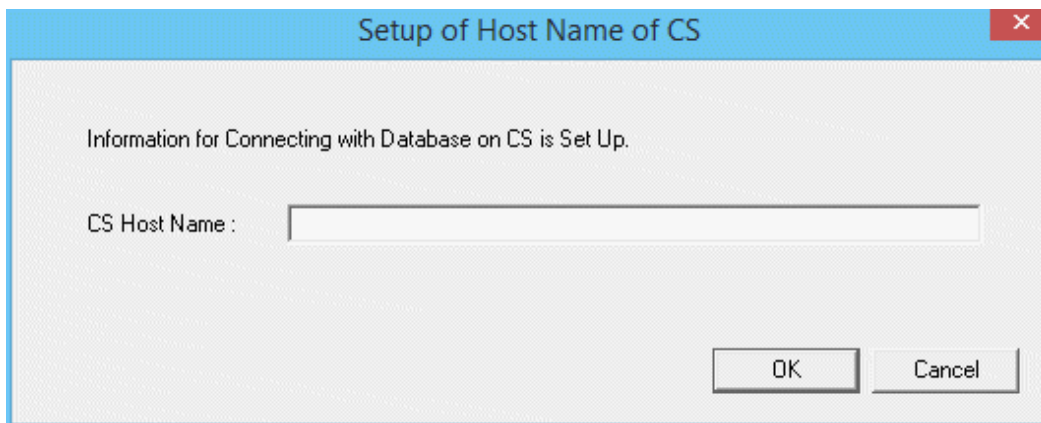
2. Set CS host name.

   Set the following information and click the **OK** button.

Item	Description
CS Host Name	Set "IP Address" or "Windows Host Name" of PC with Systemwalker Desktop Patrol CS installed. Characters within 18 characters included single-byte alphanumeric characters and single-byte symbols can be set. Besides, the specified **CS Host Name** should be set in the environment where the name can be analyzed through Systemwalker Desktop Patrol AC. ![Note icon] **Note** **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using the following pattern, and then enter the host name:

Item	Description
	- Values with 18 characters or more cannot be specified, therefore register the CS IPv6 address in the hosts file beforehand, and then specify that host name.

2.6 Install ADT

This section describes how to install the component Systemwalker Desktop Patrol ADT for connecting Systemwalker Desktop Patrol CS in order to automatically detect the device information of Systemwalker Desktop Patrol.

To install "ADT", "ADT Module" should be created in advance. For how to create "ADT Module", refer to "2.3.5.10 Set Automatic Detection Schedule (Create ADT Module)".

🅿 Point

The software distribution function can be used when installing ADT

When CT has been installed in PC with automatic detection, the software distribution function can be used to distribute and install ADT module.

🛈 Note

The PC on which the ADT will be installed must connect to a network environment that meets the following criteria:

- The subnet mask is 17 to 28 bits long.

- The connection is established using a wired LAN.

Issues to be confirmed before installation

- End the following program before installation.

    - Resident programs included virus scanning program.

The procedures for installing ADT are as follows. Besides, for the operating environment, refer to *Systemwalker Desktop Patrol User's Guide*.

1. Log on to Windows with Administrators group affiliated account.

2. Enter the following URL in the **Address** bar of Web browser.

```
http://server information (FQDN name or host name or IP address of "Systemwalker Desktop Patrol
CS")/DTP/dwl.html
```

Besides, when PC which has not be connected Systemwalker Desktop Patrol CS through network has been set as "ADT", copy to PC with "ADT" installed after ADT has been downloaded in PC connecting Systemwalker Desktop Patrol CS through other network.

3. Download menu is displayed, the following window is displayed after clicking **ADT Download**.
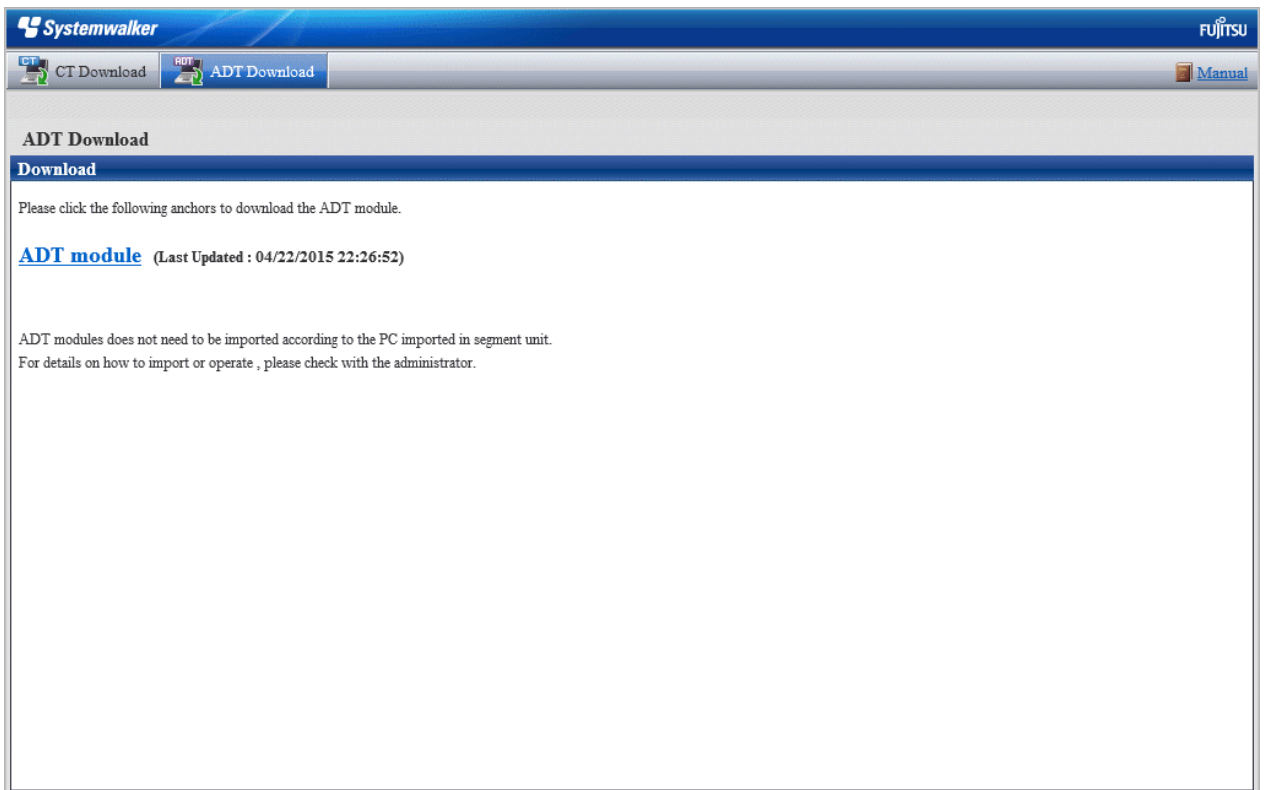
4. Click **ADT module** to download.

5. Place downloading module (ADTSetup.exe) to an arbitrary location in PC with automatic detection in each network segment and execute.

6. Enable the following installer, set the installation target and **Account Information During Task Registration**, and click the **Start** button to start installation.

[In the environment of Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008, and Windows Server(R) 2012]
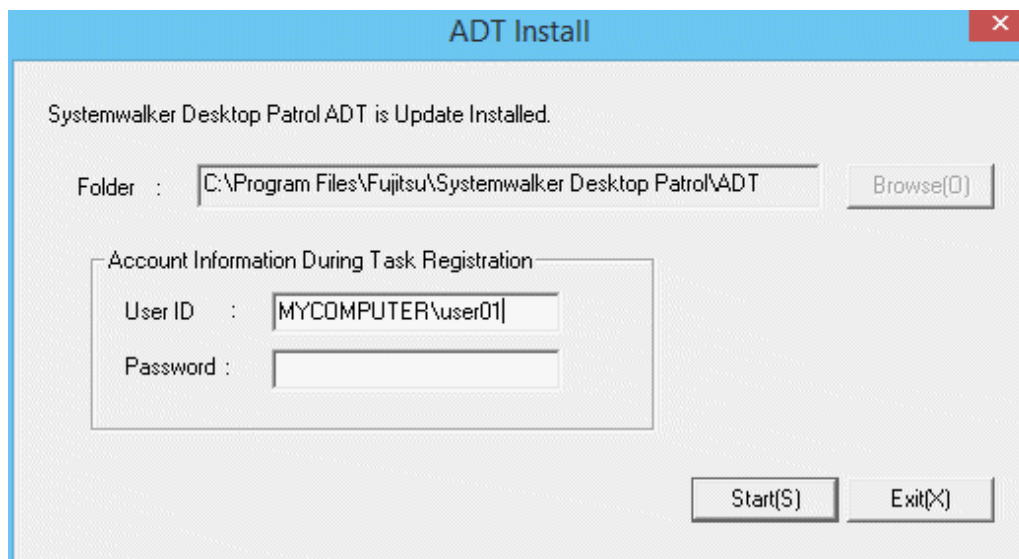
Item	Description
Folder	Set the installation target of ADT module.

Item		Description
Account Information During Task Registration (Notes)	**User ID**	Specify the user account for executing the task. Specify it with alphanumeric characters within 260 characters in the format of <Domain Name>\< User Name >.
	Password	Specify the password for the specified user ID in the user account. Specify it with alphanumeric characters within 260 characters.

Notes) Displayed only in case of Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008, and Windows Server(R) 2012.

7. The **Schedulling of Automatic Detection** window will be displayed before installation.

Enter the following information and click the **Apply** button.

Item	Description
On Demand Device Information Notification	Selected if not to notify the device information detected by ADT by scheduler.

Item		Description
Scheduled Device Information Notification		Selected if to notify the device information detected by ADT by scheduler.
Notification Target Settings	**Connection Server**	Set the server name of notification target. 🛈 **Note** . . . . **Communication in IPv6 environments** IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name: - Register the CS host name and IP address in the DNS server. - Register the CS host name and IP address in the communication source PC hosts file. . . . .
	Port Number	Set the port number of notification target. Set in case of not initial value port 80.
	Set	Used when setting proxy.
Collect Devices Not Registered in Ledger (Detailed Collection)		Select this option to perform automatic detection and information collection of devices for maintaining the management ledger. This option cannot be selected if **Collect Devices Connected to without Permission (Simple Collection)** is selected.
Scheduler Setting	**Daily**	Selected when notifying device information every day.
	Weekly	Selected when notifying device information weekly. Set as that Monday to Sunday can be selected.
	Monthly	Selected when notifying the device information monthly. Select the execution date in **Execution Date**. Besides, as **Execution Date**, if the date not existing in the set month has been specified, automatic detection cannot be performed in this month. Thus, to execute at the end of a month, study the use of execution at 00:00 on the first day of the month.
	Start Time	Set the time for starting to notify the device information. When using ADT module on server PC which does not operate around the clock, if time such as late at night has been set, then the power for PC with automatic detection might be cut off, so pay attention to the time settings.
Collect Devices Connected to without Permission (Simple Collection)		Select this option to perform automatic detection and information collection of devices connected to without permission. This option cannot be selected if **Collect Devices Not Registered in Ledger (Detailed Collection)** is selected.

	Collection Interval	Specify the interval for collecting device information when detecting devices connected to without permission. Device information will be repeatedly collected at this interval.
		
		Select one of the following intervals:
		
		  - **30 minutes**
		
		  - **1 hour**
		
		  - **2 hours**

Item		Description
		- **6 hours**
Confirm Execution Result		Display the execution result.
	Log Viewing	Display execution result log.

After completing the installation, register the following tasks in the task function of Windows.

- Name:

    SWDTPAS_ADT.job

- Operating authority:

    - In case of Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008, or Windows Server(R) 2012: specified account

Besides, if ADT module has not be started in the set aggregating timing (due to PC power not switched on, etc.), the device information will be notified at the start time for scheduler settings after ADT module is started.

The following message window will be displayed after scheduler settings have been ended, click the **OK** button.

```
Installation of ADT was Ended. A Setup becomes Effective by Rebooting System.
```

8. Click the **Apply** button to reboot the system.

About the modification of automatic detection schedule after installation is completed

When starting the automatic detection schedule and modifying the schedule after installation is completed, the system should be rebooted. The settings will be valid after the system is started next time.

2.7 Install CT

This section describes how to install CT.

Besides, in PC with Systemwalker Desktop Patrol CS or Systemwalker Desktop Patrol DS installed, Systemwalker Desktop Patrol CT will be installed at the same time.

How to install CT is follows: for the summary, refer to "1.4 Determine How to Install Client (CT) ".

- Stand-alone installation

    - Wizard pattern installation

    - Silent installation

    - Installation in an Active Directory environment

- Installation through CT Kitting

Note

CT registration password

- To use a CT registration password, ensure that the server administrator uses CustomPolicy.exe (policy for modifying custom setup command) to enable it. CT registration passwords can be set per target server (CS and DS). Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on the command.

    It is recommended to change the CT registration password using CustomPolicy.exe (policy for modifying custom setup command) once the CT is extracted.

- If a CT registration password is enabled, it must be set on the CT.

Note

. . . .

Delete the CT installer after installation is completed.

. . . .

2.7.1 Wizard Pattern Installation

The procedures for installing CT in wizard pattern are as follows. Besides, for the operating environment, refer to *Systemwalker Desktop Patrol User's Guide*.

Issues to be confirmed before installation

- End the following program before installation.

    - Resident programs included virus scanning program.

    - The **Service** window of Windows

1. Log on to Windows with Administrators group affiliated account.

    Enter the following URL in the **Address** bar of Web browser.

    ```
    http://server information (FQDN name or host name or IP address of "Systemwalker Desktop Patrol
    CS")/DTP/dwl.html
    ```

2. Display **CT Download** of the download menu.

3. Select **Server Name**, or **Server Name (with Remote Operation)** of PC as the higher server, the **Download Files** dialog box is displayed and message for confirming saving appears.

If remote operation is not required, select **Server Name**.

If remote operation is required, select **Server Name (with Remote Operation)**.

Follow the instructions of the administrator regarding which option to select.

4. Click the **Execute** button to start installation, the **Welcome to Install Systemwalker Desktop Patrol CT** window is displayed, click the **Next** button.

![Note icon] Note

. . . .

Select Run in case the following security warning window is displayed.

. . . .
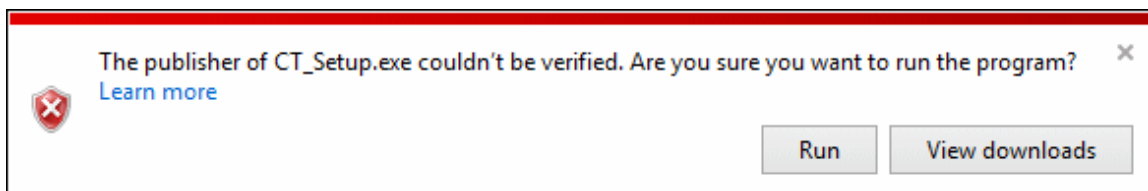
5. The **Select Installation target folder** window is displayed. (Not displayed during reinstallation.)

If you do not want to modify the displayed installation target, click the **Install** button.

To modify the installation target, modify the **Browse...** button of the folder to be modified and click the **Install** button after the folder is modified.
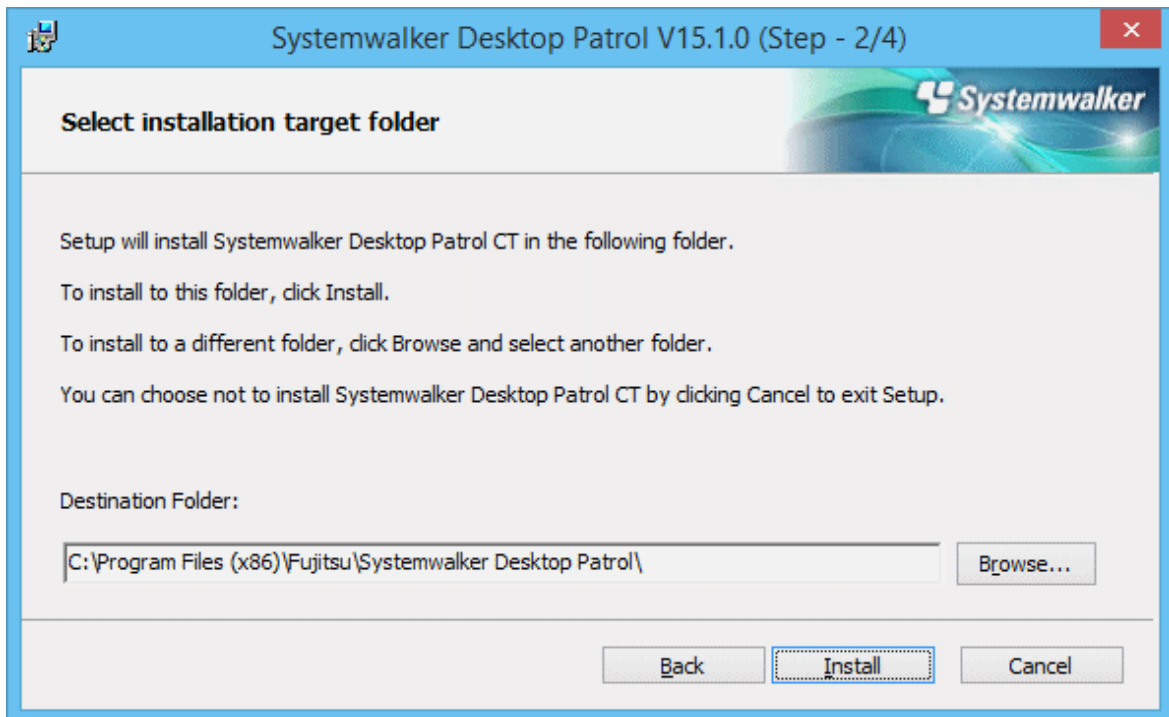
6. The **Environment Setup** dialog box is displayed.
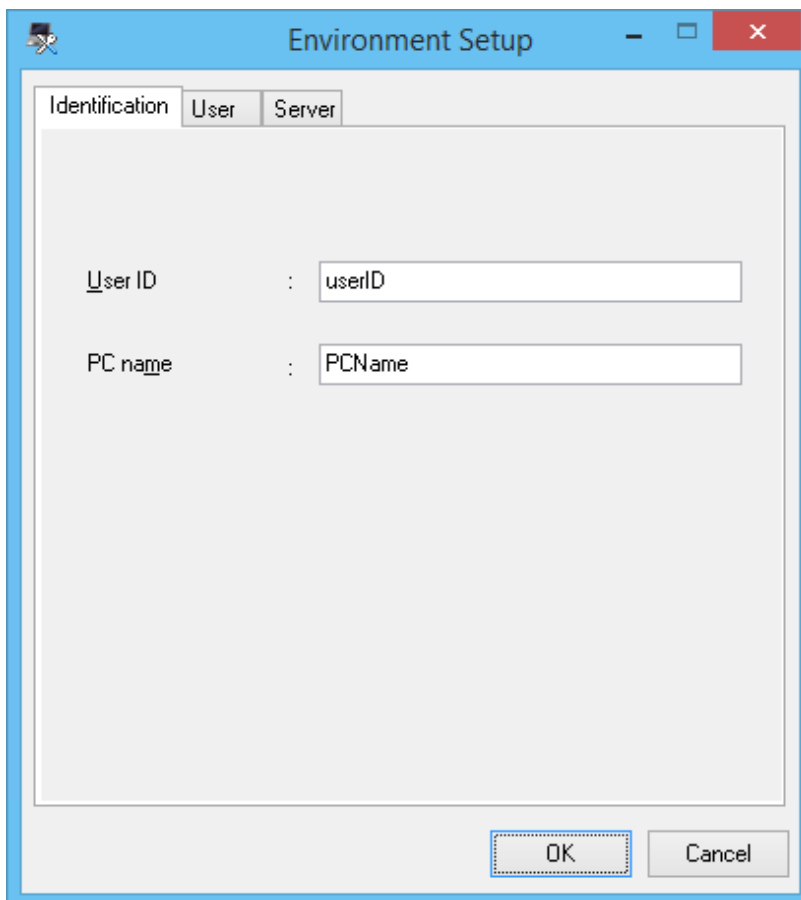
Note

....

The **Environment Setup** window will be displayed behind the background window during the installation.

Display the window by switching the window through the task bar or Alt+TAB key.

....

Enter the following information and click the **OK** button after confirming the content to start installation.

If the user ID and PC name have not been input, Inventory information cannot be collected. Make sure to input the user ID and PC name.

However, when Inventory collection has not been performed and hoping to input the user ID and PC name later, even if omitted, errors won't occur during installation. At this time, set as follows after installation.

  a. Select **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Environment Setup**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Environment Setup** to set the user ID and PC name.

  b. Select **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Inventory Collection**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Inventory Collection** to execute Inventory collection.

Environment Setup Tab	Item	Description
Identification	**User ID** (Required)	Specify the user ID to manage as Systemwalker Desktop Patrol CT. Make sure to specify.
		The user ID set here will be displayed through the main menu for identifying the user.
		Characters of 20 characters at most can be specified. Single-byte alphanumeric characters and special characters "-", "@", ".", "_" can be used.
		It is case sensitive for English letters.
	PC name (Required)	Specify the name to manage as Systemwalker Desktop Patrol CT.
		Single-byte alphanumeric characters of 20 characters at most can be specified. Besides, fullwidth characters, space and the following special characters cannot be specified.
		"+", "*", "?", "<", ">", ",", ";", ":", "\", "/", """, "|"
		Besides, even if automatically getting PC ellipsis as PC serial number has been set, situation where failed to get automatically might exists in the following cases.
		- When PC itself has no serial number
		- When the Windows Management Instrumentation (WMI) function is invalid
User	**Content**	Enter when prompting inputting in "System Administrator". Characters of 256 characters at most can be specified. Multi-byte characters, single-byte letters and numbers, single-byte space and the following special characters cannot be specified.
		"-", "@", ".", "(", ")", "[", "]", "<", ">", ":", ";", "/", "{", "}"
Server	**Connection server**	Specify the host name of connection server in FQDN format or with IP address. The settings have been performed during installation, there is no need to input/modify.

Environment Setup Tab	Item	Description
		If this value needs to be changed after installation, you can specify up to 256 alphanumeric characters, and the following symbols: - .
		The initial value is the host name set during CS/DS installation.
		📙 **Note**
		....
		When the initial value has been modified as IP address, in the environment where the host name of CS/DS cannot be analyzed according to IP address, even if Inventory information can be collected, situation where failed to download the security patches might occur.
		Confirm whether the address of connection server can be analyzed in the network environment of CT.
		....
		📙 **Note**
		....
		Communication in IPv6 environments
		IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand using one of the following patterns, and then enter the host name:
		- Register the CS and DS host name and IP address in the DNS server.
		- Register the CS and DS host name and IP address in the communication source PC hosts file.
		....
	Registered password	Specify the registration password provided by the administrator.

Besides, when performing Active Directory linkage, the **User Identification Information** tab cannot be displayed. The following values can be set automatically in the information set through the **User Identification Information** tab.

- **User ID**: logon name Windows domain (in case of "user@domain.jp", "domain\user", "user" can be set.)

- **PC name**: computer name

📙 **Note**

....

About the incorrect display during installation

When installing Systemwalker Desktop Patrol CT, situation where the message is displayed and the installation is cancelled exists.

[Error Message]

```
"The installation cannot be performed well possibly. Please reinstall after rebooting PC"
```

When the error message is displayed and the installation is cancelled, reinstall CT after rebooting OS.

....

🅿 **Point**

....

CT registration password

If a CT registration password is enabled, click the **Server** tab and enter **Registered password**.
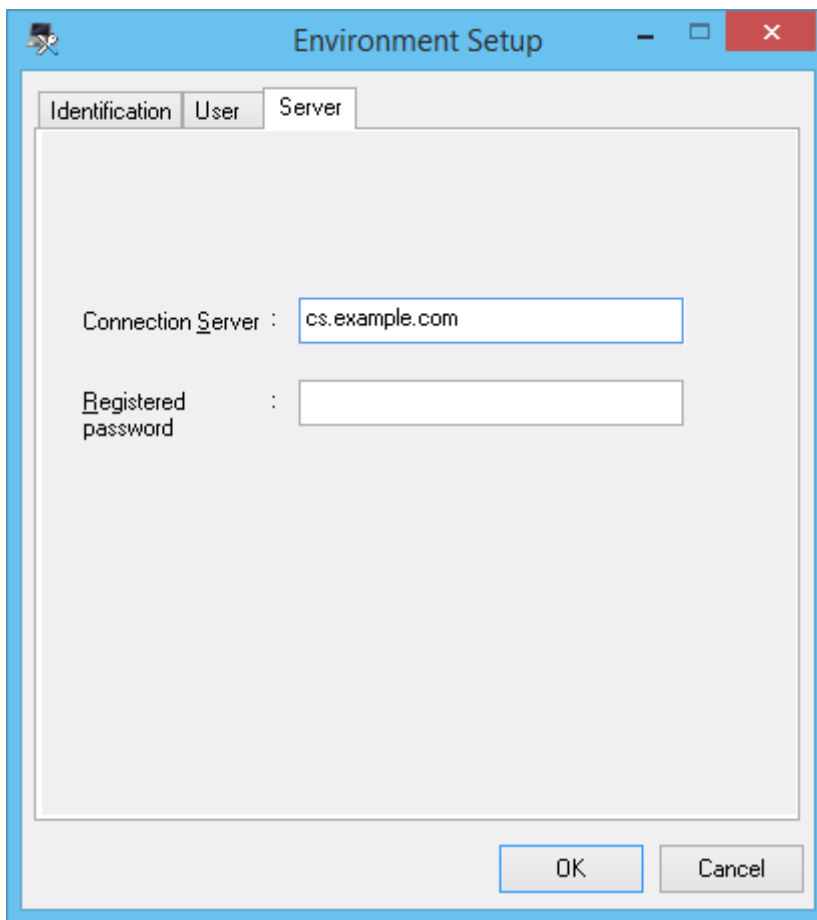
7. The **Installation Completed** window is displayed after the processing is completed normally. Click the **Finish** button. If **Server Name (with Remote Operation)** was selected, restart the operating system.
If this component was installed without the remote operation feature, inventory collection can be performed automatically after installing Systemwalker Desktop Patrol CT. If this component was installed with the remote operation feature, inventory collection will be performed automatically after the operating system is restarted.

📖 Note

When the user ID and PC name have been modified after installation

After Systemwalker Desktop Patrol CT installation is completed and the user ID or PC name has been modified, Inventory notification will be performed immediately after the modification. Thus, it is likely that even if Inventory viewing menu of the main menu has been selected, Inventory cannot be viewed.

When performing Inventory notification after the user ID or PC is modified, select **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Inventory Collection**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Inventory Collection** to perform Inventory collection.

2.7.2 Perform CT Silent Installation

The procedures for CT silent installation: besides, for the operating environment, refer to *Systemwalker Desktop Patrol User's Guide*.

Besides, silent installation cannot be performed in the security mode.

📝 **Note**

. . . .

About the execution in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012

When executing this command in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012, execute this command in the command prompt operated with the administrator authority.

. . . .

CT program supporting silent installation is saved in DVD-ROM of Systemwalker Desktop Patrol. Install it after combining it with the user ID and PC name default settings of CT environment setup of the client policy.

The installation procedures are as follows:

Issues to be confirmed before installation

- End the following programs before installation.

  - Resident programs included virus scanning program.

  - The **Service** window of Windows

1. Copy "utilities\silent\CTSetup.exe" of Systemwalker Desktop Patrol DVD-ROM to the local directory of Systemwalker Desktop Patrol CS.

2. After backing up "\Inetpub\wwwroot\DTP\CT\CTSetup.exe" of system disk, replace to the copied "CTSetup.exe" in Procedure "1.".

3. Log on to the main menu, select the **Environment Setup** > **Policy Groups** > **Customize Various Policies** > **Basic operation policy** > **Common Settings** tab, and set the **Set Initial Value** item of **CT Environment Setup**. If you are using a file containing default values, use CustomPolicy.exe (policy for modifying custom setup command) to specify it.

4. Display **Set CS** of **Environment Setup** > **CS/DS Settings and Status** of the main menu.

5. Without modifying any information in the displayed window, click the **OK** button directly.

6. Because "\Inetpub\wwwroot\DTP\CT\CT_Setup.exe" and "\Inetpub\wwwroot\DTP\CT\CTLH_Setup.exe" replaced in Procedure 2. will be created again, so confirm the update date has been modified.

   (Here, it will change to the operation of creating CT downloading module of the download menu again.)

7. If remote operation is not required, download "CT (CT_Setup.exe)" from the download menu and save it to the local directory. If remote operation is required, download "CT(CTLH_Setup.exe)" from the download menu and save it to the local directory.

8. Execute "CT_Setup.exe" or "CTLH_Setup.exe" downloaded in Procedure 7., get the default value set in Procedure 3. and perform silent installation. When using "File with Default Value Saved", the "File with Default Value Saved" should be saved to the environment variable "windir" or "TEMP" before executing "CT_Setup.exe" or "CTLH_Setup.exe".

   About the execution in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012

   In Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012, common administrator user cannot access the environment variable "windir" folder. Thus, save this file to the environment "TEMP" when using "File with Default Value Saved".

2.7.3 Installation in an Active Directory Environment

This section explains how to extract the CT in an Active Directory environment.

Overview of how to extract the CT

The flow of CT extraction in an Active Directory environment is shown below.

a. Extract the CT in a management target PC.

b. The flow of extraction is as follows:
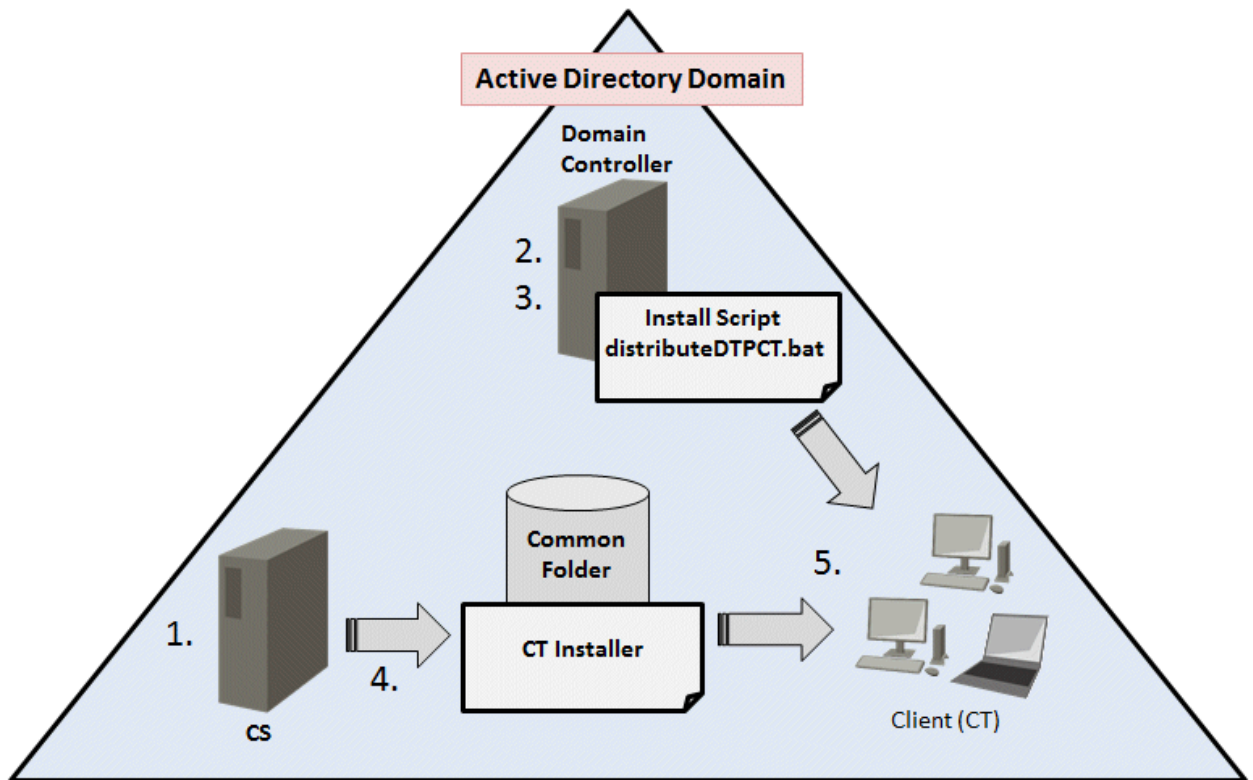
1. Create a CT program that supports silent installation

2. Edit the "distributeDTPCT.bat" installation script

3. Prepare the group policy

4. Deploy the resource created in step 1

5. Automatically install the CT in the PC to which the group policy is applied

c. Ensure that the extracted CT has been installed correctly.

d. Delete the information defined for extraction.

🖐 Note

- In this procedure, CT is extracted using the startup script for the Active Directory group policy so the CT will be installed with the SYSTEM account.

- This procedure supports new installations only.

- Execute this procedure as a user with administrator privileges.

- The installation script contains a non-encrypted password. It is the responsibility of the user to manage the installation script.

2.7.3.1 Create a CT Program that Supports Silent Installation

Create a CT program that supports silent installation. Refer to the item numbers 1 to 7 in "Issues to be confirmed before installation" for details.

2.7.3.2 Edit the Installation Script

Edit the installation script in accordance with the environment.

File name

distributeDTPCT.bat

The file is stored under the "utilities\distribute" directory on the Systemwalker Desktop Patrol DVD-ROM.

Format

The sections to be edited is as follows:

```
set SHARE_DIR=uncPathForTheSharedFolderContainingCtPgm

set SHARE_ID=userIdToAccessFolderSpecifiedInShareDirEnvVar

set SHARE_PW=passwordOfUserIdSpecifiedInShareIdEnvVar

set INSTALLER_NAME=ctPgmName
```

Parameters

The table below explains the values set for the installation script.

No.	Environment variable	Default value	Description
1	SHARE_DIR	None	UNC path for the shared folder containing the CT program is stored. This environment variable is required. This value will be used in "2.7.3.3 Register the Group Policy".
2	SHARE_ID	None	User ID used to access the folder specified in SHARE_DIR. Specify a user with write permission to the folder.
3	SHARE_PW	None	Password of the user specified in SHARE_ID.
4	INSTALLER_NAME	CT_Setup.exe	Name of the CT program created in "2.7.3.1 Create a CT Program that Supports Silent Installation". This environment variable is required.

Example

Example of edited installation script is shown below:

```
set SHARE_DIR=\\192.168.10.10\share

set SHARE_ID=user1@domain.local

set SHARE_PW=hogehoge1!

set INSTALLER_NAME=CT_Setup.exe
```

📌 **Note**

. . . .

- If SHARE_ID and SHARE_PW are omitted, the local SYSTEM account will be used to access SHARE_DIR.

- If connection to SHARE_DIR using SHARE_ID and SHARE_PW fails, the local SYSTEM account will be used to access SHARE_DIR.

. . . .

2.7.3.3 Register the Group Policy

This section explains how to register in the Active Directory group policy.

It is recommended to register the group policy in a small number of PCs and perform extraction tests first.

For Windows Server 2008 and Windows Server 2012

1. Click **Start** > **Administrative Tools** > **Group Policy Management**.

2. In the **Group Policy Management** window, click **Forest:** *domain* > **Domains** > *domain*.

3. Create a Group Policy Object in the group where the computer on which the CT will be extracted exists.
   If you are using an existing GPO, there is no need to create another one.

4. Right-click the GPO to be used, and click **Edit**.

5. In the **Group Policy Management Editor** window, click **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)**.
   In the right pane, right-click **Startup** and click **Properties**.

6. In the **Startup Properties** dialog box, click **Add**.
   In the **Add a Script** dialog box, enter "distributeDTPCT.bat" in **Script Name**, and click **OK**.

7. Copy "distributeDTPCT.bat" to the folder displayed by clicking **Show Files**.

8. Copy the CT program that supports silent installation to the folder specified for the SHARE_DIR environment variable in the installation script.

9. In the **Startup Properties** dialog box, click **OK** to enable the settings.

10. In PCs where the group policy is applied, the CT will be automatically installed during startup.

Note

The operating system in PCs on which the CT is extracted must be restarted after installation is completed.

2.7.3.4 Check the Installation Results

Use one of the following procedures to check if the CT extraction was completed normally.

- View **PC Information** in the main menu to check if the inventory information is collected from the PC where the extracted CT was installed.

- Check the installation script log output to the location below:

    - Folder

      If completed normally: *folderSpecifiedInShareDirEnvVar*\DTP\log\

      If did not complete normally: *folderSpecifiedInShareDirEnvVar*\DTP\log\error\

    - File

      yyyyMmDdHhMmSs.millisec_computerName.log (Example: 20140424120000.85_COMPUTER1.log)

If installation did not complete normally, refer to the installation result log and take appropriate action.

2.7.3.5 Cancel the Group Policy

Once CT extraction is completed, cancel the group policy.

For Windows Server 2008 and Windows Server 2012

1. Click **Start** > **Administrative Tools** > **Group Policy Management**.

2. In the **Group Policy Management** window, click **Forest:** *domain* > **Domains** > *domain*.

3. Right-click the GPO of the group in which the CT is extracted, and click **Edit**.

4. In the **Group Policy Management Editor** window, click **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)**.
   In the right pane, right-click **Startup** and click **Properties**.

5. In the **Startup Properties** dialog box, click "distributeDTPCT.bat" and click **Remove**.

6. Remove "distributeDTPCT.bat" from the folder displayed by clicking **Show Files**.

7. Remove the CT program that supports silent installation from the folder specified for the SHARE_DIR environment variable in the installation script.

8. In the **Startup Properties** dialog box, click **OK** to enable the settings.

9. Remove the GPO selected in step 3.

   If the GPO is used for other purposes, then it is not necessary to remove it.

2.7.4 Install through CT Kitting Expansion

To expand CT through Kitting, save the CT program without settings information to DVD-ROM of Systemwalker Desktop Patrol. After executing this CT program and install it to PC, use DtpKitingCT.exe (CT operating environment change) command for information setting. Some CT programs include remote operation while other CT programs do not.

The setting procedures are as follows.

1. Copy the following files of Systemwalker Desktop Patrol DVD-ROM to the local directory.
   If remote operation is not required, copy the following three files:

   - "utilities\tool\kitting\CT_Setup.exe"

   - "utilities\tool\kitting\DtpKitingCT.dat"

   "utilities\tool\kitting\DtpKitingCT.exe"

   If remote operation is required, copy the following three files:

   "utilities\tool\kitting\CTLH_Setup.exe"

   - "utilities\tool\kitting\DtpKitingCT.dat"

   - "utilities\tool\kitting\DtpKitingCT.exe"

2. If remote operation is not required, execute the copied "CT_Setup.exe" to install CT.
   If remote operation is required, execute the copied "CTLH_Setup.exe" to install the CT.

3. Use DtpKitingCT.exe (CT operating environment change) command for information setting.

   Besides, when using the command, save "DtpKitingCT.dat" to the folder same as "DtpKitingCT.exe".
   Also, if you are installing a CT program that includes remote operation, restart the operating system after installation is completed.

When performing CT Kitting expansion, create PC hard disk mirror image in "Procedure 2" and execute "Procedure 3" after copying to other PC.

For DtpKitingCT.exe (CT operating environment change) command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

Note

Systemwalker Desktop Patrol CT downloaded and installed through download menu Systemwalker Desktop Patrol CT in use already cannot be used for Kitting expansion.

2.7.5 Install to Virtual Desktop Environment

This section describes the procedures for installing CT to the virtual desktop.

According to the method for constructing the virtual desktop environment, method for installing CT need be modified.

It is described in this item according to the following order.

- System structure of the virtual desktop environment

- Install to virtual PC expanded on the virtual PC server

- Install to the terminal server

- Install to blade PC

2.7.5.1 System Structure of Virtual Desktop Environment

System structure chart of virtual desktop environment (summary) is as follows:
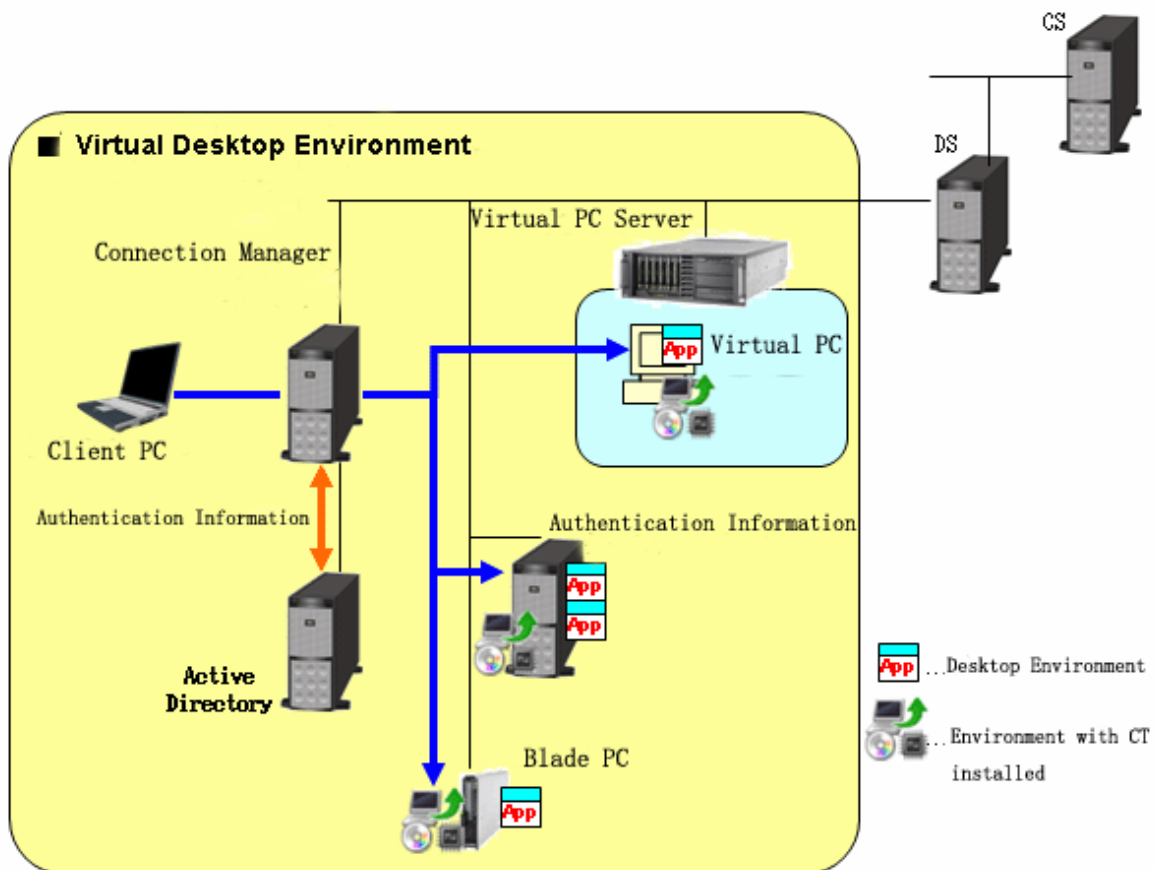
- Virtual Desktop Environment

   The user access "Desktop Environment" from Client PC via connection manager. Connection Management Server performs Active Directory authentication according to the requirements of Client PC and then distributes "Desktop Environment".

- Desktop Environment

   The desktop environment can be used in the following 3 cases

   CT is installed to PC with license management software installed (virtual PC, terminal service, blade PC).

   1. The virtual PC expanded on virtual PC server

       Multiple virtual PCs in the virtual PC server are prepared and use this PC.

   2. Terminal server

       Physical PC is used.

       Multiuser share the OS of the connection target and multiple desktop environments exist.

3. Blade PC

   Physical PC is used.

   The user uses the OS exclusively and single desktop environment exists.

2.7.5.2 Install to Virtual PC Expanded on Virtual PC Server

When installing to the virtual PC expanded on the virtual PC server, the method for constructing desktop environment is divided to "when deployed automatically by system" and "when deployed manually by administrator".

Point

How to construct virtual desktop environment

1. When deployed automatically by system (link clone and automatic desktop pool)
   After the desktop environment is copied through system mapping, the desktop environment with the same content with system mapping will be created. Increment data of system mapping is accumulated on the virtual PC.
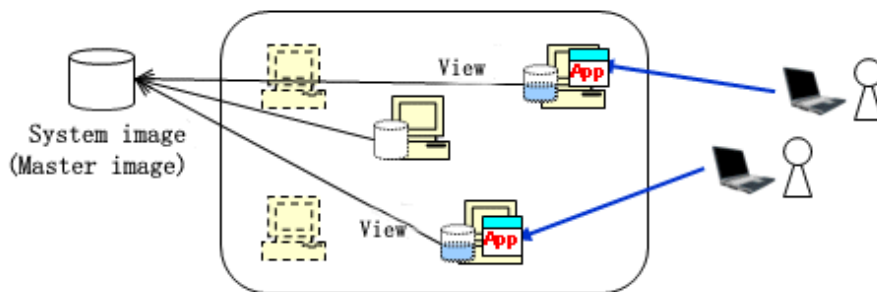
Through connection of user, the desktop environment is allocated to virtual PC pool automatically. Or, the desktop environment of required number will be copied automatically.

2. When deployed manually by the administrator (complete clone)
   Create the desktop environment which has not viewed system mapping. Besides, create the dedicated virtual PC for connecting user and save all data containing OS to virtual PC.
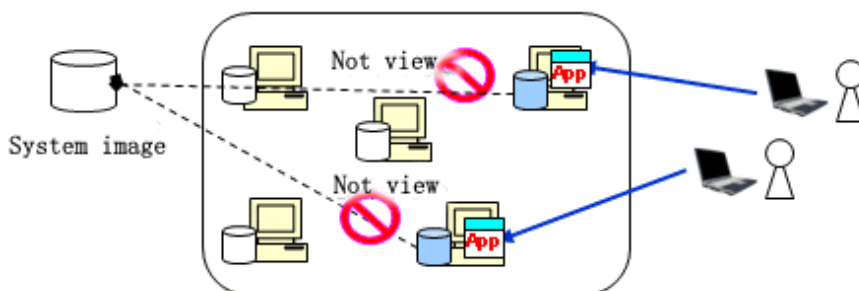
Create virtual PC in advance and allocate it as the environment for special use by use to be connected.

The following describes CT installation procedures when using the following deployment method.

When deployed automatically by system (link clone and automatic desktop pool)

1. Create policy group and register the created **Basic operation policy** and PC.

   After logging on to the main menu, click the **Customize various policies** button in the **Environment Setup** > **Policy Groups** window and click the link of policy name in the **Basic Operation Policy** tab, then the following window is displayed.

   Perform **CT Environment Setup** > **Set the initial value** of the basic operation policy (Systemwalker Desktop Patrol Policy Setting).

   Set "Logon user ID" in **User ID**. "Domain Name" is recommended in **PC Name**.

2. The administrator downloads CT Package through the download menu and installs CT Package in system mapping.

3. To deploy in the desktop pool, start the desktop environment through the virtual PC server.
   CT detects the copying of the desktop and initializes user identification information.

4. Through the connection from Client PC, reset the user identification information.
   CT judges the policy set in 1. and reset the user identification information based on the logon information.
   If automatic resetting has not been set, define the user identification information through the environment setting window.

When deployed manually by the administrator (complete clone)

1. The administrator uses and installs Kitting CT Package in system mapping.

2. The administrator creates the virtual PC using system mapping and prepares the desktop environment.

3. The administrator uses DtpKitingCT.exe (CT operating environment change command) to define the user identification information (user ID, PC name, connection target server).

2.7.5.3 Install to Terminal Server

When installing to terminal server, install according to the procedures for installing common CT.

2.7.5.4 Install to Blade PC

When installing to blade PC, install according to the procedures for installing common CT in case of not performing desktop copying (Master copying).

The procedures for installing CT if desktop copying (Master copying) between blades has been performed are as follows:

1. Create policy group and register the created **Basic operation policy** and PC.

   After logging on to the main menu, click the **Customize Various Policies** button in the **Environment Setup** > **Policy Groups** window and click the link of policy name in the **Basic Operation Policy** tab, then the following window is displayed.

   Perform **CT Environment Setup** > **Set Initial Value** of the basic operation policy (Systemwalker Desktop Patrol Policy Setting).

   Set "Login user ID" in **User ID** and set "Computer Name" in **PC Name**.

2. The administrator downloads CT Package through the download menu and installs CT Package in system mapping.

3. The administrator or system performs desktop copying.
   CT detects desktop copying and initializes the user identification information.

4. Through the connection from Client PC, reset the user identification information.
   CT judges the policy set in 1., and reset the user identification information based on the logon information.
   If automatic resetting has not been set, define the user identification information through environment setting window.

2.8 Build SS

This section explains how to install and configure the Systemwalker Desktop Patrol SS, used to manage smart device assets in Systemwalker Desktop Patrol.

Note

Note that, if the smart device assets are managed in an intranet environment only, then the SS and CS can coexist. To enable the SS and CS to coexist, the CS must be installed before the SS.

2.8.1 Install SS

This section explains how to install SS.

There are two ways to install SS:

2.8.1.1 Installation using the Wizard

Follow the steps below to install SS using the wizard:

Installation procedure

1. Insert the Systemwalker Desktop Patrol DVD-ROM in the PC.
   In the window below, select **SS Installation**.
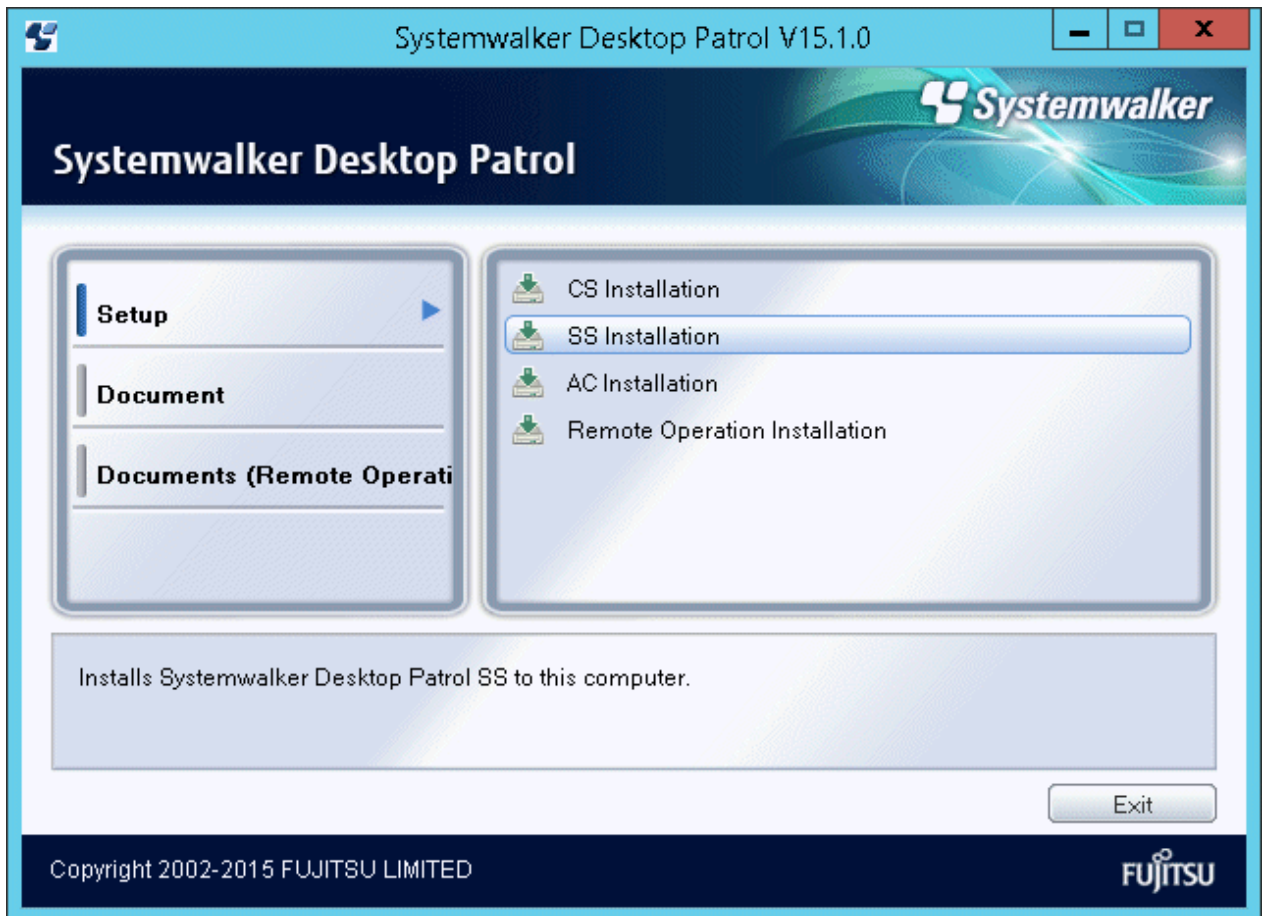
2. Specify the installation directory.

3. Once installation is completed, a message prompting the restart of the system may be displayed. Ensure that the system can be restarted, and then proceed according to the message.

2.8.1.2 Silent Installation

📖 Note

- Silent installation can only be performed when you are performing installation for the first time.

- Installation process must not be interrupted during silent installation.

Follow the steps below to perform silent installation:

1. Create an installation parameter CSV file.

   Refer to "A.3.1 Installation Parameter CSV File" for details.

   If you are performing installation using the default values for all parameters, this step is not required.

2. Use the parameter setup command to create a response file.

   Refer to "A.3.2 Parameter Setup Command" for details.

   If you did not create an installation parameter CSV file in step 1, this step is not required.

3. Execute the silent installation command.

   Refer to "A.3.4 Silent Installation Command" for details.

4. Check the installation result in the returned value and message from the silent installation command.

Refer to "A.3 Silent Installation of SS" for details on the files and commands used in, and messages output in silent installation.

2.8.2 Configure the Operating Environment for SS

This section explains how to configure the operating environment for the SS.

2.8.2.1 Configuration Based on Managed Smart Devices

Configure the following settings for managed smart devices (Android or iOS).

Android

1. Enable management of Android devices
   Execute swss_config.exe (SS environment setup command) with the /Android.enabled option

2. Specify the IP address or host name of CS.
   Execute swss_config.exe with the /cs.host option.

3. If necessary, change the port number.
   Refer to "How to Modify the Port Number" in the *Systemwalker Desktop Patrol Reference Manual* for details.

4. Configure the settings for HTTPS communication and build the certificate environment.
   Refer to "2.8.2.2 Settings for HTTPS Communication" for details.
   This step is also performed if iOS devices are managed. If managing both Android and iOS devices, perform this step only once.

5. Use SWDTP_ctrl.exe (batch starting services command) to start Systemwalker Desktop Patrol.

iOS

P Point
. . . .

Steps 1 to 4 can be perform in a single command execution.
. . . .

1. Enable management of iOS devices
   Execute swss_config.exe (SS environment setup command) with the /iOS.enabled option

2. Specify the IP address or host name of CS.
   Execute swss_config.exe with the /cs.host option.
   This step is also if performed if Android devices are managed. If managing both iOS and Android devices, execute this step only once.

3. Specify the server or reverse proxy to be connected from iOS devices.
   Execute swss_config.exe with the /iOS.connect.host, /iOS.connect.port, and /iOS.connect.profile.port. options.

4. Specify the IP address or host name of the iOS management database.
   Execute swss_config.exe with the /iOSmgr.host option.
   If iOS devices are being managed only by Systemwalker Desktop Patrol, specify the CS. But if they are also being managed by Systemwalker Desktop Keeper, specify either the CS or the Systemwalker Desktop Keeper management server that is operating the iOS management database. Once set, do not change this value.

5. If necessary, change the port number.
   Refer to "How to Modify the Port Number" in the *Systemwalker Desktop Patrol Reference Manual* for details.

6. Configure the settings for HTTP communication and build the certificate environment.
   Refer to "2.8.2.2 Settings for HTTPS Communication" for details.
   This step is also performed if Android devices are managed. If managing both Android and iOS devices, perform this step only once.

7. Use swss_ImportAppleCert.bat (registering Apple Inc. certificates command) to install the MDM certificate prepared in "2.2 Advance Preparation".

8. Use SWDTP_ctrl.exe (batch starting services command) to start Systemwalker Desktop Patrol.

Note

Notes regarding coexistence with the Systemwalker Desktop Keeper Smart Device Relay Server

- The following options of swss_config.exe (SS environment setup command) in steps 1 to 5, are only used in Systemwalker Desktop Patrol.
  - /cs.host
  - /cs.port
  - /Android.http.port
  - /Android.https.port
  - /Android.enabled
  - /usercert.enabled
  - /iOS.enabled

- The following options of swss_config.exe (SS environment setup command), are common options also used in Systemwalker Desktop Keeper.
  - /iOSmgr.host
  - /iOSmgr.port
  - /iOS.profile.port
  - /iOS.https.port
  - /iOS.connect.host
  - /iOS.connect.port
  - /iOS.connect.profile.port

- The items set in steps 6 and 7 are also used in Systemwalker Desktop Keeper.

- For items also used in Systemwalker Desktop Keeper, specify the same values in both products.
  After the items are set in Systemwalker Desktop Patrol, specifying different values in Systemwalker Desktop Keeper will result in the settings initially configured in this product changed to the new values specified in Systemwalker Desktop Keeper. Conversely, after the items are set in Systemwalker Desktop Keeper, specifying different values in this product will result in the settings initially configured in Systemwalker Desktop Keeper changed to the new values specified in this product.

2.8.2.2 Settings for HTTPS Communication

To use HTTPS communication between SS and the smart device CT, configure the settings as shown below. The configuration procedure depends on whether the server certificate is prepared by the customer or is the Systemwalker certificate.

Note

If this product coexists with the smart device relay server of Systemwalker Desktop Keeper and a certificate is registered in Systemwalker Desktop Keeper after another certificate is registered in Systemwalker Desktop Patrol, then the certificate registered in Systemwalker Desktop Keeper will be the one used for HTTPS communication between iOS smart devices and the SS.

Settings during installation

During installation, follow the steps below to configure the settings.

If the server certificate is prepared by the customer

1. Use swss_makecsr.exe to generate the certificate signature request for the server certificate.

2. Send the certificate signature request generated in step 1 to the CA, to obtain the CA certificate (intermediate CA certificate) and server certificate issued by the CA.

3. Use SWDTP_ctrl.exe to stop Systemwalker Desktop Patrol.

4. Use swss_importcert.exe to register the CA certificate (intermediate CA certificate) obtained in step 2.

5. Use swss_importcert.exe to register the server certificate obtained in step 2.

6. Use swss_config.exe to enable the use of the server certificate prepared by the customer.

7. Use SWDTP_ctrl.exe to start Systemwalker Desktop Patrol.

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on these commands.

📝 Note
∙∙∙

If step 5 is mistakenly performed before step 4, restart the procedure from step 1.
∙∙∙

If using the Systemwalker certificate

1. Execute swss_makecsr.exe with the /certfile option to generate a server certificate.

2. Use SWDTP_ctrl.exe to stop Systemwalker Desktop Patrol.

3. Execute swss_importcert.exe with the /CACERT option to register the CA certificate for Systemwalker.

4. Use swss_importcert.exe to register the server certificate obtained in step 1.

5. Use swss_config.exe to enable the use of the Systemwalker server certificate.

6. Use SWDTP_ctrl.exe to start Systemwalker Desktop Patrol.

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on these commands.

📝 Note
∙∙∙

If step 4 is mistakenly performed before step 3, repeat the procedure from step 1.
∙∙∙

Certificate renewal settings

Follow the steps below to configure the certificate renewal settings:

If the server certificate is prepared by the customer

1. Use swss_makecsr.exe to generate the certificate signature request for the server certificate.

2. Send the certificate signature request generated in step 1 to the CA, to obtain the server certificate issued by the CA.

3. Use SWDTP_ctrl.exe to stop Systemwalker Desktop Patrol.

4. Use swss_importcert.exe to register the server certificate obtained in step 2.

5. Use SWDTP_ctrl.exe to start Systemwalker Desktop Patrol.

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on these commands.

If using the Systemwalker certificate

1. Execute swss_makecsr.exe with the /certfile option to generate a server certificate.

2. Use SWDTP_ctrl.exe to stop Systemwalker Desktop Patrol.

3. Use swss_importcert.exe to register the server certificate obtained in step 1.

4. Use SWDTP_ctrl.exe to start Systemwalker Desktop Patrol.

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on these commands.

2.9 Install Smart Device CT (Android)

This section explains how to install and configure smart device CT (Android).

2.9.1 Install Smart Device CT (Android)

This section explains how to install smart device CT on the smart device that will manage the assets through inventory information collection.

Either of the following methods can be used to install smart device CT:

- Using smart device CT distributed by the administrator

  Refer to "2.9.1.1 Use Smart Device CT Distributed by the Administrator" for details.

- Downloading smart device CT from the Internet

  Refer to "2.9.1.2 Download Smart Device CT from the Internet" for details.

2.9.1.1 Use Smart Device CT Distributed by the Administrator

The administrator distributes the smart device CT apk file to the smart device user, which then installs it on each smart device.

The following methods can be used to distribute the smart device CT file:

- Copy it to an SD card (a file operation application may be required to install the smart device CT)

- Publish on a Web server within the company (so that it can be downloaded using a smart device)

- Send via email to each smart device user

To download the apk file, from the Systemwalker Desktop Patrol download menu, click **CT Download** > **CT for Smart devices**.

To install the smart device CT, follow the steps below (the example screens are from Android 4.1).

1. Open the distributed apk file and tap **Install**.
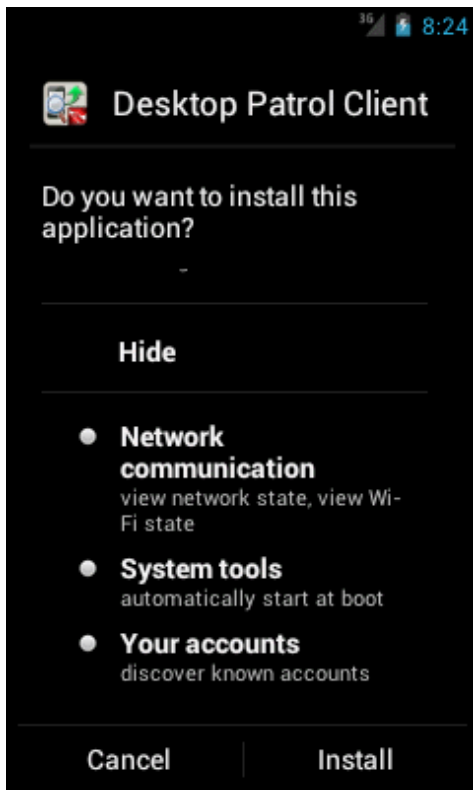
2. To start smart device CT after installation, tap **Open**.
   If you do not want to start smart device CT just yet, tap **Finish**.
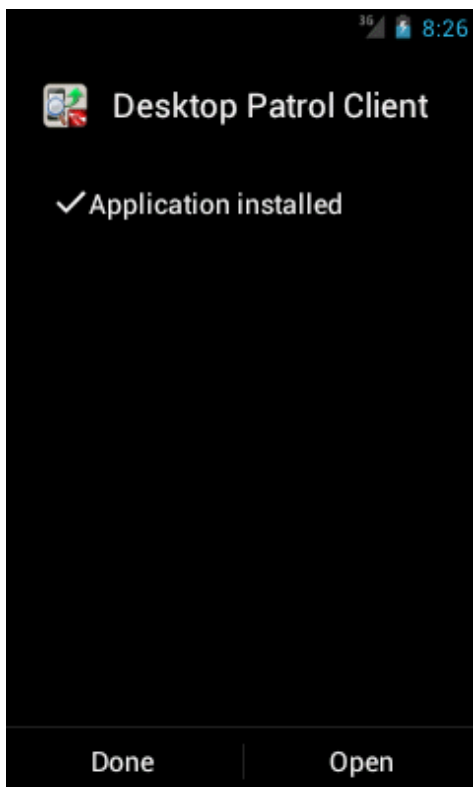
 Note

If a warning screen is displayed

If a warning screen is displayed during installation, you must change the settings and perform the installation again.

1. Tap **Settings**.
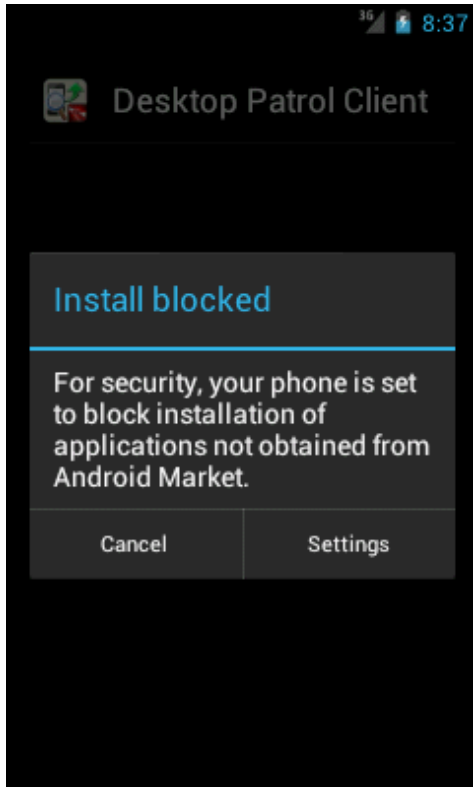
2. Select **Unknown sources**.
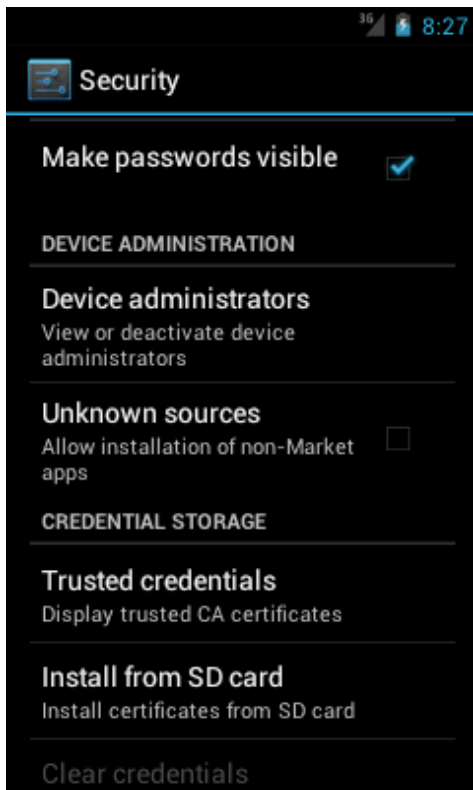
3. A confirmation dialog box will be displayed. Tap **OK**.

4. Perform installation again.

5. After installation is complete, open the settings screen and clear **Unknown sources**.

    The **Unknown sources** setting depends on the version.

    - Android 3.0 to 3.2: **Settings** > **Applications**

- Android 4.0 or later: **Settings** > **Security**

....
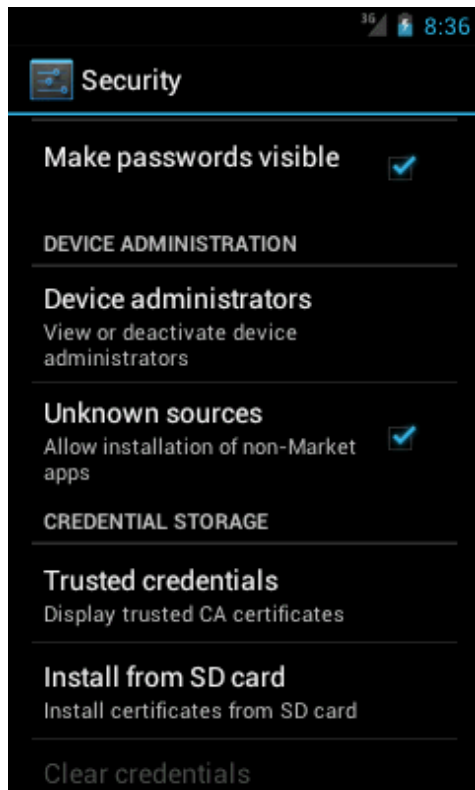
2.9.1.2 Download Smart Device CT from the Internet

The smart device user downloads Systemwalker Desktop Patrol Client from Google Play and installs it.

2.9.2 Smart Device CT (Android) Settings

This section explains how to configure smart device CT (Android) settings.

Follow the steps below to configure the settings:

1. Start the installed smart device CT.

2. If the screen below is displayed when the installed smart device CT is started, tap (or click) **Activate**.
   After you have activated, this screen will not be displayed following startup.
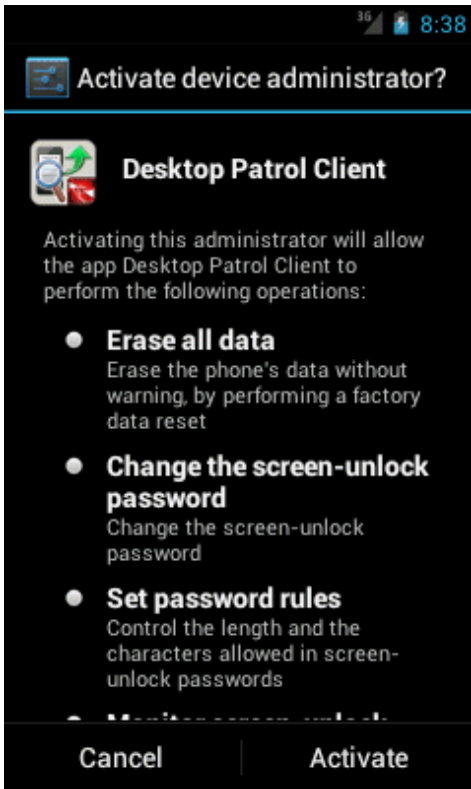
3. After starting the installed smart device CT, tap (or click) the menu button to display the options menu. Then tap **Settings**.
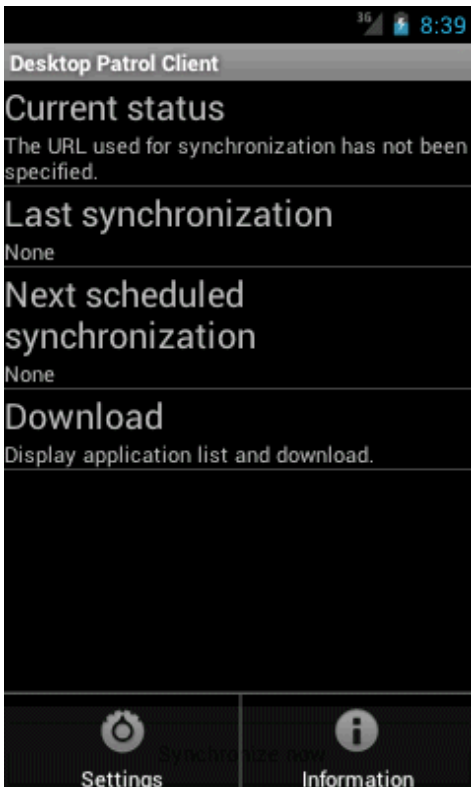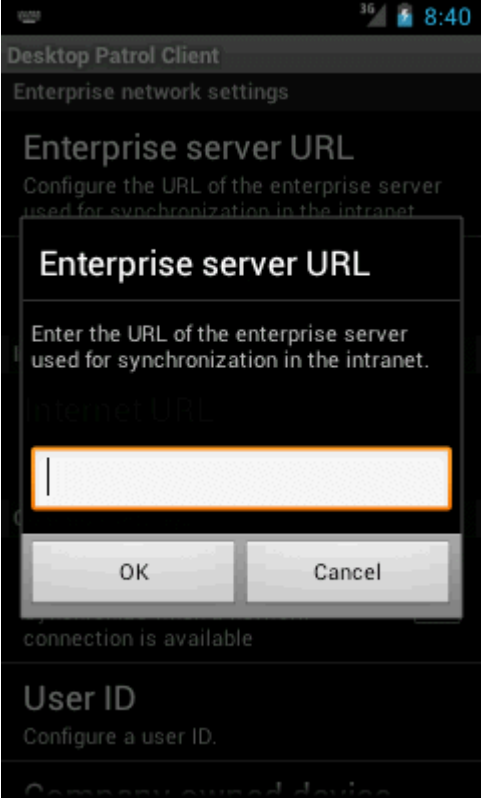
4. The setup screen will be displayed. Configure the following setting in accordance with the actual environment.

   You must set **Enterprise server URL** or **Internet URL**.
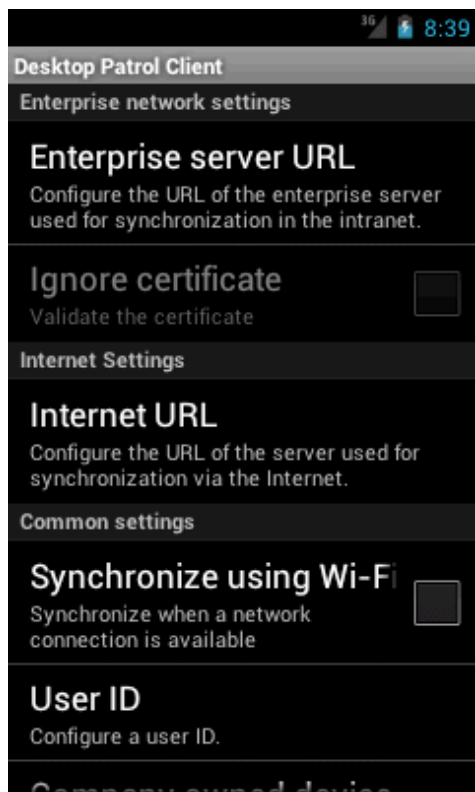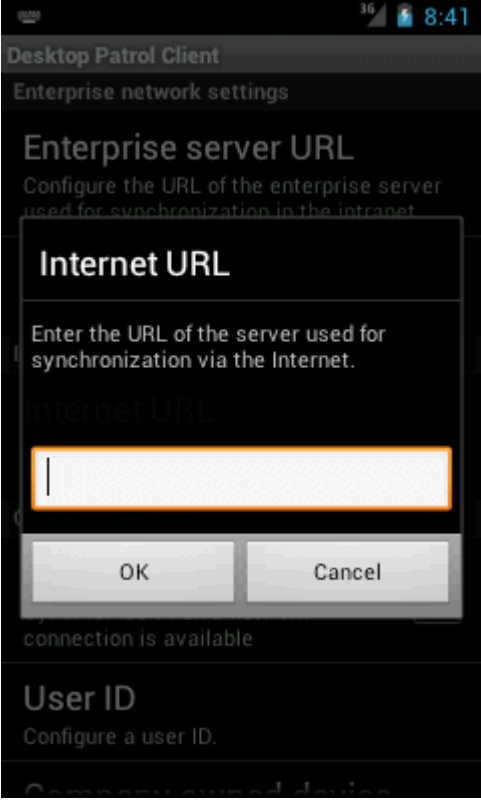
   - Enterprise network settings

Item	Description
Enterprise server URL	Specify the URL of the enterprise server to be used for synchronization within the intranet.

Item	Description
	Enter one of the following URLs, and then tap **OK**: - http://*ssHostNameOrIpAddress:portNumber*/swss/ - https://*ssHostNameOrIpAddress:portNumber*/swss/ - Reverse proxy server URL Refer to "Port Number List" in the *Systemwalker Desktop Patrol Reference Manual* for details on the port number used. If the URL starts with "http://" the default value is 38080, and if the URL starts with "https://" it is 38181. If no URL is set, inventory information will not be synchronized in the enterprise network environment.
Ignore certificate	Select this item when certificates will not be authenticated in the enterprise network. This option becomes available when you enter a URL beginning with "https://" for **Enterprise server URL**. By default, this item is not selected, so certificates will be authenticated.
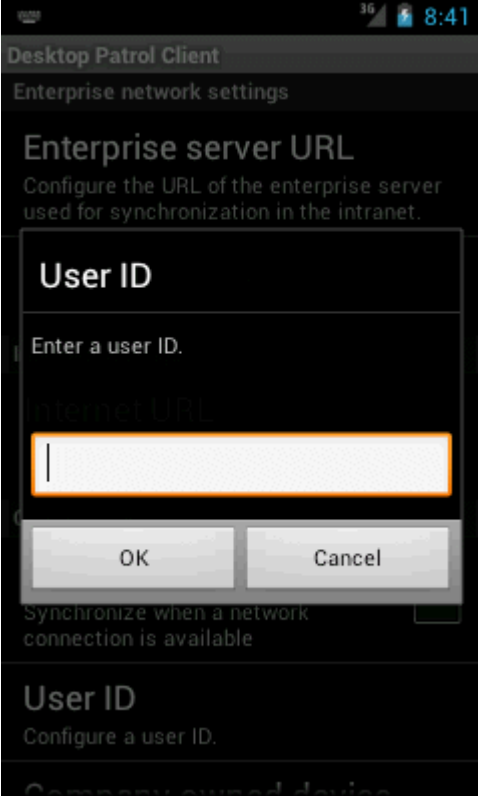
- Internet settings

Item	Description
Internet URL	Set the URL of the server to be used for synchronization via the Internet.

Item	Description
	Enter the URL of the Web server (reverse proxy server) used for Internet connection starting with "http://" or "https://", and then tap **OK**. If no URL is set, inventory information will not be synchronized in the Internet environment.

- Common settings (optional settings)

Item	Description
Synchronize using Wi-Fi connection	Select this item to synchronize inventory information only when the device is connected to a network by Wi-Fi. By default, this item is not selected, so inventory information will be synchronized when the device is connected to the network by Wi-Fi, 3G network, or other means.
User ID	Register the user ID registered in user management of Systemwalker Desktop Patrol.

Item	Description
	Registering the user ID enables you to identify, from the main menu, the smart device user and the department to which the user belongs.
	You can specify up to 20 halfwidth alphanumeric characters, and the following symbols: - @ . _
	Alphabetic characters are case-sensitive.
	If you omit the user ID, "MobileUser" is displayed as the user ID in smart device information referenced from the main menu.
Company owned device	Select this item when using a company owned device.
	By default, this item is selected, so clear it if you are using a personal device. The confirmation screen shown below is displayed only when this item is cleared. Tap **I agree** if you are using a device you bought and own yourself.

5. Tap (or click) **Back**.

6. The first time you configure this setting, the message **Synchronize now?** will be displayed. To start synchronization immediately, tap **Yes**. To start synchronization the next time automatic synchronization is implemented, tap **No**.

 Ⓟ Point

∙∙∙

Timing of inventory information synchronization

Inventory information is automatically synchronized once a day, but you can also synchronize it at any time during operations.

Refer to "How to Synchronize the Inventory Information" in the *Systemwalker Desktop Patrol Operation Guide: for Administrators* for details.

∙∙∙

2.10 Install Smart Device CT (iOS)

The iOS device user accesses the URL provided by the administrator and installs smart device CT.

Advance tasks for the administrator

Send the following URL to the iOS device user.

> https://*ssHostNameOrIpAddress*:*portNumber*/mdmi/systemwalker/

- The host name and IP address to be published must match the values specified in the /CN option for swss_makecsr.exe (generating certificate signature requests command). If they do not match, an error will be detected in certificate verification.

- Set up a network so that the host name and IP address to be published can only be accessed within the company.

- Specify the port number using swss_config.exe (SS environment setup command) with the ./iOS.connect.profile.port option.

  The default port number is 50080.

Tasks for the iOS device user

1. Access the URL provided by the administrator.
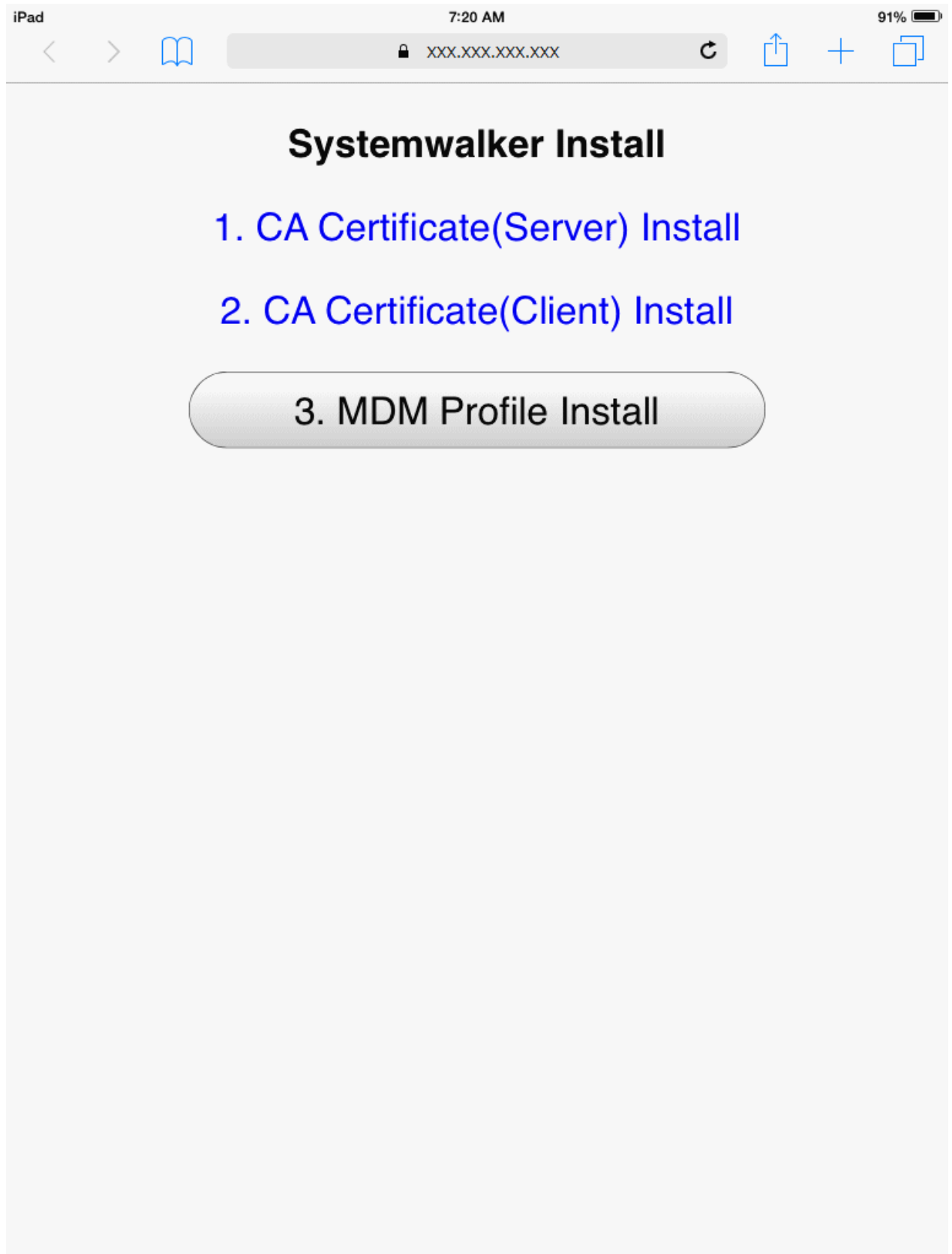
Note

2. Tap **1. CA Certificate (Server) Install**

3. The screen for installing the CA certificate will start on the iOS device. Tap **Install**.

4. The installation message **The authenticity of "Identify Certificate" cannot be verified. Installing this profile will change settings on your iPad (iPhone)** is displayed. Tap **Install Now** to proceed. If you have set a pass code lock on the iOS device, you must enter the pass code during installation.

5. After the CA certificate is installed, the screen shown below is displayed. Tap **Done**.
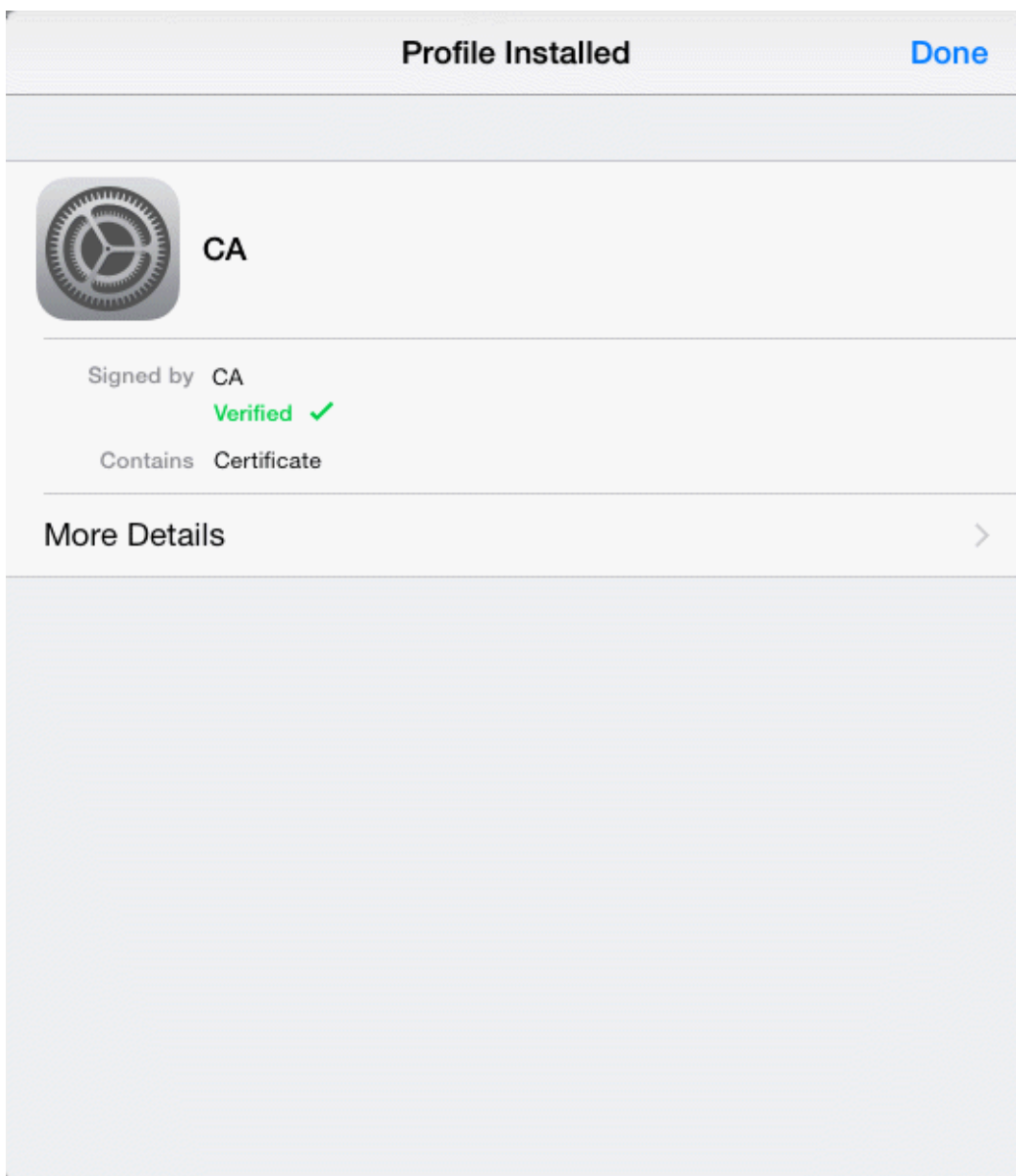
6. Tap **2. CA Certificate (Client) Install**

7. The screen for installing the CA certificate will start on the iOS device. Tap **Install**.

8. The installation message **The authenticity of "Identify Certificate" cannot be verified. Installing this profile will change settings on your iPad (iPhone)** is displayed. Tap **Install Now** to proceed. If you have set a pass code lock on the iOS device, you must enter the pass code during installation.

9. After the CA certificate is installed, the screen shown below is displayed. Tap **Done**.
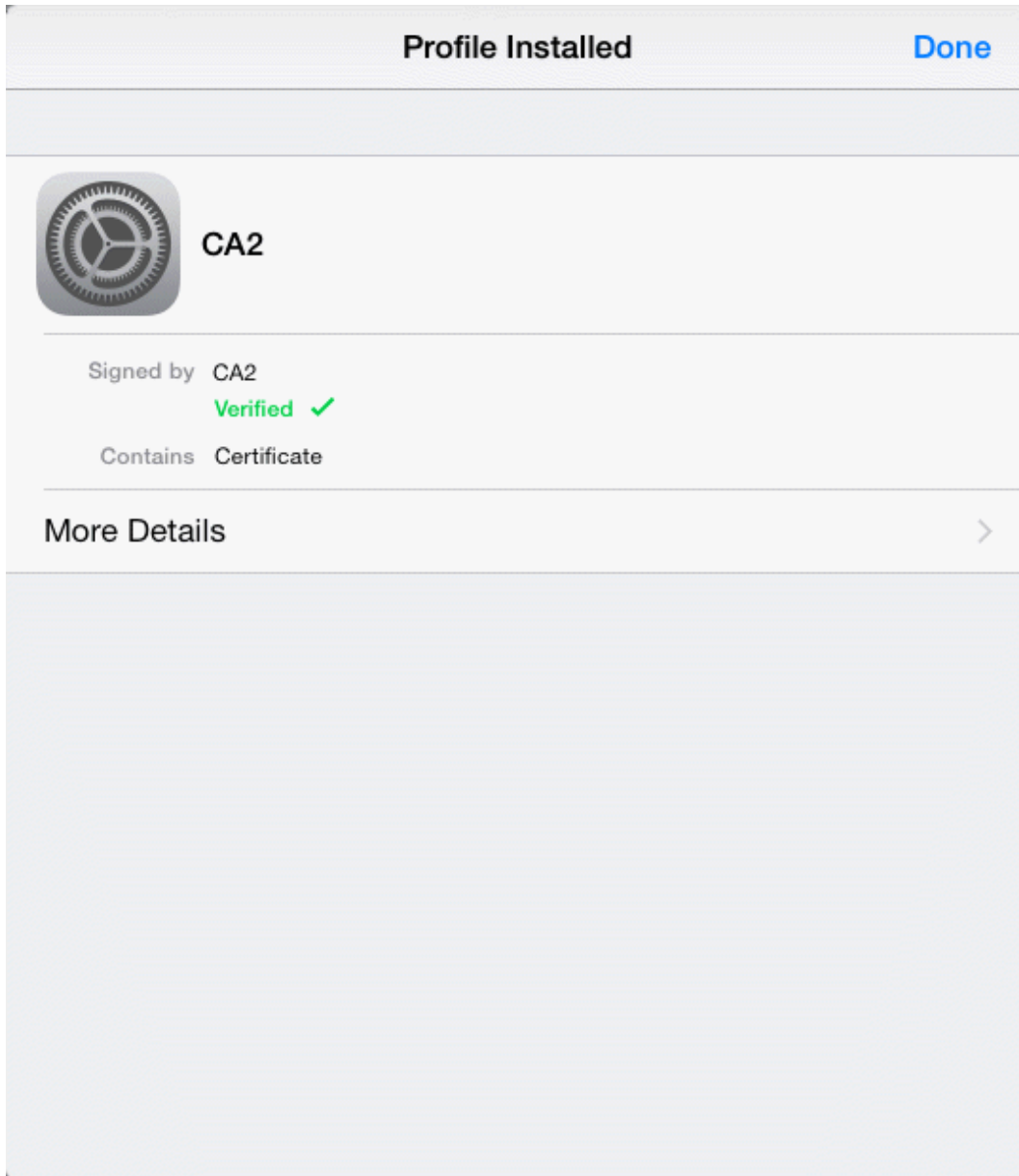
10. Tap **3. MDM Profile Install**

11. The configuration profile installation screen starts on the iOS device. Tap **Install**.

12. During installation, **Installing this profile will change settings on your iPad (iPhone)** is displayed. Tap **Install Now** to proceed.
    If you have set a pass code lock on the iOS device, you must enter the pass code during installation.
    During installation, the "Mobile Device Management" warning screen is displayed. Tap **Install** to proceed.
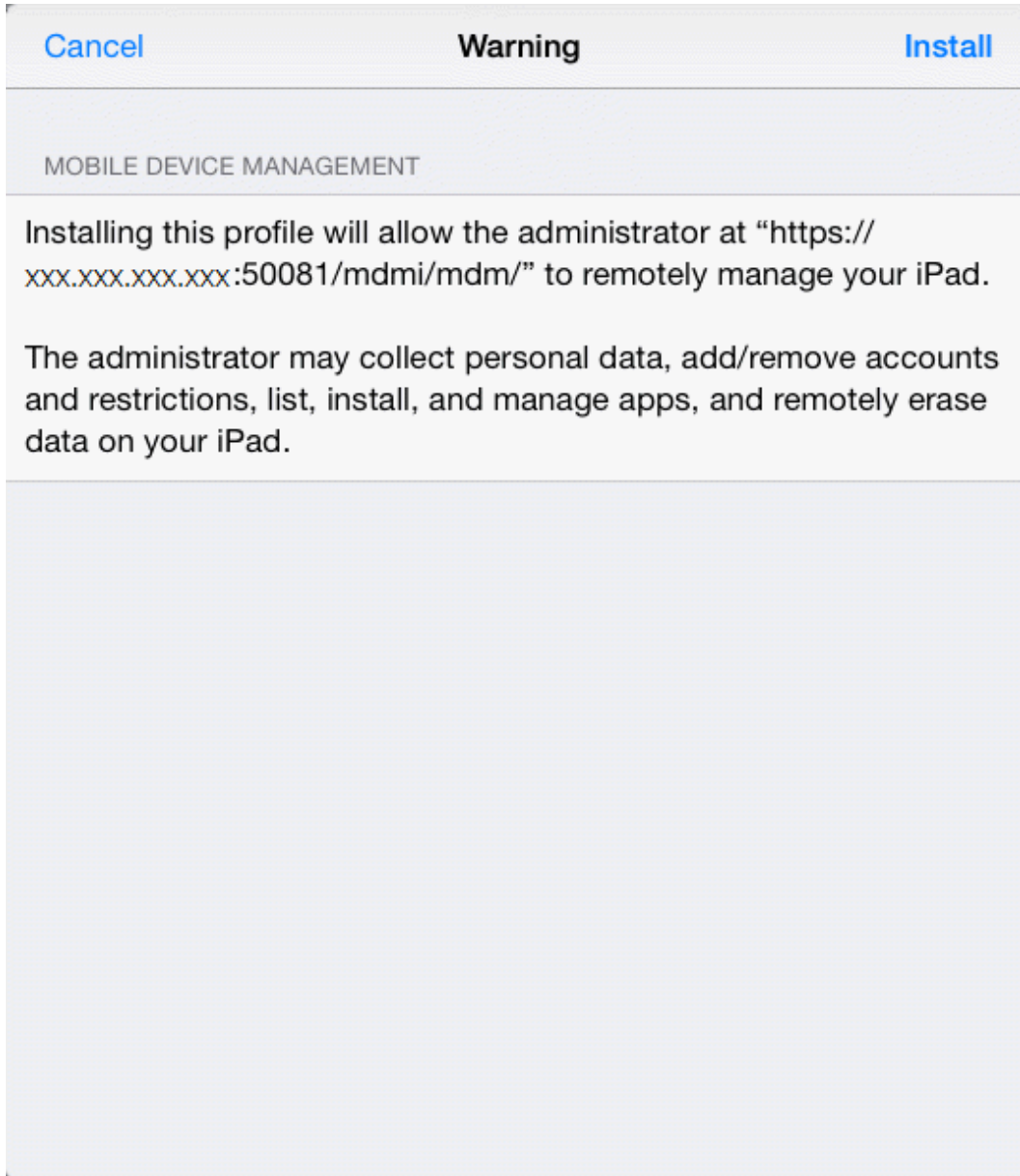
13. After installation of the MDM profile is complete, the screen shown below is displayed. Tap **Done**.
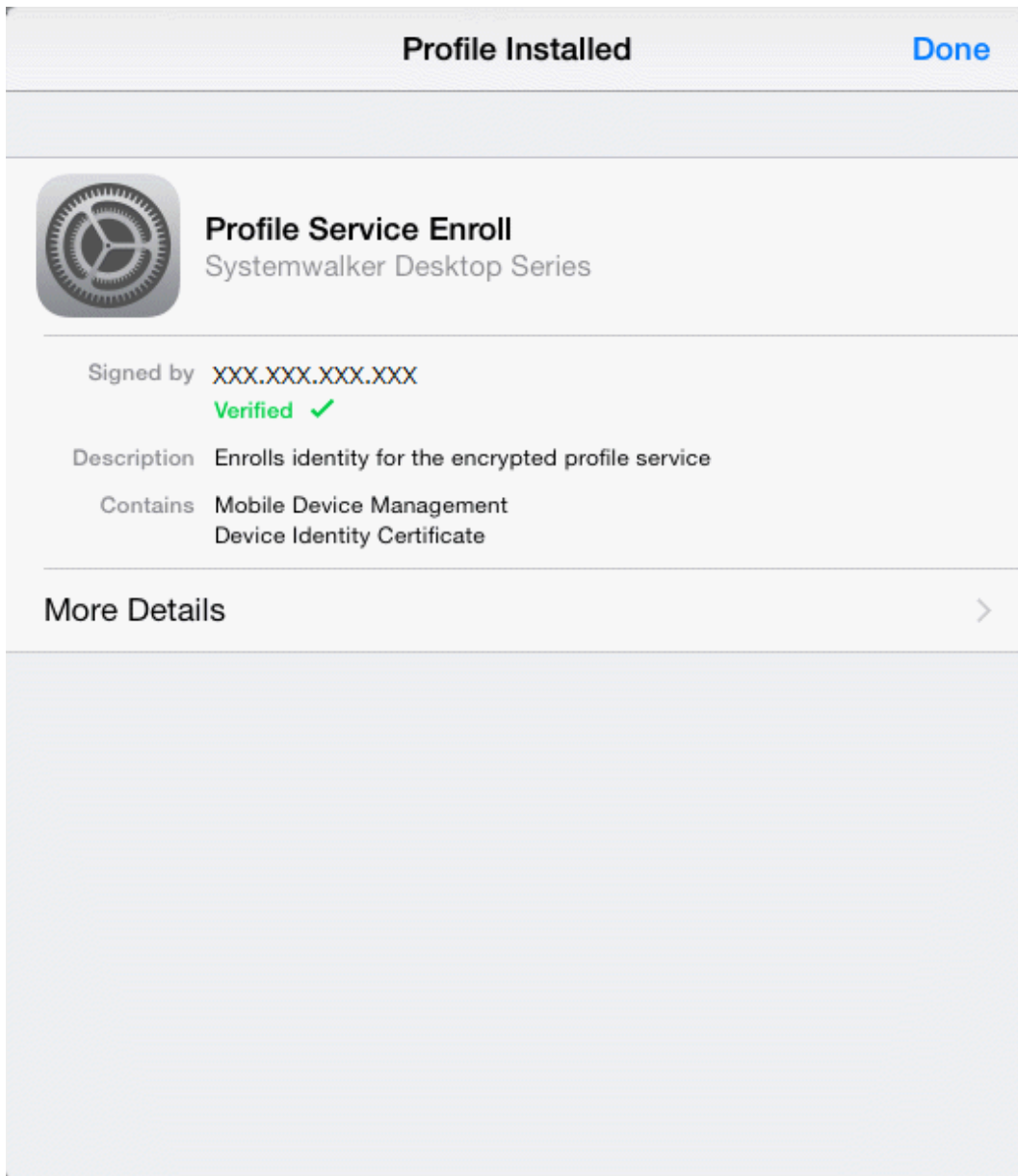
2.11 Settings of Using Remote Operation

In Systemwalker Desktop Patrol, by installing the remote operation (Systemwalker Live Help), the administrator can access PC with remote client directly for remote operation, thus, the drive of remote PC can be processed rapidly.

Install Live Help Expert in the remote operation. And install Live Help Client in the PC performed remote operation.

2.11.1 Method for Installing Live Help Expert

After installing Live Help Expert, PC with Live Help Client installed can be operated remotely.

![Note icon] Note

....

When specifying the installation target of Live Help Expert by using manual or user-defined wizard function, do not specify the folder with CS installed and its affiliated folder.

....

The installation procedures are as follows:

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. After inserting DVD-ROM of Systemwalker Desktop Patrol into PC, the following window is displayed.

If the Setup above has not been started, start "swsetup.exe" of DVD-ROM drive.

4. Select **Documents (Remote Operation)**, browse the manual and confirm the installation method.

5. Select **Remote Operation Installation** from **Setup** to complete installation.

2.11.2 Method for Installing Live Help Client

After installing Live Help Client, remote operation can be performed through PC with Live Help Expert installed.

The installation includes the following methods:

- Wizard pattern installation

- Silent installation

Method for installing Live Help Client is also recorded in the "Installation Wizard" in the displayed window when inserting DVD-ROM of Systemwalker Desktop Patrol into PC. View it.

Also, if you install a CT that includes remote operation, Live Help Client is installed. Refer to "2.7 Install CT" for details on the installation procedure for a CT that includes remote operation.

Wizard pattern installation

The procedures for installing Live Help Client in wizard pattern are as follows:

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. After inserting DVD-ROM of Systemwalker Desktop Patrol into PC, the Setup window of Systemwalker Desktop Patrol will be displayed, close it.

4. Select **My Computer** > **DVD-ROM Drive**, select **File** > **Open** of the menu.

5. In the "setup\livehelp\Client" folder, double-click "swsetup.exe".

6. The Systemwalker Live Help Client window is displayed.

   - For remote operation

7. Select **Documents**, view the manual and complete the installation.

Perform silent installation

Method of installation in silent mode is as follows:

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. After inserting DVD-ROM of Systemwalker Desktop Patrol into PC, the Setup window of Systemwalker Desktop Patrol will be displayed, close it.

4. Select **My Computer** > **DVD-ROM Drive**, select **File** > **Open** of the menu.

5. In the "setup\livehelp\LiveHelp_Client_Install" folder, double-click "Setup.bat" to perform silent installation.

2.12 Modify Installation Environment

This section describes the procedures for changing the following environment after installation.

- Move the server

- Modify IP address of the server

- Modify Windows logon user

2.12.1 Move the Server

When hoping to move DS under CS or move DS under DS to other DS as shown in the following figure in system structure, the server can be moved.

The following is the example of moving DS3 to DS2.
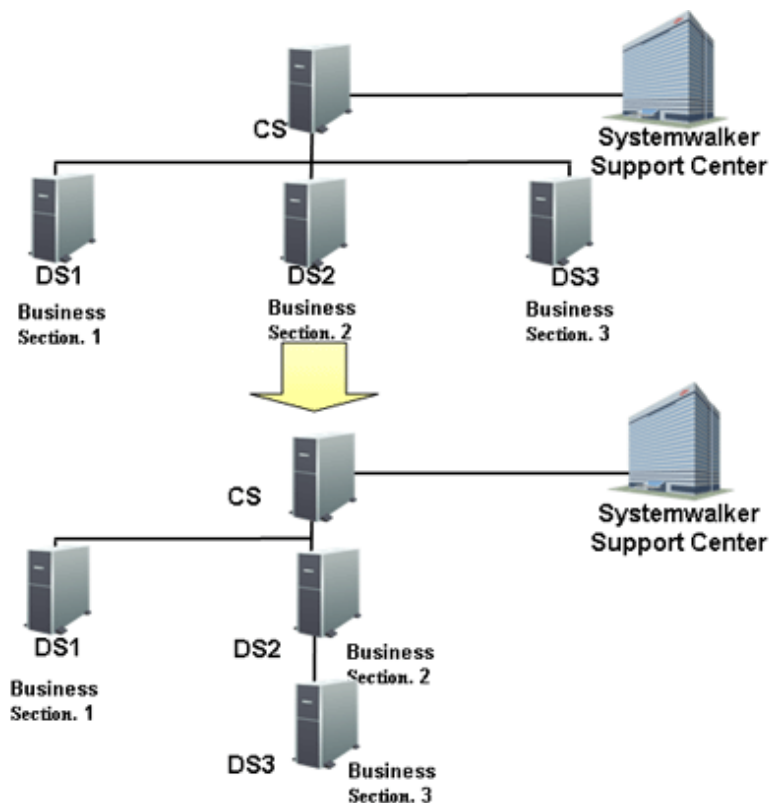
Note

When moving DS in the following status, DS cannot be moved correctly.

 - CS cannot communicate with each DS normally.

 - DS has not been installed.

 - DS has been stopped.

Move DS after confirming the following items.

 - The network between DS to be moved or deleted and CS is OK.

 - DS has been installed and started already.

If DS cannot be moved correctly, restore the network between DS and CS. Or start it in case DS has been stopped. Thus, it will be restored automatically.

The procedures for moving the server are as follows:

Note

Do not operate DS when moving it

Do not operate DS before completing moving DS to be moved.

1. Display **Environment Setup** > **CS/DS Settings and Status** through the main menu.

2. Click the link of server name.

   The following window is displayed.

3. Modify the following items.

Item	Content
Higher CS/DS	Select the higher server to be modified in the list.

4. Click the **OK** button.

   Click **Update to the Latest Information** button the in the **CS/DS Settings and Status - Settings of DS** window to confirm that the higher server of DS has been modified.

2.12.2 Modify IP Address of the Server

Modify settings on CS or DS

When modifying the settings of IP address of PC with CS or DS installed (settings modification included modification, adding and deleting), stop the service "ITBudgetMGR (INV)" of PC to be performed IP address settings modification before performing the modification.

Besides, confirm Inventory information file in process does not exist before stopping the service. If Inventory information file which has not been processed exists, data cannot be imported normally.

Inventory information file in process is saved in the following folder with the extension "*.cmp", confirm there is no file in the folder.

In addition, when modifying IP address of PC with CS installed, it can only be performed in case the host name is specified in FQDN format, or in "Host Name" of the server environment setting window on Windows during CS installation. It cannot be modified in case the host name is specified with IP address.

[Save Folder]

```
DTP installation directory\FJSVsbinv\ardus\work\IP address
```

[Example of Inventory Information File]

```
C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\FJSVsbinv\ardus\work
\10.20.30.40\1234+CT01+DS01.example.com.cmp
```

Besides, when modifying IP address directly in case the service has not been stopped and Inventory information which has not been processed is reserved, collect Inventory information again as follows.

1. Restart after stopping "ITBudgetMGR (INV)" service of PC to be performed IP address modification.

2. Display **Environment Setup** > **CS/DS Settings and Status** through the main menu and select PC to be modified IP address.

3. Click the **Update to the Latest Information** button.

Modify settings on AC

The values set for the CS host name defined in the AC must be reviewed. If the value already set is specified for the host name, and the host name can be resolved using the modified IP address, then this operation will not be required.

Refer to "Modify the settings of connection target server after installation" for details.

Modify settings on ADT

The values set for **Connection Server** defined in the ADT must be reviewed. If the value already set is specified for the host name, and the host name can be resolved using the modified IP address, then this operation will not be required.

Follow the steps below to change the settings:

1. On the PC where the ADT is installed, click **Start** > **All Programs** > **Systemwalker Desktop Patrol ADT** > **Scheduling of Automatic Detection**, or **Apps** > **Systemwalker Desktop Patrol ADT** > **Scheduling of Automatic Detection**.

2. The **Scheduling of Automatic Detection** window will be displayed.

3. Set **Connection Server** to the modified IP address or to a host name that resolves to the modified IP address.

Modify settings on SS

Follow the steps below to change settings of the IP address for the PC on which SS is installed is as follows:

If managing both Android devices and iOS devices

Configure the settings for managing Android devices and the settings for managing iOS devices.

If managing Android devices

1. Use SWDTP_ctrl.exe to stop Systemwalker Desktop Patrol.

2. Configure the settings for HTTPS communication.
   Refer to "2.8.2.2 Settings for HTTPS Communication" for details.
   If using the same CA as the one at installation, do not use swss_importcert.exe to register the CA certificate (intermediate CA certificate).
   This step is also performed if iOS smart devices are managed. If managing both iOS and Android devices, perform this step only once.

3. Use SWDTP_ctrl.exe to start Systemwalker Desktop Patrol.

4. Notify Android devices users of the enterprise server URL or internet URL.

5. The users who are notified of the URL should follow the instruction in the notification to configure the smart device CT (Android).

If managing iOS devices

1. Use SWDTP_ctrl.exe to stop Systemwalker Desktop Patrol.

2. Specify the server or reverse proxy to be connected from iOS devices.
   Execute swss_config.exe with the /iOS.connect.host option.

3. Configure the settings for HTTPS communication.
   Refer to "2.8.2.2 Settings for HTTPS Communication" for details.
   If using the same CA as the one at installation, however, do not use swss_importcert.exe to register the CA certificate (intermediate CA certificate).
   This step is also performed if Android devices are managed. If managing both Android and iOS devices, perform this step only once.

4. Use SWDTP_ctrl.exe to start Systemwalker Desktop Patrol.

5. Uninstall the CA certificate (server), CA certificate (client), and MDM profile installed in "2.10 Install Smart Device CT (iOS)".

6. Install the smart device CT (iOS) again.
   Refer to "2.10 Install Smart Device CT (iOS)" for details.

2.12.3 Modify Windows Logon User

This section describes the situation where Desktop Patrol settings should be modified when Windows logon user has been modified.

Note
....

The user name performing the following operations cannot be modified.

- Extend the operating environment through **Operation Environment Maintenance Guide**

- Back up the standard database through SWDTP_dbbk.exe

- Restore the standard database through SWDTP_dbrs.exe

- Collect data through dplook.exe

- Modify the user of the standard database through dtpctlusr.exe

The operations above require for Windows logon user for constructing the operating environment or Windows logon user added through dtpctlusr.exe (standard database user modification command).
....

User authority when executing software distribution downloading

When modifying the user name and password of Windows logon user set in the following window, modify the user name and password set in the main menu.

- Main menu

  Select policy in the **Environment Setup** > **Policy Groups** > **Customize various policies** > **Basic Operation Policy** tab of the main menu, and modify the user name and password when performing software distribution in **Specify the authority for automatic execution after software download** of the **Software Distribution** tab.

2.12.4 Install and Add Systemwalker Desktop Keeper

If you are installing and adding Systemwalker Desktop Keeper to the same machine operating Systemwalker Desktop Patrol, you must reinstall the smart device CT (iOS) on the iOS device. This procedure is only required when you are managing iOS devices.

Follow the steps below:

1. If the SS services are stopped, use SWDTP_ctrl.exe (batch starting/stopping services) on the SS to start the SS services.
   Refer to "SWDTP_ctrl.exe (Batch Starting/Stopping Services)" in the *Systemwalker Desktop Patrol Reference Manual* for details on this command.

2. Uninstall the CA certificate (server), CA certificate (client), and MDM profile.
   Refer to "5.8 Uninstalling the Smart Device CT (iOS)" for details.

3. Install the smart device CT again.
   Refer to "2.10 Install Smart Device CT (iOS)" for details.

2.13 Notes When Using Virtual OS

When using Systemwalker Desktop Patrol in the virtual OS, master the following notes first.

About settings of virtual OS software

- About resources in the virtual environment

  Memory/hard disk of the virtual environment should be one required by CT/DS.

- About the settings of virtual environment

  Distribute IP address of the virtual environment as one different from that of the virtual host device and other virtual environments.

  The network connection of virtual environment is recommended as "bridging".

- About clone environment, virtual mapping copying environment

  Do not use multiple environments created by clone or copying virtual mapping under the status DS has been installed at the same time.

  As virtual program is created by clone, virtual mapping will be under the same server status after being copied, thus, if there are multiple environments, the uniqueness of the server cannot be confirmed and as a result, the matching cannot be guaranteed.

- About the settings during shutdown.

  Do not set snapshots returned during shutdown in DS virtual environment. Because information distributed to DS will be taken back during startup, DS information might not be complete.

  The operation during virtual environment shutdown is recommended to be "Update Snapshots" or "Not Modify Snapshots".

About the management of the devices

When managing the devices in the accounts of assets, for example, to manage one device due to one piece of current Inventory information, something different from the entity device information will appear in the following cases.

- For actual PC (host PC), use (use after starting n OS in one host device) n virtual OS (Guest OS)

  Even if PC of actual device does not exist, one device could be seen in the accounts of assets, the number of devices will exceed the entity. Besides, this Guest OS will be excepted in the aggregation.

- One image of virtual OS such as VMware View is shared by multiple users and started separately

  According to the Inventory (user ID/PC name) notified for mapping information, number of devices will change.

- Host OS does not exist (Notes), all operate as virtual OS.

  Notes) Inventory in the host OS cannot be/has not been collected.

  Because Inventory information of entity PC does not exist, information such as specification and setup place of entity PC cannot be mastered.

About CT operating in virtual desktop environment

About power saving auditing and security auditing of virtual PC

- Power saving auditing and processing

  Virtual PC is operating as Guest OS on virtual PC server, physical PC does not exist. Thus, the configuration value related to power saving (time for accessing standby, etc.) of PC has no meaning. When determining CT operating in virtual PC, power saving auditing will not be performed.

- Security auditing and processing

  Because the virtual PC is operating as Guest OS on virtual server, there is no need to set BIOS/HDD password, so BISO/HDD password auditing will not be performed.

About basic operation policy

  When applying security patches to virtual PC in case of using virtual PC, it is estimated to apply system mapping (Master image).

  Thus, it is recommended not to apply by using the patch installation function of Systemwalker Desktop Patrol.

About system image update and reconstruction

  After performing the following operations and using, Inventory information in the old environment will be overwritten by the Inventory information in the new environment.

- Update and reconstruct system mapping (Master mapping) in the virtual desktop environment.

- Use PC in exchange and install CT in new PC.

- Reinstall after uninstalling in the same PC.

Supporting range of VMware View

The supporting range of VMware View when using Systemwalker Desktop Patrol is as follows.

- Type of desktop pool

Linkage clone desktop pool, included Desktop Pool completing virtual device (once called: complete clone), Manual Desktop Pool, Terminal Services Pool

- Distribution mode of user

Dedicated (dedicated distribution)

🛈 Note

....

Floating (floating distribution) is not supported.

This is because in the environment where Floating has been enabled, the desktop environment used by the user is unfixed, it will repeat other desktop environment when resetting automatically the user identification information.

....

- View Composer

Supported.

- Update and recreate the desktop

Supported.

Supporting range of Citrix XenDesktop

The supporting range of Citrix XenDesktop when operating by using Systemwalker Desktop Patrol is as follows.

- Type of devices

Dedicated, Existing and Physical

🛈 Note

....

Pooled is not supported.

This is because in the environment where the pool has been enabled, the desktop environment used by the user is unfixed, it will repeat other desktop environment when resetting automatically the user identification information.

....

Chapter 3 Maintenance

This chapter describes how to back up and restore data to be processed in Systemwalker Desktop Patrol.

3.1 Back up/Restore Operating Environment Information and Registered Software Distribution

It is recommended to periodically backup data against a hard disk fault and file corruption. All operations must be performed under CS or DS.

3.1.1 Data to be Backed up/Restored and Backup/Restoration Methods

Data to be backed up/restored

Data to be backed up/restored in DS is as follows:

	Directory/File	Remarks
Operating Environment Information	All under *<DTP Installation Directory>*\FJSVsbiis\env	-
	All under *<DTP Installation Directory>*\FJSVsbinv\etc	-
	All under *<DTP Installation Directory>*\FJSVsbinv\gather	Need not be backed up if not defined.
	All under *<DTP Installation Directory>*\FJSVsbinv\policy\emploid	-
	All under *<DTP Installation Directory>*\FJSVsbtrs\data\pol	-
	All under *<DTP Installation Directory>*\FJSVsbtrs\data\repository	-
	All under *<DTP Installation Directory>*\FJSVsbtrs\data\ordertask	-
	All under *<DTP Installation Directory>*\FJSVsbtrs\etc	-
	All under *<DTP Installation Directory>*\FJSVsbtrsc\data\repository	-
	All under *<DTP Installation Directory>*\invcl\env	-
Registered File, Software and Security Patch in Distribution Function	All under *<DTP Installation Directory>*\FJSVsbtrs\data\swc All under "Software Saving Directory"	Can be modified at installation. All under the specified directory if modified.
	All under "Extended Software Saving Directory"	Can be modified at installation. All under the specified directory if modified.

Remarks: "All under" indicates all subdirectories and files under the directory.

Backup and restoration methods

Data to be backed up has the following features.

- The amount of data is small for "Operating Environment Information"

- The amount of data is large for "File, Software and Security Patch Registered to Distribution Function"

If "Operating Environment Information" is to be backed up/restored only, the amount of data to be backed up might be small.

However, when "Operating Environment Information" is to be backed up/restored only, software and security patch should be registered again in "Software Distribution" and "Security Patch Distribution" after being restored.

Besides, because "File Distribution" cannot use again the distribution task created before backup, new distribution task should be created.

For detailed directory/file name, refer to "Data to be backed up/restored ".

Note

- CS, DS, SS should be backed up and restored at the same time.

- In CS, DS, and SS during data backup and CS, DS, and SS during data restoration, the same values must be set for the following items.

    - Product version and revise application level

    - Product installation target (installation drive and installation path, and software distribution directory (*1))

    - Saving target of Systemwalker standard database *2

    - IP address

    - Host name

    - *1: For CS and DS only

    - *2: For CS only

Backup procedure

CS backup procedure

1. Logout and finish when opening the main menu.

2. Execute the following command on the SS and CS to perform batch stop.

    - SWDTP_ctrl stop command

    For command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

3. Execute the following command to back up the operating environment information, registered distributed software, Systemwalker standard database, and iOS management database.

    - SWDTP_backup.exe

    Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

Note

For coexistence with the management server of Systemwalker Desktop Keeper V15.0.0 or later, also back up the Systemwalker Desktop Keeper management information.

4. Execute the following command on the SS and CS to perform batch start.

    - SWDTP_ctrl start

    Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

DS backup procedure

1. Stop ITBudgetMGR(INV) service in DS.

   Situation where ITBudgetMGR (INV) service has been stopped but it continues operating in the process exists. Confirm the process displayed in "Process to be stopped when backing up/restoring DS" is not in operation through the process tab in the **Windows Task Manager** window.

2. According to "Data to be backed up/restored ", back up (copy) data.

3. Start ITBudgetMGR (INV) service in DS.

4.

SS backup procedure

   Execute the following command to back up the SS.

   - SWDTP_backup.exe

   Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

Note

For coexistence with the smart device relay server of Systemwalker Desktop Keeper, also back up Systemwalker Desktop Keeper.

Backup procedure when the CS and SS coexist

1. If the main menu is open, then close it.

2. Execute the following command on the CS to perform batch stop.

   - SWDTP_ctrl stop

   Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

3. Execute the following command to back up the CS and SS.

   - SWDTP_backup.exe

   Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

Note

   - For coexistence with the management server of Systemwalker Desktop Keeper V15.0.0 or later, also back up the Systemwalker Desktop Keeper management information.

   - For coexistence with the smart device relay server of Systemwalker Desktop Keeper V15.0.0 or later, also back up Systemwalker Desktop Keeper.

4. Execute the following command on the CS to perform batch start.

   - SWDTP_ctrl start

   Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

Restoration procedure

CS restoration procedure

1. Logout and finish when opening the main menu.

2. Execute the following command on the SS and CS to perform batch stop.

   - SWDTP_ctrl stop

   For command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

3. If the Systemwalker standard database has not been built, perform construction of operation environment for the Systemwalker standard database.
Refer to "2.3.3 Construct Database" for details on the Operation Environment Maintenance Guide.

4. If iOS devices are used, ensure that the iOS management database has been built.
Refer to "2.3.4 Construct an iOS Management Database" for details.

5. Execute the following command to restore the operating environment information, registered software distribution, Systemwalker standard database, and iOS management database.

   - SWDTP_restore.exe

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

🛈 Note
. . . .
For coexistence with the management server of Systemwalker Desktop Keeper V15.0.0 or later, also restore the Systemwalker Desktop Keeper management information.
. . . .

6. Execute the following command on the SS and CS to perform batch start.

   - SWDTP_ctrl start

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

7. Re-create the DS/CT installation package in the CS server.

   In the main menu, click **Environment Setup** > **Option**.

   Click **Apply** (do not change any values).

   The DS/CT installation package will be re-created within a few minutes.

8. If a command mode CT is being used, re-create the command mode CT.

   In the main menu, click **Environment Setup** > **Software Auditing**.

   In **Select Software Dictionary Group** displayed on the left side of the window, select an appropriate group (in this case, click **Software Dictionary** > **Software** > **FUJITSU** > **CT**).

   From the list of software displayed on the right side, select one of the check boxes in **Audit**, and then clear it - this will enable **Apply** in the top right of the window.

   Click **Apply**.

   The command mode CT will be re-created within a few minutes.

DS restoration procedure

1. Stop ITBudgetMGR (INV) service in DS.

   Situation where ITBudgetMGR (INV) service has been stopped but it continues operating in the process exists. Confirm the process displayed in "Process to be stopped when backing up/restoring DS" is not in operation through the process tab in the **Windows Task Manager** window.

2. According to "Data to be backed up/restored", restore (copy) data. Besides, perform restoration after deleting "~All Under" in the table above of the restoration target.

3. Start ITBudgetMGR (INV) service in DS.

SS restoration procedure

Execute the following command to restore the SS.

   - SWDTP_restore.exe

Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

> 📓 **Note**
> ....
> For coexistence with the smart device relay server of Systemwalker Desktop Keeper, also restore Systemwalker Desktop Keeper.
> ....

Restore procedure when the CS and SS coexist

1. If the main menu is open, then close it.

2. Execute the following command on the CS to perform batch stop.

    -   SWDTP_ctrl stop

    Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

3. If the Systemwalker standard database has not been built, perform construction of operation environment for the Systemwalker standard database.
    Refer to "2.3.3 Construct Database" for details on the Operation Environment Maintenance Guide.

4. If iOS devices are being used, ensure that the iOS management database has been built.
    Refer to "2.3.4 Construct an iOS Management Database" for details.

5. Execute the following command to restore the CS and SS.

    -   SWDTP_restore.exe

    Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

> 📓 **Note**
> ....
> -   For coexistence with the management server of Systemwalker Desktop Keeper V15.0.0 or later, also restore the Systemwalker Desktop Keeper management information.
>
> -   For coexistence with the smart device relay server of Systemwalker Desktop Keeper, also restore Systemwalker Desktop Keeper.
> ....

6. Execute the following command on the CS to perform batch start.

    -   SWDTP_ctrl start

    Refer to the *Systemwalker Desktop Patrol Reference Manual* for details.

7. Re-create the DS/CT installation package in the CS server.

    In the main menu, click **Environment Setup** > **Option**.

    Click **Apply** (do not change any values).

    The DS/CT installation package will be re-created within a few minutes.

8. If you are using a command mode CT, re-create the command mode CT.

    In the main menu, click **Environment Setup** > **Software Auditing**.
    In **Select Software Dictionary Group** displayed on the left side of the window, select an appropriate group (in this case, click **Software Dictionary** > **Software** > **FUJITSU** > **CT**).

    From the list of software displayed on the right side, select one of the check boxes in **Audit**, and then clear it - this will enable **Apply** in the top right of the window.

    Click **Apply**.

    The command mode CT will be re-created within a few minutes.

Process to be stopped when backing up/restoring DS

-   atoold.exe

-   invstart.exe

- javaw.exe

- ctd.exe

3.1.2 Restoration Procedure if "DS" Assets Have Not Been Backed up

If DS is not operating as it should due to causes such as DS machine fault or OS fault, restore DS assets according to procedures for backup/restoration.

If DS assets have not been backed up, restore according to the following procedures.

Environment conditions for restoration

The environment in which the restoration can be performed according to the procedures described here must meet the following conditions.

- IP address and the host name should be the same as the ones before restoration.

- When reinstalling OS, the communication environment with CS should be complete.

The restoration procedure is as follows:

1. Install DS.

   Newly install DS.

   If DS has been installed, reinstall after uninstalling it.

2. Confirm Systemwalker Desktop Patrol DS which is newly installed.

3. Log onto the main menu and click **Environment Setup**.

   The **Environment Setup** window is displayed.

4. Click **CS/DS Settings and Status**.

   After completing DS installation, it will be displayed in the server list. When servers with the same host name are displayed, it indicates the information of the previous DS installation is remained, confirm the operation information and delete the server not in operation.

   Execute the following command when deleting.

```
Installation Target of Desktop Patrol CS\FJSVsbtrs\bin\DSDelete.exe" -host <Deleted Host Name>
```

5. When performing the policy application under DS unit, set client policy for the new installed DS.

6. Click **CS/DS Name** of the new installed DS and perform **Settings of DS**.

7. Set software distribution target server.

Click **Distribution** > **Software Distribution** of the main menu.

For detailed settings, refer to *Systemwalker Desktop Patrol Operation Guide: for Administrators*.

3.2 Extend Database

Due to causes such as increasing number of managed machines, Systemwalker standard database should be extended when modifying the database capacity.

Besides, to cope with the unexpected faults, make sure to back up before extending Systemwalker standard database for security.

Refer to "Required Hardware" in the *Systemwalker Desktop Patrol User's Guide* for details on a rough estimate of the required space.

Extend Systemwalker standard database as follows.

1. Log on with Windows logon user when constructing the operating environment.

2. Click **Start** > **All Programs** > **Systemwalker Desktop Patrol** > **Operation Environment Maintenance Guide**, or **Apps** > **Systemwalker Desktop Patrol** > **Operation Environment Maintenance Guide**.

3. The **Welcome to Operation Environment Maintenance Wizard** is displayed, click the **Next** button.
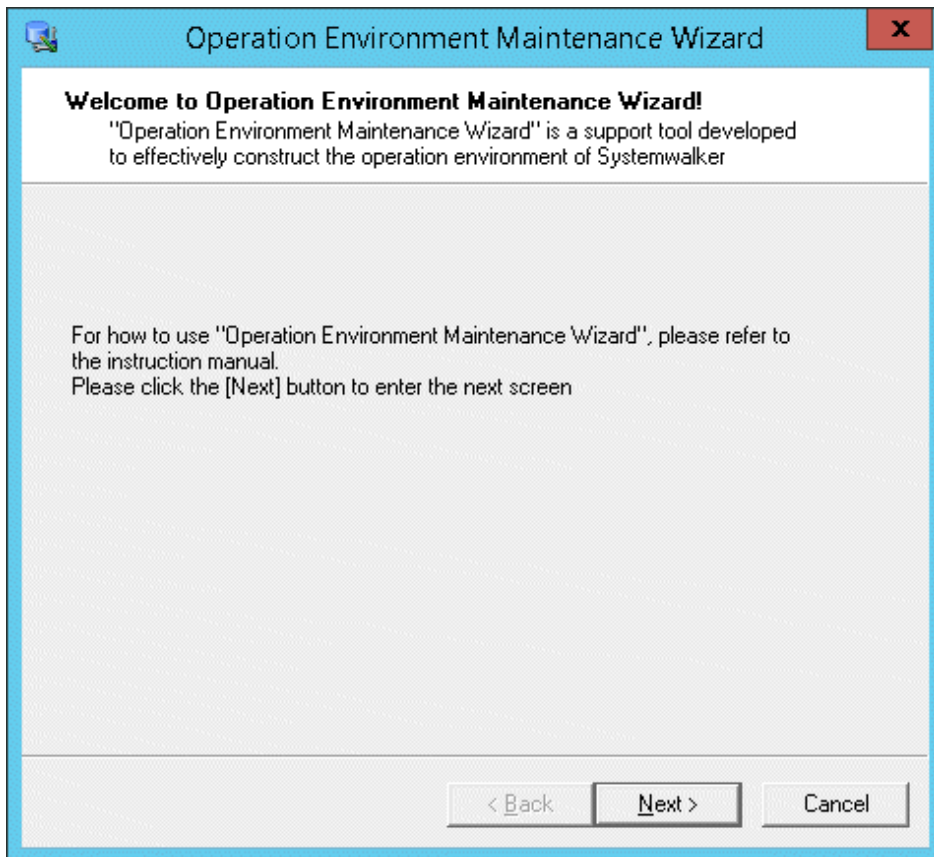
4. The **Selection Process** window is displayed, set **Operation(S)** and **Storage Location of Backup Data** and click the **Next** button.
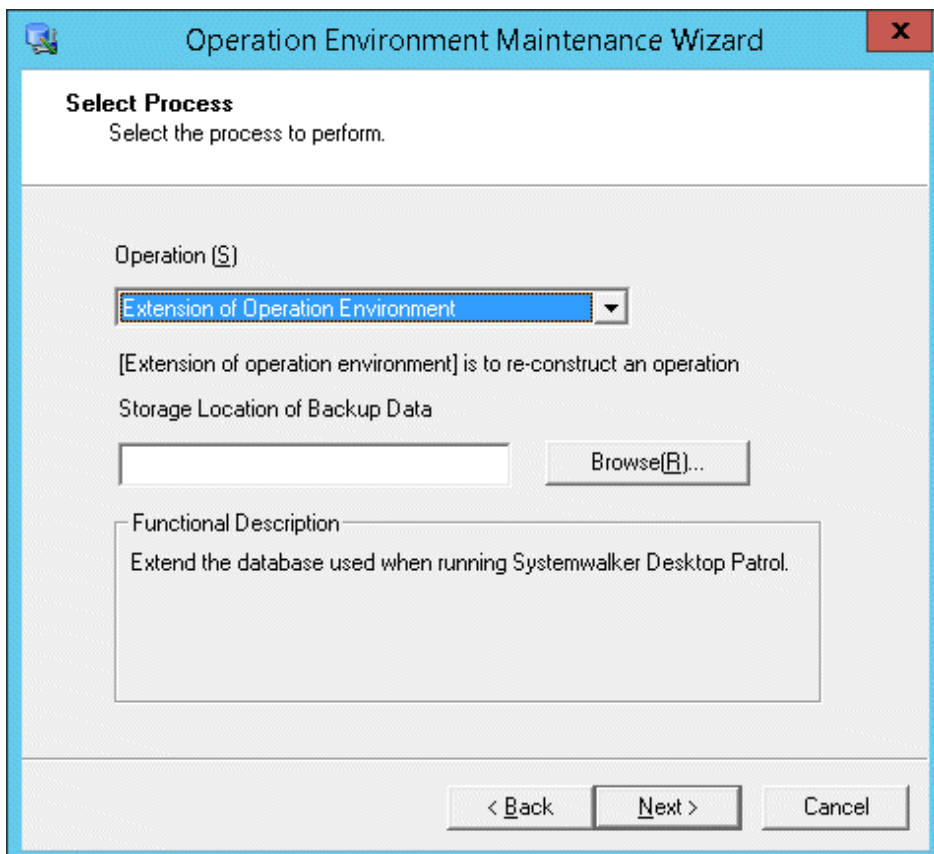
Item	Descriptions
Operation(S)	Select the processing to be executed. Select **Extension of operating environment** here.
Storage Location of Backup Data	Path name can be specified as 64 characters at most in backup data saving target. Halfwidth spaces and fullwidth characters such as hiragana and katakana cannot be specified.

5. The **This is the current usage of database** window is displayed, click the **Next** button.
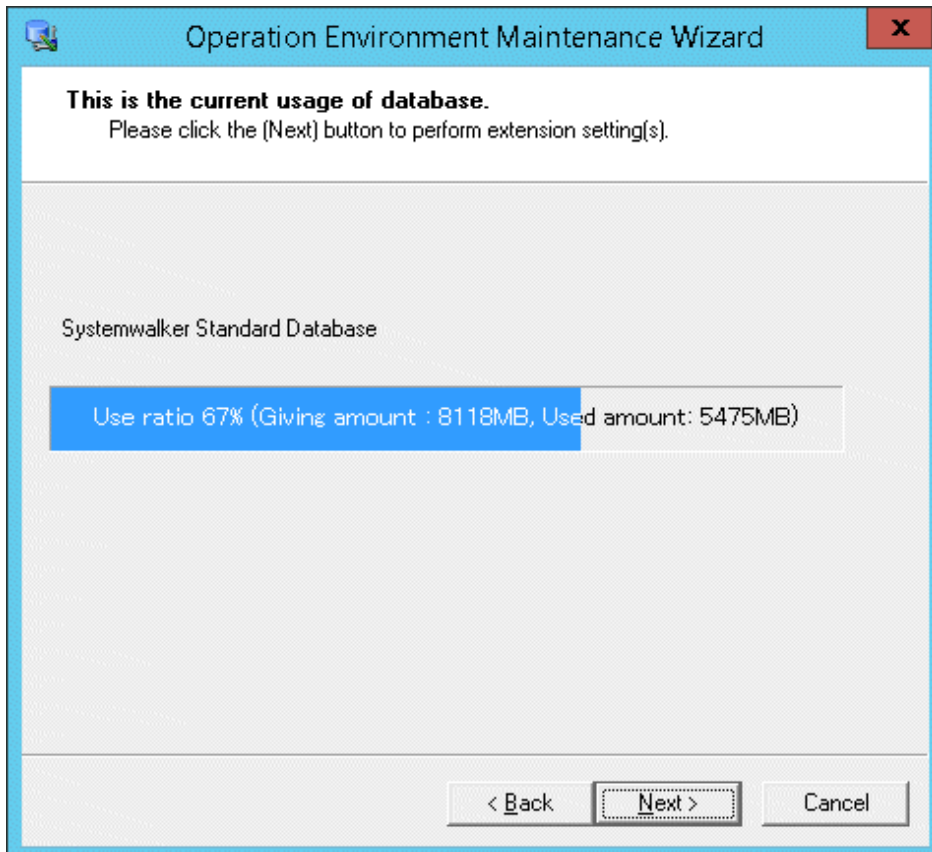
6. The **Enter database information** window is displayed. Set **Database Storage Location(D)** and **Database Settings**.

Item	Descriptions
Database Storage Location(D)	Path name can be specified with no more than 64 characters in database saving target. Halfwidth space, tab, comma (,), semicolon (;), single quotation ('), number sign (#), and fullwidth characters cannot be specified.
	When the directory name specified in the database saving target is different from "DESKTOPPATROL_DBSP", "DESKTOPPATROL_DBSP" directory will be created automatically under the specified directory and save the database in it.
	📖 **Note**
	· ·
	For the drive and folder of database storage location, do not set compressing and encryption.
	If a Systemwalker Centric Manager database has already been built, specify a different storage destination from the Systemwalker Centric Manager database.
	· ·
Number of PC(s)	Select the correspondent number of PC(s).
	When specifying an arbitrary number, enter within 100~100,000.
	For the standard of database capacity, refer to "Hardware" of *Systemwalker Desktop Patrol User's Guide*.
	📖 **Note**
	· ·
	[Number of PC(s)] is the standard for number of PC(s) that can be managed

Item	Descriptions
	"Number of PC(s)" is the standard for number of PC(s) that can be managed in Systemwalker Desktop Patrol. According to circumstances, it might be less than the specified number of PC(s). At this time, the capacity of Systemwalker standard database can be extended by performing "Extend Operating Environment".
Number of smart device(s)	Specify the number of smart devices to be managed in Systemwalker Desktop Patrol. A number from 0 to 100000 can be specified.
Number of managed non-PC(s)	Set machine (device) managed in Systemwalker Desktop Patrol. Numbers within 0~100000 can be set.

7. When performing **Collection of EXE Information** and **Collection of Software Operation Information or Control of Execution File**, click the **OK** button. Execute according to the following procedures if not set.
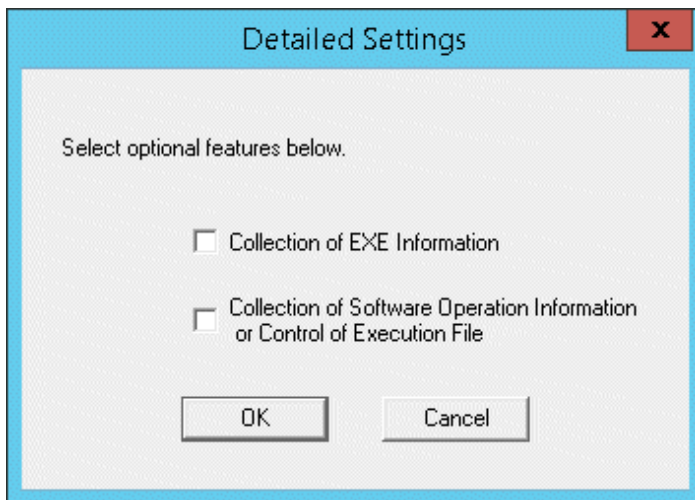
Select the collected information and click the **OK** button.

8. Click the **Next** button and the **Confirmation of Settings** window is displayed. Click the **Next** button after confirming whether the content displayed in the window is correct.

The **Execute Processing** window is displayed and start to extend the database.

Besides, when the **Cancel** button is clicked to interrupt in the process of **Extend Operating Environment**, the interrupted **Construct Operating Environment** can be restarted by executing **Operation Environment Maintenance Guide** again.
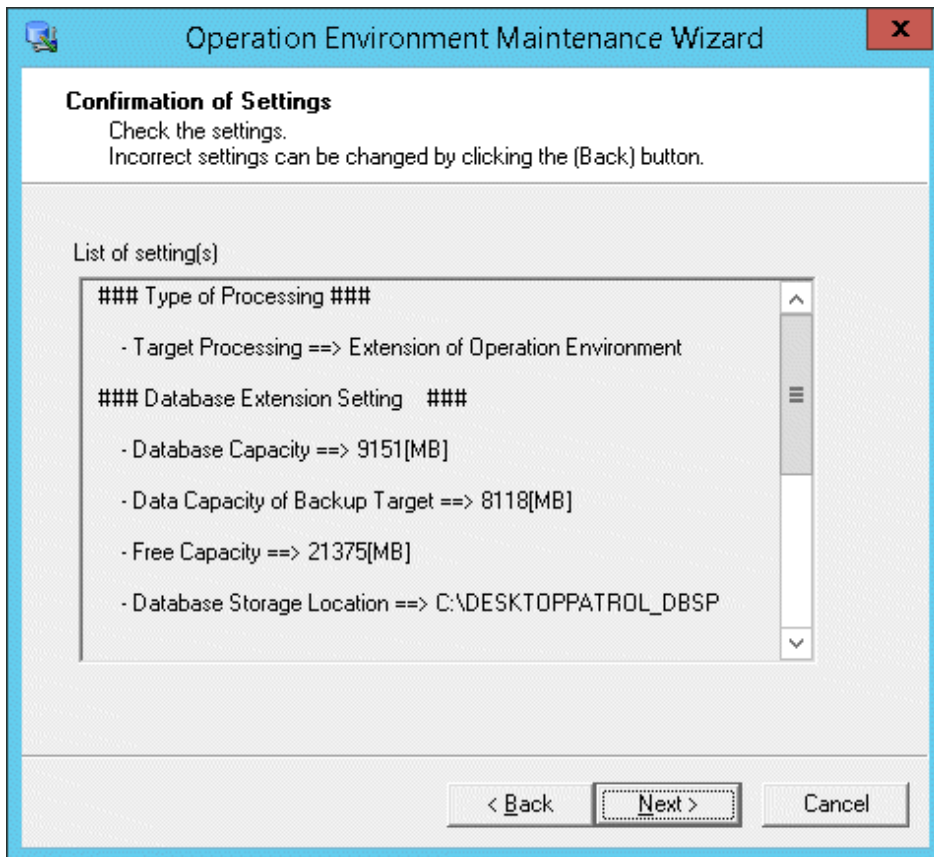
9. The **Process Completed** window is displayed after the processing is completed normally, click the **Finish** button.

Chapter 4 Version Upgrade

This chapter describes how to upgrade the version of Systemwalker Desktop Patrol.

4.1 Methods for Version Upgrade

Methods for version upgrade are as follows.

- Version upgrade for products

- Version upgrade for OS

Issues to be considered before version upgrade

- To cope with the errors during version upgrade, it is recommended to back up the old operating environment and software distribution. For how to back up, refer to the old manual.

- Version upgrade through "Remote Desktop Connection" of Windows is not supported. To perform remote operation, use LiveHelp.

Issues to be considered after version upgrade

- When you upgrade the product version from V14.2.0 or earlier, the JRE for the CS and DS will be changed. For this reason, if firewall is used in the CS and DS, the exception command for the firewall must be changed after the version upgrade. Refer to "Settings when using firewall in CS and DS" in "Port Number List" in the *Systemwalker Desktop Patrol Reference Manual* for details.

- In a PC using a web browser, the DTP web window may not be displayed correctly after the version upgrade. If this happens, delete the Internet Explorer Internet temporary files, and re-execute it.

4.2 Version Upgrade for Products

Perform version upgrade by reinstalling or applying updater. Since different components offer different range, confirm reinstallation and updater in the following table.

Besides, when upgrading the version of DS, AC, ADT, CT and smart device CT, perform after CS version upgrade.

Component	Reinstall	Apply Updater
CS	Y (Note)	N
DS	Y	Y
AC	Y	N
ADT	Y	N
CT	Y	Y
Smart device CT	Y	N

Y: can

N: cannot

(Note):Incase of the CS, Only update from V14.2.0 is possible.

Products to be performed version upgrade through reinstallation are as follows:

- Systemwalker Desktop Patrol V13.0.0/V13.2.0

- Systemwalker Desktop Patrol V14.2.0

Products to be performed version upgrade through updater are as follows:

- Systemwalker Desktop Patrol V13.0.0/V13.2.0

- Systemwalker Desktop Patrol V14.2.0

4.2.1 Procedures for Version Upgrade through Reinstallation

This section explains the procedures for version upgrade through reinstallation for each of the following components:

- In case of CS

- In case of DS

- In case of AC

- In case of ADT

- In case of CT

- Uninstall the old MC

In case of CS

Issues to be confirmed before reinstallation

- When performing reinstallation, 800MB available memory capacity is required. Confirm the available memory capacity before reinstallation.
  If the available memory capacity is insufficient, add virtual memory of PC and set the available capacity larger than 800MB.

- Ensure that there is sufficient disk space for version upgrade.

  - To upgrade from V12.0L10 or earlier, refer to "Upgrading from V12.0L10 or earlier" in "Required Hardware" in the *Systemwalker Desktop Patrol User's Guide* for a rough estimate of the space required.

  - To upgrade from V13.0.0 or later, refer to "Extending the Systemwalker standard database" in "Required Hardware" in the *Systemwalker Desktop Patrol User's Guide* for a rough estimate of the space required.

- If the 32-bit version CS is installed on a 64-bit operating system, the CS cannot be upgraded to a 64-bit version CS.

- If you install Systemwalker Desktop Patrol, for version upgrade, to an environment where Systemwalker Desktop Keeper is installed, the service managing iOS devices will be stopped automatically. In this case, the service managing iOS devices will not be available for use until the system is restarted.

The procedure for reinstalling CS is as follows:

1. Log on to Windows using an account that belongs to the Administrators group.

   Besides, you should log on it with Windows login user for constructing the environment or for constructing Symfoware by the means of using Operation Environment Maintenance Guide.

2. If you are using other applications, close them.

3. After inserting DVD-ROM of Systemwalker Desktop Patrol into PC, the following window is displayed.

   Select "CS Installation".
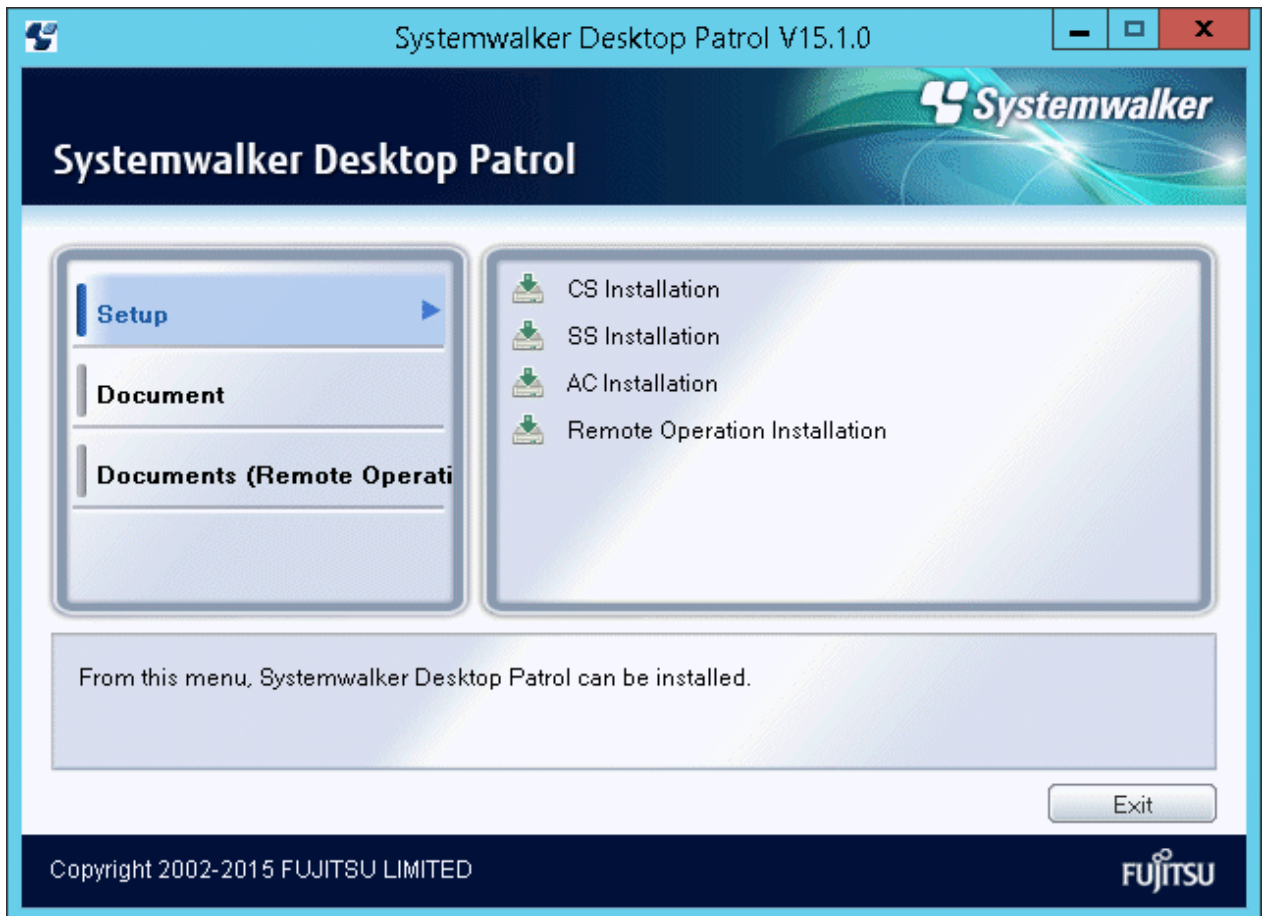
   If the Setup above has not been started, start "swsetup.exe" of DVD-ROM drive.

4. The **Welcome to the InstallShield Wizard for Systemwalker Desktop Patrol** window is displayed, click the **Next** button.

5. The **Please Read** window is displayed, confirm the content and click the **Next** button.
   In addition, when IT BudgetMGR (INV) service and World Wide Web Publishing service stop, this window will not be displayed.

6. The **Start to Copy Files** window is displayed, confirm whether the content displayed in the window is incorrect and then click the **Next** button.

   The **Installation Status** window is displayed and installation is started.

7. When the installation completes, the window shown below will be displayed.

   Click **Finish**.

8. To use the program, the system must be restarted.

   Click **Yes**.
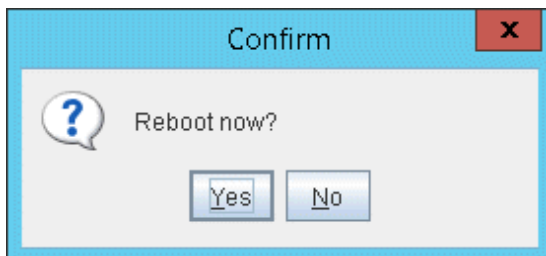
9. Register the license key.

   About the registration of the license key, refer to "2.3.2.4 Register the license key".

10. Register the latest software dictionary.

    Register the latest software dictionary saved in the DVD-ROM before starting an operation.

    Copy to local disk temporarily during registration. Besides, because the software dictionary saved in DVD-ROM is read-only, modify as read-write.

    Saving target: < DVD-ROM Drive>:\utilities\supportcenter

    For details, refer to "AtoolETPGT.exe (Apply Software Dictionary)" in the *Systemwalker Desktop Patrol Reference Manual*.

📙 Note
. . . .

About first software dictionary registration after upgrade

After upgrade, it takes time for first software dictionary registration processing.

Wait until AtoolETPGT.exe command processing is completed.
. . . .

Ensure that Symfoware Server is not being used by other products or applications. Once it is ensured that Symfoware Server is not being used by other products or applications, delete Symfoware Server.

From **Control Panel**, start **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**, and select and delete the following products:

- "Symfoware Client" or "Symfoware Server Client"

- "Symfoware Server" or "Symfoware Server Enterprise Edition"

When using Systemwalker Desktop Patrol V13.2.0 or earlier version or Windows Server(R) 2003

Upgrade by the following procedure.

1. Upgrade to Systemwalker Desktop Patrol V14.2.0

2. Backup data

3. Upgrade OS by server replace

4. Recovery data

5. Upgrade to Systemwalker Desktop Patrol V15.1.0

In case of DS

The procedure for reinstalling DS is as follows.

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. Input the following URL in the **Address** bar of Web browser.

```
http://server information (FQDN name or host name or IP address of [Systemwalker Desktop Patrol
CS])/DTP/index.html
```

4. The login window is displayed, enter **User ID** and **Password** and click the **Login** button.

5. The main menu is displayed, click **CS/DS Settings and Status** in the **Environment Setup** window, the following window is displayed.

6. Click **Download** of PC as the higher server of DS to be reinstalled.

7. The **Download Files** dialog box is displayed and message for confirming saving appears. Click the **Open** button.

8. The **Welcome** window is displayed. Click the **Next** button.

   Start to install automatically.

9. The **Installation Completed** window is displayed after the processing is completed normally. Click the **Finish** button.

   Systemwalker Desktop Patrol is modified as the available status.

When using Systemwalker Desktop Patrol V11.0L10 version

Upgrade by the following procedure.

1. Backup data

2. Upgrade OS by server replace

3. Recovery data

4. Upgrade to Systemwalker Desktop Patrol V15.1.0

In case of AC

Reinstallation procedure for the AC is shown below:

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. Insert the Systemwalker Desktop Patrol DVD-ROM in the PC.

   In the window below, select **AC Installation**
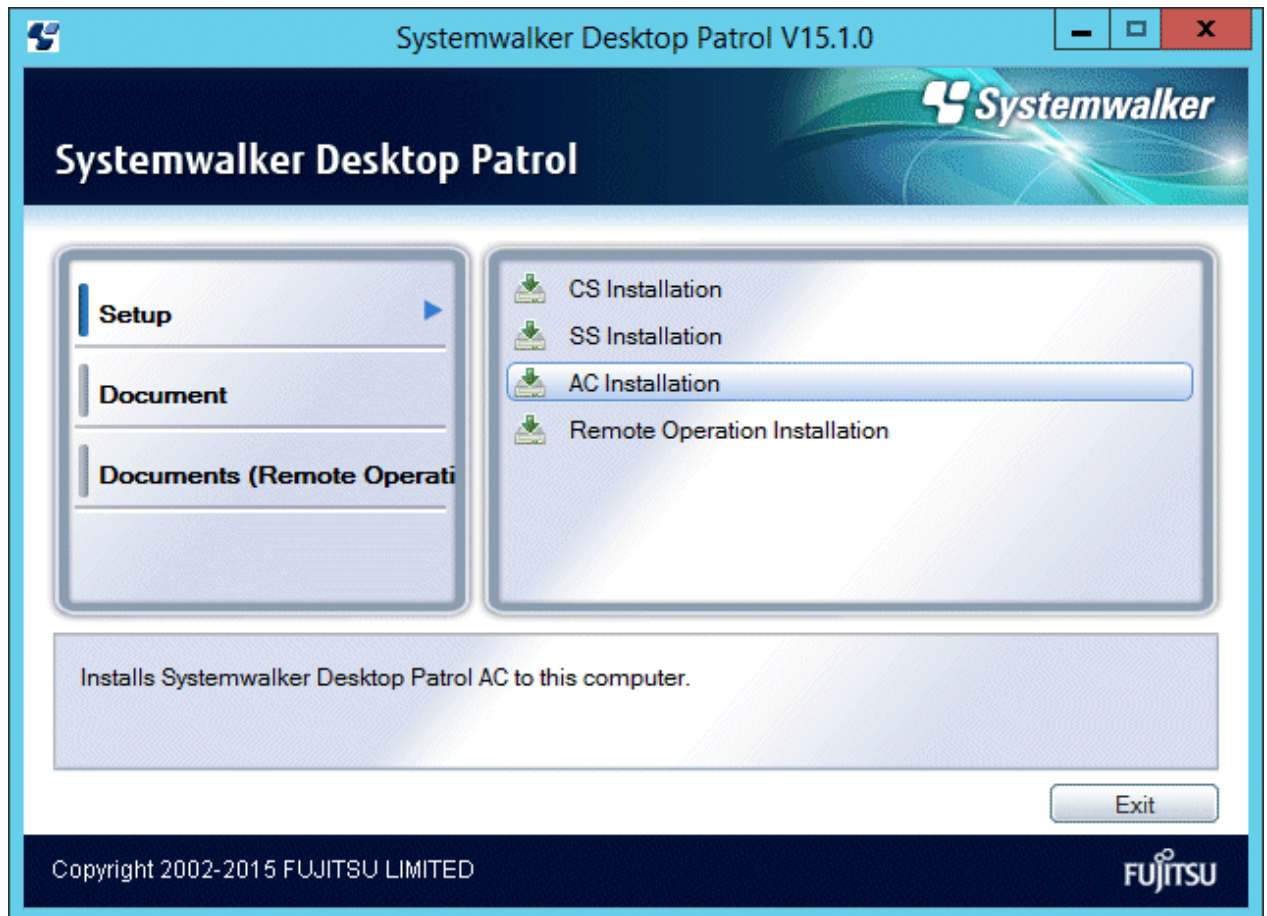
   If the above installer window is not displayed, start "swsetup.exe" in the DVD-ROM drive.

4. The **Welcome to the InstallShield Wizard for Systemwalker Desktop Patrol** window will be displayed. Click **Next**.

5. The **Start Copying Files** window will be displayed. Ensure that the information displayed in the window is correct, and click **Next**.

   The **Installation Status** window will be displayed, and installation process will start.

6. The **Setup has been completed normally.** window will be displayed. Click **Finish**.

In case of ADT

1. Log on to Windows using an account that belongs to the Administrators group.

2. Enter the following URL in the address bar of your web browser.

```
http://serverInfo (FQDN name, or host name or IP address of Systemwalker Desktop Patrol CS)/DTP/
dwl.html
```

   To use a PC that is not connected with Desktop Patrol CS as "ADT", download the ADT module on another PC that is connected with Desktop Patrol CS, and copy the module to the PC on which "ADT" will be installed.

3. The download menu will be displayed. Click **ADT Download**, and the following window will be displayed.
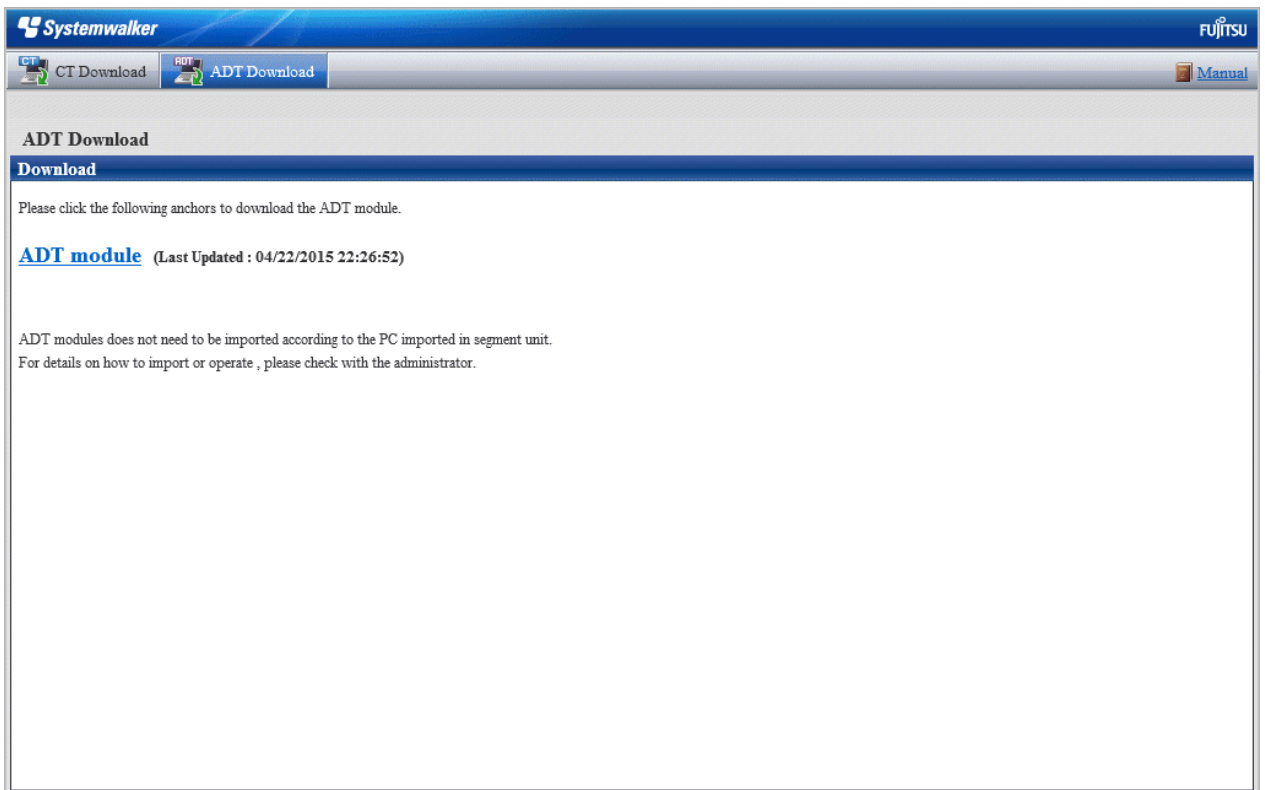
4. Click **ADT module** to start downloading.

5. Place the download module (ADTSetup.exe) in any automatic detection PC directory in each segment, and execute it.

6. The following installer will start. Set the installation directory and **Account Information During Task Registration**. Click **Start**.

[For Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008, and Windows Server(R) 2012]
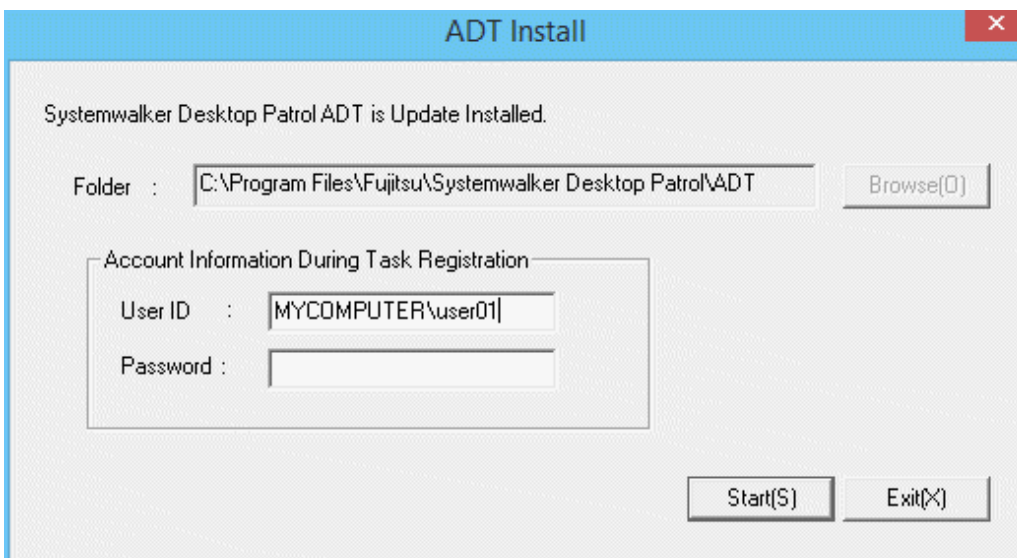
Item	Description
Folder	ADT module installation directory.

Item		Description
Account Information During Task Registration (*1)	**User ID**	User account used for installation. Specify using the *domain\userName* format with up to 260 alphanumeric characters or less.
	Password	Password of the specified user ID. Specify up to 260 alphanumeric characters.

*1: Displayed for Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008, and Windows Server(R) 2012 only.

7. Before installation completes, the **Scheduling of Automatic Detection** window will be displayed.

Enter the following information and click **Apply**.

Item name	Description
On Demand Device Information Notification	Select this option to send device information detected on the ADT without using schedule.

Item name		Description
Scheduled Device Information Notification		Select this option to send device information detected on the ADT according to the specified schedule.
Notification Target Settings	**Connection Server**	Name of the notification target server. ⚑ **Note** . . . . **Communication in an IPv6 environment** IPv6 IP addresses cannot be specified. If performing communication in an IPv6-only environment, register one of the following beforehand and enter the host name: - Register the CS and DS host name or IP address in the DNS server - Register the CS and DS host name or IP address in the communication source PC hosts file . . . .
	Port Number	Port number of the notification target. The default value is 80.
	Set	Sets the proxy.
Collect Devices Not Registered in Ledger (Detailed Collection)		Select this option to perform automatic detection and information collection of devices for maintaining the management ledger. This option cannot be selected if **Collect Devices Connected to without Permission (Simple Collection)** is selected.
Scheduler Setting	**Daily**	Select this option to send device information every day.
	Weekly	Select this option to send device information weekly. Any day(s) between Monday and Sunday can be selected for this setting.
	Monthly	Select this option to send device information monthly. Set **Execution Date** to the day when notification will be sent. Note that if the day specified in **Execution Date** does not exist for a certain month, automatic detection will not be performed for that month. For this reason, if you intend to execute notification at the end of the month, consider setting the execution operation at 0:00 on the first day of each month instead.
	Start Time	Time at which device information notification will start. If operating the ADT module on a server PC other than those running 24 hours a day, be careful about setting the time because the power for the automatic detection PCs may be turned off during late night/early morning.
Collect Devices Connected to without Permission (Simple Collection)		Select this option to perform automatic detection and information collection of devices connected to without permission. This option cannot be selected if **Collect Devices Not Registered in Ledger (Detailed Collection)** is selected.

Item name		Description
	Collection interval	Specify the interval for collecting device information when detecting devices connected to without permission. Device information will be repeatedly collected at this interval. Select one of the following intervals: - 30 minutes - 1 hour - 2 hours - 6 hours
Confirm Execution Result		Settings to display the execution result.
	Log Viewing	Display the execution result log.

Once installation completes, the following tasks will be registered in the Windows task features:

- Name:

  SWDTPAS_ADT.job

- Operation privileges:

  - For Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008, and Windows Server(R) 2012: Specified account

Note that if the ADT module is not started at the set notification time (because the PC power is off, for example), the device information will be sent at the next scheduled start time after the ADT module is started.

When the schedule setting is completed, the following message window will be displayed. Click **OK**.

```
Installation of ADT was ended. A setup becomes effective by rebooting system.
```

8. Click **OK** to restart the system.

In case of CT

The procedure for reinstalling CT is as follows:

1. Log on Windows with Account affiliated Administrators group.

   Input the following URL in the **Address** bar of Web browser.

```
http://server information (FQDN name or host name or IP address of "Systemwalker Desktop Patrol
CS")/DTP/dwl.html
```

2. Display the download menu.

3. Select **Server Name**, or **Server Name (with Remote Operation)** for PC as the higher server, and then the message for confirming saving is displayed in the **Download Files** dialog.
   If the remote operation function is not required, select **Server Name**.
   If the remote operation function is required, select **Server Name (with Remote Operation)**.
   Follow the instructions of the administrator to decide which to select.

4. Click the **Execute** button to start installation, the **Welcome to the InstallShield Wizard for Systemwalker Desktop Patrol CT Program** window is displayed. Click the **Next** button.

   Start installation automatically.

Note

. . . .

When the following security warning window is displayed, select Run.
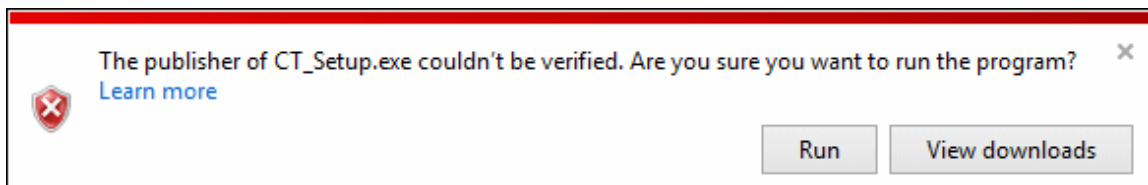
. . . .

5. The **Installation Completed** window is displayed after the processing is completed normally. Click the **Finish** button.

   Systemwalker Desktop Patrol is modified into available status.

When using Systemwalker Desktop Patrol V11.0L10 version

Upgrade by the following procedure.

1. Uninstall the CT

2. Upgrade OS

3. Install the CT of Systemwalker Desktop Patrol V15.1.0

Uninstall the old MC

"MC" cannot be used since V14.2.0.

When upgrading the version of products, uninstall the old "MC" according to the following procedure.

1. Delete the "Systemwalker Desktop Patrol (MC)" program from **Add or Remove Programs**.

2. After deleting the program, some relating folders might have not been deleted. At this time, delete the installation target folder of this product through Explorer after rebooting OS.

   Example) Delete the folder C:\Program Files\Fujitsu\Systemwalker Desktop Patrol MC

4.2.2 Procedures for Version Upgrade by Applying Updater

By registering updater, updater can be applied in DS and CT automatically.

The information for version upgrade in V15.1.0 is as follows:

DS information

Input Item	Configuration Value
Name (cannot be modified)	V15.1.0-R1.1-SN1501
Version	1
Descriptions	DS updater V15.1.0-R1.1-SN1501

CT information

Input Item	Configuration Value
Name (cannot be modified)	V15.1.0-R1.1-SN1551
Version	1
Descriptions	CT updater V15.1.0-R1.1-SN1551

🖐 **Note**
. . . .

Updated notes

- Execute the command in the status that Desktop Patrol service (IBudgetMGR (INV)) has been started.

- When DS updater only is saved to the updated saving target folder, register only DS updater. Same as the case of CT updater.

- Updater with the same version as the registered updater cannot be registered. However, in case DS updater has been registered while CT updater has not, register only CT updater. In case CT updater has been registered but DS updater has not, register only DS updater.

- CT updater cannot be applied by using policy group. It is applied to all the CTs affiliated to the distribution server.

- CT updater cannot be applied manually through the software download window. It will all be applied automatically.

- If V15.0.1 or earlier version is used, connections from V15.0.1 or earlier DS and CT must be authorized using CustomPolicy.exe (modifying policy for custom setup command) before applying the updater.

  Once the updater is applied, reject connections from the V15.0.1 or earlier DS and CT.

- Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on CustomPolicy.exe (modifying policy for custom setup command).

• •

The procedure for version upgrade by applying updater is as follows. Apply/Distribution updater according to this procedure for version upgrade.

Register updater in CS.

If using V13.2.0/V13.2.1

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. Copy *dvdRom*\utilites\tool\updv132 to a directory on the CS.

   - \ITBudgetMGRclientUpdate.zip - CT updater

   Example:

   ```
   c:\temp\updv132\ITBudgetMGRclientUpdate.zip
   ```

4. Start the command prompt and register the CT updater.

   Execute updaterregist.exe (registering and updating). Refer to "Command Reference" in the *Systemwalker Desktop Patrol Reference Manual* for details.

   ```
   dtpInstallDir\FJSVsbtrs\bin\updaterregist.exe  -dir  updaterDir
   ```

   updaterDir: Directory in which the CT updater was stored in the step 2 above.

   Example:

   ```
   > "C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\FJSVsbrs\bin\updaterregist.exe"  -dir c:
   \temp\updv132
   ```

Point

• •

If you are using V13.2.0/V13.2.1, then after completing the above steps, do the same for "If using V14.2.0 or later" as well.

• •

If using V14.2.0 or later

1. Log on to Windows using an account that belongs to the Administrators group.

2. If you are using other applications, close them.

3. Copy <DVD-ROM>\utilities\updater to any folder on CS.

   - \ITBudgetMGRserverUpdate.zip: DS updater

   - \ITBudgetMGRclientUpdate.zip: CT updater

   (Example)

   ```
   c:\temp\updater\DS\ITBudgetMGRserverUpdate.zip
               \CT\ITBudgetMGRclientUpdate.zip
   ```

4. 3. Start the command prompt to register DS updater.

   Execute updater registration command (updaterregist.exe) as follows. For the detailed method for using the command, refer to "Command Reference" in the *Systemwalker Desktop Patrol Reference Manual*.

```
<DTP Installation Target>\FJSVsbtrs\bin\updaterregist.exe  -dir  <Updater saving folder>
```

Updater saving folder: specify the folder for saving DS updater in Procedure 2.

(Example)

```
> "C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\FJSVsbrs\bin\updaterregist.exe" -dir c:
\temp\updater\DS
```

5. 4. Then register CT updater.

```
<DTP Installation Target>\FJSVsbtrs\bin\updaterregist.exe  -dir  <Updater saving folder>
```

Updater saving folder: specify the folder for saving DS updater in Procedure 2.

(Example)

```
> "C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\FJSVsbrs\bin\updaterregist.exe"  -dir c:
\temp\updater\CT
```

6. 5. Confirm the application status.

The updater application status can be confirmed in the **Distribution** > **Software Auditing** window of the main menu.

DS updater application can be confirmed through **Distribution Preparation Status** after selecting the distribution DS updater in the **Software Distribution** > **Set Software Distribution Target** window of the main menu. "Table 4.1 Distribution preparation status message of DS updater" will be displayed in **Distribution Preparation Status**.

Table 4.1 Distribution preparation status message of DS updater

Message	Descriptions	Processing
NO ERROR (Executing delivery)	DS updater distributing	Distributing DS updater. No need to process.
NO ERROR (Completed delivery)	DS updater distribution completed	DS updater distribution has been completed. No need to process.
NO ERROR (Completed apply)	DS updater application completed	DS updater application has been completed. No need to process.
Failed to download software	DS updater download failed	Confirm the following content. - whether the available disk capacity is insufficient - whether the disk volume label is incorrect If the content above has been confirmed but cannot be solved, contact the technical staff after collecting logs.
Failed to update modules	DS updater application failed	Confirm the following content. - whether the available disk capacity is insufficient - whether the disk volume label is incorrect If the content above has been confirmed but cannot be solved, contact the technical staff after collecting logs.

Information

Application timing for the registered updater

- DS application timing

Start to apply according to the timing of **Communication Interval with Upstream CS/DS** of the select object DS window in **Environment Setup > CS/DS settings and operation status** of the main menu. The time required for application is from updater registration to the maximum **Communication Interval with Upstream CS/DS** (minute).

After rebooting PC before receiving updater, the timing for **Communication Interval with Upstream CS/DS** will be modified. The time up to application required is from PC reboot to the maximum **Communication Interval with Upstream CS/DS** (minute).

- Application timing oriented to CT

Start to apply according to the timing for receiving policy. Since policy receiving is performed in **Confirm Policy Interval**, the time required for application is from updater registration to the maximum **Confirm Policy Interval** (minute).

Besides, after rebooting PC before receiving policy, the timing for receiving policy will be modified, the time up to application required is from PC reboot to the maximum **Confirm Policy Interval** (minute).

4.3 Version Upgrade for OS

This section describes the procedure for OS version upgrade.

In case of CS

OS of PC installed with CS cannot be performed version upgrade.

In case of DS

When upgrading the version of OS of PC installed with DS, execute as follows.

1. Start **Administrative Tools** > **Service**.

   The **Services** window is displayed.

2. Select **ITBudgetMGR (INV)** and right click it.
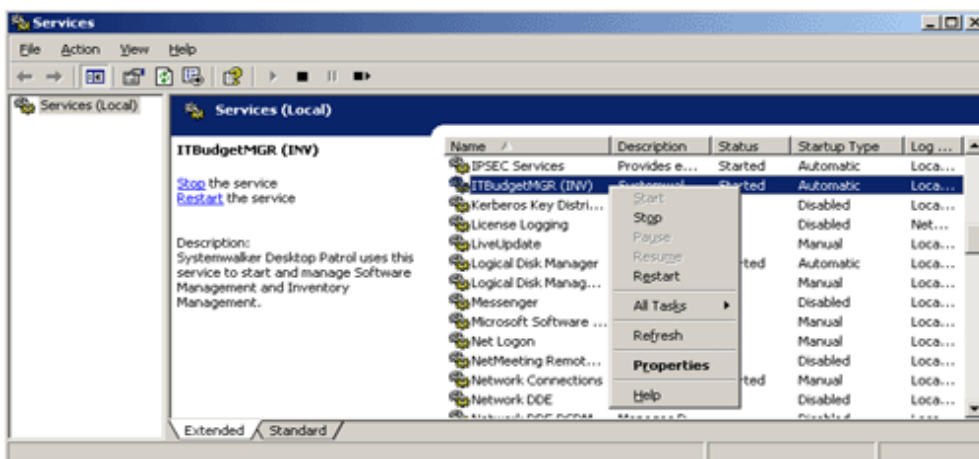
3. Select and modify the properties.

   Modify **Startup Type** from **Automatic** as **Manually**.

Select the **Stop** button in **Service Status** to stop the service.
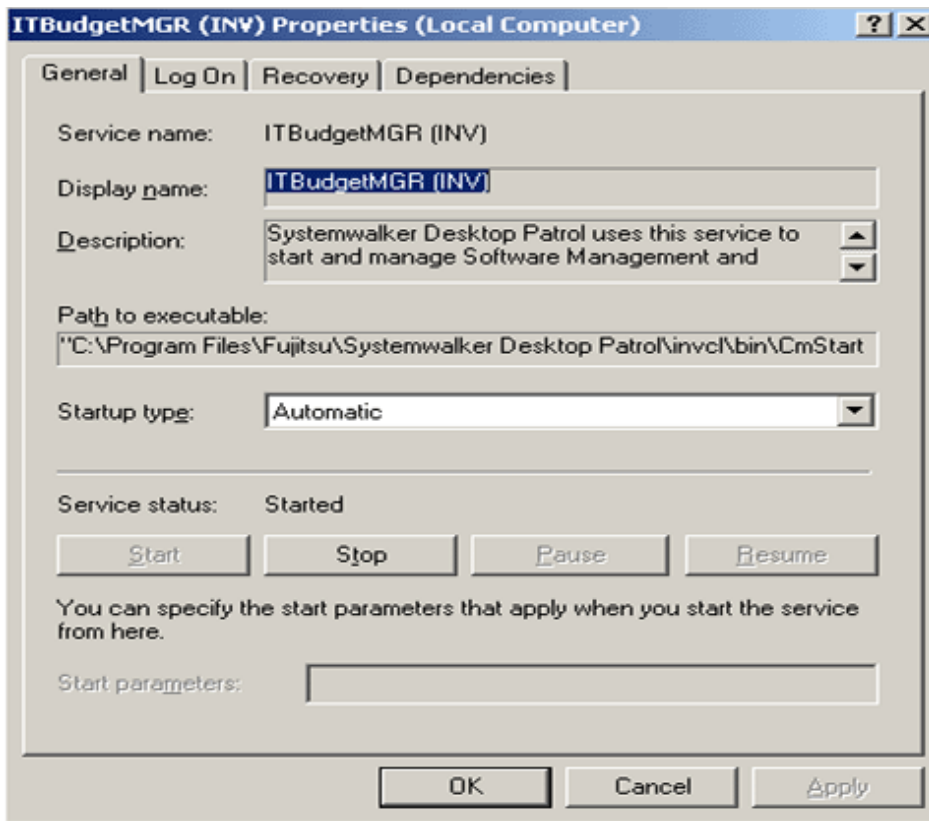
4. Close the **Services** window through the **Close** button.
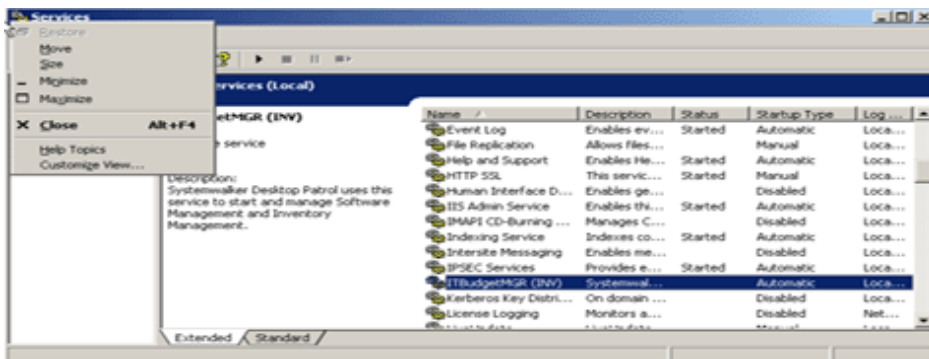
5. Upgrade OS.

6. After OS upgrade is completed, the properties window of Procedure 3 will be displayed.

7. Modify **Startup Type** from **Manual** as **Automatic**.

8. Select the **Start** button in **Service Status** to start the service.

At this time, DS can be used.

In case of AC

When upgrading the operating system of the PC on which the AC is installed from an operating system that is earlier than Windows Vista(R) to Windows Vista(R), Windows(R) 7, or Windows(R) 8, follow the steps below:

1. Upgrade OS.

2. Create the folder "(Drive for upgrading OS)\ProgramData\Fujitsu\DTPA".

3. Copy the settings file "acsetup.ini" under AC installation target folder to the created folder.

In case of ADT

When upgrading the operating system of the PC on which the ADT is installed from an operating system that is earlier than Windows Vista(R) to Windows Vista(R), Windows(R) 7, or Windows(R) 8, follow the steps below:

1. Upgrade OS.

2. Create the folder "(Drive for upgrading OS)\ProgramData\Fujitsu\DTPA".

3. Copy the settings file "Ass_AutoDetect.ini" under ADT installation target folder to the created folder.

In case of CT

When upgrading OS of PC installed with CT, perform as follows.

Note

Before upgrading the version of OS, confirm unapplied security patches that do not exist in **PC Information** > **Inventory Information** of the main menu. After performing version upgrade directly, unnecessary security patches might be applied to the new OS. Besides, for how to confirm Inventory information, refer to *Systemwalker Desktop Patrol Operation Guide: for Administrators*.

1. Click **Start** > **All Programs** > **Systemwalker Desktop Patrol CT** > **Software Download**, or **Apps** > **Systemwalker Desktop Patrol CT** > **Software Download** in CT to be upgraded, and confirm that security patches do not exist in **Patches** of tree view.

2. If security patches exist in **Patches** of tree view, apply security patches through the software download window.

3. Start **Administrative Tools** > **Service**.
   The **Services** window is displayed.

4. Select **ITBudgetMGR (INV)** and right click it.
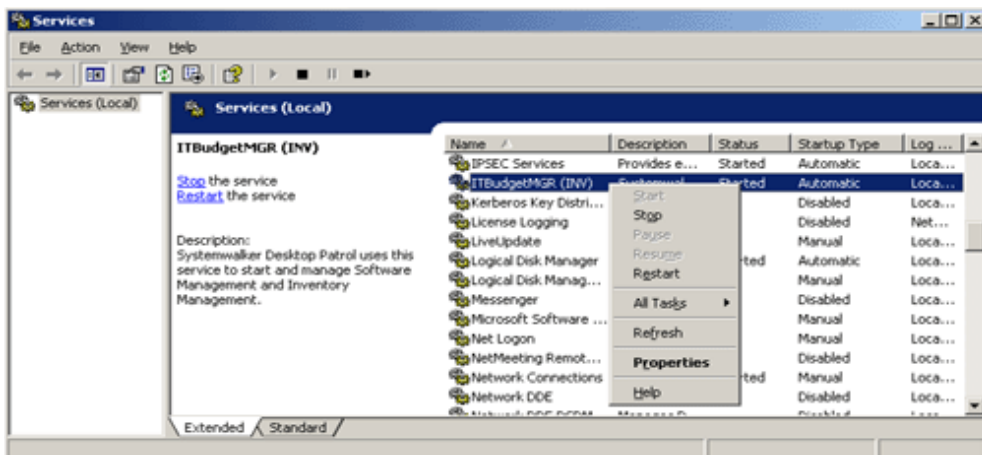
5. 5. Select and modify the properties.

   Modify **Startup Type** from **Automatic** as **Manual**.

Select the **Stop** button in **Service Status** to stop the service.
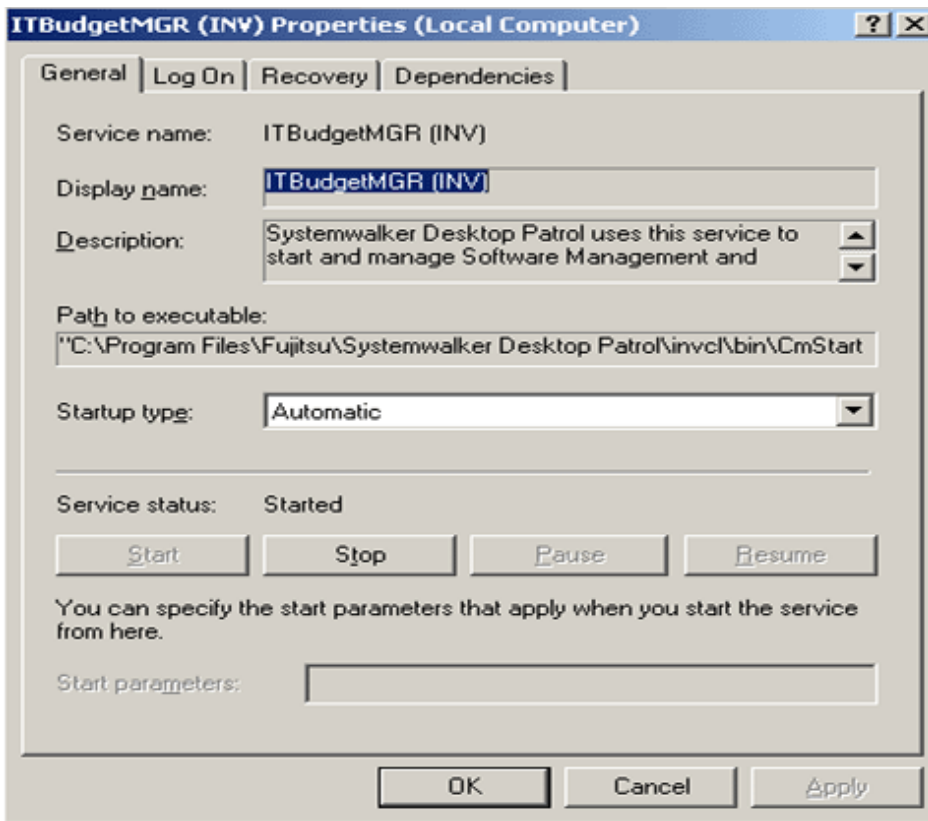
6. 6. Close the **Services** window through the **Close** button.
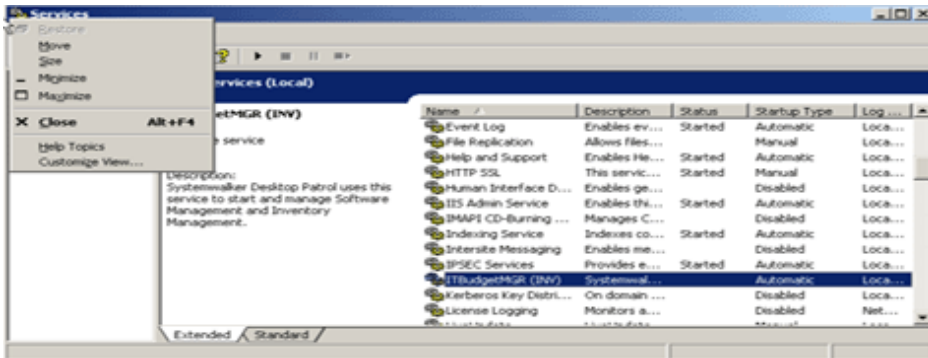
7. 7. Upgrade OS.

8. 8. After OS upgrade is completed, the properties window of Procedure 5 will be displayed.

9. 9. Modify **Startup Type** from **Manual** as **Automatic**.

10. 10. Select the **Start** button in **Service Status** to start the service.

11. 11. Logon and logoff from Windows.

At this time, CT can be used.

For SS

Back up the data, and upgrade the operating system as required.

Chapter 5 Uninstallation

This chapter describes how to uninstall Systemwalker Desktop Patrol.

5.1 Uninstall CT

This section describes how to uninstall CT.

Procedure of uninstalling CT is as follows:

1. Delete the program

2. Delete the installation folder

3. Delete CT information from PC information on CS.

Besides, when uninstalling the entire product (also including deleting CS), omit procedure 3.

Regarding the execution of procedure 3 when reinstalling CT

When reinstalling CT, whether procedure 3 need be executed is depended on the settings during reinstallation.

- Set the user ID and PC name as the same: procedure 3 omitted

- Set the user ID and PC name as different: procedure 3 needed

    Without performing procedure 3, the previous Inventory information will be reserved directly.

Delete the program

1. Log on to Windows with The account that belongs to the Administrator group.

2. Start **Control Panel** > **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**.

3. Select **Systemwalker Desktop Patrol CT** and click the **Delete** button.

4. When CT uninstallation is prohibited, the following window for entering password will be displayed after clicking the **Yes** button in the window for confirming deletion.

    Enter the password set through CTPolicy.exe (Client environment setup) command. For command details, refer to *Systemwalker Desktop Patrol Reference Manual*.

5. Start to uninstall. After it is completed normally, the **Uninstallation Completed** window is displayed.

📒 Note

. . . .
When executing in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012

When executing in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012, the user account control window of the following message will appear, select **Allowed**.

```
Unrecognizable program requests to access the computer.
```
. . . .

Delete the installation folder

After the program is deleted, related folders might have not been deleted. At this time, delete the installation target folder of this product through Explorer after restarting OS.

Example) Delete the folder C:\Program Files\Fujitsu\Systemwalker Desktop Patrol

Delete CT information from PC information on CS

After the installation folder is deleted, CT information managed by CS need be deleted.

Delete by using the following 2 methods.

- Delete from section tree

- Delete by search

Procedure of deletion is as follows:

[When Deleting from Section Tree]

1. Enter the URL below in the **Address** column on the Web Browser.

```
http://server-information (FQDN name or host name or IP address of [Systemwalker Desktop
Patrol CS])/DTP/index.html
```

2. The login window is displayed, input the following information and click the **Logon** button.

   - **User ID** text box: User ID of "System Administrator"

   - **Password** text box: Password of "System Administrator"

3. The main menu is displayed. When the initial window is not **Inventory Information** of **PC Information**, select **Inventory Information** of **PC Information**.
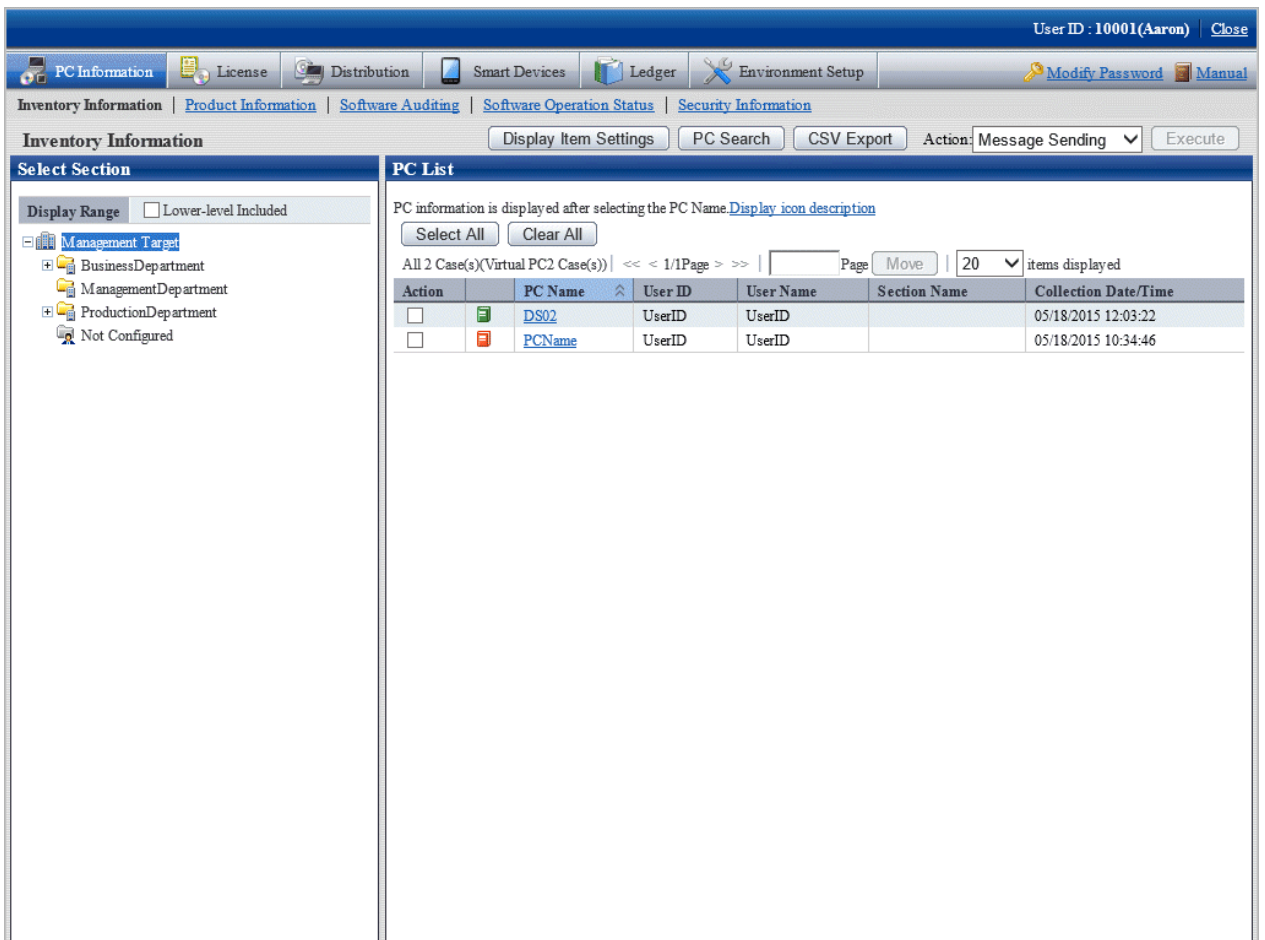
4. Select the affiliated section of PC to be uninstalled from the organization tree of **Select Section**.

5. Select PC to be uninstalled, click the **Execute** button after selecting **Delete** in the processing, delete Inventory information.

[Delete by Search]

It is the same as the procedure before step 4 of [When Deleting from Section Tree].

1. Click the **PC Search** button in the **Inventory Information** window, the following window is displayed.

2. Enter the information about the PC to be uninstalled and click the **Search** button, list of PCs matching the search conditions is displayed.

3. Select the PC to be uninstalled, click the **Execute** button after selecting **Delete** in the processing, delete Inventory information.

5.2 Uninstall ADT

This section describes how to uninstall ADT.

Procedure of uninstalling ADT is as follows:

Delete the program

1. Log on to Windows with The account that belongs to the Administrator group. When other application is in use, end this application.

2. Start **Control Panel** > **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**.

3. Select **Systemwalker Desktop Patrol ADT** and click the **Delete** button.

4. Start to uninstall. After it is completed normally, the **Uninstallation Completed** window is displayed.

🖐 **Note**

· ·

When executing in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012

When executing in Windows Vista(R), Windows(R) 7, Windows(R) 8, Windows Server(R) 2008 or Windows Server(R) 2012, the user account control window of the following message, select **Allowed**.

```
Unrecognizable program requests to access the computer.
```

Delete the installation folder

After the program is deleted, related folder might have not been deleted. At this time, delete the installation target folder of this product through Explorer after restarting OS.

Example) Delete the folder C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\ADT

5.3 Uninstall DS

This section describes how to uninstall DS.

Besides, after Systemwalker Desktop Patrol DS is uninstalled, Systemwalker Desktop Patrol CT installed with it will also be uninstalled.

Procedure of uninstall DS are as follows:

1. Delete DS information from server information on CS.

2. Delete the program

3. Delete the installation folder

4. Delete DS information from PC information on CS.

Delete DS information from server information on CS.

Delete DS server information from CS.

The deleting method is as follows:

1. Start the command prompt and execute the following command.

```
Installation Directory of Desktop Patrol CS\FJSVsbtrs\bin\DSDelete.exe" -host <Deleted DS Host
Name>
```

Delete the program

1. Log on to Windows with The account that belongs to the Administrator group.

2. Start **Control Panel** > **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**.

3. Select **Systemwalker Desktop Patrol (DS)** and click the **Delete** button.

4. Start to uninstall. After it is completed normally, the **Uninstallation Completed** window is displayed.

Delete the installation folder

Delete the following folder.

- After the program is deleted, related folder might have not been deleted. At this time, delete the installation target folder of this product through Explorer after restarting OS.

  Example) Delete the folder C:\Program Files\Fujitsu\Systemwalker Desktop Patrol

- When the software saving directory is not specified under the installation folder of DS, even if DS is uninstalled, the software distribution data will remain instead of being deleted. At this time, delete the unnecessary data under the software saving target directory after uninstalling DS.

Delete DS information from PC information on CS.

Delete PC information with DS installed from CS.

For deleting procedures, refer to "Delete CT information from PC information on CS" of "Uninstall CT".

5.4 Uninstall AC

This section describes how to uninstall AC.

Procedure of uninstalling AC is as follows:

Delete the program

1. Log on to Windows with The account that belongs to the Administrator group. When other application is in use, end this application.

2. Click **Start** > **All Programs** > **Fujitsu** > **Uninstall (middleware)**, or **Apps** > **All Programs** > **Fujitsu** > **Uninstall (middleware).**

> 📝 Note
> ....
> - To uninstall the Systemwalker Desktop Patrol AC, use **Uninstall (middleware)**.
>
> - When uninstalling the Systemwalker Desktop Patrol AC because of installation failure or for some other reason, Systemwalker Desktop Patrol AC may be displayed in the **Incomplete install** tab. If the Systemwalker Desktop Patrol AC is not displayed in the **Currently installed products** tab, click the **Incomplete install** tab to check that Systemwalker Desktop Patrol AC is displayed. Always use the procedure below to uninstall the Systemwalker Desktop Patrol AC.
> ....

3. Select **Systemwalker Desktop Patrol AC** and click **Remove -** a confirmation message will be displayed.

4. Click **Uninstall**.

5. Once uninstallation completes, click **Finish** to exit the uninstaller.

6. Click **Close** in the **Uninstall (middleware)** window to exit **Uninstall (middleware)**.

> 📝 Note
> ....
> The user account control window of the following message may appear, select **Allowed**.
>
> ```
> Unrecognizable program requests to access the computer.
> ```
> ....

> 📝 Note
> ....
> If this product has been removed via **Control Panel** > **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**, follow this procedure after removing it, and then remove the Systemwalker Desktop Patrol AC from **Uninstall (middleware)**.
> ....

Delete the installation folder

After the program is deleted, related folder might have not been deleted. At this time, delete the installation target folder of this product through Explorer after restarting OS.

Example) Delete the folder C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\AC

5.5 Uninstall CS

This section describes how to uninstall CS.

The same uninstallation procedure must be followed regardless of the types of installation procedure.

Procedure of uninstall CS are as follows:

1. Uninstall remote operation (Live Help Expert and Live Help Client)

2. Delete the program

3. Restart OS

4. Delete WWW Server information

5. Delete the installation folder

Uninstall remote operation (Live Help Expert and Live Help Client)

Even if CS is uninstalled, the remote operation (Live Help Expert and Live Help Client) installed on CS will not be uninstalled. When uninstalling the remote operation, uninstall following the Procedure of uninstalling remote operation.

Delete CS program

1. Log on to Windows with The account that belongs to the Administrator group.

2. Click **Start** > **All Programs** > **Fujitsu** > **Uninstall (middleware),** or **Apps** > **All Programs** > **Fujitsu** > **Uninstall (middleware)**.

P Point
. . . .
When uninstalling the Systemwalker Desktop Patrol because of installation failure or for some other reason, Systemwalker Desktop Patrol may be displayed in the **Incomplete install** tab. If Systemwalker Desktop Patrol is not displayed in the **Currently installed products** tab, click the **Incomplete install** tab to check that Systemwalker Desktop Patrol is displayed.
. . . .

3. Select **Systemwalker Desktop Patrol** and click **Remove -** a confirmation message will be displayed.

4. Click **Uninstall**.

5. Once uninstallation completes, click **Finish** to exit the uninstaller.

6. Click **Close** in the **Uninstall (middleware)** window to exit **Uninstall (middleware)**.

Note
. . . .
- To uninstall the Systemwalker Desktop Patrol, use **Uninstall (middleware)** tool. If this product has been removed via **Control Panel** > **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**, follow this procedure after removing it, and then remove this product using **Uninstall (middleware)**.

- If Systemwalker Desktop Patrol is not displayed in **Uninstall (middleware)**, then remove it by selecting **Control Panel** > **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**.
. . . .

1.

Restart OS

Restart OS.

Delete WWW Server information

Stop IIS, and confirm the following folders through Explorer, delete them if they are not deleted.

- <*IIS Main Directory*>\wwwroot\DTP

- <*IIS Main Directory*>\scripts\DTP

Delete the installation folder

Delete the following folder.

After the program has been deleted, the related folder may not have been deleted. At this time, delete the installation target folder of this product through Explorer after restarting OS.

Example) Delete the folder C:\Program Files\Fujitsu\Systemwalker Desktop Patrol

- When the software saving directory is not specified under the installation folder of CS, even if CS is uninstalled, the software distribution data will remain instead of being deleted. At this time, delete the unnecessary data under the software saving target directory after uninstalling CS.

- When the saving target of CT operation status log is not specified under the installation folder of CS, even if CS is uninstalled, CT operation status log will remain instead of being deleted. Thus, delete the unnecessary data under the saving target directory of CT operation status log after uninstalling CS.

5.6 Uninstall SS

This section describes how to uninstall the SS.

To uninstall SS, follow the steps below:

Remove the program

1. Log on to Windows using an account that belongs to the Administrators group. If you are using other applications, close them.

2. Execute swss_config.exe (SS environment setup command) to configure the following settings:

    - Disable Android device management by specifying the option with /Android.enabled.

    - Disable iOS device management by specifying the option with /iOS.enabled.

    Refer to the *Systemwalker Desktop Patrol Reference Manual* for details on swss_config.exe (SS environment setup command).

3. Click **Start** > **All Programs** > **Fujitsu** > **Uninstall (middleware),** or **Apps** > **All Programs** > **Fujitsu** > **Uninstall (middleware)**.

📌 Note
. . . .
- To uninstall the Systemwalker Desktop Patrol SS, use **Uninstall (middleware)**.

- When uninstalling the Systemwalker Desktop Patrol SS because of installation failure or for some other reason, Systemwalker Desktop Patrol SS may be displayed in the **Incomplete install** tab. If the Systemwalker Desktop Patrol SS is not displayed in the **Currently installed products** tab, click the **Incomplete install** tab to check that the Systemwalker Desktop Patrol SS is displayed. Always use the procedure below to uninstall the Systemwalker Desktop Patrol SS.
. . . .

4. Select **Systemwalker Desktop Patrol SS** and click **Remove** - a confirmation message will be displayed.

5. Click **Uninstall**.

6. Once uninstallation completes, click **Finish** to exit the uninstaller.

7. Click **Close** in the **Uninstall (middleware)** window to exit **Uninstall (middleware)**.

📌 Note
. . . .
If this product has been removed via **Control Panel** > **Add or Remove Programs**, or **Programs and Features** > **Uninstall a program**, follow this procedure after removing it, and then remove the Systemwalker Desktop Patrol SS from **Uninstall (middleware)**.
. . . .

Deleting the installation directory

After a program is removed, related directories may remain. If this happens, delete the installation directory for this product in Windows Explorer after the operating system is restarted.

Example: Delete C:\Program Files\Fujitsu\Systemwalker Desktop Patrol\SS

5.7 Uninstalling the Smart Device CT (Android)

If the smart device CT is no longer required on an Android device, follow the steps below to uninstall it (the example screenshots are from Android 4.1).

1. Open the setup screen and tap **Desktop Patrol Client** from the list of administrators.

   The list of administrators depends on the version.

   - Android 3.0 to 3.2: **Settings** > **Location and security** > **Device administrator**

   - Android 4.0 or later: **Settings** > **Security** > **Device administrators**
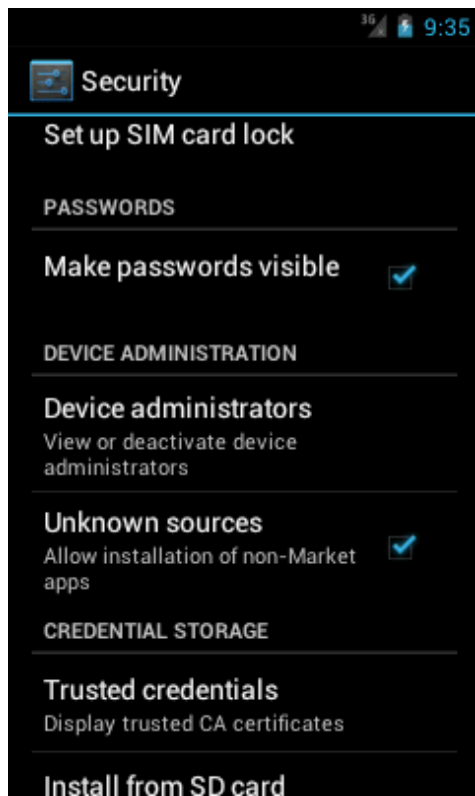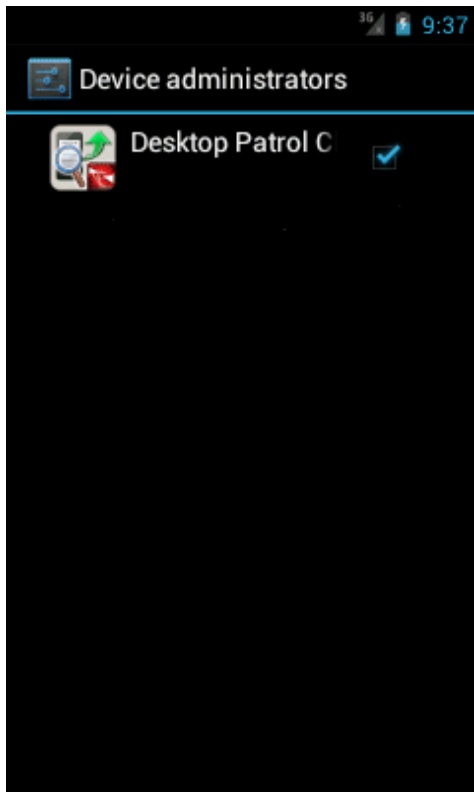
2. A confirmation window will be displayed. Tap **Deactivate**.
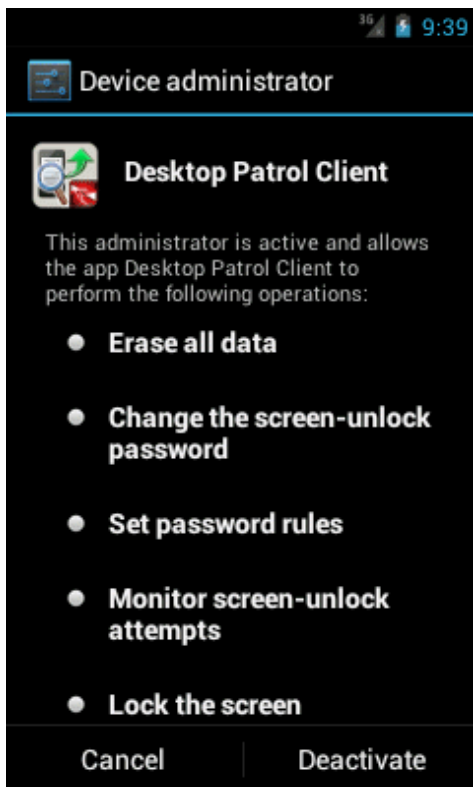
3. Open the setup screen and tap **Desktop Patrol Client** from the list of applications.

   The list of applications depends on the version.

   - Android 3.0 to 3.2: **Settings** > **Applications** > **Manage applications**

- Android 4.0 or later: **Settings** > **Apps**
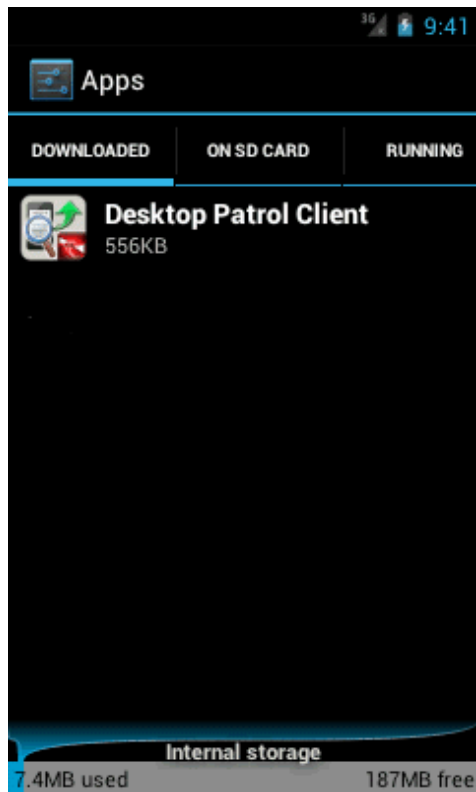
4. Tap **Uninstall** to uninstall smart device CT.
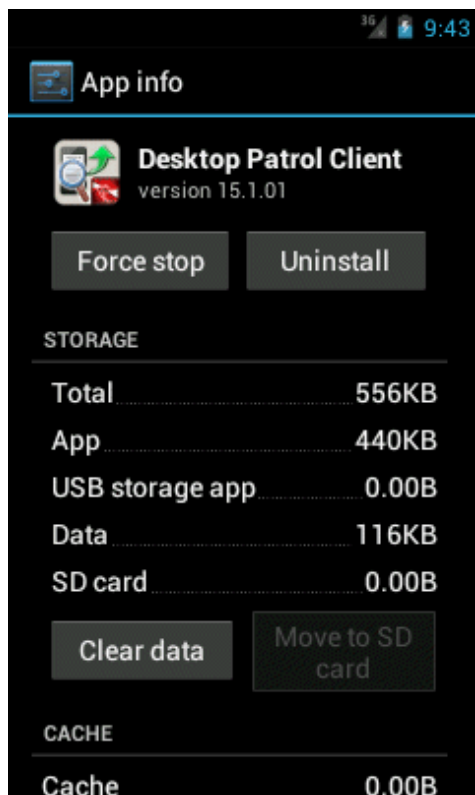
5.8 Uninstalling the Smart Device CT (iOS)

If the smart device CT is no longer required on an iOS device, follow the steps below to uninstall it (the example screens are from iOS 6.0.1).
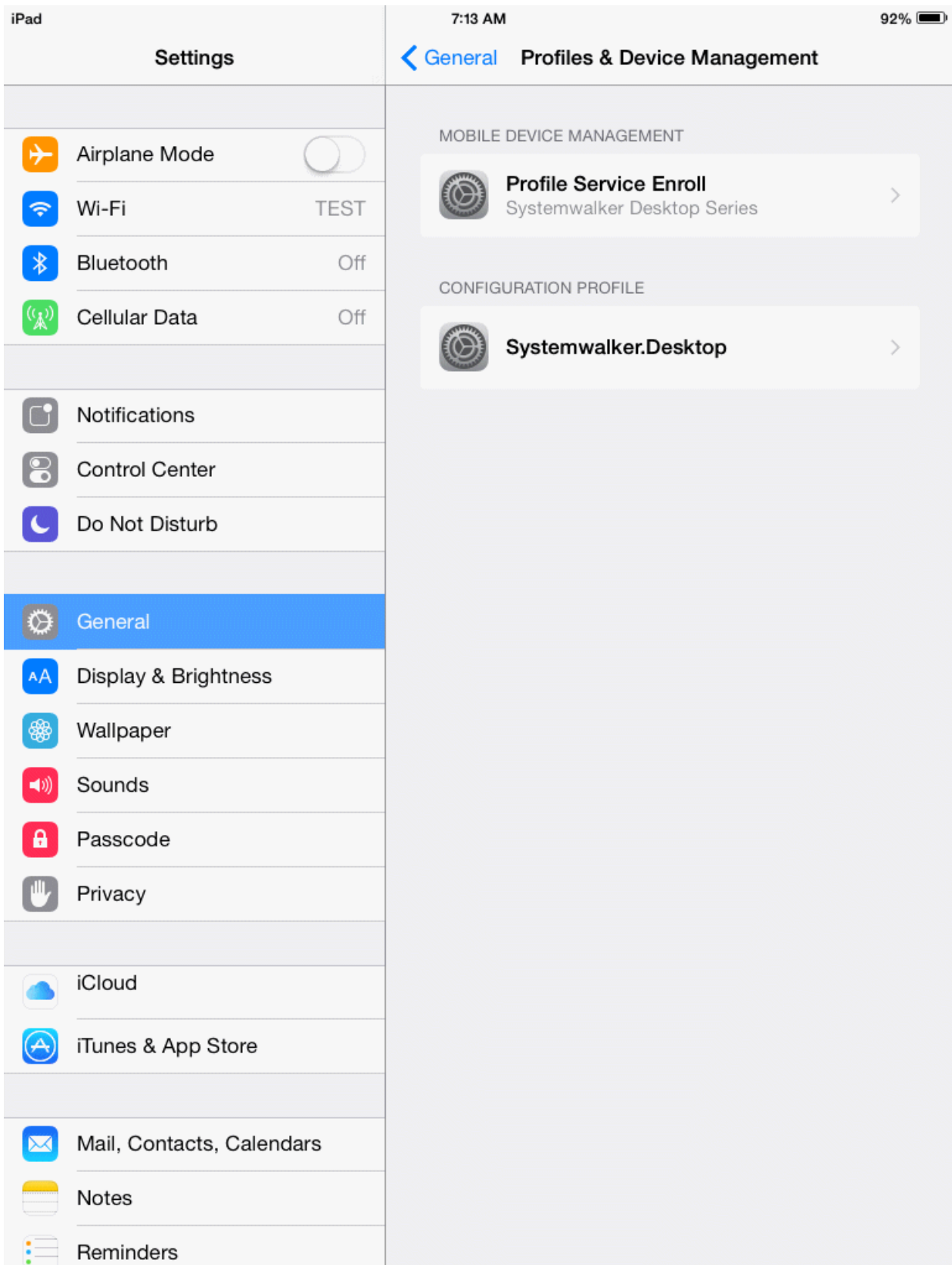
In the iOS device, select **Settings** > **General** > **Profile**, and delete the following profiles.

- Profile Service Enroll

- CA certificate (server)

- CA certificate (client)

5.9 Notes after Uninstallation

Notes after Systemwalker Desktop Patrol uninstallation are explained below:

Uninstalling Uninstall (middleware)

Uninstall (middleware) is a common tool for Fujitsu middleware products. It manages information about Fujitsu middleware products installed, as well as launching the product uninstallers.

![Note]

- This tool also manages information about Fujitsu middleware products other than Systemwalker Desktop Patrol. Do not uninstall this tool unless it is absolutely necessary.

  If this tool is uninstalled accidentally, perform the following procedure to install it again.

  1. Log in to the machine where the tool is to be installed as a user belonging to the Administrators group, or switch to an account with administrator privileges.

  2. Insert the product media in the drive.

  3. Run the install command.

     ```
     productMedia\CIR\cirinst.exe
     ```

- To uninstall this tool, perform the procedure below.

  1. Start **Uninstall (middleware)** and ensure that there are no other Fujitsu middleware products left on the system. Start the tool as follows:

     Click **Start** > **All Programs** > **Fujitsu** > **Uninstall (middleware)**, or **Start** > **All Programs** > **Fujitsu** > **Uninstall (middleware)**.

  2. If there are no Fujitsu middleware products left, execute the uninstallation command below:

     ```
     %SystemDrive%\FujitsuF4CR\bin\cirremove.exe
     %ProgramFiles%\Fujitsu\FujitsuF4CR\bin\cirremove.exe # For 32-bit operating system
     %ProgramFiles(x86)%\Fujitsu\FujitsuF4CR\bin\cirremove.exe # For 64-bit operating system
     ```

  3. When **This software is a common tool of Fujitsu products. Are you sure you want to remove it?** is displayed, enter "y" to continue with uninstallation.

     After a few seconds, uninstallation will be complete.

  4. After uninstallation, the directory below and its files will remain, so they must be manually deleted.

     %SystemDrive%\FujitsuF4CR

     %ProgramData%\Fujitsu\FujitsuF4CR

Appendix A Server Silent Installation

This appendix describes files, commands, and messages used in silent installation of the Systemwalker Desktop Patrol server.

A.1 Silent installation of CS

This section explains silent installation of CS.

A.1.1 Installation Parameter CSV File

Specify the installation parameters in a CSV file using the format specified in this section.

Character encodings

ASCII

Format

```
installInfo,softwareName,softwareName
installInfo,OS,os
installInfo,Version,version
installInfo,Name,installerName
parameters,paramKey,paramValue
parameters,...,...
```

📝 Note

- Do not change any installInfo parameter from the sample content.

- When specifying a file path in a parameters parameter, do not exceed 256 halfwidth characters, otherwise, a parameter error will occur.

- Specify one or more parameters in the parameters parameter.

- If double quotation marks are used to enclose data, then all fields within the same record must be enclosed in double quotation marks.

- Do not specify spaces in the first column or in the second column.

- Spaces cannot be specified before or after fields enclosed in double quotation marks.

📖 Information

A sample installation parameter CSV file is stored in the following folder of the product media (DVD-ROM).

- Folder
  dvdRom:\citool\CS\sample\

  - If installing a 32-bit version of CS on a 32-bit version of the operating system or installing a 64-bit version of CS on a 64-bit version of the operating system:
    sample_install.csv

  - If installing a 32-bit version of CS on a 64-bit version of the operating system:
    sample32_install_x64.csv

parameters parameter

The parameters are described below.

No.	Parameter	Parameter information		Description
1	Desktop Patrol installation directory	Key	InstallDir	Specify the installation directory for this product. Install this product in a folder that is not used for other programs. Optional (if this parameter is omitted, the key must be omitted as well).
		Data type	String	
		Default value	If installing a 32-bit version of CS on a 32-bit version of the operating system, or installing a 64-bit version of CS on a 64-bit version of the operating system: C:\Program Files\Fujitsu\Systemwalker Desktop Patrol If installing a 32-bit version of CS on a 64-bit version of the operating system: C:\Program Files (x86)\Fujitsu\Systemwalker Desktop Patrol	
2	IIS (Internet Information Services) home folder	Key	IISHomeDir	Specify the IIS home folder specified in the installation destination PC. Optional (if this parameter is omitted, the key must be omitted as well).
		Data type	String	
		Default value	C:\Inetpub	
3	Server name	Key	ServerName	Specify the name of the company that will install Systemwalker Desktop Patrol CS. Specify up to 50 characters using halfwidth alphanumeric characters, and the following symbols: - @ . Example: Fujitsu Limited Optional (if this parameter is omitted, the key must be omitted as well).
		Data type	String	
		Default value	CS	
4	Host name	Key	HostName	Specify the FQDN format, IP address or computer name of the PC where Systemwalker Desktop Patrol CS will be installed. Specify up to 50 characters, using alphanumeric characters, hyphens and periods. Example: cs.example.com Also, it is necessary to specify a name that can be resolved using the Systemwalker Desktop Patrol DS/CT that will be connected. This value cannot be changed after installation. When communicating in an IPv6 environment, refer to the notes below. Optional (if this parameter is omitted, the key must be omitted as well).
		Data type	String	
		Default value	(Host name or IP address retrieved automatically from the system)	
5	Software distribution port number	Key	SoftwarePort	Specify the port number used for software distribution. The default is 2922. If changing the port number, specify a value from 5001 to 65535 that does not conflict with other systems. This value cannot be changed after installation.
		Data type	number	
		Default value	2922	

No.	Parameter	Parameter information		Description
				Optional (if this parameter is omitted, the key must be omitted as well).
6	Port number for inventory transmission	Key	InventoryPort	Specify the port number to be used for inventory transfer. The default is 2856. If changing the port number, specify a value from 5001 to 65535 that does not conflict with other systems. This value cannot be changed after installation. Optional (if this parameter is omitted, the key must be omitted as well).
		Data type	number	
		Default value	2856	
7	Software distribution directory	Key	SoftwareDir	Specify the software distribution directory using an absolute path of up to 128 halfwidth characters. The following symbols cannot be specified: / * ? \ " < > | If changing the directory, specify a directory that has sufficient available space. Also, if applying security patches automatically, specify a directory with sufficient available space on a drive other than the Windows installation drive. In order to prevent the occurrence of insufficient disk space due to software registration/distribution or automatic application of security patches, you should specify an area other than the disk space where the operating system is installed for the software distribution directory. This value cannot be changed after installation. Optional (if this parameter is omitted, the key must be omitted as well).
		Data type	String	
		Default value	(*csInstallDir*>\FJSVsbtrs\data\swc)	
8	Maximum size	Key	SoftwareDirMaxSize	Specify the maximum disk size (in MB) for the software distribution directory. Specify the maximum size using a number from 1 to 999999. If omitted, the available space of the specified directory will be used. You can specify a value equal to or greater than the available space of the drive specified for the software distribution directory. Specify a value according to the environment design of the PC. Optional (if this parameter is omitted, the key must be omitted as well).
		Data type	number	
		Default value	(Same as when this value is omitted)	
9	Database directory	Key	SETUPDIR	Specify the database directory. Specify a path name using up to 64 characters. The directory cannot contain halfwidth spaces. If the database directory is not DESKTOPPATROL_DBSP, a directory with that name will be automatically created
		Data type	String	
		Default value	C:\DESKTOPPATROL_DBSP	

No.	Parameter	Parameter information		Description
				under the specified directory, and the database will then be stored in it.
				Optional (if this parameter is omitted, the key must be omitted as well).
10	Number of PCs	Key	CLIENT	Specify the estimated number of PCs that can be managed by Systemwalker Desktop Patrol.
		Data type	number	You can specify a number from 100 to 100000.
		Default value	300	
				Optional (if this parameter is omitted, the key must be omitted as well).
11	Number of smart devices	Key	SMARTDEVICE	Specify the number of smart devices to be managed by Systemwalker Desktop Patrol. You can specify a number from 0 to 100000.
		Data type	number	
		Default value	0	
				Optional (if this parameter is omitted, the key must be omitted as well).
12	Number of managed devices except PCs	Key	EXCEPTCLIENT	Specify the number of devices (fixtures) to be managed by Systemwalker Desktop Patrol. You can specify a number from 0 to 100000.
		Data type	number	
		Default value	0	
				Optional (if this parameter is omitted, the key must be omitted as well).
13	User ID	Key	UserID	Specify a system account used when operating the main menu and the user ID to be managed as Systemwalker Desktop Patrol CT.
		Data type	String	The user ID specified here will be displayed in the main menu and is used to identify the user.
		Default value	systemadmin	You can specify up to 20 halfwidth alphanumeric characters and the following symbols: - @ . _. Alphabetic characters are case-sensitive.
				Optional (if this parameter is omitted, the key must be omitted as well).
14	Password	Key	PASSWD	Specify the system account password for operating the main menu.
		Data type	String	Specify from 4 to 12 halfwidth alphanumeric characters, halfwidth spaces, and the following halfwidth symbols: - = * + ' @ ~ ( ) & $ # " ! ? % \ . , / : ; ` [ ] | < > { _ }
		Default value	systemadmin	Alphabetic characters are case-sensitive.
				Optional (if this parameter is omitted, the key must be omitted as well).
15	PC name	Key	PCName	Specify a name to be managed as Systemwalker Desktop Patrol CT.
		Data type	String	You can specify up to 20 halfwidth alphanumeric characters. You cannot specify spaces and the following symbols: + * ? < > , ; : \ / " |
		Default value	(The first 20 characters of the host name (HostName key))	

No.	Parameter	Parameter information		Description
				Optional (if this parameter is omitted, the key must be omitted as well).
16	Contents of user information 1	Key	UserInfo1	Specify this item when you have been instructed to do so by the system administrator. You can specify up to halfwidth alphanumeric characters, halfwidth spaces, and the following symbols: - @ . ( ) [ ] < > : ; / { }
		Data type	String	
		Default value	Null	
				Optional (if this parameter is omitted, the key must be omitted as well).
17	Contents of user information 2	Key	UserInfo2	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
18	Contents of user information 3	Key	UserInfo3	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
19	Contents of user information 4	Key	UserInfo4	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
20	Contents of user information 5	Key	UserInfo5	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
21	Contents of user information 6	Key	UserInfo6	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
22	Contents of user information 7	Key	UserInfo7	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
23	Contents of user information 8	Key	UserInfo8	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
24	Contents of user information 9	Key	UserInfo9	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
25	Contents of user information 10	Key	UserInfo10	Refer to the explanation of "Contents of user information 1".

No.	Parameter	Parameter information		Description
		Data type	String	
		Default value	Null	

🗒 Note

. . . .

Communication in IPv6 environments

IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand by using one of the following patterns, and then enter the host name:

- Register the CS and DS host name and the IP address in the DNS server.

- Register the CS and DS host name and the IP address in the communication source PC hosts file.

. . . .

A.1.2 Parameter Setup Command

If customizing parameters, create a response file in which the parameters were changed using the parameter setup command, and use this file for silent installation.

Command name

dvdRom:\citool\CS\dtp_instparam.exe

Syntax

dtp_instparam.exe -infile *installParmCsvFile* -outfile *responseFile*

Options

Option	Description
-infile	Specify the installation parameter CSV file. If the path includes spaces, enclose it in double quotation marks.
-outfile	Specify the output destination of the response file for silent installation. If a file already exists in the output destination, it will be overwritten. If the path includes spaces, enclose it in double quotation marks.

Output format

The return value is 0 if the command ends normally.

The return value is other than 0 if the command ends abnormally. If this happens, refer to the error message output to the console and take appropriate action.

Examples

The following command specifies the parameters in the installation parameter CSV file C:\dtp.csv, and creates the response file C:\dtp.iss for silent installation:

dtp_instparam.exe -infile C:\dtp.csv -outfile C:\dtp.iss

A.1.3 Messages Output by the Parameter Setup Command

This section describes the messages output by the parameter setup command.

Command syntax errors

ERROR: Too few arguments.

Cause

An argument required for executing the command is missing.

Action

Check the syntax of the command.

ERROR: The syntax of the command is incorrect.

Cause

The syntax of the specified command is incorrect.

Action

Check the syntax of the command.

ERROR: Cannot find the file specified -infile.

Cause

The installation parameter CSV file specified in the -infile option does not exist.

Action

Check the path of the installation parameter CSV file.

Installation parameter CSV file format errors

These messages are output if the installation parameter CSV file format is invalid.

ERROR: CSV file error:code = 1, Invalid CSV error.

Cause

The CSV definition format is incorrect.

Action

The CSV data specified in the installation parameter CSV file does not match the format described in "A.1.1 Installation Parameter CSV File".

Ensure that there is no invalid CSV data in the file.

ERROR: CSV file error:code = 2, installInfo/Name is required.

Cause

The installInfo parameter Name is not specified.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 3, Invalid installInfo key.

Cause

The specified installInfo is incorrect.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 4, Duplicated installInfo key.

Cause

The same parameter definition has been defined in duplicate in installInfo.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 5, Invalid character length.

Cause

The specified string is too long.

Action

Ensure that the specified string is not too long.

ERROR: CSV file error:code = 6, Invalid character format or encoding.

Cause

The character encoding of the installation parameter CSV file is incorrect.

Action

Ensure that the character encoding of the installation parameter CSV file is correct.

ERROR: CSV file error:code = 8, Parameter is required.

Cause

A parameter value has not been specified.

Action

Check the parameter values.

Parameter check errors

These messages are output if a parameter value specified in the installation parameter CSV file is incorrect.

ERROR: Parameter error. [%1]Maximum size is %2 characters.

Cause

A value of parameter %1 exceeds the maximum string length of %2 characters.

Action

Review the parameter values, and specify a value up to the maximum number of characters.

ERROR: Parameter error. [%1] Invalid character. Double-byte characters.

Cause

The %1 key contains fullwidth characters.

Action

Do not specify fullwidth characters.

ERROR: Parameter error. [%1] Invalid character. Half-width kana characters.

Cause

The %1 key contains halfwidth kana characters.

Action

Do not specify halfwidth kana characters.

ERROR: Parameter error. [%1] Invalid character.

Cause

The %1 key contains an invalid character (such as a control character).

Action

Check the character types that can be specified, and delete all characters that cannot be specified.

ERROR: Parameter error. [%1] Invalid character '%2'.

Cause

The %1 key contains the invalid character %2.

Action

Do not specify invalid characters.

ERROR: Parameter error. [%1] The path specified must be an absolute path.

Cause

An absolute path is not specified in the %1 key.

Action

Specify an absolute path.

ERROR: Parameter error. [%1]Valid range is from %2 to %3.

Cause

An out-of-range number is specified as the value in the %1 key.

Action

Specify a number from %2 to %3.

ERROR: Parameter error. [%1]Invalid format.

Cause

The format of the %1 key is incorrect. For example, a 0 precedes the number.

Action

Check the format. If a 0 precedes the number, remove it.

Other errors

ERROR: Load "%1" failed.

Cause

The required DLL %1 could not be loaded.

Action

Check if the provided csv_parse.dll resource exists in the citool\common directory, and if the dtpparam.dll resource exists in the citool\CS\dll directory.

ERROR: GetProcAddress %1 failed.

Cause

Failed to retrieve the function %1 in the DLL.

Action

Contact Fujitsu technical support.

ERROR: FreeLibrary "%1" failed.

Cause

Failed to retrieve FreeLibrary of DLL %1.

Action

Contact Fujitsu technical support.

ERROR: An unexpected exception occurred.

Cause

An unexpected error occurred.

Action

Contact Fujitsu technical support.

ERROR: An unexpected exception occurred(dtpparam.dll).

Cause

An unexpected error occurred in dtpparam.dll.

Action

Contact Fujitsu technical support.

ERROR: Cannot create output file.

Cause

Failed to create the output file.

Action

Check the path of the output file specified for the -outfile option.

A.1.4 Silent Installation Command

The silent installation command performs silent installation of CS.

Command name

dvdRom:\citool\CS\silentsetup.bat

Syntax

silentsetup.bat [*responseFile*]

Options

Option	Description
Response file (optional)	Specify this option if you want to change the parameters to be used during setup from their default values. If omitted, the default values will be used for all parameters.
	Specify the file using its absolute path, and if the path includes spaces, enclose it in double quotation marks.
	The string must be up to 256 halfwidth characters (excluding the double quotation marks).

Privilege required/execution environment

- Administrator privileges are required.

- This command is to be executed by the system administrator.

- To use this command in Windows Server(R) 2008, right-click to display the menu and then select **Run as administrator** and execute this command on the **Command Prompt** window.

- To use this command in Windows Server(R) 2012, display the desktop and execute this command on a **Command Prompt** window that has been started by selecting **Run as Administrator**.

- Only new installations are supported.

Return values

0: Ended normally

Other than 0: Ended abnormally

Output format

This command outputs messages to the console and to the message file.

Silent installation start and end messages are output to the console standard output. If the command ends abnormally, an error message is output.

After the command ends, check the setup result output to the message file.

The result is output to *csInstallDir*\log\dtpsilent.log if the command ends normally, or to *windowsFolder*\dtpsilent.log if it ends abnormally.

Examples

Perform silent installation with the response file C:\dtp.iss.

```
dvdRom:\citool\CS\silentsetup.bat C:\dtp.iss
```

A.1.5 Messages Output by the Silent Installation Command

This section explains the messages output during installation.

Messages output to the console

Information messages

Systemwalker Desktop Patrol CS silent setup start.

Cause

Installation of Systemwalker Desktop Patrol CS started.

Action

Wait until the installation ends.

Install successful.

Cause

Systemwalker Desktop Patrol CS was installed successfully.

Action

Refer to the message file *csInstallDir*\log\dtpsilent.log to check if the installation ended normally. If the message file indicates that a restart is required, perform a restart. Proceed with the tasks described in "2.3.4 Construct an iOS Management Database" and later sections.

Error messages

[ERROR0001]Administrator privileges are required.

Cause

Administrator privileges are required.

Action

Execute as a user with Administrator privileges.

[ERROR0002]Systemwalker Desktop Patrol CS already exists.

Cause

Systemwalker Desktop Patrol is already installed.

Action

This command only supports new installations.

[ERROR0003]Install Disc is corrupted. "Progress.exe" not exists.

Cause

A file required for installation was not found.

Action

Ensure that the installation disk is not corrupted.

[ERROR0004]Install Disc is corrupted. "setup.exe" not exists.

Cause

A file required for installation was not found.

Action

Ensure that the installation disk is not corrupted.

[ERROR0005]"%1" not exists.

Cause

The specified response file %1 was not found.

Action

Ensure that the response file exists.

[ERROR0006]Install failed.

Cause

Failed to install the product. An invalid parameter value may be specified.

Action

Refer to the message file *windowsFolder*\dtpsilent.log and take appropriate action. If action cannot be taken, contact Fujitsu technical support.

[ERROR0007]Install failed.

Cause

Failed to install the product. Copying of files may have failed.

Action

Refer to the message file *windowsFolder*\dtpsilent.log and take appropriate action. If action cannot be taken, contact Fujitsu technical support.

[ERROR0008]Install failed.

Cause

Failed to install the product. Installation of components may have failed.

Action

Refer to the message file *windowsFolder*\dtpsilent.log and take appropriate action.

- If "SETUP.EXE for Desktop Patrol (CS) has exited abnormally." is recorded in the message file, refer to events for which the source is MsiInstaller in the event log (application), and take appropriate action.
  If "Product: Systemwalker Desktop Patrol CS -- Error 27511. Installation failed. Check the cause of failure and execute installation again." is recorded in the event log under the above conditions, the likely cause is that the IP address or computer name could not be retrieved from the system as the default host name. In that case, specify the host name in the parameter file (recommended), or review the settings to enable retrieval of the system IP address or computer name, and after uninstallation, install the product. If the problem cannot be resolved, contact Fujitsu technical support.

- If "Operation environment construction failed : 50" is recorded in the message file, the following causes may be possible:

    - There is insufficient available space for building the database.

    - One of the parameters parameter No. 9 to 14 specified in the installation parameter CSV file is invalid. Refer to and correct the parameters parameter No. 9 to 14 in the "A.1.1 Installation Parameter CSV File", and use the parameter setup command to create the response file again.

  After removing the cause of the problem and uninstalling, perform the installation. If the problem cannot be resolved, contact Fujitsu technical support.

- If other actions cannot be taken, contact Fujitsu technical support.

[ERROR0009]Install failed.

Cause

Failed to install the product.

Action method

Refer to the message files *windowsFolder*\dtpsilent.log and *windowsFolder*\dtpcirresult.log, and take appropriate action. If action cannot be taken, contact Fujitsu technical support.

A.2 Silent Installation of DS

This section explains silent installation of DS.

A.2.1 Installation Parameter CSV File

Specify the installation parameters in a CSV file using the format specified in this section.

Character encodings

ASCII

Format

```
installInfo,softwareName,softwareName
installInfo,OS,osName
installInfo,Version,version
installInfo,Name,installerName
parameters,paramKey,paramValue
parameters,...,...
```

📒 Note

. . . .

- Do not change any installInfo parameter from the sample content.

- When specifying a file path in a parameters parameter, do not exceed 256 halfwidth characters, otherwise a parameter error will occur.

- Specify one or more parameters in the parameters parameter.

- If double quotation marks are used to enclose data, then all fields within the same record must be enclosed in double quotation marks.

- Do not specify spaces in the first column or in the second column.

- Spaces cannot be specified before or after fields enclosed in double quotation marks.

. . . .

📘 Information

. . . .

A sample installation parameter CSV file is stored in the following folder of the product media (DVD-ROM).

- Folder
  dvdRom:\citool\DS\sample\

  - If installing DS on a 32-bit version of the operating system:
    sample_install.csv

  - If installing DS on a 64-bit version of the operating system:
    sample32_install_x64.csv

. . . .

parameters parameter

The parameters are described below.

No.	Parameter	Parameter format		Description
1	Desktop Patrol installation directory	Key	InstallDir	Specify the installation directory for this product.
		Data type	String	Install this product in a folder that is not used for other programs.
		Default value	If installing DS on a 32-bit version of the operating system: C:\Program Files\Fujitsu \Systemwalker Desktop Patrol If installing DS on a 64-bit version of the operating system: C:\Program Files (x86)\Fujitsu \Systemwalker Desktop Patrol	Optional (if this parameter is omitted, the key must be omitted as well).
2	Product language	Key	Language	Specify the product language 'ja' (Japanese version) or 'en' (global version).
		Data type	String	

No.	Parameter	Parameter format		Description
		Default value	When OS (locale) is Japanese: ja When OS (locale) is besides Japanese: en	'ja' can be specified only Japanese OS environment. Example: en This value cannot be changed after installation. Optional (if this parameter is omitted, the key must be omitted as well).
3	Server name	Key	ServerName	Specify the section name where Systemwalker Desktop Patrol DS will be installed.
		Data type	String	
		Default value	DS	Specify up to 50 characters using halfwidth alphanumeric characters, and the following symbols: - @ . Example: Fujitsu Limited Optional (if this parameter is omitted, the key must be omitted as well).
4	Host name	Key	HostName	Specify the FQDN format, IP address or computer name of the PC where Systemwalker Desktop Patrol DS will be installed.
		Data type	String	
		Default value	(Host name or IP address retrieved automatically from the system)	Specify up to 50 characters, using alphanumeric characters, hyphens and periods. Example: ds.example.com Also, it is necessary to specify a name that can be resolved using the Systemwalker Desktop Patrol DS/CT that will be connected. This value cannot be changed after installation. When communicating in an IPv6 environment, refer to the notes below. Optional (if this parameter is omitted, the key must be omitted as well).
5	Software distribution directory	Key	SoftwareDir	Specify the software distribution directory using an absolute path of up to 128 halfwidth characters. The following symbols cannot be used: / * ? \ " < > | If changing the directory, specify a directory that has sufficient available space.
		Data type	String	
		Default value	(*dsInstallDir*\FJSVsbtrs\data\swc)	
				Also, if applying security patches automatically, specify a directory with sufficient available space on a drive other than the Windows installation drive. In order to prevent the occurrence of insufficient disk space due to software registration/distribution or automatic application of security patches, you should

No.	Parameter	Parameter format		Description
				specify an area other than the disk space where the operating system is installed for the software distribution directory.
				This value cannot be changed after installation.
				Optional (if this parameter is omitted, the key must be omitted as well).
6	Maximum size	Key	SoftwareDirMaxSize	Specify the maximum disk size (in MB) for the software distribution directory.
		Data type	number	Specify the maximum size using a number from 1 to 999999.
		Default value	(Same as when this value is omitted)	
				If omitted, the available space of the specified directory will be used.
				You can specify a value equal to or greater than the available space of the drive specified for the software distribution directory.
				Specify a value according to the environment design of the PC.
				Optional (if this parameter is omitted, the key must be omitted as well).
7	Proxy server name	Key	ProxyServer	Specify the proxy server name.
		Data type	String	Specify the FQDN or IP address using up to 64 halfwidth alphanumeric characters, hyphens (-) or periods (.).
		Default value	(Proxy server is not used)	
				Omit this parameter if a proxy server will not be used.
				When communicating in an IPv6 environment, refer to the notes below.
				Optional (if this parameter is omitted, the key must be omitted as well).
8	Proxy port number	Key	ProxyPort	Specify the proxy server port number.
		Data type	number	Specify a numeric value between 1 and 65535.
		Default value	8080	
				Optional (if this parameter is omitted, the key must be omitted as well).
9	Proxy user name	Key	ProxyUser	Specify a user name for the proxy sever using up to 256 halfwidth characters.
		Data type	String	
		Default value	Null	Optional (if this parameter is omitted, the key must be omitted as well).
10	Proxy password	Key	ProxyPasswd	Specify a password for the proxy sever using up to 256 halfwidth characters.
		Data type	String	
		Default value	Null	Optional (if this parameter is omitted, the key must be omitted as well).
11	Domain name that will not use a proxy server	Key	NoProxyDomains	Specify a domain name that will not use a proxy server. Multiple domain names must
		Data type	String	

No.	Parameter	Parameter format		Description
		Default value	Null	be separated by spaces. Specify the domain name using up to 2064 halfwidth characters.
				Specify the domain name using halfwidth alphanumeric characters, hyphens (-) or periods (.).
				Optional (if this parameter is omitted, the key must be omitted as well).
12	User ID	Key	UserID	Specify a user ID to be managed as Systemwalker Desktop Patrol CT.
		Data type	String	The user ID specified here will be displayed in the main menu and is used to identify the user.
		Default value	systemadmin	You can specify up to 20 halfwidth alphanumeric characters, and the following symbols: - @ . _ Alphabetic characters are case-sensitive.
				Optional (if this parameter is omitted, the key must be omitted as well).
13	PC name	Key	PCName	Specify a name to be managed as Systemwalker Desktop Patrol CT.
		Data type	String	You can specify up to 20 halfwidth alphanumeric characters. You cannot specify spaces and the following symbols: + * ? < > , ; : \ / "	
		Default value	(The first 20 characters of the host name (HostName key))	
				Optional (if this parameter is omitted, the key must be omitted as well).
14	Contents of user information 1	Key	UserInfo1	Specify this item when you have been instructed to do so by the system administrator.
		Data type	String	You can specify up to 256 characters. You can specify halfwidth alphanumeric characters, halfwidth spaces, and the following symbols: - @ . ( ) [ ] < > : ; /
		Default value	Null	
				Optional (if this parameter is omitted, the key must be omitted as well).
15	Contents of user information 2	Key	UserInfo2	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
16	Contents of user information 3	Key	UserInfo3	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
17	Contents of user information 4	Key	UserInfo4	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	

No.	Parameter	Parameter format		Description
18	Contents of user information 5	Key	UserInfo5	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
19	Contents of user information 6	Key	UserInfo6	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
20	Contents of user information 7	Key	UserInfo7	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
21	Contents of user information 8	Key	UserInfo8	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
22	Contents of user information 9	Key	UserInfo9	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	
23	Contents of user information 10	Key	UserInfo10	Refer to the explanation of "Contents of user information 1".
		Data type	String	
		Default value	Null	

🔔 Note

. . . .

Communication in IPv6 environments

IPv6 addresses cannot be specified. For communication in IPv6-only environments, register beforehand by using one of the following patterns, and then enter the host name:

- Register the CS and DS host name and the IP address in the DNS server.

- Register the CS and DS host name and the IP address in the communication source PC hosts file.

. . . .

A.2.2 Parameter Setup Command

If customizing parameters, create a response file in which the parameters were changed using the parameter setup command, and use this file for silent installation.

Command name

dvdRom:\citool\DS\dtpds_instparam.exe

Syntax

dtpds_instparam.exe -infile *installParmCsvFile* -outfile *responseFile*

Options

Option	Description
-infile	Specify the installation parameter CSV file. If the path includes spaces, enclose it in double quotation marks.
-outfile	Specify the output destination of the response file for silent installation. If a file already exists in the output destination, it will be overwritten. If the path includes spaces, enclose it in double quotation marks.

Output format

The return value is 0 if the command ends normally.

The return value is other than 0 if the command ends abnormally. If this happens, refer to the error message output to the console and take appropriate action.

Examples

The following command specifies the parameters in the installation parameter CSV file C:\dtp_ds.csv, and creates the response file C:\dtp_ds.iss for silent installation:

```
dtpds_instparam.exe -infile C:\dtp_ds.csv -outfile C:\dtp_ds.iss
```

A.2.3 Messages Output by the Parameter Setup Command

This section describes the messages output by the parameter setup command.

Command syntax errors

ERROR: Too few arguments.

Cause

An argument required for executing the command is missing.

Action

Check the syntax of the command.

ERROR: The syntax of the command is incorrect.

Cause

The syntax of the specified command is incorrect.

Action

Check the syntax of the command.

ERROR: Cannot find the file specified -infile.

Cause

The installation parameter CSV file specified in the -infile option does not exist.

Action

Check the path of the installation parameter CSV file.

Installation parameter CSV file format errors

These messages are output if the installation parameter CSV file format is invalid.

ERROR: CSV file error:code = 1, Invalid CSV error.

Cause

The CSV definition format is incorrect.

Action

The CSV data specified in the installation parameter CSV file does not match the format described in "A.2.1 Installation Parameter CSV File".

Ensure that there is no invalid CSV data in the file.

ERROR: CSV file error:code = 2, installInfo/Name is required.

Cause

The installInfo parameter Name is not specified.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 3, Invalid installInfo key.

Cause

The specified installInfo is incorrect.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 4, Duplicated installInfo key.

Cause

The same parameter definition has been defined in duplicate in installInfo.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 5, Invalid character length.

Cause

The specified string is too long.

Action

Ensure that the specified string is not too long.

ERROR: CSV file error:code = 6, Invalid character format or encoding.

Cause

The character encoding of the installation parameter CSV file is incorrect.

Action

Ensure that the character encoding of the installation parameter CSV file is correct.

ERROR: CSV file error:code = 8, Parameter is required.

Cause

A parameter value has not been specified.

Action

Check the parameter values.

Parameter check errors

These messages are output if a parameter value specified in the installation parameter CSV file is incorrect.

ERROR: Parameter error. Invalid Software ID.

Cause

The parameter setup command that was started does not correspond to the installer name specified in the installation parameter CSV file.

Action

Execute the parameter setup command corresponding to the installer name specified in the installation parameter CSV file.

ERROR: Parameter error. [%1]Maximum size is %2 characters.

Cause

A value of parameter %1 exceeds the maximum string length of %2 characters.

Action

Review the parameter values, and specify a value up to the maximum number of characters.

ERROR: Parameter error. [%1] Invalid character. Double-byte characters.

Cause

The %1 key contains fullwidth characters.

Action

Do not specify fullwidth characters.

ERROR: Parameter error. [%1] Invalid character. Half-width kana characters.

Cause

The %1 key contains halfwidth kana characters.

Action

Do not specify halfwidth kana characters.

ERROR: Parameter error. [%1] Invalid character.

Cause

The %1 key contains an invalid character (such as a control character).

Action

Check the character types that can be specified, and delete all characters that cannot be specified.

ERROR: Parameter error. [%1] Invalid character '%2'.

Cause

The %1 key contains the invalid character %2.

Action

Do not specify invalid characters.

ERROR: Parameter error. [%1] The path specified must be an absolute path.

Cause

An absolute path is not specified in the %1 key.

Action

Specify an absolute path.

ERROR: Parameter error. [%1]Valid range is from %2 to %3.

Cause

An out-of-range number is specified as the value in the %1 key.

Action

Specify a number from %2 to %3.

ERROR: Parameter error. [%1]Invalid format.

Cause

The format of the %1 key is incorrect. For example, a 0 precedes the number.

Action

Check the format. If a 0 precedes the number, remove it.

Other errors

ERROR: Load "%1" failed.

Cause

The required DLL %1 could not be loaded.

Action

Ensure that the provided csv_parse.dll resource exists in the citool\common folder.

ERROR: GetProcAddress %1 failed.

Cause

Failed to retrieve the function %1 in the DLL.

Action

Contact Fujitsu technical support.

ERROR: FreeLibrary "%1" failed.

Cause

Failed to retrieve FreeLibrary of DLL %1.

Action

Contact Fujitsu technical support.

ERROR: An unexpected exception occurred.

Cause

An unexpected error occurred.

Action

Contact Fujitsu technical support.

ERROR: Cannot create output file.

Cause

Failed to create the output file.

Action

Check the path of the output file specified for the -outfile option.

A.2.4 Silent Installation Command

The silent installation command performs silent installation of DS.

Command name

dvdRom:\citool\DS\silentsetup.exe

Syntax

silentsetup.exe [*responseFile*]

Options

Option	Description
Response file (optional)	Specify this option if you want to change the parameters to be used during setup from their default values. If omitted, the default values will be used for all parameters.
	Specify the file using its absolute path, and if the path includes spaces, enclose it in double quotation marks.
	The string must be up to 256 halfwidth characters (excluding the double quotation marks).

Privilege required/execution environment

- Administrator privileges are required.

- This command is to be executed by the system administrator.

- To use this command in Windows Server(R) 2008, right-click to display the menu and then select **Run as administrator** and execute this command on the **Command Prompt** window.

- To use this command in Windows Server(R) 2012, display the desktop and execute this command on a **Command Prompt** window that has been started by selecting **Run as Administrator**.

- Only new installations are supported.

- Refer to "2.4.1.2 Silent Installation " to check if the DS installer DSSetup.exe and server environment setup file ATOOL_policy_ds.zip are deployed.

Return values

0: Ended normally

3010: Ended normally (restart required)

Other: Ended abnormally

Output format

This command outputs messages to the console and to the event log.

Silent installation start and end messages are output to the console standard output. If the command ends abnormally, an error message is output.

Examples

Perform silent installation with the response file C:\dtp_ds.iss.

dvdRom:\citool\DS\silentsetup.exe C:\dtp_ds.iss

A.2.5 Messages Output by the Silent Installation Command

This section explains the messages output during installation.

Messages output to the console

Information messages

Systemwalker Desktop Patrol DS silent setup start.

Cause

Installation of Systemwalker Desktop Patrol DS started.

Action

Wait until the installation ends.

Install successful.

Cause

Systemwalker Desktop Patrol DS was installed successfully.

Action

Proceed to "2.4.2 Set DS Operation Environment".

Install successful. Reboot required.

Cause

Systemwalker Desktop Patrol DS was installed successfully. A restart is required.

Action

Restart the PC. After restarting, proceed to "2.4.2 Set DS Operation Environment".

Error messages

[ERROR0001]Administrator privileges are required.

Cause

Administrator privileges are required.

Action

Execute as a user with Administrator privileges.

[ERROR0002]Systemwalker Desktop Patrol already exists.

Cause

Systemwalker Desktop Patrol is already installed.

You cannot install Systemwalker Desktop Patrol in an environment where CS, DS or CT is installed.

Action

This command only supports new installations of DS.

[ERROR0003]"DSSetup.exe" not exists.

Cause

The DS installer (DSSetup.exe) was not found.

Action

Deploy the DS installer in accordance with "2.4.1.2 Silent Installation ".

[ERROR0004]"ATOOL_policy_ds.zip" not exists.

Cause

The server environment setup file ATOOL_policy_ds.zip was not found.

Action

Deploy the server environment setup file in accordance with "2.4.1.2 Silent Installation ".

[ERROR0005]"%1" not exists.

Cause

The specified response file %1 was not found.

Action

Ensure that the response file exists.

[ERROR0006]Install failed.

Cause

Failed to install the product. There is an abnormality in the environment.

Action

Ensure that there are no other installers running. Also, ensure that the system satisfies the requirements.

If the problem cannot be resolved, contact Fujitsu technical support.

[ERROR0007]Install failed.

Cause

Failed to install the product. Copying of files may have failed.

Action

Ensure that the deployed DS installer obtained from CS is the same as the file on CS.

If the problem cannot be resolved, contact Fujitsu technical support.

[ERROR0008]Install failed.

Cause

Failed to install the product. Installation of components may have failed.

Action

Refer to events for which the source is MsiInstaller in the event log (application), and take appropriate action.

If "Product: Systemwalker Desktop Patrol DS -- Error 27511. Installation failed. Check the cause of failure and execute installation again." is recorded in the event log under the above conditions, the likely cause is that the IP address or computer name used for the host name could not be retrieved from the system. Specify the host name in the parameter file (recommended), or review the setup to enable retrieval of the system IP address or computer name, and execute the silent installation command again.

If the problem cannot be resolved, contact Fujitsu technical support.

A.3 Silent Installation of SS

This section explains silent installation of SS.

A.3.1 Installation Parameter CSV File

Specify the installation parameters in a CSV file using the format specified in this section.

Character encodings

ASCII

Format

```
installInfo,softwareName,softwareName
installInfo,OS,osName
installInfo,Version,version
installInfo,Name,installerName
parameters,paramKey,paramValue
parameters,...,...
```

📑 **Note**

. . . .

- Do not change any installInfo parameter from the sample content.

- When specifying a file path in a parameters parameter, do not exceed 256 halfwidth characters, otherwise a parameter error will occur.

- Specify one or more parameters in the parameters parameter.

- If double quotation marks are used to enclose data, then all fields within the same record must be enclosed in double quotation marks.

- Do not specify spaces in the first column or in the second column.

- Spaces cannot be specified before or after fields enclosed in double quotation marks.

. . . .

📖 **Information**

. . . .

A sample installation parameter CSV file is stored in the following folder of the product media (DVD-ROM).

- Folder
  dvdRom:\citool\SS\sample\

  - If installing SS on a 32-bit version of the operating system:
    sample_install.csv

  - If installing SS on a 64-bit version of the operating system:
    sample32_install_x64.csv

. . . .

parameters parameter

The parameters are described below.

No.	Parameter	Parameter format		Description
1	Desktop Patrol installation directory	Key	InstallDir	Specify the installation directory for this product.
		Data type	String	Specify the path name using up to 100 characters. The folder name can contain alphanumeric characters, halfwidth spaces and the following symbols: - ( )
		Default value	If installing SS on a 32-bit version of the operating system: C:\Program Files\Fujitsu \Systemwalker Desktop Patrol\SS If installing SS on a 64-bit version of the operating system: C:\Program Files (x86)\Fujitsu \Systemwalker Desktop Patrol\SS	Install this product in a folder that is not used for other programs. Optional (if this parameter is omitted, the key must be omitted as well).

A.3.2 Parameter Setup Command

If customizing parameters, create a response file in which the parameters were changed using the parameter setup command, and use this file for silent installation.

Command name

dvdRom:\citool\SS\dtpss_instparam.exe

Syntax

```
dtpss_instparam.exe -infile installParmCsvFile -outfile responseFile
```

Options

Option	Description
-infile	Specify the installation parameter CSV file. If the path includes spaces, enclose it in double quotation marks.
-outfile	Specify the output destination of the response file for silent installation. If a file already exists in the output destination, it will be overwritten. If the path includes spaces, enclose it in double quotation marks.

Output format

The return value is 0 if the command ends normally.

The return value is other than 0 if the command ends abnormally. If this happens, refer to the error message output to the console and take appropriate action.

Examples

The following command specifies the parameters in the installation parameter CSV file C:\dtp_ss.csv, and creates the response file C:\dtp_ss.ini for silent installation:

```
dtpss_instparam.exe -infile C:\dtp_ss.csv -outfile C:\dtp_ss.ini
```

A.3.3 Messages Output by the Parameter Setup Command

This section describes the messages output by the parameter setup command.

Command syntax errors

ERROR: Too few arguments.

Cause

An argument required for executing the command is missing.

Action

Check the syntax of the command.

ERROR: The syntax of the command is incorrect.

Cause

The syntax of the specified command is incorrect.

Action

Check the syntax of the command.

ERROR: Cannot find the file specified -infile.

Cause

The installation parameter CSV file specified in the -infile option does not exist.

Action

Check the path of the installation parameter CSV file.

Installation parameter CSV file format errors

These messages are output if the installation parameter CSV file format is invalid.

ERROR: CSV file error:code = 1, Invalid CSV error.

Cause

The CSV definition format is incorrect.

Action

The CSV data specified in the installation parameter CSV file does not match the format described in "A.3.1 Installation Parameter CSV File".

Ensure that there is no invalid CSV data in the file.

ERROR: CSV file error:code = 2, installInfo/Name is required.

Cause

The installInfo parameter Name is not specified.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 3, Invalid installInfo key.

Cause

The specified installInfo is incorrect.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 4, Duplicated installInfo key.

Cause

The same parameter definition has been defined in duplicate in installInfo.

The installInfo parameters have been changed from the sample content.

Action

Change the installInfo parameters to the sample content and then reexecute.

ERROR: CSV file error:code = 5, Invalid character length.

Cause

The specified string is too long.

Action

Ensure that the specified string is not too long.

ERROR: CSV file error:code = 6, Invalid character format or encoding.

Cause

The character encoding of the installation parameter CSV file is incorrect.

Action

Ensure that the character encoding of the installation parameter CSV file is correct.

ERROR: CSV file error:code = 8, Parameter is required.

Cause

A parameter value has not been specified.

Action

Check the parameter values.

Parameter check errors

These messages are output if a parameter value specified in the installation parameter CSV file is incorrect.

ERROR: Parameter error. [%1]Maximum size is %2 characters.

Cause

A value of parameter %1 exceeds the maximum string length of %2 characters.

Action

Review the parameter values, and specify a value up to the maximum number of characters.

ERROR: Parameter error. [%1] The path specified must be an absolute path.

Cause

An absolute path is not specified in the %1 key.

Action

Specify an absolute path.

ERROR: Parameter error. [%1] Invalid character '%2'.

Cause

The %1 key contains the invalid character %2.

Action

Do not specify invalid characters.

ERROR: Parameter error. [%1] The path specified is invalid ("%2").

Cause

The %1 key contains the invalid path %2.

Action

Specify a different path to those used for other programs.

Other errors

ERROR: Load "%1" failed.

Cause

The required DLL %1 could not be loaded.

Action

Ensure that the provided csv_parse.dll resource exists in the citool\common folder.

ERROR: GetProcAddress %1 failed.

Cause

Failed to retrieve the function %1 in the DLL.

Action

Contact Fujitsu technical support.

ERROR: FreeLibrary "%1" failed.

Cause

Failed to retrieve FreeLibrary of DLL %1.

Action

Contact Fujitsu technical support.

ERROR: An unexpected exception occurred.

Cause

An unexpected error occurred.

Action

Contact Fujitsu technical support.

A.3.4 Silent Installation Command

The silent installation command performs silent installation of SS.

Command name

dvdRom:\citool\SS\silentsetup.bat

Syntax

silentsetup.bat [*responseFile*]

Options

Option	Description
Response file (optional)	Specify this option if you want to change the parameters to be used during setup from their default values. If omitted, the default values will be used for all parameters.
	Specify the file using its absolute path, and if the path includes spaces, enclose it in double quotation marks.
	The string must be up to 256 halfwidth characters (excluding double quotation marks).

Privilege required/execution environment

- Administrator privileges are required.

- This command is to be executed by the system administrator.

- To use this command in Windows Server(R) 2008, right-click to display the menu and then select **Run as administrator** and execute this command on the **Command Prompt** window.

- To use this command in Windows Server(R) 2012, display the desktop and execute this command on a **Command Prompt** window that has been started by selecting **Run as Administrator**.

- Only new installations are supported.

Return values

0: Ended normally

Other than 0: Ended abnormally

Output format

This command outputs messages to the console and to the message file.

Silent installation start and end messages are output to the standard output of the console. Also, when the command ends abnormally, an error message will be output.

After the command ends, check the setup result output to the message file.

The result is output to *ssInstallDir*\log\dtpsssilent.log if the command ends normally, or to *windowsFolder*\dtpsssilent.log if it ends abnormally.

Examples

Perform silent installation specifying the response file C:\dtp_ss.ini.

dvdRom:\citool\SS\silentsetup.bat C:\dtp_ss.ini

A.3.5 Messages Output by the Silent Installation Command

This section explains the messages output during installation.

Messages output to the console

Information messages

Systemwalker Desktop Patrol SS silent setup start.

Cause

Installation of Systemwalker Desktop Patrol SS started.

Action

Wait until the installation ends.

Install successful.

Cause

Systemwalker Desktop Patrol SS was installed successfully.

Action

Refer to the message file *ssInstallDir*\log\dtpsssilent.log and ensure that the installation ended normally. Proceed to "2.8.2 Configure the Operating Environment for SS".

Error messages

[ERROR0001]Administrator privileges are required.

Cause

Administrator privileges are required.

Action

Execute as a user with Administrator privileges.

[ERROR0002]Systemwalker Desktop Patrol SS already exists.

Cause

Systemwalker Desktop Patrol is already installed.

Action

This command only supports new installations.

[ERROR0004]Install Disc is corrupted. "setup.exe" not exists.

Cause

A file required for installation was not found.

Action

Ensure that the installation disk is not corrupted.

[ERROR0005]"%1" not exists.

Cause

The specified response file %1 was not found.

Action

Ensure that the response file exists.

[ERROR0006]Install failed.

Cause

Failed to install the product. An invalid parameter value may be specified.

Action

Refer to the message file *windowsFolder*\dtpsssilent.log and take appropriate action. If action cannot be taken, contact Fujitsu technical support.

[ERROR0007]Install failed.

Cause

Failed to install the product. Copying of files may have failed.

Action

Refer to the message file *windowsFolder*\dtpsssilent.log and take appropriate action. If action cannot be taken, contact Fujitsu technical support.

[ERROR0008]Install failed.

Cause

Failed to install the product.

Action method

Refer to the message files *windowsFolder*\dtpsssilent.log and *windowsFolder*\dtpsscirresult.log, and take appropriate action. If action cannot be taken, contact Fujitsu technical support.