



Security Center Installation and Upgrade Guide for NEC Cluster 5.11

Document last updated: May 9, 2022

Legal notices

©2022 Genetec Inc. All rights reserved.

Genetec Inc. distributes this document with software that includes an end-user license agreement and is furnished under license and may be used only in accordance with the terms of the license agreement. The contents of this document are protected under copyright law.

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

This publication may not be copied, modified, or reproduced in any form or for any purpose, nor can any derivative works be created therefrom without Genetec Inc.'s prior written consent.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Synergis™, Valcri™, their respective logos, as well as the Mobius Strip Logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.

Other trademarks used in this document may be trademarks of the manufacturers or vendors of the respective products.

Patent pending. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™, and other Genetec™ products are the subject of pending patent applications, and may be the subject of issued patents, in the United States and in other jurisdictions worldwide.

All specifications are subject to change without notice.

Document information

Document title: Security Center Installation and Upgrade Guide for NEC Cluster 5.11

Original document number: EN.500.071-V5.11.0.0(1)

Document number: EN.500.071-V5.11.0.0(1)

Document update date: May 9, 2022

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide describes how to install and upgrade Security Center on a two-node (two servers) NEC mirrored cluster with a Windows Server 2008 operating system.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

Contents

Preface

| | |
|----------------------------|-----|
| Legal notices | ii |
| About this guide | iii |

Chapter 1: Before you install

| | |
|---|---|
| NEC clustering for Security Center | 2 |
| NEC ExpressCluster terminology | 3 |
| Minimum server requirements for NEC cluster | 4 |
| Security Center system requirements | 5 |
| Planning checklist for NEC cluster | 6 |

Chapter 2: Installing Security Center in a NEC ExpressCluster environment

| | |
|---|----|
| Preparing your servers for clustering | 8 |
| Best practices for installing NEC ExpressCluster | 10 |
| Installing Security Center Server for NEC Cluster | 11 |
| Activating Security Center license using the web | 12 |
| Activating Security Center license manually | 15 |
| Upgrading Security Center NEC cluster | 20 |
| Backward compatibility requirements for Security Center | 21 |

Chapter 3: Configuring Security Center NEC Cluster

| | |
|---|----|
| Configuring Security Center Server for the cluster | 28 |
| Moving Security Center server's license and configuration files | 28 |
| Stopping Genetec™ Watchdog from restarting Genetec™ Server | 28 |
| Configuring Directory authentication in a cluster environment | 30 |
| Configuring the mirrored VertX settings folder | 31 |
| Configuring SQL Server for the cluster | 32 |
| Configuring NEC ExpressCluster X Edition | 36 |
| Creating the script files manually | 36 |
| Creating the cluster | 37 |
| Finalizing the cluster configuration | 37 |
| Cluster configuration tests | 39 |

| | |
|---|----|
| Where to find product information | 40 |
|---|----|

| | |
|-----------------------------|----|
| Technical support | 41 |
|-----------------------------|----|

Before you install

This section includes the following topics:

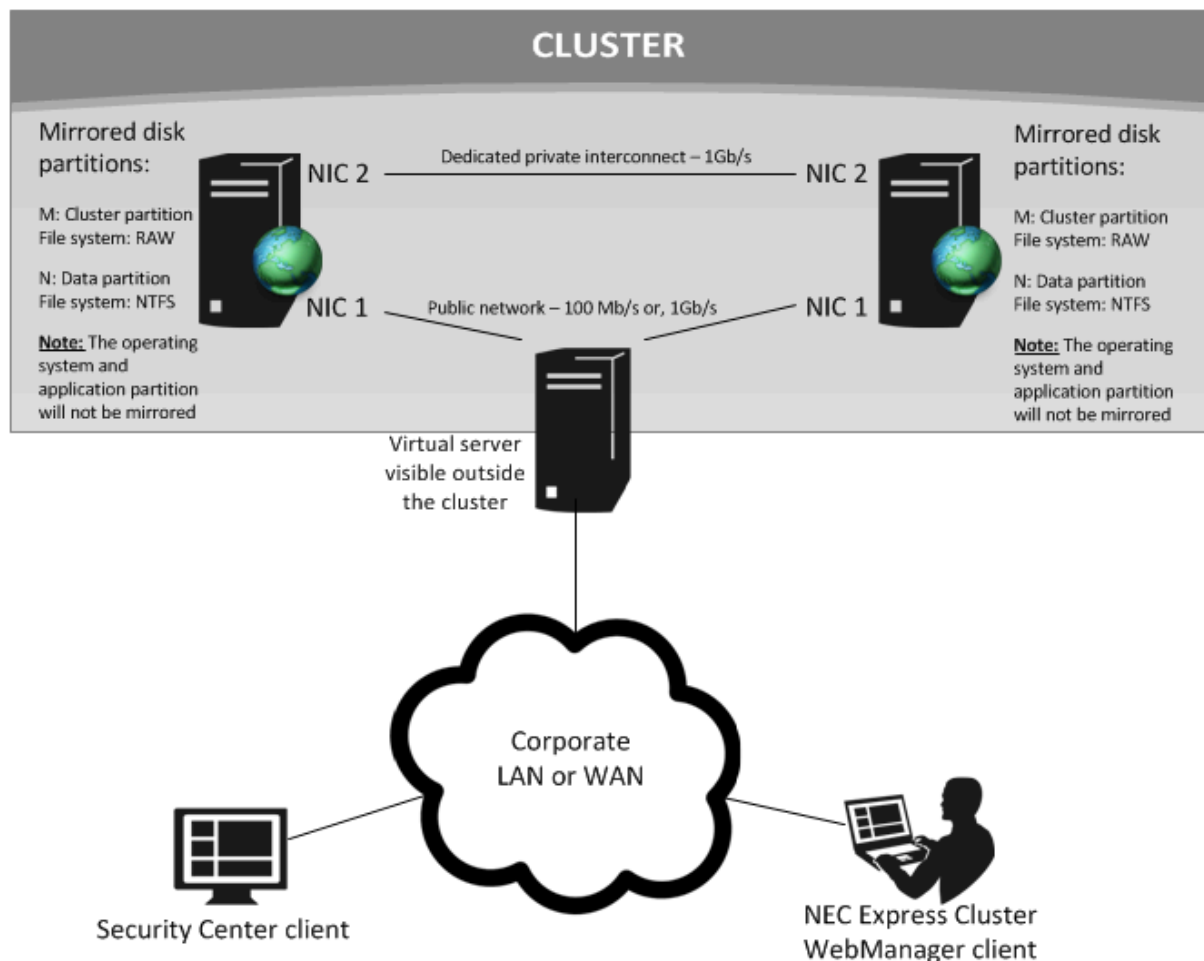
- ["NEC clustering for Security Center "](#) on page 2
- ["NEC ExpressCluster terminology"](#) on page 3
- ["Minimum server requirements for NEC cluster"](#) on page 4
- ["Security Center system requirements"](#) on page 5
- ["Planning checklist for NEC cluster"](#) on page 6

NEC clustering for Security Center

Your NEC ExpressCluster X Edition provides synchronous data mirroring between two (or more) servers. Fast application recovery and data protection is ensured in case of a system failure.

Clustering ensures that your Security Center server's configuration files and database files found on one server are mirrored on another server.

A virtual IP address is used to accept incoming client connections. The cluster then monitors the active server's hardware and software. If a failure is detected, the cluster replaces the active server with the standby server so that the system remains online. Clients do not know whether the active server or the standby server is managing the system as they are still connected to the same IP address.



NEC ExpressCluster terminology

The following terms are used to describe the components of a NEC ExpressCluster:

| Term | Description |
|------------------------|---|
| Public network | The network hosting the Security Center server and clients. |
| Private network | Also known as <i>Interconnect network</i> . The dedicated link connecting the two clustered servers together. |
| Active node | The clustered server actively managing Security Center. |
| Standby node | The clustered server waiting on standby. |
| Heartbeat | A signal that servers in a cluster send to each other to detect a failure in the cluster. |

Minimum server requirements for NEC cluster

Your servers should be identical in terms of hardware, operating system, and software. NEC ExpressCluster, SQL server, and Security Center each have their own set of minimum requirements.

The following table lists the minimum requirements as a combination of all three:

| Component | Requirements |
|---------------------------------|--|
| CPU and memory | Refer to the <i>Security Center System Requirements</i> . Click here for the most recent version of this document. |
| Operating system | Refer to your NEC ExpressCluster System Requirements. NOTE: English, Chinese and Japanese operating systems are only supported by NEC cluster. |
| Disk partitions | Each server will need two identically configured disk partitions (apart from your C:/). One for the <i>cluster partition</i> (64 MB RAW) and one for the <i>mirrored partition</i> (40 GB or more NTFS). These partitions should not be on the same physical disk as the operating system and software, so two physical hard drives are required. IMPORTANT: For systems with more than 1,000 entities (cameras, doors, cardholders, etc) three physical hard drives are required for performance reasons. |
| Network cards | Each server will need two network cards. One to accept external client connections and the other for the cluster's <i>interconnection</i> . 1Gb/s cards are recommended. |
| NEC Client workstation | A workstation needs to be identified as the NEC Client workstation. It will be used for configuration and administration of the cluster. |
| SQL Server | SQL Server 2014 Express is bundled on the Security Center download package. But for installations where the database size will grow over 10 GB (very rare), two copies of SQL Standard or Enterprise will be needed. |
| Database management tool | SQL Management Studio needs to be installed on both servers. |

Security Center system requirements

For Security Center to perform as expected, the following hardware and software components are required. To determine which configuration is best suited for your application, contact our Sales Engineering team at salesengineering@genetec.com.

Planning checklist for NEC cluster

You will need to know the following information before starting your cluster installation.

| Cluster component | Description | Your system |
|--|--|-------------|
| Cluster name | Name of the cluster configuration. | |
| Failover group name | Name of the failover group | |
| Failover floating IP | Static IP address used by clients to access Security Center services within the cluster. | |
| Management floating IP | Static IP used to access cluster management services. | |
| Virtual computer name | Name to be used to access the server (Active or Standby) currently hosting the Security Center services. | |
| Active Node name | Name of the active server used in cluster configurations. | |
| Active Node Public IP address | Static IP address used in the public IP network. | |
| Active Node Public Subnet mask | Subnet mask used in the public IP network. | |
| Active Node Public Default Gateway | Default Gateway used in the public IP network. | |
| Active Node Public Preferred DNS server address | Static IP address of the Preferred DNS server in the public IP network. | |
| Active Node Private IP | Static IP address used in the interconnect IP network. | |
| Active Node Private Subnet mask | Subnet mask used in the interconnect IP network. | |
| Standby Node Name | Name used for identification in the cluster configuration. | |
| Standby Node Public IP | Static IP address used in the public IP network. | |
| Standby Node Public Subnet mask | Subnet mask used in the public IP network. | |
| Standby Node Public Default Gateway | Default Gateway used in the public IP network. | |
| Standby Node Public preferred DNS server | Static IP address used in the interconnect IP network. | |
| Standby Node Private IP | Static IP address used in the interconnect IP network. | |
| Standby Node Private Subnet mask | Subnet mask used in the interconnect IP network. | |

Installing Security Center in a NEC ExpressCluster environment

This section includes the following topics:

- ["Preparing your servers for clustering"](#) on page 8
- ["Best practices for installing NEC ExpressCluster"](#) on page 10
- ["Installing Security Center Server for NEC Cluster"](#) on page 11
- ["Activating Security Center license using the web"](#) on page 12
- ["Activating Security Center license manually"](#) on page 15
- ["Upgrading Security Center NEC cluster"](#) on page 20

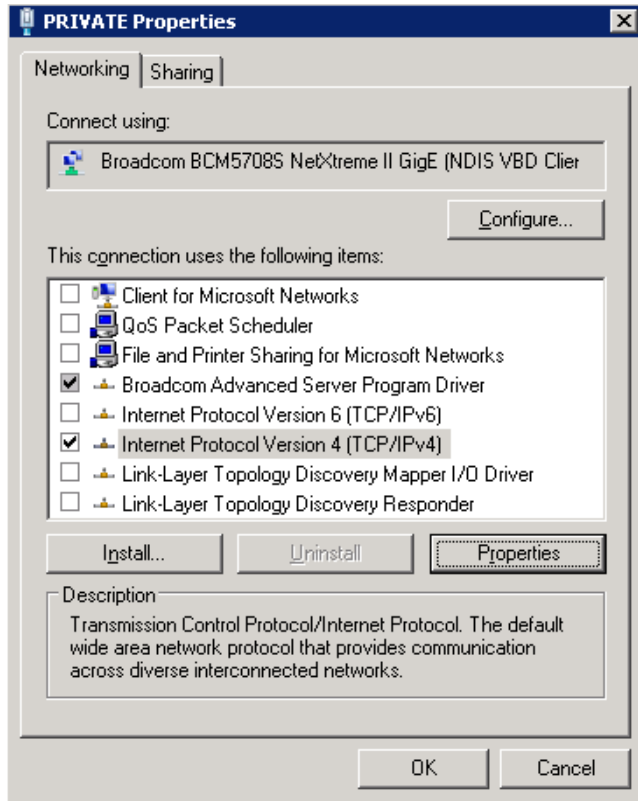
Preparing your servers for clustering

Before installing the NEC ExpressCluster software, you must prepare the servers.

To prepare your servers for clustering:

- 1 Make sure that each server has two network cards and two physical hard disks.
- 2 Configure your first hard disk with one partition only. It will be used for your operating system and software.
- 3 Configure your second hard disk with two partitions. One is called the cluster partition (64 MB raw) and the other is called the data partition (40 GB or more, NTFS). The data partition will contain Security Center's SQL database files as well as the server's configuration files. This data will be mirrored between the two servers.
IMPORTANT: Not only must the partitions be identical on both servers, but the drive letters assigned must also be identical.
- 4 Create the following folders on the data partition for mirroring:
 - *N:\Genetec Security Center 5.11\ConfigurationFiles*
 - *N:\MSSQL\DATA*
 - *N:\VertX***NOTE:** In this example "N:" is the drive letter assigned to your mirrored data partition. The folder *N:\VertX* is only necessary if you are using HID VertX controllers.
- 5 If your system has more than 1,000 entities, or requires extensive reporting, a third disk should be configured with another cluster partition and data partition. SQL's *.ldf files will be clustered from one disk and SQL's *.mdf files will be clustered from another physical disk. This step is added for performance stability in larger systems.
- 6 Install the same operating system on both servers.
- 7 In Windows, rename the first network card as "Public". This is the network interface that will accept incoming client connections. Repeat on the second server.
- 8 Rename the second network card as "Private" or "Interconnect". This is for the dedicated interconnection between the two clustered servers. Repeat on the second server.
- 9 Order the *Public* and *Private* network interfaces as follows:
IMPORTANT: The network interface on the *Private* network must be Window's first available network interface.
 - a) Log on to the first node in the cluster using an administrative Windows account.
 - b) Click **Start > Run**, and type **ncpa.cpl**.
 - c) In the **Network Connections** window, click the **Advanced** menu, and then click **Advanced settings**.
TIP: If the **Advanced** menu does not appear at the top of the window, press Alt.
 - d) In the **Connections** list, select the *Private* network connection, and use the arrow buttons on the right to bring it to the top of the list.
 - e) Click **OK**.
 - f) Repeat the steps on all remaining cluster nodes.
- 10 On each server, configure the *Public* network card to use the same IP subnet.
- 11 On each server, configure *Private* network card to use the same IP subnet.

- 12 Disable all network card features of the *Private* NIC except TCP/IP version 4 (and, if it appears in the list, the driver).



- 13 From the command line, test whether the two servers nodes can *ping* each other over their public interface and over their private interface.

Best practices for installing NEC ExpressCluster

It is assumed that you are familiar with the concept of clustering and how to install and configure the NEC ExpressCluster X Edition for Windows.

When installing the NEC ExpressCluster software, keep the following points in mind:

- NEC clusters can be set up with several different configurations. Note that we are using their *High availability* cluster configuration using *mirror disks* with *2 nodes*.
- The NEC software should be installed on the servers' C:/ drive, not a mirrored disk.
- The identical folder path is required on both servers for the NEC software installation.
- NEC cluster licenses will be required after the installation.
- DO NOT reboot either server until the NEC ExpressCluster has been installed on both.
- Apart from installing the cluster software on two servers, you will also need to install the *NEC WebManager* on a workstation. This application is used to manage the cluster.

For more information about the NEC ExpressCluster X Edition for Windows, see the NEC documentation supplied with the NEC ExpressCluster software, or available at <http://support.necam.com/EnterpriseSW/EC/>

Installing Security Center Server for NEC Cluster

After the NEC ExpressCluster software has been installed, you must install Security Center Server and SQL Server on your active server first, and then on your standby server.

Before you begin

A Security Center license will be needed for each main server.

To install Security Center server:

- 1 Install Security Center Server including the appropriate Omnicast™ compatibility pack, if necessary, and SQL Server. For more information, see the *Security Center Installation and Upgrade Guide*.
- 2 Launch the Server Admin application and do the following:
 - a) If the server is a Security Center main server (hosting the Directory role), [apply the Security Center license in the Server Admin](#).

NOTE: Two Security Center server licenses are needed; one for each server.

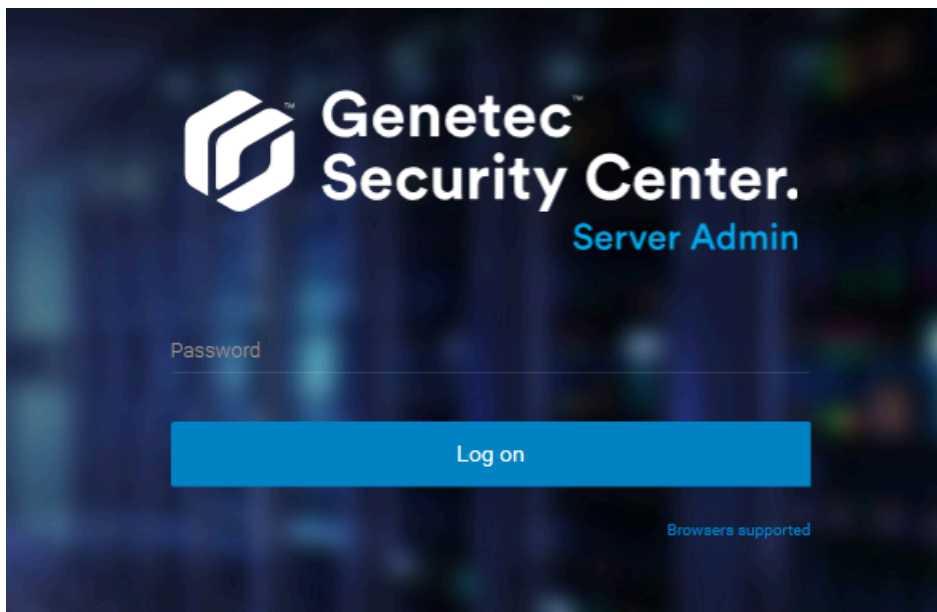
 - b) In the Server Admin, make sure that the network card binding for the **Genetec Server** is set to **Any**.
 - c) Close the Server Admin and reboot the server.
- 3 Repeat the steps on the standby server.
- 4 Using your Config Tool application, log on to the active Security Center server to ensure that the roles you need have been successfully created.
For more information, see the *Security Center Administrator Guide*.
- 5 Install Security Center (see the *Security Center Installation Guide*).

Activating Security Center license using the web

After you install Security Center on the main server or promote an expansion server to a main server, you must activate your Security Center license on the main server. If you have Internet access, you can activate your Security Center license using *web activation* from Server Admin.

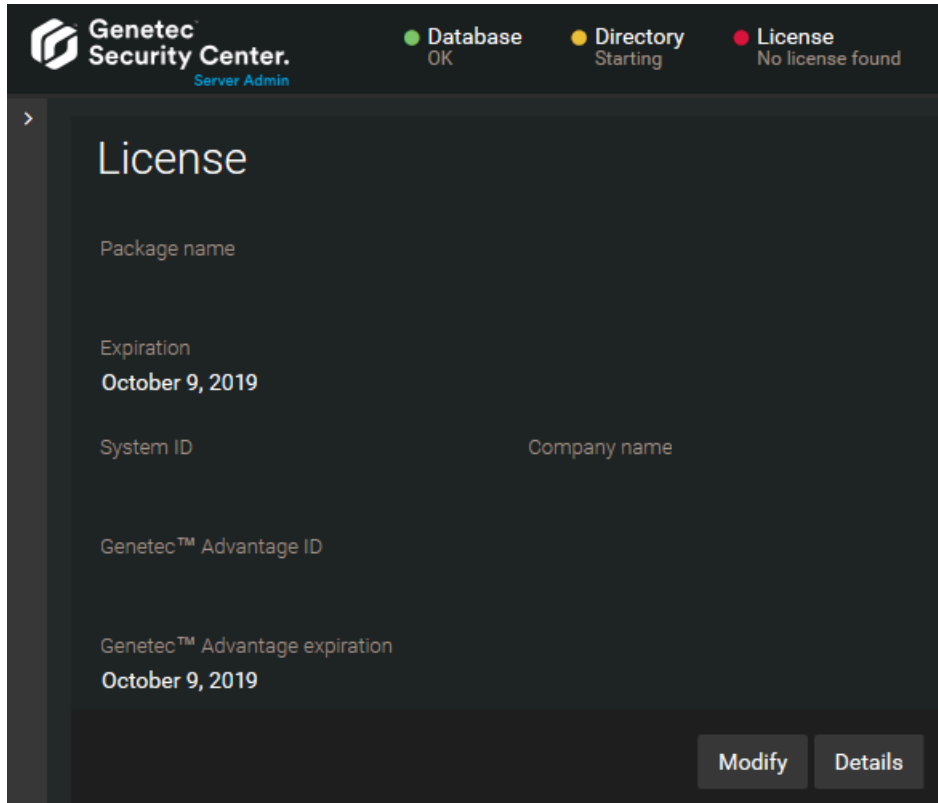
To activate your Security Center license using web activation:

- 1 Open the Server Admin web page by doing one of the following:
 - If connecting to Server Admin from the local host, double-click **Genetec™ Server Admin** (🌐) in the *Genetec Security Center* folder in the Windows Start menu.
 - If you are not on the main server, type `https://computer:port/Genetec` in your web browser, where *computer* is the hostname or the IP address of your server and *port* is the web server port specified during the Security Center expansion server installation.
- 2 Enter the server password that you set during the server installation, and click **Log on**.

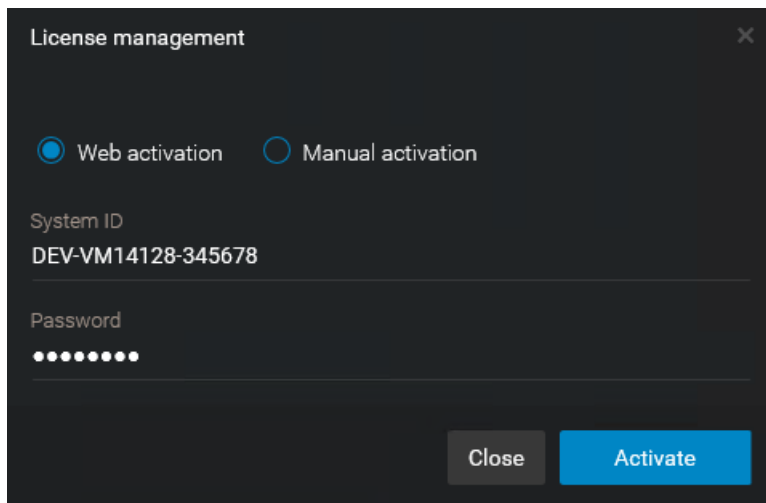


The Server Admin *Overview* page opens.

- 3 In the **License** section, click **Modify**.

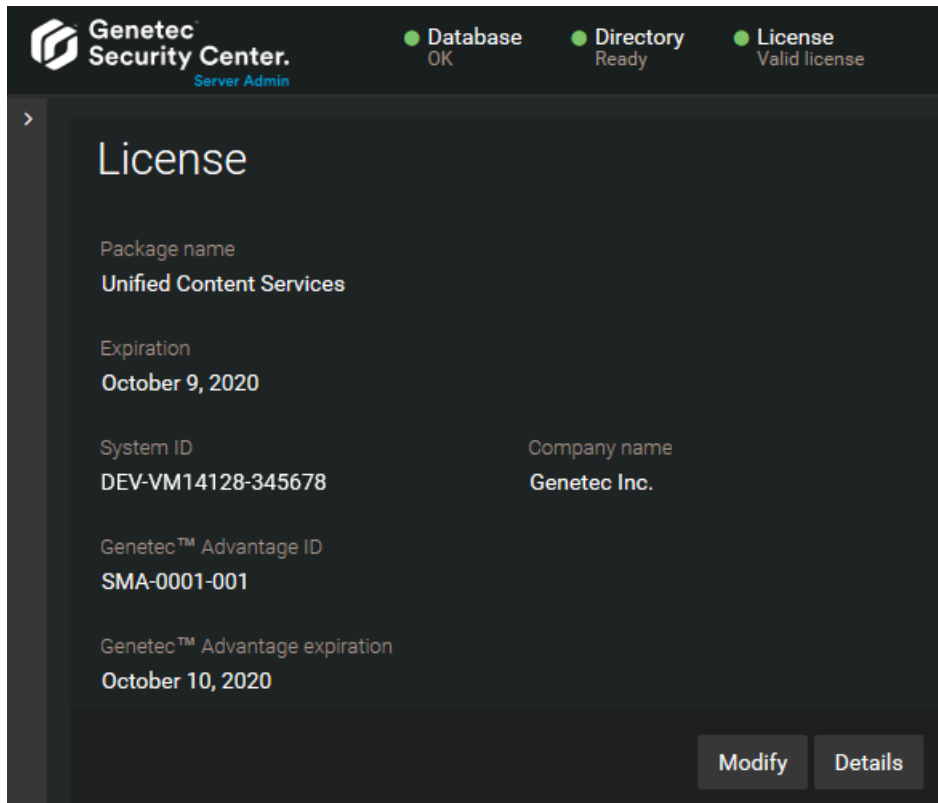


- 4 In the *License management* dialog box, click **Web activation** and enter your **System ID** and **Password**. Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.



5 Click **Activate**.

Your license information appears in the *License* section of the *Server Admin Overview* page.

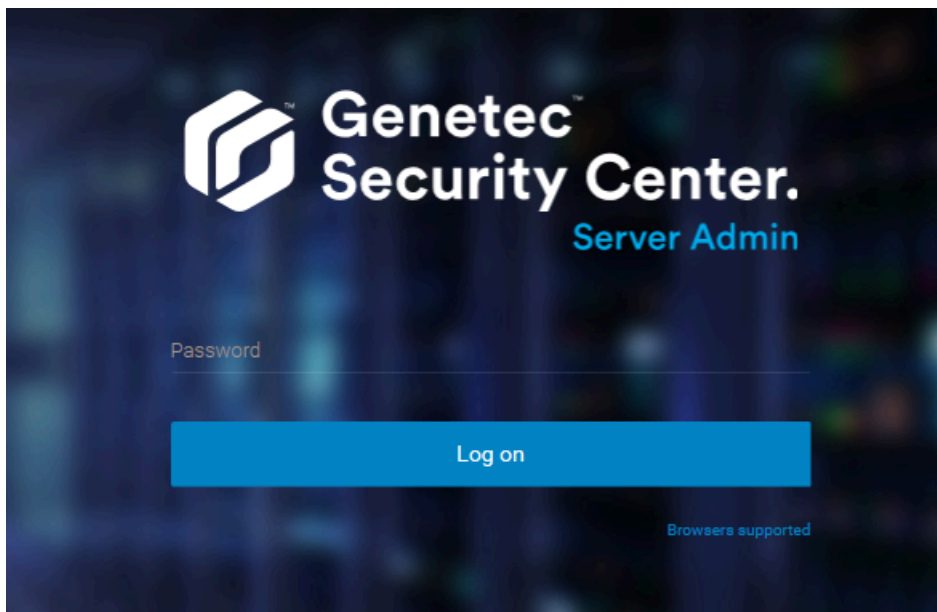


Activating Security Center license manually

After you install Security Center on the main server or promote an expansion server to a main server, you must activate your Security Center license on the main server. If you do not have Internet access, you can activate your Security Center license using *manual activation* from Server Admin and GTAP.

To activate your Security Center license manually:

- 1 Open the Server Admin web page by doing one of the following:
 - If connecting to Server Admin from the local host, double-click **Genetec™ Server Admin** (🔒) in the *Genetec Security Center* folder in the Windows Start menu.
 - If you are not on the main server, type `https://computer:port/Genetec` in your web browser, where *computer* is the hostname or the IP address of your server and *port* is the web server port specified during the Security Center expansion server installation.
- 2 Enter the server password that you set during the server installation, and click **Log on**.

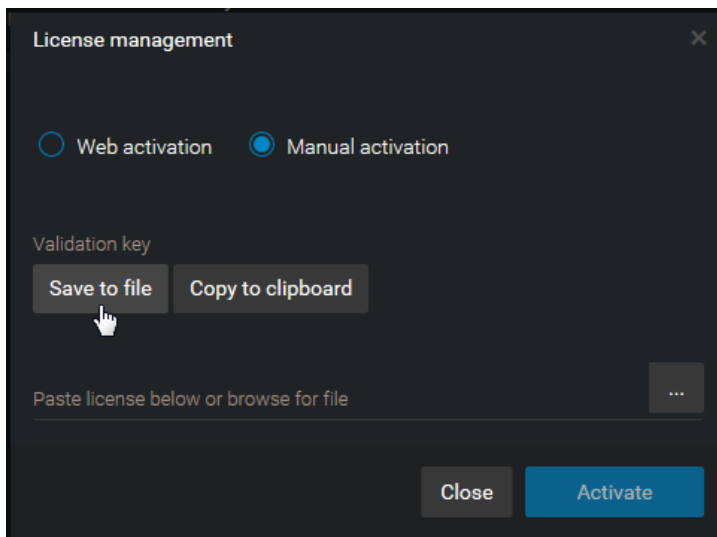


The Server Admin *Overview* page opens.

- 3 In the **License** section, click **Modify**.



- 4 In the *License management* dialog box, click **Manual activation**, and then under *Validation key*, click **Save to file**.



The validation key is a sequence of numbers (in hexadecimal text format) generated by Security Center that uniquely identifies your server. The validation key is used to generate the license key that unlocks your Security Center software. The license key can only be applied to the server identified by the validation key.

A text file named *validation.vk* is saved to your default *Downloads* folder. Copy the file to a USB key or a location that you can access from a computer that has internet access.

- 5 From a computer with internet access, open the Genetec™ Technical Assistance Portal (GTAP) at: <https://portal.genetec.com/support>.

The screenshot shows the Genetec Portal login interface. At the top is the Genetec Portal logo. Below it is a 'Login' header. The main content area is split into two columns. The left column has a blue background and contains a 'Username *' field with a placeholder 'Email or System ID', a 'Password *' field, and two buttons: 'Login' and 'Reset Password'. The right column has a white background and contains the text 'Welcome to the Genetec Portal', a 'Services' section with links for 'Channel Partner' and 'Technical Assistance', and a 'Registration' section with links for 'Technical Assistance (for users of Genetec solutions)', 'Channel Partners', and 'Consultants'. At the bottom of the page, there is a footer with a link to 'Go to Genetec.com website' and a copyright notice '© 2013-2019 Genetec Inc. All rights reserved.'

- 6 On the *Login* page, do one of the following:
- Enter your system ID and password, and then click **Login**.
Your system ID and password are specified in the *Security Center License Information* document. Our Customer Service team sends you this document when you purchase the product.
 - Enter the email address for your GTAP user account and password, and then click **Login**
- 7 On the GTAP home page, open the **Genetec Portal** menu and click **Technical Assistance > System Management**.

- 8 On the *System Management* page, type your system ID and click **Search**.
The *System Information* page opens.

The screenshot shows the Genetec Portal interface. At the top, there's a blue header with the Genetec logo and a search bar. Below the header, a green sidebar contains a 'System Information' icon. The main content area displays the system ID 'DEM-160419-627239' and the license status 'Active until Oct 23, 2020'. There are buttons for 'Reset system password' and 'Product Download'. On the right, there's a section for 'Genetec™ Advantage Information' showing the type 'Genetec™ Advantage', contract number '11-2954-0930', and expiration date 'Expiring on Mar 22, 2024'.

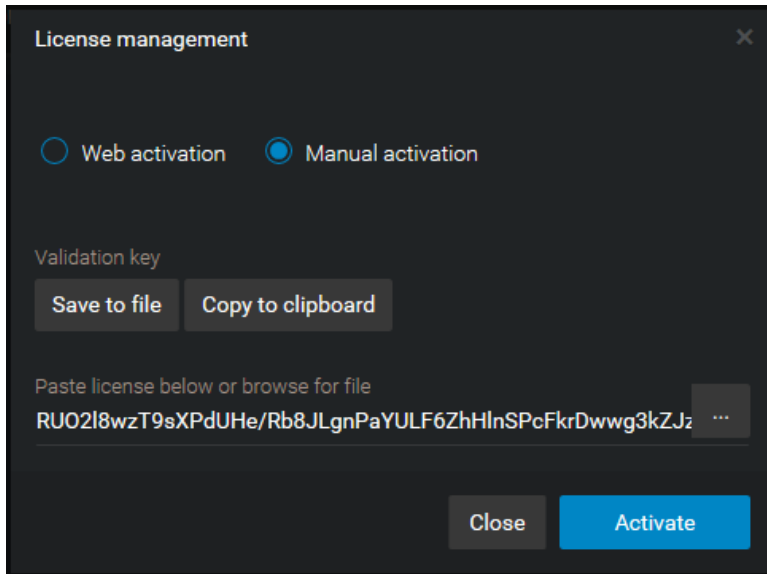
- 9 In the *License information* section, click **Activate license**.

The screenshot shows the 'License information' section. It includes a 'Version' dropdown set to 'Security Center 5.11' and a 'Product' label 'Security Center 5.11 (Enterprise)'. Below this is a table with four columns: 'Machine', 'Status', 'Validation Key', and 'License Key'. The first row shows 'Directory' as the machine, 'Not Activated' as the status, and a red 'Activate license' button. There is also a 'License content' button.

- 10 In the dialog box that opens, browse to your validation key (.vk file), and click **Submit**.
- 11 When you receive the License activation successful message, click **Download** under *License Key* and save the license key to a file.
The default file name is your system ID, followed by *_Directory_License.lic*.
- 12 Return to the Server Admin that is connected to your Security Center main server.

13 In the *License management* dialog box, do one of the following:

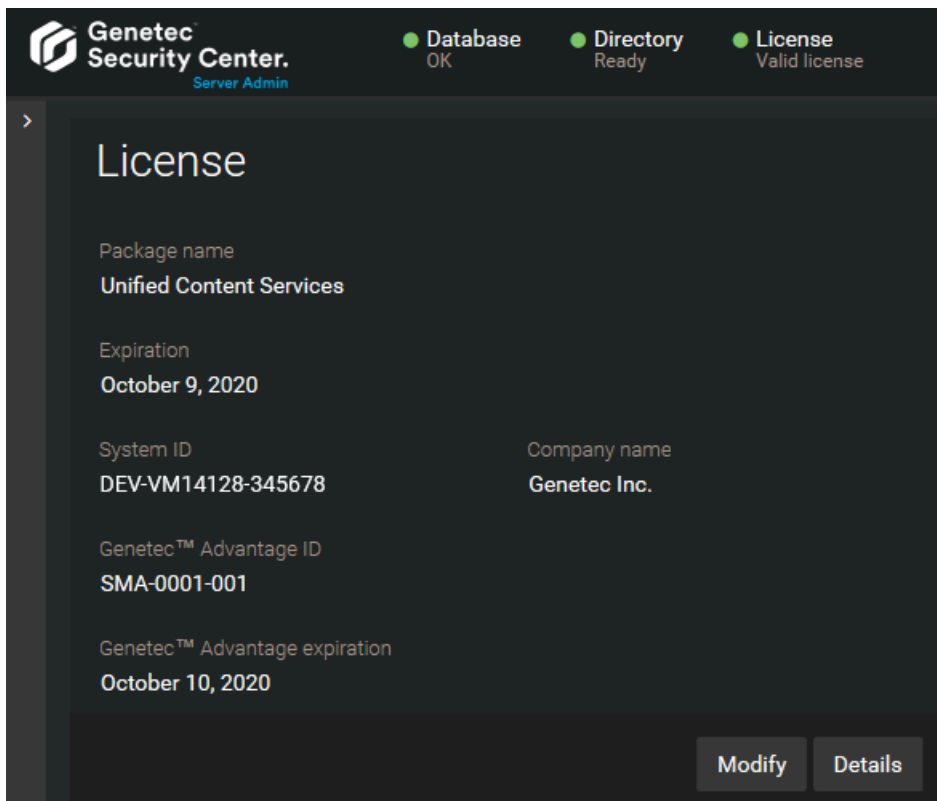
- Paste your license information from the license key file by copying the content from a text editor.
- Browse for the license key (.lic file), and click **Open**.



The 'License management' dialog box has a dark background. At the top, it has a title bar with a close button. Below the title bar, there are two radio buttons: 'Web activation' (unselected) and 'Manual activation' (selected). Underneath, there is a 'Validation key' section with two buttons: 'Save to file' and 'Copy to clipboard'. Below these buttons, there is a text area with the placeholder 'Paste license below or browse for file'. The text area contains the license key 'RU02l8wzT9sXPdUHe/Rb8JLgnPaYULF6ZhHlnSPcFkrDwwg3kZJz' followed by a three-dot menu icon. At the bottom right, there are two buttons: 'Close' and 'Activate'.

14 Click **Activate**.

Your license information appears in the *License* section of the Server Admin *Overview* page.



The 'Genetec Security Center. Server Admin' page has a dark background. At the top, there is a header with the Genetec logo and the text 'Genetec Security Center. Server Admin'. To the right of the header, there are three status indicators: 'Database OK', 'Directory Ready', and 'License Valid license'. Below the header, there is a 'License' section. The section contains the following information: 'Package name: Unified Content Services', 'Expiration: October 9, 2020', 'System ID: DEV-VM14128-345678', 'Company name: Genetec Inc.', 'Genetec™ Advantage ID: SMA-0001-001', and 'Genetec™ Advantage expiration: October 10, 2020'. At the bottom right of the section, there are two buttons: 'Modify' and 'Details'.

Upgrading Security Center NEC cluster

To upgrade Security Center in a NEC ExpressCluster environment, you must disable automatic failover for the NEC ExpressCluster, and then upgrade Security Center on the active and standby servers.

Before you begin

You must have the same *ConfigurationFiles* folder on both the mirrored and local hard drives.

1. Copy the *ConfigurationFiles* folder from the mirrored drive (*N:\Program Files (x86)\Genetec Security Center 5.7\ConfigurationFiles*) to your local drive (*C:\Program Files (x86)\Genetec Security Center 5.8\ConfigurationFiles*).
2. Repeat for each node in your NEC cluster.

NOTE: In this example "N:" corresponds to the drive letter assigned to your mirrored data partition. The actual drive letter will depend on your NEC cluster.

To upgrade Security Center NEC cluster:

- 1 Open the *NEC WebManager* application.
- 2 From the drop-down list, select **Config Mode**.
- 3 Click **Groups > failover**.
- 4 In the **Resources** tab, right-click **script**, and then click **Properties**.
- 5 Click the **Details** tab.
- 6 Select the *start.bat* file, and then click **Edit**.
- 7 Find the following lines of code:

```
armload MSSQL /s /a /r 3 /fov /wait 30 MSSQL$SQLEXPRESS
armload GenetecServer /s /a /r 3 /fov GenetecServer
armload GenetecWatchdog /s /a /r 3 /fov GenetecWatchdog
```

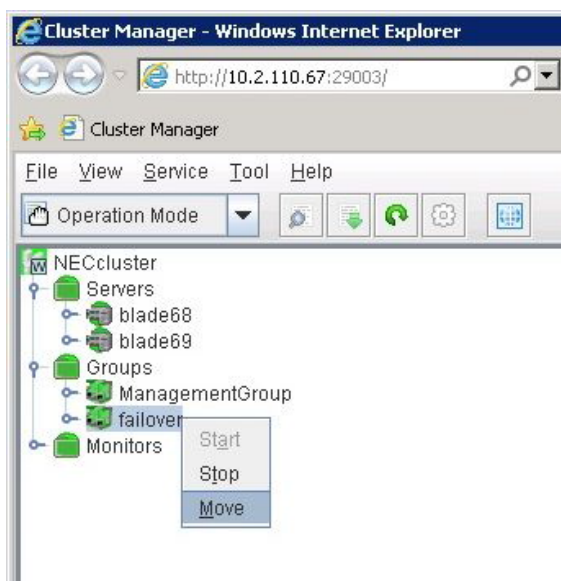
- 8 Add `rem` to the beginning of the lines as follows:

```
rem armload MSSQL /s /a /r 3 /fov /wait 30 MSSQL$SQLEXPRESS
rem armload GenetecServer /s /a /r 3 /fov GenetecServer
rem armload GenetecWatchdog /s /a /r 3 /fov GenetecWatchdog
```

- 9 Click **File > Save**, and then click **File > Exit**.
- 10 In the *NEC WebManager*, click **Apply > OK**.
- 11 Click **File > Apply the Configuration File**.
- 12 To confirm your changes, click **Yes > OK**.
- 13 From the drop-down list at the top of the *NEC WebManager*, select **Operation Mode**.
- 14 Click **Groups > failover**.
- 15 In the **Started Server** row, see which server is active.
- 16 Connect to the active server, and make sure that Config Tool and Security Desk are not running.
- 17 Upgrade Security Center.
For more information about upgrading to Security Center 5.11, see the *Security Center Installation and Upgrade Guide*.
- 18 Start Config Tool and Security Desk, and confirm that everything is working properly.

19 In the *NEC WebManager*, force the active server to failover to the standby server as follows:

- a) Under **Groups**, right-click **failover**, and then click **Move**.



- b) Select the standby server in the list.

The standby server becomes the active server.

20 Repeat **Step 16** to **Step 19** on the active server.

21 To set the NEC ExpressCluster back to normal operation mode, enable automatic failover as follows:

- From the drop-down list in the *NEC WebManager*, select **Config Mode**.
- Click **Groups > failover**.
- In the **Resources** tab, right-click **script**, and then click **Properties**.
- Click the **Details** tab.
- Select the *start.bat* file, and then click **Edit**.
- Find the following lines of code:

```
rem armload MSSQL /s /a /r 3 /fov /wait 30 MSSQL$SQLEXPRESS
rem armload GenetecServer /s /a /r 3 /fov GenetecServer
rem armload GenetecWatchdog /s /a /r 3 /fov GenetecWatchdog
```

- g) Remove **rem** from the beginning of the lines as follows:

```
armload MSSQL /s /a /r 3 /fov /wait 30 MSSQL$SQLEXPRESS
armload GenetecServer /s /a /r 3 /fov GenetecServer
armload GenetecWatchdog /s /a /r 3 /fov GenetecWatchdog
```

- Click **File > Save**, and then click **File > Exit**.
- In the *NEC WebManager*, click **Apply > OK**.

22 Click **File > Apply the Configuration File**.

23 To confirm your changes, click **Yes > OK**.

24 From the drop-down list at the top of the *NEC WebManager*, select **Operation Mode**.

Backward compatibility requirements for Security Center

Security Center is backward compatible with many Security Center components from the three previous major versions.

IMPORTANT: Security Center is compatible with the three previous *major versions*. A server or workstation that is three major versions behind can connect to the Directory, but one that is four major versions behind

cannot. To retain backward compatibility when upgrading your system in stages, no part of Security Center can be more than three major versions apart. For systems that are four to six major versions behind, upgrade in two steps to maintain backward compatibility.

IMPORTANT: Adding backward compatible connections slows down the performance of the Directory. It is only recommended as a temporary solution before you are able to upgrade all servers and workstations.

The requirements for Security Center backward compatibility are as follows:

- **Upgrading to the latest version:** When upgrading, you must always upgrade the main server hosting the Directory role and Config Tool. Always upgrade each expansion server hosting a role type that is not backward compatible.
- **Using new features:** To use the new features introduced in version , upgrade your Security Center servers.
- **Role assigned to multiple servers:** If a role is assigned to multiple servers, such as in a failover configuration, all of its servers must be running the same version of Security Center.
- **Directory assigned to multiple servers:** All Directory servers must use the exact same version, meaning that all four digits of their version numbers must be the same. For example, if you upgrade to Security Center , you must upgrade all Directory servers to .

Backward compatibility between Security Center roles

Each new version of Security Center includes new role features that might not be compatible with earlier versions. The Security Center roles that are backward compatible are outlined in the following table.

IMPORTANT: All expansion servers hosting a non-backward compatible role must be upgraded to the same version as the main server hosting the Directory.

| 5.11 role | Backward compatible with 5.8, 5.9 and 5.10 | |
|---|--|----|
| | Yes | No |
| Access Manager | ✓ | |
| Active Directory | ✓ (5.9 and later) | |
| ALPR Manager | ✓ | |
| Formerly LPR Manager (5.9.2.0 and earlier) | | |
| Archiver | ✓ | |
| Authentication Service (OpenID & SAML2) | | ✓ |
| Authentication Service (WS-Federation) | | ✓ |
| Formerly Active Directory Federation Services | | |
| Authentication Service (WS-Trust) | | ✓ |
| Formerly Active Directory Federation Services | | |
| Auxiliary Archiver | ✓ | |
| Camera Integrity Monitor (hidden) | ✓ | |
| Cloud Playback | ✓ (5.10.0.0 and later) | |
| Directory Manager | | ✓ |

| 5.11 role | Backward compatible with 5.8, 5.9 and 5.10 | |
|--------------------------------------|--|----|
| | Yes | No |
| Global Cardholder Synchronizer (GCS) | | ✓ |
| Health Monitor | | ✓ |
| Intrusion Manager | ✓ | |
| Map Manager | ✓ | |
| Media Gateway | ✓ | |
| Media Router | | ✓ |
| Mobile Credential Manager | ✓ (5.10.0.0 and later) | |
| Mobile Server | ✓ | |
| Omnicast™ Federation™ | ✓ | |
| Plugin (all instances) | See Supported plugins in Security Center . | |
| Point of Sale | | ✓ |
| Privacy Protector™ (hidden) | ✓ (5.7 SR1 and later) | |
| Record Caching Service | ✓ (5.10.0.0 and later) | |
| Record Fusion Service | ✓ (5.10.0.0 and later) | |
| Report Manager | | ✓ |
| Reverse Tunnel | ✓ | |
| Reverse Tunnel Server | ✓ | |
| Security Center Federation™ | ✓ | |
| Unit Assistant | ✓ (5.10.1.0 and later) ¹ | |
| Wearable Camera Manager | | ✓ |
| Web Server | ✓ | |
| Web-based SDK | ✓ | |
| Zone Manager | ✓ | |

¹ Unit Assistant is only backward compatible for the unit password management feature. The unit certificate management feature has only been introduced in 5.11.0.0.

Backward compatibility with Security Center tasks

The Security Center 5.11 tasks that are backward compatible with Security Desk 5.8, 5.9 and 5.10 are summarized in the following table:

| Task category | Task type | Backward compatible with Security Desk 5.8, 5.9 and 5.10 | |
|--------------------------------|--------------------------------------|--|----|
| | | Yes | No |
| Operation | Monitoring (live and playback video) | ✓ | |
| | Maps | ✓ | |
| | Dashboards | ✓ | |
| | Health dashboard | ✓ (5.8.1.0 and later) | |
| | Remote | | ✓ |
| | Cardholder management | ✓ ¹ | |
| | Credential management | ✓ ¹ | |
| | Visitor management | ✓ ¹ | |
| | People counting | ✓ | |
| | Hotlist and permit editor | ✓ | |
| | Inventory management | ✓ | |
| | Mustering | ✓ (5.9.0.0 and later) | |
| Alarm management | Alarm monitoring | ✓ | |
| | Alarm report | ✓ | |
| Investigation | Genetec Clearance™ activities | See Supported plugins in Security Center . | |
| | Incidents | ✓ | |
| | Transactions | | ✓ |
| | Zone activities | ✓ | |
| | Area activities | ✓ | |
| Investigation > Access control | Door activities | ✓ | |
| | Cardholder activities | ✓ | |
| | Visitor activities | ✓ | |
| | Area presence | ✓ | |
| | Time and attendance | ✓ | |

| Task category | Task type | Backward compatible with Security Desk 5.8, 5.9 and 5.10 | |
|-------------------------------------|-------------------------------------|--|----|
| | | Yes | No |
| | Credential activities | ✓ | |
| | Credential request history | ✓ | |
| | Elevator activities | ✓ | |
| | Visit details | ✓ ¹ | |
| | | | |
| Investigation > Asset management | Asset activities | | ✓ |
| | Asset inventory | | ✓ |
| Investigation > ALPR | Hits | ✓ | |
| | Hits (Mutli-region) | ✓ | |
| | Reads | ✓ | |
| | Reads (Mutli-region) | ✓ | |
| | Patroller tracking | ✓ | |
| | Inventory report | ✓ | |
| | Daily usage per Patroller | ✓ | |
| | Logons per Patroller | ✓ | |
| | Reads/hits per day | ✓ | |
| | Reads/hits per zone | ✓ | |
| | Zone occupancy | ✓ | |
| | Parking sessions | ✓ | |
| | Parking zone activities | ✓ | |
| | | | |
| | | | |
| Investigation > Intrusion detection | Intrusion detection area activities | ✓ | |
| Investigation > Record fusion | Records | ✓ (5.10.0.0 and later) | |
| Investigation > Video | Archives | ✓ | |
| | Bookmarks | ✓ | |
| | Camera events | ✓ | |
| | Motion search | ✓ | |
| | Video file explorer | ✓ | |

| Task category | Task type | Backward compatible with Security Desk 5.8, 5.9 and 5.10 | |
|------------------------------|---------------------------------|--|----|
| | | Yes | No |
| Maintenance | Forensic search | ✓ | |
| | Security video analytics | ✓ | |
| | System status | ✓ | |
| | Audit trails | ✓ | |
| | Activity trails | ✓ | |
| | Health history | ✓ | |
| | Health statistics | ✓ | |
| Maintenance > Access control | Hardware inventory | ✓ | |
| | Access control health history | ✓ | |
| | Access control unit events | ✓ | |
| | Cardholder access rights | ✓ | |
| | Door troubleshooter | ✓ | |
| | Access rule configuration | ✓ | |
| | Cardholder configuration | ✓ ¹ | |
| | Credential configuration | ✓ | |
| | I/O configuration | ✓ | |
| | Intrusion detection unit events | ✓ | |
| Maintenance > Video | Camera configuration | ✓ | |
| | Archiver events | ✓ | |
| | Archiver statistics | ✓ | |
| | Archive storage details | ✓ | |
| | Wearable camera evidence | ✓ | |

¹ Saved reports that use filters with **During the next** time intervals are not compatible with Security Desk 5.8 and earlier.

Configuring Security Center NEC Cluster

This section includes the following topics:

- ["Configuring Security Center Server for the cluster"](#) on page 28
- ["Configuring Directory authentication in a cluster environment"](#) on page 30
- ["Configuring the mirrored VertX settings folder"](#) on page 31
- ["Configuring SQL Server for the cluster"](#) on page 32
- ["Configuring NEC ExpressCluster X Edition"](#) on page 36
- ["Cluster configuration tests"](#) on page 39

Configuring Security Center Server for the cluster

You must make some changes to Security Center Server for it to be protected with failover by the cluster.

To configure Security Center Server for the cluster:

- 1 Move the server's license file to a non-mirrored folder, and move the configuration files to a mirrored disk.
- 2 Stop the Genetec™ Watchdog service from restarting the Genetec™ Server service.
The cluster will monitor and control the Genetec™ Server service, so you do not want the Genetec™ Watchdog service trying to start or stop the server anymore.

Moving Security Center server's license and configuration files

As part of configuring Security Center Server for a clustered environment, you must move the server's license file to a non-mirrored folder, and move the configuration files to a mirrored disk.

To move Security Center server's license and configuration files:

- 1 On both servers, stop the Genetec™ Watchdog service and the Genetec™ Server service.
 - a) Click **Start > Control Panel > Administrative Tools > Services**.
 - b) Select the *Genetec™ Watchdog* service and click **Stop Service** on the toolbar at the top of the page.
 - c) Select the *Genetec Server* service and click **Stop Service** on the toolbar at the top of the page.
 - d) Minimize, but don't close the *Services* window.
- 2 Move the Genetec™ Server's license file (*license.gconfig*) from *C:\Program Files\Genetec Security Center 5.11\ConfigurationFiles* to the Security Center root folder (*C:\Program Files\Genetec Security Center 5.11*).
- 3 Using **Notepad**, paste the following text into an empty text file:

```
<?xml version="1.0" encoding="utf-8" ?>
<configurationPath path="N:\Genetec Security Center 5.11\ConfigurationFiles">
  <forceRoot name="License"/>
</configurationPath>
```

This file contains four lines. It will point to your mirrored data drive ("N:" is used in the example) as the location of your configuration files and your local root folder as the location of your license file. If your mirrored data drive is configured differently, adjust the file with your mirrored drive path.

- 4 Save the text file with the name *ConfigurationPath.gconfig* in your Security Center root folder (*C:\Program Files\Genetec Security Center 5.11*)
- 5 Repeat the steps on your standby server.

A supplementary server configuration file called *ConfigurationPath.gconfig* is created. This file tells the server to look in an alternative path for your configuration files (the mirrored data drive) and an alternative path for the server license.

Stopping Genetec™ Watchdog from restarting Genetec™ Server

Once clustering is set up, the cluster will monitor and control the Genetec™ Server service, so you do not want the Genetec™ Watchdog service trying to start or stop the Genetec™ Server service anymore.

To stop the Genetec™ Watchdog service from restarting the Genetec™ Server service:

- 1 Use Notepad to open the file *GenetecWatchdog.gconfig* found in the path *N:\Program Files\Genetec Security Center 5.11\ConfigurationFiles*.

- 2 Edit the file to include the string: `preventServiceRestart="true"`.

The third line now reads:

```
<Watchdog serverPort="4534" registrationRetryDelay="00:00:15"  
  responsivenessTimeout="00:02:00" emailFilterLevel="None"  
  preventServiceRestart="true">
```

- 3 Repeat the steps on your standby server.
- 4 Start the Genetec™ Server service on both servers.

Configuring Directory authentication in a cluster environment

If you are using trusted certificates to communicate with the Security Center Directory in a cluster environment, you must configure a shared folder for all nodes in the cluster, and you must install the same certificate and its private key on all nodes. From the clients' perspective, all nodes in a cluster are the same server, therefore, they must all use the same certificate.

What you should know

During Security Center installation, you have the option to force all client and server applications to validate the identify certificate of the Directory before connecting to it. With Directory authentication enabled, users are prompted to accept all unknown Directory certificates. If accepted, the certificate is put in a list of trusted certificates, known as the white list, and the same users will not be prompted again in the future when connecting to the same Directory.

To configure trusted Directory certificates in a clustered environment:

- 1 Perform the following on all nodes found in your cluster:
 - a) Open the configuration file: `<InstallDir>\Configuration files\GeneralSettings.gconfig`.
`<InstallDir>` is the installation folder usually located at:
`N:\Program Files (x86)\Genetec Security Center 5.11`.
 - b) Between the `<Configuration>``</Configuration>` XML markers, add the following line and save the file:
`<certWhiteList CertificateCacheFolder="N:\temp\cache" />`
NOTE: "N:\V" represents the drive letter to the server's external storage medium.
 The location of your white list certificate cache is now configured on the node.
- 2 Export the identity certificate of the master node, along with its private key, and install it on the personal certificate store of the secondary nodes.

Configuring the mirrored VertX settings folder

If you have HID VertX controllers on your system, the VertX specific settings must be found in the mirrored data partition so the Access Manager does not need to re-synchronize all units every time the active node switches machine.

Before you begin

Make sure you have created the folder `N:\VertX` on the mirrored data partition.

What you should know

Specific settings for VertX units are stored in a file named *VertXConfig.gconfig*. This file is saved by default in the folder `C:\Program Files\Genetec Security Center 5.11\ConfigurationFiles` on the server hosting the Access Manager role. This file is not created by default if only default VertX settings are being used.

To configure the mirrored VertX settings folder:

- 1 Create or modify the file *VertXConfig.gconfig* using one of the following methods.
 - If the file does not exist, use Notepad, and paste the following text into an empty text file:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <Vertx VertXFolderPath="N:\VertX"/>
</configuration>
```

- If this file already exists, add the attribute `VertXFolderPath="N:\VertX"` to the file.

The folder `"N:\VertX"` is the folder you created on the mirrored data partition. The path must be absolute. Relative paths are not accepted.

- 2 Save or move the file *VertXConfig.gconfig* to the configuration files folder on the mirrored data partition (we used `N:\Genetec Security Center 5.11\ConfigurationFiles` in our example).
- 3 If you are moving from a non-clustered to a clustered environment, move all existing VertX-specific subfolders from the Security Center root folder to the mirrored VertX settings folder.

The VertX-specific subfolders are:

- `\VertXConfigAndLogs`
- `\VertXEEPROMCache`
- `\VertXFileCache`
- `\VertXTempFiles`

After you finish

All VertX unit settings and unit synchronization statuses will be saved to this mirrored folder.

Configuring SQL Server for the cluster

To configure your SQL database server for a clustered environment, you must move the database to your mirrored data partition so that the contents of the database are identical on the active server and the standby server.

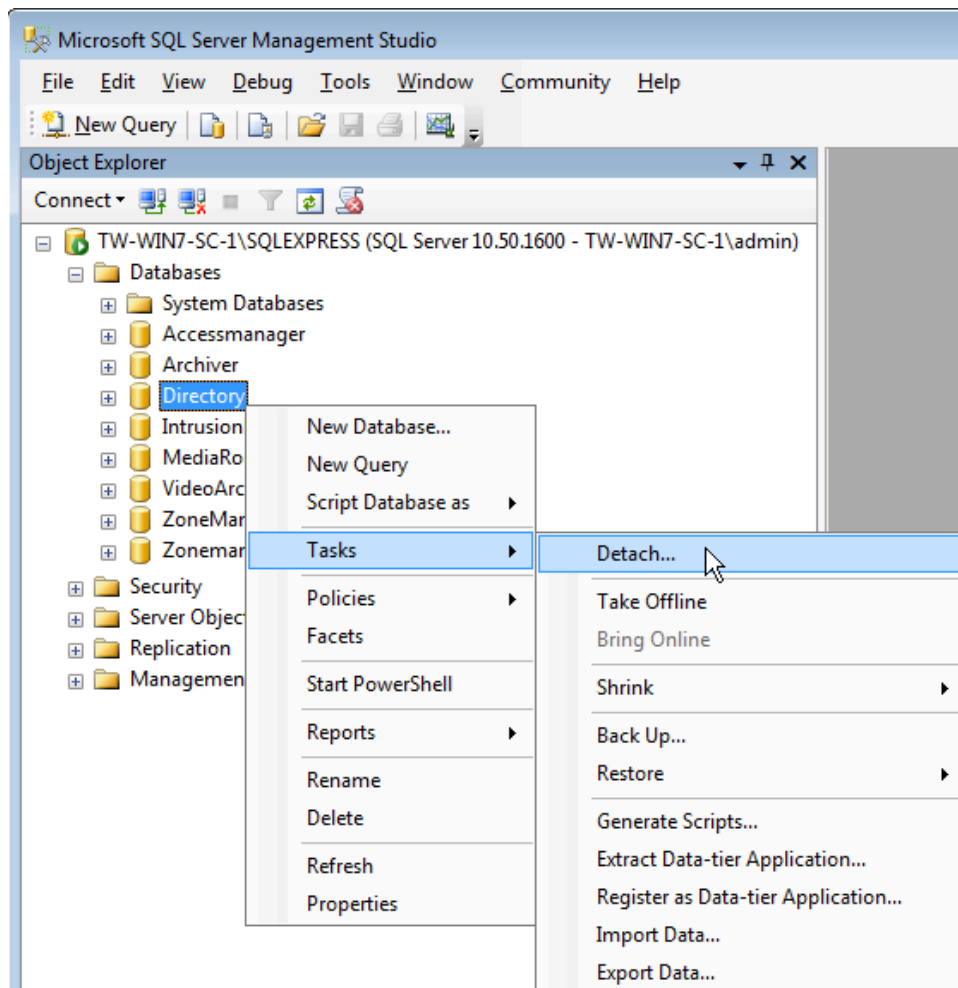
To configure the SQL Server for the cluster:

- 1 On both servers, stop the Genetec™ Watchdog service and the Genetec™ Server service as follows:
 - a) Click **Start > Control Panel > Administrative Tools > Services**
 - b) Select the *Genetec™ Watchdog* service and click **Stop Service** on the toolbar at the top of the page.
 - c) Double-click the *Genetec™ Watchdog* service and set the **Startup Type** to **Manual**.
 - d) Select the *Genetec Server* service and click **Stop Service** on the toolbar at the top of the page.
 - e) Double-click the *Genetec™ Server* service and set the **Startup Type** to **Manual**.

- 2 In *SQL Management Studio*, you will need detach all Security Center databases before the database files can be moved to your mirrored data partition. Detaching a database removes it from the instance of the Microsoft SQL Server but leaves intact the database, with its data files and transaction log files.
 - a) Open SQL Management Studio and connect to the Security Center database instance (by default the instance name is *SQLEXPRESS*)

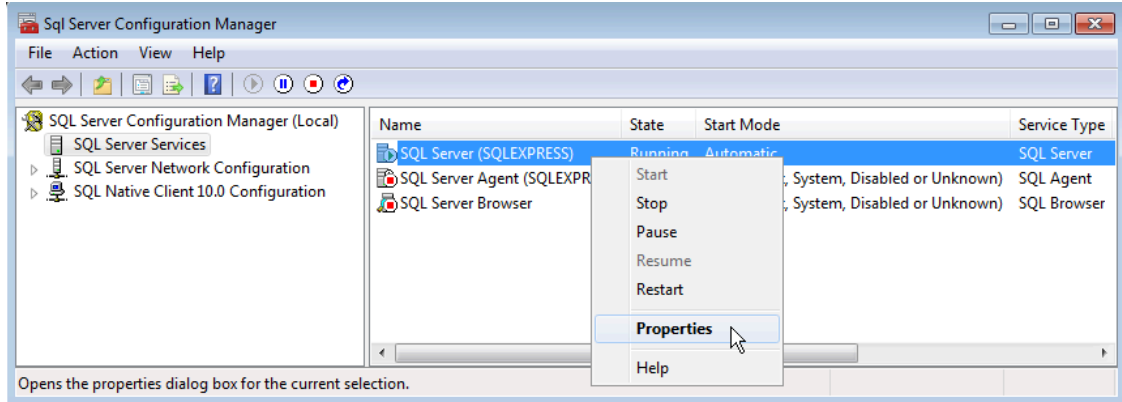


- b) Right click on each one of the Security Center databases and select **Task > Detach**.

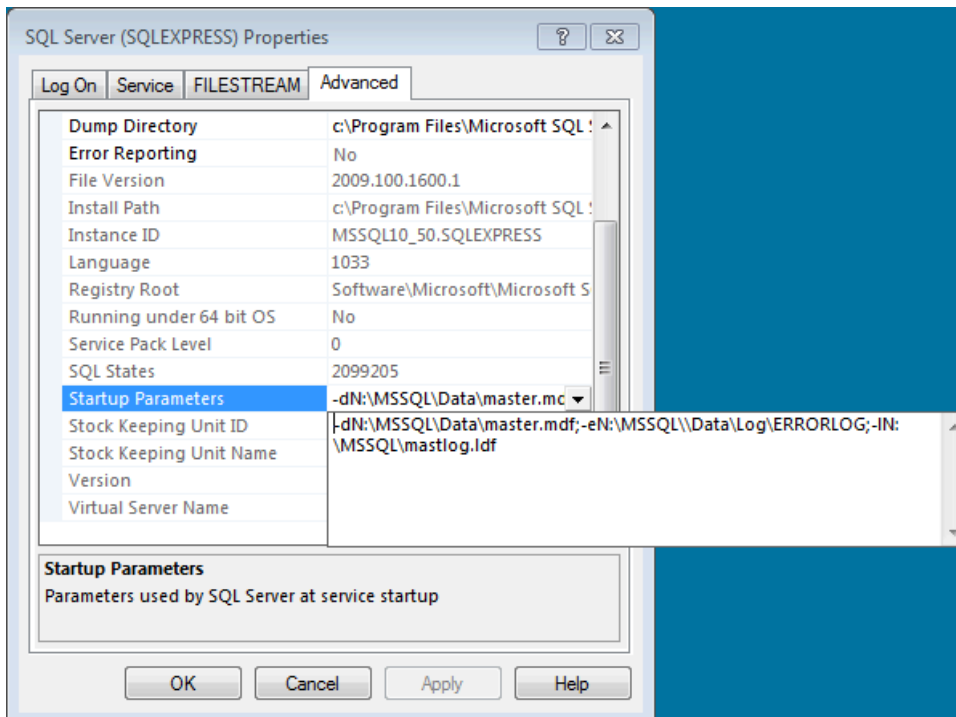


- 3 Move the Security Center *.MDF and *.LDF database files from their default folder (*C:/Program Files/Microsoft SQL Server/MSSQL10_50.SQLEXPRESS/MSSQL/DATA*) to the SQL folder on the mirror partition created earlier (*N:/MSSQL/DATA*).

- 4 Stop the SQL service on both servers.
- 5 Using *SQL Server Configuration Manager*, modify the SQL startup parameters for the master database on both servers.
 - a) Open your *SQL Server Configuration Manager*.
 - b) Select **SQL Server Services** in the pane on the left.
 - c) Right-click on **SQL Server (SQLEXPRESS)** and select **Properties**.



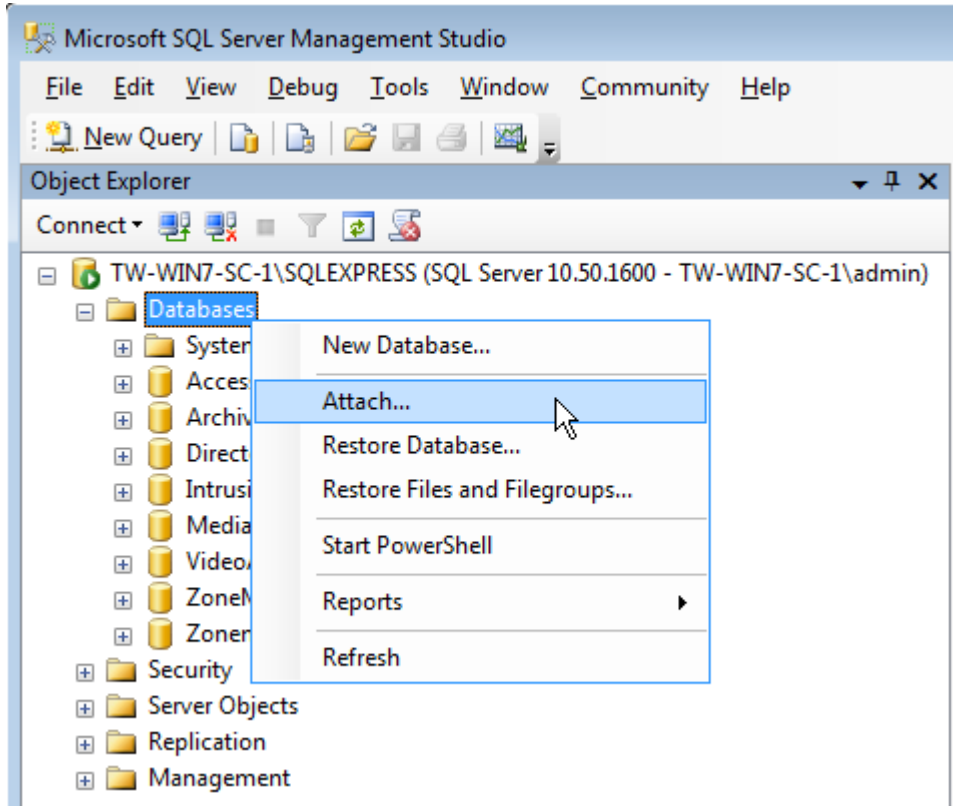
- d) Select the **Advanced** tab in the **SQL Server (SQLEXPRESS) Properties** window.
- e) Modify the field **Startup Parameters** to point to the new master database path.



In this example we have modified the startup parameters to: **-dN:/MSSQL/Data/master.mdf;-eN:/MSSQL/Data/Log/ERRORLOG;-IN:/MSSQL/mastlog.ldf**, whereby the field points to the new (mirrored) drive and folder path of our master database (N:/MSSQL/Data).

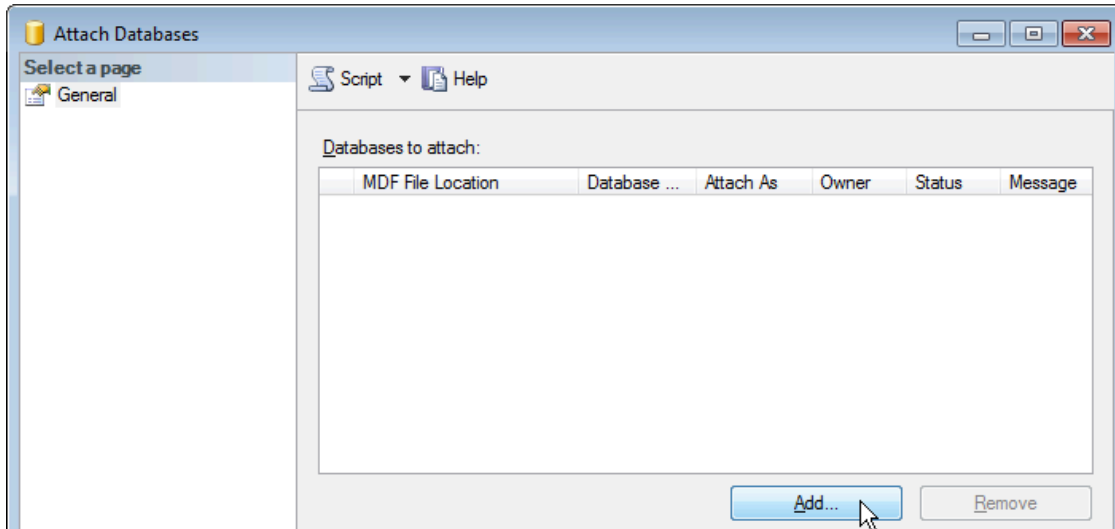
- 6 Move the master database (master.mdf and master.ldf) for the active server to the SQL folder on the mirror partition created earlier (*N:/MSSQL/DATA*). Delete the master database (master.mdf and master.ldf) on the standby server (it will be replicated from the active server).
- 7 Restart SQL service on both servers.
- 8 Reconnect SQL Management studio to SQL server for the active server.

- 9 Re-attach the Security Center databases.



- 10 When prompted to point to the database to be attached, use the **Add** button to browse to the new path of your (moved) master database.

IMPORTANT: This step needs to be performed on the standby server as well but it is not possible at this point. Once the cluster configuration has been completed, you will need to force a failover to the standby server, then connect SQL Management Studio to its SQL server to re-attach the same databases.



- 11 Make sure that all the databases that were previously detached are re-attached.

Configuring NEC ExpressCluster X Edition

Before the NEC cluster can offer failover protection, you must create two script files, and use the *NEC WebManager* to configure the cluster.

To configure NEC ExpressCluster X Edition:

- Create the script files.
- Create the cluster.
- Finalize the cluster configuration.

Creating the script files manually

You must create two scripts files before the NEC cluster can offer failover protection.

What you should know

The required script files are called *Start.bat* and *Stop.bat*. They can be found in the */Tools* folder of your Security Center installation package, or downloaded from GTAP, at <http://portal.genetec.com/support>.

To create the script files manually:

- 1 To prepare your *start.bat* script, open Notepad and paste the following lines of code:

```
rem *****
rem *                start.bat                *
rem *****

IF "%CLP_EVENT%" == "START"    GOTO GEN_PROC
IF "%CLP_EVENT%" == "FAILOVER" GOTO GEN_PROC
IF "%CLP_EVENT%" == "RECOVER" GOTO EXIT

rem CLUSTERPRO Server is not started
ARMBCAST /MSG "CLUSTERPRO Server is offline" /A
GOTO EXIT

rem *****
rem Normal Startup process
rem *****
:GEN_PROC

rem Check Disk
IF "%CLP_DISK%" == "FAILURE" GOTO ERROR_DISK

rem Start services
armload MSSQL /s /a /r 3 /fov /WAIT 30 MSSQL$SQLEXPRESS
armload GenetecServer /s /a /r 3 /fov GenetecServer
armload GenetecWatchdog /s /a /r 3 /fov GenetecWatchdog
GOTO EXIT

rem *****
rem Irregular process
rem *****

rem Process for disk errors
:ERROR_DISK
ARMBCAST /MSG "Failed to connect the switched disk partition" /A
GOTO EXIT

:EXIT
```

- 2 Save the file in a temporary location like your Windows desktop with the name *Start.bat*.

- 3 To prepare your *Stop.bat* script, open Notepad and paste the following lines of code:

```
rem *****
rem *                stop.bat                *
rem *****

IF "%CLP_EVENT%" == "START"    GOTO GEN_PROC
IF "%CLP_EVENT%" == "FAILOVER" GOTO GEN_PROC

rem CLUSTERPRO Server is not started
ARMBCAST /MSG "CLUSTERPRO Server is offline" /A
GOTO EXIT

:GEN_PROC

rem Check Disk
IF "%CLP_DISK%" == "FAILURE" GOTO ERROR_DISK

rem ** Stop the Genetec Services **
armkill GenetecWatchdog
armkill GenetecServer
armkill MSSQL

GOTO EXIT

rem *****
rem Irregular process
rem *****

rem Process for disk errors
:ERROR_DISK
ARMBCAST /MSG "Failed to connect the switched disk partition" /A

:EXIT
```

- 4 Save the file in a temporary location like your Windows desktop with the name *Stop.bat*.

After you finish

Keep the two script files aside for the moment. They will be applied to the cluster later.

Creating the cluster

After you create the two script files, you must create the cluster itself using the NEC WebManager application.

To create the cluster:

- 1 Open the *NEC WebManager* on your cluster management workstation.
- 2 From the **File** menu, select **Cluster Generation Wizard**
- 3 Refer to your planning checklist to configure your new cluster through the wizard.

Related Topics

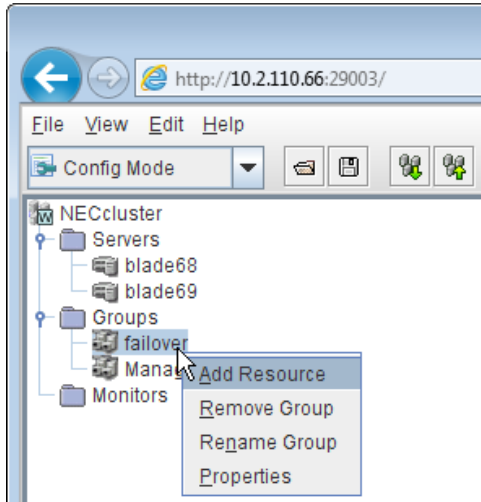
[Planning checklist for NEC cluster](#) on page 6

Finalizing the cluster configuration

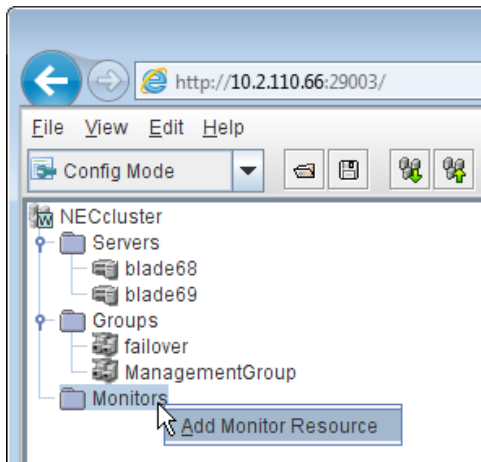
After creating the cluster, you must configure it.

To finalize the cluster configuration:

- 1 Use the *NEC ClusterManager* application on the workstation used for cluster management to add the *Start script* and *Stop script* batch files.
- 2 Change the Cluster Manager's view from **Operation mode** to **Configuration mode**.
- 3 Right-click the failover group and select **Add Resource**.
The **Resource Definition of Group (failover)** wizard opens.



- 4 Select **Type: script resource**, and click **Next**.
- 5 Accept the defaults for **dependencies**, and click **Next**.
- 6 Accept the defaults for **Recovery operations**, and click **Next**.
- 7 On the **Scripts** page, click **Add** and select your *Start.bat* script file.
- 8 On the **Scripts** page, click **Add** and select your *Stop.bat* script file.
- 9 Click **Finish**.
- 10 Right-click **Monitors**, and select **Add Monitor Resource**.



- 11 Add the following **Monitors**:
 - **IP monitor** for your network gateway.
 - **Mirror connect monitor** for your clustered mirror disk.
 - **Mirror disk monitor** for your clustered mirror disk.
 - **NIC Link Up/Down monitor** for your active server and standby server's public network interface.
 - **Service monitor** for the Microsoft SQL Server.

Cluster configuration tests

To test your Security Center cluster configuration, try the following four failover tests:

| Description of task | Data transition time |
|---|----------------------|
| Failover Test #1 - NEC move operation | |
| Using the NEC ClusterManager, perform a “move” operation to switch active to standby and standby to active. The standby server should become active and the active should become standby. | 10 minutes |
| Let the servers operate for a period of 30 minutes. | n/a |
| Using the NEC ClusterManager, perform a “move” operation to revert to the original configuration. | 10 minutes |
| Failover Test #2 - Windows OS shutdown of Security Center and active server | |
| Perform a standard Windows shutdown of the Security Center and Omnicast™ Primary servers, failover to Secondary Security Center and Omnicast™ servers. | 5 minutes |
| Let the Secondary failover servers operate for a period of 30 minutes. | n/a |
| After 30 minutes, bring up the Primary Security Center and Omnicast™ servers and switch operation back to these servers from the Secondary servers | 5 minutes |
| Failover Test #3 - Disconnect the Public NIC on the Security Center active server | |
| Disconnect the Public NIC on the Security Center active server. Operations should automatically switch over to the standby server. | 5 minutes |
| Let the secondary failover server operate for a period of 30 minutes. | n/a |
| Reconnect the Public NIC on Security Center's primary server. | 5 minutes |
| Failover Test #4 - Disconnect the Interconnect NIC on Security Center active server used to relay the heartbeat of primary server to secondary (failover) server | |
| Disconnect the network cable on the Security Center primary server used to relay the heartbeat of the server to the secondary (failover) server; operations should continue to be maintained by the primary server. | n/a |
| Keep the network cable disconnected for a period of 30 minutes. | n/a |
| Reconnect the network cable on the Security Center primary server; wait for the SQL database on the secondary (failover) server to get updated. | 5 minutes |

Where to find product information

You can find our product documentation in the following locations:

- **Genetec™ TechDoc Hub:** The latest documentation is available on the TechDoc Hub. To access the TechDoc Hub, log on to [Genetec™ Portal](#) and click [TechDoc Hub](#). Can't find what you're looking for? Contact documentation@genetec.com.
- **Installation package:** The Installation Guide and Release Notes are available in the Documentation folder of the installation package. These documents also have a direct download link to the latest version of the document.
- **Help:** Security Center client and web-based applications include help, which explains how the product works and provide instructions on how to use the product features. To access the help, click **Help**, press F1, or tap the ? (question mark) in the different client applications.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec™ TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

To access the TechDoc Hub, log on to [Genetec™ Portal](#) and click [TechDoc Hub](#). Can't find what you're looking for? Contact documentation@genetec.com.

- **Genetec™ Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec™ Lifecycle Management (GLM) documents: [Genetec™ Assurance Description](#) and [Genetec™ Advantage Description](#).

Additional resources

If you require additional resources other than the Genetec™ Technical Assistance Center, the following is available to you:

- **Forum:** The Forum is an easy-to-use message board that allows clients and employees of Genetec Inc. to communicate with each other and discuss many topics, ranging from technical questions to technology tips. You can log on or sign up at <https://gtapforum.genetec.com>.
- **Technical training:** In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to <http://www.genetec.com/support/training/training-calendar>.

Licensing

- For license activations or resets, please contact GTAC at <https://portal.genetec.com/support>.
- For issues with license content or part numbers, or concerns about an order, please contact Genetec™ Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, please contact Genetec™ Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Please contact GTAC at <https://portal.genetec.com/support> to address any issue regarding Genetec™ appliances or any hardware purchased through Genetec Inc.