Get migration settings

Provides support for optional encryption in Nomad PBA. Provides computer association details in 1E Application Migration. Used in computer **Replace** and **Refresh** (Wipe and Load destructive and non-destructive) scenarios. This task can be configured to run under either the capture phase or the restore phase. Its behavior differs depending on which phase it's run under.

> It is independent from existing PBA task sequence actions but is designed to be used in conjunction with them.

Actions	When run, this task: 1. Provides an encryption key to the task sequence action by querying Configuration Manager for a computer association or by generating one itself. 2. Makes the name of the source machine available during a restore by relying on its name stored in the computer association.
Context	Get Migration Settings integrates with Nomad Peer BackUp Assistant (PBA), providing a cryptographic key that can be used to secure captured user data stored on a PBA host. For WSA type deployments, it is also possible for user data to be encrypted and stored onto USB media, if PBA is not available. Step behaviour will depend on user requirements and deployment scenario. Before describing the operation of Get Migration Settings fully, a brief explanation of the different deployment scenarios in which the step operates is provided. *Replace Scenarios* This is where the user is being migrated to new or replacement hardware. A computer association in ConfigMgr is a native object that defines the logical relationship between the old and new computer. When the computer association is created in the site, an encryption key is automatically created and stored in the site database. In this scenario, the step will attempt to identify the appropriate computer association in order to obtain the key. For non-WSA type deployments, the presence of a valid computer association is mandatory and the step will fail if it is not found. WSA deployments also allow users to enter the name of the new computer at the time the Assistant runs, forgoing the need for the pre-provisioned computer association. *Wipe and Load* A Wipe and Load can be destructive (disk reformat and data loss) and non-destructive (file level wipe of the disk where areas of the file system can be preserved). Wipe and Load non-destructive user state capture utilizes file system hard links and therefore does not require external storage or data encryption. Wipe and Load destructive requires user data is saved off onto another device (Nomad PBA) or external device before reformat of the disk (USB media can be used as an alternative to Nomad PBA when using WSA). For this scenario, a ConfigMgr Computer Association is not used. Get Migration Settings will itself generate a unique encryption key based upon the ConfigMgr client identifier and AES 256 hashing algorithm. The key is stored in the task sequence environment for access during capture and restore in the native variable **OSDStateEncryptDecryptKey.** **Operation** Get Migration Settings is designed to support both the Replace and Wipe and Load (Refresh OS) deployment scenarios. The step's behaviour is different depending on deployment scenario. The step, by default will assume a Replace scenario. In order to operate for Wipe and Load (Refresh OS), the task sequence variable **DEPLOYMENTTYPE = REFRESH**, must be set prior to executing the step. As well as provisioning the USMT encryption key, the step is also responsible for instantiating TS variables SourceComputerName and PBAComputerName. During the restore process, the source machine name is used to identify the location of captured user data if using Nomad PBA (PBAComputerName) as well as resolving the list of applications to install as defined by 1E Application Migration (SourceComputerName). By default, the step will attempt to provide a key for encryption of captured user data.

The following is new functionality in Nomad 6.3.200

- Customers that do not require encryption are able to disable key provisioning by setting the TS variable 1EDisableUSMTEncryption = True, prior to running the step. In this case, the step's only function is in providing the source machine name for 1E Application Migration.
- Customers that do not wish to use a ConfigMgr Computer Association in key provisioning have the option of using Get Migration Settings to generate the key instead. How the encryption key is derived for each deployment scenario is summarized in the table below.

Deployment type	**Key source options**	
	ConfigMgr Computer Association	**Get Migration Settings**
Replace Capture/Restore	✓	
WSA-Replace Capture/Restore	✓	✓ New
Wipe and Load Non-Destructive	NA	
Wipe and Load Destructive		✓
WSA-Wipe and Load Destructive		✓

All WSA type deployments require Nomad 6.3.200 and above

Task sequence position

The table below indicates the use of the step for different deployment scenarios. The Get Migration Settings step can operate in one of 2 modes: Capture and Restore. Mode is set in the step UI. For a Replace Capture and Wipe and Load task sequence, the step must be used in Capture mode and inserted into the TS prior to the Capture User Files and Settings step. For Wipe and Load, having implemented the step in Capture mode, it is not necessary to insert the step again before the Restore User Files and Settings step. Typically, in Capture mode, the step will reside in the Capture User Files and Settings group.

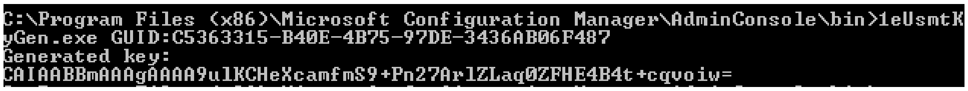
For a Wipe and Load Non-Destructive task sequence, the step does not provision an encryption key as file system hard-links are used negating any requirement for secure storage, in this case the step will only set the SourceComputerName variable for use in 1E Application Migration.

The step must be used in Restore mode for a Replace Restore type task sequence. The step must be positioned before the Restore User Files and Settings step. Typically, in Restore mode, the step will reside in the Restore User Files and Settings group.

OS Deployment type **(WSA and Non-WSA)**	**Get Migration Settings**	
	Capture mode	**Restore mode**
Replace Capture/Restore	✓	✓
Wipe and Load Destructive (Refresh OS)	✓	
Wipe and Load Non-Destructive (Refresh OS)	✓ (No encryption key provisioned)	
In-place Upgrade	NA	

Key recovery

If you need to recover the key generated by the step (perhaps your Wipe and Load Destructive or Replace Restore TS failed before restoring the user data) you can do so using the command line tool **1eUsmtKeyGen.exe.** This tool is part of Installing the Configuration Manager console extensions and is installed at location <ProgramFiles>\Microsoft Configuration Manager\AdminConsole\bin\NomadBranchAdminUIExt. It can be called via the Windows Console as shown below:



```
C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin>1eUsmtK
yGen.exe GUID:C5363315-B40E-4B75-97DE-3436AB06F487
Generated key:
CAIAABBmAAAgAAAA9ulKCHeXcamfmS9+Pn27ArlZLaq0ZFHE4B4t+cqvoiw=
```

It takes the SCCM client guid of the source machine as an argument and generates the exact key that would have been generated during the TS. To know the SCCM client guid of any computer, please consult the 'SMS_Unique_Identifier0' column in the view 'dbo.v_R_System' of the config manager database.

While entering the argument, please remember that:

1. If the client guid contains the prefix "GUID:" it MUST be included (see above screenshot).
2. The case of the argument does not matter; two arguments differing only in case result in the same key being generated.
3. It should be the client guid of the source computer, i.e. the machine from where the user state is being migrated, not that of the destination computer where the state is being migrated to.

The generated key will be printed in base64 format on the Windows Console. You can copy it and use it as is with the usmt "/key" option to recover the user data.

Associated variables

Variable	Description
OSDStateEncryptDecryptKey	Native variable that hosts the key used to secure captured user data
PBAComputerName	Name of the computer on which user data was captured
SourceComputerName	Name of the computer for which the Application Migration list is obtained. Usually the same as PBAComputer
1EDisableUSMTEncryption	If true, then an encryption key is not provisioned.
DeploymentType	If set to Refresh, then an encryption key is not provisioned.

Configurable parameters

Parameter	Default value	Description
Name	Get Migration Settings	Name for the custom task sequence action.
Description	Action to get encryption key for user state and name of the source computer if needed.	Description for the custom task sequence action.
Capture user state		Used during the state capture phase.
Restore user state		Used during the state restore phase.