

# **ID Federation Release Notes**

## **3.3.0.1**

This, "ID Federation Release Notes" contains the information about the latest release function of ID Federation and impact on our customers.

### **1. Overview**

We provide the following functions for convenience for users and administrators of ID Federation .

### **2. Contents provided**

#### **( 1 ) Added Support Browser**

Microsoft Edge is added to the support browser.

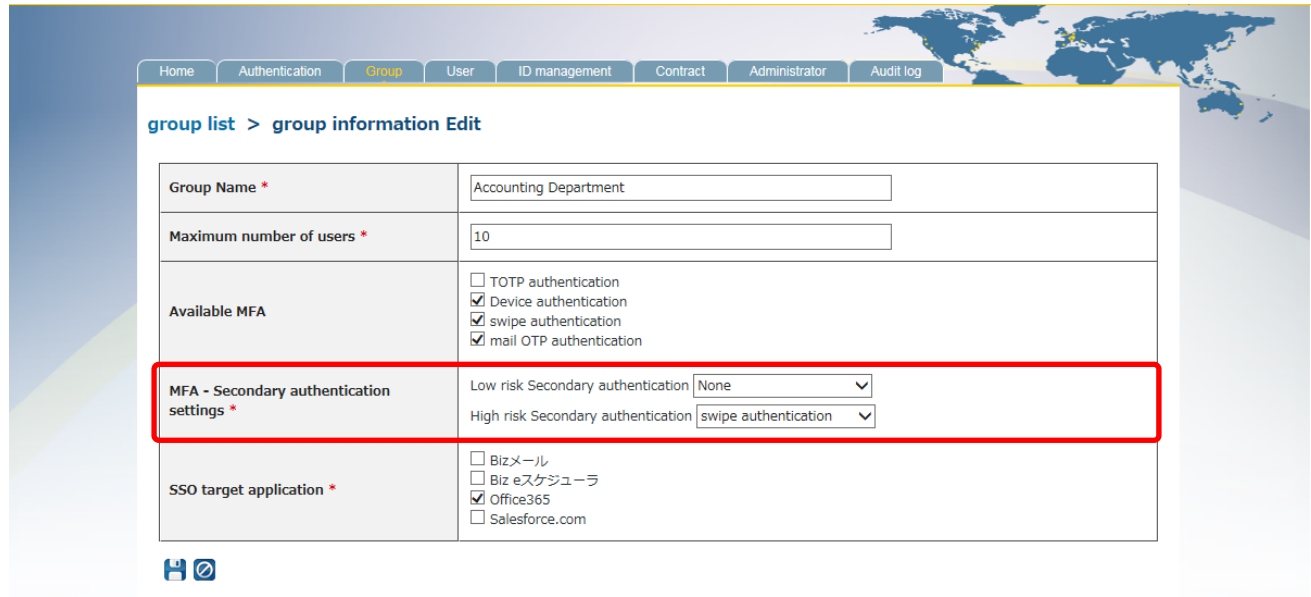
\*Since the multifactor authentication option [machine authentication] uses Active X,  
Microsoft Edge is excluded from the support browser.

## ( 2 ) Added group unit multi-factor authentication (secondary authentication) setting function

It is possible to set the presence or absence of multi-factor authentication (secondary authentication) and the authentication method for each group.

\*In the current version, the setting of the multi-factor authentication (secondary authentication) is applied to the group in common.

[Multi-factor authentication (secondary authentication) setting screen of the group]



The screenshot displays the 'group information Edit' screen in a web application. The navigation bar at the top includes links for Home, Authentication, Group (highlighted), User, ID management, Contract, Administrator, and Audit log. The breadcrumb trail shows 'group list > group information Edit'. The form contains several fields:

Group Name *	Accounting Department
Maximum number of users *	10
Available MFA	<input type="checkbox"/> TOTP authentication <input checked="" type="checkbox"/> Device authentication <input checked="" type="checkbox"/> swipe authentication <input checked="" type="checkbox"/> mail OTP authentication
MFA - Secondary authentication settings *	Low risk Secondary authentication: None High risk Secondary authentication: swipe authentication
SSO target application *	<input type="checkbox"/> Bizメール <input type="checkbox"/> Biz eスケジュール <input checked="" type="checkbox"/> Office365 <input type="checkbox"/> Salesforce.com

At the bottom left of the form, there are icons for saving and refreshing the page.

### (3) Added unpairing function of swipe authentication

A corporate administrator can unpair from the screen of the ID portal.

\*In the current version, the ID Federation help desk was unpairing after receiving a request from the customer.

[Swipe authentication unpairing screen]

User ID *	<input type="text" value="User01"/>	
user name	<input type="text" value="山田"/>	<input type="text" value="一郎"/>
contact email address *	<input type="text" value="example01@abc.com"/>	
device authentication default e-mail address	<input type="text" value="device authentication default e-mail address"/>	
mail OTP contact email address	<input type="text" value="mail OTP contact email address"/>	
mail message language	<div><div><div></div></div><div></div></div> "Language" in the contract information will apply to the mail messages.:Japanese	
group	<div><div>Sales Department</div><div></div></div>	
status *	<div><div>Available</div><div></div></div>	
SSO password *	<div><div><input type="checkbox"/> User needs to change password at next login.</div><div><input type="checkbox"/> Change the current password.</div><div><input type="checkbox"/> Reset the password.</div></div>	
multi-factor authentication	<div><div><input type="checkbox"/> Reset the device authentication settings.</div><div><input type="checkbox"/> Reset TOTP authentication settings.</div><div><input checked="" type="checkbox"/> Unpair terminal for Swipe authentication</div></div>	
Company	<input type="text"/>	Copyright (c) 2017 NTT Comm

## ( 4 ) Added operation items by user CSV collective registration and account Sync (SCIM-API)

With CSV collective registration and account Sync (SCIM - API), the following items can be referred, registered and updated.

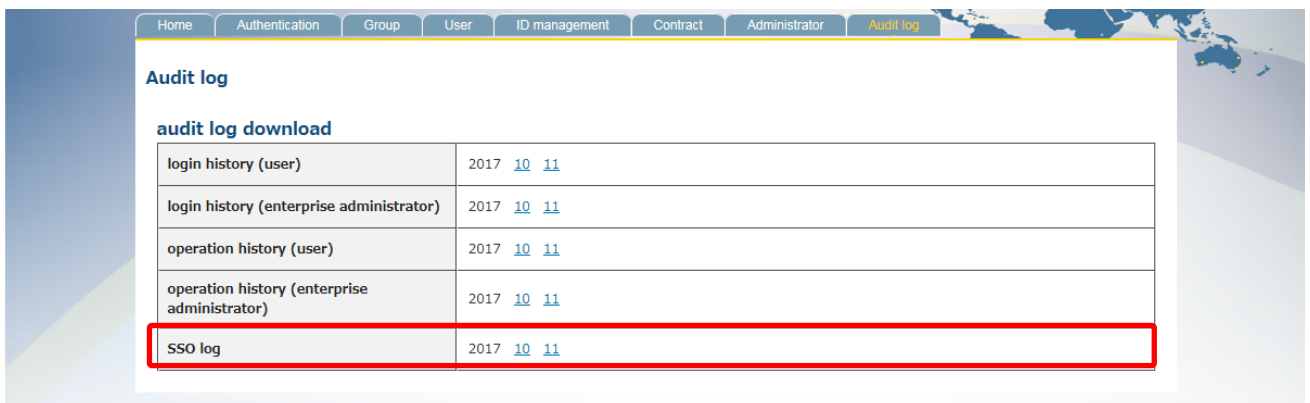
- User status
- Initial password change flag
- Machine authentication reset flag
- TOTP reset flag
- Number of contract IDs

\*Only the account Sync (SCIM - API) corresponds to the contract ID number

## ( 5 ) Added audit log file

The user's SSO (single sign-on) history was added to the output file of the audit log.

[Audit log download screen]



The screenshot shows a web interface with a navigation bar at the top containing links: Home, Authentication, Group, User, ID management, Contract, Administrator, and Audit log (which is highlighted). Below the navigation bar, the page title is "Audit log". Underneath, there is a section titled "audit log download" containing a table. The table has two columns: the first column lists log types, and the second column shows the year "2017" followed by two blue hyperlinks labeled "10" and "11". The last row of the table, "SSO log", is highlighted with a red border.

audit log download	
login history (user)	2017 <a href="#">10</a> <a href="#">11</a>
login history (enterprise administrator)	2017 <a href="#">10</a> <a href="#">11</a>
operation history (user)	2017 <a href="#">10</a> <a href="#">11</a>
operation history (enterprise administrator)	2017 <a href="#">10</a> <a href="#">11</a>
SSO log	2017 <a href="#">10</a> <a href="#">11</a>

## **(6) Changed user status**

After the administrator changes the status of the user from "lockout" to "available", if the user does not login within the day of the change date, the function to automatically return to "lockout" is removed.

## **3. Schedule**

This function will be applied after maintenance work.

- Maintenance period

Start time : 2018-1-21 22:00 JST

Estimated End time : 2018-1-22 06:00 JST