



User Manual

Printed copy for reference only. For the most up-to-date information, please refer to the online help.

Revision Date: April 8, 2024

Table of Contents

- Overview
 - Shield Guard
 - Licensing Requirements
 - System Requirements
 - Device Requirements
- Setting Up Shield Guard
 - Acquiring the Shield Guard Service
 - Shield Guard Tenants
 - Acquiring the Shield Guard Agent
 - Installing the Shield Guard Agent
 - Completing the Installation
- Using the Shield Guard Portal
 - Accessing the Portal
 - Home Page
 - Plans Page
 - Password Vaults
 - My Profile Page
 - Admin Area
 - Select a Tenant Page
 - Licensing Page
 - Portal Page Elements
 - Dashboard Page
 - Users Page
 - Settings Page
- Managing Devices
 - Overview of Devices
 - Importing Devices

- Creating Device Groups
- Assigning a Policy to Devices
- Viewing and Maintaining Devices
- Managing Policies
 - Managing Security Policies
 - Password Management
- Reports and Logs
 - Overview
 - Shield Guard Reports
 - Shield Guard Logs
- Reference
 - Troubleshooting
 - Frequently Asked Questions (FAQ)

Overview

Shield Guard

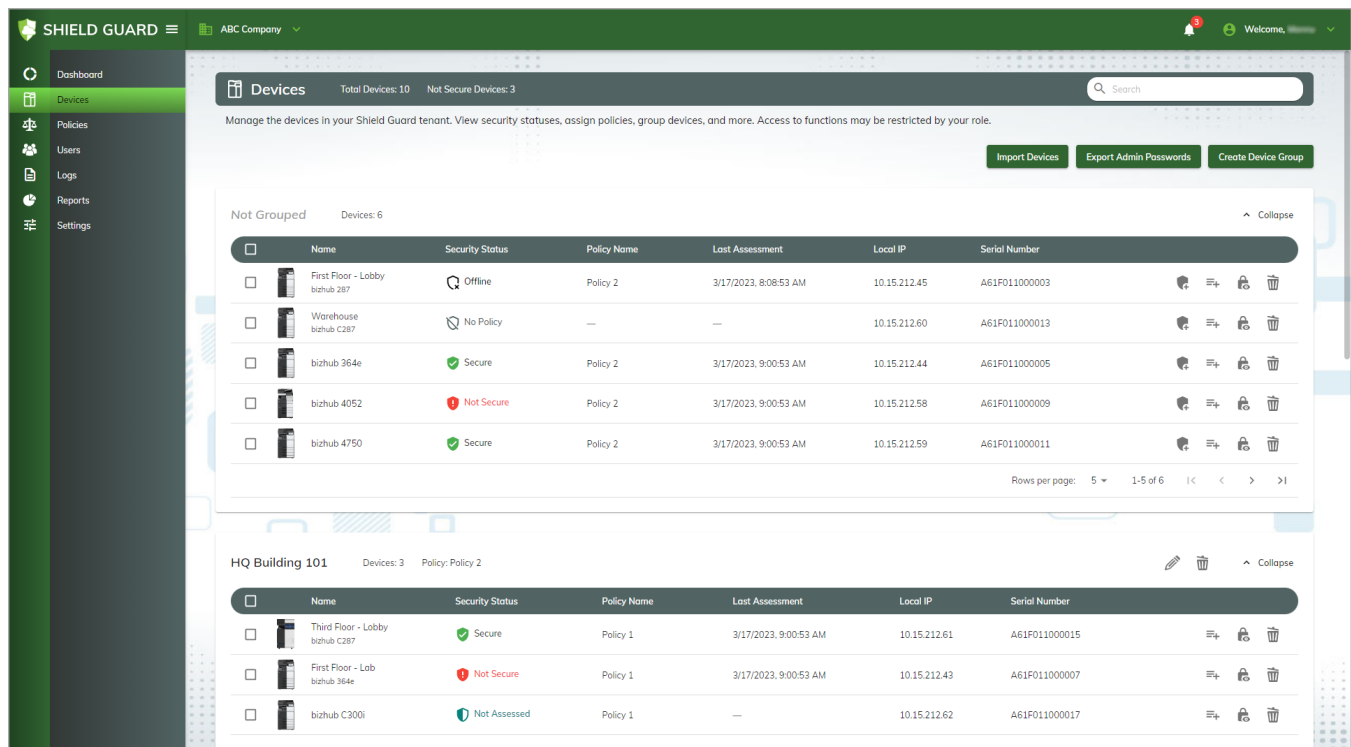


Shield Guard is a cloud-based, online, device fleet security service that enables organizations to remotely monitor and manage the security status of one or more **devices**, strengthening control over **device security**. With Shield Guard, you no longer need to physically access your devices to monitor their security. Instead, Shield Guard's online service enables you to simultaneously monitor and manage all the devices in your fleet - remotely, via the cloud.

Shield Guard is fully integrated with MarketPlace, and is available to purchase and install from the **MarketPlace website**. For information on **Shield Guard plans**, access the **Shield Guard Home page** and click on the **CHOOSE YOUR PLAN** button.

Note: This Online Help website describes all available Shield Guard features (that is, the features in the Shield Guard **Enterprise license plan**). If your Shield Guard plan does not include all features, the Help may describe features not available to you.

The following illustration shows the **Devices page** from the Shield Guard Portal, listing several devices in a sample Shield Guard license plan (the Enterprise plan).



Name	Security Status	Policy Name	Last Assessment	Local IP	Serial Number
First Floor - Lobby bizhub 287	Offline	Policy 2	3/17/2023, 8:08:53 AM	10.15.212.45	A61F011000003
Warehouse bizhub C287	No Policy	—	—	10.15.212.60	A61F011000013
bizhub 364e	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.44	A61F011000005
bizhub 4052	Not Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.58	A61F011000009
bizhub 4750	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.59	A61F011000011
Rows per page: 5 1-5 of 6					
HQ Building 101 Devices: 3 Policy: Policy 2					
Name	Security Status	Policy Name	Last Assessment	Local IP	Serial Number
Third Floor - Lobby bizhub C287	Secure	Policy 1	3/17/2023, 9:00:53 AM	10.15.212.61	A61F011000015
First Floor - Lab bizhub 364e	Not Secure	Policy 1	3/17/2023, 9:00:53 AM	10.15.212.43	A61F011000007
bizhub C300i	Not Assessed	Policy 1	—	10.15.212.62	A61F011000017

Note the following:

- The **Title bar** indicates the current **tenant** is the ABC Company.
- The **Navigation pane** on the left shows the pages available in the **Admin area**.
- The **Information bar** indicates the tenant contains a total of ten devices, three of which are currently **assessed as Not Secure**.
 - Six of the devices belong to the Not Grouped table, indicating that currently they are not part of any **device group**. Five are visible in the illustration. The sixth device could be viewed by viewing the next page in the table (by clicking on the right arrowhead on the table footer).
 - Three of the devices appear in the HQ Building 101 device group table, indicating that currently they are part of that device group.
 - One device does not appear due to space limitations in the illustration.

About Shield Guard

Shield Guard monitors the **security policy settings** of **supported Konica Minolta MFPs (multi-function peripheral devices) and SFPs (single-function peripheral devices)**. Shield Guard consists of the following components:

1. **Shield Guard Service** - An online platform that enables users to remotely monitor the security settings of any device on which the Shield Guard Agent is installed. The online platform is known as the Shield Guard Portal. The website address is:

getshieldguard.com/

Anyone with a MarketPlace account can access the portal to view purchasing options. Members of a Shield Guard **tenant** can access additional areas of the portal based on their assigned **role(s)** in the group.

2. **Shield Guard Agent** - Once **installed on a device and then launched**, the Shield Guard Agent communicates with the Shield Guard Portal at user-defined intervals. The agent:
 - a. Receives and stores security policy settings from the Shield Guard Portal.
 - b. Compares the configuration of the device's security settings with the configuration of the corresponding settings in the policy.
 - c. Reports any device settings that do not comply with the policy, and/or any policy settings that were changed since the last **heartbeat sync**, back to the portal as part of the agent's **device check**.

Thus, the agent and the portal communicate regularly. If all settings match, the portal assesses the device as Secure. If one or more settings do not match, the portal assesses the device as Not Secure.

Monitoring the Security of Devices in a Tenant

After each policy assessment, the portal updates the current **security statuses** of the devices in the tenant and displays the information in several areas of the portal, including the following:

- **Dashboard page** - Displays an at-a-glance overview of the tenant's device security.
- **Devices page** - Displays the security status of each device in the tenant.
- **Logs page** - Displays detailed information on security logs recorded by Shield Guard, including any individual settings that failed a policy assessment.

Elements of a Shield Guard Tenant

Use of Shield Guard requires the purchase of the following:

- A Shield Guard Service **license plan** - At the time of purchase, you must also specify a **billing method**.
- One or more **device licenses** - one for each device you want to monitor.
- The free Shield Guard **agent** - one for each device you want to monitor.

The purchase of the service creates a **tenant** for the plan. The following sections provide overviews of the main elements of a tenant.

Licenses

Shield Guard is licensed by **device** (not, for example, by user). Once you purchase a **license plan**, you can add devices to the tenant created by the purchase. To add a device to a tenant, the following must be true:

- The Shield Guard Agent must be currently installed on the device (in order for MarketPlace, and the Shield Guard Portal, to connect to the device).
- A device license must be available in the tenant.

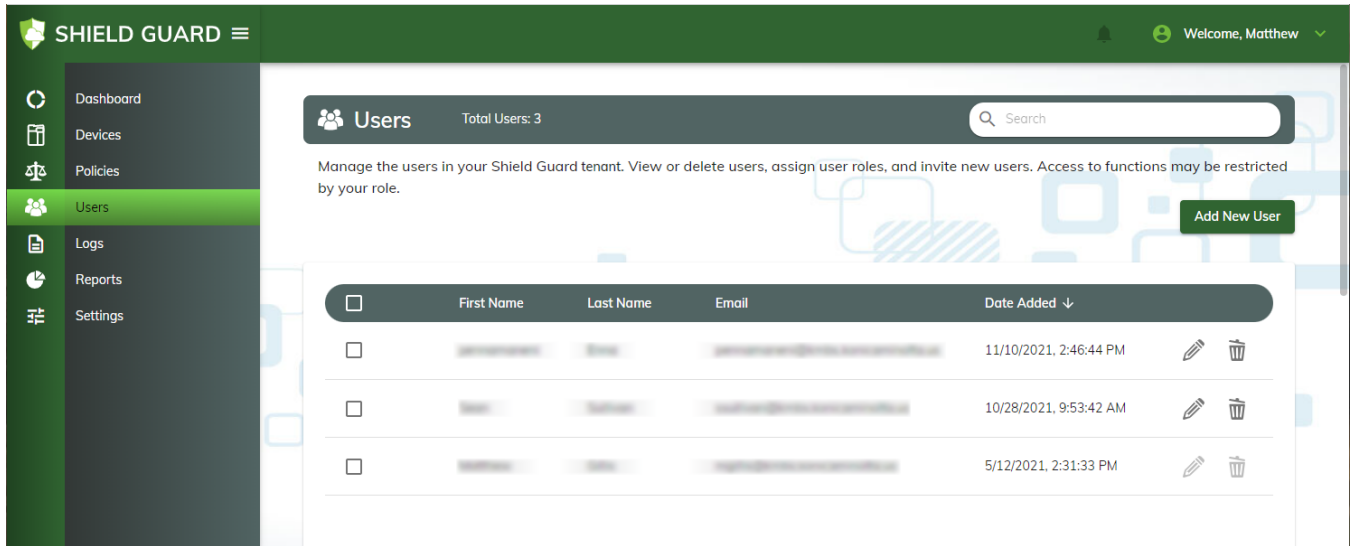
You can purchase device licenses as part of your purchase of a license plan, and/or you can purchase device licenses for an existing tenant at any time. The number of device licenses you purchase determines the maximum number of devices you can add to the group. Note that you can also remove devices from a tenant to make their licenses available for assignment to other devices.

The purchaser of the Shield Guard Service (that is, a license plan) becomes the **owner** of the tenant and has full access to the portal, including the **Users page** via which other users can be invited to join the group. Users invited to join the group do not need to purchase a license plan.

Users

Shield Guard tenants can contain an unlimited number of **users**. The purchaser of the license plan (the group owner) can invite others to join the group. Each invitation includes a **role assignment** within the tenant for the invitee. Roles determine the pages of the Shield Guard Portal a member

can access. For example, only tenant members with access to the Users page can invite others to join the group. The following illustration shows the Users page.



Password Vaults

In addition to **roles**, Shield Guard restricts user access to pages in the portal by means of **password vaults**. Shield Guard requires each tenant member to create their own password vault in which to store their sensitive data. The Create Vault window appears automatically for this purpose. Thereafter, in each Shield Guard session, tenant members must first unlock their vault before accessing any vault-protected pages in the portal. The Unlock Vault window appears automatically for this purpose.

Create Vault



All Shield Guard tenant members must create a vault with a master key to store their Shield Guard data and protect their tenant from unauthorized access. You will use your vault master key to unlock the vault each time you access Shield Guard.

Management Type

Decentralized Key Management

Security

Convenience

Decentralized Key Management requires you specify a vault master key and then provide it each time you open a Shield Guard session. If you lose your vault master key and its recovery key, only a member of the same tenant can restore your access to your vault and the password data stored within. For more information, refer to Shield Guard Online Help.

Master Key

|

Confirm Master Key

CREATE

Unlock Vault

Please enter your master key to unlock your vault.

Master Key

Forgot master key?

UNLOCK

Note: The Unlock Vault window appears only for tenant members using the Decentralized method for vault key management. For tenant members using the Centralized method, Shield Guard unlocks the vault automatically.

Devices

Shield Guard supports all **MarketPlace devices**. To monitor devices in Shield Guard, you must **add them to a tenant**. To add a device to a tenant, the Shield Guard Agent must be installed on the device and an unassigned device license must be available in the group. Once added to a tenant, you can **assign a security policy to the device** and device monitoring can begin.

Import Devices from MarketPlace

Import devices from MarketPlace to your Shield Guard license plan here. Select one or more available devices and use the Arrow button to add them to Shield Guard.

Note: The list of available devices is restricted to devices in your MarketPlace account with the Shield Guard agent installed.

<input checked="" type="checkbox"/> Available Devices 1/5 selected	<input type="checkbox"/> Selected Devices 0/0 selected
<input checked="" type="checkbox"/> Second Floor - QA (C556) A61F0114002047	
<input type="checkbox"/> Second Floor - Lab (C554) A61F011400234	
<input type="checkbox"/> C358 A31F011400204	
<input type="checkbox"/> C354 A31F011400234	
<input type="checkbox"/> Second Floor - Dev (C558) A61F011400204	
<input type="checkbox"/> C356 A31F0114002047	

>

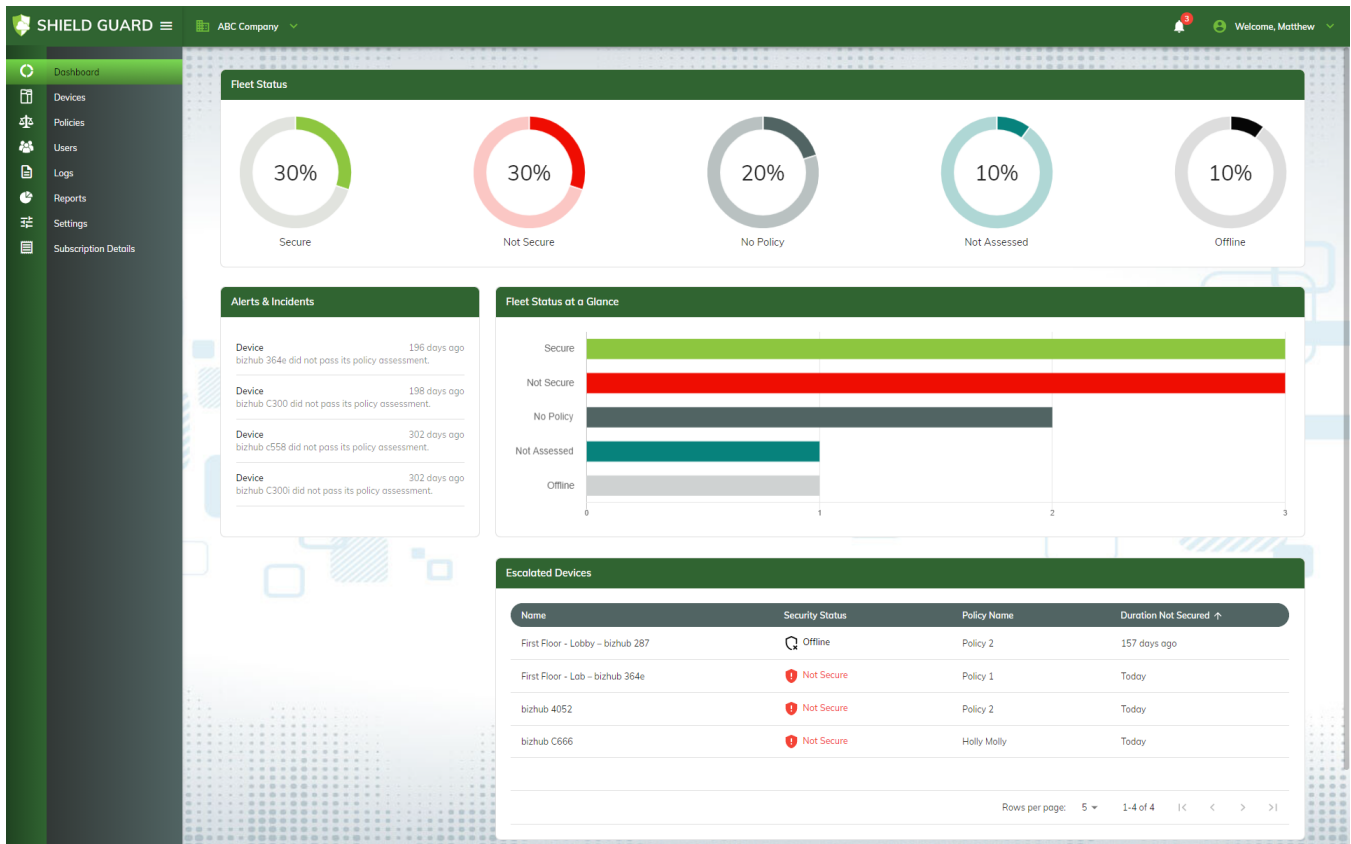
<

IMPORT

Note: Devices can belong to only one tenant at a time.

Policies

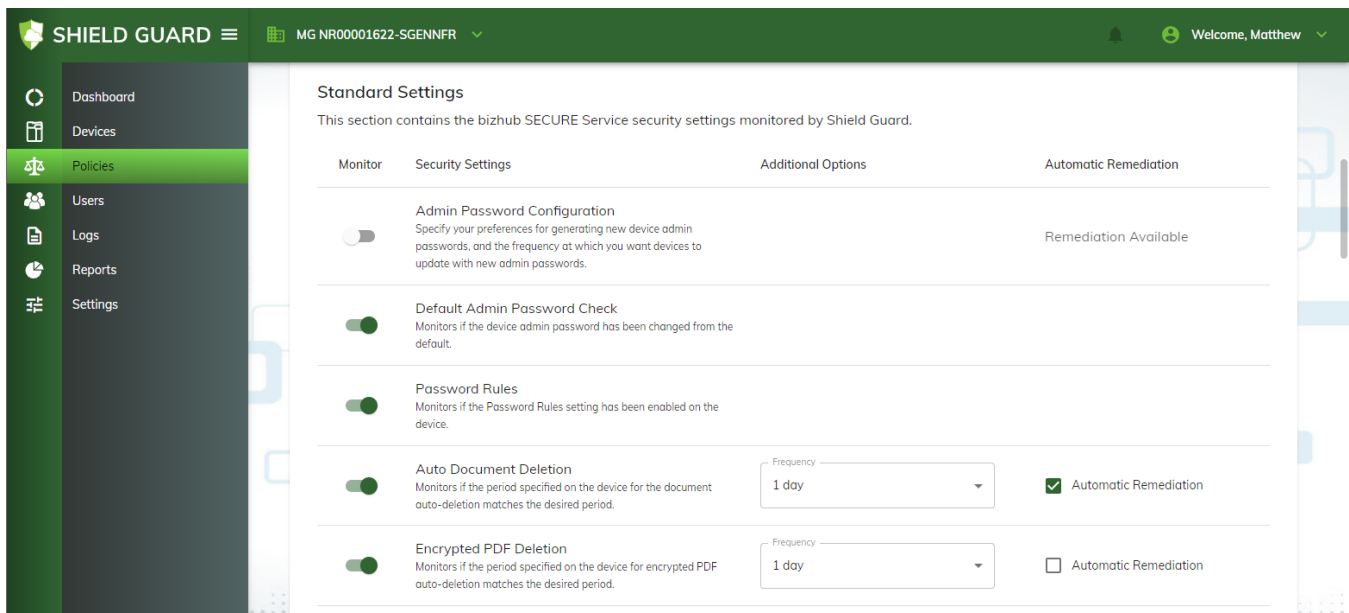
Shield Guard supports device security settings protected by bizhub **Standard**, **Platinum**, and **Ultimate**. You can **create** as many **security policies** as you like. For each policy, you toggle on the Shield Guard security settings you want to monitor on a group of devices, then assign the policy to the devices. For each setting toggled on in the policy, Shield Guard monitors the corresponding device setting at a user-defined interval (for example, every hour). If non-compliant settings are found on a device, the Shield Guard Portal updates with the information to alert tenant members so corrective action can be taken. The following illustration shows the **Dashboard page**, providing an overview of the security statuses of devices in a tenant and indicating that several are currently assessed as Not Secure:



Automatic Remediation

Many Shield Guard policy settings include an option to **automatically remediate** the device's corresponding setting if in a non-compliant state. Shield Guard will automatically modify the device setting to match the policy setting. If automatic remediation is not active for a setting, or the setting does not support automatic remediation, the setting must be changed manually, at the device, to return it to a compliant state.

The following illustration shows the Policies page. The Automatic Remediation column indicates the policy settings that support automatic remediation. In this illustration, automatic remediation is enabled for the Auto Document Deletion setting:



Policy Settings and Communication Frequency

For each policy, you select the device settings you want to monitor. In addition, you specify the **frequencies** at which:

- The Shield Guard Agent communicates with the Shield Guard Portal to update the agent with any changes made to the policy. This is called the “server heartbeat sync frequency”.
- The Shield Guard Agent performs a device check, comparing the current statuses of the device settings monitored by the assigned policy to the configurations of the settings in the policy. This is called the “Check MFP local settings frequency”.
- The Shield Guard Portal assigns the status of “Offline” to a device because the agent has not communicated with it within a specified amount of time. This is called the “Offline threshold”.

<p>Server heartbeat sync frequency Specify how often you want the agent to contact the portal. Changes to assigned policies will be reported to the agent on the device at this frequency.</p> <p>Frequency <input type="text" value="5 minutes"/></p>	<p>Check MFP local settings frequency Specify how often you want the agent to run a device self-check. Any settings found not to be in compliance with the Shield Guard policy are reported to the portal.</p> <p>Frequency <input type="text" value="1 minute"/></p>	<p>Offline threshold Shield Guard reports a device as offline if it has not received communication from the MFP after the number of heartbeats configured below.</p> <p>Tolerance <input type="text" value="3"/></p>
---	--	---

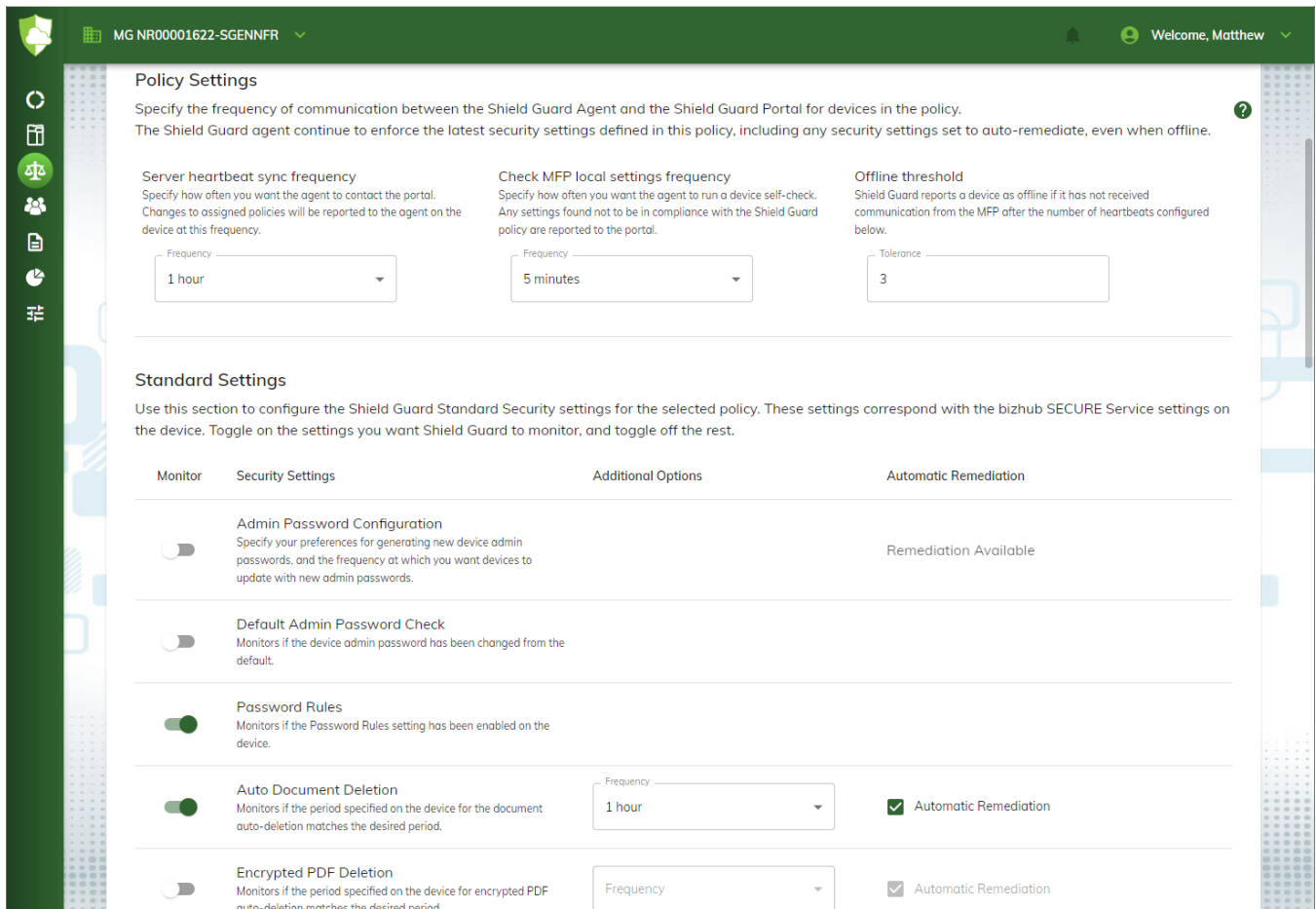
Note: The Shield Guard Agent runs only when the **Shield Guard screensaver** is running on the device.

A Sample Custom Security Policy

The following is a policy scenario outlining the basic steps Shield Guard performs when monitoring and maintaining security for devices assigned to a security policy. The scenario describes a typical communication frequency configuration between portal and device. Two settings are toggled on, including one with automatic remediation active.

Assume the following scenario for a Shield Guard policy:

- The Server Heartbeat Sync Frequency is set to one hour.
- The Check MFP Local Settings Frequency is set to five minutes.
- The Password Rules setting is toggled on.
- The Auto Document Deletion setting is toggled on, with the deletion frequency set to one hour and the **Automatic Remediation** option enabled.
- All other policy settings are toggled off.



In this scenario, the following occurs:

1. Every hour, the agent pings the portal. If any of the policy's settings on the portal have been modified since the last heartbeat sync, the agent updates with the new settings.
2. Every five minutes, the agent performs a device check of the device's security settings. As part of the device check, the agent:
 - a. References the policy settings acquired in the most recent heartbeat sync, checking only the settings that are toggled on in the policy.
 - b. Performs **automatic remediation** on any device settings for which:

- Automatic remediation is enabled in the policy.
- The device setting is not compliant with the policy setting.

Note: The device must also support the Automatic Remediation feature.

c. Searches for any device settings that have changed (whether manually at the device or through automatic remediation) since the last device check. If any device settings have changed, the agent reports to the portal the current status of all device settings monitored by the policy.

3. The portal performs an assessment of the security policy. If any device settings are not compliant with the policy settings, Shield Guard assesses the policy as Not Secure.

Note: If the device check finds no changes to the device settings, the agent does not report to the portal and no policy assessment is made.

4. If, after 3 heartbeat syncs (the 3 being specified at the Tolerance field), the agent has not communicated with the portal, the portal assumes the device is asleep or powered off, and assigns the device a status of Offline.

Further assume that the agent found the device's Password Rules setting to be enabled and thus in compliance with the security policy. However, the agent found the device's Auto Document Deletion setting to be enabled but set to a deletion frequency of one day (24 hours). As a result:

- The Auto Document Deletion setting on the device is not compliant with the policy setting.
- The agent automatically remediates the device setting to match the policy setting of 1 hour. Because one or more device settings were changed, the agent reports the change to the portal and the portal performs an assessment of the policy. Because the agent remediated the device setting to match the policy setting, Shield Guard assesses the setting as compliant and the device as Secure.
- However, if automatic remediation did not occur (for example, the device does not support automatic remediation), the agent would report to the portal that the device setting is not compliant with the policy and the portal would then assess the device as Not Secure.

Licensing Requirements

To use Shield Guard, the following licenses are required:

1. A **Shield Guard Service license plan**.
2. A Shield Guard device license for each device you want to monitor.

Shield Guard Service and Device licenses are available for purchase here:

konicaminoltamarketplace.com/market/product/sg-plans

3. One or more **Shield Guard Agent** licenses, available free of charge here:

konicaminoltamarketplace.com/market/product/moar

About Licenses

Shield Guard Service licenses are associated with Shield Guard plans. For information on the plans that are available for Shield Guard, access the **Plans page**. You can also access the Plans page via the **Home page**. On the Home page, click on the **CHOOSE YOUR PLAN** button.

When you purchase a plan, you also specify a **billing method** (subscription or term).

Note: Once you activate your Shield Guard license, you can view information on the associated **license plan** via the **Licensing** page on the Shield Guard portal.

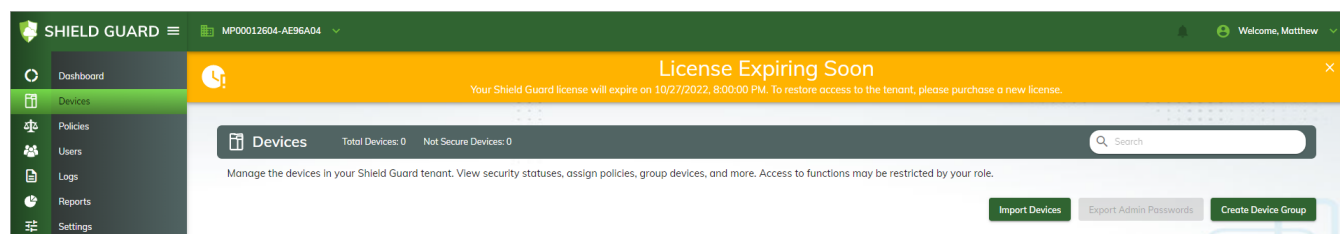
If Your License Expires

If your Shield Guard Service license expires, you must purchase a new license plan to continue using Shield Guard. To purchase a license plan, access the **Shield Guard product page** in MarketPlace, or contact your Shield Guard representative.

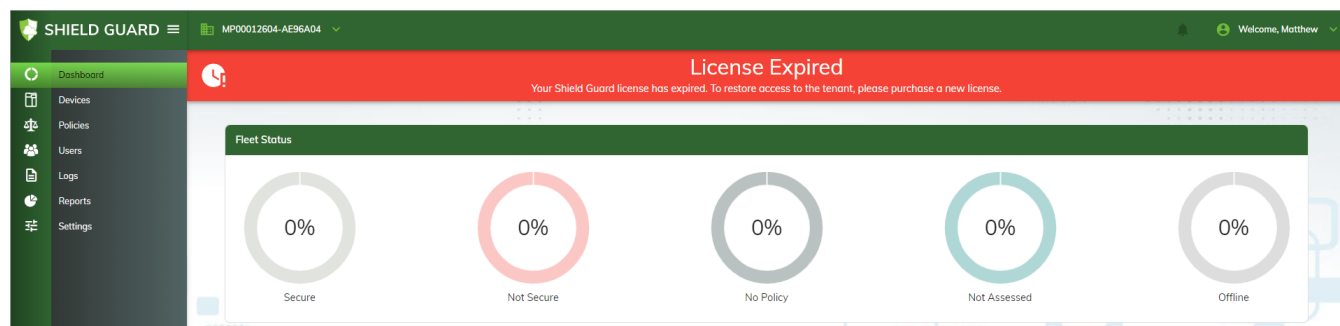
Note: If your license expires in one tenant but you have access to other tenants, you can continue to access any tenant for which you have an active license.

For **term licenses**, the expiration date is determined at the time of purchase. **Subscription licenses** run indefinitely until cancelled. Upon cancellation, the expiration date becomes the last day of the current billing period. For trial licenses, the expiration date is set at 30 days after purchase.

As your license's expiration date approaches, a "License Expiring Soon" banner will appear on all screens in the Shield Guard Portal, indicating the time at which your license will expire. See the following illustration:



If your license expires, a "License Expired" banner will replace the "License Expiring Soon" banner.

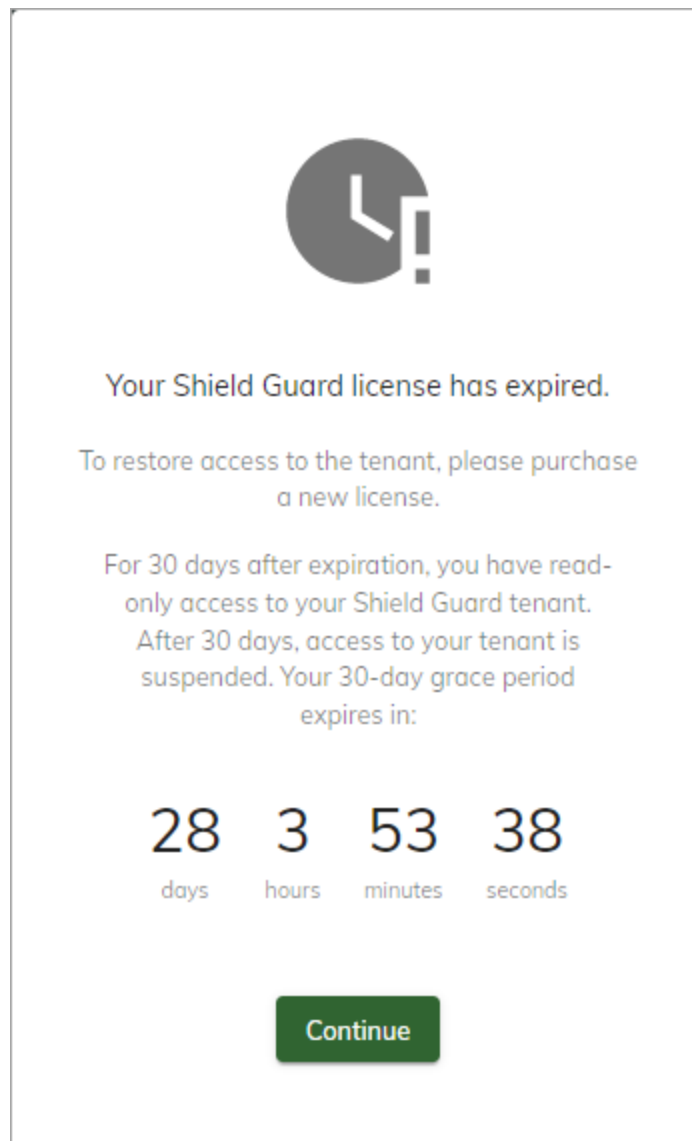


Grace Periods for Expired Licenses

Once a license expires, Shield Guard suspends all functionality for the tenant and deactivates all security policies in the tenant. A grace period begins, during which the tenant remains accessible but all tenant members are restricted to view-only access. Tenant members can also download CSV (comma-separated-value) files during the grace period, for example, via the **Export Admin Passwords** button.

- Expired paid licenses - 30-day grace period.
- Expired free-trial licenses - 15-day grace period.

At the time of expiration, a pop-up screen appears indicating the license has expired. A countdown timer displays, indicating the expiration date and time of the grace period. Going forward, the pop-up screen will appear each time you access the portal or, if you have access to multiple tenants, each time you access a tenant with an expired license. To exit the pop-up screen, click on the **Continue** button. See the following illustration:



During the grace period, tenant information remains preserved and, if a new license is purchased, can be transferred to the new license. If the grace period expires and a new license has not been purchased, access to the tenant is suspended. tenant information remains preserved for 60 more days.

Important! If the 60-day period expires and a new license has not been purchased, Shield Guard permanently removes all data and information associated with the tenant.

Shield Guard Plans

Shield Guard Service licenses are purchased as part of a Shield Guard plan. For information on the plans that are available for Shield Guard, access the **Plans page**. You can also access the Plans page via the **Home page**. On the Home page, click on the **CHOOSE YOUR PLAN** button.

System Requirements

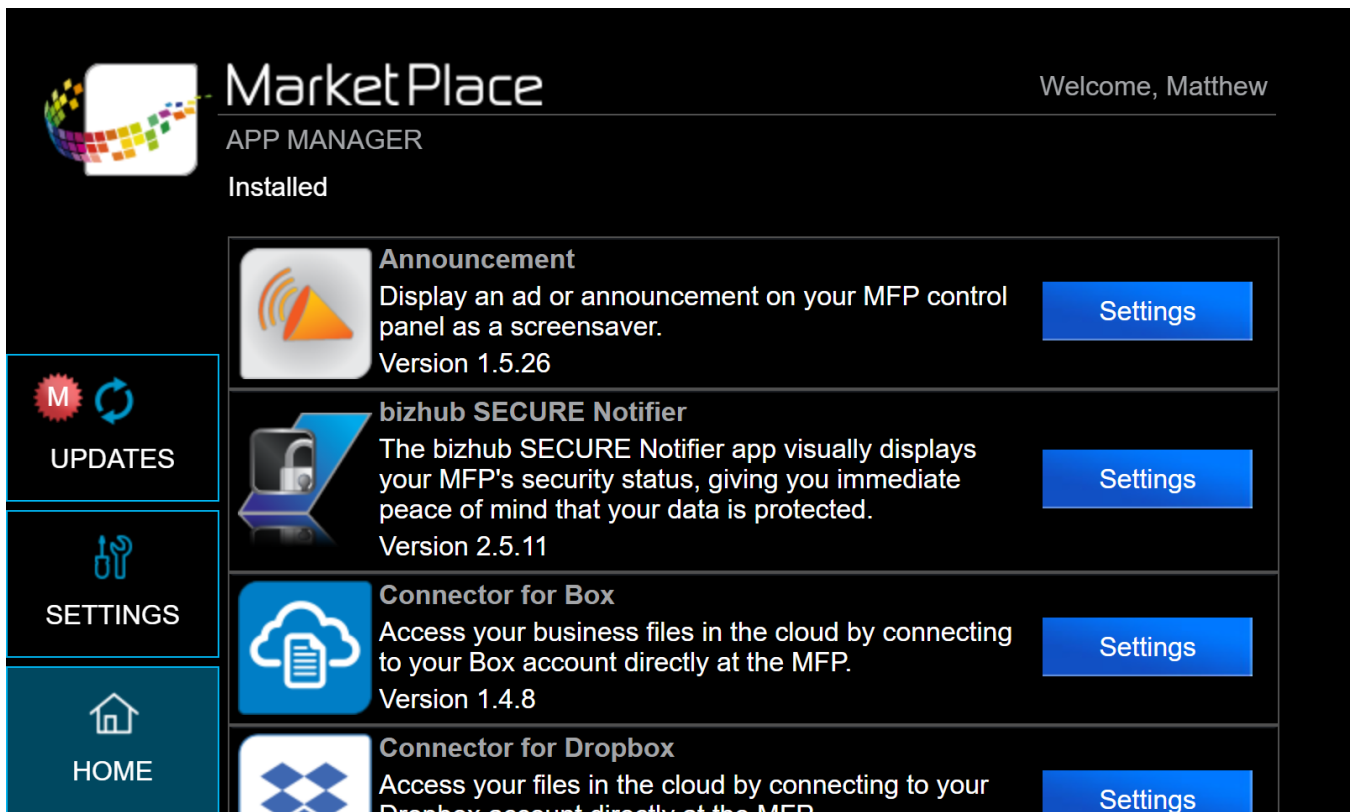
To install and access the **Shield Guard Service**, the following items are required:

- A **MarketPlace** account.
- A **Shield Guard Service license**.
- The **Shield Guard Agent** installed on each device you want to monitor.
- **MarketPlace Client** version 5.4.0 or later.

MarketPlace Client

Prior to installing the Shield Guard Agent, be sure to update MarketPlace Client to version 5.4.0 or later. To check for available updates, do the following:

1. Log in to MarketPlace's App Manager on your device(s). Once logged in, if a red "M" notification appears on the **Updates** button, an update to the MarketPlace Client is available.
2. To update to the newest version of the MarketPlace Client, tap on the **Updates** button. See the illustration below:



Note: You can also update MarketPlace Client using the MarketPlace **Auto Updates** feature.

Device Requirements

The following sections describe the requirements for devices using Shield Guard.

Supported Devices

For a list of devices that support Shield Guard, access the **Shield Guard product page** on the MarketPlace site.

Note: Some Shield Guard functionality is supported only on **i-Series devices**.

Connection Requirements

For a device to use Shield Guard, it must be connected to the internet.

In addition, the device must be able to connect to the following domain and port:

- device.getshieldguard.com
- port 443

Configuration Requirements

The following sections describe the configuration requirements for devices using Shield Guard. Note that to access these settings, you must be an **admin of the device**.

IWS Settings

Shield Guard supports only devices equipped with IWS (Internet Web Server). All **MarketPlace devices** are equipped with IWS. Be sure each device meets Shield Guard's **minimum requirement for IWS version**.

Device Admin Password Permissions

On each device running Shield Guard, set the "Password Change Permission" setting to "Allow".

The following lists the steps for the C4050i device. You can perform them at the device or via Web Connection.

1. At the device, log in to the device and access the Administrator Settings page.
2. Tap on Network.
3. Tap on IWS Settings.
4. Tap on Administrator Password Change Setting.
5. Tap on "MarketPlace".
6. Tap on the **Edit** button.
7. Set "Password Change Permission" to "Allow".
8. Tap on the **OK** button.

Notes:

- The steps for other devices may vary slightly. Please refer to the device's user manual.
- If the setting is not available in Web Connection, you must perform the steps at the device.
- Some older devices may automatically disable this setting. When troubleshooting issues with **Password Management** on a pre-i-Series device, be sure to confirm this setting is enabled.
- For all i-Series devices assigned to a policy, when you toggle on the Admin Password Configuration setting in the policy, Shield Guard will automatically configure the "Password Change Permission" setting on the device (see Step 7 above) to "Allow".

Setting Up Shield Guard

Acquiring the Shield Guard Service

The purchase of a **Shield Guard Service license plan** creates a **tenant** and provides **privileged tenant members** with access to the **Admin area** of the **Shield Guard Portal**.

To purchase a Shield Guard Service license plan, do the following:

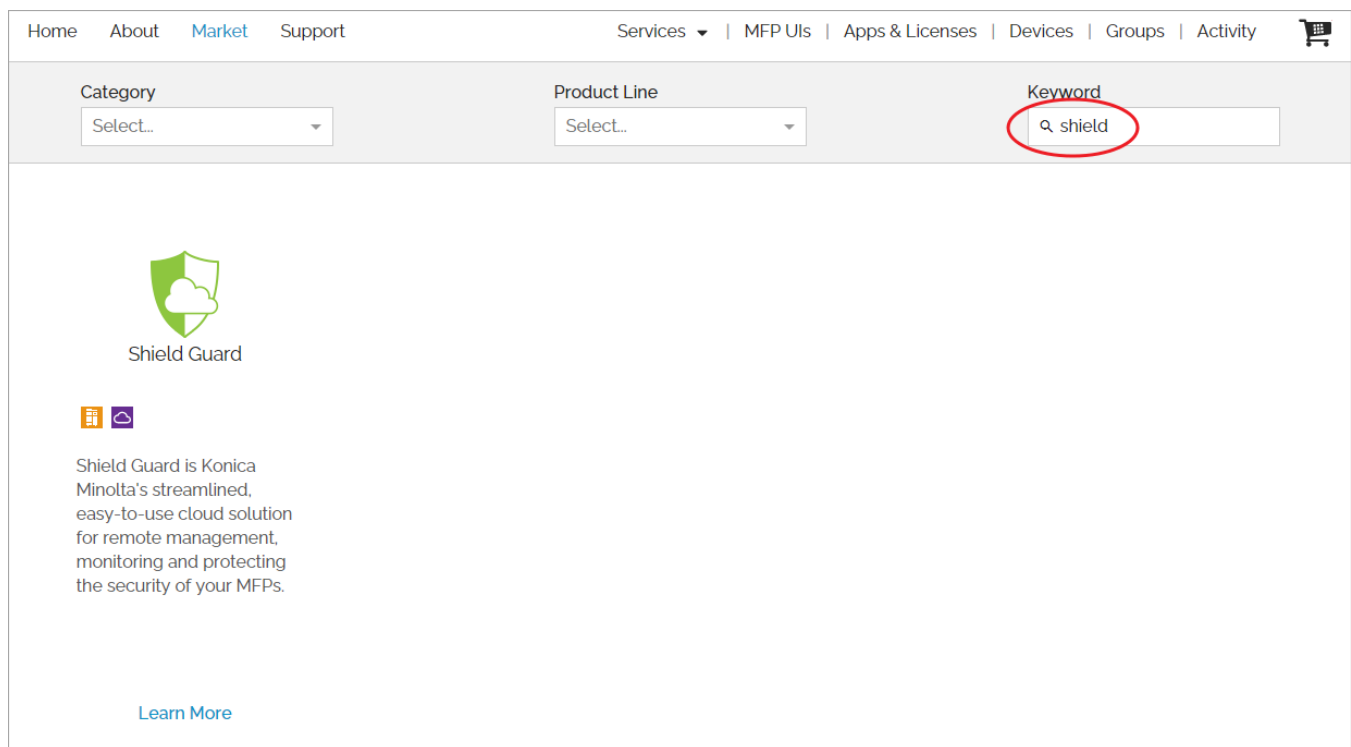
1. Access the MarketPlace site:

konicaminoltamarketplace.com/

2. Log in to your MarketPlace account.

3. Access the Market page.

4. Enter “shield” into the Search field. The Shield Guard card appears. See the following illustration:



5. Click on the Shield Guard card. The Shield Guard page appears with the Shield Guard Agent selected:

Select your *Shield Guard* product:

Shield Guard Agent	Shield Guard Service
--------------------	----------------------



Shield Guard Agent



\$0.00

-	1	+
---	---	---

Buy Now

6. Click on the **Shield Guard Service** button. The Shield Guard Service product page appears:

Select your *Shield Guard* product:

Shield Guard Agent	Shield Guard Service
--------------------	----------------------



Shield Guard Service



Demo

7. Click on the **Demo** button. A message appears indicating a Shield Guard Service demo license is now associated with your MarketPlace account. The demo license is valid for 30 days from activation and provides device licenses for up to 10 devices.
8. The activation of the Demo license creates a tenant, of which you are the owner. To begin configuring your tenant, access the Shield Guard Portal here:

getshieldguard.com/

Note: Only one demo license is available per MarketPlace account.

Shield Guard Tenants

The purchase and activation of a **Shield Guard Service license plan** creates a Shield Guard tenant. The tenant:

- Provides user access to the Admin area of the Shield Guard portal, where remote management of device security is conducted. Only authorized users can access a tenant and the functionality in the Admin area.
- Stores the data collected by Shield Guard - data generated by the users, devices, and policies that have been added to the tenant. All collected data is protected within the tenant, with access restricted to authorized users.

Note: Once you activate your Shield Guard license, you can view information on your **license plan** via the **Licensing** page on the Shield Guard portal.

Shield Guard tenants consist of the following:

- **Devices - MarketPlace-authorized devices** added to a Shield Guard tenant.
- **Policies** - Sets of device security check parameters. Each policy contains settings that correspond to the security settings available for supported Konica Minolta MFPs (multi-function peripheral devices) and SFPs (single-function peripheral devices).
- **Users** - Members of the Shield Guard tenant. A member's **role** determines their access privileges in the portal.

See Also: Elements of a Tenant

Multiple Tenancies

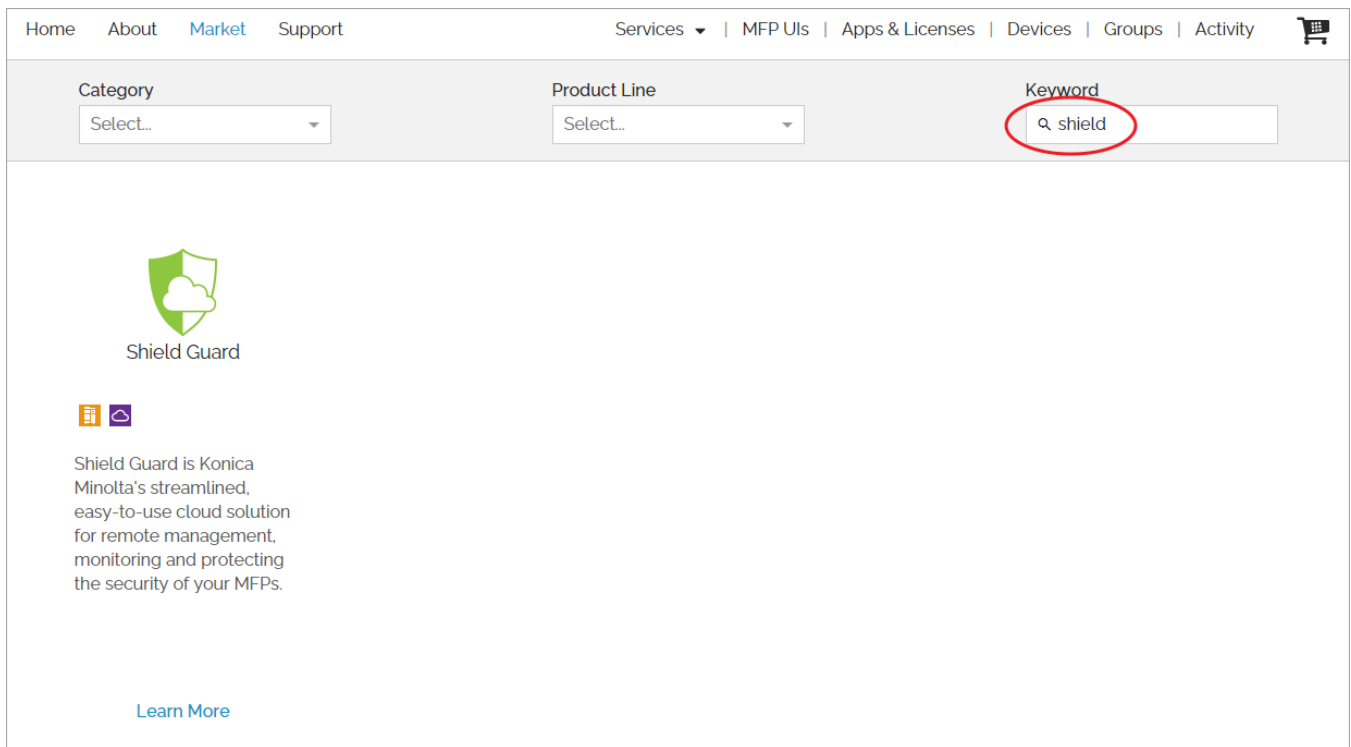
The vast majority of organizations using Shield Guard will require only one tenant to manage the security of their MarketPlace devices. However, if you purchase and activate multiple licenses, each tenant created is added to your portal. When you login to the **Admin area**, the **Select a Group page** appears where you can select a tenant to view and edit. Once in the Admin area, you can change to another tenant using the **Shield Guard Tenant button**. Only one tenant can be open at a time.

Acquiring the Shield Guard Agent

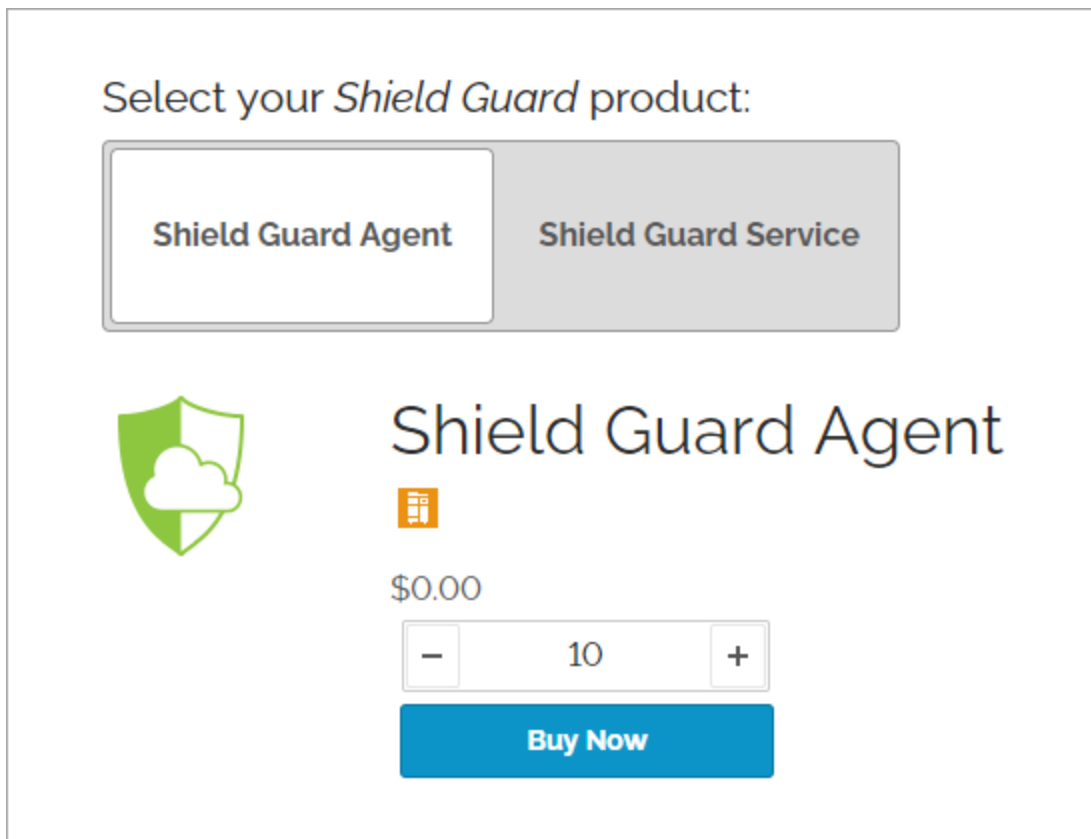
The Shield Guard Agent is free of charge with a MarketPlace account. You must install it on each device you want Shield Guard to monitor. Once **installed and launched on a device**, the device (that is, the agent) can then communicate with the Shield Guard Portal.

To acquire one or more Shield Guard Agents, do the following:

1. Go to the MarketPlace website:
konicaminoltamarketplace.com/
2. Log in to your MarketPlace account.
3. Access the Market page.
4. Enter “shield” into the Search field. The Shield Guard card displays on the page. See the following illustration:



5. Click on the Shield Guard card. The Shield Guard page appears with the Shield Guard Agent selected:



6. Specify the number of agent licenses you want to acquire.

7. Click on the **Buy Now** button and follow MarketPlace's checkout process. When complete, you can **install the agents on your devices**.

Once you purchase a Shield Guard **license plan** and device licenses for each device you want Shield Guard to monitor, you can then add the devices to your tenant and assign a security policy to the devices. Device monitoring can then begin.

Installing the Shield Guard Agent

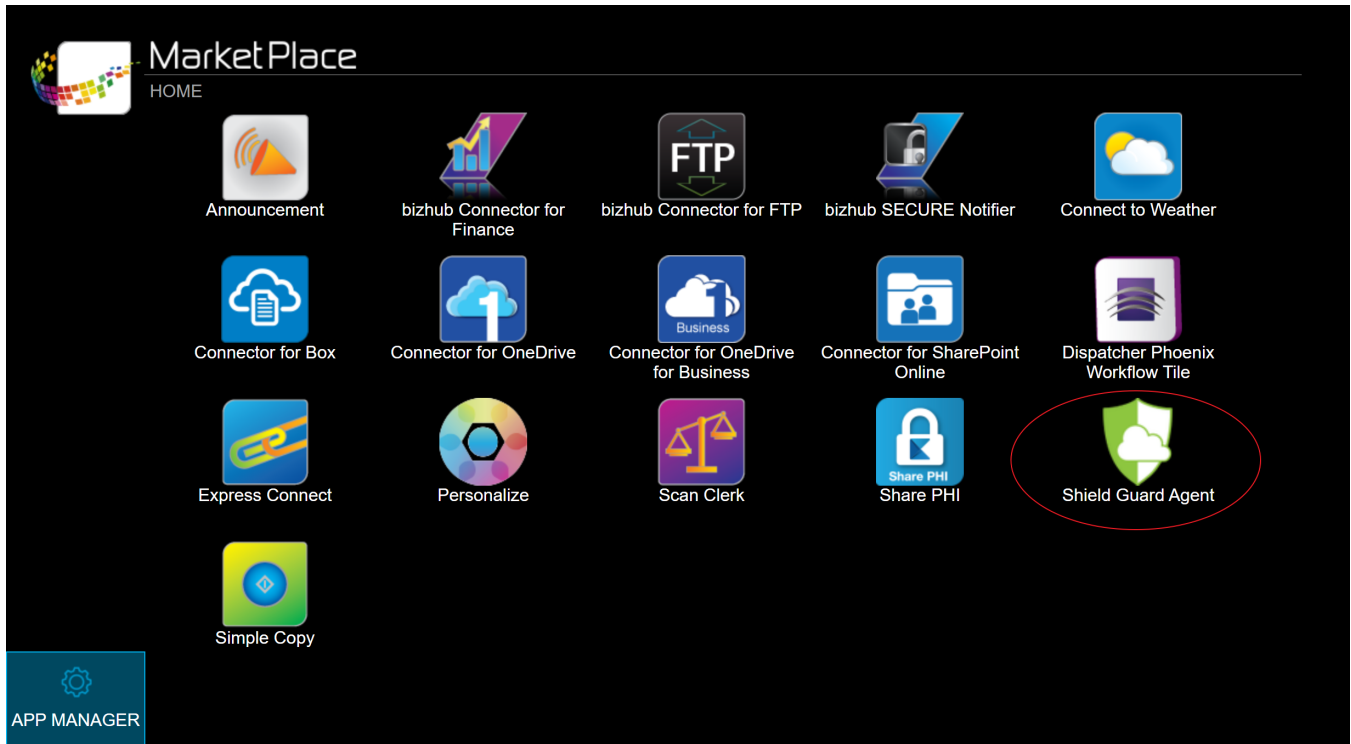
Similar to MarketPlace apps, you have the following options when installing the Shield Guard Agent on your devices:

- **Use the MarketPlace website**
- **Use the App Manager at the device panel**

Note: Prior to installing the Shield Guard Agent on your devices, refer to the **Device Requirements** topic for a list of supported devices. This topic also describes the **configuration requirements** for devices running Shield Guard.

Once you **install and launch the agent on a device**, the device can communicate with the **Shield Guard Portal** and the device becomes available for **import** into a **tenant**.

Once installed, the agent requires no further configuration. The Shield Guard Agent icon appears on the device's App menu, as shown in the image below.



If you tap on the icon, the agent launches and the Shield Guard splash screen displays. The splash screen displays the same image as the Shield Guard **screensaver** displays. To exit the splash screen, click on the MarketPlace icon.

Launching the Agent

Shield Guard requires the agent to be running in order for the agent to communicate with the portal (and for the portal to communicate back to the agent). The agent launches in the following ways:

- Automatically when the **Shield Guard screensaver** is active on a device.
- Manually when you tap on the Shield Guard icon on the device's Home page.

Once launched, the agent communicates with the portal at **user-defined time intervals** specified in the Shield Guard policy.

Screensaver

The Shield Guard Agent **launches** automatically when the Shield Guard screensaver launches on a device. The screensaver runs serially along with any other MarketPlace screensavers active on the device.

The Shield Guard screensaver runs as part of the MarketPlace Screensaver app. If any other screensaver app is enabled on a device, you must instead enable the MarketPlace Screensaver app

before the Shield Guard Agent can run on the device. The agent can communicate with the portal only when the Shield Guard screensaver is active on the screen, and not when other screensavers are active on the screen.

See the following illustration:



Updating the Agent

We recommend you always install the latest version of the Shield Guard Agent on your devices. MarketPlace's **Auto Updates** feature is enabled by default on all MarketPlace devices. If it remains enabled on all your Shield Guard devices, then MarketPlace will ensure your devices have the latest version of the Shield Guard Agent as soon as it becomes available.

If Auto Updates has been disabled on one or more devices in your Shield Guard tenant, you must **manually** monitor the Shield Guard Agent on those devices and install the latest version when it becomes available.

Note: To view the version number (and serial number) of the Shield Guard Agent currently installed on a device, access the device and view the Shield Guard Settings page in the MarketPlace App Manager.

Completing the Installation

Once you **acquire a Shield Guard Service license** and **install and launch the Shield Guard Agent** on one or more devices, the following occurs for each device:

1. The devices become available for import into a **tenant** via the **Devices page** on the portal. To add devices to a tenant, use the **Import Devices from MarketPlace** window.
2. On the portal, when you **assign a security policy to a device**, Shield Guard makes an initial device assessment and the following occurs:
 - The agent queries the portal and retrieves and stores the current policy settings.
 - The agent reports the statuses of the device's security settings to the portal.
 - The portal compares the statuses of the device's security settings to the corresponding settings in the policy and assesses the device as Secure or Not Secure based on the device's compliance to the **security policy**.
 - The **Dashboard** and Devices pages on the Shield Guard Portal update to include the current statuses of all devices monitored by the security policy.
 - The **Logs page** updates to include details of recent activity within the tenant.
3. Once the initial device assessment is complete, you can begin to remotely monitor the security status of the device.
4. Henceforth, Shield Guard monitors the device's security status based on the **communication frequency settings** configured in the Policy Settings. No other configuration at the portal is necessary.

Note: The portal includes two **sample policies** to help you get started, or you can **create your own custom policies**.

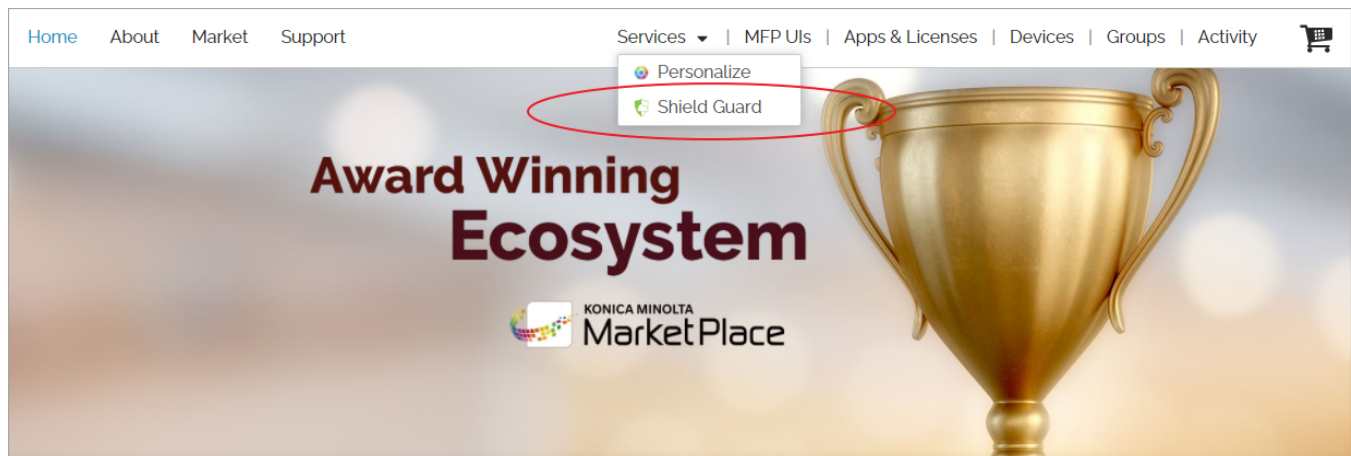
Using the Shield Guard Portal

Accessing the Portal

Once you purchase a **Shield Guard Service** license from MarketPlace, you can sign in to the Shield Guard Portal using your MarketPlace credentials. In the portal, you can configure your **tenant** and monitor the security statuses of devices in the tenant.

To access the Shield Guard Portal, use the following web address: getshieldguard.com/.

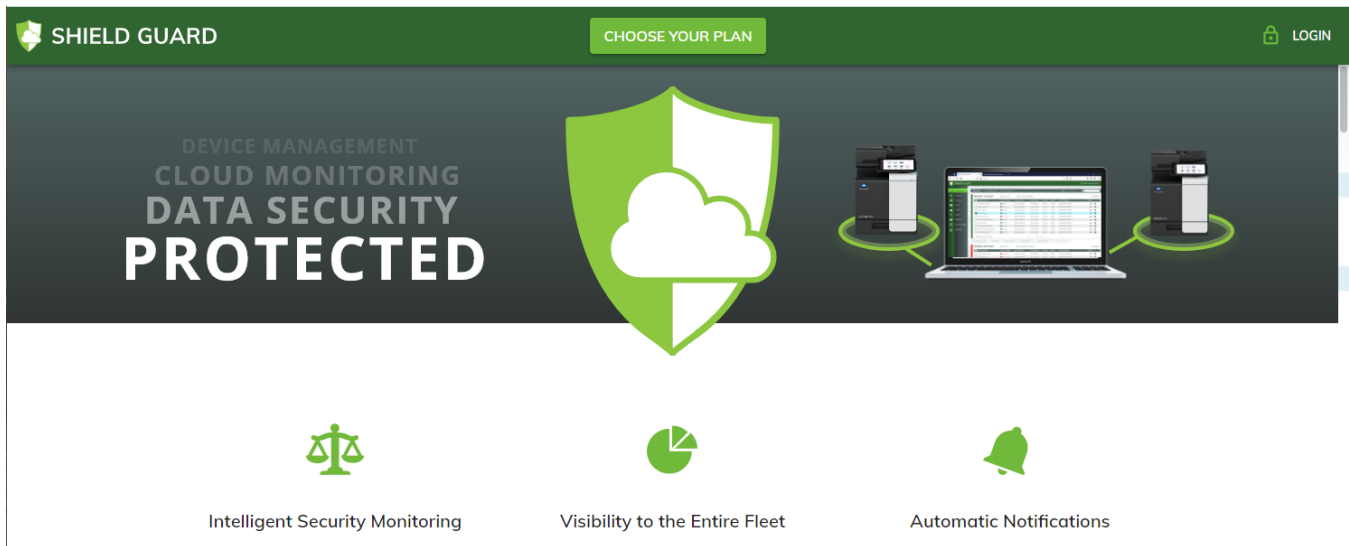
Note: You can also access the portal via the Services menu on the MarketPlace website:



Until you are a member of a Shield Guard tenant, only the **Home** and **Plans** pages are available on the portal. Once you join a tenant, you can log in to the tenant using your MarketPlace credentials. Once logged in, you can access the **My Profile page** and any pages in the **Admin area** to which your assigned **roles** permit you to access.

Logging In

To log in to your Shield Guard tenant, access the Shield Guard Portal. The Home page appears. Click on the **LOGIN** button on the **Title bar**:



One of the following occurs:

- If not already signed in to MarketPlace, a sign-in window appears. Enter your MarketPlace credentials in the fields provided.
- If already signed in to MarketPlace, you are logged in via Single Sign-On (SSO).

Once logged in, the Home page appears displaying the **Welcome** button on the Title bar:



Cookie Settings

The first time you access the Shield Guard Portal, the Cookie Settings window appears where you can view a list of web cookies used by Shield Guard. To access the Shield Guard site, you must agree to Shield Guard's use of these required (technically necessary) web cookies. To agree, click on the **Accept** button. Thereafter, you can access the Cookie Settings window via the link on the Shield Guard **footer bar**.

Home Page

The Shield Guard Portal Home page appears first when you access the **portal**. It displays information on Shield Guard's extensive capabilities, indicates the logged-in user (if any), and provides access to the **Plans page** via the **CHOOSE YOUR PLAN** button.

DEVICE MANAGEMENT
CLOUD MONITORING
DATA SECURITY
PROTECTED



Intelligent Security Monitoring

Shield Guard is an advanced cloud platform for remote, secure monitoring of your MFP fleet. With Shield Guard's intuitive yet powerful features, admins can configure and monitor security policies remotely, via the cloud. Admins can quickly assess their overall MFP security via a centralized graphical Dashboard, ensuring that any security threats are immediately detected while saving both time and effort. The zero-footprint MFP Shield Guard Agent allows for continuous monitoring, eliminating the need for constant ping or scheduling of assessments. Shield Guard features easy-to-use tools for policy and device management, timely security alerts, powerful password management features, and more, providing immediate peace of mind knowing your devices are protected.



Visibility to the Entire Fleet

The Shield Guard Portal enables admins to easily monitor all of their MFPs remotely, from a single location. Once you install the free Shield Guard Agent on your devices, they become available for import into the Shield Guard Portal. Once imported, you can organize devices into groups for better management. The portal's graphical Dashboard page displays an at-a-glance overview of your fleet security, as well as lists of alerts, incidents, and devices requiring attention. The Logs page lists all security logs generated for devices, policies, and users. The Reports page includes a series of pre-configured reports detailing your device's security status. Shield Guard puts eyes on your entire fleet!

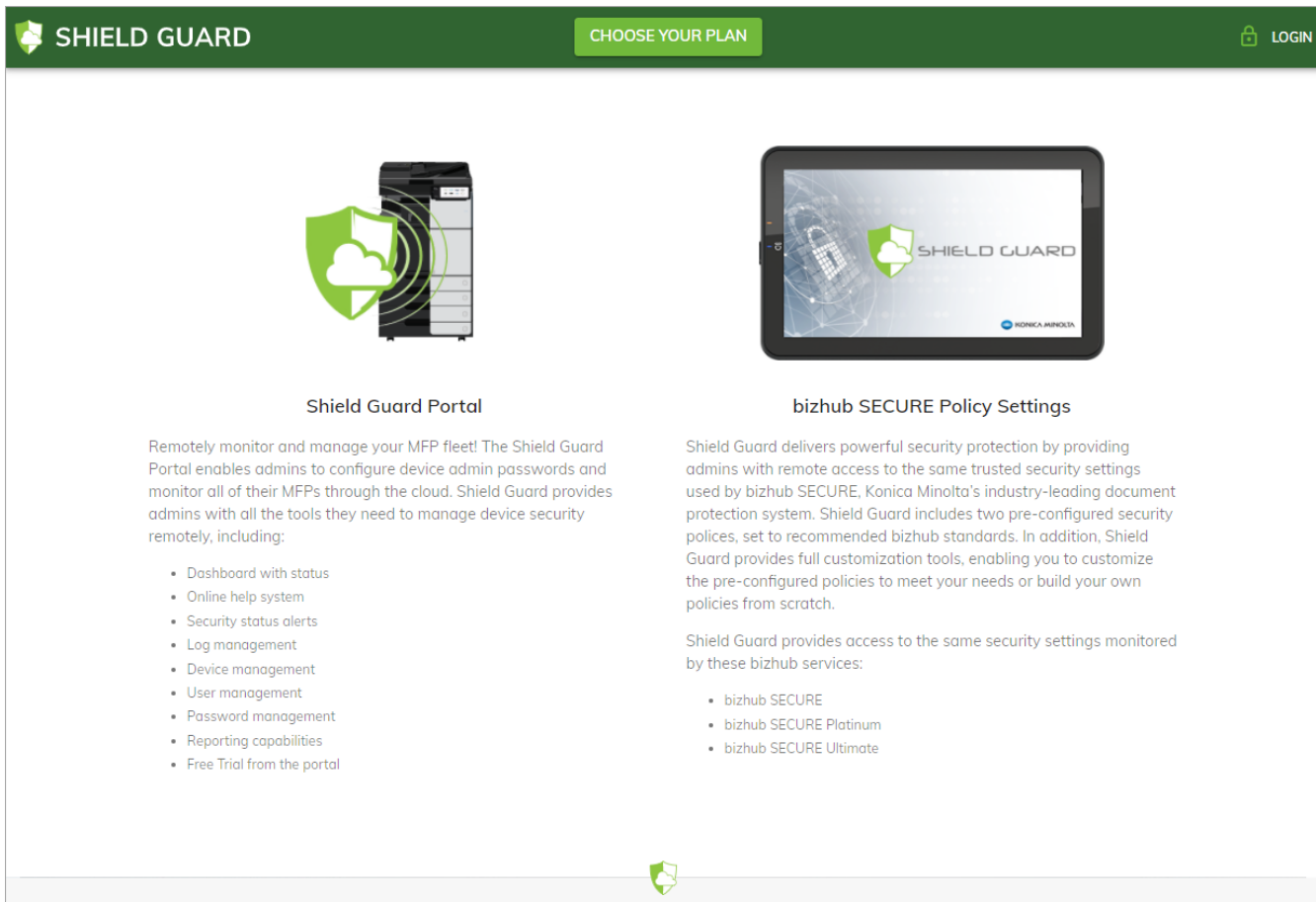


Automatic Notifications

Admins can create their own security policies to monitor their MFPs, select a pre-configured policy, set policies for individual devices and/or specified device groups, and more! Once the Shield Guard Agent assesses the MFP's compliance to the assigned policy and communicates the assessment back to the Shield Guard Portal, alerts can be sent to designated admins identifying any MFPs not in compliance with the policy. The portal's Dashboard, Logs, and Reports pages provide access to the security data collected by Shield Guard. Shield Guard enables admins to quickly identify security breaches and take the necessary steps to remediate the issues and restore their devices to compliance.



The Home page provides illustrations and detailed information on Shield Guard. See the following illustration:



The Home page also includes the **Footer bar**, providing access to additional resources on the Shield Guard portal, for example Shield Guard's privacy policy.

Plans Page

The Plans page provides all the information you need to choose the ideal Shield Guard plan for your team. To access the page, click on the **CHOOSE YOUR PLAN** button on the **Home page**. The following illustration shows the Plans page:

SHIELD GUARD Welcome, Marcus

Choose Your Security Plan

Introducing a cloud-based remote MFP Security Monitoring Solution. Get instant peace of mind knowing your entire MFP fleet is protected with Shield Guard. Features include a graphical dashboard, tools for device and policy management, automatic alerts, remediation capabilities, reporting, and more! Select the policy that works best for your security needs.

Starter

For small departments

For pricing
Contact Us

(annual prepaid)

Graphical dashboard and built-in tools to help you easily define and deploy security policies across your fleet.

[LEARN MORE](#)

Business

For your entire organization

For pricing
Contact Us

(annual prepaid)

Ideal for businesses focusing on security monitoring. Includes password management and remediation.

[LEARN MORE](#)

Enterprise

For advanced administrative control

For pricing
Contact Us

(annual prepaid)

Designed for companies that require full security monitoring and management system. Includes automated policy remediation and advanced analytics.

[LEARN MORE](#)

[FREE TRIAL](#)

Shield Guard is licensed per device.

To return to the Home page, click on the Shield Guard logo at the top of the screen. You can also click on **Return to Home Page** at the top of the Plans page.

Notes:

- When you purchase a paid Shield Guard plan, you must also specify a **billing method**.
- When you select a license plan on the Plans page, you are transported to the MarketPlace site where you can complete the process. Once you complete the purchase, return to the **Shield Guard Portal** and configure your tenant using the **Admin area**.

Shield Guard License Plans

Shield Guard is available in several plans described below. Each plan has an increasing number of features, culminating in the Enterprise plan containing the most advanced administrative controls for Shield Guard.

Note: For plan options available in your region, contact your local Shield Guard sales representative.

Starter Plan

Designed for smaller departments, the introductory Starter plan provides everything you need for remote security monitoring and management of your device fleet, including a Dashboard page as well as security alerts, log-viewing, and basic reporting.

Business Plan

The Business plan offers all of the functionality included in the Starter plan, along with a variety of advanced monitoring and management features/functions including device password remediation and advanced device management.

Enterprise Plan

The Enterprise plan includes all of the functionality included in the Business plan, as well as the sophisticated administrative controls and reporting capabilities required for larger, more complex business customers. The Enterprise plan includes:

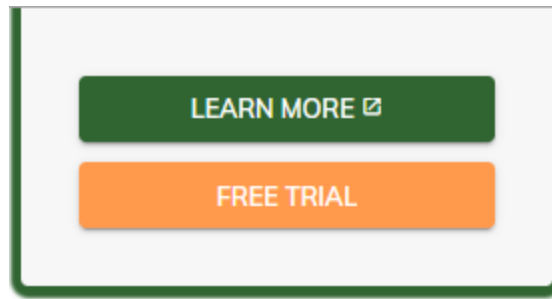
- Advanced reporting capabilities
- A comprehensive Admin dashboard
- Automatic policy remediation
- Time-saving policy management features
- More!

Free Trial License

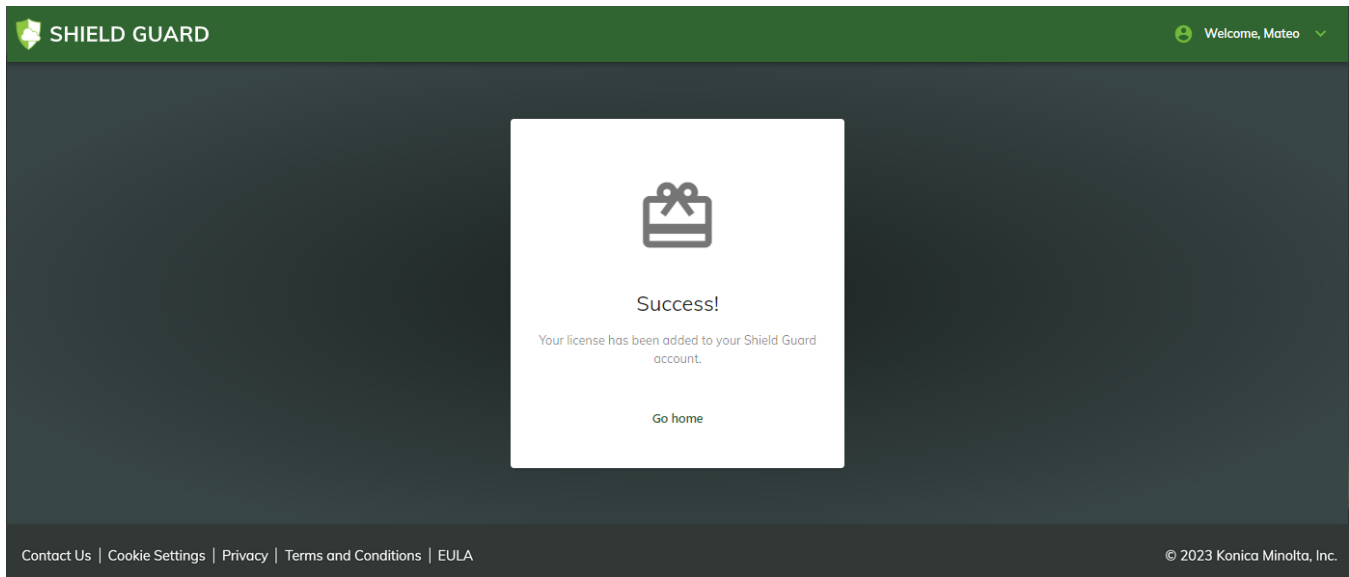
Each MarketPlace user has access to a 30-day free-trial license for the Shield Guard Enterprise Plan. This license includes all the features of the Enterprise plan, and provides up to 10 device licenses. If you later choose to purchase a Shield Guard plan, you can **transfer** any data you generated on your trial license to your purchased account.

To get a free trial license, do the following:

1. Log in to the Shield Guard portal. The Home page appears.
2. On the Home page, click on the **CHOOSE YOUR PLAN** button. The Plans page appears.
3. On the Plans page, on the Enterprise card, click on the **FREE TRIAL** button. If you are logged in to the portal and the Free Trial button is not active, the free trial license has already been consumed for the logged-on user and is thus no longer available. The following illustration shows the Free Trial button in an active state:



4. Shield Guard redirects you to MarketPlace. Follow the purchasing process to create the trial license. When the purchase process is complete, you return to the Shield Guard portal. In the window that appears, click on the **Go Home** link:



5. The Home page of the Shield Guard Portal appears, where you can log in and access your trial tenant.

Shield Guard’s free trial is restricted to one per MarketPlace account. As the **end of the trial period approaches**, Shield Guard sends a notification to the email account associated with the trial license. The notification includes the expiration date of the license and your options for purchasing a paid license for Shield Guard.

Note: You can also access the free trial license via the Product page for the **Shield Guard Service**.

Comparing Shield Guard Plans

To view a table comparing the features in each plan, access the **Feature Comparison section of the Plans page** in the Shield Guard Portal.

Password Vaults

Password vaults are a security feature in Shield Guard, providing an additional layer of protection inside the Shield Guard portal. The user authentication process during **login** protects the portal

from external breaches while password vaults (together with **Shield Guard roles**) protect data within the portal.

Use of Shield Guard requires a password vault. The first time you attempt to access a **vault-protected page** in the Shield Guard portal, the **Create Vault** window appears and prompts you to create your vault.

Each vault requires a **master key** to unlock it. During the vault-creation process, you generate your vault master key. If using the **Decentralized** method for **vault key management**, you must manually create your vault key. If using the **Centralized** method, Shield Guard creates the key for you.

Once created, you must unlock your vault the first time in each Shield Guard session that you attempt to access a vault-protected page. If using the Decentralized method for vault key management, the **Unlock Vault** window appears and you must manually provide your vault key. If using the Centralized method, Shield Guard provides the key for you.

Once unlocked, the vault remains open until you perform an action that causes Shield Guard to lock the vault, for example logging out of the Shield Guard session. Shield Guard's automatic vault-locking process:

1. Takes a snapshot of your current data,
2. Stores the data in your vault, and
3. Encrypts the vault.

Vault Protections

Password vaults provide the following protections for **Shield Guard tenants**:

- Store and encrypt the admin passwords of devices added to the tenant, protecting the devices from unauthorized access.
- Protect pages on the portal containing sensitive information against unauthorized access. Such pages are **vault-protected**, and require a vault key to access.

Note: Depending on your method for **vault key management**, your vault key may be stored outside of your vault, thus providing additional security for your vault key.

Managing a Password Vault

Password vault management involves the following major elements:

1. **Vault** - Password vaults are associated with tenant members. Your vault protects your data across all tenants of which you are a member. That is, vaults are user-specific, not tenant-specific.
2. **Vault master key** - As part of the vault-creation process, you generate a vault master key that will be used to unlock your vault thereafter.

3. **Tenant member vault key management method** - Tenant members can choose from two methods by which to manage their vault keys:
 - **Decentralized** - Tenant members create and manage their vault key.
 - **Centralized** - Shield Guard creates and manages their vault key.
4. **Tenant Vault Key Management setting** - Authorized tenant members (members with the License Plan Management **permission**) can use the Tenant Vault Key Management section of the Settings page to restrict tenant members to the Decentralized method only, such that tenant members have no access to the Centralized method.

In summary:

1. Each tenant member creates a vault and generates a vault key to unlock the vault thereafter.
2. The steps tenant members must take when creating their vault, and the tasks each must perform to maintain their vault key, are determined by the tenant member vault key management method they choose.
3. An authorized tenant member can restrict the tenant to use of the Decentralized vault key management method only.

Creating Your Password Vault

The first time in a Shield Guard session that you attempt to access a **vault-protected** page, Shield Guard checks for your vault key. If you have not yet created your password vault, the Create Vault window appears and you must create it.

The contents of the Create Vault window, and the information you are required to provide, differ depending on your membership status in the tenant and the **tenant vault key management** configuration for the tenant. The following list describes the scenarios that determine the contents of the Create Vault window.

- You are a **tenant owner** who is **accessing the tenant for the first time**.
- You are a tenant member whose tenant has been configured for **Decentralized Only vault key management**.
- You are a tenant member whose tenant has been configured for **Decentralized or Centralized vault key management**.
- You are a member of no Shield Guard tenants, but have been invited to join one.

Vault Creation for Tenant Owners

If you are the **tenant owner** accessing the tenant for the first time, once you log in to the tenant, the Create Vault window appears:

Create Vault ?

All Shield Guard tenant members must create a vault with a master key to store their Shield Guard data and protect their tenant from unauthorized access. You will use your vault master key to unlock the vault each time you access a Shield Guard restricted page.

Once you click on the Create button to create your vault, the Settings page appears and you can begin to configure your tenant.

! DO NOT FORGET THIS MASTER KEY.

Master Key

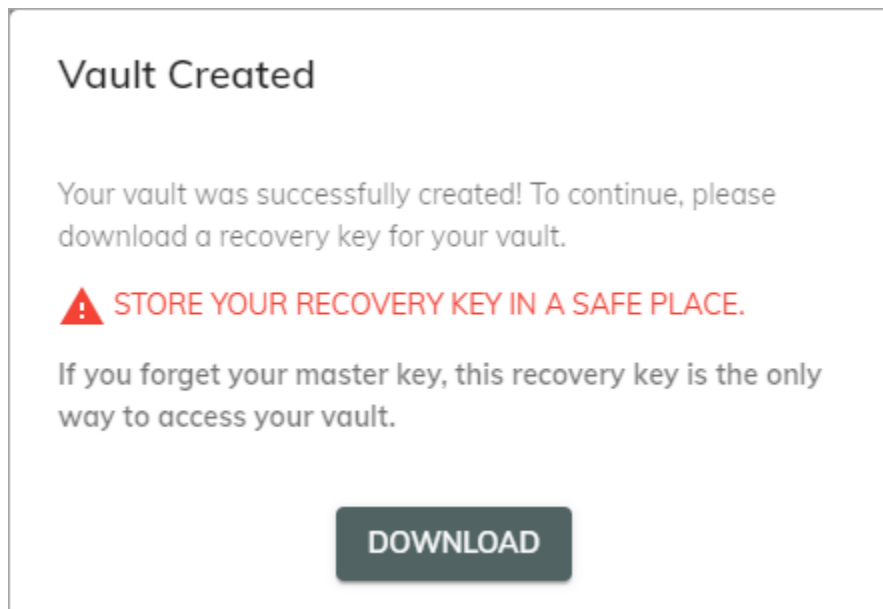
Confirm Master Key

CREATE

Note: The above window also appears for Shield Guard invitees who have been invited to join a tenant but are currently not a member of any tenant.

Use this window to specify a master key for your vault. Do the following:

1. In the Create Vault window, in the **Master Key** field, specify a master key for your vault.
2. In the **Confirm Master Key** field, re-enter the master key. Once the contents of the two fields match, the **CREATE** button activates.
3. To activate the vault, click on the **CREATE** button. To abandon the process, click outside of the window.
4. Once you activate the vault, the Vault Created window appears. To continue, you must download a recovery key. See the following illustration:



5. In the Vault Created window, click on the **Download** button.
6. If a navigation window appears, navigate to the location where you want to store the recovery key and click on **Open**. If no navigation window appears, the key downloads to the default download location on your local drive.

Important! Be sure to complete the download process of your recovery key and take note of where you store it. If you forget your master key, you can use the recovery key to create a new master key. If you lose the recovery key as well, you must use the **Reset Vault** feature to regain access to your vault.

Note: As the first member of your tenant, the tenant defaults to the Decentralized vault key management method and so you are not required to specify one for your vault. Thus, the Management Type field does not appear in the Create Vault window. Conversely, the Management Type field will appear for all other tenant members as part of their vault-creation process. The options available at that field are controlled by the **Tenant Vault Key Management field** in your tenant.

Once you complete the vault-creation process, you can begin to configure your tenant.

Vault Creation for Decentralized Only

If the **Tenant Vault Key Management field** for your tenant is set to Decentralized Only, the Management Type field in the Create Vault window is inactive and you must use the Decentralized method. See the following illustration:

Create Vault ?

All Shield Guard tenant members must create a vault with a master key to store their Shield Guard data and protect their tenant from unauthorized access. You will use your vault master key to unlock the vault each time you access Shield Guard.

Management Type
Decentralized Key Management

Security
Convenience

Decentralized Key Management requires you specify a vault master key and then provide it each time you open a Shield Guard session. If you lose your vault master key and its recovery key, only a member of the same tenant can restore your access to your vault and the password data stored within. For more information, refer to Shield Guard Online Help.

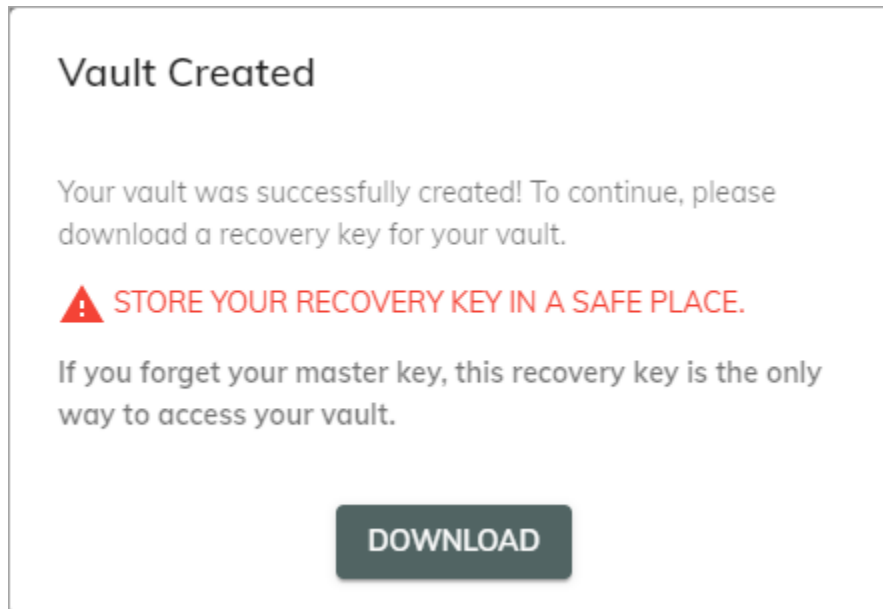
Master Key

Confirm Master Key

CREATE

To create your vault, do the following:

1. In the Create Vault window, in the **Master Key** field, specify a master key for your vault.
2. In the **Confirm Master Key** field, re-enter the master key. Once the contents of the two fields match, the **CREATE** button activates.
3. To activate the vault, click on the **CREATE** button. To abandon the process, click outside of the window.
4. Once you activate the vault, the Vault Created window appears. To continue, you must download a recovery key. See the following illustration:



5. In the Vault Created window, click on the **Download** button.
6. If a navigation window appears, navigate to the location where you want to store the recovery key and click on **Open**. If no navigation window appears, the key downloads to the default download location on your local drive.

Important! Be sure to complete the download process of your recovery key and take note of where you store it. If you forget your master key, you can use the recovery key to create a new master key. If you lose the recovery key as well, you must use the **Reset Vault** feature to regain access to your vault.

Vault Creation for Decentralized or Centralized

If the **Tenant Vault Key Management field** for your tenant is set to Decentralized or Centralized, the Management Type field in the Create Vault window is active and you can make a selection. See the following illustration:

Create Vault ?

All Shield Guard tenant members must create a vault with a master key to store their Shield Guard data and protect their tenant from unauthorized access. You will use your vault master key to unlock the vault each time you access Shield Guard.

Management Type

Decentralized Key Management

Security
User Convenience

Decentralized Key Management requires you specify a vault master key and then provide it each time you open a Shield Guard session. If you lose your vault master key and its recovery key, only a member of the same tenant can restore your access to your vault and the password data stored within. For more information, refer to Shield Guard Online Help.

⚠ DO NOT FORGET THIS MASTER KEY:

Master Key

Confirm Master Key

CREATE

To create your vault, do the following:

1. In the Create Vault window, in the **Management Type** field, select a **vault key management method** for your vault.
 - a. If you select Centralized, then when you click on the **CREATE** button, Shield Guard creates and stores your vault key for you, and the process is complete. To abandon the process, click outside of the window.
 - b. If you select Decentralized, follow the steps listed in the **Vault Creation for Decentralized Only** section to create your vault.

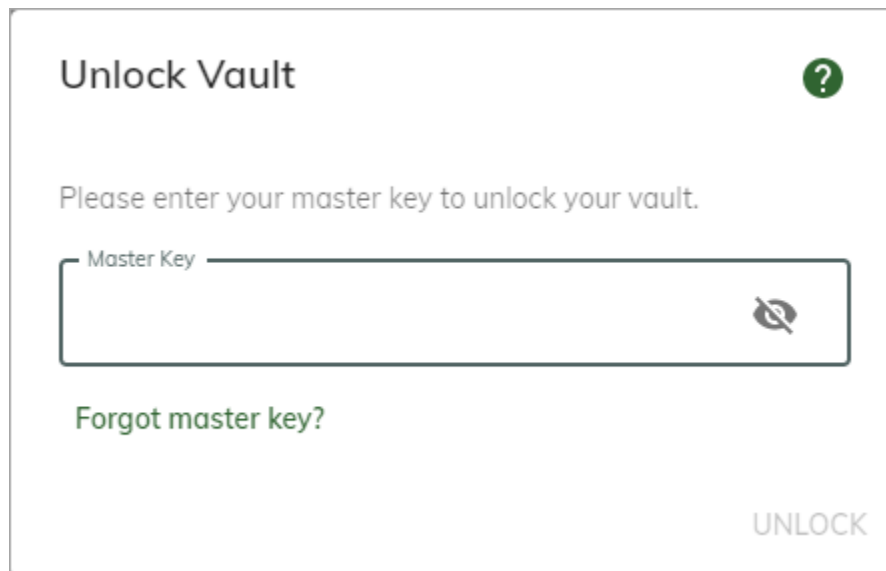
Vault Maintenance for Decentralized Key Management

Once you create your vault, Shield Guard manages your vault data regardless of your vault key management method. If you use the **Decentralized** method, you are responsible for several vault key management tasks:

- **Unlocking your vault** when prompted by Shield Guard.
- **Changing your vault key** when necessary.
- **Using the Recovery key** when necessary.
- **Resetting your vault** when necessary.

Unlocking Your Password Vault

If you use the **Decentralized** method for vault key management, you must manually unlock your vault when prompted by Shield Guard. The Unlock Vault window appears for this purpose. This window appears the first time in a Shield Guard session that you attempt to access a **vault-protected** page. To unlock the vault, enter your **master key**. See the following illustration:



Unlock Vault ?

Please enter your master key to unlock your vault.

Master Key 👁

[Forgot master key?](#)

UNLOCK

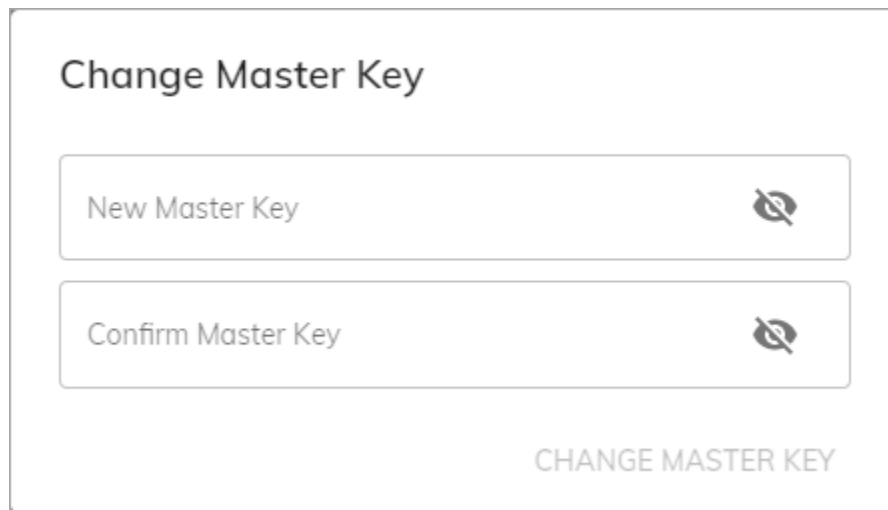
Once you unlock the vault, it remains open until you do any of the following, each of which cause the vault to lock automatically:

- Refresh the page.
- Navigate away from the site by modifying the URL for your Shield Guard page.
- Log out of the Shield Guard site.

Changing Your Vault's Master Key

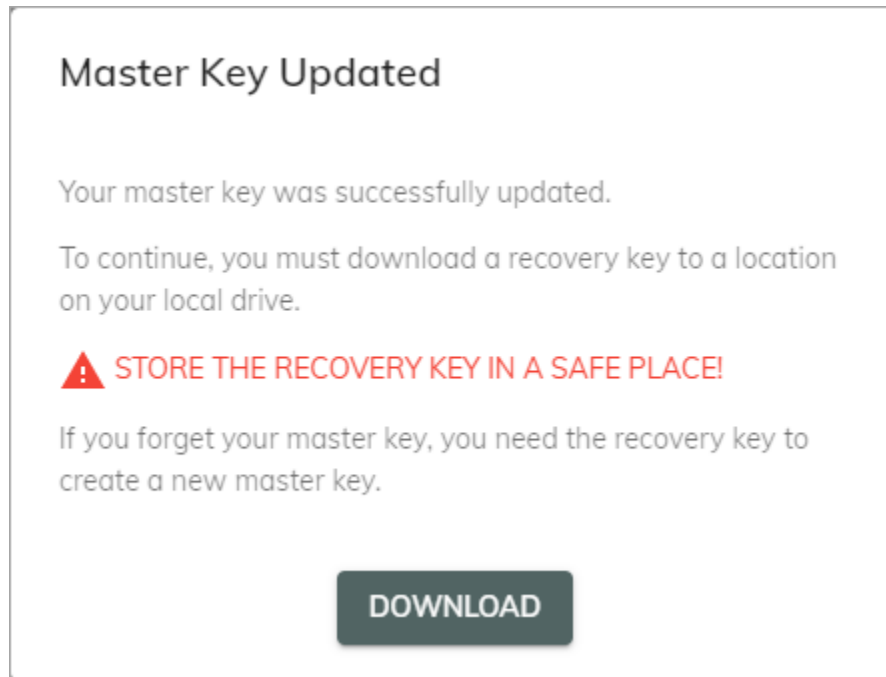
If you use the **Decentralized** method for vault key management, you can manually change your **vault master key**. We recommend you update your vault key on a regular basis. You have the following options:

- Use the **Forgot master key?** option on the Unlock Vault window. This option requires that you provide a valid recovery key.
- Use the **CHANGE MASTER KEY** option in the **Vault Key Options** section of the My Profile page. Do the following:
 1. Access the My Profile page.
 2. In the Vault Key Options area, click on the **CHANGE MASTER KEY** button. The Change Master Key window appears. See the following illustration:



The illustration shows a window titled "Change Master Key". It contains two text input fields. The first field is labeled "New Master Key" and the second is labeled "Confirm Master Key". Both fields have a small icon of a key with a slash through it on the right side. At the bottom right of the window is a button labeled "CHANGE MASTER KEY".

3. In the Change Master Key window, enter the master key in the **New Master Key** field and then re-enter it in the **Confirm Master Key** field. Once the contents of the two fields match, the **CHANGE MASTER KEY** button activates. Click on this button to change your master key. The Master Key Updated window appears. To continue, you must download a recovery key. See the following illustration:



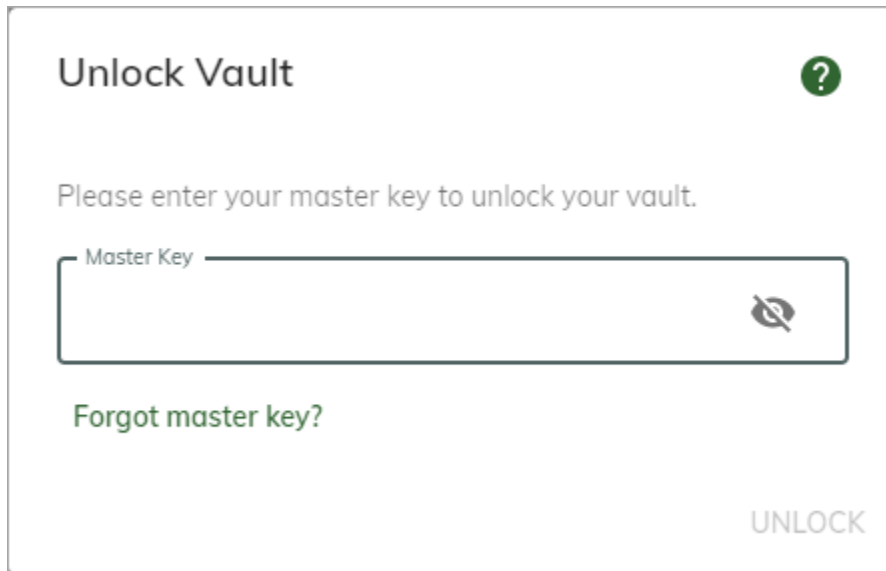
4. In the Master Key Updated window, click on the **Download** button.
5. If a navigation window appears, navigate to the location where you want to store the recovery key and click on **Open**. If no navigation window appears, the key downloads to the default download location on your local drive.

Important! Be sure to complete the download process of your recovery key and take note of where you store it. If you forget your master key, the recovery key is the only means by which you can create a new master key.

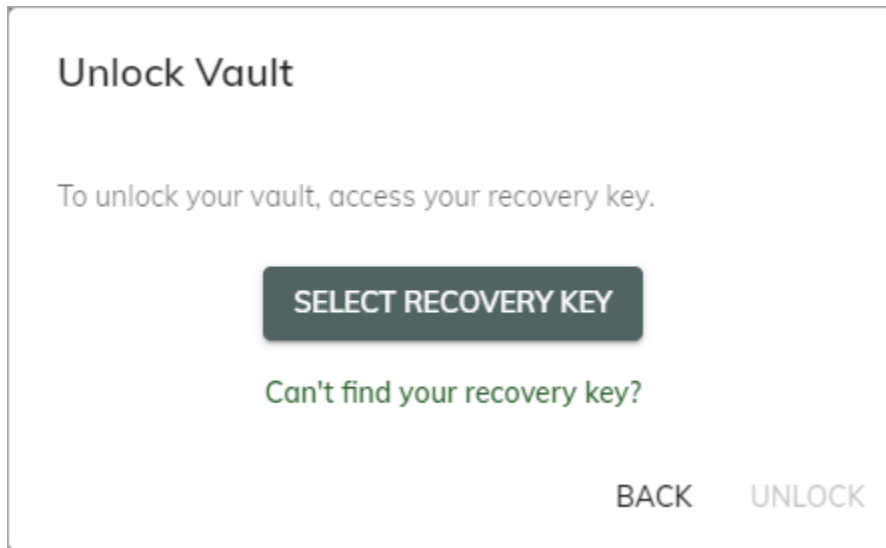
Using the Recovery Key

If you use the **Decentralized** method for vault key management and you forget your **master key**, you can use your recovery key to create a new master key. Shield Guard prompts you to generate a recovery key as part of the vault-creation process, and each time you update the master key thereafter. Your recovery key should be stored on your local drive. If not, you can **download a new recovery key**.

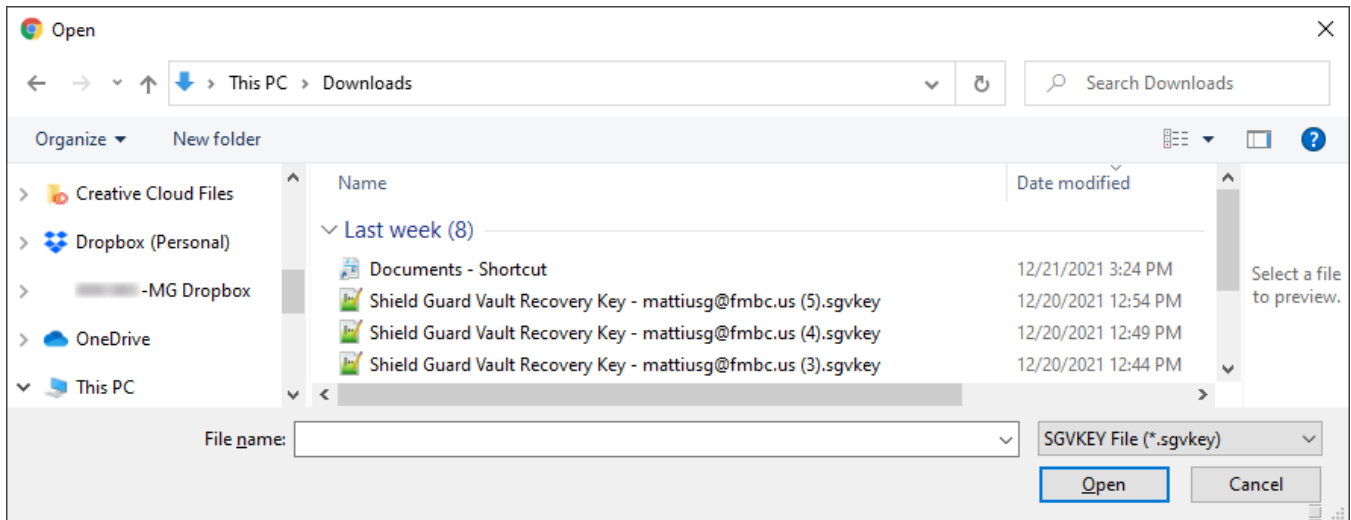
When the Unlock Vault window appears and you do not have the master key to unlock the vault, do the following:



1. Click on the **Forgot master key?** option. The **SELECT RECOVERY KEY** button appears:

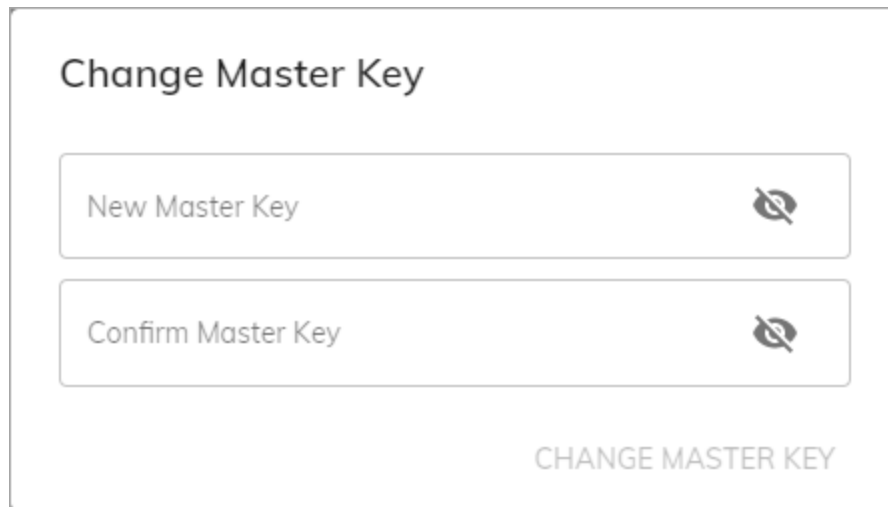


2. Click on the **SELECT RECOVERY KEY** button. A navigation window appears:

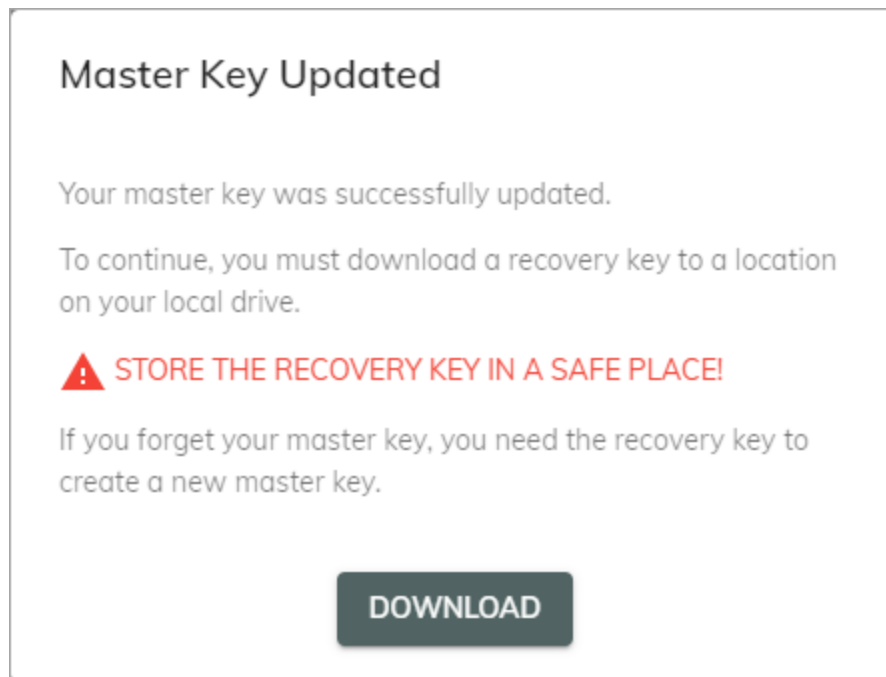


3. Navigate to the location where the recovery key is stored and open the file. The Change Master Key window appears, as in the following illustration:

Note: If you select an improper recovery key, an error message appears. To continue, you must select the proper recovery key or click on the **Back** button to return to the previous screen.



4. In the Change Master key window, enter the master key in the **New Master Key** field and then re-enter it into the **Confirm Master Key** field. Once the content of the two fields matches, the **CHANGE MASTER KEY** button activates. Click on this button to change your master key. The Master Key Updated window appears. To continue, you must download a recovery key. See the following illustration:



5. In the Master Key Updated window, click on the **Download** button.
6. If a navigation window appears, navigate to the location where you want to store the recovery key and click on **Open**. If no navigation window appears, the key downloads to the default download location on your local drive.

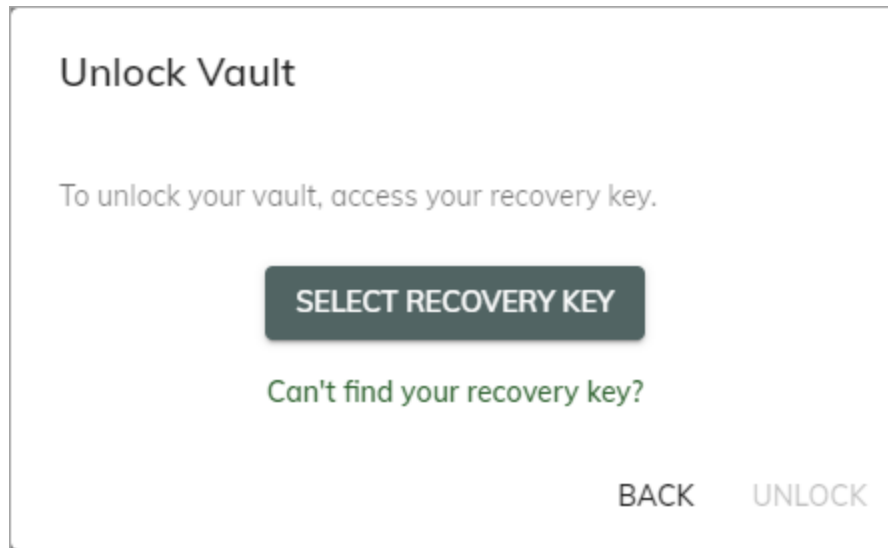
Important! Be sure to complete the download process of your recovery key and note of where you store it. If you forget your master key, the recovery key is the only means by which you can create a new master key.

About Recovery Keys

- When you download a **recovery key**, it becomes associated with the **master key** and is valid until you change the master key. Whenever you create or modify a master key, Shield Guard prompts you to download a recovery key. That recovery key becomes associated with the new master key, and any previous recovery keys are invalidated.
- If you download multiple recovery keys, you can identify the valid recovery key by selecting the file with the most recent date.
- We recommend you delete any invalid recovery keys.

Resetting Your Vault

If you use the **Decentralized** method for vault key management and you lose both your **vault master key** and its **recovery key**, you can attempt to reestablish access to your vault by clicking on the **Can't find your recovery key?** option in the **Unlock Vault** window.



Note: If you use the **Centralized** method for vault key management, Shield Guard maintains your vault key and you will never need to use the Reset Vault procedure.

The Reset Vault process alerts other members (if any) of your tenant to send you a link, via which you can reset your vault master key and regain access to your vault data (including device admin passwords). If you are the only member of your tenant, you can manually reset your vault master key but all data in the vault will be destroyed.

The Reset Vault window lists the tenants of which you are a member and the recovery option available for each. See the following illustration:

Reset Vault

If you lose both your vault master key and your recovery key, you can reset your vault. This process alerts other members (if any) of your tenant to send you a link, via which you can reset your vault master key and regain access to your vault data (including device admin passwords). If you are the only member of your tenant, you can manually reset your vault master key but all data in the vault will be destroyed.

Your account has access to the following tenants, each of which will need to be added to your newly generated vault. For vaults with other users, those users will be alerted that you need assistance in recovering your vault.

Tenant	Recovery Options
NR00001605-SGENNFR	Manual Reset
NR00001622-SGENNFR	User-assisted recovery

I understand that my access to this tenant will be restored only when I reset my vault. * **Required**

I understand that if I manually reset my vault, all data in the vault will be destroyed, including device admin passwords. If a device's admin password is lost, an authorized Konica Minolta service technician may be needed to reset the device's admin password. Additionally, for policies using Manual Password Generation, I must re-enable the Admin Password Configuration setting and provide a new manual password.

I understand that a technician may be needed to restore access. * **Required**

CANCEL

SAVE

User-Assisted Recovery

If any of your tenants has active members other than you, the Recovery Options column in the Reset Vault window displays “User-assisted recovery” and you may be able to restore your access to the tenant and recover the contents of your vault. When you click on the **SAVE** button, Shield Guard sends an email to all members of all your tenants indicating you are locked out of the tenant and require an invitation to rejoin. The email includes a link that, when clicked on, sends you an invitation email containing a link to rejoin the tenant. When you rejoin a tenant, you will be

prompted to reset your vault master key. Your access to the tenant, and your vault data associated with it, is now restored.

Note: If no other tenant member is able to send you an invitation email (for example, they have lost their master and recovery keys, too), you must contact your support representative to assist you in accessing the **Manual Reset** option to reset your vault.

Manual Reset

If you are the only member of a tenant, the Recovery Options column in the Reset Vault window will display “Manual Reset” for that tenant. This indicates that no one else is able to access the tenant and send you an invitation to rejoin the tenant. In such cases, your only option to rejoin your tenant is to use the Manual Reset procedure. You will be prompted to create a new vault, and your access to the tenant will be restored, but your vault data for the tenant will be lost. If you have no other access to the admin passwords of the devices in the tenant, you will need to contact your support representative to arrange for a technician to retrieve the passwords for each of the devices.

Vault Maintenance for Centralized Key Management

Once you create your vault, Shield Guard manages your vault data regardless of your vault key management method.

For vault key management, if you use the **Centralized** method, then Shield Guard manages the key for you and you have no manual tasks for key management. Shield Guard assumes responsibility for:

- Unlocking your vault
- Updating your vault key
- Safeguarding your vault key. Shield Guard will never lose the key, so you will not need to:
 - Create a recovery key or use a recovery key
 - Reset your vault

Vault-Protected Pages

In addition to storing sensitive data in the vault, password vaults restrict access to pages in the Shield Guard portal that contain sensitive information. These pages are called “vault-protected” pages. In each Shield Guard session, Shield Guard restricts access to these pages until the **vault master key** is provided. Once the vault has been unlocked, all vault-protected pages become accessible.

The following Shield Guard pages are vault-protected:

- **Devices page**
- **Users page**

- **Policy Editor**
- **My Profile page**

Vault Master Keys

As part of the vault creation process, each tenant member generates a vault master key they will use thereafter to unlock their vault. Vault key management is an important aspect of Shield Guard best practices. If a vault master key is lost, the tenant member can be blocked from accessing the tenant and the device password data in the vault can be lost. Shield Guard provides ways for tenant members to safeguard their vault keys and restore them if lost. And, Konica Minolta technicians can retrieve a device's admin password in the event that no tenant member can provide the password. However, it is recommended you safeguard your vault keys to avoid downtime from your tenants and their devices.

Vault Key Management

Vault key management involves the following tasks for tenant members:

- Selecting a **vault key management method**.
- Creating a vault master key to unlock their vault.
- Safeguarding the key once created.
- **Changing the key** as needed.
- **Restoring the key** if lost.

Note: For tenant members who select the **Centralized** method for vault key management, Shield Guard performs these tasks automatically.

The vault key management method determines:

- The location at which the vault master key is stored (locally or in the cloud).
- Who is responsible for securing and preserving the key (the tenant member or Shield Guard).
- Who provides the key when Shield Guard requires it (the tenant member or Shield Guard).

Vault Key Management Methods

Shield Guard provides two methods for tenant members to manage their vault keys:

Decentralized Key Management

In this method, Shield Guard manages the vault but not the vault key. By storing the key in a "decentralized" location (separately from Shield Guard), an additional element of security is provided.

Tenant members using the Decentralized method are responsible for:

- **Creating their vault key,**
- **Safeguarding their vault key,**
- **Changing their key** as needed,
- **Recovering their vault key** if lost,
- **Resetting their vault key** if both the master and recovery keys are lost, and
- Entering their vault key whenever requested by Shield Guard.

Centralized Key Management

In this method, Shield Guard manages both the tenant member's vault and vault key in the cloud and provides it automatically when requested by Shield Guard. This method provides a level of convenience for tenant members, and Shield Guard will never lose the key.

Note: Tenants can be **configured** to block the use of the Centralized method within the tenant.

Tenant Vault Key Management Options

Authorized Tenant members (members with the License Plan Management **permission**) can edit the **Tenant Vault Key Management section of the Settings page**. This section contains the following options for tenant vault key management:

- **Decentralized Key Management** - Require tenant members to use the **Decentralized** key management method.
- **Centralized or Decentralized Key Management** - Allow tenant members to choose their vault key management method (Decentralized Key Management or **Centralized** key management).

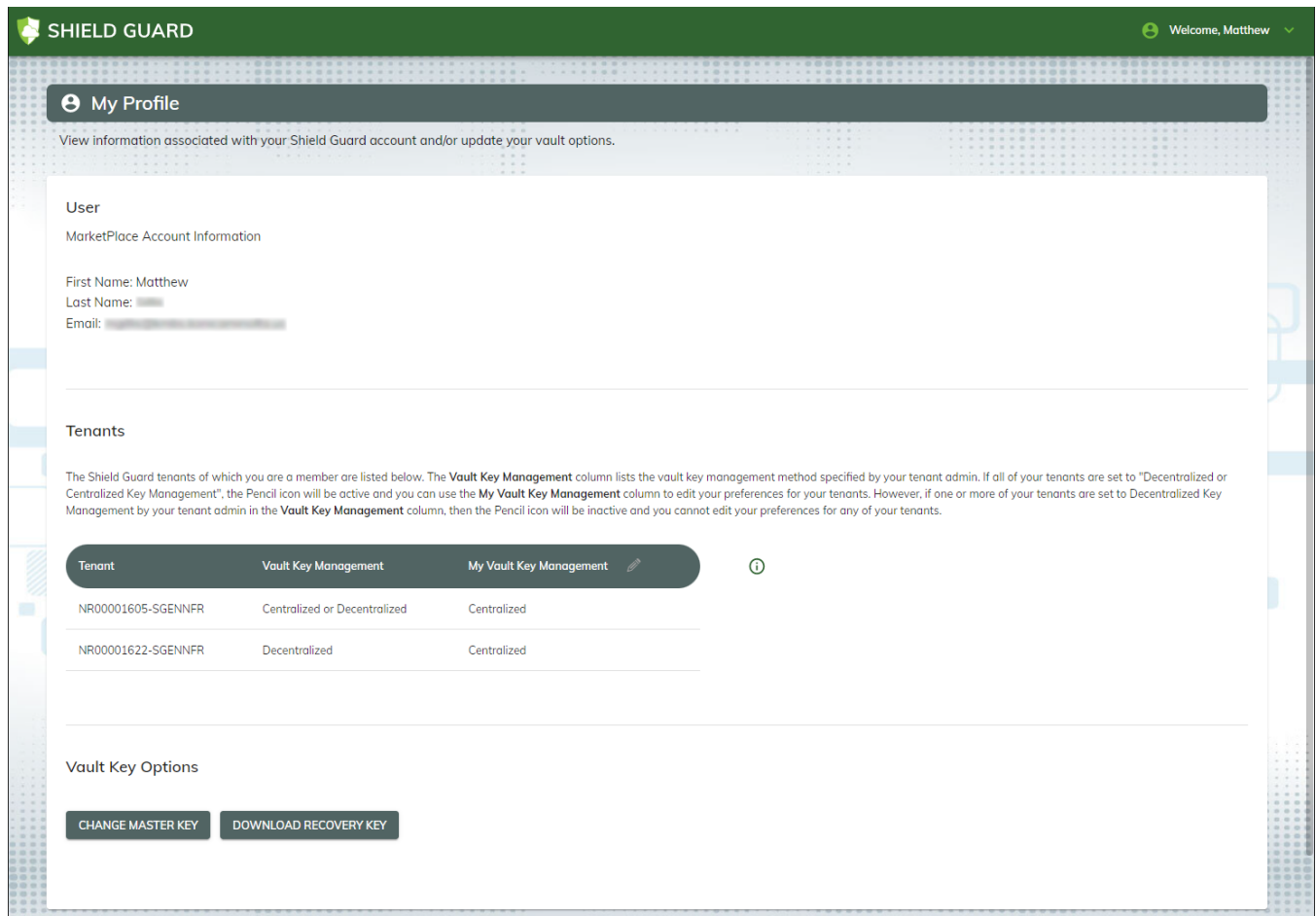
Note: Tenant vault key management applies to tenants as a whole. It is distinct from “tenant *member* vault key management”, which refers to the vault key management method that must be applied to each individual password vault.

Viewing the Device Admin Password

Once you unlock the password vault, you can **view the admin passwords for devices** in your tenant.

My Profile Page

The My Profile page provides information on your Shield Guard account as well as options for maintaining your **vault master key**. You access this page by clicking on the **Welcome button** on the Title bar and selecting “My Profile” from the menu that appears. The My Profile page appears in the following illustration:



Viewing User Information

The User section displays information from your MarketPlace account, including the following:

- First and last name
- MarketPlace account email address

Viewing Tenant Information

The Tenants section contains a table listing the following:

- The **tenant(s)** of which you are a member.
- The **tenant vault key management option** specified for each tenant.
- The **tenant member vault key management method** currently applied to each of your tenants.

The Vault Management column lists the vault key management method specified by your tenant admin. If all of your tenants are set to “Decentralized or Centralized Key Management”, the Pencil icon in the table header will be active and you can edit your preferences for your tenants. However, if one or more of your tenants are set to Decentralized Key Management, then the Pencil icon will be inactive and you cannot edit your preferences for any of your tenants.

If you click on the Pencil icon when it is active, the Modify My Vault Management window appears. Click on the dropdown to view your options for vault key management. If you make any changes to your vault management selections, the **SAVE** button activates. Click this button to save your changes, or navigate away from the page to abandon your changes.

Vault Key Options

Use this section to manage the **master key** for your **password vault**. Your options are described in the following sections.

Changing your Vault’s Master Key

We recommend you **change your master key** on a regular basis.

Downloading a Recovery Key

If you lose your master key, you can create a new master key using your **recovery key**. When you create your vault, and each time you update the master key thereafter, Shield Guard prompts you to download a recovery key.

If you lose the recovery key, you can generate another one. You must either be currently logged in to the Shield Guard portal, or you must log in to the portal (providing your master key in the process).

Do the following:

1. Click on the **DOWNLOAD RECOVERY KEY** button.
2. If a navigation window appears, navigate to the location where you want to store the recovery key and click on **Open**. If no navigation window appears, the key downloads to the default download location on your local drive.

Important! Be sure to complete the download process of your recovery key and make note of where you store it. If you forget your master key, the recovery key is the only means by which you can create a new master key.

Note: If you lose both your master key and its recovery key, you must use the **Reset Vault** feature to regain access to your vault.

Admin Area

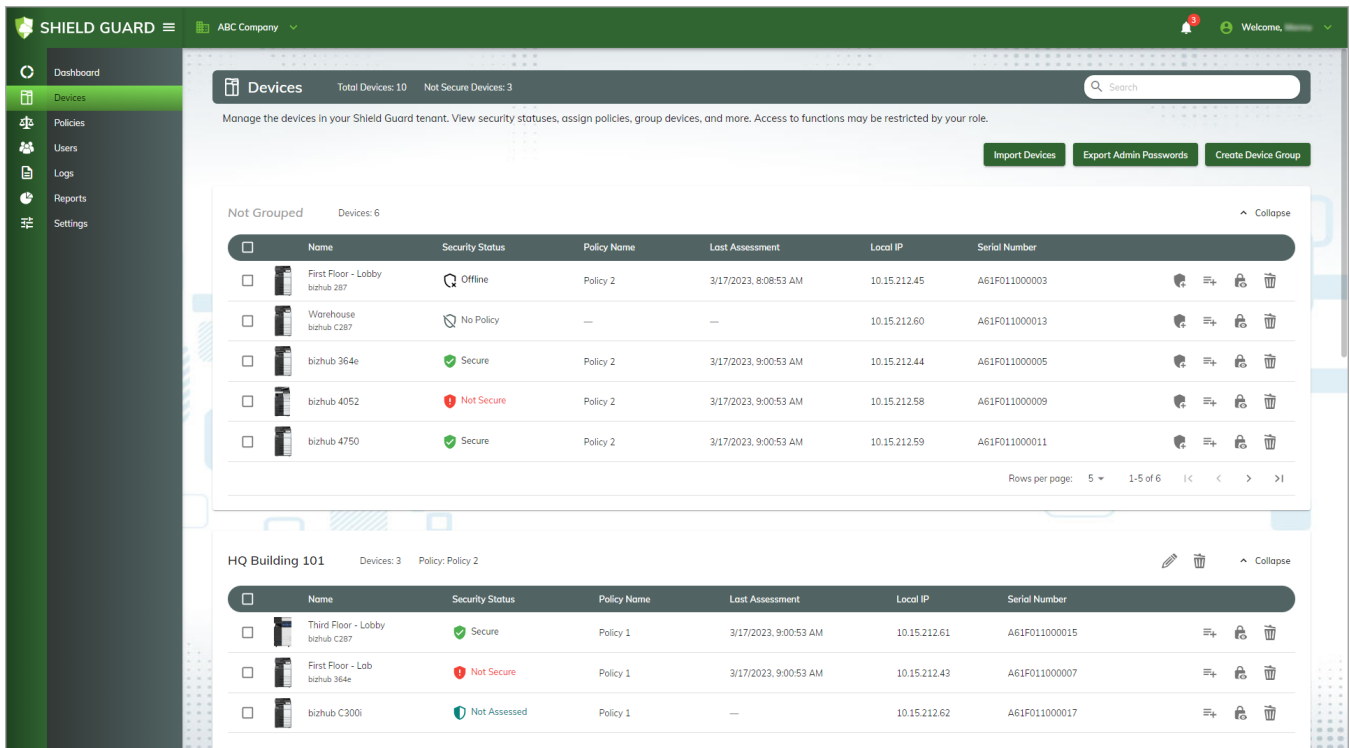
The Admin area of the Shield Guard Portal contains the pages you use to configure, monitor, and maintain your Shield Guard **tenant**. You access the Admin area by clicking on the **Welcome** button then selecting **Admin** from the menu that appears. The Admin area consists of the following pages.

- **Dashboard Page**
- **Devices Page**
- **Policies Page**
- **Users Page**
- **Logs Page**
- **Reports Page**
- **Settings Page**

Notes:

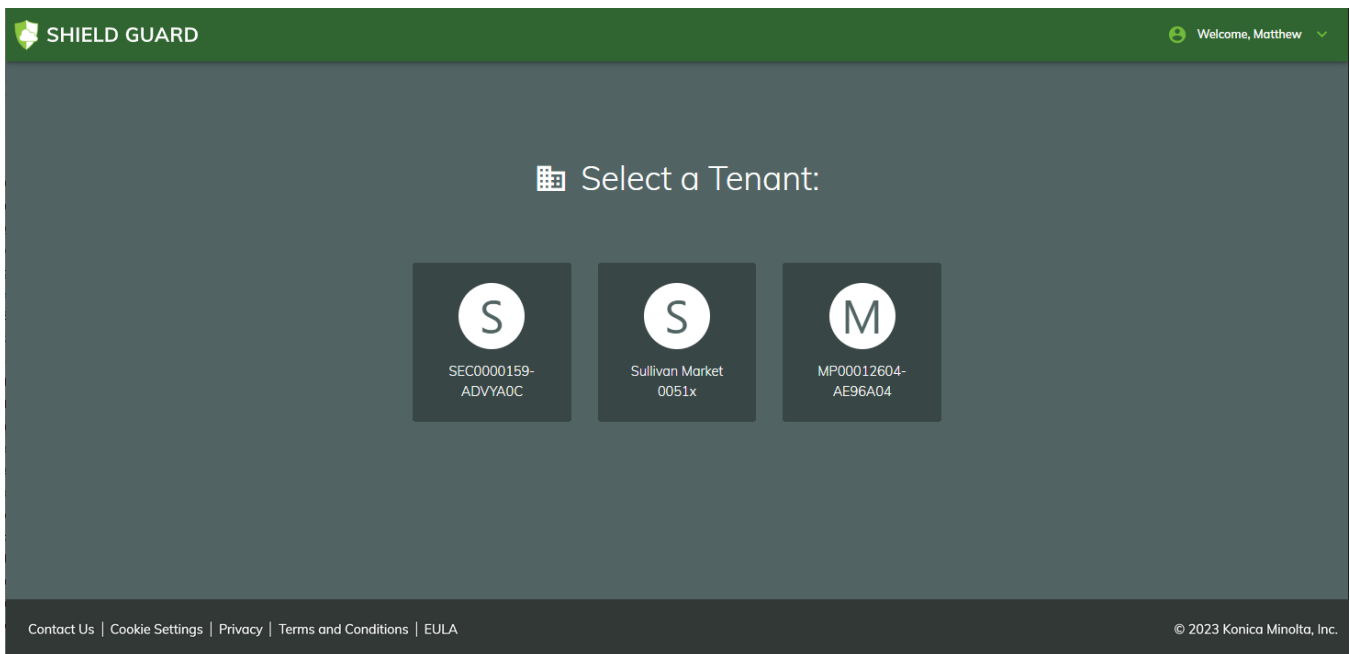
- Many pages in the Admin area are **vault-protected** and require a vault key to access.
- One or more pages in the Admin area may not be available to you, depending on your **license plan** and **role**.
- Each page in the Admin area includes various **page elements** common to all pages in the Admin area.

The following illustration shows the Devices page. “Devices” is selected in the **Navigation pane** and the Devices page displays in the Content area:

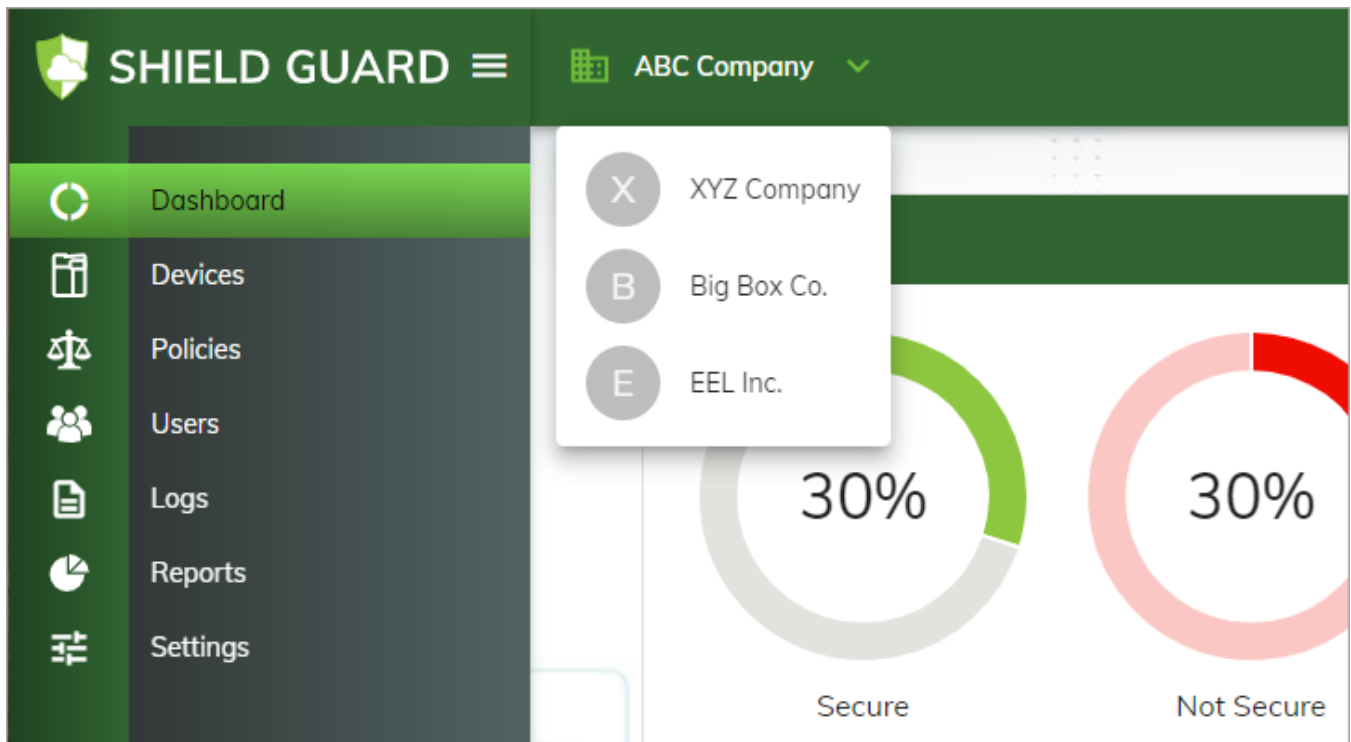


Select a Tenant Page

If you are a member of multiple Shield Guard **tenants**, use this page to select the tenant you want to access. This page displays the tenants of which you are a member, as in the following illustration:



Select the tenant you want to view or edit. The **Dashboard page** for the tenant appears. The name of the tenant displays on the **Title bar**. To change to another tenant, click on the name and select another tenant from the menu that appears. See the following illustration:



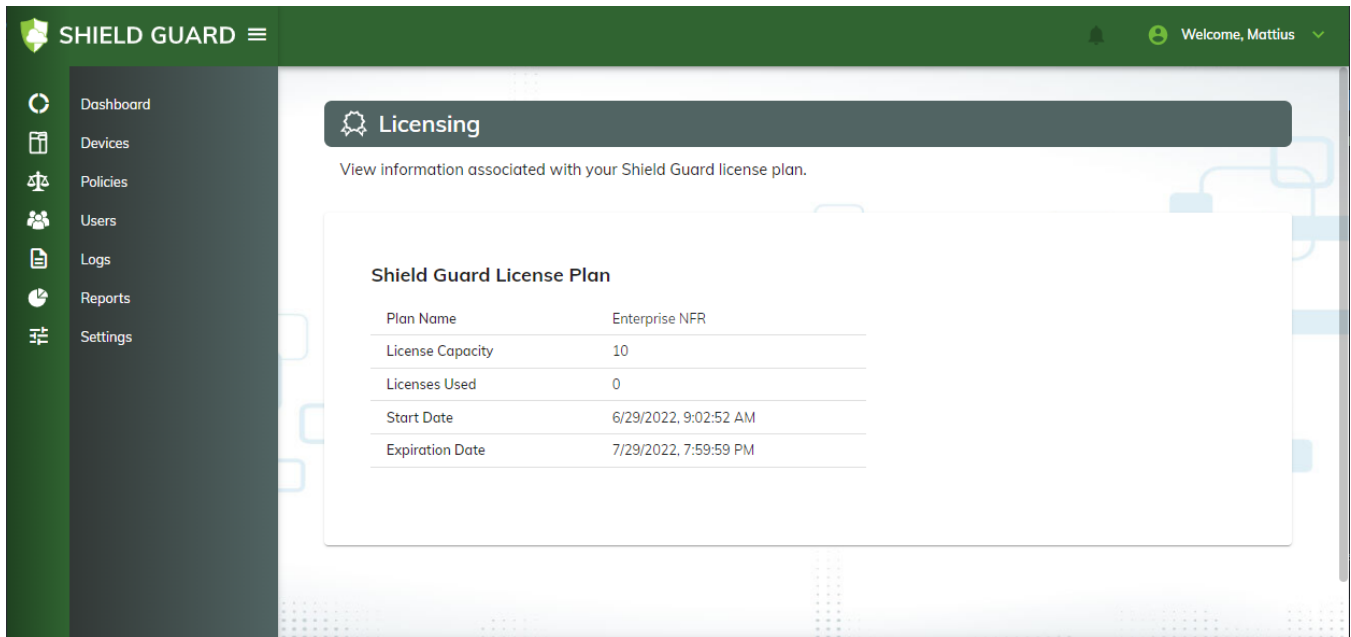
Note: If you are a member of only one tenant, note the following:

- The Select a Tenant page does not appear. Instead, when first accessing the portal, you proceed directly to the Dashboard page.
- The name of the tenant does not display on the Title bar.

Licensing Page

The Licensing page displays information on the license plan associated with your **tenant**. You can access the Licensing page via the **Welcome** button. Access is restricted to tenant members with License Plan Management **permission**.

The following illustration shows the Licensing page for a 30-day trial license plan called Enterprise NFR:



Note: If you have access to multiple tenants, the Licensing page displays information only for the tenant you are currently accessing on the portal.

Shield Guard License Plans

Your license plan consists of the selections you made at the time of purchase, including the following:

1. **Billing method** (Subscription or Term). This selection determines the frequency at which you are billed for use of Shield Guard.
2. **Shield Guard plan** - For example, the Enterprise plan. This selection determines the Shield Guard features available in your tenant and partly determines the cost of your license plan.
3. Device licenses - A separate device license is required for each device you want Shield Guard to monitor. This selection determines the number of devices you can monitor with Shield Guard and partly determines the cost of your license plan.
4. Shield Guard Agent licenses (free) - The agent must be installed on each device you want Shield Guard to monitor.

Thus, the license plan you create during the purchasing process determines your billing requirements for maintaining a Shield Guard license in good standing and the functional capacity of your Shield Guard tenant.

Shield Guard Billing Options

The following billing options are available for Shield Guard:

- Subscription - A monthly subscription license, billed at the beginning of each billing cycle, until you cancel the subscription.

- Term - A one-year term license, billed at the time of purchase.

The license type you purchase determines the frequency at which you are billed for use of Shield Guard. The amount you are billed is determined by the Shield Guard plan you purchase and the number of device licenses you purchase with your plan.

Notes:

- The type of billing method you choose does not affect your purchase options. You can purchase any Shield Guard plan available in your region, and you can purchase any quantity of device licenses.
- A free, 30-day **trial license** is available, providing full access to the Enterprise plan. You can upgrade from your trial license to a purchased plan.

Subscription Licenses

Shield Guard subscription licenses are available in a monthly billing cycle. Payment is due at the beginning of each billing period, as determined by the purchase date. The plan remains active until the end of the period, when a new monthly billing period begins. If you cancel your subscription, the license plan remains active until the end of the current billing period.

The Licensing page displays the following information for subscription licenses:

- Current Subscription - The current license plan, for example, the Enterprise plan.
- License Capacity - The total number of device licenses purchased under the license plan, and the maximum number of devices that can be added to the tenant under the current plan.
- Licenses Used - The number of licenses in the plan currently assigned to a device.
- Billing Frequency - The frequency at which payments must be made to sustain the subscription.

Modifying Your Subscription

You can upgrade your subscription license plan and/or modify the license capacity for the plan at any time. If your subscription has lapsed, you can purchase a new license plan (subscription or term) at any time. To downgrade or cancel your subscription license, contact your local Shield Guard sales representative.

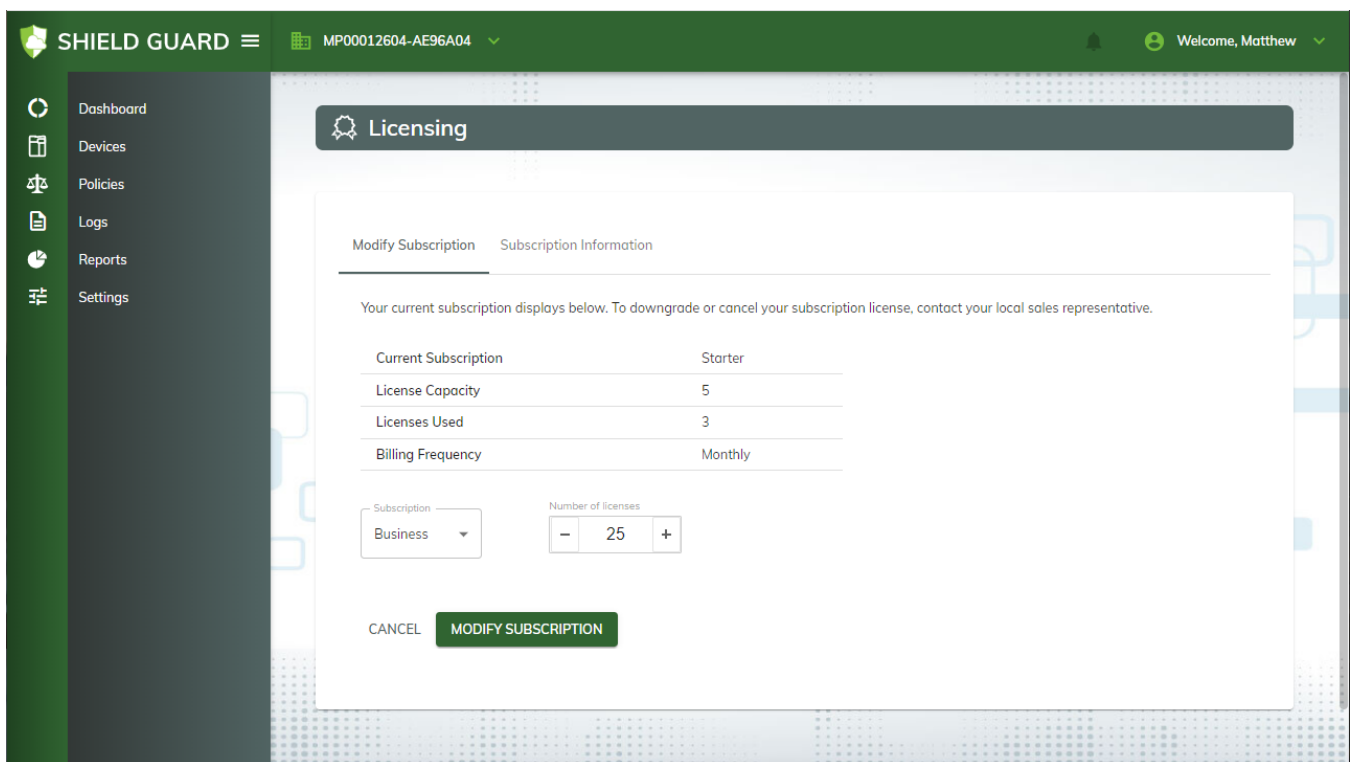
Note: Only Shield Guard subscription licenses include the option to modify the license plan. Term licenses or trial licenses cannot be modified.

To modify the configuration of a Shield Guard subscription license plan, do the following:

1. Access the **tenant** whose license plan you want to modify (required only if you belong to multiple tenants).
2. Access the Licensing page, and click on the **Modify Subscription** tab.

3. At the **Subscription** field, your current plan displays. To change the plan, click on the current plan and select a new plan from the list that appears. Note that if your current plan is Enterprise, the upgrade option is not available.
4. At the **Number of Licenses** field, the current number of licenses purchased under your license plan displays. To modify the quantity, select the current quantity and then enter the new license capacity. You can also use the - or + buttons to change the quantity decrementally or incrementally, respectively.
5. Once you modify either the **Subscription** or **Number of licenses** field, the **MODIFY SUBSCRIPTION** button activates, indicating a change to the current license plan is pending.

The following illustration shows a subscription for the Starter plan with a license capacity of 5. In the Subscription field, “Business” has been selected as the new plan, and the Number of licenses field has been modified to 25 licenses. The **MODIFY SUBSCRIPTION** button is active, indicating a change to the current license plan is pending:



6. Once you have made your selection(s), click on the **MODIFY SUBSCRIPTION** button. The Modify Subscription window appears displaying your current license plan configuration as well as your proposed changes to the plan, including the updated cost for each billing period. See the following illustration:

Modify Subscription

It looks like you want to modify your subscription. Please confirm the details below.

	Current Plan	New Plan
Subscription	Starter	Business
License Capacity	5	25
Subscription Cost	\$ ██ /month	\$ ██ /month

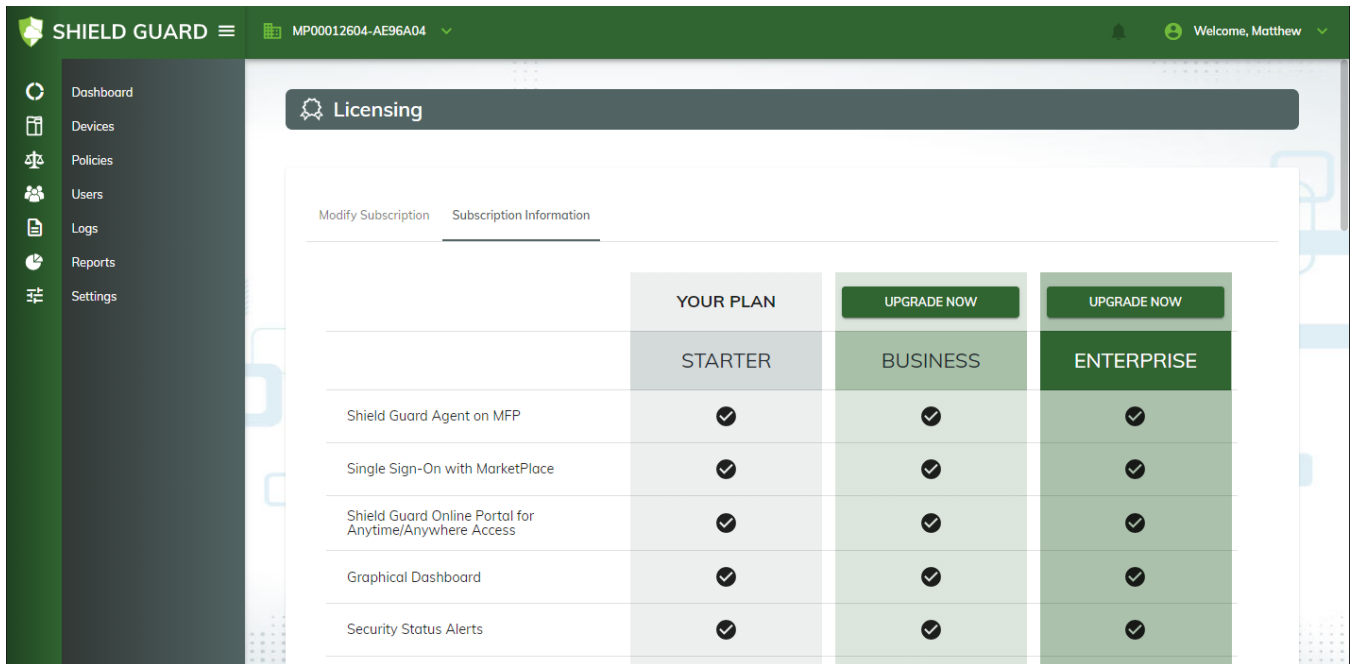
Updated Subscription Cost
\$**██**/month

CANCEL **CONFIRM**

7. To proceed with the changes to your subscription license plan, click on the **CONFIRM** button. The Licensing page updates with the new configuration. Or, to abandon your changes, click on the **CANCEL** button.

Upgrade Options for Your Shield Guard Plan

To view your upgrade options and compare the features available in your Shield Guard plan with the features available in your upgrade options, click on the Subscription Information tab. The following illustration shows the upgrade options for a user with the Starter plan:



Term Licenses

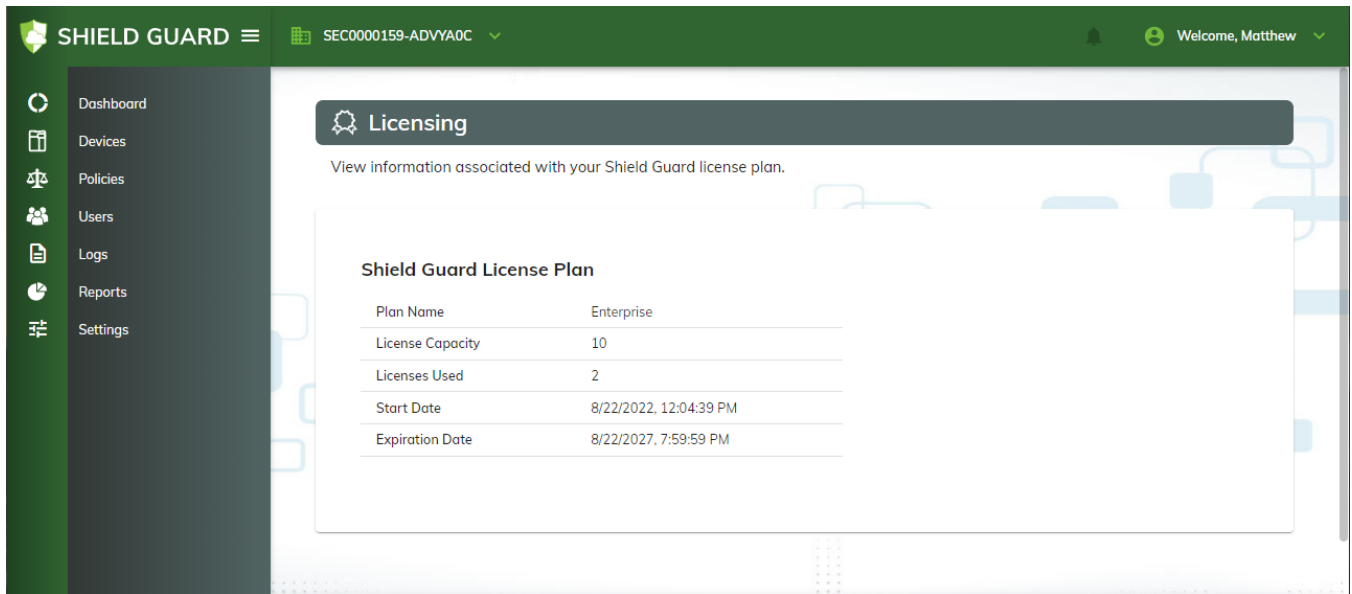
Shield Guard term licenses are available on a yearly basis, for any number of years you choose. Payment is due upon purchase, and the plan remains active from the date of purchase until the number of years on your license expires. You can renew your term license at any time. If you cancel your term license, the license plan remains active until the end of the term.

Note: Term licenses and trial licenses cannot be modified. Only Shield Guard subscription licenses include the option to modify the license plan.

To view information on a term license, access the **tenant** whose license plan you want to view (required only if you belong to multiple tenants). The Licensing page displays the following information for term licenses:

- Plan name - The type of Shield Guard plan, for example, Enterprise.
- License capacity - The total number of licenses purchased under the plan, and the maximum number of devices you can add to the tenant.
- Licenses used - The number licenses in the plan currently assigned to a device.
- Start date - The date and time on which the license plan was started.
- Expiration date - The date and time on which the license plan will end, or did end.

The following illustration shows the Licensing page for a term license:



Trial Licenses - Upgrading to a Paid License

To upgrade your **free trial license** to a paid license, use the Upgrade License area on the Licensing page. This area appears only for free-trial tenants.

The screenshot shows a web portal interface for license management. At the top, there's a green header with a user profile 'Welcome, Matthew' and a tenant ID 'JH000259-SGTRIAL'. The main content area is titled 'Licensing' and contains a table of license details and an upgrade section.

Shield Guard License Plan	
Plan Name	Enterprise Free Trial
License Capacity	1
Licenses Used	0
Start Date	3/11/2024, 2:37:06 PM
Expiration Date	4/10/2024, 7:59:59 PM

Upgrade License

To upgrade your license plan, please contact your authorized sales representative to obtain a purchase code

Enter a purchase code to upgrade your license.

Purchase Code:

You can upgrade your trial license at any time while it is active. As your **expiration date** approaches, Shield Guard displays a warning banner showing the expiration date.

To upgrade to a paid license, do the following:

1. Obtain a purchase code from your Shield Guard representative.
2. Enter the purchase code into the Purchase Code field.
3. Select **Submit**. A confirmation message appears, and the Licensing page updates to display your upgraded plan.

Notes:

- Purchase codes are not case-sensitive.
- The device count for your purchase code must be equal to, or greater than, the licenses currently being used in the tenant. This quantity is displayed at the Licenses Used field on the Licensing page. If your purchase code has insufficient licenses, you must either purchase additional device licenses or **remove devices from the tenant**.

Portal Page Elements

Each page in the **Shield Guard Portal** consists of several common elements. Note that the functionality of some of these elements varies depending on whether or not you are logged in to the portal. Each is described below.

Title bar

The Title bar appears at the top of the portal screen. It displays the site name as well as access to other information and site options. The following illustration shows the Title bar as it appears within the **Admin area**:



Any of the following buttons/icons may appear on the Title bar, depending on your location within the portal.

Name	Description
Site name	Displays the site name. If you click on the site name from within the Admin area , the Dashboard page appears. If you click on the site name from outside the Admin area, the Home page appears.
Expand/Collapse Menu button	Controls the display of the Navigation pane . Click on this button to expand or collapse the pane. When the Navigation pane is expanded, the names of the available pages in the site appear along with their icon. When collapsed, only the icons appear. If you hover over the collapsed pane, the pane expands showing the page names. To lock the pane to its expanded state, click on this button while hovering over the collapsed pane.
Shield Guard tenant	If you are a member of multiple Shield Guard tenants, the name of the current tenant displays here. To select another tenant, click on the drop-down menu and select a tenant from the list that appears. If you are a member of only one tenant, this selection option does not appear.
Notifications icon	A red badge next to the icon indicates notifications are available. Click to view the Notifications list. To acknowledge a notification, click on the associated Dismiss button. The notification is removed from the Notifications list. To exit the Notifications list, click outside the list area. Any notifications you did not dismiss are preserved, and the notification count in the red circle updates to account for any notifications you dismissed. If no red badge appears next to the Notifications icon, no notifications are available.
Welcome button	Accesses a dropdown menu with various options . This button appears only if logged in to the portal. If not logged in, the LOGIN button appears.

LOGIN Button

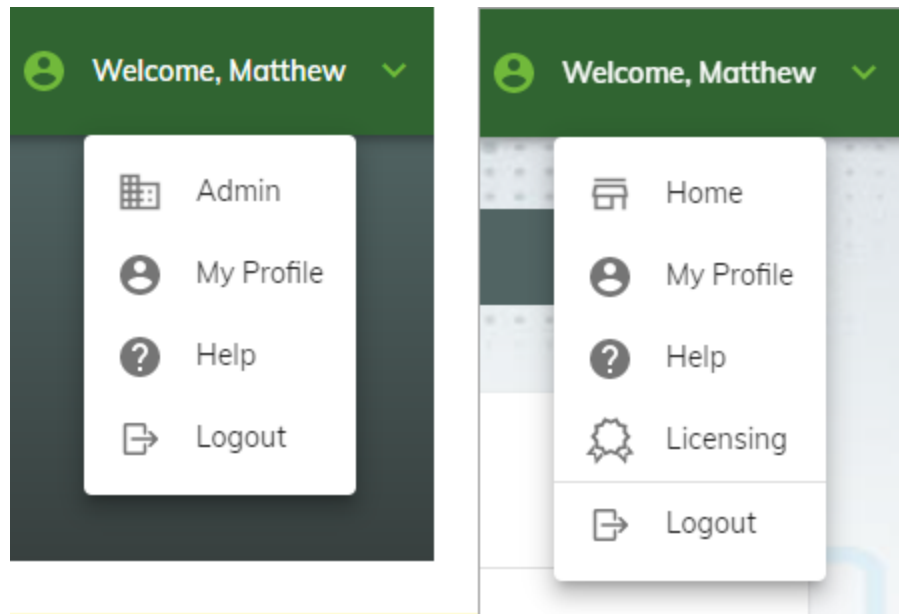


The **LOGIN** button accesses the Login screen or, if already logged in to the MarketPlace, logs you in to the portal via single-sign-on (SSO). It appears on the right end of the Title bar when logged out of the Shield Guard portal. When logged in, the **Welcome** button appears instead.

Welcome Button

The **Welcome** button appears on the right end of the **Title bar** when logged in to the Shield Guard portal. It includes the name of the logged-on user as well as a drop-down menu providing access to areas of the portal, for example the **My Profile** page. The drop-down menu also includes the **Logout** button.

The options available on the **Welcome** button drop-down menu vary depending on your current logged-in status, for example, whether you are currently accessing the Admin area or the Home page. In the following illustration, the left image shows the options available via the Home page, the right image shows the options available via the Admin area:



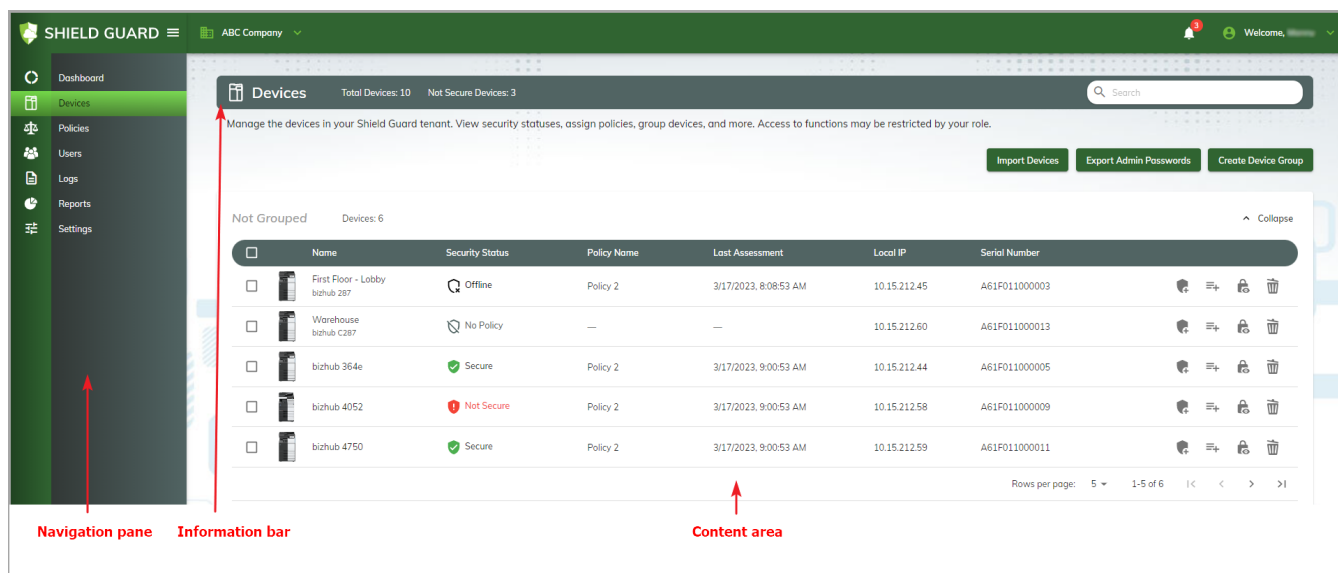
The following describes the options available on the Welcome button drop-down menu, and the situations in which the options appear.

- **Admin** - Accesses the **Admin area**. This option appears only if you are not currently accessing the Admin area.
- **Home** - Accesses the **Home** page. This option appears only if you are currently accessing the Admin area.
- **My Profile** - Accesses the **My Profile** page. This option appears only if you are not currently accessing the My Profile page.
- **Help** - Opens the Shield Guard online help in a new window.
- **Licensing** - Accesses the **Licensing** page. This option appears only if:
 - You are currently accessing the Admin area.
 - You have selected a tenant (required only if you have access to multiple Shield Guard tenants).
 - You have License Plan Management **permission** for the current tenant.
- **Logout** - Logs you out of the portal.

Page Elements

- **Navigation pane** - Provides links to the pages available to display in the Content area. The Navigation pane is collapsible. Use the **Expand/Collapse Menu** button.
- **Information bar** - Appears near the top of most pages in the portal. This bar displays the name of the page currently appearing in the Content area. If applicable, the bar displays a count of the items available to display in the Content area as well as a **Search** field you can use to filter the list of items that display on the page, for example, if the list is long.
- **Content area** - Displays the page currently selected in the Navigation pane.

The following illustration shows the Devices page:



Footer Bar

The Footer bar appears at the bottom of all pages in the **Shield Guard Portal**. See the following illustration:



The Footer bar contains links to the following:

- **Contact Us** - Opens the MarketPlace Contact page in a new window.
- **Cookie Settings** - Accesses the **Cookie Settings window**, where you can view a list of web cookies used on the Shield Guard site.
- **Privacy** - Accesses the Privacy Policy page on the Shield Guard Portal.
- **Terms and Conditions** - Accesses the Terms and Conditions on the Shield Guard Portal.

- **EULA** - Accesses the End-User License Agreement page (EULA) on the Shield Guard Portal.

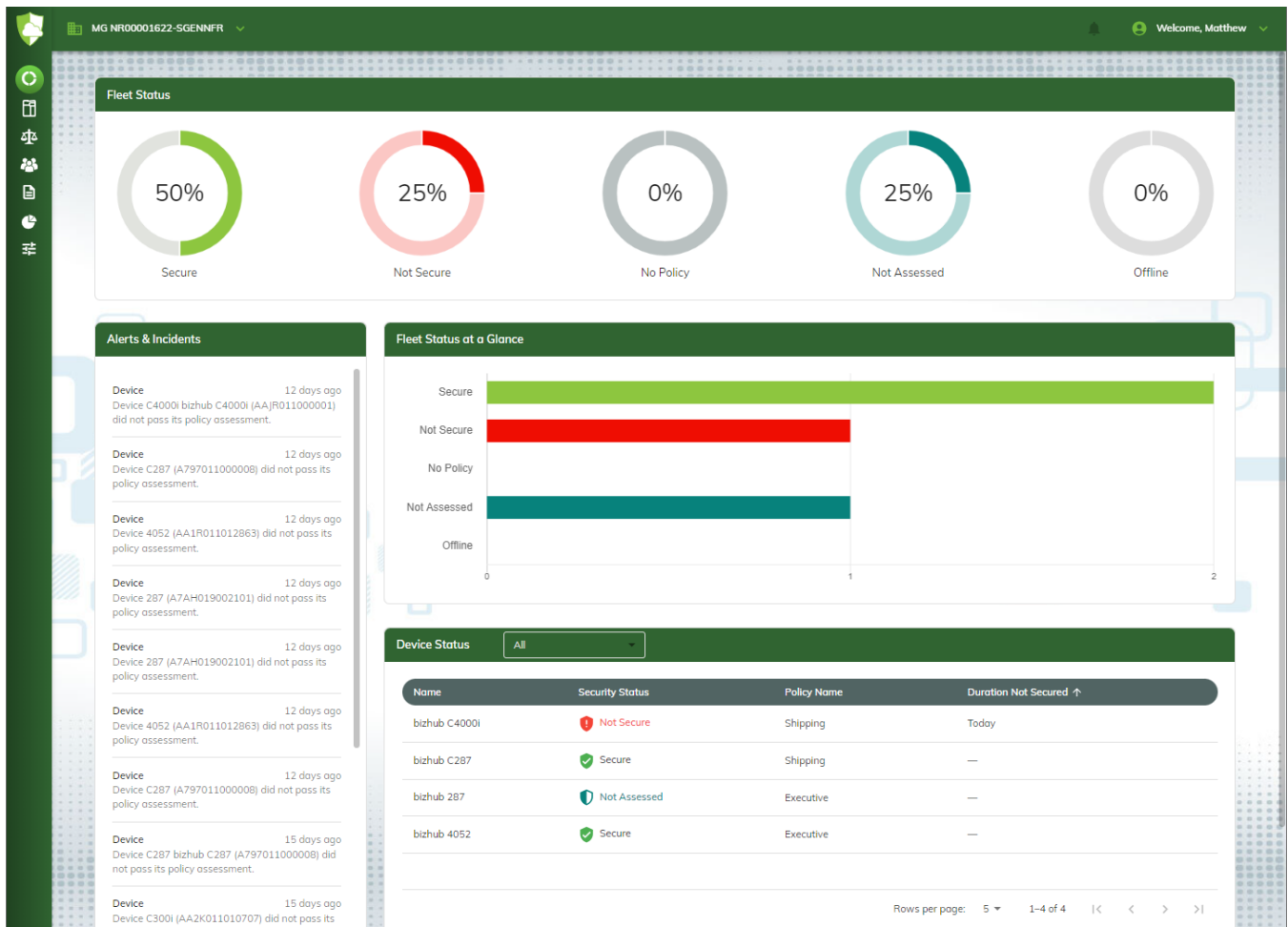
Dashboard Page

The Dashboard page displays an overview of the security statuses of the devices in your tenant. At a glance, you can view the following:

- A list of alerts and incidents.
- The overall security status of your fleet of devices.
- The security status of individual devices in your fleet.

In addition, the Dashboard page includes several clickable options that provide direct access to additional security information on your tenant devices.

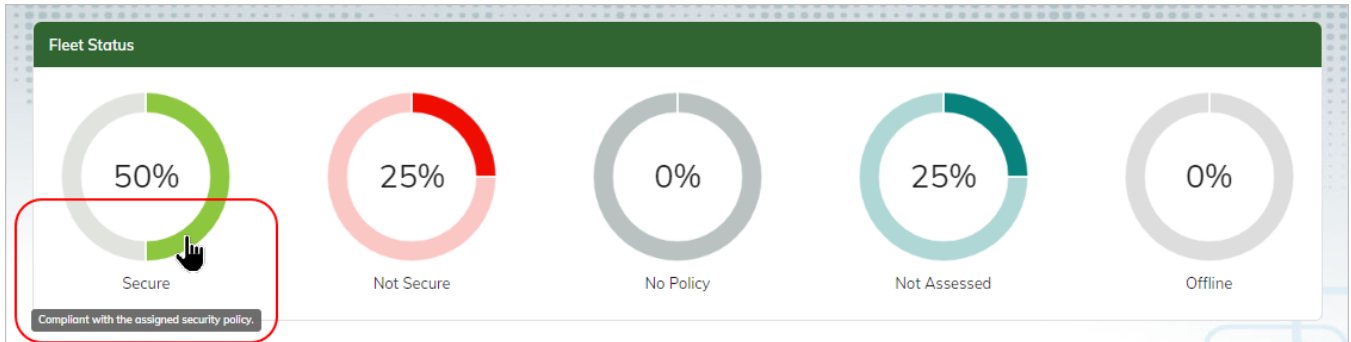
The Dashboard page appears in the following illustration:



The Dashboard page consists of the following areas of information:

Fleet Status

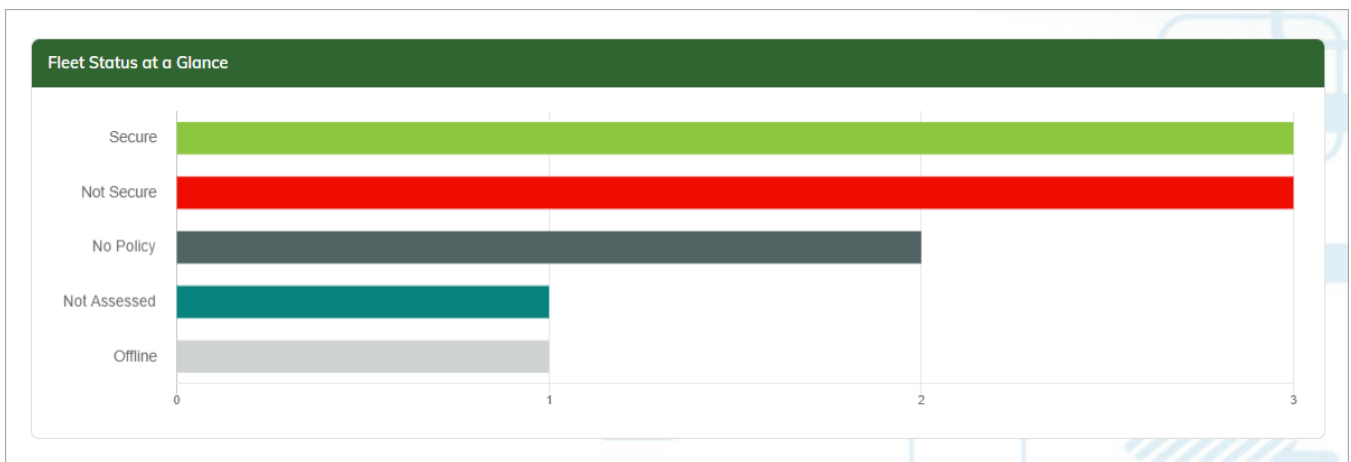
This panel displays a donut graph for each of Shield Guard’s **security statuses**. Each time Shield Guard performs a security assessment on a device (as determined by the **heartbeat sync frequency** specified for the security policy), a security status is assigned to the device based on the assessment. The donut graphs show the percentage of devices in the tenant that were assigned that status in Shield Guard’s most recent security assessment. If you hover your pointer over a donut graph, a brief description of the security status displays.



Note: If you select a donut graph, the **Device Status table** updates to display the devices with that status.

Fleet Status at a Glance

This panel displays a bar graph for each of Shield Guard’s **security statuses**. Each time Shield Guard performs a security assessment on a device (as determined by the **heartbeat sync frequency** specified for the security policy), a security status is assigned to the device based on the assessment. The bar graphs show the number of devices in the tenant that were assigned that status in Shield Guard’s most recent security assessment. If you hover your pointer over a bar, the actual number of devices with that status displays.

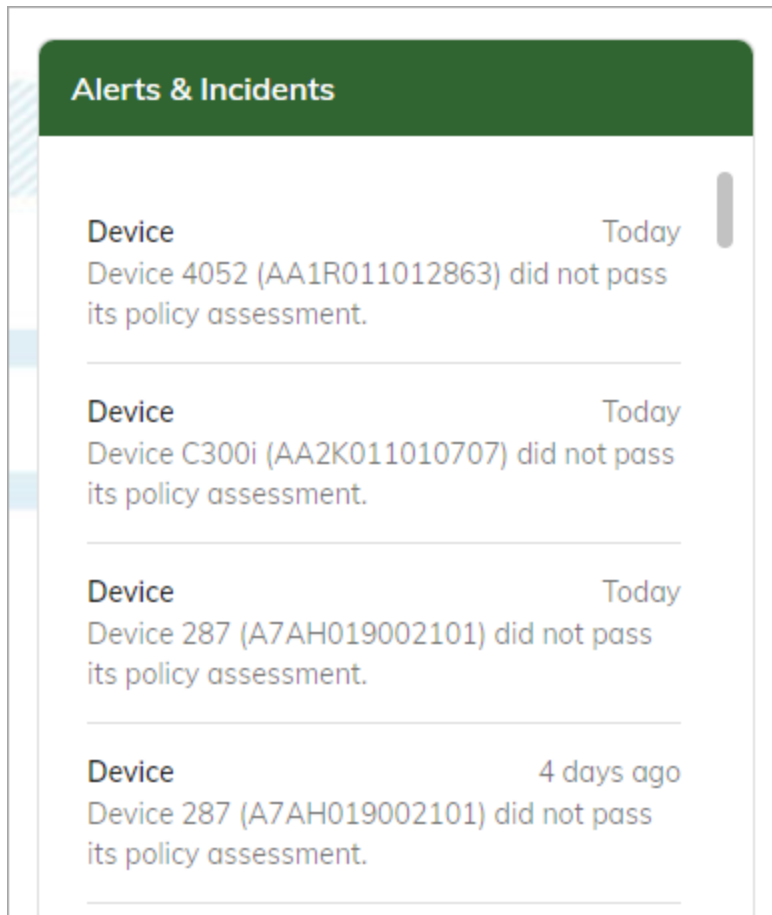


Note: If you select “Fleet Status at a Glance”, the Reports page appears showing a pre-filtered report of device status changes in the last 30 days.

Alerts & Incidents

This panel lists alerts generated by security policy assessments. The following information displays:

- Alert type - For example, device alerts or user alerts.
- Date and time of incident - The number of days that have elapsed since the incident occurred. If you hover the pointer over this display, the actual date and time appear.
- Description of the alert - Additional information on the alert. For example, device alerts include the device name and serial number as well as whether the device passed the security assessment performed on the day indicated.



Device Status

This table lists the current security status of all devices in the tenant. For Not Secure devices, the Duration Not Secured column lists the date on which the device was assessed as Not Secure. The table header includes a dropdown menu, via which you can filter the table to display a selected status.

Device Status			
All			
Name ↑	Security Status	Policy Name	Duration Not Secured
bizhub 287	Not Assessed	Executive	—
bizhub 4052	Secure	Executive	—
bizhub C287	Secure	Shipping	—
bizhub C4000i	Not Secure	Shipping	Today

Rows per page: 5 1-4 of 4

Note: If you select a row in the table, the **Logs page** appears where you can view the log event that initiated the status change for the device.

Remediating Not-Secure Devices

Most Shield Guard settings include an **auto remediation** option, via which Shield Guard can bring a setting into compliance without human intervention. If the device does not support auto-remediation for the setting, or auto-remediation fails to bring the setting into compliance, you will likely need to access the device and manually update the setting.

To bring “Offline” devices “online” (for example, devices that are powered off or “asleep”), you must manually power-on or awaken the device to bring it online for Shield Guard to monitor.

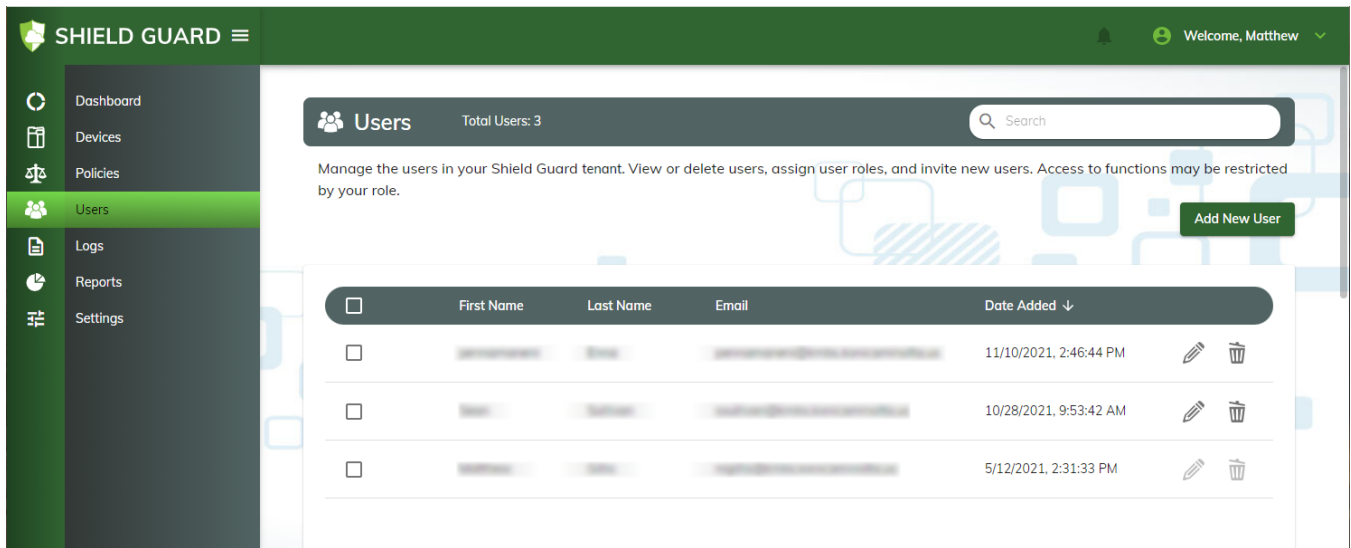
Occasionally, you may need to **adjust your Shield Guard policy settings** to address a failed assessment. However, over time, most of your remedial action will occur at the device and less on the Shield Guard Policies page.

Users Page

Use the Users page to view and manage the members of a **tenant**. The Users page:

- Lists the total number of members in the tenant.
- Lists the members in the tenant.
- Displays information on each member.
- Provides options to add, delete, and assign access roles to members.

All users joining a tenant are granted read-only access to the tenant and can download CSV (comma-separated-value) files (for example, from the **Reports page**). In addition, authorized members can assign **access roles** to selected users, providing the ability to edit certain pages in the portal, for example the Devices page. The following illustration shows the Users page:



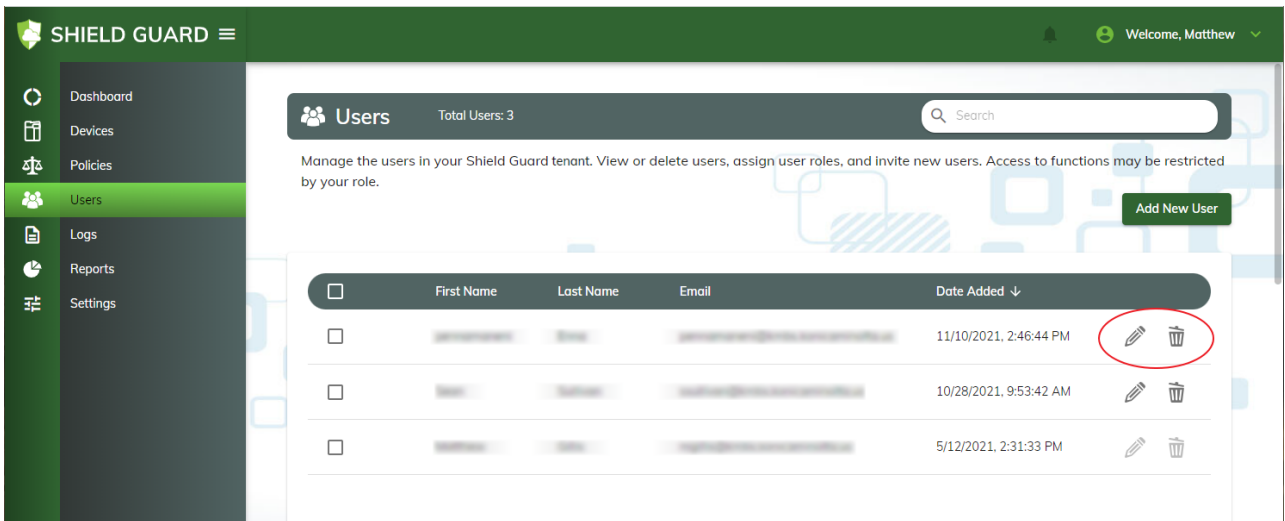
Managing the Users Table

The Users table lists the members in your tenant and displays the following information for each member.

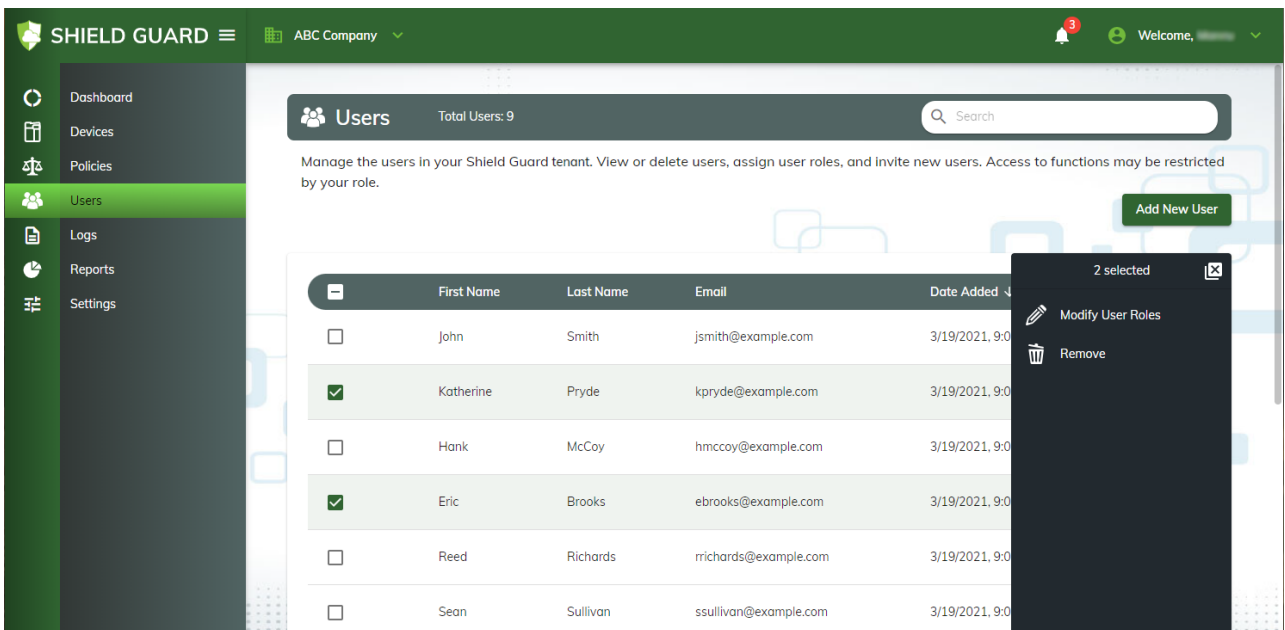
- **First Name** - The member's first name.
- **Last Name** - The member's last name.
- **Email** - The member's email address.
- **Date Added** - The date and time on which the member was added to the tenant.

In addition to the above information, the Users table includes the following:

- A header row where, if you click on a column header, the table sorts by that column. The column header displaying an arrow (up or down) indicates the current sort criteria and sort order (ascending or descending).
- Selection boxes you can use to select users on which to perform an action. Selection boxes appear on the left side of the Users table.
 - To select one user at a time, click on the selection box in the row containing the user.
 - To select all users in the tenant, click on the selection box in the table header.
- Action icons providing access to the functions you can perform on a user, for example the Remove User function. If you click on an Action icon in the Users table, you access the function directly. See the following illustration:



- A Bulk Action panel that appears when you check one or more selection boxes. All available Action icons appear in the panel, and if you click on an Action icon, the function is applied to all selected users. In the following illustration, two items in the table have been selected, the Bulk Action panel appears on the right, and the available actions appear in the panel:



Users and Roles

All users must have a MarketPlace account before they can join (or create) a tenant. The user who creates the tenant is the tenant owner. The tenant owner has full access within the Shield Guard Portal. All other users must be invited to join the tenant via the **Add New User** button. As part of the invitation process, users can be granted one or more access roles permitting them to modify

features/functions within the Shield Guard system. Users with no assigned roles are restricted to read-only access and cannot modify any settings on the portal.

Note: A tenant owner's access roles cannot be modified by other users, and the tenant owner cannot be deleted from the tenant. To transfer the tenant owner's license to another user account (for example, if the tenant owner leaves the company), contact your Shield Guard support representative.

In addition to granting access roles to new users via the Add New User process, existing users' (tenant members') access roles can be modified via the Users table on the Users page. Only users with the User Management role can grant or modify user roles in the Shield Guard system. The following user access roles are available:

- Device/Policy Management - Users can:
 - Add/edit/remove devices.
 - Create/apply/edit security policies for devices in the tenant.
- User Management - Users can
 - Add/remove users.
 - Assign/unassign user roles in the tenant.
- License Plan Management - Users can
 - Access the **Licensing page** to view and/or modify the **license plan**.
 - Edit the name and the Tenant Vault Key Management setting of the tenant via the **Settings page**.

Adding a New User

To add a new user to the tenant, use the **Add New User** button to send an invitation. You can send user invitations either by email or by generating a link and sending it to the recipient. As part of the invitation, you can grant one or more access roles to the user. User invitations are valid for 7 days. Once the invitation is accepted, the user will appear on the tenant's Users page.

Note: Only users with the User Management role can access the **Add New User** button.

Do the following:

1. On the Users page, click on the **Add New User** button. The Add New User window appears.

Add New User

To invite a new user to the tenant, specify an email address.

Note: Invitations can be used only once. They expire after 7 days.

By email By link

User*

Roles

By default, all users are granted read-only access to the tenant. To assign roles to the user, check one or more boxes below.

- Device/Policy Management
Add/edit/remove devices. Create/edit/delete security policies. Apply/remove policies to/from devices.
- User Management
Add/remove users. Modify users' roles.
- License Plan Management
Modify the license plan and/or the tenant name.

I understand this user may be able to view sensitive information such as device passwords. * **Required**

INVITE

2. Specify the method by which to invite the user and the access roles (if any) you want to grant to the user. You have the following options:
 - **By email** - Send an email using your local default email account. The email contains a link that, when clicked on, adds the user to the tenant. Do the following:
 1. Click on the **By email** tab. The **User** field and the available access roles appear.
 2. In the **Roles** area, check the box next to the access roles (if any) you want to grant to the user.

3. In the **User** field, enter the user's email address. Once the field contains a valid email address, the **Invalid email address** message disappears.
 4. Check the box at the **I understand...** field. Once you check this box and the **User** field contains a valid email address, the **INVITE** button activates.
 5. Click on the **INVITE** button. Your default email app opens, displaying the email you just created.
 6. In your default email app, send the email.
- **By link** - Generate a link you can copy and send to the user. Do the following:
 1. Click on the **By link** tab. The **Invitation link** field and the available access roles appear.
 2. In the **Roles** area, check the box next to the access roles (if any) you want to grant to the user.
 3. Click on the **GET LINK** button. The link appears in the **Link** field and is copied to your clipboard.
 4. Access the app you want to use to send the link and paste the link into the message you want to send. Include any information you want to provide to the recipient, for example that the invitation will expire in 7 days.

Modifying User Roles

To modify one or more users' access roles, do the following:

1. Check the selection box in the Users table for each user whose roles you want to modify. The Bulk Action panel appears.

Note: If you select multiple users, you must assign the same set of roles to each user.

2. Click on the **Modify User Roles** icon. The Modify User Roles window appears.

Modify User Roles

Select the roles that you would like to assign to the selected users.

By default, all users are granted read-only access to the tenant. To assign roles to the user, check one or more boxes below.

- Devices/Policies Management**
Add/edit/remove devices and create/apply/edit security policies for those devices.
- User Management**
Add/remove users and modify user roles.
- License Plan Management**
Modify license plans, edit the name of license groups, and request license termination.

3. The Modify User Roles window displays the existing roles for the selected user(s). Note the following:
 - A checked box indicates the role is currently assigned to all selected users.
 - A grey box enclosing a white bar indicates an indeterminate (mixed) state for the role with regard to the selected users. That is, some of the selected users are assigned the role, some are not.
 - An empty box indicates the role is not currently assigned to any of the selected users.
4. Make any modifications to the set of roles you want to assign to the selected user(s). Note that if any of the selection boxes are in a mixed state, you cannot save your changes.
5. Once all boxes are in a valid state, the **SAVE** button activates. To preserve your changes, click on this button. To abandon your changes, click outside the Modify User Roles window.

Deleting a User

To delete a user, click on the Delete icon associated with the user in the Users table.

To delete multiple users, do the following:

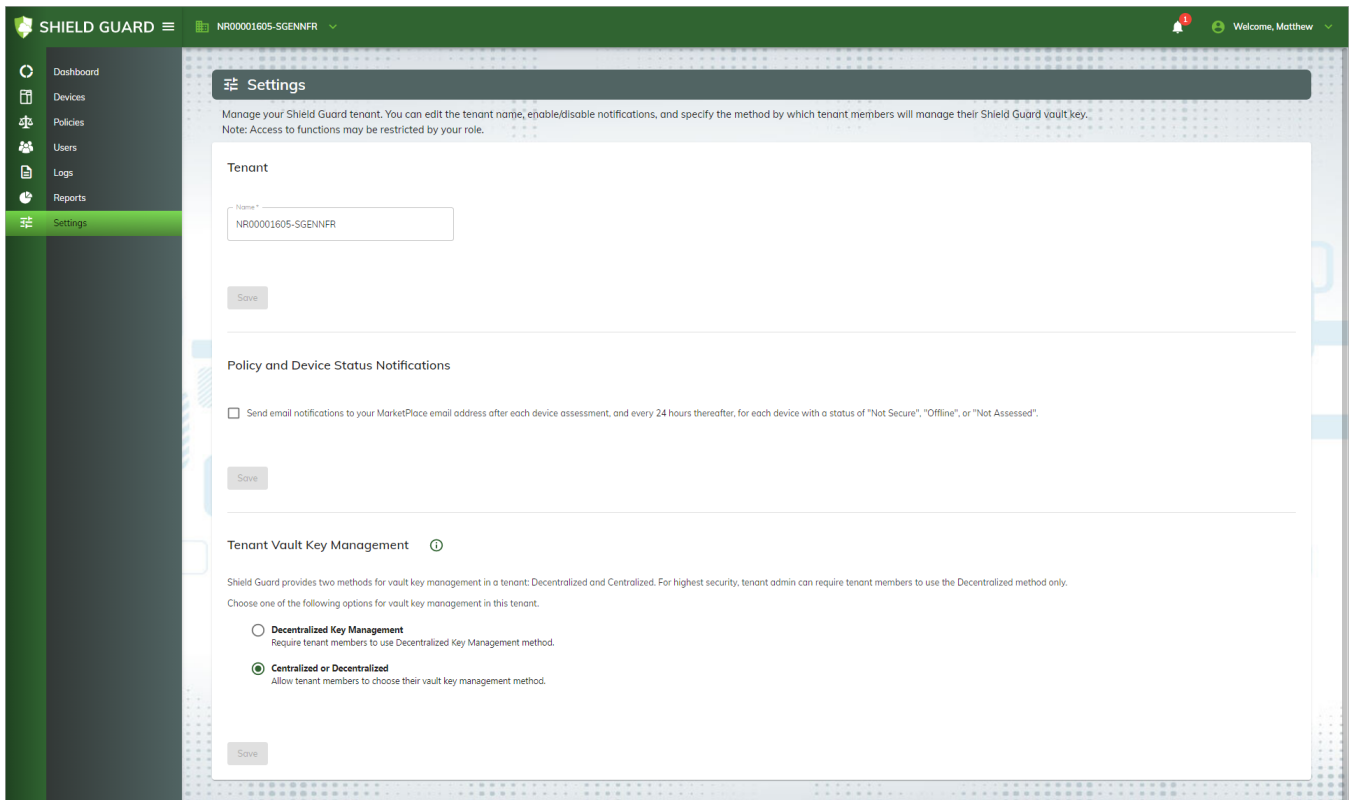
- Check the selection box for each user you want to delete from the tenant. To select all users, click on the selection box in the header row of the Users table.

- Once you select one or more users, the Bulk Action pane appears. Click on the Remove icon in the pane. The selected users are removed from the tenant.

Note: Tenant owners cannot be deleted from the tenant. Thus, the Delete icon is inactive for the tenant owner.

Settings Page

Use this page to configure settings for the current **tenant**, including tenant vault management options. See the following illustration:



Your configuration options are contained in the following sections of the page:

Tenant

An authorized tenant member (any member with the License Plan Management **permission**) can use this section to modify the tenant name.

- **Name** - When you first create a tenant, a default tenant name appears here. Specify a descriptive name for the tenant.

Policy and Device Status Notifications

To send email notifications to your MarketPlace email address regarding policy and device status, place a check the box. Otherwise, leave the box blank.

Shield Guard sends notifications when a device status changes to “Not Secure,” “Offline,” or “Not Assessed.”

Tenant Vault Key Management

An authorized tenant member (any member with the License Plan Management **permission**) can use this section to select a tenant vault key management option for the tenant. The default setting is Decentralized Key Management.

Note: The Tenant Vault Key Management setting applies to the tenant as a whole. It is distinct from the “tenant *member* vault key management method”, which refers to the **vault key management method** that must be applied to each individual password vault.

See the following illustration:

Tenant Vault Key Management ⓘ

Shield Guard provides two methods for vault key management in a tenant: Decentralized and Centralized. For highest security, tenant admin can require tenant members to use the Decentralized method only. Choose one of the following options for vault key management in this tenant.

Decentralized Key Management
Require tenant members to use Decentralized Key Management method.

Centralized or Decentralized
Allow tenant members to choose their vault key management method.

- **Decentralized Key Management** - Require users connecting to this tenant to use Decentralized Key Management. If you select this option, tenant members are restricted to the **Decentralized** method.
- **Decentralized Key Management or Centralized Key Management** - Allow users to choose their vault management method. Users have the option to select either Decentralized or **Centralized** key management.

Note: If you change the Tenant Vault Key Management selection to Decentralized Key Management, any tenant members or pending members who use the Centralized method will be restricted from the tenant. Tenant members using the Decentralized method at the time of the change can continue to use their current vault and key.

Shield Guard sends an email with this information to each restricted member, and also posts a banner in each tenant member’s portal indicating they are currently restricted from the tenant. The banner includes a link to the My Profile page, where the Modify My Vault Key Management window appears and the tenant member can change their vault management method to Decentralized and create a vault master key.

Managing Devices

Overview of Devices

Shield Guard monitors the security settings of **supported Konica Minolta MFPs (multi-function peripheral devices) and SFPs (single-function peripheral devices)** on which the Shield Guard Agent is installed. **Installing and launching the agent on a device** makes the device available for import into a **tenant** via the Shield Guard Portal's Devices page. Devices in a tenant can be assigned a security policy. Once a policy is assigned to a device, security monitoring of the device can begin.

On the Devices page, **privileged users** can:

- **Import devices** into the tenant.
- **View a list of issues** for a Not Secure device.
- **Export Admin Passwords** to a CSV (comma-separated-value) file.
- **Create device groups** in which to organize devices.
- **Assign a security policy** to a device or a device group.
- **View a list of devices** in the tenant, including their security information.

To access the Devices page, click on **Devices** in the **Navigation pane**. See the following illustration:

The screenshot shows the SHIELD GUARD interface for the 'Devices' page. The navigation pane on the left includes Dashboard, Devices, Policies, Users, Logs, Reports, and Settings. The main content area shows a summary of 'Total Devices: 10' and 'Not Secure Devices: 3'. Below this, there are two tables of devices. The first table, 'Not Grouped', lists 6 devices with various security statuses. The second table, 'HQ Building 101', lists 3 devices, including one that is 'Not Secure' and one that is 'Not Assessed'. Each device row includes a checkbox, name, security status, policy name, last assessment, local IP, and serial number, along with action icons for edit, lock, and delete.

Name	Security Status	Policy Name	Last Assessment	Local IP	Serial Number
First Floor - Lobby bizhub 287	Offline	Policy 2	3/17/2023, 8:08:53 AM	10.15.212.45	A61F011000003
Warehouse bizhub C287	No Policy	—	—	10.15.212.60	A61F011000013
bizhub 364e	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.44	A61F011000005
bizhub 4052	Not Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.58	A61F011000009
bizhub 4750	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.59	A61F011000011

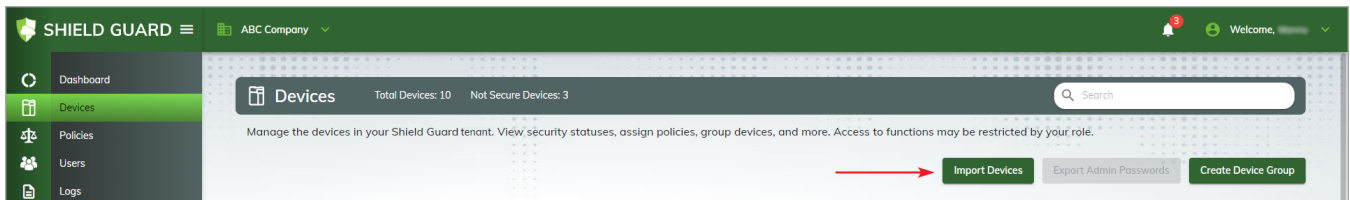
Name	Security Status	Policy Name	Last Assessment	Local IP	Serial Number
Third Floor - Lobby bizhub C287	Secure	Policy 1	3/17/2023, 9:00:53 AM	10.15.212.61	A61F011000015
First Floor - Lab bizhub 364e	Not Secure	Policy 1	3/17/2023, 9:00:53 AM	10.15.212.43	A61F011000007
bizhub C300i	Not Assessed	Policy 1	—	10.15.212.62	A61F011000017

Notes:

- Each device with Shield Guard installed must have the **Password Change Permission** setting set to “Allow” at the device.
- The first time you access this page in a session, Shield Guard prompts you to **unlock the password vault**.

Importing Devices

For Shield Guard to monitor a device, you must first import it into a **tenant**. To import one or more devices into the tenant, click on the **Import Devices** button.



The Import Devices from MarketPlace window appears:

Import Devices from MarketPlace

Import devices from MarketPlace to your Shield Guard license plan here. Select one or more available devices and use the Arrow button to add them to Shield Guard.

Note: The list of available devices is restricted to devices in your MarketPlace account with the Shield Guard agent installed.

Available Devices 1/5 selected	Selected Devices 0/0 selected
<input checked="" type="checkbox"/> Second Floor - QA (C556) A61F0114002047	
<input type="checkbox"/> Second Floor - Lab (C554) A61F011400234	
<input type="checkbox"/> C358 A31F011400204	
<input type="checkbox"/> C354 A31F011400234	
<input type="checkbox"/> Second Floor - Dev (C558) A61F011400204	
<input type="checkbox"/> C356 A31F0114002047	

IMPORT

The Available Devices panel lists all devices for which the following is true:

- The Shield Guard Agent is **installed and has been launched at least once**.
- You have administrative privileges.

Note: Any devices already assigned to another tenant (whether by you or another user) appear dimmed and are not available for selection.

To import devices, do the following:

1. In the Available Devices panel, click on the selection box next to each device you want to add to the tenant. To select all available devices, click on the box in the panel header.
2. Once you select a box, the > button between the panels activates. When you have selected all the devices you want to add, click on the > button. The devices appear in the Selected Devices panel and the **Import** button activates.

3. To remove one or more devices from the Selected Devices panel, click on their associated boxes and then click on the < button. The devices return to the Available Devices panel.

Note: To exit the Import Devices from MarketPlace window without adding any devices, click outside of the window at any time.

4. When the Selected Devices panel contains all the devices you want to add to the tenant, click on the **Import** button. You return to the Devices page, and the device(s) appear in the Devices table.

Note: Adding a device to a tenant requires a **device license**. If sufficient licenses are not available to fulfill your request, an error message appears. All available licenses are assigned, and you can purchase additional device licenses for any devices that were not imported.

Creating Device Groups

Use device groups to organize the devices in your **tenant**. A device can belong to only one device group at a time. Once you create a device group, you can use the **Move to Device Group** option to add devices to the group.

To create a device group, click on the **Create Device Group** button.



The Create a Device Group window appears:

Create a Device Group

Enter a name for the device group you want to create. You have the option to assign a security policy.

Name

Policy
None

CREATE

In the Create a Device Group window, do the following:

1. **Name** - Enter a descriptive name for the group.
2. **Policy** - To assign a policy to the device group, click on the drop-down. Select a policy from the list that appears. The selected policy appears in the field. To assign no policy to the device group, select “None”.
3. **Create** - Once you specify a name for the group, this button activates and you can click on it to create the group. You return to the Devices page where a table appears for the new device group. You may have to scroll the page to see the table. To add devices to the group, find the device table containing the devices you want to add and use the **Move to Device Group option** action option.

Note: To exit the Create a Device Group window without creating any device groups, click outside of the window at any time.

Moving Devices to a Device Group

To move one or more devices into a device group, use the **Move to Device Group** button.

All devices moved into the device group assume the group’s assigned security policy. If no policy has been assigned to the group, the moved devices assume an Unassigned status.

1. Access the Move to Device Group window by doing one of the following:
 - a. To move a single device into a device group, click on the associated **Move to Device Group** button in the Devices table. See the following illustration:

Not Grouped		Devices: 6					Collapse	
<input type="checkbox"/>	Name	Security Status	Policy Name	Last Assessment	Local IP	Serial Number		
<input type="checkbox"/>	First Floor - Lobby bizhub 287	Offline	Policy 2	3/17/2023, 8:08:53 AM	10.15.212.45	A61F011000003		
<input type="checkbox"/>	Warehouse bizhub C287	No Policy	—	—	10.15.212.60	A61F011000013		
<input type="checkbox"/>	bizhub 364e	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.44	A61F011000005		
<input type="checkbox"/>	bizhub 4052	Not Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.58	A61F011000009		
<input type="checkbox"/>	bizhub 4750	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.59	A61F011000011		
<input type="checkbox"/>	bizhub C666	No Policy	—	3/17/2023, 9:00:53 AM	10.15.212.52	A61F011000621		

- b. To move multiple devices into a device group, check the selection box for each device. The Bulk Actions panel appears. Click on the **Move to Device Group** button in the panel.
2. When you click on the **Move to Device Group** button, the Move to Device Group window appears. See the illustration below:

Move to Device Group

Please select the device group that the devices should be moved to.

Device Group

HQ Building 101

MOVE

3. Using the **Device Group** field, click on the drop-down and select the device group into which you want to move the selected device(s).
4. Click on the **Move** button. You return to the Devices page, and the device(s) are now grouped within the specified device group.

Modifying a Device Group

To modify a device group, click on the **Edit button** () located above the device group table. The Modify Device Group window appears. See the following illustration:

Modify Device Group

Modify a device group's name or assigned policy.

Name
HQ Building 101

Policy
Policy 2

MODIFY

Use the **Name** field to edit the group name. Use the **Policy** field to assign a different security policy or no policy. If no policy is currently assigned to the device group, you can assign a policy to the device group.

Assigning a Policy to Devices

Users can assign a **security policy** to one or more ungrouped devices, or to all devices in a **device group**.

Note that when you assign a policy to a device, all toggled on settings in the policy (and their **remediation** capabilities, if any) are applied to the device beginning with the first **heartbeat sync**. This can affect the settings of other devices to which the policy is assigned or, if the device is in a device group, other devices in that group.

For example, if you assign a policy for which **Random Password Generation** is toggled on, Shield Guard will generate a random password and assign it to both the device and any other devices covered by that policy.

Single, Ungrouped Devices

Do the following:

1. In the Not Grouped device table, click on the associated **Assign Policy** button. The Assign Policy window appears.
2. Using the **Policy** field, click on the drop-down and select the policy you want to assign to the selected device. See the illustration below:

Assign Policy

Specify the policy you want to assign to the selected devices.

Policy

South Wing

ASSIGN

3. Click on the **Assign** button. You return to the Devices page, and the Policy Name column updates for the selected device.


Multiple Ungrouped Devices

Do the following:

1. In the Not Grouped device table, select the devices to which you want to apply the policy. The **Bulk Action** panel appears.
2. In the Bulk Action panel, click on **Assign Policy**. The Assign Policy window appears.
3. In the Assign Policy window, click on the **Policy** field drop-down and select the policy you want to assign to the selected devices.
4. Click on the **Assign** button. You return to the Devices page, and the Policy Name column updates for the selected devices.

Devices in a Device Group

Do the following:

1. Above the device group's table, click on the Edit icon (). The Modify Device Group window appears.
2. In the Modify Device Group window, click on the **Policy** field drop-down and select the policy you want to assign to the devices in the device group. See the following illustration:

Modify Device Group

Modify a device group's name or assigned policy.

Name
South Wing

Policy
Advanced Policy

MODIFY

3. Click on the **Modify** button. You return to the Devices page, and the Policy Name column updates for the selected devices.

Viewing and Maintaining Devices

The **Content area** of the Devices page contains one or more tables listing the devices in the **tenant**. The **Information bar** lists the total devices in the group and the number of those devices whose **security status** is Not Secure. The bar also contains the **Search** field you can use to filter the list of devices that appear in the device tables.

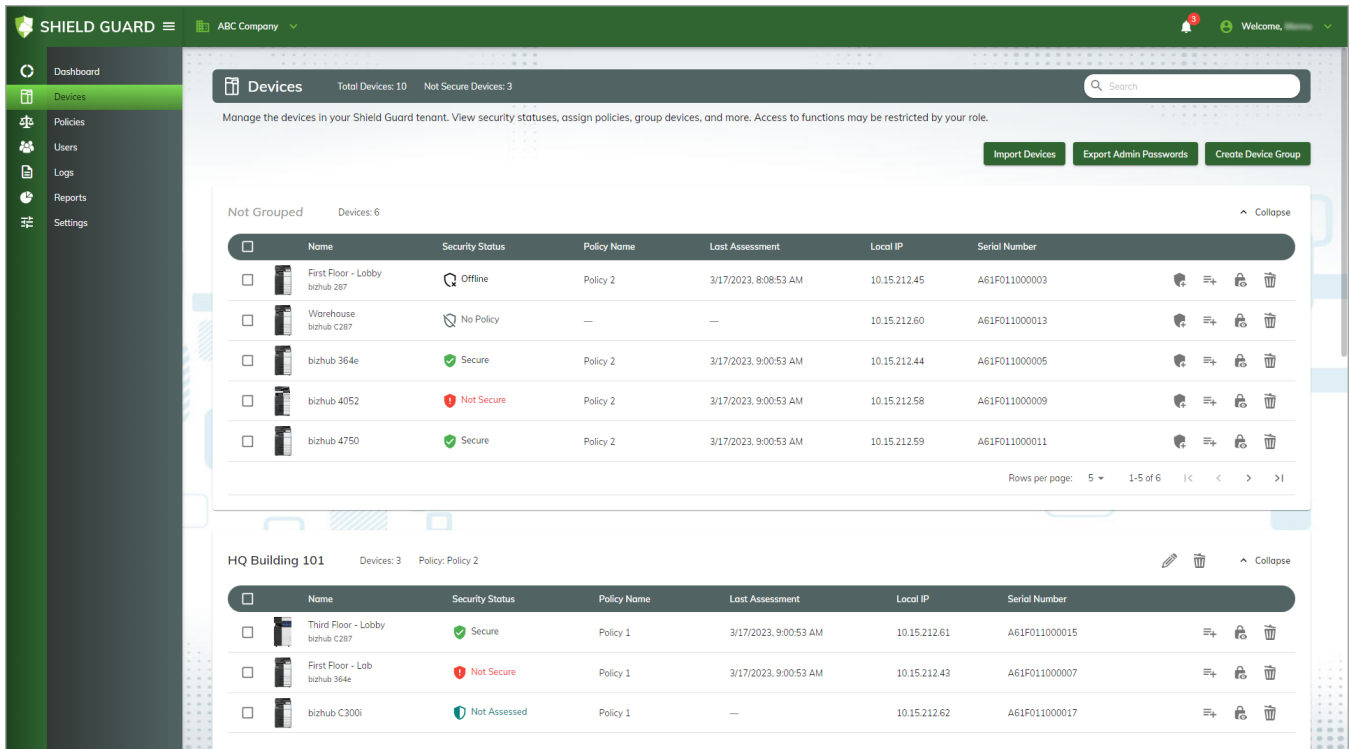
When you first create a tenant, all devices (if any) in the group appear in a single, unnamed table. Once you begin adding **device groups**, associated device tables are added to the page. All devices currently assigned to a device group appear in their associated table. All devices not currently assigned to a device group appear in the “Not Grouped” table located near the top of the page, above the device group tables. Note that the Not Grouped table appears only if one or more devices in the tenant are not currently assigned to a device group.

For each device table, information appears above the header bar, for example group name and device quantity. To collapse the table to make room on the page for other tables, click on the **Collapse** button. To expand a collapsed table, click on the **Expand** button.

The following illustration shows a portion of the Devices page. Note the following:

- The **Title bar** indicates the current tenant is the ABC Company.

- The Information bar indicates the tenant contains a total of ten devices, three of which are currently assessed as Not Secure.
 - Six of the devices belong to the Not Grouped table. Five are visible in the illustration. The sixth device could be viewed by viewing the next page in the table (by clicking on the right arrowhead on the table footer).
 - Three of the devices appear in the HQ Building 101 device group table.
 - One device does not appear due to space limitations in the illustration.



Device Information

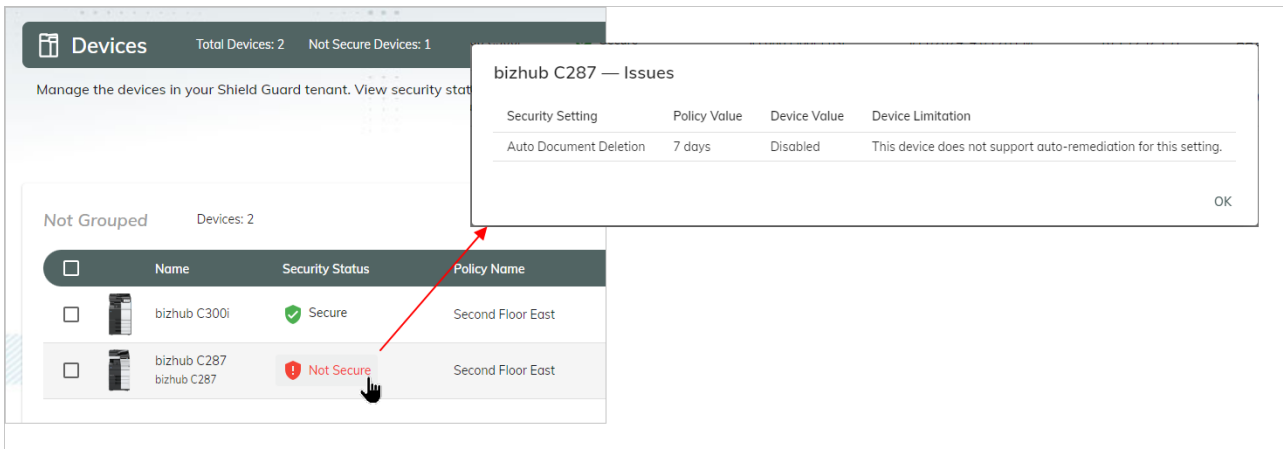
The device tables show the following columns of information for each device in the table:

- **Name** - The device name displays here. The default device name is the device model, but the default name can be user-defined via the MarketPlace site on the Devices page.
- **Security Status** - A device's security status updates each time Shield Guard performs a security assessment. For each device in the table, one of the following security statuses appears:
 - **No policy assigned** - The device has been added to the tenant, but no security policy is currently assigned to the device.
 - **Secure** - The device is compliant with the assigned **security policy**. All security settings are currently assessed as Secure.

- **Not Secure** - The device is not compliant with the assigned security policy. One or more security settings is currently assessed as Not Secure.
- **Not Assessed** - A policy has been assigned to the device but the device has not yet been assessed by Shield Guard. The device will be assessed the next time the Shield Guard Agent **communicates** with the Shield Guard Portal.
- **Offline** - The Shield Guard Agent's most recent attempt to communicate with the Shield Guard Portal was unsuccessful. Any of the following could prevent communication:
 - The device is powered off.
 - An issue with the agent.
 - An issue with output internet connectivity from the device.
 - Any other issue preventing the agent from establishing a connection.

Note: While a device may show an Offline status, the Shield Guard Agent continues to enforce the latest security settings defined in the assigned policy, including any security settings set to auto-remediation.

Note: For a Not Secure device, select the **Not Secure** icon to view a list of the issues causing the device to fail its policy assessment.



- **Policy Name** - The name of the assigned security policy (if any) displays. To apply a policy to the device or change the policy currently assigned to the device, click on the **Assign Policy** button.
- **Last Assessment** - A timestamp indicating the last time any of the following occurred for the device since the previous assessment:
 - The agent performed a self-check on the device, as determined by the **Check MFP local settings frequency** setting in the policy.
 - A security policy was assigned to the device.

- One or more settings in the device’s security policy were updated via the Shield Guard Portal.
- One or more settings on the device were updated, corresponding to toggled on policy settings on the device’s assigned policy. The agent ignores changes to any device settings for which the corresponding policy setting is toggled off.
- The device’s security status changed, for example from Secure to Not Secure because the Password Security Duration time period expired without a change to the device password.
- **Local IP** - The local IP address for the device displays.
- **Serial Number** - The device’s serial number displays.

Device Actions

For each device on the Devices page, action icons are available such as Assign Policy. You can apply actions to a device **individually**, to devices in **bulk**, or to a **device group**.

The following illustration shows the action icons available for not-grouped devices:

The screenshot shows a table titled "Not Grouped" with 6 devices. The table has columns for Name, Security Status, Policy Name, Last Assessment, Local IP, and Serial Number. To the right of each row, there are four action icons: a plus sign, a list icon, a lock icon, and a trash icon. These icons are circled in red in the original image. At the bottom right of the table, there is a "Rows per page" dropdown set to 5 and a "1-5 of 6" indicator.

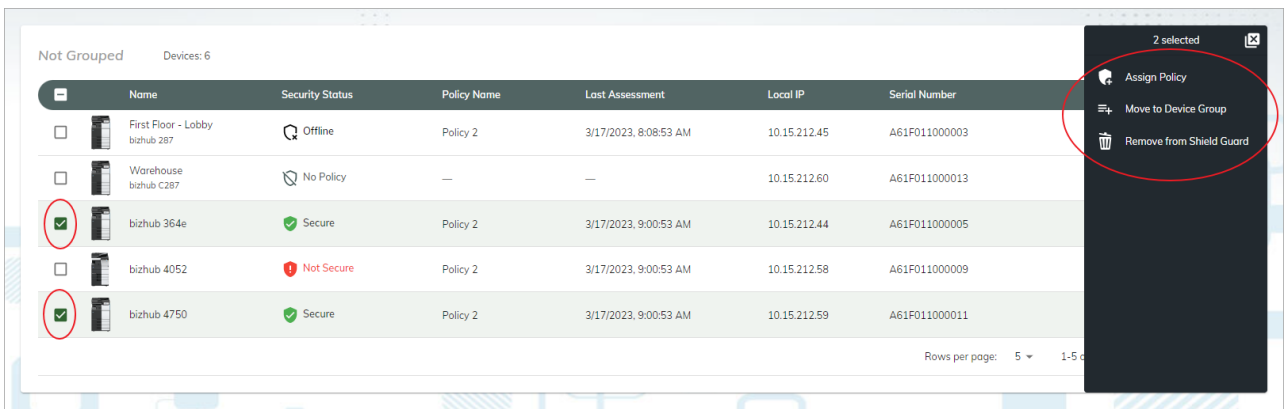
<input type="checkbox"/>	Name	Security Status	Policy Name	Last Assessment	Local IP	Serial Number	
<input type="checkbox"/>	First Floor - Lobby bizhub 287	Offline	Policy 2	3/17/2023, 8:08:53 AM	10.15.212.45	A61F011000003	
<input type="checkbox"/>	Warehouse bizhub C287	No Policy	—	—	10.15.212.60	A61F011000013	
<input type="checkbox"/>	bizhub 364e	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.44	A61F011000005	
<input type="checkbox"/>	bizhub 4052	Not Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.58	A61F011000009	
<input type="checkbox"/>	bizhub 4750	Secure	Policy 2	3/17/2023, 9:00:53 AM	10.15.212.59	A61F011000011	

Action Options

The following options are available for devices in a table:

- **Selection Boxes** - To select one or more items on which to perform an action, check the box for each item. To select all devices in the Devices table, check the box on the table header. To de-select a box, click on the box again.

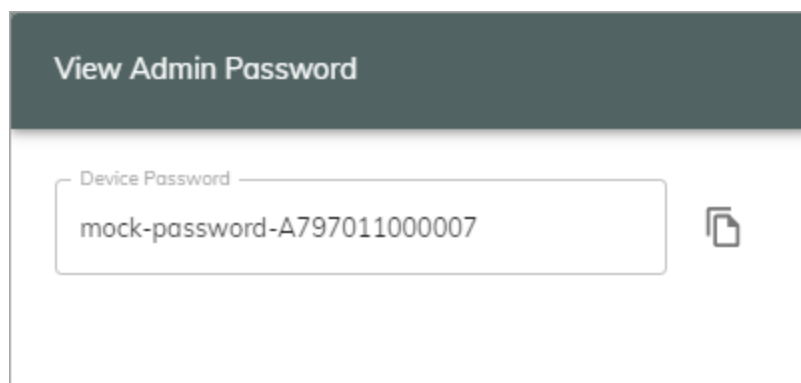
When you check a box, the **Bulk Actions panel** appears to the right of the table displaying the number of items currently selected and any actions that can be performed on multiple items simultaneously. To perform an action on all selected items, click on an action. If you click on the **X** in the Bulk Actions panel, no actions are performed, you return to the Devices table, and all items are de-selected. See the following illustration:



- **Assign Policy** - To assign a security policy to a device, click on this button. The **Assign Policy window** appears. Click on the drop-down menu and select a policy from the list that appears.
- **Move to Device Group** - To move the device to a device group, click on this button. The **Move to Device Group window** appears.
- **View Admin Password** - To view the admin password for the device, click on this button. The **View Admin Password Window** appears.
- **Remove from Shield Guard** - To remove the device from the tenant, click on this button. In the window that appears, click on Remove. The device is removed from the group and is now available for selection in the **Import Devices from MarketPlace** window where you can it add to a tenant. To return to the Devices page without removing the device, click on the **Cancel** button.
- **Edit** - Accesses the **Modify Device Group window**. Available only for device groups.

Viewing the Admin Password

To view the admin password for a device, click on the associated **View Admin Password button** in the Devices table. The View Admin Password window appears, displaying the admin password for the selected device. See the following illustration:



To copy the password to the clipboard, click on the **Copy** button next to the **Device Password** field.

Admin Password Unknown

If the View Admin Password button is inactive, you cannot view the password on this page. The “Admin password unknown” message appears when you hover the pointer over the button, indicating Shield Guard is out of sync with the device’s admin password.

For Shield Guard to access and display the admin password for a device, the following must be true:

- A security policy must be assigned to the device.
- The **Admin Password Configuration** setting must be toggled on for the policy.
- The admin password stored in the Shield Guard Agent must **match** the device’s admin password.

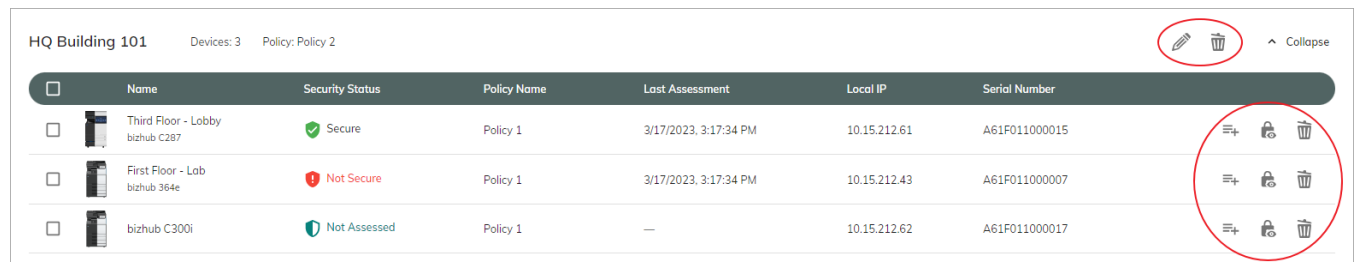
Note: Once the above is true for the device, the device admin password will be accessible after the next heartbeat sync occurs and you refresh the page.

Applying an Action to an Individual Device



















To apply an action to an individual device, click on the action icon in the associated row. You can also check the selection box on the left side of the table and select an action from the **Bulk Actions panel**. Once you select an action, a pop-up window will appear in which you can perform the action.

Applying an Action to a Device Group

For devices in a device group, a slightly different set of options is available than for un-grouped devices. Like un-grouped devices, each device in the group has a set of action options. However, additional action options are available above the table header. These are device group actions. The following illustration shows the action icons available for the device group “HQ Building 101”:



The screenshot shows a table for the device group "HQ Building 101" with 3 devices. Above the table header, there are icons for edit and delete, and a "Collapse" button. The table has columns for Name, Security Status, Policy Name, Last Assessment, Local IP, and Serial Number. Each row has a selection checkbox on the left and a set of action icons (edit, lock, delete) on the right. Red circles highlight the edit and delete icons above the table header and the action icons for each device row.

HQ Building 101		Devices: 3	Policy: Policy 2				  
<input type="checkbox"/>	Name	Security Status	Policy Name	Last Assessment	Local IP	Serial Number	
<input type="checkbox"/>	 Third Floor - Lobby bizhub C287	 Secure	Policy 1	3/17/2023, 3:17:34 PM	10.15.212.61	A61F011000015	  
<input type="checkbox"/>	 First Floor - Lab bizhub 364e	 Not Secure	Policy 1	3/17/2023, 3:17:34 PM	10.15.212.43	A61F011000007	  
<input type="checkbox"/>	 bizhub C300i	 Not Assessed	Policy 1	—	10.15.212.62	A61F011000017	  

Device group actions apply an action to all devices in the device group. The following actions are available:

-  **Edit** - Accesses the **Modify Device Group window**.

-  **Delete** - Deletes the device group.

Exporting Device Admin Passwords

To export the current tenant's device admin passwords to a CSV file, use the **Export Admin Passwords** button. For example, you can use the CSV file for archival purposes or for use outside of Shield Guard.

If Shield Guard can find admin passwords for one or more devices in the tenant, this button is active. If you click on it, a CSV file downloads immediately to your local drive. If no device admin passwords are found, the button is inactive.

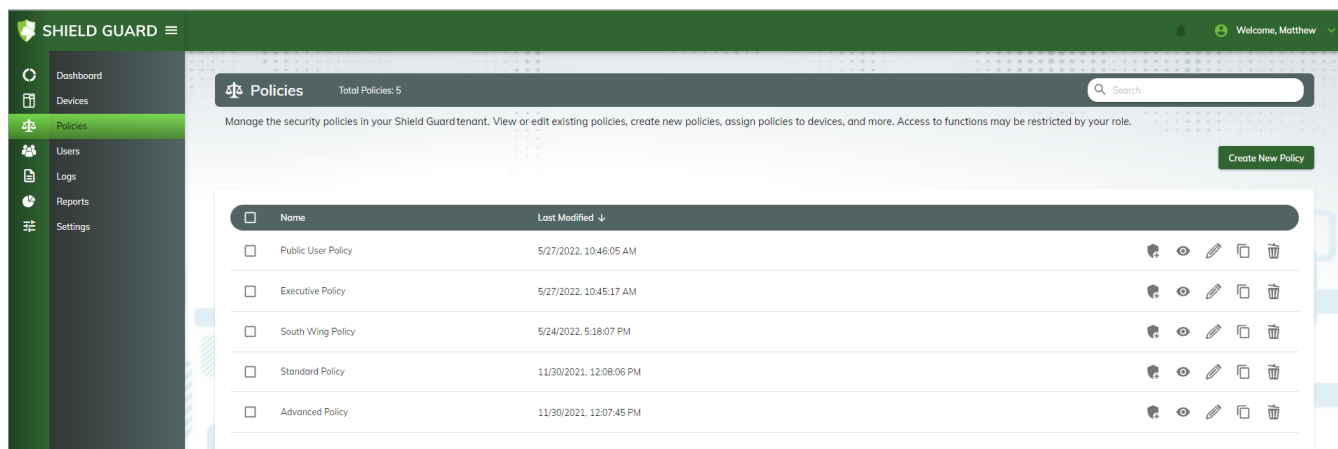
The exported file contains the following information for each device in the tenant:

- Device name
- Device serial number
- Device admin password (if known by Shield Guard)

Managing Policies

Managing Security Policies

To create and maintain Shield Guard security policies for your **tenant**, click on **Policies** in the Navigation pane. The Policies page appears in the following illustration, showing three **custom policies** and the two **sample security policies**:



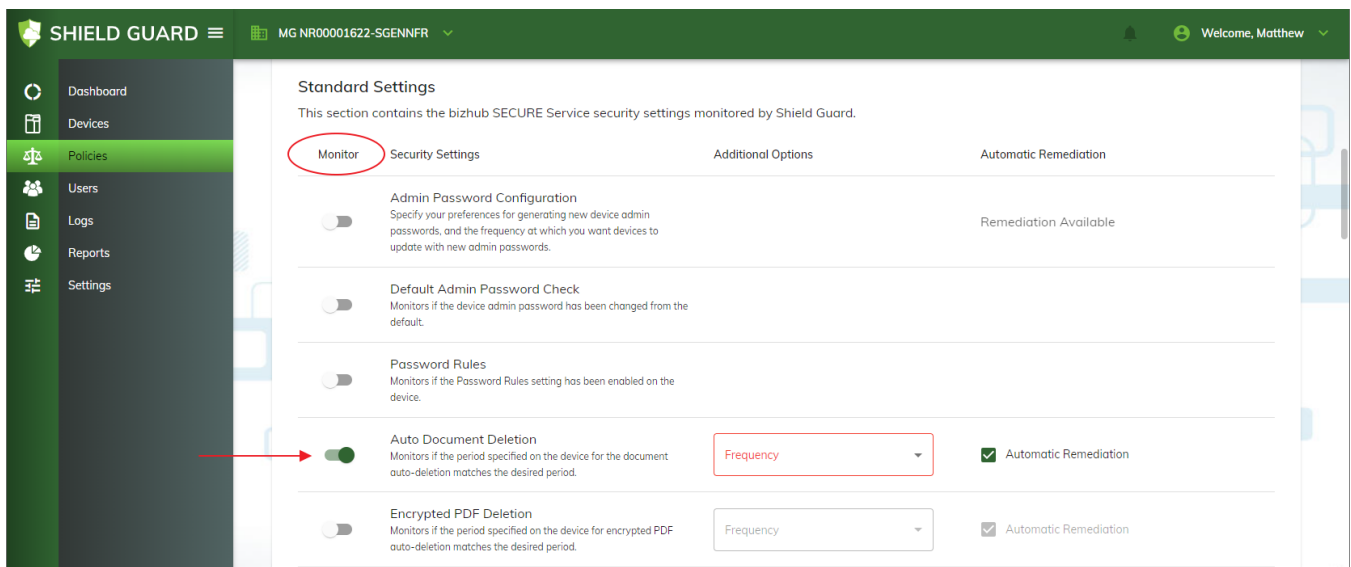
The Policies page provides access to the security policies in your tenant. Each individual policy is capable of monitoring security settings for **supported Konica Minolta MFPs (multi-function peripheral devices) and SFPs (single-function peripheral devices)**, and each policy is fully customizable. In addition, most policy settings include an **Automatic Remediation** option to automatically bring the device's corresponding setting into compliance with the policy setting.

Note: Shield Guard supports all bizhub **Standard** and **Platinum** device security settings, as well as select **Ultimate** settings.

About Security Policies

Shield Guard security policies enable you to remotely monitor and maintain the security settings for any device in a Shield Guard tenant. You access the tenant and its security policies via the Shield Guard Portal. Each tenant can contain an unlimited number of security policies and devices.

Each Shield Guard security policy contains the same list of settings - settings that correspond to the security switches available in Konica Minolta devices. You customize your policies via the Monitor column in the Security settings tables. You toggle on the policy settings you want Shield Guard to monitor, and toggle off the policy settings you want Shield Guard to ignore. In the following illustration, the Auto Document Deletion setting has been toggled on, and is awaiting the user to specify the frequency at which to delete documents.



For each policy setting you toggle on, Shield Guard compares the setting with the device's corresponding setting. If the policy setting matches the device's setting, Shield Guard assesses that setting as compliant. If Shield Guard assesses all device security settings as compliant with the policy, the device receives a **security status** of Secure.

If Shield Guard assesses one or more device settings as not compliant with the policy, the device receives a status of Not Secure. The **Dashboard** and **Devices** pages display a Not Secure status for the device, and the **Logs** page lists the individual settings assessed as Not Secure.

Once you **assign a security policy** to a **device** (or **device group**), Shield Guard can begin remote monitoring of the device(s). Once assigned, the policy runs continuously, communicating with the **Shield Guard agent** at **user-defined intervals**. The agent queries the portal for the current policy settings, then compares the device's settings with the policy's corresponding settings. If any issues are found, the portal updates with the information so you can take corrective action.

Notes:

- For the Shield Guard agent to communicate with the Shield Guard Portal (and the portal to communicate back to the agent), the agent must be running. The agent launches automatically when the **Shield Guard screensaver** is active on a device.
- Any changes you make to settings in a security policy are applied at the first **server heartbeat sync** that occurs after the Shield Guard screensaver launches.
- To help you get started, Shield Guard includes two **sample security policies**. You can use these policies in any way that meets your needs.

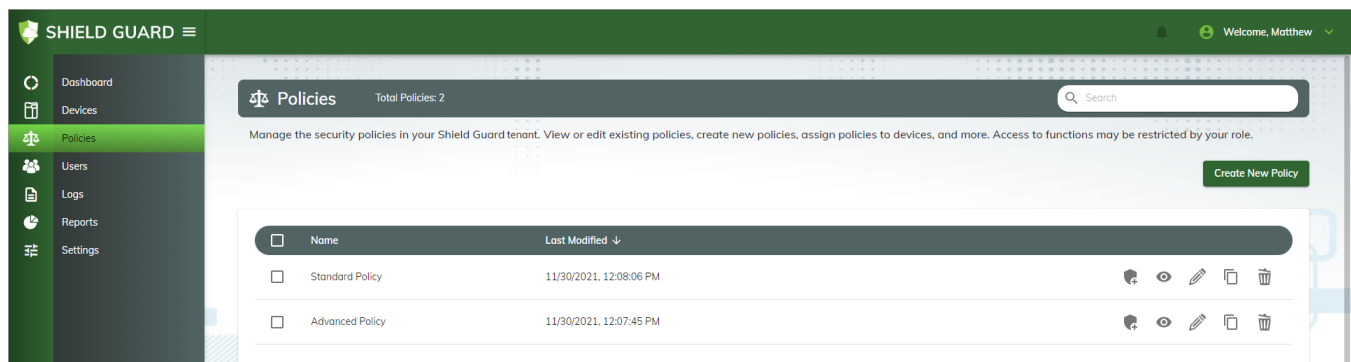
Device Restrictions

Shield Guard supports all **bizhub devices supported by MarketPlace**. However, the functionality of some Shield Guard policy settings is restricted to newer devices. Note the following:

- **Platinum settings** are supported only on i-Series devices, with the exception of User Authentication and Public Authentication, which are supported on all MarketPlace devices.
- **Ultimate settings** are supported only on i-Series devices on which the LK-116 Virus Scan i-Option has been installed.
- **Automatic Remediation** is supported only on i-Series devices, with the exception of Admin Password Configuration, for which automatic remediation is supported on all MarketPlace devices.
- Due to device limitations, devices using microSD cards do not support all Shield Guard policy settings.

Sample Security Policies

Shield Guard includes two sample security policies, the Standard Policy and the Advanced Policy. You can use these policies in any way that meets your needs. The following illustration shows the Policies page listing the sample policies:



For the sample security policies, all **security settings** are included, and you have the following options:

- **View** a policy's current configuration.

- **Assign** the policy to one or more devices as-is, without modifications.
- **Modify** the security settings and assign the policy to one or more devices.
- Rename the policy and assign it to devices under the new name, with or without modifications to security settings.

Notes:

- You can also **create a new policy** from scratch.
- The **Overview** topic includes a description of a **sample custom policy**.

Policies Table

The Policies table lists all policies in the tenant. See the following illustration:

<input type="checkbox"/>	Name	Last Modified ↓				
<input type="checkbox"/>	Public User Policy	5/27/2022, 10:46:05 AM				
<input type="checkbox"/>	Executive Policy	5/27/2022, 10:45:17 AM				
<input type="checkbox"/>	South Wing Policy	5/24/2022, 5:18:07 PM				
<input type="checkbox"/>	Standard Policy	11/30/2021, 12:08:06 PM				
<input type="checkbox"/>	Advanced Policy	11/30/2021, 12:07:45 PM				

The **Information bar** at the top of the Policies page contains the following information, fields, and buttons:

- **Page Icon** - The icon representing the current page.
- **Page Name** - The name of the current page.
- **Total Policies** - A running list of the total number of security policies in the current tenant.
- **Search** - A search filter you can use to restrict the policies displayed in the Policies table to a string you specify.
- **Create New Policy** - This button provides access to the **Create a New Policy page**.






The Policies table provides information on, and **action options** for, each device, including the following:

- **Name** - The name of the policy.
- **Last Modified** - The date and time at which the policy was last modified.

- **Rows per page** - This option appears at the bottom of the Policies table display. Use it to specify the number of policy rows to display per page. For example, if your tenant contains many policies, you can specify a large number of policies per page, such as 25. The more policies per page, the less likely you will have to navigate to another page of policies.
- **Previous/Next buttons** - If your tenant contains more policies than the number of rows specified at the **Rows per page** field, these buttons (next to the **Rows per page** field) activate. Use them to navigate to other pages of the policies table.

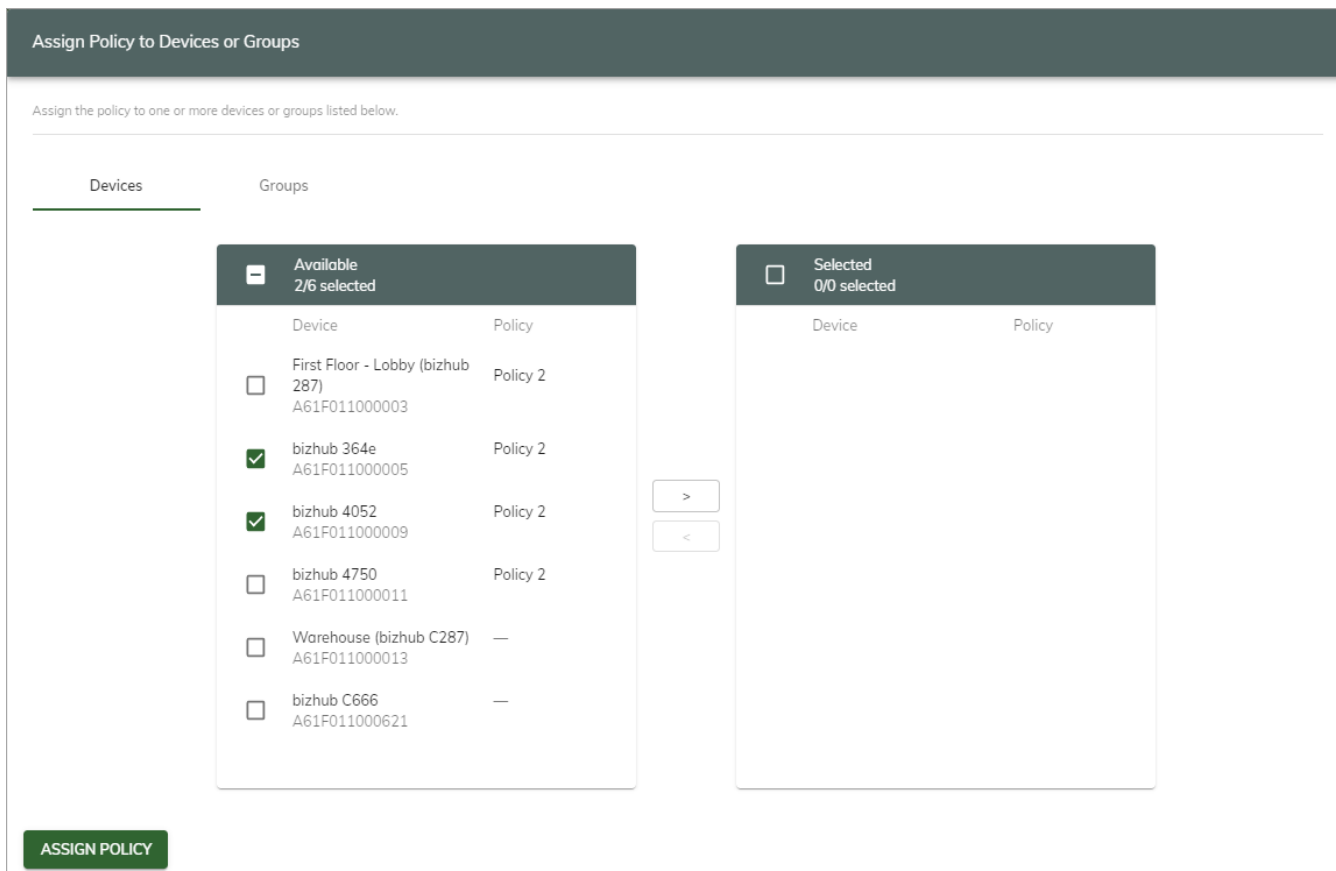
Action Options in the Policies Table

In addition to information on each policy, the Policies table provides access to action options you can use to modify a policy and/or apply it to a **device**. Click on the associated button to access the action. The following table lists the action options available for each policy.

Action Icon	Function
	Assign Policy - Accesses the Assign Policy to Devices window.
	Show Policy - Accesses the View Policy page.
	Edit Policy - Accesses the Edit Policy page.
	Clone Policy - Creates a copy of the policy and displays it in the Edit Policy page where you can give the policy a unique name and modify it to suit your needs.
	Delete Policy - Deletes the policy.

Assigning a Policy to Devices or Device Groups

To assign a security policy to devices or device groups, click on the **Assign Policy** button for a policy in the Policies table. The Assign Policy to Devices or Groups window appears. The following illustration shows the window when the Devices tab is selected:



In the Available panel, all devices from your MarketPlace account appear, restricted to devices that have not yet been assigned to a group (whether by you or another user). Do the following:

1. In the Available panel, click on the selection box next to each device to which you want to assign the security policy. To select all available devices, click on the box in the panel header.
2. Once you select a box, the > button between the panels activates. When you have selected all the devices you are interested in, click on the > button. The devices appear in the Selected panel.
3. To remove one or devices from the Selected panel, click on their associated boxes and then click on the < button. The devices return to the Available panel.

Note: To exit the Assign Policy to Devices or Groups window without selecting any devices, click outside the window at any time.

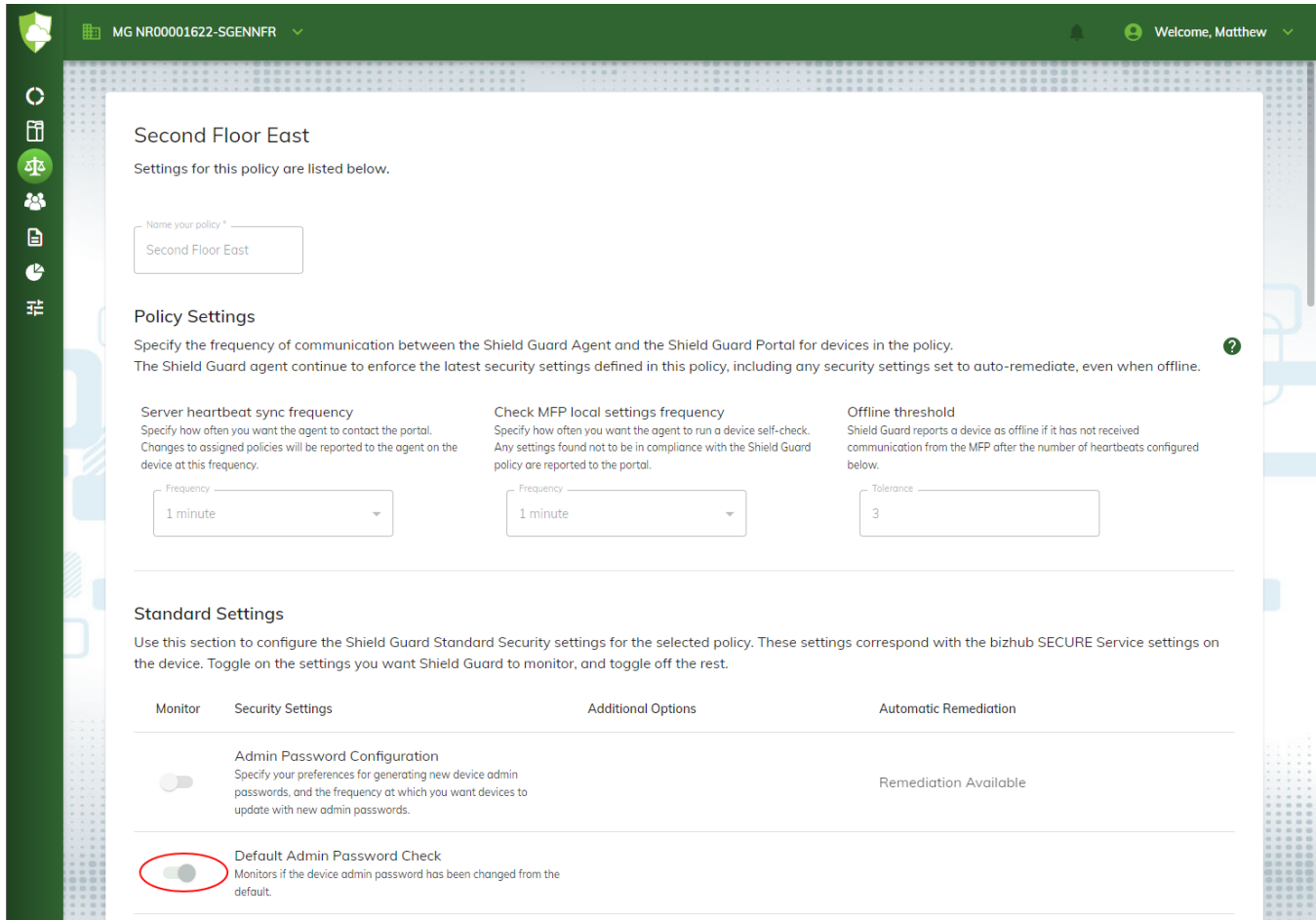
4. When the Selected panel contains all the devices you are interested in, click on the **ASSIGN POLICY** button. You return to the Policies page. If you now access the Devices page, you can see the policy you assigned is now listed in the Policy Name column for each device you selected for policy assignment.

To assign the policy to all devices in a device group, click on the Groups tab and use the same procedure as described for the Devices tab.

Note: You can also assign a policy to the devices in a group using the **Modify Device Group** window on the Devices page.

Viewing Security Policies

The View Policy page appears when you click on the **Show** button for a policy in the Policies table. It displays a read-only version of the selected policy. The following illustration shows the top portion of a security policy called “Second Floor East”, in which the Default Admin Password Check setting has been toggled on.



Creating Policies

To create a new, custom security policy, access the Policies page, where you have the following options when creating a policy:

- Create a new policy from scratch - Click on the **Create New Policy** button to access the Create a New Policy page.
- Rename an existing policy - On the Policies page, click on the **Edit** button associated with the policy you want to rename. The **Edit Policy page** appears where you can rename and otherwise modify the policy to suit your preferences. For example, you can modify and rename one of the **sample policies**.

Notes:

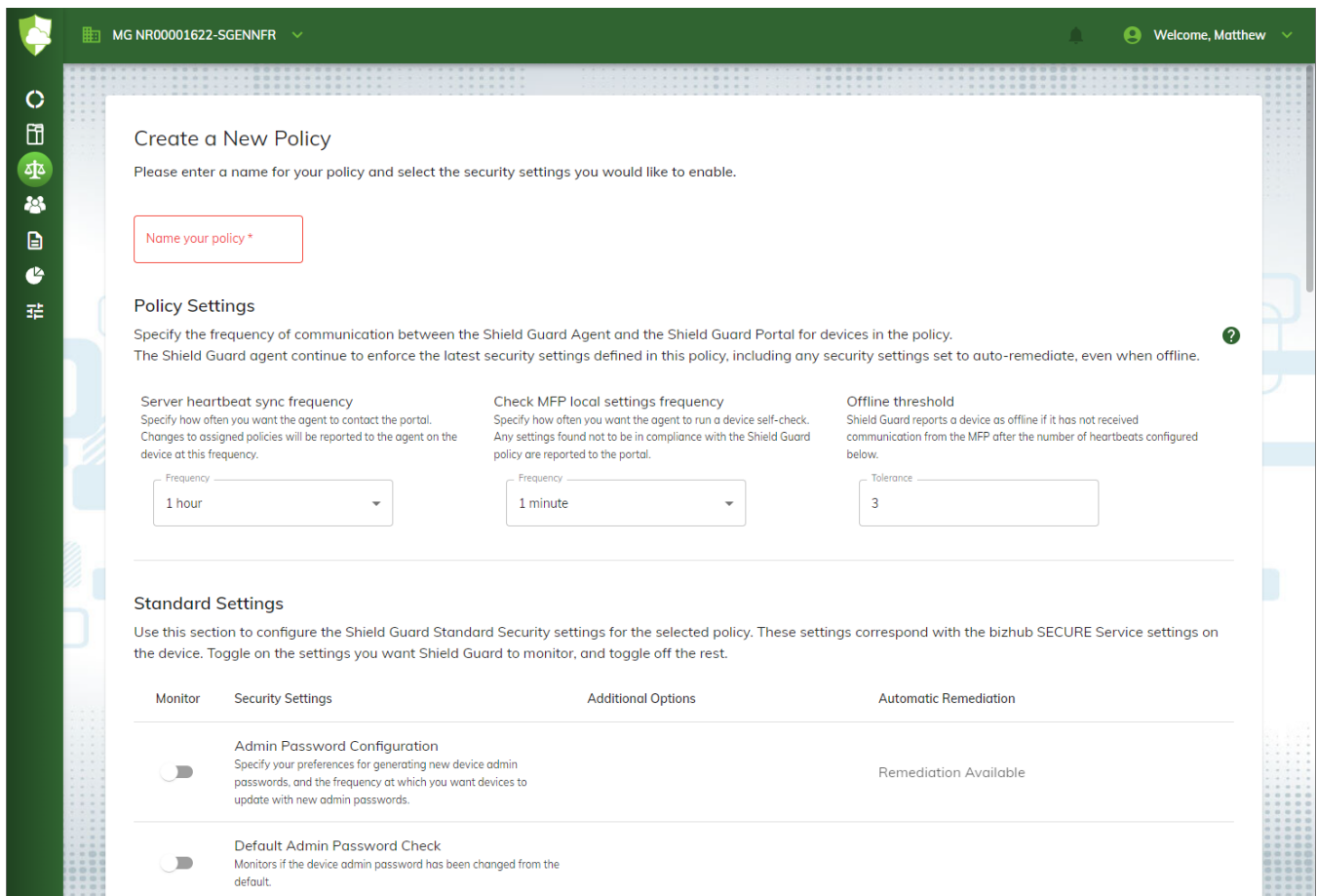
- Not all devices support all Shield Guard security settings. For example, some older devices do not support some **bizhub Platinum Security settings**. If you toggle on a setting in Shield Guard that is not supported on a device, Shield Guard will assess the setting as Not Secure, causing the device to fail its security assessment. If you toggle off the setting, Shield Guard will ignore the setting during assessments.
- For devices that do not support **automatic remediation**, activating automatic remediation on a setting has no effect.
- The **Overview** topic includes a description of a **sample custom policy**.

Creating a New Policy

The Create a New Policy page accesses the policy template, which you use to create a new policy. The template includes Shield Guard policy settings corresponding with each of the security settings available in **supported Konica Minolta MFPs (multi-functional peripheral devices) and SFPs (single-function peripheral devices)**. Each Shield Guard security setting can be toggled on or off.

Some settings include an **Additional Options** field. If you toggle on such a setting, the **Additional Options** field becomes a **required field**.

To create a new policy from scratch, access the Policies page and click on the **Create New Policy** button. The Create a New Policy page appears:



In the policy template, all settings are toggled off by default. The Create a New Policy page consists of the following sections:

- **Policy Settings**
- **Standard Security Settings**
- **Platinum Security Settings**
- **Ultimate Security Settings**

To create a new security policy, take the following steps:

Step 1 - Name your policy

Use the **Name your policy** field to specify a meaningful name for the policy. This is a **required field**.

Step 2 - Specify Policy Settings

Use this section to specify the frequency of communications between the Shield Guard Agent and the Shield Guard Portal for devices to which the current security policy is assigned. Specify the following:

- **Server heartbeat sync frequency** - Specify the frequency by which you want the agent to communicate with the Shield Guard Portal to retrieve the latest changes (if any) to the security policy. The agent stores the latest settings until the next heartbeat sync.

Note: Once you apply this setting to a policy, if you later modify the setting, changes are applied at the completion of the previously scheduled sync. For example, if the current setting is 7 days and you change it to 15 minutes, the change will be applied at the next sync (7 days after the previous sync). Thereafter, syncs will occur every 15 minutes, until you change the setting again.

- **Check MFP local settings frequency** - Specify the frequency by which you want the agent to run a “device check”. A device check records the current status of each of the device’s security settings for which the corresponding policy setting is toggled on (and ignores the toggled-off settings). If any of the following occurred since the last device check, the agent notifies the portal:
 - One or more settings on the device were modified.
 - One or more device settings do not match their corresponding policy setting.

If the agent reports any issues to the portal, the portal runs an assessment of the policy to determine if any device settings are not compliant with the policy.

- **Offline threshold** - Specify the number of server heartbeats you want to elapse without a communication from the agent before Shield Guard reports a device in the policy as Offline. For example, if you set the heartbeat sync frequency to 5 minutes and the offline threshold tolerance to 3, then if the agent on a device has not pinged the portal in the last 15 minutes, the portal assumes the device is offline and assigns that **status** to the device.

Notes:

- The Shield Guard Agent communicates with the portal only when the **Shield screensaver** is active on the device. That is, once the screensaver activates on a device, the agent then communicates based on your settings here until the screensaver deactivates. For example, if you set the Check MFP local settings frequency to 5 minutes, then after 5 minutes expires, the policy will run a check on each device as soon as the screensaver runs on the device. If the screensaver is running as the 5 minutes expires, the device check begins immediately.
- The **Overview** topic includes a description of a **sample custom policy** with a typical communication frequency configuration between portal and device.

Step 3 - Specify Security Settings to Monitor

Shield Guard policies assess only settings for which monitoring is toggled on in Shield Guard. To toggle on the settings you want Shield Guard to monitor, use the Monitor column on the Policies page. Toggle off the settings you want Shield Guard to ignore.

Note: Some devices may not include all settings supported by Shield Guard, and/or not provide an API that Shield Guard can use to access and assess the setting. Thus, you may configure a policy to monitor a setting that Shield Guard cannot. When Shield Guard attempts to assess such a setting, a log is generated.

Shield Guard Assessments

If a Shield Guard security setting contains additional configuration options, then Shield Guard assesses each option to determine compliance with the policy. For example, the Auto Document Deletion setting, when toggled on, includes a requirement to specify a frequency at which to delete the documents (one hour, one day, etc.). For Shield Guard to assess this setting as Secure, the frequency specified on the device must match the frequency specified in the Shield Guard policy.

However, if a monitored Shield Guard setting contains no additional options (for example, the Password Rules setting), then Shield Guard assesses only whether or not the setting is enabled on the device. If the setting is enabled on the device, Shield Guard assesses it as Secure, and Not Secure otherwise.

Security Settings Tables

The following sections include the Security Settings tables (**Standard**, **Platinum**, and **Ultimate**). Each table includes the following columns of information:

- Shield Guard Setting - The name of the Shield Guard setting.
- Functionality at the Device - The functionality of the device setting (when enabled) that corresponds to the Shield Guard setting.
- Shield Guard Assessment - Shield Guard's assessment of the setting. Monitoring for the setting must be toggled on for Shield Guard to assess the device setting.
- Automatic Remediation - Indicates if Shield Guard supports **automatic remediation** for the setting. If both the Shield Guard setting and the device setting support automatic remediation, then Shield Guard can remediate it.

Standard Security Settings

Use this section to configure the Shield Guard Standard Security settings for the current policy. The Standard Security settings correspond with the bizhub SECURE Service settings supported by the device. Toggle on all settings you want the policy to monitor. Be sure to configure the additional options (if any) for the settings you toggle on. Toggle off all other settings.

The following **table** lists the Standard Security settings as well as descriptions of the device's corresponding bizhub SECURE Standard Security settings and how Shield Guard assesses those settings.

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
Admin Password Configuration	Devices have no corresponding setting. Instead, Shield Guard can update the device's admin password based on user-defined settings in Shield Guard.	Monitors the admin password on the device. If due for an update, Shield Guard assesses the setting as Not Secure, generates a new password, sends it to the device, and assesses the setting as Secure after the next device assessment.	Y
Default Admin Password Check	Devices have no corresponding setting. Instead, each device's Admin Password setting is initially set to a default. Admins can use this field to specify their own password for the device.	<p>Monitors the admin password on the device. If the password has been changed from the device's default, Shield Guard assesses the setting as Secure.</p> <p>Note: The Default Admin Password Remediation setting requires this setting (Default Admin Password Check) to be toggled on in order to remediate admin passwords. Thus, if you attempt to toggle off this setting while the Default Admin Password Remediation setting is toggled on, a warning message appears with two options. If you click on OK, both settings are toggled off. If you click on Cancel, both settings remain toggled on. No warning message appears if the Default Admin Password Remediation setting is not currently toggled on, or if you are attempting to toggle on this setting (Default Admin Password Check).</p>	N

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
Password Rules	Imposes character requirements on device admin passwords, whether generated by Shield Guard or specified manually at the device. An example of a character requirement is a minimum password length.	Monitors the Password Rules setting on the device. If enabled, Shield Guard assesses the setting as Secure.	N
Auto Document Deletion	Deletes stored data after a user-defined period expires, including data stored in personal or public user boxes, and system boxes. Not supported on MicroSD storage devices.	Monitors the Document Delete Time setting on the device. If the time period specified at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
Encrypted PDF Deletion	Deletes stored, encrypted PDFs after a user-defined period expires. Not supported on MicroSD storage devices.	Monitors the Encrypted PDF Delete Time setting on the device. If the time period specified at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
ID + Print Deletion	Deletes stored, secure print data in the ID & Print user box after a user-defined period expires. Not supported on MicroSD storage devices.	Monitors the ID & Print Delete Time setting on the device. If the time period specified at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
Secure Document Deletion	Deletes documents stored in the Secure Print user box after a user-defined period expires. Not supported on MicroSD storage devices.	Monitors the Delete Secure Print File setting at the device. If the frequency interval specified at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
Temporary Data Overwrite	Overwrites stored temporary data after it expires, in addition to deleting it, providing added security. Not supported on i-Series devices.	Monitors the Overwrite HDD Data setting at the device. If enabled, Shield Guard assesses the setting as Secure.	N
Storage Encryption	Encrypts the MFP's storage device.	Monitors the device's storage device (hard drive (HDD), solid-state drive (SSD), or MicroSD). If encryption has been enabled on the device, Shield Guard assesses the setting as Secure.	N

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
Storage Lock Password	Imposes a password requirement to access the device's storage device.	Monitors the storage device password requirement setting on the device. If enabled, Shield Guard assesses the setting as Secure. Hard drive (HDD) or solid-state drive (SSD) only. MicroSD not supported.	N

Platinum Security Settings

Use this section to configure the Shield Guard Platinum Security settings for a selected policy. These settings correspond with the bizhub SECURE Platinum settings on the device. Toggle on the settings you want Shield Guard to monitor, and toggle off the rest. Be sure to configure the additional options (if any) for the settings you toggle on.

Note: Platinum Security settings are **supported only on i-Series devices**, with the exception of User Authentication and Public Authentication, which are available for use on **all devices supported by Shield Guard**.

The following **table** lists the Platinum Security settings as well as descriptions of the device's corresponding bizhub SECURE Platinum Security settings and how Shield Guard assesses those settings.

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
User Authentication	Activates the user authentication requirement at the device.	Monitors the User Authentication setting on the device. If enabled, Shield Guard assesses the setting as Secure. This Platinum Security setting is available for use on all devices supported by Shield Guard. Note: If you attempt to toggle off monitoring of this setting while the Public Authentication setting is toggled on, a warning message appears indicating the Public Authentication setting will be toggled off as well. That is, to monitor the Public Authentication setting, you must also monitor this setting.	N

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
<p>Public Authentication</p>	<p>Applies a user-defined mode of restriction on public user's access to the device. Configuration options are listed below:</p> <p>Restricted - Restricts public users from logging in to the device. To log in, users must have a personal account.</p> <p>On with login - Activates the Public User shared account, and requires public users to log in with the public user password.</p> <p>On without login - Activates the Public User shared account, and allows public users to log in without the public user password.</p>	<p>Monitors the Public Authentication setting at the device. If the mode specified at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure. This Platinum Security setting is available for use on all devices supported by Shield Guard.</p> <p>Note: If you attempt to toggle on monitoring of this setting while the user Authentication setting is toggled off, a warning message appears indicating the User Authentication setting will be toggled on as well. That is, to monitor this setting, you must also monitor the User Authentication setting.</p>	<p>N</p>
<p>Mode Using SSL/TLS</p>	<p>Enables a user-defined SSL/TLS login mode on the device.</p>	<p>Monitors the Mode Using SSL/TLS setting on the device. If the SSL/TLS mode on the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.</p>	<p>Y</p>

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
SSL/TLS Version Setting	Enables a user-defined range of SSL/TLS versions to be available for use on the device.	Monitors the SSL/TLS Version setting on the device. If the range of SSL/TLS versions specified on the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
Admin Mode Logout Time	Applies an automatic admin-mode logout time for the device. When the device is in Admin mode, if no device activity occurs for the specified period, the device logs out. Not accessible at the device. Must be accessed via the Web Connection app.	Monitors the automatic admin-mode logout setting on the device. If the time period specified at the device for automatic admin-mode logout matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
User Mode Logout Time	Applies an automatic user-mode logout time for the device. When the device is in User (Public) mode, if no device activity occurs for the specified period, the device logs out. Not accessible at the device. Must be accessed via the Web Connection app.	Monitors the automatic user-mode logout setting on the device. If the time period specified at the device for automatic user-mode logout matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
FTP Server	Activates the FTP Server function on the device. Not supported on MicroSD storage devices.	Monitors the FTP Server setting on the device. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
FTP TX	Activates the FTP Transmission function on the device. Not supported on MicroSD storage devices.	Monitors the FTP TX setting on the device. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
Job Log	Transmits audit logs to a specified WebDAV server. MicroSD storage devices support only the Auto (syslog) transmission method.	Monitors the Job Log setting on the device. When you enable this setting, additional options appear. You must select at least one log type to obtain, and specify a transmission method for the logs. If you select the Manual (XML) method, you must also specify your preference for overwriting the log file in the event the log storage area reaches capacity. If you select Restrict , a warning message appears indicating that once log storage reaches capacity, the device will prevent users from running additional jobs until the log storage area is cleared. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
Service Location Protocol	Activates Service Location Protocol (SLP) on the device.	Monitors the SLP setting on the device. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
MFP Shared Folder Deletion	Deletes documents stored in the device's Shared folder after a user-defined period expires. Not supported on MicroSD storage devices.	Monitors the "MFP Shared Folder Deletion" setting at the device. If the frequency interval specified at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
SNMP v1/v2c	Activates SNMP (Simple Network Management Protocol) v1/v2c on the device.	Monitors the SNMP v1/v2c setting on the device. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
SNMP v3	Activates SNMP (Simple Network Management Protocol) v3 on the device.	Monitors the SNMP v3 settings on the device. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y

SNMP v3 Settings

Shield Guard can monitor, and **auto-remediate**, SNMP v3 settings on supported devices. The Simple Network Management Protocol (SNMP) is designed to enable remote configuration and monitoring of device settings across a local network. Version 3 of SNMP includes improvements to the prior protocols (v1/v2c), providing additional security to prevent unauthorized access and manipulation of the settings within a device.

Note the following:

- Shield Guard support for SNMP v3 is limited to Konica Minolta i-Series devices.
- At this time, Shield Guard does not support **password management** for SNMP v3. Password management for SNMP v3, for example, changing a password, must be done at the device.
- For information on SNMP v3 or how your devices interact with the protocol, refer to the product's documentation.

The following illustration shows Shield Guard's default SNMP v3 settings:

SNMP v3
 Checks the SNMP v3 setting on the device to see if it matches the setting here. ✔ Automatic Remediation


<p>Status Monitors and reports the status of Simple Network Management Protocol (SNMP) v3 on the device.</p>	<p>Status <input type="text" value="Enabled"/></p>	✔ Automatic Remediation
<p>Port Number Checks the UDP Port setting on the device to see if it matches the setting here. The default port for SNMP is 161, but you can edit this field.</p>	<p>Port Number <input type="text" value="161"/></p>	✔ Automatic Remediation
<p>Context Name Checks the Context Name setting on the device to see if it matches the setting here.</p>	<p><input style="border: 1px solid red;" type="text" value="Context Name"/></p>	✔ Automatic Remediation
<p>Discovery User Permissions Checks the Discovery User Permissions setting on the device to see if it matches the setting here.</p>	<p>Status <input type="text" value="Enabled"/></p>	✔ Automatic Remediation
<p>Discovery User Name Checks the Discovery User Name setting on the device to see if it matches the setting here.</p>	<p>Discovery User Name <input type="text" value="public"/></p>	
<p>Read User Name Checks the Read User Name setting on the device to see if it matches the setting here.</p>	<p>Read User Name <input type="text" value="initial"/> </p>	✔ Automatic Remediation
<p>Read Security Level Checks the Read Security Level setting on the device to see if it matches the setting here.</p>	<p>Read Security Level <input type="text" value="Authentication OFF"/></p>	✔ Automatic Remediation
<p>Write User Name Checks the Write User Name setting on the device to see if it matches the setting here.</p>	<p>Write User Name <input type="text" value="restrict"/> </p>	✔ Automatic Remediation
<p>Write Security Level Checks the Write Security Level setting on the device to see if it matches the setting here.</p>	<p>Write Security Level <input type="text" value="Authentication OFF"/></p>	✔ Automatic Remediation
<p>Encryption Algorithm Checks the Encryption Algorithm setting on the device to see if it matches the setting here.</p>	<p>Encryption Algorithm <input type="text" value="AES-128"/></p>	✔ Automatic Remediation
<p>Authentication Method Checks the Authentication Method setting on the device to see if it matches the setting here.</p>	<p>Authentication Method <input type="text" value="SHA-1"/></p>	✔ Automatic Remediation

The following lists Shield Guard’s SNMP v3 settings and describes how Shield Guard assesses a device’s corresponding settings. For all Shield Guard settings, if the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.

- Status - Monitors and reports the status of the SNMP v3.
- Port Number - Monitors the UDP Port setting on the device. The default port for SNMP is 161, but you can edit this field. Note that SNMP v1/v2c also uses the SNMP port.
- Context Name - Monitors the Context Name setting on the device. Accepts up to 63 characters.
- Discovery User Permissions - Enables the Discovery User Name setting.
 - Discovery User Name - Monitors the Discovery User Name setting on the device. Accepts 1 to 32 characters.

- Read User Name - Monitors the Read User Name setting on the device. Accepts up to 32 characters.
 - Read Security Level - Monitors the Read Security Level setting on the device.
- Write User Name - Monitors the Write User Name setting on the device. Accepts up to 32 characters.
 - Write Security Level - Monitors the Write Security Level setting on the device.
- Encryption Algorithm - Monitors the Encryption Algorithm setting on the device.
- Authentication Method - Monitors the Authentication Method setting on the device.

Notes:

- All Shield Guard SNMP v3 settings support **automatic remediation**. However, the SNMP Settings feature must be enabled on the device. Due to device limitations, Shield Guard cannot monitor or enable this setting remotely. Thus, to auto-remediate SNMP v3 settings at a device, you must manually toggle on the SNMP Settings switch at the device.
- If  appears next to a field (for example, Read User Name), you can select it to auto-generate a random text string and insert it into the field.
- Shield Guard provides default values for all SNMP v3 fields except the Context Name field, for which **you must provide a value before you can save the policy**.
- Spaces are restricted from use in SNMP v3 settings, as well as the following characters:

Restricted Character	Description
\	backslash
'	single quote
"	double quote
#	pound sign

Ultimate Security Settings

Use this section to configure the Shield Guard Ultimate Security settings for a selected policy. These settings correspond with the bizhub SECURE Ultimate settings on the device. Toggle on the settings you want Shield Guard to monitor, and toggle off the rest. Be sure to configure the additional options (if any) for the settings you toggle on.

Notes:

- If you configure Shield Guard to monitor an Ultimate setting on a device that does not support the setting, Shield Guard will assess the setting as Not Secure.
- Shield Guard Ultimate Security settings are **supported only on i-Series devices on which:**

- **The LK-116 Virus Scan i-Option is supported.**

- The LK-116 Virus Scan i-Option has been installed.

The following **table** lists the Ultimate Security settings as well as descriptions of the device’s corresponding bizhub SECURE Ultimate Security settings and how Shield Guard assesses those settings.

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
Virus Scan License	Devices have no corresponding setting. Instead, if the LK-116 Virus Scan i-Option is licensed on the device, then Ultimate Security settings are available on the device and Shield Guard can monitor the settings.	Monitors the LK-116 i-Option on the device. If the LK-116 i-Option has been licensed (installed and enabled) on the device, Shield Guard assesses the setting as Secure.	N
Log Pattern File Version	Devices have no corresponding setting. Instead, the LK-116 Virus Scan i-Option installs a pattern file (a database of virus information) onto the device to identify and eradicate viruses.	Polls the device for the version of the antivirus pattern file . If a change is detected, the Shield Guard agent sends the updated value to the log in the Shield Guard portal.	N
Pattern File Updates	Displays an alert on the MFP panel when the virus scan pattern file fails to update.	Monitors the “Update failure of pattern file” setting at the device. If enabled, Shield Guard assesses the setting as Secure.	Y
Real-Time Scanning	Enables admins to enable/disable the Real-Time Scanning option on the device. This option scans all files sent, scanned, or accessed by the device, as well as files located on USB drives.	Monitors the Real-Time Scanning setting on the device. If enabled, the Job Control Levels appear where you can specify how you want the device to respond when the LK-116 kit detects a virus. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y

Shield Guard Setting	Functionality at the Device	Shield Guard Assessment	Automatic Remediation?
Regular Scan	Enables admins to enable/disable the Regular Scan option on the device. This option performs a full virus scan of the device at a user-specified interval. Note: Enabling this option on the device can impact device performance, so we recommend you schedule the scan to occur at off-peak hours.	Monitors the Regular Scan setting on the device. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure. Note: When scheduling a regular scan to occur monthly, if the day of the month you select exceeds the number of days in a given month, the scan will occur on the final day of that month. For example, if you select 31, then in April, the scan will occur on April 30 (the last day in April). Note that, for scheduling purposes, devices always consider February to have 28 days.	Y

Note: If neither of the above scanning options are enabled on the device, then:

- No virus scanning occurs.
- No check of the pattern file version occurs.
- No update of the pattern file occurs, so no log indicating a change to the pattern file will be generated.

The Antivirus Pattern File

The LK-116 Virus Scan i-Option includes an antivirus pattern file. This file is a database of virus information that is constantly updated to include the latest antivirus information from around the globe. As part of the installation of the LK-116 Virus Scan i-Option onto a device, the antivirus pattern file is installed onto the device.

In order for the LK-116 Virus Scan i-Option to maintain the latest version of the pattern file on a device, note the following:

- The device must be connected to the internet.
- Virus scanning must occur. That is, at least one of the scanning options (Real-Time Scanning or Regular Scan) must be enabled on the device.

A virus scan triggers a check of the pattern file. If an updated version is available, it is downloaded to the device and the scan proceeds using the new pattern file. If no new version is available, the scan proceeds using the existing pattern file.

Monitoring Changes to the Antivirus Pattern File

Shield Guard can monitor changes to the antivirus pattern file on each device assigned to a security policy. If the following is true, then Shield Guard will create a log for every change detected in the antivirus pattern file on a device:

- The device **supports the LK-116 Virus Scan i-Option**.
- The LK-116 kit has **completed its initial installation**. If Shield Guard assesses the device before the installation is complete, a log will be generated showing a device value of "Pending".
- The Log Pattern File Version setting is enabled in the policy.
- At least one of the virus scanning options (Real-Time Scanning or Regular Scan) is enabled on the device.

The LK-116 kit should complete its installation automatically, within a few minutes. If not, consider the following remedies:

- Reboot the device to trigger the pattern file update.
- Confirm that your network settings are not preventing the update.
- Configure the proxy server (if any) to allow the device to pull the pattern file update, as this is independent of the proxy settings used by MarketPlace and Shield Guard. In the Web Connection app, access the following:

Network/Machine Update Settings/HTTP Proxy Settings
- Contact your authorized Konica Minolta service team to take action to resolve the problem, including potentially updating the device's firmware.

Device Support for the LK-116 Virus Scan i-Option

Not all devices support the LK-116 Virus Scan i-Option, including some i-Series devices. If you configure a Shield Guard policy to monitor Ultimate settings (that is, you enable the Virus Scan License setting), note the following:

Device Supports LK-116?	Configuration of LK-116 at the Device	Shield Guard Assessment of the Virus Scan License Setting	Shield Guard Log
No	Not Applicable	Not Secure	Labels the device value as "Not supported"
Yes	LK-116 is installed, but none of its settings are enabled	Secure	None

Device Supports LK-116?	Configuration of LK-116 at the Device	Shield Guard Assessment of the Virus Scan License Setting	Shield Guard Log
Yes	LK-116 is not installed	Not Secure	Labels the device value as “Not installed”

Supported Ultimate Settings

Shield Guard’s support for bizhub SECURE Ultimate is contingent on your Shield Guard **license plan**. If a setting or control does not appear in Shield Guard, your license plan does not support it. See the following table:

Shield Guard Plan	Shield Guard Support
Enterprise	Full monitoring of Ultimate settings, and remediation of applicable settings.
Business	Full monitoring of Ultimate settings.
Starter	Monitoring of the LK-116 Virus Scan i-Option to determine if it is licensed on the device.

Note: Your license plan affects only Shield Guard functionality. It does not affect the functionality of Ultimate Security settings on the device.

Step 6 - Save

The **Save** button is inactive until all **required fields** contain valid responses. If you click on this button when it is active, your current configuration is preserved and you return to the Policies page where the policy appears in the Policies table. To exit the page without saving, you can either navigate to another page or click on the browser’s **Back** button.

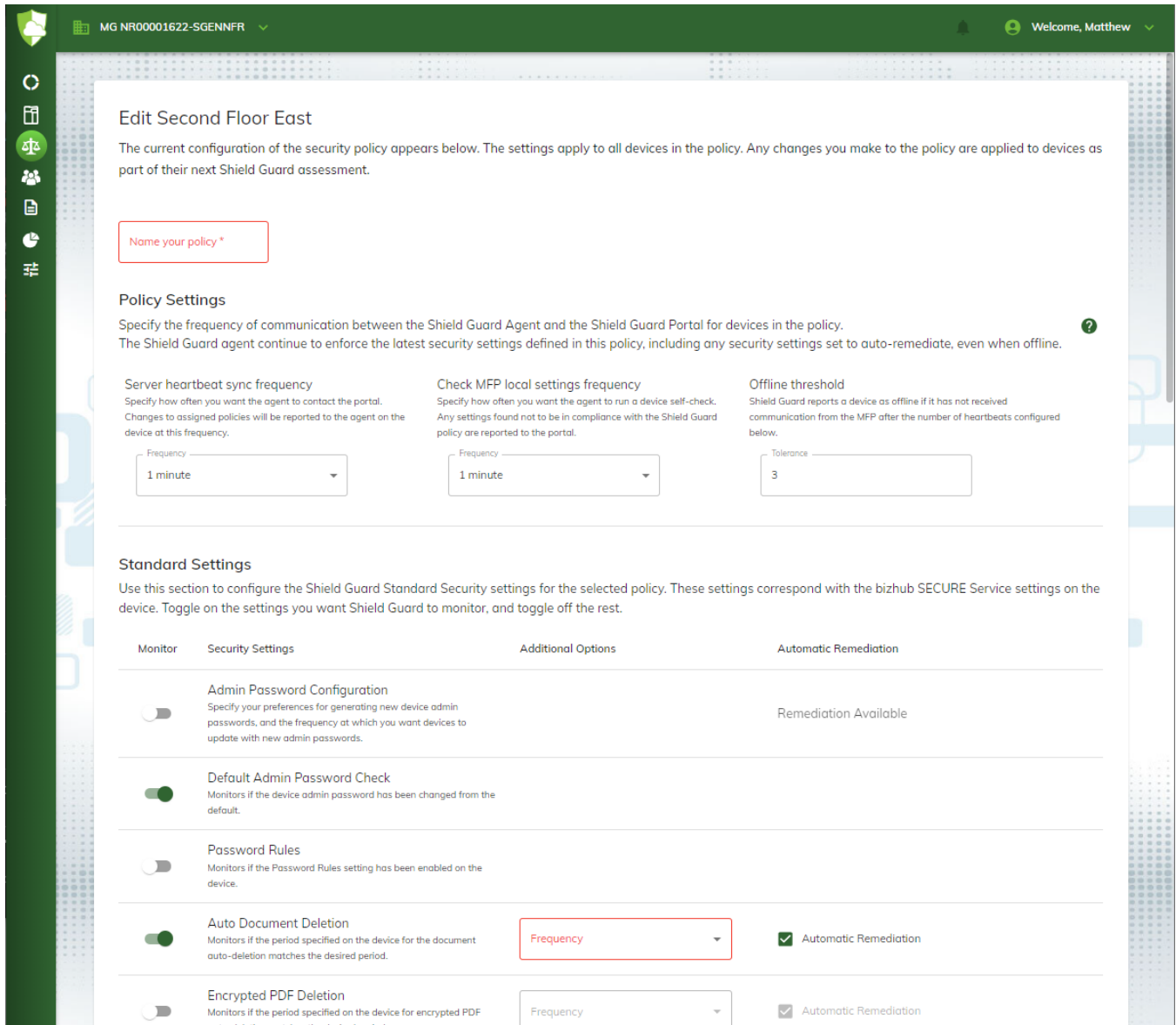
A Note on Required Fields and Saving Security Policies

On the Edit Policy page (and the Create a New Policy page, as well), fields requiring a valid response display in **red**. The following fields are required on the Policies page:

- **Name your policy** - Each policy requires a unique name.
- **Additional Options** - If you toggle on a setting for which additional options exist, the **Additional Options** field for that setting activates and becomes a required field for the policy.

In the illustration below, the Edit Policy page appears. Note the following:

- The **Name your policy** field displays in red, indicating it is a required field awaiting a valid response.
- The Auto Document Deletion setting has been toggled on, and the dropdown field displays in red, indicating it is awaiting a response.



Auto-Remediating Non-Compliant Device Security Settings

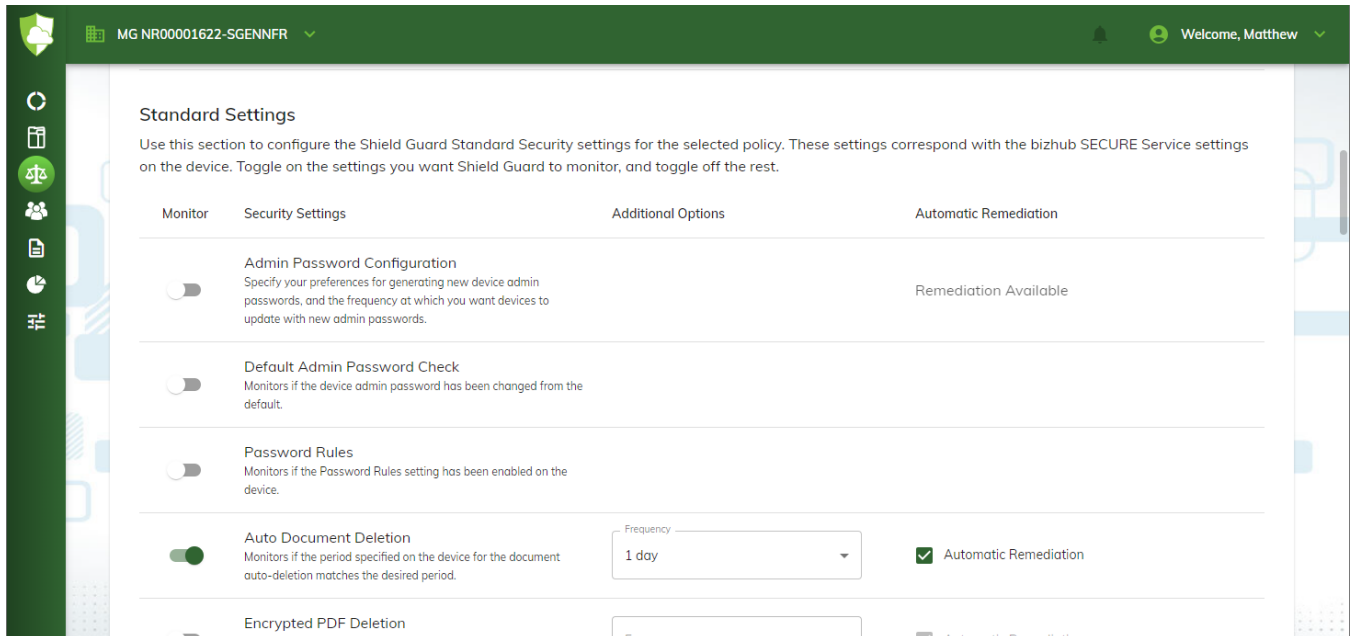
Most Shield Guard security policy settings have an automatic remediation option to automatically bring non-compliant device security settings into compliance with the policy. If such a policy setting is toggled on and its Automatic Remediation box is checked, then Shield Guard will automatically remediate the setting as part of its device assessment. If automatic remediation is not active for a setting, or the setting does not support automatic remediation, the setting must be changed manually, at the device, to return it to a compliant state.

Note: Automatic Remediation is supported only on:

- The **Enterprise plan**.
- **i-Series devices**, with the exception of Admin Password Configuration, which is supported on all MarketPlace devices. For devices that do not support automatic remediation, activating automatic remediation on a setting has no effect.

In the following illustration, note the following:

- The Auto Document Deletion setting is toggled on.
- The deletion frequency is set to 1 day.
- The Automatic Remediation box is selected.



With this configuration, each Shield Guard assessment will ensure all devices in the policy have their Auto Document Deletion setting enabled and the document deletion frequency set to 1 day. Shield Guard will automatically remediate any non-compliant settings to a compliant state.

Note: The **Overview** topic includes a description of a **sample custom policy** that lists the basic steps Shield Guard performs when monitoring and maintaining security for devices assigned to a security policy, including the step in which automatic remediation is applied to a setting.

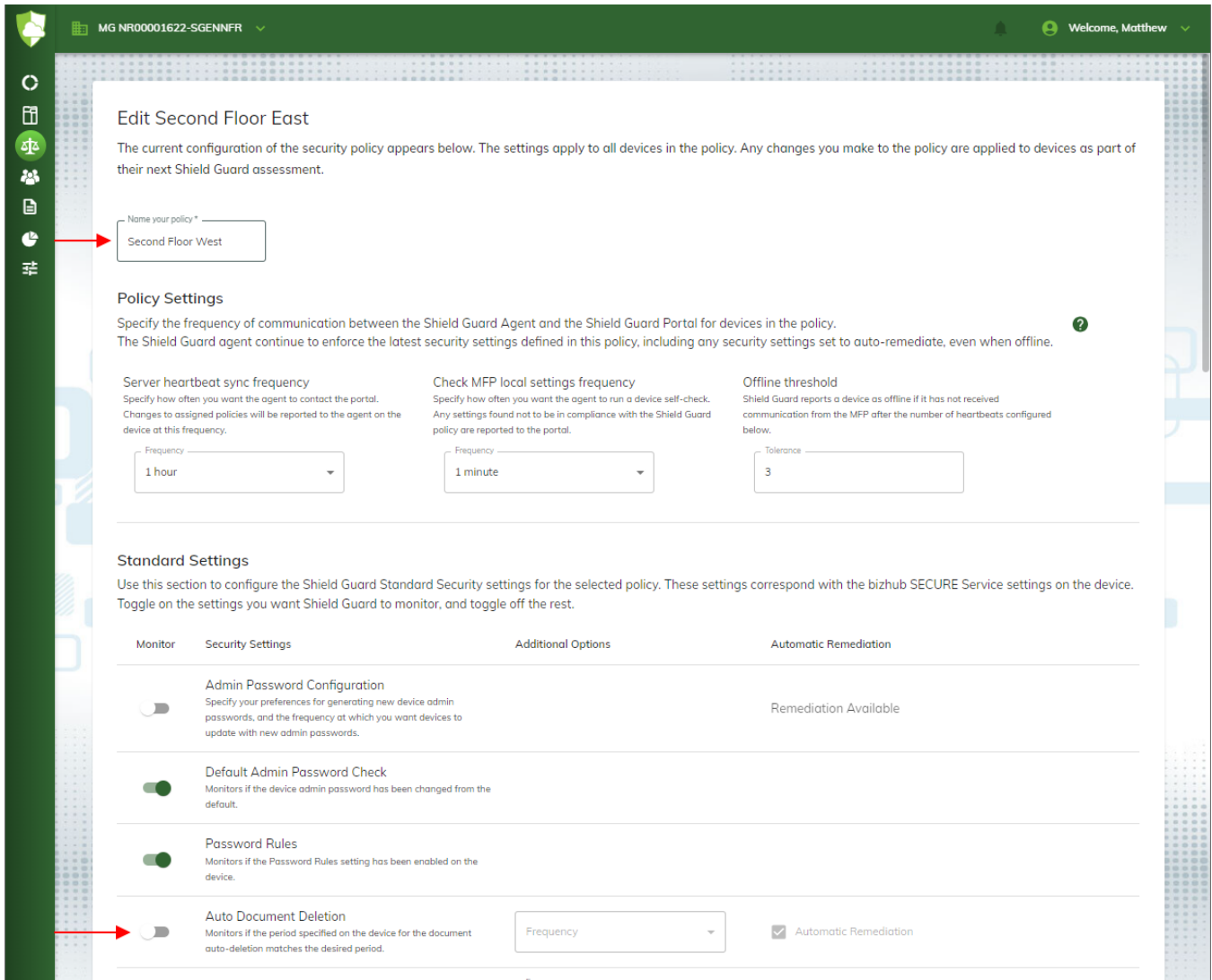
Editing a Policy

To edit a security policy, click on the **Edit** button for the policy in the Policies table. The Edit Policy page appears.

You can change the policy name and/or toggle on (or off) one or more **security settings**. Many settings have additional options allowing you to fine-tune your preferences. For details on the individual fields on the Edit a Policy page, **click here**.

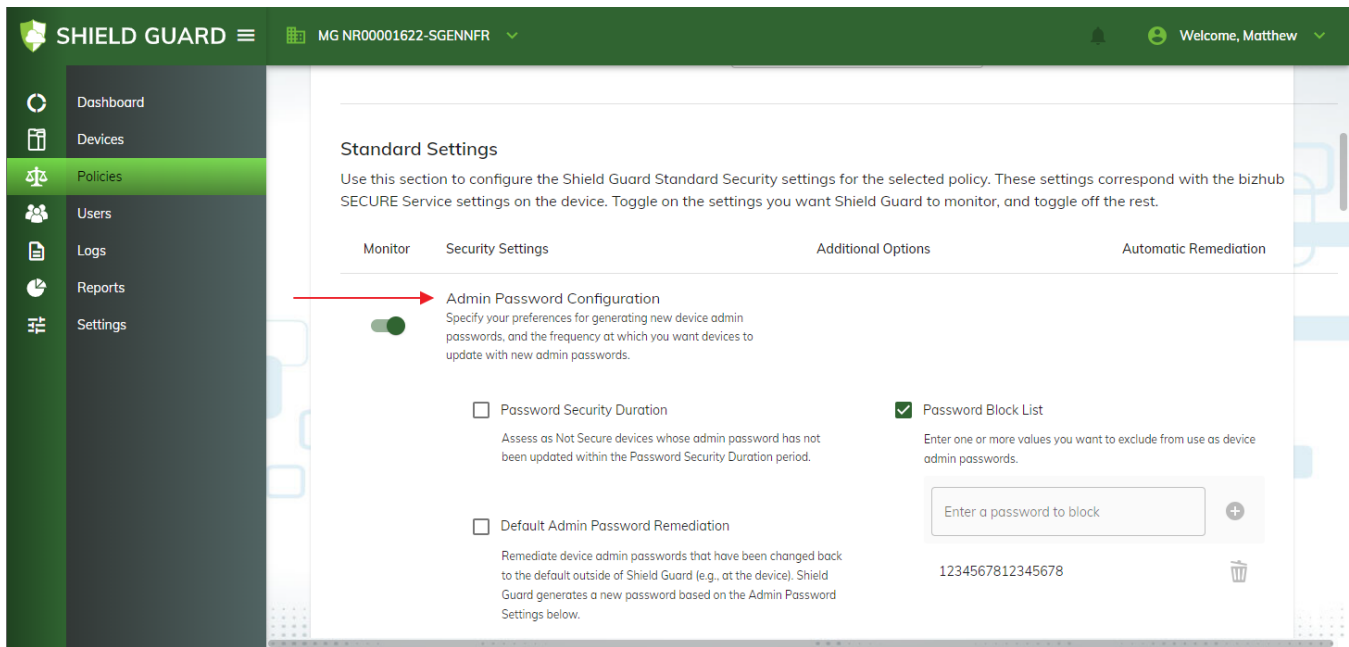
Note: Any changes you make to security settings in an existing security policy are applied at the next **server heartbeat sync**. This includes changing the server heartbeat sync frequency itself.

The following illustration of the Edit Policy page shows a security policy called “Second Floor East” where the policy name has been changed to “Second Floor West” and the Auto Document Deletion security setting has been toggled off.



Password Management

You can configure Shield Guard security policies to monitor, and automatically generate, device admin passwords for devices assigned to the policy. Use the Admin Password Configuration section of the Policies page. The following illustration shows the page as it appears when the setting is toggled on, displaying some of the configuration options on the page:



Note: Any changes you make to security settings in an existing security policy are applied at the next **server heartbeat sync**.

Using the Device Admin Password Configuration Feature

Toggling On the Admin Password Configuration setting provides access to powerful features that enable you to remotely control the password management of devices in the policy. Note the following device requirements for this feature:

- The device's **Password Change Permission** setting must be set to "Allow".
- The device's admin password must be currently **verified with Marketplace**.
- The verified password must **match** the **Shield Guard policy's admin password**.

Note: The passwords do not need to match for the initial sync of the policy with the devices in the policy. This is required only for assessments that occur after the initial sync.

If at any time Shield Guard assesses a device that fails to meet any of the above requirements, Shield Guard will assess the device as Not Secure and suspend password management and/or remediation for the device until all requirements are met.

Note: A device's Password Rules setting can affect Shield Guard's ability to update the device's admin password. See the **Password Options** section below.

Matching a Device's Admin Password with the Shield Guard Policy's Password

For Shield Guard to manage and/or remediate a device's admin password, the password must be currently **verified with Marketplace**. A device's password becomes unverified if it is changed manually at the device and then not re-verified. Shield Guard assesses such devices as Not Secure and generates a **log** in which the Device Value column gives a value of "Password unknown".

To rectify a mismatched password, you have the following options. Note that for both of these options, you must provide the device's current admin password:

- Change the device's admin password to match the policy's password. Do the following:
 1. Access the policy in the Shield Guard Portal and note the password currently stored in the policy.
 2. At the device, manually change the admin password to match the policy's password. For more information on this process, refer to the device's user guide.
 3. Verify the password with Marketplace. Do one of the following:
 - At the device panel, click on the App Manager button and, if prompted, provide the device's admin password.
 - In Marketplace, on the Devices page, verify (or re-verify) the device's admin password.

- Change the policy's password to match the device's admin password.
 1. Access the policy in the Shield Guard Portal.
 2. Use the **Manual Password** option to change the policy's password to the match device's current password.
 3. Verify the password with Marketplace. Do one of the following:
 - At the device panel, click on the App Manager button and, if prompted, provide the device's admin password.
 - In Marketplace, on the Devices page, verify (or re-verify) the device's admin password.

Once rectified, and an assessment occurs for the device, the passwords will match and the Admin Password Configuration setting will no longer cause Shield Guard to assess the device as Not Secure.

Configuring Device Admin Passwords

If you enable the Admin Password Configuration setting, the following options appear:

- **Password Security Duration** - To specify a password security duration for the admin password for each device assigned to the policy, check the box at this field. The **Duration** field appears. Click on the drop-down and select a time period from the list that appears.

If you enable this setting, then all devices whose admin password has not been updated within the specified time period (for example, 1 day) will be assessed as Not Secure. Note the

following:

- The password security duration includes a grace period of up to 10 minutes. For example, if you set the password duration to 1 day, then if the password is not changed within one day plus the grace period, the policy will fail assessment. The grace period provides extra time in the event the device is delayed in receiving the password changes, for example, the device is in Sleep mode.
- The password duration you specify must be greater than the **heartbeat sync frequency**.
- You can automatically update admin passwords based on the duration you specify. On the Random Password tab at the Admin Password Generation field, enable the **Automatically update password based on password security duration** setting (described below). This option is available only for random password generation.
- **Default Admin Password Remediation** - To automatically update the device's password whenever it is changed back to the device default password outside of Shield Guard (e.g., at the device), check the box at this field. The password updates based on the settings in the **Admin Password Generation** section.

Note: To remediate admin passwords, the **Default Admin Password Check** setting must also be toggled on. Thus, if you attempt to enable this setting while the Default Admin Password Check setting is not toggled on, a warning message appears with the option to automatically enable that setting. To enable both settings, click on **OK**. To preserve the Toggled Off status for both settings, click on **Cancel**. If the Default Admin Password Check setting is already toggled on, or if you are attempting to toggle off this setting (Default Admin Password Remediation), no warning message appears.

- **Password Block List** - To specify one or more passwords you want to prevent users from using as the admin password for devices in the tenant, check the box and specify the passwords you want to block. This option is toggled on by default, but you can toggle it off.

If you check the box at this field, the **Enter a password to block** field appears, and below that the default device admin password appears. This password is automatically included in the blocked password list, and it cannot be removed.

To add a password to the blocked list, enter it into the field. The **Plus** button activates. Click on the button to add the password to the list. Repeat the process for any additional passwords you want to add to the blocked list.

When finished, click on the **Save** button to update the policy. Note that if you disable the Password Block List feature (leave the check box blank), any user-defined passwords in the policy are removed from the block list.

Generating Device Admin Passwords

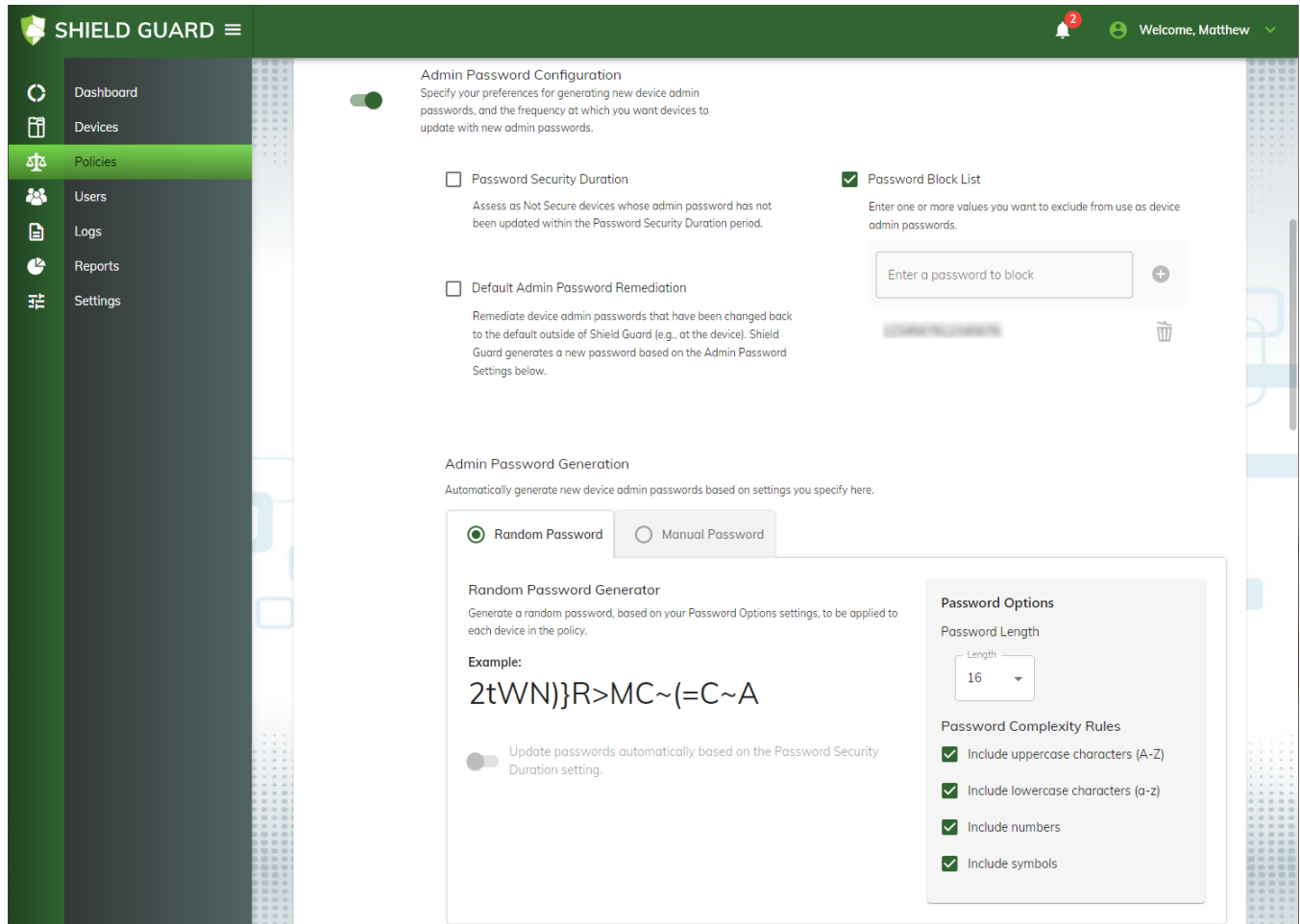
We strongly recommend you replace the default admin password with your own password for each device in your fleet, and we recommend you update your passwords regularly. Shield Guard provides the following methods of updating device admin passwords:

- **Random Password Generator**

- **Manual Password Generator**

Using the Random Password Generator

To generate a random password for each device in the tenant, click on the **Random Password** button. See the following illustration:



When you save the policy, Shield Guard:

- Generates the password based on the requirements specified in the **Password Options** section.
- Applies the password to each device at the next server heartbeat sync.

You can then view the password at the **View Admin Password** action button on the Devices page.

Generating Random Passwords Automatically

In addition to the initial password described above, you can generate random passwords automatically at a specified interval. Use the following field:

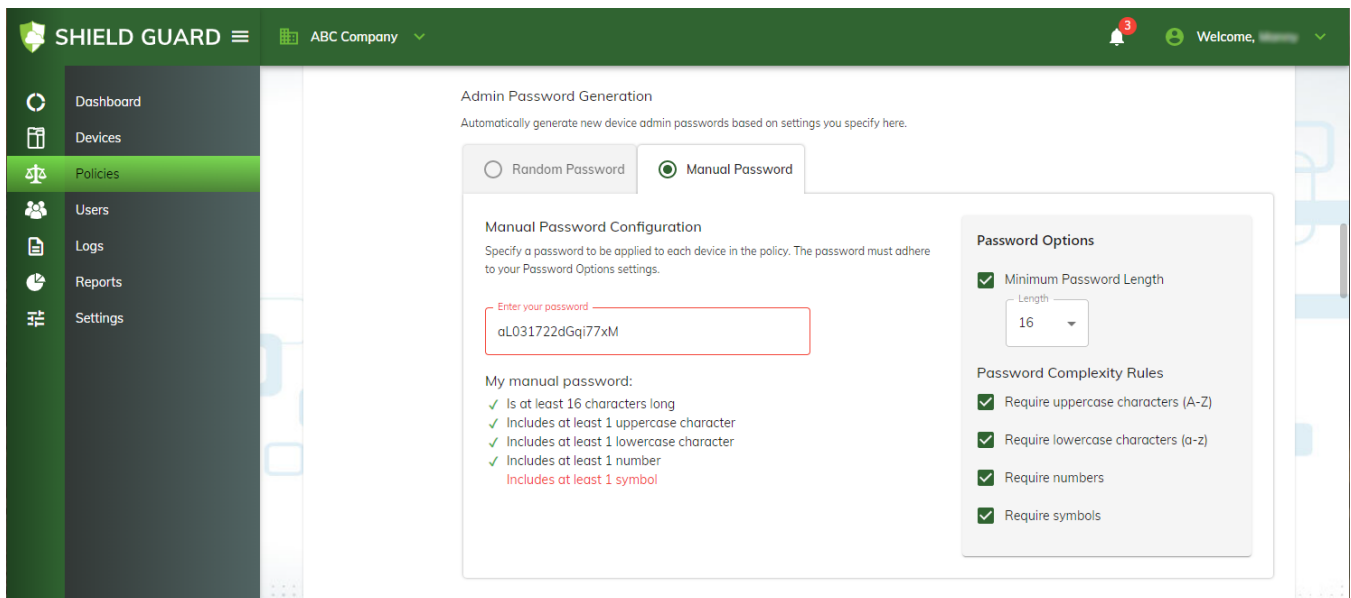
- **Update passwords automatically based on the Password Security Duration setting** - If you enable the **Password Security Duration** setting above, this field activates and, if you also enable this setting, you can schedule automatic updates for your device admin passwords based on the duration specified. For example, if you:
 - Enable the **Password Security Duration** setting
 - Specify 1 day as the password security duration period
 - Toggle on the **Update passwords automatically based on the Password Security Duration** setting

Then, at the next server heartbeat sync that occurs after the password security duration period expires, the device will not pass compliance. However, Shield Guard will generate a new password and, at the next server heartbeat sync, the new password will enable the device to meet compliance.

Note: If the **server heartbeat sync** is set to a period longer than the password security duration, Shield Guard will always assess the device as Not Secure. That is, because applying the new password occurs during a second assessment of the device, that assessment will never occur in time to update the password so that the device complies with the **Password Security Duration** setting.

Using the Manual Password Generator

To manually generate a custom password for each device in the tenant, click on the **Manual Password** button. See the following illustration:



Do the following:

1. Specify one or more password requirements in the **Password Options** panel. Your password string must meet the requirements before you can save the policy. If you do not specify any

password requirements, Shield Guard still applies a minimum requirement of at least four characters in the string.

2. Enter your password string.
3. Click on the **Save** button when done. The **Save** button activates once the string meets all password requirements and no other issues exist for any settings in the policy.

When you save the policy, Shield Guard generates the password and applies it to each device in the policy at the next server heartbeat sync. You can then view the password at the **View Admin Password** action button on the Devices page.

Password Options

This panel in the **Admin Password Configuration** section contains options for imposing password requirements (for example, a minimum length) on passwords generated by Shield Guard.

Note: The Shield Guard Password Options setting does not override the device's Password Rules setting. Instead, it only imposes restrictions on the passwords generated by Shield Guard before they are actually sent to the device. Shield Guard will not generate a password that does not meet all restrictions imposed by the Password Options setting. However, a password generated by Shield Guard may still fail the requirements imposed by the device's Password Rules setting. For example, if Shield Guard generates a 16-character password based on a minimum length requirement and sends it to a device whose minimum length requirement is set to 20 characters, the update will fail and the password will not be updated.

For **random password generation**, Shield Guard applies the requirements you specify to all passwords generated.

For **manual password generation**, Shield Guard displays descriptive text in the **Please use a password that:** section for each password requirement you activate. The descriptive text displays in **red** until the password string meets the requirement, at which time the text turns to black. For example, if you activate the **Require Symbols** option, the descriptive text "Includes at least 1 symbol" will display in **red**, unless the password string contains one or more symbol characters. See the illustration above.

The following options are available:

- **Minimum Password Length** - This field appears only for manual password generation. To require manual passwords to meet a minimum length, check the box. The **Length** field activates.
 - **Length** - For random passwords, specify the password length. For manual passwords, specify a minimum length. Click on the dropdown and select a number from the list that appears. Note that a password length of 16 or more characters is considered "strong" while 15 or less characters is considered "weak".
- **Password Complexity Rules** - Check the box next to the rules you want to apply for device admin password generation.

- **Require uppercase characters (A-Z)** - Require the password to contain at least one uppercase character.
- **Require lowercase characters (a-z)** - Require the password to contain at least one lowercase character.
- **Require numbers** - Require the password to contain at least one numeric character.
- **Require symbols** - Require the password to contain at least one symbol character.

Reports and Logs

Overview

From the Shield Guard Portal, you can view reports on **device statuses** and view detailed logs of Shield Guard activity for real-time monitoring of your devices and licenses, equipping you with the information you need to respond decisively to security events.

- **Reports** - Using Shield Guard's Report Generator tool, you can do the following:
 - Export reports into CSV (comma-separated-value).
 - Schedule reports to generate automatically at a specific date and/or time **(Coming Soon!)**.
- **Logs** - Shield Guard's Log Viewer enables you to view activity logs, displaying critical information about your system such as security issues, failed assessments, and more.

The Logs page appears in the illustration below:

SHIELD GUARD ABC Company Welcome

Logs Search

View security logs (device, policy, or user) generated within your Shield Guard plan.

Importance	Type	Event	Date ↓
Info	Device	Device 364e (A112233440003) passed its policy assessment.	2/18/2021, 9:41:44 AM
Info	Device	Device 364e (A112233440002) passed its policy assessment.	2/18/2021, 9:40:04 AM
Info	Device	Device 558 (A112233440001) passed its policy assessment.	2/18/2021, 9:38:24 AM
Info	Device	Device 558 (A1122334400017) setting Auto Document Deletion remediated from 3 days to 7 days.	2/18/2021, 4:08:24 AM
Info	Device	Device C300 (A1122334400019) setting SSL/TLS Version Setting remediated from range TLSv1.1 - TLSv1.3 to range TLSv1.2 - TLSv1.3.	2/17/2021, 10:35:04 PM
Warning	Device	Device 364e (A112233440004) did not pass its policy assessment.	2/7/2021, 11:41:44 PM
Warning	Device	Device C300 (A112233440005) did not pass its policy assessment.	2/6/2021, 7:55:04 PM
Info	Device	Device 558 (A1122334400011) passed its policy assessment.	2/6/2021, 7:55:04 PM
Info	Device	Device 364e (A112233440008) passed its policy assessment.	10/25/2020, 4:55:04 PM
Warning	Device	Device C300i (A112233440007) did not pass its policy assessment.	10/25/2020, 4:53:24 PM

Rows per page: 10 1-10 of 17

Shield Guard Reports

Shield Guard reports generate report data on device activity in the tenant. You can then view the report on the screen and/or export the report to a CSV file. The page shows both graphic and tabular representations of the found data, and reflects any filtering you apply to the results. Report data includes activity for any device that was ever in the tenant, even if the device is not currently in the tenant.

To begin working with reports, select the Reports option from the **Navigation pane**.

Reports

View a scheduled report or, to create a new report, use the Filters panel to specify a report type, report name, etc. Select **Create Report** to display the results on the screen. To further filter the results, select the **Funnel** icon in the viewing area. When done, select **Schedule**.

Filters Clear

Select Fleet Status Report
Device Status

Select Date Range
Date Range
Last 7 Days

Create Report

Export a Report ^

Please fill in the following information in order to receive a report via email as specified by the frequency.

Report Name

Format
CSV

Frequency

Cancel Export

Fleet Status - Devices Assessed

Last 7 Days 03/19/2024 TO 03/26/2024

Secure Not Secure Offline

Name	Security Status	Policy Name	Device Group	Date	Serial Number
bizhub 4052	Secure	Executive		3/26/2024, 1:20:24 PM	AA1R011012863
bizhub C287	Offline	—	—	3/21/2024, 3:55:04 PM	A797011000008
bizhub C4050	Offline	—	—	3/20/2024, 6:50:04 PM	AA1N011001611

Use the Reports page to:

- Create a new report.
- Filter report data, for example, by device and/or device status.
- Export a report.
- Schedule a report.

Creating a Report

Creating a report consists of the following basic steps:

1. Specify your inclusion criteria, including the date range.
2. Generate the report (via the **Create Report** button).
3. Filter the report to include only the data you want to see.
4. Specify export criteria, including a frequency for receiving scheduled reports.

Filters Panel

The Filters panel includes the following configuration options:

Select Fleet Status Report

The following report type is available:

- Device Status - Lists device status events (events in which a device's status changed to Secure, Not Secure, or Offline) for devices in the tenant.

Note: For a breakdown of the current device statuses in the tenant, including the No Policy and Not Assessed statuses, visit the **Dashboard page**.

Select Date Range

Select a day or a range of dates whose data you want to include in the report:

- Last 30 Days
- Last 7 Days
- Yesterday
- Today
- Custom

Create Report Button

Once you select a date range, the **Create Report** button activates. Select this button to generate the report. The report displays in both graphic and tabular form on the screen.

Note: If you hover your pointer over a data point on the graph, information on the data point appears.

Export a Report

Once you select a date range, the fields in the **Export a Report** area activate. Use these fields to export the tabular data to a CSV file. Specify the following export criteria:

- Report Name - Give the report a descriptive name.
- Format - The report format defaults to CSV.
- Frequency - Select the frequency at which to export the report:
 - Once - Activates the **Export** button, via which you can export the report immediately.
 - Weekly - Activates the **Schedule** button, via which you can schedule the report to generate and export on the following Monday.
 - Monthly - Activates the **Schedule** button, via which you can schedule the report to generate and export on the first day of the following month.

- Yearly - Activates the **Schedule** button, via which you can schedule the report to generate and export on the first day of the following year (January 1).

Notes:

- All scheduled reports:
 - Are listed in the Scheduled Reports List.
 - Continue to export at the selected frequency until removed from the Scheduled Reports List.
 - Generate a notification email that is sent to your MarketPlace email account.
- Notification emails contain a link that, when selected, downloads the report to the destination specified in your browser. If you are not logged in to the tenant at the time you click on the link, a warning message appears and you must log in before the report will download.
- If you schedule a report with a Custom date range, each edition of the report (weekly, monthly) will contain the same data as the original.
- If you schedule a report with a “Last 7 Days” or “Last 30 Days” date range, each edition of the report will contain different data. That is, the date from which the “last 7 days” is established will be different each time the report is sent out, and thus the data will be different.

Filtering the Report

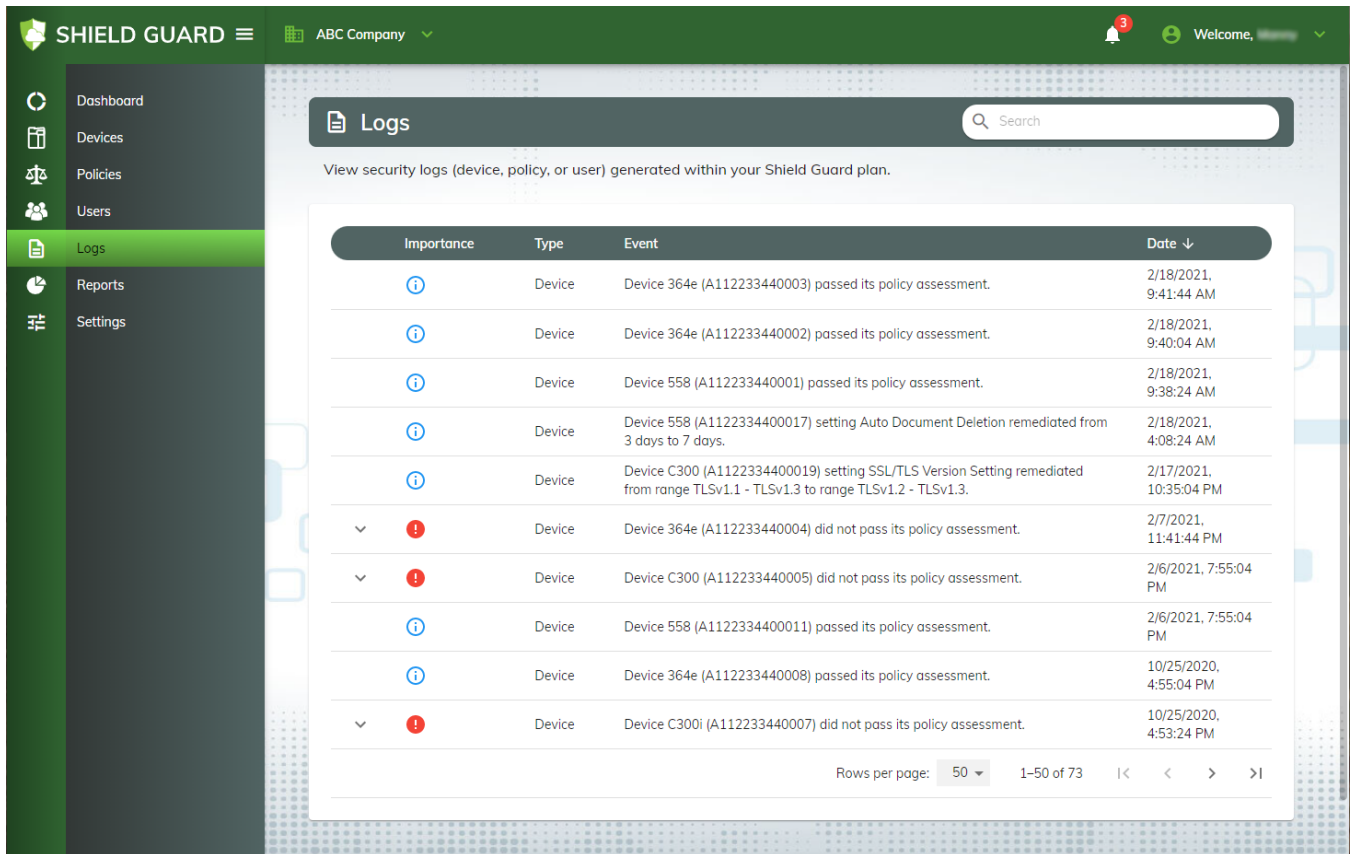
When you select the **Create Report** button, all of the data found from your report criteria appears in the data table. If you select the Funnel icon above the data table, the Filter Report window appears, in which you can filter this data by:

- Devices - Restrict the report to status events for one or more devices in the tenant.
- Data Columns - Restrict the report to display only selected columns of data.
- Events - Restrict the report to display only events in which the device status changed to the selected statuses, for example, Not Secure and Offline.

Note: Any filtering you apply to a report is reflected on the screen as well as in the exported version of the report.

Shield Guard Logs


Shield Guard’s Log Viewer displays a list of security events that occurred for devices in the tenant. To access the Log Viewer, select the Logs option from the **Navigation pane**. See the following illustration:



The list of security events appears in the Logs table. If you click on a column header, the table sorts by that column. To reverse the sort order, click on the column header again.

The **Rows per page** dropdown menu controls the number of logs that appear on a single page. If the number of existing logs exceeds the number of rows per page, you can view additional pages of logs by clicking on the angle brackets (< or >) to the right of the rows per page.

The Logs table contains the following information:

Column	Description
	View log details.
Importance	The severity of the event (high or low).
Type	The type of event (Device/Policy).
Event	A description of the event.
Date	The date and time that the event occurred.

About Log Events

Shield Guard generates an event log for any of the following occurrences:

- When a Shield Guard security assessment detects a change in a device’s **security status**, for example from Not Assessed to Secure. That is, not all assessments generate a log. Note that Shield Guard performs security assessments based on the security policy’s **frequency settings**.
- Certain updates to a policy, or to users and/or devices in a policy, including the following:
 - A Shield Guard policy is created, or a setting is modified.
 - The Shield Guard agent is removed from a device in the policy.
 - A device is added to, or removed from, a tenant.
 - A device is added to, or removed from, a Shield Guard policy.
 - A device in a tenant goes online or offline.
 - A user is added to, or removed from, a tenant.

Viewing Log Details

If a “down” chevron appears in a row of the Logs table, additional information is available about the log entry. To view log details, click on the chevron. The details appear and the chevron switches to “up”. To hide details, click on the Up chevron.

The following illustration shows the most recent assessment of Device 287 with a “low” importance rating, while an assessment of the same device four minutes before shows a “high” importance rating. The Log details for that assessment identify the security settings involved and indicate which Shield Guard policy values do not match the device values. Those device values were then modified by the user to match the Shield Guard policy values, so that subsequent logs rated the importance as “low”.

SHIELD GUARD Welcome, Matthew

Logs Search

View security logs (device, policy, or user) generated within your Shield Guard plan.

Importance	Type	Event	Date ↓
📘	Device	Device 287 (A7AH019002101) passed its policy assessment.	9/20/2021, 1:02:52 PM
📘	Device	Device C287 (A797011000008) passed its policy assessment.	9/20/2021, 1:02:46 PM
📘	Device	Device 287 (A7AH019002101) passed its policy assessment.	9/20/2021, 1:01:46 PM
📘	Policy	Policy Second Floor East (2440567637011-DBbwje5Qih1dBCRX3YMzvW) updated in tenancy (DM00005717-SGAAA01) license	9/20/2021, 1:00:15 PM
⬆️ 🚫	Device	Device 287 (A7AH019002101) did not pass its policy assessment.	9/20/2021, 12:58:26 PM

Issues

Security Setting	Policy Value	Device Value
Password Rules	Enabled	Disabled
User Authentication	Enabled	Disabled

⬇️ 🚫	Device	Device C287 (A797011000008) did not pass its policy assessment.	9/20/2021, 12:53:52 PM
⬇️ 🚫	Device	Device 287 (A7AH019002101) did not pass its policy assessment.	9/20/2021, 12:47:25 PM
⬇️ 🚫	Device	Device 287 (A7AH019002101) did not pass its policy assessment.	9/20/2021, 12:45:04 PM
⬇️ 🚫	Device	Device 287 (A7AH019002101) did not pass its policy assessment.	9/20/2021, 12:44:03 PM
⬇️ 🚫	Device	Device C287 (A797011000008) did not pass its policy assessment.	9/20/2021, 12:42:37 PM

Rows per page: 50 1-50 of 73 < > >>

Filtering the Logs Table

To filter the Logs table to list only events containing a specified string, use the **Search** field. The following illustration shows the Logs page, filtered by the following string:

offline device

The Search returns all logs in which both “offline” and “device” appear somewhere in the log. Note that search strings are not case-sensitive.

The screenshot shows the 'Logs' section of the Shield Guard interface. A search bar at the top right contains the text 'offline device'. Below the search bar, a table displays a list of security logs. Each log entry includes an importance icon (an 'i' in a blue circle), a 'Type' of 'Device', an 'Event' description, and a 'Date' with a downward arrow indicating it is sorted in descending order.

Importance	Type	Event	Date ↓
i	Device	Device C300i (AA2K011010707) from tenancy (NR00001622-SGENNFR) went offline	3/11/2024, 12:10:04 PM
i	Device	Device C300i (AA2K011010707) from tenancy (NR00001622-SGENNFR) went offline	3/11/2024, 9:35:04 AM
i	Device	Device C300i (AA2K011010707) from tenancy (NR00001622-SGENNFR) went offline	3/8/2024, 5:10:04 PM
i	Device	Device C300i (AA2K011010707) from tenancy (NR00001622-SGENNFR) went offline	3/8/2024, 1:40:05 PM
i	Device	Device C287 bizhub C287 (A797011000008) from tenancy (NR00001622-SGENNFR) went offline	3/8/2024, 7:45:04 AM
i	Device	Device C300i (AA2K011010707) from tenancy (NR00001622-SGENNFR) went offline	3/7/2024, 5:25:04 PM
i	Device	Device C287 bizhub C287 (A797011000008) from tenancy (NR00001622-SGENNFR) went offline	3/7/2024, 5:15:04 PM
i	Device	Device 287 (A7AH019002101) from tenancy (NR00001622-SGENNFR) went offline	3/7/2024, 3:50:04 PM
i	Device	Device 287 (A7AH019002101) from tenancy (NR00001622-SGENNFR) went offline	3/7/2024, 3:00:04 PM

If you place quotation marks around your search string, the Search returns all logs in which an exact match of the search string appears somewhere in the log:

"offline device"

In the following illustration, searching for the exact string returned no matches:

The screenshot shows the 'Logs' section of the Shield Guard interface. The search bar at the top right contains the text '"offline device"'. Below the search bar, the table area is empty, displaying the text 'No data available' in the center.

Importance	Type	Event	Date ↓
No data available			

Reference

Troubleshooting

Most Shield Guard troubleshooting issues arise from Shield Guard losing synchronization with MarketPlace and/or one or more devices, for example if a device's admin password is changed outside of Shield Guard. These issues can often be resolved by **reinstalling the Shield Guard agent on the affected devices**, and/or **re-syncing the devices to Shield Guard**.

Note: Before trying the above solutions, visit the **FAQ** topic to see if your issue is described there.

Offline Devices

Shield Guard cannot **communicate with a device** if it is **offline** (for example, powered off or in sleep mode). Once the device is back online, Shield Guard can re-establish communication with the device.

Error Messages

If you receive an error message such as “Something went wrong”, retry the process. If the error message appears again, check your internet connection. If the issue persists, contact **Shield Guard support**.

Frequently Asked Questions (FAQ)

This topic lists questions often asked by Shield Guard users, organized by subject:

- **Password management**
- **Licensing and tenants**
- **Shield Guard portal**
- **Shield Guard agent**

Note: For information on using the MarketPlace site, access the **MarkePlace FAQ** page.

Device Admin Password Management

Shield Guard can remotely manage your device’s admin passwords. Most issues involving **password management** can be resolved by **reinstalling the Shield Guard agent on the affected devices**, and/or **re-syncing the devices to Shield Guard**.

1. My Shield Guard policy is set to automatically **generate** and **remediate** device admin passwords on devices assigned to the policy. However, on one device the password is not changing and Shield Guard is still assessing the device as Secure.

Solution: The device may have lost synchronization with Shield Guard. Try **reinstalling** the Shield Guard agent. Do the following:

- a. Uninstall the Shield Guard agent on the device.
 - b. Reinstall the Shield Guard agent onto the device.
 - c. **Re-import** the device into Shield Guard.
 - d. **Reassign** the Shield Guard policy to the device.
2. A co-worker changed the device’s admin password manually, at the device. The device is now Not Secure and Shield Guard will not remediate the device password or generate a new one.

Solution: If a device's admin password is changed manually, outside of Shield Guard, password synchronization with Shield Guard is broken and Shield Guard cannot maintain password management for the device. Shield Guard assesses such devices as Not Secure and generates a **log** indicating a 'password unknown' condition for the device. To restore Shield Guard's password management of the device, you must **re-synchronize the device with Shield Guard**.

Licensing and Tenants

1. What is a license plan?

Solution: Use of Shield Guard requires the purchase of a **license plan**.

2. What is a tenant?

Solution: The purchase of a license plan creates a Shield Guard **tenant**.

Shield Guard Portal

The Shield Guard portal is a website where you can shop for a Shield Guard license plan and, once purchased, manage the tenant created by the purchase.

1. What is automatic remediation?

Solution: Shield Guard can automatically remediate many of your device's security settings. If Shield Guard assesses a device setting as Not Secure, and the setting supports auto-remediation, then Shield Guard will automatically bring the setting into compliance with the assigned Shield Guard policy.

The Automatic Remediation column on the Policies page indicates the settings that Shield Guard can automatically remediate. All other settings must be manually remediated, at the device.

Shield Guard Agent

The Shield Guard agent is a free app you install on each device that you want Shield Guard to monitor. Installing the app enables the device to communicate with the Shield Guard portal.

1. How do I ensure I have the latest version of the agent installed on my devices?

Solution: MarketPlace's **Auto Updates** feature ensures all your apps, including the Shield Guard agent, are up to date.