GEN 7 R2 Cherwell ITSM Integration Module

NNT CHANGE TRACKER GENERATION 7 R2

June 2019 ©New Net Technologies

Contents

Positioning

Cherwell® is a leader in the Service Management space but it still suffers from one of the major change management blindspots – what changes have *actually* been implemented?

By integrating Change Tracker with Cherwell your capability for *change control* is transformed.
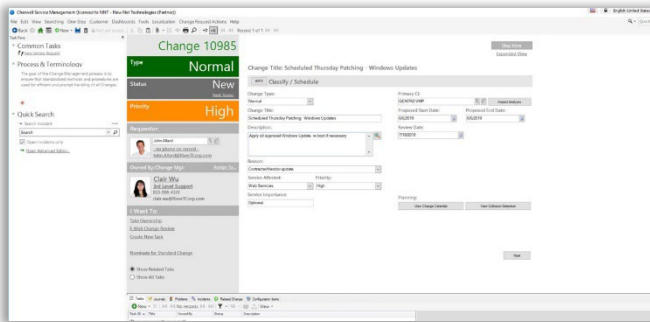

Figure 1: Change Request raised and approved in Cherwell

Approved changes are validated automatically, with a full audit trail of what actually changed provided and reconciled with your Change Requests. By leveraging Change Tracker Intelligent Change Control™, repeated or recurring change patterns can be modelled and re-used to segregate pre-approved changes from the unexpected and genuinely suspicious changes. This reduction of change noise revolutionizes breach detection, clearly exposing insider and zero day malware activity.

How else can you accurately ensure that intended changes were delivered as requested and approved?

Human error has long since been held as the biggest source of unplanned downtime – mistakes are made and systems end-up misconfigured, not just affecting service delivery but leaving the organization more vulnerable to attack. The danger in todays' IT environment is that ironically, the better the change management process, the more a false sense of security can develop and the more easily bad changes can exist. With the emphasis on the approval and review process prior to changes being made, bad changes can be left hiding in plain sight.

Change Tracker™ puts a spotlight on all changes made. Changes made during a prescribed planned change window get validated against the expected change profile - any exceptions, such as misconfigurations or additional non-scoped changes are exposed for review and remediation where required.
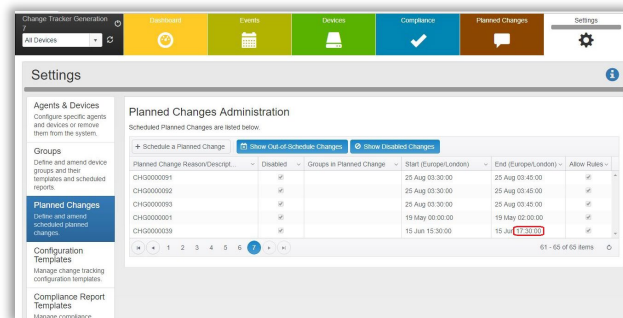

Figure 2: New and updated Change Requests are synced with Change Tracker to profile corresponding Planned Changes

All Unplanned Changes are also recorded in full –ho made the change, with before and after exposure of changes clearly reported. These are prioritized as Cherwell® incidents – changes will be automatically analyzed using continuously updated Threat Intelligence – NNT F.A.S.T. Cloud™. In reality, in a well-run secure IT environment, most unplanned changes will be emergency changes or unexpected-but-benign changes such as automatic software updates. They may not be dangerous changes or breach activity but as a non-approved changes, they must be reviewed. The beauty of this approach is that it also ensures that the most suspicious, potentially dangerous unexpected changes are also clearly categorized as critical.

Note: As of June 2019 ServiceNow® and Sunview ChangeGear are both supported and support for other ITSM systems will be added over time, please contact support@nntws.com for updates

Installation Pre-Requisites

The NNT ITSM Integration module is a Windows Service and interacts with your Change Tracker Gen 7 R2 Hub and your ITSM product via https API operations. As such the ITSM Integration Module may be installed and run from the Hub server itself or from any other suitable Windows platform with network connectivity to both Gen 7 R2 Hub and ITSM Product.

SYSTEM ELEMENT	RECOMMENDED
CPU	DUAL CORE CPU OR 2 VCORES
MEMORY	4GB
DISK FREE	10GB*
OPERATING SYSTEM – 64BIT ONLY	WINDOWS SERVER 2016
MICROSOFT .NET FRAMEWORK	VERSION .NET 4.7.2**
DATABASE	SQL Lite (Pre-Packed with Installer)

*10GB Minimum based on base requirements but storage requirements are directly related to Change Request volume for your ITSM system

** Download details: Microsoft .NET Framework 4.7.2 (missing components will be downloaded automatically, provided the server has internet access)

Please run a Windows Update to ensure all above components are fully up to date.

To download the software go to http://www.newnettechnologies.com/Member-Downloads/ and use the username and password provided to you in your 'Welcome to NNT' email, or contact us at info@nntws.com if you still need your account details.

Installing NNT ITSM Integration Module

Installation is provided by a standard Windows `setup.exe` installer file, please make sure you execute the setup using *'Run As Administrator'.* Select which ITSM Integration is required, either Cherwell, ServiceNow or Sun View ChangeGear, more ITSM Integrations are continually being added so please check with support@nntws.com for the latest developments.
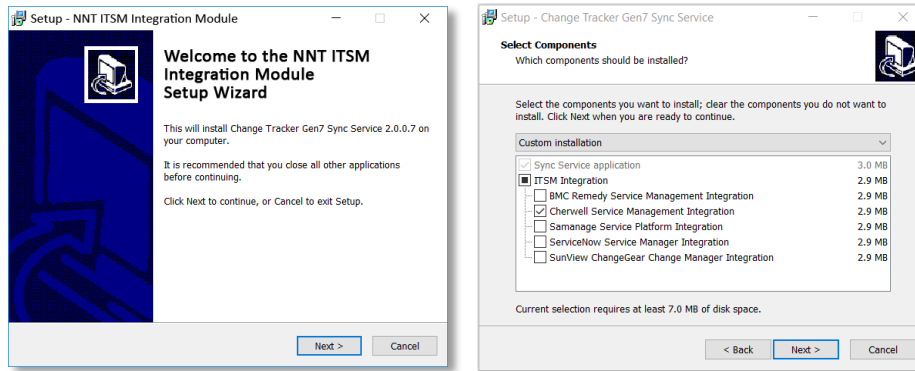
The NNT ITSM Integration module interacts with both your Change Tracker Gen 7 R2 Hub and your ITSM product via secure API operations. As such, it is necessary to provide the ITSM Integration Module with the Hub URL and username and password.

NNT best practice is to allocate a dedicated user account with 'Change Approver' role and use this for all ITSM Integration functions.
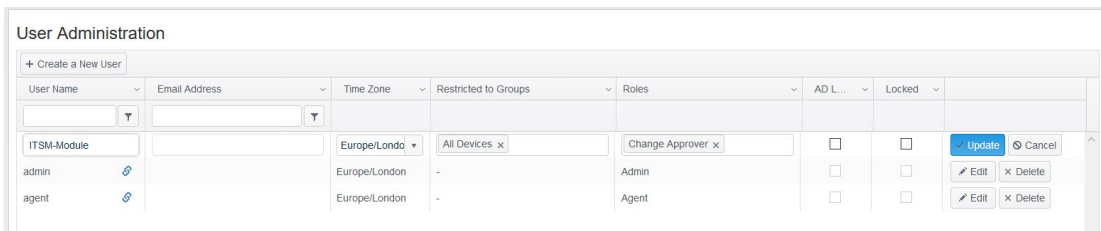
Use these account credentials when prompted by the installer and use the 'Test my hub connection' option when available.
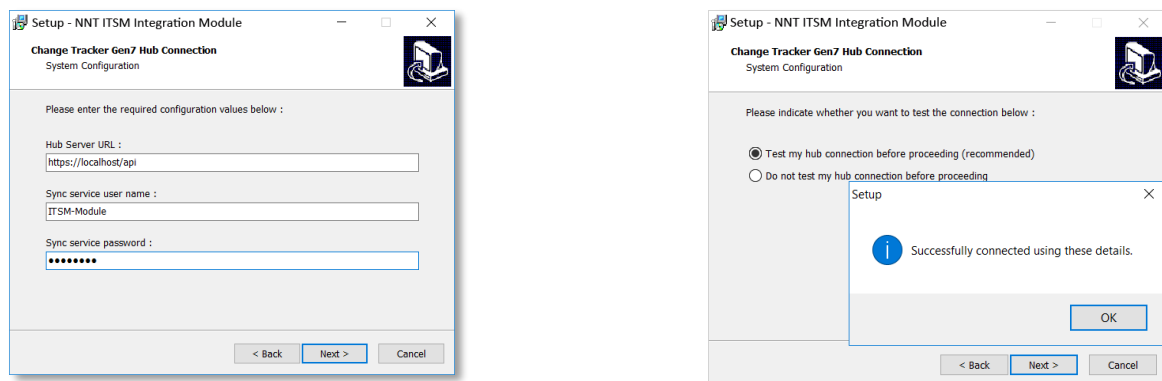
Similarly for the ITSM Product access, a dedicated account should be established with a Cherwell ITSM Client key with API access.

See https://help.cherwell.com/bundle/cherwell_rest_api_950_help_only/page/oxy_ex-1/content/system_administration/rest_api/csm_rest_obtaining_client_ids.html

In the event that the credentials and/or the URL for the Gen 7 Hub or ITSM Product are incorrect, the automated test will report this as in the example below.
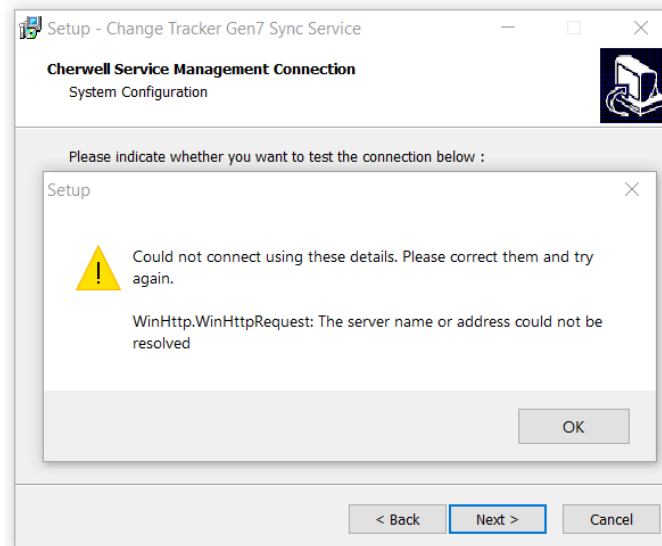
Finally – Please contact NNT Support if you need help at any stage

If you still are experiencing issues please contact support@nntws.com
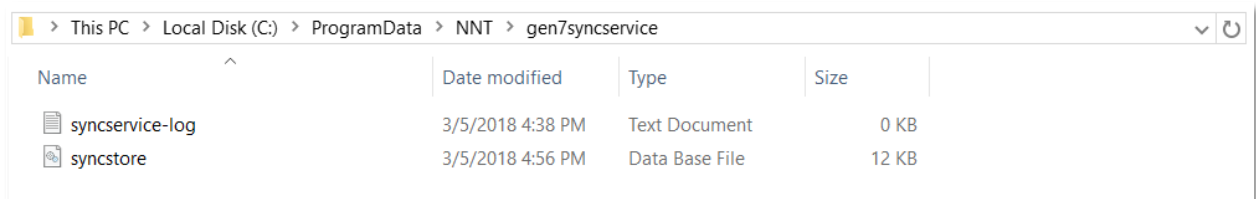
Standard Operation

The ITSM Integration module default operation is to request a list of all open and updated Change Requests every 30 seconds. The requests are filtered so that only Change Requests assigned a Category of 'Software' or 'Network' (Cherwell) or 'Software' or 'Network:Install/configure' (ChangeGear).

These parameters and others are controlled via the `Gen7SyncService.exe.config` configuration file, located by default in the `C:\Program Files\NNT Change Tracker Suite\Gen7SyncService` folder.

See later section for syntax and structure.

File Locations

Note that all program files will be installed by default to `Program Files\NNT Change Tracker Suite\Gen7SyncService`. In addition, there is also a local SQL Lite database file and log file written to the `ProgramData\NNT\gen7syncservice` folder.

Name	Date modified	Type	Size
syncservice-log	3/5/2018 4:38 PM	Text Document	0 KB
syncstore	3/5/2018 4:56 PM	Data Base File	12 KB

Please contact NNT Support if you need help at any stage

If you still are experiencing issues please contact support@nntws.com

The Gen7SyncService.exe.config File

These defaults are controlled via the `Gen7SyncService.exe.config` configuration file, located by default in the `C:\Program Files\NNT Change Tracker Suite\Gen7SyncService` folder.

Significant sections of the 'appSettings' config file are as follows:

Retry Attempts and Retry Interval

```
<appSettings>
  <add key="restSyncProvider.retryTimes" value="3" />
  <add key="restSyncProvider.retryMilliseconds" value="250" />
```

Retry attempts and retry interval are controlled here. Should be left as default.

Start Time Filter

```
<add key="restSyncProvider.startSyncTimeUtc" value="2018-03-09T14:22:26" />
```

This setting acts as a filter for Change Requests with only CRs with a Start Time later than the defined value being processed by the ITSM module. The default value is set as the time of installation but could be manually defined to an earlier point in time if it was desirable to process older Change Requests.

Gen 7 Hub URL and API Access Credentials

```
<add key="changeTrackerRestSyncProvider.baseUrl" value="https://localhost/api" />
<add key="changeTrackerRestSyncProvider.userName" value="ITSM-Integration" />
```

URL for the Gen 7 Hub being used, along with the username to be used for API operations. This works in conjunction with the later key `E.changeTrackerRestSyncProvider.password`, which is an encrypted record of the password provided during installation.

If it is necessary to reset the username or password for the Gen 7 Hub API access, you can re-run the installer and enter the new values, or alternatively, entries can be edited here after stopping the service. For the password key, it is necessary to change the notation from Encrypted to plain text as below, the new password will be encrypted as soon as the service is started.

Change…

```
<add key="E.changeTrackerRestSyncProvider.password" value="AQAAANCMnd8BfdERj…d9Zps6eoT" />
```

…to…

```
<add key="changeTrackerRestSyncProvider.password" value="password" />
```

Cherwell Change Request 'Category' Filter

This setting provides a filter for Cherwell Change Requests. Any API operation argument values added here will be used by the ITSM Integration Module to filter results. The value is transposed to the `sysparm_query` parameter of the request, for more information see https://developer.servicenow.com/app.do#!/rest_api_doc?id=r_TableAPI-GET

```
<add key="CherwellChangeRequestRestSyncAdapter.getIncrementalChangesFilter"
 value="categoryINSoftware,Network" />
```

Cherwell Integration Module Poll Period

This setting defines the poll time period in milliseconds. The default value of 30,000 ms results in Change Requests being processed every 30s.

```
<add key="CherwellImportJob.intervalMilliseconds" value="30000" />
```

Cherwell API URL and Credentials

Similar to the Gen 7 Hub URL and API Access Credentials settings explained earlier, these can be edited directly within the config file or just re-run the setup.exe and enter updated values when prompted.

```
<add key="CherwellRestSyncProvider.baseUrl" value=" https://CherwellITSM/CherwellAPI" " />
<add key="CherwellRestSyncProvider.userName" value="NNT" />
<add key="cherwellRestSyncProvider.clientId" value="xxxxxxxxxxxxx" />
```

Finally – Please contact NNT Support if you need help at any stage

If you still are experiencing issues please contact support@nntws.com

Creating Cherwell Incidents from Gen 7 R2 Change Tracker

An additional common requirement for users of Cherwell with Change Tracker Gen 7 R2 is the need to create a new ITSM Incident for any Unplanned Changes. By definition, any changes detected by Change Tracker that are not part of a scheduled, approved Change Request should be investigated as security incidents. This approach is a key foundational security control and a critical aspect of the SecureOps approach to embedding security within ITSM.

Overview

1. Ensure InBound Email Action (CSM) is enabled within your Cherwell instance to create new Incidents from received emails
2. Ensure Change Tracker Gen 7 is configured to use an SMTP Email service
3. Ensure a suitable user account is created within Change Tracker for Cherwell incidents, using a suitable email account for the Cherwell instance and with User Notifications set for Unplanned Changes

Step 1 – Configure Email monitoring within Cherwell

Please contact your Cherwell Support Team or query
https://help.cherwell.com/bundle/csm_administration_960_help_only/page/content/shared/configure_global_e-mail_accounts.html

Step 2 – Configure InBound Email Action within ServiceNow

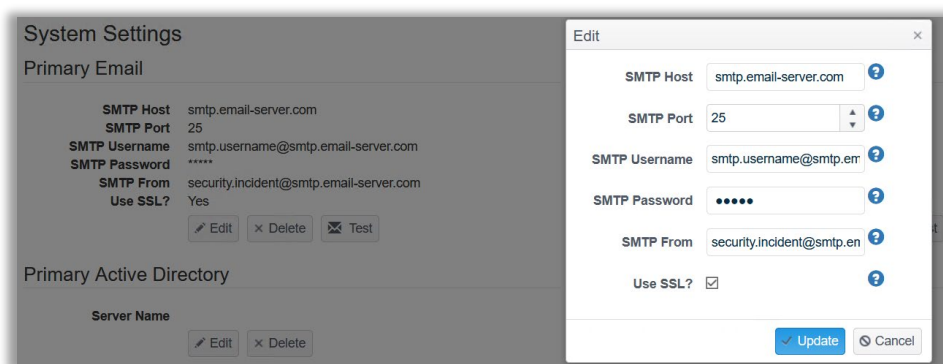Please contact your Cherwell Support Team or query
https://help.cherwell.com/bundle/csm_administration_960_help_only/page/content/suite_features/e-mail/define_monitor_item_action_options.html

An email monitor item action open to Add/Create new incident)

Step 3 – Ensure Change Tracker Gen 7 R2 is configured to use an SMTP Email service

Your Change Tracker Gen 7 R2 system will already be configured to use your SMTP server if you worked through the Change Tracker Getting Started and Admin Guides. Log in to your Gen 7 R2 instance and go to Settings -> System Settings -> Primary Email

After entering SMTP details, test that emails/messages are being sent OK by using the Test button.
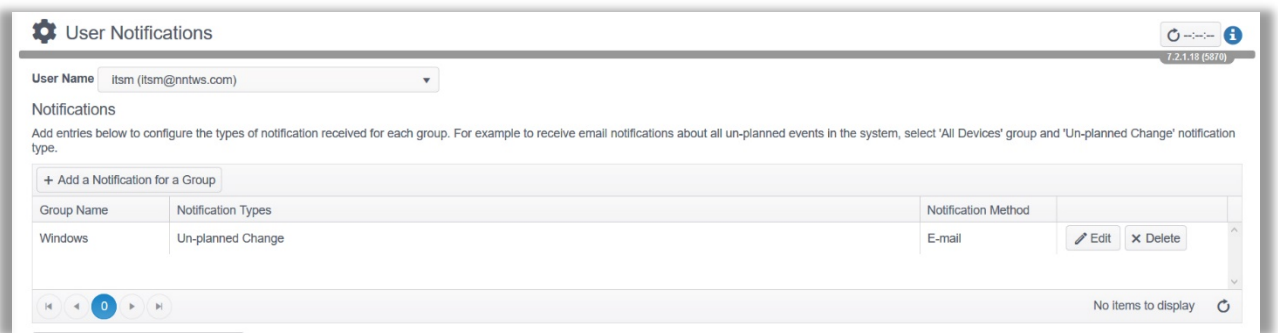

https://supportnntws.atlassian.net/wiki/spaces/HELPDESK/pages/13579393/9.+Alerting+-+Being+Notified+of+Events

Step 4 –Change Tracker Gen 7 user alert setup

Create a new user to act as your ServiceNow instance – this can be the same user used for the ITSM Integration Module to interact with the Gen 7 R2 API. Most important for Incident Creation is that the email address of your ServiceNow instance POP3 service is assigned to the user.
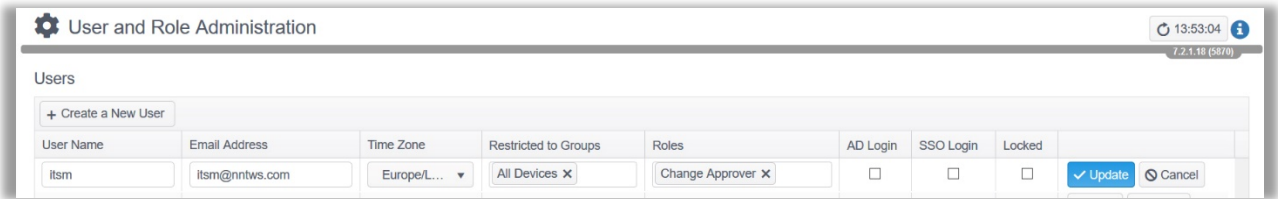
Finally you need to assign a User Notification Email for Unplanned Changes to this user. This will ensure that any Unplanned Changes are alerted using the email address configured for your ServiceNow instance user. In turn, the InBound Email Action will process the email to create an Incident.

https://supportnntws.atlassian.net/wiki/spaces/HELPDESK/pages/13571293/g.+Gen+7+Settings+Page+-+User+Administration

Finally – Please contact NNT Support if you need help at any stage

If you still are experiencing issues please contact support@nntws.com