NEC

Internet Services Help

Settings and Operation

GM2173E9-1
NEC Corporation

Table of Contents

1 Feature Settings using Internet Services

1.1 Configuring Wi-Fi Connection Settings using IEEE802.1X Authentication Method

Connecting to the High Security Network

The Wi-Fi connection feature on the device supports IEEE802.1X authentication. To use IEEE802.1X authentication method, which requires a certificate, get the necessary certificate issued by the certificate authority and import it to the device from Internet Services.

Note

In order to import certificates via Internet Services, the settings for encrypting HTTP communications must be configured. For more information on Internet Services operation and how to set encryption for HTTP communication, refer to "Configuration of HTTP Communications Encryption" (p. 6).

1. **Log in to Internet Services as system administrator.**
2. **Import a certificate.**
   1) **Click [System] > [Security] > [Certificate Settings].**
   2) **Click [Import].**
   3) **Click [Browse] to specify the name of the file to import.**
   4) **Enter the password of the certificate for [Password].**
   5) **Enter the password again for [Retype Password].**
   6) **Click [Start].**
   7) **Refresh the web browser.**
3. **Configure Wi-Fi connection and security settings.**

   Note

   The procedure varies depending on the selected certificate method.

   1) **Click [Network] > [Wi-Fi].**
   2) **Enable [Enable].**
   3) **Enter the SSID in [SSID].**
   4) **Select [WPA2 Enterprise] in [Encryption].**
   5) **Select [Authentication Method].**
   6) **Enter the EAP-Identity value in [Identity].**
   When EAP-TLS is selected for the authentication method, proceed to step 11.

Note

Ask your RADIUS server administrator for the EAP-Identity.

7) **For PEAPv0 MS-CHAPv2, EAP-TTLS/PAP, EAP-TTLS/CHAP, or EAP-TTLS/MS-CHAPv2, enter the login user name and password for WPA-Enterprise authentication in [User Name] and [Password].**

8) **Retype the password in the [Retype Password] field for confirmation.**

9) **Select the imported CA certificate in [Root Certificate].**

10) **When EAP-TLS is selected, select the imported client certificate in [Client Certificate].**

11) **Click [Save].**

12) **Click [Restart Now].**

The device is rebooted and the settings are applied.

1.2 Encryption Settings

Configuration of HTTP Communications Encryption

Step1 Certificate Arrangement

Prepare for the certificate used for encrypting the HTTP communication. To set up a certificate using Internet Services, you can have the device create a self-signed certificate for the SSL server or can import any registered certificate (issued by another CA) to the device.

Note

You cannot import a certificate that already has been registered either as [Device Certificate] or [Other Certificates]. Delete the registered certificate beforehand.

How to create the self-signed certificate (for SSL server)

1. **Log in to Internet Services as system administrator.**
2. **Click [System].**
3. **Click [Security] > [Certificate Settings].**
4. **Click [Create] > [Generate Self-Signed Certificate].**
5. **Set each item as necessary.**
6. **Click [Start].**
7. **Click [Close] after the certificate has been generated.**

How to import the certificate issued by another CA

Before importing the certificate issued by another CA, create the self-signed certificate and make the settings so that HTTP communication is encrypted.

1. **Log in to Internet Services as system administrator.**
2. **Click [System].**
3. **Click [Security] > [Certificate Settings] > [Import].**
4. **Click [Browse] and select the file to import on the displayed dialog box, then click [Open].**

   Note

   You can also directly enter the path of the file to import.
5. **Enter the password of the certificate to [Password].**
6. **Enter the same password as the previous step to [Retype Password].**
7. **Click [Start].**
8. **Click [Close] after the import has finished.**

Step2 Certificate Settings

Register the certificate for the server with the device.

Note

Until making the setting of this section, a self-generated certificate is automatically set as the server certificate.

1. **Log in to Internet Services as system administrator.**
2. **Click [System].**
3. **Click [Security] > [SSL/TLS Settings].**
4. **Select a certificate at [Device Certificate - Server].**

   Important

   If no certificate is selectable, confirm that the device certificate is registered with [System] > [Security] > [Certificate Settings].

5. **Set [HTTP - SSL/TLS Communication Port Number] as necessary.**

   Important

   Do not set the same port number as other ports.

6. **Click [Save].**
7. **Click [Restart Now] after the touch screen instructs to restart the device.**

Configuration of Encryption Using IPsec

When setting [Digital Signature] for [IKE Authentication Method] to make IPsec communication, register a certificate with the device. No certificate is registered with the device by factory default. Import an IPsec certificate. After importing a certificate, configure IPsec.

When the IKE authentication method is set to [Preshared Key], skip the step 1 "Certificate Arrangement" and go to step 2 "Configuration of IPsec".

Important

You cannot import a certificate that already has been registered either as [Device Certificates] or [Other Certificates]. Delete the registered certificate beforehand.

Note

If a certificate to be imported as an IPsec certificate contains V3 extension "KeyUsage", "digitalSignature" bit must be asserted.

Step1 Certificate Arrangement

To configure a certificate using Internet Services, configure the encryption settings for HTTP communications, and then import a certificate issued by another CA to use it for the IPsec certificate.

Note

- The public key of the certificate that can be imported to the device shall be either of RSA® public key (up to 4096 bits) and ECC public key P-256/P-384/P-521.
- You cannot use a self-signed certificate created with Internet Services for IPsec.

See

For details on how to configure the encryption settings for HTTP communication, refer to "Configuration of HTTP Communications Encryption" (p. 6).

1. **Log in to Internet Services as system administrator.**
2. **Click [System].**
3. **Click [Security] > [Certificate Settings] > [Import].**
4. **Click [Browse] and select the file to import on the displayed dialog box, then click [Open].**

   Note

   You can also directly enter the path of the file to import.

5. **Enter the password of the certificate to [Password].**
6. **Enter the same password as the previous step to [Retype Password].**
7. **Click [Start].**
8. **Click [Close] after the import has finished.**

Step2 Configuration of IPsec

1. **Click [Network] > [Protocols] > [IPsec].**
2. **Enable the [Enable].**
3. **Click [IKE Authentication Method] to set the IKE authentication method.**

   ### For Digital Signature Method

   1) **Select [Digital Signature].**
   2) **Click [Device Certificate].**
   3) **Select the certificate to use for authentication, then click [Save].**

   ### For Preshared Key Method

   1) **Select [Preshared Key].**
   2) **Enter the text string to become the preshared key, then click [Save].**

4. **Configure other settings as required.**

Step3 Communication Destination Device Settings

This section explains the settings of the party being communicated with.

The necessary settings are as follows:

- Create an IP security policy
- Assign the IP security policy

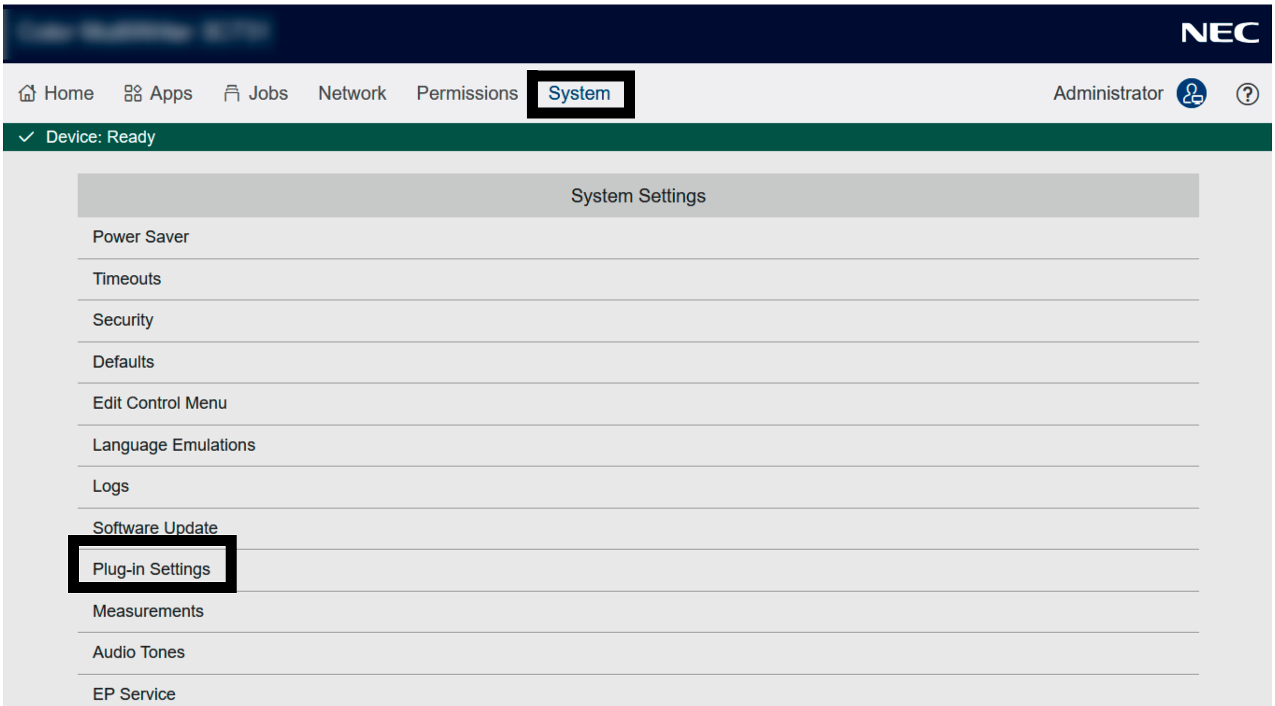
See

For information on how to set above settings, refer to the help of the communication destination device.

1.3 Other Settings

Configuration of IC Card Reader

1. **Log in to Internet Services as system administrator.**
2. **Click [System] > [Plug-in Settings].**



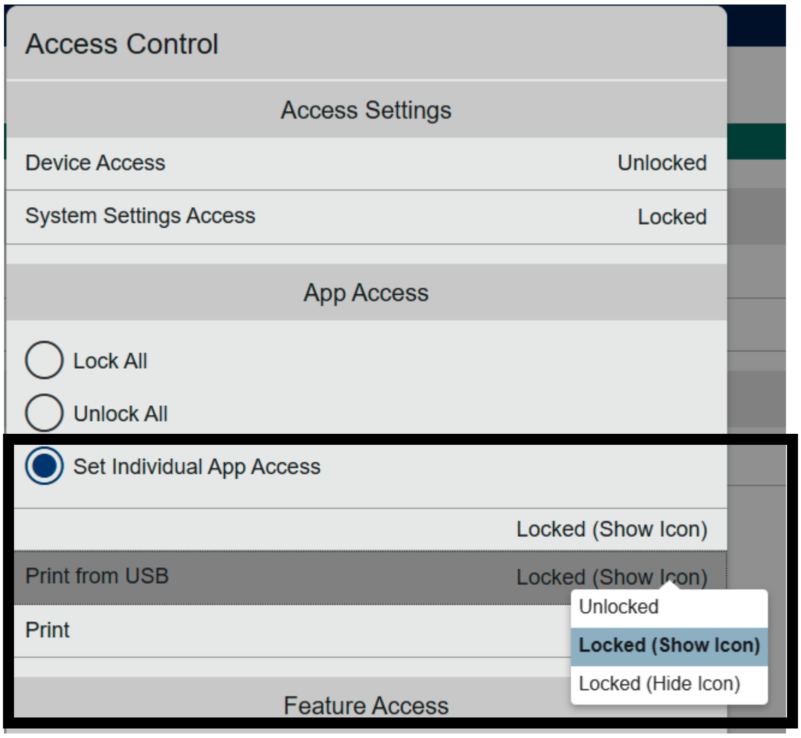
3. **Click ⋮ of optional connected IC card reader from [Embedded Plug-ins], and then select [View].**
4. **Place a check mark for the using IC card and click ✎.**
5. **Enter the required information and click [Apply].**

Access Control

The following shows the procedure to restrict access by apps.

1. **Log in to Internet Services as system administrator.**
2. **Click [Permissions] > [Permissions] > [Access Control].**

3. **Select [Set Individual App Access] under [App Access] and set the restricted operation of app.**



Access Control

Access Settings

Device Access Unlocked

System Settings Access Locked

App Access

○ Lock All

○ Unlock All

● Set Individual App Access

Locked (Show Icon)

Print from USB Locked (Show Icon)

Print

Feature Access

- Unlocked

  The service operation is not restricted.

- Locked (Show Icon)

  On the device home screen, the service is displayed with a lock icon. Authentication is required to use this service.

- Locked (Hide Icon)

  On the device home screen, the service is not displayed. Authentication is required to use this service.

4. **Click [Save].**

1.4 Exchange Online/Outlook.com SMTP/ POP3 Server Settings

Use Internet Services to set up the SMTP/POP3 server of Exchange Online/Outlook.com that uses OAuth 2.0 authentication.

Important

- Only one SMTP/POP3 server each can be set. The latest setting will become valid.
- If you have set up the SMTP/POP3 server of Exchange Online/Outlook.com that uses OAuth 2.0 authentication, the settings made on the control panel of the machine will not be enabled, and the SMTP server name and POP3 server name will be blank. When the SMTP server name or POP3 server name is input on the control panel, the setting of [Service Provider] for Internet Services changes to [Not Selected].

APP Registration using Microsoft Entra ID

In order for the machine to access the SMTP/POP3 server, register the APP using Microsoft Entra ID.

1. **Sign in to Azure Portal using the global administrator's account and select [Microsoft Entra ID].**
2. **Select [Manage] > [APP registrations] on the left side of the screen, and then click [New registration] in the upper area of the screen.**
3. **Enter the display name of the application into the [Name] field in [Register an application].**
   Example: Mail App
4. **In [Supported account types], select [Accounts in this organizational directory only].**
5. **Click [Register] at the lower part of the screen.**
6. **Select [Manage] > [Authentication] on the left side of the screen, and then click [Add a platform] in [Platform configurations].**
7. **In [Configure platforms] on the right side of the screen, select [Mobile and desktop applications].**
8. **For [Redirect URIs] in [Configure Desktop + devices] on the right side of the screen,**
   select "https://login.microsoftonline.com/common/oauth2/nativeclient" and click [Configure] at the lower part of the screen.
9. **In [Advanced settings] > [Allow public client flows] > [Enable the following mobile and desktop flows] at the lower part of the screen, select [Yes] then click [Save].**
10. **Select [API permissions] on the left side of the screen, and then click [Add a permission] in [Configured permissions].**
11. **In [Request API permissions] on the right side of the screen, select [Microsoft Graph] in [Microsoft APIs].**
12. **For [What type of permissions does your application require?], select [Delegated permissions].**

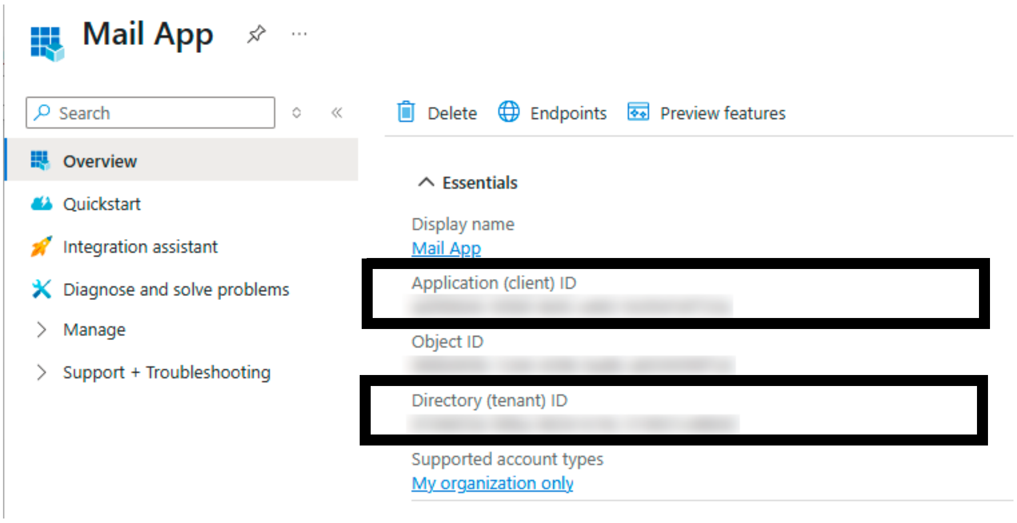
13. **Select the following access permissions.**

- OpenId permissions
  email
  offline_access
- POP
  POP.AccessAsUser.All
- SMTP
  SMTP.Send

14. **Click [Add permissions] at the lower part of the screen.**

15. **Select [Overview] on the left side of the screen, then copy [Application (client) ID] and [Directory (tenant) ID].**

These IDs will be used when authenticating from Internet Services. For the setting method, refer to "SMTP Server Settings using Internet Services" (p. 13) and "POP3 Server Settings using Internet Services" (p. 14).



Display name
Mail App

Application (client) ID
[redacted]

Object ID
[redacted]

Directory (tenant) ID
[redacted]

Supported account types
My organization only

SMTP Server Settings using Internet Services

1. **Log in to Internet Services as system administrator.**

2. **Set DNS server and Proxy server as necessary.**

3. **Click [Network] > [Protocols] > [SMTP] and enable [Port (Email Notification)].**

4. **Click [Service Provider] to select [Exchange Online / Outlook.com].**

5. **To [Tenant] and [Client ID], paste the respective values of [Directory (tenant) ID] and [Application (client) ID] that were copied in "APP Registration using Microsoft Entra ID" (p. 11).**

6. **Click [Save].**

Important

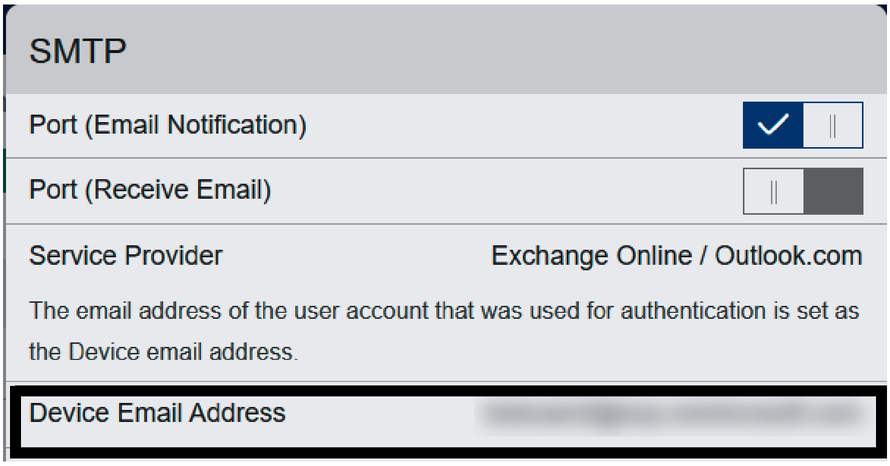
Do not change the settings except for [Port Number for Receiving Email], [Tenant] and [Client ID] if there is no particular reason.

7. **Click [Next] on the [Enter Authentication Code] screen.**

8. **On the input screen, enter the code that is displayed on the [Enter Authentication Code] screen then click [Next].**

9. **On the sign-in screen, sign in with the account set up with the email address for sending.**

10. **Close the sign-in screen after a successful sign in.**
The email address for the signed-in account will be set as the Device Email Address.



SMTP

Port (Email Notification) ✓

Port (Receive Email) ○

Service Provider: Exchange Online / Outlook.com

The email address of the user account that was used for authentication is set as the Device email address.

Device Email Address: [redacted]

Important

It is required that the UPN (User Principal Name) of the signed-in account be the same as the Device Email Address.
After a sign in, from the [Device Details] dialog box of Internet Services or from the control panel of the machine, do not change the Device Email Address to a string different from the UPN of the signed-in account. An authentication error results if changed.

POP3 Server Settings using Internet Services

1. **Log in to Internet Services as system administrator.**
2. **Set DNS server and Proxy server as necessary.**
3. **Click [Network] > [Protocols] > [POP3] and enable [Port (Receive Email)].**
4. **Click [Service Provider] to select [Exchange Online / Outlook.com].**
5. **To [Tenant] and [Client ID], paste the respective values of [Directory (tenant) ID] and [Application (client) ID] that were copied in "APP Registration using Microsoft Entra ID" (p. 11).**
6. **Click [Save].**

   Important

   Do not change the settings except for [Polling Interval], [Tenant] and [Client ID] if there is no particular reason.

7. **Click [Next] on the [Enter Authentication Code] screen.**
8. **On the input screen, enter the code that is displayed on the [Enter Authentication Code] screen then click [Next].**
9. **On the sign-in screen, sign in with the account set up with the email address for receiving.**
10. **Close the sign-in screen after a successful sign in.**

2 Feature Operation using Internet Services

2.1 Print

Printing using Internet Services

Allows you to print files without using a print driver.

Note

CMYK TIFF and JPEG (JFIF) files are not supported.

1. **Start Internet Services.**
2. **Tap [Print File] at the bottom of the Home screen.**
3. **Click [Browse], and then specify the file.**
4. **Set each item in [Print Settings] as required.**
5. **Click [Print].**

Print via NFC

If your mobile device supports the NFC touch print feature, holding the mobile device near the NFC area on the control panel allows you to print files easily.

To enable the NFC feature on the device, use Internet Services.

1. **Log in to Internet Services as system administrator.**
2. **Click [Network] > [NFC].**
3. **Enable [Active Tag] and [NFC Card Reader].**
4. **Click [Save].**

AirPrint

AirPrint is a printing service provided by Apple Inc. By using AirPrint, you can request a document print instruction to the device from macOS/OS X computers or iOS installed devices such as iPad/iPhone, without installing any print drivers or special software.

Note

For the latest information of AirPrint, refer to Apple Inc. official website.

AirPrint Settings

1. **Log in to Internet Services as system administrator.**
2. **Click [Network].**
3. **Click [AirPrint^{TM}] under [Mobile Printing] to enable the [Enable].**

   Note

   If the device is connected via USB, also enable the [USB Connection].

4. **Configure the settings as required.**
5. **Click [Save].**

   Note

   Rebooting the device is required to enable the settings. Reboot the device following the message on the screen.

Computer Settings (For macOS/OS X only)

The device must be registered to the computer before using AirPrint.

Note

When you use AirPrint via USB communication, this setting is unnecessary because the device is automatically registered to the computer when the device and the computer are connected with the USB cable.

1. **From a computer connected to the network, select the [Apple] menu > [System Preferences].**
2. **Select [Printers & Scanners].**
3. **Click [+] (Add).**

   Note

   If a drop-down menu is shown when you click [+] (Add), select [Add Printer or Scanner].

4. **Select the device from the [Name] list.**

   Note

   Printers in the network are searched automatically and listed in the [Name] list. If the device is not in the list, check the network settings of the device and the computer.

5. **Click [Use] > [Secure AirPrint] or [AirPrint] > [Add].**
   The device is added to [Printers] in the [Printers & Scanners] screen.

Printing

Printing from iOS

This section describes how to request a print instruction from iOS, using iPad as an example.

1. **Open the document you want to print.**
2. **From the ⬆ menu, tap [Print].**
3. **Tap [Select Printer].**
4. **Select the device and configure the print settings.**
5. **Tap [Print].**

Printing from macOS/OS X

1. **Open the document you want to print.**
2. **From the [File] menu, select [Print].**
3. **Select the device from [Printer]. Confirm the print settings, and click [Print].**

Note

You can only select the print settings available for the device.

2.2 User Authentication Operations

Changing Password by Login Users

The system administrator can set or change passwords using Internet Services.

1. **Log in to Internet Services as system administrator.**
2. **Click [Permissions].**
3. **Click the user to edit from [User Accounts].**
4. **Click [Change Password] to enter the new password.**
5. **Click [Save].**