

Customer Release Notes

Product Extreme Defender Application

Software Version 03.41.14

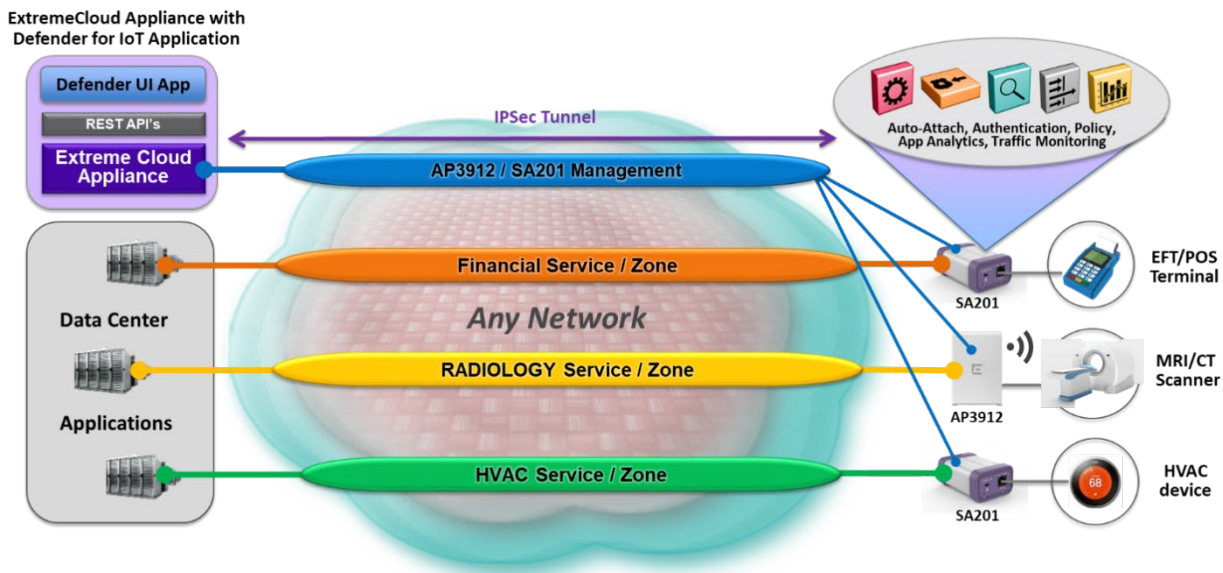
May 19, 2020

INTRODUCTION

This document provides specific information for Extreme Defender Application software version 03.41.14.

Extreme Defender Application is a Docker-based application that operates with the ExtremeCloud Appliance to provide streamlined IoT security functions. Defender Application 03.41.14 supports the Defender Adapter (SA201) and the WLAN AP3912 access points to apply and manage security policies to IoT devices.

The Defender Application is downloadable to the ExtremeCloud Appliance and provides the added capability of easy inventory management of devices protected by the Defender Adapter (SA201) and AP3912 access points.



Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest software versions, visit the download site at:
www.extremenetworks.com/support/

SOFTWARE SPECIFICATION

Status	Version No.	Type	Release Date
GA Version	03.41.14	Feature Release	May 19, 2020
Maintenance Release	03.31.07	Maintenance Release	March 26, 2020
GA Version	03.31.06	Feature Release	September 2019
GA Version	03.21.06	Feature Release	July 2019
Maintenance Release	03.01.54	Maintenance Release	May 2019
Maintenance Release	03.01.19	Maintenance Release	December 2018
GA Version	03.01.16	Major Release	October 2018
Beta	03.00.21	Beta Release	September 2018

INSTALLATION AND CONFIGURATION NOTES

Note:

Defender Application installation has been simplified using the ExtremeCloud Appliance.

From the ExtremeCloud Appliance user interface, go to **Administration > Applications**, select the plus sign icon and follow the installation dialog to install Extreme Defender Application.

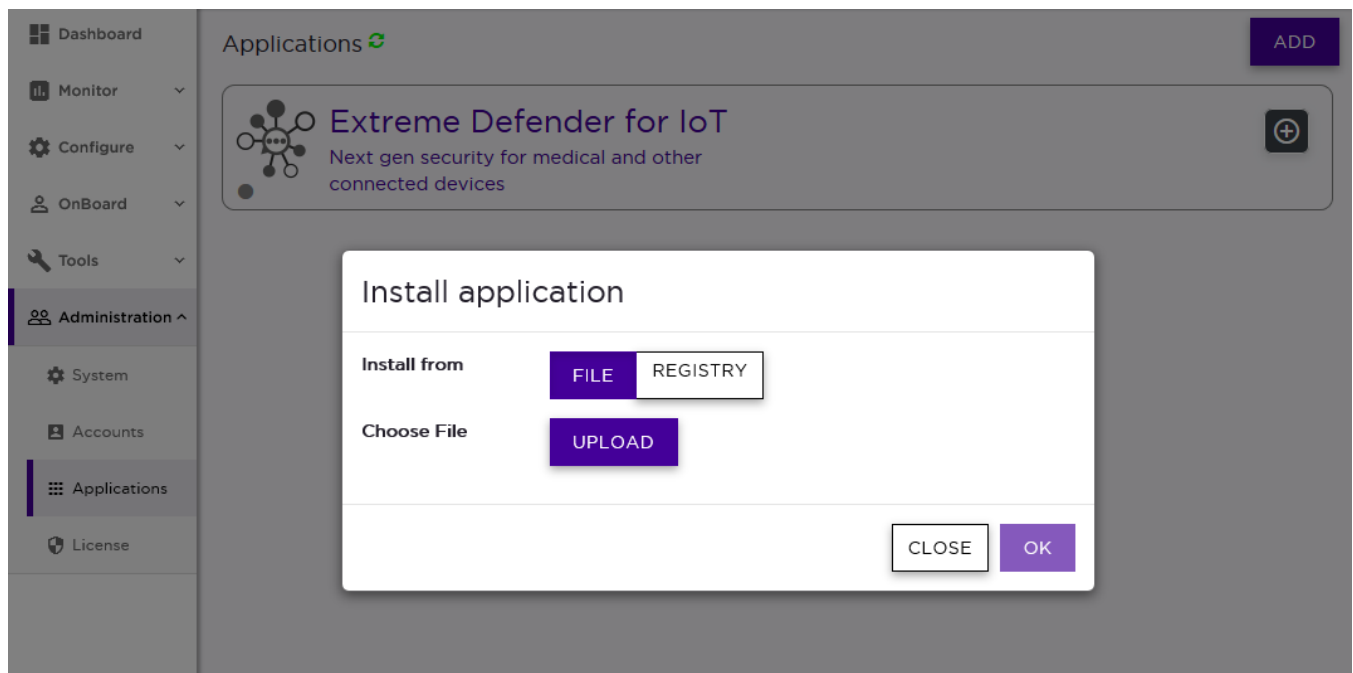


Figure 1: Install Defender by Uploading Application Docker File

Note:

Defender Application 03.31.06 (or later) requires the user to generate and upload an API key prior to accessing the application.

To generate the API key:

1. From the ExtremeCloud Appliance user interface, go to **Administration > Accounts**.
2. Select a Full Admin user, then select **Generate API Key**.
3. Download the generated API key as a file.

To upload the API key:

1. From the ExtremeCloud Appliance user interface, go to **Administration > Applications**.
2. Select the **Show application stats** icon for Defender Application.
3. Select the **Configuration Files** tab.
4. Click on the “**api-keys.json**” file name and select the **Upload** icon to upload the generated API key.

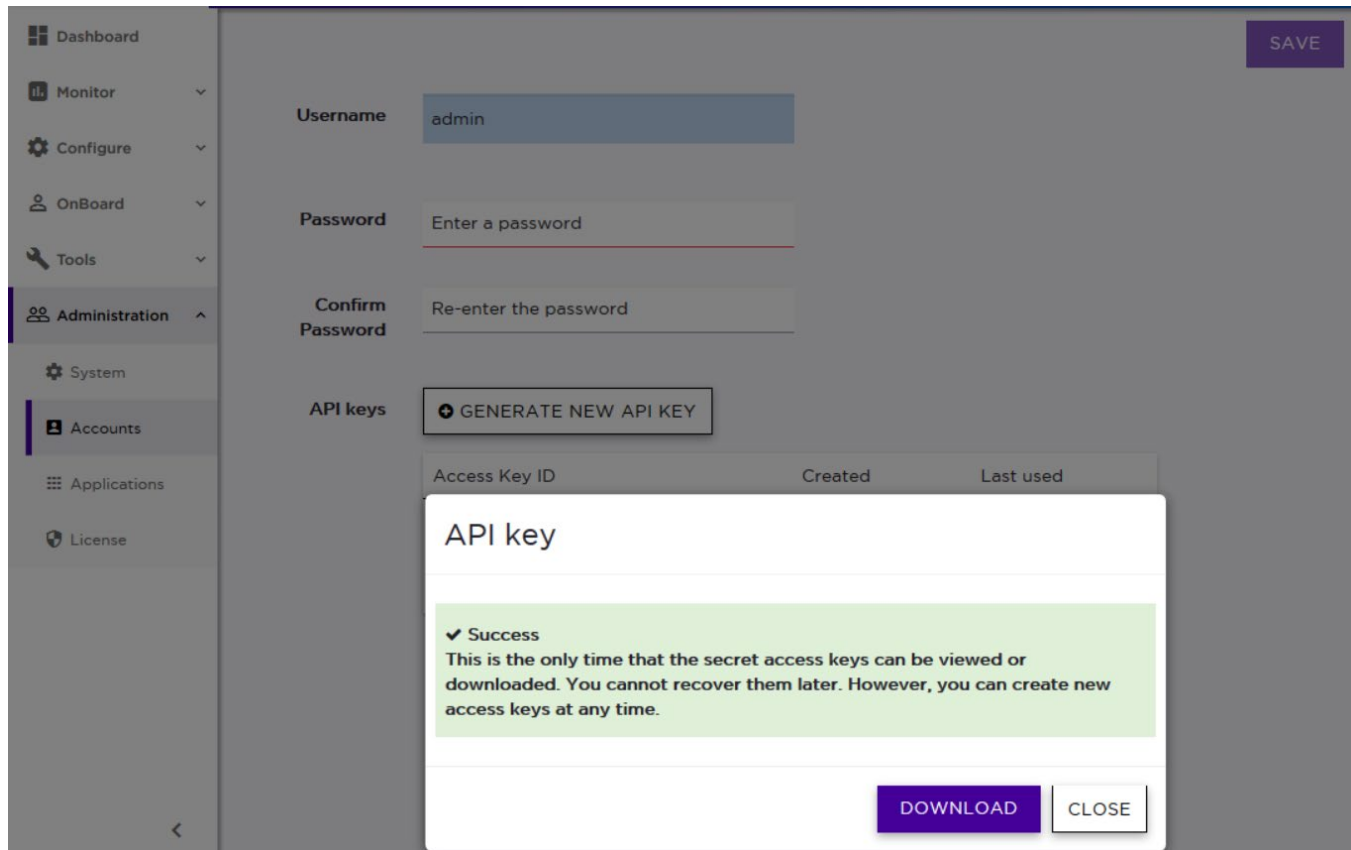


Figure 2: Generate and Download API Key for Full Admin User

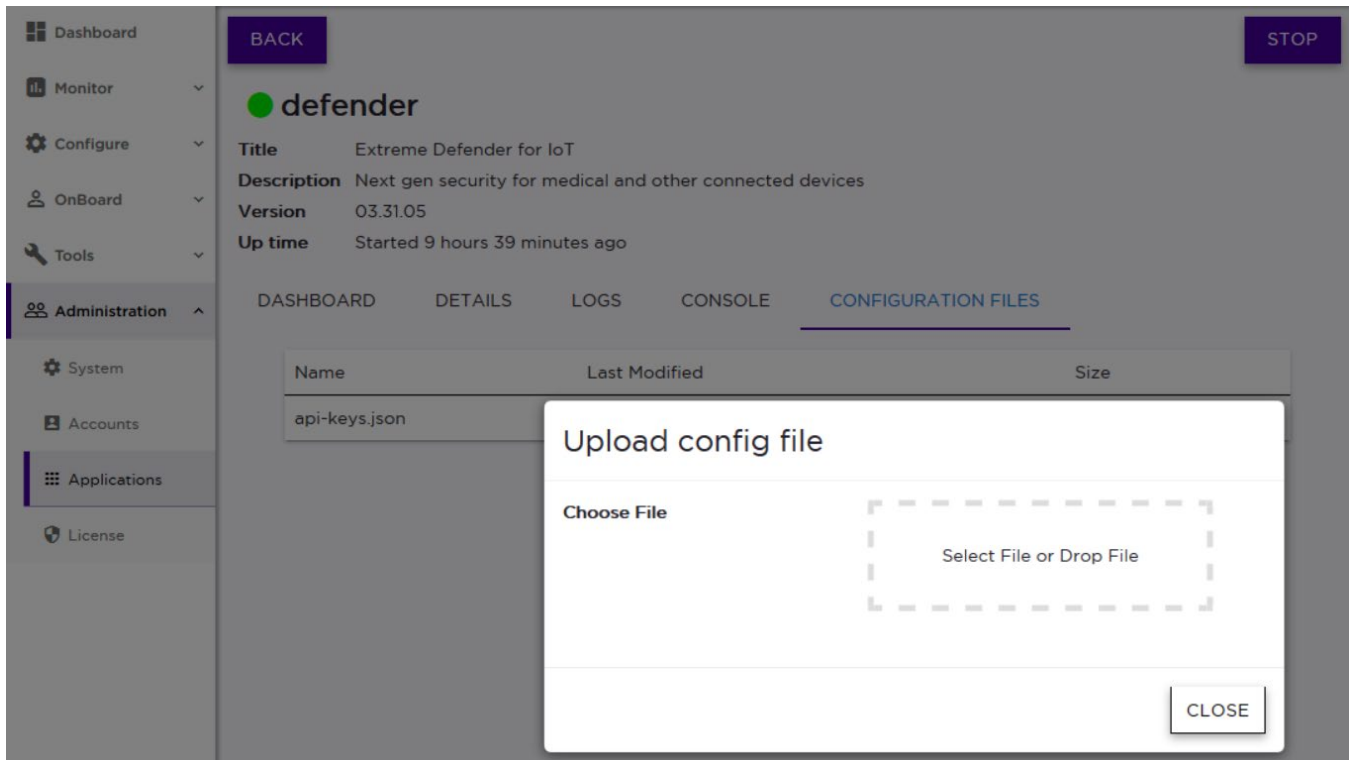


Figure 3: Upload Generated API Key for Defender Application

ENHANCEMENTS IN 03.41.14

This release requires ExtremeCloud Appliance release 4.76.04 or later. Please upgrade the ExtremeCloud Appliance prior to upgrading or installing Extreme Defender Application.

Provided event management capability that allows administrators to receive email notification events related to the status of managed Inventory or *Protected* Devices:

- Inventory (Defender devices) change of status (Active->Inactive)
- Protected Devices (end-systems) change of status (Active->Inactive), (Inactive->Active)

Provided an audit trail capability to record all configuration changes within the application made by the administrator, such as changes in Roles, Policy and Group extensions, managed device attributes, and licenses.

Provided a configuration backup function that allows you to export configuration settings to the managing host and restore the configuration. Configuration settings include: Inventory details, Device details, and licensing state or licenses.

Extended the application capacity to support 10,000 devices/clients.

ISSUES FIXED IN 3.31.07

ID	DESCRIPTION
DEFENDER-334	Improved synchronization with ExtremeCloud Appliance (host instance) addressing situations where client may be attached and displayed on the appliance, but not listed in the Defender Protected Devices view.

ENHANCEMENTS IN 3.31.06

This release requires ExtremeCloud Appliance release 4.56 or later. Please upgrade the ExtremeCloud Appliance prior to upgrading/installing the Extreme Defender Application.
Supports local user accounts with three access levels (full-admin, user, read-only) and tag-based device filtering.
Supports L7 rule editing in policy generation.
Removes enforced dependency on DFNDR_SITE to determine whether to re-run wizard. Customer can rename or even delete the DFNDR_SITE site. Supports editing of default site name when running installation wizard.
Supports site selection when onboarding Access Points and Adapters.
Supports adding name and asset ID for protected devices.

ISSUES FIXED IN 3.31.06

ID	DESCRIPTION
nse0003668	Fixed Protected Device table showing inactive device as "not licensed".
nse0003894	Fixed removal of inactive clients.
DEFENDER-246	Added ability for user to rename default site name created by installation wizard.
DEFENDER-260	Enhanced policy editing page to match the policy editing capabilities of ExtremeCloud Appliance.
DEFENDER-282	Fixed client removal processing to update license count correctly.

KNOWN RESTRICTIONS AND LIMITATIONS

There have been occasional reports that following an upgrade, the Extreme Defender Application may display “Container is either not installed or not running”. This issue is currently under investigation and will be addressed in an upcoming release. The recovery workaround at this time is to reboot the host ExtremeCloud Appliance.

In certain cases, It may take up to 50 seconds for the the wireless client information to be shown correctly at the defender page.

GLOBAL SUPPORT

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
<https://extremeportal.force.com/>

By Email: support@extremenetworks.com

By Web: <https://extremeportal.force.com/>

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119

For information regarding the latest software available, recent release note revisions and documentation, or if you require additional assistance, please visit the Extreme Networks Support website.