Extreme Platform ONE Security Okta JIT Integration Guide

Rev 02
November 2025

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

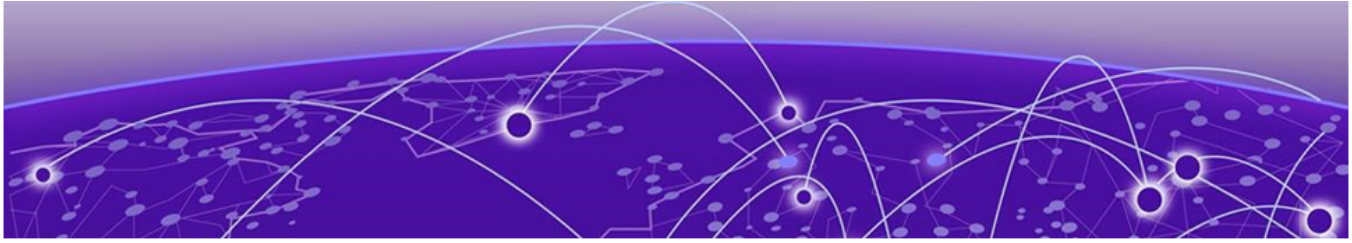


Table of Contents

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

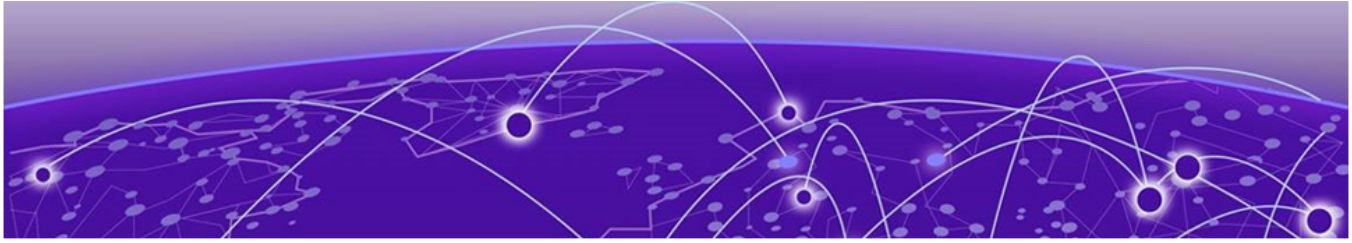
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



Integration Overview

The Extreme Platform ONE Security API Service Integration provides a secure, scalable interface to access your Okta directory without requiring individual user credentials. This integration is primarily designed for automated synchronization of users and groups, ensuring consistent and centralized identity management across the Extreme Platform ONE Security environment.

Synchronize Users and User Groups with Okta

Synchronizing Users and User Groups from Okta is required to ensure policies can be applied to users connecting with Okta credentials in Extreme Platform ONE Security.

Just in Time (JIT) Synchronization – this method has Extreme Platform ONE Security reach into Okta and pull users and user groups on a polled basis. This method leverages an OIDC application to integrate with the Okta APIs.

For JIT integration, the setup in Okta will be completed first, followed by the configuration of Extreme Platform ONE Security.

Configure Okta JIT

1. Sign into your Okta admin console.
2. Go to **Applications** and search for **Extreme Platform ONE Security API Service** under the **Browse App Integration Catalog**.
3. Click the **Add Integration** button.
4. Click **Install and Authorize**.

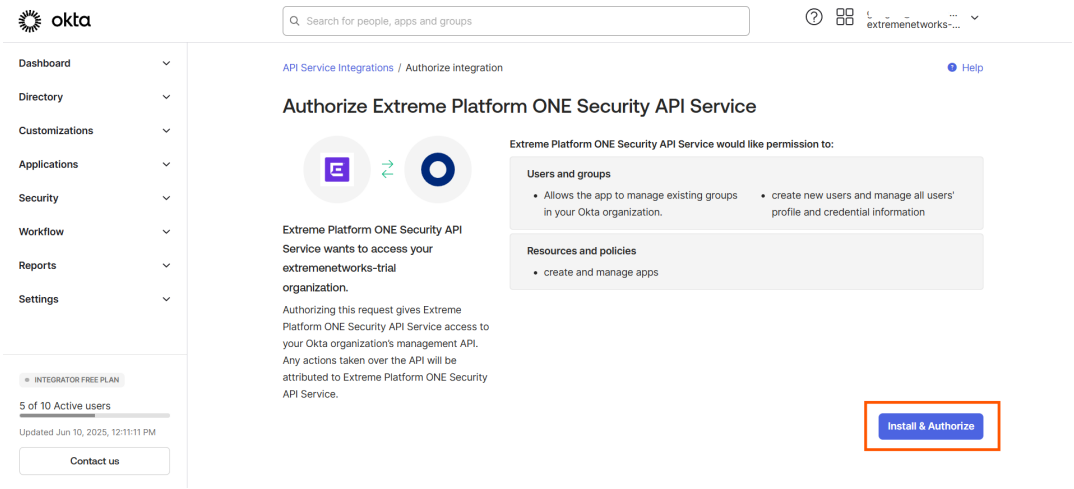


Figure 1: Extreme Platform ONE Security API Service Settings

The following API scopes are automatically applied:

- `okta.users.manage`
- `okta.apps.manage`
- `okta.groups.manage`

5. Note the **API Service Client Secret** for Extreme Platform ONE Security configuration.
6. Click **Done**.
7. Note the **Okta Org Domain** (without the https prefix. e.g. trial-4343365.okta.com) and **API Service Client ID**.
8. Create an OIDC application:
   a. Navigate to **Applications** > **Applications** and click **Create App Integration**.
   b. In the resulting window, select **OIDC – OpenID Connect** as the sign-in method.
   c. For **Application type** enter **Web Application** and click **Next**.
   d. In the **New Web App Integration** window, enter a new integration name in the **App Integration name** field and select **Client Credentials** under **Grant Type**.

      Note
      Leave the rest of the fields to their defaults as current purpose is to sync user and user groups.

   e. Under **Assignments**, in the **Controlled Access** section, select your preferred option or enable **Allow everyone in your organization to access**.
   f. Disable the **Enable immediate access with Federation Broker Mode** checkbox.
   g. Click **Save**.
9. Assign users and user groups that you want to sync.

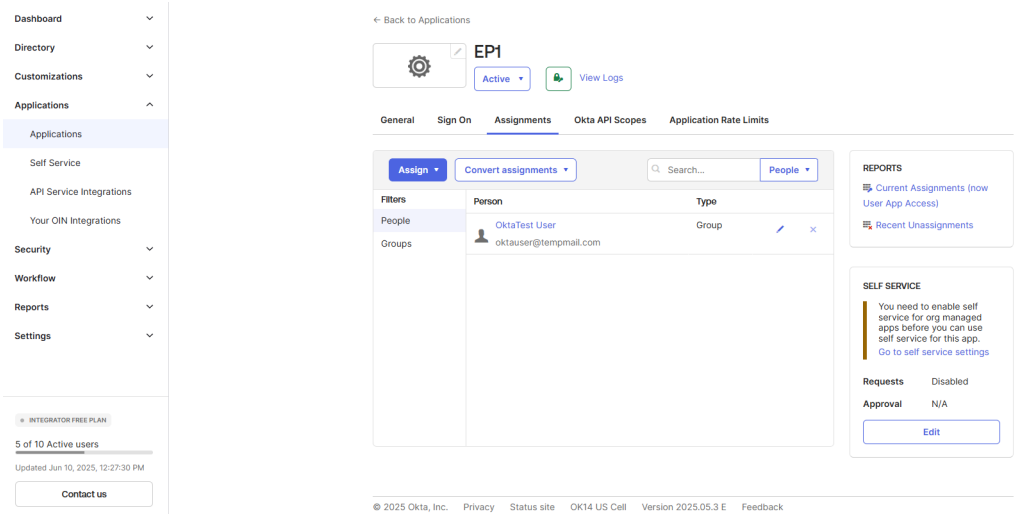


Figure 2: Assign Users and User Groups

10. Copy the OIDC application **Client ID**.

Configure Extreme Platform ONE Security JIT Integration

1. Log into your Extreme Platform ONE Security tenant.

2. Navigate to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. Select **Add IdP Profile**.
4. Fill in the required details:
   - **Set Up IdP** - Select **Sync Users and User Groups** from the Purpose drop-down list.
   - **Approved Domains** - If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**.
   - **Select Identity Provider** - Select **Okta** from the **Identity Provider** drop-down list.
   - **Setup Guidelines** -
     - Select **JIT (Just in Time)** for the **Sync Using** drop-down list.
     - Paste the copied credentials from Okta:
       - API Service Client ID
       - API Service Client Secret Key
       - Application Access Client ID
       - Org Domain
5. Click **Save** to complete the setup.