Security Center 5.2
Installation Guide for Windows Cluster

Click [here](#) for the most recent version of this document.
About this guide

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

The procedures in this guide can be extended to additional nodes.

This guide is written for those responsible for installing Security Center. It assumes you are familiar with the following concepts and systems:

- Genetec's Security Center solution and its architecture
- Windows system administration
- Windows Server 2008 Failover Clustering and its deployment

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.
Before you install

This section describes what you need to know and do before installing and configuring your clustered Security Center system.

This section includes the following topics:

- "About the Windows Server failover cluster for Security Center" on page 2
- "System setup" on page 3
- "Which roles can fail over?" on page 4
- "Windows Failover Clustering terminology" on page 4
- "Planning checklist" on page 6
About the Windows Server failover cluster for Security Center

A Windows 2008 Server failover cluster ensures fast application recovery and data protection in case of a system failure. If your active Security Center server fails, the failover server in the cluster will bring Security Center back online.

A virtual IP address is used to accept incoming client connections. The cluster then monitors the active server. If a failure is detected, the cluster replaces the active server with the failover 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.
System setup

This section describes the setup and configuration of a two node (two servers) failover cluster on a Windows Server 2008 operating system. Your Security Center server and SQL Server 2008 R2 will be protected by the Windows cluster.

Before installing and configuring your clustered Security Center system, make sure you have the following:

- A Windows Server 2008 failover cluster must already be installed and operational.
- A Microsoft SQL Server 2005 or 2008 instance must already be installed and operational.
- You must have the Security Center installation DVD available.

The configuration that we will be using requires three distinct networks:

1. **Data network**: Used for general network communications. This network should be used for video traffic, access control, DNS queries, time synchronization, remote management, and Active Directory authentication. Additionally, a floating IP address must be configured on this network for connecting the clustered Security Center services, the non-clustered Security Center services that may be running on standalone servers, and the Security Center Client applications.

2. **Cluster network**: Used for inter-node communication only. It is recommended to dedicate a separate network on a different subnet for the cluster heartbeat. If there are only two nodes in the cluster, using a crossover link between them is recommended.

3. **Storage network**: External storage is required for successful Windows clustering of a Security Center system. The storage will contain the SQL database files, the Security Center files and (possibly) the video recording files.

**NOTE** As of Windows 2008, all clustered nodes must be part of the same Active Directory domain and must be capable of resolving each other's host names via DNS or the host file. It is recommended to deploy multiple redundant domain controllers and DNS servers on the DATA network to ensure the cluster's uptime in case of domain controller or DNS server failure.
Which roles can fail over?

Security Center server roles supported for failover with Windows ExpressCluster:

- Directory role
- Active Directory role
- Access Manager role
- Report Manager role
- Archiver role
- Zone Manager role
- Intrusion Manager role
- Omnicast federation role

Windows Failover Clustering terminology

This guide uses the following terms to describe the components of a Windows Failover Cluster:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public network</td>
<td>Also known as the <em>Data network</em>. The network hosting the Security Center server and clients.</td>
</tr>
<tr>
<td>Private network</td>
<td>Also known as <em>Cluster network</em>. The dedicated link connecting the two clustered servers together.</td>
</tr>
<tr>
<td>Active node</td>
<td>The clustered server actively managing Security Center.</td>
</tr>
<tr>
<td>Passive node</td>
<td>The clustered server waiting on standby.</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>The cluster’s health-monitoring mechanism between cluster nodes. This health checking allows nodes to detect failures of other servers.</td>
</tr>
<tr>
<td>Resource</td>
<td>A hardware or software component in a failover cluster (such as a disk, an IP address, or a network name).</td>
</tr>
</tbody>
</table>
**Minimum server requirements**

Your servers should be identical in terms of hardware, operating system, and software. Windows Server 2008 cluster, SQL server and Security Center each have their own set of minimum requirements. This table lists the minimum requirements as a combination of all three:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating system</strong></td>
<td>This guide is based on clustering Security Center server in a Windows Server 2008 environment. Windows Server 2003 is also supported for the clustering of Security Center server.</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>External storage for Security Center server’s configuration files, database files and video archives (if the server is managing an archiver role) is required. Serial attached SCSI, Fibre channel or iSCSI are recommended.</td>
</tr>
<tr>
<td><strong>Network cards</strong></td>
<td>A minimum of two network cards are required. One for the public (data) network and one for the private (cluster) network. A third network card may be required for connection to the external storage.</td>
</tr>
<tr>
<td><strong>SQL Server</strong></td>
<td>While SQL Express is bundled with the Security Center installation disk, it is not supported for clustering. Instead, SQL Standard or Enterprise (2005 or 2008) must be used.</td>
</tr>
</tbody>
</table>
Planning checklist

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Windows domain accessible from data network</td>
<td>ClusterDomain</td>
</tr>
<tr>
<td>Security Center Domain</td>
<td>Used for the Security Center services. Must be local admin on all cluster nodes.</td>
<td>DOMAIN\SecurityCenterServices</td>
</tr>
<tr>
<td>SQL Server IP Address</td>
<td>IP Address of Microsoft SQL Server engine</td>
<td>172.16.1.20</td>
</tr>
<tr>
<td>SQL Server Host Name</td>
<td>Optional host name of SQL Server engine</td>
<td>SQLHostName</td>
</tr>
<tr>
<td>SQL Server instance</td>
<td>Microsoft SQL Server instance name.</td>
<td>SQLInstance</td>
</tr>
<tr>
<td>Cluster Name</td>
<td>Name of the cluster</td>
<td>FailoverCluster</td>
</tr>
<tr>
<td>Management IP Address</td>
<td>Floating address for management only</td>
<td>172.16.0.100</td>
</tr>
<tr>
<td>Security Center IP Address</td>
<td>Floating IP address used by Security Center</td>
<td>172.16.0.200</td>
</tr>
<tr>
<td>Security Center subnet</td>
<td>Subnet mask for Data network</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>Host name</td>
<td>Network name of the cluster node</td>
<td>ClusterNode1</td>
</tr>
<tr>
<td>IP Address 1</td>
<td>IP Address on data network</td>
<td>172.16.0.1</td>
</tr>
<tr>
<td>Subnet 1</td>
<td>Subnet mask on data network</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>DNS Server</td>
<td>DNS server on the data network</td>
<td>172.16.1.10</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Network gateway on data network</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>IP Address 2 (Optional)</td>
<td>IP Address on cluster network. (Not mandatory if only using two network cards)</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>Subnet 2 (Optional)</td>
<td>Subnet mask on cluster network. (Not mandatory if only using two network cards)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Host name</td>
<td>Network name of the cluster node</td>
<td></td>
</tr>
<tr>
<td>IP Address 1</td>
<td>IP Address on data network</td>
<td>172.16.0.2</td>
</tr>
<tr>
<td>Subnet 1</td>
<td>Subnet mask on data network</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>DNS Server</td>
<td>DNS server on the data network</td>
<td>172.16.1.10</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Network gateway on data network</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>IP Address 2 (Optional)</td>
<td>IP Address on cluster network.  (Not mandatory if only using two network cards)</td>
<td>192.168.1.2</td>
</tr>
<tr>
<td>Subnet 2 (Optional)</td>
<td>Subnet mask on cluster network. (Not mandatory if only using two network cards)</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Installing Security Center in a Windows Server 2008 Failover Cluster

This section explains how to install Security Center in a Windows cluster environment.

This section includes the following topics:

- "Install Windows Server 2008 cluster and SQL 2008 Server" on page 9
- "Prepare the servers' operating systems" on page 10
- "Install Security Center server" on page 11
1 Install your Windows cluster.

The design and installation of a Windows Server failover cluster is outside of the scope of this guide. However, step by step guides and other technical documentation is available from Microsoft to guide you through the cluster installation process:


2 Install your SQL server into the cluster.

The installation of a clustered SQL server is outside of the scope of this guide. However, step by step guides and other technical documentation is available from Microsoft to guide you through the SQL cluster installation process:

- http://support.microsoft.com/kb/254321

**IMPORTANT** When installing the new database server, the SQL Server software files can be installed in the default path on the C: drive but the database itself must reside on the external storage so that it can be used by both servers in the cluster.
Prepare the servers’ operating systems

Before you begin: Before deploying the Security Center server on to the failover cluster, the following procedures must be performed on the servers:

1. Create an Active Directory Domain Account for the Security Center services.
   - Log on to the Active Directory domain controller of the Windows domain that the cluster nodes are part of.
   - Create a new user account on the domain named Security CenterServices.
   - Ensure that this domain account has local administrative rights on all cluster nodes.

2. Enable permissions to log on to the Microsoft SQL Server.
   - Log onto the Microsoft SQL Server engine and add the domain account created above as an administrative login of the Microsoft SQL Server engine.

3. Disable the Windows Firewall service.
   - Log on to the first node in the cluster using an administrative Windows account.
   - To view the active Windows services list, click on Start > Run, and enter services.msc.
   - Double-click on the Windows Firewall service.
   - In the Windows Firewall Properties window, set Manual as the Startup type. Click Stop (if available) and then OK.
   - Repeat this procedure on all remaining cluster nodes.

4. Set the Windows Network Interface Binding Order.
   - The network interface on the data network must be Windows’ first available network interface.
   - Log on to the first node in the cluster using an administrative Windows account.
   - To view the network interface properties, click Start > Run, and enter ncpa.cpl
   - If the Advanced menu does not appear at the top of the window, press the Alt key on the keyboard.
   - Click Advanced > Advanced Settings
   - Select the connection corresponding to the data network and use the arrow buttons on the right to bring it to the top of the list
   - Click OK to save the settings.
   - Repeat this procedure on all remaining cluster nodes.
Install Security Center server

**IMPORTANT**  A Security Center server license is needed for each server node.

**NOTE**  Security Center must be installed on all cluster nodes.

1. Log on to the first node in the cluster using the domain account created for the Security Center services earlier.

2. Insert the Security Center software DVD, launch the Setup utility, and click on Server installation.

3. Follow the Security Center server installation wizard installing a server with the Directory role.

4. At the Database Server Selection page, do the following:
   a. Select Use an existing database server.
   b. In the Database Server field, enter the Microsoft SQL Server instance in the SERVER\Instance format.
      **NOTE**  You must choose the correct pre-existing database server in order for the Windows 2008 Server Failover Clustering to function properly.

5. Click Next.

6. At the Services logon parameters page, do the following:
   a. Select Specify the username and password for all services.
   b. In the Username field, enter the Security Center Services domain account name created earlier using the DOMAIN\Account format.
   c. In Password field, enter the account password.
   d. Click Next.

7. Click Install to begin the Security Center installation process.

8. At the end of the installation, the Security Center Server Admin will be launched by the Security Center installer.

9. Activate the Security Center Directory license that is dedicated to this server.

10. In the Server Admin, click the Genetec Server tab.

11. From the Network card drop-down list, select Any.

12. Close the Server Admin to complete the Security Center server software installation.

13. Reboot the server.
14 The Security Center services must be stopped and set to Manual startup type. To do this:
   a  Go to Control Panel > Administrative Tools > Services to open the Services management console dialog box.
   b  Double click the Genetec Server service.
   c  Click Stop to stop the service.
   d  Change the Startup type from Automatic to Manual.
   e  Click OK to save the changes.
15 Repeat Step 14 for the Genetec Watchdog service.
16 Repeat Step 1 to Step 15 for all nodes of the cluster.
Configuring your Security Center
Windows cluster

This section explains how to configure Security Center once the cluster software, Security Center Server, and SQL Server have been installed.

This section includes the following topics:

- "Move the server’s configuration files and license file" on page 14
- "Prepare the script for access control" on page 15
Move the server's configuration files and license file

The Genetec Server’s configuration files must be moved to the shared external storage, and the server’s license file must be moved to an alternative folder path.

1. On both servers, stop the Genetec Server service and move the license file (license.gconfig) from C:\Program Files\Genetec Security Center 5.2\ConfigurationFiles to the Security Center root folder (C:\Program Files\Genetec Security Center 5.2).

2. Using Notepad, create a file called ConfigurationPath.gconfig in the root folder to indicate the location (on your mirrored disk) of the configuration files.

   This file will contain four lines. It will point to your mirrored data drive as the location of your configuration files and your local root folder as the location of your license file. You can use the following as the contents of your ConfigurationPath.gconfig file.

   ```xml
   <?xml version="1.0" encoding="utf-8" ?>
   <configurationPath path="N:\Genetec Security Center 5.2 ConfigurationFiles">
       <forceRoot name="License"/>
   </configurationPath>
   
   NOTE "N:\" represents the drive letter to the server’s external storage medium.
   
3. On the active server node, move the configuration files from their default path to the new configuration folder on your mirrored data partition.

4. Repeat the Step 1 and Step 2 on your failover server node.

5. Start the Genetec Server service on the active server node.
Prepare the script for access control

If the Access Manager role (for access control) is running on the clustered servers, a special script must be prepared for it to run properly within the clustered environment.

1. Using Notepad create a new file called script.bat.
2. Paste the following into script.bat:

   ```
   IF EXIST C:\Program Files (x86)\Genetec Security Center 5.2\VertXFileCache
       rmdir /S /Q "C:\Program Files (x86)\Genetec Security Center 5.2\VertXFileCache"
   IF EXIST C:\Program Files (x86)\Genetec Security Center 5.2\VertXTempFiles
       rmdir /S /Q "C:\Program Files (x86)\Genetec Security Center 5.2\VertXTempFiles"
   PAUSE
   
   CAUTION The code above represents the default installation path on a 64-bit server. If your installation path is different or, if you are using a 32-bit server you will need to edit the path indicated in the script.
   ```
3. Save the file script.bat in the default Security Center installation folder (C:\Program Files (x86)\Genetec Security Center 5.2\ on a 64-bit computer, or C:\Program Files\Genetec Security Center 5.2\ on a 32-bit computer).
4. Open the Failover Cluster Manager.
5. Add the script.bat file as an application as follows:
   a. Under Services and applications, right click your Windows Cluster Resource (identified with the gear icon), and then click Add a Resource > 2- Generic Application.
   b. In the Command line field in the Generic Application Settings page, type the path where you saved the script.bat file in Step 3, and the name of the script.bat file.
      
      C:\Program Files (x86)\Genetec Security Center 5.2\script.bat on a 64-bit computer, or
      C:\Program Files\Genetec Security Center 5.2\script.bat on a 32-bit computer.
   c. Click Next > Next > Finish.
   
   Under the Other Resources section, the script Application appears as Offline.
Prepare the script for access control

d Right-click script Application, and then click Bring this resource online.
Index

C
clustering
  Windows Server failover clustering, 2
configuring
  access control scripts for Windows Server failover clustering, 15
  Genetec server for Windows Server failover clustering, 14
contacting technical support, 19

D
demo license, acquiring, 19
document information, ii
documentation. See production documentation

L
licensing, 19

P
product documentation, about, 18

S
server requirements
  Windows Server failover clustering, 5
system setup
  Windows Server failover clustering, 3

T
technical support, contacting, 19

W
Windows Server failover clustering
  about, 2
  configuring
    access control scripts, 15
    Genetec server, 14
  prerequisites
    planning checklist, 6
    preparing servers, 10
    server requirements, 5
    system setup, 3
  supported roles, 4
  terminology, 4
Where to find product documentation

You can find our product documentation in the following locations:

- **Installation package.** The documentation is available in the Documentation folder of the installation package. Some of the documents also have a direct download link to the latest version of the document.

- **Genetec Technical Assistance Portal (GTAP).** The latest version of the documentation is available from the GTAP Documents page. Note, you’ll need a username and password to log on to GTAP.

- **Help.** Security Center client and web-based applications include help, which explain how the product works and provide instructions on how to use the product features. Patroller and the Sharp Portal also include context-sensitive help for each screen. 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 Genetec customer, you have access to the Genetec Technical Assistance Portal (GTAP), where you can find information and search for answers to your product questions.

- **Genetec Technical Assistance Portal (GTAP).** GTAP is a support website that provides in-depth support information, such as FAQs, knowledge base articles, user guides, supported device lists, training videos, product tools, and much more. Prior to contacting GTAC or opening a support case, it is important to look at this website for potential fixes, workarounds, or known issues. You can log in to GTAP or sign up at [https://gtap.genetec.com](https://gtap.genetec.com).

- **Genetec Technical Assistance Center (GTAC).** If you cannot find your answers on GTAP, you can open a support case online at [https://gtap.genetec.com](https://gtap.genetec.com). For GTAC’s contact information in your region see the Contact page at [https://gtap.genetec.com](https://gtap.genetec.com).

**NOTE** Before contacting GTAC, please have your System ID (available from the About button in your client application) and your SMA contract number (if applicable) ready.

- **Licensing.**
  - For license activations or resets, please contact GTAC at [https://gtap.genetec.com](https://gtap.genetec.com).
  - 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).

Additional resources

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

- **GTAP Forum.** The Forum is an easy to use message board that allows clients and Genetec staff to communicate with each other and discuss a variety of topics, ranging from technical questions to technology tips. You can log in or sign up at [https://gtapforum.genetec.com](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/Services](http://www.genetec.com/Services).