Self-Led Onboarding Project Plan for User Device Tracker

INSTALLATION

☐ Confirming installation for the Orion® Platform
The first step in the engagement will be to make sure SolarWinds® User Device Tracker (UDT) is installed. If it isn't installed, we'll help guide you through the installation.

☐ Install Orion Platform products in a new environment:
  Documentation

MANAGING NODES/AD IN UDT

☐ How to add nodes to UDT
After installation, the next step is to take any added nodes and make sure they're being monitored with UDT.

☐ Select Orion nodes for monitoring with UDT:
  Documentation

☐ Port Management:
  Documentation

☐ How to add AD to UDT
In this section, we'll show you what credentials are required and how to add your Active Directory® (AD) domain controllers to track users who sign-in to the network.

☐ Manage Active Directory Credentials:
  Documentation

☐ Select an Active Directory domain controller to track user logins:
  Documentation
□ UDT settings

All the individual modules we have for the Orion Platform have their own module-specific settings. At the point, it's also helpful to go over the UDT settings in detail to see what's available.

□ UDT Settings:

  Documentation

NAVIGATING UDT

We'll cover the main widgets displayed here and how to customize the page and dashboards.

□ Device Tracker Summary:

This is the default view when using UDT. You should cover the main widgets that are displayed here as well as how to customize the page and dashboards.

□ Device Tracker:

  Documentation

□ How to locate network devices

One of the main functions of UDT is the search, which allows you to find any user, device, port, etc.

□ UDT Search:

  Documentation

ROGUE DEVICES/WHITE LIST AND WATCH LIST

□ Rogue List

Rogue devices are any endpoints not marked as safe through the rules of the whitelist. In this section, you'll go over the options you have when a rogue device appears on the network.

□ Rogue Devices:

  Documentation
**How to create a White List**

In the section, you will cover the rules on the white list designed to mark devices as safe, which will prevent alerts from triggering for rogue devices.

- **Manage the White List:**
  - [Documentation](#)

**Explain the Watch List**

The watch list allows us to track users and devices in the network, and you'll look at where this information is displayed on the Device Tracker Summary page.

- **Manage Watch List:**
  - [Documentation](#)

**UDT ALERTS**

**Out-of-the-Box Alerts and Best Practices**

In this section, there are a handful of Out-of-the-Box Alerts that come with the installation of UDT. In this section you will learn about these default alerts and how to modify them with best practices.

- **Best Practices With Alerting in the Orion Platform:**
  - [Documentation](#)

**Creating Alerts with UDT**

You have the ability to create your own alerts. In this section you will learn how to create alerts from scratch and how to perform actions like sending emails or creating event logs.

- **UDT Alerts:**
  - [Documentation](#)

- **Configure a UDT Alert:**
  - [Documentation](#)
UDT REPORTS

☐ Review and Schedule Reports

Currently, there are 11 out-of-the-box reports. This section covers best practices and how to modify and schedule the reports.

☐ UDT Reports:
  
  Documentation

☐ Creating/Modifying Reports

Alongside the default reports, you also have the option to create your own. In this section, you'll go over the basics of creating and scheduling reports to meet your needs.

☐ Creating a Web-Based Report in the Orion Platform:
  
  Documentation