RemoteConnect Support

Operating Instructions

Management Site Security Policy Guide

TABLE OF CONTENTS

5. Configuring E-mail Settings

6. Viewing the Login Log

1. Introduction

Overview

You can manage user IDs with stricter security by using the security policy setting function for user IDs and the login log function in OPTiM ID.

You can configure the number of login attempts and the password expiration for user IDs by using the security policy setting function. Notifications of login locks due to exceeding the maximum allowable number of login attempts and password expiration can be sent by configuring the manager's e-mail address in advance in the security policy settings.

You can view the login attempt results of user IDs by using the login log function. In addition to login logs for OPTiM ID, login logs for the operator tool are also displayed.

Functions

	Function name	Description
1	Log-in Lock	You can lock out user IDs that failed to log in after the specified number of attempts by configuring a login attempt limit in the security policy settings.
2	Password Expiration	You can restrict logins by user IDs with expired passwords by configuring password expiration in the security policy settings.
3	E-mail Sending	Notifications of login locks due to exceeding the maximum allowable number of login attempts and password expirations can be sent by configuring e-mail addresses in advance in the security policy settings.
4	Login Log	You can view the login logs of the operator tool and OPTiM ID at the Log screen of OPTiM ID.

How to Read This Manual

Symbols

This manual uses the following symbols:

Note

Indicates supplementary relevant information.

[ ]

Indicates the names of the keys that appear on the computer screen.

Disclaimer

To the maximum extent permitted by applicable laws, in no event will the manufacturer be liable for any damages whatsoever arising out of failures of this product, losses of documents or data, or the use or non-use of this product and operation manuals provided with it.

Make sure that you always copy or have backups of important documents or data. Documents or data might be erased due to your operational errors or malfunctions of the machine. Also, you are responsible for taking protective measures against computer viruses, worms, and other harmful software.

In no event will the manufacturer be responsible for any documents created by you using this product or any results from the data executed by you.

Notes

Some illustrations in this manual might be slightly different from the machine.

Contents of this manual are subject to change without prior notice.

Some functions explained in this manual do not work in this product.

Terminology

OPTiM ID

Means this service.

URL

The address of a website. Example: http://www.xxxx.co.jp

Application (app)

The services and software that can be used by OPTiM ID.

Browser

Software to view the Internet. (For example, Internet Explorer or Firefox.)

Log

Shows management site usage conditions and operation history in OPTiM ID.

Trademarks

Internet Explorer is a registered trademark of Microsoft Corp. in the United States and/or other countries.

Firefox® is a registered trademark of the Mozilla Foundation.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

2. Configuring the Security Policy

You can configure the security policy in OPTiM ID.

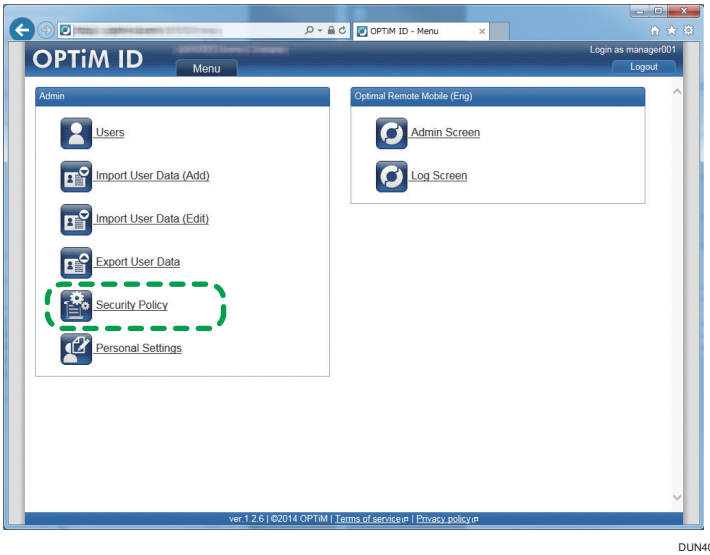
You can configure the maximum allowable number of login attempts and password expiration in the security policy.

You can send notifications of login locks and password expirations by configuring the manager's e-mail address.

Displaying the Security Policy

Displaying the [Security Policy] Screen

1. **Click [Security Policy] on the [Menu] screen.**



DUN401

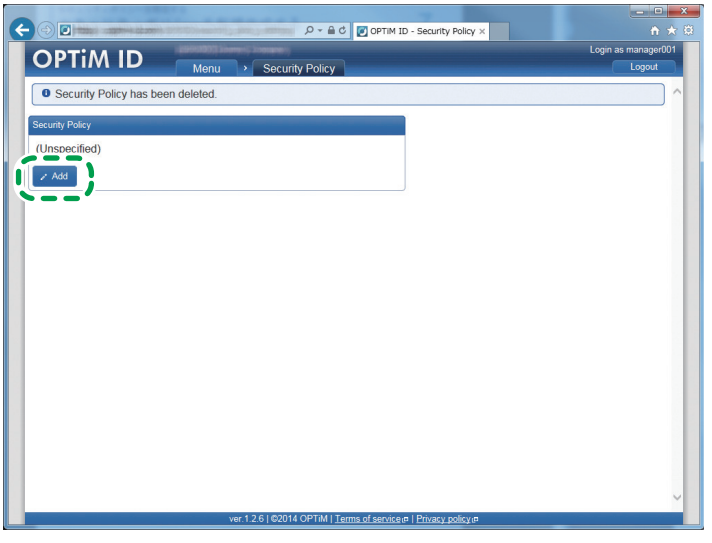
Note

- For the procedure to display the OPTiM ID menu screen, see Management Site Administrator's Guide.

2. **The [Security Policy] screen is displayed.**

Creating a New Security Policy

1. **Click [Add] on the [Security Policy] screen.**



DUN404

Note

- For the procedure to display the [Security Policy] screen, see page 9 "Displaying the [Security Policy] Screen".

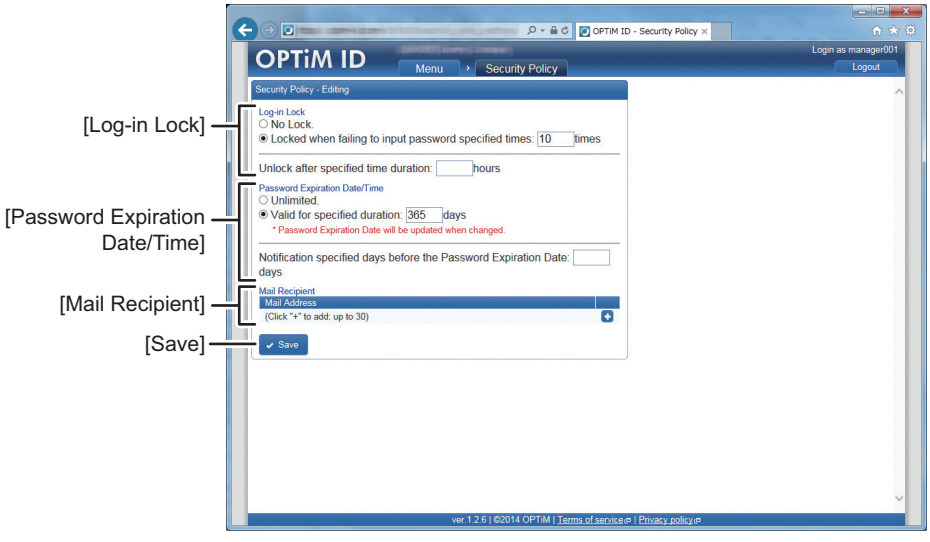
2. **Enter the necessary information, and then click [Save].**

Note

- For the entry items, see page 11 "Security Policy Setting Items".

3. **The security policy settings are registered.**

Security Policy Setting Items



DUN407

[Log-in Lock]

The login lock settings are displayed.

For details, see page 15 "Configuring the Login Lock".

[Password Expiration Date/Time]

The password expiration settings are displayed.

For details, see page 21 "Configuring Password Expiration".

[Save]

Click to save the security policy settings.

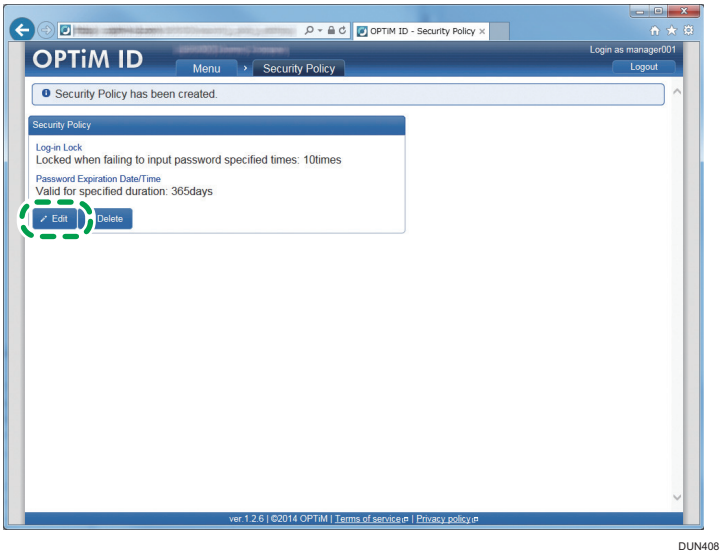
[Mail Recipient]

E-mail recipient settings are displayed.

For details, see page 31 "Configuring E-mail Settings".

Editing the Security Policy

1. **Click [Edit] on the [Security Policy] screen.**



DUN408

Note

- For the procedure to display the [Security Policy] screen, see page 9 "Displaying the [Security Policy] Screen".

2. **Enter the necessary information, and then click [Save].**

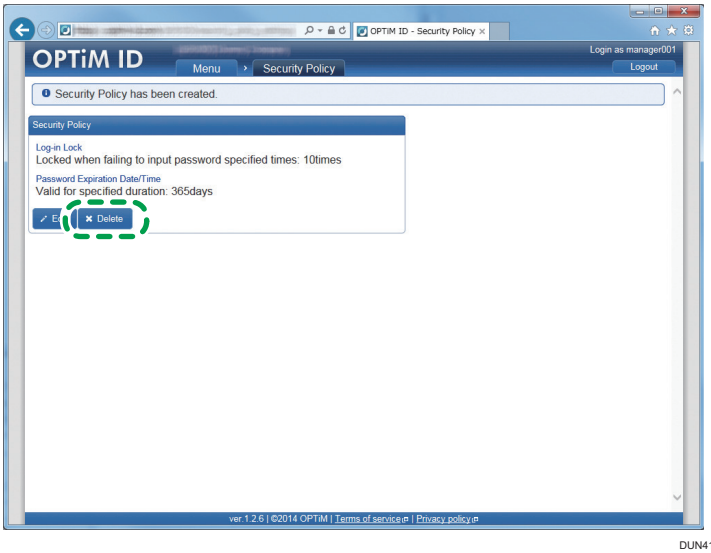
Note

- To discard changes, click [Cancel].
- For the entry items, see page 11 "Security Policy Setting Items".

3. **The security policy settings are changed.**

Deleting the Security Policy

1. **Click [Delete] on the [Security Policy] screen.**



DUN411

Note

- For the procedure to display the [Security Policy] screen, see page 9 "Displaying the [Security Policy] Screen".

2. **Click [OK].**
3. **The security policy settings are deleted.**

3. Configuring the Login Lock

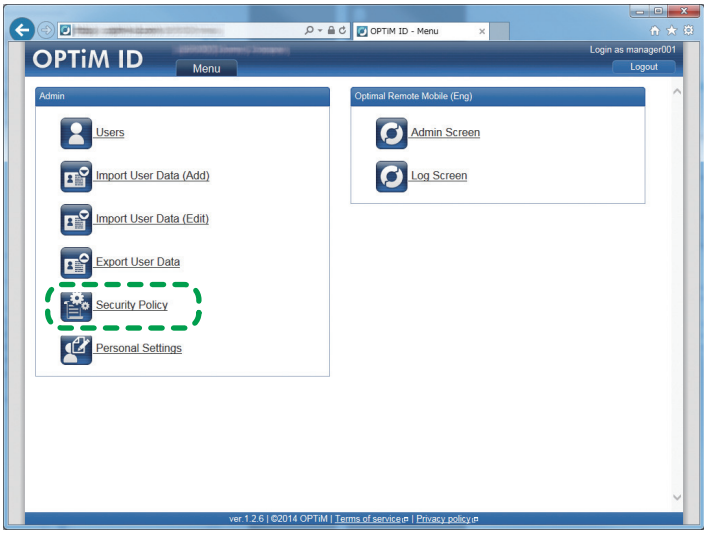
You can lock out user IDs that failed to log in after the specified number of attempts by configuring a login attempt limit in the security policy settings.

To clear the login lock, select either automatic clear after a specified time period or manual clear by the manager.

Displaying the Login Lock Settings

Displaying the Login Lock Settings Screen

1. **Click [Security Policy] on the [Menu] screen.**



DUN414

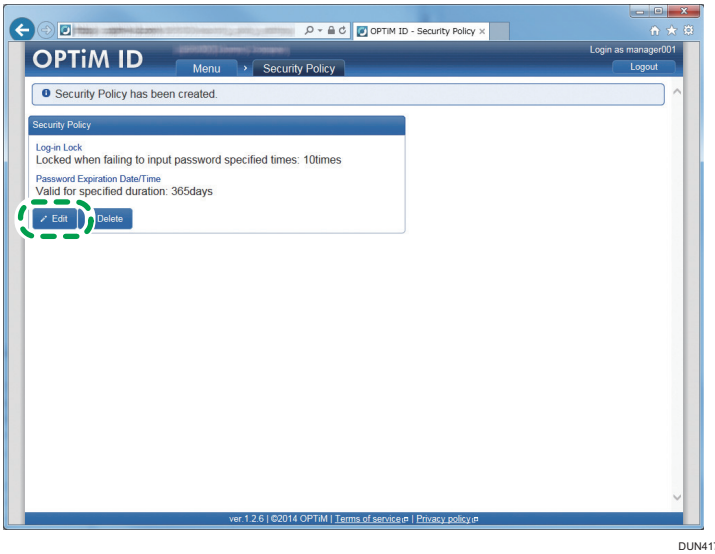
Note

- For the procedure to display the OPTiM ID menu screen, see the Management Site Administrator's Guide.

2. **The login lock settings are displayed on the [Security Policy] screen.**

Editing the Login Lock Settings

1. **Click [Edit] on the [Security Policy] screen.**



DUN417

Note

- For the procedure to display the [Security Policy] screen, see page 9 "Displaying the [Security Policy] Screen".

2. **Edit the necessary information, and then click [Save].**

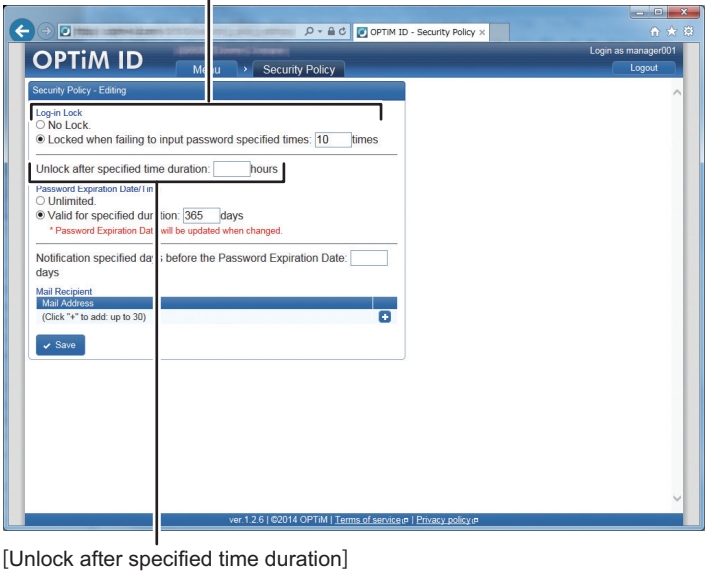
Note

- To discard changes, click [Cancel].
- For the entry items, see page 17 "Login Lock Settings Screen Items".

3. **The login lock settings are changed.**

Login Lock Settings Screen Items

Selection of [No Lock./Locked when failing to input password specified times]



[Unlock after specified time duration]

DUN420

Selection of [No Lock./Locked when failing to input password specified times]

To turn on the login lock, select [No Lock./Locked when failing to input password specified times], and then enter a number from 4 to 100 to specify the upper limit for login attempts.

To turn off the login lock, select [No Lock.].

[Unlock after specified time duration]

This section is displayed when the [No Lock./Locked when failing to input password specified times] is selected.

To clear the login lock automatically after a specified time period, enter a login lock time (hours).

Specify a login lock time (hours) by entering a number from 1 to 24.

If this field is left blank, the login lock time is not configured.

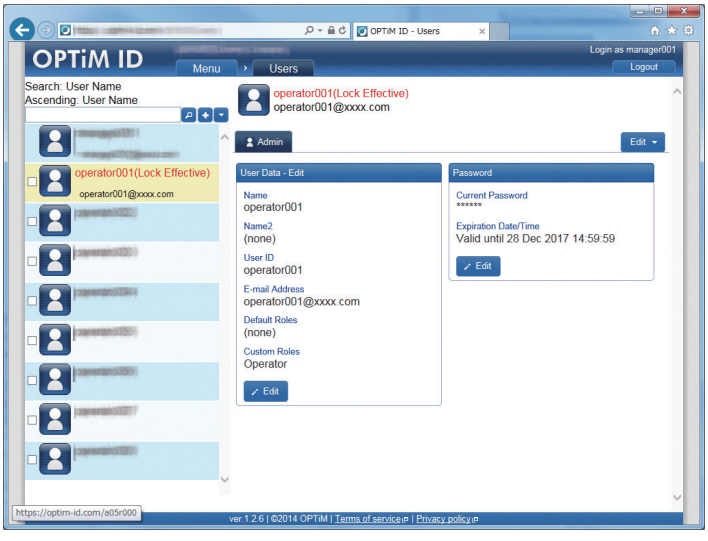
Screen during a Login Lock

Login Screen during a Login Lock

After the specified number of failed login attempts, the account is locked, and the user cannot log in to the operator tool or OPTiM ID.

User Screen during a Login Lock

When the user has been locked out, [(Locked)] is displayed beside the user ID.


OPTiM ID - Users
OPTiM ID
Menu
Users
Login as manager001
Logout
Search: User Name
Ascending: User Name
operator001(Lock Effective)
operator001@xxxx.com
Admin
Edit
User Data - Edit
Name
operator001
Name2
(none)
User ID
operator001
E-mail Address
operator001@xxxx.com
Default Roles
(none)
Custom Roles
Operator
Edit
Password
Current Password
******
Expiration Date/Time
Valid until 28 Dec 2017 14:59:59
Edit
https://optim-id.com/a05r000
ver.1.2.6 | ©2014 OPTiM | Terms of service | Privacy policy

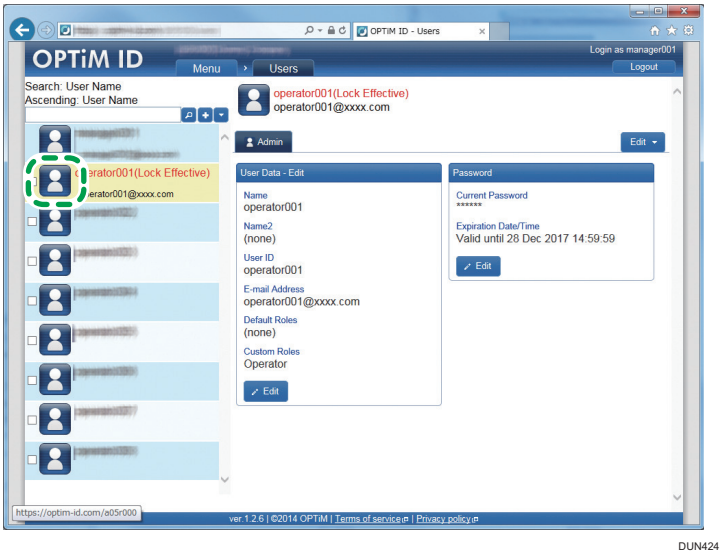
DUN423

Clearing the Login Lock

Clearing the Login Lock Manually

A manager can clear a login lock of the user manually.

1. **In the user list on the [Users] screen, click the icon of the user whose login lock you want to release.**



DUN424

Note

- For details about how to display the [Users] screen, see the Management Site Administrator's Guide.

2. **Click [Edit], and then click [Perform Unlock.] in the Operation menu that appears.**
3. **Click [OK].**
4. **The login lock is released.**

4. Configuring Password Expiration

You can restrict logins by user IDs with expired passwords by configuring password expiration in the security policy settings.

A function is provided to display a warning notification to encourage a password update when a user ID with a password that will expire soon tries to login to the operator tool or OPTiM ID. To use this function, configure the number of days of notice for the password expiration.

Displaying Password Expiration

Displaying the Password Expiration Settings Screen

1. **Click [Security Policy] on the [Menu] screen.**

DUN427

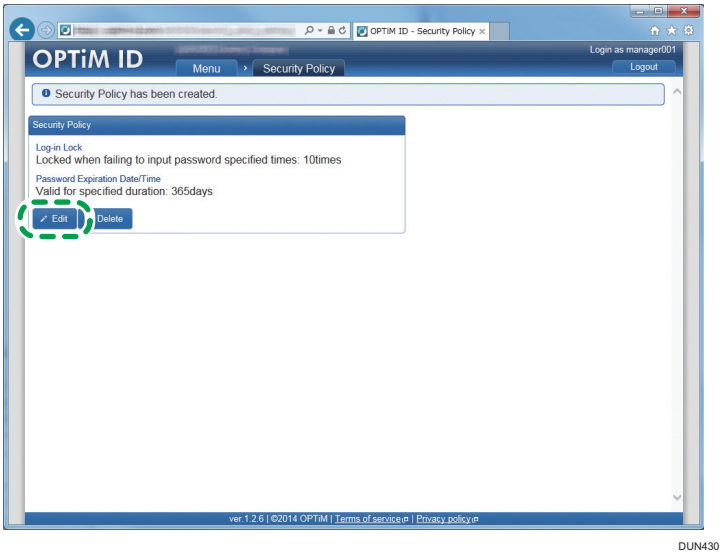
Note

- For the procedure to display the OPTiM ID menu screen, see the Management Site Administrator's Guide.

2. **The password expiration settings are displayed on the [Security Policy] screen.**

Editing the Password Expiration Settings

1. **Click [Edit] on the [Security Policy] screen.**



DUN430

Note

- For the procedure to display the [Security Policy] screen, see page 9 "Displaying the [Security Policy] Screen".

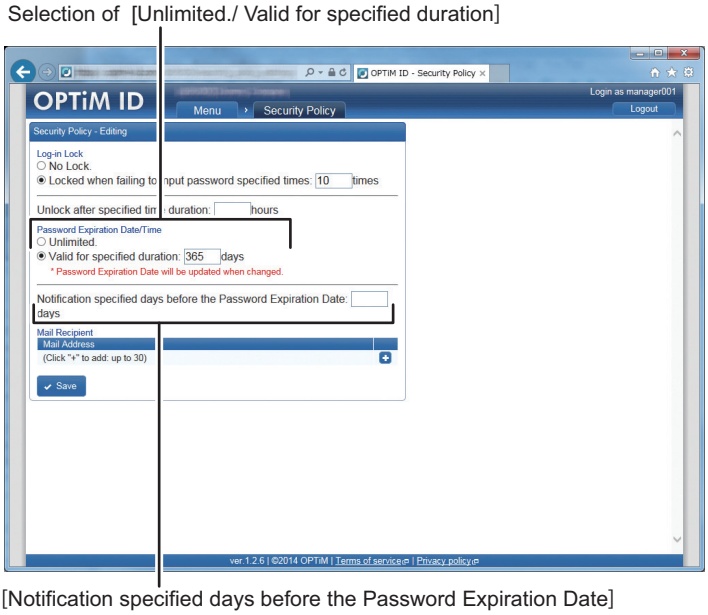
2. **Edit the necessary information, and then click [Save].**

Note

- To discard changes, click [Cancel].
- For the entry items, see page 23 "Password Expiration Settings Screen Items".

3. **The password expiration settings are changed.**

Password Expiration Settings Screen Items



DUN433

Selection of [Unlimited./ Valid for specified duration]

To enable password expiration, select [Valid for specified duration], and then specify the password validity period (days) by entering a number from 31 to 365.

To disable password expiration, select [Unlimited.].

Note

- If the password expiration settings are changed, password expiration for all users is updated.

[Notification specified days before the Password Expiration Date]

This section is displayed if [Valid for specified duration] is selected.

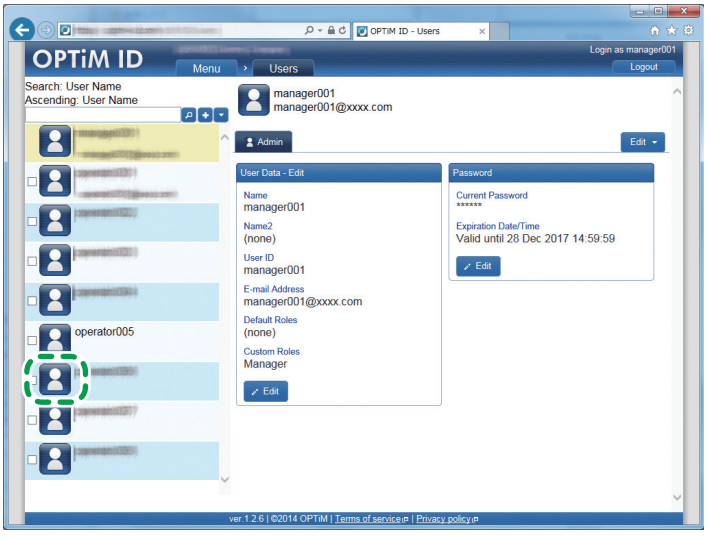
To notify a user before a password expires, enter the number of days to start the warning.

Specify the start date for the password expiration warning by entering a number from 10 to 30.

If this field is left blank, the user is not notified before the password expires.

Displaying the Password Expiration of a User

1. **In the user list on the [Users] screen, click the icon of the user you want to show its password expiration.**



DUN434

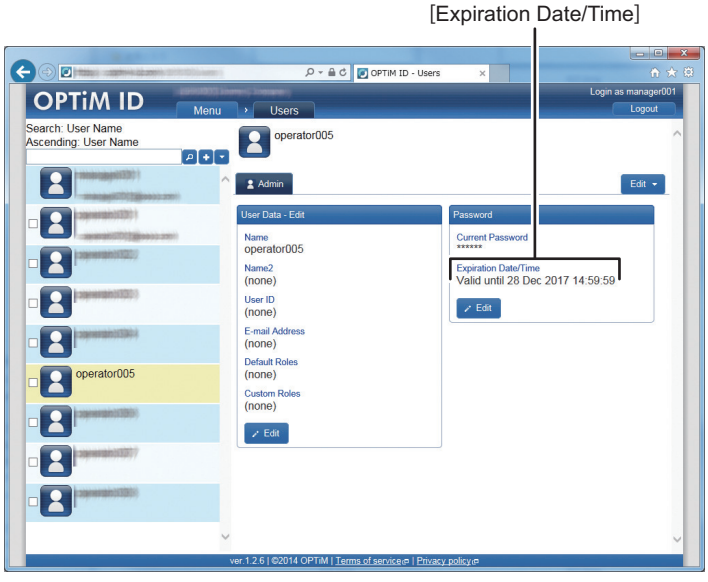
Note

- For details about how to display the [Users] screen, see the Management Site Administrator's Guide.

2. **The password expiration is displayed.**

How to Check the Password Expiration of a User

In the user list, click the user to be checked.



DUN436

[Expiration Date/Time]

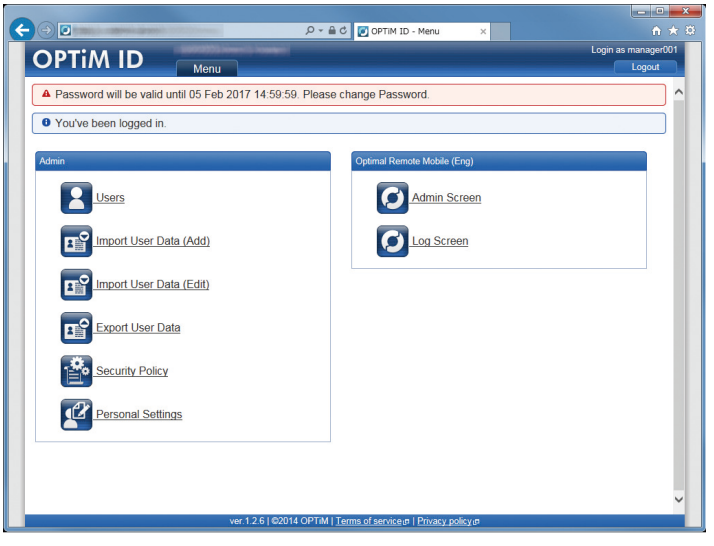
This section is displayed if password expiration is enabled.

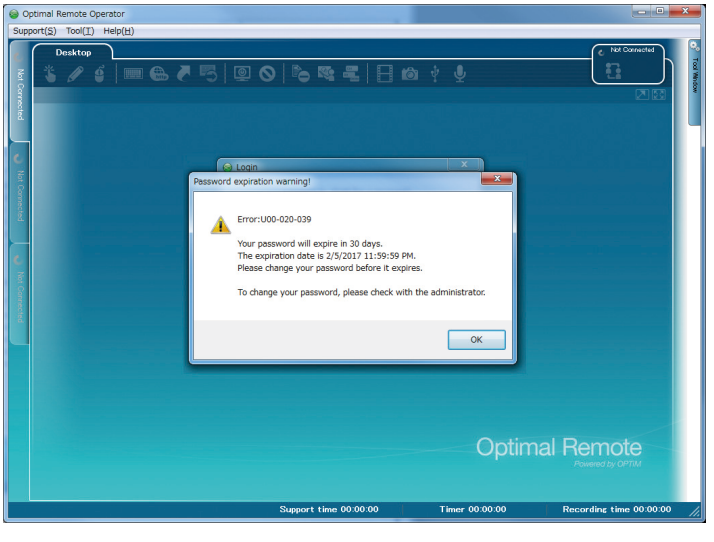
This section is displayed in red characters during the warning notification period for password expiration.

Password Expiration Warning Notification Screen

Login Password Expiration Warning Screen

A warning notification is displayed when the user logs in to the operator tool or OPIiM ID for the specified number of days before password expiration.





Screen When a Password Has Expired

Login Screen of Password Expiration Warning

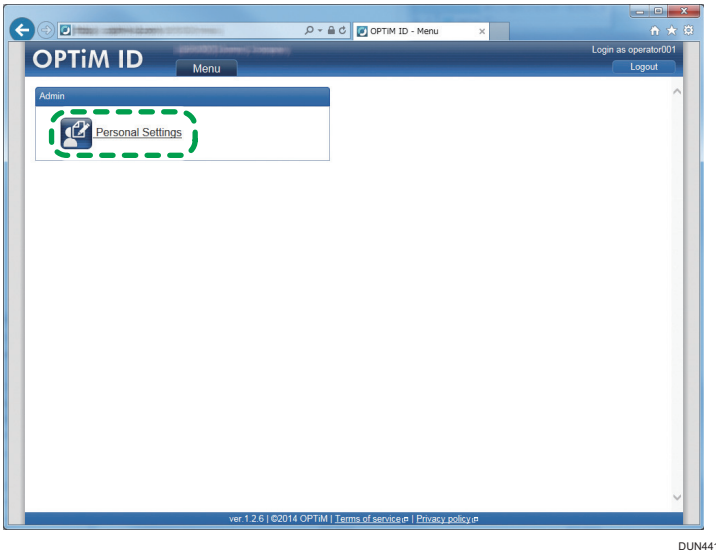
When a password has expired, the expiration message is displayed in the login screen of the operator tool or OPTiM ID, and it is not possible to log in to the operator tool or OPTiM ID.

Changing the Login Password

Changing from the Personal Settings of OPTiM ID

Change your password during the password validity period. You can change the password from the Personal Settings of OPTiM ID.

1. **Click [Personal Settings] on the [Menu] screen.**



DUN441

2. **Under [Password], click [Edit].**
3. **Enter the new password, and then click [Save].**

Note

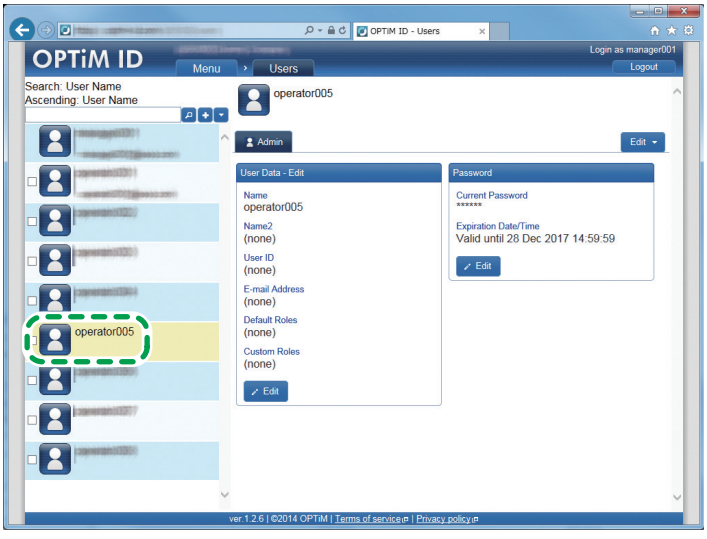
- To discard changes, click [Cancel].

4. **The password is changed.**

Changing from the [Users] Screen of OPTiM ID

If a user did not change the password during the password validity period, a manager must configure the password of the user again. It can be changed from the [Users] screen of OPTiM ID.

1. **In the user list on the [Users] screen, click the icon of the user whose password you want to change.**



DUN450

Note

- For details about how to display the [Users] screen, see the Management Site Administrator's Guide.

2. **Under [Password], click [Edit].**
3. **Enter a password, and then click [Save].**
4. **The password is changed.**

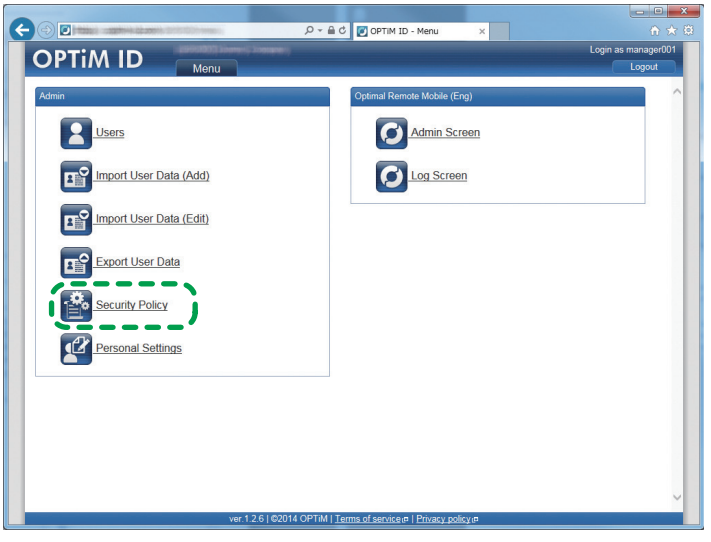
5. Configuring E-mail Settings

Notifications of login locks due to exceeding the maximum allowable number of login attempts and password expirations can be sent by configuring e-mail addresses in advance in the security policy settings.

Displaying the E-mail Sending Settings

Displaying the E-mail Sending Settings Screen

1. **Click [Security Policy] on the [Menu] screen.**



DUN453

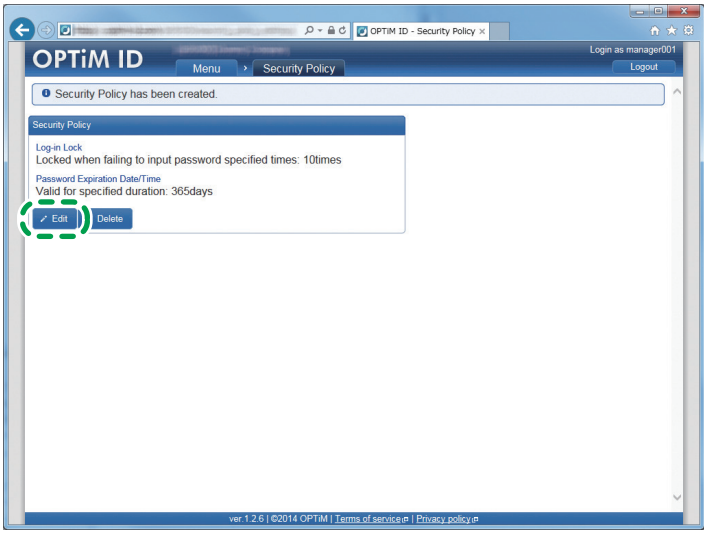
Note

- For the procedure to display the OPTiM ID menu screen, see the Management Site Administrator's Guide.

2. **The e-mail sending settings are displayed on the [Security Policy] screen.**

Editing E-mail Sending Settings

1. **Click [Edit] on the [Security Policy] screen.**



DUN456

Note

- For the procedure to display the [Security Policy] screen, see page 9 "Displaying the [Security Policy] Screen".

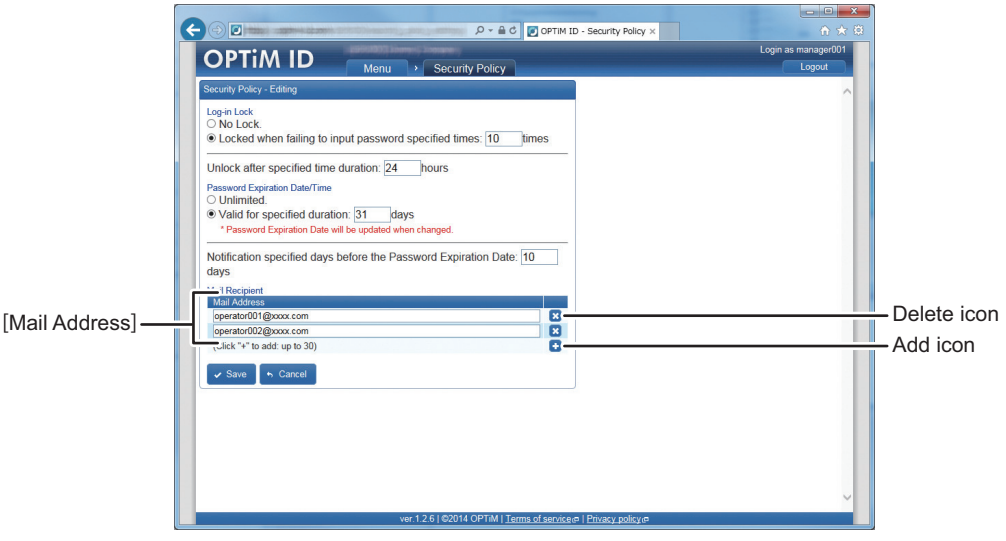
2. **Edit the necessary information, and then click [Save].**

Note

- To discard changes, click [Cancel].
- For the entry items, see page 33 "E-mail Sending Settings Screen Items".

3. **The e-mail sending settings are changed.**

E-mail Sending Settings Screen Items



DUN459

[Mail Address]

Enter an e-mail address of 255 characters or less using alphanumeric characters and symbols.

Add icon

Click to add an entry field to the e-mail address list. You can add up to 30 addresses

Delete icon

Click to remove the entry field.

6. Viewing the Login Log

You can view the login logs of the operator tool and OPTiM ID on the Log screen of OPTiM ID.

Displaying the Login Log

Displaying the [Log] Screen

1. **Click [Log] on the [Menu] screen.**
2. **The [Log] screen is displayed.**

Description of the [Log] Screen

Search function

You can use the search function to specify the log data to be displayed.

Enter the time data and search keyword, and then click (Search) icon.

If you enter the time data only, all logs from the specified period are displayed.

If you enter a search keyword only, all logs including the keyword are displayed.

[Time data]: You can enter time data (date and time) manually (example: 2011/05/16 01:00), and you can also specify the time by clicking the entry field and selecting from the calendar that appears. For details, see page 35 "Using the Calendar Screen".

[Search]: Enter the search keyword.

Log

Displays the login and operation logs of the management site.

Using the Calendar Screen

If you click the time data entry field of the search function, a calendar is displayed.

The specified date and time are displayed in the time data entry field.

1. **Clicking this icon displays the calendar of the previous month.**
2. **Clicking this icon displays the calendar of the next month.**
3. **Click a day to specify the date.**

   The current date and selected date are displayed in light blue and dark blue, respectively. (When the current date is selected, it is not displayed in dark blue.)
4. **The specified time is displayed.**

5. **You can specify the time by moving the sliders. The time moves in increments of 10 minutes.**
6. **Clicking [Close] closes the calendar screen.**
7. **Clicking [Current] specifies the current date and time.**

Types of Login Logs

The login log displays 6 types of logs according to the login route, login result, and reason for a login failure.

	Details of login log	Description
1	User [name] logged in. (Global IP address)	Log of a login by a user ID in OPTiM ID
2	User [name] failed to log in. (Global IP address)	Log of a failed login attempt by a user ID in OPTiM ID
3	User ID [user ID] failed to log in. (Global IP address)	Log of a failed login attempt by a user ID not in OPTiM ID
4	User [name] logged in from "(App)*1". (Global IP address)	Log of a login from the operator tool by a user ID in OPTiM ID
5	User [name] failed to log in from "(App)*1". (Global IP address)	Log of a failed login attempt from the operator tool by a user ID in OPTiM ID
6	User ID [user ID] failed to log in from "(App)*1". (Global IP address)	Log of a failed login attempt from the operator tool by a user ID not in OPTiM ID

*1 The fully qualified domain name (FQDN) and other information of the server used to log in is displayed at the position of App.

Logs other than the login log are also displayed on the log screen.

	Functions	Instances reported in the output log
1	User	Creation, editing, and deletion of accounts
2	Role	Creation, editing, and deletion of roles
3	Security Policy	Creation, editing, and deletion of security policies

Note

- The details of editing are not saved in the log.