

# Restore Secure Encrypted Backup

## OPERATING INSTRUCTIONS

**Copyright**

© Ericsson AB 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Description</b>	<b>1</b>
<b>2</b>	<b>Procedure</b>	<b>1</b>
2.1	Restore Secure Encrypted Backup	1



Restore Secure Encrypted Backup



# 1 Description

This instruction describes how to restore a secure backup.

## 2 Procedure

### 2.1 Restore Secure Encrypted Backup

#### Prerequisites

- No documents are required.
- No tools are required.
- The following conditions must apply:
  - No other backup operation is in progress.
  - The backup to restore is available in the system.
  - The name and path of the backup to restore is known.
  - An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

#### Steps

1. Navigate to the `BrmBackupManager` managed object, for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,BrM=1,BrmBackupManager=SYSTEM_DATA
```

2. Specify the secure backup to restore, for example:

```
(BrmBackupManager=SYSTEM_DATA)>BrmBackup=SECURE_BACKUP_20181009_175907
```

3. Start the restore operation and provide the backup password:

```
(BrmBackup= SECURE_BACKUP_20181009_175907)>
```

```
(BrmBackup= SECURE_BACKUP_20181009_175907)>restoreSecuredBackupWithPasswd --backupPassword
```

```
Enter backupPassword:
```



```
(BrmBackup= SECURE_BACKUP_20181009_175907)>restoreSecuredBackup
WithPasswd --backupPassword *****
```

The system returns output true or false.



## Attention!

Risk of system malfunction or traffic disturbance.

A cluster reboot is automatically triggered when restoring a System Data backup. The resulting in-service performance impact corresponds to the time required for a cluster to restart after reboot.

4. Verify that the backup was successfully restored, for example:

```
(BrmBackup=SECURE_BACKUP_20181009_175907>) show -v
```

The following is an example output:

```
BrmBackup=SECURE_BACKUP_20181009_175907
[...]
  asyncActionProgress <read-only>
    actionId=3 <read-only>
    actionName="RESTORE" <read-only>
    additionalInfo=[] <empty>
    progressInfo="PERMIT_PHASE is completed" <read-only>
    progressPercentage=33 <read-only>
    result=NOT_AVAILABLE <read-only>
    resultInfo="" <read-only>
    state=RUNNING <read-only>
    timeActionCompleted="1970-01-01T05:00:00" <read-only>
    timeActionStarted="2018-10-10T10:55:54" <read-only>
    timeOfLastStatusUpdate="2018-10-10T10:55:55" <read-only>
  progressReport <read-only>
    actionId=3 <read-only>
    actionName="RESTORE" <read-only>
    additionalInfo=[] <empty>
    progressInfo="PERMIT_PHASE is completed" <read-only>
    progressPercentage=33 <read-only>
    result=NOT_AVAILABLE <read-only>
    resultInfo="" <read-only>
    state=RUNNING <read-only>
    timeActionCompleted="1970-01-01T05:00:00" <read-only>
    timeActionStarted="2018-10-10T10:55:54" <read-only>
    timeOfLastStatusUpdate="2018-10-10T10:55:55" <read-only>
  [...]
```



**Note:** When performing a System Data backup restore, the restore progress can be monitored (refer to [View Progress Report](#)) until the system reboot is triggered. After the system is rebooted, the progress report is reset to default values.