Moxa Remote Connect Server Software User's Manual

Edition 1.1, June 2019

www.moxa.com/product

Moxa Remote Connect Server Software User's Manual

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Table of Contents

1

Introduction

This document describes how to establish remote connections for engineers to machines, and machine to machine communication in Moxa Remote Connect's Server portal.

The following topics are covered in this chapter:

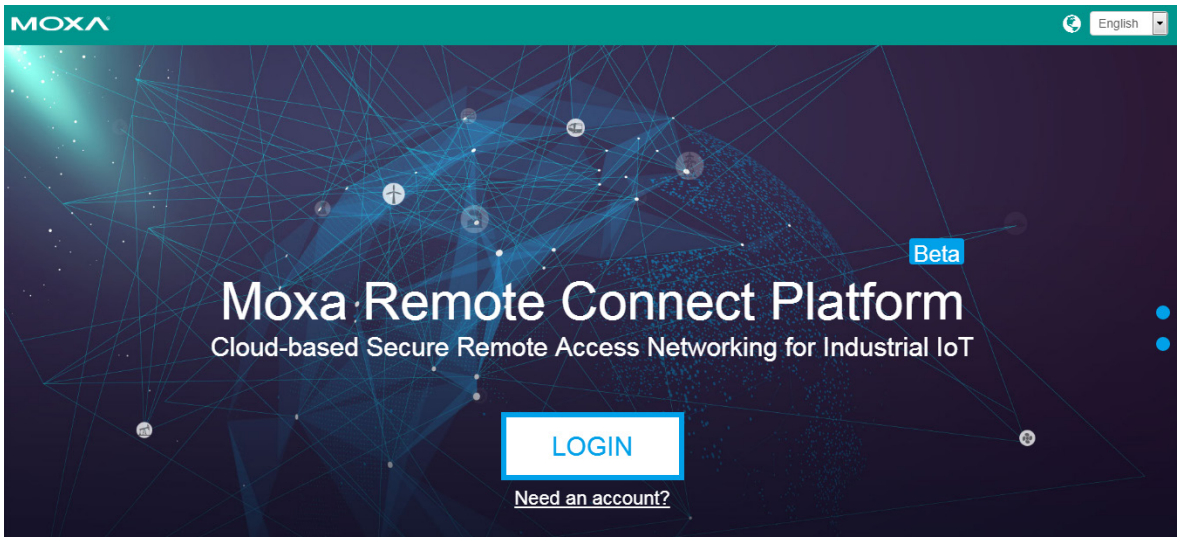
- **Administration Layers**
- **Administrator and Privilege**
- **Login and Logout**

Administration Layers

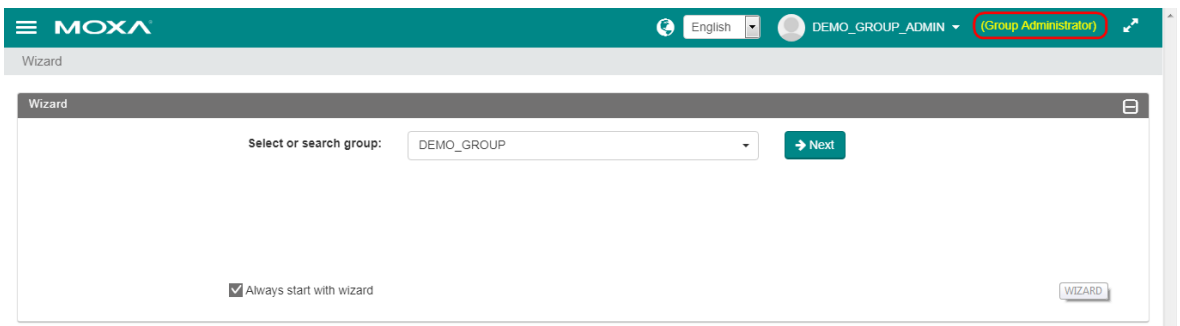
The Moxa Remote Connect (MRC) server has three layers of administration for different privileges and purposes. The top layer is "System", the second layer is "Domain", and the third layer is "Group". Each layer has its individual administrator account created by the administrator of the upper layer. After installation, there is a default system administrator account the first time a user logs in to the MRC server portal. The first time the system is used, users need to create "Domains" / "Domain Administrators", and "Groups" / "Group Administrators" in the system.

NOTE "System Administrator" can create "Domains" and "Domain Administrators", but cannot create "Groups" and "Group Administrators". To create "Group" / "Group Administrators", users must login as "Domain Administrator".

When logging into the portal as a System Administrator, the administrator can create multiple domains for different service accounts. When logging in to the portal as a Domain Administrator, the domain administrator can create multiple groups for different applications. When logging into the portal as a Group Administrator, the group administrator can directly manage (add/remove/modify) the remote connections of MRC client accounts and MRC gateways for interconnecting engineers and field Ethernet devices. After logging into the portal, users can see what type of privilege they have in the top right corner of the portal.



Showing the privilege of the current account.



Administrator and Privilege

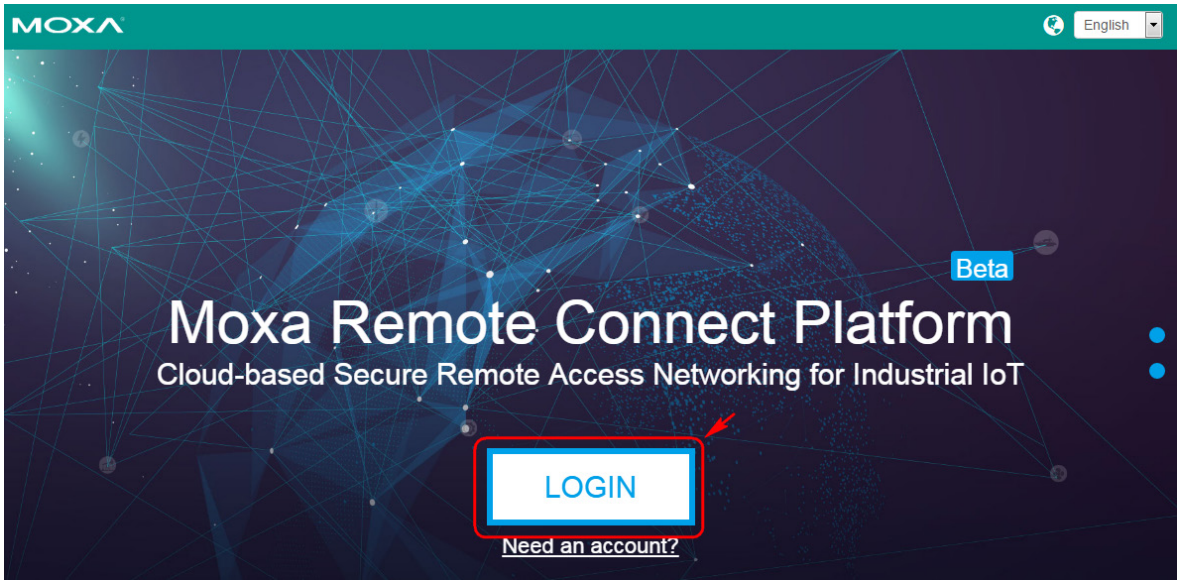
Administrator	Description	Privilege
System Admin	Default login: admin, password: Your EC2 instance ID (see note)	Create, delete, and modify a service domain and domain administrators
Domain Admin	Created by System Admin	Create, delete, and modify a device group and group administrators
Group Admin	Created by Domain Admin	Create, delete, and modify MRC gateways and MRC clients and manage remote connections

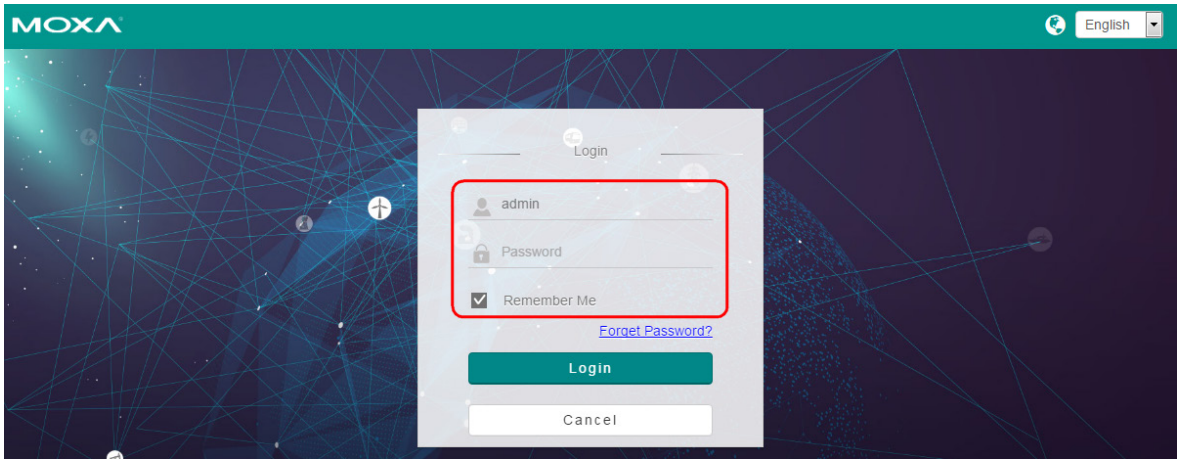
NOTE Your EC2 instance ID can be retrieved from your Amazon AWS console. After signing in to the AWS management console, please go to "Service", then "EC2", and click on "Instances".

Login and Logout

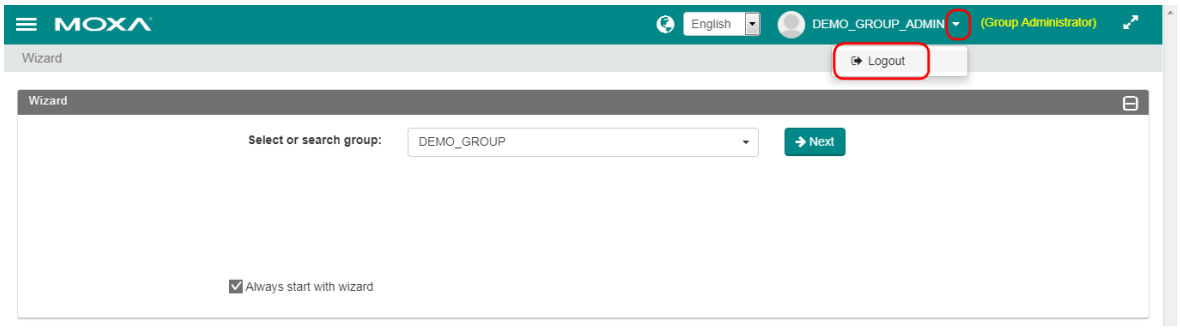
After installing a Moxa Remote Connect server, please make sure it is connected to the Internet. Users can access the portal through a HTTPS connection.

Click the "LOGIN" button to log into the portal.





Click on the account name at the top of the web page to log out of the system.



2

Install License

Allowed Privilege: ☑ System Admin ☐ Domain Admin ☐ Group Admin

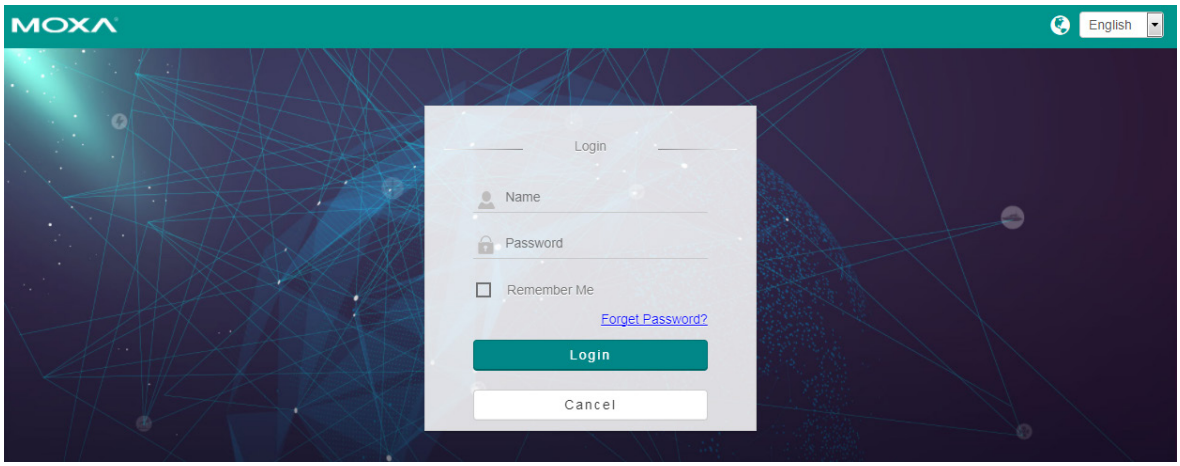
The following topics are covered in this chapter:

- **Install Activation License**
- **Install Server Node Upgrade License**

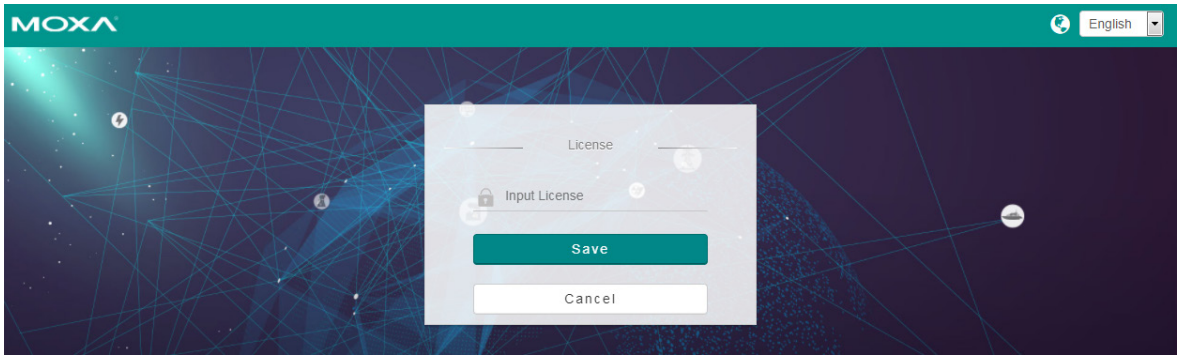
Install Activation License

If you choose "Moxa Remote Connect (BYOL)" from Amazon Marketplace, you need to order Moxa Remote Connect Server Activation License (MRC Server Activation License) from Moxa's channels, and input the activation license after the first login (System Administrator) to activate your MRC Server.

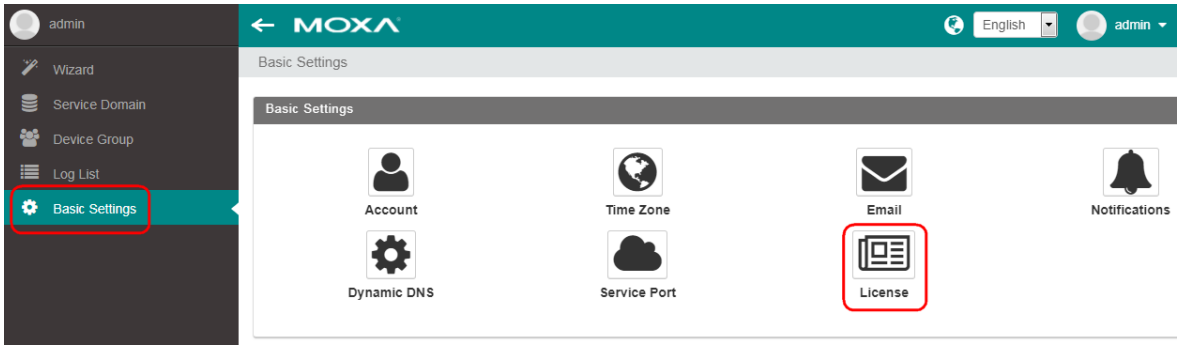
Step 1: Log in as the System Administrator

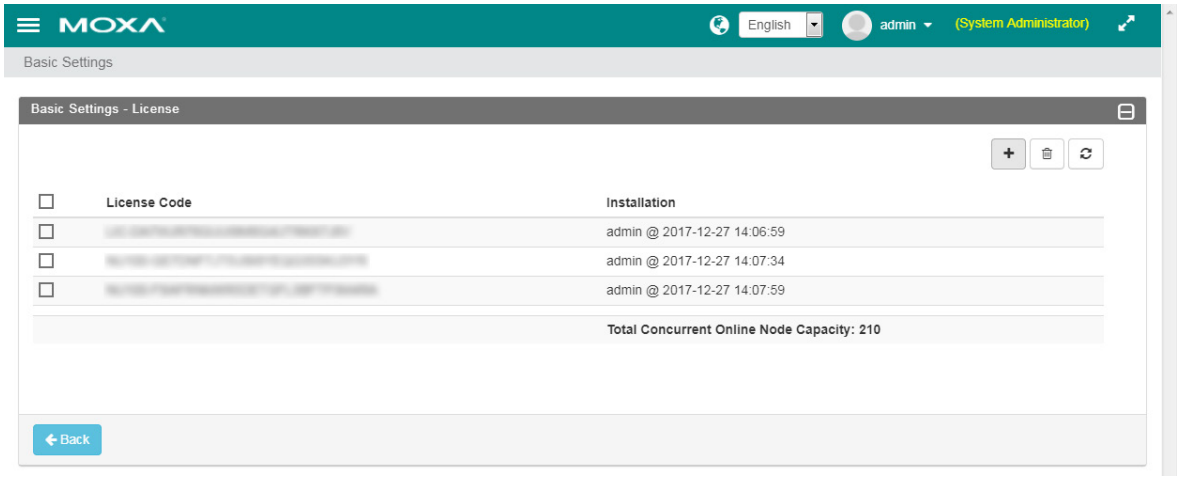


Step 2: Input MRC Server Activation License and click on "Save"



Step 3: Check the installation of the license

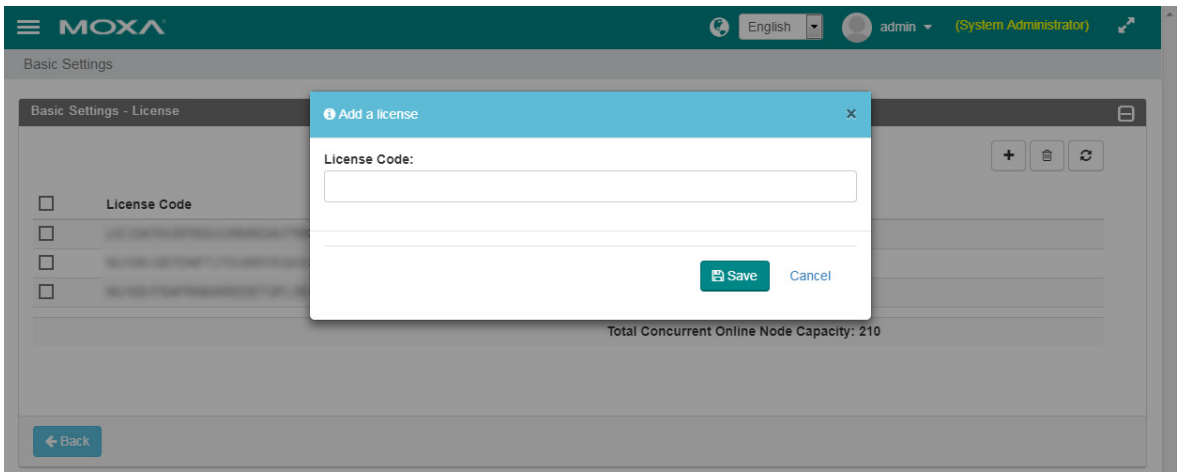




NOTE By default, installation of the activation license comes with the system capacity of 10 concurrent online nodes. For adding more concurrent online nodes, please order a MRC Server Node Upgrade license.

Install Server Node Upgrade License

Click on + to install "Server Node Upgrade License" for enlarging the concurrent online node capacity of the server; click on 🗑 to remove the license; click on ↻ to refresh the license status.

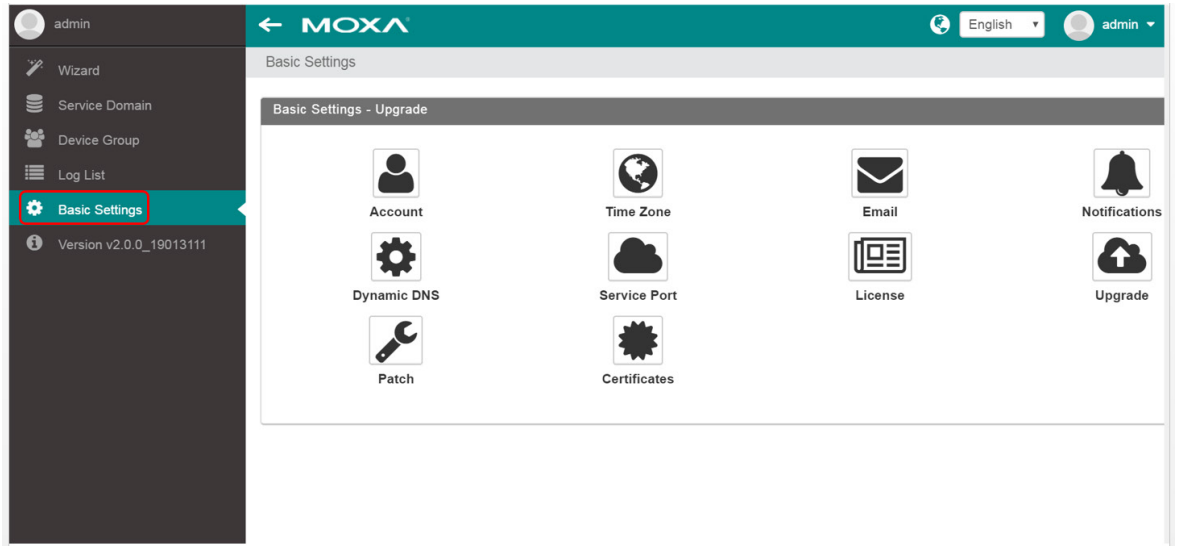


3

Basic Setting

Allowed Privilege: ☑ System Admin ☑ Domain Admin ☑ Group Admin

Click on the menu and select “Basic Settings” to set up the basic configurations of the Moxa Remote Connect portal.



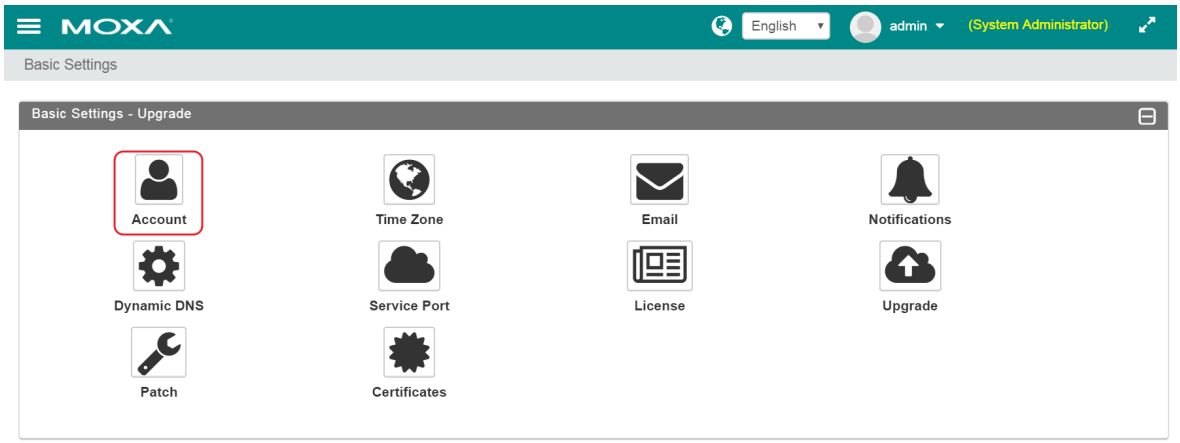
The following topics are covered in this chapter:

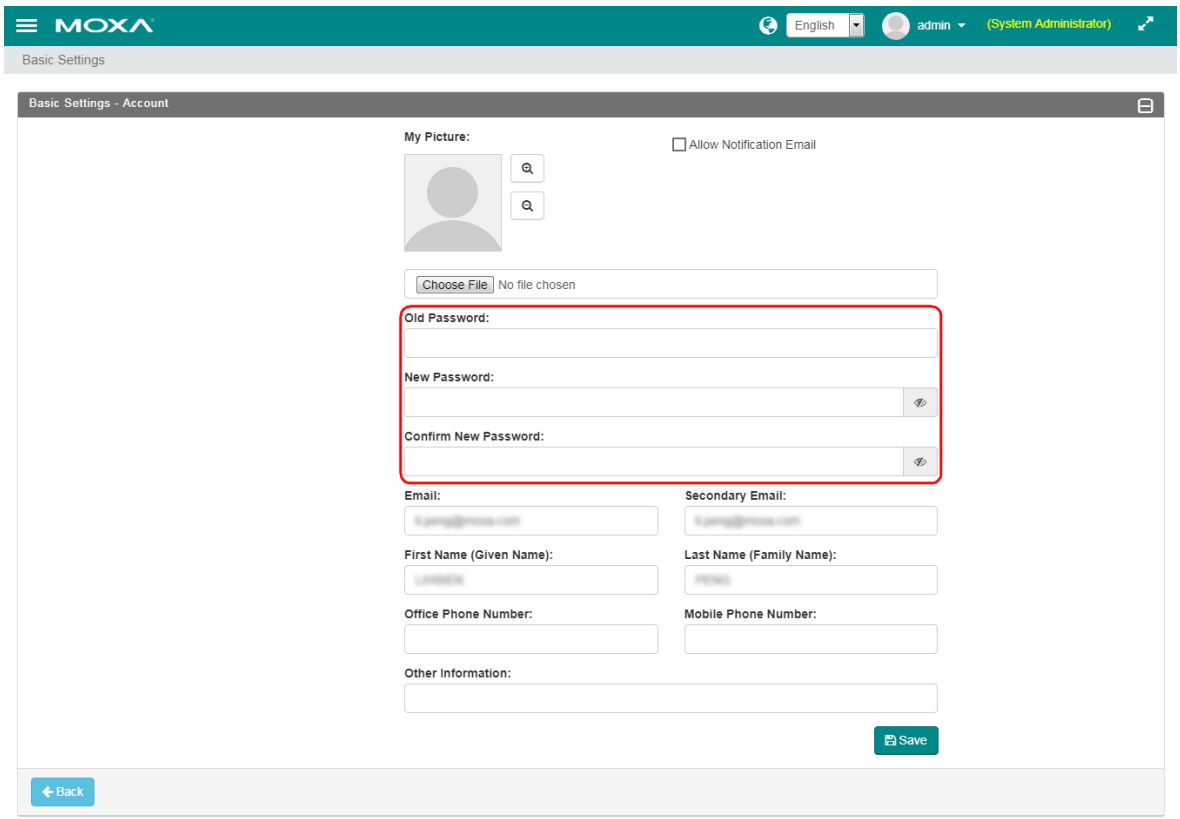
- **Account**
- **Time Zone**
- **Email**
- **Notifications**
- **Dynamic DNS**
- **Service Port**
- **Backup**
- **Upgrade**
- **Patch**
- **Certificate**

Account

Allowed Privilege: ☑ System Admin ☑ Domain Admin ☑ Group Admin

It is highly suggested to change the default password after logging in the Moxa Remote Connect portal. Modifying the administrator's profile is also suggested.

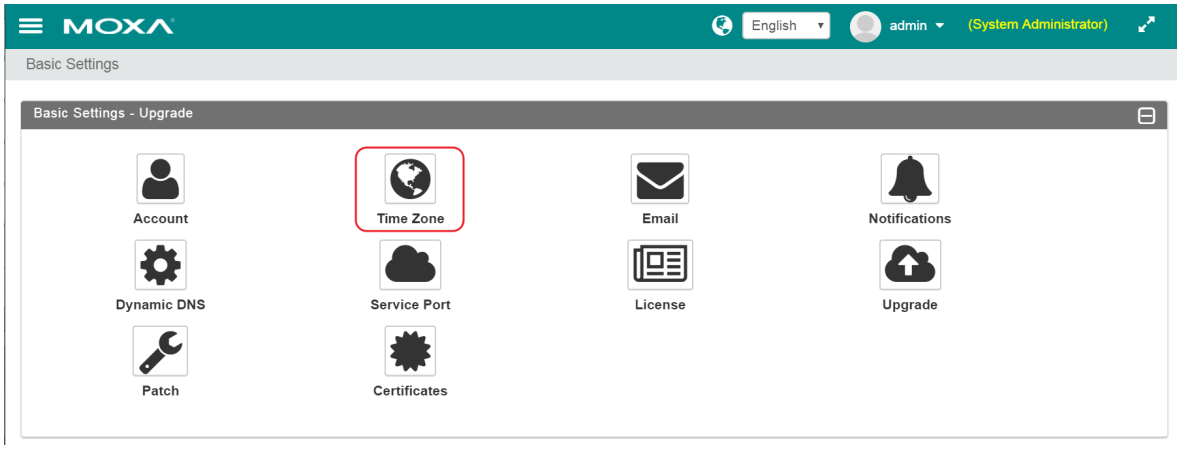


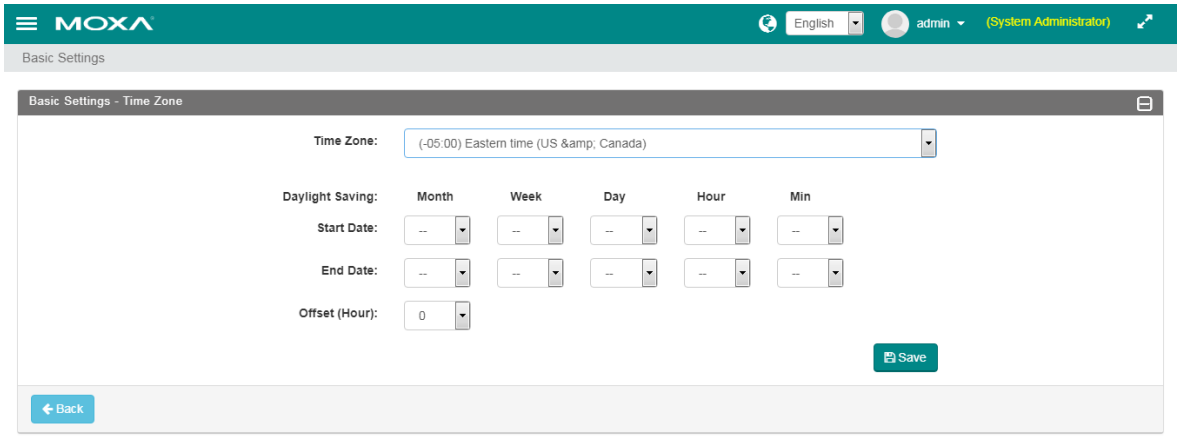


Time Zone

Allowed Privilege: ☑ System Admin ☑ Domain Admin ☑ Group Admin

Change the time zone setting of the Moxa Remote Connect portal to synchronize the recording time of logs and events. The MRC system, service domains, and device groups can set up the individual time zone to display their own events and logs.

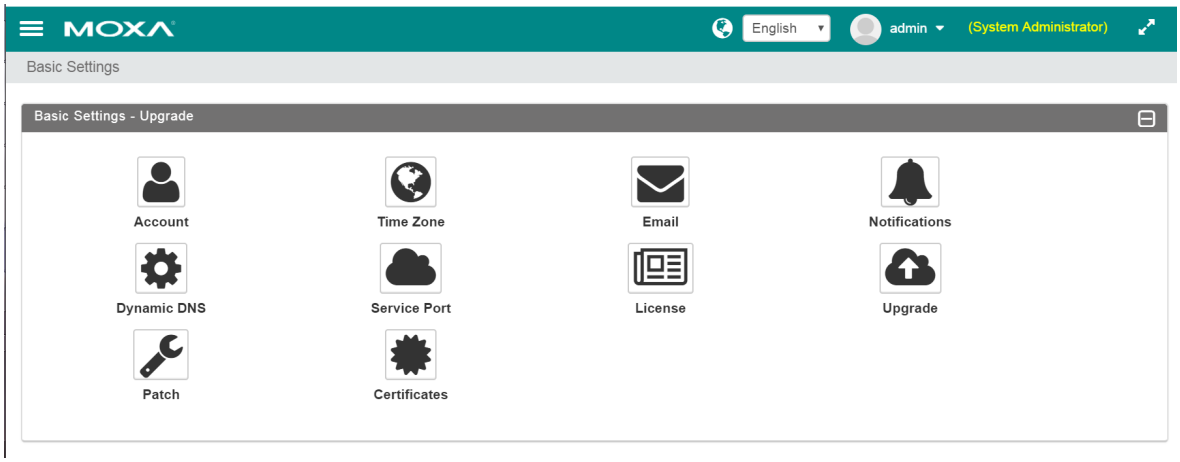




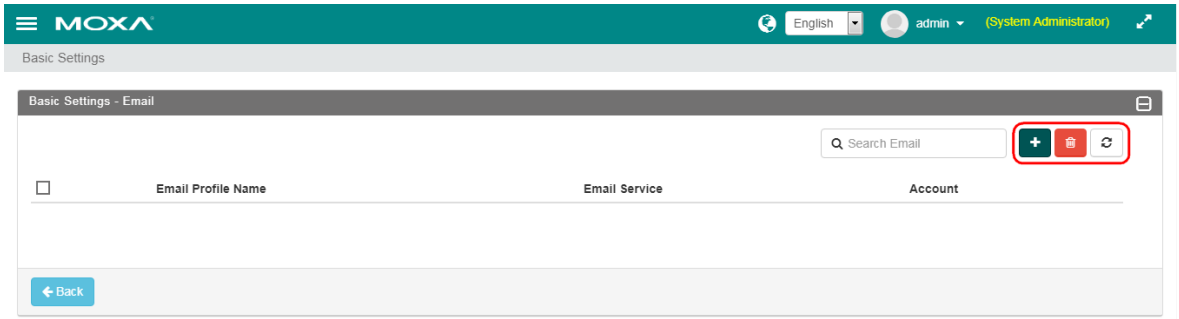
Email

Allowed Privilege: ☑ System Admin ☑ Domain Admin ☑ Group Admin

The system, domain, or group administrators can set up individual email accounts for sending out the notification via email. This email account is where the event or notification emails are sent from.



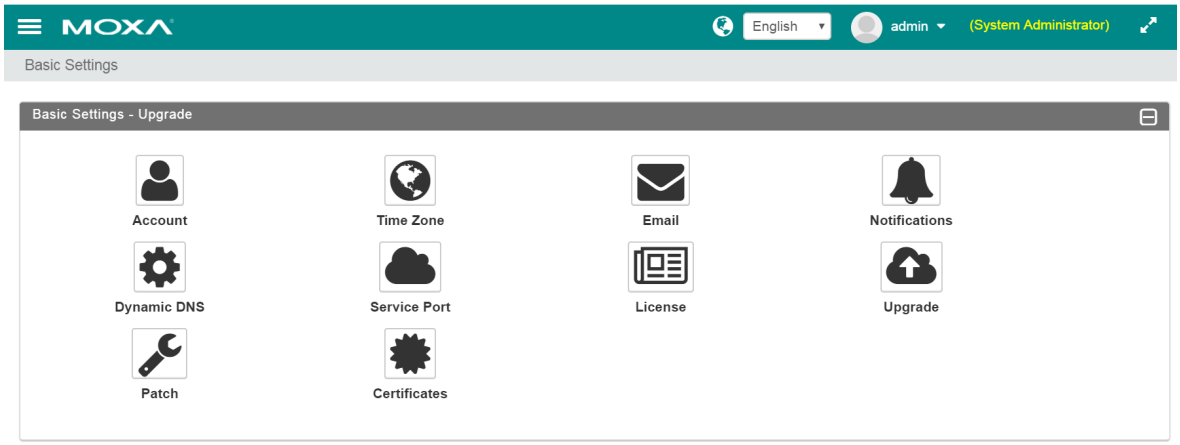
Click on + to add an email account. Click on 🗑 to remove an email account. Click on ↻ to refresh the display of the email settings page.

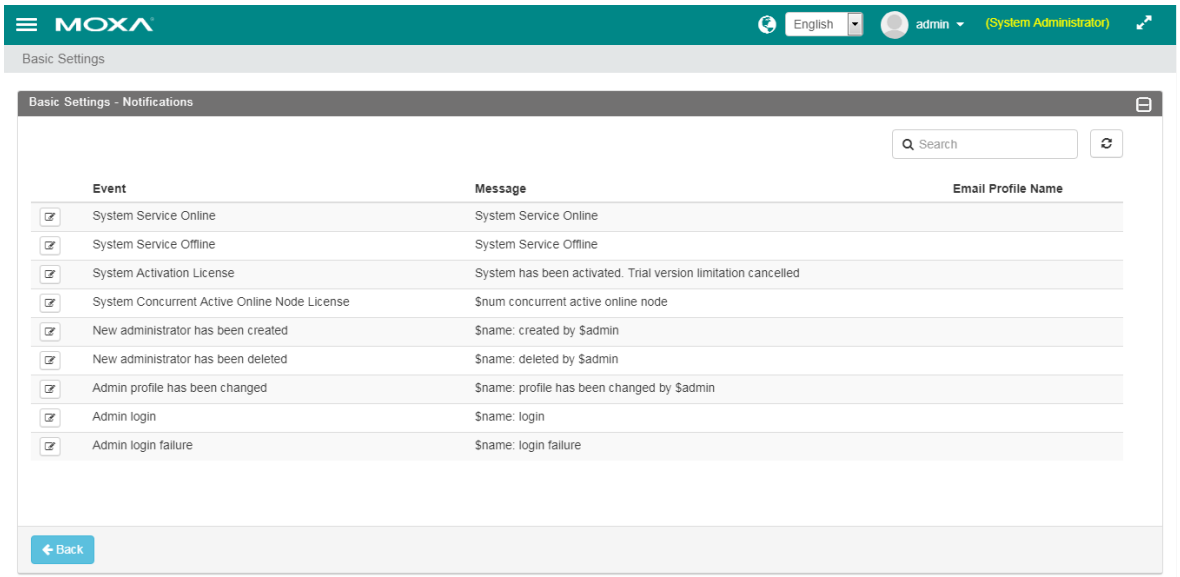


Notifications

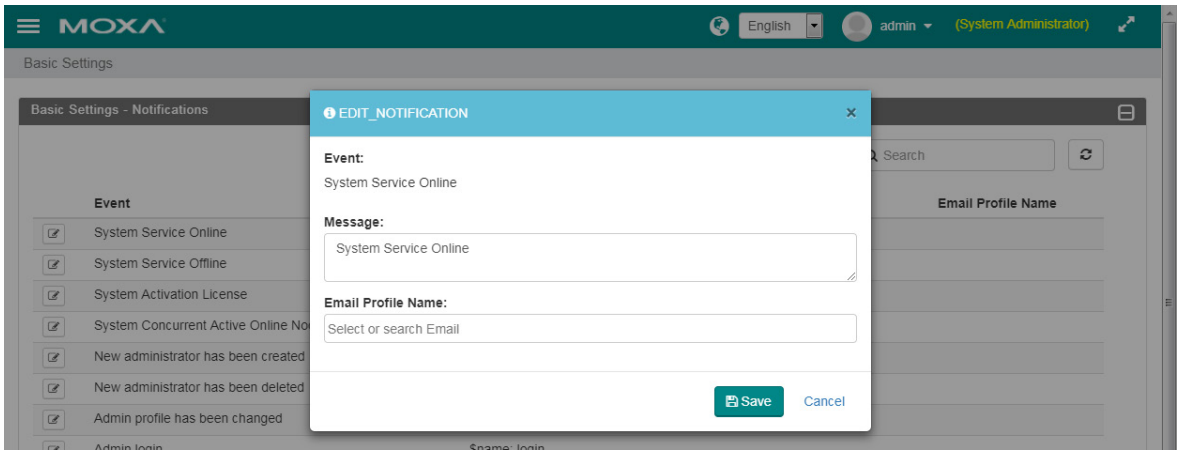
Allowed Privilege: ☑ System Admin ☑ Domain Admin ☑ Group Admin

The administrators can set up user-defined notification messages and event types to be sent to the notification receivers.

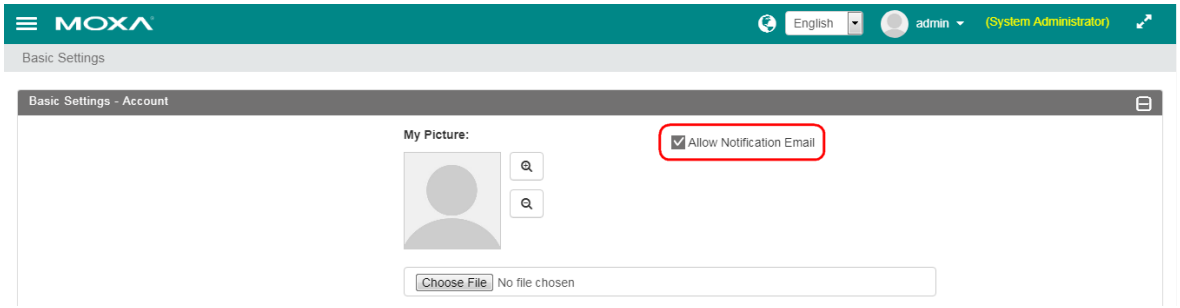




Click on to edit the self-defined system message for the events. Select the Email Profile Name which has been set up in the Email settings for sending out the event message. Users can leave them unchanged by sending out the event notifications by the default message.



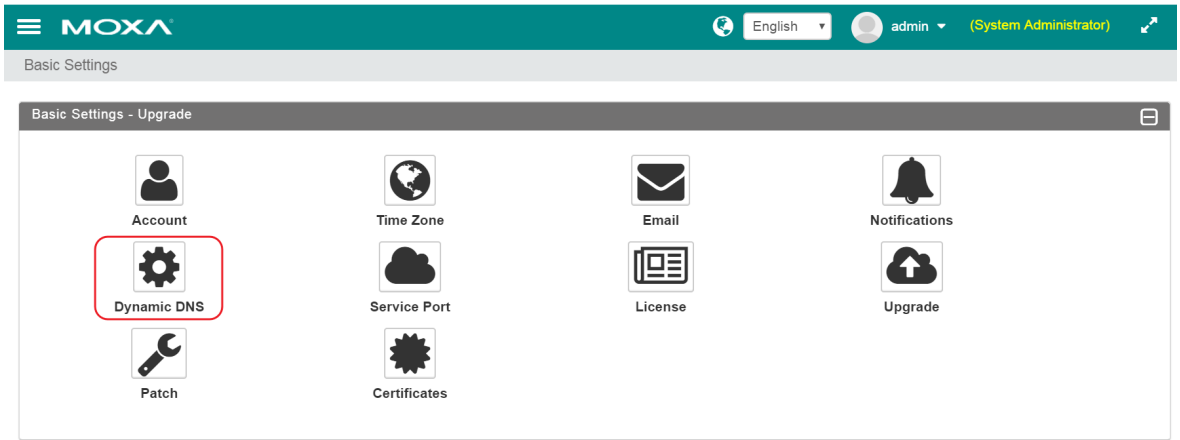
NOTE If an administrator would like to receive the notification email sent out by the MRC portal, the administrator should enable the feature "Allow Notification Email" in the account profile settings.

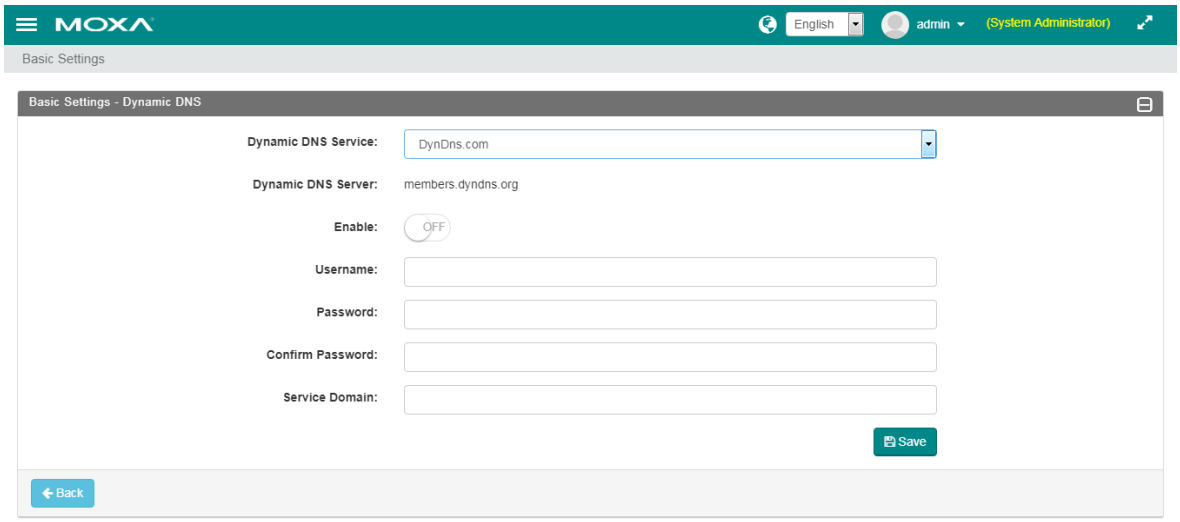


Dynamic DNS

Allowed Privilege: ☑ System Admin ☐ Domain Admin ☐ Group Admin

The MRC portal must have a public IP address and support major dynamic DNS services including DynDNS, FreeDNS, NO-IP, and PubYun for the system administrator to assign a domain name for the portal if the public IP address is not fixed.

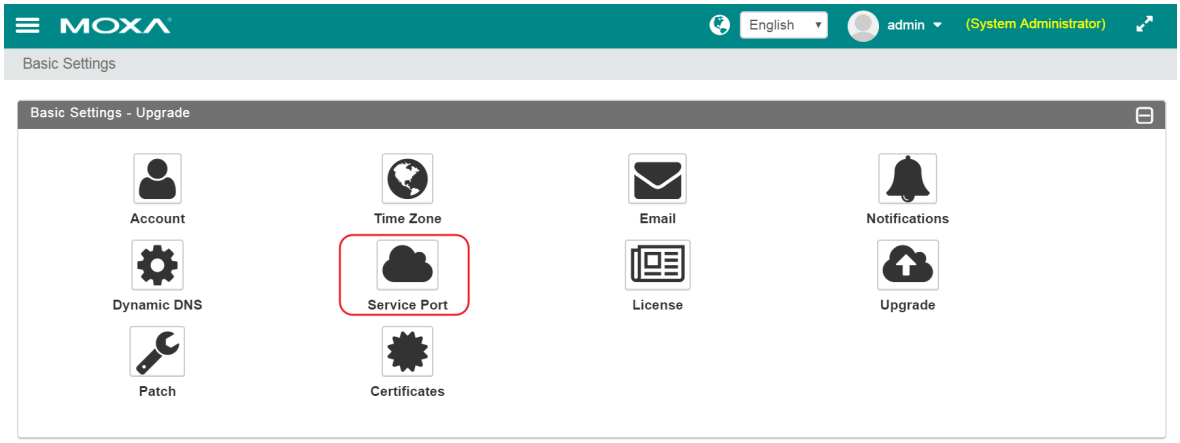


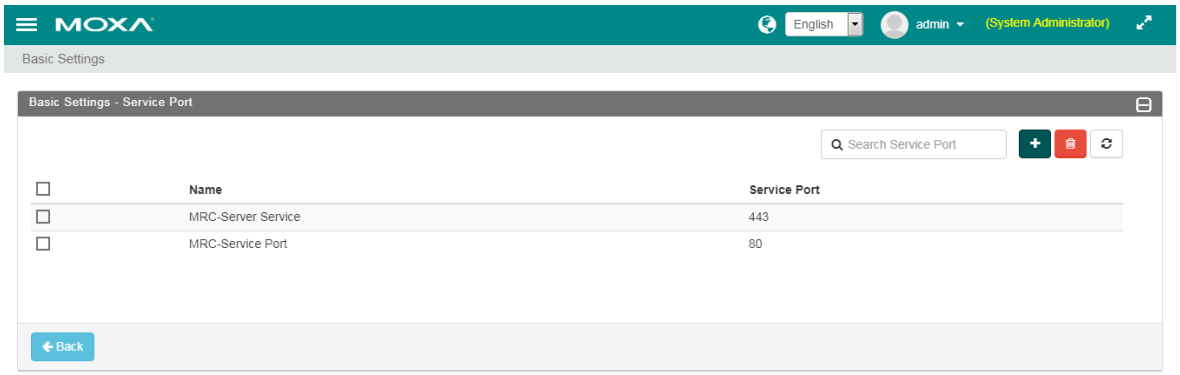


Service Port

Allowed Privilege: ☑ System Admin ☐ Domain Admin ☐ Group Admin

The "Service Port" of the MRC portal is used for the MRC gateways and MRC clients to establish the remote access tunnels with the MRC portal. By default, the service port is port 443 which is commonly accepted as public Internet service. The system administrator can assign multiple service ports if there is a special requirement of the outgoing service port limitation in the field where MRC gateways or MRC clients are located.





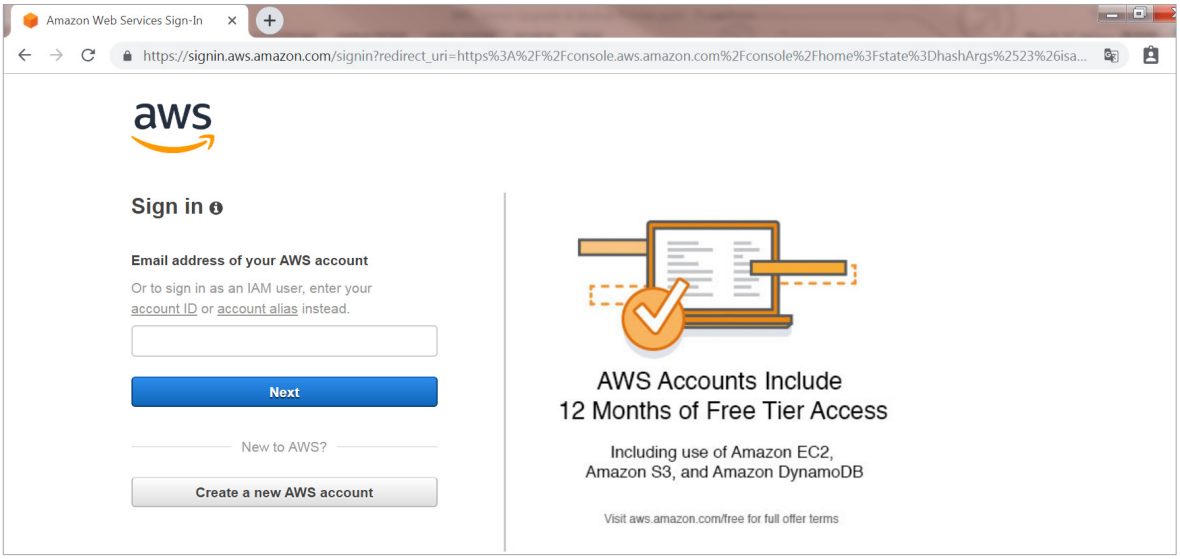
Click on  to add a service port. Click on  to remove a service port. Click on to refresh the display of the service port settings.

Backup

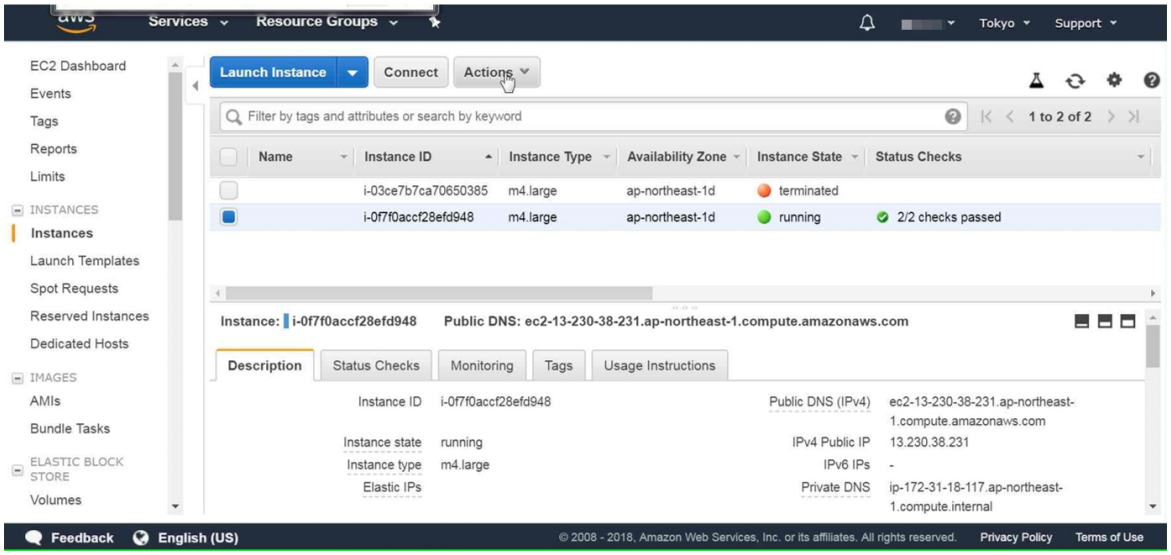
Before upgrading the MRC server, it is suggested to first back up the MRC server configurations. Users can use the "Create Image" function in the AWS platform to back up the MRC server. The process can be completed in a few clicks.

Users have to log in to the AWS management console to use the function "Create Image" to back up the MRC server configurations.

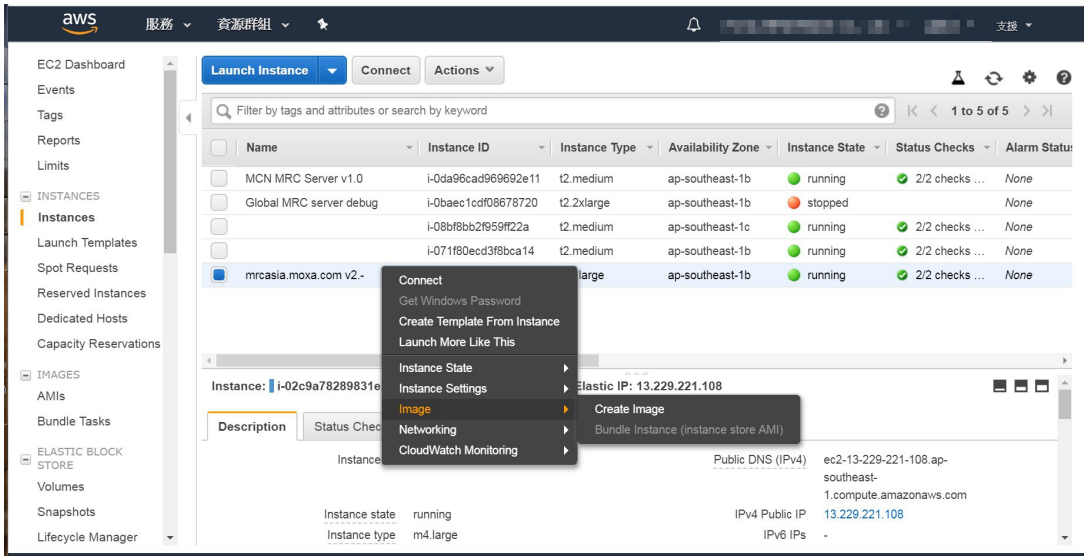
Users can log in by signing in with their AWS Account ID and password:
https://aws.amazon.com/tw/console/



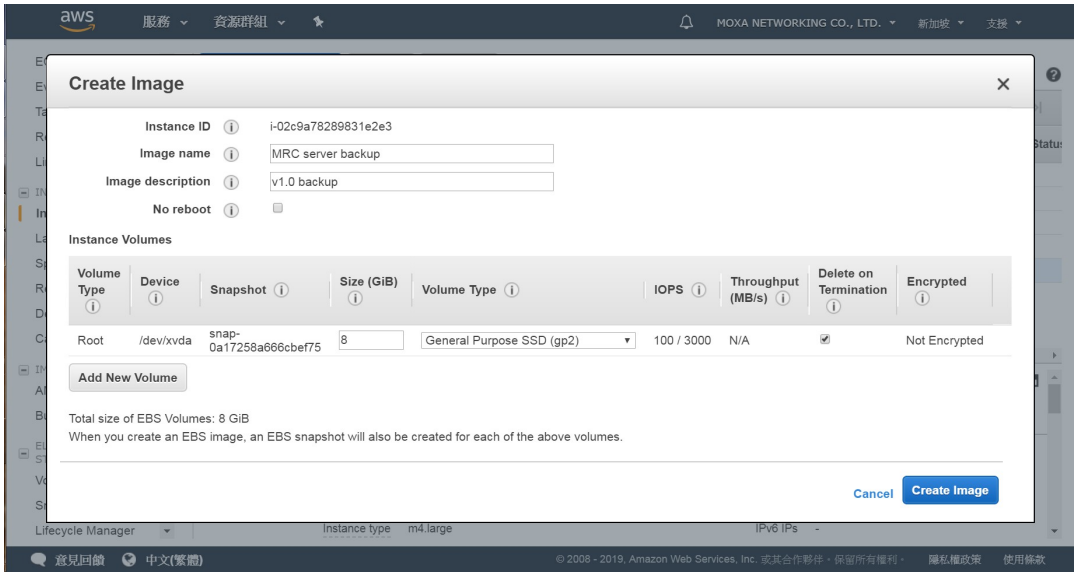
After users have entered the AWS console, they should choose the instance that the MRC server is running on.



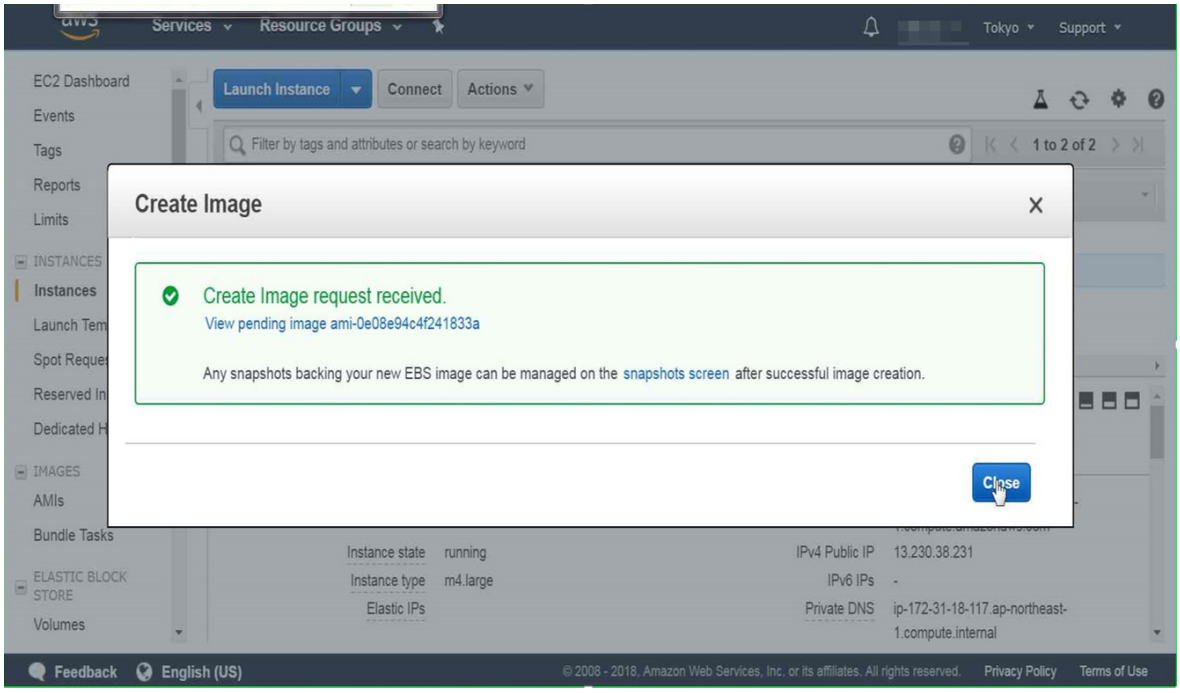
Right click to open the tab and choose "Create Image".



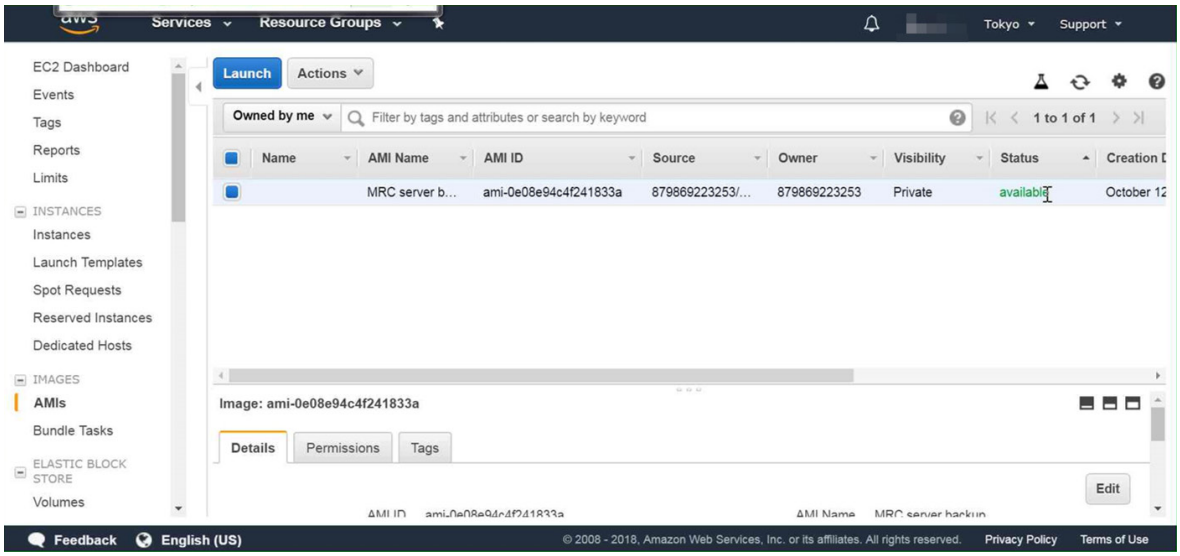
Name the image and click "Create Image".



Create a backup of the MRC server image and get the ID of the image.



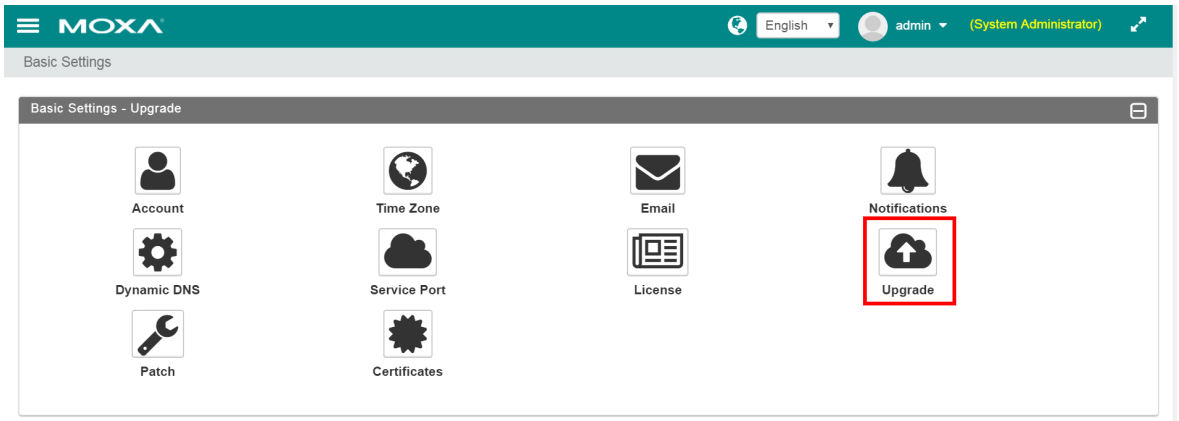
Click the "AMI" tab, and choose the image you want to recover and press "Launch". Once the AMI has launched, AWS will create another instance for this server.

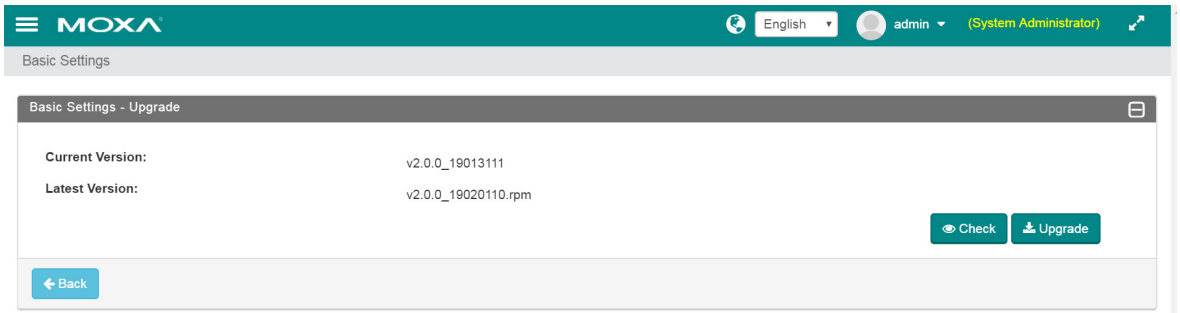


Upgrade

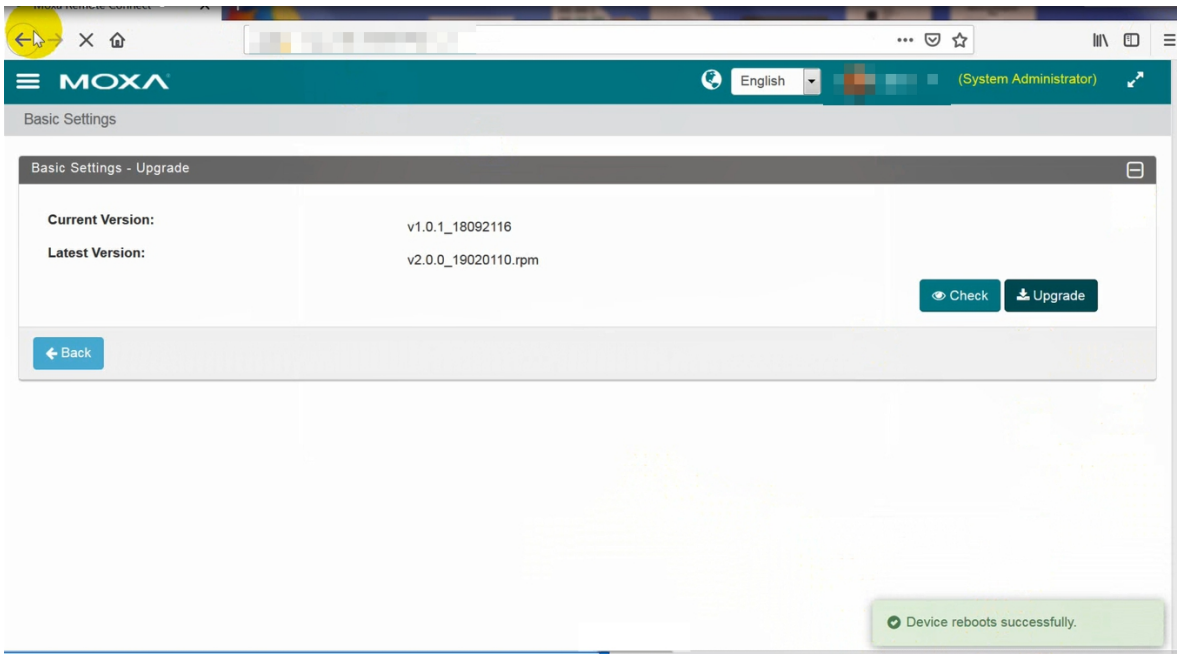
Allowed Privilege: ☑ System Admin ☐ Domain Admin ☐ Group Admin

Under the "Upgrade" section of the MRC portal, users can upgrade their MRC server to the latest version. Click **Check** to get the latest server version information. Click **Upgrade** to upgrade to the latest server version.

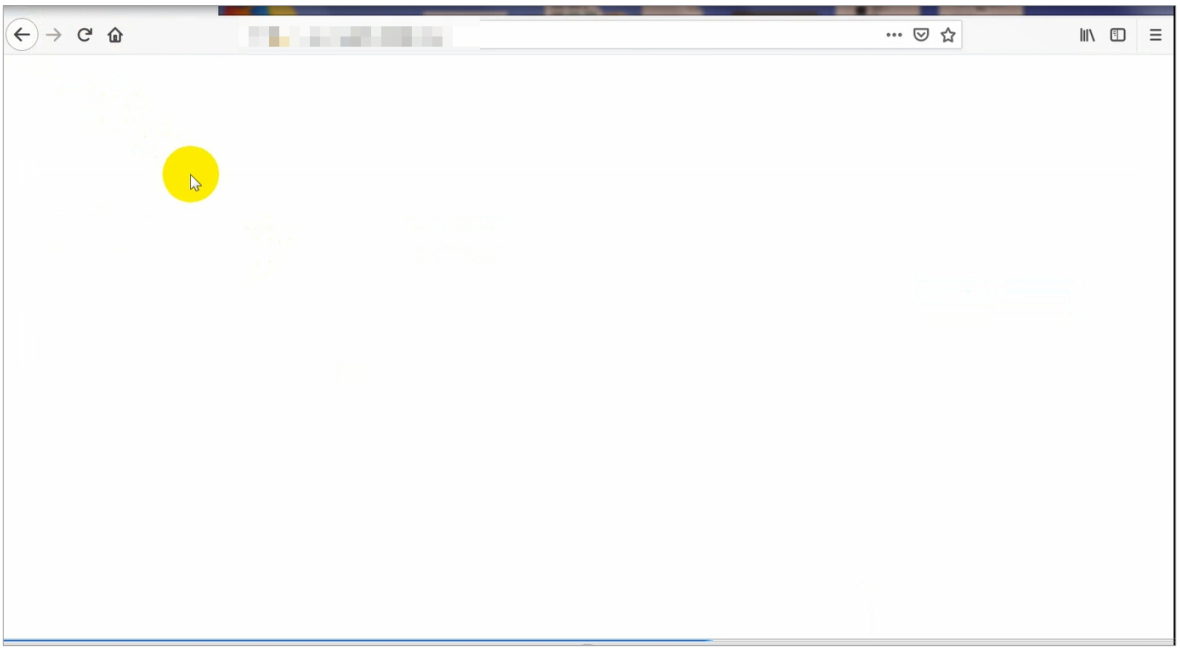




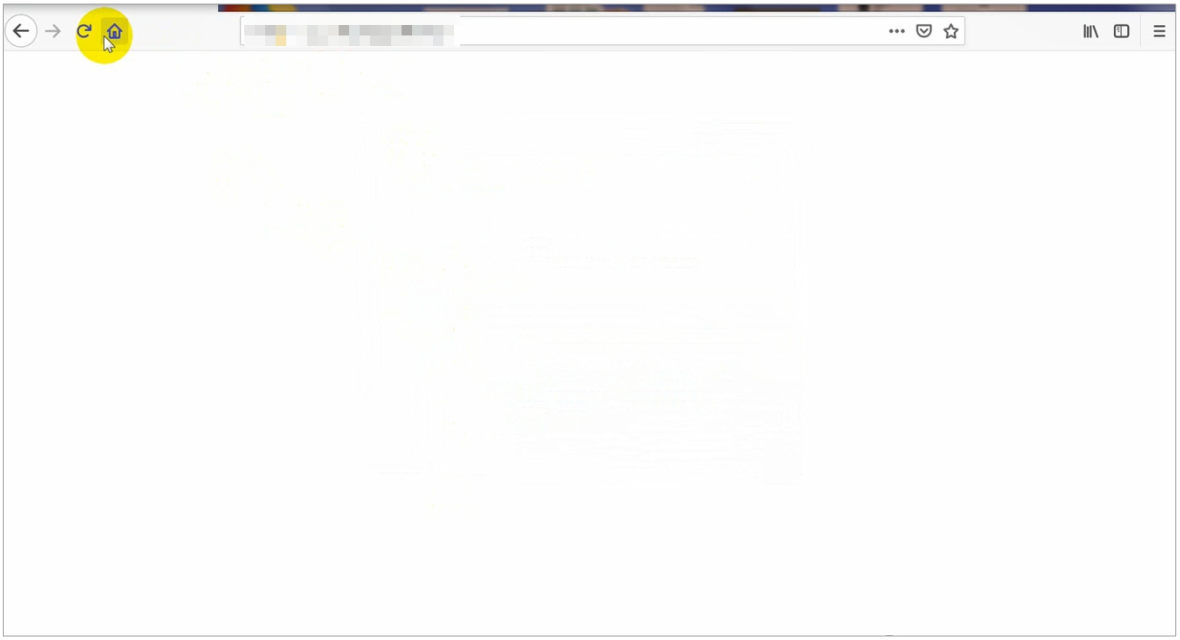
When the server has been upgraded to v2.0, the AWS EC2 instance will reboot automatically.



It will take about two minutes to reboot the AWS EC2 instance.



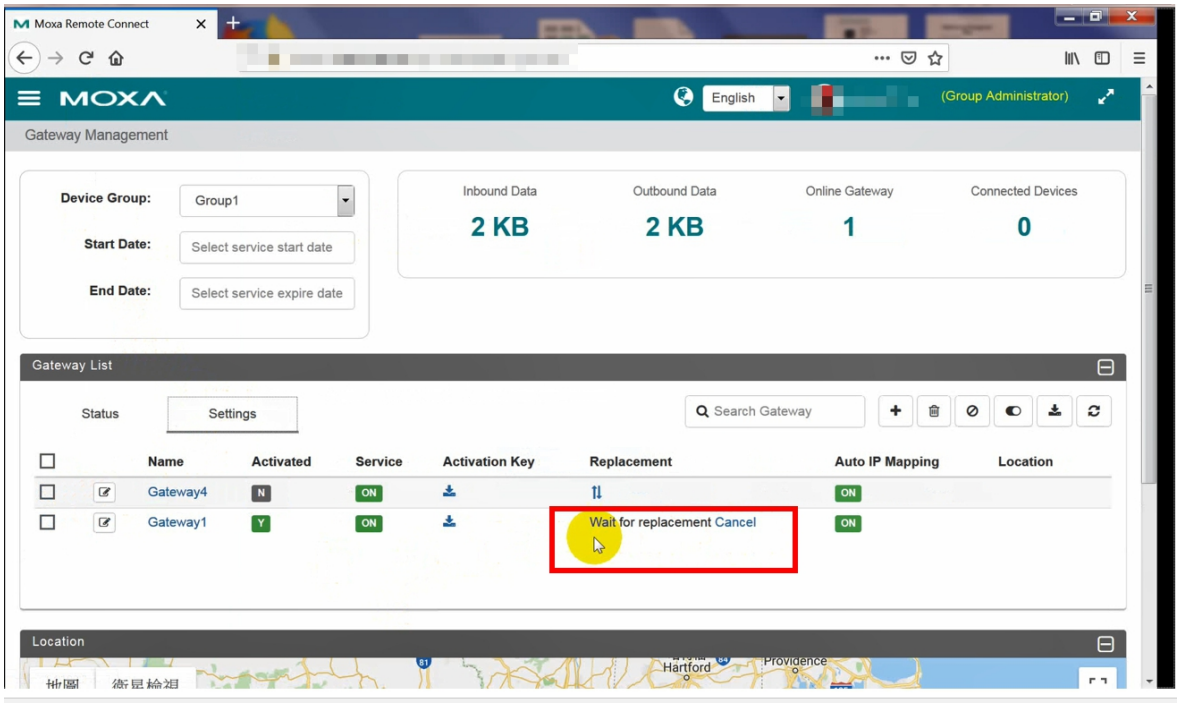
Once the AWS EC2 instance has rebooted successfully, you can refresh the browser, and then return to the MRC server login page.



When the server has been upgraded to v2.0, the gateway status will show "wait for replacement".

This message indicates that gateway has not yet upgraded to v2.0. and the server is waiting for the gateway to upgrade.

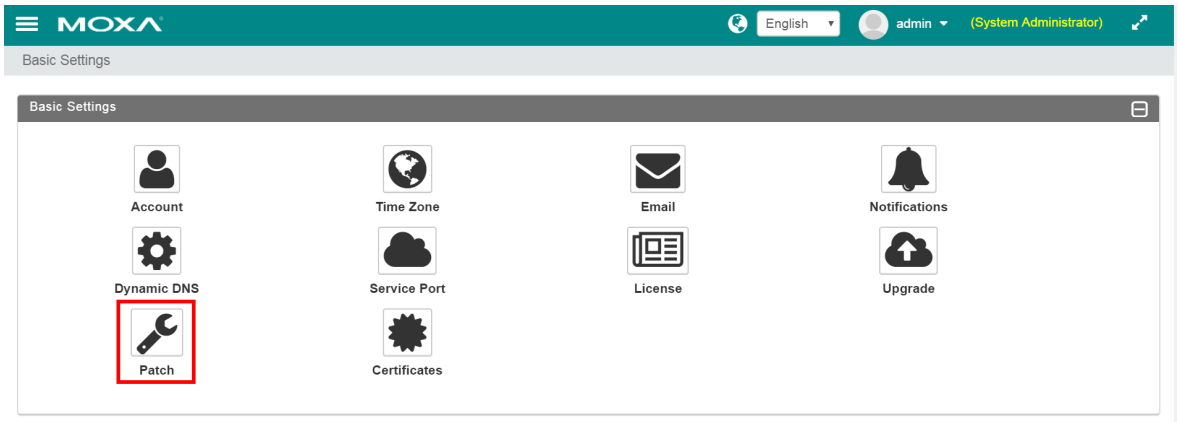
Once the gateway has been upgraded to v2.0, this message will disappear.

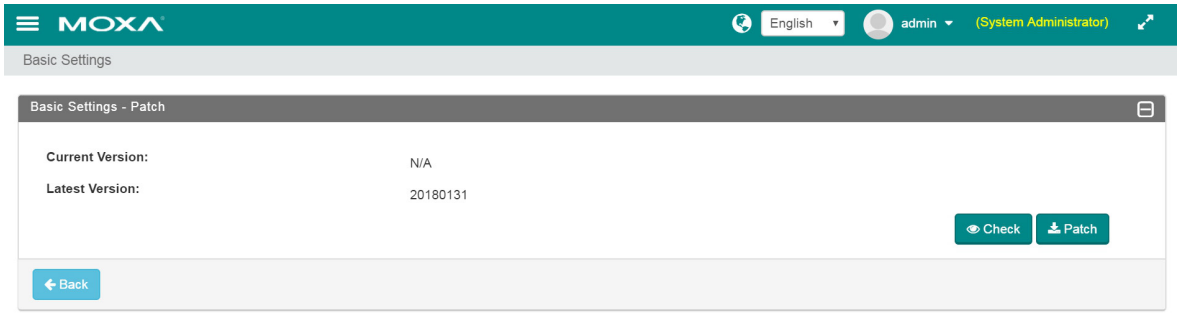


Patch

Allowed Privilege: ☑ System Admin ☐ Domain Admin ☐ Group Admin

Under the "Patch" section of the MRC portal, users can update the patch that fixes any vulnerabilities for their MRC server. Moxa will release security patches to fix vulnerabilities when required. Users can click **Patch** to check for the latest vulnerability fixes and decide whether to install the patch. Click **Check** to get the latest security patch version information. Click **Upgrade** to confirm the installation of the latest security patch.

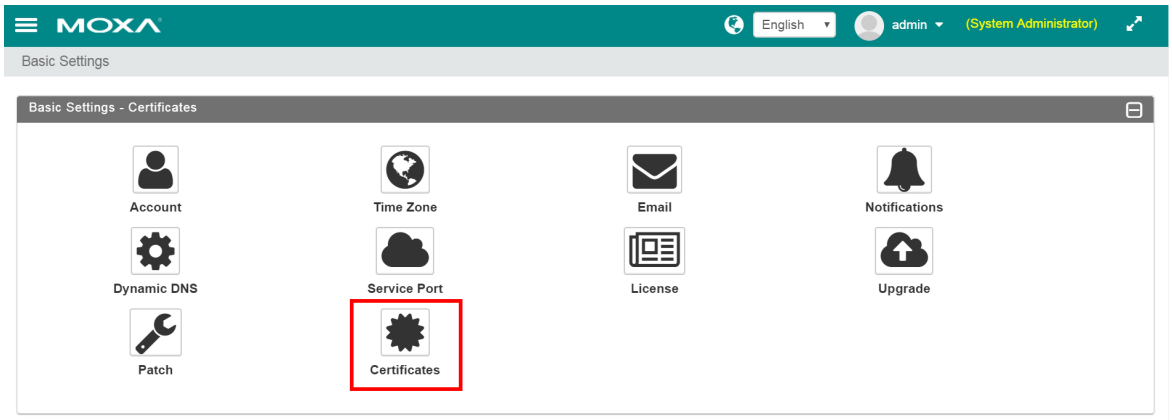




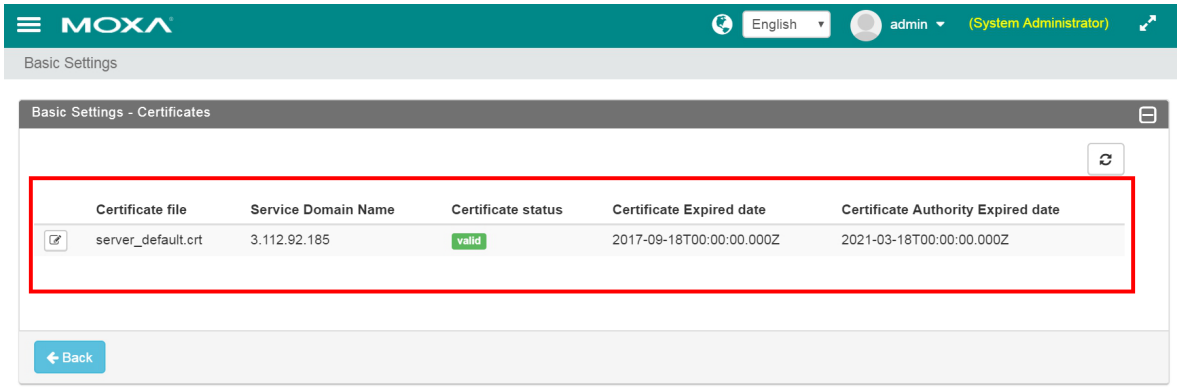
Certificate

Allowed Privilege: ☑ System Admin ☐ Domain Admin ☐ Group Admin

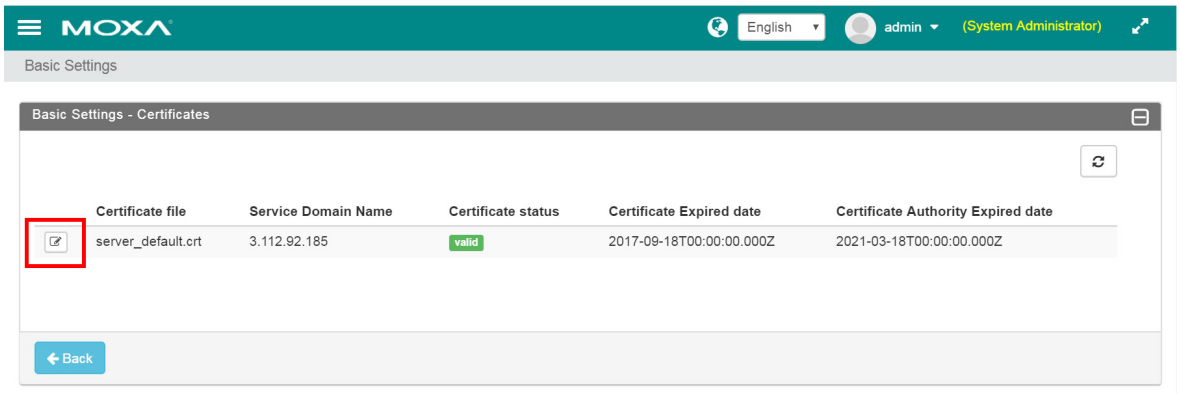
Under the "Certificate" section of the MRC portal, users can insert the certificate which is recognized by the system administrator in the MRC server. With this function, the system administrator can make sure that users connect to the correct MRC server portal rather than an incorrect MRC server portal. Before the system administrator imports a certificate, it is suggested that the MRC domain name is set up successfully, and the certificate is with the MRC domain name.

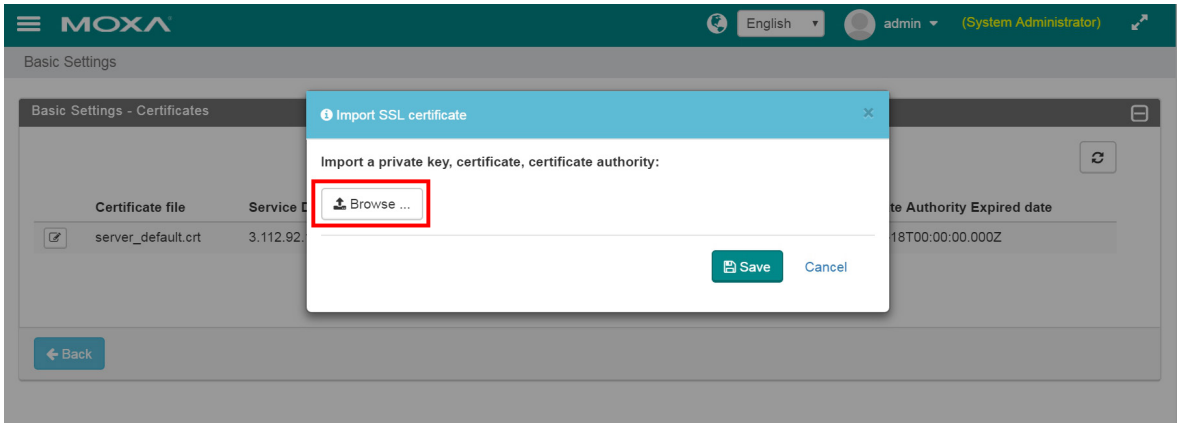


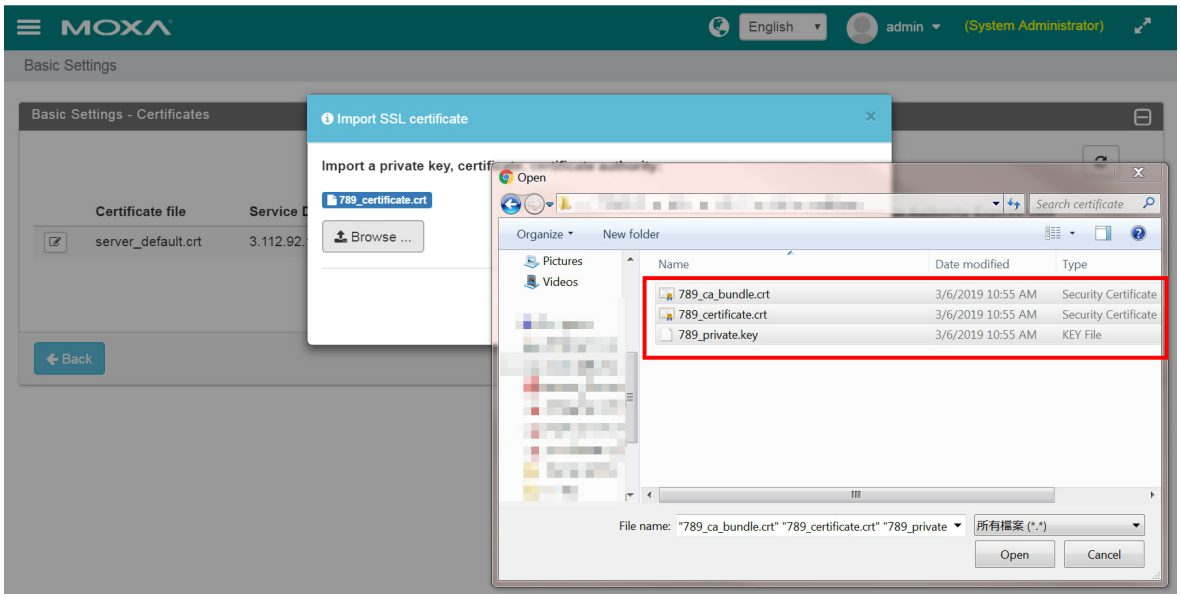
By default, the MRC server is installed with a certificate issued by Let's Encrypt Authority X3. Users can change to other certificates for the MRC server.

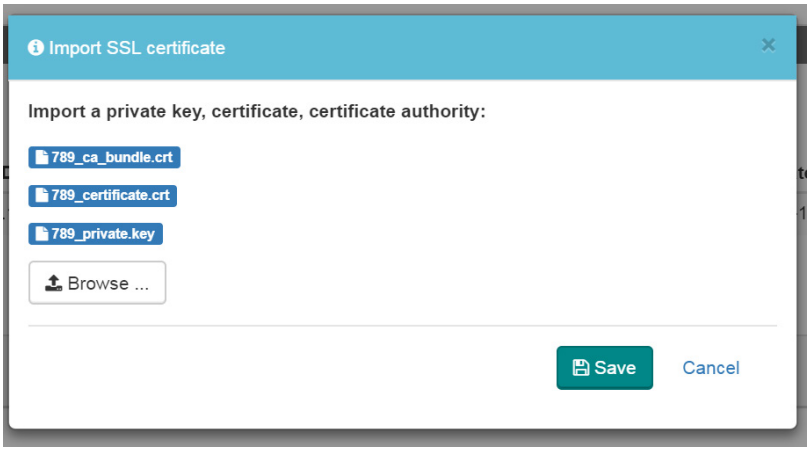


Click to import an SSL certificate that you trust. Click **Browse** to import the certificate. The completed certificate includes three files: certificate.crt, ca.crt, and private.key. Users can choose three files at one time. Then click "Save" to import the certificate into the MRC server. After importing the certificate successfully, the MRC server will automatically log out.







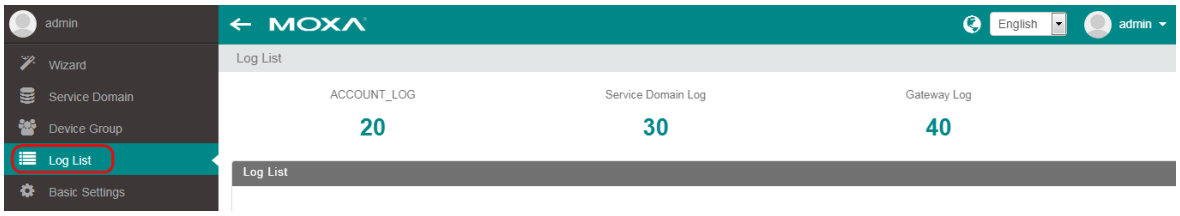

Import SSL certificate
Import a private key, certificate, certificate authority:
789_ca_bundle.crt
789_certificate.crt
789_private.key
Browse ...
Save
Cancel

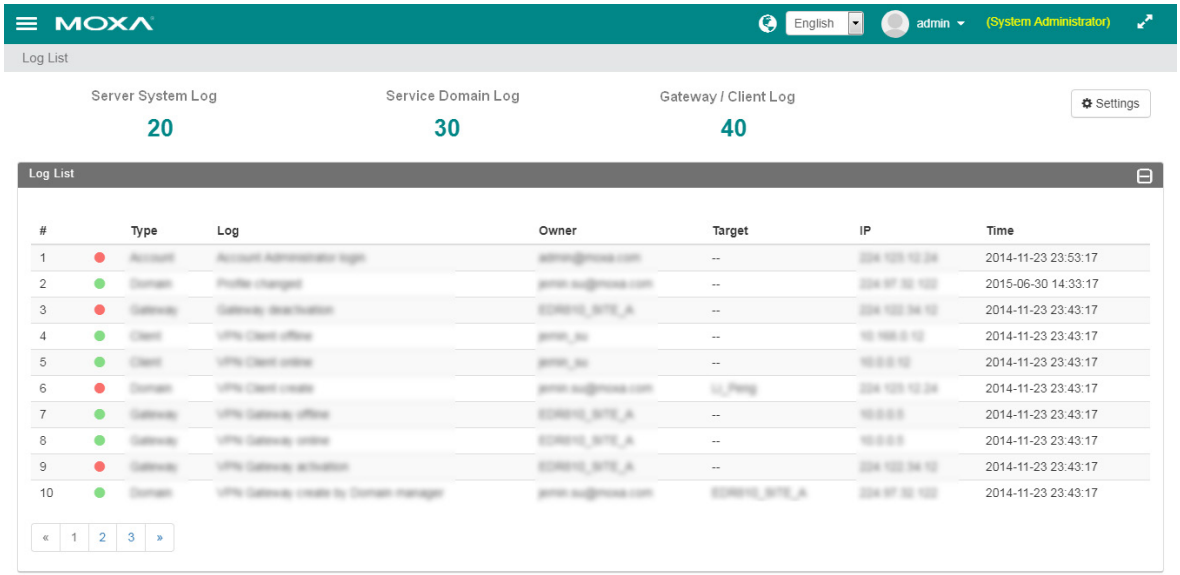
4

Log List

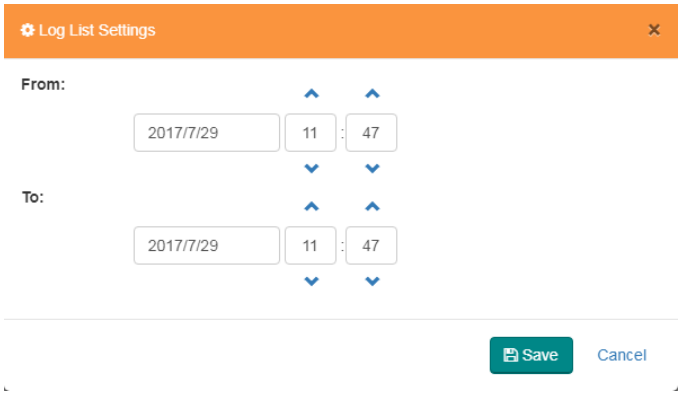
Allowed Privilege: ☑ System Admin ☑ Domain Admin ☑ Group Admin

The administrators can read logs depending on their privilege levels. The system admin can review all the logs and events that happened in the MRC portal. The domain admin can only review the logs and events happened in the domain. The group admin can only review the logs and events that happened within their group.





Click on Settings to choose the period for the event logs that you want displayed.



5

Log in as System Administrator

Allowed Privilege: ☑ System Admin ☐ Domain Admin ☐ Group Admin

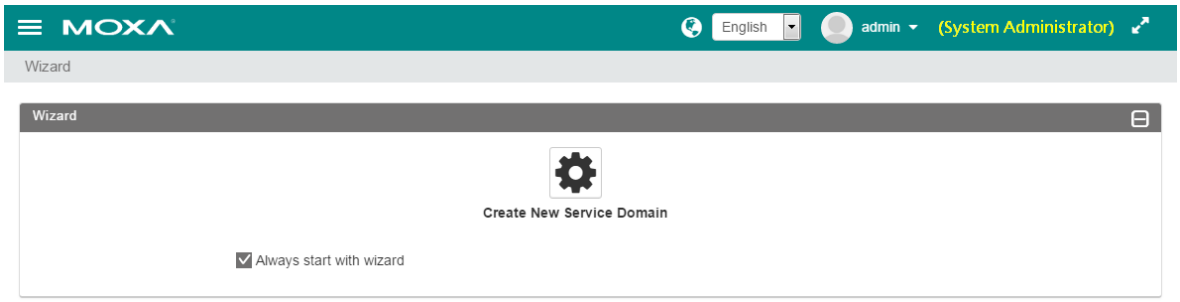
When logging into the MRC portal, it leads you to "Wizard" for quick settings.

The following topics are covered in this chapter:

- **Wizard–Creating a Service Domain and a Domain Administrator**
- **Service Domain Management**
- **Service Domain Status and Settings**
- **Service Domain Administrator Management**
- **Device Group Management**
- **Device Group Status and Settings**

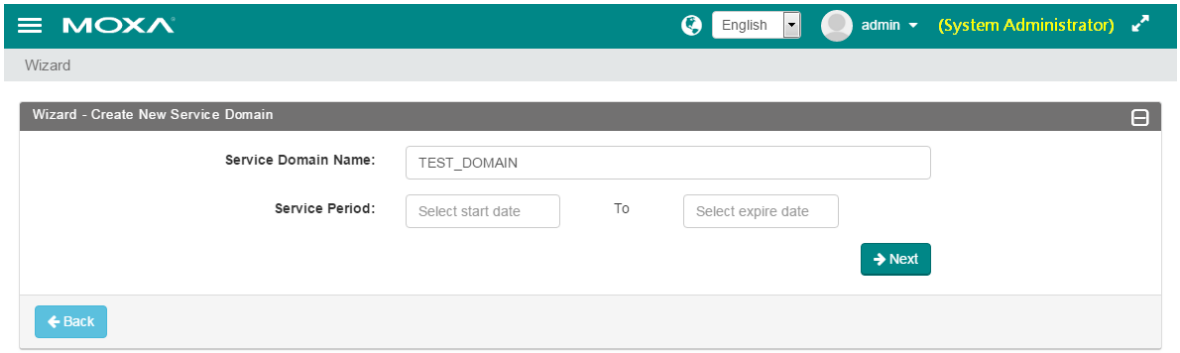
Wizard–Creating a Service Domain and a Domain Administrator

When logging into the MRC portal as system administrator, the portal leads users to the wizard page for creating new service domains. Users can uncheck the "Always start with wizard" to skip this page for the next time they login.



Click on  to start the wizard for creating a new service domain.

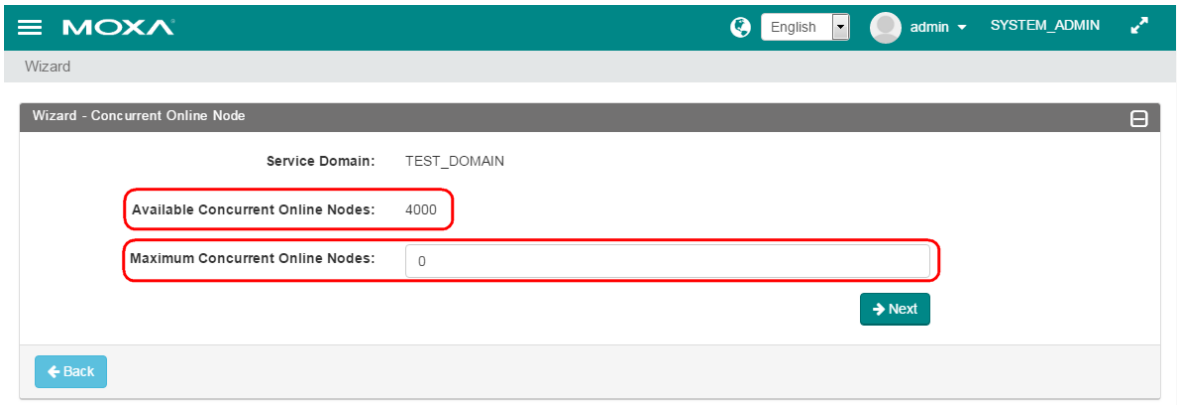
Step 1: Input the service domain name, and select the service period. The connectivity service will be available during the administrator-defined service period, and when the service expires, the service domain will stop the connectivity service until the system administrator changes the service period. At this moment, all of the remote connections are cut off. Leaving the "Service Period" empty enables the connectivity service to be available permanently. Then, click on "Next" for the next step.

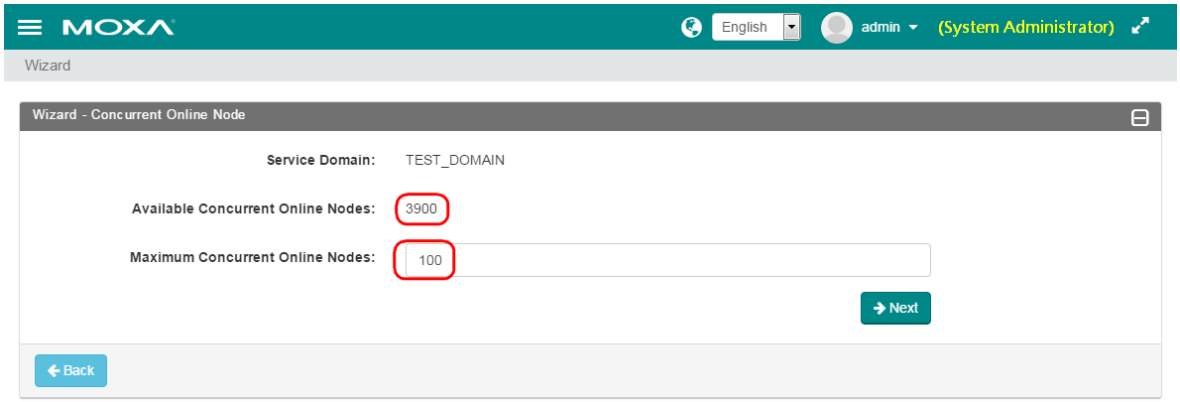


NOTE Once the service period expires, all the connections of the gateways and the clients in the groups of the domain will be cut off.

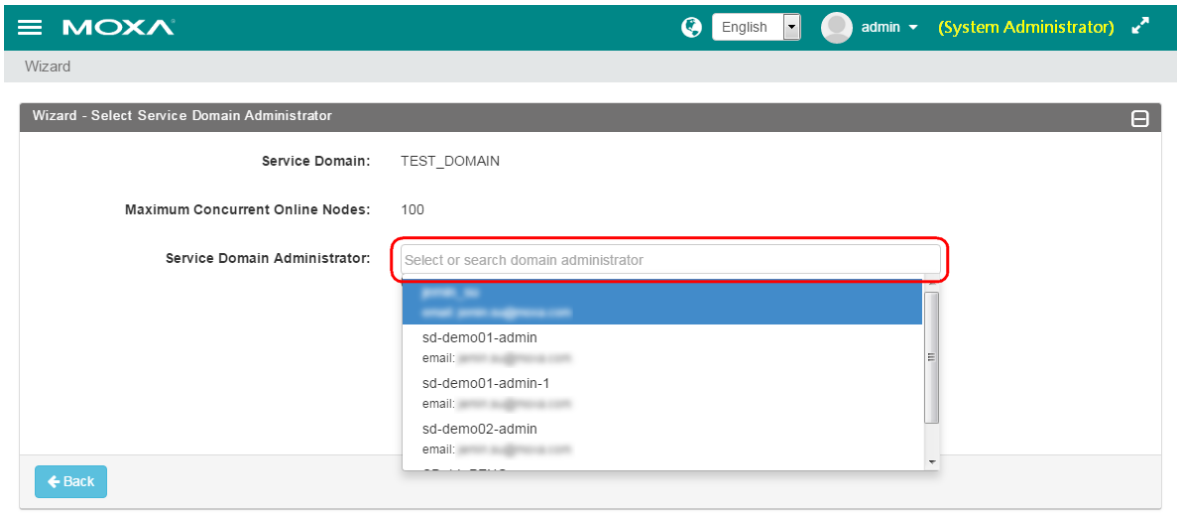
Step 2: Allocate the "Concurrent Online Nodes" capacity for the service domain. "Available Concurrent Online Nodes" means the current available resources you have in the system. After allocating the resources for the service domain, the system automatically deducts the number from the available resource right away. Then, click on "Next" for the next step.

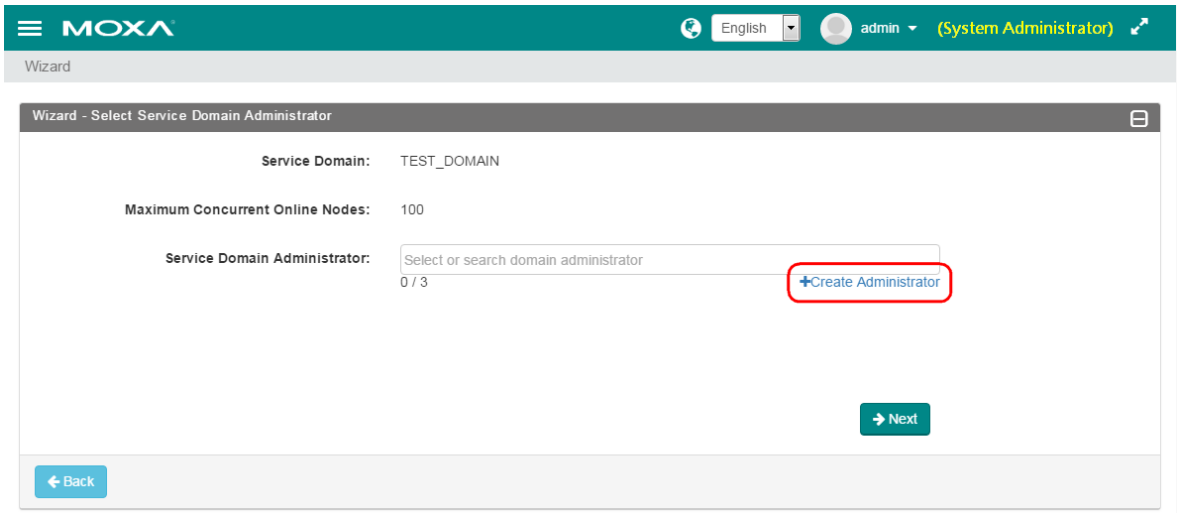
NOTE System Administrators can purchase a "MRC Server Node Upgrade" license to increase the amount of concurrent online node resources that can be used on the MRC Server.

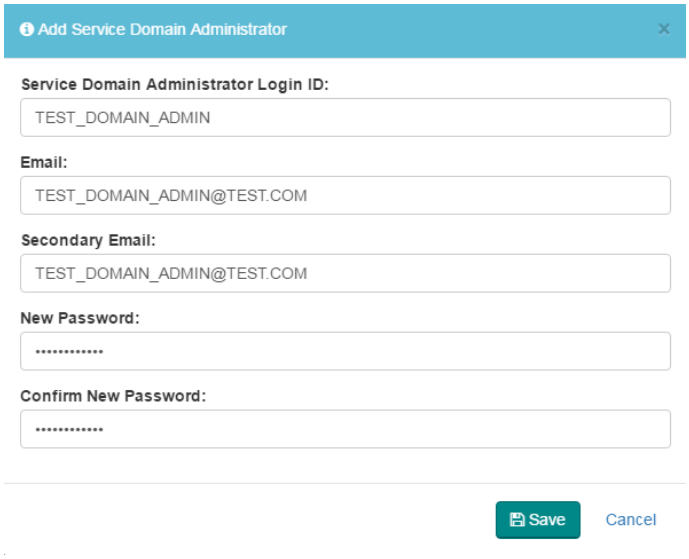




Step 3: Create or add a domain administrator for this service domain. Click on the blank to select one from the domain administrator list, or click on "Create Administrator" to create a new domain administrator for the service domain. One service domain can be assigned to multiple administrators for co-administration. Click on "Next" for the next step.



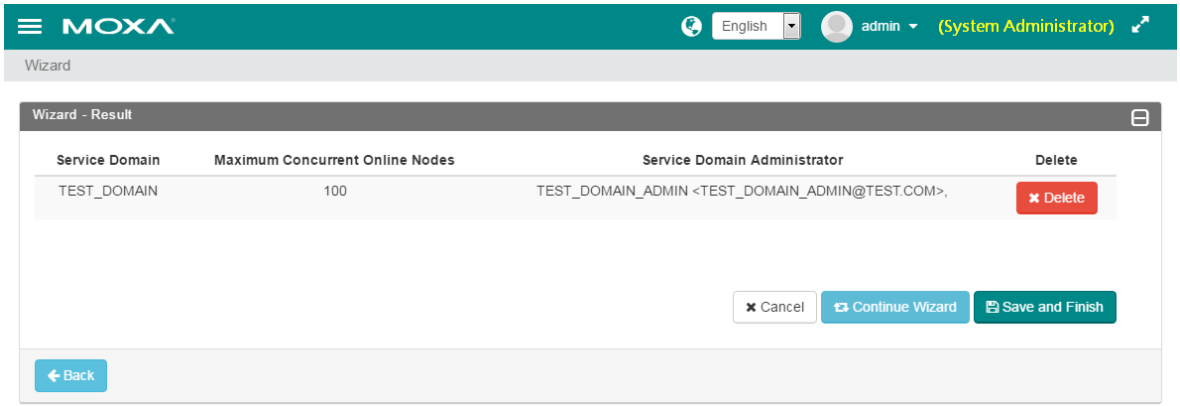




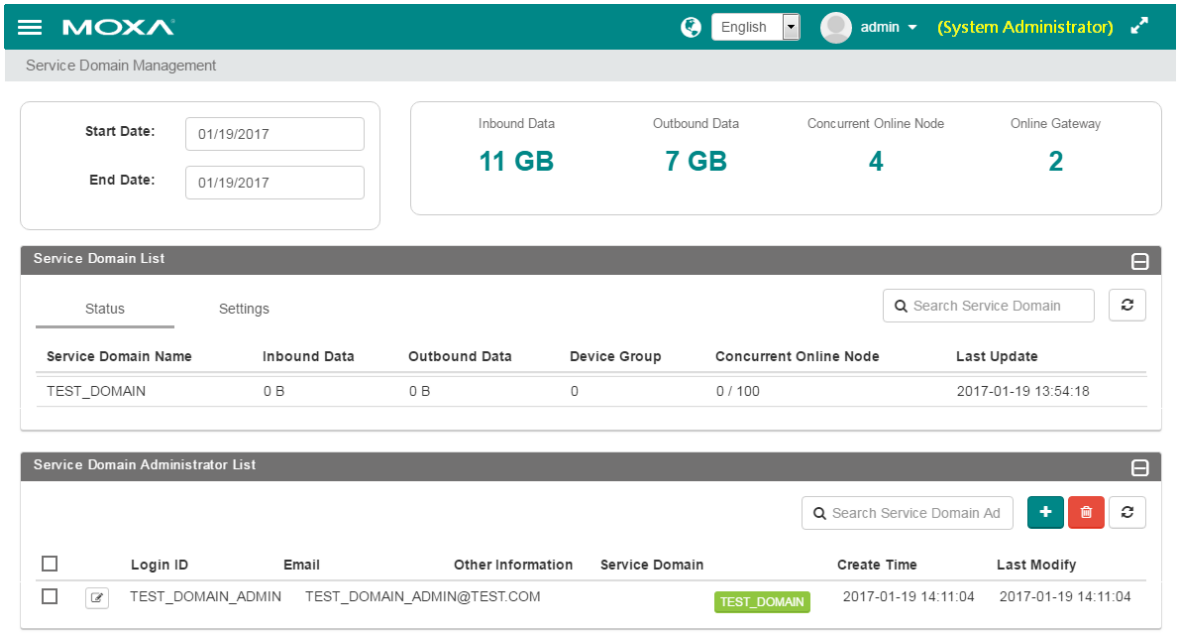
NOTE A maximum of 3 domain administrator accounts can be added for one domain.

Step 4: The system administrator can see the results of the wizard operation. Click "Continue Wizard" to continue creating multiple service domains or click "Save and Finish" to save the current configuration to the system. Click "Delete" to remove the unwanted item.

NOTE The temporary provision will not be saved in the system if users click on "Cancel" or jump to other pages before clicking "Save and Finish".

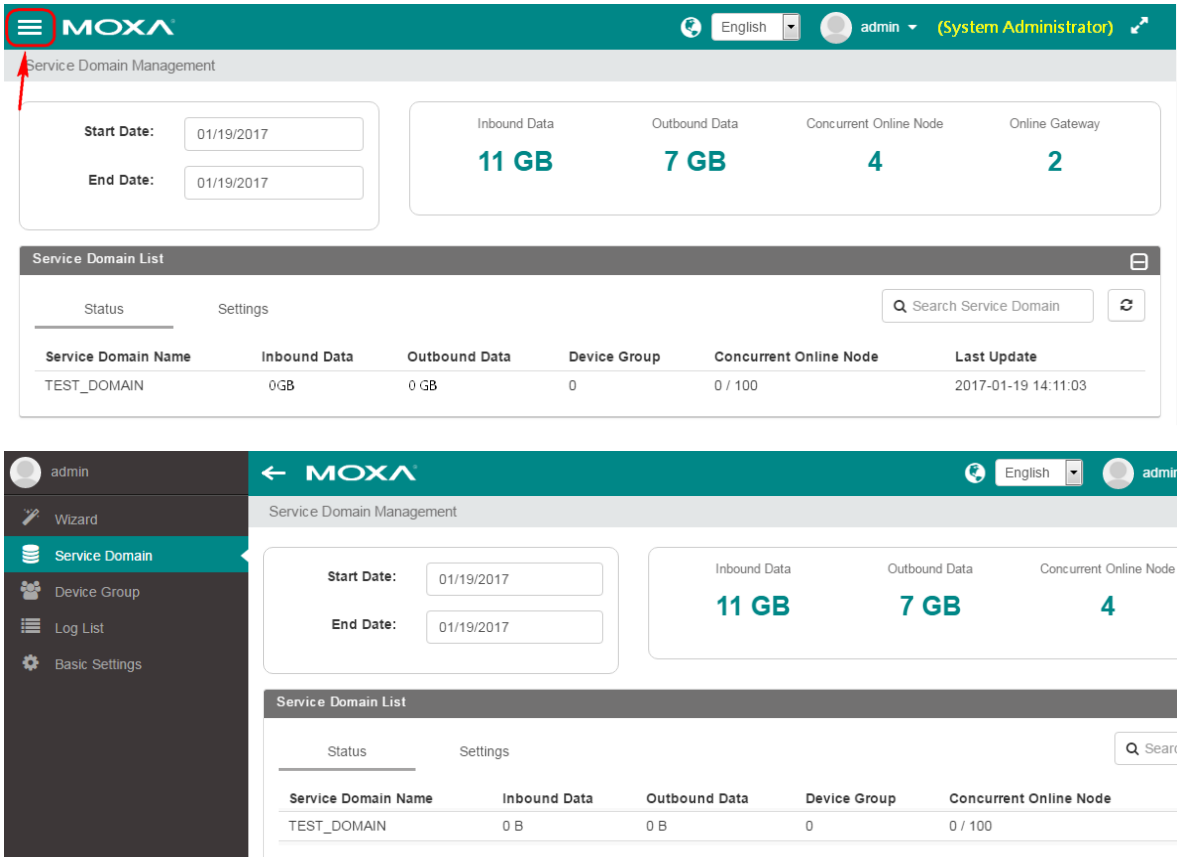


After the wizard, the system administrator will be redirected to the service domain management web page for the overview of the service domains and the domain administrators in the system. There is a dashboard of the data usage for this server system at the top of the web page.



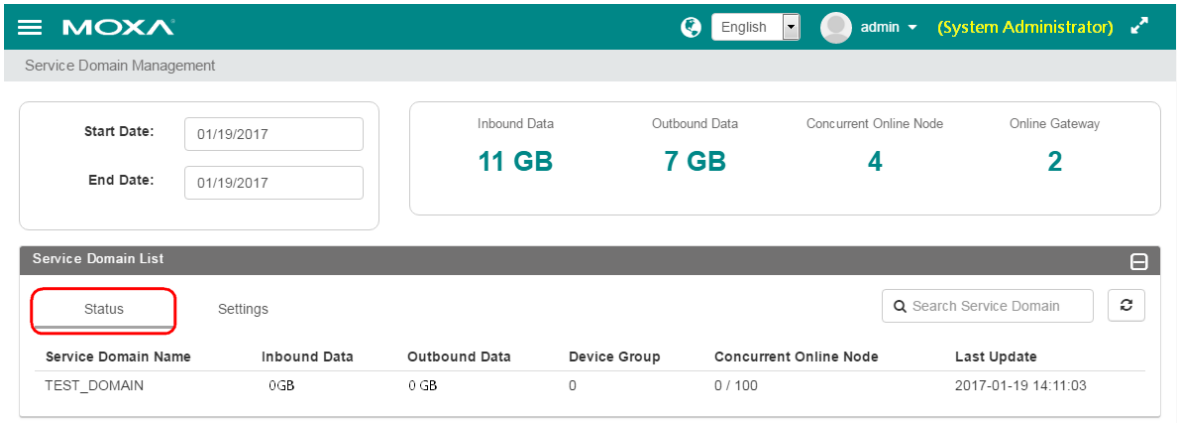
Service Domain Management

Click on the menu and choose the Service Domain for the service domain management.

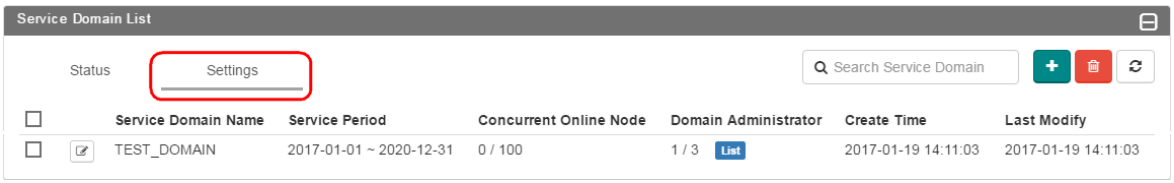


Service Domain Status and Settings

On the service domain management web page, click "Status" and to get the real-time status of the data usage, amount of device groups, and the available resource of the concurrent online nodes in this service domain.



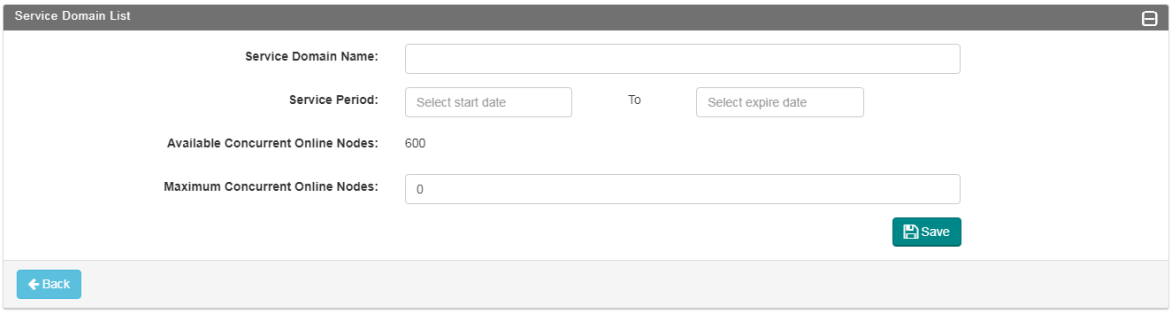
Click on "Settings" to add, delete, or modify a service domain.



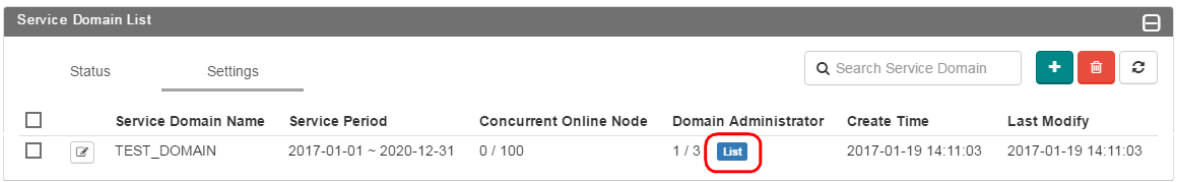
System administrators can click on to add a new service domain. Tick and select a service domain before clicking on to delete it. Click on to get the updated settings.

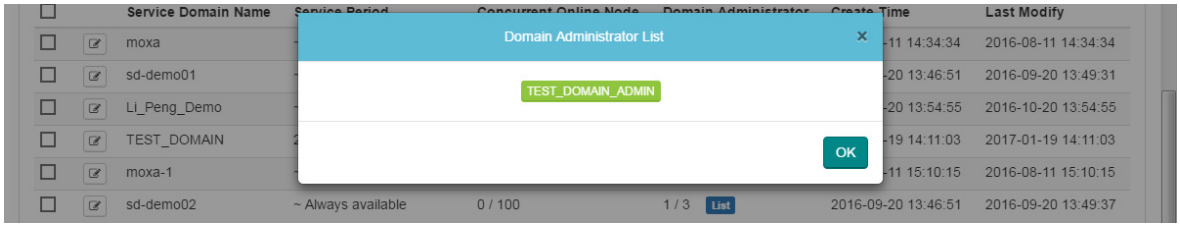
WARNING

Removing a service domain will also remove all the groups, gateways, and clients of the domain.

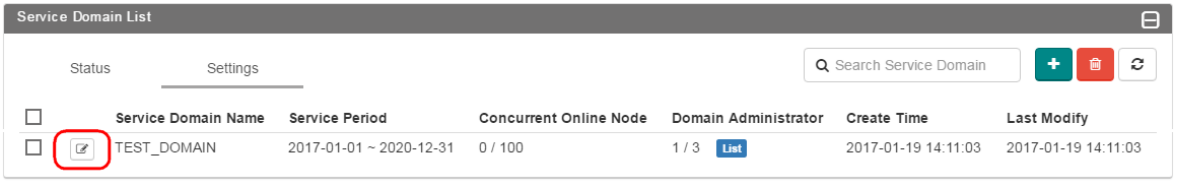


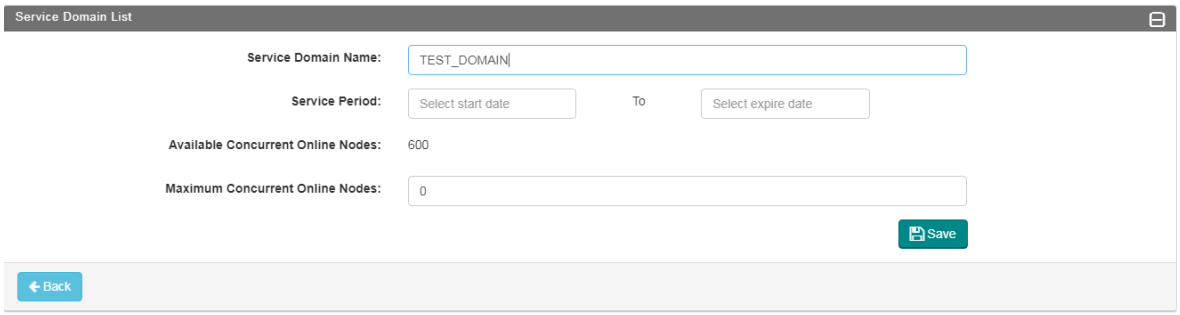
Click on List to get the domain administrator list of the service domain.





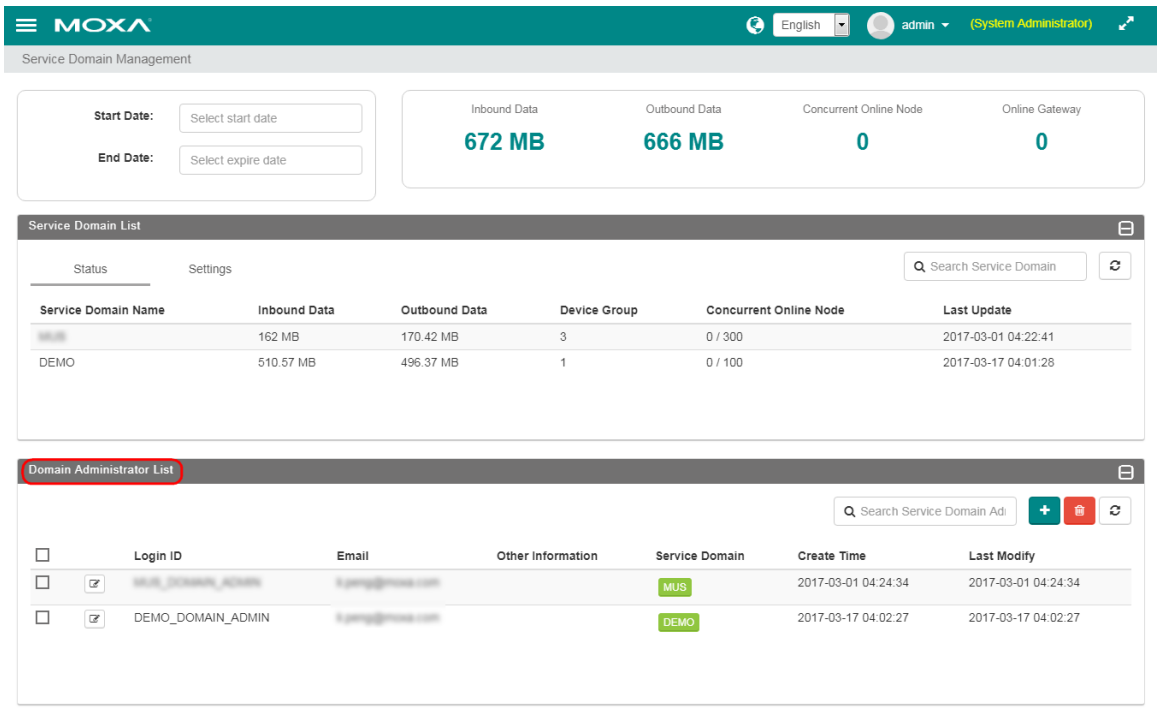
Click on  to modify the service period or the amount of allocated concurrent online node resources for each service domain.



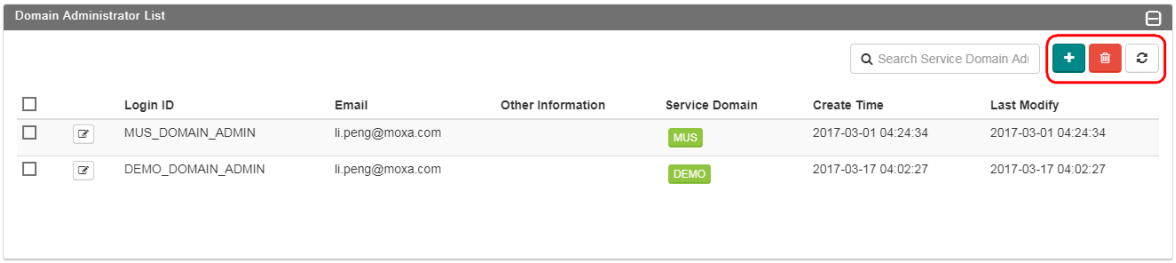


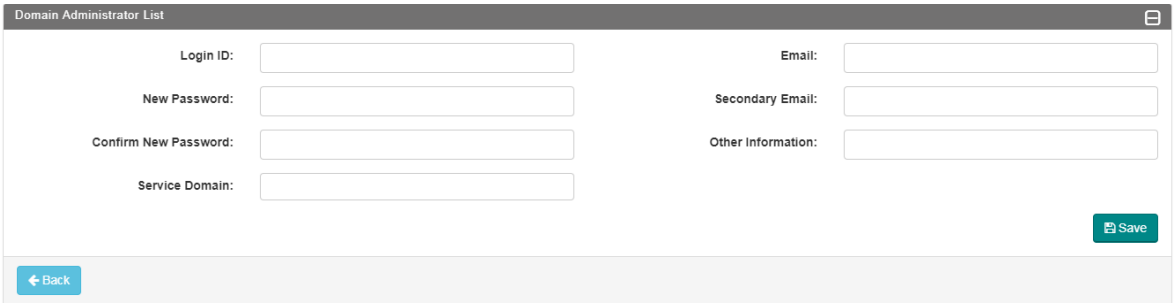
Service Domain Administrator Management

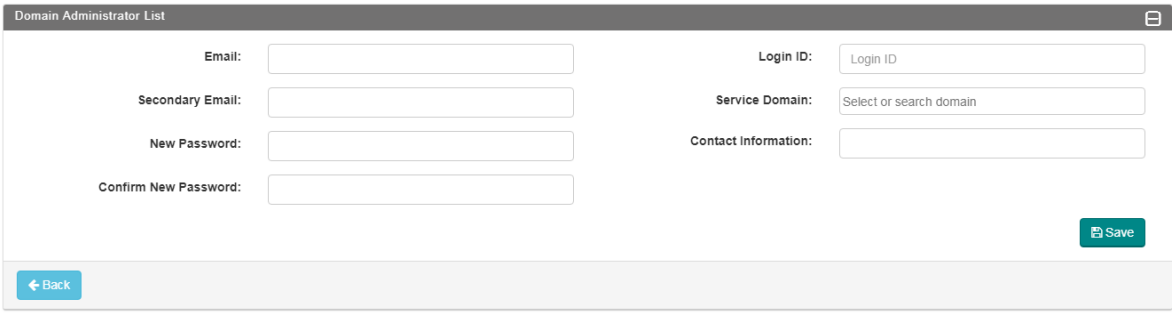
In the "Domain Administrator List", the system administrator can add and remove a domain administrator. The system administrator can also re-assign the domain administrators to different service domains.



Click on + for adding a new service domain administrator from here. Tick and select a service domain before clicking on to delete it. Click on to get the updated settings. Click the "EDIT" icon to modify the domain administrator settings.

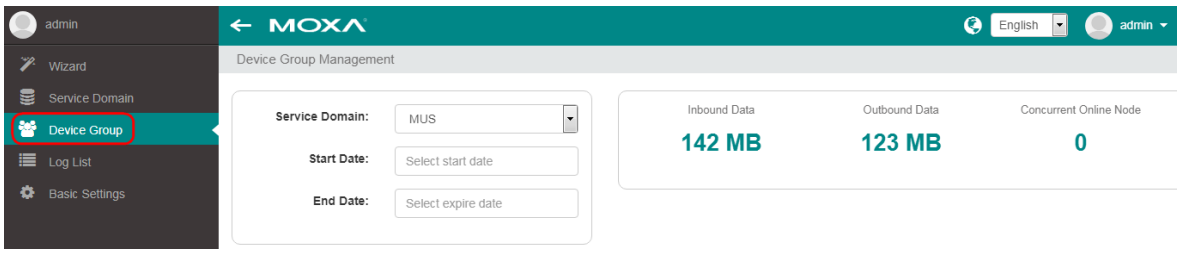


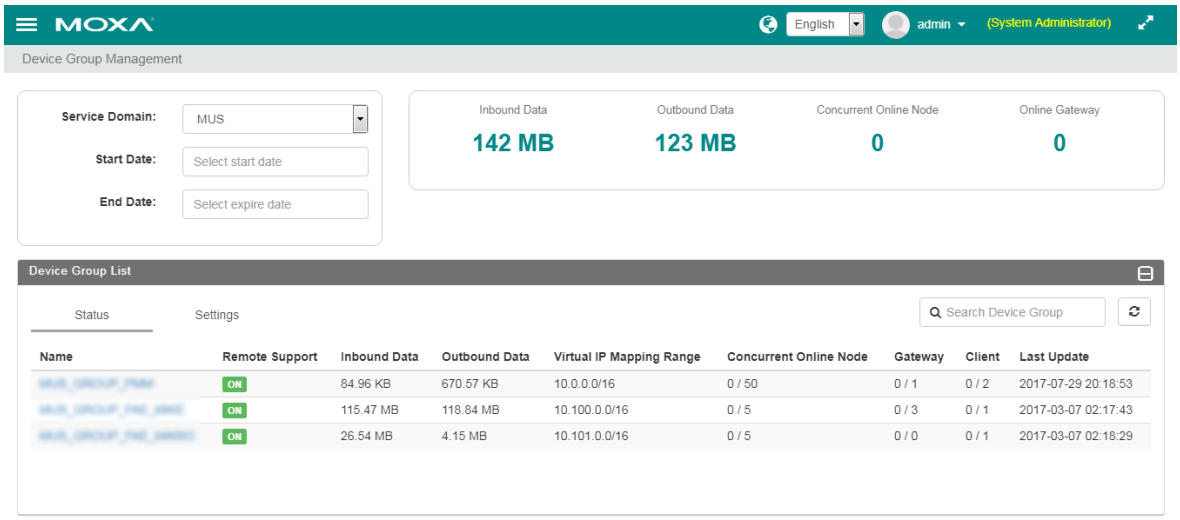




Device Group Management

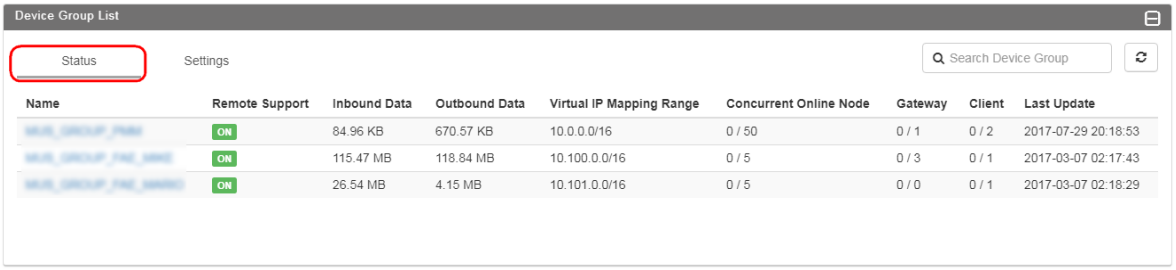
Click on "Device Group", the system administrators can look up the device group status and change the device group settings while the "Remote Support" function is enabled by the group administrator. Only "Remote Support"-enabled device groups are displayed in the device group management list under the system administrator.



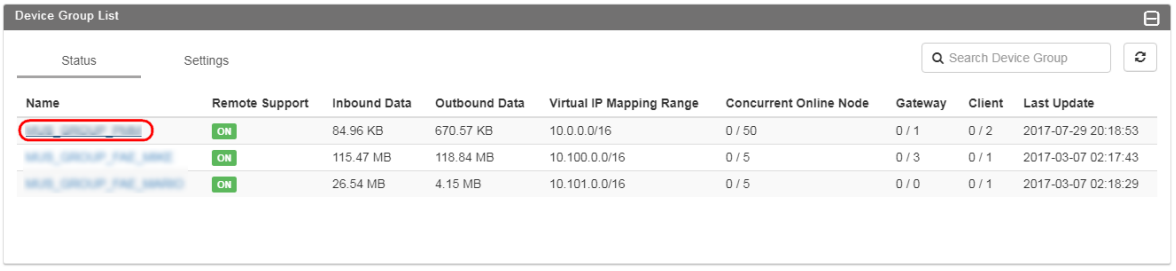


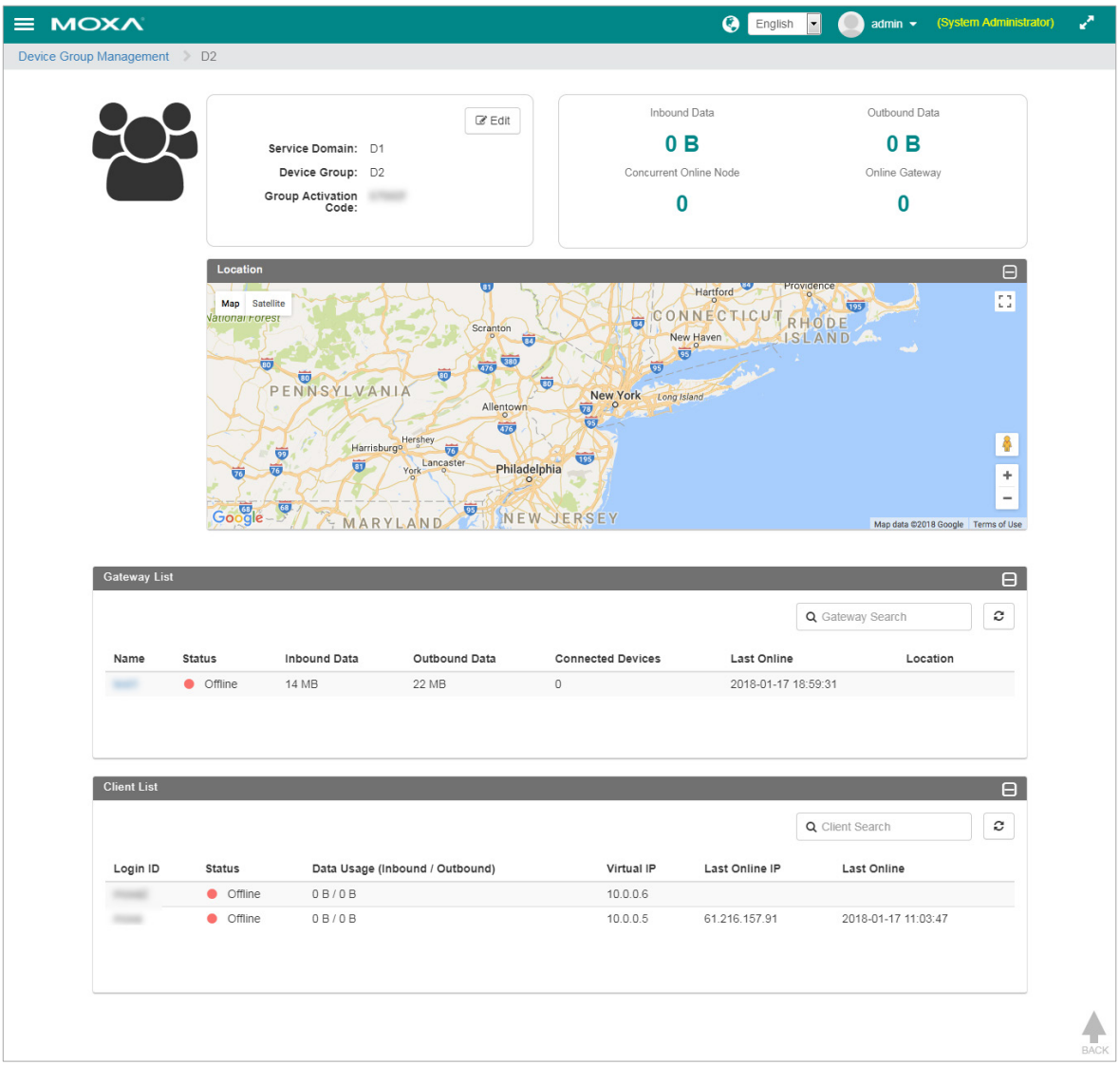
Device Group Status and Settings

Status: Click on "Status" to review the device group status of data usage and the concurrent online node usage. For example, "0/50" means that the total number of concurrent online nodes is 0 and the current allocated concurrent online node resource is 50.

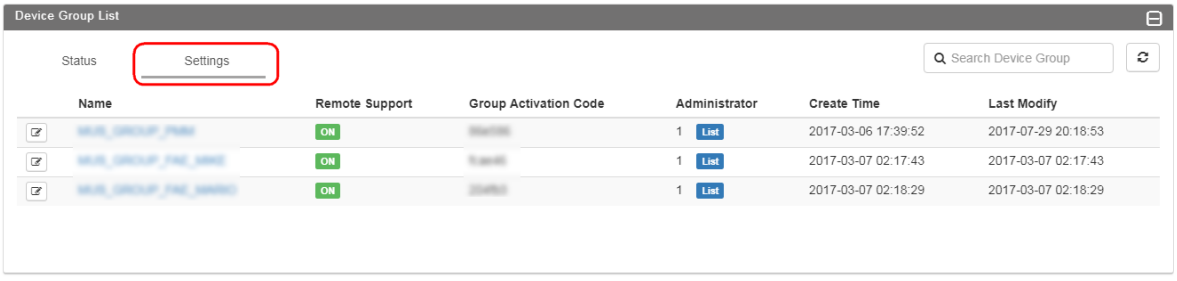


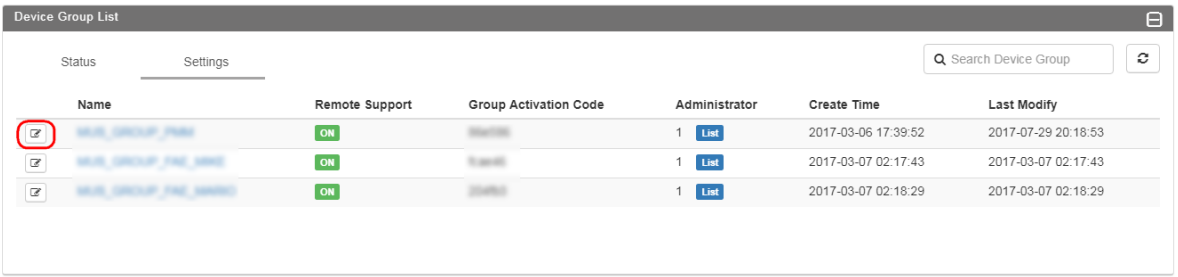
If the status of "Remote Support" of the group is ON (determined by the group administrator), then the domain administrator can click on the name of the device group and get more detailed information of the group.

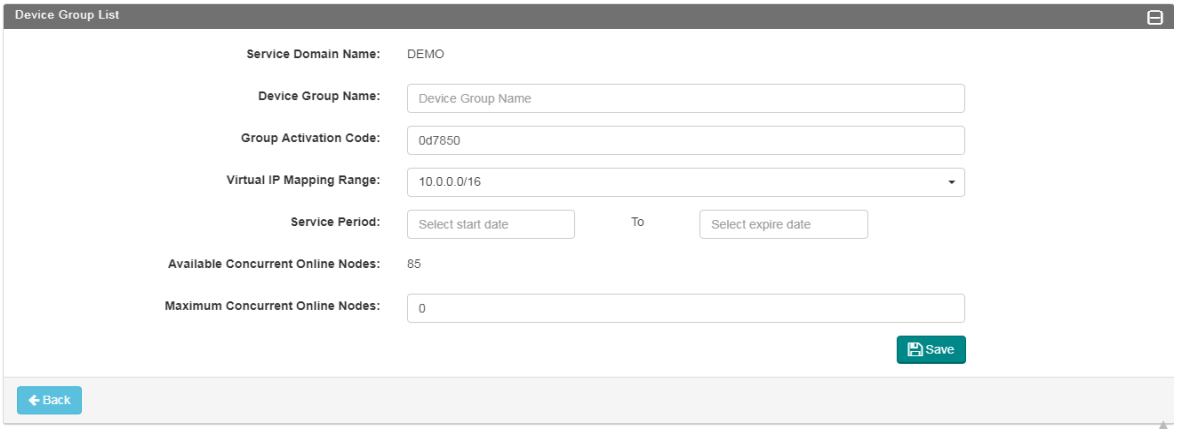




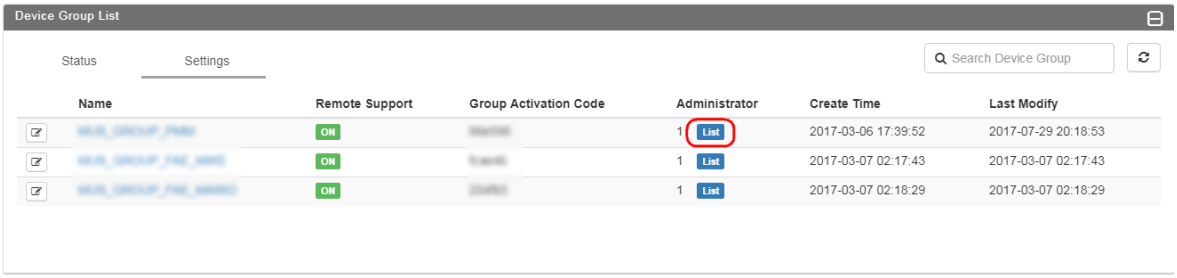
Settings: Click on "Settings" and  to modify the Device Group's settings including name, service period, and the allocated concurrent online node resource.

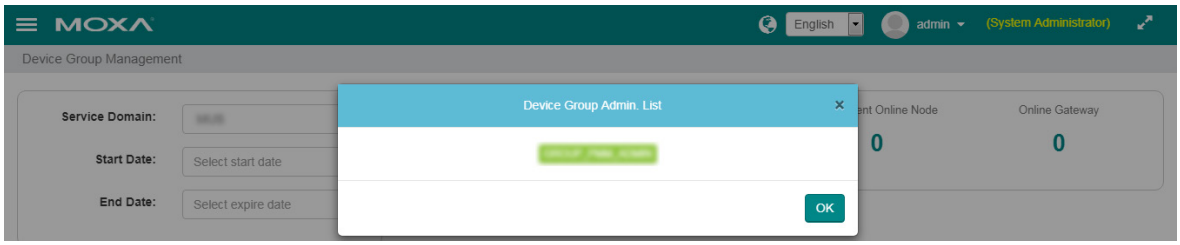






Click on **List** to get the group administrator list of the device group.





6

Log in as Service Domain Administrator

Allowed Privilege: ☐ System Admin ☑ Domain Admin ☐ Group Admin

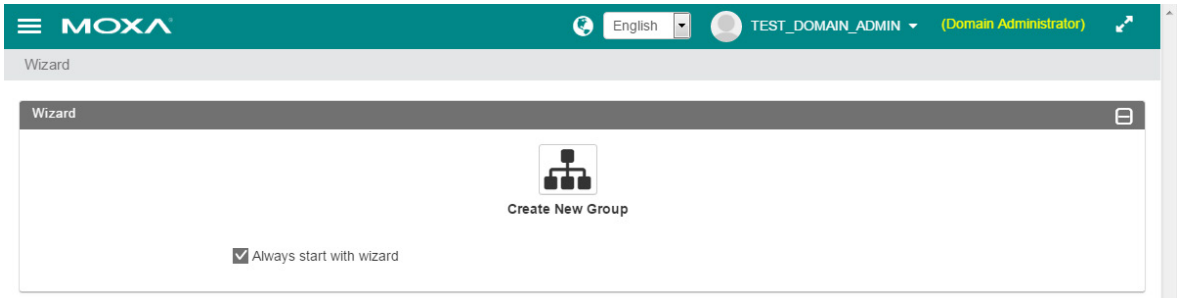
When logging into the MRC portal, it leads you to wizard page for quick settings.

The following topics are covered in this chapter:

- **Wizard–Creating a Device Group and a Group Administrator**
- **Service Domain Management**
- **Service Domain Status and Settings**
- **Service Domain Administrator Management**
- **Device Group Management**
- **Device Group Status and Settings**
- **Device Group Administrator Management**

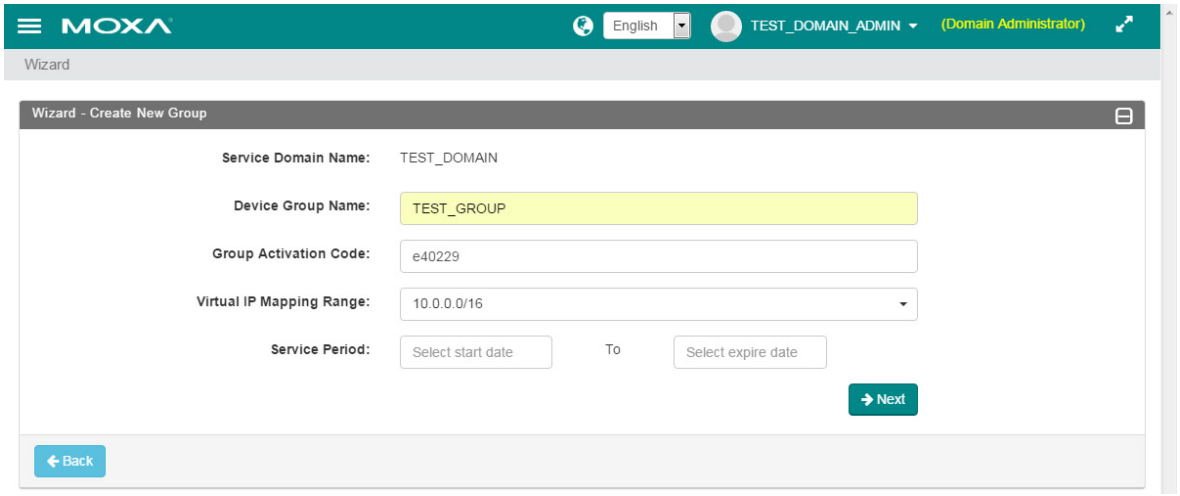
Wizard–Creating a Device Group and a Group Administrator

When logging into the MRC portal as domain administrator, the portal leads users to the wizard page for creating new device groups. Users can uncheck the "Always start with wizard" to skip this page for the next time they login.



Click on  to start the wizard for creating a new device group.

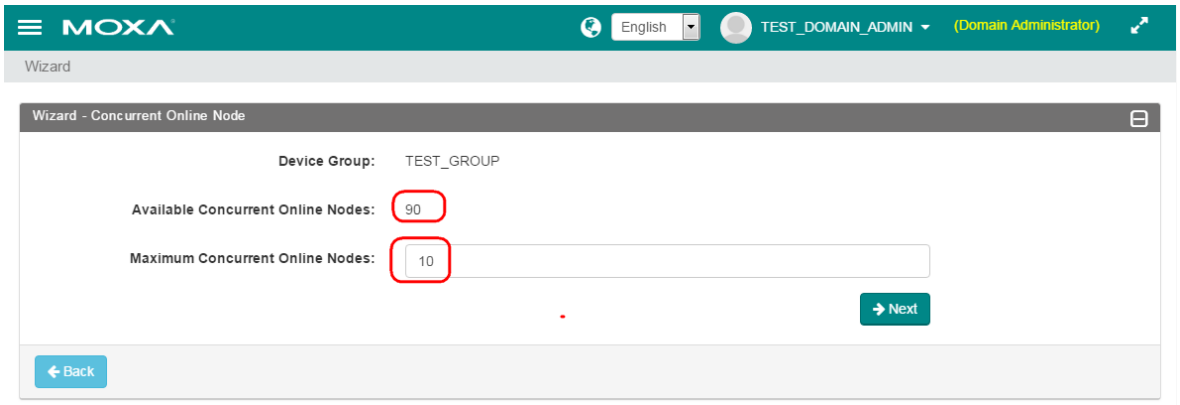
Step 1: Input the device group name, and choose the designated virtual IP mapping range for the MRC gateways, field local machines, and MRC clients, then, select the service period for the device group. The connectivity service will be available during the service period defined by the system administrator, and when the service expires, the device group will stop the connectivity service until the service domain administrator changes the service period. At this moment, all of the remote connections are cut off. Leaving the date empty means the connection is available permanently. Then, click on "Next" for the next step.



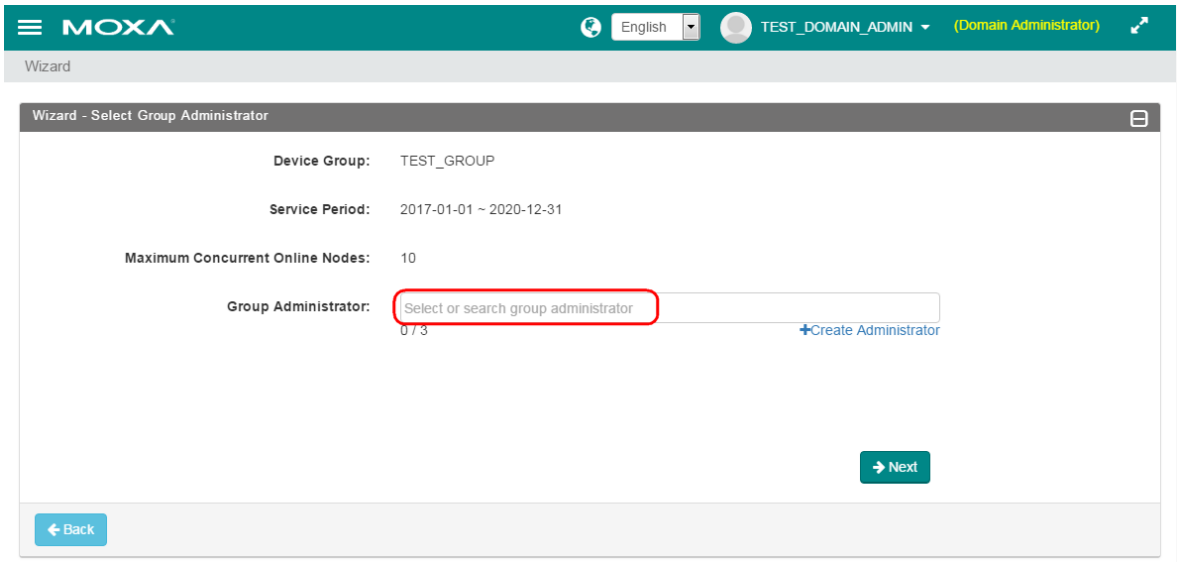
NOTE The Group Activation Code is used for authenticating the manually registered MRC gateway from local web management console.

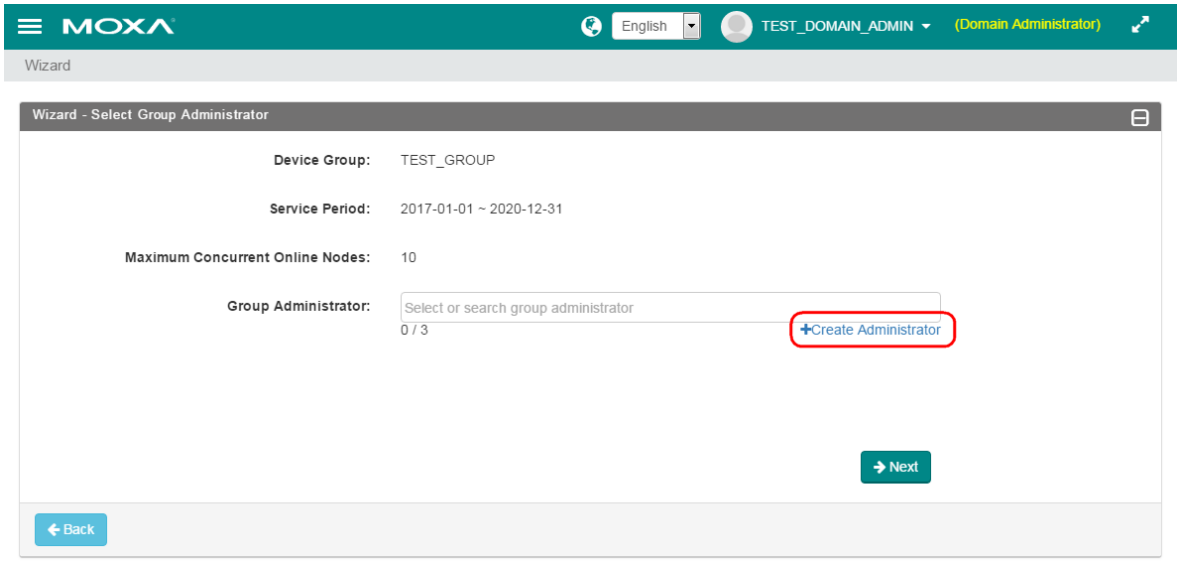
Step 2: Allocate the "Concurrent Online Nodes" capacity for the device group. "Available Concurrent Online Nodes" means the current available resources you have in the system. After allocating the resources for the device group, the system automatically deducts the number from the available resource right away. Then, click on "Next" for the next step.

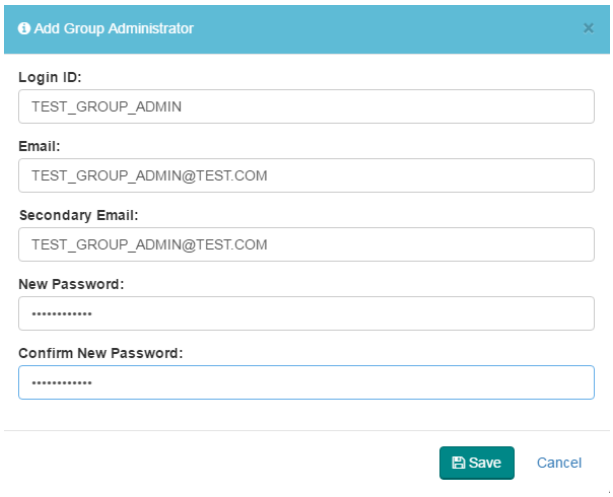
NOTE The resource of "Concurrent Online Node" is controlled by System Administrator, who can purchase extra and install if necessary.



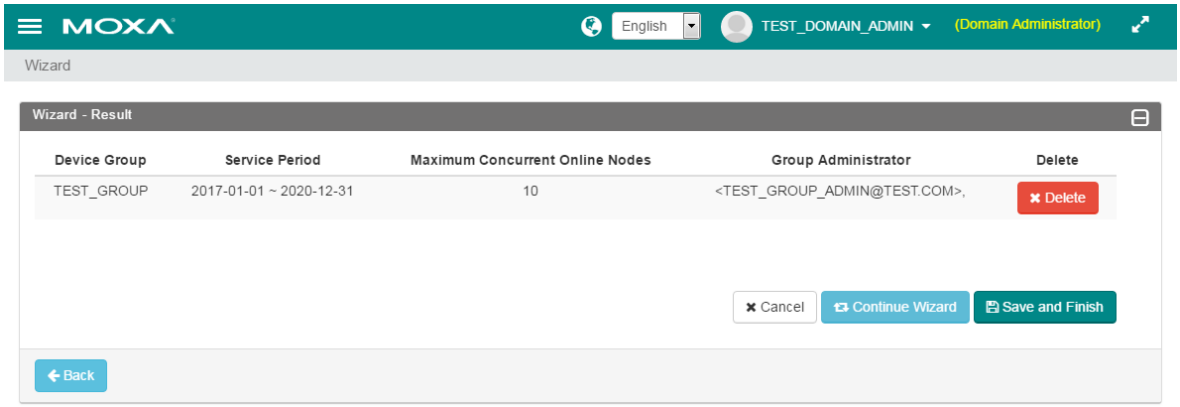
Step 3: Create or add a device group administrator for this device group. Click on the blank to select one from the group administrator list, or click on "Create Administrator" for creating a new group administrator for the device group. One device group can be assigned with multiple administrators. Click on "Next" for the next step.



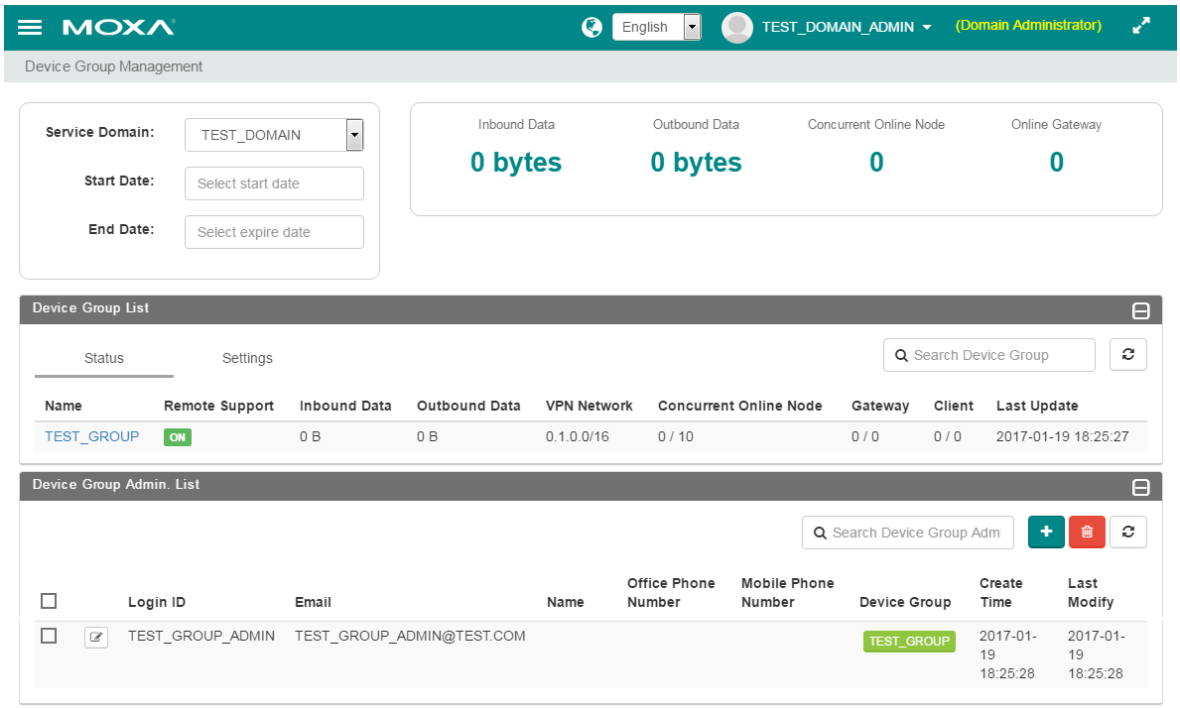




Step 4: The domain administrator can see the result of the wizard operation and choose "Continue Wizard" to create multiple device groups or "Save and Finish" to save the current configuration to the system. The domain administrator can also delete unwanted service domains from the list before saving the list into the system.

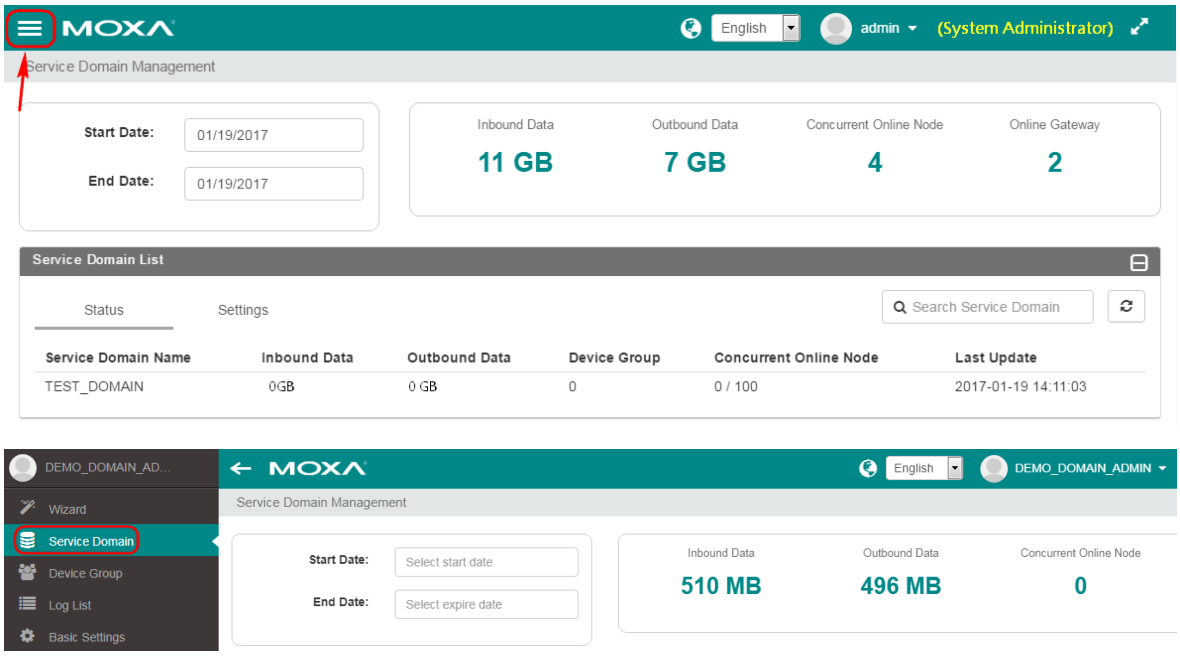


After the wizard, the domain administrator will be redirected to the device group management web page for the overview of the device groups and the group administrators in the service domain. There is a dashboard of the data usage for this service domain at the top of the web page.



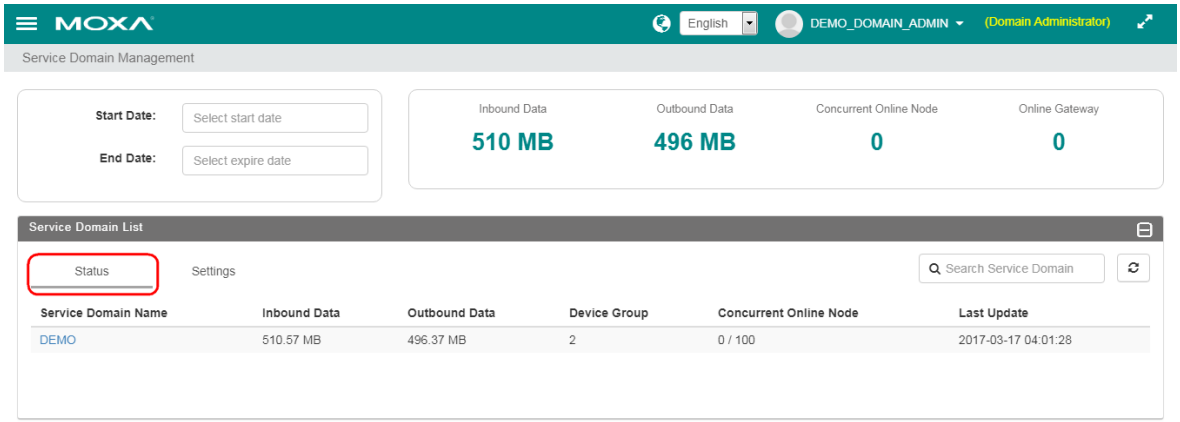
Service Domain Management

Click on the menu and choose the Service Domain for the service domain management.

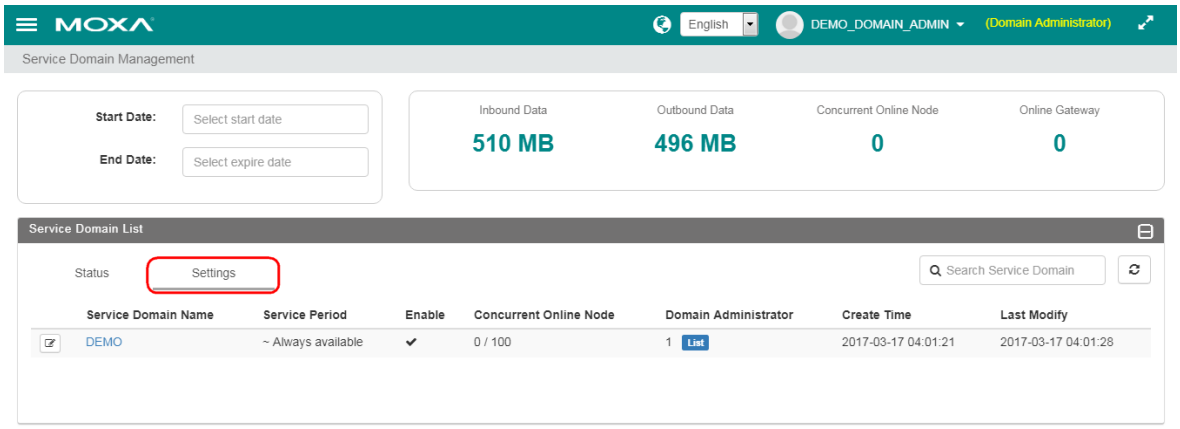


Service Domain Status and Settings

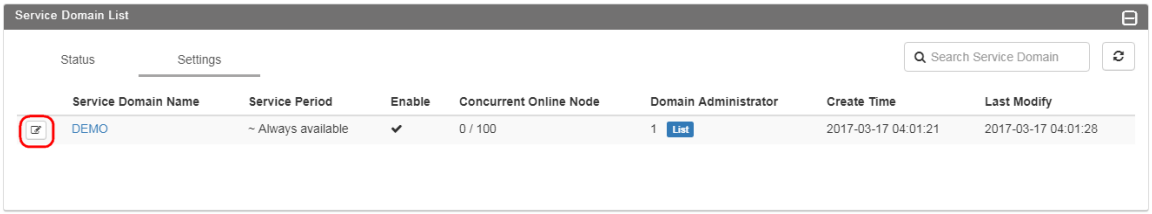
Status: On the service domain management web page, click "Status" and to get the real-time status of the data usage, amount of device groups, and the available resource of the concurrent online nodes in this service domain. For example, "0/100" means the total number of concurrent online nodes is 0 and the current allocated concurrent online node resource is 100.


MOXA
English
DEMO_DOMAIN_ADMIN
(Domain Administrator)
Service Domain Management
Start Date:
Select start date
End Date:
Select expire date
Inbound Data
510 MB
Outbound Data
496 MB
Concurrent Online Node
0
Online Gateway
0
Service Domain List
Status
Settings
Search Service Domain
Service Domain Name
Inbound Data
Outbound Data
Device Group
Concurrent Online Node
Last Update
DEMO
510.57 MB
496.37 MB
2
0 / 100
2017-03-17 04:01:28

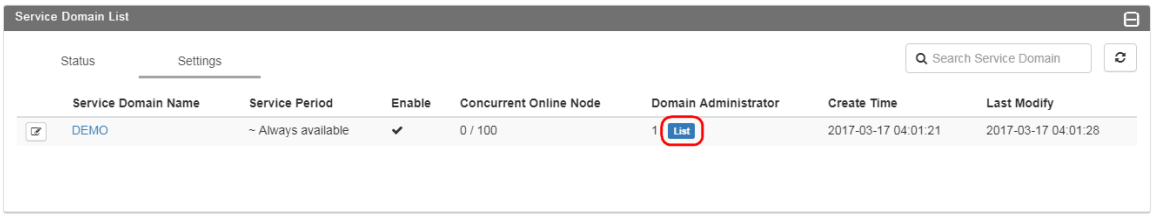
Settings: Click on "Settings" to review the connectivity service period, the account activation status, and the concurrent online nodes usage of the service domain.

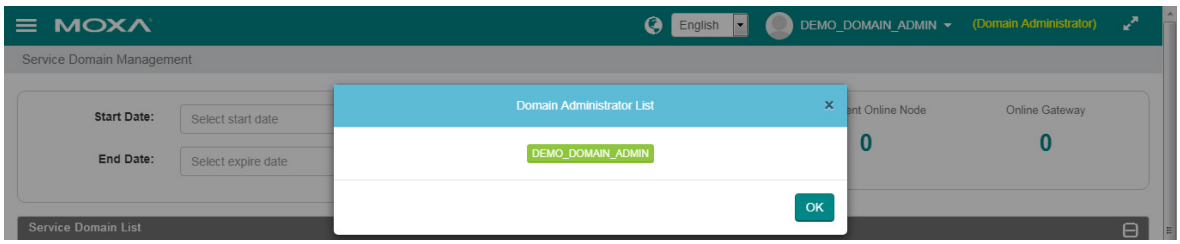


Click on  to change the "Remote Support" settings. Then, click "Save". Enabling the "Remote Support" feature allows upper layer administrators to manage the domain if the domain administrator encounters any problems. Disabling the "Remote Support" feature prevents any other authority from managing the domain except the domain administrator.



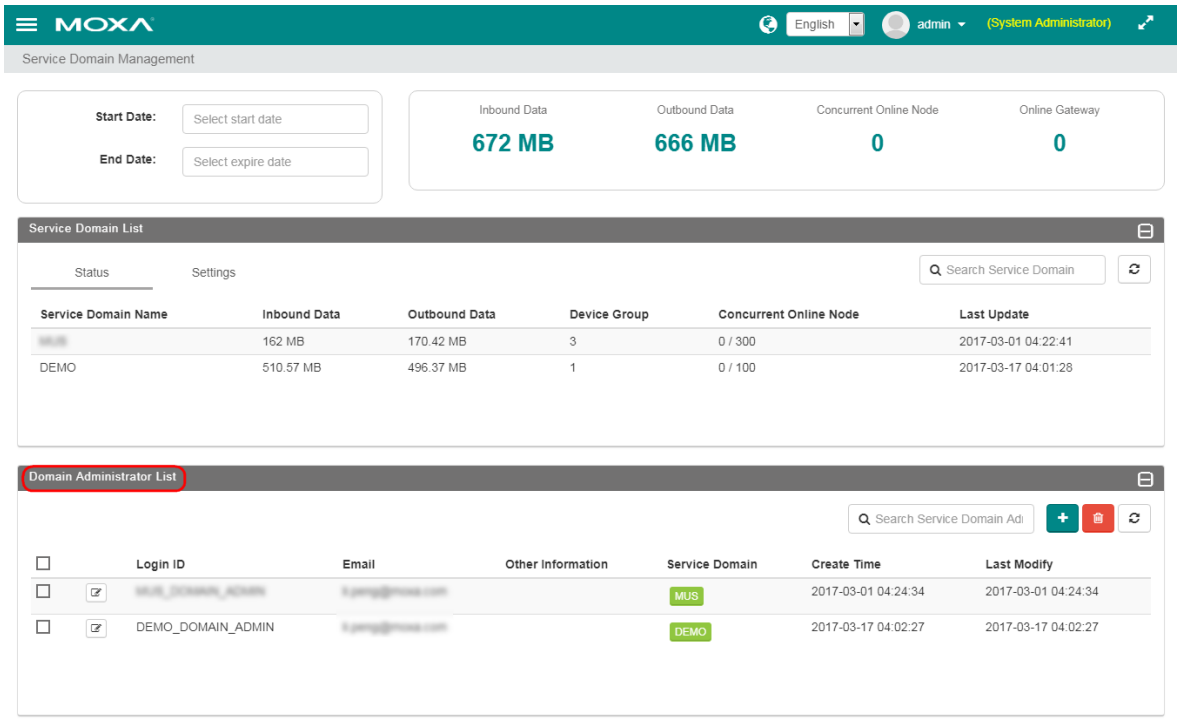
Click on  to get the domain administrator list of the service domain.



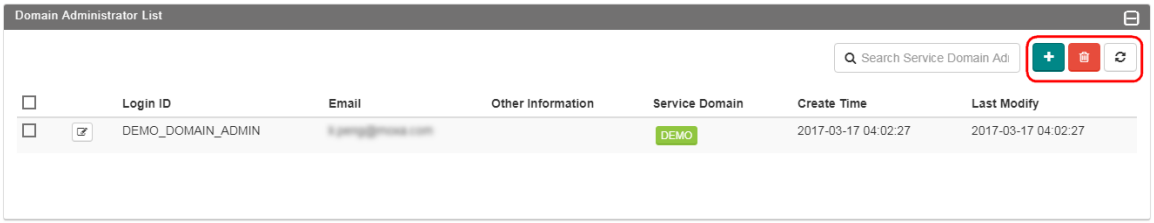


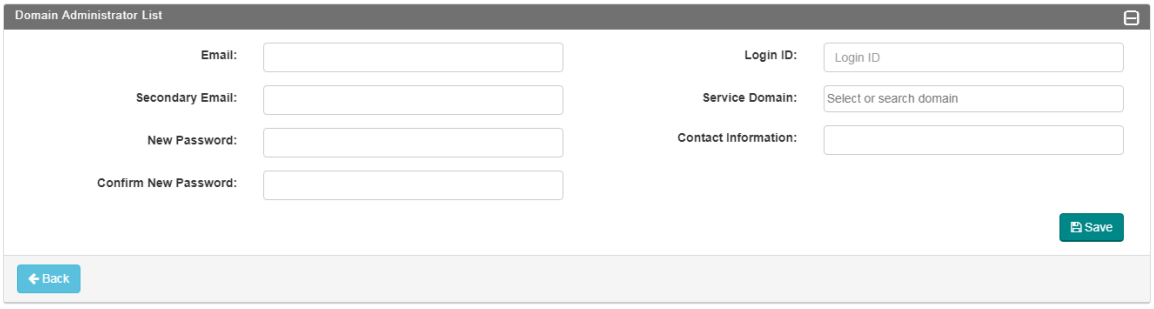
Service Domain Administrator Management

The domain administrator can add or remove additional domain administrators for co-management.



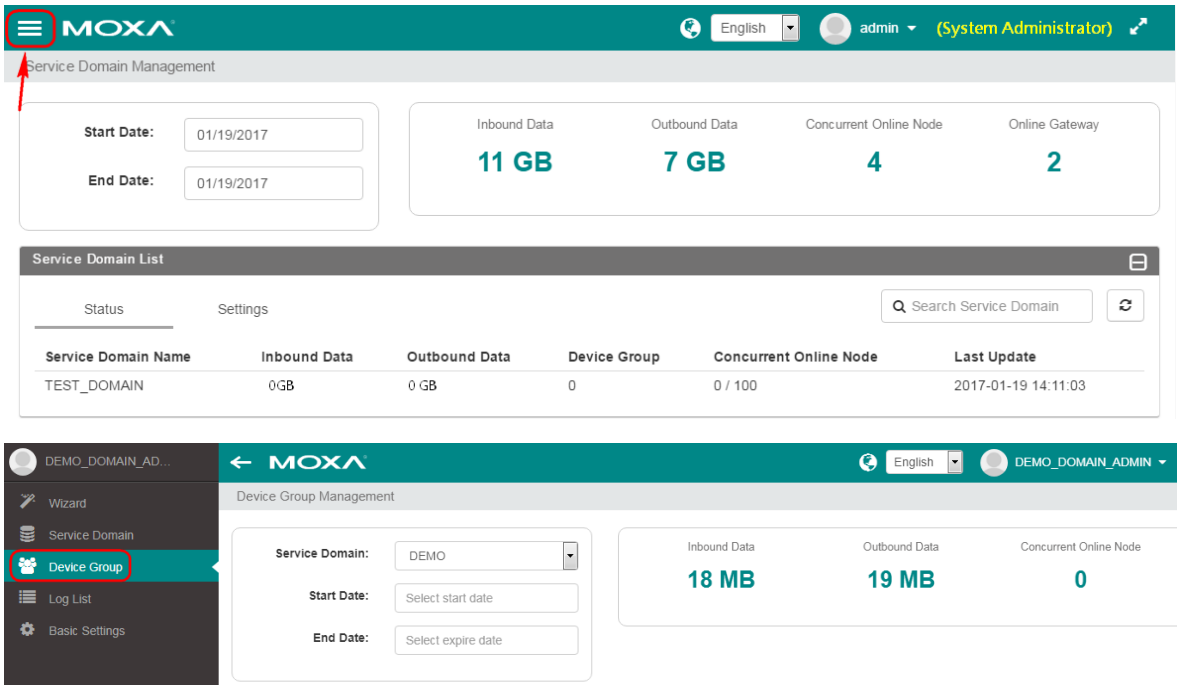
Click  to add a new service domain administrator. Tick and select a service domain administrator before clicking on  to delete it. Click on to get updated settings.





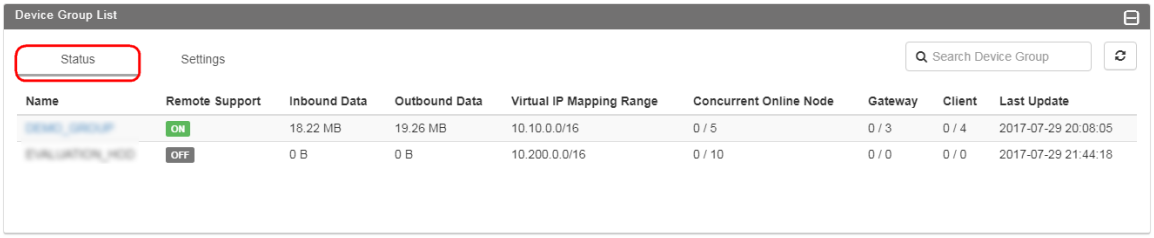
Device Group Management

Click on the menu and choose Device Group in order to perform device group management.

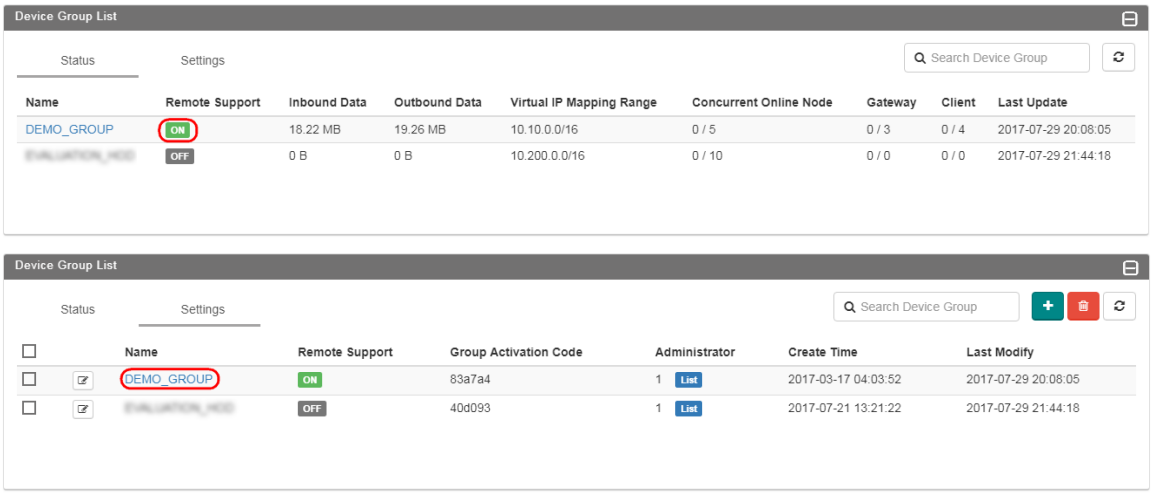


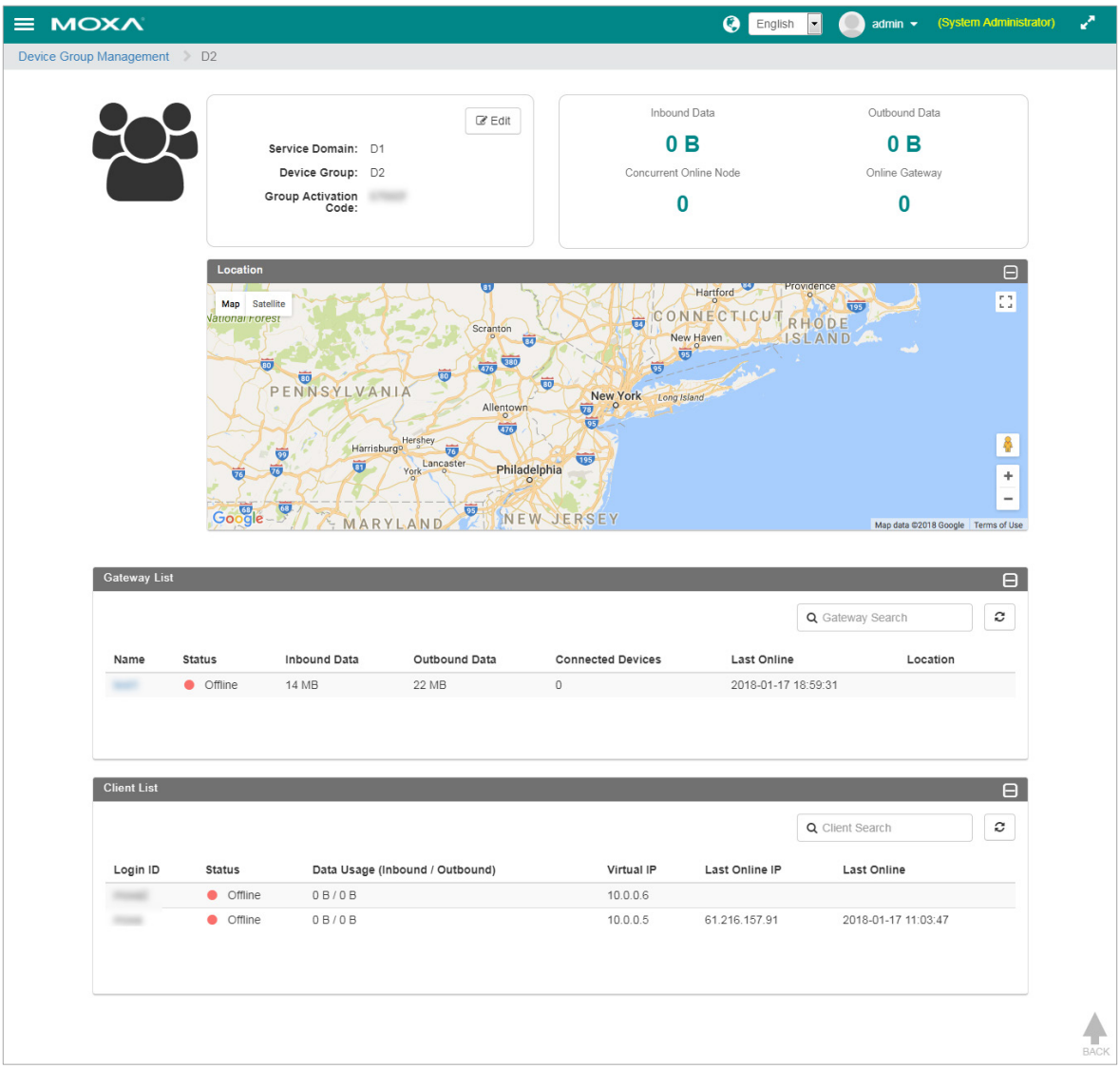
Device Group Status and Settings

Status: Click "Status" to review the device group status of data usage, the allocated virtual IP Mapping range, and the concurrent online node usage. For example, "0/5" means the total number of concurrent online node is 0 and the current allocated concurrent online node resource is 5.



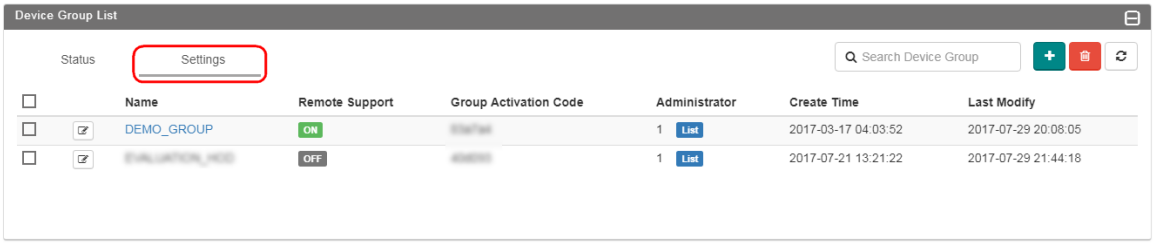
Only when the status of "Remote Support" of the group is ON (defined and set up by the group administrator), the domain administrator can click on the name of the device group and get more detailed information for troubleshooting.





NOTE "Group Activation Code" allows users to activate a MRC gateway manually via a local web console or sign in a client manually via the MRC Client software.

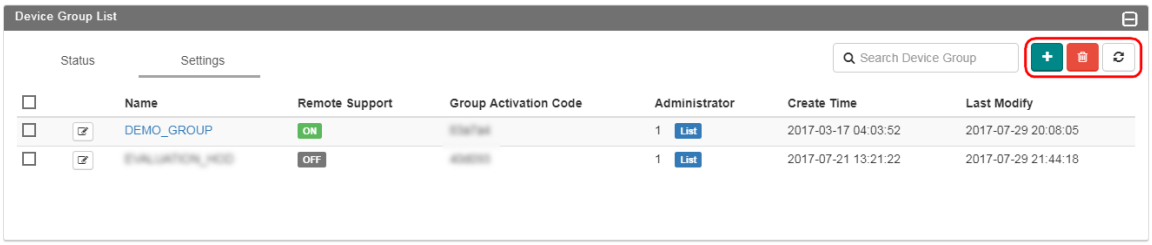
Settings: Click "Settings" to add or remove device groups.

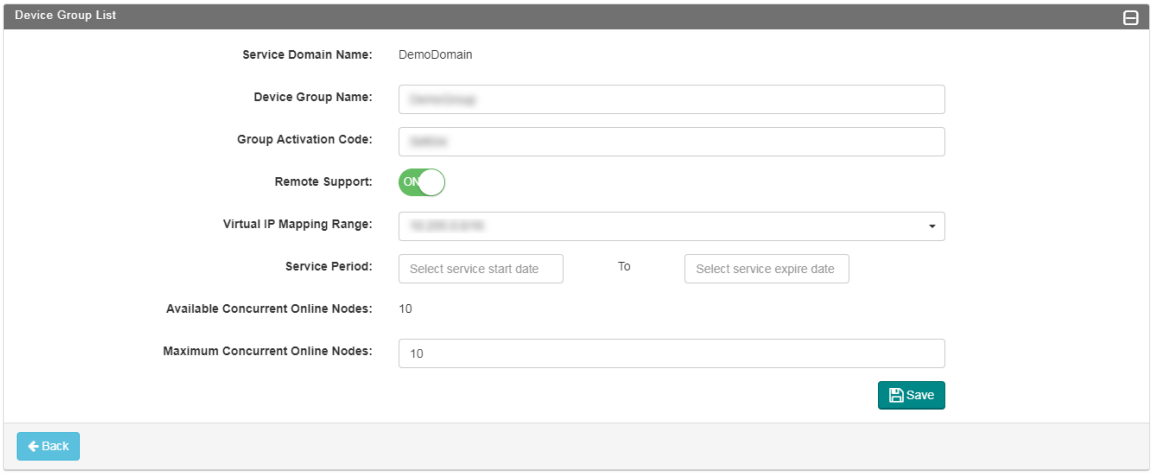


Click + to add a new service domain from here. Tick and select a service domain before clicking 🗑 to delete it. Click ↻ to get updated settings.

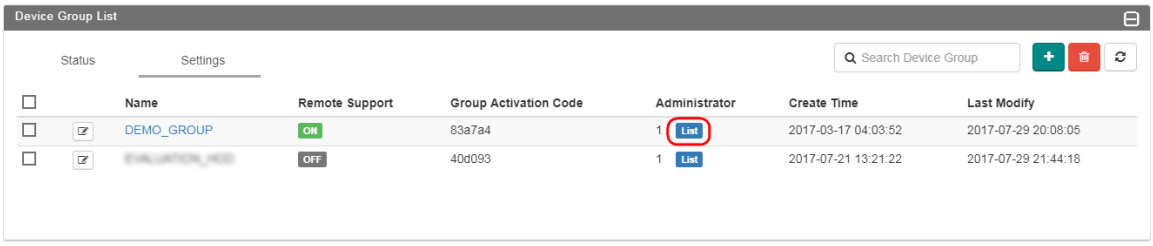
WARNING

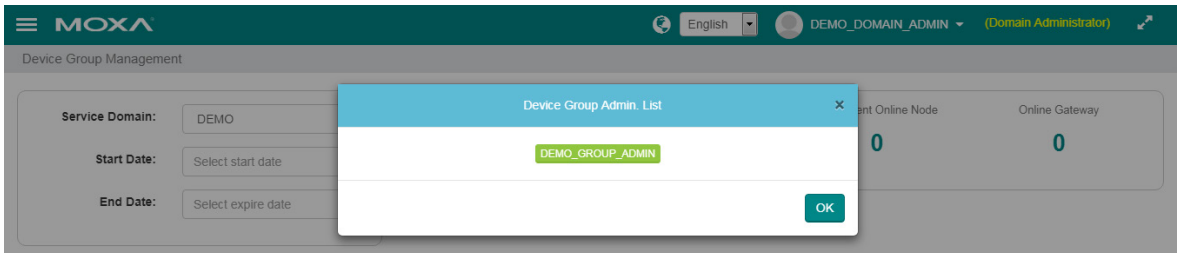
Removing a device group will also remove the gateways and clients that belonged to the device group.



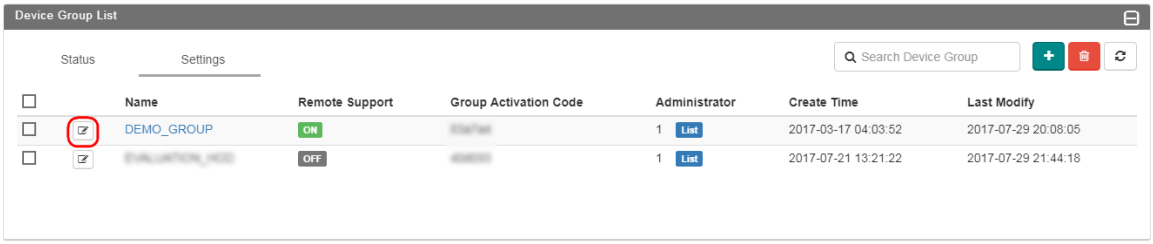


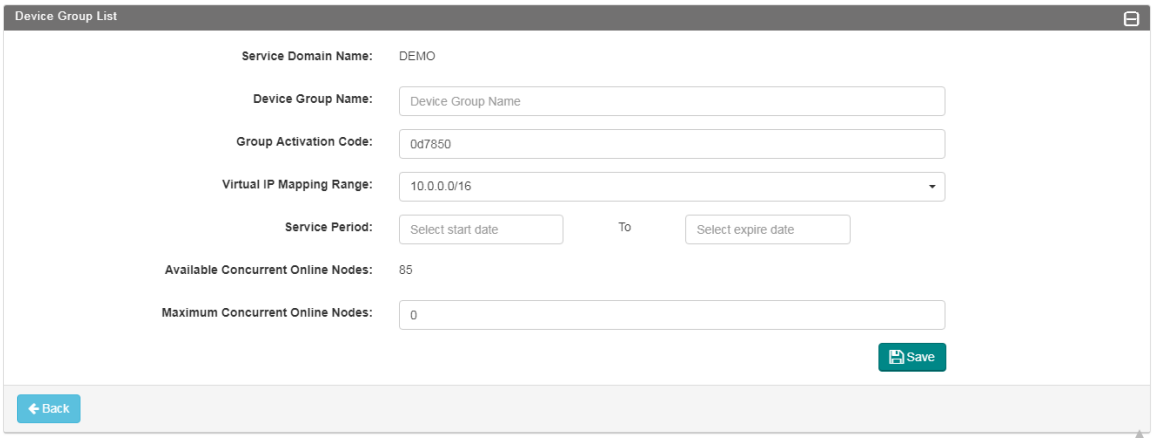
Click **List** to get the group administrator list of the device group.





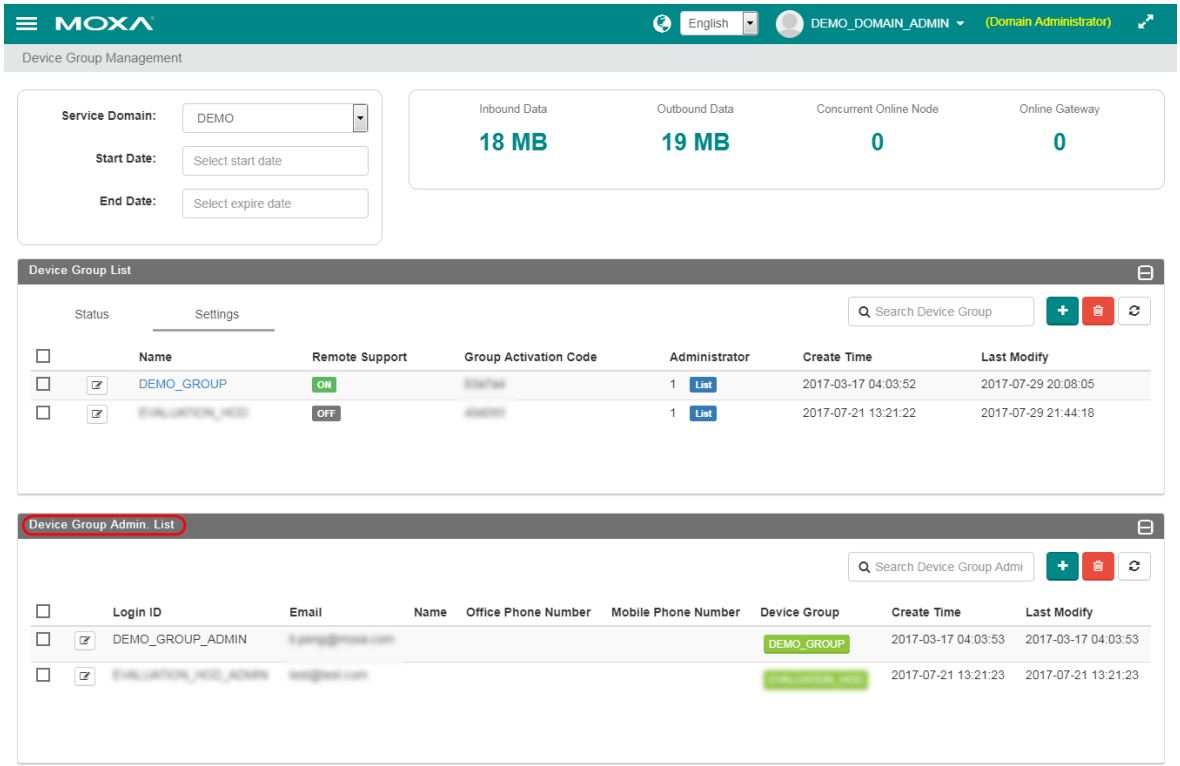
Click  to modify the group name, group activation code, service period, and allocated concurrent online node resource for each device group.



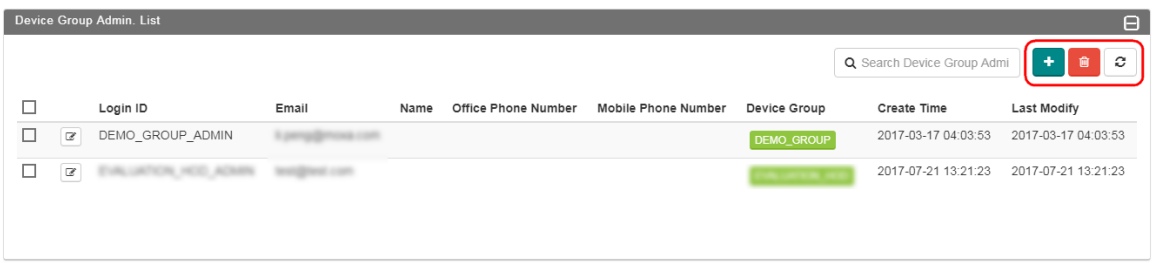


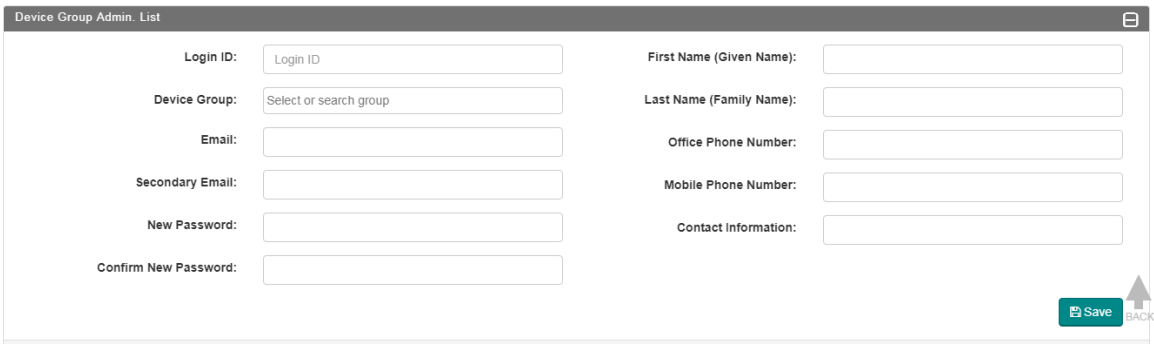
Device Group Administrator Management

The domain administrator can add or remove device group administrators for the device group.

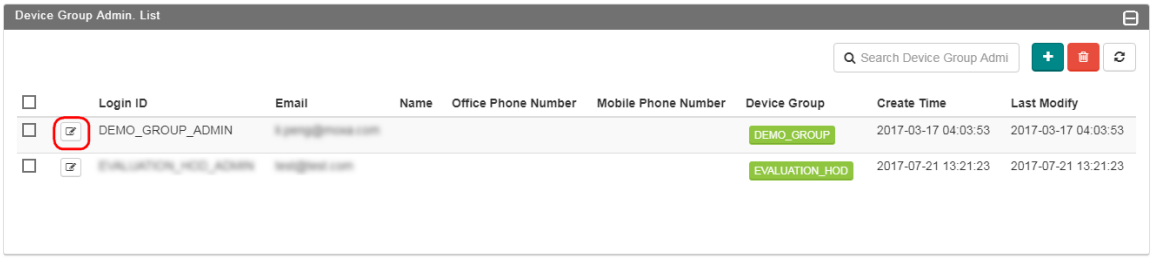


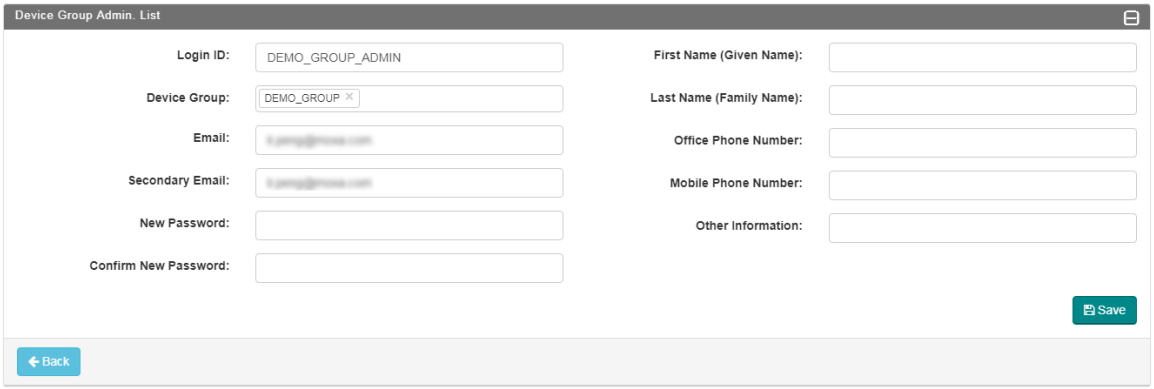
Click  to add a new device group administrator. Tick and select a device group administrator and click  to delete it. Click to get the updated settings.





Click  to modify the group administrator's profiles.





7

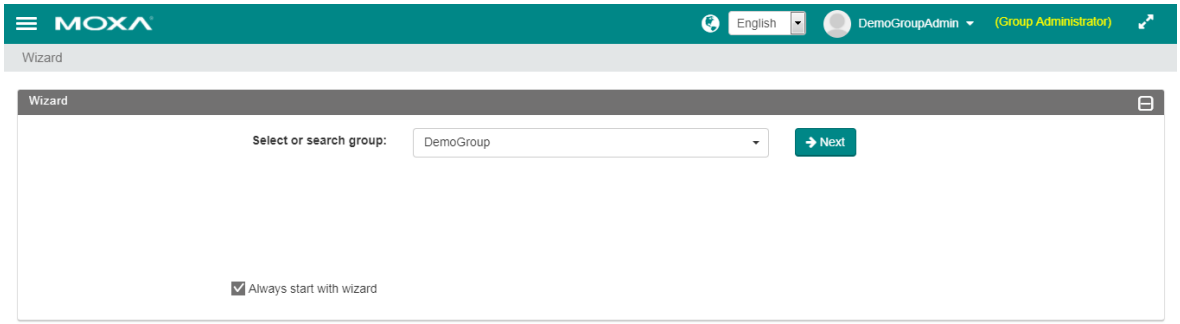
Log in as Device Group Administrator

The following topics are covered in this chapter:

- **Wizard–Creating a Gateway**
- **Wizard–Creating a Client**
- **Device Group Management**
- **Gateway Management**
  - Activate a Gateway
  - Deactivate a Gateway
  - Replace a Gateway Appliance with a Spare Part
  - Monitor the Status of the Gateways
  - Manage Local Devices of a Gateway
- **Client Management in a Device Group**
  - Add a Client Account
  - Remove a Client Account
  - Enable/Disable Clients
  - Download an Activation Key for a Client
  - Monitor a Client Status

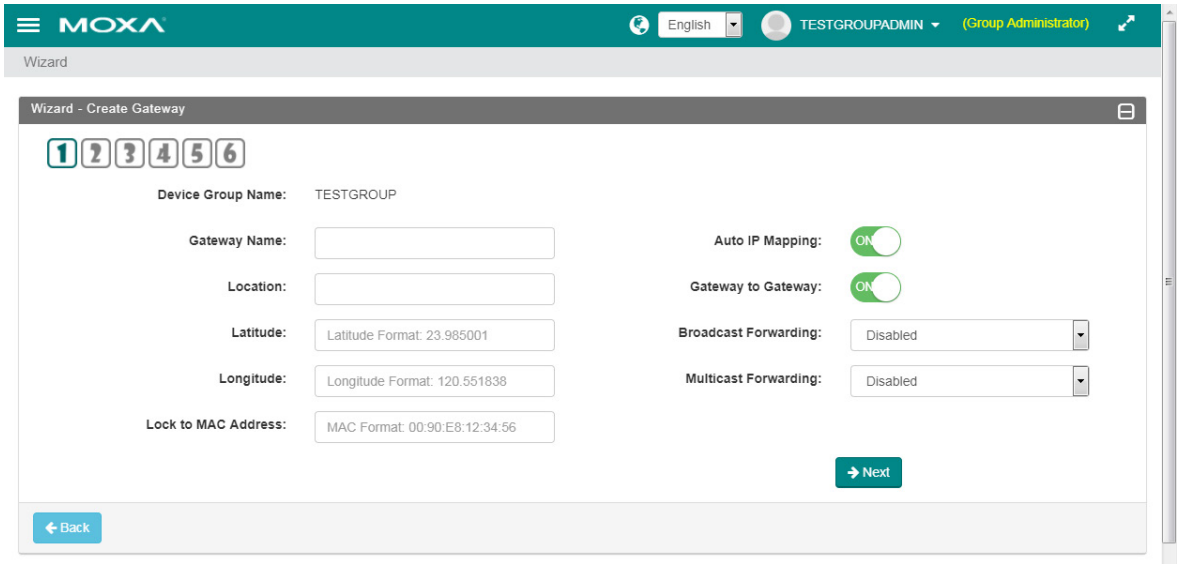
Wizard–Creating a Gateway

When users sign into the MRC portal as group administrator, the web console leads users to the wizard page for creating new gateways and clients. Users can untick the "Always start with wizard" to skip the page for the next login. Choose the group and click "Create Gateway" for creating a MRC-Gateway by wizard.



Step 1: Input the gateway name, location, and GPS coordinates. The GPS coordinates help users to track the location of the gateway on Google Maps. Users can enter key words in the "Location" and the MRC server will find the best location of the GPS coordinates from Google Maps.

NOTE The MRC gateway name is used to identify the gateway and it must be unique in the group.



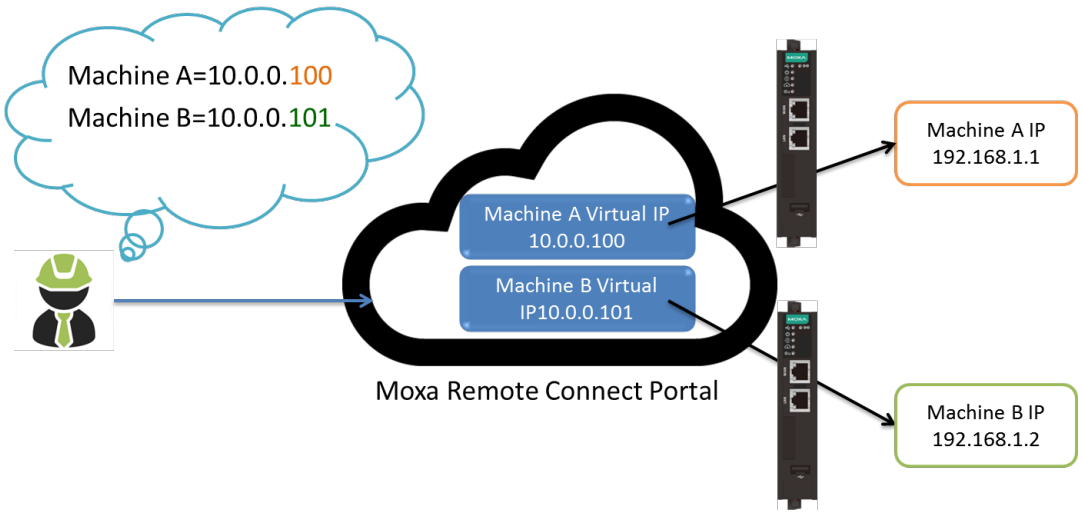
[Lock to MAC Address]

The MRC gateway settings can be locked to a certain unit by its MAC address. The activation key that has been generated after this time will only be authorized for use on MRC gateways that have that MAC address.

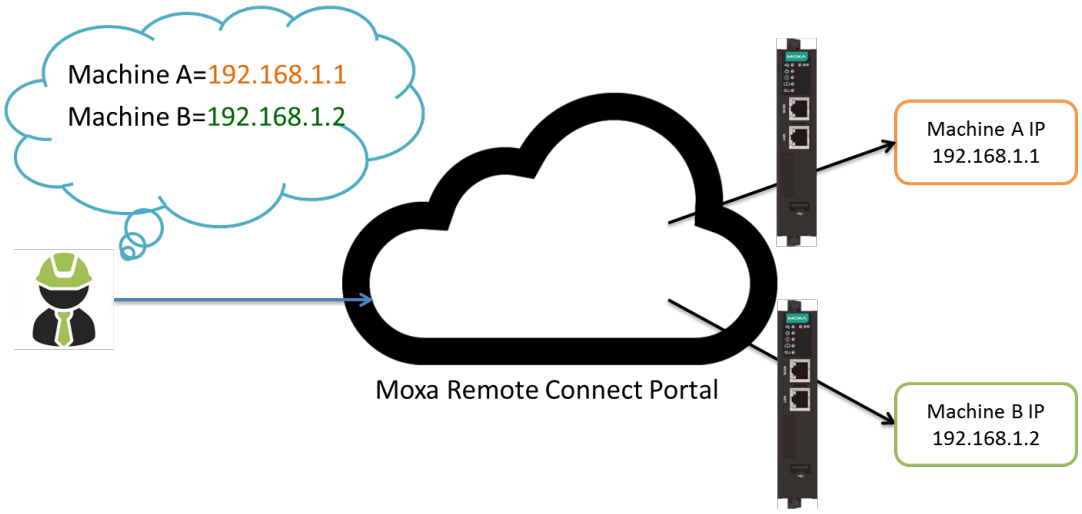
[Auto IP Mapping]

To prevent conflicts with the field machine IP address and field network configuration changes, it is recommended to use the "Auto IP Mapping" feature. With the feature enabled, the MRC gateway and each of the machines connected to the MRC gateway will be assigned an individual virtual IP address within the device group. This virtual IP address represents the device and the MRC clients can use the virtual IP addresses to access each machine without an IP address conflict.

Enabling Auto IP Mapping:



Disabling Auto IP Mapping:



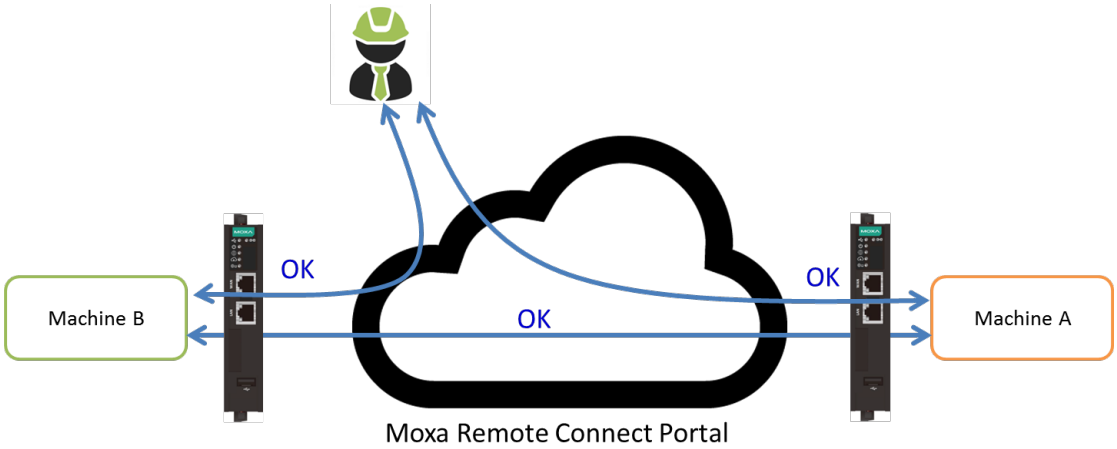
[Broadcast Forwarding and Multicast Forwarding]

The MRC gateway and the MRC portal support different types of industrial communication. For example, an EtherNet/IP application may need to enable Multicast Forwarding, and broadcast search application may need to enable Broadcast Forwarding.

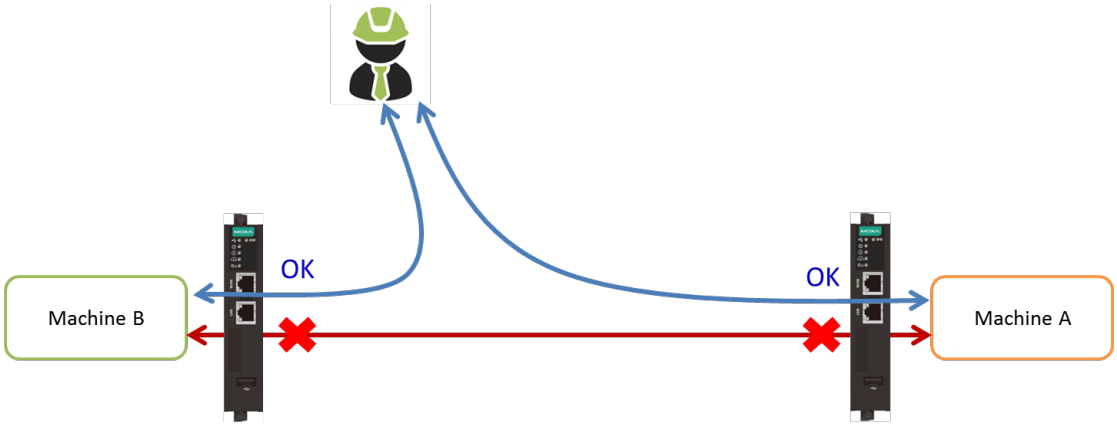
[Gateway to Gateway]

In some applications, machine to machine communication is not necessary. Disabling the "Gateway to Gateway" function will block traffic coming from the machines that are connected to other MRC gateways. It allows only the MRC client to access the machines behind the MRC gateway. On the contrary, enabling the function allows machine to machine communications through the MRC gateways.

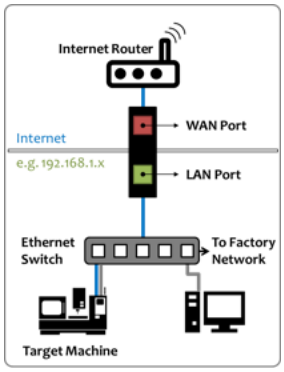
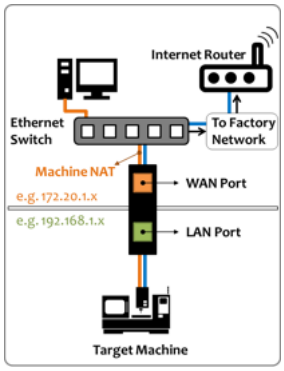
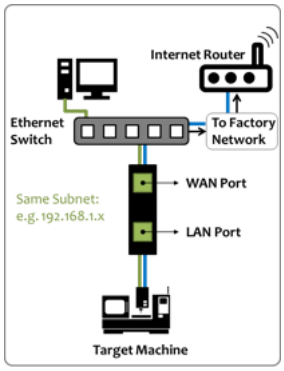
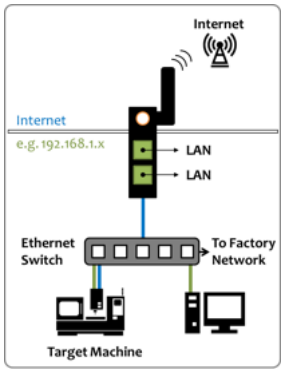
Enable Gateway to Gateway:



Disable Gateway to Gateway:

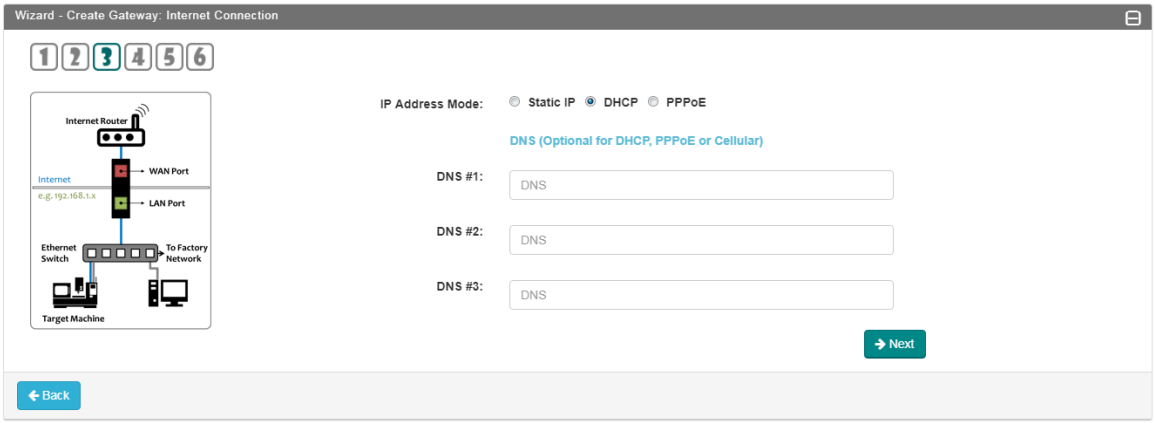


Step 2: Set up the field Internet access for an MRC gateway. If the information is not available, users can choose any of the scenarios and it can be setup later from the local web console afterwards. (For more details refer to MRC Gateway User Manual).

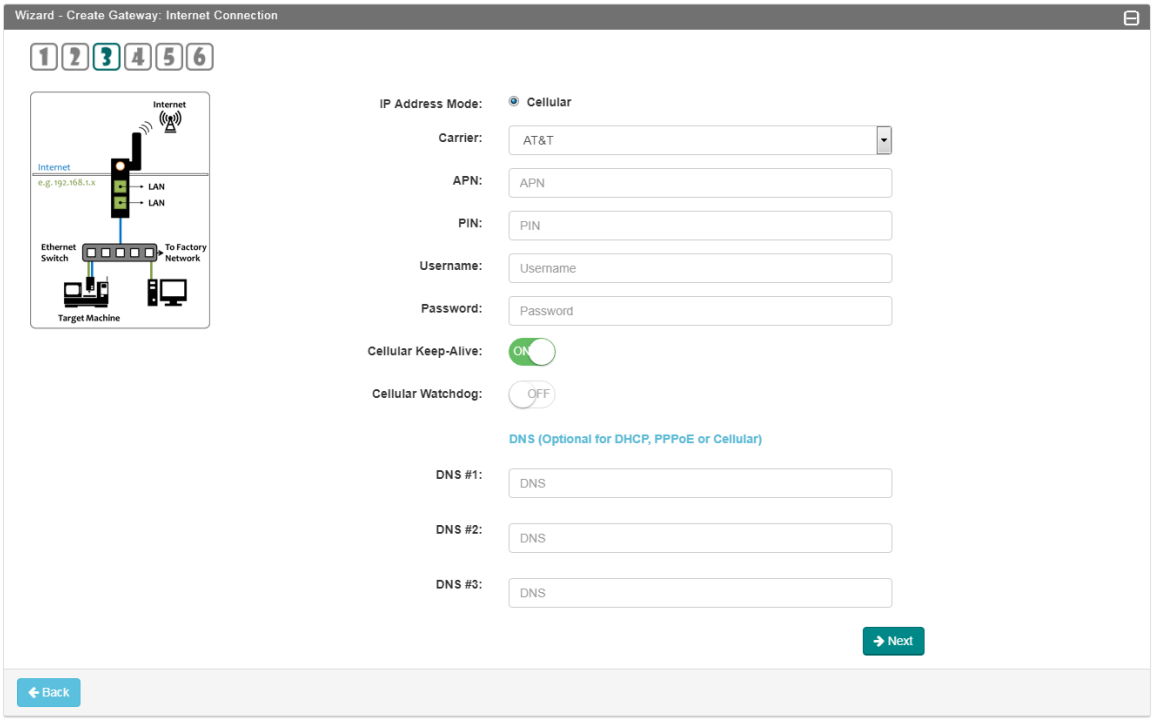
Scenario	Installation of Network Scenario	Description
#1 WAN-LAN mode Using an external ADSL modem for MRC gateway's WAN Internet access		In this scenario, connect MRC gateway's WAN port to the ADSL modem, and connect the LAN port directly to the Ethernet device or to the local network where the machine's network is located via an Ethernet switch. DHCP, static IP, and PPPoE are supported for Internet access in the MRC gateway's WAN configuration.
#2 WAN-LAN with NAT Mode Using the existing factory or office network for MRC gateway's Internet access but separate the machine from the factory network.		In this scenario, separate the target Ethernet device from its original network and install the MRC gateway in between. Connect the MRC gateway's WAN port to the original factory network where Internet access is available, and connect MRC gateway's LAN port to the target Ethernet device (for multiple devices, an Ethernet switch can be installed). In this case, though the Ethernet device has been separated from the original network, it does not affect the communication path from the device to others located in the original network, but if the communication path is reversed, you may need to set up an external NAT IP address for the devices.
#3 Transparent-LAN mode Using the existing factory or office network for MRC gateway's Internet access within the same subnet of the machine		In this scenario, install the MRC gateway between the target Ethernet device and the original network. Connect the MRC gateway's WAN port to the original network and use the factory network's ISP for Internet access. Connect the MRC gateway's LAN port to the target Ethernet device without needing to change the network configuration of the device.
#4 Cellular-WAN mode Using the cellular network for MRC gateway's Internet access		In this scenario, insert a SIM card for the cellular Internet access, and connect LAN port to the target Ethernet device (for multiple devices, an Ethernet switch can be installed).

Step 3: Configure WAN for Internet access.

Setting of scenario #1, #2, and #3:



Setting of scenario #4: (for cellular model only)

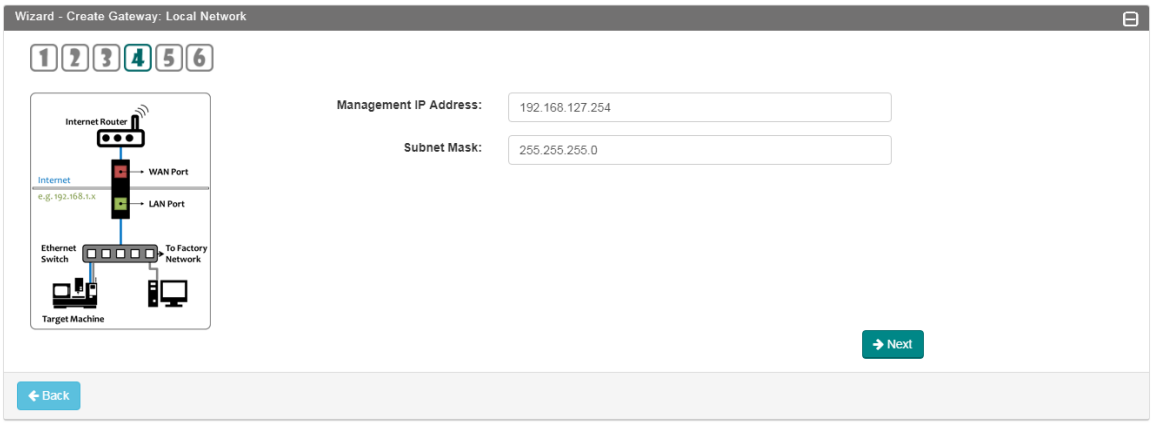


WARNING

Some carriers will stop the cellular data service if there is no active traffic for a certain period of time. It is suggested to enable "Cellular Keep-Alive". In addition, to prevent the cellular module having an unknown connection status with the carrier, users can enable "Cellular Watchdog" to restart the cellular module automatically once a problem has been detected.

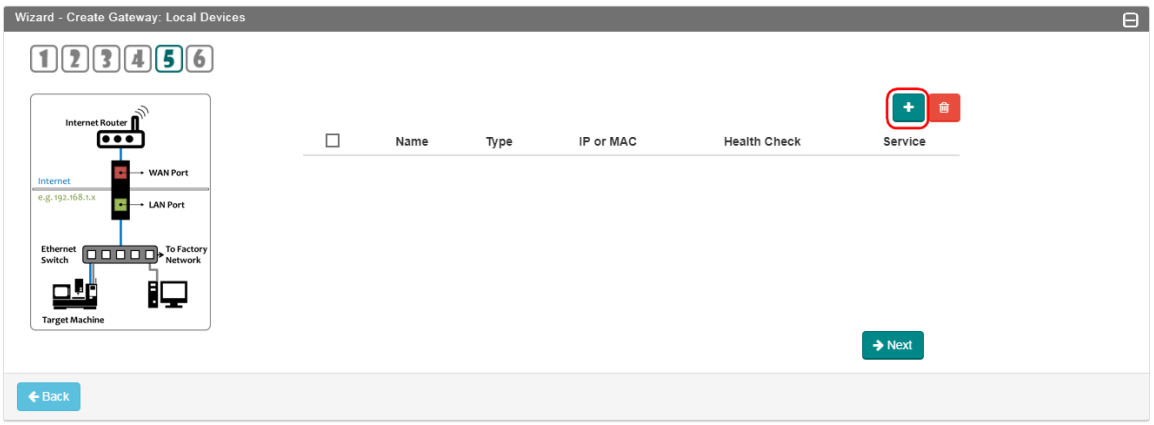
Step 4: Assign a management LAN IP address for the MRC gateway. The LAN configuration and the subnet mask must match the network settings of the local machines connected to the gateway's LAN port. Click "Next" for the next step.

NOTE Skip this step for scenario #3.



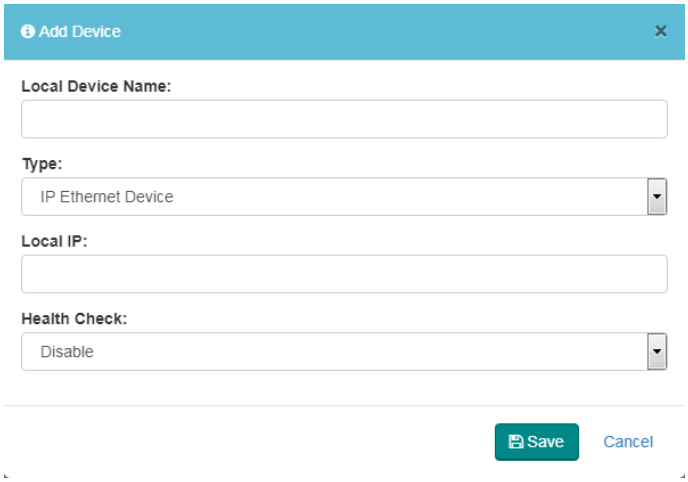
Step 5: Add the target Ethernet devices or machines into the list for remote access. All IP-based machines in the list will be automatically assigned with a virtual IP address if "Auto IP Mapping" is turned on. If "Auto IP Mapping" is turned off, the target Ethernet devices or machines will use the original local IP addresses for the remote access.

Click + to add a machine for remote access.

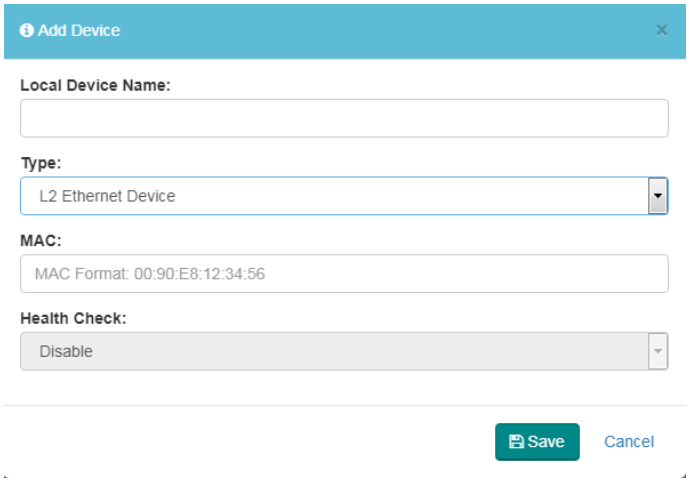


In put the local device name and the local original IP address of the target Ethernet devices or machines. If the local Ethernet device is a layer 2 device, please input the device's MAC address. The gateway can also perform a health check of the connection through Ping Check or Port Link. (If a switch is connected to the gateway's LAN port, Ping Check is recommended. If a machine is directly connected to the gateway, Port Link is also an option.)

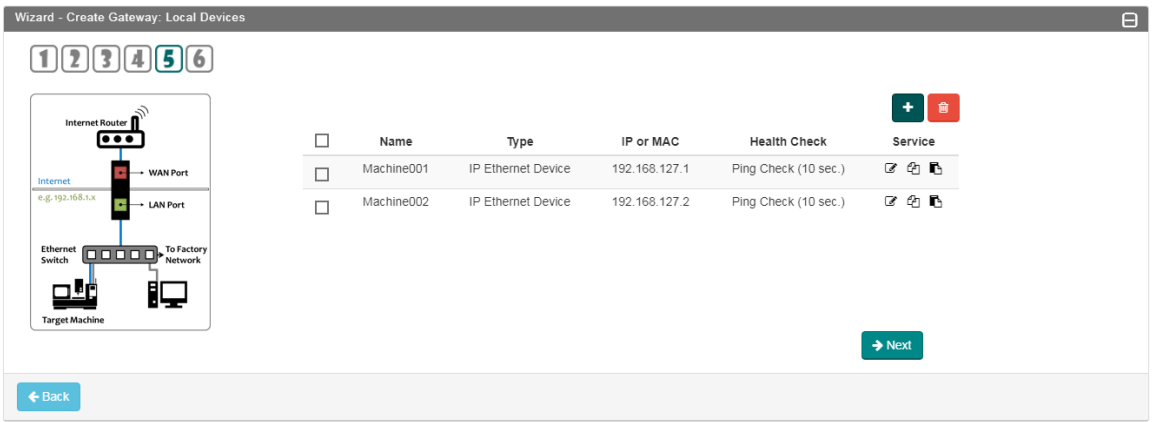
Adding an IP Ethernet Device:



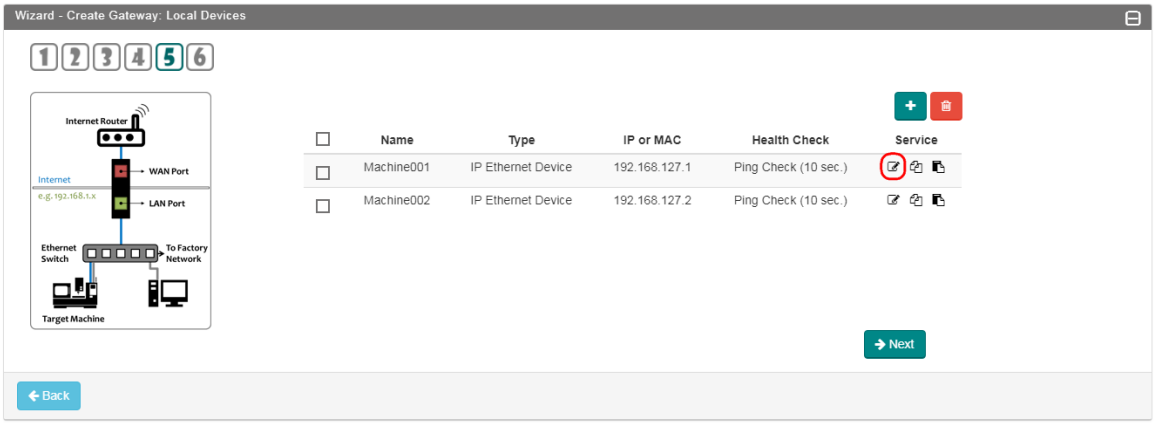
Adding a layer 2 Ethernet Device:

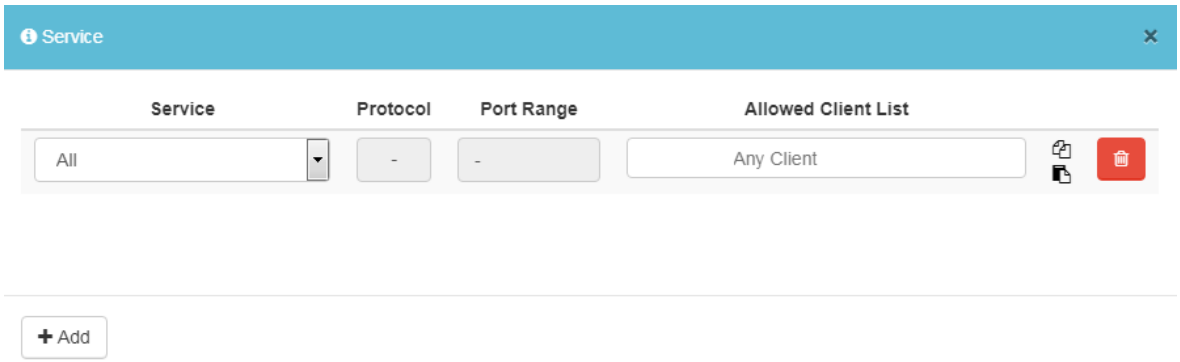


NOTE In order to enhance cyber security, remote access will be limited to defined Ethernet devices in the MRC gateway and does not interrupt or disrupt the original factory network. A maximum of 25 devices can be added into the list for remote access.

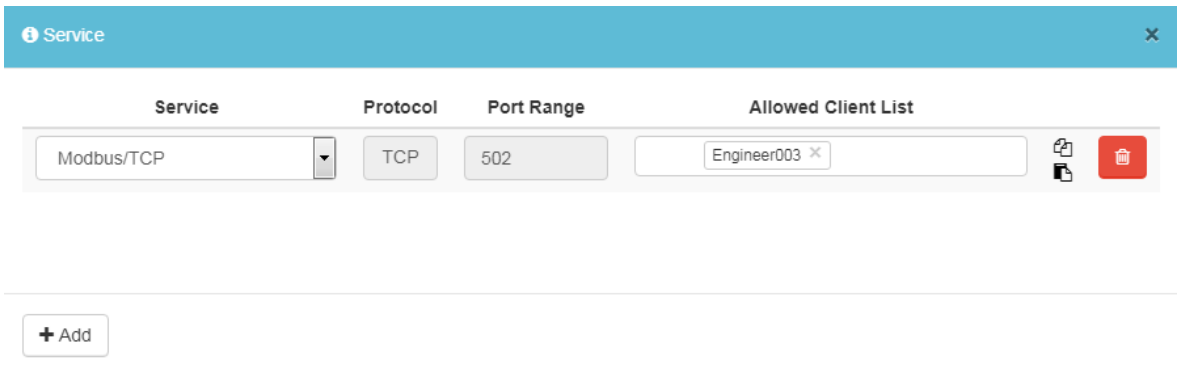


Click to edit the available service of the device for remote access. By default, the remote access function can connect to all the services of the device. To enhance security, you can limit each of the services to selected MRC clients only.

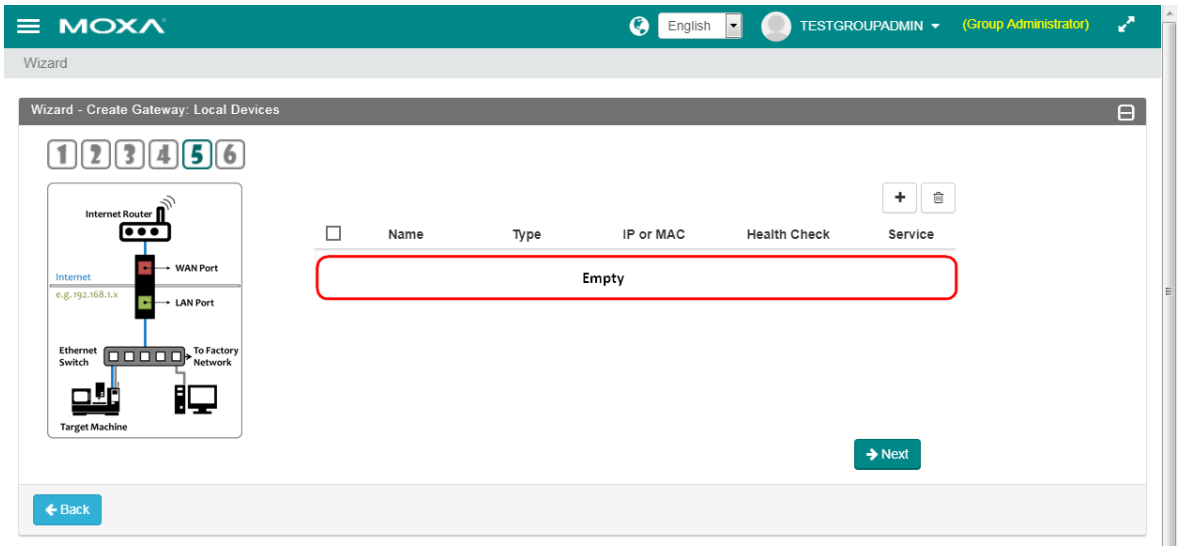




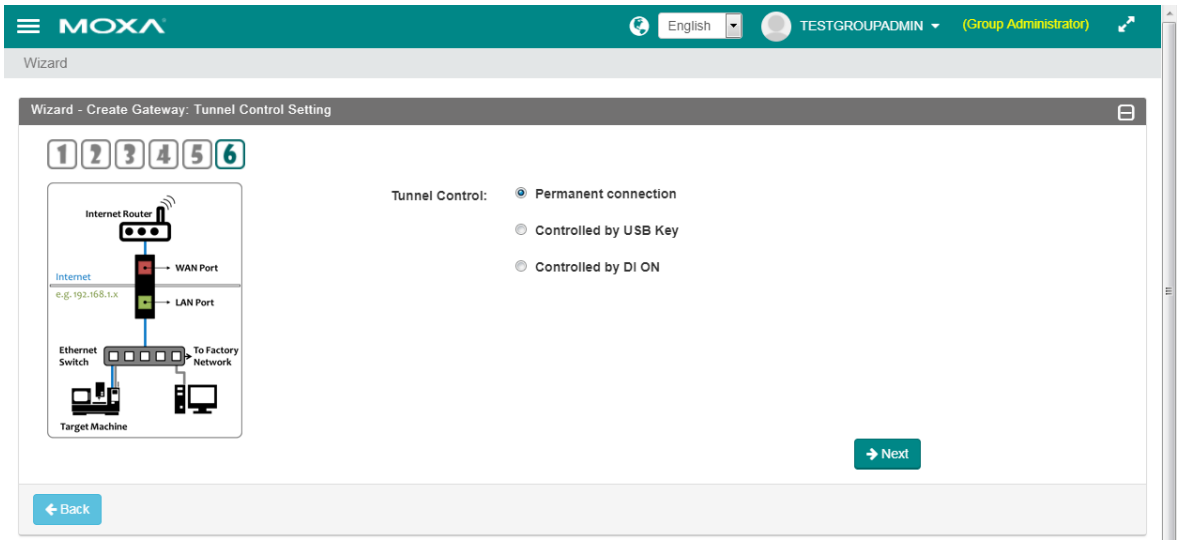
For example, there is a Modbus TCP device that only allows Engineer003 to have remote access. You can configure the service to the MRC client as shown below. Multiple service rules are acceptable for a service whitelist.



NOTE For site-to-site networking, leaving the device list empty allows a remote connection to access the WHOLE LOCAL SUBNET defined as the LAN subnet of the gateway. For example, if the LAN configuration of the gateway is 192.168.127.254/24, all the Ethernet devices or machines with the IP address 192.168.127.x connected together with the MRC gateway's LAN are available for remote access.

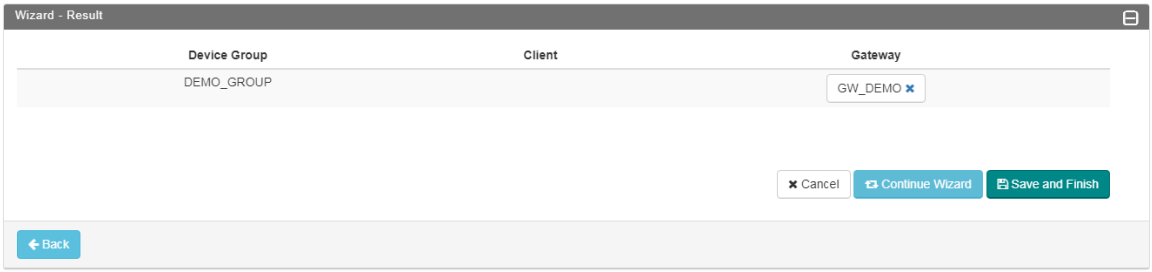


Step 6: Select a connection mode of the MRC gateway. Click "Next" for the next step.



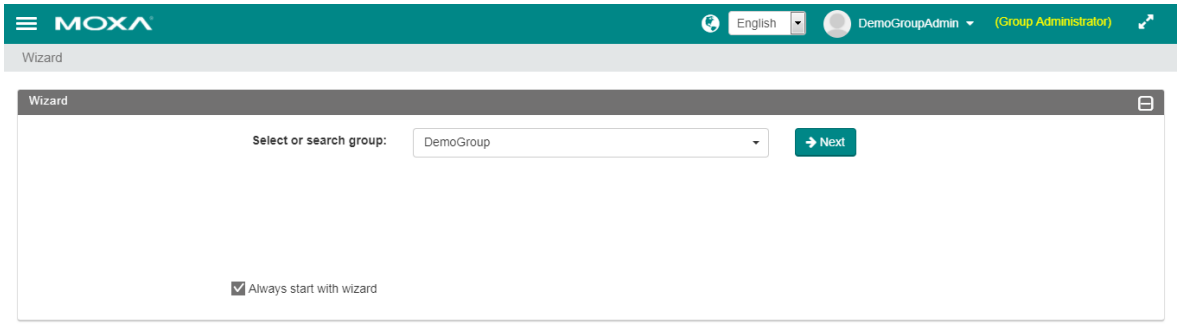
- **Permanent connection:**
  The MRC gateway will keep a permanent VPN connection to the MRC portal for the clients' access.
- **Controlled by USB Key:**
  The MRC gateway will trigger the VPN connection to the MRC portal only when the USB key (with the activation file) is inserted. When the USB key is removed, the MRC gateway will disconnect the VPN from the MRC portal and all the Ethernet devices or machines will not be reachable from the clients in the device group.
- **Controlled by DI ON:**
  The MRC gateway will trigger the connection to the MRC-Server only when the DI status is ON. When the DI status turns to OFF, the MRC gateway will disconnect itself from the MRC portal and all the machines are not reachable from the clients in the device group.

Step 7: Click "Save and Finish" to finish the wizard or click continue to keep creating multiple gateways or new clients.

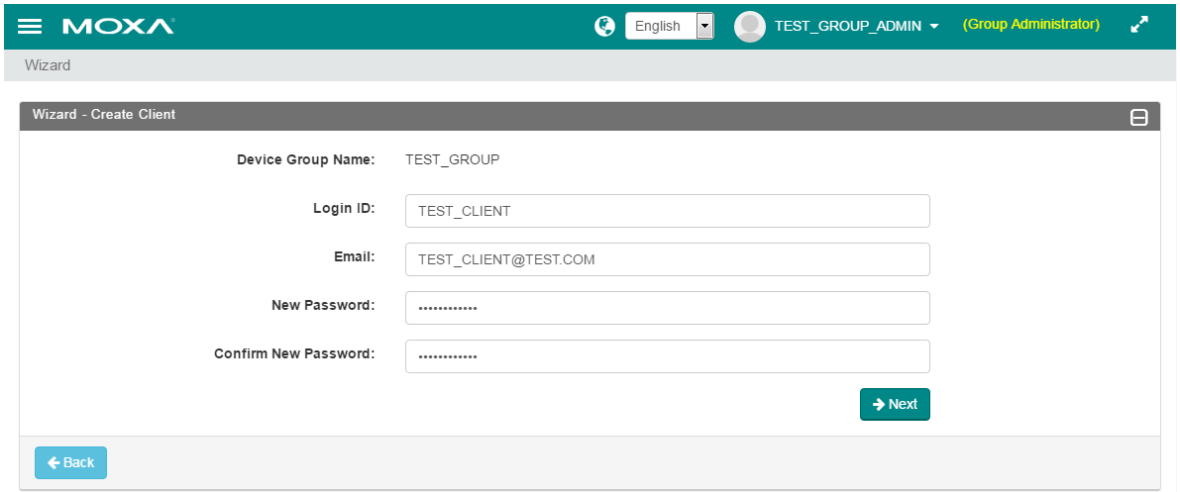


Wizard–Creating a Client

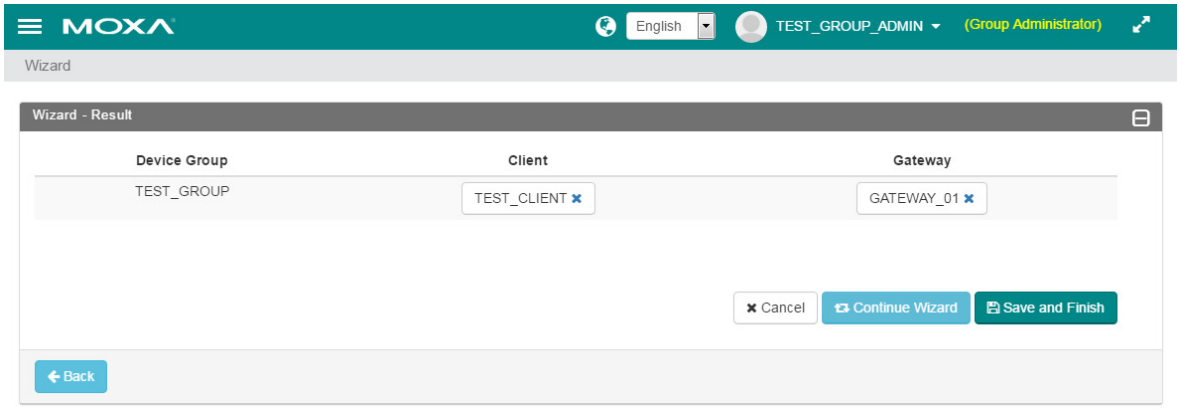
When logging in the MRC portal as group administrator for the first time, the web console leads users to the wizard page for creating new gateways and clients. Users can untick the "Always start with wizard" to skip the page for the next login. Choose group and click on "Create Gateway" to create a MRC-Gateway by wizard.



Step 1: Input the login ID, email, and password. The Login ID and the email must be unique in the system. Users can use either the login ID or email to sign into the MRC portal with the MRC-Client software. Click "Next" for the next step, then, click "Save and Finish".

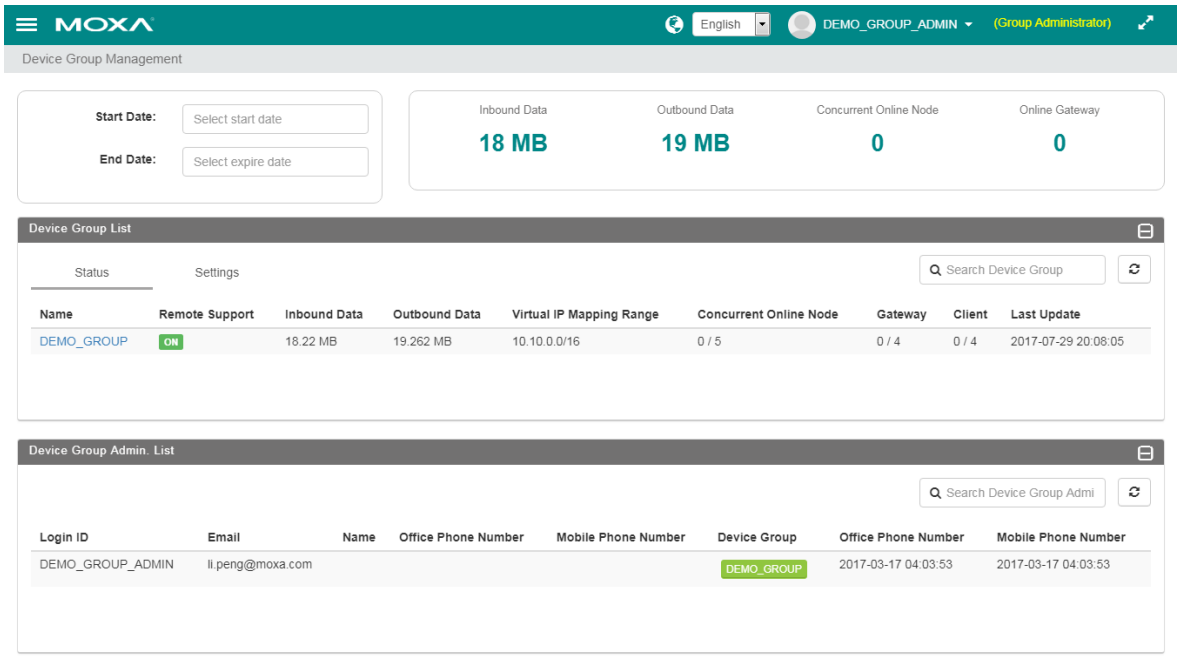


Step 2: Click "Continue Wizard" and start over the wizard. Click "Save and Finish" to update the settings in the MRC server.

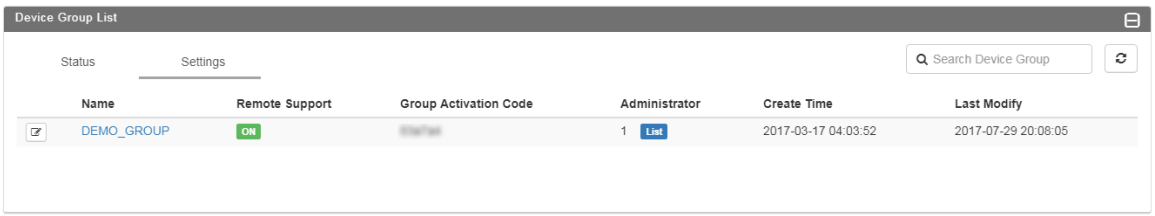


Device Group Management

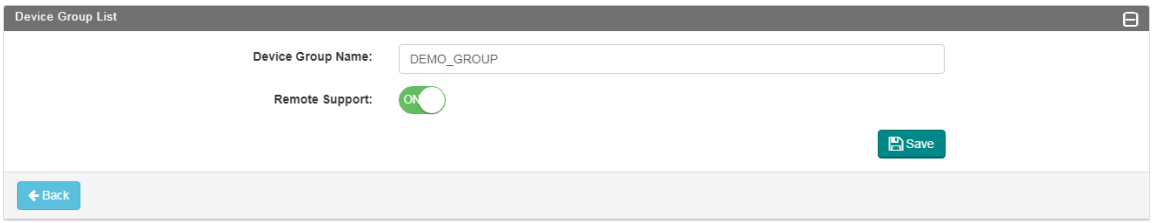
After the wizard, the group administrator will be redirected to the device group management web page for the overview of data usage, concurrent online node usage, and group administrator list of the device group.



Click "Settings" to check the Group Activation Code or modify the group configurations.

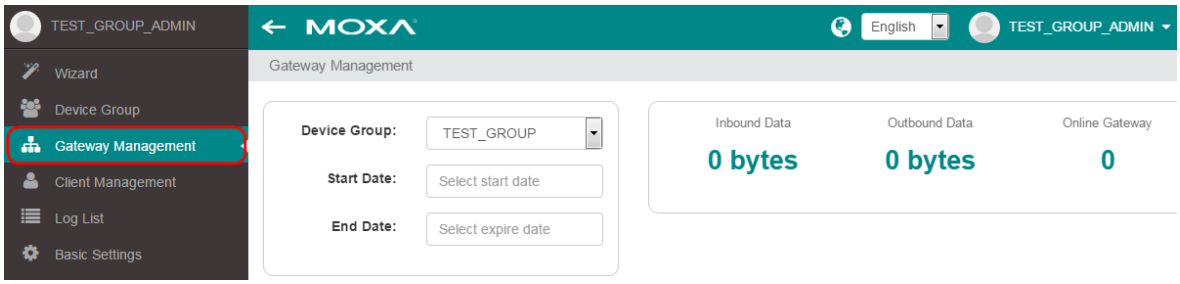


Click  to edit the device group's name and configure the "Remote Support" settings. When enabling the "Remote Support", the higher level administrator can view the device group settings and provide necessary support. (The gateways and clients are still invisible to higher level administrators for cyber security reasons.)

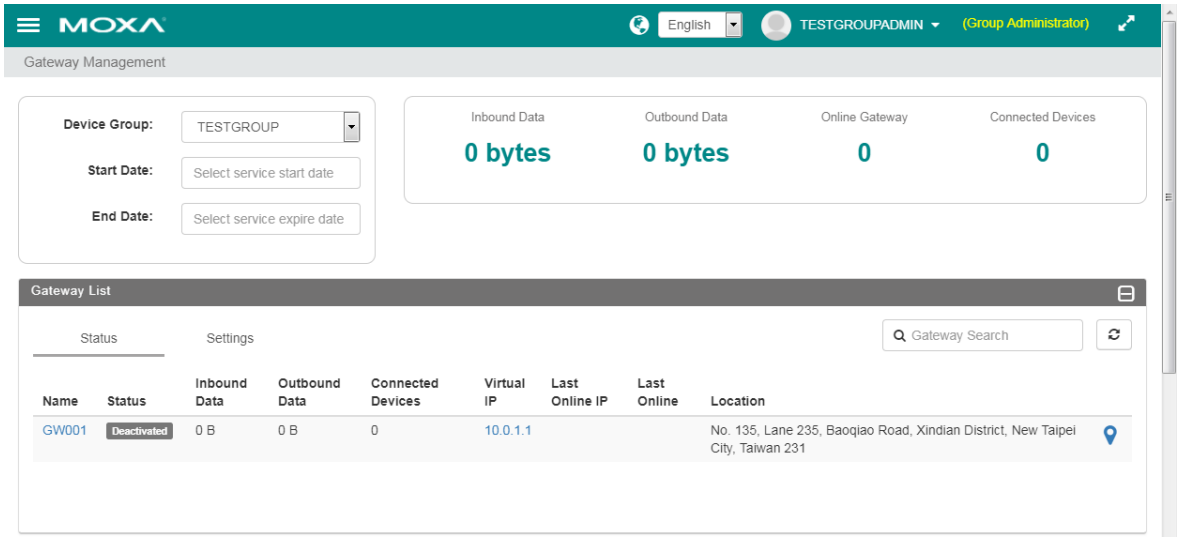


Gateway Management

Go to the "Gateway Management" page from the main menu to monitor the status and configure gateways in the device group.

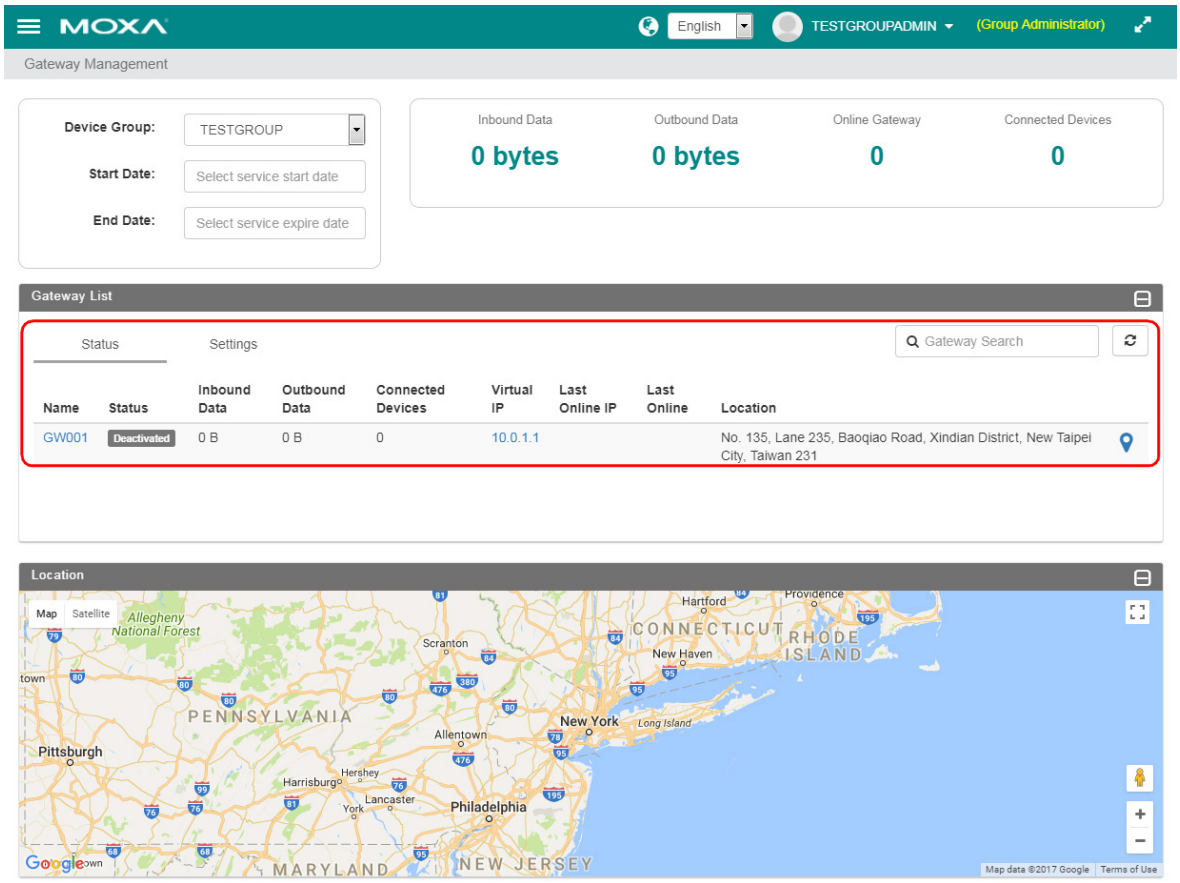


On the dashboard, the group administrator can monitor the data usage of all the gateways in the device group and how many gateways are currently online.

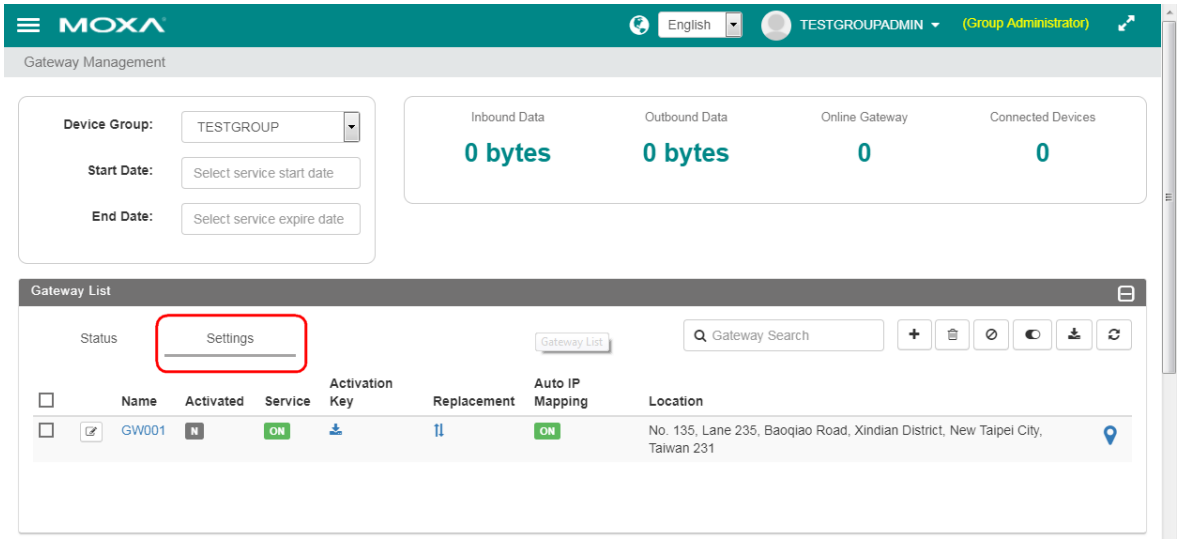


In the middle of the page, the group administrator can monitor the status for all the individual gateways in the device group including the data usage, the connected devices, and the gateway's virtual IP address.

Click  can see the location of the gateway on Google Maps.



Click "Settings" to add a gateway, stop gateway services, deactivate a gateway, or download all of the gateway activation keys.



Click the action buttons to add, remove, deactivate, start/stop connections, download keys, and refresh the table.

Add a new gateway.

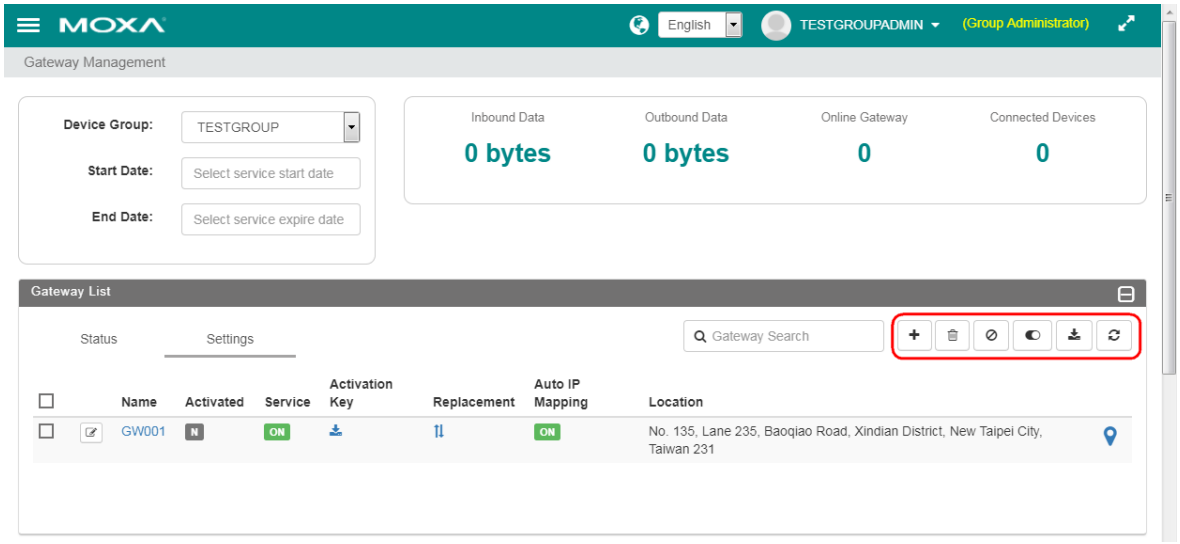
Remove selected gateways.

Deactivate selected gateways.

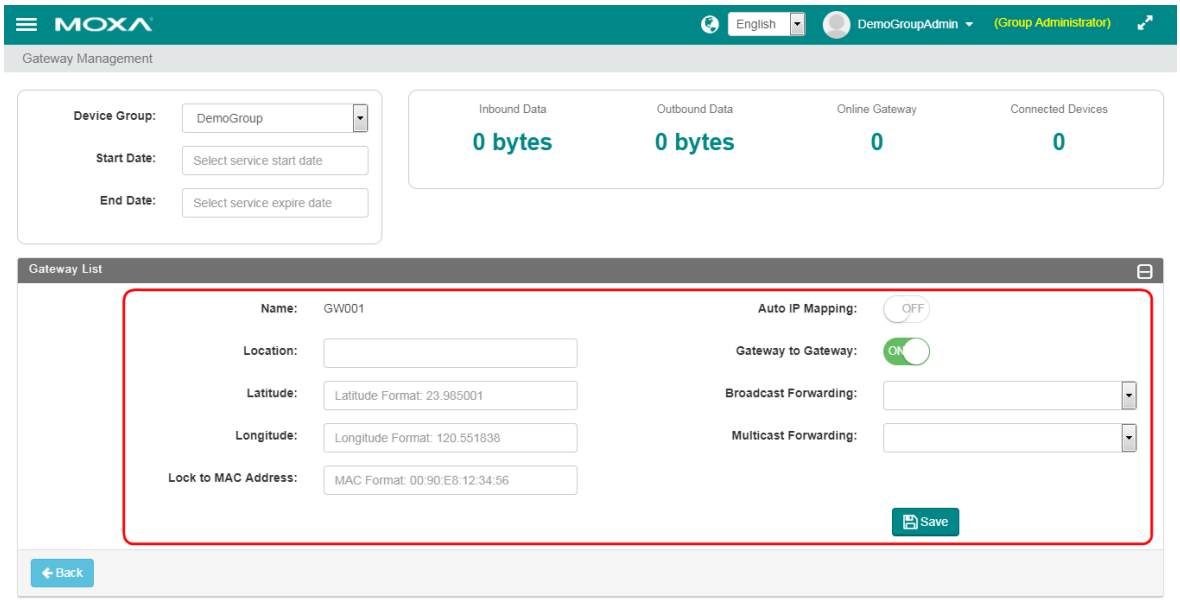
Start or stop connection of selected gateways.

Download keys of selected gateways.

Refresh the information of the table.



Click to modify the settings of the gateway.



Activate a Gateway

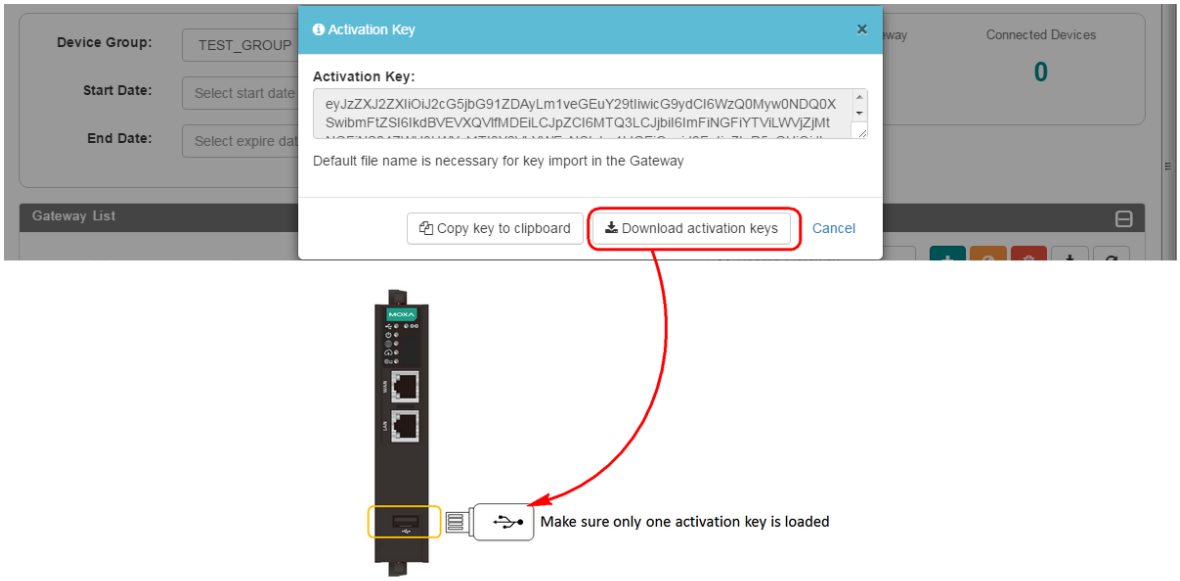
When the MRC gateway settings are created in the device group, the status is set to "De-activated". To activate a gateway appliance, the group administrator should download the activation key and load it into the gateway appliance.

Click  to download the activation key. There are three methods to activate the gateway appliance:

Download the activation key from MRC Server management portal, and deploy to the field by one of the following methods:

Method 1: Load the activation key into a USB dongle and install the gateway appliance with Internet access, then, insert the USB dongle into the gateway and turn on the power.

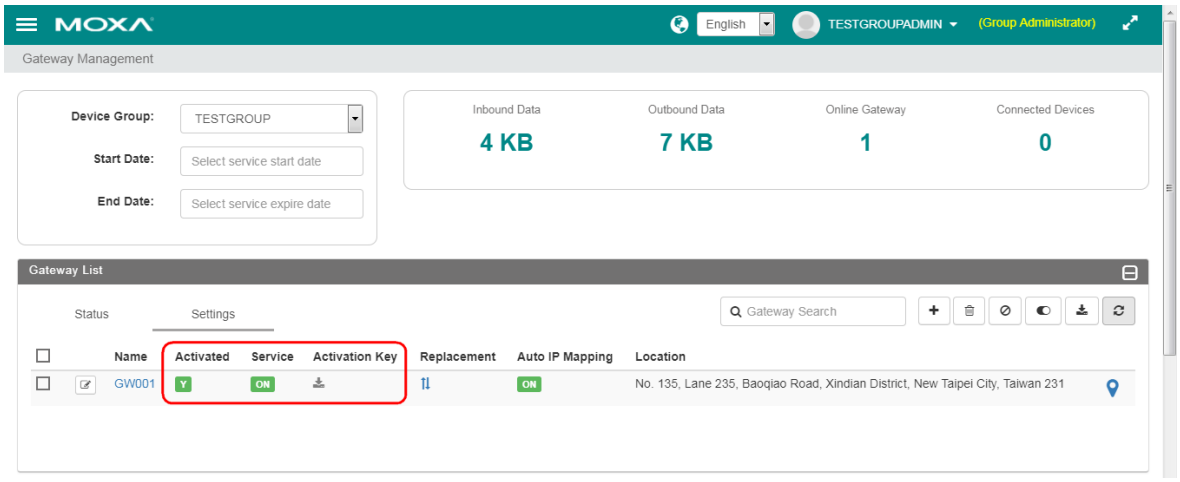
NOTE Activate a gateway by USB dongle (with activation key file). USB format supports FAT, FAT32, and NTFS.



OR

Method 2: Access the web console of the gateway from LAN port and follow the wizard to input the string and activate the gateway. (Refer to MRC Gateway User Manual)

After successfully activating a gateway, the group administrator will see the gateway is "Activated" and the service is ON. The activation key can only be downloaded for one device.

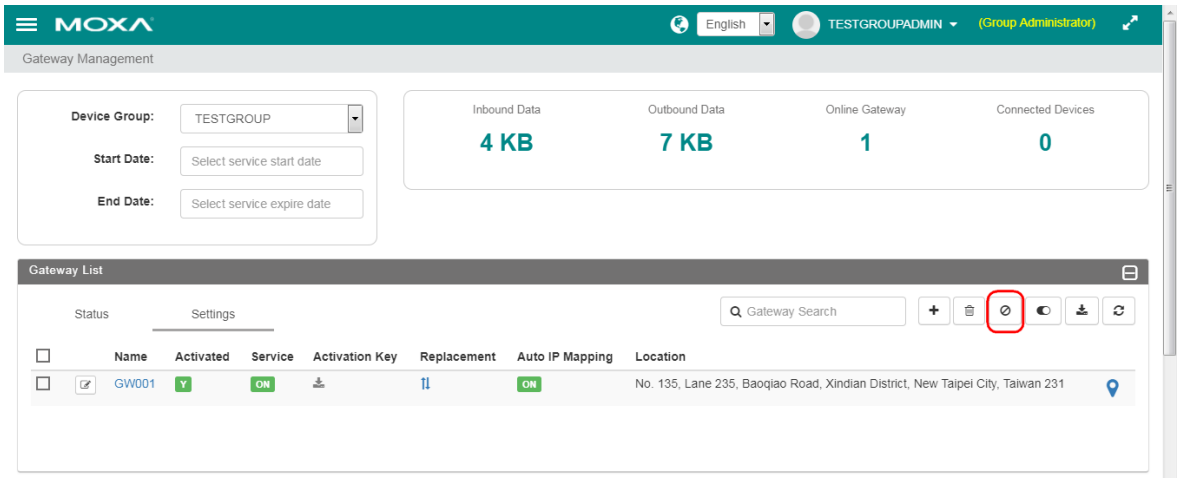


NOTE One activation key can only activate one gateway. Once the activation key has been used, it belongs to that gateway only and cannot be used to activate others.

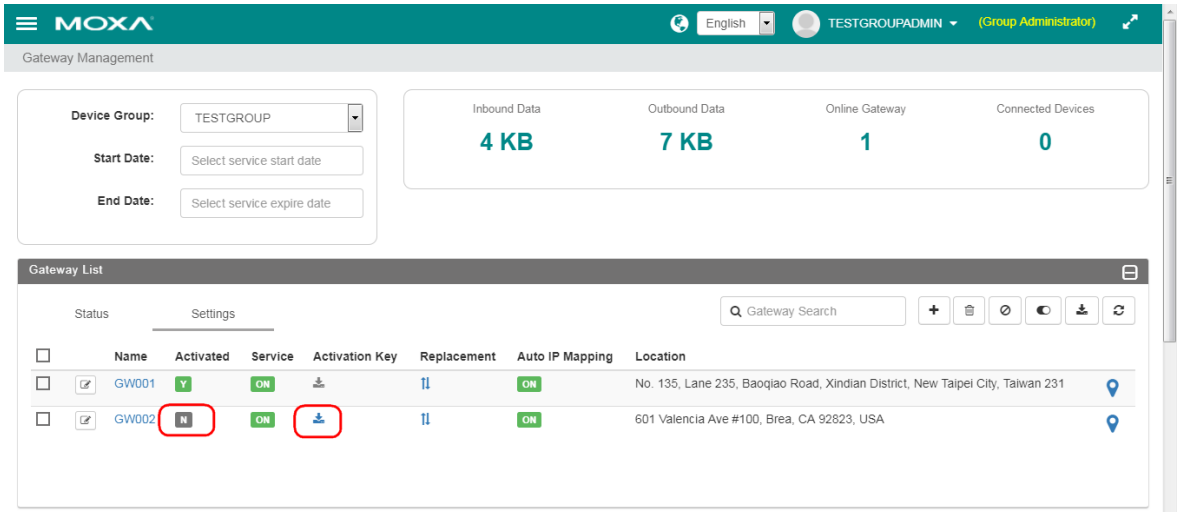
NOTE If the field MRC gateway needs to be replaced, then, you can click for a replacement and download the key again for the new MRC gateway. During this period, the old gateway is no longer available for remote access.

Deactivate a Gateway

The group administrator has authority to deactivate a gateway and determining the connectivity status of the gateway. Select a gateway and click to deactivate it.

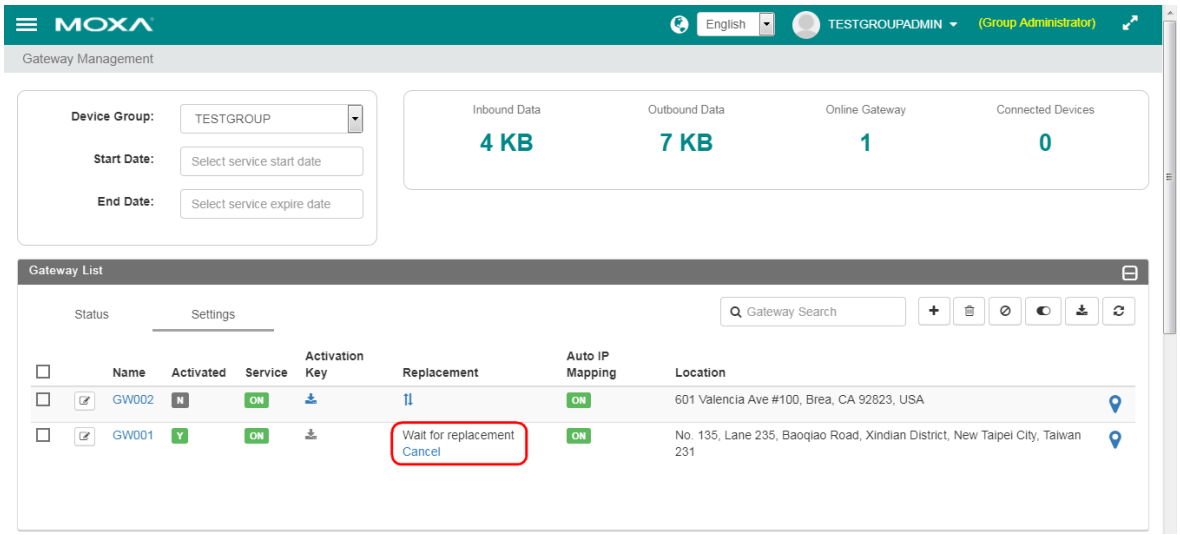


After deactivating the gateway, the system will regenerate a new activation key for users to download. Users need to send this new key to the gateway appliance owner for activating the gateway again. The old key would no longer be valid.



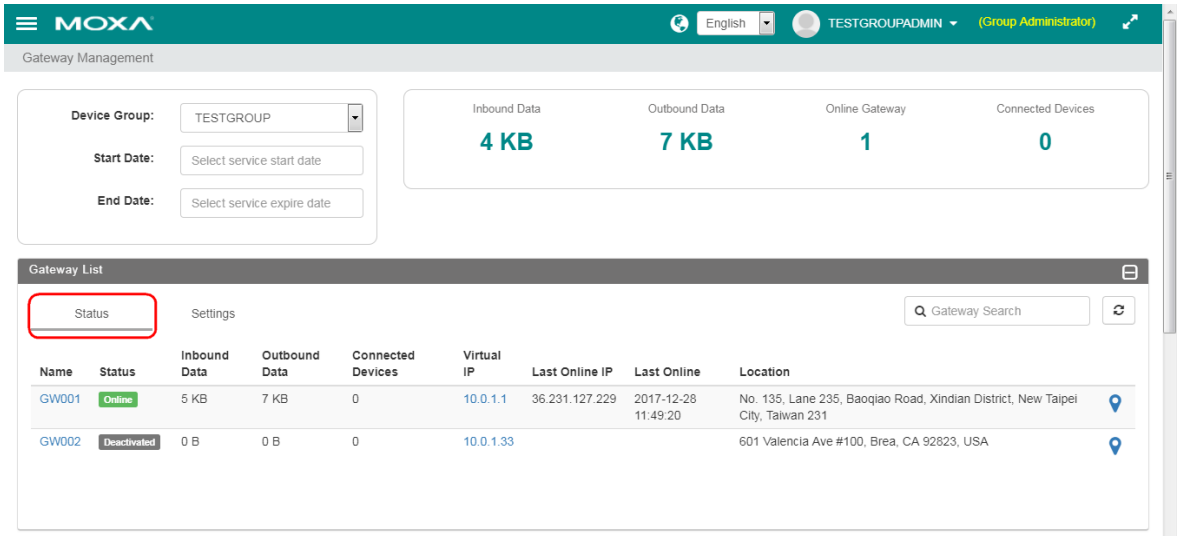
Replace a Gateway Appliance with a Spare Part

When a gateway is not working, the group administrator can change the status of the gateway to "Waiting for Replacement" in the MRC portal and prepare a new gateway for field gateway replacement. In this status, the gateway appliance owner can use the activation key of the old gateway to activate a new gateway. If the gateway owner has lost the activation key, the group administrator can download the activation key again and send it to the gateway appliance owner to activate the new gateway.



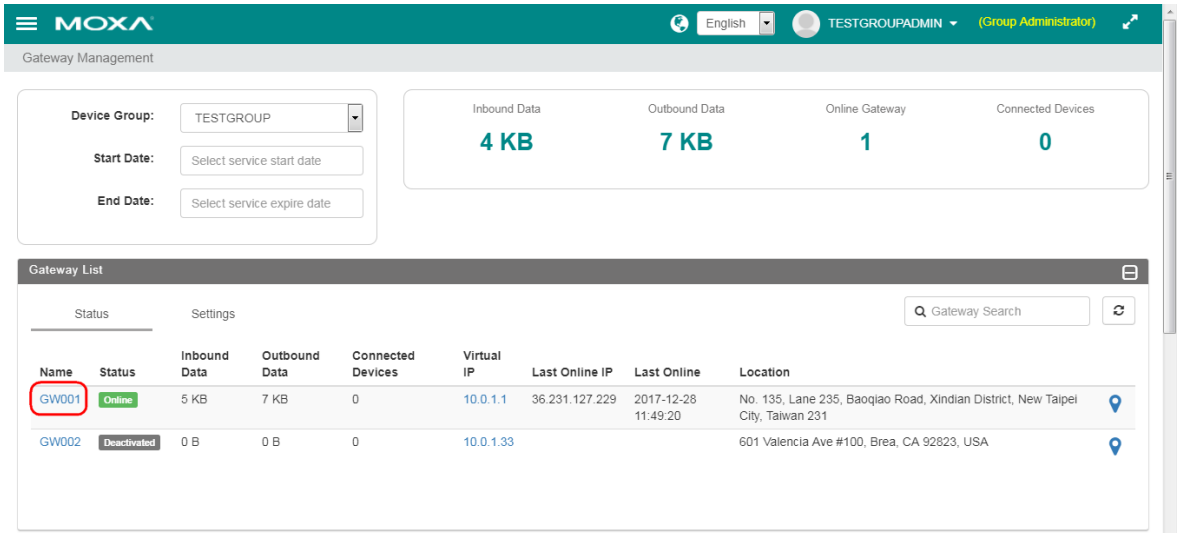
Monitor the Status of the Gateways

By clicking on "Status", the group administrator can see the online and offline status of the gateways. In the status table, the group administrator can also see the data usage, the virtual IP address of each gateway, and the IP address of the last gateway to go online.



Manage Local Devices of a Gateway

The group administrator can add or remove local devices of gateways in the MRC portal. Applying the change will automatically synchronize the database into the remote gateways when the gateways are online. Click on the name of the gateway to monitor and look up the virtual IP mapping of each device.



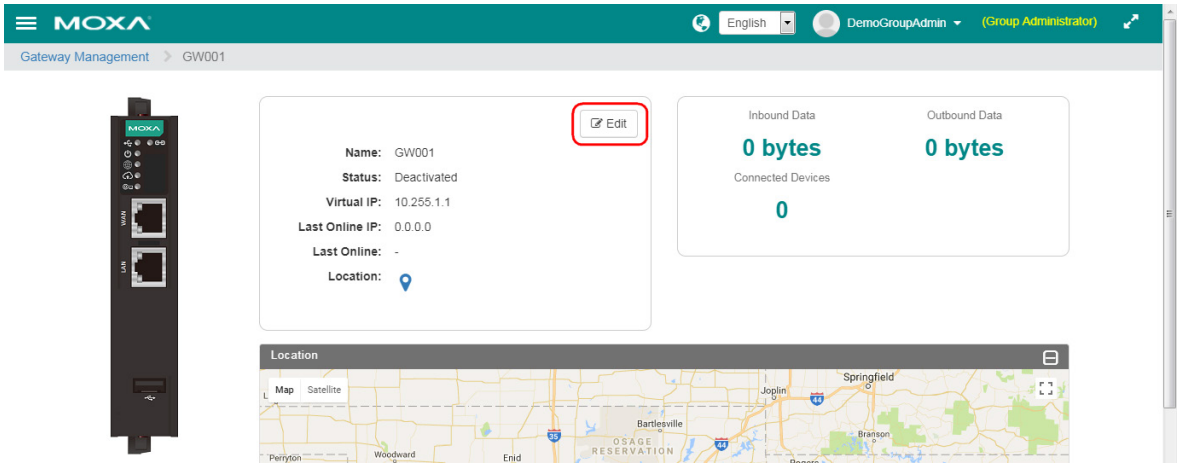
Click "Status" to monitor the instant online and offline stats of the devices when the "Health Check" feature is turned on.

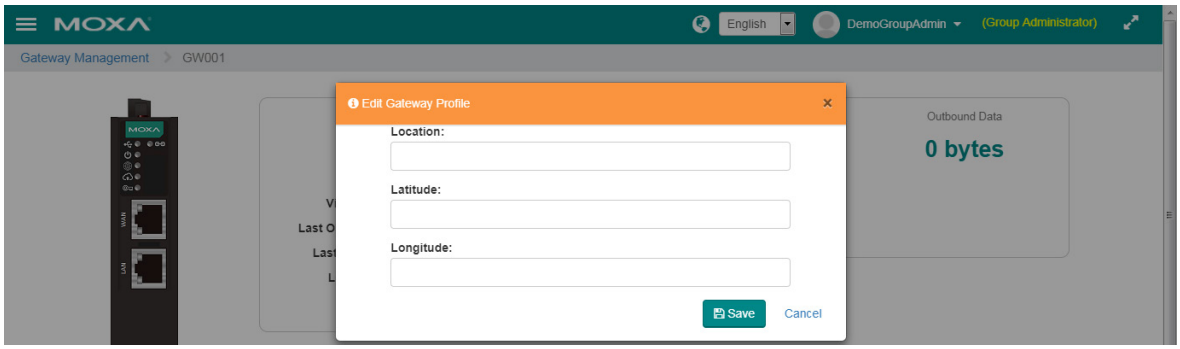
Online The MRC gateway can get PING responses from the device or the port link is ON.

Offline The MRC gateway cannot get PING responses from the device or the port link is DOWN.

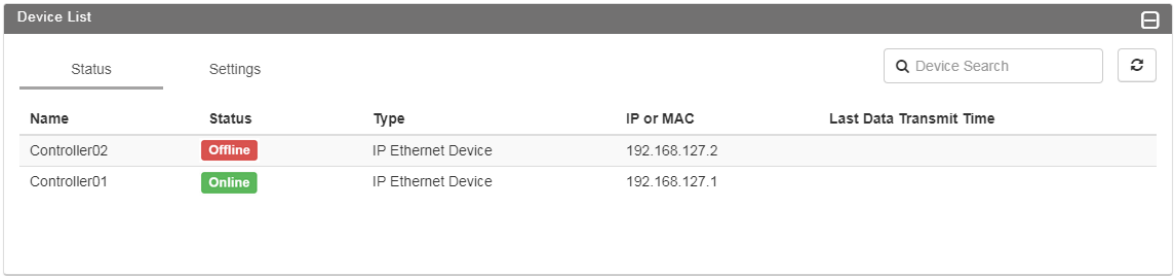
Unknown Health Check is turned off.

Click on the name of the gateway to get the detailed gateway information. Then click Edit to set up the location and the coordinates of the gateway.

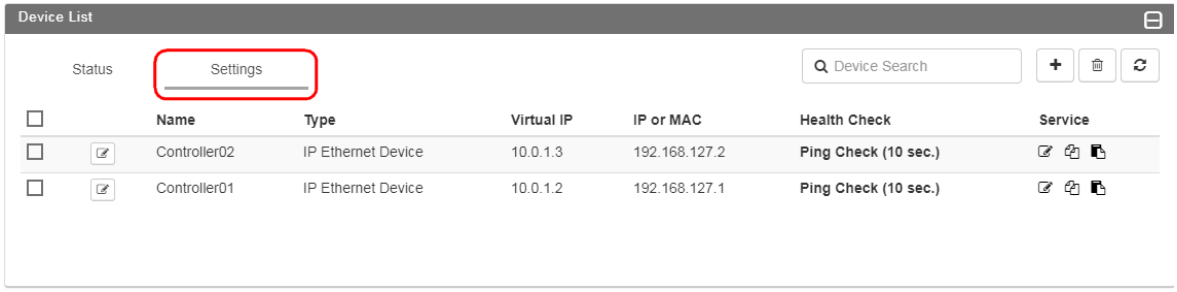




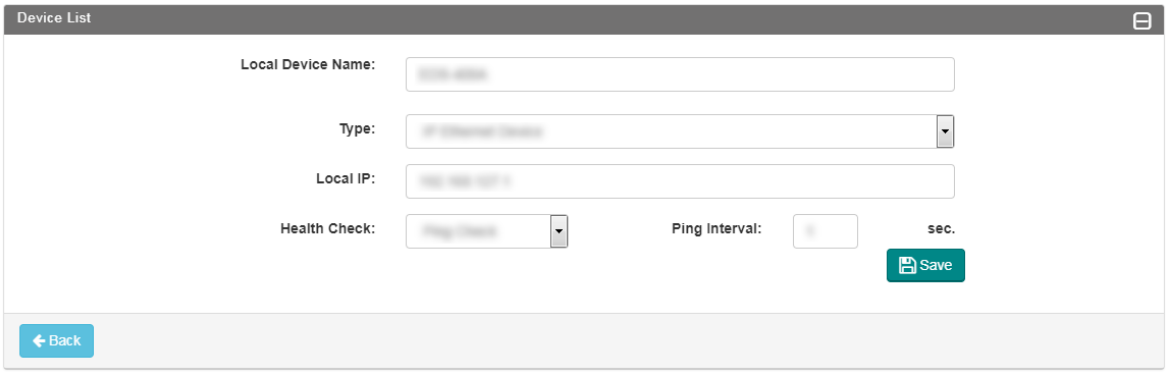
Scroll down the page to display the device list and set up the configuration of local devices.



Click "Settings" to add or remove the devices in the whitelist.



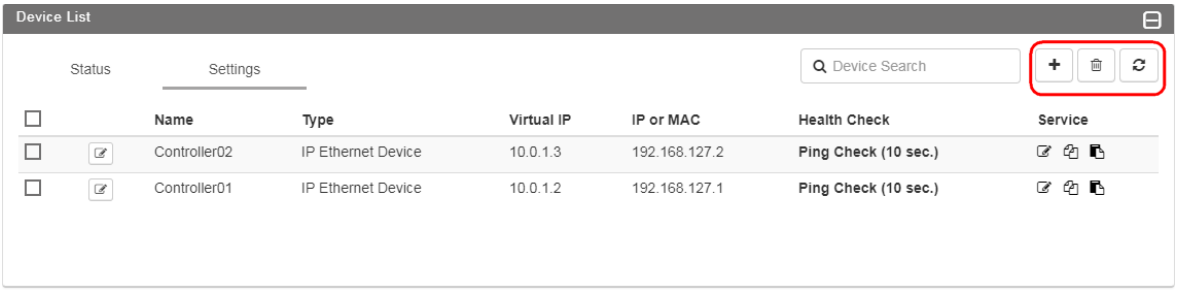
Click on the "EDIT" icon to modify the device group's settings.



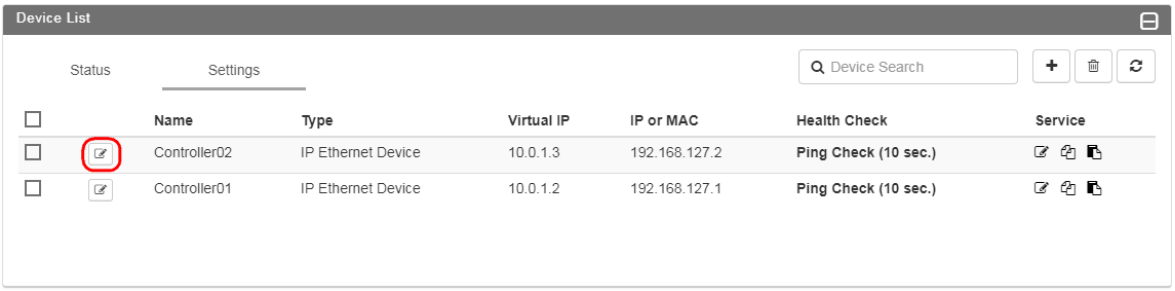
Click to add a new device. Tick and select a device before clicking to remove it from the whitelist.

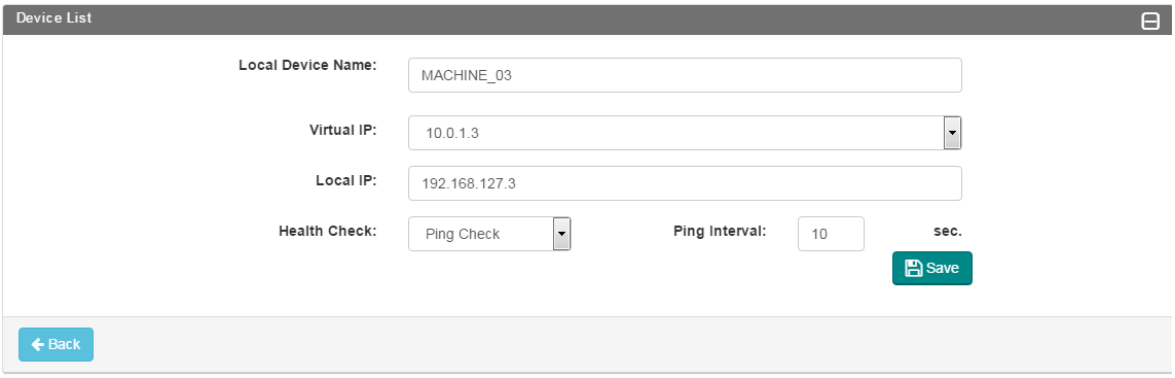
WARNING

Removing all the devices and leaving the whitelist empty will change the gateway to Site-to-Site mode for the remote access of the whole LAN subnet.



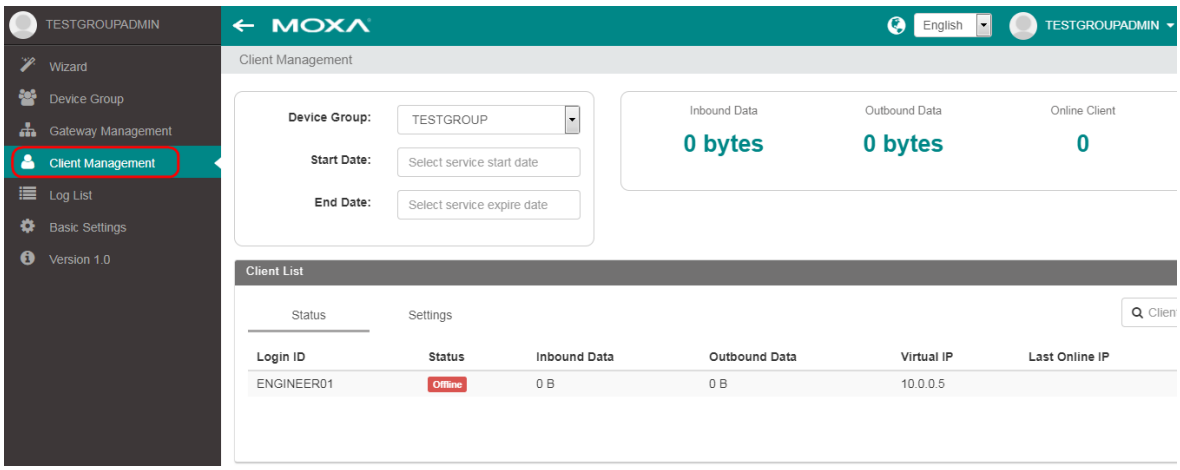
Click  to modify the settings of the device.





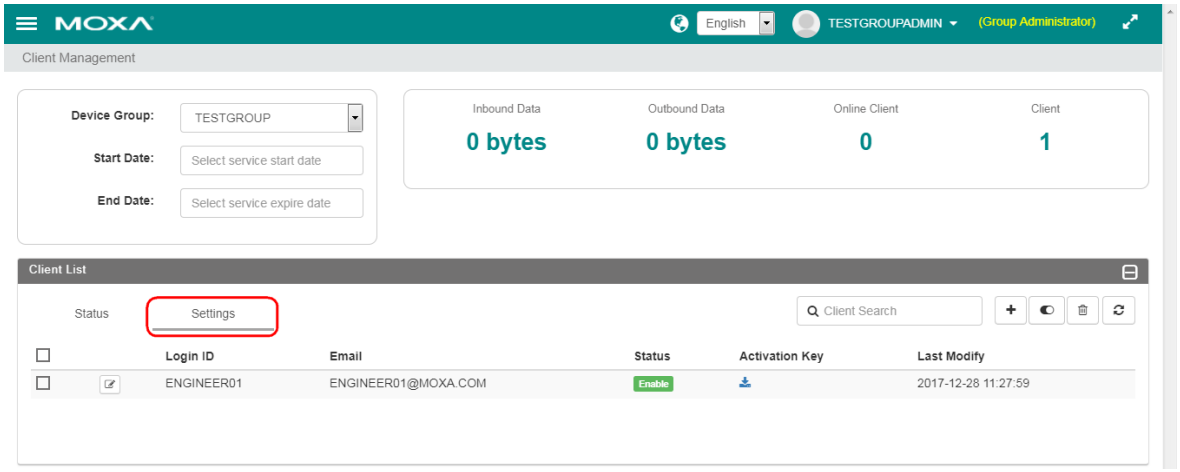
Client Management in a Device Group

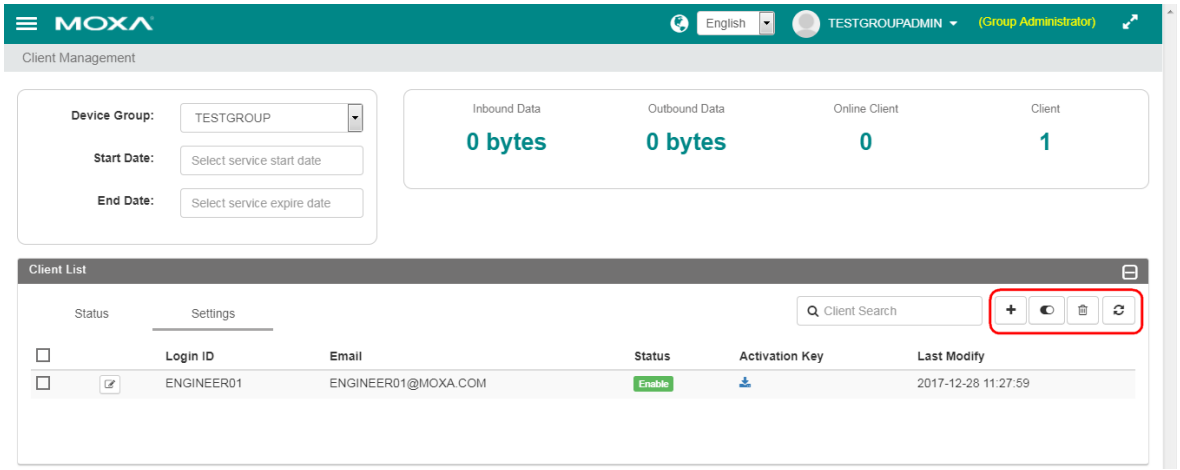
Go to "Client Management" from the main menu to monitor the status and set up the client accounts in the device group for PC-based devices (e.g. data server, engineer's laptop.) to connect with a MRC Server.



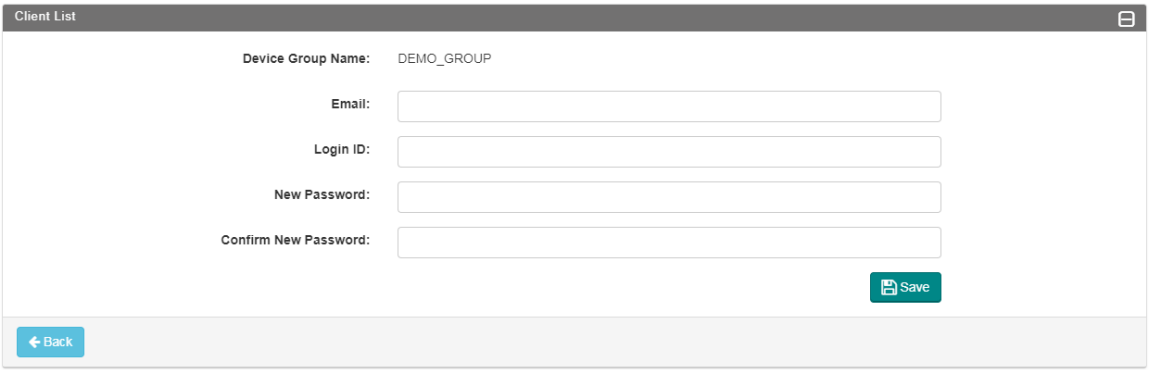
Add a Client Account

Click "Settings" to add or remove the clients. Click + to add a new client account, and click 🗑 to remove the selected clients. Click ⏻ to enable/disable the client service for remote access. Click the "REFRESH" button to get the updated information.



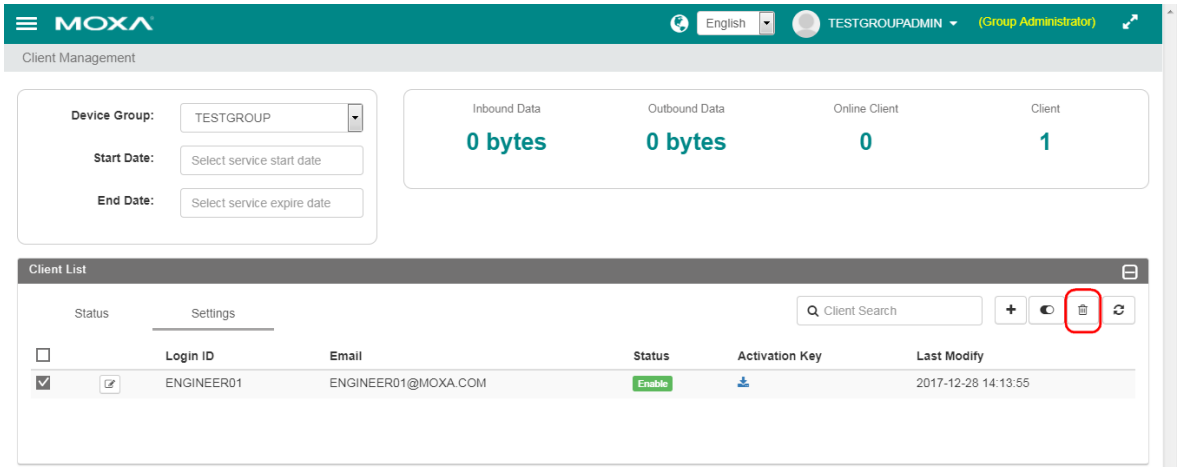


When adding a new client account, the email and Login ID of the client account should be unique in the MRC portal without any duplications.



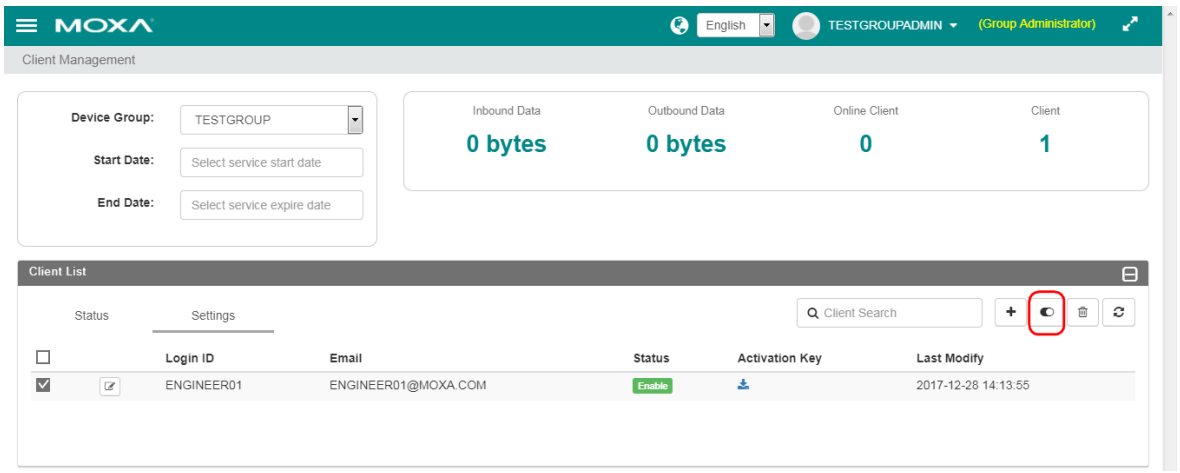
Remove a Client Account

Tick and select a client account before clicking to remove it from the client list.



Enable/Disable Clients

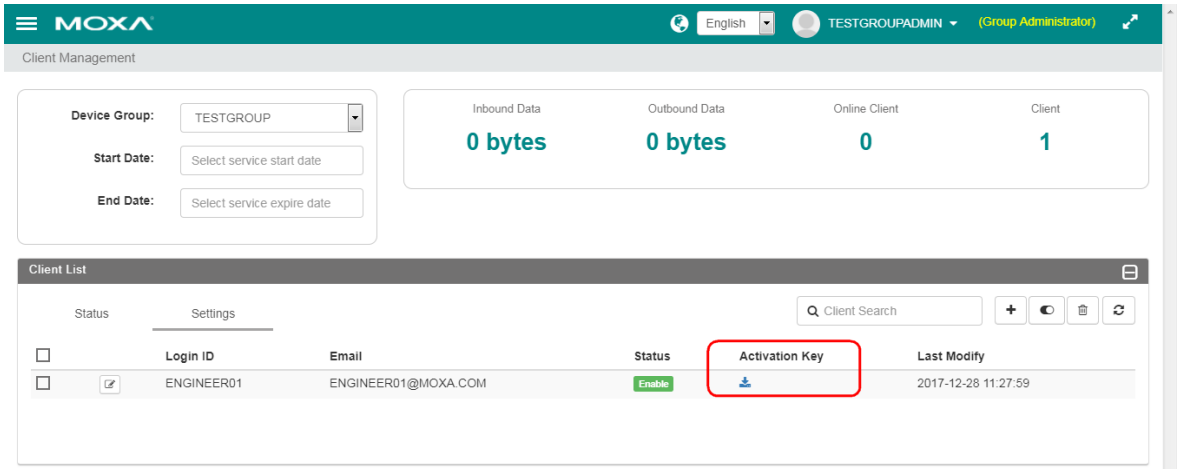
Click  to enable or disable the remote access service of the selected clients.



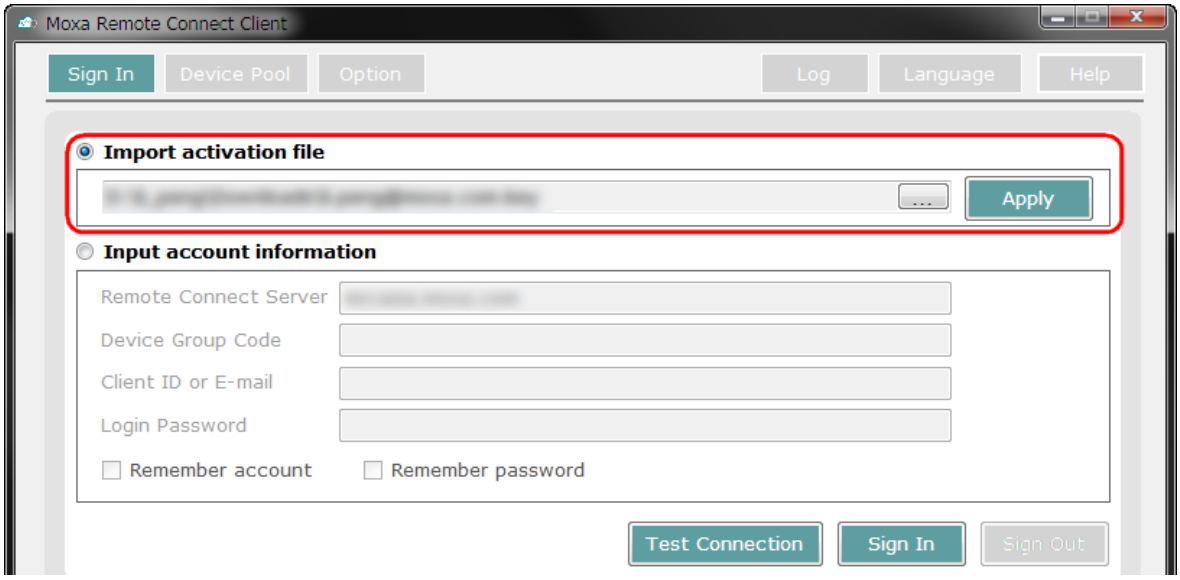
Download an Activation Key for a Client

After creating a client in the device group, the group administrator should download the activation key and send it to the user, for example the service engineer, loading it into MRC Client software to authenticate the laptop for remote access to the field machines through the MRC Server. (Refer to Moxa Remote Connect Client Software User Guide.)

Step 1: Click to download the activation key.

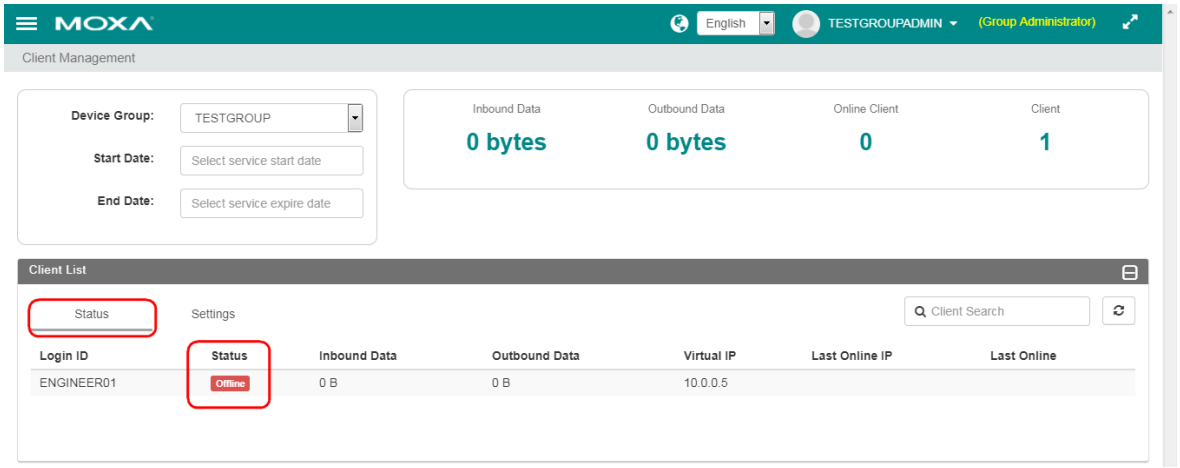


Step 2: Send the key to your engineer who will load the key into the MRC-Client software.



Monitor a Client Status

The group administrator can also check the online and offline status of the individual client connection.



8

Traffic Routing and Data Security

All end-to-end traffic through the MRC platform is encrypted using the AES-256 encryption method. The MRC server only redirects these encrypted packets to their own destination without decryption or storing the data between the client and the gateway. The network traffic is routed and broadcasted only within one device group, and that of different device groups are isolated from each other. In addition, the database of gateways and client accounts is also isolated within one device group.