Tenable Security Center Security Best Practices Guide

Last Revised: October 03, 2025

Table of Contents

Overview **4**

Pre-Deployment Best Practices **5**

Disk Space Requirements 5

Baseline Strategy 5

Zone Repository Configuration 6

User Management 6

Data Management 7

Post-Deployment Best Practices **9**

License Count 10

Scanning Best Practices 11

Storage Best Practices 12

Steps to Archive Logs 12

Steps to Unarchive Logs 13

Cron Job and Disk Space Clean-up Suggestions 13

Nightly Cleanup 15

Core Tasks of Nightly Cleanup 15

Backups 17

Backup Requirements 18

Backups via Tenable Core 20

Backups via CLI for Tenable Security Center Supported Unix Hosts 22

Migration 24

Pre-Upgrade Steps **25**

Post-Upgrade Steps **26**

Contact Support **27**

Overview

This document describes best practices that provide users a better experience in terms of guidance, recommendation of established methods that help to achieve stability, and efficient management practices.

The document includes the following sections:

- Pre-Deployment Best Practices
- Post-Deployment Best Practices
- Pre-Upgrade Steps
- Post-Upgrade Steps
- Contact Support

> **Note**: This document is not intended to be a rulebook for Tenable Security Center usage, but to provide a baseline and recommendations for the smoother use of Tenable Security Center.

Pre-Deployment Best Practices

This section covers configuration best practices for Tenable Security Center in the pre-deployment phase. The following areas are covered:

- Disk Space Requirements
- Baseline Strategy
- Zone Repository Configuration
- User Management
- Data management

> **Important**: Each area or concept is explained in detail and must be regarded as guidance rather than strict rules when using Tenable Security Center. However, disk space requirements are non-negotiable, and Tenable strongly recommends that you make sure that disk space is appropriately allocated to prevent any database corruption.

Disk Space Requirements

The capacity required for a Tenable Security Center deployment varies depending on several variables. For guidance for the storage requirement for a specific scenario and the amount of active IPs, see Disk Space Requirements.

This, however, should be taken as a baseline, as the actual storage needed by Tenable Security Center fluctuates depending on the overall activity.

Tenable Core + Tenable Security Center OVA Specification

OVA image has a default disk size of 250 GB. This may not suffice to satisfy your organization’s requirement and you may need to expand the disk space. For more information about adding and expanding disk space in the Tenable Core + Tenable Security Center setup, see Add or Expand Disk Space in the Tenable Security Center documentation.

Baseline Strategy

After the disk space requirements are identified, the next approach is to establish a baseline on how much disk space Tenable Security Center consumes in production. This is important for future disk requirements, backup size estimations, and other scenarios where such information is valuable. The following are the scenarios where disk space is consumed:

- Identify the type and number of scans being run on a daily, monthly, quarterly, and yearly basis.
- Reports that are being generated and kept.
- Frequency of backing up the system and storing it locally.
- Trend data (for example, trending line charts and trending area charts).

The baselining is flexible and can be done in various ways, as long as the goal, which is to know the periodic graphical storage consumption, is achieved.

Zone Repository Configuration

There are various options for how data is stored in Tenable Security Center, such as combining data types into a single repository or separating them out. An example is splitting Vulnerability Assessment, Nessus Network Monitor, and Compliance Audit scan results into different repositories, so that you can delete or manage these different sets of data easily.

> **Note**: The maximum repository size is 64 GB. For best performance, Tenable recommends splitting repositories larger than 32 GB. For more information, see Repositories in the Tenable Security Center documentation.

User Management

Tenable Security Center uses Organizations, Groups, and Roles to define user permissions.

Tenable recommends working with one organization as much as possible, unless you have specific requirements for managing your users. For example, if there are users located in different geographical locations, you may want to create one organization per location. This ensures proper data segmentation when users are attempting to access data or resources in Tenable Security Center. For more information, see Organizations.

Groups provide more granularity for user permissions. Tenable recommends using different Groups to provision permissions for objects to different users, based on the level of access that they require. For more information, see Groups.

Lastly, Tenable recommends using the eight system-provided roles as much as possible, without creating custom roles unless necessary. You may find it more efficient to use the system-provided roles as these roles cover most use cases. For more information, see Roles.

For TNS-authenticated users, Tenable recommends implementing the following for increased account security:

- Enable the **User Must Change Password** option to ensure users change their password upon initial login.
- Inform users to set their passwords with sufficient complexity — 9 to 12 characters with at least one uppercase letter, one lowercase character, one special character, and one number. This can be enforced using the **Minimum Password Length** and **Password Complexity** options.
- Enable the **Password Expiration** option in line with your organization's existing password expiration policy.
- Enforce account disabling for inactive users using the **Days Users Remain Enabled** option.
- Enforce account lockout for too many failed login attempts using the **Maximum Login Attempts** option.

For more information about these account security options, see TNS User Account Options and Security Settings in the Tenable Security Center documentation.

> **Note**: LDAP and SAML user accounts must have account security enforced by the System Administration team.

Data Management

All Tenable Security Center repositories have Vulnerability Data Lifetime settings. The default value for data retention period is 365 days (other than passive vulnerability data, which has a default value of 7 days). The more assets you scan, the more data Tenable Security Center has to store and retain in your repositories. Hence, Tenable recommends adjusting this value according to your organization's data retention policies. Consider the disk space required to store all of this vulnerability data for all of your assets.

In addition, all newly created repositories have a default setting of 30 days of trending data. Trending data requires additional disk space, therefore you must adjust the setting for Trending according to your disk space availability as well.

Note: Trending data takes up the largest portion of disk space in typical Tenable Security Center deployments.

For more information about the hardware requirements for Tenable Security Center, see Disk Space Requirements in the Tenable Security Center documentation.

Post-Deployment Best Practices

This section includes configuration best practices for Tenable Security Center to achieve smoother usage of the product. The following sections include a comprehensive breakdown of each aspect:

- License Count
- Scanning Best Practices
- Storage Best Practices
- Nightly Cleanup
- Backups

Note: The best practices included in these sections serve as guidelines, rather than rigid rules for post-deployment practices, in Tenable Security Center.

License Count

Tenable recommends that you periodically review your scanned assets and clear old or unwanted assets from Tenable Security Center.

To do this, set the vulnerability lifetime for your repositories. This feature automatically ages out assets after a number of days that you specify. For more information, see the **Vulnerability Data Lifetime** settings for your local repositories and **Data Expiration Configuration** settings.

> **Note:** Tenable Security Center clears the assets after the nightly cleanup process runs.

In addition to using the data lifetime and expiration options to remove vulnerabilities in the repositories, you can enable the **Immediately remove vulnerabilities from scanned hosts that do not reply** option in your Active Scan settings to clear stale assets or unresponsive hosts.

Depending on your organization’s policy and age-out configuration, you can perform this activity quarterly. This practice helps you identify accidental scanning activities when you detect a sudden spike in license count usage.

Scanning Best Practices

Tenable recommends that you read the Tenable Security Center Scan Tuning Guide before configuring your scans.

For quick scans, Tenable recommends using pre-defined scanning templates available in Tenable Security Center. This reduces the need for you configure detailed scan settings. Select the scanning template that best suits your scanning requirements. For most use cases, the **Basic Network Scan** and **Advanced Scan** templates are sufficient. For more information about scan templates, see Scan Policy Templates in the Tenable Security Center documentation.

If you are using repositories that are not Universal Repositories, and you are scanning static assets (assets that do not change their IP address), disable the **Track hosts which have been issued new IP address** option. If the asset changes its IP address regularly (for example, via DHCP), enable this option. This option helps Tenable Security Center track hosts and merge vulnerabilities to the host asset for the same host. For more information about this option, see Active Scan Settings.

Tenable recommends keeping the **Enable safe checks** option (which is enabled by default for all scan policies) enabled, as this helps to prevent unnecessary scan target or service outages stemming from the scanner attempting to exploit a vulnerability that may have an adverse impact on the target. For more information about this option, see Scan Policy Options.

If you are using assets instead of IP address or DNS name to define scan targets, ensure that you first build your inventory list using a **Host Discovery** scan, according to the Troubleshooting Scan Error "Entered IPs and Assets are empty" knowledge base article, so that you do not run into an error where Tenable Security Center shows empty IP addresses and assets.

Storage Best Practices

The following are some of the storage best practices that you can follow in Tenable Security Center:

Reports

Generated report housekeeping is encouraged as these files do not age out and need to be manually removed. Old reports unnecessarily consume a considerable amount of disk space. You can adjust the Data Expiration Settings and the default value is 365 days.

Tenable Security Center Backup

It is a good practice to store the backup of Tenable Security Center on a backup server other than where it is installed. This not only assists in freeing up disk space, but also avoids a single point of failure.

Storage Housekeeping

Overall, storage housekeeping is essential to maintain Tenable Security Center's performance, security, and overall health. It promotes efficiency, stability, and a positive user experience while reducing potential risks and issues.

For better understanding what Tenable Security Center logs consist of and to assist the administrator in decision-making on log file deletion and archiving, the following articles describe log file contents, which files can be removed, and how to delete them in detail:

- An overview of Tenable Security Center application logs
- Free up disk space in Tenable Security Center

Archiving depends on your organization's policy. Tenable recommends that you can keep at least two months' worth of logs while archiving at least one year period of logs to free up disk space and storing it to a secured backup server for future use.

Steps to Archive Logs

In this example, the Administrative logs for March 2023 and April 2023 is archived.

1. Navigate to the Administrative logs directory and run the command to archive the logs:

   ```
   #cd /opt/sc/admin/logs
   #tar -zcvf Archived-File-Name.tar.gz YYYYMM.log YYYYMM.log
   ```

2. Move these files to the backup server.

Steps to Unarchive Logs

In this example, the Administrative logs for March 2023 and April 2023 is unarchived.

1. Move the *Archived-File-Name.tar.gz* file to the Administrative logs directory.

2. Browse through the Administrative logs directory where the archived file was moved, then run the command to unarchive the logs.

   ```
   #tar -xzvf Archived-File-Name.tar.gz
   ```

Cron Job and Disk Space Clean-up Suggestions

Periodically, the Tenable Security Center may encounter instances of insufficient disk space. In such situations, Tenable recommends that you adhere to these recommendations to clean up the outdated data.

> **Tip**: Tenable recommends that the Tenable Security Center folder is routinely cleaned up every 30 days to ensure that the disk space does not grow out of control.

The following files are safe to be removed:

- The leftover `feed.xxxxx` files in the directory */opt/sc/data*.

Tenable Security Center generates the feed files during the feed update and these are removed when the feed update completes. If such files are present, it indicates that there might be connection issues to the feed server. These files are safe to be removed. Only the most current file must not be removed.

It is safe to remove the `feed.xxxxx` file, which is more than one hour. If a feed update is in progress, then you cannot remove that file.

For a list of files that can be safely removed, see the What Touch Debug Files Are Safe to Delete? knowledge base article.

The following are some other files that you can remove:

- Older `application.db` and `plugins.db` under `/opt/sc`.
- Older log files and touch debugging files.

Nightly Cleanup

The Tenable Security Center nightly cleanup is a scheduled task that operates at 0020 hours (12:20 AM) each night, which allows for the seamless processing of information to get updated without requiring user intervention. The primary goal of this process is to optimize system performance by performing various essential tasks, ensuring a smooth and efficient working environment.

Core Tasks of Nightly Cleanup

The nightly cleanup process involves several pivotal tasks aimed at maintaining the quality and efficiency of Tenable Security Center operations:

Data Removal

The nightly cleanup process is responsible for removing diverse types of data that have exceeded their expiration dates. This includes asset and scan data, as well as trending data that is no longer relevant. The removal of redundant data optimizes storage space and prevents the accumulation of irrelevant information, ensuring that the system operates with maximum efficiency.

Removal of Miscellaneous Files

In addition to data removal, the nightly cleanup process targets the removal of miscellaneous files on the system's backend. This includes logs and other files that may accumulate over time. The removal of these files contributes to freeing up disk space and further enhancing system performance.

To derive maximum benefit from the Tenable Security Center nightly cleanup, Tenable recommends organizations to adhere to the following best practices:

Scans Timing

To mitigate potential performance impacts, schedule the vulnerability scans and other resource-intensive tasks after the nightly cleanup process is complete. This ensures that system resources are available for scan execution, minimizing any operational disruptions and optimizing scan efficiency.

Regularly Monitor Disk Space

Regularly monitor the available disk space to ensure that the nightly cleanup process is effectively freeing up storage resources. Maintaining an optimal level of free disk space is crucial for overall system performance and stability.

Accuracy of the System Time Zone

It is essential to recognize that the nightly cleanup job's execution time is set based on the system's time zone during installation. This means that if the system's time zone changes post-installation, the execution time remains unaffected. Organizations must keep this in mind while scheduling tasks to align with the nightly cleanup.

Backups

It is assumed that you already have a schedule for system backups as per your backup policies. Tenable recommends that, at minimum, the system back ups are more frequent than once a month as Tenable Security Center releases upgrades on a quarterly basis.

Tenable recommends performing backups before you perform these common scenarios:

- Tenable Security Center upgrades
- OS upgrades
- Any hardware / OS changes to the Tenable Security Center host
- Modifications recommended by Tenable Support

Tenable advises against modifying the Tenable Security Center databases on your own. Tenable Support engineers may provide SQL commands from the Tenable Security Center developers to modify the Tenable Security Center databases as part of the troubleshooting process. Steps provided may include backup steps that are more specific, before running the SQL commands, though a full backup can also be considered.

Backup Requirements

Before you back up your Tenable Security Center system, do ensure the following:

- All Tenable Security Center services are stopped

To stop Tenable Security Center and all running jobs manually, you can follow these steps:

1. Stop Tenable Security Center:

   ```
   # systemctl stop SecurityCenter
   ```

2. Check if there are any processes still running:

   ```
   # ps -fu tns
   ```

3. If any processes are listed, run the following commands to stop them:

   > **Note**: Killing the process stops all running processes, including scans that are currently running. Since this is typically the last resort, Tenable recommends that you wait for around 30 minutes to allow all pending tasks to be completed.

   ```
   # killall -u tns
   # killall httpd
   ```

4. Repeat the process until there are no Tenable Security Center processes running.

Tenable Core backup tasks attempt to stop all Tenable Security Center jobs before starting, so avoid having any Tenable Security Center scan jobs scheduled around the same time, and allow enough buffer time for the scan to finish before the scheduled backup time.

- Avoid having any resource-intensive jobs around the same time to prevent resource contention
- Sufficient disk space on the host

For Tenable Core:

It is assumed that you have configured remote storage as per the steps in Configure Storage for Tenable Core Backups.

Before transferring the backup to the remote store, Tenable Core first compresses the contents of the resource chosen for the backup on `/opt/tenablecore/backup/tmp`. This means the free storage on the `/opt` partition of Tenable Core must be twice the total occupied space of the `/opt/` directory for the initial compression to succeed.

That is, if Tenable Security Center is 2 GB, `/opt` needs a minimum of 4 GB free space.

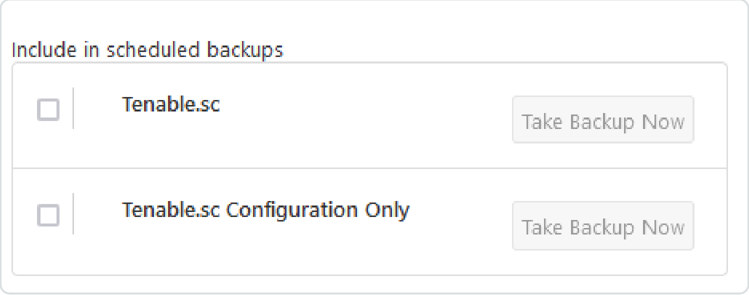
For more information, see the Tenable Core remote backup fails with error 'Not enough space to take the requested backup' knowledge base article.

For Tenable Security Center supported Unix hosts, Tenable recommends similar amounts of free space to avoid the archival commands running into errors due to insufficient disk space.

Backups via Tenable Core

To perform a backup of Tenable Security Center data (as per the steps in Perform an On-Demand Backup):

1. Log in to Tenable Core via the user interface.
2. In the left navigation bar, click **Backup/Restore**.
3. To take an ad hoc backup, in the **Available modules** section, check the type of backup, then click **Take Backup Now**.

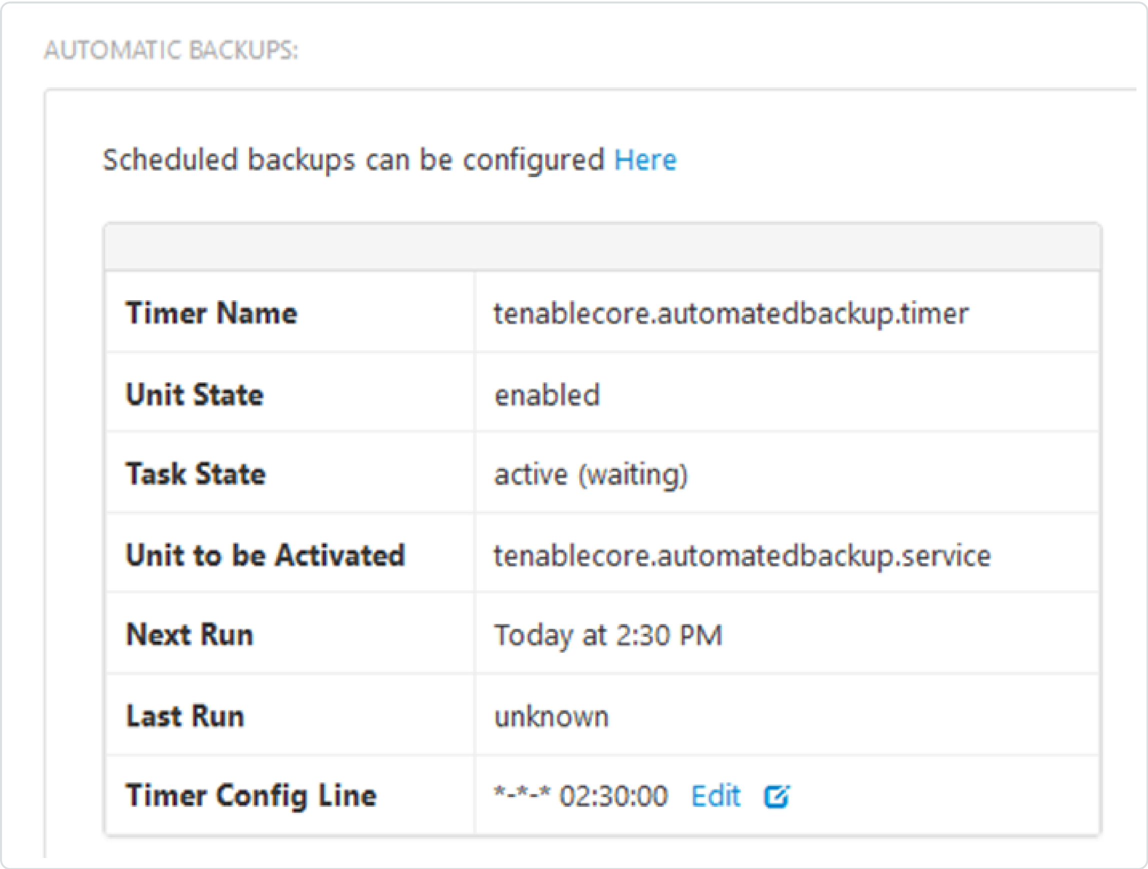
   

   Tenable Security Center — This takes a full backup.

   Tenable Security Center Configuration Only — Configuration backups only back up Tenable Security Center configurations as detailed in Configurations Included in a Configuration Backup.

   > **Note**: Configuration backups do not include data such as vulnerability data, trend data, licenses, or secure connection settings.

For scheduled backups, edit the **Timer Config Line** accordingly in **Automatic Backups**.



AUTOMATIC BACKUPS:

Scheduled backups can be configured Here

Timer Name	tenablecore.automatedbackup.timer
Unit State	enabled
Task State	active (waiting)
Unit to be Activated	tenablecore.automatedbackup.service
Next Run	Today at 2:30 PM
Last Run	unknown
Timer Config Line	*-*-* 02:30:00 Edit

Backups via CLI for Tenable Security Center Supported Unix Hosts

The following steps describe how to perform backup for Tenable Security Center from the command line using a root account (or equivalent access) on Unix hosts. This can also be used as an alternative for Tenable Core backup, if remote storage is not available.

To access the CLI with root level access on Tenable Core:

1. Access the command line by logging in as an Administrator to the Tenable Core user interface.
2. Check **Re-use administrative privileges** or switch to administrative access.
3. Go to the terminal.
4. Escalate to root access using the following command:

   ```
   # sudo su
   ```

5. Retype the password.
6. In root CLI, stop all Tenable Security Center services. To stop Tenable Security Center services, follow the steps provided in Backup Requirements.
7. Once all Tenable Security Center steps are stopped, proceed with the archival of the Tenable Security Center folders.
8. Backup Tenable Security Center folder:

   ```
   # tar -pzcf sc_backup.tar.gz /opt/sc
   ```

9. (Example) To move the file to another location for easier retrieval, move the file to `/tmp`:

   ```
   # cp sc_backup.tar.gz /tmp
   ```

10. Change its ownership:

    ```
    # chmod 755 sc_backup.tar.gz
    ```

11. Access the host via an SFTP client.

12. Copy the file, and delete it afterward as needed to free up disk space.

For more information, see Perform a Backup.

Migration

For migration between hosts with operating systems that are different, Tenable recommends using Tenable Core. For more information, see Cross-Machine Migration for Tenable Core + Tenable Security Center.

If you do not use the Tenable Core method, ensure that the restore is to the same operating system type and version (for example, CentOS 7 to CentOS 8).

Pre-Upgrade Steps

Follow these steps before you upgrade Tenable Security Center:

Check Release Notes for Upgrade Paths and Tenable Security Center Version

See the Release Notes for upgrade paths.

Halt or Complete Running Jobs

Tenable recommends that you stop all running Tenable Security Center processes before you start an upgrade. If any processes are running (for example: Tenable Nessus scans), the following message appears along with the related process names and their PIDs:

"SecurityCenter has determined that the following jobs are still running. Please wait a few minutes before performing the upgrade again. This will allow the running jobs to complete their tasks."

If you get the same message, you can either stop the process manually or wait for jobs to complete before you proceed.

To stop processes, see the steps provided in the Backups section in the Post-Deployment Best Practices.

Perform Backup

Make sure to perform a Tenable Security Center backup before you upgrade. For more information, see Backup and Restore.

Post-Upgrade Steps

Follow these steps after you upgrade Tenable Security Center:

Log Monitoring

After an upgrade, Tenable recommends that you check the Tenable Security Center system logs for any error or warning messages. Error or warning messages can be indicators of issues caused by components broken due to the upgrade. For more information about the Tenable Security Center system logs, see System Logs.

Scan Monitoring

Monitor your scans launched from Tenable Security Center for any anomalies after an upgrade. If you notice any of the following symptoms, consider seeking assistance:

- Scans have completed successfully in the past but are not completing (ending in partial status) after an upgrade
- Scans aborting after an upgrade
- Scans taking longer than usual to complete

Contact Support

When you encounter issues with your product usage, Tenable Technical Support is here to help. Refer to the Opening a case with Technical Support - Best Practices knowledge base article for best practices when opening Support cases. This can potentially speed up the entire process.

Tenable enables its customers to choose an appropriate case priority when creating Technical Support cases via the Tenable Community. These priorities range from P1 – P4, with P1 being the most critical and P4 being the least critical. Customers must use their best judgment when applying case priorities to ensure their case gets handled appropriately, and Technical Support may adjust the priority of a case up or down to classify the priority level more accurately. Tenable strongly encourages customers with a P1 critical issue to call Technical Support, to avoid any delays associated with email. Following are some examples to assist customers with setting their case priority.

Priority	Examples
P1 - Critical Product functionality completely degraded – critical impact to business operation	• Product service (excluding agents and clients) will not start • Product inaccessible to all users • Upgrade failures that block users from accessing the product • Tenable Nessus, Tenable Security Center, or Tenable Vulnerability Management cannot scan (that is, all scans error and cannot launch)
P2 - High Product functionality severely degraded – severe impact to business operations	• Reports will not launch or generate • Unable to query vulnerabilities, all dashboards, or all scan results • Linking failure of scanners, LCE, or NNM (excluding agents and clients)
P3 - Medium General errors/issues – product	• Generally the default priority • False positives or negatives

impaired however business operations remain functional	• Scanning and reporting errors • Errors with non-core functionality (asset and target lists, SMTP or LDAP integration) • Plugin update failures • Initial installation and setup issues • Requests for testing upgrades before production installation
P4 - Informational Basic information or assistance with Tenable products – little to no impact on business operations	• How do I? • What ports must be opened for the product to work? • Do you have a plugin that scans for ‘X’? • What IPs count against my Tenable Security Center license? • Do you have ‘X’ feature?