NNT Recommended Change Control Program

A New Net Technologies Whitepaper

Mark Kerrison

CEO - New Net Technologies

www.nntws.com

NNT
SECURITY THROUGH SYSTEM INTEGRITY
NOW PART OF netwrix

Introduction

The purpose of this overview is not to replace existing best practice approaches to Change Management or in any way attempt to re-write existing sensible ITSM Change Management Process such as the formerly labeled ITIL.

In fact, however you choose to implement changes within your IT environment, we recommend at least some process outside of NNT- Change Tracker is established to manage changes specifically within these standard change groups:

- Standard Change & Normal Change
- Emergency Change

> *"If you allow changes to occur within your IT environment without any control, it is impossible to retain a secure and compliant state."*

So why the need for Change Control?

Simply put:

"If you allow changes to occur within your IT environment without any control, it is impossible to retain a secure and compliant state'.

Let's also address a quick point of definition between the term: '***Change Management***' and '***Change Control***'. Change Control, as it relates to this guide, is very different to traditional approaches to Change Management. The latter we recommend should fall within existing prescribed ITSM guidelines for requesting, reviewing and approving changes within your environment. NNT can advise you on best practices for this and we are also able to assist you in the identification and even supply of systems that will help with your Change Management process.

Change Control, however, is defined as the process of understanding and monitoring the actual changes that occur with a specific focus on spotting changes that may cause harm. You can conveniently think of Change Management as the process required to request, review, approve and commission changes, while Change Control is the active analysis of actual changes that have occurred.

> *"NNT FAST Cloud automatically approves the validity of file changes as they occur, resulting in a huge reduction in change noise."*

Need for Change Control Continued...

Change Management, whilst essential, can be seriously flawed from a security standpoint without some form of Change Control. The reason being that Change Management makes the assumption that the changes approved and commissioned by the Change Advisory Board – CAB (The group of people assigned to review and approve changes) are in fact those actually carried out.

This is somewhat compounded by the routine nature within which 'Release & Deployment' occurs. Typically done at the same time & same day weekly.

With best intentions we may have unwittingly created a '***blind spot***'.

Change Control conversely seeks to examine all changes that 'actually' occur and reconcile these with what we expected along with further analysis of the changes to ensure no hidden malware or zero day infections exist.

Simply put, you need Change Control to ensure the changes that are happening aren't harmful.

The NNT Change Control Process Explained

NOTE: This guide is not meant as a user manual. We will reference features and configurations that will require some knowledge of NNT Change Tracker. For help in using or becoming more familiar with NNT Change Tracker, please speak to your Account Representative and we will be delighted to assist and walk you through any of the concepts discussed here.

At a minimum, you will need an up to date copy of NNT Change Tracker. For the very best results, we recommend the inclusion of NNT FAST Cloud along with the NNT Managed Change Control Program, which are both services now offered by NNT to augment Change Tracker specifically to improve Change Control.

For those not familiar, the FAST in NNT FAST Cloud stands for 'File Approved Safe Technology'. This is a solution that leverages external threat intelligence and whitelisted facilities to automatically approve the validity of File Changes as they occur. The result is a huge reduction in '***change noise***'.

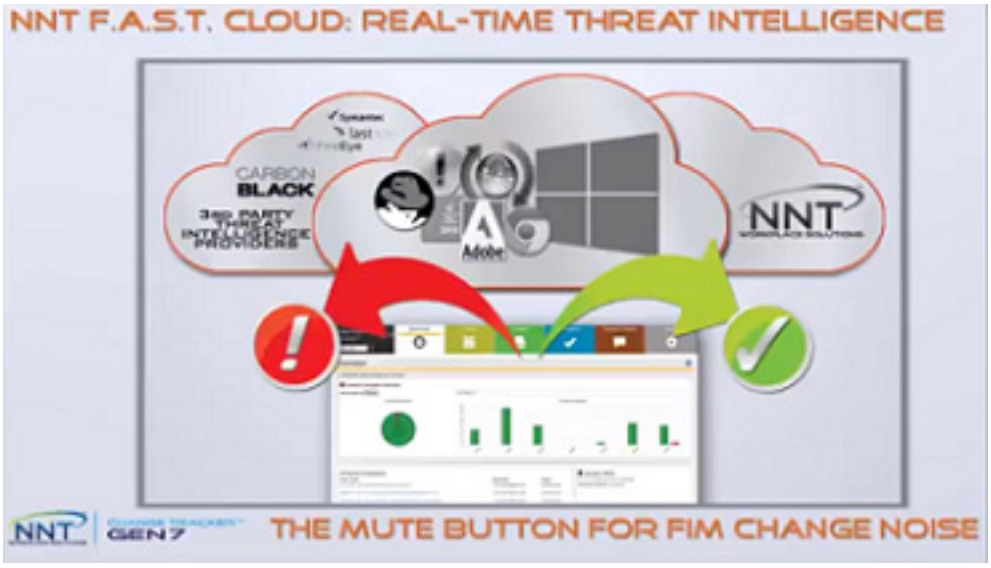


***Figure 1**: NNT FAST Cloud leverages external threat intelligence and whitelisted facilities to automatically approve the validity of File Changes as they occur.*

> *"Whilst the changes may not have been previously examined & approved, we're able to confirm them as 'non-harmful'."*

The NNT Change Control Process Continued...

You can certainly use this guide without FAST Cloud and/or the Managed Change Control Program, but we would strongly recommend these are added if budget will allow.

Within NNT Change Tracker we have adopted the simple principle of 'Planned versus Unplanned Change Detection'.

Planned changes will typically fall into one of the following three categories:

- Changes that were planned & detailed ahead of time but not checked after the event for authenticity: itil v2 'Forward Schedule of Changes' FSC
- Changes that were planned ahead of time that will be checked for authenticity as the changes occur: Standard ITSM FSC combined with NNT Closed Loop Intelligent Planned Change Control System (CLICCS) - Recommended
- Changes that were not planned ahead of time but are approved based on previous knowledge of the changes and their adherence to the criteria for which they were previously approved: NNT Intelligent Planned Change Control System - Recommended

Within these categories you will be able to further define changes, which are unplanned yet acceptable if you are using FAST Cloud. These could include unplanned but whitelisted for example. So whilst the changes may not have been previously examined and approved, we are able to confirm them to be 'non-harmful'.

Unplanned Changes' fall into three prime categories:

- Changes that were non-harmful
- Changes that were harmful
- Changes that were potentially harmful

Given that our main objective is to enhance existing 'Change Management' process and specifically be able to spot harmful or potentially harmful changes, this guide is focused on the 'holds and moves' available to us to better spot & deal with the changes listed above.

This guide pre-supposes that NNT Change Tracker is set up properly, that devices are all listed within defined groups, and that those groups include all relevant policy templates including any associated planned change rules.

NOTE: The set up of NNT Change Tracker at a basic level is key. Lean on the NNT support team to make sure all the right exclusions and policy settings are correct. If you are under the NNT Managed Change Control Program then all of this will be taken care of as a matter of course.

If you aren't sure about the set up of your software and you have a current support and maintenance agreement in place, please speak with your Account Representative and request a free system evaluation. NNT will review the set up of your software free of charge and where necessary introduce additional configuration and/or upgrade to a later version.

Figure 2: NNT Change Tracker works with popular service desk and change management systems such as ServiceNow, Remedy, and ChangeGear, for example.

Stage One- Effective Change Control- Ad-hoc Repeatable, Acceptable, Unplanned Changes

NOTE: This assumes that the NNT Managed Change Control Program has not been purchased and that the user will manage changes independently of NNT consultants. If the NNT Managed Change Control Program has been purchased, NNT will initiate and monitor all of the items below on your behalf.

What we are aiming for is to see absolutely no changes unless there is an associated 'Planned Change Record'. As part of this program, we will be encouraging you to build as much process as you can, in order to reduce or entirely eradicate any changes occurring that cannot be associated with a '***Forward Schedule of Changes***'.

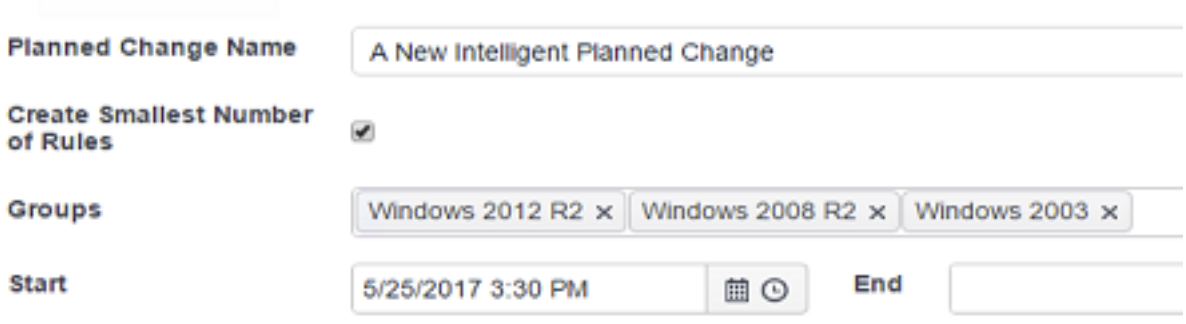
However! Our experience is such that changes may continue to occur outside of any planned change process, which may not be in any way harmful. Therefore, stage one is designed to help you handle these changes. A key component in better handling these would be NNT FAST Cloud, but in the absence of that the following guidelines are recommended:

Once Change Tracker is installed and set up, we will begin to see changes reported. Without any intervention, unless NNT FAST Cloud is being used, these changes will by default be reported as 'Unplanned'.

We recommend a review of the changes with any contextual information provided by NNT such as who made the change, what changed, and where and to start to think about how you would like these fairly random, potentially esoteric changes to be treated in the future.

Changes that you consider to be entirely irrelevant should be excluded. Be very careful here because whilst changes may seem irrelevant to you, they may still be susceptible to attack, particularly the case where file changes are concerned. In these situations we may be better off containing these within an intelligent planned change.

Changes that we regard as normal but likely to be repeated should be added to an '***Intelligent Planned Change Rule***' within the 'Events Screen'. We would recommend that an 'Auxiliary' or 'Reserved' Intelligent Planned Change Category be created to put these changes into. As time goes by, you can add more of these changes into this category and you will notice that the number of unplanned changes being reported will start to reduce in numbers as your NNT software continues to be exposed to the changes that are routine, acceptable, and typical.



Stage One Continued..

Within a period of around 3 to 6 months, we should have observed and created a rule to handle most if not all changes that fall into this category and we can now focus on Stage 2 – Forward Planned Changes with Intelligent Change Control.

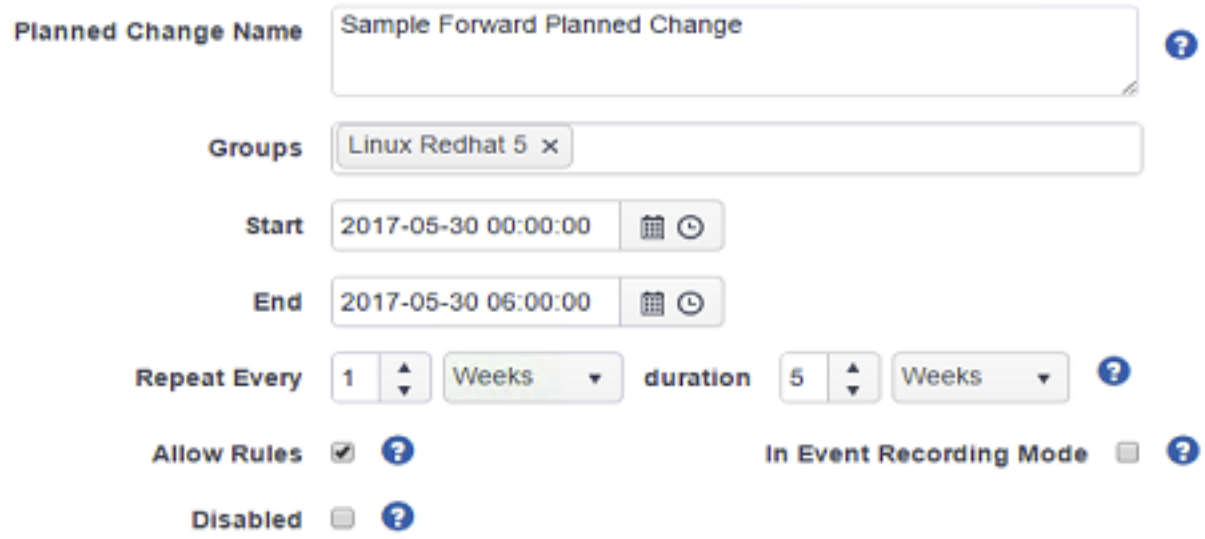
Stage Two- Forward Planned Change Control

The smartest and the most effective way to control changes within your environment is to link them to an approved change. NNT Change Tracker provides the opportunity to ensure this happens independently within the software or via integration with most popular service desk and change management systems such as Service Now, Remedy & Change Gear for example.

Being able to link changes to a pre-approved Change Rule and having the ability to compare actual changes with the detail of that change rule is where we want you to be.

This may be the biggest challenge for many of our customers. Size of task, process, and coordination of effort often means that changes continue to occur outside of any planned change approvals and the IT team are unable to prevent this from continuing.

NOTE: The NNT Managed Change Control Program exists for this reason. The Change Control Program is an ongoing dedicated review of all changes conducted by a qualified NNT consultant who will be able to contain all changes within either a '***Forward Planned Change***' or a '***Retrospective Planned Change***' using rules & logic to ensure that the changes taking place are fundamentally non-harmful.



Once again there are options available to handle all forward planned change instances, so lets walk through them right away.

- First option would be a single or recurring planned change. Within NNT – Change Tracker we can build a planned change window, assign this to devices or groups, and even pre-build the precise planned change profile by recording the changes made by either a patch or new software release on a pre-production system before rolling it out.

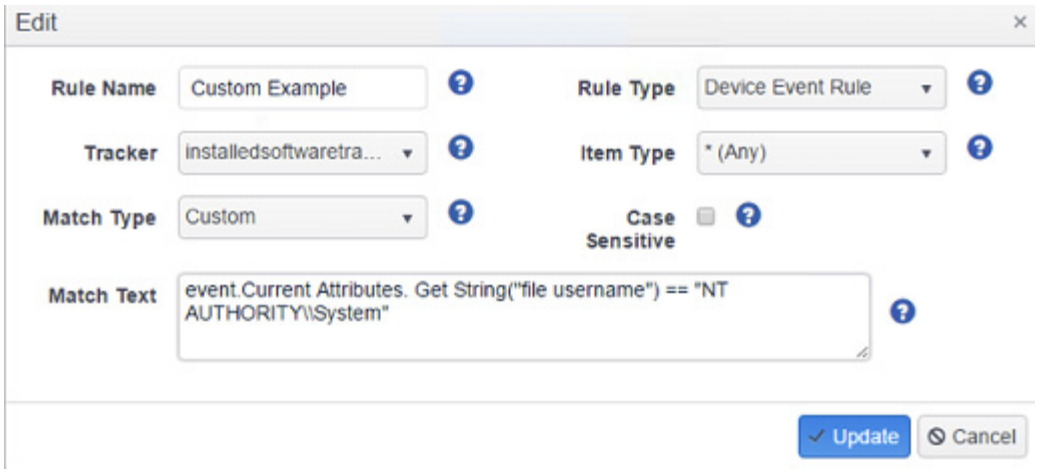
Stage Two Continued..

- We recommend that a recurring planned change is created for Patch-Deployment and that Patches are pre-staged on a pre-production machine. NNT will record the changes specific to that patch which can then be promoted to all production systems. Any anomalies or unexpected changes will be reported immediately- no Blind Spot!

- All Normal Changes outside of regular patch windows should also be planned ahead of time. Some detail of the workflow for approvals can be set up within NNT-Change Tracker or for a more detailed, comprehensive ITSM process, integration with a 3rd party system is advised. We recommend using our integration kits available for systems such as Service Now, Remedy & Change Gear.

- If pre-staging changes is impossible, (perhaps due to time and resource restraint), then a simple planned change window may be created & assigned to the relevant devices, with a change description provided. A report will always be available for review after the planned change window has ended.

- Finally, NNT provides a comprehensive 'Planned Change Rules Editor'. This is a somewhat complex system, but can be used to include associated rules for what constitutes an acceptable planned change. This might include the username making the change whether the change included the deletion or addition or whether the change altered the size of the item in question such as a Log File for example.



We recommend seeking assistance from NNT support when tackling advanced planned change rules.

The final part of this particular section would be to ensue that the changes you are tracking are relevant. Speak to NNT support to ensure all change policies are tracking items that are of interest. The more you track the more changes will be reported. Just make sure these are relevant to you as all environments are of course different. NNT is always on-hand to help, so please don't sweat over the help guides – call us- we will be delighted to assist.

Summary

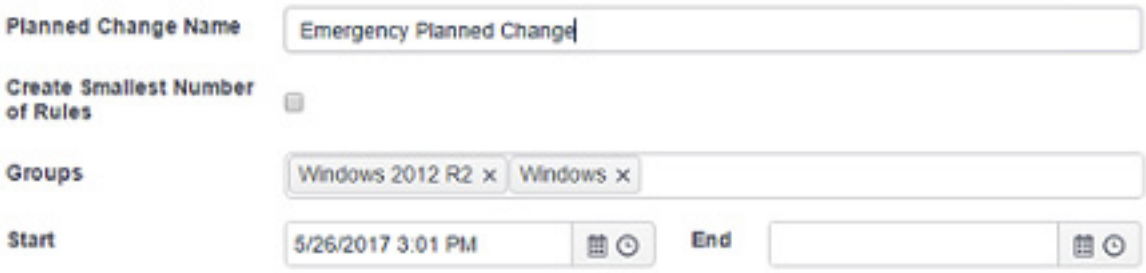
By now, we should have rules & process in place to capture changes that are either:

- Planned & detailed ahead of time, but not checked after the event for authenticity
- Planned ahead of time that will be checked for authenticity as the changes occur (Recommended)
- Not planned ahead of time, but are approved based on previous knowledge of the changes and their adherence to the criteria for which they were previously approved (Recommended)

If your planned change processes are tight and our rules for intelligently approving ad-hoc changes are in good shape, you should not (in theory) now see any unplanned changes at all unless they are either – Emergency Changes or Harmful/Potentially Harmful.

Emergency Changes

From time to time and within standard ITSM guidelines, you will need to make '***Emergency Changes***'. These can be fed directly into NNT Change Tracker or they can be approved after the event. How you decide to handle these will be largely down to preference. However, we strongly recommend that there is a published process for these and if you like, we can help build some rules into Change Tracker to approve changes based on a user group, which may help with this type of change if required.



Inevitably there will still be changes reported that fall outside of any pre-existing rule or process. The magic ingredient here will be you – was there ever any doubt about that? The means to contain and manage changes exists, but we do need some commitment from our customers to work with us to ensure unplanned changes are taken seriously.

If NNT-Change Tracker is set up properly there should be few to no unplanned changes! Where unplanned changes are detected, you are presented with the opportunity to become a little more secure by either taking steps to block those changes, create a rule to approve them in the future, or address process to ensure the changes are handled differently.

If you combine this process with services such as the FAST Cloud and the NNT Change Control Program you will be in the enviable position of being vastly better armed to spot potentially harmful changes that may just be the difference between breach and no breach.

Whatever you decide, please ask to speak with one of our 'Qualified Change Consultants'. We are keen to help you whether you use NNT software or not.

About NNT

NNT Change Tracker Gen provides continuous protection against known and emerging cyber security threats in an easy to use solution, offering true enterprise coverage through agent-based and agentless monitoring options.

- NNT analyses every configurable component within your IT Estate and allows you to define a 'Known, Good, Secure and Compliant State' for all of your in scope systems.
- NNT-Change Tracker scans your devices and compares them to a standard policy, either user defined or based on an industry standard such as the Center for Internet Security (CIS).
- Policies can be automatically assigned based on the device type or priority via a centrally managed console.
- Gen7 is able to fully automate change approval for you, using the NNT FAST (File Approved-Safe technology) that combines unique intelligent change control knowledge base and whitelists.
- With NNT's real-time capabilities, unlike traditional scanning or exclusively agentless technologies, potential breaches to systems or policies are spotted immediately.

NNT Change Tracker Gen 7 helps you to prevent security breaches of your systems by providing you with a powerful feature-rich, easy to use and affordable solution for validating, achieving and maintaining compliance with corporate governance or security standards.

www.nntws.com

UK Office - Spectrum House, Dunstable Road, Redbourn, AL3 7PR
Tel: +44 8456 585 005

US Office - 9128 Strada Place, Suite 10115, Naples, Florida 34108
Tel: +1-888-898-0674

NNT Change Tracker Gen 7 - Real-Time, continuous FIM...and Certified by the Center for Internet Security

- Change Tracker Gen 7 has been certified by the CIS which means you can trust NNT to accurately deliver the most comprehensive, consensus-derived hardening checklists
- NNT provide CIS Benchmark checklist coverage for all Windows, Unix and Linux Operating Systems, SQL Server and Oracle Database Systems, and for Network Devices and appliances such as Cisco ASA firewalls
- Compliance is continuously enforced meaning vulnerabilities are highlighted more quickly than with traditional vulnerability scanners
- Better still, NNT Change Tracker Gen 7 provides continuous real-time FIM across all system, application, driver and configuration files providing peace of mind that system integrity is being maintained
- And if the worst case scenario does happen and your systems are breached or infected with malware, this will be detected within seconds, minimizing damage and costs

TO REQUEST A FREE TRIAL OR DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT info@nntws.com