Holden Hewett
Technical Writer HQ Capstone Project
December 2021

Table of Contents

Site Manager - Reports UI Overview and Usage Guide

Holden Hewett
Updated a few seconds ago

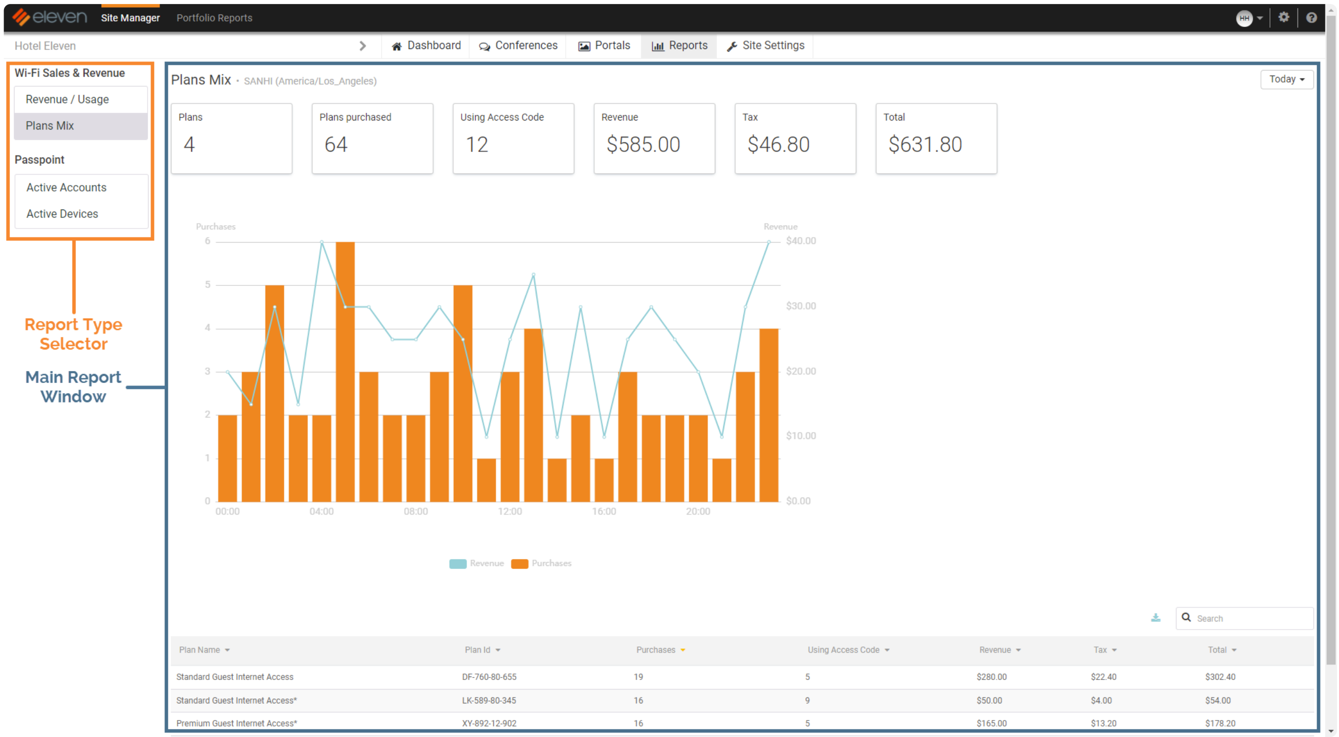
Unfollow

Overview

You can use Site Manager > Reports to run and view statistical data about a given site. There are multiple Report Types that you can run for the different Site Types of Site Manager Portfolios such as Wi-Fi Sales & Revenue, Passpoint, or Multi-Family.

When you first navigate to the Reports page, Site Manager runs the default report from today's date. From there, you can adjust the date range using the Date Selector for the active report or select a different report in the Report Type Selector.

The Site Manager Reports screen contains two main sections: the report type selector and the main report window.



Report Type Selector

Main Report Window

Plans Mix · SANHI (America/Los_Angeles)

Plans	Plans purchased	Using Access Code	Revenue	Tax	Total
4	64	12	$585.00	$46.80	$631.80

Plan Name	Plan Id	Purchases	Using Access Code	Revenue	Tax	Total
Standard Guest Internet Access	DF-760-80-655	19	5	$280.00	$22.40	$302.40
Standard Guest Internet Access*	LK-589-80-345	16	9	$50.00	$4.00	$54.00
Premium Guest Internet Access*	XY-892-12-902	16	5	$165.00	$13.20	$178.20

Report Type Selector

The reports that appear in the report type selector change depending on the Site Type of the Portfolio assigned to the site you are viewing in Site Manager. The Portfolio Site Type also determines which report is run by default when you first navigate to Site Manager > Reports.

Click each report type to change which report the main report window displays. **Table-1** below describes each report type and which Portfolio Site Type enables them.

Table-1 Report Types, associated Portfolio Site Types, and descriptions

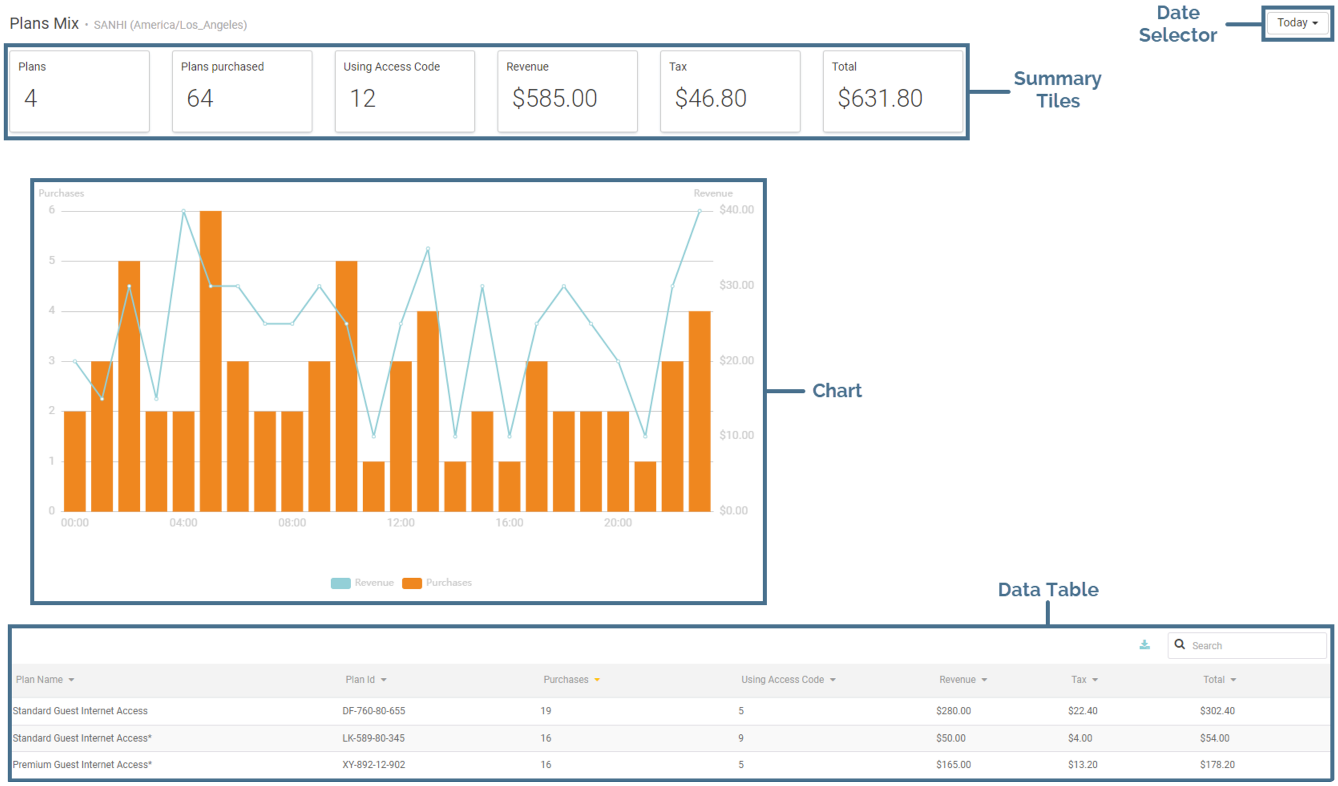
Report Type	Portfolio Site Type	Description
Revenue / Usage	Hospitality	Displays the revenue, taxes, and totals for the chosen period and breaks down the service plans into access codes and PMS transaction methods. (Default report for Hospitality)
Plans Mix	Hospitality	Displays the total number of service plans and how many of each were purchased along with the total revenue, tax, and totals for the chosen period.
Active Accounts	Hospitality w/ Passpoint	Displays the total number of active Passpoint accounts and their associated loyalty levels for the chosen period.
Active Devices	Hospitality w/ Passpoint	Displays the total number of active devices using Passpoint and breaks down the Operating Systems of each device for the chosen period.
Throughput by User	Multi-Family	Displays the data throughput of each resident and the total number of devices, users, and devices per user for the chosen period. (Default report for Multi-Family)

You can reference the Site Manager - Reports - Report Types article for more information on each report type output.

Main Report Window

The main report window is where you can view and interact with the data each report returns. Reports display the following primary components:

- **Date Selector** - Determines the period in which you run the report. Click this button and choose from a list of preset periods or enter a custom date range to run the report.
- **Summary Tiles** - Each summary tile displays key metrics in the report providing a high-level or at-a-glance view of the returned data.
- **Chart** - Displays key metrics in a line, bar, or mixed chart. Some report types contain chart-style controls allowing you to view different types of charts.
- **Data Table** - A table of all metrics returned in the report. You can search for specific values or sort by column in the table using data tools on all report types.



Plans Mix • SANHI (America/Los_Angeles)

Date Selector

Plans	Plans purchased	Using Access Code	Revenue	Tax	Total
4	64	12	$585.00	$46.80	$631.80

Summary Tiles

Chart

Data Table

Plan Name ▾	Plan Id ▾	Purchases ▾	Using Access Code ▾	Revenue ▾	Tax ▾	Total ▾
Standard Guest Internet Access	DF-760-80-655	19	5	$280.00	$22.40	$302.40
Standard Guest Internet Access*	LK-589-80-345	16	9	$50.00	$4.00	$54.00
Premium Guest Internet Access*	XY-892-12-902	16	5	$165.00	$13.20	$178.20

Run a Report with a Custom Date Range

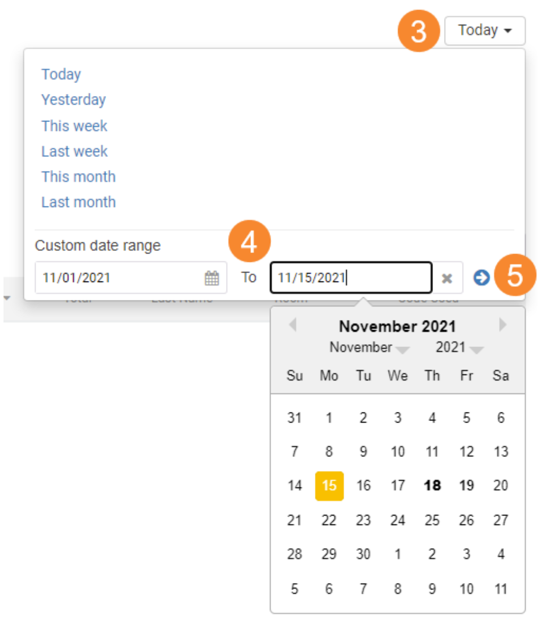
Holden Hewett
Updated 9 days ago

Unfollow

Overview

Run reports to view different statistics about a site.

1. From the Site Manager Dashboard, click **Reports**.
2. In the top left, select the desired report type.
3. In the top right, click **Today** (date selector) button.
4. In the **Custom date range** section, enter the start and ends dates for the report.
5. Click (Go).



Custom date range

11/01/2021 To 11/15/2021

November 2021

November 2021

Su	Mo	Tu	We	Th	Fr	Sa
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

Site Manager displays a report with the selected report type from the date range you chose.

> **Eleven Tip**
> Want to run a different report for the same custom date range? Simply switch between each report type in the top left and Site Manager will run each report type using the custom date range you chose.

Related Links

- Site Manager - Reports UI Overview and Usage Guide
- Site Manager - Reports - Report Types

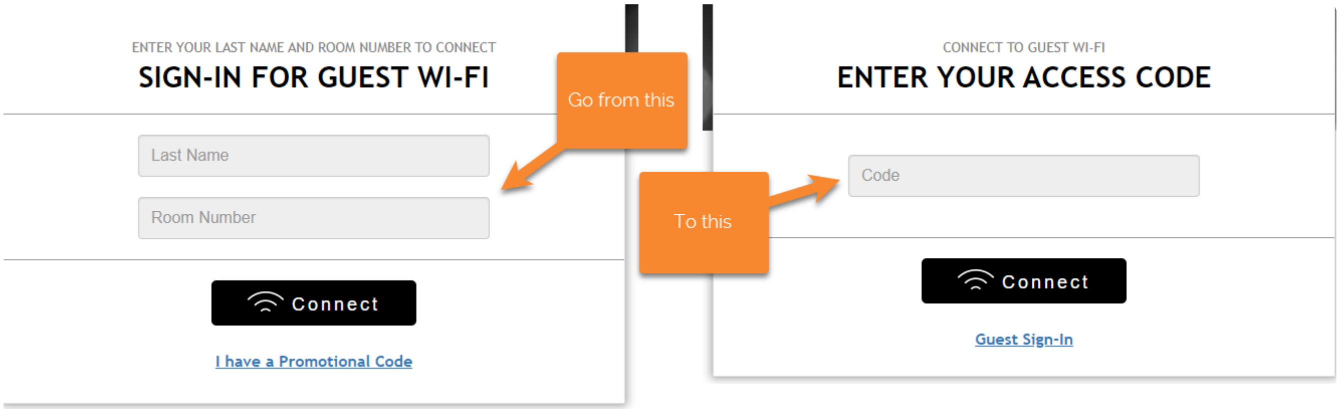
How do I change the default portal page?

Holden Hewett
Updated 6 days ago

Unfollow

Question

How do I change the default portal page?



You may not want to show the Last Name and Room Number option on the default portal page of some or all service areas for some properties. For example, you need to display the access code prompt for public spaces like meeting service areas as the default portal page.

> **Eleven Tip** Access codes are called different names depending on the Portal Manager template you choose for your portal. Some of our partner brands use specific terms for their branding. Below is a list of acceptable terms used for Access Code:
>
> - Access Code
> - Promotional Code
> - Promo Code

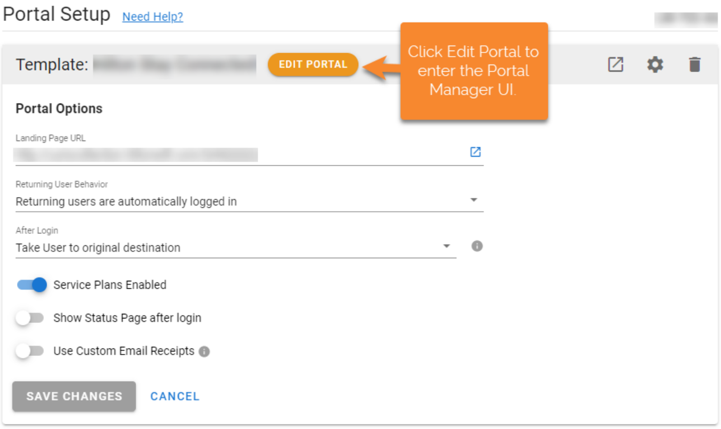
Want to remove alternate login options? Check out the How do I remove alternate authentication options from a portal page? FAQ for more information.

Answer

Follow the steps below to change the default portal page to display the access code prompt:

1. In the ElevenOS Org Tree, navigate to the desired service area.
2. Navigate to **Setup > Portal**.

3. Click **Edit Portal** to enter the Portal Manager UI.



Portal Setup Need Help? [redacted]

Template: [redacted] EDIT PORTAL

Click Edit Portal to enter the Portal Manager UI.

Portal Options

Landing Page URL: [redacted]

Returning User Behavior: Returning users are automatically logged in

After Login: Take User to original destination

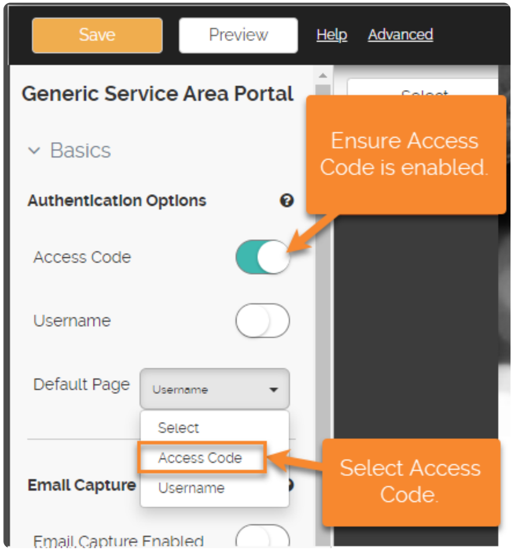
● Service Plans Enabled

○ Show Status Page after login

○ Use Custom Email Receipts

SAVE CHANGES CANCEL

4. In the side menu, expand **Basic Options**.
5. Under Authentication Options, enable **Access Code**.
6. In the Default Page dropdown select **Access Code.**



Save Preview Help Advanced

Generic Service Area Portal

Basics

Authentication Options

● Access Code

○ Username

Default Page: Username

- Select
- Access Code
- Username

Email Capture

○ Email Capture Enabled

Ensure Access Code is enabled.

Select Access Code.

7. Click **Save** and exit Portal Manager.
8. Click **Save Changes** on the Setup > Portal screen.
9. If you need to edit the portal page on additional Service Areas, repeat **steps 1 - 7**.

Was this article helpful?

✓ Yes ✕ No

0 out of 0 found this helpful

Return to top

Recently viewed articles

Related articles

eleven

Community Holden Hewett

Eleven > Setup & Configuration > ElevenOS Documentation

Search

Articles in this section

Understanding RadSec

Holden Hewett
Updated a few seconds ago

Unfollow

What is RadSec?

The RadSec protocol (RFC6614) securely and reliably transports RADIUS requests over insecure or shared networks like at a hotel or airport.

The relationship between RADIUS and RadSec is similar to HTTP and HTTPS. RadSec communications use the same expected level of encryption and security when browsing the internet.

About RADIUS

Before understanding the benefits of RadSec, you must understand the fundamentals of RADIUS first.

Conventional RADIUS uses the unreliable transport protocol UDP, which does not guarantee the delivery of messages. Therefore, RADIUS limits the number of request retransmissions and doesn't guarantee message arrival either. This unreliability sometimes causes RADIUS requests to be lost or dropped on congested networks.

Additionally, conventional RADIUS requests transport the information they contain mostly in cleartext. RADIUS requests include username, IP address, login times, and password (encrypted with a shared secret using a potentially weak encryption algorithm).

Finally, conventional RADIUS cannot prove that the RADIUS server or client is who they say. Therefore, spoofing RADIUS servers and clients using UDP-based RADIUS proxying is relatively easy. As a result, it allows threat actors to gain valuable information about a network or its users.

About RadSec

With RADIUS fundamentals out of the way, let's look at how RadSec solves the shortcomings of RADIUS.

First, RadSec uses the TCP/IP transport protocol to send RADIUS request messages reliably, eliminating lost or dropped requests due to network congestion. Second, TCP/IP transport also makes the RADIUS communication stream tamper-proof; altering or removing RADIUS requests cannot occur undetected.

Next, RADIUS encrypts requests with Transport Layer Security (TLS). TLS is a much more robust encryption algorithm than conventional RADIUS uses. It encrypts all of the RADIUS request information, not just the password. Thus, any data sniffed while in transit is unreadable by attackers or eavesdroppers.

Lastly, RadSec can provide mutual authentication with Public Key certificates. Using Public Key certificates validates the client and server of RADIUS communications, preventing spoofing or masquerading of proxy RADIUS servers and clients.

Was this article helpful?

✓ Yes ✕ No

0 out of 0 found this helpful

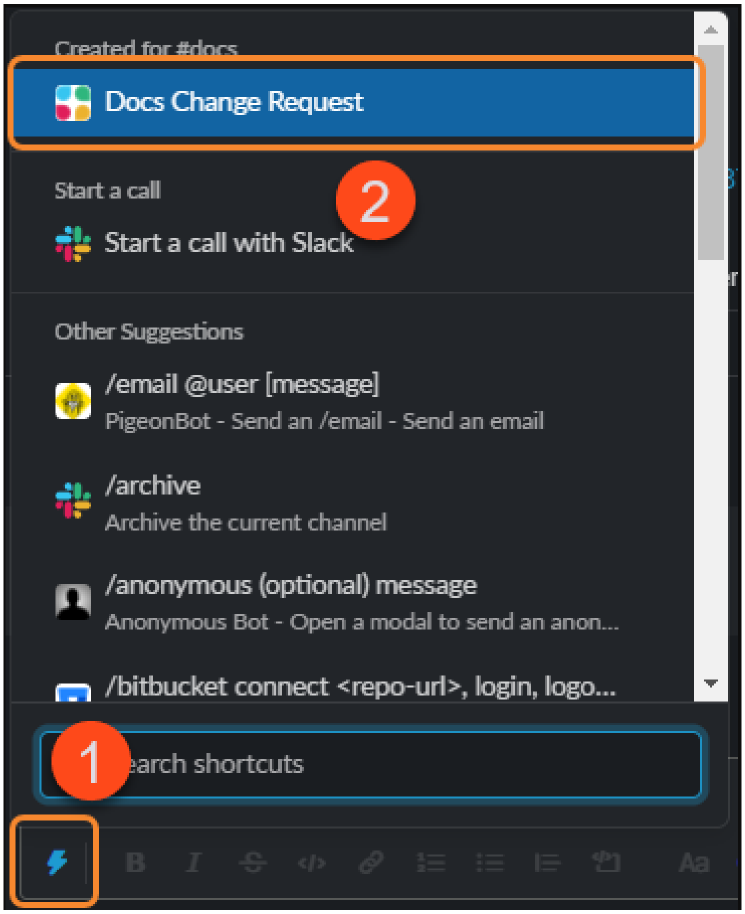
Documentation Change Request Memo

The Docs team has updated its process for internal documentation change requests. Please familiarize yourself with the new process below. Moving forward, please do not direct message the Docs team directly for any documentation change requests. It is challenging for the Docs team to keep track of direct messages in Slack, email, or other means. This new process centralizes all documentation requests, allowing the Docs team to prioritize and keep track of all submissions. The main benefit of this is that your documentation change requests aren't forgotten and have higher visibility within the Docs team.

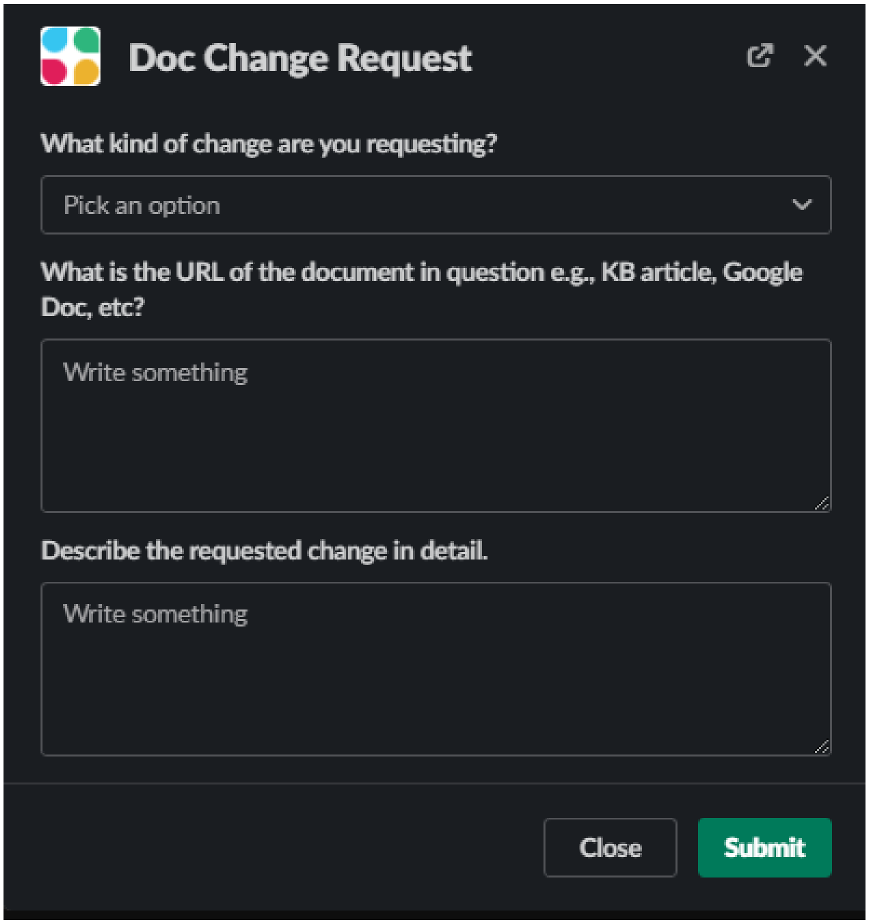
The Docs team is open to feedback in making this process as easy as possible for Elevenites to let us know about documentation related to creating new documentation, bugs, updates to screenshots, and more.

How to Submit a Docs Change Request

1. In the Slack **#docs channel** message box, click the **Shortcuts (lightning bolt)** button.
2. Select the **Docs Change Request** shortcut.


Created for #docs
Docs Change Request
2
Start a call
Start a call with Slack
Other Suggestions
/email @user [message]
PigeonBot - Send an /email - Send an email
/archive
Archive the current channel
/anonymous (optional) message
Anonymous Bot - Open a modal to send an anon...
/bitbucket connect <repo-url>, login, logo...
1
earch shortcuts
Aa

3. In the **Doc Change Request form**, fill out all fields to the best of your ability.



Doc Change Request

What kind of change are you requesting?

What is the URL of the document in question e.g., KB article, Google Doc, etc?

Describe the requested change in detail.

4. Click **Submit**.
   This submits the request as a message to the #docs channel and sends a direct message to the Docs team that you have a pending request.

Error 406 History

Error 406 is continuing to frustrate the CustomerX support team. During the new resident onboarding process at sites using the MDU PPK portal template, error 406 is displayed to residents with several different causes. Despite being heavily documented, error 406 is still challenging for property managers, Eleven Software integrators, and even Eleven Customer Success (CS).

CustomerX's frustration comes from not having enough direction from the error message or our documentation to triage or escalate to their programming team when necessary. There are at least nine different causes for error 406 to occur. The main problem is that CustomerX's teams have varying levels of access to Site Manager, ElevenOS, or the network hardware, making it difficult to fix the problem when the error message is generic and provides no concrete information.

The latest example of CustomerX's frustration is illustrated in the snippet from ticket### below (snippet removed). Even though CustomerX has access to nine known causes of error code 406 during the resident onboarding process, they still need to contact Eleven support to determine the exact cause so they don't escalate unnecessarily to their internal teams. The process is as follows:

1. First, the resident contacts the property manager to resend the invitation link per the instructions in the error 406 message.
2. Together, the resident and property manager find that the link still doesn't work even after resending the invitation email.
3. Next, the property manager calls CustomerX support to repeat the troubleshooting steps they just tried with the customer.
4. Then, the property manager and CustomerX perform even more troubleshooting steps from CustomX's support decision trees.
5. CustomerX then calls Eleven CS, who then requests the invitation link from the resident. This step can take days.
6. Eleven CS opens the resident's invitation link and looks in browser developer tools to find the internal error message, revealing the actual problem.
7. Finally, Eleven CS gets back to tell CustomerX what the actual problem is and how to fix it.

This process takes up everyone's time, is inefficient and frustrating, and could be streamlined should we decide the effort to improve the error 406 messaging is worth it.

Improvement Ideas

Since multiple audiences view error messages, the end-user (resident) mustn't be confused by a lingo/jargon-heavy error message. The CS team and I have come up with the following ideas to make error code 406 be more practical and more accurately identify the problem causing it:

- Change the error message wording
- Add sub-codes to the error message modal

Change the error message wording

Not long ago, our engineers released a code to allow all invitation links to remain valid no matter how many times a new link is sent. As a result, suggesting sending a new link is now an inefficient and redundant troubleshooting step. Instead, we could update the Invalid Link error (code 406) to remove the mention of sending another link and add something about the property manager contacting their network administrator for assistance.

Add sub-codes to the error message modal

When error 406 is displayed to an end-user, the cause for error 406 is already available in browser developer tools but is not shown to the end-user. Currently, our documentation does not mention how to view this internal error message as we do not want this to be a common practice for CustomerX. Could we somehow leverage that internal error message in the end-user-facing error message, as seen in the screenshot below (screenshot removed)?

Could we change error code 406 to include sub-codes? 406-1, 406-2, 406-3, etc? For example, 406-1 could be an incorrect PAN mapping, and 406-2 could be no VLAN found on the controller. When the resident provides that sub-code to the property manager, they can call the integrator (CustomerX or soon to be many more integrators/partners) who could reference an article in our knowledge base that explains each sub-code in the Eleven KB.

This process would be more efficient for everyone involved. Of course, it won't solve all our problems, but it could make it less frustrating from a user experience perspective.
Could the error message in browser developer tools be put in the clickable (easter egg) error code in the modal, as seen in the mockup image below (screenshot removed)?